

アクセス・インテグレーター・サービス



## AIS 機構の使用と構成 バージョン 3.3



アクセス・インテグレーター・サービス



## AIS 機構の使用と構成 バージョン 3.3

お願い

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

本書は、IBM アクセス・インテグレーター・サービスのバージョン 3.3 に適用されます。また、新版や TNL で特に指示がない限り、以降のリリースや修正レベルにも適用されます。

本マニュアルについてご意見やご感想がありましたら

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

からお送りください。今後の参考にさせていただきます。

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

<http://www.infocr.co.jp/ifc/books/>

をご覧ください。（URL は、変更になる場合があります）

原 典： SC30-3989-01  
Access Integration Services  
Using and Configuring Features  
Version 3.3

発 行： 日本アイ・ビー・エム株式会社

担 当： ナショナル・ランゲージ・サポート

第1刷 1999.8

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

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

© Copyright International Business Machines Corporation 1994, 1999. All rights reserved.

Translation: © Copyright IBM Japan 1999



# 目次

図	xvii
表	xix
特記事項	xxi
本書のオンライン・バージョンのご使用条件	xxiii
商標	xxv
まえがき	xxvii
本書の対象読者	xxvii
ソフトウェアについて	xxvii
本書における表記法	xxviii
ライブラリーの概説	xxix
IBM 2212 ソフトウェア・ライブラリーの変更の要約	xxx
ヘルプの入手	xxxi
下位レベル操作環境の終了	xxxii
<b>第1章 帯域幅予約および優先待ち行列の使用</b>	<b>1</b>
帯域幅予約システム	1
フレーム・リレー上の帯域幅予約	3
待ち行列化のサポート	4
廃棄可能性	4
トラフィック・クラス処理のためのデフォルト回線定義	5
BRS の VOFR 用構成	5
優先待ち行列	6
帯域幅予約なしの優先待ち行列	6
トラフィック・クラスの構成	7
BRS とフィルター	8
MAC アドレス・フィルターとタグ	8
TCP/UDP ポート番号フィルター	9
IPv4 TOS ビット・フィルター	9
IP 保護トンネルおよび 2 次フラグメント内の SNA トラフィック用の IP バージョン 4 優先順位ビット処理の使用	10
ブリッジ・トラフィックの SNA および APPN フィルター	12
フィルターの優先順位	13
サンプル構成	13
フレーム・リレー回線のトラフィック・クラス処理にデフォルト回線定義を使用する場合	13
<b>第2章 帯域幅予約の構成および監視</b>	<b>21</b>
帯域幅予約構成の概説	21
帯域幅予約の構成コマンド	22
Activate-IP-precedence-filtering	26
Add-circuit-class	26
Add-class	26
Assign	28
Assign-circuit	30
Change-circuit-class	31

Change-class . . . . .	31
Circuit . . . . .	31
Clear-block . . . . .	32
Create-super-class . . . . .	32
Deactivate-IP-precedence-filtering . . . . .	33
Deassign . . . . .	33
Deassign-circuit . . . . .	33
Default-circuit-class . . . . .	33
Del-circuit-class . . . . .	34
Default-class . . . . .	34
Del-class . . . . .	34
Disable . . . . .	35
Disable-hpr-over-ip-port-numbers . . . . .	35
Enable . . . . .	35
Enable-hpr-over-ip-port-numbers . . . . .	36
Interface . . . . .	37
List . . . . .	38
Queue-length . . . . .	40
Set-circuit-defaults . . . . .	41
Show . . . . .	41
Tag . . . . .	42
Untag . . . . .	43
Use-circuit-defaults . . . . .	43
帯域幅予約監視プロンプトへのアクセス . . . . .	43
帯域幅予約監視コマンド . . . . .	44
Circuit . . . . .	45
Clear . . . . .	45
Clear-Circuit-Class . . . . .	45
Counters . . . . .	46
Counters-circuit-class . . . . .	46
Interface . . . . .	47
Last . . . . .	47
Last-circuit-class . . . . .	47
<b>第3章 MAC フィルターの使用 . . . . .</b>	<b>49</b>
MAC フィルターと DLSw トラフィック . . . . .	49
MAC フィルター・パラメーター . . . . .	50
フィルター項目パラメーター . . . . .	50
フィルター・リスト・パラメーター . . . . .	50
フィルター・パラメーター . . . . .	51
MAC フィルター・タグの使用 . . . . .	51
<b>第4章 MAC フィルターの構成および監視 . . . . .</b>	<b>53</b>
MAC フィルター構成プロンプトへのアクセス . . . . .	53
MAC フィルター構成コマンド . . . . .	53
Attach . . . . .	54
Create . . . . .	54
Default . . . . .	55
Delete . . . . .	55
Detach . . . . .	56
Disable . . . . .	56
Enable . . . . .	56

List	57
Move.	57
Reinit.	57
Set-Cache	58
Update	58
更新サブコマンド	58
Add	59
Delete	60
List	60
Move.	61
Set-Action	61
MAC フィルター監視プロンプトへのアクセス	61
MAC フィルター監視コマンド	62
Clear	62
Disable	63
Enable	63
List	63
Reinit.	64
<b>第5章 WAN 復元の使用</b>	<b>65</b>
WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローの概説	65
WAN 復元	65
WAN 再ルート	66
ダイヤル・オン・オーバーフロー	67
始める前に	67
WAN 復元の構成手順	68
2 次ダイヤル回線の構成	69
<b>第6章 WAN 復元の構成および監視</b>	<b>71</b>
WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローの構成コマンド	71
Add	71
Disable	73
Enable	74
List	75
Remove	75
Set	76
WAN 復元インターフェース監視プロセスへのアクセス	79
WAN 復元監視コマンド	79
Clear	80
Disable	80
Enable	81
Set	82
List	85
<b>第7章 WAN 再ルート・フィーチャー</b>	<b>91</b>
WAN 再ルートの概説	91
ダイヤル・オン・オーバーフロー	92
WAN 再ルートの構成	93
サンプル WAN 再ルート構成	93
<b>第8章 ネットワーク・ディスパッチャー・フィーチャーの使用</b>	<b>99</b>
ネットワーク・ディスパッチャーの概説	99

ネットワーク・ディスパッチャーの使用による TCP および UDP トラフィックの バランシング . . . . .	100
ネットワーク・ディスパッチャーの高可用性 . . . . .	101
障害の検出 . . . . .	103
データベースの同期 . . . . .	103
回復方法 . . . . .	103
IP 引き継ぎ . . . . .	103
ネットワーク・ディスパッチャーの構成 . . . . .	104
構成ステップ . . . . .	106
TN3270 でのネットワーク・ディスパッチャーの使用 . . . . .	111
構成の要点 . . . . .	112
明示的な LU とネットワーク・ディスパッチャー . . . . .	113
Web サーバー・キャッシュでのネットワーク・ディスパッチャーの使用 . . . . .	113
eNetwork ホスト・オンデマンド・クライアント・キャッシュでのネットワーク ・ディスパッチャーの使用 . . . . .	113
スケーラブル高可用性キャッシュ (SHAC) でのネットワーク・ディスパッチャ ーの使用 . . . . .	114
<b>第9章 ネットワーク・ディスパッチャー・フィーチャーの構成および監視</b> . . . . .	117
ネットワーク・ディスパッチャー構成コマンドへのアクセス . . . . .	117
ネットワーク・ディスパッチャー構成コマンド . . . . .	117
Add . . . . .	118
Clear . . . . .	124
Disable . . . . .	125
Enable . . . . .	126
List . . . . .	127
Remove . . . . .	129
Set . . . . .	131
ネットワーク・ディスパッチャー監視コマンドへのアクセス . . . . .	137
ネットワーク・ディスパッチャー監視コマンド . . . . .	137
List . . . . .	138
Quiesce . . . . .	139
Report . . . . .	140
Status . . . . .	141
Switchover . . . . .	144
Unquiesce . . . . .	144
<b>第10章 IBM eNetwork ホスト・オンデマンド・クライアント・キャッシュの   構成と監視</b> . . . . .	145
ホスト・オンデマンド・クライアント・キャッシュの構成 . . . . .	145
ホスト・オンデマンド・クライアント・キャッシュ構成環境へのアクセス . . . . .	149
ホスト・オンデマンド・クライアント・キャッシュのコマンド . . . . .	149
Activate . . . . .	150
Add . . . . .	150
Delete . . . . .	150
List . . . . .	151
Modify . . . . .	152
ホスト・オンデマンド・クライアント・キャッシュ監視環境へのアクセス . . . . .	153
ホスト・オンデマンド・クライアント・キャッシュ監視コマンド . . . . .	153
Activate . . . . .	154
Clear . . . . .	154
Enable . . . . .	155

Delete . . . . .	155
Disable. . . . .	155
List . . . . .	156
Modify. . . . .	158
<b>第11章 Web サーバー・キャッシュの使用 . . . . .</b>	<b>159</b>
Web サーバー・キャッシュの概説 . . . . .	159
キャッシュ . . . . .	161
HTTP プロキシの使用 . . . . .	164
スケーラブル高可用性キャッシュ . . . . .	165
外部キャッシュ制御マネージャーの概要 . . . . .	169
依存関係テーブル . . . . .	169
外部キャッシュ制御プロトコル . . . . .	170
外部キャッシュ制御プロトコル (ECCP) のベクトル形式 . . . . .	173
<b>第12章 Web サーバー・キャッシュの構成と監視 . . . . .</b>	<b>201</b>
Web サーバー・キャッシュの構成 . . . . .	201
Web サーバー・キャッシュ環境へのアクセス . . . . .	207
Web サーバー・キャッシュのコマンド . . . . .	207
Activate . . . . .	208
Add. . . . .	208
Delete . . . . .	209
List . . . . .	210
Modify. . . . .	211
Web サーバー・キャッシュ監視環境へのアクセス . . . . .	214
Web サーバー・キャッシュ監視コマンド . . . . .	215
Activate . . . . .	215
Clear . . . . .	216
Enable . . . . .	216
Delete . . . . .	216
Disable. . . . .	217
List . . . . .	217
Modify. . . . .	220
<b>第13章 コード化サブシステムの構成と監視 . . . . .</b>	<b>221</b>
コード化サブシステムの構成 . . . . .	221
List . . . . .	222
Set . . . . .	222
コード化サブシステムの監視 . . . . .	223
List . . . . .	224
<b>第14章 データ圧縮の構成と監視 . . . . .</b>	<b>229</b>
データ圧縮の概説 . . . . .	229
データ圧縮の概念 . . . . .	229
データ圧縮の基本 . . . . .	230
考慮事項 . . . . .	232
PPP リンクのデータ圧縮の構成と監視 . . . . .	234
PPP リンクのデータ圧縮の構成 . . . . .	234
PPP リンクのデータ圧縮の監視 . . . . .	236
フレーム・リレー・リンクのデータ圧縮の構成と監視 . . . . .	237
フレーム・リレー・リンクのデータ圧縮の構成 . . . . .	237
フレーム・リレー・リンクのデータ圧縮の監視 . . . . .	239
例: フレーム・リレー・インターフェースまたは回線上の圧縮の監視 . . . . .	239

<b>第15章 ローカルまたはリモート認証の使用</b>	241
認証、許可、および会計 (AAA) セキュリティー	241
AAA セキュリティーとは	241
PPP の使用	242
有効な PPP セキュリティー・プロトコル	242
ログインの使用	243
有効なログイン / 管理セキュリティ・プロトコル	244
トンネルの使用	244
有効なトンネル・セキュリティ・プロトコル	244
パスワード規則	245
認証サーバーとは	245
SecurID サポート	246
<b>第16章 認証の構成</b>	249
認証構成プロンプトへのアクセス	249
認証構成コマンド	249
Disable	249
List	250
Login	251
Nets-info	253
Password-rules	253
PPP	255
Servers	257
Set	260
Tunnel	261
User-profiles	263
<b>第17章 暗号化プロトコルの使用および構成</b>	269
暗号化制御プロトコルを使用した PPP の暗号化	269
PPP の ECP 暗号化の構成	269
PPP の ECP 暗号化の監視	270
Microsoft ポイントツーポイント暗号化 (MPPE)	271
MPPE の構成	271
MPPE の監視	272
フレーム・リレー・インターフェース上の暗号化の構成	272
フレーム・リレー・インターフェース上の暗号化の監視	273
<b>第18章 ポリシー機能の使用</b>	275
ポリシーの概説	275
ポリシーの決定と実施	275
ポリシー・オブジェクト	278
LDAP とポリシー・データベースの対話	283
ポリシー・スキーマ	285
規則の生成	287
構成例	288
QOS を指定した IPSec/ISAKMP ポリシー	288
IPSec/ISAKMP だけのポリシー	297
すべての公衆トラフィックをドロップする (フィルター規則)	300
LDAP ポリシー検索エンジンの構成と使用可能化	303
<b>第19章 ポリシー機能の構成と監視</b>	307
ポリシー構成プロンプトへのアクセス	307
ポリシー構成コマンド	307

Add . . . . .	308
Change. . . . .	321
Copy . . . . .	321
Delete . . . . .	321
Disable. . . . .	321
Enable . . . . .	321
List . . . . .	321
LDAP ポリシー・サーバー構成コマンド . . . . .	322
Disable LDAP . . . . .	322
Enable LDAP . . . . .	322
Set Default-Policy . . . . .	323
Set LDAP . . . . .	325
Set Refresh . . . . .	326
ポリシー監視プロンプトへのアクセス . . . . .	327
ポリシー監視コマンド . . . . .	327
Disable. . . . .	327
Enable . . . . .	328
Reset . . . . .	328
Search . . . . .	328
Status . . . . .	329
List . . . . .	329
Test. . . . .	330
<b>第20章 IP セキュリティーの使用 . . . . .</b>	<b>333</b>
IP セキュリティーの概説. . . . .	333
保護トンネルの使用. . . . .	333
IP セキュリティーの概念. . . . .	334
IP セキュリティー用語 . . . . .	334
IP 認証ヘッダー . . . . .	336
IP カプセル化セキュリティ・ペイロード . . . . .	337
AH と ESP の使用 . . . . .	337
セキュリティ・アソシエーション. . . . .	338
トンネル・モードとトランスポート・モード . . . . .	338
トンネル内トンネル・モード . . . . .	341
パス最大伝送単位ディスカバリー. . . . .	341
IP セキュリティー・トンネルを使用したネットワークの図 . . . . .	342
インターネット・キー交換の使用. . . . .	343
インターネット・キー交換フェーズ. . . . .	344
IP セキュリティー・トンネルのネゴシエーション . . . . .	345
公開キー・インフラストラクチャーの使用 . . . . .	346
PKI の構成 . . . . .	346
手動 IP セキュリティーの使用 (IPv4) . . . . .	350
手動 IP セキュリティーの使用 (IPv6) . . . . .	350
<b>第21章 IP セキュリティーの構成および監視 . . . . .</b>	<b>351</b>
インターネット・キー交換の構成 (IPv4) . . . . .	351
公開キー・インフラストラクチャーの構成 (IPv4). . . . .	352
証明書の取得 . . . . .	352
公開キー・インフラストラクチャー構成コマンド . . . . .	353
Add. . . . .	353
Change. . . . .	353
Delete . . . . .	354

List . . . . .	354
手動 IP セキュリティーの構成 (IPv4) . . . . .	355
アルゴリズムの構成 . . . . .	356
暗号化キーの構成 . . . . .	356
IP セキュリティー構成環境へのアクセス . . . . .	356
手動 IP セキュリティー構成コマンド . . . . .	357
Add Tunnel . . . . .	357
Change Tunnel . . . . .	362
Delete Tunnel . . . . .	363
Disable . . . . .	363
Enable . . . . .	364
List . . . . .	364
Set . . . . .	365
手動トンネルの構成 (IPv4) . . . . .	366
ルーター A のトンネルの構成 . . . . .	366
ルーター B のトンネルの構成 . . . . .	366
例: ESP を使用した IP セキュリティー・トンネルの手動構成 . . . . .	366
例: ESP と ESP-NULL を使用した IP セキュリティー・トンネルの手動構成 . . . . .	367
手動 IP セキュリティーの構成 (IPv6) . . . . .	367
アルゴリズムの構成 . . . . .	368
暗号化キーの構成 . . . . .	368
IP セキュリティー構成環境へのアクセス . . . . .	368
手動 IP セキュリティー構成コマンド . . . . .	368
手動トンネルの構成 (IPv6) . . . . .	369
ルーター A の IP セキュリティー・トンネルの作成 . . . . .	369
ルーター A のパケット・フィルターの構成 . . . . .	369
ルーター A のパケット・フィルター・アクセス制御規則の構成 . . . . .	370
ルーター A の IP セキュリティーと IP のリセット . . . . .	370
ルーター B の IP セキュリティー・トンネルの作成 . . . . .	371
ルーター B のパケット・フィルターの構成 . . . . .	371
ルーター B のパケット・フィルター・アクセス制御規則の構成 . . . . .	371
ルーター B の IP セキュリティーと IPv6 のリセット . . . . .	372
例: ESP を使用した IP セキュリティー・トンネルの構成 . . . . .	372
例: ESP と ESP-NULL を使用した IP セキュリティー・トンネルの構成 . . . . .	372
手動 IP セキュリティーの監視 (IPv4) . . . . .	373
インターネット・キー交換環境へのアクセス . . . . .	373
インターネット・キー交換監視コマンド . . . . .	373
公開キー・インフラストラクチャー環境へのアクセス (IPv4) . . . . .	375
公開キー・インフラストラクチャー監視コマンド . . . . .	375
IP セキュリティー監視環境へのアクセス (IPv4) . . . . .	377
IP セキュリティー監視コマンド (IPv4) . . . . .	378
手動 IP セキュリティーの監視 (IPv6) . . . . .	383
IP セキュリティー監視環境へのアクセス . . . . .	383
IP セキュリティー監視コマンド (IPv6) . . . . .	384
<b>第22章 差別化サービス機能の使用 . . . . .</b>	<b>385</b>
差別化サービスの概説 . . . . .	385
差別化サービスの用語 . . . . .	388
差別化サービスの構成 . . . . .	388
<b>第23章 差別化サービスの構成と監視 . . . . .</b>	<b>391</b>



差別化サービス構成プロンプトへのアクセス	391
差別化サービス構成コマンド	391
Delete	392
Disable	392
Enable	392
List	393
Set	393
差別化サービス監視環境へのアクセス	396
差別化サービス監視コマンド	396
Clear	396
DScache	397
List	398
<b>第24章 レイヤー 2 トンネルの使用 (L2TP、PPTP、L2F)</b>	<b>403</b>
L2TP の概説	403
L2TP の用語	404
サポートされるフィーチャー	405
タイミングに関する考慮事項	406
LCP に関する考慮事項	407
レイヤー 2 トンネルの構成	407
<b>第25章 レイヤー 2 トンネル・プロトコルの構成と監視</b>	<b>413</b>
L2T インターフェース構成プロンプトへのアクセス	413
L2 トンネル・インターフェース構成コマンド	413
Disable	414
Enable	414
Encapsulator	414
List	414
Set	415
L2 トンネル機能構成プロンプトへのアクセス	415
L2 トンネル機能構成コマンド	416
Add	416
Disable	417
Enable	418
Encapsulator	419
List	419
Set	419
L2 トンネル監視プロンプトへのアクセス	421
L2 トンネル監視コマンド	421
Call	421
Kill	424
Memory	424
Start	425
Stop	425
Tunnel	425
<b>第26章 ネットワーク・アドレス変換の使用</b>	<b>429</b>
ネットワーク・アドレス・ポート変換	431
静的アドレス・マッピング	431
NAT 静的アドレス・マッピング	431
NAPT 静的アドレス・マッピング	431
NAT 用のパケット・フィルターおよびアクセス制御規則の設定	432

例: IP フィルターとアクセス制御規則をもつ NAT の構成 . . . . .	432
<b>第27章 ネットワーク・アドレス変換の構成および監視 . . . . .</b>	<b>437</b>
ネットワーク・アドレス変換の構成環境へのアクセス . . . . .	437
ネットワーク・アドレス変換構成コマンド . . . . .	437
Change. . . . .	438
Delete . . . . .	438
Disable. . . . .	439
Enable . . . . .	439
List . . . . .	439
Map. . . . .	440
Reserve . . . . .	441
Reset . . . . .	443
Set . . . . .	443
Translate . . . . .	444
ネットワーク・アドレス変換監視環境へのアクセス . . . . .	444
ネットワーク・アドレス変換監視コマンド . . . . .	445
List . . . . .	445
Reset . . . . .	446
<b>第28章 LAN へのダイヤルイン・アクセス (DIALs) サーバーの使用 . . . . .</b>	<b>447</b>
ダイヤルイン・アクセスを使用する前に . . . . .	449
ダイヤルイン・アクセスの構成 . . . . .	449
ダイヤルイン・インターフェースの構成 . . . . .	449
ダイヤルアウト・インターフェースを構成する前に . . . . .	452
ヌル・モデムの使用. . . . .	452
ダイヤルアウト・インターフェースの構成 . . . . .	452
グローバル DIALs パラメーターを構成する前に . . . . .	454
サーバー提供の IP アドレス . . . . .	454
動的ホスト構成プロトコル (DHCP) . . . . .	455
動的ドメイン名サーバー (DDNS). . . . .	457
<b>第29章 DIALs の構成. . . . .</b>	<b>459</b>
DIALs グローバル構成環境へのアクセス . . . . .	459
DIALs グローバル構成コマンド . . . . .	459
Add. . . . .	460
Delete . . . . .	461
Disable. . . . .	461
Enable . . . . .	462
List . . . . .	463
Set . . . . .	465
DIALs グローバル監視環境へのアクセス . . . . .	468
DIALs グローバル監視コマンド . . . . .	468
Clear . . . . .	468
List . . . . .	469
Reset . . . . .	471
ダイヤルアウト・インターフェース構成コマンド . . . . .	471
Set . . . . .	472
ダイヤルイン・インターフェースの監視 . . . . .	472
ダイヤルアウト・インターフェースの監視 . . . . .	472
Clear . . . . .	472
List . . . . .	473

<b>第30章 DHCP サーバーの使用</b>	475
DHCP の概要	475
DHCP の動作	475
リースの更新	477
クライアントの移動	477
サーバー・オプションの変更	477
DHCP サーバーの数	478
1 台の DHCP サーバー	478
複数の DHCP サーバー	478
BOOTP サーバー	479
特殊な DHCP クライアント	479
リース時間	480
概念と用語	480
DHCP サーバーとリースのパラメーター	483
DHCP オプション	483
オプションの形式	483
クライアントに対して提供されている基本オプション	485
ホストに対する IP レイヤー・パラメーターのオプション	488
インターフェースに対する IP レイヤー・パラメーターのオプション	489
インターフェースに対するリンク・レイヤー・パラメーターのオプション	489
TCP パラメーター・オプション	490
アプリケーションおよびサービス・パラメーターのオプション	490
DHCP 拡張オプション	492
IBM 固有のオプション	495
ベンダー・オプション	496
DHCP 用の IP の構成	496
IP アドレスの追加	497
IP シンプル・インターネット・アクセスの使用	497
DHCP サーバーのサンプル構成	498
ASCII テキスト・ファイル	498
OPCON (Talk 6) 構成	499
<b>第31章 DHCP サーバーの構成と監視</b>	503
DHCP サーバー構成環境へのアクセス	503
DHCP サーバー構成コマンド	503
Add	504
Change	510
Delete	514
Disable	518
Enable	518
List	519
Set	525
DHCP サーバー監視環境へのアクセス	533
DHCP サーバー監視コマンド	533
Disable	534
Enable	534
List	534
Reset	534
Request	535
<b>第32章 シン・サーバー・フィーチャーの使用</b>	539
ネットワーク・ステーションの概説	539

シン・サーバー・フィーチャーの概説 . . . . .	540
BootP/DHCP サポート . . . . .	541
ネットワーク・ステーションとの通信に使用するプロトコル . . . . .	542
RFS の使用 . . . . .	542
TFTP の使用 . . . . .	542
NFS の使用 . . . . .	543
ファイル・キャッシュの更新 . . . . .	543
シン・サーバー環境の構成 . . . . .	543
構成に関する推奨事項 . . . . .	544
BootP/DHCP サーバーの構成 . . . . .	545
シン・サーバー環境用のサーバーの構成 . . . . .	545
BootP リレーの構成 . . . . .	545
内部 IP アドレスの構成 . . . . .	546
TSF の構成 . . . . .	546
サンプル構成 . . . . .	546
AS/400 の構成 . . . . .	546
IBM 2212 (TSF) の構成 . . . . .	548
<b>第33章 シン・サーバー機能の構成および監視 . . . . .</b>	<b>553</b>
TSF 構成環境へのアクセス . . . . .	553
TSF 構成コマンド . . . . .	553
Add . . . . .	553
Delete . . . . .	559
List . . . . .	559
Modify . . . . .	560
Set . . . . .	561
TSF 監視環境へのアクセス . . . . .	562
TSF 監視コマンド . . . . .	562
Delete . . . . .	563
Flush . . . . .	563
List . . . . .	563
Refresh . . . . .	567
Reset . . . . .	567
Restart . . . . .	567
Set . . . . .	567
<b>第34章 VCRM の構成および監視 . . . . .</b>	<b>569</b>
VCRM 構成環境へのアクセス . . . . .	569
VCRM 監視環境へのアクセス . . . . .	569
VCRM 監視コマンド . . . . .	570
Clear . . . . .	570
Queue . . . . .	570
<b>第35章 音声アダプターの使用 . . . . .</b>	<b>573</b>
音声アダプターの概説 . . . . .	573
2212 音声ポートと通信するための Nuera F200 の構成 . . . . .	574
ダイヤル・プランの構成 . . . . .	576
Nuera F200 と通信するための 2212 音声ポートの構成 . . . . .	577
Nuera F200 を使用しない通信 . . . . .	578
2212 間の通信 . . . . .	578
ローカル・コール・ルーティング . . . . .	578
<b>第36章 音声アダプターの構成と監視 . . . . .</b>	<b>579</b>

音声機能構成環境へのアクセス	579
音声アダプター構成コマンド	579
Add	580
Delete	583
List	583
Modify	585
Reorder-Call-Rule	585
Set	586
音声ネットワーク構成コマンド	589
List	589
Set	590
音声アダプター監視環境へのアクセス	592
音声アダプター監視コマンド	592
Calls	593
Status	595
Trace Call	596
付録. リモート AAA 属性	597
Radius	597
キーワード	597
TACACS+	598
略語集	601
用語集	611
索引	643





1. PPP BRS トラフィック・クラスとトラフィック・クラス優先待ち行列の関係	2
2. フレーム・リレー BRS 回線クラスとトラフィック・クラスの関係	2
3. WAN 再ルート	92
4. サンプル WAN 再ルート構成	94
5. 1 つのクラスターと 2 つのポートを持つように構成されたネットワーク・ ディスパッチャーの例	104
6. 3 つのクラスターと 3 つの URL を持つように構成されたネットワーク・ ディスパッチャーの例	105
7. 3 つのクラスターと 3 つのポートを持つように構成されたネットワーク・ ディスパッチャーの例	106
8. 高可用性ネットワーク・ディスパッチャー構成	107
9. 2 つのキャッシュと、ネットワーク・ディスパッチャー、クライアント、 およびバックエンド・サーバー	115
10. Web サーバー・キャッシュを使用しないネットワーク・ディスパッチャー	160
11. キャッシュ・ヒットがない場合の Web サーバー・キャッシュを使用した ネットワーク・ディスパッチャー	160
12. キャッシュ・ヒットがある場合の Web サーバー・キャッシュを使用した ネットワーク・ディスパッチャー	161
13. キャッシュ要求が検出された場合	166
14. 要求が担当のキャッシュに転送される場合	167
15. 要求がバックエンド・サーバーに転送される場合	167
16. 要求が担当のキャッシュに転送され、検出されなかった場合	168
17. コマンド応答ベクトル	174
18. サブベクトルの形式	178
19. サブフィールドの形式	196
20. データ・ディクショナリーを使用した双方向データ圧縮の例	232
21. PPP リンク上の圧縮の構成例	235
22. PPP インターフェースの圧縮の監視	237
23. フレーム・リレー・リンクの圧縮の構成例	238
24. SecurID ユーザー名とパスコード	246
25. SecurID パスコードと次のトークン	246
26. IP パケットのフローとポリシー・データベース	276
27. ポリシー構成オブジェクトの関係	283
28. インターネットを経由するトラフィックの保護	285
29. ポリシー・スキーマの構造	286
30. QOS を指定した IPSec/ISAKMP の構成	289
31. IPSec の構成と前の定義の再利用	297
32. HMAC MD5 認証メッセージの作成	337
33. AH によって保護されたデータグラムの形式	339
34. ESP によって保護されたデータグラムの形式	339
35. AH トンネル内での ESP のネスト	340
36. IPSec によって保護された L2TP パケット	340
37. IPSec と NAT を使用したネットワーク	343
38. DiffServ データ・パケットのパス	385
39. バッファ、待ち行列、およびスケジューラーの関係	387
40. L2TP ネットワークの例	404
41. NAT を実行するネットワーク	430
42. NAT を実行するネットワーク	433

43.	ダイヤルインをサポートする DIALs サーバーの例 . . . . .	448
44.	ダイヤルアウトをサポートする DIALs サーバーの例 . . . . .	449
45.	ダイヤルイン・インターフェースの追加 . . . . .	451
46.	スコープの概念 . . . . .	481
47.	シン・サーバーのないリモート・ネットワーク・ステーション . . . . .	541
48.	シン・サーバーのあるリモート・ネットワーク・ステーション . . . . .	541
49.	TSF サンプル構成 . . . . .	546
50.	F200 と 2212 音声ポートの通信 . . . . .	574
51.	音声ポートのコール処理情報の構成 . . . . .	575



# 一 表

1. 帯域幅予約構成コマンドの要約 (BRS Config> プロンプトから利用可能)	22
2. フレーム・リレー・インターフェースの BRS [i #] Config> プロンプトから利用可能な構成コマンド	24
3. BRS トラフィック・クラス処理コマンド	24
4. 帯域幅予約監視コマンドの要約	44
5. MAC フィルター構成コマンドの要約	53
6. 更新サブコマンドの要約	58
7. MAC フィルター監視コマンドの要約	62
8. WAN 復元構成コマンドの要約	71
9. WAN 復元監視コマンド	79
10. ディスパッチャーのループバック装置の別名指定用のコマンド	110
11. 各種オペレーティング・システムのルート削除コマンド	111
12. ネットワーク・ディスパッチャー構成コマンド	117
13. アドバイザー名とポート番号	118
14. パラメーター構成の制限	124
15. ネットワーク・ディスパッチャー監視コマンド	137
16. ホスト・オンデマンド・クライアント・キャッシュ構成コマンドの要約	149
17. ホスト・オンデマンド・クライアント・キャッシュ監視コマンドの要約	153
18. Web サーバー・キャッシュの構成コマンドの要約	207
19. Web サーバー・キャッシュ監視コマンドの一覧	215
20. ES 構成コマンド	222
21. ES 監視コマンド	223
22. PPP データ圧縮構成コマンド	235
23. PPP データ圧縮監視コマンド	236
24. データ圧縮構成コマンド	238
25. フレーム・リレー・データ圧縮監視コマンド	239
26. PPP セキュリティー・プロトコルの設定	242
27. ログイン・セキュリティ・プロトコルの設定	244
28. トンネル・セキュリティ・プロトコルの設定	245
29. 認証構成コマンド	249
30. ログイン・サブコマンド	251
31. ログイン・サブコマンド	253
32. PPP サブコマンド	255
33. サーバー・サブコマンド	257
34. トンネル・サブコマンド	261
35. ユーザー・プロファイル構成コマンド	263
36. IKE フェーズ 1 照会と、戻される決定	277
37. IKE フェーズ 2 照会と、戻される決定	278
38. ポリシー構成コマンド	307
39. LDAP 構成コマンド	322
40. ポリシー監視コマンド	327
41. 各種のトンネル・ポリシーを使用して構成されたアルゴリズム	356
42. IP セキュリティー構成コマンドの要約	357
43. 各種のトンネル・ポリシーを使用して構成されたアルゴリズム	368
44. IKE 監視コマンドの一覧	373
45. PKI 監視コマンドの一覧	375
46. IP セキュリティー監視コマンドの要約	378
47. DiffServ 構成コマンド	391

	48. DiffServ 監視コマンド . . . . .	396
	49. L2 トンネル・インターフェース構成コマンド . . . . .	413
	50. L2 トンネル機能構成コマンド . . . . .	416
	51. L2 トンネル監視コマンド . . . . .	421
	52. NAT 構成コマンド . . . . .	437
	53. NAT 監視コマンド . . . . .	445
	54. DIALs グローバル構成コマンド . . . . .	459
	55. DIALs グローバル監視コマンド . . . . .	468
	56. ダイアルアウト・インターフェース構成コマンド . . . . .	471
	57. ダイアルアウト・インターフェース監視コマンド . . . . .	472
	58. DHCP サーバー構成コマンドの要約 . . . . .	503
	59. DHCP サーバー監視コマンドの要約 . . . . .	533
	60. TSF 構成コマンドの要約 . . . . .	553
	61. TSF 監視コマンドの要約 . . . . .	562
	62. VCRM 監視コマンド . . . . .	570
	63. 音声構成コマンドの要約 . . . . .	579
	64. 音声ポート・コマンドの要約 . . . . .	589
	65. 音声アダプター監視コマンドの要約 . . . . .	592

---

## 特記事項

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

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

〒106-0032 東京都港区六本木3丁目2-31

AP事業所

IBM World Trade Asia Corporation

Intellectual Property Law & Licensing

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

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



---

## 本書のオンライン・バージョンのご使用条件

弊社は、お客様に対して以下のことを許諾します。

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

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



---

## 商標

次の用語は、米国あるいはその他の国々における IBM Corporation の商標です。

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

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

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

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





---

## まえがき

本書には、ルーター・ユーザー・インターフェースを使用して IBM 2212 に導入されたフィーチャーを構成および操作するのに必要な情報が記載されています。本書で説明しているフィーチャーが、どの IBM 2212 でもサポートされるわけではありません。装置特定のフィーチャーの場合は、次でそのことを示しています。

- 該当する章またはそこで記載されている内容の注記
- 「まえがき」の中の、サポートするフィーチャーおよび装置を表示している個所

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

---

## 本書の対象読者

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

**追加情報の入手:** 資料が印刷された後に変更が行われる場合もあります。追加情報をご利用いただける場合、または資料の印刷後に変更が必要になった場合は、構成プログラム・ディスクットのディスクット 1 のファイル (README という名前のファイル) に変更内容を収めてあります。このファイルは、ASCII テキスト・エディターを使用してご覧ください。

---

## ソフトウェアについて

IBM アクセス・インテグレーター・サービスは、IBM 2212 (ライセンス・プログラム番号 5639-F73) をサポートするソフトウェアです。このソフトウェアには、次に挙げる構成要素が含まれています。

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

基本コードは工場ですべて 2212 に導入済みです。

- IBM アクセス・インテグレーター・サービス用構成プログラム (本書では、構成プログラムと呼んでいます)。これは、独立型ワークステーションから装置を構成す

ることを可能にするグラフィカル・ユーザー・インターフェースです。構成プログラムにはエラー検査およびオンライン・ヘルプ情報が含まれます。

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

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

---

## 本書における表記法

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

1. コマンドの省略形は、次のように下線を引いて表示しています。

```
reload
```

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

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

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

パラメーターの値として、キーワードの 1 つを選択してください。

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

```
time host ...
```

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

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

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

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

5. キーボードのキーの組み合わせは、次のように表示します。

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

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

6. キーボードのキーの名前は、次のように表示します。例: **Enter**

7. 変数 (すなわち、ユーザーが定義するデータを表すのに使用される名前) は、イタリック体で表示します。たとえば、次のように入力します。

```
File Name: filename.ext
```

---

## ライブラリーの概説

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

<http://www.networking.ibm.com/2212/2212prod.html>

次のリストは、IBM 2212 ライブラリーの資料を作業別に並べています。

### 計画

#### **GA27-4215**

*IBM 2212 入門と計画の手引き*

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

### 導入

#### **GA88-6572**

*IBM 2212 アクセス・ユーティリティー 導入および初期構成の手引き*

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

#### **GX27-4048**

*2212 Hardware Configuration Quick Reference*

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

### 診断および保守

#### **GY27-0362**

*IBM 2212 Access Utility Service and Maintenance Manual*

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

### 運用およびネットワーク管理

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

#### **SD88-6062**

*ソフトウェア使用者の手引き*

この資料では、次を説明しています。

- アクセス・インテグレーター・サービスソフトウェアの構成、監視、および使用。
- アクセス・インテグレーター・サービス コマンド行ルーター・ユーザー・インターフェースを使用しての、IBM 2212 と共に出荷されるネットワーク・インターフェースおよびリンク・レイヤー・プロトコルの構成および監視。

### SD88-6063

AIS 機構の使用と構成

### SD88-6064

プロトコル構成および監視 参照資料 第 1 巻

### SD88-6065

プロトコル構成および監視 参照資料 第 2 巻

これらの資料は、アクセス・インテグレーター・サービスのコマンド行ルーター・ユーザー・インターフェースにアクセスし、これを使用して、本製品に同梱されているルーティング・プロトコル・ソフトウェアを監視および構成する方法を説明しています。

装置がサポートする各プロトコルに関する情報も含まれています。

### SC88-6373

イベント・ログ・システム・メッセージの手引き

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

### 構成

#### GC88-6657

マルチプロトコル/アクセス・サービス製品 構成プログラム 使用者の手引き

この資料は、構成プログラムの使用方法について説明しています。

### 安全性

#### SD21-0030

*Caution: Safety Information--Read This First*

この資料は IBM 2212 に同梱されており、IBM 2212 の導入および保守作業に適用される注意と危険についての注意書きが収められています。

### 製品情報

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

この IBM Web ページは、ワールド・ワイド・ウェブ (WWW) を通して製品情報を提供しています。

---

## IBM 2212 ソフトウェア・ライブラリーの変更の要約

次のリストは、バージョン 3.3 で行われた変更の内容を示しています。変更の内容は、次のとおりです。

#### • 新しい機能

- コード化サブシステム (ES)
- 動的ホスト構成プロトコル (DHCP) サービス
- バーチャル私設ネットワーク (VPN)
  - ディレクトリー・サービス: LDAP のサポート
  - ISAKMP/Oakley のサポート
  - レイヤー 2 転送 (L2F)
  - ポイントツーポイント・トンネル・プロトコル (PPTP)

- 差別化サービス
- フレーム・リレー CIR、Bc、および Be に対する最高 J2 6 Mbps のサポート。
- フレーム・リレーを経由した音声
- フレーム・リレー・パケット断片化
- フレーム・リレーを経由した音声パケットの転送
- WAN の高度なサポート
- デジタル・モデム・アダプター用の ISDN 信号方式
- 拡張機能
  - IP の拡張機能
    - 汎用 IPv4 ルーティング・ポリシー
    - IPv6 パケット・フィルター、動的構成、および DHCP リレー・エージェントのサポート
  - SDLC の拡張機能
    - 1 次グループ・ポーリング
    - 両方向同時通信
  - ルーター内の待ち行列に入れる非セッション・メッセージの数を制御できるようにする DLSw 構成パラメーター
  - シン・サーバー機能のパフォーマンス強化
  - TN3270 の拡張機能
    - IBM eNetwork ホスト・オンデマンド・クライアント・キャッシュ
    - ホストによって開始される動的 LU 定義
    - DLSw を介した複数の PU SA
  - ブリッジングの機能強化
    - IPX SR-TB のサポート
  - X.25 動的構成のサポート
  - IPX の機能強化
    - 構成可能 RIP ティック
    - フレーム・リレー SVC を介した IPXWAN
  - コマンド行インターフェースのコマンド補完機能
  - ハイパフォーマンス・システム・カードでの Web サーバー・キャッシュのサポート (外部キャッシュ・マネージャー、高可用性とスケーラビリティの強化など)
- 変更個所の表示
 

本書で加えられた技術上の変更個所には、左側の欄外に縦線 (|) を引いて示してあります。

---

## ヘルプの入手

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

## 下位レベル操作環境の終了

ソフトウェアは複数レベルの構造になっているので、2212 を構成または操作するときには、2 次、3 次、およびさらに下位レベルの環境に入ります。すぐ上のレベルに戻るためには、**exit** コマンドを入力します。2 次レベルに達するためには、2 次レベルのプロンプト (Config> または +) が得られるまで繰り返し **exit** を入力します。

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

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

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

---

## 第1章 帯域幅予約および優先待ち行列の使用

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

- 『帯域幅予約システム』
- 3ページの『フレーム・リレー上の帯域幅予約』
- 6ページの『優先待ち行列』
- 8ページの『BRS とフィルター』
- 13ページの『サンプル構成』

---

### 帯域幅予約システム

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

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

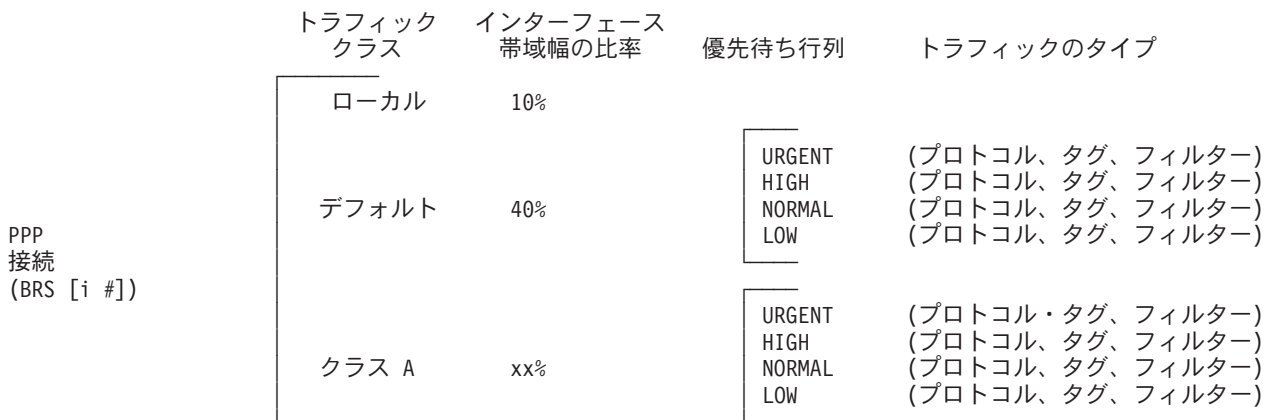
PPP インターフェースでは、トラフィック・クラス (t-classes) を定義し、各トラフィック・クラスに PPP インターフェースの帯域幅の比率を割り振ります。少なくとも 2 種類のトラフィック・クラスがあります。

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

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

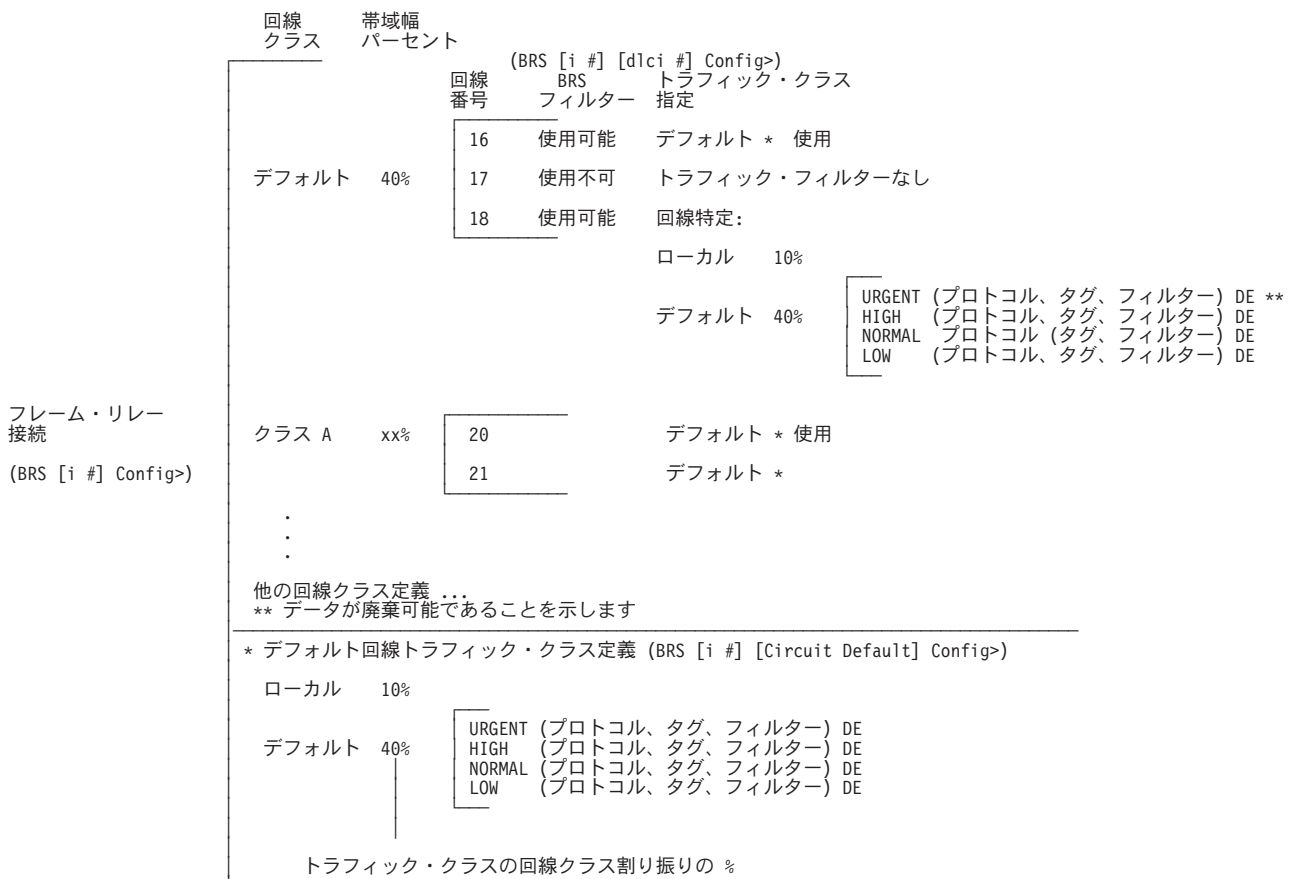
フレーム・リレー・インターフェースでは、回線クラス (c-classes) を定義し、各回線クラスに、フレーム・リレー・インターフェースの帯域幅の比率を割り振ります。少なくとも 1 つの回線クラス (DEFAULT 回線クラス) が存在し、すべての回線が最初はこのクラスに割り当てられます。ユーザーは追加の回線クラスを作成し、それらの回線クラス (c-classes) に回線を割り当てることができます。各フレーム・リレー回線では、トラフィック・クラス (t-classes) を定義し、各トラフィック・クラスに、そのフレーム・リレーの帯域幅の比率を割り振ることができます。フレーム・リレー回線のトラ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

## BRS および優先待ち行列の使用



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

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



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

図 2. フレーム・リレー BRS 回線クラスとトラフィック・クラスの関係



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

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

帯域幅予約は、次の接続タイプ上で実行されます。

- フレーム・リレー (シリアル・ラインまたはダイヤル回線インターフェース)
- PPP (シリアル・ラインまたはダイヤル回線インターフェース)

---

## フレーム・リレー上の帯域幅予約

帯域幅予約は、2 つのレベルで帯域幅を予約することができます。

- インターフェース・レベルでは、インターフェースの帯域幅の比率を回線クラス (*c-classes*) に割り当てることができます。各回線クラスには、1 つまたは複数の回線が含まれます。
- 回線レベルでは、トラフィック・クラス (*t-class*) を定義し、回線の帯域幅の比率を割り振ることができます。( **create-super-class** コマンドによって作成されたトラフィック・クラスは、帯域幅とは関連がありませんが、回線に対して定義された他の *t-class* すべてに優先されます。)

BRS がフレーム・リレーからパケットを受信すると、構成された *c-class* と *t-class* が使用されて、パケットをいつ送信するかが決定されます。BRS は、*c-class*、回線、*t-class*、および *t-class* 内の優先順位を基準にして、パケットを待ち行列化します。回線が割り当てられた *c-class* は、*c-class* の待ち行列に入れられ、*c-class* の待ち行列は適切に重みを考慮した待ち行列化アルゴリズムに従ってソートされます。*c-class* 内では、送信するパケットのある回線はラウンドロビン方式によってサービスを受けます。それぞれの *c-class* 内にある *t-class* も、適切に重みを考慮した待ち行列化アルゴリズムに従ってソートされます。*t-class* 内で、パケットは優先順位 (緊急、高、通常、低) に従ってさらに待ち行列化されます。

パケットは、次の基準をすべて満たすと待ち行列から削除され、送信されます。

1. 次の *c-class* にある次のパケットである
2. その *c-class* 内の次の回線にある次のパケットである
3. その *c-class* に属する次の *t-class* 内のパケットの 1 つである
4. その *t-class* に属する次に優先順位が高いグループ内の次のパケットである

BRS に対してインターフェースと回線を使用可能にして、*c-class* と *t-class* を構成しなければ、回線はすべてデフォルトと呼ばれる 1 つの *c-class* に割り当てられます。この構成を使用すると、*c-class* の待ち行列にはデフォルト *c-class* だけが存在し、送

## BRS および優先待ち行列の使用

信するパケットのある c-class 内の回線はそれぞれラウンドロビン順に処理されます。BRS をこのように動作させたい場合は、すべての回線をそのままデフォルト c-class に入れておき、他の回線クラスは作成しません。

孤立した回線と、BRS を明示的に使用可能にしていない回線は、すべての環境でこのデフォルト BRS 待ち行列化環境を使用します。BRS は、これらの回線にデフォルト c-class を割り当てます。

BRS を構成するには、次の手順に従ってください。

1. インターフェースに対して BRS を使用可能にする。
2. 回線に対して BRS を使用可能にし、c-class を追加する。
3. c-class に回線を割り当てる。
4. 必要に応じ、それぞれの c-class に対して t-class を定義する。

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

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

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

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

## 待ち行列化のサポート

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

## 廃棄可能性

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

## トラフィック・クラス処理のためのデフォルト回線定義

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

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

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

## BRS の VOFR 用構成

専用回線を通じて、音声フレームを伝送できます。この場合は、インターフェースと回線に対して BRS を使用可能にし、音声に関連した回線にはデフォルト値をそのまま使用します。複数の c-class を作成して、音声専用の回線は比率の大きい帯域幅と関連付けた c-class に割り当て、データに関連した回線は比率の小さい帯域幅と関連付けた回線クラスに割り当てることができます。

音声とその他のトラフィックが両方とも同じ回線を経由して伝送される場合は、インターフェースと回線に対して BRS を使用します。一部の回線を優先せずに、すべての回線がラウンドロビン方式でサービスを受けるようにする場合は、デフォルト c-class のほかに追加の c-class を作成しないとよいでしょう。この場合、音声とデータを両方とも伝送するそれぞれの回線ごとに、**create-super-class** コマンドを使用して t-class を作成し、このクラスに VOFR トラフィックを割り当てておくことをお勧めします。必要に応じて追加の t-class も作成し、これらの t-class に他のタイプのトラフィックを割り当てます。この構成によって、音声トラフィックが他のトラフィックすべてに優先されるようになり、断片化が使用可能になっている場合は、断片化されたデータ・セグメント間にセグメント化されない音声フレームをインターリーブできます。音声とデータを同じインターフェース経由で送信する場合は、フレーム・リレー・インターフェースで断片化を使用可能にしておくことをお勧めします。断片化によってフレームが小さくなるので、連続する音声フレーム間の遅延も少なくなります。

## BRS および優先待ち行列の使用

断片化を使用可能にする方法については、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の“フレーム・リレー・インターフェースの構成および監視” の章にある **enable fragmentation** コマンドを参照してください。

---

## 優先待ち行列

帯域幅予約は、指定されたトラフィック・クラス (*t-classes*) に対して、接続の総帯域幅の比率を割り振ります。他のすべての *t-class* より高い優先順位をもつ

**create-super-class** コマンドによって作成された *t-class* を除き、BRS の *t-class* は帯域幅の比率に関連付けられます。プロトコルとフィルター・データを *t-class* に割り当てることができ、*t-class* 内の特定の優先待ち行列に割り当てることができます。優先待ち行列を使用すれば、トラフィック・クラス内の特定の待ち行列に、設定値を指定してプロトコルまたはフィルターを割り当てることができます。BRS の *t-class* は、同じ名前によって識別されるパケットの集まりです。たとえば、“ipx” という名前のクラスは、すべての IPX パケットを表します。

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

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

優先順位は、ユーザーが指定したトラフィック・クラス (*t-class*) に割り当てられます。

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

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

BRS の場合、PPP およびフレーム・リレー WAN 接続の優先待ち行列の長さを設定することができます。**queue-length** コマンドの説明は、40ページの『Queue-length』を参照してください。

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

## 帯域幅予約なしの優先待ち行列

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

## トラフィック・クラスの構成

**add-class** コマンドを使用してトラフィック・クラスを作成し、次に **assign** コマンドを使用して、そのクラスにトラフィックのタイプを割り当てます。トラフィックは、そのプロトコル・タイプに基づいて、あるいは特定のタイプのプロトコル・トラフィックを識別する (たとえば、SNMP IP パケット) フィルターに基づいて、トラフィック・クラスに割り当てられます。

サポートされるプロトコル・タイプは、次のとおりです。

- IP
- ARP
- DNA
- VINES
- IPX
- OSI
- VOFR
- AP2
- ASRT
- SNA/APPN-ISR
- APPN-HPR
- HPR/IP

## BRS フィルター

帯域幅予約を使用すると、特定のプロトコル・トラフィックを、同じプロトコル・タイプを使用する他のトラフィックとは異なる扱いにすることができます。たとえば、SNMP IP トラフィックを、他の IP トラフィックとは異なるトラフィック・クラスおよび優先順位に割り当てるといったことが可能です。この例では、特定のプロトコル・トラフィックをフィルターに掛ける (つまり、固有に識別する) ので、SNMP は BRS フィルターです。IP、ASRT (ブリッジング)、および APPN-HPR プロトコルのトラフィックを帯域幅予約によってフィルターに掛けることができます。次のフィルターがサポートされています。

- IP トンネル伝送
- IP 経由の SDLC トンネル伝送 (SDLC リレー)
- IP 経由の BSC トンネル伝送 (BSC リレー)
- Rlogin
- Telnet
- SNA/APPN-ISR
- APPN-HPR
- SNMP
- IP マルチキャスト
- DLSw
- MAC フィルター
- NetBIOS
- Network-HPR
- High-HPR
- Medium-HPR
- Low-HPR
- XTP



## BRS および優先待ち行列の使用

- TCP/UDP ポート番号またはソケット
- TOS バイト
- 優先順位ビット

---

## BRS とフィルター

ここでは、BRS を各種のフィルターと共に使用方法について説明します。

### MAC アドレス・フィルターとタグ

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

タグ付けプロセスは、MAC フィルター構成コンソールでフィルター項目を作成し、それにタグ番号を割り当てることによって行われます。このタグ番号は、このタグに対応するすべてのパケットのトラフィック・クラスを設定するのに使用されます。タグ値は、現在は 1 ~ 64 の範囲でなければなりません。MAC フィルターについて詳しくは、49ページの『第3章 MAC フィルターの使用』を参照してください。

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

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

タグは、IP トンネルの例に見られるように、“グループ”とも呼ばれます。IP トンネルのエンドポイントは、任意の数のグループに属することができます。パケットは、MAC アドレス・フィルターのタグ付けフィーチャーによって、特定のグループに割り当てられます。MAC フィルターについての追加情報は、49ページの『第3章 MAC フィルターの使用』および 53ページの『第4章 MAC フィルターの構成および監視』を参照してください。

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

1. filter config> プロンプトで MAC フィルター構成コマンドを使用して、ブリッジを通過するパケットのタグを設定する。詳しくは、49ページの『第3章 MAC フィルターの使用』を参照してください。
2. 帯域幅予約 tag コマンドを使用して、帯域幅予約のタグを参照する。

3. 帯域幅予約 **assign** コマンドを使用して、BRS タグを t-class に割り当てる。  
**assign** コマンドは、その BRS t-class 内の待ち行列優先順位も指定するように求めるプロンプトを出します。

## TCP/UDP ポート番号フィルター

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

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

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

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

## IPv4 TOS ビット・フィルター

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

## BRS および優先待ち行列の使用

このフィルターは、TOS バイトの高位 3 ビットだけを対象とする BRS IPv4 優先順位フィルターよりも広範な用途に使用できます。BRS TOS ビット・フィルター・サポートは、TOS ビットを設定するための IP アクセス制御サポートと組み合わせて使用すると、保護トンネル経由で転送されるトラフィック (断片化されている)、あるいは BRS UDP および TCP ポート番号フィルター・サポートでは識別できないトラフィックをフィルター処理することが可能になります。IP アクセス制御サポートは、BRS IPv4 優先順位ビット・フィルターに対応した APPN のハードコーディング優先順位ビット値を使用せずに、TOS ビット値をユーザー定義の値に設定することも可能にします。したがって、BRS IPv4 優先順位ビット・フィルターの代わりに、IP アクセス制御および BRS TOS フィルター・サポートをご使用になることをお勧めします。

13ページの『フィルターの優先順位』で説明しているように、TOS フィルターの一致は、IPv4 優先順位ビット・フィルターおよびその他の IP 特定フィルターより先に検査されます。TOS1 フィルターから始めて、TOS1 ~ TOS5 フィルターの一致が順次に検査されます。最大 5 つの TOS フィルターを定義することができます。

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

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

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

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

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

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



## BRS および優先待ち行列の使用

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

次の 3 種類のトラフィックは、IPv4 優先順位値 '011'b にマップされます。

- APPN/HPR が IP を介してルートされるときに送信される APPN/HPR XID トラフィック
- DLSw トラフィック
- TN3270 トラフィック

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

- SNA/APPN-ISR (APPN/HPR XID 交換に使用される)
- DLSw
- Telnet

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

TN3270 トラフィックが、クライアントによって、BRS が使用可能な広域ネットワークを介して 2212 に送信される場合、クライアントが優先順位ビットを '011'b に設定していない限り、BRS はクライアントからのトラフィックに優先順位を付けることはできません。

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

1. BRS では、BRS が IPv4 優先順位ビットに基づいてフィルター処理する必要があるかどうかを構成します。BRS は、IP 保護トンネル伝送パケット、または TCP および UDP 2 次フラグメント・パケットに対してだけ、このタイプのフィルター処理を実行します。
2. DLSw、IP 経由 HPR、および TN3270 を構成する場合、これらのプロトコル・タイプのそれぞれについて、2212 が発信するパケットに対して IPv4 優先順位ビットを設定する必要があるかどうかを指定します。

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

1. BRS で IPv4 優先順位フィルターをアクティブにする。

## BRS および優先待ち行列の使用

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

## ブリッジ・トラフィックの SNA および APPN フィルター

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

**注:** フレーム・リレー BAN パケットが、このカテゴリに入ります。

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

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

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

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

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

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

## フィルタの優先順位

1 つのパケットが複数の BRS フィルタ・タイプに一致することもあり得ます。たとえば、SNA が入っている IP トンネル伝送ブリッジ・パケットは、IP トンネル伝送フィルタと SNA/APPN-ISR フィルタに一致する可能性があります。パケットが BRS フィルタ・タイプに一致するかどうかを判別するときのフィルタの評価順序は、次のとおりです。

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

注: 括弧内は、フィルタが適用されるプロトコルです。

---

## サンプル構成

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

注:

- 1** 機能 BRS を構成します。
- 2** インターフェース 1 の BRS を使用可能にします。
- 3** 回線 16、17、18 の BRS を使用可能にします。これらの回線では、トラフィック・クラス処理のデフォルト回線定義が使用されます。
- 4** トラフィック・クラス処理のデフォルト回線定義を定義するために set-circuit-defaults メニューにアクセスします。

## BRS および優先待ち行列の使用

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

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

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

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

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

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

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

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

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

default class is DEFAULT

BRS [i 1] Config>?
ENABLE
DISABLE
SET-CIRCUIT-DEFAULTS
```

```

CIRCUIT
ADD-CIRCUIT-CLASS
DEL-CIRCUIT-CLASS
CHANGE-CIRCUIT-CLASS
DEFAULT-CIRCUIT-CLASS
ASSIGN-CIRCUIT
DEASSIGN-CIRCUIT
QUEUE-LENGTH
LIST
SHOW
CLEAR-BLOCK
EXIT
BRS [i 1] Config>set-circuit-defaults 4
BRS [i 1] [circuit defaults] Config>?
ADD-CLASS
DEL-CLASS
CHANGE-CLASS
DEFAULT-CLASS
TAG
UNTAG
ASSIGN
DEASSIGN
LIST
EXIT
BRS [i 1] [circuit defaults] Config>add 5
Class name [DEFAULT]?DEF1
Percent bandwidth to reserve [10]? 5
BRS [i 1] [circuit defaults] Config>add
Class name [DEFAULT]?DEF2
Percent bandwidth to reserve [10]?5
BRS [i 1] [circuit defaults] Config>assign ip
Class name [DEFAULT]?DEF1
Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
Frame Relay Discard Eligible <NO/YES> [NO]?
BRS [i 1] [circuit defaults] Config>assign asrt
Class name [DEFAULT]? DEF2
Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
Frame Relay Discard Eligible <NO/YES> [NO]?
BRS[i 1] [circuit defaults] Config>list

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

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

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

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

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

assigned tags:

default class is DEFAULT with priority NORMAL

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

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 16 using defaults.

```

## BRS および優先待ち行列の使用

```
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 4

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

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

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

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

assigned tags:

default class is DEFAULT with priority NORMAL
```

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

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

```
protocol and filter assignments:
```

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

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

```
BRS [i 1] Config>circuit 17
```

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

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

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

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



```

protocol OSI with default priority is not discard eligible
protocol VOFR with default priority is not discard eligible
protocol AP2 with default priority is not discard eligible

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

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

assigned tags:

default class is DEFAULT with priority NORMAL

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

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

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

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

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

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

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

assigned tags:

default class is DEFAULT with priority NORMAL

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

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

```

## BRS および優先待ち行列の使用

protocol and filter assignments:

Protocol/Filter	Class	Priority	Discard Eligible
IP	DEF1	NORMAL	NO
ARP	DEFAULT	NORMAL	NO
DNA	DEFAULT	NORMAL	NO
VINES	CIRC171	NORMAL	NO
IPX	DEFAULT	NORMAL	NO
OSI	DEFAULT	NORMAL	NO
VOFR	DEFAULT	NORMAL	NO
AP2	DEFAULT	NORMAL	NO
ASRT	DEF2	NORMAL	NO

```
BRS [i 1] [dlci 17] Config>exit
BRS [i 1] Config>set-circuit-defaults
BRS [i 1] [circuit defaults] Config>change DEF1 3
Percent bandwidth to reserve [ 5]? 10
BRS [i 1] [circuit defaults] Config>change DEF2
Percent bandwidth to reserve [5]? 10
BRS [i 1] [circuit defaults] Config>list
```

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

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

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

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

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

assigned tags:

```
default class is DEFAULT with priority NORMAL
```

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

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

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

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



```

    protocol AP2 with default priority is not discard eligible

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

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

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 1] [dlci 16] Config>exit
BRS [i 1] Config>circuit 17
BRS [i 1] [dlci 17] Config>list

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

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

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

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

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

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

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 1] [dlci 17] Config>use-circuit-defaults 9
This circuit is currently NOT using circuit defaults...
Are you sure you want to delete current definitions and use defaults ? (Yes or
[No]): yes
Defaults are in effect for this circuit.
Please reload router for this command to take effect.
BRS [i 1] [dlci 17] Config>
*restart
Are you sure you want to reload the gateway? (Yes or [No] ):yes
*t 6
Gateway user configuration
Config>feature brs
Bandwidth Reservation User Configuration
BRS Config>interface 1
BRS [i 1] Config>circuit 17
BRS [i 1] [dlci 17] Config>list

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

```

## BRS および優先待ち行列の使用

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

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

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

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

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

assigned tags:

default class is DEFAULT with priority NORMAL

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

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

protocol and filter assignments:
```

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

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

## 第2章 帯域幅予約の構成および監視

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

この章には、次の内容が記載されています。

- 『帯域幅予約構成の概説』
- 22ページの『帯域幅予約の構成コマンド』
- 43ページの『帯域幅予約監視プロンプトへのアクセス』
- 44ページの『帯域幅予約監視コマンド』

### 帯域幅予約構成の概説

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

1. OPCON (\*) プロンプトで **talk 6** と入力する。
2. Config> プロンプトで **feature brs** と入力する。
3. BRS Config> プロンプトで **interface #** と入力する。
4. BRS [i 0] Config> プロンプトで **enable** と入力する。

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

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

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

- a. BRS [i 0] Config> プロンプトで **circuit #** と入力する。ただし、# は構成する回線の番号です。
  - b. BRS [i 0] [dlci 16] Config> プロンプトで **enable** と入力する。これは回線プロンプト・レベルで、この例では、回線 (DLCI) 番号は 16 です。
  - c. BRS [i 0] [dlci 16] Config> プロンプトで **exit** と入力して、インターフェース・レベル・プロンプトに戻る。
  - d. BRS t-classes を定義したい各回線ごとに、ステップ 4a ~ 4c を繰り返します。
5. ルーターをReload する。
  6. 使用可能にした特定のインターフェースに対して帯域幅予約を構成するために、ステップ 1 ~ 3 を繰り返します。
  7. PPP インターフェースの BRS を構成している場合は、BRS[i 0]Config> プロンプトで、24ページの表3 に示されている構成コマンドを使用して、トラフィック・クラスを構成し、そのトラフィック・クラスにプロトコル、フィルター、およびタグを割り当てます。FR インターフェースの BRS を構成している場合は、ステップ 8 ~ 10 に従います。

## BRS の構成

- FR インターフェースの BRS を構成している場合は、24ページの表2 に示されているコマンドを使用して、回線クラスを構成し、その回線クラスに回線を割り当てることができます。
- デフォルトの回線定義を使用したい場合は、BRS[i 0]Config> プロンプトで **set-circuit-defaults** コマンドを入力します。これにより BRS[i 0][circuit defaults] プロンプトが表示されるので、ここで 24ページの表3 から該当するコマンドを使用して、トラフィック・クラスを構成し、そのトラフィック・クラスにプロトコル、フィルター、およびタグを割り当てることができます。トラフィック・クラス処理のデフォルト回線定義を定義する作業が完了したら、“exit” と入力して、BRS[i 0] Config> プロンプトに戻ります。
- トラフィック・クラス処理のデフォルト回線定義を使用できない FR 回線がある場合には、**circuit permanent-virtual-circuit circuit\_number** と入力します。これで回線プロンプトにアクセスできるので、ここから 24ページの表3 に示されたコマンドを使用して、トラフィック・クラス処理の回線特定の定義を作成します。

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

**talk 6 (t 6)** コマンドは、構成プロセスにアクセスします。

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

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

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

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

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

---

## 帯域幅予約の構成コマンド

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

表 1. 帯域幅予約構成コマンドの要約 (BRS Config&gt; プロンプトから利用可能)

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

## BRS と優先待ち行列の構成

表2. フレーム・リレー・インターフェースの BRS [i #] Config> プロンプトから利用可能な構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxiiページの『ヘルプの入手』を参照してください。
Add-circuit-class	帯域幅 c-class の名前とその帯域幅の比率を設定します。
Assign-circuit	指定された回線を指定された帯域幅 c-class に割り当てます。
Change-circuit-class	帯域幅 c-class に構成された帯域幅の量を変更します。
Circuit	BRS 回線レベル・プロンプト (BRS [i x][dlci y] Config>) にアクセスします。ここから 表3 に示されたコマンドを使用して、フレーム・リレー回線上の帯域幅予約を構成することができます。
Clear-block	現行インターフェースに関連した構成データを SRAM から消去します。回線クラス構成データおよびトラフィック・クラスのデフォルト回線定義が消去されます。
Deassign-circuit	指定された回線をデフォルトの c-class に復元します。
Default-circuit-class	デフォルト帯域幅 c-class の名前とそのインターフェース帯域幅の比率を設定します。
Del-circuit-class	指定された帯域幅 c-class を削除します。
Disable	インターフェース上の帯域幅予約を使用不可にします。
Enable	インターフェース上の帯域幅予約を使用可能にします。
List	c-classes と割り当てられた回線定義を SRAM から表示します。
Queue-length	優先待ち行列内のパケット数の最大値と最小値を設定します。
Set-circuit-defaults	BRS [i x] [circuit defaults] Config> コマンド・プロンプトにアクセスし、表3 から該当するコマンドを使用して、トラフィック・クラス処理のデフォルト回線定義を作成できるようにします。
Show	現在定義されている c-classes と、割り当てられている回線を、SRAM から表示します。
Exit	直前のコマンド・レベルに戻ります。xxxiiページの『下位レベル操作環境の終了』を参照してください。

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

表3. BRS トラフィック・クラス処理コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxiiページの『ヘルプの入手』を参照してください。
Add-class	指定された量の帯域幅をユーザー定義のトラフィック・クラスに割り当てます。
Create-super-class	スーパークラス と呼ばれる t-class を定義します。
Assign	プロトコルまたはフィルターを、構成されたトラフィック・クラスに割り当てます。
Change-class	帯域幅 t-class に対して構成された帯域幅の量を変更します。
Clear-block	PPP インターフェースまたはフレーム・リレー回線のトラフィック・クラスとプロトコル、フィルター、およびタグ割り当て構成データを、SRAM から消去します。 注: このコマンドは BRS [i x] [circuit defaults] Config> プロンプトからは使用できません。
Deassign	指定されたパケットまたはフィルターの待ち行列化を、デフォルトの t-class と優先順位に復元します。



表 3. BRS トラフィック・クラス処理コマンド (続き)

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

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

**注:**

1. BRS インターフェース・メニュー内から **clear-block**、**disable**、**enable**、**list**、および **show** コマンドを出すと、選択されたインターフェースに構成されている帯域幅予約情報に影響を与えたり、表示したりします。BRS 回線メニュー内からこれらのコマンドを出した場合は、パーマネント・パーチャル・サーキット (PVC) に構成されているフレーム・リレー帯域幅予約情報にだけ影響を与えたり、表示したりします。
2. 帯域幅予約コマンドを使用する前に、次のことを念頭に入れてください。
  - 他の構成コマンドを使用する前に、**interface** コマンドを使用して、インターフェースを選択しておくことが必要です。(BRS 構成は、これを強制的に要求します。)

## BRS と優先待ち行列の構成

- *Class-name* パラメーターは、大文字小文字の区別をします。
  - 現行の *class-names* を見たい場合は、**list** または **show** コマンドを使用します。
  - インターフェースまたは回線上の帯域幅予約を使用可能にした後は、回線およびトラフィック・クラスを追加/削除/変更したり、回線またはプロトコルを動的に割り当てたりすることができます。有効にするためにルーターを再ロードする必要があるコマンドは、**enable**、**disable**、**use-circuit-defaults**、および **clear-block** コマンドだけです。
3. **t-class** および **c-class** 構成変更を有効にするために、ルーターを再ロードする必要はありません。

## Activate-IP-precedence-filtering

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

構文:

**activate-ip-precedence-filtering**

## Add-circuit-class

注: フレーム・リレーの構成時にだけ使用されます。

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

構文:

**add-circuit-class** *class-name* %

## Add-class

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

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



構文:

```
add-class [class-name or class#] %
```

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

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

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

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

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

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

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

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

assigned tags:

default class is DEFAULT with priority NORMAL
```

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

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

BRS [i 2] [dlci 128]>list

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

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

class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
```

## BRS と優先待ち行列の構成

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

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

assigned tags:

default class is DEFAULT with priority NORMAL

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

## Assign

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

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

**注:** VOFR プロトコルは、フレーム・リレー・インターフェースを経由して音声パケットを送信する場合に使用されます。回線が音声パケットだけを伝送する場合は、回線に t-class を 1 つだけ割り当て、プロトコルを VOFR に指定します。割り当てることができる t-class は 1 つだけです。これは、t-class が 1 つならば別のものに対する優先順位がないからです。複数の t-class がある場合、音声を伝送しない t-class が帯域幅を制御して、音声トラフィックの伝送に干渉する可能性があります。音声トラフィックが即時に送信されるようにするために、VOFR トラフィックには優先順位 *Urgent* だけを指定する必要があります。

回線が音声とともにデータ・トラフィックも伝送する場合は、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の“フレーム・リレー・インターフェースの構成および監視”にある **enable fragmentation** コマンドで説明されている、フレーム・リレーでの断片化を回線に対して構成する必要があります。この構成は、大きなデータ・パケットが帯域幅を使い切らないようにして、音声パケットを十分な速さで通すために必要です。

**構文:**

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

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

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

## BRS と優先待ち行列の構成

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

### 例 1:

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

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

```
BRS [i 2] [dlci 128]>assign ?
IP
ARP
DNA
VINES
IPX
OSI
VOFR
AP2
ASRT
TUNNELING-IP
SDLC/BSC-IP
RLOGIN-IP
TELNET-IP
NETBIOS
SNA/APPN-ISR
SNMP-IP
MULTICAST-IP
DLSW-IP
TAG1
TAG2
TAG3
TAG4
TAG5
APPN-HPR
NETWORK-HPR
HIGH-HPR
MEDIUM-HPR
LOW-HPR
XTP-IP
UDP_TCP1
UDP_TCP2
UDP_TCP3
UDP_TCP4
UDP_TCP5
TOS1
TOS2
TOS3
TOS4
TOS5
Protocol or filter name [IP]? TOS1 1
Class name [DEFAULT]? class1 2
Priority [NORMAL]?
Frame Relay Discard Eligible [NO]?
TOS Mask [1-FF] [FF]?
TOS Range (Low) [0-FF] [0]? 1
TOS Range (High) [1]? 3
BRS [i 2] [dlci 128]> list

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

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

class DEFAULT has 40% bandwidth allocated
```

## BRS と優先待ち行列の構成

```
the following protocols and filters are assigned:
  protocol IP with default priority is not discard eligible
  protocol ARP with default priority is not discard eligible
  protocol DNA with default priority is not discard eligible
  protocol VINES with default priority is not discard eligible
  protocol IPX with default priority is not discard eligible
  protocol OSI with default priority is not discard eligible
  protocol VOFR with default priority is not discard eligible
  protocol AP2 with default priority is not discard eligible
  protocol ASRT with default priority is not discard eligible
```

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

assigned tags:

default class is DEFAULT with priority NORMAL

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

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

protocol and filter assignments:

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

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

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

## Assign-circuit

注: フレーム・リレーの構成時にだけ使用されます。

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

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

構文:

**assign-circuit** # class name

## Change-circuit-class

注: フレーム・リレーの構成時にだけ使用されます。

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

構文:

**change-circuit-class** class-name %

## Change-class

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

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

構文:

**change-class** [class-name or class#] %

## Circuit

注: フレーム・リレーの構成時にだけ使用されます。

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

構文:

**circuit**

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

**PVC の例:**

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

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

## BRS と優先待ち行列の構成

### SVC の例:

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

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

フレーム・リレー回線に対して **enable** コマンドを出し、ルーターをリスタートまたは再ロードすると、その回線に対して次の構成コマンドが利用可能になります。

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

## Clear-block

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

### 構文:

#### **clear-block**

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

### 例:

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

## Create-super-class

PPP インターフェースまたはフレーム・リレー回線に対し、スーパークラス と呼ばれる t-class を構成するには、 **create-super-class** コマンドを使用します。それぞれの PPP インターフェースまたはフレーム・リレー回線ごとに、スーパークラスを 1 つだけ構成できます。スーパークラスには、帯域幅の比率は関連付けられません。スーパークラスに割り当てられたプロトコルまたはフィルター・データは、他のすべての t-class に割り当てられたプロトコルまたはフィルター・データに優先して、PPP インターフェースまたはフレーム・リレー回線上を伝送されます。音声パケットとデータ・パケットの両方とも伝送する回線に対しては、VOFR プロトコルのスーパー

クラスを構成する必要があります。この環境では、音声を送送するためのスーパークラスを構成することによって、音声パケットが優先されるようになります。

構文:

create-super-class

## Deactivate-IP-precedence-filtering

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

構文:

deactivate-ip-precedence-filtering

## Deassign

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

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

構文:

deassign [prot-class or filter-class]

## Deassign-circuit

注: フレーム・リレーの構成時にだけ使用されます。

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

構文:

deassign-c #

## Default-circuit-class

注: フレーム・リレーの構成時にだけ使用されます。

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



## BRS と優先待ち行列の構成

構文:

**default-circuit-class** *class-name %*

## Del-circuit-class

注: フレーム・リレーの構成時にだけ使用されます。

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

構文:

**del-circuit-class** *class-name*

## Default-class

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

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

構文:

**default-cl** *[class-name or class#] priority*

## Del-class

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

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

構文:

**del-class** *[class-name or class#]*



## Disable

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

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

構文:

disable

## Disable-hpr-over-ip-port-numbers

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

構文:

disable-hpr-over-ip-port-numbers

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

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

## Enable

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

構文:

enable

注:

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

## BRS と優先待ち行列の構成

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

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

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

default class is DEFAULT

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

## Enable-hpr-over-ip-port-numbers

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

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

構文:

**enable-hpr-over-ip-port-numbers**

例:

```
BRS Config> enable-hpr-over-ip-port-numbers
XID exchange port number [12000]?
HPR net trans prio port number [12001]?
HPR high trans prio port number [12002]?
HPR medium trans prio port number [12003]?
HPR low trans prio port number [12004]?
```

### XID exchange port number

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

有効値: 1024 ~ 65535

デフォルト値: 12000

### Network priority port number

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

有効値: 1024 ~ 65535

デフォルト値: 12001

#### High exchange port number

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

有効値: 1024 ~ 65535

デフォルト値: 12002

#### Medium exchange port number

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

有効値: 1024 ~ 65535

デフォルト値: 12003

#### Low exchange port number

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

有効値: 1024 ~ 65535

デフォルト値: 12004

## Interface

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

構文:

```
interface                interface#
```

注:

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

## BRS と優先待ち行列の構成

特定のインターフェース上の帯域幅予約を使用可能にするには、BRS Config> プロンプトで、その特定プロトコルまたはフィーチャーをサポートするインターフェースの番号を入力します。これにより、この章で説明している **BRS enable** 構成コマンドを使用できるようになります。インターフェース番号を使用可能にした後、2212 をリスタートまたは再ロードして、このコマンドを有効にしてからでないと、インターフェースに他の構成変更を加えることはできません。

注:

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

## List

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

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

構文:

```
list interface#
```

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

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

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

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

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

### 例 1

```

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

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

The use of HPR over IP port numbers is disabled

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

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

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

default class is DEFAULT

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

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

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

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

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 2] Config>

```

## 例 2

```

BRS [i 1] [d1ci 17] Config>list

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

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

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

class CLASS1 has 10% bandwidth allocated
the following protocols and filters are assigned:
protocol IP with priority NORMAL is not discard eligible
protocol ARP with priority NORMAL is not discard eligible

```

## BRS と優先待ち行列の構成

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

### 例 3

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

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

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

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

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

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

assigned tags:

default class is DEFAULT with priority NORMAL

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

### 例 4

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

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

The use of HPR over IP port numbers is enabled.

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

## Queue-length

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

構文:

**queue-length** *maximum-length minimum-length*

## BRS と優先待ち行列の構成

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

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

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

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

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

## Set-circuit-defaults

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

構文:

**set-circuit-defaults**

## Show

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

構文:

**show** *interface#*

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

- BRS [i x] Config> - インターフェース番号 *x* のインターフェース・レベル・プロンプト。



## BRS と優先待ち行列の構成

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

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

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

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

### 注:

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

## Tag

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

### 構文:

```
tag mac_filter_tag#
```

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

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



## Untag

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

構文:

```
untag mac_filter_tag#
```

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

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

## Use-circuit-defaults

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

構文:

```
use-circuit-defaults
```

注:

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

例:

```
BRS [i 1] [d1ci 17] Config>use-circuit-defaults
This circuit is currently NOT using circuit defaults...
Are you sure you want to delete current definitions and use defaults ? (Yes or
[No]): y
Defaults are in effect for this circuit.
Please reload router for this command to take effect.
BRS [i 1] [d1ci 17] Config>
```

---

## 帯域幅予約監視プロンプトへのアクセス

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

1. OPCON プロンプト (\*) で **talk 5** と入力する。
2. GWCON プロンプト (+) で **feature brs.** と入力する。

## BRS の監視

3. BRS> プロンプトで **interface #** と入力する。ただし、# は監視するインターフェースの番号です。これにより、インターフェース・レベル・プロンプト BRS [i x]> が表示されます。ただし、x はインターフェース番号です。
4. フレーム・リレーの場合だけ、インターフェース・プロンプトで **circuit #** と入力して、このインターフェース上の監視する回線を指定する。  
これにより、回線レベル・プロンプト BRS [i x] [dlci y]> が表示されます。ただし、x はインターフェース番号で、y は回線番号です。
5. プロンプトで、該当する監視コマンドを入力する。（『帯域幅予約監視コマンド』を参照してください。）

**talk 5 (t 5)** コマンドは、監視プロセスにアクセスします。

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

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

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

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

帯域幅予約監視プロンプト (BRS>) にアクセスしたら、表4 に説明されている特定の監視コマンドのどれでも入力できます。

---

## 帯域幅予約監視コマンド

ここでは、帯域幅予約監視コマンドの要約を示し、個々のコマンドについて説明します。表4 は、帯域幅予約監視コマンドを示しています。使用できるコマンドは、BRS 監視プロンプト (BRS>、BRS [i x]>、または BRS [i x] [dlci y]>) によって異なります。

表4. 帯域幅予約監視コマンドの要約

コマンド	FR でだけ使用	機能
? (ヘルプ)		このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxiページの『ヘルプの入手』を参照してください。
Circuit	yes	フレーム・リレーのパーマネント・バーチャル・サーキット (PVC) の DLCI を選択します。フレーム・リレーの帯域幅予約トラフィックを監視するには、回線プロンプト・レベルにあることが必要です。
Clear		現在の t-class カウンターをクリアし、それらを <b>last</b> t-class カウンターとして保管します。カウンターはクラス別に表示されます。
Clear-circuit-class	yes	現在の c-class カウンターをクリアし、それらを <b>last</b> c-class カウンターとして保管します。カウンターはクラス別に表示されます。
Counters		現在の t-class カウンターを表示します。

表 4. 帯域幅予約監視コマンドの要約 (続き)

コマンド	FR でだけ使用	機能
Counters-circuit-class Interface	yes	現在の c-class カウンターを表示します。 監視するインターフェースを選択します。 注: このコマンドは、他の帯域幅予約監視コマンドを使用する前に入力する必要があります。
Last		最後に保管された t-class カウンターを表示します。
Last-circuit-class	yes	最後に保管された c-class カウンターを表示します。
Exit		直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

## Circuit

注: フレーム・リレーを監視するときだけに使用します。

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

構文:

**circuit** *permanent-virtual-circuit-#*

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

```
CLEAR
COUNTERS
LAST
EXIT
```

## Clear

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

構文:

**clear**

## Clear-Circuit-Class

注: フレーム・リレーを監視するときだけに使用します。

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

構文:

**clear-circuit-class**

## Counters

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

構文:

**counters**

例: **counters**

```
Bandwidth Reservation Counters
interface number 1
Class      Pkt Xmit    Bytes Xmit    Bytes Ovfl    Pkt Ovfl    Q_len
LOCAL      10           914           0           0           0
  LOW       0           0           0           0           0
  NORMAL    10          914           0           0           0
  HIGH      0           0           0           0           0
  URGENT    0           0           0           0           0
DEFAULT    55          5555          0           0           0
  LOW       0           0           0           0           0
  NORMAL    20          5020          0           0           0
  HIGH      0           0           0           0           0
  URGENT    35          535           0           0           0
CLASS_1     5           910           0           0           0
  LOW       0           0           0           0           0
  NORMAL    5           910           0           0           0
  HIGH      0           0           0           0           0
  URGENT    0           0           0           0           0
CLASS_2     70          4123          0           0           0
  LOW       10          617           0           0           0
  NORMAL    55          3117          0           0           0
  HIGH      0           0           0           0           0
  URGENT    5           389           0           0           0
TOTAL      140         11502         0           0
```

**Bytes Ovfl**

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

**Pkt Ovfl**

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

**Q\_len** それぞれのトラフィック・クラスの中で、それぞれの優先待ち行列にあって送信を待機しているパケットの現在の数。

**Counters-circuit-class**

注: フレーム・リレーを監視するときだけに使用します。

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

構文:

**counters-circuit-class**

例: **counters-circuit-class**

```
Bandwidth Reservation Circuit Class Counters
Interface 1
```

Class	Pkt Xmit	Bytes Xmit	Bytes Ovf1
DEFAULT	25	3402	26
CIRCLASS1	1	56	0
CIRCLASS2	0	0	0
TOTAL	26	3458	26

## Interface

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

構文:

```
interface interface#
```

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

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

## Last

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

構文:

```
last
```

## Last-circuit-class

注: フレーム・リレーを監視するときだけに使用します。

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

構文:

```
last-circuit-class
```



---

## 第3章 MAC フィルターの使用

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

- 『MAC フィルターと DLSw トラフィック』
- 50ページの『MAC フィルター・パラメーター』

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

注: MAC フィルターはトンネル・トラフィックにも適用できます。

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

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

MAC フィルターは、次の 3 つのオブジェクトから構成されます。

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

---

## MAC フィルターと DLSw トラフィック

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

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

次の例では、Bridge Net 番号は 7 です。

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

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

### MAC フィルター・パラメーター

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

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

### フィルター項目パラメーター

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

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

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

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

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

### フィルター・リスト・パラメーター

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

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

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

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



## フィルター・パラメーター

次のパラメーターは、フィルターを構成するのに使用されます。

- フィルター・リスト名: *ASCII-string 1 . . . ASCII-string n*
- インターフェース番号: *IFC-number*
- ポート方向: INPUT または OUTPUT
- デフォルト・アクション: INCLUDE、EXCLUDE、または TAG
- デフォルト・タグ: *tag-value*

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

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

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

## MAC フィルター・タグの使用

MAC フィルター・タグの使用法のいくつかを次に説明します。

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

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



---

## 第4章 MAC フィルターの構成および監視

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

- 61ページの『MAC フィルター監視プロンプトへのアクセス』
- 62ページの『MAC フィルター監視コマンド』

---

### MAC フィルター構成プロンプトへのアクセス

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

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

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

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

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

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

---

### MAC フィルター構成コマンド

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

次のコマンドを使用して、MAC フィルター・フィーチャーを構成します。

表 5. MAC フィルター構成コマンドの要約

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

## MAC フィルターの構成

表 5. MAC フィルター構成コマンドの要約 (続き)

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

## Attach

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

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

構文:

**attach** *filter-list-name filter-number*

## Create

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

構文:

**create** *list filter-list-name*  
*filter [input or output] interface-number*

**list** *filter-list-name*

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

**filter [input or output] interface-number**

フィルターを作成し、それをインターフェース番号で指定されたインターフェース上の INPUT または OUTPUT 方向に対応するネットワークに置きます。デフォルトでは、このフィルターはフィルター項目を付けずに作成され、デフォルト・アクションは INCLUDE であり、ENABLED にされます。

**Default**

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

構文:

```
default                exclude filter-number
                        include filter-number
                        tag tag-number filter-number
```

**exclude filter-number**

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

**include filter-number**

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

**tag tag-number filter-number**

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

**Delete**

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

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

構文:

```
delete                list filter-list
                        filter filter-number
```

**list filter-list**

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

## MAC フィルターの構成

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

**filter** *filter-number*

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

## Detach

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

構文:

**detach** *filter-list-name filter-number*

## Disable

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

構文:

**disable** *all*  
*filter filter-number*

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

**filter** *filter-number*

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

## Enable

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

構文:

**enable** *all*  
*filter filter-number*

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

**filter** *filter-number*

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

## List

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

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

さらに、各フィルターについて、次の情報が表示されます。

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

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

構文:

```
list                                all
                                     filter filter-number
```

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

**filter** *filter-number*

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

## Move

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

構文:

```
move                                filter-list-name1 filter-list-name2 filter-number
```

## Reinit

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

構文:

```
reinit
```

## MAC フィルターの構成

### Set-Cache

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

構文:

**set-cache** *cache-size filter-number*

### Update

**update** コマンドは、特定のフィルター・リストを情報を追加または削除するのに使用します。必要なフィルター・リスト名を指定してこのコマンドを使用すると、その特定フィルター・リストの `Filter filter-list-name Config>` プロンプトが表示されます。こうして表示された新たなプロンプトから、指定されたリストの情報を変更することができます。

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

構文:

**update** *filter-list-name*

---

## 更新サブコマンド

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

表 6. 更新サブコマンドの要約

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

次のサブコマンドを使用して、フィルター・リストを更新します。



## Add

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

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

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

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

```
構文: add                               source hex-MAC-addr hex-Mask
                                           destination hex-MAC-addr hex-Mask
                                           window MAC offset-value hex-data hex-mask
                                           window INFO offset-value hex-data hex-mask
```

### **source** *hex-MAC-addr hex-Mask*

発信元 MAC アドレスと比較するための 16 進数を追加します。

**hex-MAC-addr** は、最大 16 桁の偶数の 16 進数で、前に 0x を付けずに入力する必要があります。

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

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

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

### **destination** *hex-MAC-addr hex-Mask*

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

## MAC フィルターの構成

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

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

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

オフセットが情報フィールドの先頭から計算されることを除いて、

**add window mac** コマンドと同様です。

## Delete

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

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

構文:

**delete** *filter-item-number*

## List

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

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

構文:

**list** canonical  
noncanonical  
mac-address canonical  
mac-address noncanonical  
window

### canonical

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

### mac-address canonical

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

**noncanonical**

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

**mac-address noncanonical**

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

**window**

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

## Move

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

構文:

```
move filter-item-name1 filter-item-name2
```

## Set-Action

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

構文:

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

---

## MAC フィルター監視プロンプトへのアクセス

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

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

## MAC フィルターの構成

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

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

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

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

---

## MAC フィルター監視コマンド

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

表7. MAC フィルター監視コマンドの要約

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

次のコマンドを使用して、MAC フィルター・フィーチャーを監視します。

### Clear

**clear** コマンドは、フィルター統計を消去するのに使用します。

構文:

```
clear                                all  
                                       filter filter-number
```

**all**     **list all** コマンドによってリストされた統計を消去します。

**filter** *filter-number*

**list filter** コマンドによって表示された統計を消去します。

## Disable

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

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

構文:

```
disable                all
                        filter filter-number
```

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

**filter filter-number**

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

## Enable

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

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

構文:

```
enable                all
                        filter filter-number
```

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

**filter filter-number**

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

## List

**list** コマンドは、現在ルーターで実行されている各フィルターの統計および設定値の要約を表示するのに使用します。 **list all** コマンドを使用すると、各フィルターの次の情報が表示されます。

- デフォルト・アクション

## MAC フィルターの構成

- キャッシュ・サイズ
- デフォルト・タグ
- 状態 (使用可能 / 使用不可)
- INCLUDE、EXCLUDE、または TAG としてフィルターされたパケットの数

さらに、指定のフィルターに対する **list filter** コマンドでは、次の情報も表示されます。

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

構文:

```
list                                all
_
                                     filter filter-number
```

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

**filter filter-number**

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

## Reinit

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

構文:

```
reinit
_
```

---

## 第5章 WAN 復元の使用

この章には、次の内容が記載されています。

- 『WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローの概説』
- 67ページの『始める前に』
- 68ページの『WAN 復元の構成手順』
- 69ページの『2 次ダイヤル回線の構成』

---

### WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローの概説

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

3 つのフィーチャーのすべての構成コマンドを、「WAN 復元の構成」の章に収めています。WAN 再ルートおよびダイヤル・オン・オーバーフローに関する追加情報は、91ページの『第7章 WAN 再ルート・フィーチャー』を参照してください。

### WAN 復元

WAN 復元は、最も基本的な機能です。WAN 復元を使用する場合は、1 次リンクと 2 次リンクを構成します。1 次リンクに障害が起きた場合、2 次リンクがスタートし、1 次リンクの特性を引き継ぎます。2 次リンクは 1 次リンクからのプロトコル定義を使用するので、2 次リンクにプロトコル定義を構成する必要はありません。

#### WAN 復元の場合:

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

注: 1 次リンクに BRS が構成されており、その 1 次リンクが WAN 復元の 1 次 / 2 次のペアの片方である場合、2 次リンクにも BRS を構成する必要があります。



## WAN 復元の使用

通常は、WAN 復元が構成されている場合には、2 次リンクは 1 次リンクと同じ機能を引き継ぎます。しかし BRS については、これは該当しません。そのため、BRS は 1 次リンクと 2 次リンクの両方で構成する必要があります。

## WAN 再ルート

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

### WAN 再ルートの場合:

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

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

**注:** I.430/I.431 およびチャネル化 T1/E1 ダイヤル回線は、明示的に構成することなく、WRS 1 次として使用することができます。

- 代替リンクは、ダイヤル・オンデマンド・ダイヤル回線であってはなりません (ダイヤル回線に対して **set idle 0** を構成する必要があります)。
- **enable wrs** コマンドを使用して、WRS フィーチャーを使用可能にする必要があります。



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

## ダイヤル・オン・オーバーフロー

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

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

### ダイヤル・オン・オーバーフローの場合:

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

WAN 再ルートについて詳しくは、91ページの『第7章 WAN 再ルート・フィーチャー』を参照してください。

---

## 始める前に

WAN 復元を構成する前に、次の用意が必要です。

## WAN 復元の使用

- 1 次シリアル・インターフェース (専用回線) が PPP 用に構成されている。ルーター上の任意のシリアル・インターフェースを使用できます。
- 対応するダイヤル回線をもつインターフェースがルーター上に構成されている。ISDN インターフェースまたは V.25bis インターフェースを基本ネットワークとして使用することができます。
- 2 次ダイヤル回線が、1 次インターフェースがダウンしたときにダイヤルするように構成されている。ダイヤル回線をこのように構成するには、ダイヤル Circuit Config> プロンプトで **set idle** コマンドを使用して、アイドル・タイマーをゼロに設定します。このコマンドは、ダイヤル回線がダイヤル・オンデマンドにならないようにします。
- リンクの一方の端の 2 次ダイヤル回線がコール送信専用構成されている。Circuit Config> プロンプトで **set calls outbound** コマンドを使用して構成します。  
  
注: 2 次インターフェースにはプロトコル・アドレスを構成しないでください。2 次リンク (ダイヤル回線) が活動状態になると、1 次インターフェースのプロトコル割り当てが使用されます。
- リンクの他方の端の 2 次ダイヤル回線がコール受信専用構成されている。Circuit Config> プロンプトで **set calls inbound** コマンドを使用して構成します。

---

## WAN 復元の構成手順

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

次のステップに従って、ルーター上の WAN 復元を構成します。

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

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

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

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

3. 追加した 2 次ダイヤル回線上の WAN 復元を使用可能にする。たとえば、次のように入力します。

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

4. ルーター上の WAN 復元をグローバルに使用可能にする。たとえば、次のように入力します。

```
WRS Config>enable wrs
```

5. ルーターをリスタートして、構成変更を有効にする。

## 2 次ダイヤル回線の構成

ダイヤル回線を構成するには、次の手順で行います。

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

```
Config> list device
```

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

```
Config> add device dial-circuit
```

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

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

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

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

```
Config> network 3
```

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

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

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

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

6. バックアップ接続の一方の端 (たとえば、ルーター A) をコール受信用に設定するために、次のように入力する。

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

7. バックアップ接続の他方の端 (たとえば、ルーター B) をコール発信用に設定するために、次のように入力する。

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

注:

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

## WAN 復元の使用

## 第6章 WAN 復元の構成および監視

この章では、WAN 復元の構成コマンドおよび動作コマンドについて説明します。この章には、次の内容が記載されています。

- 79ページの『WAN 復元インターフェース監視プロセスへのアクセス』
- 79ページの『WAN 復元監視コマンド』

注: ダイアル回線の構成については、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の『ダイアル回線の構成および監視』を参照してください。ダイアル回線は、WAN 再ルートを構成する際のインターフェースとして使用できます。

### WAN 復元、WAN 再ルート、およびダイアル・オン・オーバーフローの構成コマンド

WAN 復元構成コマンドを使用して、WAN 復元インターフェース構成を作成または変更することができます。ここでは、WAN 復元構成コマンドの要約を示し、個々のコマンドについて説明します。

表8 は、WAN 復元構成コマンドとその機能を示しています。これらのコマンドは WRS Config> プロンプトで入力します。WRS Config> にアクセスするには、Config> プロンプトで **feature wrs** と入力します。

表 8. WAN 復元構成コマンドの要約

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

#### Add

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

構文:

```
add                               alternate-circuit  
                                     secondary-circuit
```

### alternate-circuit

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

#### 例:

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

#### Alternate interface number

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

#### Primary interface number

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

### secondary-circuit

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

#### 例:

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

#### Secondary interface number

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

#### Primary interface number

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

## Disable

**disable** コマンドは、WAN 復元機能、WAN 復元における 1 次 / 2 次の組み合わせ、WAN 再ルートにおける 1 次 / 代替の組み合わせ、または 1 次 / 代替のペアに対するダイヤル・オン・オーバーフローを使用不可にするのに使用します。

構文:

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

**alternate-circuit** *interface#*

WAN 再ルートの 1 次 / 代替の組み合わせを使用不可にします。

例:

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

**Alternate interface number**

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

**dial-on-overflow** *alt-intfc#*

指定された代替リンクを使用するすべての 1 次 / 代替の組みに対するダイヤル・オン・オーバーフローを使用不可にします。

例:

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

**Alternate interface number**

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

**secondary-circuit** *interface#*

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

例:

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

**Secondary interface number**

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

**wrs**

ルーター上の WAN 復元機能をグローバルに使用不可にします。これは、WAN 再ルートおよびダイヤル・オン・オーバーフローも使用不可にされることを意味しています。



### Enable

**enable** コマンドは、WAN 復元フィーチャー、WAN 復元における 1 次 / 2 次の組み合わせ、WAN 再ルートにおける 1 次 / 代替の組み合わせ、または 1 次 / 代替のペアに対するダイヤル・オン・オーバーフローを使用可能にするのに使用します。

構文:

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

**alternate-circuit** *interface#*

代替回線を使用可能にします。

例:

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

**Alternate interface number**

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

**dial-on-overflow**

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

例:

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

**Primary interface number**

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

**add-threshold**

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

**drop-threshold**

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

**bandwidth monitoring interval**

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



**Minimum time to keep alternate up**

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

**secondary-circuit interface#**

指定された 2 次リンクによる 1 次リンクの復元を使用可能にします。

例:

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

**Secondary interface number**

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

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

## List

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

構文:

**list**

例:

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

Primary Interface	Secondary Interface	Secondary Enabled						
4 - WAN PPP	7 - PPP Dial Circuit	No	1st Stab	Subseq Stab	TOD Start	Revert Stop	Back Stop	Stab
1 - WAN Frame Re	2 - WAN Frame Relay	Yes	dflt	dflt	Not Set	Not Set	15	

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

## Remove

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

構文:

## WAN 復元の構成

remove alternate-circuit  
secondary-circuit

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

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

### Alternate-interface#

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

### Primary-interface#

これは、除去される代替に以前に結合された 1 次インターフェースのインターフェース番号です。デフォルトは 0 です。

### 例:

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

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

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

### Secondary-interface#

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

### Primary-interface#

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

### 例:

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

## Set

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

### 構文:

set ? default  
first-stabilization  
routing-stabilization  
stabilization  
start-time-of-day-revert-back  
stop-time-of-day-revert-back

**default**

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

**first-stabilization**

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

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

**stabilization**

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

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

**first-stabilization**

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

例:

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

**Primary interface number**

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

**First primary stabilization time**

この 1 次インターフェースの安定化時間。デフォルトは 1 です。

**routing-stabilization**

ルーティング安定化の値を設定します。このパラメーターは、1 次リンクがアップになっていることが検出され、安定化 (stabilization) タイマー (設定されていれば) が満了した後、1 次リンクと代替リンクの両方が引き続きアップのままになる秒数を定義します。ルーティング安定化時間は、OSPF や RIP などのルーティング・プロトコルに、新しいルートが使用可能かどうか認識するための十分な時間を与えるためのものです。ルーティング安定化タイマーがなければ、代替ルートが使用不可になって 1 次ルートがまだ見つからない間、数秒間トラフィックが中断されることがあります。

再ルートの前に代替リンクがアップになった場合は、代替リンクはそのままアップになり、ルーティング安定化タイマーは無視されます。再ルートの前、または再ルート中に代替リンクがダウンになった場合は、代替リンクはそのままダウンになり、ルーティング安定化タイマーと安定化タイマーは両方とも無視されます。

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

**Primary interface number**

有効値: 0 ~ ルーターに対して構成されたインターフェースの数

デフォルト値: 0

**ルーティング安定化タイマー**

有効値: 1 ~ 3600 秒

デフォルト値: 0

### stabilization

1 次リンクがアップであることが最初に検出された後、1 次リンクに対してルーティングの再初期設定処理を開始する前に必要な秒数を設定します。安定化タイマーが満了すると、ルーティング安定化タイマーが構成されていなければ、代替リンクはダウンになります。ルーティング安定化タイマーは、安定化タイマーが満了するとすぐに開始され、OSPF や RIP などのルーティング・プロトコルが 1 次リンク上にルートを再確立するまで、1 次リンクと代替リンクの両方を十分な時間アップに保って、代替リンクのトラフィックを維持します。

例:

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

#### Primary interface number

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

#### Primary stabilization time

1 次インターフェースの安定化時間。デフォルトは 1 です。

### start-time-of-day-revert-back

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

例:

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

#### Primary interface number

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

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

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

### stop-time-of-day-revert-back

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

例:

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

**Primary interface number**

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

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

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

---

## WAN 復元インターフェース監視プロセスへのアクセス

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

```
+ feature wrs
```

---

## WAN 復元監視コマンド

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

WRS プロンプトにアクセスするには、GWCON (+) プロンプトで **feature wrs** と入力します。表9 は、WRS コマンドとその機能を示しており、後でそれぞれのコマンドについて説明しています。

表9. WAN 復元監視コマンド

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

## WAN 復元の構成

### Clear

**clear** コマンドは、**list** コマンドを使用して表示された、WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローの統計を消去するのに使用します。

構文:

**clear**

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

### Disable

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

構文:

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

#### alternate-circuit

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

例:

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

#### Alternate circuit number

これは、代替回線の番号です。デフォルトは 0 です。

#### dial-on-overflow

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

#### secondary-circuit

特定の 1 次インターフェースに対応する 2 次インターフェースによる復元を、次の **restart**、**reload**、または **enable secondary-circuit** コマンドまで使用不可にします。両方のインターフェースとも構成済みであり、WRS 構成内で相互が結合されていることが必要です。

通常は、**talk 5** (GWCON) の **disable** コマンドによりインターフェースは非活動状態にされ、非活動状態のままになりますが、WAN 復元の 2 次の場合

は、そうではありません。2 次インターフェースに適用される **disable** コマンドは、インターフェース自体は使用不可にしません。現行のコールだけを使用不可にします (つまり、活動状態のコールが切断されます)。2 次回線を使用不可にするためには、WAN 復元監視プロンプトで **disable secondary-circuit** と入力し、トップ・レベルの GWCON プロンプトで 2 次インターフェースを使用不可にすることが必要です。

例:

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

#### Secondary interface number

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

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

## Enable

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

構文:

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

#### alternate-circuit

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

例:

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

#### Alternate circuit number

これは、代替回線のインターフェース番号です。デフォルトは 0 です。

#### dial-on-overflow

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

例:

```
WRS> dial-on-overflow

For dial-on-overflow, only IP traffic can overflow to the alternate interface.
Primary interface number [0]? 1
add-threshold (1-100% utilization) [90]?
```



## WAN 復元の構成

```
drop-threshold(0-99% utilization) [60]?
bandwidth test interval(10-200 seconds) [15]?
minimum time to keep the alternate up (20-21600 sec.) [300]?
Dial-on overflow is enabled.
Remember to configure the primary interface's line speed!

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

### secondary-circuit

指定された 2 次リンクによる 1 次リンクの復元を使用可能にします。

例:

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

### Secondary interface number

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

**wrs** ルーター上の WAN 復元フィーチャーを使用可能にします。WAN 復元、WAN 再ルート、またはダイヤル・オン・オーバーフローを行うためには、このフィーチャーを使用可能にすることが必要です。

## Set

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

構文:

```
set ?                               default
                                       first-stabilization
                                       routing-stabilization
                                       stabilization
                                       start-time-of-day-revert-back
                                       stop-time-of-day-revert-back
```

### default

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

例:

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

### first-stabilization

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

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

### stabilization

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

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



**first-stabilization**

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

例:

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

**Primary interface number**

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

**First primary stabilization time**

この 1 次インターフェースの安定化時間。デフォルトは 1 です。

**routing-stabilization**

ルーティング安定化の値を設定します。このパラメーターは、1 次リンクがアップになっていることが検出され、安定化 (stabilization) タイマー (設定されていれば) が満了した後、1 次リンクと代替リンクの両方が引き続きアップのままになる秒数を定義します。ルーティング安定化時間は、OSPF や RIP などのルーティング・プロトコルが、新しいルートが使用可能かどうか認識するために十分な時間を使えるようにするためのものです。ルーティング安定化タイマーがなければ、代替ルートが使用不可になって 1 次ルートがまだ見つかからない間、数秒間トラフィックが中断されることがあります。

再ルートの前に代替リンクがアップになった場合は、代替リンクはそのままアップになり、ルーティング安定化タイマーは無視されます。再ルートの前、または再ルート中に代替リンクがダウンになった場合は、代替リンクはそのままダウンになり、ルーティング安定化タイマーと安定化タイマーは両方とも無視されます。

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

**Primary interface number**

有効値: 0 ~ ルーターに対して構成されたインターフェースの数

デフォルト値: 0

**ルーティング安定化タイマー**

有効値: 1 ~ 3600 秒

デフォルト値: 0

**stabilization**

1 次リンクがアップであることが最初に検出された後、1 次リンクでルーティングの再初期設定処理を開始する前に必要な秒数を設定します。安定化タイマーが満了すると、ルーティング安定化タイマーが構成されていなければ、代替リンクはダウンになります。ルーティング安定化タイマーは、安定化タイマーが満了するとすぐに開始され、OSPF や RIP などのルーティング・プロトコルが 1 次リンク上にルートを再確立するまで、1 次リンクと代替リンクの両方を十分な時間アップに保って、代替リンクのトラフィックを維持します。

例:

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

### Primary interface number

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

### Primary stabilization time

1 次インターフェースの安定化時間。デフォルトは 1 です。

### start-time-of-day-revert-back

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

#### 例:

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

### Primary interface number

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

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

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

### stop-time-of-day-revert-back

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

#### 例:

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

### Primary interface number

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

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

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

## List

**list** コマンドは、WAN 復元の 1 次 / 2 次のペアの 1 つまたはすべて、あるいは WAN 再ルートの 1 次 / 代替のペアの 1 つまたはすべてに関する情報を表示するために使用します。

構文:

```
list all
      alternate-circuit
      secondary-circuit
      summary
```

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

例:

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

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

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

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

### Total restoral attempts

1 次に障害が発生し、ルーターが 2 次リンクの起動を試みた回数

### Completions

復元の試みに成功した (2 次がアップになり、使用された) 回数

### Total packets forwarded

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

### Longest Completed Restoral Period

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

### Total Overflow Attempts

オーバーフローが原因での試行回数

### Completions

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

### Longest Completed Overflow Period

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

### Primary Net Interface

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

### Secondary Net Interface

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

### Restoral Enabled

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

### Restoral Active

復元が活動状態かどうか (Yes または No) を示します。

### Current/Longest Duration

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

### Primary Net Interface

対応する代替インターフェースによってバックアップされるインターフェース

### Alternate Net Interface

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

### Re-route/Overflow Enabled

再ルートおよびオーバーフローが使用可能であるかどうか (Yes または No) を示します。

### Re-route/Overflow Active

再ルートおよびオーバーフローが活動状態かどうか (Yes または No) を示します。

### Recent Re-route Overflow Duration

代替ネットワーク・インターフェースの最新の再ルートおよびオーバーフローの時間数を、時間、分、秒数で示します。

### Alternate-circuit

代替回線の合計数を提供します。監視オペレーターは、WAN 再ルートの状態、および各代替インターフェースと対応の 1 次マッピングに関する統計を検索することができます。

#### 例:

```
WRS>1i alt 7
Primary 1:FR/0 Frame Relay V.35/V.36
Alternate 7:PPP/1 Point to Point V.25bis Dial Circuit
reroute Enabled, currently inactive
overflow Enabled, currently inactive
Primary first stabilization time: default (0 seconds)
Primary stabilization time: default (0 seconds)
Routing-stabilization time: 15 seconds
Time-of-day revert back not configured: start = 0, stop = 0
Restored 0 times (0 attempts)
Overflow 0 times (0 attempts)
```

### Primary Interface

この代替インターフェースによってバックアップされるインターフェース

**Alternate Interface**

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

**Reroute Enabled**

この 1 次インターフェースの再ルートが現在使用可能になっているかどうかを示します。

**Overflow Enabled**

この 1 次インターフェースのオーバーフローが現在使用可能になっているかどうかを示します。

**Primary first stabilization**

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

**First stabilization**

1 次リンクがアップであることが最初に検出された後、ルーティングを代替リンクから 1 次リンクに戻す前に必要な秒数を設定します。1 次リンクがこの秒数だけアップ状態に保たれるまでは、ルーティングは代替リンクを介して継続されます。

**Routing stabilization**

ルーティングを 1 次リンクに戻した後、代替リンクをダウンにする前に必要な秒数。この時間は、1 次リンクと代替リンクが両方ともアップのままになります。このインターバルは、OSPF や RIP などのルーティング・プロトコルに、1 次インターフェースを経由したルートが使用可能かどうか認識するための時間を与えるためのものです。

**Time-of-day revert back**

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

**Restored times**

1 次インターフェースを再ルートするための試行回数

**Overflow times**

ダイヤル・オン・オーバーフローの試行回数

**secondary-circuit**

各 2 次回線の合計数を提供します。監視オペレーターは、WAN 復元状態、および各 2 次インターフェースと対応の 1 次とのマッピングに関する統計を検索することができます。

例:

```
list secondary-circuit
Secondary interface number [0]? 1
```

Primary Interface	Secondary Interface	Secondary Enabled
1 PPP/0 Point to Poi	3 PPP/1 Point to Poi	Yes

```
Router primary interface state = Up
```

## WAN 復元の構成

```
Router secondary interface state = Available
Restoral Statistics:
    Primary restoral attempts =      6    completions =    5
    Restoral packets forwarded =   346
    Most recent restoral period in hrs:min:sec      00:08:20
```

### Primary Interface

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

### Secondary Interface

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

### Secondary Enabled

この 1 次インターフェースの復元が現在使用可能になっているかどうかを示します。

### Router Primary Interface State

1 次インターフェースの状態が、次のどれか 1 つであることを示します。

Up - リンクがアップであることを示します。

Down - リンクがダウンであることを示します。

Disabled - オペレーターがリンクを使用不可にしたことを示します。

Not present - リンクは構成されているが、ハードウェアに問題があることを示します。

### Router Secondary Interface State

対応する 2 次インターフェースの状態が、次のどれか 1 つであることを示します。

Up - リンクがアップであることを示します。

Down - リンクがダウンであることを示します。これは、Config>プロンプトまたはオペレーター・コンソールで、2 次の基本ネットが使用不可にされている場合にも起こります。

Available - リンクが待機モードにあることを示します。

Testing - リンクが接続確立中であることを示します。

### 復元の統計:

#### Primary Restoral Attempts

1 次に障害が発生し、ルーターが 2 次リンクの起動を試みた回数

#### Restoral Packets forwarded

このフィールドには、転送されたパケットの合計数が表示されます。

#### Most Recent Restoral Period

これは、前回の使用時または現行の復元の使用時の、2 次がアップであった時間数を示します。

### summary

各 2 次回線の合計数を提供します。

例:

**list summary**

WAN Restoral is enabled with 3 circuit(s) configured

```
Total restoral attempts =      3 completions =      2
Total packets forwarded =    346
Longest restoral period in hrs:min:sec  00:08:20
```

Primary Interface and State	Secondary Interface and State
-----	-----
1 PPP/0 - Up	3 PPP/1 - Available

**Total restoral attempts**

1 次に障害が発生し、ルーターが 2 次リンクの起動を試みた回数

**Completions**

復元の試みに成功した (2 次がアップになり、使用された) 回数

**Total packets forwarded**

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

**Longest restoral period**

このフィールドは、現行の使用期間はカウントせずに、復元が使用された最長時間を時間、分、秒数で表示します。

**Primary Interface and State**

対応する 2 次によってバックアップされるインターフェース。有効な状態は、次のとおりです。

Up - リンクがアップであることを示します。

Down - リンクがダウンであることを示します。

Disabled - オペレーターがリンクを使用不可にしたことを示します。

Not present - リンクは構成されているが、ハードウェアに問題があることを示します。

**Secondary Interface and State**

対応する 1 次をバックアップするのに使用されているダイヤル回線。有効な状態は、次のとおりです。

Up - リンクがアップであることを示します。

Down - リンクがダウンであることを示します。これは、Config> プロンプトまたはオペレーター・コンソールで、2 次の基本ネットが使用不可にされている場合にも起こります。

Testing - リンクが接続確立中であることを示します。

Available - リンクが待機モードにあることを示します。

## WAN 復元の構成



---

## 第7章 WAN 再ルート・フィーチャー

この章では、WAN 再ルート・フィーチャーについて説明します。この章には、次の内容が記載されています。

- 『WAN 再ルートの概説』
- 93ページの『WAN 再ルートの構成』

---

### WAN 再ルートの概説

WAN 再ルートは、代替ルートを設定することによって、1 次リンクに障害が起きたときに、ルーターが自動的に代替ルートを通るあて先への新しい接続を開始できるようにします。WAN 復元の説明、および WAN 再ルートとダイヤルオン・オーバーフローを合わせて使用する方法については、65ページの『WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローの概説』を参照してください。

WAN 再ルート・プロセスは、次のとおりです。

1. 1 次リンクの障害を検出する。
2. 代替リンクに切り替える。
3. 1 次リンクの回復を検出する。
4. 1 次リンクに戻す。

代替リンクは、ルート可能プロトコル (たとえば、IP、IPX) を構成できる任意のリンクを使用することができ、代替リンクのデータ・リンク・タイプは、1 次リンクのデータ・リンク・タイプと一致している必要はありません。たとえば、代替リンクには、LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ダイヤル回線などを使用できます。代替リンクに使用できないインターフェース・タイプの例としては、SDLC シリアル・インターフェース、SRLY シリアル・インターフェース、および V.25bis や ISDN のような基本ネットがあります。

**注:** 1 次リンクまたは代替リンクがダイヤル回線の場合、そのダイヤル回線はダイヤル・オンデマンド用に構成することはできません。ダイヤル回線がダイヤル・オンデマンドを実行できないようにダイヤル回線を構成するには、Circuit Config> プロンプトで **set idle 0** コマンドを使用します。詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の『ダイヤル回線の構成および監視』を参照してください。

## WAN 再ルートの構成

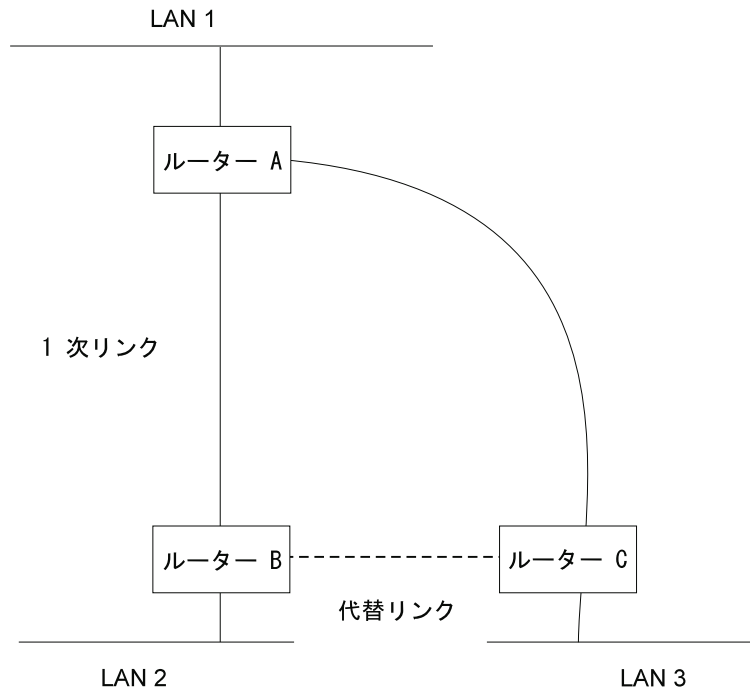


図3. WAN 再ルート. 通常は、ルーター A と B の間、およびルーター A と C の間に接続があります。ルーター A と B の間の 1 次リンクに障害が起きた場合、WAN 再ルートは、ルーター B と C の間に代替リンクを確立します。これにより、ルーター A と B は、ルーター C を介して通信できるようになります。

## ダイヤル・オン・オーバーフロー

ダイヤル・オン・オーバーフローでは、1 次リンクのトラフィック速度が指定の限界値に達すると、IP トラフィック用の代替インターフェースを使用することができます。これは、1 次インターフェースが必ずしもダウンしなくても、代替リンクが起動されることを意味しています。1 次インターフェースのトラフィックが指定の限界値に達すると、ルーターは代替リンクを起動します。ダイヤル・オン・オーバーフローを使用するためには、WAN 再ルートが構成されており、1 次インターフェースがフレーム・リレーである必要があります。ダイヤル・オン・オーバーフローで代替インターフェースに切り替えることができる唯一のプロトコルは、IP です。ダイヤル・オン・オーバーフローを使用する場合も、RIP の代わりに、OSPF を IP ルーティング・プロトコルとして使用する必要があります。

ダイヤル・オン・オーバーフローの構成については、71ページの『WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローの構成コマンド』を参照してください。

## 帯域幅の監視

WAN 再ルートの構成時に、ダイヤル・オン・オーバーフローの帯域幅監視のインターバルを指定することができます。1 次インターフェースの送受信の帯域幅が監視されます。1 次インターフェースの帯域幅が追加 限界値に達すると、代替インターフェースを起動するための WAN 再ルート要求が生成されます。WAN 再ルートが代替インターフェースの起動に成功すると、IP は 1 次インターフェースを介したルーティングを停止し、代替インターフェースを介してルーティングを開始します。

WAN 再ルートが代替ルートの起動に成功しない場合、1 次インターフェースの帯域幅使用率が除去 限界値を下回るまで、代替インターフェースの起動を定期的に試みません。

1 次インターフェースの送受信の帯域幅使用率が除去 限界値に達し、構成された最小アップ・タイムが満了すると、代替インターフェースは除去されます。これにより、IP は代替インターフェースを介したルーティングを停止し、1 次インターフェースの使用を開始します。

追加限界値および除去限界値は、1 次リンクに構成した回線速度の比率として指定されます。構成された回線速度は、必ずしもリンクの実際の速度と一致するとは限りません。リンク上の各方向のトラフィックの量は、別々に計算されます。どちらかの方向のトラフィックが指定した比率より大きい場合、限界値を超過したと見なされます。

---

## WAN 再ルートの構成

次に示すのは、WAN 再ルートを構成するのに必要なステップです。次で、これらのタスクを実行する方法の例を示します。

WAN 再ルートを構成するには、次の作業が必要です。

- 1 次リンクを構成する。
- 代替リンクを構成する。
- 代替リンクを 1 次リンクに割り当てる。1 次リンクの安定化 (stabilization) 期間も指定できます。

安定化時間が終わった後 (構成されている場合) に行われる 1 次リンクへの復帰時刻 (time-of-day revert-back) を指定することができます。これにより、ユーザーが希望する時刻まで 2 次をアップに維持し、オフ・ピーク時に 1 次に復帰させるといったことが可能になります。

**注:** 1 次リンクと代替リンクは、異なるデータ・リンク・タイプであっても構いません。1 次リンクおよび代替リンクには、次のものを使用できます。

- LAN インターフェース
- PPP シリアル・インターフェース
- フレーム・リレー・シリアル・インターフェース
- X.25 シリアル・インターフェース
- PPP ダイアル回線
- フレーム・リレー・ダイアル回線

## サンプル WAN 再ルート構成

94ページの図4 は、ISDN を介するフレーム・リレー・ダイアル回線を代替リンクとして使用している WAN 再ルートを示しています。ルーター A とルーター C 間のフレーム・リレー DLCI に障害が起きた場合、WAN 再ルートはダイアル回線を使用してルーター D を経由する代替リンクを確立します。営業所から本社への 1 次リン

## WAN 再ルートの構成

クの 1 つに障害が起きた場合、WAN 再ルートは別の営業所を経由して本社に接続する代替ルートを確立します。

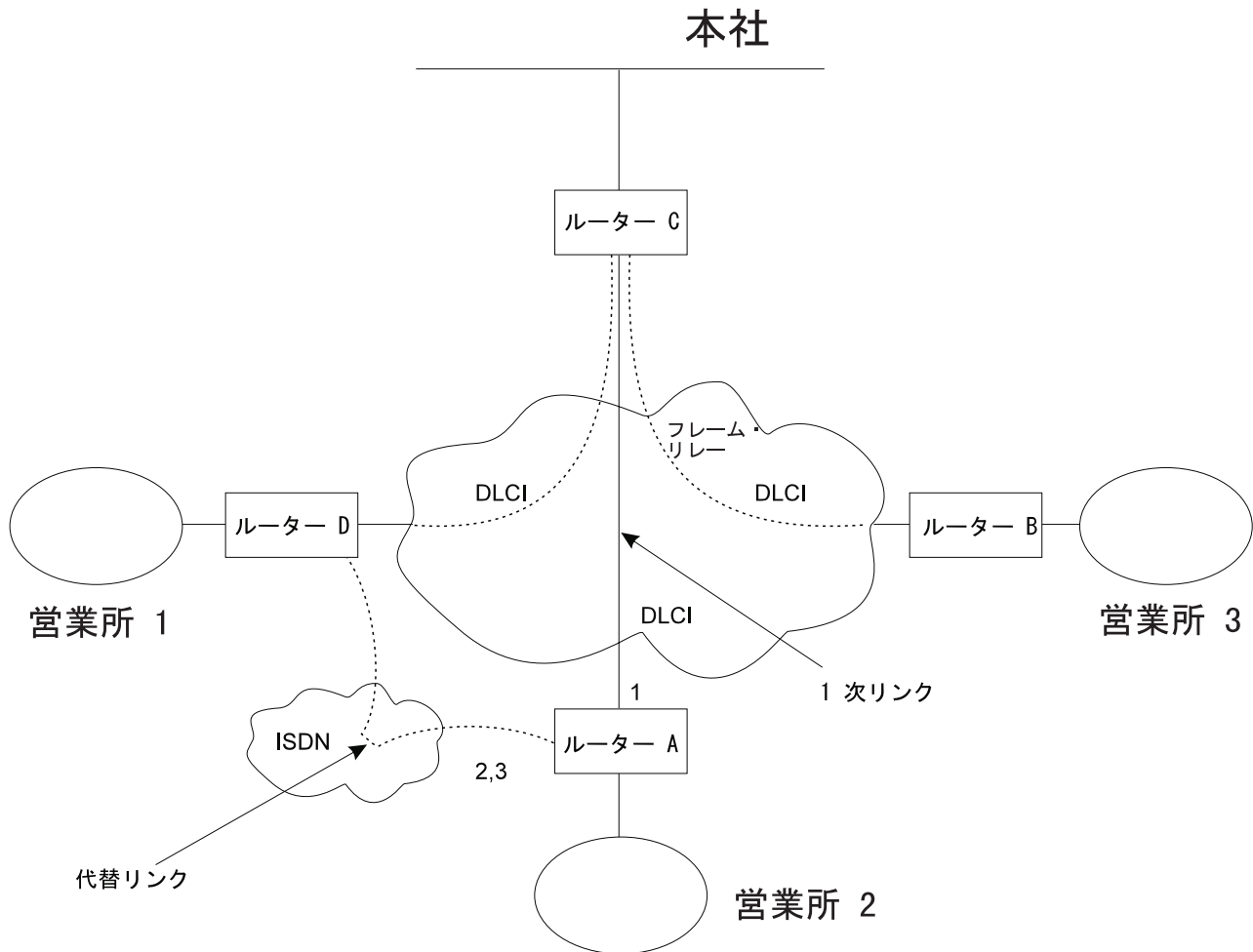


図4. サンプル WAN 再ルート構成. 営業所はフレーム・リレーを使用して本社に接続

次では、図4 のルーター A 上の WAN 再ルートを設定する方法について説明します。次のタスクが必要になります。

- 1 次フレーム・リレー・インターフェース (1) を構成して、そのフレーム・リレー・インターフェースに必要な PVC または必要な PVC グループを設定するか、あるいは No-PVC フィーチャーを使用可能にする。
- ISDN インターフェース (2) およびそのフレーム・リレー・ダイヤル回線 (3) を構成する。
- ダイヤル回線を、1 次フレーム・リレー・インターフェースの代替リンクとして割り当て、ダイヤル回線の `Circuit Config>` プロンプトで **set idle 0** コマンドを出して、この回線のダイヤル・オンデマンドを使用不可にする。
- 任意選択で、次のものも指定できます。
  - 1 次リンクの安定化 (stabilization) 期間
  - 1 次リンクの復帰時刻 (time-of-day revert-back) ウィンドウ

これらのタスクについて詳しくは、次に説明します。

## フレーム・リレー・インターフェースの構成

ルーター A 上に WAN 再ルート用のフレーム・リレー・インターフェースを構成するには、1 次フレーム・リレー・インターフェース上のルーター A と C 間に PVC を追加します。

他のルーターへの接続が失われたときに、1 次 FR インターフェースが自身をダウンとして宣言するようにさせるには、3 通りの方法を選択できます。

1. No-PVC フィーチャーを使用可能にする。このフィーチャーが使用可能のとき、活動状態の PVC がないと、FR インターフェースはダウンします。
2. ある PVC を必須として構成するが、その PVC を必須 PVC グループの中にも含まない。この場合、その PVC が非活動状態になると、FR インターフェースはダウンします。
3. 1 組の PVC を必須として構成し、必須 PVC グループに含める。この場合、必須 PVC グループのすべての PVC が非活動状態になると、FR インターフェースはダウンします。

フレーム・リレー・インターフェースの構成は、次の手順で行います。

1. ISDN インターフェース上のデータ・リンクをフレーム・リレーに設定する (まだ行っていない場合)。

```
Config>set data-link frame relay
Interface Number [0]? 2
```

2. フレーム・リレー構成プロセスに入る。

```
Config>network
What is the network number [0]?2
Frame Relay user configuration
FR Config>
```

**注:** 1 次フレーム・リレー・インターフェースを構成するために、残りの 2 つのステップのうちの 1 つ だけを実行します。

3. **add permanent-virtual-circuit** コマンドを使用して、PVC を追加する。

PVC を必須として構成するには、次のようにします。

『Is circuit required for interface operation ?』という問いに対して **y** と入力する。

PVC を必須 PVC グループのメンバーとして構成するには、次のようにします。

- a. 『Does circuit belong to a Required PVC group ?』という問いに対して **y** を入力する。
- b. 『What is the group name ?』の問いに回答して、グループ名を入力する。

すでに PVC が追加されている場合は、**change permanent-virtual-circuit** コマンドを使用して、PVC を必須として構成し、該当する場合は、それを必須 PVC グループに割り当てます。詳しくは、アクセス・インテグレーション・サービス ソフトウェア使用者の手引きの『フレーム・リレー・インターフェースの使用』の項を参照してください。

```
FR Config>add permanent-virtual-circuit
Circuit number [16]?
Committed Information Rate (CIR) in bps [64000]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
```

## WAN 再ルートの構成

```
Assign circuit name []?  
Is circuit required for interface operation [N]?y  
Does the circuit belong to a required PVC group [N]? y  
What is the group name []?group1
```

4. 必要な場合は、No-PVC フィーチャーを使用可能にする。

**注:** このステップは、直前のステップを飛ばした場合にだけ 実行してください。

```
FR Config>enable no-pvc
```

この他にも、フレーム・リレーに対して設定できるパラメーターがあります。詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の‘フレーム・リレーの使用’の項を参照してください。

## ISDN インターフェースとダイヤル回線の構成

ルーター A とルーター D 間の ISDN インターフェースとダイヤル回線を構成します。ISDN インターフェースおよびダイヤル回線の構成方法について詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の‘ISDN インターフェースの使用’の項を参照してください。

WAN 復元とは異なり、代替リンクとして使用されるダイヤル回線には、ルーティング・プロトコルを構成する必要があります。このルート可能プロトコルは、保守パケットを送信するのを防止できないので、代替リンクは再ルートの必要がなくても接続を確立します。この場合、代替リンクを再ルートにだけ使用したいときは、ダイヤル回線を使用不可に設定します。ダイヤル回線を使用不可にするには、Config> プロンプトで **disable interface** コマンドを入力します。

ISDN インターフェースに複数のダイヤル回線を割り当てた場合、ダイヤル回線に優先順位を設定することができます。すべての B チャンネルが、物理インターフェース上に活動状態のダイヤル回線を持っており、高い優先順位の回線がパケットを受信する場合、最低優先順位の接続は終了され、高い優先順位の回線が接続を確立します。

優先順位は 0 ~ 15 に設定できます。15 が最高優先順位の回線で、0 が最低優先順位の回線です。新規ダイヤル回線のデフォルト優先順位は 8 です。優先順位を変更する場合は、Circuit Config> プロンプトで **set priority** と入力します。

## 代替リンクの割り当てと構成

WAN 再ルート構成プロセスに入って、ダイヤル回線を LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ダイヤル回線の代替リンクとして割り当て、必要な場合には、安定化期間 (stabilization periods) または復帰時刻 (time-of-day revert-back) ウィンドウ (もしくは、その両方) を指定します。

安定化期間には、次の 3 種類があります。

- **最初の安定化期間 (First stabilization period)** は、ルーターが最初に 1 次インターフェースの起動を試みたときに、1 次インターフェースが活動状態になるのを待つ時間の長さです。最初の安定化期間が経過しても 1 次がアップにならない場合、WAN 再ルートは代替リンクを起動します。



- 安定化期間 (*Stabilization period*) は、ルーターが代替リンクから 1 次リンクに戻る前に、1 次リンクの信頼性を確認するために待つ時間の長さです。
- ルーティング安定化期間 (*Routing stabilization period*) は、ルーターが代替リンクから 1 次リンクに戻る前に、1 次リンクと代替リンクの両方をアクティブのままにする時間の長さです。この時間は、OSPF や RIP などのルーティング・プロトコルが、代替リンクがダウンになる前に 1 次リンク経由の新しいルートが使用可能かどうか認識するために使用します。

復帰時刻 (*time-of-day revert-back*) ウィンドウは、1 次がアップになり、構成された安定化期間が経過した後で 1 次に戻す具体的な時刻です。

ユーザーは 24 時間クロックを使用して、復帰ウィンドウの開始時刻と停止時刻を指定します。開始時刻に達するまで、2 次はアップのまま維持され、ダウンにされません。1 次がアップになる時刻が、開始時刻と停止時刻 (ウィンドウ内の) の間にある場合、安定化期間が経過した後、ただちに 1 次リンクに切り替わります。

代替リンクの割り当てと構成は、次の手順で行います。

1. WAN 復元構成プロセスに入る。

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

2. ダイヤル回線を、1 次フレーム・リレー・インターフェースの代替リンクとして割り当てる。

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

3. 代替回線を使用可能にする。

```
WRS Config>enable alternate-circuit
Alternate interface number [0]? 4
```

4. オプションで、最初の安定化期間を指定する。

特定の 1 次インターフェースに対する最初の安定化期間を設定するには、**set first-stabilization-period** コマンドを使用します。特定の期間が設定されていないすべてのインターフェースに対するデフォルトの最初の安定化期間を設定するには、**set default first-stabilization-period** コマンドを使用します。

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

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

5. オプションで、安定化期間を設定する。特定のインターフェースに対する安定化期間を設定するには、**set stabilization-period** コマンドを使用します。特定の期間が設定されていない、すべてのインターフェースに対するデフォルトの安定化期間を設定するには、**set default stabilization-period** コマンドを使用します。

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

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

6. オプションで、ルーティング安定化期間を指定する。特定のインターフェースに対するルーティング安定化期間を設定するには、**set routing-stabilization** コマンドを使用します。

## WAN 再ルートの構成

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

7. オプションで、復帰時刻の範囲を指定する。

特定のインターフェース・ウィンドウの開始時刻と停止時刻を設定するには、`start-time-of-day-revert-back` コマンドと `stop-time-of-day-revert-back` コマンドを使用します。デフォルト値のゼロは、ウィンドウが構成されないことを意味します。24 時間クロックは、午前 1 時に開始して、夜中の 24 時に終了します。開始時刻と停止時刻が同じ (ただし、ゼロでない) 場合、復帰は正確にその時刻に起こります。

次は、復帰ウィンドウの設定を示す 2 つの例です。

- a. 開始時刻が 23 で、停止時刻が 3 のとき、午後 11 時から午前 3 時までの復帰ウィンドウを生成します。
- b. 開始時刻が 1 で、停止時刻が 5 のとき、午前 1 時から午前 5 時までの復帰ウィンドウを生成します。

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



---

## 第8章 ネットワーク・ディスパッチャー・フィーチャーの使用

この章では、ネットワーク・ディスパッチャー・フィーチャーの使用法について説明します。この章には、次の内容が記載されています。

- 『ネットワーク・ディスパッチャーの概説』
- 100ページの『ネットワーク・ディスパッチャーの使用による TCP および UDP トラフィックのバランシング』
- 101ページの『ネットワーク・ディスパッチャーの高可用性』
- 104ページの『ネットワーク・ディスパッチャーの構成』
- 111ページの『TN3270 でのネットワーク・ディスパッチャーの使用』
- 113ページの『Web サーバー・キャッシュでのネットワーク・ディスパッチャーの使用』
- 113ページの『eNetwork ホスト・オンデマンド・クライアント・キャッシュでのネットワーク・ディスパッチャーの使用』
- 114ページの『スケーラブル高可用性キャッシュ (SHAC) でのネットワーク・ディスパッチャーの使用』

ネットワーク・ディスパッチャーは、IBM 研究部門が開発したロード・バランシング・テクノロジーを使用して、新規の接続のたびに、それを受け取るのに最も適したサーバーを判別します。これは、Solaris、Windows NT、および AIX 用の IBM eNetwork ディスパッチャーで使用されている技術と同じものです。

---

### ネットワーク・ディスパッチャーの概説

ネットワーク・ディスパッチャーとは、TCP/IP セッション要求をサーバー・グループ内の種々のサーバーに転送し、すべてのサーバー間で要求のロード・バランシングを取ることによって、サーバーの性能を高めるフィーチャーです。この転送は、ユーザーおよびアプリケーションには透過的に行われます。ネットワーク・ディスパッチャーは、E メール、ワールド・ワイド・ウェブ (WWW) サーバー、分散並列データベース照会、およびその他の TCP/IP アプリケーションなどのサーバー・アプリケーションに役立ちます。

ネットワーク・ディスパッチャーは、サーバー・グループへのステートレス UDP アプリケーション・トラフィックのロード・バランシングを取るのにも役立ちます。

ネットワーク・ディスパッチャーは、ピーク需要時の問題に対処するための、強力で、柔軟で、拡張が容易なソリューションを提供することにより、ユーザーのサイトの潜在的な能力を最大限に発揮させることができます。ネットワーク・ディスパッチャーは、ピーク需要時に、着信要求を処理するための最適なサーバーを自動的に見つけます。

ネットワーク・ディスパッチャー機能は、ロード・バランシングを取るのにドメイン名サーバーを使用しません。ロード・バランシングと管理を固有に組み合わせたソフトウェアを使用して、サーバー間のトラフィックのバランスを取ります。ネッ

## ネットワーク・ディスパッチャーの使用

トワーク・ディスパッチャーは、障害のあるサーバーを検出し、他の利用可能なサーバーにトラフィックを転送することもできます。

ネットワーク・ディスパッチャー・マシンに送られるすべてのクライアント要求は、ネットワーク・ディスパッチャーが、動的に設定される重みに基づいて最適サーバーと判断したサーバーに転送されます。これらの重みは、デフォルト値を使用することも、構成プロセスで値を変更することもできます。

サーバーからクライアントへの応答には、ネットワーク・ディスパッチャーは介入しません。ネットワーク・ディスパッチャーと通信するために、サーバー上にソフトウェアを追加する必要はありません。

ネットワーク・ディスパッチャー機能は、大規模で、拡張が容易なサーバー・ネットワークを、安定した状態で効率的に管理するためのキーになります。ネットワーク・ディスパッチャーを使用すると、多数の個別のサーバーをリンクして、単一のバーチャル・サーバーのように見せることができます。世界からは、ユーザーのサイトは単一の IP アドレスのように見えます。ネットワーク・ディスパッチャーは、ドメイン名サーバーから独立して機能します。要求はすべてネットワーク・ディスパッチャー・マシンの IP アドレスに送られます。

ネットワーク・ディスパッチャーでは、SNMP ベースの管理アプリケーションを使用して、基本的な統計および潜在的なアラート状態を受信し、ネットワーク・ディスパッチャーを監視することができます。詳しくは、プロトコル構成および監視 参照資料 第 1 巻 の『SNMP 管理』の項を参照してください。

ネットワーク・ディスパッチャーは、クラスター化されたサーバーへのトラフィックのロード・バランシングに大きく貢献し、サイトの安定した、効率的な管理を実現します。

---

## ネットワーク・ディスパッチャーの使用による TCP および UDP トラフィックのバランシング

ロード・バランシングには、さまざまなアプローチがあります。ある方法では、最初のサーバーが遅かったり応答しない場合、ユーザーが任意に異なるサーバーを選択することができます。ある方法はラウンドロビン方式を採用し、ドメイン名サーバーが、要求を処理するサーバーを選択します。この方法は比較的優れていますが、ターゲット・サーバー上の現在のロードは考慮に入れられず、ターゲット・サーバーが利用可能であるかどうかさえ考慮されません。

ネットワーク・ディスパッチャーは、要求のタイプ、サーバー上のロードの分析、またはユーザーが割り当てる一組の構成可能な重みに基づいて、種々のサーバーへの要求のロード・バランスを取ることができます。異なるタイプのバランシングを個別に管理するために、ネットワーク・ディスパッチャーには、次のコンポーネントが装備されています。

### 実行プログラム

受信した要求のタイプに基づいて、接続のロード・バランスを取ります。一般的な要求のタイプとしては、HTTP、FTP、および Telnet があります。このコンポーネントは、常に実行されます。

### アドバイザー

サーバーに照会し、各サーバーのプロトコルを用いて結果を分析します。アドバイザーは適切な重みを設定するために、この情報をマネージャーに渡します。アドバイザーは、任意選択のコンポーネントです。

ネットワーク・ディスパッチャーは、FTP、HTTP、SMTP、NNTP、POP3、および Telnet 用のアドバイザー、IBM 2210、IBM 2212、および IBM 2216 内の TN3270 サーバーと一緒に稼働する TN3270 アドバイザー、および MVS システム上のワークロード・マネージャー (WLM) と一緒に稼働する MVS アドバイザーをサポートします。WLM は、個々の MVS ID のワークロードの量を管理します。ネットワーク・ディスパッチャーは、WLM を利用して、OS/390 V1R3 以降 のリリースを稼働する MVS サーバーへの要求のロード・バランスを取ることができます。

UDP プロトコル専用のプロトコル・アドバイザーはありません。MVS サーバーを使用している場合は、MVS システム・アドバイザーを使用してサーバーのロード情報を提供することができます。ポートが TCP および UDP トラフィックを扱っている場合も、適切な TCP プロトコル・アドバイザーを使用して、そのポートのアドバイザー入力を提供できます。ネットワーク・ディスパッチャーは、この入力を使用して、そのポート上の TCP および UDP の両方のトラフィックのロード・バランスを取ります。

### マネージャー

次に基づいて、サーバーの重みを設定します。

- 実行プログラムの内部カウンター
- プロトコル・アドバイザーによって提供されたサーバーからのフィードバック
- システム・モニター (MVS アドバイザー) からのフィードバック

マネージャーは、任意選択のコンポーネントです。ただし、ユーザーがマネージャーを使用しない場合、ネットワーク・ディスパッチャーは、現行のサーバーの重みに基づいてラウンドロビン・スケジューリング方式でロードのバランスを取ります。

ネットワーク・ディスパッチャーを使用してステートレス UDP トラフィックのロード・バランスを取る場合は、要求内のあて先 IP アドレスを使用してクライアントに応答したサーバーだけを使用する必要があります。詳しくは、109ページの『ネットワーク・ディスパッチャー用のサーバーの構成』を参照してください。

---

## ネットワーク・ディスパッチャーの高可用性

ネットワーク・ディスパッチャーの基本機能には次のような特性があり、いろいろな観点から、これが単一障害点になることを示しています。

- 入ってくるすべてのトラフィックを調べます。既存の接続への一部のパケットが、異なるネットワーク・ディスパッチャーを経由する異なるパスを使用してサーバーに達する場合、サーバーは即時にその接続をリセットします。
- 確立されたすべての接続を追跡し、それを終了することはありませんが、ネットワーク・ディスパッチャーの接続・テーブルからエントリーが失われると、接続はリセットされます。

## ネットワーク・ディスパッチャーの使用

- それより前のホップ・ルーターからは、それが最終ホップであり、接続の終端であるように見えます。

これらの特性により、次のような障害が発生した場合、クラスター全体にとって重大なものになります。

- 何らかの理由でネットワーク・ディスパッチャーに障害が生じた場合、すべての接続テーブルが失われます。したがって、クライアントからサーバーへの既存の接続もすべて失われます。クライアントをサーバーに誘導できる第 2 のネットワーク・ディスパッチャーが存在すると仮定しても、通常のルーティング・プロトコル遅延 (数分かかることもある) の後でしか、新しい接続を確立することができません。
- 直前の IP ルーターへの構成済みネットワーク・ディスパッチャー・インターフェースに障害が生じた場合、同じネットワーク・ディスパッチャーに到達できる別のインターフェースが存在する必要があります。その場合は IP ルーターによって回復されますが (ARP エージング機構を使用して、数分の遅れで)、そうでない場合は、すべての接続が失われます。
- サーバーにインターフェースするネットワーク・ディスパッチャーに障害が生じた場合、直前のホップ・ルーターはそのネットワーク・ディスパッチャーが最終ホップであるものと想定するので、新しい接続を再ルートしません。既存の接続は失われ、新しい接続は確立されないことになります。

どの障害の場合も (これらは、ネットワーク・ディスパッチャーの障害だけでなく、ネットワーク・ディスパッチャーの近隣の障害でもあります)、すべての既存の接続は失われます。標準 IP 回復機構を搭載したバックアップ用のネットワーク・ディスパッチャーを備えている場合でも、最善の場合でも、回復に時間がかかり、しかも新規の接続にしか適用されません。最悪の場合には、接続は回復しません。

ネットワーク・ディスパッチャーの可用性を高めるために、ネットワーク・ディスパッチャー高可用性機能は、次の機構を使用しています。

- 同じクライアント、同じサーバー・クラスターへの接続性、およびネットワーク・ディスパッチャー相互間の接続性を備えている 2 つのネットワーク・ディスパッチャー。
- ネットワーク・ディスパッチャーの障害を検出するための、2 つのネットワーク・ディスパッチャー間の『ハートビート』機構
- 各ネットワーク・ディスパッチャーから到達できる IP ホストと到達できないホストを識別するための到達可能性基準
- ネットワーク・ディスパッチャー・データベース (つまり、接続テーブル、到達可能性テーブル、およびその他のテーブル) の同期化
- アクティブ・ネットワーク・ディスパッチャー (特定のサーバー・クラスターを担当する) とスタンバイ・ネットワーク・ディスパッチャー (そのサーバー・クラスターに継続的に同期化される) を選ぶ論理
- 論理またはオペレーターがアクティブとスタンバイを切り替えることに決定した場合、迅速に IP の引き継ぎを実行する機構

## 障害の検出

障害検出の基本的基準 (ハートビート・メッセージによって検出される、アクティブ・ネットワーク・ディスパッチャーとスタンバイ・ネットワーク・ディスパッチャー間の接続性の損失) の他に、『到達可能性基準』と呼ばれるもう 1 つの障害検出機構があります。ネットワーク・ディスパッチャーの構成時に、各ネットワーク・ディスパッチャーが正しく作動するために到達可能でなければならないホストのリストを指定します。ホストは、ルーター、IP サーバー、またはその他のタイプのホストが可能です。ホスト到達可能性は、そのホストに PING することによって入手します。

ハートビート・メッセージを送れない場合、あるいはアクティブ・ネットワーク・ディスパッチャーが到達可能性基準を満たさなくなり、スタンバイ・ネットワーク・ディスパッチャーが到達可能である場合、切り替えが行われます。利用可能なあらゆる情報に基づいて決定を下せるように、アクティブ・ネットワーク・ディスパッチャーは、その到達可能性の機能をスタンバイ・ネットワーク・ディスパッチャーに定期的送信します。スタンバイ・ネットワーク・ディスパッチャーは、その機能を自身の機能と比較して、切り替えるかどうかを決定します。

## データベースの同期

1 次用とバックアップ用のネットワーク・ディスパッチャーは、“ハートビート” 機構を使用して、双方のデータベースを同期化します。ネットワーク・ディスパッチャーのデータベースには、接続テーブル、到達可能性テーブル、およびその他の情報が入っています。ネットワーク・ディスパッチャー高可用性機能は、データベース同期プロトコルを使用して、両方のネットワーク・ディスパッチャーの接続テーブルに同じエントリーが含まれているようにします。この同期プロトコルは、既知の伝送遅延の誤差を考慮に入れます。プロトコルは、データベースの初期同期化を行い、その後は定期的に更新してデータベースの同期を維持します。

## 回復方法

ネットワーク・ディスパッチャーに障害が生じた場合、IP 引き継ぎ機構が、速やかにすべてのトラフィックをスタンバイ・ネットワーク・ディスパッチャーに転送します。データベース同期機構によって、スタンバイはアクティブ・ネットワーク・ディスパッチャーと同じエントリーを持つことが保証されています。ネットワーク (クライアントとバック・エンド・サーバー間の中間部分のハードウェアまたはソフトウェア) に障害が発生した場合、作動しているスタンバイ・ネットワーク・ディスパッチャーを通る代替パスが存在するときは、その代替パスを経由するように切り替えられます。

## IP 引き継ぎ

注: クラスタ IP アドレスは、直前のホップ・ルーター (IP ルーター) と同じ論理サブネット上に存在するものと想定しています。

IP ルーターは、ARP プロトコルを用いてクラスター・アドレスを解決します。IP 引き継ぎを行うために、ネットワーク・ディスパッチャー (スタンバイがアクティブになる) は、自分自身に対して ARP 要求を出します。これは、そのクラスターの論



## ネットワーク・ディスパッチャーの使用

理サブネットに属するすべての直接接続ネットワークに同報通信されます。それより前のホップの IP ルーターは、それぞれの ARP テーブルを更新して (RFC826 に従って)、そのクラスターへのすべてのトラフィックを、新たにアクティブになった (前はスタンバイだった) ネットワーク・ディスパッチャーに送るようにします。

---

## ネットワーク・ディスパッチャーの構成

ユーザー・サイトをサポートするネットワーク・ディスパッチャーを構成するには、いろいろな方法があります。ユーザー・サイトにホスト名が 1 つしかなく、すべてのカスタマーがそれに接続する場合は、1 つのクラスターと任意の数のポート (接続を受信する) を定義することができます。この構成を 図5 に示します。

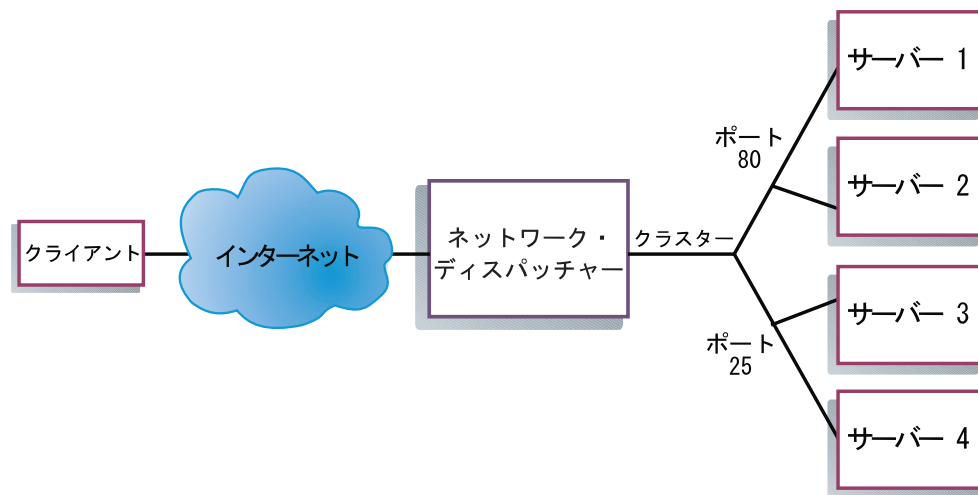


図5. 1 つのクラスターと 2 つのポートを持つように構成されたネットワーク・ディスパッチャーの例

ユーザー・サイトで、複数の会社または部門がそれぞれ異なる URL を使用してサイトにアクセスする競合タイプのホスト接続を行っている場合には、ネットワーク・ディスパッチャーを別の方法で構成する必要があります。この場合は、105 ページの図6 に示すように、各会社または部門ごとに 1 つのクラスターを定義し、その URL で接続を受け取る任意の数のポートを構成することができます。

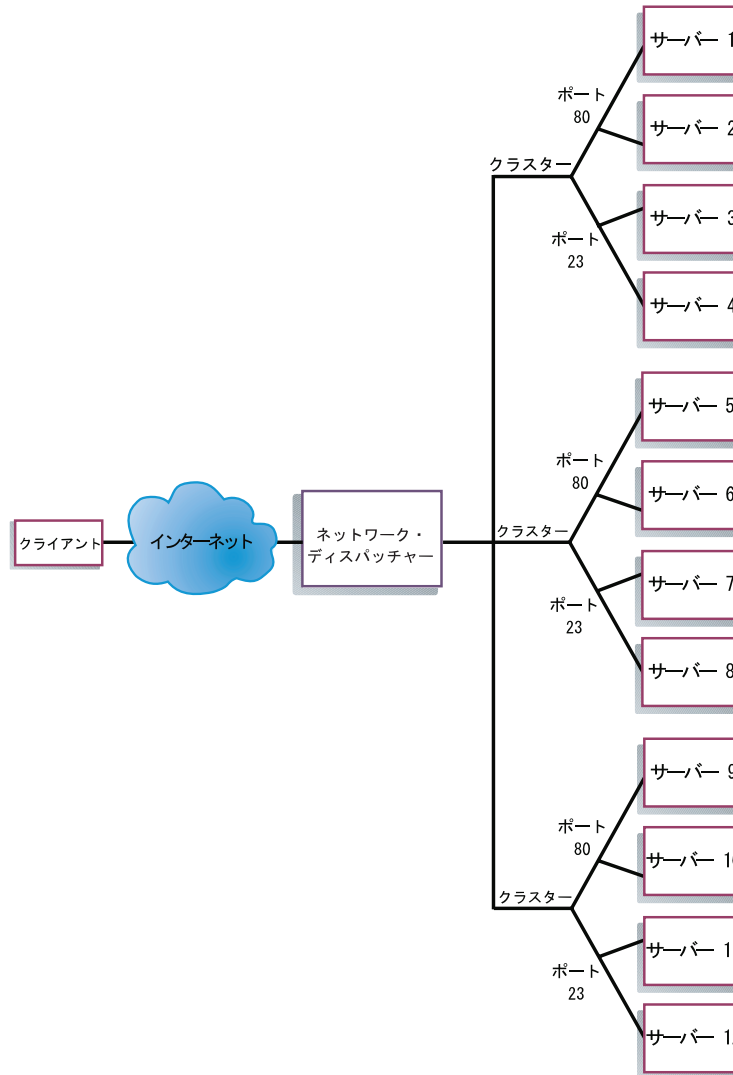


図6. 3つのクラスターと3つのURLを持つように構成されたネットワーク・ディスパッチャーの例

第3のネットワーク・ディスパッチャー構成方法は、サポートされる各プロトコル専用のサーバーが多数ある非常に大規模なサイトに適しています。たとえば、大きなダウンロード可能ファイル専用の直接 T3 回線を、個別の FTP サーバーに構成するといったことが可能です。この場合は、106ページの図7に示すように、各プロトコルについて、1つのポートで複数のサーバーを持つクラスターを定義することができます。

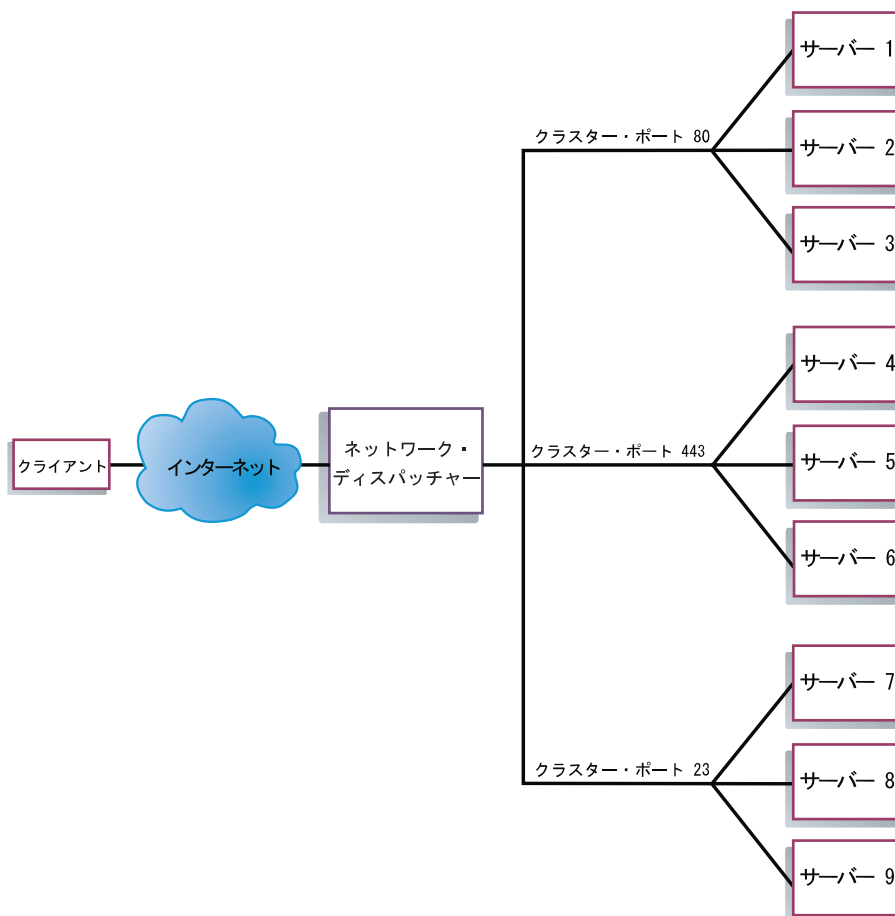


図7.3 3つのクラスターと3つのポートを持つように構成されたネットワーク・ディスパッチャーの例

### 構成ステップ

ネットワーク・ディスパッチャーを構成する前に、次のことを行います。

1. ネットワーク・ディスパッチャーがサーバーへの直接インターフェースを持っていることを確認する。サーバーはエンタープライズ・ルーターまたはインターネットへの独立した接続を持つことができ、これによりサーバーからクライアントへの発信トラフィックは、ネットワーク・ディスパッチャーをバイパスすることができます。ただし、この独立した接続は構成する必要はありません。

ユーザーのネットワークにとって高可用性が重要である場合は、107ページの図8に示した標準的な高可用性構成を参照してください。



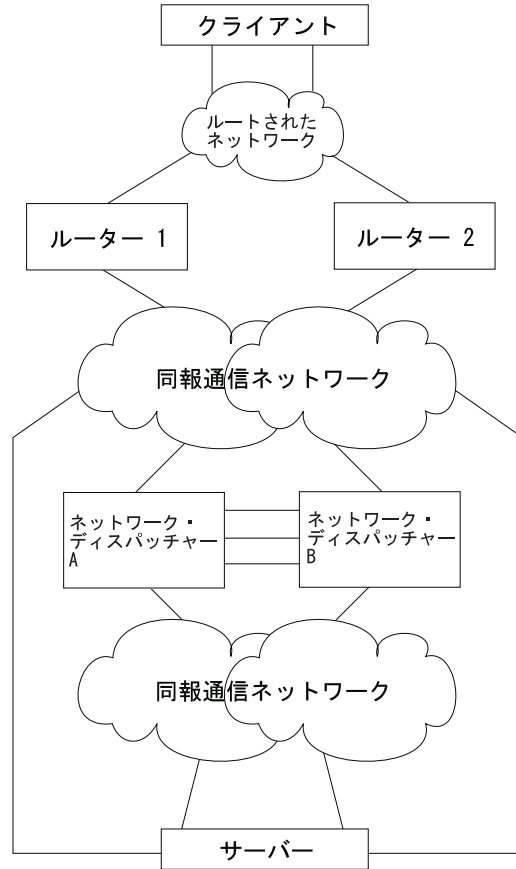


図 8. 高可用性ネットワーク・ディスパッチャー構成

2. 装置のインターフェースを構成する。この構成には、すべてのインターフェース、すべてのインターフェース上の IP アドレス、およびすべての該当するプロトコルが含まれます。ルーターの内部 IP アドレスがネットワーク・ディスパッチャーによって使用されるので、このアドレスも `set internal-ip-address` コマンドを使用して構成する必要があります。内部 IP アドレスは、ネットワーク・ディスパッチャーで構成されたクラスター・アドレスと一致してはなりません。**set internal-ip-address** コマンドについて詳しくは、[プロトコル構成および監視 参照資料 第 1 巻の『IP の構成および監視』](#)を参照してください。
3. 装置をリブートまたはリスタートする。

## IBM 2212 上のネットワーク・ディスパッチャーの構成

IBM 2212 上のネットワーク・ディスパッチャーを構成するには、次のようにします。

1. **feature ndr** コマンドを使用して、ネットワーク・ディスパッチャー機能にアクセスする。
2. **enable executor** および **enable manager** コマンドを使用して、実行プログラムとマネージャーを使用可能にする。
3. **add cluster** コマンドを使用して、クラスターを構成する。ネットワーク・ディスパッチャーは特定のクラスター・アドレスを公示しないので、クラスター・アドレスを選択する必要があります。クラスター・アドレスは、ネットワーク・ディスパッチャー・ルーターの公示されたローカル・サブネットに含まれてい

## ネットワーク・ディスパッチャーの使用

なければなりません。通常このサブネットは、ネットワーク・ディスパッチャーがネクスト・ホップ・ルーターからクライアント・トラフィックを受信するサブネットです。

**注:** クラスターの IP アドレスは、ルーターの内部 IP アドレスと一致してはならず、ルーター上で定義されたインターフェース IP アドレスとも一致してはなりません。

4. 対応するプロトコルにサービスする各サーバー・クラスターに対して、**add port** コマンドを使用して、TCP および UDP あて先ポートを構成する。ポートの例は、HTTP の場合は 80、FTP の場合は 20 または 21、および Telnet の場合は 23 です。
5. **add server** コマンドを使用して、サーバーを構成する。サーバーは、常にポートとクラスターに対応しています。1 つのサーバーは複数のポートにサービスすることができ、1 つのポートは複数のサーバーからサービスを受けることができます。サーバーのオペレーティング・システムが複数の別名をサポートする場合は、1 つのサーバーが複数のクラスターに所属することもできます。
6. **add advisor** コマンドを使用して、アドバイザーを構成する。

**注:**

- a. MVS アドバイザーの場合、どのクラスターにもポート番号値 (デフォルト = 10007) を定義してはなりません。このポート番号は、MVS アドバイザーが MVS システム内の WLM との通信するためにだけ使用します。
  - b. TN3270 アドバイザーの場合は、2 つのポート値を入力します。クライアントとサーバー間の通信に使用するポート番号値 (デフォルト = 23) を、該当するクラスターに定義する必要があります。通信ポート値 (デフォルト = 10008) は、どのクラスターにも定義してはなりません。通信ポート値は、TN3270 アドバイザーが TN3270 サーバーからロード情報を収集するためにだけ使用します。
7. **enable advisor** コマンドを使用して、構成したアドバイザーを使用可能にする。

高可用性のネットワーク・ディスパッチャーを構成している場合は、次のステップを続けてください。そうでない場合は、これで構成は完了です。

**注:** 次のステップは、1 次ネットワーク・ディスパッチャーで実行した後、バックアップでも実行してください。データベースが正しく同期化されるのを確認するために、バックアップの実行プログラムを使用可能にする前に、1 次ネットワーク・ディスパッチャーの実行プログラムを使用可能にしておくことが必要です。

8. **add backup** コマンドを使用して、このネットワーク・ディスパッチャーが 1 次であるかバックアップであるか、または切り替えが手動であるか自動であるかを構成する。
9. **add heartbeat** コマンドを使用して、1 次ネットワーク・ディスパッチャーとバックアップ・ネットワーク・ディスパッチャー間のハートビートを実行するすべてのパスを構成する。パスは、発信元とあて先の IP アドレスで指定します。1 つのインターフェースに障害が起きても、1 次とバックアップ・マシン間のハートビート通信が損なわれないようにするために、1 次とバックアップ・ネットワーク・ディスパッチャー間には、複数のハートビート・パスを構成しておくことを強くお勧めします。

10. 完全なサービスを保証するために、**add reach** コマンドを使用して、ネットワーク・ディスパッチャーが到達できなければならないホスト IP アドレスのリストを構成する。通常は、これはサーバー、エンタープライズ・ルーター、または管理ステーションのサブセットになります。

**set**、**remove**、および **disable** コマンドを使用して、構成を変更することができます。これらのコマンドについて詳しくは、117ページの『第9章 ネットワーク・ディスパッチャー・フィーチャーの構成および監視』を参照してください。

## ネットワーク・ディスパッチャー用のサーバーの構成

ネットワーク・ディスパッチャーを使用するためにサーバーを構成する手順は、次のとおりです。

1. ループバック装置に別名を付ける。

TCP および UDP サーバーが機能するためには、ループバック装置 (通常は **lo0** と呼ばれる) をクラスター・アドレスに設定する (できれば、別名を付ける) ことが必要です。ネットワーク・ディスパッチャーは、パケットをサーバー・マシンに転送する前に、IP パケット内のあて先 IP アドレスを変更しません。ループバック装置をクラスター・アドレスに設定または別名指定した場合、サーバー・マシンはクラスター・アドレスあてのパケットを受け入れます。

サーバーが自分の IP アドレスではなくクラスター・アドレスを使用してクライアントに応答するという事は、重要なことです。このことは、TCP サーバーの場合は問題になりませんが、UDP サーバーの場合は、クラスター・アドレスあてに送信された要求に応答するとき自分の IP アドレスを使用するものが含まれています。サーバーが自分の IP アドレスを使用している場合、一部のクライアントは、それが予期した発信元 IP アドレスからのものではないために、サーバーの応答を廃棄してしまいます。要求からのあて先 IP アドレスをクライアントへの応答に使用する UDP サーバーだけを使用することが必要です。この場合、要求からのあて先 IP アドレスは、クラスター・アドレスです。

ネットワーク・インターフェースの別名指定をサポートするオペレーティング・システム (AIX、Solaris、または Windows NT など) を使用している場合は、ループバック装置の別名をクラスター・アドレスに指定する必要があります。別名をサポートするオペレーティング・システムを使用する利点は、複数のクラスター・アドレスにサービスするようにサーバー・マシンを構成できることです。

別名をサポートしないオペレーティング・システム (HP-UX および OS/2 など) を使用している場合は、**lo0** をクラスター・アドレスとして設定する必要があります。

サーバーが、TCP/IP V3R2 を実行する MVS システムの場合、VIPA アドレスをクラスター・アドレスとして設定する必要があります。これはループバック・アドレスとして機能します。VIPA アドレスは、MVS ノードに直接接続されたサブネットに属してはなりません。MVS システムが TCP/IP V3R3 を実行している場合は、ループバック装置をクラスター・アドレスとして設定する必要があります。高可用性を使用している場合、高可用性引き継ぎ機構を正しく機能させるためには、MVS システム内の RouteD を使用可能にしなければなりません。

**注:** この章に示されているコマンドは、次のオペレーティング・システムおよびレベルでテスト済みです。すなわち、AIX 4.1.5 と 4.2、HP-UX 10.2.0、

## ネットワーク・ディスパッチャーの使用

Linux、OS/2 Warp Connect バージョン 3.0、OS/2 Warp バージョン 4.0、Solaris 2.5 (Sun OS 5.5)、および Windows NT 3.51 と 4.0 です。

ループバック装置の設定または別名指定には、表10 に示すように、ご使用のオペレーティング・システムのコマンドを使用してください。

表 10. ディスパッチャーのループバック装置の別名指定用のコマンド

システム	コマンド
AIX	<b>ifconfig lo0 alias cluster_address</b>
HP-UX	<b>ifconfig lo0 cluster_address</b>
Linux	<b>ifconfig lo:1 cluster_address netmask up</b>
OS/2	<b>ifconfig lo cluster_address</b>
Solaris	<b>ifconfig lo0:1 cluster_address 127.0.0.1 up</b>
Windows NT	<ol style="list-style-type: none"> <li>a. 「スタート」をクリックして、「設定」をクリックします。</li> <li>b. 「コントロール・パネル」をクリックし、「ネットワーク」をダブルクリックします。</li> <li>c. まだ行っていない場合は、MS ループバック・アダプター・ドライバーを追加します。 <ol style="list-style-type: none"> <li>1) 「ネットワーク」ウィンドウで、「アダプター」をクリックします。</li> <li>2) 「MS ループバック・アダプター」を選択して、「OK」をクリックします。</li> <li>3) 指示されたら、インストール CD またはディスクを挿入します。</li> <li>4) 「ネットワーク」ウィンドウで、「プロトコル」をクリックします。</li> <li>5) 「TCP/IP プロトコル」を選択し、「プロパティ」をクリックします。</li> <li>6) 「MS ループバック・アダプター」を選択して、「OK」をクリックします。</li> </ol> </li> <li>d. ループバック・アドレスをクラスター・アドレスとして設定します。デフォルトのサブネット・マスク (255.0.0.0) を受け入れ、ゲートウェイ・アドレスは入力しないでください。  <b>注:</b> 「ネットワークの設定」をいったん終了し、再びこの画面に入らないと、「TCP/IP 構成」の下に「MS ループバック・ドライバー」が表示されないことがあります。</li> </ol>

### 2. 余分なルートがないかチェックする。

一部のオペレーティング・システムでは、デフォルトのルートが作成されており、削除することが必要になる場合があります。

- a. Windows NT 上に余分なルートがないか検査するには、**route print** コマンドを使用します
- b. すべての UNIX システムおよび OS/2 上に余分なルートがないか検査するには、**netstat -nr** コマンドを使用します
- c. Windows NT の例: route print コマンドを入力すると、次のようなテーブルが表示されます。(この例は、デフォルトのネットマスク 255.0.0.0 を使用して、クラスター 9.67.133.158 への余分なルートを検出し、除去する場合は示しています。)

## ネットワーク・ディスパッチャーの使用

```
Active Routes:
Network Address          Netmask  Gateway Address  Interface  Metric
0.0.0.0          0.0.0.0    9.67.128.1      9.67.133.67  1
9.0.0.0          255.0.0.0   9.67.133.158   9.67.133.158  1
9.67.128.0       255.255.248.0  9.67.133.67    9.67.133.67  1
9.67.133.67      255.255.255.255  127.0.0.1     127.0.0.1    1
9.67.133.158     255.255.255.255  127.0.0.1     127.0.0.1    1
9.255.255.255    255.255.255.255  9.67.133.67    9.67.133.67  1
127.0.0.0        255.0.0.0    127.0.0.1     127.0.0.1    1
224.0.0.0        224.0.0.0    9.67.133.158   9.67.133.158  1
224.0.0.0        224.0.0.0    9.67.133.67    9.67.133.67  1
255.255.255.255  255.255.255.255  9.67.133.67    9.67.133.67  1
```

- d. "Gateway・アドレス" 列でクラスター・アドレスを見つけます。余分なルートがある場合、そのクラスター・アドレスは 2 度表示されます。この例では、クラスター・アドレス (9.67.133.158) が 2 行目と 8 行目に表示されています。
- e. クラスター・アドレスが表示されている各行で、ネットワーク・アドレスを見つけます。これらのルートのうちの一方は必要なものであり、他方の余分なルートを削除することが必要です。削除すべき余分なルートは、ネットワーク・アドレスがクラスター・アドレスの第 1 桁で始まっており、その後 3 つのゼロが続いているものです。この例では、余分なルートは 2 行目のもので、そのネットワーク・アドレスは 9.0.0.0 になっています。

```
9.0.0.0          255.0.0.0    9.67.133.158   9.67.133.158  1
```

### 3. 余分なルートを削除する。

余分なルートを削除するには、表11 から、該当するオペレーティング・システムのコマンドを使用します。

表 11. 各種オペレーティング・システムのルート削除コマンド

オペレーティング・システム	コマンド
AIX	<b>route delete -net</b> <i>network_address cluster_address</i>
HP-Unix	<b>route delete</b> <i>cluster_address cluster_address</i>
Solaris	ルートを削除する必要はありません。
OS/2	ルートを削除する必要はありません。
Windows NT	<b>route delete</b> <i>network_address cluster_address</i> 注: このコマンドは MS-DOS プロンプトで入力する必要があります。

## TN3270 でのネットワーク・ディスパッチャーの使用

ネットワーク・ディスパッチャーは、大規模な 3270 環境に TN3270E サーバー・サポートを提供するために TN3270 サーバー機能を稼働している 2210、2212、ネットワーク・ユーティリティ、または 2216 のクラスターで使用することができます。TN3270 アドバイザーを使用して、ネットワーク・ディスパッチャーは各 TN3270E サーバーからのロード統計をリアルタイムで収集し、ロードを TN3270 サーバー間に可能な限り最適に配分することができます。ネットワーク・ディスパッチャー・ルーターの外部の TN3270 サーバーに加えて、クラスター内の TN3270 サーバーの中の 1 台を内部にする、つまりネットワーク・ディスパッチャーと同じルーター内で稼働することができます。



### 構成の要点

TN3270E サーバーの構成は、サーバーの前にネットワーク・ディスパッチャーが存在しても、しなくても、基本的には同じです。事実、TN3270E サーバーは、クライアントからのトラフィックが別のマシンを経由して転送されたかどうかを認知しません。ただし、ネットワーク・ディスパッチャー用に外部 TN3270 サーバーを設定する際には、いくつかの点に注意する必要があります。

- ネットワーク・ディスパッチャーはサーバーに転送するときにパケット内のあて先 IP アドレス (つまり、クラスター・アドレス) を変更しないので、各サーバー内の TN3270 サーバー IP アドレスは、クラスター IP アドレスに等しく設定しなければなりません。
- TN3270 サーバー機能を稼働するルーターは、パケットをサーバー機能に転送するためには、ルーター内で稼働している TN3270 機能の IP アドレスを知っていることが必要です。そのため、各 TN3270 サーバー上でも、TN3270 サーバー IP アドレス (つまり、クラスター・アドレス) をルーターの内部 IP アドレスとして、またはルーターのインターフェースの 1 つの 2 次アドレスとして定義する必要があります。
- TN3270E サーバー上で使用されているルーティング・プロトコル (たとえば、OSPF または RIP) の中に、クラスター・アドレスを公示するものが含まれていないことを確認する必要があります。クライアント・ネットワークに関する限り、ネットワーク・ディスパッチャー・ルーターはクラスター・アドレスを“占有”している必要があります。ネットワーク・ディスパッチャーは特定のクラスター・アドレスを公示しないので、クラスター・アドレスを選択する必要があります。クラスター・アドレスは、ネットワーク・ディスパッチャー・ルーターの公示されたローカル・サブネットに含まれていなければなりません。
- クライアントからネットワーク・ディスパッチャーへのトラフィックが、ネットワーク・ディスパッチャーからサーバーへのトラフィックと同じ LAN 上を流れる場合、クラスター・アドレスへの ARP に対してサーバーが応答しないようにする必要があります。すなわち、サーバーのインターフェース上では、クラスター・アドレスをこの LAN に定義することはできません。クライアントのトラフィックを受け取る LAN 上の ARP に応答するのは、ネットワーク・ディスパッチャーが唯一であるようにする必要があります。その代わりに、クラスター・アドレスを別のインターフェース上のインターフェース・アドレスとして TN3270 サーバー上で構成することもでき、TN3270 サーバーの内部 IP アドレスとして構成することもできます。
- ネットワーク・ディスパッチャー内で、固有なサーバー IP アドレスを指定してそれぞれの TN3270 サーバーを構成する必要があります。TN3270 サーバー機能を実行するルーター上でも、このアドレスをインターフェース・アドレスとして構成する必要があります。

TN3270 サーバーがネットワーク・ディスパッチャーと同じルーター内にある場合は、次のことが当てはまります。

- 内部 TN3270 サーバーの TN3270 サーバー IP アドレスは、クラスター・アドレスに設定する必要があります。ただし、内部サーバーの場合、このアドレスを内部 IP アドレスまたはインターフェース・アドレスとしてルーター上で定義してはなりません。

- TN3270 サーバーが外部にある場合は、TN3270 サーバー IP アドレスを内部 IP アドレスまたはインターフェース・アドレスとしてルーター上で定義する必要があります。TN3270 サーバーが内部にある場合は、TN3270 サーバー IP アドレスを内部 IP アドレスまたはインターフェース・アドレスとしてルーター上で定義してはなりません。TN3270 サーバーは、内部または外部のどちらかとして設定できますが、両方としては設定できず、交互に切り替えることもできません。このため、両方のネットワーク・ディスパッチャー・ルーター内に、内部 TN3270 サーバーを使用してネットワーク・ディスパッチャー高可用性ソリューションを設定する際は、一方のルーターのネットワーク・ディスパッチャーは他方のルーターの TN3270 サーバーとロード・バランスを取ることができません。ネットワーク・ディスパッチャーは、自身の内部サーバー、および外部サーバーとして設定されたサーバーすべてとロード・バランスを取ることができます。

## 明示的な LU とネットワーク・ディスパッチャー

ネットワーク・ディスパッチャー環境で明示的 LU を定義する場合は、特別な注意が必要です。暗黙的または明示的 LU へのセッション要求を、任意のサーバーに転送することができます。このことは、どのサーバーにセッションが転送されるのかは前もって分からないので、明示的 LU は各サーバーに定義しておく必要があることを意味しています。

---

## Web サーバー・キャッシュでのネットワーク・ディスパッチャーの使用

Web サーバー・キャッシュ用のクラスターとポートを定義するには、ネットワーク・ディスパッチャーを使用する必要があります。cache モードを指定してポートを定義する場合は、キャッシュ区画を構成するように指示するプロンプトが出されます。この例については、201ページの『第12章 Web サーバー・キャッシュの構成と監視』の **add port** コマンドを参照してください。キャッシュ区画の構成値は、Config> プロンプトで **f webc** コマンドを使用して Web サーバー・キャッシュのフィーチャー構成に直接進むことにより、後から更新できます。Web サーバー・キャッシュについて詳しくは、159ページの『第11章 Web サーバー・キャッシュの使用』、および 201ページの『第12章 Web サーバー・キャッシュの構成と監視』を参照してください。

---

## eNetwork ホスト・オンデマンド・クライアント・キャッシュでのネットワーク・ディスパッチャーの使用

ホスト・オンデマンド・クライアント・キャッシュ用のクラスターとポートを定義するには、ネットワーク・ディスパッチャーを使用する必要があります。hod client cache モードを指定してポートを定義する場合は、キャッシュ区画を構成するように指示するプロンプトが出されます。この例については、145ページの『ホスト・オンデマンド・クライアント・キャッシュの構成』の **add port** コマンドを参照してください。キャッシュ区画の構成値は、Config> プロンプトで **f hod** コマンドを使用してホスト・オンデマンド・クライアント・キャッシュのフィーチャー構成に直接進むことにより、後から更新できます。ホスト・オンデマンド・クライアント・キャッシュについて詳しくは、145ページの『第10章 IBM eNetwork ホスト・オンデマンド・クライアント・キャッシュの構成と監視』を参照してください。

## スケーラブル高可用性キャッシュ (SHAC) でのネットワーク・ディスパッチャーの使用

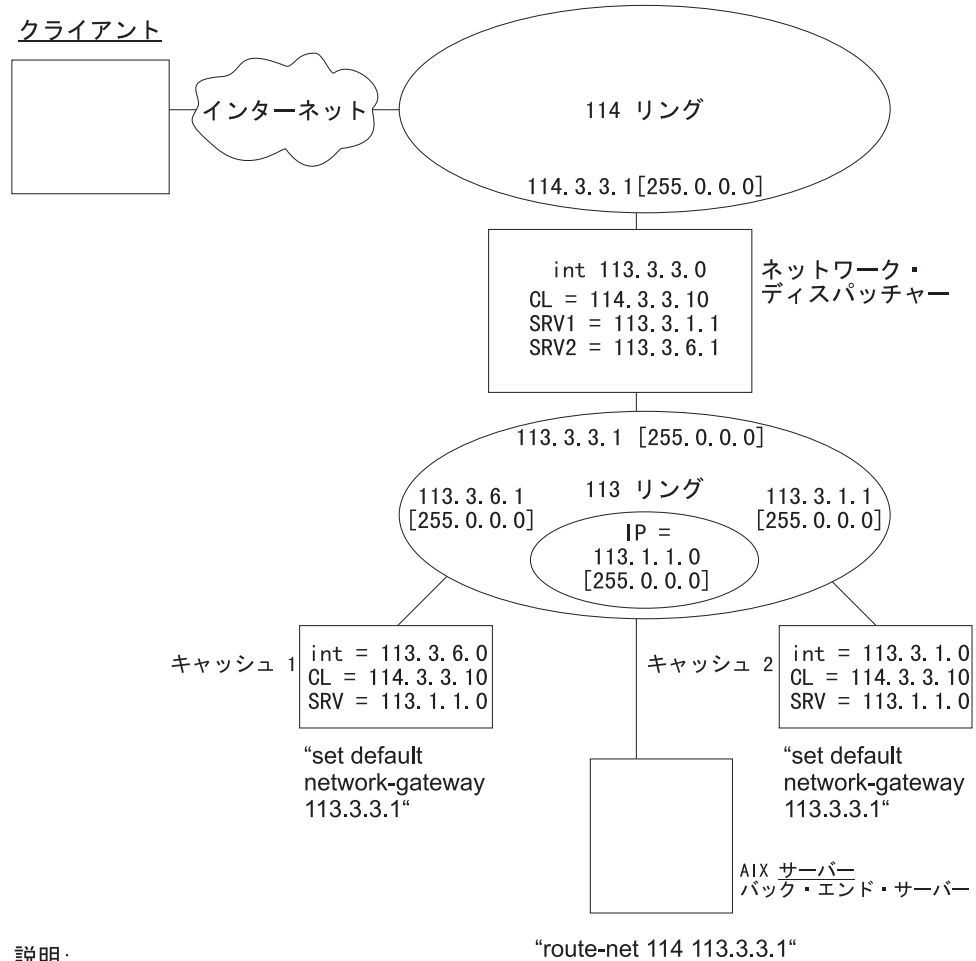
ここでは、スケーラブル高可用性キャッシュ (SHAC) に対するネットワーク・ディスパッチャーの使用について説明し、115ページの図9 にネットワーク内での SHAC を示します。スケーラブル高可用性キャッシュ (SHAC) は、Web サーバー・キャッシュのグループと、分離したネットワーク・ディスパッチャーで成り立っています。キャッシュは、ネットワーク・ディスパッチャー内ではサーバーとして構成されます。グループ内のキャッシュは、共通のクラスターとポートを共有します。ネットワーク・ディスパッチャー内では、同一のクラスター値とポート値がプログラムされます。ポートのモードは `extcache` に設定され、これはポートが外部スケーラブル・キャッシュ配列を送ることを示します。118ページの『Add』の `add port` コマンドを参照してください。

**注:** ネットワーク・ディスパッチャーに複数のキャッシュ・グループを配置できません。

アドバイザーとマネージャーは、SHAC に不可欠なものです。SHAC が存在するポート上では、HTTP アドバイザーを使用可能にする必要があります。構成されたキャッシュが操作可能かどうかを判別するために、アドバイザー照会が使用されます。初期の接続確立時には、マネージャーに基づいて接続がキャッシュまでルーティングされます。したがって、アドバイザーを組み込むようにマネージャーの比率を設定する必要があります。これは、キャッシュが使用可能または使用不可になった場合に重要です。

他のサーバーと同様に、キャッシュのインターフェース IP アドレスがサーバー・アドレスとして使用されます。115ページの図9 はその一例です。このアドレスには、重要な IP アドレス、ネットマスク、およびルーティング情報が含まれています。実際には、ほとんどのクライアントはインターネット上にあります。どのような場合でも、クライアントからキャッシュへのルートはネットワーク・ディスパッチャーを通過する必要があります (したがって、クライアントは図の 113 には接続できません)。





説明:

CL: クラスター・アドレス。注-この例では、ポート 80 (デフォルト http ポート) の使用が想定されています。

INT: 22XX ルーターの内部アドレス

SRV: CL に関連したサーバー・アドレス

"...": 接続を確立するための追加のルーティング・コマンド

図9.2 2つのキャッシュと、ネットワーク・ディスパッチャー、クライアント、およびバックエンド・サーバー



## 第9章 ネットワーク・ディスパッチャー・フィーチャーの構成および監視

この章では、ネットワーク・ディスパッチャー・フィーチャーの構成コマンドおよび動作コマンドについて説明します。この章には、次の内容が記載されています。

- 『ネットワーク・ディスパッチャー構成コマンドへのアクセス』
- 『ネットワーク・ディスパッチャー構成コマンド』
- 137ページの『ネットワーク・ディスパッチャー監視コマンドへのアクセス』
- 137ページの『ネットワーク・ディスパッチャー監視コマンド』

### ネットワーク・ディスパッチャー構成コマンドへのアクセス

ネットワーク・ディスパッチャー構成環境にアクセスするには、次のようにします。

1. OPCON プロンプト (\*) で **talk 6** と入力する。
2. Config > プロンプトで **feature ndr** コマンドを入力する。

### ネットワーク・ディスパッチャー構成コマンド

表12 は、ネットワーク・ディスパッチャー構成コマンドの要約を示しており、表の後に個々のコマンドの説明があります。これらのコマンドは NDR Config > プロンプトで入力します。

表12. ネットワーク・ディスパッチャー構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxixページの『ヘルプの入手』を参照してください。
Add	ネットワーク・ディスパッチャーの各種のコンポーネント (アドバイザー、クラスター、ポート、およびサーバーを含む) を構成します。
Clear	ネットワーク・ディスパッチャー構成全体を消去します。
Disable	ネットワーク・ディスパッチャーのバックアップ、実行プログラム、およびマネージャー・コンポーネントを使用不可にします。特定のアドバイザーも使用不可にします。
Enable	ネットワーク・ディスパッチャーのバックアップ、実行プログラム、およびマネージャー・コンポーネントを使用可能にします。特定のアドバイザーも使用可能にします。
List	ネットワーク・ディスパッチャー構成全体または構成の特定部分を表示します。
Remove	ネットワーク・ディスパッチャー構成の特定部分を除去します。
Set	アドバイザー、クラスター、ポート、サーバー、またはネットワーク・ディスパッチャー・マネージャーの構成パラメーターを変更します。
Exit	直前のコマンド・レベルに戻ります。 xxxixページの『下位レベル操作環境の終了』を参照してください。

## Add

**add** コマンドは、アドバイザー、クラスター、ポート、サーバー、および到達可能アドレスを構成するのに使用します。高可用性の場合には、このネットワーク・ディスパッチャーが1次かバックアップかを構成することができ、ハートビートおよびデータベース同期に使用するIPアドレスも構成できます。

構文:

```

add                advisor . . .
                    backup . . .
                    cluster . . .
                    heartbeat . . .
                    port . . .
                    reach . . .
                    server . . .
    
```

**Advisor** *name port# interval timeout comm-port*

アドバイザーの名前とポートを指定します。このパラメーターは、アドバイザーが特定のプロトコルに関する情報を収集する頻度、およびアドバイザーがプロトコルを利用不能と見なすまでに必要な時間数も指定します。

**name** アドバイザーのタイプを指定します。

表 13. アドバイザー名とポート番号

アドバイザー番号	アドバイザー名	デフォルト・ポート番号
0	FTP	21
1	HTTP	80
2	MVS	10007
3	TN3270	23
4	SMTP	25
5	NNTP	119
6	POPS	110
7	TELNET	23

有効値: 0 ~ 7

デフォルト値: 1

**port#** このアドバイザーのポート番号を指定します。

有効値: 1 ~ 65535

デフォルト値: 表13 を参照

**interval**

アドバイザーが各サーバーのプロトコルを照会する頻度 (秒数) を指定します。この値の半分の時間、サーバーから応答がないと、アドバイザーはそのプロトコルを利用不能と見なします。

有効値: 0 ~ 65535

デフォルト値: 5

**timeout**

アドバイザーがプロトコルを利用不能と見なすまでに必要な時間間隔 (秒数) を指定します。

マネージャーは、ロード・バランシングを決めるのに古い情報が使用されるのを防止するために、タイム・スタンプがこのパラメーターで設定された時刻より古いアドバイザーからの情報は使用しません。アドバイザー・タイムアウトは、アドバイザー・ポーリング間隔より大きい値でなければなりません。タイムアウトの方が小さいと、マネージャーは使用する必要がある報告を無視してしまいます。デフォルトでは、アドバイザーの報告はタイムアウトになりません。

このタイムアウト値は通常、アドバイザーを使用不可にした場合に適用されます。このパラメーターを、前に説明した `interval/2` タイムアウト (これは、サーバーの応答がない時間に関するものです) と混同しないでください。

**有効値:** 0 ~ 65535

**デフォルト値:** 0、これは、プロトコルは常に利用可能と見なされることを意味しています。

**Comm-port**

TN3270 アドバイザーが TN3270 サーバーと通信するのに使用するポート番号を指定します。このパラメーターは、TN3270 アドバイザーの入力にだけ使用します。

**有効値:** 1 ~ 65535

**デフォルト値:** 10008

**注:** マネージャー・コンポーネントはアドバイザーの前提条件なので、アドバイザーを使用可能にする前に、マネージャーを使用可能にしておく必要があります。ロード・バランシングの決定に使用されるサーバーの重みを設定する際に、マネージャーがアドバイザーの入力を考慮するようにマネージャーの比率を設定する必要があります。アドバイザーが正しく稼働するためには、**set internal-ip-address** コマンドを使用して、内部 IP アドレスを設定しておくことも必要です。**set internal-ip-address** コマンドについて詳しくは、プロトコル構成および監視 参照資料 第 1 巻の『IP の構成および監視』を参照してください。

**例 1:**

```
add advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nnntp,6=pop3,7=telnet) [1]? 1
Port number [80]?
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 10
```

**例 2:**

```
add advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nnntp,6=pop3,7=telnet) [1]? 3
Port number [23]?
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 10
Communication Port number [10008]?
```

## ネットワーク・ディスパッチャーの構成

### **backup** *role strategy*

このネットワーク・ディスパッチャーがバックアップであるか、1次であるかを指定します。

**role** これが1次ネットワーク・ディスパッチャーであるか、バックアップ・ネットワーク・ディスパッチャーであるかを定義します。このコマンドは、冗長構成を使用し、高可用性機能を実行したい場合にだけ使用します。その場合には、ハートビート (**add heartbeat**) および到達可能性 (**add reach**) も構成する必要があります。

有効値: 0 または 1

0 = 1次

1 = バックアップ

デフォルト値: 0

### **strategy**

ネットワーク・ディスパッチャーは、自動的に1次モードに戻るのか、手動で戻すのかを指定します。1次ネットワーク・ディスパッチャーに障害が起きてスタンバイになり (バックアップがIP引き継ぎ機能を実行したことを意味します)、その後で再び利用可能になったとき、*strategy* が *automatic* に設定されている場合は、データベースが同期されるとただちに自動的に活動ネットワーク・ディスパッチャーになります。*strategy* が *manual* に設定されている場合、元の1次はスタンバイ・モードになり、オペレーターが **talk 5** で **switchover** コマンドを使用しないと、再びそれを活動状態にすることはできません。144ページの『Switchover』を参照してください。

有効値: 0 または 1

0 = 自動

1 = 手動

デフォルト値: 0

### 例:

```
add backup
Role (0=Primary, 1=Backup) [0]?
Switch back strategy (0=Auto, 1=Manual) [0]?
```

### **cluster** *address FIN-count FIN-timeout Stale-timer*

クラスタのIPアドレス、および実行プログラムがネットワーク・ディスパッチャー・データベースから不要情報収集を行う頻度を指定します。ネットワーク・ディスパッチャーは特定のクラスタ・アドレスを公示しないので、クラスタ・アドレスを選択する必要があります。クラスタ・アドレスは、ネットワーク・ディスパッチャー・ルーターの公示されたローカル・サブネットに含まれていなければなりません。通常このサブネットは、ネットワーク・ディスパッチャーがネクスト・ホップ・ルーターからクライアント・トラフィックを受信するサブネットです。

**注:** クラスタのIPアドレスは、ルーターの内部IPアドレスと一致してはならず、ルーター上で定義されたインターフェースIPアドレスとも一致してはなりません。

**address**

クラスターの IP アドレスを指定します。

**有効値:** 任意の有効な IP アドレス

**デフォルト値:** 0.0.0.0

**FIN-count**

実行プログラムが *FIN-timeout* または *Stale-timer* の経過後にネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みる前に、FIN 状態にあることが必要な接続の数を指定します。

**有効値:** 0 ~ 65535

**デフォルト値:** 4000

**FIN-timeout**

接続が FIN 状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みます。

**有効値:** 0 ~ 65535

**デフォルト値:** 30

**Stale-timer**

接続が非活動状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから接続の情報の除去を試みます。

**有効値:** 0 ~ 65535

**デフォルト値:** 1500

**例:**

```
NDR Config>add cluster
Cluster Address [0.0.0.0]? 113.3.1.12
FIN count [4000]?
FIN time out [30]?
Stale timer [1500]?
Cluster 113.3.1.12 has been added.
Fincount has been set to 4000 for cluster 113.3.1.12
Fintimeout has been set to 30 for cluster 113.3.1.12
Staletimer has been set to 1500 for cluster 113.3.1.12
NDR Config>
```

**heartbeat address1 address2**

ハートビート・メッセージ用の 1 つのパスを指定します。高信頼性の作動を行うためには、複数のエントリを構成することをお勧めします。ハートビート・メッセージは、*address1* (このネットワーク・ディスパッチャーに属する) から *address2* (相手のネットワーク・ディスパッチャーに属する) へ流れます。

**address1**

ハートビート・メッセージの発信元のこのネットワーク・ディスパッチャーのインターフェースの IP アドレスを指定します。

**有効値:** 任意の IP アドレス

**デフォルト値:** 0.0.0.0

**address2**

ハートビート・メッセージのあて先のピア・ネットワーク・ディス

## ネットワーク・ディスパッチャーの構成

パッチャーのインターフェースの IP アドレスを指定します。このアドレスは、*address1* に指定されたインターフェースから到達可能でなければなりません。

**有効値:** 任意の IP アドレス

**デフォルト値:** 0.0.0.0

**例:**

```
add heartbeat
Source Heartbeat address [0.0.0.0]? 131.2.25.90
Target Heartbeat Address [0.0.0.0]? 131.2.25.92
```

**port** *cluster-address port# port-type max-weight port-mode*  
ポートとポートの属性を指定します。

### cluster-address

クラスターの IP アドレスを指定します。

**有効値:** 任意の IP アドレス

**デフォルト値:** 0.0.0.0

**port#** このクラスターのプロトコルのポート番号を指定します。

**有効値:** 1 ~ 65535

**デフォルト値:** 80

### port-type

このポートでロード・バランスを取ることができる IP トラフィックのタイプを指定します。サポートされるタイプは、次のとおりです。

- 1 = TCP
- 2 = UDP
- 3 = 両方

**有効値:** 1、2、3

**デフォルト値:** 3

### max-weight

このポート上のサーバーの最大重みを指定します。これは、実行プログラムが各サーバーに分配する要求数の相違に影響します。

**有効値:** 0 ~ 100

**デフォルト値:** 20

### port-mode

ポートが、1 つのクライアントからの要求をすべて 1 つのサーバーに送る (sticky と呼ばれる) か、パッシブ ftp を使用する (pftp) か、Web サーバー・キャッシュ を使用する (cache) か、外部スケーラブル・キャッシュ配列を送る (extcache) か、ホスト・オンデマンド・クライアント・キャッシュを使用するか、またはこのクラスターでは特定のプロトコルを使用しない (none) かを指定します。

**有効値:** 0 ~ 5。ただし、

- 0 = none



- 1 = sticky
- 2 = pftp
- 3 = cache
- 4 = extcache
- 5 = hod client cache

デフォルト値: 0

**例:**

```
Config>feature ndr
NDR>add cluster 1.2.3.4 4000 30 1500
NDR>add port
Cluster address [0.0.0.0]? 1.2.3.4
Port number [80]? 80
Port type [3]?
Maximum weight [20]?
Port mode [0=none, 1=sticky, 2=pftp, 3=cache 4=extcache 5=hod client cache ]? 0
```

**注:**

1. ポート・モード 3 (cache=3) を選択した場合は、Web サーバー・キャッシュについて 201ページの『第12章 Web サーバー・キャッシュの構成と監視』を参照してください。
2. ポート・モード 5 (hod client cache=5) を選択した場合は、Web サーバー・キャッシュについて 145ページの『第10章 IBM eNetwork ホスト・オンデマンド・クライアント・キャッシュの構成と監視』を参照してください。

**reach address**

ネットワーク・ディスパッチャーが正しく動作するために到達可能であることが必要なホスト・アドレスを指定します。これは、サーバー・アドレス、ルーター・アドレス、管理ステーション・アドレス、あるいはその他の IP ホストのいずれでも構いません。

**address**

ターゲット IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

**例:**

```
add reach
Address to reach [0.0.0.0]?
```

**server cluster-address port# server-address server-weight server-state**

クラスター内のサーバーの属性を指定します。

**cluster-address**

このサーバーが属するクラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

**port#** このサーバーへの接続を介して実行されるプロトコルを指定します。

有効値: 1 ~ 65535

デフォルト値: 80

## ネットワーク・ディスパッチャーの構成

### server-address

サーバーの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

### server-weight

実行プログラムのために、サーバーの重みを指定します。これは、ネットワーク・ディスパッチャーがこの特定サーバーに要求を送信する頻度に影響を与えます。

有効値: 0 ~ add port コマンドで指定した *max-weight* の値

デフォルト値: port コマンドの *max-weight* の値

### server-state

実行プログラムが処理を開始するときに、サーバーを利用可能と見なすか、利用不能と見なすかを指定します。

有効値: 0 (ダウン) または 1 (アップ)

デフォルト値: 1

例:

```
add server
Cluster address [0.0.0.0]? 131.2.25.91
Port number [80]? 80
Server address [0.0.0.0]? 131.2.25.94
Server weight [35]?
Server state (down=0 up=1) [1]?
```

## パラメーター構成の制限

表14 は、ネットワーク・ディスパッチャーに構成できる種々の項目の制限を示しています。

表 14. パラメーター構成の制限

パラメーター	制限
アドバイザー	8 / 2212
クラスター	32 / 2212
ハートビート	8 / 2212
ポート	8 / クラスター
リーチ	8 / 2212
サーバー	32 / 構成されたポート、128 / 構成されたすべてのクライアントの もとの各ポート番号
固有のサーバー IP ア ドレス	32 / 2212

## Clear

**clear** コマンドは、ネットワーク・ディスパッチャー構成全体を消去するのに使用します。

構文:

**clear**

## Disable

**disable** コマンドは、ネットワーク・ディスパッチャーのコンポーネントを使用不可にするのに使用します。

構文:

```
disable          advisor . . .
                   backup
                   executor
                   manager
```

**advisor** *name port#*

ネットワーク・ディスパッチャーからアドバイザを使用不可にします。

**name** アドバイザのタイプを指定します。

詳しくは、118ページの表13 を参照してください。

有効値: 0 ~ 7

デフォルト値: 0

**port#** このアドバイザのポート番号を指定します。

有効値: 1 ~ 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

例:

```
disable advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nnntp,6=pop3,7=telnet) [1]? 1
Port number [0]? 80
```

**backup**

ネットワーク・ディスパッチャーのバックアップ機能を使用不可にします。

例:

```
disable backup
Backup is now disabled.
```

**executor**

ネットワーク・ディスパッチャーの実行プログラムを使用不可にします。実行プログラムを使用不可にすると、ネットワーク・ディスパッチャー機能は使用不可になります。

例:

```
disable executor
Executor is now disabled.
```

**注:** 実行プログラムを使用不可にすると、マネージャー、アドバイザ、および高可用性機能は停止します (現在、稼働している場合)。

**manager**

ネットワーク・ディスパッチャーのマネージャーを使用不可にします。マネージャーは、任意選択のコンポーネントです。ただし、ユーザーがマネージ

## ネットワーク・ディスパッチャーの構成

ャーを使用しない場合、ネットワーク・ディスパッチャーは、現行のサーバーの重みに基づいてラウンドロビン・スケジューリング方式でロードのバランスを図ります。

例:

```
disable manager
Manager is now disabled.
```

注: マネージャーはアドバイザーの前提条件なので、マネージャーを使用不可にすると、すべてのアドバイザーは稼働を停止します。

## Enable

**enable** コマンドは、ネットワーク・ディスパッチャーのコンポーネントを使用可能にするのに使用します。

構文:

```
enable                advisor . . .
                        backup
                        executor
                        manager
```

**advisor** *name port#*

ネットワーク・ディスパッチャーに対してアドバイザーを使用可能にします。

**name** アドバイザーのタイプを指定します。

詳しくは、118ページの表13 を参照してください。

有効値: 0 ~ 7

デフォルト値: 0

**port#** このアドバイザーのポート番号を指定します。

有効値: 1 ~ 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

例:

```
enable advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nnntp=6=pop3,7=telnet) [1]? 1
Port number [0]? 80
```

注: マネージャー・コンポーネントはアドバイザーの前提条件なので、アドバイザーを使用可能にする前に、マネージャーを使用可能にしておく必要があります。ロード・バランシングの決定に使用されるサーバーの重みを設定する際に、マネージャーがアドバイザーの入力を考慮するようにマネージャーの比率を設定する必要があります。アドバイザーが正しく稼働するためには、**set internal-ip-address** コマンドを使用して、内部 IP アドレスを設定しておくことも必要です。**set internal-ip-address** コマンドについて詳しくは、『プロトコル構成および監視 参照資料 第 1 巻』の『IP の構成および監視』を参照してください。

**backup**

ネットワーク・ディスパッチャーのバックアップ機能を使用可能にします。

**例: enable backup**

**注:** バックアップを使用可能にする前に、少なくとも 1 つのハートビートを追加する必要があります。

**executor**

ネットワーク・ディスパッチャーの実行プログラムを使用可能にします。

**例:**

```
enable executor
Executor is now enabled.
```

**manager**

ネットワーク・ディスパッチャーのマネージャーを使用可能にします。

**例:**

```
enable manager
Manager interval was set to 2.
Manager proportions were set to 50 50 0 0
Manager refresh cycle was set to 2
Manager sensitivity was set to 5.
Manager smoothing factor was set to 1.50.
```

初めてマネージャーを使用可能にすると、次のデフォルト値を使用して、マネージャー・レコードが作成されます。

<b>Interval:</b>	2 秒
<b>Refresh-Cycle:</b>	2
<b>Sensitivity:</b>	5 %
<b>Smoothing:</b>	1.5
<b>Proportions:</b>	
	<b>Active:</b> 50%
	<b>New:</b> 50%
	<b>Advisor:</b> 0
	<b>System:</b> 0

上記のパラメーターについての説明は、131ページの『Set』を参照してください。

**List**

**list** コマンドは、ネットワーク・ディスパッチャーに関する情報を表示するのに使用します。

**構文:**

```
list all
      advisor
      backup
```

## ネットワーク・ディスパッチャーの構成

cluster  
manager  
port  
server

**all** すべてのネットワーク・ディスパッチャー構成情報を表示します。これには、アドバイザー、バックアップ、クラスター、マネージャー、ポート、およびサーバーに対して表示される情報と同じものが含まれています。

### 例:

```
NDR Config> list all
```

```
Executor: Enabled
```

```
Manager: Enabled
```

Interval	Refresh-Cycle	Sensitivity	Smoothing	
2	2	5 %	1.50	
Proportions:	Active	New	Advisor	System
	50 %	50 %	0 %	0 %

#### Advisor:

Name	Port	Interval	TimeOut	State	CommPort
http	80	5	0	Enabled	
MVS	10007	15	0	Enabled	
TN3270	23	5	0	Enabled	10008

#### Backup: Enabled

Role	Strategy
PRIMARY	AUTOMATIC

Reachability:	Address	Mask	Type
	131.2.25.93	255.255.255.255	HOST
	131.2.25.94	255.255.255.255	HOST

#### HeartBeat Configuration:

Source Address:	131.2.25.90	Target Address:	131.2.25.92
Source Address:	132.2.25.90	Target Address:	132.2.25.92

#### Clusters:

Cluster-Addr	FIN-count	FIN-timeout	Stale-timer
131.2.25.91	4000	30	1500

#### Ports:

Cluster-Addr	Port#	Weight	Port-Mode	Port-Type
131.2.25.91	23	20 %	none	TCP
131.2.25.91	80	20 %	none	Both

#### Servers:

Cluster-Addr	Port#	Server-Addr	Weight	State
131.2.25.91	23	131.2.25.93	20 %	up
131.2.25.91	23	131.2.25.94	20 %	up
131.2.25.91	80	131.2.25.93	20 %	up
131.2.25.91	80	131.2.25.94	20 %	up

### advisor

ネットワーク・ディスパッチャーのアドバイザーの構成を表示します。

### backup

ネットワーク・ディスパッチャーのバックアップ構成を表示します。

### cluster

ネットワーク・ディスパッチャーのクラスターの構成を表示します。

### manager

ネットワーク・ディスパッチャーのマネージャーの構成を表示します。

### port

ネットワーク・ディスパッチャーのポートの構成を表示します。

### server

ネットワーク・ディスパッチャーのクラスターに対応するサーバーの構成を表示します。

## Remove

**remove** コマンドは、ネットワーク・ディスパッチャー構成の一部を削除するのに使用します。

構文:

```

remove
    advisor . . .
    backup
    cluster . . .
    heartbeat . . .
    port . . .
    reach . . .
    server . . .

```

**advisor** *name port#*

ネットワーク・ディスパッチャー構成から特定のアドバイザーを除去します。

**name** アドバイザーのタイプを指定します。

詳しくは、118ページの表13 を参照してください。

有効値: 0 ~ 7

デフォルト値: 0

**port#** このアドバイザーのポート番号を指定します。

有効値: 1 ~ 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

例:

```

remove advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet) [0]?
Advisor port [0]? 80

```

**backup**

高可用性機能を除去します。

**注:** バックアップは、ハートビートおよびリーチ機能の前提条件なので、バックアップを除去すると、ハートビートおよびリーチは稼働を停止します。

例: **remove backup**

**cluster** *address*

ネットワーク・ディスパッチャー構成からクラスターを除去します。

**address**

クラスターの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

## ネットワーク・ディスパッチャーの構成

注: クラスターを除去すると、そのクラスターに関連したすべてのポートおよびサーバーも除去されます。

例:

```
remove cluster
WARNING: Deleting a cluster will make any port or server
        associated with it to also be deleted.
Cluster address [0.0.0.0]? 131.2.25.91
```

### heartbeat *address*

ネットワーク・ディスパッチャー構成からハートビート・アドレスを除去します。

#### address

ターゲット・ネットワーク・ディスパッチャーの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

例:

```
remove heartbeat
Target address [0.0.0.0]? 131.2.25.92
```

### port *cluster-address port#*

ネットワーク・ディスパッチャー構成内の特定クラスターからポートを除去します。

#### cluster-address

クラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

**port#** このクラスターのプロトコルのポート番号を指定します。

有効値: 1 ~ 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

注:

1. ポートを除去すると、そのポートに関連したすべてのサーバーも除去されます。
2. 除去するポートのポート・モードがキャッシュの場合、関連した Web サーバー・キャッシュのプロキシ構成も除去されます。
3. 除去するポートのポート・モードがホスト・オンデマンド・クライアント・キャッシュの場合、関連したホスト・オンデマンド・クライアント・キャッシュのプロキシ構成も除去されます。

例:

```
remove port
WARNING: Deleting a port will make any server
        associated with it also be deleted.  [0.0.0.0]? 7.82.142.15
Port number [0]? 80
Cluster address [0.0.0.0]? 20.21.22.15
```



**reach** *address*

ネットワーク・ディスパッチャーが到達可能であることが必要なホストのリストからサーバーを除去します。

**address**

クラスターの IP アドレスを指定します。

**有効値:** 任意の IP アドレス

**デフォルト値:** 0.0.0.0

**例:**

```
remove reach
Target address [0.0.0.0]? 9.82.142.15
```

**server** *cluster-address port# server-address*

ネットワーク・ディスパッチャー構成内のクラスターとポートからサーバーを除去します。

**cluster-address**

クラスターの IP アドレスを指定します。

**有効値:** 任意の IP アドレス

**デフォルト値:** 0.0.0.0

**port#** このクラスターのプロトコルのポート番号を指定します。

**有効値:** 1 ~ 65535

**デフォルト値:** なし。ユーザーがポート番号を入力する必要があります。

**server-address**

クラスターの IP アドレスを指定します。

**有効値:** 任意の IP アドレス

**デフォルト値:** 0.0.0.0

**例:**

```
remove server
Cluster address [0.0.0.0]? 7.82.142.15
Port number [0]? 80
Server address [0.0.0.0]? 20.21.22.15
```

## Set

**set** コマンドは、既存のアドバイザー、クラスター、ポート、またはサーバーの属性を変更するのに使用します。ネットワーク・ディスパッチャーのマネージャーの属性を定義することもできます。

**構文:**

```
set advisor . . .
      cluster . . .
      manager . . .
      port . . .
```

`server . . .`

**advisor** *name port# interval timeout comm-port*

アドバイザのポート番号、インターバル、およびタイムアウトを変更します。

**name** アドバイザのタイプを指定します。

詳しくは、118ページの表13 を参照してください。

有効値: 0 ~ 7

デフォルト値: 0

**port#** このアドバイザのポート番号を指定します。

有効値: 1 ~ 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

**interval**

アドバイザが各サーバーのプロトコルを照会する頻度を指定します。この値の半分の時間が、サーバーから応答がないまま満了すると、アドバイザはそのプロトコルを利用不能と見なします。

有効値: 0 ~ 65535

デフォルト値: 5

**timeout**

アドバイザがプロトコルを利用不能と見なすまでに必要な時間間隔 (秒数) を指定します。

マネージャは、ロード・バランシングを決めるのに古い情報が使用されるのを防止するために、タイム・スタンプがこのパラメータで設定された時刻より古いアドバイザからの情報は使用しません。アドバイザ・タイムアウトは、アドバイザ・ポーリング間隔より大きい値でなければなりません。タイムアウトの方が小さいと、マネージャは使用する必要がある報告を無視してしまいます。デフォルトでは、アドバイザの報告はタイムアウトになりません。

このタイムアウト値は通常、アドバイザを使用不可にした場合に適用されます。このパラメータを、前に説明した `interval/2` タイムアウト (これは、サーバーの応答がない時間に関するものです) と混同しないでください。

有効値: 0 ~ 65535

デフォルト値: 0、これは、プロトコルは常に利用可能と見なされることを意味しています。

**comm-port**

TN3270 アドバイザが TN3270 サーバーと通信するのに使用するポート番号を指定します。このパラメータは、TN3270 アドバイザの入力にだけ使用します。

有効値: 1 ~ 65535

デフォルト値: 10008

例:

```
set advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nnntp=6=pop3,7=telnet) [0]?
Port number [0]? 21
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 20
```

**cluster** *address FIN-count FIN-timeout Stale-timer*

ネットワーク・ディスパッチャー構成内のクラスターの *FIN-count*、*FIN-timeout*、および *Stale-timer* を変更します。

**address**

クラスターの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

**FIN-count**

実行プログラムが *FIN-timeout* または *Stale-timer* の経過後にネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みる前に、*FIN* 状態にあることが必要な接続の数を指定します。

有効値: 0 ~ 65535

デフォルト値: 4000

**FIN-timeout**

実行プログラムがネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みる前に経過する必要がある秒数を指定します。

有効値: 0 ~ 65535

デフォルト値: 30

**Stale-timer**

接続が非活動状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから接続情報の除去を試みます。

有効値: 0 ~ 65535

デフォルト値: 1500

例:

```
set cluster
Cluster address [0.0.0.0]? 131.2.25.91
FIN count [4000]? 4500
FIN timeout [30]? 40
Stale timer [1500]? 2000
```

**manager** *interval proportion refresh sensitivity smoothing*

マネージャーが要求を満たす最善サーバーを判別するのに使用する値を設定します。

**interval**

実行プログラムが接続のロード・バランシングに使用するサーバーの重みが、マネージャーによって更新される前に経過する時間 (秒数) を指定します。

## ネットワーク・ディスパッチャーの構成

有効値: 0 ~ 65535

デフォルト値: 2

### proportion

マネージャーが重み付けを決定する際の外部ファクターの相対的な重要度を指定します。比率の合計は 100 に等しくなければなりません。ファクターには、次のものがあります。

**active** 実行プログラムによって追跡される各 TCP/IP サーバー上の活動状態の接続の数

有効値: 0 ~ 100

デフォルト値: 50

**new** 実行プログラムによって追跡される各 TCP/IP サーバー上の新規接続の数

有効値: 0 ~ 100

デフォルト値: 50

### advisor

ネットワーク・ディスパッチャーに定義されたプロトコル・アドバイザーからの入力

有効値: 0 ~ 100

デフォルト値: 0

### system

MVS WLM システム監視ツールによって提供される MVS システム・アドバイザーからの入力

有効値: 0 ~ 100

デフォルト値: 0

### refresh

マネージャーが実行プログラムから状態を要求する頻度を指定します。このパラメーターは、*intervals* の回数として指定します。

有効値: 0 ~ 100

デフォルト値: 2

### sensitivity

ポート上のすべてのサーバーの重みの比率の変動を指定します。この後、マネージャーは、実行プログラムが接続のロード・バランスに使用する重みを更新します。

有効値: 0 ~ 100

デフォルト値: 5

### smoothing

サーバーの重みの変動できる量の限界を指定します。

平滑化 (smoothing) は、要求の分配が変動する頻度を最小限にします。平滑化インデックスが高くなると、重みの変動は少なくなります。平滑化インデックスが低くなると、重みの変動は大きくなります。

## ネットワーク・ディスパッチャーの構成

有効値: 1.0 ~ 42 949 673.00 の間の 10 進値

デフォルト値: 1.5

注: 小数点次 2 桁までしか指定できません。

例:

```
set manager
Interval (in seconds) [2]? 3
Active proportion [50]? 40
New proportion [50]? 38
Advisor proportion [0]? 20
System proportion [0]? 2
Refresh cycle [2]? 4
Sensitivity threshold [5]? 10
Smoothing index (>1.00) [1.50]? 200
```

**port** *cluster-address port# port-type max-weight port-mode*

特定のクラスターとポート番号の *port-type*、*max-weight*、および *port-mode* を変更します。

### cluster-address

クラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

**port#** このクラスターのプロトコルのポート番号を指定します。

有効値: 1 ~ 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

### port-type

このポートでロード・バランスを取ることができる IP トラフィックのタイプを指定します。

有効値:

**tcp=1**

**upd=2**

**both=3**

デフォルト値: 3

### max-weight

このポート上のサーバーの重みを指定します。これは、実行プログラムが各サーバーに分配する要求数の相違に影響します。

有効値: 0 ~ 100

デフォルト値: 20

### port-mode

ポートが、1 つのクライアントからの要求をすべて 1 つのサーバーに送る (*sticky* と呼ばれる) か、パッシブ *ftp* を使用する (*pftp*) か、Web サーバー・キャッシュを使用する (*cache*) か、外部スケラブル・キャッシュ配列を送るか、ホスト・オンデマンド・クライアント

## ネットワーク・ディスパッチャーの構成

ト・キャッシュを使用するか、またはこのクラスターではプロトコルを使用しない (none) かを指定します。

有効値:

**none=0**

**sticky=1**

**pftp=2**

**cache=3**

**extcache=4**

**hod client cache=5**

デフォルト: 0 (none)

例:

```
set port
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]? 23
Port type (tcp=1, udp=2, both=3) [3]?
Max. weight (0-100) [20]? 30
Port mode (none=0, sticky=1, pftp=2, cache=3, extcache=4 hod client cache=5) [0]?
```

注:

1. ポート・モード 3 (cache=3) を選択した場合は、Web サーバー・キャッシュについて 201ページの『第12章 Web サーバー・キャッシュの構成と監視』を参照してください。
2. ポート・モード 5 (hod client cache=5) を選択した場合は、Web サーバー・キャッシュについて 145ページの『第10章 IBM eNetwork ホスト・オンデマンド・クライアント・キャッシュの構成と監視』を参照してください。

**server** *cluster-address port# server-address weight state*

クラスター内の特定のサーバーの状態およびサーバーの重みを変更します。

**cluster-address**

このサーバーが属するクラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

**port#** このクラスターのプロトコルのポート番号を指定します。

有効値: 1 ~ 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

**server-address**

サーバーの IP アドレスを指定します。

有効値: 任意の有効なサーバー・アドレス

デフォルト値: 0.0.0.0

**state** 実行プログラムが処理を開始するときに、サーバーを利用可能と見なすか、利用不能と見なすかを指定します。

有効値: 0 (ダウン) または 1 (アップ)

デフォルト値: 1

**weight**

実行プログラムのために、サーバーの重みを指定します。これは、ネットワーク・ディスパッチャーがこの特定サーバーに要求を送信する頻度に影響を与えます。

有効値: 0 ~ add port コマンドで指定した *max-weight* の値

デフォルト値: port コマンドの *max-weight* の値

**例:**

```
set server
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]?
Server address [0.0.0.0]?
Server weight [20]? 25
Server state (down=0, up=1) [1]? 1
```

## ネットワーク・ディスパッチャー監視コマンドへのアクセス

ネットワーク・ディスパッチャー監視環境にアクセスするには、次のようにします。

1. OPCON プロンプト (\*) で **talk 5** と入力する。
2. GWCON プロンプト (+) で **feature ndr** と入力する。

ネットワーク・ディスパッチャーは、SNMP を使用して監視することもできます。詳しくは、プロトコル構成および監視 参照資料 第 1 巻の『SNMP 管理』の項を参照してください。

## ネットワーク・ディスパッチャー監視コマンド

表15 は、ネットワーク・ディスパッチャー監視コマンドの要約を示しており、表の後に個々のコマンドの説明があります。これらのコマンドは NDR > プロンプトで入力します。

表 15. ネットワーク・ディスパッチャー監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxページの『ヘルプの入手』を参照してください。
List	現在構成されているアドバイザー、クラスター、ポート、またはサーバーの属性を表示します。
Quiesce	これ以上の接続要求をサーバーに送信してはならないことを指定します。ハートビートおよびリーチ機能も一時的に停止します。
Report Status	アドバイザーおよびマネージャーに関する情報の報告を表示します。カウンター、クラスター、ポート、サーバー、アドバイザー、マネージャー、およびバックアップの現在の状態を表示します。
Switchover	スタンバイ・モードで動作しているネットワーク・ディスパッチャーを、強制的に活動ネットワーク・ディスパッチャーにします。このコマンドは、切り替えモードとして「手動」を指定した場合に使う必要があります。

## ネットワーク・ディスパッチャーの構成

表 15. ネットワーク・ディスパッチャー監視コマンド (続き)

コマンド	機能
Unquiesce	サーバーが構成されている各ポート上の以前に静止されたサーバーに対して、ネットワーク・ディスパッチャーのマネージャーは 0 より大きい重みを割り当てることができるようにします。このアクションにより、選択されたサーバーに対して新規の接続要求を送ることができるようになります。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

## List

**list** コマンドは、ネットワーク・ディスパッチャーに関する情報を表示するのに使用します。

構文:

```
list                advisor
                    cluster
                    port
                    server
```

### advisor

ネットワーク・ディスパッチャーのアドバイザーの構成を表示します。

例:

```
list advisor
Advisor list requested.
```

ADVISOR	PORT	TIMEOUT	STATUS
ftp	21	5	ACTIVE
Http	80	unlimited	ACTIVE
MVS	10007	unlimited	ACTIVE
TN3270	23	unlimited	ACTIVE

### cluster

ネットワーク・ディスパッチャーのクラスターの構成を表示します。

例:

```
list cluster
EXECUTOR INFORMATION:
-----
Version: 01.01.00.00 - Tue Dec 10 14:15:58 EST 1996
Number of defined clusters: 2

CLUSTER LIST:
-----
 131.2.25.91
 10.11.12.2
```

**port** ネットワーク・ディスパッチャーのポートの構成を表示します。

例:

```
list port
Cluster Address [0.0.0.0]? 131.2.25.91
```

CLUSTER:	131.2.25.91		
PORT	MAXWEIGHT	PORT MODE	PORT TYPE



23	30	none	TCP
80	20	none	both

**server** ネットワーク・ディスパッチャーのクラスターに対応するサーバーの構成を表示します。

例:

```
list server
Cluster Address [0.0.0.0]? 131.2.25.91

PORT 23 INFORMATION:
-----
Maximum weight..... 20
Port mode..... NONE
Port type..... TCP
All up nodes are weight zero... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UPD Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 TCP Count: 0 UPD Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1

PORT 80 INFORMATION:
-----
Maximum weight..... 20
Port mode..... NONE
Port type..... BOTH
All up nodes are weight zero... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UPD Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 TCP Count: 0 UPD Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
```

## Quiesce

**quiesce** コマンドは、ハートビートまたはリーチ機能を一時的に停止するか、それ以上の接続要求をサーバーに送信しないように指定するのに使用します。

構文:

```
quiesce          heartbeat
                 manager
                 reach
```

**heartbeat** *address*

ハートビート機能用に選択されたパスを停止します。 *address* は、このネットワーク・ディスパッチャーのハートビート・メッセージの送信先のリモート・ネットワーク・ディスパッチャーの IP アドレスです。

例:

```
quiesce heartbeat
Remote Address [0.0.0.0]? 131.2.25.94
```

**manager** *address*

指定されたサーバーには、それ以上の接続要求をしてはならないことを指定します。 *Address* は、そのサーバーの IP アドレスです。

例:

## ネットワーク・ディスパッチャーの構成

```
quiesce manager
Server Address [0.0.0.0]? 131.2.25.93
```

### reach address

到達可能かどうかを判別するためのネットワーク・ディスパッチャーによる指定のアドレスへのポーリングを停止します。ただし、*address* は、到達可能性基準に含まれている IP アドレスです。

例:

```
quiesce reach
Reach Address [0.0.0.0]? 131.2.25.92
```

## Report

**report** コマンドは、アドバイザーまたはマネージャーの報告を表示するのに使用します。

構文:

```
report a ad man
          _advisor
          _manager
```

### advisor type port#

特定のアドバイザーに関する情報の報告を表示します。

**type** アドバイザーのタイプです。アドバイザー・タイプについては、118ページの表13を参照してください。

**port#** ポート番号です。

例:

```
report advisor
0=ftp,1=http,2=MVS,3=TN3270,4=smt,5=nn,6=pop3,7=telnet
Advisor name [0]? 1
Port number [0]? 80
```

ADVISOR:	http
PORT:	80
131.2.25.93	0
131.2.25.94	16

### manager

現在のマネージャー情報の報告書を表示します。

例:

```
report manager
```

HOST TABLE LIST	STATUS
131.2.25.93	ACTIVE
131.2.25.94	ACTIVE

131.2.25.91	WEIGHT	ACTIVE %	50	NEW %	50	PORT %	0	SYSTEM %	0	
PORT: 23	NOW	NEW	WT	CONNECT	WT	CONNECT	WT	LOAD	WT	LOAD
131.2.25.93	10	10	10	0	10	0	0	0	-999	-1
131.2.25.94	10	10	10	0	10	0	0	0	-999	-1
PORT TOTALS:	20	20		0		0		0		-2

131.2.25.91	WEIGHT	ACTIVE % 50	NEW % 50	PORT % 0	SYSTEM % 0				
PORT: 80	NOW NEW	WT	CONNECT	WT	CONNECT	WT	LOAD	WT	LOAD
131.2.25.93	10 10	10	0	10	1	16	0	-999	-1
131.2.25.94	10 10	10	0	10	1	3	16	-999	-1
PORT TOTALS:	20 20		0		0		16		-2

ADVISOR	PORT	TIMEOUT	STATUS
http	80	unlimited	ACTIVE
MVS	10007	unlimited	ACTIVE

Manager report requested.

## Status

**status** コマンドは、アドバイザー、バックアップ、カウンター、クラスター、マネージャー、ポート、およびサーバーの状態を入手するのに使用します。

構文:

```

status
  _advisor
  _backup
  _cluster
  _counter
  _manager
  _ports
  _servers
    
```

**advisor** *name port#*

特定のアドバイザーの状態を入手します。

**name** アドバイザーのタイプを指定します。アドバイザー・タイプについては、118ページの表13 を参照してください。

**port#** ポート番号です。

例:

```

status advisor
0=ftp, 1=http, 2=MVS 3=TN3270, 4=SMTP, 5=NNTP, 6=POP3, 7=TELNET
Advisor name [0]?
Port number [0]? 21
    
```

```

Advisor ftp on port 21 status:
=====
Interval..... 10
    
```

**backup**

バックアップ機能の状態を入手します。

例:

```

status backup
Dumping status ...
Role : PRIMARY Strategy : AUTOMATIC State : ND_ACTIVE Sub-State : ND_SYNCHRONIZED
<<Preferred Target : 132.2.25.92>>

Dumping HeartBeat Status ...
.....Heartbeat target : 131.2.25.92 Status : UNREACHABLE
.....Heartbeat target : 132.2.25.92 Status : REACHABLE
    
```

## ネットワーク・ディスパッチャーの構成

```
Dumping Reachability Status ...
.....Host:131.2.25.93 Local:REACHABLE
.....Host:131.2.25.94 Local:REACHABLE
```

### cluster address

指定されたクラスターの状態を入手します。ただし、*address* は、クラスターの IP アドレスです。

例:

```
status cluster
Cluster Address [0.0.0.0]? 131.2.25.91

EXECUTOR INFORMATION:
-----
Version: 01.01.00.00 - Tue Dec 10 14:15:58 EST 1996

CLUSTER INFORMATION:
-----
Address..... 131.2.25.91
Number of target ports..... 2
FIN clean up count..... 4000
Connection FIN timeout..... 30
Active connection stale timer... 1500

PORT 23 INFORMATION:
-----
Maximum weight..... 20
Port mode..... NONE
Port type..... TCP
All up nodes are weight zero... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0
Active: 0 FIN 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0
Active: 0 FIN 0 Status: up Saved Weight: -1

PORT 80 INFORMATION:
-----
Maximum weight..... 20
Port type..... BOTH
Port mode..... NONE
All up nodes are weight zero... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0
Active: 0 FIN 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0
Active: 0 FIN 0 Status: up Saved Weight: -1
```

### counter

すべてのカウンターの状態を入手します。

例:

```
status counter
Internal counters from executor:
-----
Total number of packets into executor..... 2684
Total packets for cluster processing (C)... 2684
Packets not addressed to a cluster(port)... 0

Cluster processing results:
-----
Errors..... 0
Discarded..... 0
Forward requested..... 2684
Forward requested..... 0
Forward discarded with error..... 0

Other processing problems:
-----
Total packets dropped (C)..... 0
```

### manager

マネージャーの状態を入手します。

例:

```

status manager
Number of defined hosts... 2
Sensitivity..... 0%
Smoothing factor..... 2
Interval..... 3
Weights refresh cycle.... 4

Active connections gauge proportion..... 40%
New connections counter(delta) proportion... 38%
Advisor gauge proportion..... 20%
System Metric proportion..... 2%

Manager status requested.

```

**port** *cluster-address* *port#*

特定のポートの状態を入手します。ただし、

*cluster-address*

クラスタの IP アドレスです。

*port#* クラスタのポート番号です。

**例:**

```

status port
Cluster Address [0.0.0.0]? 131.2.25.91
Port number [0]? 80

PORT 80 INFORMATION:
-----
Maximum weight..... 20
Port mode..... NONE
Port type..... BOTH
All up nodes are weight zero... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 12345 TCP Count: 10000 UDP count 2345
Active: 3431 FIN 3780 Complete 3431 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 7890 Active: 2980 FIN 2390 Status: up
Saved Weight: -1

```

**server** *address*

特定のサーバーの状態を入手します。ただし、*address* は、サーバーが属するクラスタの IP アドレスです。

**例:**

```

status server
Cluster Address [0.0.0.0]? 131.2.25.91

PORT 23 INFORMATION:
-----
Maximum weight..... 20
Port mode..... NONE
Port type..... TCP
All up nodes are weight zero... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 140 TCP Count: 100 UDP Count: 40
Active: 50 FIN 45 Complete 50 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 250 TCP Count: 100 UDP Count: 40
Active: 60 FIN 54 Complete 50 Status: up Saved Weight: -1

PORT 80 INFORMATION:
-----
Maximum weight..... 20
Port mode..... NONE
Port type..... BOTH
All up nodes are weight zero... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 12345 TCP Count: 10000 UDP Count: 2345
Active: 3431 FIN 3780 Complete 3431 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 7890 TCP Count: 10000 UDP Count: 2345
Active: 2980 FIN 2390 Complete 3431 Status: up Saved Weight: -1

```



---

## 第10章 IBM eNetwork ホスト・オンデマンド・クライアント・キャッシュの構成と監視

ホスト・オンデマンド・クライアント・キャッシュを使用すれば、Web ベースのクライアントが、Java ベースの端末エミュレーション・プログラムを使用して SNA ホスト・アプリケーションに接続できます。端末エミュレーション・プログラムは、TN3270 を使用してクライアントをホストに接続します。このサポートによって、TN3270E サーバーとして機能する IBM 2212 は、端末エミュレーション・アプレットをキャッシュに入れ、要求に応じてクライアント・ブラウザにアプレットを提供できます。アプレットは、クライアントが初回に要求したときに Web サーバーから検索され、メモリーに格納されて、アプレットに対する HTTP get 要求に応じてクライアントに提供されます。

### 注:

1. ホスト・オンデマンド・クライアント・キャッシュと Web サーバー・キャッシュは、1 つの構成内で共存できません。
2. ホスト・オンデマンドは、ハイパフォーマンス・システム・カード上でだけ稼働します。

この章では、ホスト・オンデマンド・クライアント・キャッシュ機能を構成する方法、およびホスト・オンデマンド・クライアント・キャッシュ監視コマンドを使用する方法を説明します。この章の内容は次のとおりです。

- 『ホスト・オンデマンド・クライアント・キャッシュの構成』
- 149ページの『ホスト・オンデマンド・クライアント・キャッシュ構成環境へのアクセス』
- 149ページの『ホスト・オンデマンド・クライアント・キャッシュのコマンド』
- 153ページの『ホスト・オンデマンド・クライアント・キャッシュ監視環境へのアクセス』
- 153ページの『ホスト・オンデマンド・クライアント・キャッシュ監視コマンド』

ホスト・オンデマンド・クライアント・キャッシュを操作する外部キャッシュ制御マネージャーの使用については、169ページの『外部キャッシュ制御マネージャーの概要』を参照してください。

---

## ホスト・オンデマンド・クライアント・キャッシュの構成

ホスト・オンデマンド・クライアント・キャッシュは、ネットワーク・ディスパッチャーと一緒に使用する必要があります。ホスト・オンデマンド・クライアント・キャッシュを初めて使用する場合は、その前にまず次のことを行う必要があります。

1. Config> プロンプトで **feature ndr** コマンドを使用して、talk 6 によってネットワーク・ディスパッチャーにアクセスする。
2. 実行プログラムを使用可能にする。
3. クラスタを追加する。
4. ポートを追加する。

## ホスト・オンデマンド・クライアント・キャッシュの構成と監視

5. 1 台または複数台のサーバーを追加する。

その後、構成コマンドと監視コマンドを使用して、ホスト・オンデマンド・クライアント・キャッシュ環境を更新できます。

**注:** Talk 6 によってネットワーク・ディスパッチャーを変更すると現行の稼働構成が変更されるのに対し、ホスト・オンデマンド・クライアント・キャッシュを変更した場合は、Talk 6 の **activate** コマンド、または Talk 5 feature HOD Client Cache によって明示的にアクティブ化しないかぎり、現行の稼働構成は変更されません。この例外は、Talk 6 feature NDR によって HTTP プロキシ用のクラスター/ポートを削除した場合です。この場合は、ホスト・オンデマンド・クライアント・キャッシュ用の HTTP プロキシも、現行の稼働構成から削除されます。

**例:**

```
Config>f ndr
NDR Config>enable executor
NDR Config>add cluster
Cluster Address [0.0.0.0]? 113.3.1.10
FIN count [4000]?
FIN time out [30]?
Stale timer [1500]?
Cluster 113.3.1.10 has been added.
Fincount has been set to 4000 for cluster 113.3.1.10
Fintimeout has been set to 30 for cluster 113.3.1.10
Staletimer has been set to 1500 for cluster 113.3.1.10
NDR Config>add port
Cluster Address [0.0.0.0]? 113.3.1.10
Port number [80]? 80
Port type(tcp=1, udp=2, both=3) [3]?
Max. weight (0-100) [20]?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 extcache=4 hod client cache=5) [0]? 5
Default server TCP connection timeout (Range 5-240 seconds) [120]?
Default client TCP connection timeout (Range 5-240 seconds) [120]?
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]?
URL mask to identify Java applet [*.*.jar]?
Default expiration time for Java applet
(1-10080 minutes or 0 for no expiration) [60]?
Do you want to add a URL mask? [No]:

Host On-Demand Client Cache partition number 0 has been successfully created.
Requested port has been added to cluster 113.3.1.10
Port Mode has been set to hod for port 80 in cluster 113.3.1.10
Maxweight has been set to 20 for port 80 in cluster 113.3.1.10
Port Type has been set to Both for port 80 in cluster 113.3.1.10
NDR Config>exit
```

次では、例のパラメーターとその説明です。

### cluster-address

クラスターの IP アドレスを指定します。

**注:** クラスター IP アドレスは、直前のホップ・ルーター (IP ルーター) と同じ論理サブネット上に存在するものと想定しています。

**有効値:** 任意の有効な IP アドレス

**デフォルト値:** 0.0.0.0

### FIN-count

実行プログラムが *FIN-timeout* または *Stale-timer* の経過後にネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みる前に、FIN 状態にあることが必要な接続の数を指定します。

**有効値:** 0 ~ 65535



## ホスト・オンデマンド・クライアント・キャッシュの構成と監視

デフォルト値: 4000

**FIN-timeout** 接続が FIN 状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みます。

有効値: 0 ~ 65535

デフォルト値: 30

**Stale-timer** 接続が非活動状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから接続の情報の除去を試みます。

有効値: 0 ~ 65535

デフォルト値: 1500

**port#** このクラスターのプロトコルのポート番号を指定します。

有効値: 1 ~ 65535

デフォルト値: 80

**port-type** このポートでロード・バランスを取ることができる IP トラフィックのタイプを指定します。サポートされるタイプは、次のとおりです。

- 1 = TCP
- 2 = UDP
- 3 = 両方

有効値: 1、2、3

デフォルト値: 3

**max-weight** このポート上のサーバーの最大重みを指定します。これは、実行プログラムが各サーバーに分配する要求数の相違に影響します。

有効値: 0 ~ 100

デフォルト値: 20

**port-mode** ポートが、1 つのクライアントからの要求をすべて 1 つのサーバーに送る (sticky と呼ばれる) か、パッシブ ftp を使用する (pftp) か、外部スケーラブル・キャッシュ配列を送るか (extcache)、ホスト・オンデマンド・クライアント・キャッシュを使用するか、またはこのクラスターでは特定のプロトコルを使用しない (none) かを指定します。

有効値: 0、1、2、4、5。ただし、

- 0 = none
- 1 = sticky
- 2 = pftp
- 4 = extcache
- 5 = hod client cache

デフォルト値: 0

## ホスト・オンデマンド・クライアント・キャッシュの構成と監視

### Default server TCP connection timeout

サーバー接続の有効期限が切れるまでの時間を指定します。

有効値: 5 ~ 240 秒

デフォルト値: 120 秒

### Default client TCP connection timeout

クライアント接続の有効期限が切れるまでの時間を指定します。

有効値: 5 ~ 240 秒

デフォルト値: 120 秒

### Do you want to modify Host On-Demand Client Cache partition?

ホスト・オンデマンド・クライアント・キャッシュ区画の構成を変更できます。

有効値: Yes または No

デフォルト値: No

### Maximum partition size

このホスト・オンデマンド・クライアント・キャッシュ区画に対して割り振るメモリの最大量を指定します。この値が現在使用可能なメモリの量を超える場合は、値は無視され、最大区画サイズは設定されません。

有効値: 1 ~ 4095 メガバイト、または 0 (最大値なし)

デフォルト値: 0 (最大値なし)

### URL mask to identify Java applets

Java アプレットを識別するために使用される URL マスクを指定します。

有効値: 任意の URL マスク

デフォルト値: \*.jar\*

### Default expiration time for Java applet

Java アプレットに適用されるデフォルト有効期限を指定します。

有効値: 1 ~ 10080 分、または 0 (有効期限なし)

デフォルト値: 60

### Do you want to add a URL mask?

ホスト・オンデマンド・クライアント・キャッシュに追加する新しい URL マスクを指定します。URL マスクを使用すると、個々のオブジェクト、またはオブジェクトのグループを、URL を基準にして含めたり除外したりすることができます。

有効値: Yes または No

デフォルト値: No

URL マスクを指定するときは、ワイルドカード文字を使用できます。ワイルドカードを使えるのは、ホスト・オンデマンド・クライアント・キャッシュ用にネットワーク・ディスパッチャーを構成するとき、あるいは HOD Client Cache プロンプトから **add** または **modify url** コマンドを使用するときです。ワイルドカードとして使用で

## ホスト・オンデマンド・クライアント・キャッシュの構成と監視

きる文字は、\* (アスタリスク) または # (番号記号) です。ワイルドカードは URL の一部としてどの位置にでも使用できます。

\* は、URL の一部として、文字なし、または全文字を表します。

例: \*abc.html は、次のような URL マスクをフィルターに掛けます。

```
abc.html  
finabc.html  
defchtjqsprabc.html
```

# は、1 文字を表します。

例: ab#.html は、次のような URL マスクをフィルターに掛けます。

```
abc.html  
abf.html  
abo.html
```

ホスト・オンデマンド・クライアント・キャッシュ機能用の初期クラスターとポートを構成するには、ネットワーク・ディスパッチャーを使用する必要があります。ポート・モードをホスト・オンデマンド・クライアント・キャッシュ・ポートとして構成して、クラスターとポートを追加したら、HOD Client Cache Config> プロンプトでホスト・オンデマンド・クライアント・キャッシュの構成パラメーターを変更、表示できます。

ネットワーク・ディスパッチャーについては、122 ページを参照してください。

---

## ホスト・オンデマンド・クライアント・キャッシュ構成環境へのアクセス

ホスト・オンデマンド・クライアント・キャッシュ構成環境にアクセスするには、Config> プロンプトで **f hod client cache** コマンドを入力します。

```
Config> f h  
HOD Client Cache Config>
```

---

## ホスト・オンデマンド・クライアント・キャッシュのコマンド

ここでは、ホスト・オンデマンド・クライアント・キャッシュ構成コマンドを説明します。表16 は、ホスト・オンデマンド・クライアント・キャッシュ構成コマンドの一覧です。これらのコマンドは、ホスト・オンデマンド・クライアント・キャッシュ機能のパラメーターを指定します。これらの変更内容をアクティブにするには、ルーターをリスタートします。

表 16. ホスト・オンデマンド・クライアント・キャッシュ構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxi ページの『ヘルプの入手』を参照してください。
Activate	最新の構成を使用して、ホスト・オンデマンド・クライアント・キャッシュ区画をアクティブにします。
Add	URL マスクを追加します。
Delete	URL または区画を削除します。
List	ホスト・オンデマンド・クライアント・キャッシュの情報を表示します。

## ホスト・オンデマンド・クライアント・キャッシュの構成と監視

表 16. ホスト・オンデマンド・クライアント・キャッシュ構成コマンドの要約 (続き)

コマンド	機能
Modify	ホスト・オンデマンド・クライアント・キャッシュの情報を変更します。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

### Activate

**activate** コマンドは、最新の構成を使用してホスト・オンデマンド・クライアント・キャッシュの区画すべてを初期設定するために使用します。

構文:

**activate**

例:

```
HOD Client Cache Config>act ?
ACTIVATE ALL initializes the Host On-Demand Client Cache partition, using
the latest configuration.
If you want to keep the active configuration, use the
ENABLE PARTITION command.
```

### Add

**add** コマンドは、URL マスクを追加するために使用します。

構文:

**add** urlmask

例:

```
HOD Client Cache Config>add url
New URL mask []? *newmask*
Include or Exclude from HOD Client Cache (i or e) [i]? i
Set default expiration time? [No]: y
Default expiration time
(1-10080 minutes or 0 for no expiration) [0]? 60
The URL mask has been added to HOD Client Cache partition number 0.
```

注: プロキシと区画を追加するには、ネットワーク・ディスパッチャーを使用して **add port** コマンドまたは **set port** コマンドを実行する必要があります。

### Delete

**delete** コマンドは、URL マスクまたは区画を削除するために使用します。

構文:

**delete** partition  
urlmask

**partition**

ホスト・オンデマンド・クライアント・キャッシュの区画を削除します。

**urlmask**

ホスト・オンデマンド・クライアント・キャッシュから削除する URL マスクの名前。

例:

## ホスト・オンデマンド・クライアント・キャッシュの構成と監視

```
HOD Client Cache Config>del part
HOD Client Cache partition number 0 has been deleted.
```

### 例:

```
HOD Client Cache Config>delete url
URL masks defined : 1
1: INCLUDE '*newmask*'
   Default expiration time: 60 minutes (1 hrs 0 mins)
URL mask number [1]?1
The URL mask for HOD Client Cache partition number 0 has been deleted.
```

**注:** プロキシを削除するには、ネットワーク・ディスパッチャー機能を使用して、関連したポートまたはクラスター (あるいはその両方) を削除するか、ポートのポート・モードをホスト・オンデマンド・クライアント・キャッシュ以外に変更する必要があります。

## List

**list** コマンドは、ホスト・オンデマンド・クライアント・キャッシュの情報を表示するために使用します。

### 構文:

```
list                all
                       external
                       partition
                       proxy
                       urlmask
```

**all** ホスト・オンデマンド・クライアント・キャッシュ内で定義されている区画、すべてのポート、プロキシ、およびマスクを表示します。

### external

外部キャッシュ制御マネージャーに関する情報を表示します。

### partition

ホスト・オンデマンド・クライアント・キャッシュの区画を表示します。

**proxy** ホスト・オンデマンド・クライアント・キャッシュのプロキシを表示します。

### urlmask

ホスト・オンデマンド・クライアント・キャッシュの定義済み URL マスクを表示します。

### 例: list all

```
HOD Client Cache Config>list all
Host On-Demand Client Cache Partition 0
  Cluster address 113.3.1.10, Port 80

1 Host On-Demand Client Cache partition defined.
```

### 例: list external

```
HOD Client Cache Config>list ext
External cache manager : Enabled
Port number             : 82
TCP timeout             : 120 seconds
```

### 例: list partition

## ホスト・オンデマンド・クライアント・キャッシュの構成と監視

```
HOD Client Cache Config>list pa
Host On-Demand Client Cache Partition 0
Maximum partition size      : Unlimited
URL mask to identify Java applets: '*.jar'
Default expiration time for Java applet: 60
Associated proxies (cluster port): (113.3.1.10 80)

1 Host On-Demand Client Cache partition defined.
```

例: list proxy

```
HOD Client Cache Config>li pro
1) Cluster address 113.3.1.10, Port 80, HOD Client Cache partition 0
HTTP proxy number [1]? 1
HTTP Proxy 1
HOD Client Cache Partition: 0
Cluster Address      : 113.3.1.10
Port Number         : 80
Server Connection Timeout : 120 seconds
Client Connection Timeout : 120 seconds
```

例: list urlmask

```
HOD Client Cache Config>list url
URL masks defined : 1
1: INCLUDE '*newmask*'
Default expiration time: 60 minutes (1 hrs 0 mins)
```

## Modify

**modify** コマンドは、ホスト・オンデマンド・クライアント・キャッシュの構成情報を変更するために使用します。

構文:

```
modify          external
                  partition
                  proxy
                  urlmask
```

**external**

外部キャッシュ制御マネージャーの特性を変更します。

**partition**

既存のホスト・オンデマンド・クライアント・キャッシュ区画の特性を変更します。

**proxy** 既存の HTTP プロキシの特性を変更します。

**urlmask**

既存の URL マスクを変更します。

例: modify external

```
HOD Client Cache Config>mod ext
External cache manager port number (0 to disable) [82]? 83
TCP connection timeout (Range 5-240 seconds) [120]?
Do you want to modify the encryption key? [No]:
The external cache manager has been modified.
```

例: modify partition

```
HOD Client Cache Config>modify partition
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]? 2000
URL mask to identify Java applet [*.jar]?
```

## ホスト・オンデマンド・クライアント・キャッシュの構成と監視

```
Default expiration time for Java applet
(1-10080 minutes or 0 for no expiration) [60]?
Host On-Demand Client Cache partition 0 has been modified.
```

例: modify proxy

```
HOD Client Cache Config>mod proxy
1) Cluster address 113.3.1.10, Port 80, HOD Client Cache partition 0
HTTP proxy number [1]? 1
Default server TCP connection timeout (Range 5-240 seconds) [120]? 200
Default client TCP connection timeout (Range 5-240 seconds) [120]?
The HTTP proxy has been modified.
```

例: modify url

```
HOD Client Cache Config>modify url
URL masks defined : 1
1: INCLUDE '*newmask*'
Default expiration time: No expiration
URL mask number [1]?
New URL mask [*newmask*]?
Include or Exclude from HOD Client Cache (i or e) [i]?
Set default expiration time? [No]: y
Default expiration time
(1-10080 minutes or 0 for no expiration) [0]? 60
URL mask number 1 has been modified.
```

---

## ホスト・オンデマンド・クライアント・キャッシュ監視環境へのアクセス

ホスト・オンデマンド・クライアント・キャッシュ監視環境にアクセスするには、`t 5` の構成プロンプトで `f hod client cache` コマンドを入力します。

`+f h`

---

## ホスト・オンデマンド・クライアント・キャッシュ監視コマンド

表17 は、ホスト・オンデマンド・クライアント・キャッシュ監視コマンドの一覧です。

表17. ホスト・オンデマンド・クライアント・キャッシュ監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxiiページの『ヘルプの入手』を参照してください。
Activate	最新の構成を使用して、ホスト・オンデマンド・クライアント・キャッシュの情報をアクティブにします。
Clear	ホスト・オンデマンド・クライアント・キャッシュの区画からオブジェクトをすべて消去するか、ホスト・オンデマンド・クライアント・キャッシュの統計を消去します。
Enable	ホスト・オンデマンド・クライアント・キャッシュの区画を使用可能にします。
Delete	ホスト・オンデマンド・クライアント・キャッシュの区画、プロキシ、または URL マスクを削除します。
Disable	ホスト・オンデマンド・クライアント・キャッシュの区画を使用不可にします。
List	ホスト・オンデマンド・クライアント・キャッシュの情報を表示します。
Modify	ホスト・オンデマンド・クライアント・キャッシュの情報を変更します。
Exit	直前のコマンド・レベルに戻ります。xxxiiページの『下位レベル操作環境の終了』を参照してください。

## Activate

**activate** コマンドは、ホスト・オンデマンド・クライアント・キャッシュの区画またはプロキシ、または特定のプロキシをアクティブにするために使用します。

構文:

```
activate          all
                   external
                   partition
                   proxy
```

**all** ホスト・オンデマンド・クライアント・キャッシュの区画、定義済みのプロキシすべて、および定義済みの外部キャッシュ制御マネージャーをアクティブにします。

**external**

外部キャッシュ制御マネージャーをアクティブにします。

**partition**

ホスト・オンデマンド・クライアント・キャッシュの区画をアクティブにします。

**proxy**

ホスト・オンデマンド・クライアント・キャッシュのプロキシをアクティブにします。

例: activate all

```
HOD Client Cache>act all
Host On-Demand Client Cache partition 0 must be disabled to reactivate it.
Do you wish to continue? [No]: y
```

例; activate partition

```
HOD Client Cache>act pa
Host On-Demand Client Cache partition 0 must be disabled to reactivate it.
Do you wish to continue? [No]: y
Do you wish clear this partition? [No]: y
Do you wish to enable this partition? [Yes]: y
```

例; activate proxy

```
HOD Client Cache>activate pr
1) Cluster address 113.3.1.10, Port 80, HOD Client Cache partition 0
Enter proxy number: [1]? 1
You are trying to activate an existing proxy.
Doing this will cause the proxy to be terminated before
being reactivated.
Do you wish to continue? [No]: y
```

## Clear

**clear** コマンドは、ホスト・オンデマンド・クライアント・キャッシュの区画からオブジェクトをすべて消去するため、または統計を消去するために使用します。

注: 区画からオブジェクトを消去しても、その区画の統計は消去されません。

構文:

```
clear             partition
                   statistics
```



**partition**

区画からオブジェクトをすべて消去します。

**statistics**

区画に存在する統計を消去します。

例: clear partition

```
HOD Client Cache>clear pa
HOD Client Cache partition 0 must be disabled to clear its contents.
Do you wish to continue? [No]: y
Do you wish to enable this partition? [Yes]: y
```

## Enable

**enable** コマンドは、ホスト・オンデマンド・クライアント・キャッシュの区画を使用可能にするために使用します。

構文:

**enable** partition

例:

```
HOD Client Cache>enable partition
```

## Delete

**delete** コマンドは、ホスト・オンデマンド・クライアント・キャッシュの区画を削除するために使用します。

構文:

**delete** partition

**partition**

ホスト・オンデマンド・クライアント・キャッシュの区画を削除します。

例: delete partition

```
HOD Client Cache>delete partition
WARNING: This will delete partition and free all memory!
Do you wish to continue? [No] : yes
HOD Client Cache>
```

## Disable

**disable** コマンドは、ホスト・オンデマンド・クライアント・キャッシュの区画を使用不可にするために使用します。

構文:

**disable** partition

例:

```
HOD Client Cache>disable partition
```

## List

**list** コマンドは、ホスト・オンデマンド・クライアント・キャッシュの区画、すべてのポリシーとプロキシ、または指定のポリシーまたはプロキシに関する情報を表示するために使用します。

構文:

```
list                all  
                    delete  
                    depend  
                    external  
                    item  
                    partition  
                    policy  
                    proxy
```

**all** ホスト・オンデマンド・クライアント・キャッシュの区画、すべてのポリシー、およびすべてのプロキシを表示します。

**delete** ホスト・オンデマンド・クライアント・キャッシュの区画から最近削除された 100 項目を表示します。

**depend**  
区画の依存関係テーブルを表示します。

**external**  
外部キャッシュ制御マネージャーに関する情報を表示します。

**item** ホスト・オンデマンド・クライアント・キャッシュの区画にある現在項目を表示します。

**partition**  
ホスト・オンデマンド・クライアント・キャッシュの区画情報を表示します。

**policy** ホスト・オンデマンド・クライアント・キャッシュのポリシー情報を表示します。

**proxy** ホスト・オンデマンド・クライアント・キャッシュのプロキシ情報を表示します。

例: list all

```
HOD Client Cache>list all  
HOD Client Cache Partition 0          Status: Enabled  
    Cluster address: 113.3.1.10 Port 80  
1 partition(s) active.  
External Cache Manager Port: 83  
    Connection timeout: 120 seconds
```

例: list delete

```
HOD Client Cache>list delete  
  
Delete Table  
URL string -- hit count  
=====
```

'/abc.html'	-- 4
'/soccer.html'	-- 2
'/tennis.html'	-- 1
'/curling.html'	-- 3

例: list dependency

```
HOD Client Cache>list depend
Dependency table for Partition 0
-----
dep: tennis_info
  count of URLs: 2
  URLs:
    tennis_roster.html
    tennis_schedule.html
dep: soccer_info
  count of URLs: 2
  URLs:
    soccer_roster.html
    soccer_schedule.html
dep: schedule
  count of URLs: 2
  URLs:
    tennis_schedule.html
    soccer_schedule.html
```

例: list external

```
HOD Client Cache>list external
External Cache Manager Port: 83
  Connection timeout: 120 seconds
  Current number of connections: 0
```

例: list item

```
HOD Client Cache>list item

Current number of items: 5
URL String -- hit count
=====
'/' -- 2
'/file5k.html' -- 1
'/file4k.html' -- 1
'/file2k.html' -- 3
'/file1k.html' -- 1
```

例: list partition

```
HOD Client Cache>list partition
HOD Client Cache Partition 0          Status: Enabled
  Cluster address: 113.3.1.10, Port 80
Partition size: Current - 0 bytes Highest - 0 bytes Maximum - Unlimited
Number of objects: Current - 0 Highest - 0 Maximum - Unlimited
Maximum object size: Unlimited
HOD Client Cache purge interval : 600 minute(s)
Hit ratio: 0%
Total number of hits: 0
Total number of misses: 0
Object Excluded (Object too large):      0
                  (Object expired):      0
                  (DONT CACHE header):   0
                  (URL Mask excluded):    0
                  (Image excluded):       0
                  (Static object excluded): 0
                  (Dynamic object excluded): 0
                  (Cache disabled):       0
Objects explicitly Included: 0
Total number of purged objects: 0
Purged objects (Cache full): 0
                  (Object stale): 0
                  (Purged by user): 0
                  (Invalidation): 0
```

例: list policy

```
HOD Client Cache>list policy
URL mask to identify Java Applets: *.jar
  Default lifetime: 60 minute(s)
URL masks defined:
  1: INCLUDE *newmask*
    Default expiration time: 60 minutes (1 hrs 0 mins)
```

## ホスト・オンデマンド・クライアント・キャッシュの構成と監視

例: list proxy

```
HOD Client Cache>list proxy
  1) Cluster address 113.3.1.10, Port 80, HOD Client Cache Partition 0
Enter proxy number: [1]? 1
Proxy 1: assigned to HOD Client Cache partition 0
Cluster address: 113.3.1.10    Port number: 80
Server Connection Timeout: 120 seconds
Client Connection Timeout: 120 seconds
Client connections: 0 current / 0 at highest point
Server connections: 0 current / 0 at highest point
Total cache hits: 0
Total cache misses: 0
Cache misses (object not in cache): 0
              (unsupported method): 0
              (can't send response): 0
              (non-cached request): 0
```

## Modify

**modify** コマンドは、外部キャッシュ制御マネージャーを変更するために使用します。

構文:

**modify** external

例: modify external

```
HOD Client Cache Config>mod ext
External cache manager port number (0 to disable) [83]? 82
TCP connection timeout (Range 5-240 seconds) [120]?
Do you want to modify the encryption key? [No]: n
```

---

## 第11章 Web サーバー・キャッシュの使用

この章では、2212 Web サーバー・キャッシュ機能について説明します。この章には、次の内容が記載されています。

- 『Web サーバー・キャッシュの概説』
- 164ページの『HTTP プロキシの使用』
- 165ページの『スケーラブル高可用性キャッシュ』
- 169ページの『外部キャッシュ制御マネージャーの概要』

---

### Web サーバー・キャッシュの概説

Web サーバー・キャッシュは、ハイパフォーマンス・システム・カードを備えた 2212 モデルでだけ使用できます。ハイパフォーマンス・システム・カードを備えていない 2212 モデルは、アップグレードできます。詳しくは、IBM 担当員にお尋ねください。

Web サーバー・キャッシュは、頻繁に要求される Web ページを速く検索できるように保管します。Web サーバー・キャッシュは、頻繁に要求される項目をクライアントの近くに保管することにより、ファイル・サービスと通信接続に現在使用されているサーバーの資源を解放します。2212 Web サーバー・キャッシュは、ホストの通信オーバーヘッドを減らすと同時に、Web ページへの高速アクセスを可能にします。2212 Web サーバー・キャッシュには、次の特徴があります。

- 静的な無保護 Web ページを保管します
- HTTP クライアントとサーバーがキャッシュにアクセスできるようにします
- キャッシュ集団と無効化ポリシーのユーザー定義が可能です
- ネットワーク・ディスパッチャー機能を使用してサーバー間のワークロードのバランスを実行し、バックアップ・キャッシュ機能を提供します
- 将来、サーバーの指示によるキャッシュ機能のプラットフォームとなります

**注:** Web サーバー・キャッシュとホスト・オンデマンド・クライアント・キャッシュの両機能は、1 つの構成内で共存できません。

TCP/IP 接続をサポートする 2212 のネットワーク・インターフェースはすべて、Web サーバー・キャッシュ、HTTP サーバー、およびクライアントの間の接続をサポートします。

160ページの図10 は、Web サーバー・キャッシュを使用しない場合のネットワーク・ディスパッチャーの動作を示しています。

## Web サーバー・キャッシュの使用

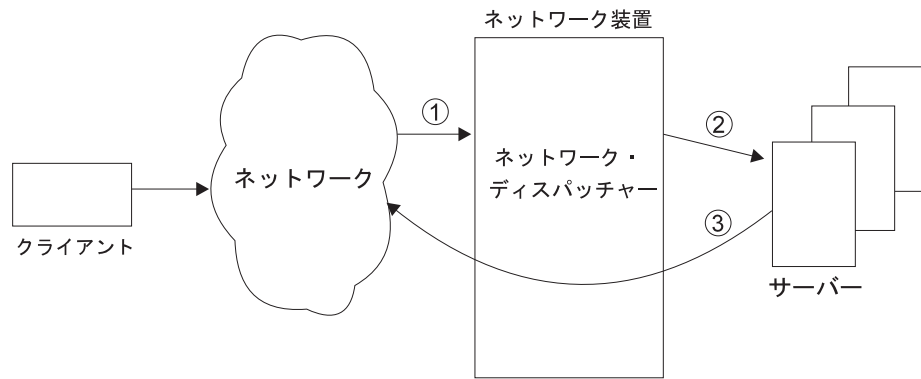


図 10. Web サーバー・キャッシュを使用しないネットワーク・ディスパッチャー

1. クラスタ・アドレスに対する要求が着信する
2. ネットワーク・ディスパッチャーは、要求をサーバーに転送する
3. サーバーは、応答をクライアントに返信する

図11は、要求されたページが現在はキャッシュに入っていない場合の Web サーバー・キャッシュを使用したネットワーク・ディスパッチャーの動作を示しています。Web サーバー・キャッシュは、ポリシーが許可すれば、応答をキャッシュにロードします。

HTTP プロキシについては、164ページの『HTTP プロキシの使用』を参照してください。

区画とは、キャッシュのコア・メモリの 1 区分です。キャッシュの各区画は独立して区分されているので、装置が複数のクラスターをサポートできます。

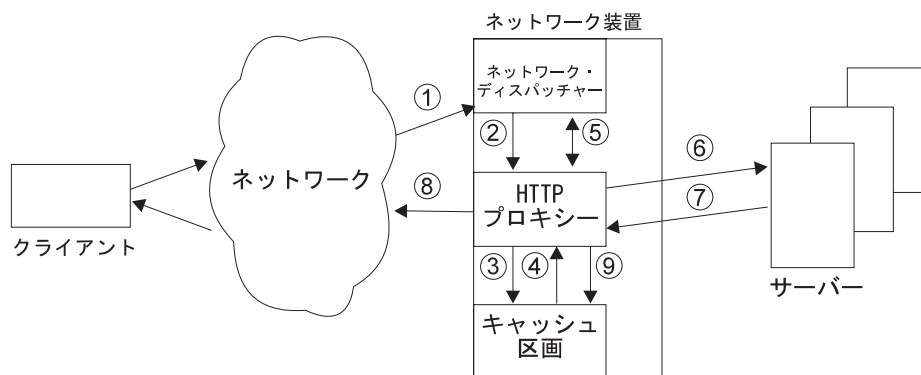


図 11. キャッシュ・ヒットがない場合の Web サーバー・キャッシュを使用したネットワーク・ディスパッチャー

1. クラスタ・アドレスに対する要求が着信する
2. ネットワーク・ディスパッチャーは、要求を HTTP プロキシに転送する (アクティブになっていれば)
3. HTTP プロキシは、キャッシュ区画を検索する
4. HTTP プロキシは、キャッシュ区画の中に要求されたページを検出できなかった

## Web サーバー・キャッシュの使用

5. HTTP プロキシは、新しい接続のために必要ならば、ネットワーク・ディスパッチャーからサーバー情報を入手する
6. HTTP プロキシは、要求をサーバーに転送する。(TCP 接続の場合、送信元 IP アドレスは 2212 ネットワーク・インターフェースのアドレスです。あて先 IP アドレスは、サーバー・インターフェースの IP アドレスです。)
7. サーバーは、応答を HTTP プロキシに返信する
8. HTTP プロキシは、応答をクライアントに送信する
9. HTTP プロキシは、ポリシーが許可すれば、応答をキャッシュ区画にロードする

図12は、要求されたページが現在キャッシュに入っている場合の Web サーバー・キャッシュを使用したネットワーク・ディスパッチャーの動作を示しています。

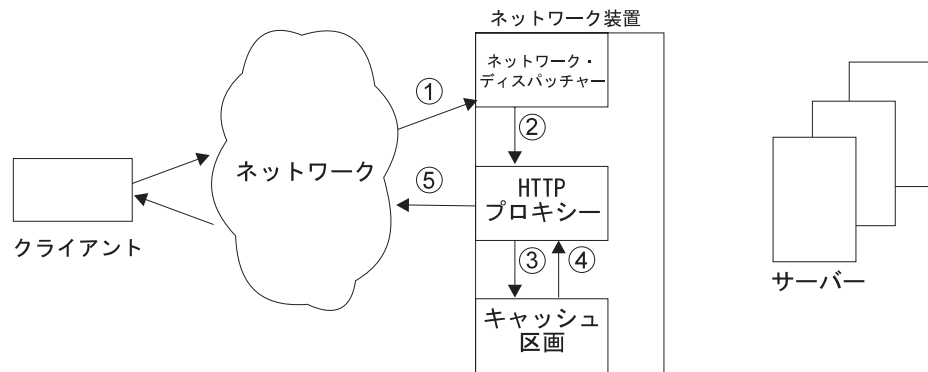


図12. キャッシュ・ヒットがある場合の Web サーバー・キャッシュを使用した ネットワーク・ディスパッチャー

1. クラスタ・アドレスに対する要求が着信する
2. ネットワーク・ディスパッチャーは、要求を HTTP プロキシに転送する
3. HTTP プロキシは、キャッシュ区画を検索する
4. HTTP プロキシは、キャッシュ区画の中に要求されたページを検出した
5. HTTP プロキシは、応答をクライアントに返信する

## キャッシュ

2212 Web サーバー・キャッシュには、次の機能があります。

### Web ページのキャッシュ

2212 は、サーバーから要求されたオブジェクトをキャッシュに入れることができます。このキャッシュは、透過キャッシュと呼ばれます。talk 6 を使用して、区画の透過キャッシュを使用可能または使用不可にすることができます。

透過 (自動) キャッシュのほかには、手動キャッシュがあります。この場合、外部のエージェントがキャッシュ・マネージャーを使用して、Web ページをキャッシュに入れます。外部 Web キャッシュについては、169ページの『外部キャッシュ制御マネージャーの概要』を参照してください。

## Web サーバー・キャッシュの使用

古くなったキャッシュ・オブジェクトは、自動的に削除されます。 2212 Web サーバー・キャッシュは、HTTP 1.0 と 1.1 の両方のサーバーとクライアントをサポートします。

### 柔軟なキャッシュ・ポリシー

ユーザーは、幅広いクラスの Web オブジェクト (イメージ、非イメージ静的ページ、動的ページ) をキャッシュに入れるかどうか指定できます。オブジェクトとキャッシュ区画の最大サイズも指定できます。さらに、URL マスクを指定すれば、ユーザーの環境に合わせて Web オブジェクトのクラスを明示的に含めたり除外したりすることもできます。

### 透過キャッシュ・ポリシーのフローチャート

1. キャッシュが使用可能になっていて、透過キャッシュが使用可能になっているか?
  - いいえ - オブジェクトはキャッシュに入れられない。
  - はい - 次のチェックに進む。
2. オブジェクト・サイズは最大オブジェクト・サイズ以内か?
  - いいえ - オブジェクトはキャッシュに入れられない。
  - はい - 次のチェックに進む。
3. オブジェクトの有効期限が切れているか?
  - いいえ - 次のチェックに進む。
  - はい - オブジェクトはキャッシュに入れられない。
4. HTTP ヘッダーは使用されるか? HTTP ヘッダーのどれか 1 つが使用されたか?

**注:** 使用される HTTP ヘッダーは、DO 宣言または DONT 宣言を指定したキャッシュ制御ヘッダーです。

- a. いいえ - HTTP ヘッダーは使用されないか、オブジェクトにヘッダーがない。
  - 1) URL が除外マスクによって除外されているか?
    - はい - オブジェクトはキャッシュに入れられない。
    - いいえ - 次のチェックに進む。
  - 2) 包含マスクによって URL が包含されているか?
    - はい - 163ページの5 のステップに進む。
    - いいえ - 次のチェックに進む。
  - 3) これは動的オブジェクトか?
    - いいえ - 次のチェックに進む。
    - はい - オブジェクトは動的。
      1. 動的オブジェクトはキャッシュ可能か?
        - はい - 次のチェックに進む。
        - いいえ - オブジェクトはキャッシュに入れられない。
  - 4) オブジェクトはイメージ (.jpg または .gif) か?
    - いいえ - 次のチェックに進む。
    - はい - オブジェクトはイメージ。



1. イメージはキャッシュ可能か?
  - はい - 次のチェックに進む。
  - いいえ - オブジェクトはキャッシュに入れられない。
- 5) オブジェクトは静的非イメージか?
  - いいえ - 次のチェックに進む。
  - はい - オブジェクトは静的非イメージ・ファイル。
    1. 静的非イメージはキャッシュ可能か?
      - はい - 次のチェックに進む。
      - いいえ - オブジェクトはキャッシュに入れられない。
  - b. はい - HTTP ヘッダーが使用されていて、オブジェクトにキャッシュ制御ヘッダーが含まれているか?
    - 1) HTTP ヘッダーは "DO" キャッシュを指示しているか?
      - a) いいえ - オブジェクトはキャッシュに入れられない。
      - b) はい - 次のチェックに進む。
5. 区画にオブジェクト用の空間はあるか?

**注:** オブジェクト用の空間を作るために、最も古く使用されたオブジェクトが削除されます。

- いいえ - オブジェクトはキャッシュに入れられない。
- はい - オブジェクトはキャッシュに入れられる。

### 複数の独立したキャッシュのサポート

最大 16 の区画をサポートしているため、1 台の 2212 が複数のクラスターに独立したキャッシュ・サービスを提供できます。キャッシュ区画は完全に独立しています。それぞれのキャッシュ区画は、独自の内容とポリシーを維持します。

### 完全な TCP/IP サーバー接続

TCP/IP プロトコル・スイートをサポートするすべての 2212 ネットワーク・インターフェースにわたって、サーバー、クライアントの両方と通信できます。

### バックエンド・サーバーとのロード・バランシング (ネットワーク・ディスパッチャーによる)

ネットワーク・ディスパッチャーを使用してサーバーのグループを定義し、サーバー間でロード・バランスを取ることで、キャッシュにない Web ページの検索を高速化しています。

### バックアップ・キャッシュのサポート

2 台目の 2212 をバックアップ・サーバー・キャッシュとして定義できます。ネットワーク・ディスパッチャーの高可用性機能を使用すれば、バックアップ・サーバー・キャッシュは『コールド』バックアップとして作動できます。詳しくは、101ページの『ネットワーク・ディスパッチャーの高可用性』を参照してください。

**注:** バックアップ・サーバーのキャッシュは、徐々に空になります。透過キャッシュ (例: URL の要求)、または外部キャッシュ制御マネージャー機

## Web サーバー・キャッシュの使用

能を使用して、ページを強制的にキャッシュに入れることによって、バックアップ・サーバーのキャッシュに内容を再度入れる必要があります。

---

## HTTP プロキシの使用

2212 内には、複数の HTTP プロキシが存在できます。それぞれのプロキシは、キャッシュを行っているクラスター・アドレス/ポートを表します。複数の HTTP プロキシが、1 つのキャッシュ区画を使用できます。

HTTP プロキシは、クライアントからの要求の受信を処理し、そのキャッシュ区画からクライアントの要求を満たそうと試みます。要求を満たすことができれば、HTTP プロキシはクライアントに応答を戻します。HTTP プロキシが要求を満たすことができない場合は、要求を満たすための試みとしてサーバーとの TCP 接続を開きます。サーバーが HTTP プロキシの要求に応答すると、HTTP はサーバーの応答をクライアントに転送します。HTTP プロキシは、クライアントからの応答をキャッシュに入れる必要があるかどうかを調べます。応答をキャッシュに入れる必要がある場合、HTTP プロキシは応答をキャッシュ区画にパスします。

HTTP プロキシは、次のガイドラインを使用して接続を処理します。

- HTTP プロキシは、キャッシュから GET メソッドと HEAD メソッドの要求だけを満たそうと試みます。その他の要求は、クライアントからの TCP 接続と対になっている TCP 接続を経由して、変更を加えずにサーバーに送信されます。クライアントからの TCP 接続と対になっている TCP 接続がない場合、サーバーへの新しい TCP 接続が開かれ、クライアントへの TCP 接続と対になります。
  - キャッシュ区画からは満たすことができない GET メソッドと HEAD メソッドの要求のメッセージは、TCP 接続を経由して変更を加えずにサーバーに送信されません。
  - すべての応答は、クライアントへの TCP 接続を経由して、サーバーが送信したものから変更されずにクライアントに戻されます。
  - GET メソッドの応答だけをキャッシュに入れることができます。ほかの応答は、すべてキャッシュ不能と見なされます。GET 応答は、応答の状況が受け入れ可能であり、GET 応答と区画のキャッシュ・ポリシーを照らし合わせてキャッシュが可能な場合にだけ、キャッシュに入れられます。
    - 次の状況コードのどれか 1 つを持つ応答だけがキャッシュに入れられます。HTTP プロキシは、このルールを守らない HTTP ヘッダーを入れることはしません。
- 状況コード:**
- 200 (ok)
  - 203 (non-authoritative)
  - 300 (multiple-choice)
  - 301 (moved permanently)
  - 410 (gone)
- HTTP ヘッダーが GET 要求で使用されている場合は、キャッシュのエントリーがその要求を満たすことができるかどうか判別するために、If-Modified-Since 要求ヘッダーが使用されます。他の条件ヘッダーは、すべて使用されません。Web サー

## Web サーバー・キャッシュの使用

バー・キャッシュは、キャッシュに入れられたエンティティを応答に使用できるかどうか判別するために、エンティティ・タグは使用しません。

- 要求にある Cache-Control ヘッダー宣言は無視されます。エンティティがキャッシュ区画にない場合、要求はサーバーにパスされます。

**注:** Web サーバー・キャッシュはサーバーの拡張機能なので、HTTP プロキシのように Cache-Control ヘッダーを使用しません。

- 応答では、キャッシュ・ヘッダー宣言 "do" および "dont" がサポートされます。他の宣言はすべて無視されます。"do" 宣言と "dont" 宣言は、エンティティをキャッシュに入れるかどうかを Web サーバー・キャッシュに指示するためにサーバーが使用できる新しい宣言です。

**注:** Web サーバー・キャッシュはサーバーの拡張機能なので、HTTP プロキシのように Cache-Control ヘッダーを使用しません。

- HTTP プロキシは、キャッシュから部分 GET 要求を満たそうと試みます。ただし、部分 GET 応答はキャッシュに入れられません。

**注:** 部分 GET 要求に 10 より多い範囲がある場合は、応答全体が戻されます。

- HTTP メッセージにある Host ヘッダーはすべて無視されます。これは、着信する要求はすべて同じサーバー・クラスターを対象にしていなければならないためです。
- HTTP プロキシは、永続 HTTP 接続をサポートします。

**注:** 永続接続が HTTP 1.0 レベルのクライアントから着信していて、キャッシュから応答が戻されると、クライアントは要求に基づいて Connection ヘッダーを追加します。たとえば、クライアントが長期間の接続を必要としている場合は、長期間の接続が維持されます。

- HTTP プロキシは、Authorization ヘッダーを含む要求に対してはキャッシュを使用しません。このような要求に対する応答は、キャッシュに入れられません。Proxy-Authorization ヘッダーのある応答はキャッシュに入れられません。
- HTTP プロキシは、HTTP 接続上で要求または応答の構文解析に問題が生じた場合に、HTTP 接続のトンネル動作に切り替えることができます。トンネル動作は、メッセージの構文解析をすべて停止し、要求すべてをクライアントからサーバーに転送し、応答すべてをサーバーからクライアントに転送します。
- キャッシュ区画が使用不可になっている場合は、現行と新規のクライアント接続すべてがバックエンド・サーバーに直接転送されます。
- キャッシュ区画が使用可能になっている場合は、新規のクライアント接続すべてがキャッシュによって処理されます。既存のクライアント接続は、引き続きバックエンド・サーバーに要求を直接転送します。

---

## スケーラブル高可用性キャッシュ

スケーラブル高可用性キャッシュは、接続した Web サーバー・キャッシュのグループを 1 つの大きなキャッシュとして機能させることができます。グループに入るキャッシュの最大数は 16 です。1 つのキャッシュ・メンバーに障害が起こると、キャッシュ機能がすべて終了するのではなく、キャッシュ用に使用できるメモリの合計量が減ります。構成例については、115 ページの図9 を参照してください。

## Web サーバー・キャッシュの使用

独立したキャッシュが合計キャッシュ・スペースを構成します。キャッシュが機能しなくなると、残りの機能するキャッシュによって着信ページが引き続きキャッシュに入れられます。

着信 web ページは、グループのキャッシュに保管され、使用可能なキャッシュ間で均等に分散されます。グループ内の各キャッシュは、グループにある到達可能なキャッシュの数とその IP アドレスを追跡するテーブルを維持します。1つのグループ内のキャッシュすべてに対して、テーブルは同一です。特定の URL を持っているキャッシュがどれかを判別するために、テーブルはキャッシュ・アレイ・ルーチン・プロトコル (CARP) アルゴリズムと組み合わせて使用されます。テーブルの情報は、ネットワーク・ディスパッチャー装置から得られ、HTTP アドバイザーを使用してグループ内の Web サーバー・キャッシュの状況を追跡しているキャッシュから間接的に得られます。次の図は、SHAC を使用して URL を見付ける場合のさまざまな条件を示しています。

図13 は、ネットワーク・ディスパッチャーからの要求が、要求を最初に受信したキャッシュ内で検出された場合を示しています。

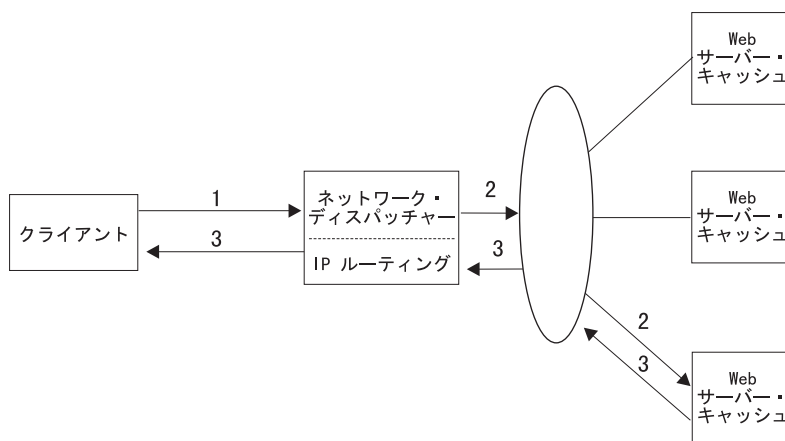


図 13. キャッシュ要求が検出された場合

1. Web ページに対する HTTP 要求が、クライアントからネットワーク・ディスパッチャーに着信する。
2. 要求は、ネットワーク・ディスパッチャーによって Web サーバー・キャッシュの 1 つに転送される。キャッシュは要求を受信し、キャッシュにその Web ページが含まれていることを検出する。
3. キャッシュは、ネットワーク・ディスパッチャーをバイパスして、クライアントに直接 Web ページを送信する。

167ページの図14 は、ネットワーク・ディスパッチャーから要求を最初に受信したキャッシュ内で要求が検出されず、別のキャッシュが URL を持っていることを CARP アルゴリズムが指摘した場合を示しています。

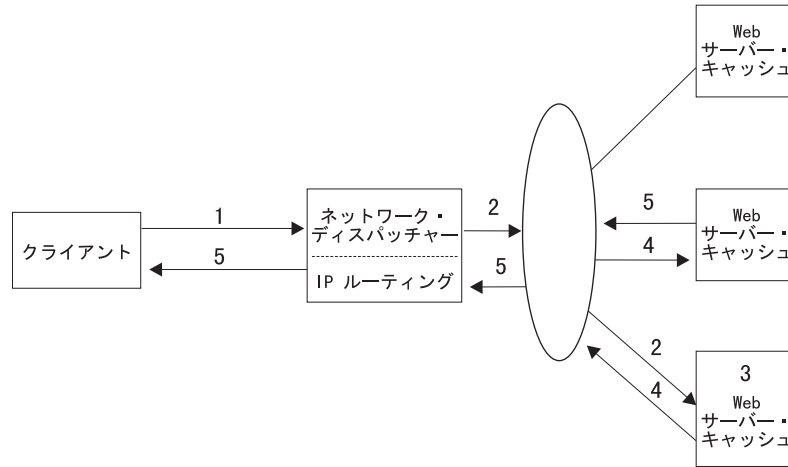


図 14. 要求が担当のキャッシュに転送される場合

1. Web ページに対する HTTP 要求が、クライアントからネットワーク・ディスパッチャーに着信する。
2. 要求は、ネットワーク・ディスパッチャーによって Web サーバー・キャッシュの 1 つに転送される。
3. キャッシュは要求を受信し、キャッシュ内でその Web ページは検出されない。キャッシュはアルゴリズムを使用して、その Web ページを担当しているキャッシュを見付ける。
4. 要求は、その Web ページを担当するキャッシュに転送される。
5. その Web ページを担当するキャッシュは要求を受信し、Web ページを検出し、Web ページをクライアントに送信する。

図 15 は、ネットワーク・ディスパッチャーから要求を最初に受信したキャッシュ内で要求が検出されなかったにもかかわらず、そのキャッシュがその URL を担当していることを CARP アルゴリズムが指摘した場合を示しています。

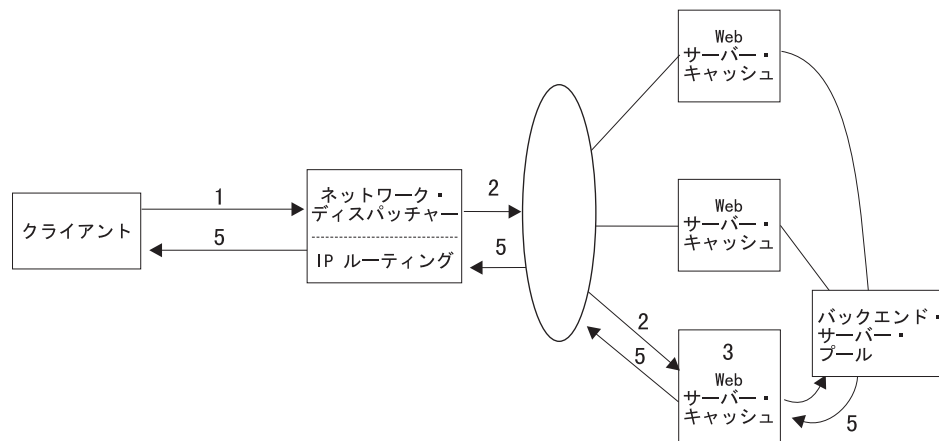


図 15. 要求がバックエンド・サーバーに転送される場合

1. Web ページに対する HTTP 要求が、クライアントからネットワーク・ディスパッチャーに着信する。

## Web サーバー・キャッシュの使用

2. 要求は、ネットワーク・ディスパッチャーによって Web サーバー・キャッシュの 1 つに転送される。
3. キャッシュは要求を受信するが、キャッシュ内でその Web ページは検出されない。キャッシュはアルゴリズムを使用して、そのキャッシュが Web ページを担当していることを判別する。
4. キャッシュは、要求をバックエンド・サーバーに送信する。
5. バックエンド・サーバーは Web ページを検出する。その Web ページは、Web ページを担当するキャッシュを経由してクライアントに戻される。キャッシュがそのページをキャッシュに入れるように構成されている場合は、Web ページがキャッシュに入れられる。構成については、201ページの『第12章 Web サーバー・キャッシュの構成と監視』を参照してください。

図16 は、キャッシュ・グループ内のどのキャッシュでも要求が検出されなかった場合を示しています。

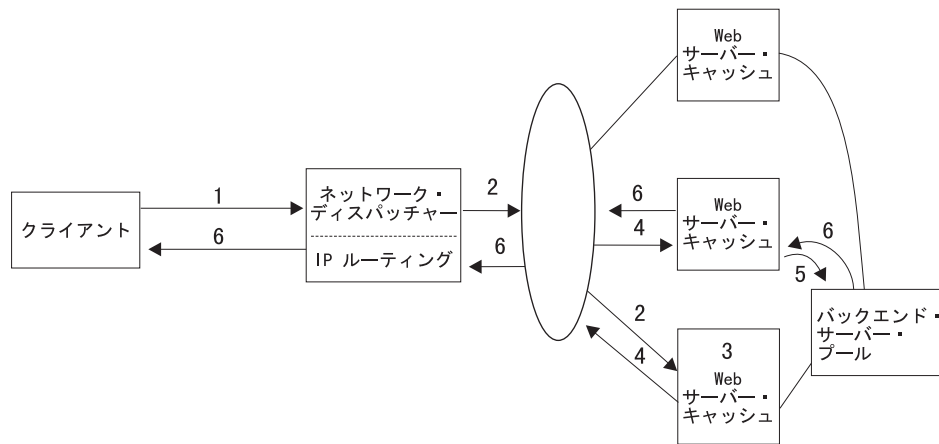


図16. 要求が担当のキャッシュに転送され、検出されなかった場合

1. Web ページに対する HTTP 要求が、クライアントからネットワーク・ディスパッチャーに着信する。
2. 要求は、ネットワーク・ディスパッチャーによって Web サーバー・キャッシュの 1 つに転送される。
3. キャッシュは要求を受信し、キャッシュ内でその Web ページは検出されない。キャッシュはアルゴリズムを使用して、その Web ページを担当しているキャッシュを見付ける。要求は、その Web ページを担当するキャッシュに転送される。
4. その Web ページを担当するキャッシュは要求を受信するが、Web ページは検出されない。
5. その Web ページを担当するキャッシュは、バックエンド・サーバー・プールに要求を送信する。
6. バックエンド・サーバーは Web ページを検出する。その Web ページは、Web ページを担当するキャッシュを経由してクライアントに戻される。キャッシュがそのページをキャッシュに入れるように構成されている場合は、Web ページがキャッシュに入れられる。構成については、201ページの『第12章 Web サーバー・キャッシュの構成と監視』を参照してください。



## 外部キャッシュ制御マネージャーの概要

外部キャッシュ制御マネージャーは、Web サーバーが Web サーバー・キャッシュとホスト・オンデマンド・クライアント・キャッシュを制御できるようにします。この制御は、外部キャッシュ制御マネージャー (ECCM) 用のユーザー定義のポートを経由して行われます。ECCM は、このポートを経由して接続を受け入れ、区画を対象としたコマンドを処理します。コマンドは、外部キャッシュ制御プロトコル (ECCP) を使用します。ECCP は、ベクトル/サブベクトル形式を使用して、要求コマンドと応答コマンドを送信します。

1 つのコマンド・ベクトルは、複数のサブベクトルを使用して複数の機能を要求できます。それぞれのサブベクトルは、新規の機能に相当します。コマンド・ベクトルは、コマンドを適用する先のキャッシュ区画を、その区画に対して定義されているクラスター・アドレスを指定することによって指示します。

ECCP は次の機能をサポートしています。

- キャッシュ区画のオブジェクトを追加/削除する
- キャッシュ区画を使用可能/使用不可にする
- キャッシュ区画のポリシーを修正/表示する
- キャッシュ区画の統計を消去/表示する
- キャッシュ区画を消去する (キャッシュ区画からオブジェクトをすべて削除する)
- キャッシュ区画を照会する (特定のオブジェクトを検索する)
- キャッシュ区画の URL マスクを追加/削除/表示/消去する
- 依存関係テーブルを修正/表示する
- 依存関係を使用してオブジェクトを無効にする

## 依存関係テーブル

外部キャッシュ制御マネージャーを使用すると、それぞれのキャッシュ区画ごとに依存関係テーブルを作成できます。このテーブルは、キャッシュ内の動的オブジェクトを処理する際に特に役立ちます。

**注:** 動的オブジェクトをキャッシュに入れる場合は、これらのオブジェクトを作成する元となった情報が変更されたときに、オブジェクトを更新する必要があります。

依存関係テーブルを作成するための情報は、外部キャッシュ制御マネージャーのインターフェースを使用してキャッシュ区画にパスする必要があります。

依存関係テーブルによって、URL オブジェクト (キャッシュに入れられた Web ページ) に依存関係ストリングを割り当てることができます。これらの依存関係は、外部キャッシュ制御マネージャーのインターフェースを使用して、Web サーバー・キャッシュの依存関係テーブルに保管されます。依存関係テーブルは、オブジェクトのソースが変更されたときに、この依存関係を持つキャッシュ区画内のオブジェクトを無効にするために使用されます。依存関係テーブルがなければ、削除するそれぞれのオブジェクトに対して別々に削除コマンドを送信しなければなりません。

**例:** 次の 3 つのデータベースには、さまざまなオブジェクトが格納されています。

## Web サーバー・キャッシュの使用

database1	database2	database3
-----	-----	-----
object_a	object_a	object_b
object_b	object_c	object_e
object_c	object_d	

ページ object\_a ~ object\_e がキャッシュに入っていると仮定します。 database2 が変更された場合は、**invalid dependency database2** コマンドを送信できます (キャッシュ制御マネージャーのインターフェースを経由して)。このとき Web サーバー・キャッシュは、object\_a、object\_c、および object\_d をキャッシュ区画から削除します。

注: オブジェクトを依存関係テーブルに入れる場合に、オブジェクトがキャッシュ区画に入っている必要はありません。

### 外部キャッシュ制御マネージャーの認証

外部キャッシュ制御マネージャーを使用して、ユーザーのアクセスを制御できます。この制御は、着信接続にユーザー ID とパスワードを要求することによって行われます。ユーザー ID とパスワードは、ログオン・ユーザー ID とパスワードに関連付けられています。装置がパスワード保護されていて、着信接続にユーザー ID とパスワードがないか、ユーザー ID とパスワードが無効である場合は、認証エラー応答が戻され、接続はクローズされます。ユーザー ID とパスワードが有効な場合、ユーザーはそのインターフェースを経由してコマンドを送信できます。

### セキュリティー

セキュリティーは、ECCP ユーザーを認証するための手段です。4 種類の認証を構成できます (RADIUS、TACACS、ローカル、または認証なし)。データ暗号化は行われません。それぞれの認証メカニズム (認証なしの場合を除く) は、ユーザー ID および関連したパスワードを両方とも要求します。この情報は、認証ベクトルを使用して 2216 にパスされます。ユーザー ID の長さは 1 ~ 8 バイトで、パスワードの長さは 1 ~ 8 バイトです。外部キャッシュ制御接続によってパスされるパスワードは、DES 暗号化を使用して暗号化する必要があります。暗号化に使用される 8 バイトのランダム・シードもパスされます。暗号化用のキーは、接続を経由してパスされません。ポートと TCP 値の設定については、211 ページの『Modify』を参照してください。

注: ルーターがパスワード保護されていない場合は、認証ベクトルは無視されません。

## 外部キャッシュ制御プロトコル

外部キャッシュ制御プロトコル (ECCP) によって、バックエンド・サーバーはルーターのキャッシュを制御できます。この制御により、キャッシュのパフォーマンスが最大になります。

ECCP は、サーバーがオブジェクトを追加および削除したり、キャッシュ・ポリシーを変更したりすることを可能にする体系化プロトコル・インターフェースです。

外部キャッシュ制御マネージャーは、接続を受け入れ、キャッシュ区画を対象にしたコマンドを処理するために、ルーター (Web サーバー・キャッシュまたはホスト・オンデマンド・クライアント・キャッシュ) 内で定義されます。



## 構成

外部キャッシュ制御マネージャーは、次のパラメーターを使用して構成されます。

### ユーザー定義ポート:

外部キャッシュ制御マネージャーが接続を `listen` して受け入れるポート番号。  
0 が構成された場合は、外部キャッシュ制御マネージャーは使用不可になっていると想定されます。

有効値: 0 ~ 65535

デフォルト値: 0

### 最大 TCP タイムアウト値:

有効値: 5 ~ 240 秒

デフォルト値: 120

### 暗号化キー:

暗号化キーは、ボックスがパスワード保護されている場合に使用されます。  
暗号化キーは、16 桁の 16 進文字 (0 ~ 9, a ~ f, A ~ F) でなければなりません。

## 外部キャッシュ制御マネージャーの機能の説明

ここでは、外部キャッシュ制御マネージャーの機能を説明します。

### オブジェクトの追加

キャッシュ区画に HTTP 応答オブジェクトを追加できます。オブジェクト・データの形式は、HTTP 応答と同じでなければなりません。外部キャッシュ制御マネージャーは、応答のヘッダーを構文解析して、必要な情報を引き出します。その後、オブジェクトがキャッシュに追加されます。

Add Object と Add (Force) Object の違いは、Add (Force) Object は DO または DONT を指定する Cache\_Control ヘッダーをすべて無視する点です。HTTP プロキシがオブジェクトをキャッシュに入れるかどうか決定するために使用する他のヘッダーは、すべて使用されます。Add Object と Add (Force) Object のどちらの場合も、オブジェクトは日付と関係なくキャッシュ区画内で置き換えられます。

### オブジェクトの削除

キャッシュから HTTP オブジェクトを削除できます。オブジェクトの URL が指定されます。

### 依存関係テーブルの使用

キャッシュ区画の依存関係テーブルは、変更および表示することができ、オブジェクトを無効にするために使用できます。

依存関係テーブルを変更する (依存関係を追加または削除する) 際には、依存関係と依存関係 URL の両方を指定する必要があります。依存関係テーブルを変更する方法はほかに 2 つあります。1 つは、テーブル全体のリセット、依存関係全体のリセット (つまり、依存関係を完全に削除する)、または URL 依存関係のリセット (つまり、す

## Web サーバー・キャッシュの使用

すべての依存関係から URL 依存関係を削除する) を行う方法です。もう 1 つは、依存関係テーブルに対してガーベッジ・コレクションを実行する方法です。ガーベッジ・コレクションは、キャッシュにその URL のオブジェクトがない依存関係 URL を、依存関係テーブルからすべて消去します。

依存関係テーブルの情報を表示する方法はいくつかあります。テーブル全体を検索することも、指定の依存関係に対する依存関係 URL をすべて検索することも、指定の依存関係 URL がある依存関係をすべて検索することもできます。

依存関係テーブルを使用して、オブジェクトをキャッシュから削除 (無効化) できます。依存関係を使用して、依存関係テーブルが検査され、その依存関係に応じた依存関係 URL がキャッシュ区画から削除されます。

### 区画の使用可能/使用不可

この機能によって、キャッシュ区画の状態を変更できます。外部キャッシュ制御マネージャーを使用するには、キャッシュ区画が正しい状態になければなりません。キャッシュ区画からすべてのオブジェクトを除去するには、キャッシュ区画を使用不可にする必要があります。

### ポリシーの使用

区画のポリシーを表示または変更できます。それぞれのポリシーを別々に処理することも、グループとして処理することもできます。ポリシーを変更する場合は、そのポリシーに応じた正しいタイプのデータをパスする必要があります。ポリシーに応じたデータの形式については、173ページの『外部キャッシュ制御プロトコル (ECCP) のベクトル形式』 (ポリシー・コマンド・サブベクトルとポリシー応答サブベクトル) を参照してください。

### 区画の除去

この機能によって、キャッシュ区画内のオブジェクトをすべて削除できます。キャッシュ区画を除去するには、キャッシュ区画を使用不可状態にする必要があります。

### オブジェクトの照会

この機能によって、オブジェクトがキャッシュ区画にあるかどうかを調べることができます。オブジェクトがキャッシュ区画内にあり、最終変更日付がある場合は、その日付が戻されます。戻される日付の形式については、173ページの『外部キャッシュ制御プロトコル (ECCP) のベクトル形式』 (照会応答サブベクトル) を参照してください。

### 統計の使用

この機能によって、キャッシュ区画の統計をリストおよびリセット (消去) できます。統計の形式については、173ページの『外部キャッシュ制御プロトコル (ECCP) のベクトル形式』 (統計応答サブベクトル) を参照してください。

## URL マスクの使用

この機能によって、キャッシュ区画の URL マスクを表示および変更できます。この機能を使用する際は、包含、除外、動的、またはホスト・オンデマンド・クライアント・キャッシュ・アプレットの URL タイプを指定する必要があります。URL タイプは 1 つだけ表示しなければなりません。この機能は複数の URL タイプに対しては動作しません。

URL マスクを追加できます。URL マスクが包含マスク、動的マスク、またはホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクの場合は、存続時間を指定する必要があります。動的マスクを追加すると、現行の動的 URL マスクが変更されます。ホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクを追加すると、現行のホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクが変更されます。URL マスクを削除することもできます。この機能は、動的 URL マスク、またはホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクの場合は無効です。特定タイプの URL マスクをすべてリセットできます。動的 URL マスクをリセットすると、デフォルトの動的 URL マスクにリセットされます。ホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクをリセットすると、デフォルトのホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクにリセットされます。

**注:** 動的マスクは Web サーバー・キャッシュ・イメージに対して使用されます。ホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクは、ホスト・オンデマンド・クライアント・キャッシュ機能を備えたイメージに対して使用されます。

## 外部キャッシュ制御プロトコル (ECCP) のベクトル形式

ECCP クライアントは、ベクトル形式を使用してコマンドを送信し、応答を受信します。ボックスがパスワード保護されている場合は、認証ベクトルが必要です。ボックスがパスワード保護されていない場合は、認証ベクトルは受信時に無視されます。

### ベクトル形式

ここでは、ベクトルのフィールドについて説明します。

## Web サーバー・キャッシュの使用

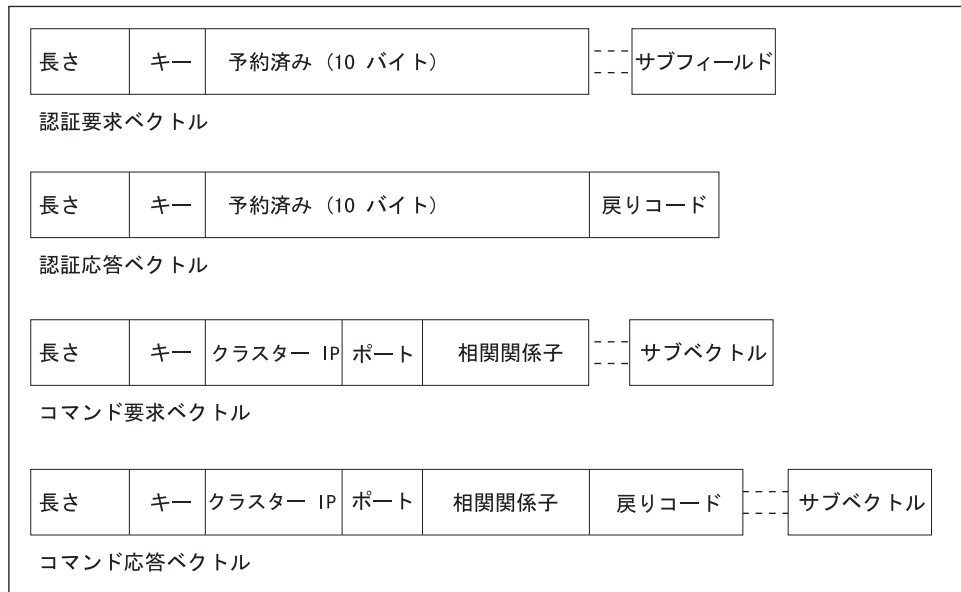


図 17. コマンド応答ベクトル

**長さ:** ベクトル全体 (長さフィールドとキー・フィールド、およびサブベクトルとサブフィールドを含む) の長さ (単位はバイト) を表す符号なしの 32 ビット値。許容される範囲は、コマンド・ベクトルの場合は 22 ~ 4GB、認証ベクトルの場合は 38 ~ 52 です。

**キー:** メジャー・ベクトル・キーを表す、符号なしの 16 ビット値。メジャー・ベクトル・キーは次のものです。

- 0x4A00 (認証要求ベクトル)
- 0x4A01 (認証応答ベクトル)
- 0x4B00 (コマンド要求ベクトル)
- 0x4B01 (コマンド応答ベクトル)

**クラスター IP:** ターゲットのキャッシュ区画に関連したキャッシュ・クラスターの IP アドレス。

**ポート:** キャッシュ区画に関連したキャッシュ・クラスターのポート番号。

**相関関係子:** ECCP クライアントがコマンド応答をコマンド要求と関連づけるために使用する、符号なしの 32 ビット値。

**戻りコード:** 戻りコードを表す符号なしの 32 ビット値。これは、応答ベクトルにだけ存在します。

ベクトルには 1 つまたは複数のサブベクトルが含まれます。認証要求ベクトルは、名前とパスワードの両サブフィールドを必要とします。コマンド要求ベクトルには、1 つまたは複数のサブベクトルが含まれます。コマンド要求ベクトルに複数のサブベクトルが含まれている場合は、コマンド応答ベクトルにも複数のサブベクトルが存在します。重大エラーが発生した場合は、コマンド応答ベクトルの戻りコード・フィールドに反映されます。

## 認証要求ベクトル

ボックスがパスワード保護されている場合は、認証要求ベクトルが外部キャッシュ制御接続の最初のベクトルでなければなりません。ボックスがパスワード保護されていない場合は、このベクトルは無視されます。

### 0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含む、ベクトルの長さ (単位はバイト)。

### 4 ~ 5

キー

0x4A00

### 6 ~ 15

予約済み

将来の利用のために予約されています。

### 16 ~ n

名前サブフィールド。

### n+1 ~ m

パスワード・サブフィールド

## コマンド要求ベクトル

コマンド要求ベクトルは、外部キャッシュ制御マネージャーにコマンドを送信します。ボックスがパスワード保護されている場合は、コマンドを受け入れる前に、まず外部キャッシュ制御マネージャーが有効な認証要求ベクトルを受け取る必要があります。

### 0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含む、ベクトルの長さ (単位はバイト)。

### 4 ~ 5

キー

0x4B00

### 6 ~ 9

クラスター IP アドレス

ターゲットのキャッシュ区画に関連したキャッシュ・クラスター (HTTP プロキシ) の IP アドレス。

### 10 ~ 11

ポート

ターゲットのキャッシュ区画に関連したキャッシュ・クラスター (HTTP プロキシ) のポート番号。

### 12 ~ 15

相関関係子



**0 ~ 3**

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

**4 ~ 5**

キー

0x4B01

**6 ~ 9**

クラスター IP アドレス

ターゲットのキャッシュ区画に関連したキャッシュ・クラスター (HTTP プロキシ) のクラスター IP アドレス。

**10 ~ 11**

ポート

ターゲットのキャッシュ区画に関連したキャッシュ・クラスター (HTTP プロキシ) のポート番号。

**12 ~ 15**

相関関係子

相関関係子は、コマンド応答を対応するコマンド要求と関連づけるために使用されます。

**16 ~ 19**

戻りコード

これは、ベクトルの戻りコードです。198ページの『戻りコード』を参照してください。

**20 ~ n**

サブベクトル

次のサブベクトルのうち 1 つまたは複数が付けられる場合があります、付けられない場合もあります。

- Add Object 応答サブベクトル (0x0101)
- Add (Force) Object 応答サブベクトル (0x0111)
- Delete Object 応答サブベクトル (0x0401)
- Dependency 応答サブベクトル (0x0A01)
- Disable 応答サブベクトル (0x0301)
- Enable 応答サブベクトル (0x0201)
- Policy 応答サブベクトル (0x0501)
- Purge 応答サブベクトル (0x0601)
- Query 応答サブベクトル (0x0701)
- Statistics 応答サブベクトル (0x0801)
- URL Mask 応答サブベクトル (0x901)

## サブベクトルの形式

ここでは、サブベクトルの形式について説明します。サブベクトルは、メジャー・ベクトルと同じ基本形式に従います。

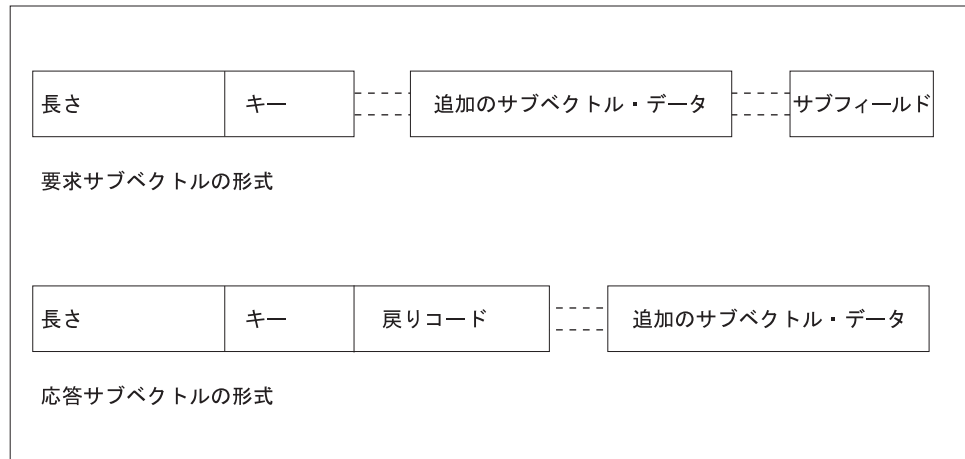


図 18. サブベクトルの形式

**長さ:** サブベクトル全体 (長さフィールドとキー・フィールド、およびサブフィールドを含む) の長さ (単位はバイト) を表す符号なしの 32 ビット値。許容される範囲は 6 ~ 4GB です (上の境界はチェックされません)。

**キー:** サブベクトル・キーを表す、符号なしの 16 ビット値。要求サブベクトル・キーには次のものがあります。

- 0x0100 (WEB オブジェクトを追加する)
- 0x0110 (WEB オブジェクトを追加し、キャッシュ制御ヘッダーは無視する)
- 0x0200 (区画のキャッシュを使用可能にする)
- 0x0300 (区画のキャッシュを使用不可にする)
- 0x0400 (WEB オブジェクトを削除する)
- 0x0500 (キャッシュ・ポリシーを変更または表示する)
- 0x0600 (区画から WEB オブジェクトをすべて削除する)
- 0x0700 (WEB オブジェクトが区画にあるかどうか判別する)
- 0x0800 (キャッシュ統計値をリセットまたは表示する)
- 0x0900 (URL マスクを追加、削除、表示する)
- 0x0A00 (依存関係を追加、削除、表示、リセットする)

戻される応答サブベクトル・キーは次のとおりです。

- 0x0101 (WEB オブジェクトを追加する)
- 0x0111 (WEB オブジェクトを追加し、キャッシュ制御ヘッダーは無視する)
- 0x0201 (区画のキャッシュを使用可能にする)
- 0x0301 (区画のキャッシュを使用不可にする)
- 0x0401 (WEB オブジェクトを削除する)
- 0x0501 (キャッシュ・ポリシーを変更または表示する)



- 0x0601 (区画から WEB オブジェクトをすべて削除する)
- 0x0701 (WEB オブジェクトが区画にあるかどうか判別する)
- 0x0801 (キャッシュ統計値をリセットまたは表示する)
- 0x0901 (URL マスクを追加、削除、表示する)
- 0x0A01 (依存関係を追加、削除、表示、リセットする)

**戻りコード:** 要求サブベクトルの戻りコードを表す符号なしの 32 ビット値。これは、応答サブベクトルにだけ存在します。

**Add Object コマンド・サブベクトル:** Add Object コマンド・サブベクトルは、キャッシュ区画に Web オブジェクトを追加するために使用されます。

**0 ~ 3**

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

**4 ~ 5**

キー

0x0110

**6 ~ n**

URL サブフィールド

**n+1 ~ m**

オブジェクト・サブフィールド

**Add (force) Object コマンド・サブベクトル:** Add (force) Object コマンド・サブベクトルは、キャッシュ区画に Web オブジェクトを追加するために使用されます。これは、オブジェクトのキャッシュ制御ヘッダーが無視されるという点で Add Object コマンド・サブベクトルとは異なります。

**0 ~ 3**

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

**4 ~ 5**

キー

0x0100

**6 ~ n**

URL サブフィールド

**n+1 ~ m**

オブジェクト・サブフィールド

**Delete Object コマンド・サブベクトル:** Delete Object コマンド・サブベクトルは、キャッシュ区画から Web オブジェクトを削除するために使用されます。

**0 ~ 3**

長さ

## Web サーバー・キャッシュの使用

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

### 4 ~ 5

キー

0x0400

### 6 ~ n

URL サブフィールド

**Dependency コマンド・サブベクトル:** Dependency コマンド・サブベクトルは、依存関係テーブルを修正/表示するため、依存関係テーブルを使用してオブジェクトを無効にするために使用されます。

### 0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

### 4 ~ 5

キー

0x0A00

### 6 ~ 7

コマンド

実行する dependency コマンド。

#### 0x0001

依存関係テーブルを入手する (依存関係については、依存関係タイプを参照)

#### 0x0002

依存関係テーブルに新しい依存関係/依存関係 URL を追加する

#### 0x0003

依存関係から依存関係/依存関係 URL を削除する

#### 0x0004

依存関係テーブルの情報をリセットする (依存関係については、依存関係タイプを参照)

#### 0x0005

依存関係に基づいてオブジェクトを無効にする

#### 0x0006

依存関係テーブルのガーベッジ・コレクションを行う

### 8 ~ 9

依存関係タイプ

依存関係タイプ・フィールドは、変更するデータを指定するために使用されます。このデータは、Dependency コマンドを使用して変更されます。

#### 0x0000

依存関係タイプなし

**0x0001**

テーブル全体に対してコマンドを使用する。

- 上のコマンドが 0x0001 (Get) の場合 - テーブル全体を入手する。
- 上のコマンドが 0x0004 (Reset) の場合 - テーブル全体を消去する。

**0x0002**

依存関係に基づいてコマンドを使用する。

- 上のコマンドが 0x0001 (Get) の場合 - 指定の依存関係に応じた URL をすべて入手する。
- 上のコマンドが 0x0004 (Reset) の場合 - テーブルから依存関係を消去する。

**0x0003**

URL に基づいてコマンドを使用する。

- 上のコマンドが 0x0001 (Get) の場合 - 指定の依存関係 URL に応じた依存関係をすべて入手する。
- 上のコマンドが 0x0004 (Reset) の場合 - テーブルから依存関係 URL を消去する。

**10 ~ n**

ゼロまたは任意数のサブフィールド。

**依存関係サブフィールド**

注: 両方のサブフィールドが必要な場合は、このサブフィールドが最初でなければなりません。  
次のコマンド-依存関係タイプを使用する場合に必要です。

コマンド	依存関係タイプ
0x0001	0x0002
0x0002	0x0000
0x0003	0x0000
0x0004	0x0002
0x0005	0x0000

**URL サブフィールド**

注: 両方のサブフィールドが必要な場合は、このサブフィールドが 2 番目でなければなりません。  
次のコマンド-依存関係タイプを使用する場合に必要です。

コマンド	依存関係タイプ
0x0001	0x0003
0x0002	0x0000
0x0003	0x0000
0x0004	0x0003

**Disable コマンド・サブベクトル:** Disable コマンド・サブベクトルは、キャッシュ区画を使用不可にするために使用されます。

**0 ~ 3**

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

**4 ~ 5**

キー

0x0300

**Enable コマンド・サブベクトル:** Enable コマンド・サブベクトルは、キャッシュ区画を使用可能にするために使用されます。

## Web サーバー・キャッシュの使用

### 0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

### 4 ~ 5

キー

0x0200

**Policy コマンド・サブベクトル:** Policy コマンド・サブベクトルを使用すると、キャッシュ区画を変更でき、またキャッシュ区画の情報を表示できます。

### 0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

### 4 ~ 5

キー

0x0500

### 6 ~ 7

コマンド

実行するコマンド。

**0x0001**

ポリシーの入手

**0x0002**

ポリシーの更新

### 8 ~ 9

ポリシー・タイプ

ポリシー・タイプは、変更するデータを指定するために使用されます。このデータは、Policy コマンドを使用して変更されます。

**0x0001**

透過キャッシュ

**0x0002**

HTTP キャッシュ制御ヘッダー

**0x0003**

キャッシュ動的オブジェクト

**0x0004**

キャッシュ・イメージ・オブジェクト ("\*.gif"、 "\*.jpg")

**0x0005**

キャッシュ静的オブジェクト

**0x0006**

動的オブジェクトのデフォルト存続時間

<b>0x0007</b>	イメージ・オブジェクトのデフォルト存続時間
<b>0x0008</b>	静的オブジェクトのデフォルト存続時間
<b>0x0009</b>	ガーベッジ・コレクション間の時間 (単位は秒)
<b>0x000A</b>	最大区画サイズ (MB)。
<b>0x000B</b>	キャッシュ区画のオブジェクトの最大数
<b>0x000C</b>	キャッシュ区画のオブジェクトの最大サイズ
<b>0xFFFF</b>	すべてのポリシーに対する操作。

注: コマンドが **get (0x0001)** の場合は、これがサブベクトルの最後になります。

#### 10 ~ n

上のポリシー・タイプに応じて、次のどれか 1 つ。

ポリシー・タイプ = 0x0001、0x0002、0x0003、0x0004、または 0x0005 の場合:

#### 10 ~ 11

設定値

- 0x0001 (使用可能)
- 0x0002 (使用不可)

ポリシー・タイプ = 0x0006、0x0007、または 0x0008 の場合

#### 10 ~ 13

オブジェクトの存続時間 (単位は分) を表す値。

範囲は 0 ~ 10080 で、0 は有効期限のないオブジェクトを表します。

ポリシー・タイプ = 0x0009 の場合

#### 10 ~ 13

キャッシュ除去間隔 (単位は分) を表す値。

範囲は 0 ~ 720 で、0 はガーベッジ・コレクションを使用不可にすることを示します。

ポリシー・タイプ = 0x000A の場合

#### 10 ~ 11

最大区画サイズ (単位は MB) を表す値。範囲は 0 ~ 4095 で、0 は制限がないことを示します。

注: この値は検査されません。

ポリシー = 0x000B の場合

## Web サーバー・キャッシュの使用

### 10 ～ 13

オブジェクトの最大数を表す値。

範囲は 0 ～ 100000 で、0 は制限がないことを示します。

注: この値は検査されません。

ポリシー = 0x000C の場合

### 10 ～ 13

キャッシュ区画のオブジェクトの最大サイズを表す値。

範囲は 512 ～ 300000 で、0 を入力すると制限なしになります。

注: この値は検査されません。

ポリシー = 0xFFFF の場合

### 10 ～ 11

キャッシュ透過 (設定値)

- 0x0001 (使用可能)
- 0x0002 (使用不可)

### 12 ～ 13

HTTP キャッシュ制御ヘッダー (設定値)

- 0x0001 (使用可能)
- 0x0002 (使用不可)

### 14 ～ 15

キャッシュ動的 (設定値)

- 0x0001 (使用可能)
- 0x0002 (使用不可)

### 16 ～ 17

キャッシュ・イメージ (設定値)

- 0x0001 (使用可能)
- 0x0002 (使用不可)

### 18 ～ 19

キャッシュ静的 (設定値)

- 0x0001 (使用可能)
- 0x0002 (使用不可)

### 20 ～ 21

最大区画サイズ (単位は MB) を表す値。

範囲は 0 ～ 4095 で、0 は制限がないことを示します。

注: この値は検査されません。

### 20 ～ 21

最大区画サイズ (単位は MB) を表す値。

範囲は 0 ～ 4095 で、0 は制限がないことを示します。

注: この値は検査されません。

**22 ~ 25**

オブジェクトの最大数を表す値。

範囲は 0 ~ 1000000 で、0 は制限がないことを示します。

注: この値は検査されません。

**26 ~ 29**

キャッシュ区画のオブジェクトの最大サイズを表す値。

範囲は 512 ~ 3000000 で、0 を指定すると制限なしになります。

注: この値は検査されません。

**30 ~ 33**

動的オブジェクトの存続時間 (単位は分) を表す値。

範囲は 0 ~ 10080 で、0 は有効期限のないオブジェクトを表します。

注: この値は検査されません。

**34 ~ 37**

イメージ・オブジェクトの存続時間 (単位は分) を表す値。

範囲は 0 ~ 10080 で、0 を指定すると制限なしになります。

注: この値は検査されません。

**38 ~ 41**

静的オブジェクトの存続時間 (単位は分) を表す値。

範囲は 0 ~ 10080 で、0 は制限がないことを表します。

注: この値は検査されません。

**42 ~ 45**

キャッシュ除去間隔 (単位は分) を表す値。

範囲は 0 ~ 720 で、0 はガーベッジ・コレクションを使用可能にすることを示します。

**Purge コマンド・サブベクトル:** Purge コマンド・サブベクトルは、キャッシュ区画からオブジェクトをすべて消去するために使用されます。

**0 ~ 3**

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

**4 ~ 5**

キー

0x0600

**Query コマンド・サブベクトル:** Query コマンド・サブベクトルは、指定の URL がキャッシュ区画にあるかどうか検査するために使用されます。

## Web サーバー・キャッシュの使用

### 0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

### 4 ~ 5

キー

0x0700

### 6 ~ n

URL サブフィールド

**Statistics コマンド・サブベクトル:** Statics コマンド・サブベクトルは、キャッシュ区画の統計値を入手/リセットするために使用されます。

### 0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

### 4 ~ 5

キー

0x0800

### 6 ~ 7

コマンド

- 0x0001 - キャッシュ区画の統計値を入手する。
- 0x0004 - キャッシュ区画の統計値をリセットする。

**URL Mask コマンド・サブベクトル:** URL Mask コマンド・サブベクトルは、キャッシュ区画に関連した URL マスクを表示/修正するために使用されます。

### 0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

### 4 ~ 5

キー

0x0900

### 6 ~ 7

コマンド

- 0x0001 - 現在定義されている URL マスクを入手する (戻されるマスクのタイプについては、下記の URL タイプを参照)。
- 0x0002 - 指定の URL マスクを追加する (追加されるマスクのタイプについては、下記の URL タイプを参照)。
- 0x0003 - 指定の URL マスクを削除する (削除されるマスクのタイプについては、下記の URL タイプを参照)。



注: 動的 URL マスク、またはホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクの削除は、無効な機能です。

- 0x0004 - 下記の URL タイプの URL マスクをすべてリセットする。

8 ~ 9

URL タイプ

- 0x0001 - 包含
- 0x0002 - 除外
- 0x0003 - 動的
- 0x0004 - ホスト・オンデマンド・クライアント・キャッシュ・アプレット

10 ~ 13

存続時間

範囲は 0 ~ 10080 で、0 は有効期限のないオブジェクトを表します。URL タイプが包含 (0x0001)、動的 (0x0003)、またはホスト・オンデマンド・クライアント・キャッシュ (0x0004) の場合に、Add (0x0002) コマンドに対してだけ使用されます。

注: コマンドが **GET (0x0001)** または **Clear (0x0004)** の場合は、これがサブベクトルの最後になります。

14 ~ n

URL コマンド・サブベクトル 1 つ。

**Add Object 応答サブベクトル:** Add Object 応答サブベクトルは、Add (force) Object コマンド・サブベクトルに回答するために使用されます。

0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

4 ~ 5

キー

0x0101

6 ~ 9

戻りコード

198ページの『戻りコード』を参照してください。

**Add (force) 応答サブベクトル:** Add (force) 応答サブベクトルは、Add (force) Object コマンド・サブベクトルに回答するために使用されます。

0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

4 ~ 5

キー

0x0111

## Web サーバー・キャッシュの使用

6 ~ 9

戻りコード

198ページの『戻りコード』を参照してください。

**Delete Object 応答サブベクトル:** Delete Object 応答サブベクトルは、Add (force) Object コマンド・サブベクトルに応答するために使用されます。

0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

4 ~ 5

キー

0x0401

6 ~ 9

戻りコード

198ページの『戻りコード』を参照してください。

**Dependency 応答サブベクトル:** Dependency 応答サブベクトルは、Dependency コマンド・サブベクトルに応答するために使用されます。

0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

4 ~ 5

キー

0x0A01

6 ~ 9

戻りコード

198ページの『戻りコード』を参照してください。

## 10 ~ n

ゼロまたは任意数のサブフィールド。

**依存関係サブフィールド**

注: このサブフィールドは、依存関係に関する URL コマンド・サブフィールドの前になければなりません。次のコマンド-依存関係タイプを使用する場合に必要です。詳しくは、180ページの『Dependency コマンド・サブベクトル』を参照してください。

コマンド	依存関係タイプ	
0x0001	0x0001	注: 依存関係サブフィールドの後にある URL サブフィールドは、その依存関係にある依存関係 URL です。
0x0001	0x0003	

**URL サブフィールド**

注: 両方のサブフィールドが必要な場合は、このサブフィールドが 2 番目になければなりません。次のコマンド-依存関係タイプを使用する場合に必要です。

コマンド	依存関係タイプ	
0x0001	0x0001	注: URL サブフィールドの前にある依存関係サブフィールドは、その依存関係にある URL です。
0x0001	0x0002	

**Disable 応答サブベクトル:** Disable 応答サブベクトルは、Disable コマンド・サブベクトルに応答するために使用されます。

## 0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

## 4 ~ 5

キー

0x0301

## 6 ~ 9

戻りコード

198ページの『戻りコード』を参照してください。

**Enable 応答サブベクトル:** Enable 応答サブベクトルは、enable コマンド・サブベクトルに応答するために使用されます。

## 0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

## 4 ~ 5

キー

0x0201

## 6 ~ 9

戻りコード

198ページの『戻りコード』を参照してください。

**Policy 応答サブベクトル:** Policy 応答サブベクトルは、Policy コマンド・サブベクトルに応答するために使用されます。

## Web サーバー・キャッシュの使用

### 0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含む、ベクトルの長さ (単位はバイト)。

### 4 ~ 5

キー

0x0501

### 6 ~ 9

戻りコード

198ページの『戻りコード』を参照してください。

**Policy コマンド・サブベクトルが PUT (0x0002) の場合は、これがサブベクトルの最後になります。**

### 10 ~ n

Policy コマンド・サブベクトルのポリシー・タイプに応じて、次のどれか 1 つ。

ポリシー・タイプ = 0x0001、0x0002、0x0003、0x0004、または 0x0005 の場合:

#### 10 ~ 11

設定値

- 0x0001 (使用可能)
- 0x0002 (使用不可)

ポリシー・タイプ = 0x0006、0x0007、または 0x0008 の場合

#### 10 ~ 13

オブジェクトの存続時間 (単位は分) を表す値。

範囲は 0 ~ 10080 で、0 は有効期限のないオブジェクトを表します。

ポリシー・タイプ = 0x0009 の場合

#### 10 ~ 13

キャッシュ除去間隔 (単位は分) を表す値。

範囲は 0 ~ 720 で、0 はガーベッジ・コレクションを使用不可にすることを示します。

ポリシー・タイプ = 0x000A の場合

#### 10 ~ 11

最大区画サイズ (単位は MB) を表す値。 範囲は 0 ~ 4095 で、0 は制限がないことを示します。

**注:** この値は検査されません。

ポリシー = 0x000B の場合

#### 10 ~ 13

オブジェクトの最大数を表す値。

範囲は 0 ～ 100000 で、0 は制限がないことを示します。

注: この値は検査されません。

ポリシー = 0x000C の場合

**10 ～ 13**

キャッシュ区画のオブジェクトの最大サイズを表す値。

範囲は 512 ～ 300000 で、0 を入力すると制限なしになります。

注: この値は検査されません。

ポリシー = 0xFFFF の場合

**10 ～ 11**

キャッシュ透過 (設定値)

- 0x0001 (使用可能)
- 0x0002 (使用不可)

**12 ～ 13**

HTTP キャッシュ制御ヘッダー (設定値)

- 0x0001 (使用可能)
- 0x0002 (使用不可)

**14 ～ 15**

キャッシュ動的 (設定値)

- 0x0001 (使用可能)
- 0x0002 (使用不可)

**16 ～ 17**

キャッシュ・イメージ (設定値)

- 0x0001 (使用可能)
- 0x0002 (使用不可)

**18 ～ 19**

キャッシュ静的 (設定値)

- 0x0001 (使用可能)
- 0x0002 (使用不可)

**20 ～ 21**

最大区画サイズ (単位は MB) を表す値。

範囲は 0 ～ 4095 で、0 は制限がないことを示します。

注: この値は検査されません。

**22 ～ 25**

オブジェクトの最大数を表す値。

範囲は 0 ～ 1000000 で、0 は制限がないことを示します。

注: この値は検査されません。

## Web サーバー・キャッシュの使用

### 26 ~ 29

キャッシュ区画のオブジェクトの最大サイズを表す値。

範囲は 512 ~ 3000000 で、0 を指定すると制限なしになります。

注: この値は検査されません。

### 30 ~ 33

動的オブジェクトの存続時間 (単位は分) を表す値。

範囲は 0 ~ 10080 で、0 は有効期限のないオブジェクトを表します。

注: この値は検査されません。

### 34 ~ 37

イメージ・オブジェクトの存続時間 (単位は分) を表す値。

範囲は 0 ~ 10080 で、0 を指定すると制限なしになります。

注: この値は検査されません。

### 38 ~ 41

静的オブジェクトの存続時間 (単位は分) を表す値。

範囲は 0 ~ 10080 で、0 は制限がないことを表します。

注: この値は検査されません。

### 42 ~ 45

キャッシュ除去間隔 (単位は分) を表す値。

範囲は 0 ~ 720 で、0 はガーベッジ・コレクションを使用不可にすることを示します。

**Purge 応答サブベクトル:** Purge 応答サブベクトルは、Purge コマンド・サブベクトルに  
応答するために使用されます。

### 0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの  
長さ (単位はバイト)。

### 4 ~ 5

キー

0x0601

### 6 ~ 9

198ページの『戻りコード』を参照してください。

**Query 応答サブベクトル:** Query 応答サブベクトルは、指定の URL がキャッシュ  
区画にあるかどうか検査するために使用されます。

### 0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの  
長さ (単位はバイト)。

4 ~ 5

キー

0x0701

6 ~ 9

戻りコード

198ページの『戻りコード』を参照してください。

注: 戻りコードが正しくない場合 (0x00000000 でない) は、これがサブベクトルの最後になります。

10 ~ 37

オブジェクトが最後に変更された時刻 (単位は GMT)。

注: 戻りコードが 0x00000000 でなかった場合、または戻りコードがキャッシュ区画によって認識されない場合は、このフィールドは存在しません。

10 ~ 13

秒数

14 ~ 17

分数

18 ~ 21

時間数

22 ~ 25

1 月からの月数 (0 ~ 11)

26 ~ 29

1900 年からの年数

30 ~ 33

日曜日からの日数 (0 ~ 6)

34 ~ 37

日

**Statistics 応答サブベクトル:** Statistics 応答サブベクトルは、Statistics コマンド・サブベクトルに応答します。

0 ~ 3

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトル全体の長さ (単位はバイト)。

4 ~ 5

キー

0x0801

6 ~ 9

戻りコード

これは、サブベクトルの戻りコードです。

10 ~

## Web サーバー・キャッシュの使用

### 10 ~ 13

キャッシュ区画の現在のバイト数。この数は実体のバイト数だけを反映し、ヘッダーや制御ブロックを格納するために使用されるバイト数は含みません。

### 14 ~ 17

キャッシュ区画のバイト数の上限基準点。

### 18 ~ 21

キャッシュ区画の現在のオブジェクト数。

### 22 ~ 25

キャッシュ区画のオブジェクト数の上限。

### 26 ~ 29

オブジェクトがキャッシュ区画内で検出された合計回数。

### 30 ~ 33

オブジェクトがキャッシュ区画内で検出されなかった合計回数。

### 34 ~ 37

包含 URL マスクによって明示的にキャッシュ区画に追加されたオブジェクトの数。

### 40 ~ 43

キャッシュがオフになっていたためにキャッシュ区画に追加されなかったオブジェクトの数。

### 44 ~ 47

オブジェクトが大きすぎるためにキャッシュ区画に追加されなかったオブジェクトの数。

### 48 ~ 51

HTTP 制御ヘッダーに DONT CACHE が指定されているためにキャッシュ区画に追加されなかったオブジェクトの数。

### 52 ~ 55

URL マスクによって明示的に除外されていたためにキャッシュ区画に追加されなかったオブジェクトの数。

### 56 ~ 59

オブジェクトが古くなったためにキャッシュ区画に追加されなかったオブジェクトの数。

### 60 ~ 63

イメージ・オブジェクトを明示的にキャッシュに入れなかったために、キャッシュ区画に追加されなかったオブジェクトの数。

### 64 ~ 67

静的オブジェクトを明示的にキャッシュに入れなかったために、キャッシュ区画に追加されなかったオブジェクトの数。

### 68 ~ 71

動的オブジェクトを明示的にキャッシュに入れなかったために、キャッシュ区画に追加されなかったオブジェクトの数。



**72 ~ 75**

キャッシュがいっぱいになったため、または全キャッシュ区画が Web サーバー・キャッシュで可能な合計量を超えたために除去されたオブジェクトの数。

**76 ~ 79**

オブジェクトの存続時間が満了したために除去されたオブジェクトの数。

**80 ~ 83**

URL の指定、または区画全体の除去によって、明示的に除去されたオブジェクトの数。

**84 ~ 87**

依存関係が無効になったために除去されたオブジェクトの数。

**URL Mask 応答サブベクトル:** URL Mask 応答サブベクトルは、URL Mask コマンド・サブベクトルに応答するために使用されます。

**0 ~ 3**

長さ

長さフィールドとキー・フィールド、およびサブベクトルを含むベクトルの長さ (単位はバイト)。

**4 ~ 5**

キー

0x0901

**6 ~ 9**

戻りコード

これは、サブベクトルの戻りコードです。198ページの『戻りコード』を参照してください。

**10 ~ n**

ゼロまたはそれ以上の URL サブベクトル (URL Mask コマンド・サブベクトルが GET (0x0001) の場合)。

## サブフィールドの形式

ここでは、サブフィールドのフィールドについて説明します。

## Web サーバー・キャッシュの使用

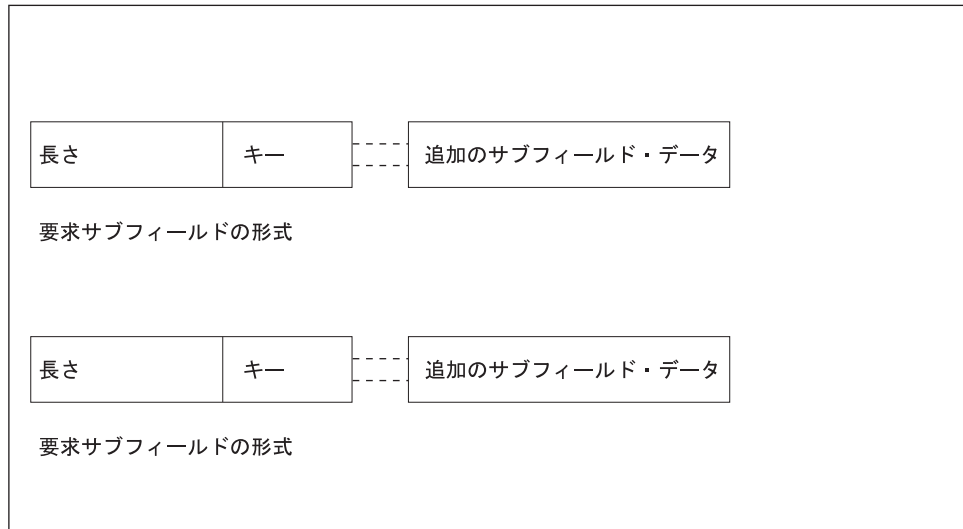


図 19. サブフィールドの形式

**長さ:** サブフィールド全体 (長さフィールドとキー・フィールドを含む) の長さ (単位はバイト) を表す符号なしの 32 ビット値。許容される範囲は 6 ~ 4GB です。

**キー:** サブフィールド・キーを表す符号なしの 16 ビット値。コマンドのサブフィールド・キーには次のものがあります。

- 0x0010 (プロトコル "http:" とインターネット・リソース・アドレスを取り除いた URL。たとえば URL "http://192.9.200.50/file1.html" は、"/file1.html" として送信されます)。
- 0x0020 (HTTP 応答メッセージ形式の WEB オブジェクト)
- 0x0030 (ECCP ユーザーの名前。このサブフィールドは、認証ベクトルの場合に必要です)
- 0x0040 (ECCP ユーザーのパスワード。このサブフィールドは、認証ベクトルの場合に必要です)
- 0x0050 (依存関係サブフィールド)

応答サブフィールド・キーは、次のとおりです。

- 0x0011 (プロトコル "http:" とインターネット・リソース・アドレスを取り除いた URL)
- 0x0051 (依存関係サブフィールド)

**依存関係サブフィールド:** URL Mask 応答サブベクトルの依存関係サブフィールド。

**0 ~ 3**

長さ

長さフィールドとキー・フィールドを含むベクトルの長さ (単位はバイト)。

**4 ~ 5**

キー

0x0050 - 要求

0x0051 - 応答

6 ~ n

依存関係

長さは 1 ~ 50 でなければなりません。

**名前サブフィールド:** URL Mask 応答サブベクトルの名前サブフィールド。

0 ~ 3

長さ

長さフィールドとキー・フィールドを含むベクトルの長さ (単位はバイト)。

4 ~ 5

キー

0x00030 - 要求

6 ~ n

名前

長さは 1 ~ 8 でなければなりません。

**オブジェクト・サブフィールド:** URL Mask 応答サブベクトルのオブジェクト・サブフィールド。

0 ~ 3

長さ

長さフィールドとキー・フィールドを含むベクトルの長さ (単位はバイト)。

4 ~ 5

キー

0x002 - 要求

6 ~ n

オブジェクト

オブジェクトは、HTTP 応答と同じ形式でなければなりません。オブジェクトは文字の配列です。

**パスワード要求サブフィールド:** URL Mask 応答サブベクトルのパスワード要求サブフィールド。

0 ~ 3

長さ

長さフィールドとキー・フィールドを含むベクトルの長さ (単位はバイト)。

4 ~ 5

キー

0x0400

6 ~ 14

暗号化に使用されるシード (8 バイトでなければなりません)。

15 ~ n

パスワード

長さは 1 ~ 8 で、暗号化されている必要があります。

## Web サーバー・キャッシュの使用

**URL 要求サブフィールド:** URL Mask 応答の URL 要求サブフィールド。

### 0 ~ 3

長さ

長さフィールドとキー・フィールドを含むベクトルの長さ (単位はバイト)。

### 4 ~ 5

キー

0x0010 - 要求

0x0011 - 応答

### 6 ~ n

URL または URL マスク

これは文字の配列で、配列の長さは 1 ~ 255 でなければなりません。

## 戻りコード

応答ベクトルの戻りコードのほかに、それぞれの応答サブベクトルの戻りコードをチェックすることが重要です。重大エラーが検出された場合は、応答ベクトルの戻りコードは非ゼロ値になります。この場合、コマンドのコマンド・サブベクトルに、対応する応答サブベクトルがある場合とない場合があります。

### 戻りコードと説明:

0000 0000: 操作は正常に完了した  
0001 0000: オブジェクトが検出されなかった  
0002 0000: キャッシュ区画はすでに使用可能になっている  
0003 0000: キャッシュ区画はすでに使用不可になっている  
0004 0000: キャッシュ区画は使用可能になっていない  
0005 0000: キャッシュ区画は定義されていない  
0006 0000: キャッシュ区画は終了している  
0007 0000: URL サブフィールドが必要だが存在しない  
0008 0000: 指定された除去間隔が無効である  
0009 0000: サポートされない設定値  
000A 0000: サポートされないコマンド値  
000B 0000: サポートされないポリシー・タイプ値  
000C 0000: サポートされない URL タイプ値  
000D 0000: サポートされないベクトル・キー  
000E 0000: サポートされないサブベクトル・キー  
000F 0000: オブジェクトのヘッダーを構文解析できない  
0010 0000: 記憶域を入手できない  
0011 0000: オブジェクトが大きすぎて区画を追加できない  
0012 0000: ベクトル形式が無効である  
0013 0000: オブジェクトはキャッシュ不能である  
0014 0000: HTTP 構文解析エラーが検出された  
0015 0000: オブジェクト・サブフィールドが必要だが存在しない  
0016 0000: 依存関係サブフィールドが指定されていないか無効である  
0017 0000: 認証ベクトルが必要である  
0018 0000: 認証ベクトルは必要でなく、したがって無視される  
0019 0000: 依存関係が依存関係テーブルにない

001A 0000: 依存関係 URL が依存関係テーブルにない  
 001B 0000: サポートされない依存関係タイプ  
 001C 0000: ECC に対するユーザー ID/パスワード/許可が正しくない  
 001D 0000: ボックスにイメージをロードするための URL マスクが正しくない  
 FF01 yyyy: コマンドが失敗した。最後の 2 バイトに追加情報があります。  
     0101: オブジェクトが検出されなかった。  
     0102: オブジェクトをキャッシュに入れることができなかった。  
     0103: オブジェクトはすでに区画に存在している。  
     0104: 区画の初期設定が失敗した (最大数の区画がすでにアクティブになっている)。  
     0105: 区画がアクティブになっている。  
     0106: 区画がアクティブになっていない。  
     0107: 区画が保留状態にあり、コマンドを実行できない。  
         数秒間待って、コマンドを再度試行してください。  
     0108: 区画が定義されていない。  
     0109: URL タイプがサポートされていない。  
     010A: URL ポインターが無効。  
     010B: 区画番号が無効。  
     010C: 区画コマンドがサポートされていない。  
     010D: 区画ポインターが無効。  
     010E: 区画ハンドルがアクティブな区画を参照していない。  
     010F: 区画ハンドルが有効な区画を参照していない。  
     0110: ポリシー・ポインターが必要だが存在しない。  
     0111: 統計ポインターが必要だが存在しない。  
     0112: 除去間隔が長すぎる。  
     0113: 依存関係にすでに URL がある。  
 0FFF: 外部キャッシュ制御が使用できない。  
 FFF9: 記憶域を獲得できない。  
 FFFA: 区画ハンドルを獲得できない。  
 FFFB: ポリシー SRAM ポインターが必要だが存在しない。  
 FFFC: 区画 SRAM ポインターが必要だが存在しない。  
 FFFD: キャッシュの有効期限間隔の割り振り/初期設定ができない。  
 FFFE: キャッシュ区画の割り振り/初期設定ができない。  
 FFFF: キャッシュ・コアの割り振り/初期設定ができない。

## Web サーバー・キャッシュの使用

---

## 第12章 Web サーバー・キャッシュの構成と監視

この章では、Web サーバー・キャッシュ機能を構成する方法と、Web サーバー・キャッシュ監視コマンドを使用する方法を説明します。この章の内容は次のとおりです。

- 『Web サーバー・キャッシュの構成』
- 207ページの『Web サーバー・キャッシュ環境へのアクセス』
- 207ページの『Web サーバー・キャッシュのコマンド』
- 214ページの『Web サーバー・キャッシュ監視環境へのアクセス』
- 215ページの『Web サーバー・キャッシュ監視コマンド』

---

### Web サーバー・キャッシュの構成

Web サーバー・キャッシュは、ネットワーク・ディスパッチャーと一緒に使用する必要があります。Web サーバー・キャッシュを初めて使用する場合は、その前にまず次のことを行う必要があります。

1. Config> プロンプトで **feature ndr** コマンドを使用して、talk 6 によってネットワーク・ディスパッチャーにアクセスする。
2. 実行プログラムを使用可能にする。
3. クラスタを追加する。
4. ポートを追加する。
5. 1 台または複数台のサーバーを追加する。

その後、構成コマンドと監視コマンドを使用して、Web サーバー・キャッシュ環境を更新できます。

**注:** Talk 6 によってネットワーク・ディスパッチャーを変更すると現行の稼働構成が変更されるのに対し、Web サーバー・キャッシュを変更した場合は、Talk 6 の **activate** コマンド、または Talk 5 の **feature Webc** によって明示的にアクティブ化しないかぎり、現行の稼働構成は変更されません。この例外は、Talk 6 **feature NDR** によって HTTP プロキシ用のクラスター/ポートを削除した場合です。この場合は、Web サーバー・キャッシュ用の HTTP プロキシも、現行の稼働構成から削除されます。

**例:**

```
Config>f ndr
NDR Config>enable executor
NDR Config>add cluster
Cluster Address [0.0.0.0]? 113.3.1.10
FIN count [4000]?
FIN time out [30]?
FIN stale timer [1500]?
Cluster 113.3.1.12 has been added.
Fincount has been set to 4000 for cluster 113.3.1.10
Fintimeout has been set to 30 for cluster 113.3.1.10
Staletimer has been set to 1500 for cluster 113.3.1.10
NDR Config>add port
Cluster Address [0.0.0.0]? 113.3.1.10
Port number [80]?
Port type (tcp=1, upd=2, both=3) [3]?
Max. weight (0-100) [20]?
```

## Web サーバー・キャッシュの構成と監視

```
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 cache=3 extcache=4) [0]? 3
Do you want a new cache partition? [Yes]:
Enter cache partition [0]?
Default server TCP connection timeout (Range 5-240 seconds) [120]?
Default client TCP connection timeout (Range 5-240 seconds) [120]?
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]?
Maximum number of objects (1-100000 or 0 for no limit) [0]?
Maximum object size (512-300000 bytes or 0 for no limit) [0]?
Do you want the cache activated upon reboot? [Yes]:
Default cache purge interval (1-720 minutes or 0 to disable) [10]
Enable transparent caching? [Yes]:
Check cache control headers? [Yes]:
Cache images? [Yes]:
  Default expiration time for images
  (1-10080 minutes or 0 for no expiration) [60]?
Cache non-image static objects? [Yes]:
  Default expiration time for non-image static objects
  (1-10080 minutes or 0 for no expiration) [60]?
URL mask to identify dynamic objects [*/cgi*]?
Cache dynamic objects? [No]:
Do you want to add a URL mask? [No]:

Cache partition number 1 has been successfully created.
Requested port has been added to cluster 113.3.1.10
Maxweight has been set to 20 for port 80 in cluster 113.3.1.10
NDR Config>add server
Cluster Address [0.0.0.0] ? 113.3.1.10
Port number [80] ? 80
Server Address [0.0.0.0] ? 113.1.2.0
Server weight [20] ?
Server state (down=0, up=1) [1] ?
Server 113.1.2.0 has been added to the requested port(s) of cluster 113.3.1.10
Weight of server 113.1.2.0 has been set to 20 in port 80 of cluster 113.31.10
Server 113.1.2.0 has been set up.
NDR Config> exit
```

次では、例のパラメーターとその説明です。

### cluster-address

クラスターの IP アドレスを指定します。

**注:** クラスター IP アドレスは、直前のホップ・ルーター (IP ルーター) と同じ論理サブネット上に存在するものと想定しています。

**有効値:** 任意の有効な IP アドレス

**デフォルト値:** 0.0.0.0

**FIN-count** 実行プログラムが *FIN-timeout* または *Stale-timer* の経過後にネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みる前に、FIN 状態にあることが必要な接続の数を指定します。

**有効値:** 0 ~ 65535

**デフォルト値:** 4000

**FIN-timeout** 接続が FIN 状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みます。

**有効値:** 0 ~ 65535

**デフォルト値:** 30

**Stale-timer** 接続が非活動状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから接続の情報の除去を試みます。



有効値: 0 ~ 65535

デフォルト値: 1500

**port#** このクラスターのプロトコルのポート番号を指定します。

有効値: 1 ~ 65535

デフォルト値: 80

**port-type** このポートでロード・バランスを取ることができる IP トラフィックのタイプを指定します。サポートされるタイプは、次のとおりです。

- 1 = TCP
- 2 = UDP
- 3 = 両方

有効値: 1、2、3

デフォルト値: 3

**max-weight** このポート上のサーバーの最大重みを指定します。これは、実行プログラムが各サーバーに分配する要求数の相違に影響します。

有効値: 0 ~ 100

デフォルト値: 20

**port-mode** ポートが、1 つのクライアントからの要求をすべて 1 つのサーバーに送る (sticky と呼ばれる) か、パッシブ ftp を使用する (pftp) か、Web サーバー・キャッシュを使用するか (cache)、外部スケーラブル・キャッシュ・アレイを送るか (extcache)、またはこのクラスターでは特定のプロトコルを使用しない (none) かを指定します。

有効値: 0 ~ 4。ただし、

- 0 = none
- 1 = sticky
- 2 = pftp
- 3 = cache
- 4 = extcache

デフォルト値: 0

**Do you want a new cache partition?**

既存のキャッシュ区画を使用するか、新しい区画を使用するかを指定します。

有効値: Yes または No

デフォルト値: Yes

**Enter cache partition**

使用する既存のキャッシュ区画の番号を指定します。

有効値: 任意の既存キャッシュ区画番号

デフォルト値: 0

## Web サーバー・キャッシュの構成と監視

### Default server TCP connection timeout

サーバー接続の有効期限が切れるまでの時間を指定します。

有効値: 5 ~ 240 秒

デフォルト値: 120 秒

### Do you want to modify cache partition?

既存のキャッシュ区画の構成を変更できます。

有効値: Yes または No

デフォルト値: No

### Default client TCP connection timeout

クライアント接続の有効期限が切れるまでの時間を指定します。

有効値: 5 ~ 240 秒

デフォルト値: 120 秒

### Maximum partition size

このキャッシュ区画に割り振るメモリーの最大量を指定します。この値が現在使用可能なメモリーの量を超える場合は、値は無視され、最大区画サイズは設定されません。

有効値: 1 ~ 4095 メガバイト、または 0 (最大値なし)

デフォルト値: 0 (最大値なし)

### Maximum number of objects

キャッシュ区画に格納できるオブジェクトの最大数を指定します。ユーザーが 0 を入力した場合、キャッシュ区画はその区画に対して使用できるメモリーの量だけによって制限されます。

有効値: 1 ~ 100000 または (制限なし)

デフォルト値: 0 (制限なし)

### Maximum object size

キャッシュに入れるオブジェクトの最大サイズを指定します。この最大サイズを超えるオブジェクトは、キャッシュに入れられません。キャッシュにオブジェクトが入った後に最大オブジェクト・サイズを変更した場合は、すでにキャッシュに入っているオブジェクトが定義された最大値を一時的に超える場合があります。

有効値: 512 ~ 300000 バイト、または 0 (最大サイズなし)

デフォルト値: 0 (最大サイズなし)

### Do you want the cache activated upon reboot?

キャッシュ区画を自動的にアクティブにするか、明示的なユーザー要求によってアクティブにするかを指定します。即時アクティブ化を設定されたキャッシュ区画は、2212 のリブート時に自動的に使用可能になります。即時アクティブ化を設定されないキャッシュ区画は、ユーザーが Web サーバー・キャッシュ・コンソールで talk 5 によって区画をアクティブにするまで、使用不可状態のままになります。

有効値: Yes または No

デフォルト値: Yes

**Default cache purge interval?**

デフォルトのキャッシュ除去間隔を指定します。

有効値: 1 ~ 720 分、または 0 (使用不可)

デフォルト値: 10 分

**Enable transparent caching?**

キャッシュ内で検出されなかったオブジェクト (キャッシュ・ミス) に対するサーバーの応答を、自動的にキャッシュに入れるかどうかを指定します。

有効値: Yes または No

デフォルト値: Yes

**Check cache control headers?**

サーバーが Web サーバー・キャッシュに対して、応答がキャッシュ対象として適格かどうかを指定できるようにします。

有効値: Enabled または Disabled

デフォルト値: Disabled

**Cache images?**

イメージ・ファイル (\*.gif または \*.jpg) をキャッシュに入れるかどうか指定します。

有効値: Yes または No

デフォルト値: Yes

**Default expiration time for images**

有効値: 1 ~ 10080 分、または 0 (なし)

デフォルト値: 60 分

**Cache non-image static objects?**

非イメージ静的データ (\*cgi\* を含まないファイルと、.jpg または .gif が最後に付かないファイル) をキャッシュに入れるかどうかを指定します。

有効値: Yes または No

デフォルト値: Yes

**Default expiration time for non-image static objects**

有効値: 1 ~ 10080 分、または 0 (なし)

デフォルト値: 60 分

**URL mask to identify dynamic objects**

動的オブジェクトを識別するために使用する URL マスクを指定します。

有効値: 任意の URL マスク

デフォルト値: \*/cgi\*

## Web サーバー・キャッシュの構成と監視

### Cache dynamic objects?

動的オブジェクトをキャッシュに入れるかどうかを指定します。動的オブジェクトは、オブジェクトが要求されたときにサーバーによって構成されたオブジェクトで、データが変更されたされないにかかわらず、新しい要求があるたびに再構成されます。

有効値: Yes または No

デフォルト値: No

### Do you want to add a URL mask?

キャッシュに追加する新しい URL マスクを指定します。URL マスクを使用すると、個々のオブジェクト、またはオブジェクトのグループを、URL を基準にして含めたり除外したりすることができます。

有効値: i または e

デフォルト値: i

URL マスクを指定するときは、ワイルドカード文字を使用できます。ワイルドカードを使えるのは、Web サーバー・キャッシュ用にネットワーク・ディスパッチャーを構成するとき、あるいは f webc プロンプトから **add** または **modify url** コマンドを使用するときです。ワイルドカードとして使用できる文字は、\* (アスタリスク) または # (番号記号) です。ワイルドカードは URL の一部としてどの位置にでも使用できます。

\* は、URL の一部として、文字なし、またはすべての文字を表します。

例: \*abc.html は、次のような URL マスクをフィルターに掛けます。

```
abc.html
finabc.html
defchtjqsprabc.html
```

# は、1 文字を表します。

例: ab#.html は、次のような URL マスクをフィルターに掛けます。

```
abc.html
abf.html
abo.html
```

次の例は、ポート・モード 3 (cache=3) が選択され、新規のキャッシュ区画が追加されない場合に適用されます。

```
NDR Config>add port
Cluster Address [0.0.0.0] ? 113.3.1.11
Port number [80] ?
Max. weight (0-100) [20] ?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 cache=3 extcache=4) [0] ? 3
Do you want a new cache partition? [Yes] : n
Enter cache partition [0] ? 0
Maximum TCP segment size (Range 512-32768 bytes) [4096] ?
Default server TCP connection timeout (Range 5-240 seconds) [120] ?
Default client TCP connection timeout (Range 5-240 seconds) [120] ?
Do you want to modify cache partition [0]? No :
Requested port has been added to cluster 113.3.1.11
Maxweight has been set to 20 for port 80 in cluster 113.3.1.11
```

注: 次の例は、ポート・モード 3 (cache=3) が選択され、新規のキャッシュ区画が追加された場合に適用されます。

```

NDR Config>add port
Cluster Address [0.0.0.0]? 113.3.1.10
Port number [80]?
Port type(tcp=1, udp=2, both=3) [3]?
Max. weight (0-100) [20]?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 cache=3 extcache=4) [0]? 3
Do you want a new cache partition? [Yes]: y
Default server TCP connection timeout (Range 5-240 seconds) [120]?
Default client TCP connection timeout (Range 5-240 seconds) [120]?
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]?
Maximum number of objects (1-100000 or 0 for no limit) [0]?
Maximum object size (512-300000 bytes or 0 for no limit) [0]?
Do you want the cache activated upon reboot? [Yes]:
Default cache purge interval (1-720 minutes or 0 to disable) [10]?
Enable transparent caching? [Yes]:
Check cache control headers? [Yes]:
Cache images? [Yes]:
    Default expiration time for images
        (1-10080 minutes or 0 for no expiration) [60]?
Cache non-image static objects? [Yes]:
    Default expiration time for non-image static objects
        (1-10080 minutes or 0 for no expiration) [60]?
URL mask to identify dynamic objects [*/cgi*]?
Cache dynamic objects? [No]:
Do you want to add a URL mask? [No]:

Cache partition number 0 has been successfully created.
Requested port has been added to cluster 113.3.1.10
Maxweight has been set to 20 for port 80 in cluster 113.3.1.10
Port Type has been set to Both for port 85 in cluster 113.3.1.10
NDR Config>

```

Web サーバー・キャッシュ機能に対して初期のクラスターとポートを構成するには、ネットワーク・ディスパッチャーを使用する必要があります。ポート・モードをキャッシュ・ポートとして構成して、クラスターとポートを追加したら、WEBC Config> プロンプトで Web サーバー・キャッシュの構成パラメーターを変更および表示できます。

ネットワーク・ディスパッチャーについては、122 ページを参照してください。

---

## Web サーバー・キャッシュ環境へのアクセス

Web サーバー・キャッシュ構成環境にアクセスするには、Config> プロンプトで次のコマンドを入力します。

```

Config> feature webc
WEBC Config>

```

---

## Web サーバー・キャッシュのコマンド

ここでは、Web サーバー・キャッシュの構成コマンドについて説明します。表18は、Web サーバー・キャッシュの構成コマンドの一覧です。これらのコマンドは、Web サーバー・キャッシュ機能のパラメーターを指定します。これらの変更内容をアクティブにするには、ルーターをリスタートします。

表 18. Web サーバー・キャッシュの構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxページの『ヘルプの入手』を参照してください。
Activate	最新の構成を使用して、キャッシュ区画をアクティブにします。

## Web サーバー・キャッシュの構成と監視

表 18. Web サーバー・キャッシュの構成コマンドの要約 (続き)

コマンド	機能
Add	URL マスクを追加します。
Delete	URL または区画を削除します。
List	キャッシュ情報を表示します。
Modify	キャッシュ情報を変更します。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

## Activate

**activate** コマンドは、最新の構成を使用してキャッシュ区画すべてを初期設定するために使用します。

構文:

**activate**

例:

```
WEBC Config>act ?
ACTIVATE all initializes cache partitions, using
the latest configuration.
If you want to keep the active configuration, use the
ENABLE PARTITION command.
```

## Add

**add** コマンドは、URL マスクを追加するために使用します。

構文:

**add** urlmask

例:

```
WEBC Config>add ur1
Partition number [0]?
New URL mask []? *newmask*
Include or Exclude from cache (i or e) [i]? i
Set default expiration time? [No]:y
Default expiration time
(1-10080 minutes or 0for no expiration) [0]? 20
The URL mask has been added to cache partition 0.
```

注: プロキシと区画を追加するには、ネットワーク・ディスパッチャーを使用して **add port** コマンドまたは **set port** コマンドを実行する必要があります。

**partition number**

追加する区画の区画番号。

有効値: 任意の有効な区画番号

デフォルト値: 0

**new URL mask**

追加する URL マスクの名前。

有効値: 任意の有効な URL マスク

デフォルト値: なし

**include or exclude from cache**

URL をキャッシュに含めるか、除外するかを指定します。

有効値: i または e

デフォルト値: i

**default expiration time**

デフォルト有効期限を分単位で指定します。ゼロは、有効期限なしを指定します。

有効値: 0 ~ 10080 分

デフォルト値: 0 (有効期限なし)

## Delete

**delete** コマンドは、URL マスクまたは区画を削除するために使用します。

構文:

```
delete                partition
                        urlmask
```

**partition**

キャッシュから削除する区画の番号。

**urlmask**

キャッシュから削除する URL マスクの名前。

例:

```
WEBC Config>delete url
Partition number [0]? 0
URL masks defined : 5
  1: EXCLUDE '*index*'
  2: EXCLUDE '*comp*'
  3: INCLUDE '*tmp*'
    Default expiration time: 1 minutes
  4: INCLUDE '*stat*'
    Default expiration time: 5 minutes
  5: INCLUDE '*html*'
    Default expiration time: 1000 minutes (16 hrs 40 mins)
URL mask number [1]? 5
The URL mask for cache partition number 0 has been deleted.
```

**注:** プロキシを削除するには、ネットワーク・ディスプレイパッチャー機能を使用し、関連したポートまたはクラスター (あるいはその両方) を削除するか、ポートのポート・モードをキャッシュ以外に変更する必要があります。

**partition number**

削除する区画の区画番号。

有効値: 任意の有効な区画

デフォルト値: 0

**URL mask number**

削除する URL マスクの番号。

有効値: 任意の有効な URL マスク番号。

デフォルト値: 1

## Web サーバー・キャッシュの構成と監視

### List

**list** コマンドは、Web サーバー・キャッシュの情報を表示するために使用します。

構文:

```
list                all
                    external
                    partition
                    proxy
                    urlmask
```

**all** キャッシュに定義されているポート、区画、プロキシ、およびマスクをすべて表示します。

**external**

外部キャッシュ制御マネージャーに関する情報を表示します。

**partition**

キャッシュの区画番号を表示します。

**proxy** キャッシュに定義されているプロキシを表示します。

**urlmask**

キャッシュに定義されている URL マスクを表示します。

例: list all

```
WEBC Config>list all
Cache Partition 0
  Cluster address 113.3.1.10, Port 80

1 cache partition(s) defined.
```

例: list external

```
WEBC Config>list ext
External Cache manager : Enabled
Port number            : 82
TCP timeout            : 120 seconds
```

例: list partition

```
WEBC Config>list part
Cache Partition 0
Maximum partition size      : 1 MB
Maximum number of objects  : Unlimited
Maximum object size:       : Unlimited
Activate on reboot         : Enabled
Cache purge interval       : 10 minutes
Dynamic URL mask           : '*/cgi*' "
Transparent caching: Enabled
Check cache control headers : Disabled
Cache images                : Disabled
Cache non-image static objects: Enabled
  Default expiration time: 60 minutes (1 hrs 0 mins)
Cache dynamic objects: Disabled
Associated proxies (cluster port): (113.3.1.10 80)

1 cache partition(s) defined.
```

例: list url

```
WEBC Config>list url
Partition number [0]?
URL masks defined : 5
  1: EXCLUDE '*index*'
  2: EXCLUDE '*comp*'
  3: INCLUDE  '*tmp*' "
```



```

Default expiration time: 1 minutes
4: INCLUDE '*stat*'
Default expiration time: 2 minutes
5: INCLUDE '*html*'
Default expiration time: 1000 minutes (16 hrs 40 mins)

```

## Modify

**modify** コマンドは、Web サーバー・キャッシュの情報を変更するために使用します。

構文:

```

modify          external
                  partition
                  proxy
                  urlmask

```

### external

外部キャッシュ制御マネージャーを変更できます。

### partition

区画を変更できます。

**proxy** プロキシを変更できます。

### urlmask

URL マスクを変更できます。

例: modify external

```

WEBC Config>mod ext
External cache manager port number(0 to disable) [82]?
TCP connection timeout (Range 5-240) seconds [120]? 20
Do you want to modify the encryption key:? [No]? Y
Encryption key should be 16 characters long.
Encryption key (16 characters) in Hex (0-9, a-f, A-F):
Encryption Key again (16 characters) in Hex (0-9, a-f, A-F):
The external cache manager has been modified.

```

### external cache manager port number

変更する外部キャッシュ制御マネージャーのポート番号を指定します。

有効値: 0 ~ 255

デフォルト値: 82

### TCP connection timeout

変更する外部キャッシュ制御マネージャーの TCP 接続を指定します。

有効値: 5 ~ 240 秒

デフォルト値: 120

### do you want to modify the encryption key

暗号化キーを変更するかどうかを指定します。

有効値: yes または no

デフォルト値: no

### encryption key

変更する外部キャッシュ制御マネージャーの暗号化キー。暗号化キーは、16 文字の長さで、16 進法で表現されている必要があります。

## Web サーバー・キャッシュの構成と監視

有効値: 16 進数 (0 ~ 9, a ~ f, A ~ F)

デフォルト値: なし

例: modify partition

```
WEBC Config>modify partition
Partition number [0] ?
Maximum partition size (1-255 megabytes or 0 for no limit) [0]? 200
Maximum number of objects (1-100000 or 0 for no limit)[0]? 5000
Maximum object size (512-300000 bytes or 0 for no limit)[0]? 250000
Do you want the cache activated upon reboot? [Yes]:
Default cache purge interval (1-720 minutes or 0 to disable) [10]? 20
Enable transparent caching? [Yes]:
Check cache control headers? [Yes]:
Cache images? [Yes]:
  Default expiration time for images
    (1-10080 minutes or 0 for no expiration) [60]?
Cache non-image static objects? [Yes]:
  Default expiration time for non-image static objects
    (1-10080 minutes or 0 for no expiration) [60]?
URL mask to identify dynamic objects [*/cgi*]? *dyn*
Cache dynamic objects? [No]: y
Cache partition number 0 has been modified.
```

### partition number

変更する区画の番号。

有効値: 任意の有効な区画番号

デフォルト値: 0

### maximum partition size

変更する区画の最大区画サイズ。ゼロは、制限なしを指定します。

有効値: 1 ~ 255 メガバイト、または 0 (制限なし)

デフォルト値: 0

### maximum number of objects

区画内で変更されるオブジェクトの最大数。ゼロは、制限なしを指定します。

有効値: 0 ~ 100000、または 0 (制限なし)

デフォルト値: 0

### maximum object size

区画内で変更されるオブジェクトの最大サイズ。ゼロは、制限なしを指定します。

有効値: 512 ~ 300000、または 0 (制限なし)

デフォルト値: 0

### do you want the cache activated upon reboot

リブート後にキャッシュをアクティブにするかどうかを指定します。

有効値: yes または no

デフォルト値: yes

### default cache purge interval

デフォルトのキャッシュ除去間隔を指定します。ゼロは、デフォルトのキャッシュ除去間隔を使用不可にします。

有効値: 1 ~ 170 分、または 0 (使用不可にする)

デフォルト値: 10

**enable transparent caching**

透過キャッシュを使用可能にするかどうかを指定します。

有効値: yes または no

デフォルト値: yes

**check cache control headers**

キャッシュ制御ヘッダーを検査するかどうかを指定します。

有効値: yes または no

デフォルト値: yes

**cache images**

イメージをキャッシュに入れるかどうかを指定します。

有効値: yes または no

デフォルト値: yes

**Default expiration time for images**

イメージのデフォルト有効期限を指定します。ゼロは有効期限なしを示します。

有効値: 1 ~ 10080、または 0 (有効期限なし)

デフォルト値: 60

**cache non-image static objects**

非イメージ静的オブジェクトをキャッシュに入れるかどうかを指定します。

デフォルト値: yes

有効値: yes または no

**Default expiration time for non-image static objects**

非イメージ静的オブジェクトのデフォルト有効期限を指定します。ゼロは有効期限なしを示します。

有効値: 1 ~ 10080、または 0 (有効期限なし)

デフォルト値: 60

**url mask to identify dynamic objects**

動的オブジェクトを識別するために使用する URL マスクを指定します。

有効値: 任意の有効な url マスク

デフォルト値: \*/cgi\*

**cache dynamic objects**

動的オブジェクトをキャッシュに入れるかどうかを指定します。

有効値: yes または no

デフォルト値: no

例: modify url

```
WEBC Config>modify url
Partition number [0]?
URL masks defined : 5
1: EXCLUDE '*index*
```

## Web サーバー・キャッシュの構成と監視

```
2: EXCLUDE '*comp*'
3: INCLUDE '*tmp*'
   Default expiration time: 1 minutes
4: INCLUDE '*stat*'
   Default expiration time: 2 minutes
5: INCLUDE '*html*'
   Default expiration time: 1000 minutes (16 hrs 40 mins)
URL mask number [1] ? 4
New URL mask *stat*?
Include or Exclude from cache (i or e) [i]?
Set default expiration time? Yes :
Default expiration time
(1-10080 minutes or 0 for no expiration) [2]? 5
URL mask number 4 has been modified.
```

### partition number

変更する URL の区画番号を指定します。

有効値: 任意の有効な区画番号

デフォルト値: 0

### url mask number

変更する URL マスクの URL マスク番号を指定します。

有効値: 任意の有効な URL マスク番号

デフォルト値: 1

### new url mask \*stat\*

有効値: yes

デフォルト値: yes または no

### include or exclude from cache

変更した URL をキャッシュに含めるか、除外するかを指定します。

有効値: i または e

デフォルト値: i

### set default expiration time

デフォルト有効期限を設定するかどうかを指定します。

有効値: yes または no

デフォルト値: yes

### default expiration time

デフォルト有効期限を分単位で指定します。ゼロは、有効期限なしを指定します。

有効値: 1 ~ 10080 分、または 0 (有効期限なし)

デフォルト値: 0

---

## Web サーバー・キャッシュ監視環境へのアクセス

Web サーバー・キャッシュ監視環境にアクセスするには、t 5 構成プロンプトで **f webc** と入力します。

```
t 5>f webc
```

## Web サーバー・キャッシュ監視コマンド

表19は、Web サーバー・キャッシュ監視コマンドの一覧です。

表 19. Web サーバー・キャッシュ監視コマンドの一覧

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxixページの『ヘルプの入手』を参照してください。
Activate	最新の構成を使用して、キャッシュ区画をアクティブにします。
Clear	区画または統計を消去します。
Enable	区画を使用可能にします。
Delete	区画、プロキシー、または URL マスクを削除します。
Disable	区画を使用不可にします。
List	キャッシュ情報を表示します。
Modify	キャッシュ情報を変更します。
Exit	直前のコマンド・レベルに戻ります。 xxxixページの『下位レベル操作環境の終了』を参照してください。

## Activate

**activate** コマンドは、すべての Web サーバー・キャッシュ、または特定の区画やプロキシーをアクティブにするために使用します。

構文:

```
activate          all
                   external
                   partition
                   proxy
```

**all** 定義されたキャッシュをすべてアクティブにします。

**external** 外部キャッシュ制御マネージャーをアクティブにします。

**partition** キャッシュ内の区画をアクティブにします。

**proxy** キャッシュ内のプロキシーをアクティブにします。

例: activate all

```
WEBC>act all
Cache partition 0 must be disabled to reactivate it.
Do you wish to continue? [No]: y
WEBC>
```

例: activate Proxy

```
WEBC>act pr

1) Cluster address 113.3.1.10, Port 80, Cache partition 0
2) Cluster address 113.3.1.10, Port 81, Cache partition 0
Enter proxy number: 1 ? 1
You are trying to activate an existing proxy.
Doing this will cause the proxy to be terminated before
being reactivated.
Do you wish to continue? [No]: yes
```

## Clear

**clear** コマンドは、区画または統計を消去するために使用します。

注: 区画からオブジェクトを消去しても、その区画の統計は消去されません。

構文:

```
clear                partition  
                        statistics
```

**partition**

区画からオブジェクトをすべて消去します。

**statistics**

区画に存在する統計を消去します。

例:

```
WEBC>clear partition  
Enter partition number: [0]?  
Cache partition 0 must be disabled to clear its contents.  
Do you wish to continue? [No]: yes  
Do you wish to enable this partition? [Yes]: yes
```

**partition number**

消去する区画番号を指定します。

有効値: 任意の有効な区画番号

デフォルト値: 0

## Enable

**enable** コマンドは、区画を使用可能にするために使用します。

構文:

```
enable                partition
```

例:

```
WEBC>enable partition  
Enter partition number: [0]?
```

**partition number**

使用可能にする区画の区画番号。

有効値: 任意の有効な区画番号

デフォルト値: 0

## Delete

**delete** コマンドは、区画を削除するために使用します。

構文:

```
delete                partition
```

**partition**

キャッシュから区画を削除します。

例:

```
WEBC>delete partition
Enter partition number: [0]? 0
WARNING: This will delete partition 0 and free all memory!
Do you wish to continue? [No] : yes
WEBC>
```

#### partition number

削除する区画番号を指定します。

有効値: 任意の有効な区画番号

デフォルト値: 0

## Disable

**disable** コマンドは、区画を使用不可にするために使用します。

構文:

```
disable partition
```

#### partition

区画を使用不可にします。

例:

```
WEBC>disable partition
Enter partition number: [0]?
```

#### partition number

使用不可にする区画の区画番号を指定します。

有効値: 任意の有効な区画番号

デフォルト値: 0

## List

**list** コマンドは、Web サーバー・キャッシュ全体、区画、ポリシー、またはプロキシの情報を表示するために使用します。

構文:

```
list all
delete
depend
external
item
partition
policy
proxy
```

**all** キャッシュにある区画、ポリシー、およびプロキシをすべて表示します。

**delete** キャッシュ区画から最近削除された 100 項目を表示します。

#### depend

区画の依存関係テーブルを表示します。

## Web サーバー・キャッシュの構成と監視

### external

外部キャッシュ制御マネージャーに関する情報を表示します。

**item** キャッシュ区画にある現在の項目とヒット・カウントを表示します。

### partition

キャッシュの区画情報を表示します。

**policy** キャッシュのポリシー情報を表示します。

**proxy** キャッシュのプロキシ情報を表示します。

例:

```
WEBC>list all
Cache Partition 0          Status: Enabled
          Cluster address: 113.3.1.10 Port 80
1 partition(s) active.
External Cache Manager Port: 82
          Connection Timeout: 120 seconds
```

例:

```
WEBC>list delete
Enter partition number: [0]? 0
Delete Table
URL String -- hit count
=====
'/abc.html' -- 4
'/soccer.html' -- 2
'/tennis.html' -- 1
'/curling.html' -- 3
```

例:

```
WEBC>list depend
Enter partition number: [0]?
Dependency table for Partition 0
-----
dep: tennis_info
count of URLs: 2
URLs:
    tennis_schedule.html
    tennis_roster.html
dep: soccer_info
count of URLs: 2
URLs:
    soccer_schedule.html
    soccer_roster.html
dep: roster
count of URLs: 2
URLs:
    soccer_roster.html
    tennis_roster.html
dep: schedule
count of URLs: 2
URLs:
    soccer_schedule.html
    tennis_schedule.html
```

例:

```
WEBC>list item
Enter partition number: [0]? 0
Current number of items: 5
URL String -- hit count
=====
'/' -- 2
'/file5k.html' -- 1
'/file4k.html' -- 1
'/file2k.html' -- 3
'/file1k.html' -- 1
```

例:



```

WEBC>li part 0
Cache Partition 0          Status: Enabled
      Cluster address: 113.3.1.10, Port 80
      Cluster address: 113.3.1.10, Port 81
Partition size: Current - 0 bytes Highest - 0 bytes Maximum - Unlimited
Number of objects: Current - 0 Highest - 0 Maximum - Unlimited
Maximum object size: Unlimited
Cache purge interval: 10 minute(s)
Hit ratio: 0%
Total number of hits: 0
Total number of misses: 0
Object Excluded (Object too large):      0
                (Object expired):       0
                (DONT CACHE header):    0
                (URL excluded):         0
                (Image excluded):       0
                (Static object excluded): 0
                (Dynamic object excluded): 0
                (Cache disabled):       0
Objects explicitly Included: 0
Total number of purged objects :0
Purged objects (Cache full): 0
                (Object stale): 0
                (Purged by user): 0
                (Invalidation): 0

```

例:

```

WEBC>li pol
Enter partition number: [0]?
Transparent caching: Enabled
Cache Control Headers: Enabled
Cache images: Enabled
      Default lifetime: 0 minute(s)
Cache non-image static objects: Enabled
      Default lifetime: 0 minute(s)
Cache dynamic objects: Disabled
Dynamic URL mask: *dyn*
URL masks defined:
  1: EXCLUDE *index*
  2: EXCLUDE *comp*
  3: INCLUDE *tmp*
      Default expiration time: 1 minutes
  4: INCLUDE *stat*
      Default expiration time: 2 minutes
  5: INCLUDE *html*
      Default expiration time: 1000 minutes (16 hrs 40 mins)

```

例: キャッシュ配列の一部であるプロキシ。

```

WEBC>li pr
WEBC>li pr
  1) Cluster address 113.3.3.10, Port 80, Cache Partition 0
  2) Cluster address 113.3.3.20, Port 80, Cache Partition 0
Enter proxy number: [1]? 1
Proxy 1: assigned to cache partition 0
Cluster address: 113.3.3.10 Port number: 80
Server Connection Timeout: 120 seconds
Client Connection Timeout: 120 seconds
Client connections: 0 current / 2 at highest point
Server connections: 0 current / 2 at highest point
Total cache hits: 0
Total cache misses: 649
Cache misses (object not in cache): 649
                (unsupported method): 0
                (can't send response): 0
                (non-cached request): 0
This Proxy is part of a cache group
Source IP address for group is: 113.3.3.1
There are currently 2 Cache(s) in this group
Below are the Caches in the group:
113.3.1.1
113.3.6.1

```

例: キャッシュ配列の一部でないプロキシ。

## Web サーバー・キャッシュの構成と監視

```
WEBC>1i pr
  1) Cluster address 113.3.1.10, Port 80, Cache Partition 0
  2) Cluster address 113.3.1.10, Port 81, Cache Partition 0
Enter proxy number: [1]?
Proxy 1: assigned to cache partition 0
Cluster address: 113.3.1.10 Port number: 80
Server Connection Timeout: 240 seconds
Client Connection Timeout: 240 seconds
Client connections: 0 current / 0 at highest point
Server connections: 0 current / 0 at highest point
Total cache hits: 0
Total cache misses: 0
Cache misses (object not in cache): 0
                (unsupported method): 0
                (can't send response): 0
                (non-cached request): 0
                (invalidation): 0
```

## Modify

**modify** コマンドは、外部キャッシュ制御マネージャーを変更するために使用します。

構文:

**modify** external

例: modify external

```
WEBC Config>mod ext
External cache manager port number(0 to disable) [82]?
TCP connection timeout (Range 5-240) seconds) [120]? 20
Do you want to modify the encryption key:? [No]? Y
Encryption key should be 16 characters long.
Encryption key (16 characters) in Hex (0-9, a-f, A-F):
Encryption Key again (16 characters) in Hex (0-9, a-f, A-F):
```

**external cache manager port number**

**TCP connection timeout**

**do you want to modify the encryption key**

**encryption key**

---

## 第13章 コード化サブシステムの構成と監視

データ圧縮機能と暗号化機能は、コード化サブシステム (ES) 内で一緒にまとめられています。ES は、インターフェースまたはプロトコル用のコード化装置へのアクセスを可能にし、圧縮または暗号化用のリンクがアクティブになると自動的にアクティブになります。2212 プラットフォームでは、コード化装置は圧縮/暗号化アダプター (CEA) とソフトウェア装置です。ソフトウェア装置は、圧縮と暗号化を実行する操作ソフトウェアで構成されます。ソフトウェア装置が使用される場合、圧縮アルゴリズムと暗号化アルゴリズムはルーターのプロセッサで実行されます。CEA またはソフトウェア装置を使用するために、デフォルト構成を変更する必要はありません。

監視 (talk 5) プロンプトで **feature es** と入力すれば、ES 活動を監視できます。

ES 構成パラメーターによって、ES ソフトウェア装置が使用するメモリーの量を制限できます。デフォルト構成では、ES が必要なだけのメモリーを取得できるようになっています。メモリーの使用量を制限するには、構成プロセス (Talk 6) の **feature es** で **set** コマンドを使用します。

この章には、次の内容が記載されています。

- 『コード化サブシステムの構成』
- 223ページの『コード化サブシステムの監視』

---

### コード化サブシステムの構成

ES 構成パラメーターを使用して、ソフトウェア・コード化装置を同時に使用する圧縮セッションと暗号化セッションの数を制御できます。ソフトウェア・コード化装置は、実際にはルーターのプロセッサで実行される圧縮ライブラリーと暗号化ライブラリーの集まりです。セッションは、圧縮または暗号化を使用するように構成されたインターフェースを経由した全二重接続です。

注: ES 構成パラメーターは、CEA ではなくソフトウェア・コード化装置にだけ影響します。

一般に、データのコード化はプロセッサに負担をかける操作です。ソフトウェア・コード化セッションの数を制限することによって、ルーターのパフォーマンスに対するデータ・コード化の影響を、ある程度までに抑えることができます。たとえば、ルーターが圧縮用に構成されたダイヤルイン・インターフェースを 20 個備えていて、10 個を超えるインターフェースを同時に圧縮するとルーターのパフォーマンスに悪影響が及ぶと判断された場合、圧縮セッションの最大数は 10 に設定する必要があります。この設定によって、20 個のインターフェースのうち任意の 10 個が圧縮を使用できます。

ソフトウェア・コード化装置のメモリー所要量も、セッション数を制限する理由になることがあります。それぞれのソフトウェア圧縮セッションは、ルーターのメモリーの約 30 KB を使用し、圧縮セッションは約 2 KB を使用します。ES が過大な

## ES の構成

メモリーを使用すると、他の機能にメモリーの制約が生じて、ルーターのパフォーマンスに悪影響が及ぶ可能性があります。詳しくは、232ページの『考慮事項』を参照してください。

セッション数を記述するか、値 *unlimited*、*default*、または数値のどちらかを指定することによって、ES セッションの最小数または最大数を設定できます。値 *unlimited* と *default* の意味は同じです。これらの値を指定すると、メモリーがなくなるまで、ルーターは暗号化または圧縮のためにアクティブ化されたセッションをすべてサポートします。

**注:** ES 構成パラメーター (talk 6) を動的に再構成することはできません。変更した後のパラメーター値をアクティブにするには、ルーターをリスタートまたは再ロードする必要があります。

構成プロセス (talk 6) で ES 構成コマンドにアクセスするには、Config> プロンプトで **feature es** と入力します。ES Config> プロンプトが表示されます。表20 は、コマンドの一覧です。

表20. ES 構成コマンド

コマンド	アクション
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxiiページの『ヘルプの入手』を参照してください。
List	圧縮セッションと暗号化セッションの現行の設定値を表示します。
Set	すべてのインターフェースで使用可能な圧縮セッションの最大数を設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxiiページの『下位レベル操作環境の終了』を参照してください。

## List

**list** コマンドは、圧縮セッションと暗号化セッションの現行の設定値を表示するために使用します。

**構文:**

**list**

**例:**

```
ES Config> list
Data Compression and Encryption System Configuration
-----
Parameters used for host-based encoding:
Compression sessions:
  Reserved at initial bootup:          0
  Maximum allowed:                    unlimited
Encryption sessions:
  Reserved at initial bootup:          0
  Maximum allowed:                    unlimited
```

## Set

**set** コマンドは、データの暗号化セッションまたは圧縮セッションの最大数を設定するために使用します。

構文:

```

set sw minimum compression-sessions n, unlimited, or default
    sw maximum compression-sessions n, unlimited, or default
    sw minimum encryption-systems n, unlimited, or default
    sw maximum encryption-systems n, unlimited, or default

```

注: sw という文字は、ソフトウェア (software) の省略語です。

**software minimum compression-sessions** *n, unlimited, or default*

インターフェースで使用可能な圧縮セッションの最小数を設定します。ルーターは、この数のセッションを常に使用できるように予約します。

デフォルト値: 0

有効値: 0 ~ *unlimited*、または *default*

**software maximum compression-sessions** *n, unlimited, or default*

インターフェースで使用可能な圧縮セッションの最大数を設定します。この数のセッションがアクティブになったら、新規セッションをアクティブにすることはできません。

デフォルト値: 0

有効値: 0 ~ *unlimited*、または *default*

**software minimum encryption-sessions** *n, unlimited, or default*

インターフェースで使用可能な暗号化セッションの最小数を設定します。ルーターは、この数のセッションを常に使用できるように予約します。

デフォルト値: 0

有効値: 0 ~ *unlimited*、または *default*

**software maximum encryption-sessions** *n, unlimited, or default*

インターフェースで使用可能な暗号化セッションの最大数を設定します。この数のセッションがアクティブになったら、新規セッションをアクティブにすることはできません。

デフォルト値: 0

有効値: 0 ~ *unlimited*、または *default*

---

## コード化サブシステムの監視

監視プロセスで ES 監視コマンドにアクセスするには、+ プロンプトで **feature es** と入力します。ES Monitor> プロンプトが表示されます。表21 は、利用可能なコマンドを示しています。

表 21. ES 監視コマンド

コマンド	アクション
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxiページの『ヘルプの入手』を参照してください。

表 21. ES 監視コマンド (続き)

コマンド	アクション
List	ES ポート、回線、装置、構成、状況、または概要を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

## List

**list** コマンドは、ES に関する情報を表示するために使用します。ポート、装置、および状況を含む **list** コマンドの出力例は、**list summary** コマンドを参照してください。

構文:

```
list
    ports
    circuits
    devices
    config
    status
    summary
```

**ports list ports** コマンドは、コード化システムの潜在的なクライアントによって作成されたコード化ポートを表示します。ポートは、コード化システムと、ES を使用するように構成されたクライアントとの間にリンクを確立します。たとえば、PPP インターフェース NET 1 を経由する圧縮または暗号化が構成された場合、ポートはそのインターフェースに関連付けられます。QLen フィールドは、ポートに関連したすべての回線に対する未解決の圧縮または暗号化の要求すべての合計を表示します。特定のインターフェースを經由して構成された PPP などのクライアントは、コード化する特定のデータ・バッファを指定するときに ES に要求を出します。

状況フィールドは、ポートで何も待ち行列に入っていない場合は *Idle* を表示し、要求が処理されているかポートで待ち行列に入っている場合は *Busy* または *Waiting* を表示します。

**circuits**

**list circuits** コマンドは、コード化システムのクライアントによって定義された回線を表示します。それぞれの回線は、全二重接続に対応します。一方のエンドポイントで暗号化または圧縮されたデータは、他方で暗号化解除または解凍されます。

デフォルトでは、アクティブな回線だけが表示されます。アクティブな回線と非アクティブな回線の両方とも表示する場合は、コマンド **list circuits all** を使用します。

検出されたそれぞれの回線ごとに、ポートとユーザーが **list ports** コマンドの場合と同様に表示されます。さらに 2 行の情報が表示され、Tx 行はアウトバウンド回線を、Rx 行はインバウンド回線を示します。回線 ID は、クライアントが作成したそれぞれの回線を識別できるように指定した任意の番号です。フレーム・リレー回線の場合、この番号は関連したフレーム・リレー

ー・データ・リンク回線 (DLCI) の ID に対応します。ポイントツーポイント・リンクは、回線を 1 つだけ作成し、その回線は常に番号 1 によって識別されます。

さらに、次の項目が表示されます。

**Dev** これは、そのストリームを提供するコード化装置を表す数値です。数値は、コード化がソフトウェアによって CPU をアクティブにして実行される場合は 1、コード化が圧縮/暗号化アダプターによって実行される場合は 2 です。

**Cmpr** このフィールドは、そのストリームに対してアクティブになっている圧縮アルゴリズムまたは解凍アルゴリズムを表示します。このフィールドが *LZC* の場合は *STAC-LZC* 圧縮が使用されており、*MPPC* の場合は Microsoft® *PPC* が使用されています。ストリームがステートレス・モードで動作している場合は、アルゴリズムの名前にアスタリスク (\*) が追加されます。ステートレス・モードは、データ・パケットの処理後にそのパケットの履歴が維持されないモードです。これに対して連続モードでは、次のパケットを処理するために、前のパケットの処理から履歴が維持されます。たとえば連続圧縮では、エンコーダーは現行のパケットを効率的に圧縮するために、以前のパケットから収集した情報のキャッシュを維持します。

**Encr** このフィールドは、使用されている暗号化または暗号化解除のアルゴリズムを表示します。このフィールドは、標準 *DES* の場合は *DES*、三重 *DES* の場合は *3DES*、*RSA* の *RC4* アルゴリズムが使用されている場合は *RC4* です。ストリームがステートレス・モードで作動している場合は、名前にアスタリスク (\*) が追加されます。これは *RC4* の場合に重要ですが、*DES/3DES* の場合はあまり意味がありません。表示される名前は、使用されている基本暗号化アルゴリズムに対応し、クライアントが使用しているカプセル化形式には対応しないので注意してください。たとえば *PPP* は、*DES* を使用して暗号化を行う *DESE* (RFC 1969) と、*RC4* を使用する *MPPE* (非 Microsoft 標準) の 2 つのカプセル化方式をサポートします。

**QLen** このパラメーターは、ストリームの待ち行列の中でコード化またはデコードを待機している未解決のパケット数を示します。この数は、実際に *ES* に対して処理依頼されたパケットだけを反映していることに注意してください。クライアントによっては、独自の待ち行列を持っていて、これらの私用待ち行列から一度に数パケットだけをコード化システムに送る場合があります。

### Status

ストリームの状況の簡易表示。すべてのストリームが待機状況にあって、使用中のものがないように見えることは、異常ではありません。使用中状況を調べるには、処理サイクルの中で適度に狭い時間範囲にわたって待ち行列の活動を把握する必要があります。あり得る状態は次のとおりです。

**Idle** このストリームのパケットは待ち行列に入っていません。



**Busy** システムは、このストリームのパケットを現在処理していません (つまり、待ち行列の先頭にある項目が、その時点でコード化エンジンを通過している)。

### Waiting

要求は保留されていますが、そのストリームに現在処理中のパケットはありません。

## devices

**list devices** コマンドは、システムが使用できるコード化装置を表示します。通常、コード化装置は圧縮/暗号化アダプターを指します。ハードウェア・アクセラレーターが使用できない場合に使用されるソフトウェアは、バーチャル装置として設定され、このリストには *Host Software* 装置として表示されます。このコマンドには、**list devices** と **list device n** の 2 つの形式があります。最初の形式は、システムによって認識された装置をすべて表示する短い要約を作成します。2 番目の形式は、特定の装置 n (ただし、n は装置番号) の詳細リストを作成します。装置 1 はホスト・ソフトウェア、つまりバーチャル・コード化装置を表し、装置 2 は圧縮/暗号化アダプターを表します。番号 n の代わりにアスタリスク (\*) を使用でき、この場合は両方の装置のリストが作成されます。

**config list config** コマンドは、現行の構成パラメーターを表示します。これらは、ルーターをリスタートまたは再ロードした時点で不揮発メモリから読み取られたパラメーターです。表示される情報は、構成 (Talk 6) の **list config** コマンドによって表示されるものと同じです。

**status list status** コマンドは、グローバル状況フラグと各種のシステム統計からなる、コード化システムの状況を表示します。次に、**list status** コマンドによって表示されるフィールドを説明します。

### Last Error

コード化システムの任意のクライアントから最後に戻されたエラー・コード。これはデバッグのためのもので、サービス技術員が使用します。

### Internal Condition flags

このフィールドは、次の定義に従って内部状況を表示します。

**Ready** システムは起動しており、作動可能です。これは通常の状態です。

### Not Working

コード化システムは、何らかの内部エラーが原因で作動不能になっています。

### No Devices Available

コード化を実行する装置が使用できないことを示します。ハードウェア・ベースのエンコーダーが存在しなければ、内部ソフトウェアによってコード化が行われるので、この状態が発生することがあってはなりません。

### Out of Memory

システムはメモリーを割り振ろうとしましたが失敗しまし



た。この状態は、ルーターの RAM の容量が不足していて、コード化システムが悪影響を受けていることを示しています。

### Number of Ports

このフィールドは、ES 内に自身のポートを確立したクライアントの数を示します。ポートの定義については、**list ports** コマンドを参照してください。

### Number of Circuits

回線の定義については、**list circuits** コマンドを参照してください。

### Global Request pool size

割り振られたバッファと空きバッファの数。コード化されるそれぞれのパケットごとに、ほぼ 1 つの要求バッファが使用されます。空きバッファの数が割り振られた数より少ない場合は、コード化の処理が行われています。

### Total # of Requests processed

この値は、コード化エンジンによって処理されているバッファの合計数を示します。この数は、ルーターの前のリスタートまたは再ロード以後、システムの全クライアントによって圧縮または暗号化されたパケットの合計数とほぼ一致します。

## summary

このコマンドは、システムの概要を表示します。このコマンドは、**list status**、**list devices**、および **list ports** の各コマンドの出力を組み合わせた合成コマンドです。

### 例:

#### list summary

#### Encoding System Status

```
-----
Last Error:                14 (Stream not active)
Internal Condition flags:  0x00000001  -->
                           Ready
Number of Ports:          2
Global Request pool size:  Alloc: 32  Free: 32
Total # of Requests processed: 7059
```

#### Encoding System Devices

Device Type	Slot/Port	Status
2 Hardware Accelerator/0	2/1	Ready
1 Host Software	0/0	Ready
0 Null Device	0/0	Ready

#### Encoding System Ports

Port	User	+--Encoder State---+		+--Decoder State---+	
		QLen	Status	QLen	Status
1	Net 2 (PPP/0)	0	Idle	0	Idle
2	Net 3 (PPP/1)	0	Idle	0	Idle

## ES の監視

---

## 第14章 データ圧縮の構成と監視

この章では、フレーム・リレーおよび PPP インターフェースを介した 2212 上のデータ圧縮について説明します。この章には、次の内容が記載されています。

- 『データ圧縮の概説』
- 『データ圧縮の概念』
- 234ページの『PPP リンクのデータ圧縮の構成と監視』
- 237ページの『フレーム・リレー・リンクのデータ圧縮の構成と監視』

データ圧縮は、フレーム・リレーおよび PPP インターフェースでサポートされます。

---

### データ圧縮の概説

データ圧縮は、装置上のネットワーク・インターフェースの有効帯域幅を増やす手段を提供します。主として低速の WAN リンクで使用することを目的としています。

装置上のデータ圧縮は、PPP およびフレーム・リレー・インターフェースでサポートされます。

- PPP インターフェースの場合、圧縮はインターネット技術特別調査委員会の RFC 1962 に定義されている圧縮制御プロトコル (CCP) に準拠して実現されています。CCP は、圧縮の使用をネゴシエーションする基礎になる機構と、複数の可能な圧縮プロトコルの中から選択する手段を提供します。

この装置は、2 種類の圧縮プロトコルを提供します。すなわち、RFC 1974 に定義されている Stac-LZS と、RFC 2118 に記述されている Microsoft ポイントツーポイント圧縮プロトコル (MPPC) です。これらは両方とも Stac Electronics によって提供される圧縮アルゴリズムに基づいています。

- フレーム・リレー・インターフェースの場合、圧縮は、フレーム・リレー・フォーラム技術委員会によって作成された FRF.9、*Data Compression over Frame Relay Implementation Agreement* に準拠して実現されています。FRF.9 は、データ圧縮プロトコル (DCP) を記述し (PPP の CCP をモデルにしています)、同様に、各種の圧縮アルゴリズムおよびオプションをネゴシエーションする手段を提供しています。装置は DCP 『モード 1』ネゴシエーションをサポートします。FRF.9 には、より汎用化された『モード 2』も記述されていますが、これはサポートされません。圧縮そのものは、PPP Stac-LZS プロトコルで使用されるのと同じ圧縮エンジンを使用して行われます。

---

### データ圧縮の概念

装置上のデータ圧縮は、リンク上の利用可能な帯域幅をより効率的に使用して、ネットワーク・リンクのスループットを高める手段を提供します。その基本原理は簡単です。つまり、リンクを流れるデータをできるだけコンパクトな形にすることにより、速度が一定のリンク上で転送にかかる時間をできるだけ少なくすることです。

## データ圧縮の構成と監視

データ圧縮は、ネットワーク・モデルのさまざまなレイヤーで実行できます。たとえば、あるアプリケーションがネットワーク上の別の場所にある同位アプリケーションにデータを転送する前に圧縮する、あるいは 2 つのノード間でビット列の受け渡しだけを行っているデータ・リンク・レイヤーで装置が圧縮するといったことが可能です。この圧縮の方法とその効率は、さまざまなファクターによって決まります。このファクターとしては、圧縮を実行するネットワーク・レイヤー、圧縮機能と解凍機能が持っている圧縮されるデータに対する知識、選択された圧縮アルゴリズム、および圧縮される実際のデータなどが含まれます。通常は、最良の圧縮を達成できるのは、アプリケーション・レイヤーです。たとえば、ファイル転送アプリケーションは、圧縮する前にデータ・ファイル全体を入手できるので、ファイルに対して各種の圧縮アルゴリズムを試し、その特定ファイルのデータに最適なアルゴリズムを見つけることができます。しかし、これはその 1 つタイプのアプリケーションの圧縮としては優れた方法かもしれませんが、ネットワーク上を流れる大量のトラフィックの圧縮の一般的問題の解決にはあまり役に立ちません。現在、ほとんどのネットワーク・アプリケーションは、データを生成する時点では圧縮を行っていないからです。

装置での圧縮は、これよりはるかに低いネットワーク・レイヤー、つまりデータ・リンク・レイヤーで行われます。装置内で、リンクを介して転送される個々のパケットが圧縮されます。圧縮はパケットが装置を通過するときにリアルタイムで行われます。送信側は転送する直前にパケットを圧縮し、受信側は受信すると同時にパケットを解凍します。この動作は、高位レイヤーのネットワーク・プロトコルには透過的です。

## データ圧縮の基本

データ圧縮機能は、データ内の『冗長』情報を認識し、できるだけ冗長度の少ない別のデータ・セットを生成します。『冗長』情報とは、現在利用可能なデータに基づいて導き出すことができ、再作成が可能な情報のことを言います。たとえば、圧縮機能はデータ・ストリーム内の反復文字パターンを認識し、これらの反復パターンを、そのパターンを表す短いコード・シーケンスで置き換えます。圧縮機能と解凍機能でこれらのコード・シーケンスに関する認識が一致している限り、必ず解凍機能は圧縮されたデータから元のデータを再作成することができます。

元のデータ内のシーケンスを、圧縮された出力の対応するシーケンスにマッピングしたものを、一般に**データ・ディクショナリー**と呼んでいます。これらのディクショナリーは、静的に定義すること（圧縮機能と解凍機能が利用できる経験に基づく情報）も、動的に生成すること（通常は、圧縮する情報に基づく）もできます。静的ディクショナリーは、処理されるデータが限定された既知の性質を持っており、汎用圧縮機能を使用してもあまり効率的ではない環境に最適です。ほとんどの圧縮システム（装置上の圧縮機能も含む）は、動的ディクショナリーを使用しています。2212 上のデータ・ディクショナリーは、現在処理中のパケットと以前に処理されたパケットについての知識に基づいていますが、他のレイヤーで圧縮が行われるときに存在するデータ・ストリームを『見通す』機能は備えていません。データ・ディクショナリーが動的に生成され、以前に処理されたデータにだけ基づくシステムは、**ヒストリー**とも呼ばれます。この章の残りの部分ではヒストリーとデータ・ディクショナリーという用語を同義の用語として使用しますが、他の環境では、ヒストリーは特定の形のデータ・ディクショナリーを表すことを理解しておく必要があります。

装置は動的ディクショナリーを使用し、圧縮機能と解凍機能はそれぞれのディクショナリーを同期に保つ必要があるということは、データ圧縮は2つのエンドポイント間で受け渡されるデータ・ストリームに作用するものであることを意味しています。つまり、ルーター上の圧縮は接続指向のプロセスであり、接続のエンドポイントは、圧縮機能と解凍機能そのものです。ストリーム上で圧縮が開始されると、両端はそれぞれのデータ・ディクショナリーを事前設定された開始状態にリセットし、データを受信するとその状態を更新します。

各パケットごとに個別に圧縮を実行し、各パケットを処理する前にヒストリーをリセットすることも可能です。しかし通常は、パケットとパケットの間ではデータ・ディクショナリーはリセットされません。これは、ヒストリーは現行パケットの内容だけでなく、以前に処理されたパケットの内容にも基づくことを意味しています。これにより、圧縮機能が冗長度を除去するために検索するデータの量が増えるので、通常は全体的な圧縮効率が上がります。一例として、あるホストがIPを使用して別のホストに『PING』している場合を考えてみます。一連のパケットが送信されますが、通常、各パケットは直前に送信されたパケットとほぼ同じです。圧縮機能は、最初のパケットの圧縮ではあまり効率を上げることができないかもしれませんが、後続のパケットがそれぞれ直前に送信されたものに非常によく似ていることを認識し、それらのパケットでは非常に高率で圧縮されたバージョンを生成できるようになります。

圧縮機能と解凍機能のヒストリーは、各パケットを受信するたびに変更されるので、圧縮機構はパケットの損失、破壊、または配列変更を検知できます。装置で採用されている圧縮プロトコルには、シグナル機構が組み込まれており、これにより圧縮機能と解凍機能が同期が失われたのを検出し、相互に再同期できるようになっています(たとえば、伝送エラーのためにパケットが損失した場合などに必要になります)。これは通常、各パケットにシーケンス番号を含め、解凍機能がこの番号をチェックして、すべてのパケットを順序通りに受信していることを確認する方法で行われます。エラーを検出すると、自身を事前設定された開始状態にリセットし、圧縮機能にも同様にリセットするようにシグナルし、圧縮機能自体がリセットしたことを知らせる確認応答を待ちます(着信した圧縮パケットを廃棄して)。

リンクでの圧縮は一般的に、リンク上の両方向のデータに対して実行されます。通常は、232ページの図20に示すように、接続の各端に圧縮機能と解凍機能の両方があり、接続の他端の相手と通信します。出力(圧縮)側は、入力(解凍)側から独立して動作します。リンクの各方向でまったく異なる圧縮アルゴリズムを使用することも可能です。リンク接続が確立されると、そのリンクの圧縮制御プロトコルが相手側とネゴシエーションし、その接続で使用する圧縮アルゴリズム(1つまたは複数)を決めます。2つの端が、使用する圧縮プロトコルについて合意できない場合には、圧縮は行われず、リンクは通常どおりに作動します(つまり、パケットは圧縮されない形で転送されます)。

## データ圧縮の構成と監視

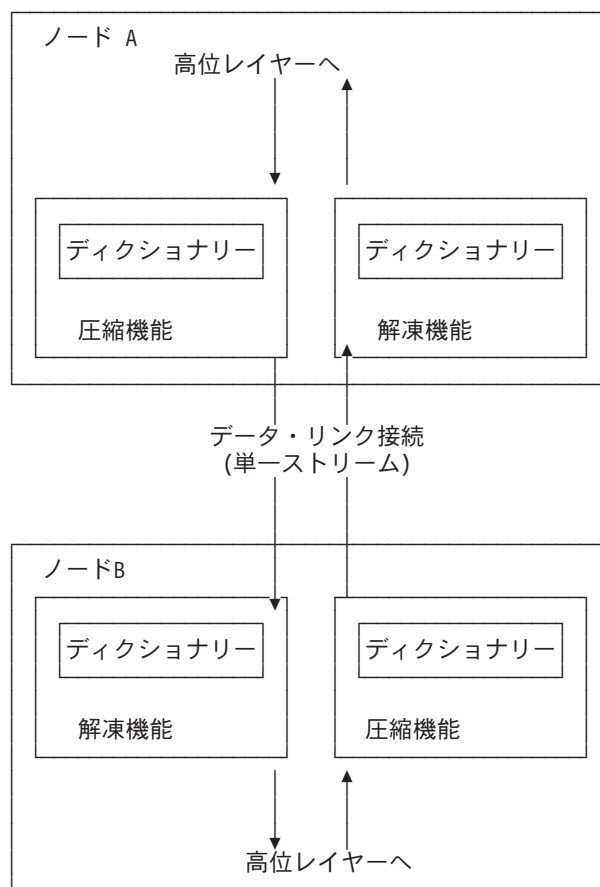


図 20. データ・辞書ナリーを使用した双方向データ圧縮の例

ストリームというのは、実際には、リンクの一端の特定の圧縮プロセスとリンクの他端の対応する解凍プロセス間の接続を表しているもので、単なる 2 つのノード間の『接続』ではなく、より具体的な意味をもっています。精巧な圧縮プロトコルは、2 つのホスト間のデータ・フローを複数のストリームに分割し、個々のストリームを独立して圧縮することも可能です。たとえば、PPP の CCP は、単一の PPP リンク上で複数のヒストリーを使用することをネゴシエーションできます。ただし、ルーターはこれをサポートしていません。

## 考慮事項

データ圧縮を使用するか、しないかの選択は、必ずしも容易ではありません。接続上の圧縮を使用可能にする前に、いくつかの要因を考慮する必要があります。

### CPU 負荷

データ圧縮は、演算に負担のかかる手順です。圧縮するデータの量が増えるほど (単位時間当たり)、装置のプロセッサにかかる負荷が大きくなります。負荷が大きくなり過ぎると、圧縮が行われる装置だけでなく、すべてのネットワーク・インターフェース上の装置の性能が低下します。



実際には、装置には複数のプロセッサが搭載されており、非対称マルチプロセッシングが使用されているので (たとえば、メイン・プロセッサと直列式で稼働するリンク入出力処理装置)、プロセッサの負荷への影響は、必ずしも簡単に測定できるわけではありません。圧縮動作はパケットの転送とオーバーラップしている部分があるので、この負荷は事実上まったく透過的であり、問題がない場合もあります。しかし、装置のプロセッサに過剰な負担をかけ、性能を低下させる可能性もあります。

おおまかな原則として、圧縮を使用可能にするのは、低速の WAN リンク、つまり速度が約 64 KB (標準的な ISDN ダイアル・リンクの速度) までのリンクにだけ限るべきです。すべてのリンク上の圧縮されるデータの総帯域幅は、1 秒につき数百 KB に限定する必要があると考えられます。ISDN 1 次群速度アダプターのすべてのチャネルで圧縮を実行するのは賢明ではありません。

コード化サブシステムのパラメーターによって、同時に圧縮を実行できる接続の数を制限できます。これを使用すると、実際に圧縮を実行する台数より多くのインターフェースに対して、圧縮を使用可能に設定することができます。活動圧縮接続数の限界に達すると、少なくとも既存の圧縮リンクが切断されるまでは、追加の接続は圧縮の使用をネゴシエーションしなくなるだけです。

### メモリーの使用量

圧縮を構成するときに考慮する必要がある 1 つの問題は、メモリー所要量です。圧縮および解凍ヒストリーは、装置の限られた資源であるメモリーをかなり使用します。たとえば、Stac-LZS アルゴリズムでは、圧縮ヒストリーに約 16 KB、解凍ヒストリーに約 8 KB 必要です。これらのヒストリーは、確立される各接続ごとに存在しなければならない (圧縮ヒストリーは、相手側ルーターの対応する解凍ヒストリーと同期される) ので、この問題は一層大きくなります。PPP リンクの場合、これは圧縮ヒストリーが 1 つと解凍ヒストリーが 1 つを意味しています (リンク上のデータ圧縮が双方向で実行されているものと想定した場合)。フレーム・リレー・リンクの場合は、このようなヒストリーが多数必要になる可能性があります (確立される各バーチャル接続 (DLCI) ごとに 1 ペア)。

装置はブート時に、圧縮ヒストリーと解凍ヒストリーを作成します。これらは常に組みにして、**圧縮セッション** として割り振られます (セッションは、1 つの圧縮ヒストリーと 1 つの解凍ヒストリーを単に結合したものです)。技術的には、圧縮と解凍は独立した機能ですが、実際には、圧縮はいつも双方向で実行されるのが一般的なので、運用を簡単にするために、メモリーの管理と構成は個々のヒストリーではなくセッションを対象に行われます。圧縮アルゴリズムによって圧縮と解凍のためのメモリー所要量は異なるので、最悪のケースに対応するために、セッションのサイズは約 30 KB に設定されます。圧縮セッションのプールは、コード化サブシステム機能の構成に従って占有されます。詳しくは、221ページの『第13章 コード化サブシステムの構成と監視』を参照してください。

装置がリンク上で圧縮接続の確立を試みる際には、必ず割り振られたセッションのプールから 1 つのセッションを確保することから始めます。利用可能なセッションがない場合には、その接続では圧縮は行われません。ルーターは、後でセッションが利用可能になった時点で、その接続での圧縮の開始を試みることもできます。

## データ圧縮の構成と監視

割り振られる圧縮セッションの数は、構成可能なパラメーターです。割り振られるセッション数の設定値は、使用されるメモリーの量と、圧縮を使用して同時に作動できる接続の最大数の両方を制限します。同時に作動する圧縮接続の数を制限することは、CPU の負荷問題を制御するのに役立つ 1 つの手段となります。

### データの内容

ある接続の圧縮を使用可能にする前に、その接続で転送されるデータの実際の性質を考慮することが必要です。圧縮は、データのタイプによって効果がさまざまです。ほぼ同一の情報が多数含まれているパケット (たとえば、IP 『PING』によって生成される 1 組のパケット) は、一般的に非常によく圧縮されます。リンクを通る標準的なランダム・テキストおよび 2 進データの圧縮比率は 1.5:1 ~ 3:1 程度です。まったく圧縮されないデータもあります。特に、すでに圧縮されているデータは、さらに圧縮されることはほとんどありません。実際には、以前に圧縮されたデータが圧縮エンジンを通過するときに拡張されることさえあります。

ある接続を通るデータのほとんどが圧縮データから成ることが前もって分かっている場合には、その接続では圧縮を使用可能にしないことをお勧めします。これに該当する例としては、主として FTP ファイル・アーカイブ・サイトとしてセットアップされたホストへの接続があります。この場合、転送に使用されるファイルはすべて圧縮した形でホストに保管されています。

### リンク・レイヤーの圧縮

考慮が必要な最後のファクターは、2 つのホスト間のネットワーク・リンクの性質です。圧縮は、装置のハードウェア・インターフェースよりも下位レイヤーで実行することもできます。特に最新モデムの多くは、ハードウェアとファームウェアにデータ圧縮機構が組み込まれています。下位レイヤー (装置の外部) のリンクで圧縮が行われる場合には、そのインターフェースの装置ではデータ圧縮を使用可能にしないのが最善です。前にも述べたように、すでに圧縮されたデータ・ストリームを圧縮しても、通常は無効であり、実際には性能がいくぶん低下することもあります。ルーターの方がリンク・ハードウェアよりはるかに圧縮効率が高いと確信できる特別な理由がない限り、圧縮はリンク・ハードウェアに任せるのが最良です。

---

## PPP リンクのデータ圧縮の構成と監視

2212 は、PPP 圧縮制御プロトコル (CCP) を使用して、リンク上での圧縮の使用をネゴシエーションします。CCP は、特定の圧縮プロトコル (リンクの各方向に異なるプロトコルを使用することも可能です) および各種のプロトコル特有のオプションの使用をネゴシエーションするための汎用機構を提供します。このソフトウェアは Stac-LZS および MPPC プロトコルをサポートするので、2 つのノード間でデータ圧縮のネゴシエーションを正常に行うためには、相手側でも少なくともこれらのアルゴリズムの 1 つがサポートされることが必要です。圧縮が機能するためには、2 つのノード間でアルゴリズム特有のオプションについて合意することも必要です。

### PPP リンクのデータ圧縮の構成

PPP リンク上のデータ圧縮を構成するには、次のようにします。



1. **enable ccp** コマンドを使用して、リンク上の CCP プロトコルを使用可能にする。これにより、リンクは他のノードと圧縮をネゴシエーションできるようになります。ネゴシエーションには、使用する圧縮アルゴリズムとプロトコル特有のオプションが含まれます。
2. **set ccp algorithms** コマンドを使用して、ネゴシエーションできる圧縮アルゴリズムを選択する。
3. **set ccp options** コマンドを使用して、各圧縮アルゴリズムのネゴシエーション可能パラメーターを設定する。

**list ccp** コマンドを使用すると、現行の圧縮構成を表示することができます。

表22 は、利用可能なコマンドを示し、図21 は、PPP リンク上の圧縮の構成例を示しています。これらのコマンドについての詳しい説明は、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの「ポイントツーポイント構成コマンド」の項を参照してください。

表 22. PPP データ圧縮構成コマンド

データ圧縮コマンド	アクション
disable ccp	データ圧縮を使用不可にします。
enable ccp	データ圧縮を使用可能にします。
set ccp options	圧縮アルゴリズムのオプションを設定します。
set ccp algorithms	圧縮アルゴリズムの優先順位付けされたリストを指定します。
list ccp	圧縮構成を表示します。

```

Config>net 6 1
PPP 6 Config>enable ccp
PPP 6 Config>set ccp alg 2
Enter a prioritized list of compression algorithms (first is preferred),
all on one single line.
Choices (can be abbreviated) are:
STAC-LZS MPPC
Compressor list [STAC-LZS]? stac mppc
PPP 6 Config>set ccp options
STAC: check mode (0=none, 1=LCB, 2=CRC, 3=Seq, 4=Ext) [3]?
STAC: # histories [1]?
PPP 6 Config>li ccp

CCP Options
-----
Data Compression enabled
Algorithm list: STAC-LZS MPPC
STAC histories: 1
STAC check_mode: SEQ

MPPE Options
-----
MPPE disabled
Optional encryption
Key generation: STATEFUL
    
```

図 21. PPP リンク上の圧縮の構成例

注:

1. **network** コマンドは、PPP リンクのネットワーク・インターフェースを選択します。リンクが PPP ダイアル回線の場合は、**encapsulator** コマンドを使用して、PPP 構成メニューにアクセスすることが必要です。

## データ圧縮の構成と監視

2. CCP を使用可能にしたが、リンクのアルゴリズムを設定しなかった場合、ソフトウェアは自動的にリンクがプロトコル STAC および MPPC を使用するよう設定します (これは、コマンド **set ccp algorithms stac mppc** を入力した場合と同じです)。

複数のアルゴリズムを設定する場合、アルゴリズムの設定順序によって、そのリンクのネゴシエーションの優先順位が決まります。

**set ccp algorithms none** を入力すると、ソフトウェアは自動的にリンク上の圧縮を使用不可にします。

MPPE が使用可能になっていて、CCP も使用可能になっている場合は、MPPC が圧縮アルゴリズムになります。

## PPP リンクのデータ圧縮の監視

圧縮の監視は、他の PPP コンポーネントの監視と同様です。アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の「インターフェース監視プロセスへのアクセス」の章で、PPP コンソール環境へのアクセス方法とコマンドについて詳しく説明しています。表23 は、圧縮関連のコマンドを表示しています。237ページの図22 は、PPP インターフェースに表示される圧縮の例です。

表 23. PPP データ圧縮監視コマンド

コマンド	機能
<b>list control ccp</b>	CCP 状態とネゴシエーション済みのオプションを表示します。
<b>list ccp</b>	CCP パケット統計を表示します。
<b>list cdp</b> または <b>list compression</b>	圧縮データグラム統計を表示します。

```

+ network 1
PPP > list control ccp

CCP State:          Open
Previous State:     Ack Sent
Time Since Change:  2 minutes and 52 seconds

Compressor:  STAC-LZS histories 1, check_mode SEQ
Decompressor: STAC-LZS histories 1, check_mode SEQ
MPPE:        Not negotiated

PPP > list ccp

CCP Statistic          In          Out
-----
Packets:               2          3
Octets:                18         27
Reset Reqs:            0          0
Reset Acks:            0          0
Prot Rejects:         1          -

PPP > list cdp

Compression Statistic  In          Out
-----
Packets:               19541      19542
Octets:                2550673   2740593
Compressed Octets:     821671    899446
Incompressible Packets: 0          0
Discarded Packets:    0          -
Prot Rejects:         0          -
Compression Ratios:   3.11      3.24

```

図 22. PPP インターフェースの圧縮の監視

---

## フレーム・リレー・リンクのデータ圧縮の構成と監視

グローバル圧縮パラメーターを構成し、インターフェース上の圧縮を使用可能にした後で、フレーム・リレー・インターフェース上の個々の回線 (PVC) のパラメーターを設定する必要があります。インターフェースに定義されている各回線ごとに圧縮を使用可能にすることができ、ネゴシエーションが正常に行われた各回線は、グローバル・プールから 1 つの圧縮セッションを使用します。インターフェース自体の圧縮を使用不可にすることもできます。これは、そのインターフェース上のどの回線も圧縮データ・トラフィックを伝送できなくなることを意味しています。

### フレーム・リレー・リンクのデータ圧縮の構成

FR リnkのデータ圧縮を構成するには、次のようにします。

1. **enable compression** コマンドを使用して、インターフェースの圧縮を使用可能にする。これにより、リンクは他のノードと圧縮をネゴシエーションできるようになります。
2. **add permanent-virtual-circuit** コマンドを使用して、圧縮データを伝送する新規の PVC ごとに圧縮を使用可能にする。 **change permanent-virtual-circuit** コマンドを使用すると、既存の PVC を変更できます。

現行の圧縮構成を表示したい場合は、**list lmi** または **list permanent-virtual-circuit** コマンドを使用します。

238ページの表24 は、フレーム・リレー・リンクの圧縮を構成するのに利用可能なコマンドを表示しています。 238ページの図23 は、フレーム・リレー・リンクの構成例

## データ圧縮の構成と監視

を示しています。詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の『フレーム・リレー構成コマンド』の項を参照してください。

```
Config> net 2
```

```
Frame Relay user configuration
```

```
FR Config> enable compression
```

```
Maximum number of run-time compression circuits (zero means no limit) [0]? 0
```

```
Do you want orphan PVCs to perform compression [Y]? n
```

```
The number of currently defined non-compression PVCs is 4
```

```
Would you like to change them all to compression PVCs [N]? y
```

```
FR Config> add perm
```

```
Circuit number [16]? 22
```

```
Committed Information Rate (CIR) in bps [65536]?
```

```
Committed Burst Size (Bc) in bits [64000]?
```

```
Excess Burst Size (Be) in bits [0]?
```

```
Assign circuit name []? cir22
```

```
Is circuit required for interface operation [N]?
```

```
Do you want to have data compression performed [Y]?
```

```
FR Config>list lmi
```

### Frame Relay Configuration

```

LMI enabled          = No   LMI DLCI              = 0
LMI type             = ANSI LMI Orphans OK          = Yes
CLLM enabled         = No   Timer Ty seconds      = 11

Protocol broadcast   = Yes  Congestion monitoring = Yes
Emulate multicast    = Yes  CIR monitoring         = No
Notify FECN source   = No   Throttle transmit on FECN = No

Data compression    = Yes  Orphan compression    = No
Compression PVC limit = None Number of compression PVCs = 2

PVCs P1 allowed     = 64   Interface down if no PVCs = No
Timer T1 seconds    = 10   Counter N1 increments     = 6
LMI N2 error threshold = 3   LMI N3 error threshold window = 4
MIR % of CIR        = 25   IR % Increment            = 12
IR % Decrement      = 25   DECnet length field       = No
Default CIR         = 65536 Default Burst Size      = 64000
Default Excess Burst = 0

```

```
FR Config>list perm
```

```

Maximum PVCs allowable = 64
Total PVCs configured  = 2

```

Circuit Name	Circuit Number	Circuit Type	CIR in bps	Burst Size	Excess Burst
cir16	16	@ Permanent	65536	64000	0
cir22	22	@ Permanent	65536	64000	0

\* = circuit is required

# = circuit is required and belongs to a required PVC group

@ = circuit is data compression capable

図 23. フレーム・リレー・リンクの圧縮の構成例

表 24. データ圧縮構成コマンド

コマンド	アクション
<b>add permanent-virtual-circuit #</b>	インターフェース上に定義された特定の PVC 上のデータ圧縮を使用可能にするのに使用します。
<b>change permanent-virtual-circuit #</b>	特定の PVC がデータを圧縮するかどうかを変更するのに使用します。

表 24. データ圧縮構成コマンド (続き)

コマンド	アクション
<b>disable compression</b>	データ圧縮を使用不可にします。
<b>enable compression</b>	データ圧縮を使用可能にします。
<b>list lmi</b>	インターフェースの現行構成を表示します。
<b>list permanent</b>	回線に関する要約情報を表示します。

注: 孤立回線上の圧縮を使用可能にすると、装置上のネイティブ PVC が利用可能な圧縮セッションの数が減ります。

すでに圧縮が使用可能になっているフレーム・リレー・インターフェース上の圧縮を使用可能にすると、ソフトウェアは、次の例に示すように、圧縮パラメーターを変更したいかどうかを尋ねます。圧縮を使用不可にせずに、インターフェースの圧縮を変更することができます。

フレーム・リレー・インターフェースの圧縮を変更する例:

```
Config> net 2
Frame Relay user configuration
FR Config> enable compression
Data compression already enabled.
Do you wish to continue and change an interface parameter [Y]
Maximum number of run-time compression PVCs (zero means no limit) [0]? 32
Do you want orphan circuits to perform compression [Y]?
The number of currently defined circuits is 5
Change all of these circuits to perform compression?
```

## フレーム・リレー・リンクのデータ圧縮の監視

圧縮の監視は、他のフレーム・リレー・コンポーネントの監視と同様です。アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の『フレーム・リレー監視コマンド』の章で、フレーム・リレー・コンソール環境へのアクセス方法とコマンドについて詳しく説明しています。表25 は、圧縮関連のコマンドを表示しています。『例: フレーム・リレー・インターフェースまたは回線上の圧縮の監視』は、フレーム・リレー・インターフェースの圧縮のリスト例です。

表 25. フレーム・リレー・データ圧縮監視コマンド

コマンド	表示
<b>list lmi</b>	インターフェースの現在の状態を表示します。
<b>list permanent</b>	回線に関する要約情報を表示します。
<b>list circuit</b>	回線の現在の状態を表示します。

### 例: フレーム・リレー・インターフェースまたは回線上の圧縮の監視

```
+ network 2
FR 2 > list lmi

Management Status:
-----
LMI enabled          = No   LMI DLCI           = 0
LMI type             = ANSI LMI Orphans OK = Yes
CLLM enabled         = No
Protocol broadcast   = Yes  Congestion monitoring = Yes
Emulate multicast    = Yes  CIR monitoring       = No
Notify FECN source   = No   Throttle transmit on FECN = No
PVCs P1 allowed      = 64  Interface down if no PVCs = No
```

## データ圧縮の構成と監視

```

Line speed (bps) = 64000 Maximum frame size = 2048
Timer T1 seconds = 10 Counter N1 increments = 6
LMI N2 threshold = 3 LMI N3 threshold window = 4
MIR % of CIR = 25 IR % Increment = 12
IR % Decrement = 25 DECnet length field = No
Default CIR = 65536 Default Burst Size = 64000
Default Excess Burst = 0

Current receive sequence = 0
Current transmit sequence = 0
Total status enquiries = 0 Total status responses = 0
Total sequence requests = 0 Total responses = 0

Data compression enabled = Yes Orphan Compression = No

Compression PVC limit = None Active compression PVCs = 1

```

### PVC Status:

-----

```

Total allowed = 64 Total configured = 1
Total active = 1 Total congested = 0
Total left net = 0 Total join net = 0

```

### FR 2 > list permanent

Circuit Number	Circuit Name	Orphan Type/ Circuit State	Frames Transmitted	Frames Received
16	circ16	No @ P/A	58364	58355
22	circ22	No & P/A	58364	58355

A - Active I - Inactive R - Removed P - Permanent C - Congested  
 \* - Required # - Required and belongs to a PVC group  
 @ - Data compression capable but not operational  
 & - Data compression capable and operational

### FR 2 > list circuit 22

Circuit name = circ22

```

Circuit state = Active Circuit is orphan = No
Frames transmitted = 58391 Bytes transmitted = 2676894
Frames received = 58383 Bytes received = 2671009
Total FECNs = 0 Total BECNs = 0
Times congested = 0 Times Inactive = 0
CIR in bits/second = 65536 Potential Info Rate = 64000
Committed Burst (Bc) = 64000 Excess Burst (Be) = 0
Minimum Info Rate = 16000 Maximum Info Rate = 64000
Required = No PVC group name = Unassigned

Compression capable = Yes Operational = Yes
R-R's received = 0 R-R's transmitted = 0
R-A's received = 0 R-A's transmitted = 0
R-R mode discards = 0 Enlarged frames = 0
Decompress discards = 0 Compression errors = 0
Rcv error discards = 0

Compression ratio = 1.00 to 1 Decompression ratio = 1.00 to 1

Current number of xmit frames queued = 0
Xmit frames dropped due to queue overflow = 0

```

---

## 第15章 ローカルまたはリモート認証の使用

認証とは、ユーザー（または、エンティティ）が誰であるかを判別するプロセスです。2212 上の PPP プロトコルに対するユーザー・アクセスを認証することは、PPP 認証プロトコルの PAP、MSCHAP、CHAP、および SPAP に関連しているため、ユーザー・プロファイル管理の柔軟性が増します。PAP、MSCHAP、CHAP、および SPAP の構成についての追加情報は、アクセス・インテグレーター・サービス ソフトウェア 使用者の手引き の ‘PPP 認証プロトコル’ の項を参照してください。

認証は、ローカルで構成することも、ユーザー構成を統合して構成する（ネットワーク上の認証サーバーを使用して、ネットワーク全体の認証要求に応じる）こともできます。IBM 2212 は、ローカルで維持される認証、および次の認証サーバー・プロトコルを設定しています。

- Radius
- TACACS
- TACACS+

---

## 認証、許可、および会計 (AAA) セキュリティー

認証、許可、および会計 (AAA) セキュリティーは、サービスへのアクセスを制御できる構成可能なプロトコルです。ローカル認証またはリモート認証を実行するように AAA を構成できます。

3 つのタイプの機能のセキュリティー・プロトコルを構成できます。

- PPP リンク
- ログイン・ユーザー (Telnet / コンソール・ログイン)
- トンネル

構成は 1 次サーバーと 2 次サーバーを設定することによって行います。サーバー情報は、AAA 構成とは別に構成し、別に保管します。サーバー・プロファイルは、構成時に付けた名前を使用します。

どの環境でも、会計はローカルに行うことはできず、Radius または TACACS+ のどちらかでなければなりません。

許可は、ローカルで行うか、あるいは Radius または TACACS+ を使用するリモート認証を介して行うことしかできません。

## AAA セキュリティーとは

AAA セキュリティーというのは、この装置のセキュリティー・システムの名前です。これには、次のものが含まれています。

**認証** ユーザーを識別するプロセス。認証は、アクセスのために名前とパスワードを使用します。

**許可** ユーザーがアクセスできるサービスを決めるプロセス。許可プロセスでは、

## ローカルまたはリモート認証の使用

未認証のユーザーが見つかることがあります。その場合、許可エージェントは、未認証ユーザーが問題のサービスへのアクセスができるかどうかを判別します。

**会計** ユーザーがセッションを開始または停止したときに記録するプロセス。サポートされる会計レコードには 2 つのタイプがあります。

### 開始レコード

サービスが開始されようとしていることを示します。

### 停止レコード

サービスが終了したことを示します。

## PPP の使用

ポイントツーポイント・プロトコル (PPP) の場合、次の機能を構成できます。

- 認証
- 許可
- 会計

各機能は独自のセキュリティー・プロトコルを持つことができ、それぞれ独立して構成することができます。

- 認証プロトコルの設定値は、許可または会計には無効です。
- 許可プロトコルの設定値は、認証または会計には無効です。
- 会計プロトコルの設定は、認証または許可には影響を与えません。
- AAA をリモートに設定すると、認証はリモートに設定され、許可もリモートに設定され、会計もリモートに設定されます。
- AAA をローカルに設定すると、認証はローカルに設定され、許可もローカルに設定され、会計は無視に設定されます。認証または許可を使用不可能にすることはできません。

この環境で使用する PPP 構成コマンドについて詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き のポイントツーポイント構成コマンドの項を参照してください。

## 有効な PPP セキュリティー・プロトコル

有効な PPP セキュリティー・プロトコルは、次のとおりです。

### 認証方式

Local、RADIUS、TACACS+、TACACS

### 許可方式

Local、RADIUS、TACACS+

### 会計方式

RADIUS、TACACS+

表 26. PPP セキュリティー・プロトコルの設定

アクション	認証	許可	会計
AAA をローカルに設定	ローカル	ローカル	無視



表 26. PPP セキュリティー・プロトコルの設定 (続き)

アクション	認証	許可	会計
AAA をリモートに設定	リモート	リモート	リモート
AUTHENT をローカルに設定	ローカル	無視	無視
AUTHOR をローカルに設定	無視	ローカル	無視
AUTHENT をリモートに設定	リモート	無視	無視
ACCOUNTING をローカルに設定	該当せず	該当せず	該当せず
AUTHOR をリモートに設定	無視	リモート	無視
ACCOUNTING をリモートに設定	無視	無視	リモート
ACCOUNTING 使用不可	無視	無視	使用不可
AUTHENT 使用不可	該当せず	該当せず	該当せず
AUTHOR 使用不可	該当せず	該当せず	該当せず

## ログインの使用

AAA ログイン構成の場合、リモートまたはローカルを選択することができます。ローカル認証が必要な場合は、ローカル許可も使用する必要があります。リモート認証が選択されている場合には、リモート許可も使用する必要があります。会計はローカルではサポートされないため、認証と許可をローカルで行う場合は、会計を使用不可にする必要があります。

**重要:** コンソール・ログインを使用可能にする前に、コンソール・ログインを使用不可にして、構成を保管してください。ログイン認証が Radius、TACACS、または TACACS+ を使用しているリモート・サーバーに設定されていて、ルーターが認証サーバーに到達できない場合には、ルーターへのアクセスは拒否されます。コンソール・ログインを使用不可にすると、ロック状態を防止することができます。

リモート認証を構成する場合、許可は別のリモート許可プロトコル (Radius または TACACS+) に設定し、会計は Radius または TACACS+ を使用するように設定することも可能です。

- AAA をローカルに設定すると、認証はローカルに設定され、許可もローカルに設定され、会計は使用不可に設定されます。
- AAA をリモートに設定すると、認証はリモートに設定され、許可もリモートに設定され、会計もリモートに設定されます。
- 認証プロトコルをローカルに設定すると、自動的に許可プロトコルを同じに設定し、会計を使用不可にします。
- 認証プロトコルをリモートに設定すると、許可プロトコルがローカルに設定されている場合にだけ、自動的に許可プロトコルを同じに設定し、会計プロトコルは無視します。
- 許可プロトコルをリモートに設定すると、認証プロトコルがローカルに設定されている場合にだけ、自動的に認証プロトコルを同じに設定し、会計プロトコルは無視します。
- 会計プロトコルをリモートに設定すると、認証プロトコルがローカルに設定されている場合にだけ、自動的に認証プロトコルを同じに設定し、許可がローカルに設定されている場合にだけ、自動的に許可プロトコルを同じに設定します。

## ローカルまたはリモート認証の使用

- 会計プロトコルを使用不可に設定しても、認証または許可プロトコルには影響を与えません。
- 認証または許可を使用不可にすることはできません。

## 有効なログイン / 管理セキュリティ・プロトコル

有効なログイン / 管理セキュリティ・プロトコルは、次のとおりです。

### 認証 / 許可方式

Local、RADIUS、TACACS Plus

### 会計方式

RADIUS、TACACS Plus

表 27. ログイン・セキュリティ・プロトコルの設定

アクション	認証	許可	会計
AAA をローカルに設定	ローカル	ローカル	使用不可
AAA をリモートに設定	リモート	リモート	リモート
AUTHENT をローカルに設定	ローカル	ローカル	使用不可
AUTHOR をローカルに設定	ローカル	ローカル	使用不可
AUTHENT をリモートに設定	リモート	ローカルの場合はリモート、その他の場合は無視	無視
AUTHOR をリモートに設定	ローカルの場合はリモート、その他の場合は無視	リモート	無視
ACCOUNTING をリモートに設定	ローカルの場合はリモート、その他の場合は無視	ローカルの場合はリモート、その他の場合は無視	リモート
ACCOUNTING 使用不可	無視	無視	使用不可
AUTHEN 使用不可	該当せず	該当せず	該当せず
AUTHOR 使用不可	該当せず	該当せず	該当せず

## トンネルの使用

トンネル認証は、トンネル許可と同じに設定します。トンネル認証をローカルまたはリモートに設定した場合は、会計を使用可能にすることができます。トンネル認証サーバーと許可サーバーは同じでなければなりません。

## 有効なトンネル・セキュリティ・プロトコル

有効なトンネル・セキュリティ・プロトコルは、次のとおりです。

### 認証 / 許可方式

Local、RADIUS

## 会計方式

RADIUS、TACACS Plus

表 28. トンネル・セキュリティー・プロトコルの設定

アクション	認証	許可	会計
AAA をローカルに設定	ローカル	ローカル	無視
AAA をリモートに設定	リモート	リモート	リモート
AUTHENT をローカルに設定	ローカル	ローカル	無視
Author をローカルに設定	ローカル	ローカル	無視
AUTHENT をリモートに設定	リモート	リモート	無視
AUTHOR をリモートに設定	リモート	リモート	無視
ACCOUNTING をリモートに設定	無視	無視	リモート
ACCOUNTING 使用不可	無視	無視	使用不可
AUTHENT 使用不可	該当せず	該当せず	該当せず
AUTHOR 使用不可	該当せず	該当せず	該当せず

## パスワード規則

ローカル認証では、パスワードを使用してログイン・アクセスを制御することができます。次の規則のどれか、またはすべてに照らして、パスワードを検査することができます。

注: 次の規則は、PPP ユーザー・ログインだけに当てはまり、コンソール・ログインには当てはまりません。

- 長さが最小文字数である。必要な文字数を設定します。
- 少なくとも 1 字の英字が含まれている。
- 少なくとも 1 字の非英字が含まれている。
- 最初の位置に非数字がある。
- 最後の位置に非数字がある。
- 前のパスワードで使用されたのと同じ連続文字が 3 字しか含まれていない。
- 2 連続文字しか含まれていない。
- ユーザー ID がパスワードの一部として含まれていない。
- 直前の 3 つのパスワードのどれとも同じでない。
- 所定の日数の経過後に変更された。パスワードの変更の間隔の日数を設定します。
- 特定の回数のログイン失敗後にロックアウト。失敗の回数を設定します。

## 認証サーバーとは

認証サーバーとは、ネットワークのユーザー ID とパスワードの妥当性を検査するネットワーク内のサーバーです。装置が認証サーバーを通して認証するように構成されている場合、装置は認証プロトコルからパケットを受信すると、ユーザー ID とパスワードをサーバーにパスして認証を依頼します。ユーザー ID とパスワードが正しい場合、サーバーは肯定応答します。その場合、装置は要求の発信元と通信するこ

## ローカルまたはリモート認証の使用

とができます。装置から受け取ったユーザー ID とパスワードが見つからない場合、サーバーは装置に否定応答します。その場合、装置は認証要求を受け取ったセッションを拒否します。

## SecurID サポート

2212 は、Security Dynamics ACE/サーバーで SecurID を使用するダイヤルイン・クライアントを認証することができます。このサポートは、ACE/サーバー上で TACACS、TACACS+、または RADIUS を使用して、クライアントを認証します。このダイヤルイン・クライアントの構成は、2212 の他のダイヤルイン・クライアントと同様に行います。

ダイヤルイン・クライアントは通常のようにログオンしますが、パスワードとして SecurID パスコードを使用します。SecurID パスコードは、4 ~ n 桁の PIN 番号とその後の SecurID トークン・カードからの番号で構成されます。(PIN の最大桁数は、サーバーによって異なります。) ユーザー ID とパスワードは、次のようになります。

ユーザー名:

パスワード:

図 24. SecurID ユーザー名とパスコード

ACE/サーバーは、ログオンを認証するときに、クライアントに対して次のトークンを入力するように要求することがあります。次のトークンとは、トークン・カードの次のトークンです。次のトークンの最大桁数は、クライアントが使用している SecurID トークン・カードによって異なります。クライアントはパスワードの入力を求められたときに、`passcode*token` の形式で、パスコードと次のトークンを入力することができます。たとえば、次のように入力します。

ユーザー名:

パスワード:

図 25. SecurID パスコードと次のトークン

**注:** サーバーがクライアントに次のトークンを入力するように要求した場合、クライアントは、次のようにしなければなりません。

1. PIN を入力する。
2. カードからの新規のトークンを待ち、そのトークンを入力する。
3. \* の後に、カードからの次のトークンを入力する。

ACE/サーバーの管理者は、サーバーが次のトークンまたは新規の PIN を要求する条件を構成します。

ダイヤルイン・クライアントは、次のトークンを入力する必要がある場合に、認証システムから警報を受け取れるようにするためには、SPAP を使用する必要があります。クライアントが SPAP を使用せず、ログオンに成功しなかった場合、passcode\*token 形式を使用して、新規パスワードの入力を試みる必要があります。それでも成功しない場合は、クライアントと ACE/サーバーとの間に別の問題がある可能性があります。

### 制約

次のような制限があります。

- Security Dynamics Inc. (SDI) および DES 暗号化はサポートされません。
- SecurID 『New PIN』機能はサポートされません。
- TACACS は『New PIN』または『Next-Token』機能をサポートしません。クライアントは、ログインするときに次のトークンを指定することはできませんが、サーバーはそれを使用しません。
- コールバック用に構成されたクライアントはサポートされません。
- TACACS または TACACS+ で CHAP を使用する場合、CHAP 再チャレンジ間隔を 0 に設定してください。
- RADIUS 認証を使用する場合は、CHAP を使用しないでください。
- クライアントは、TACACS+ および SPAP を使用すると最良の結果が得られます。
- マルチリンクを使用して SecurID 認証を行う Windows 3.1 DIALs クライアントはサポートされません。
- SecurID 認証を使用する場合は、最新のクライアント・ソフトウェア (たとえば、Windows 95 または OS/2) を使用することを強くお勧めします。

ローカルまたはリモート認証の使用

## 第16章 認証の構成

この章では、認証の構成コマンドおよび動作コマンドについて説明します。この章には、次の内容が記載されています。

- 『認証構成プロンプトへのアクセス』
- 『認証構成コマンド』

### 認証構成プロンプトへのアクセス

Authent config > プロンプトにアクセスするには、次のようにします。

1. \* プロンプトで **talk 6** と入力する。
2. Config > プロンプトで **feature auth** と入力する。

### 認証構成コマンド

表29 は、Authent config > プロンプトで利用可能なコマンドを示しています。

表 29. 認証構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxi ページの『ヘルプの入手』を参照してください。
Disable	AAA の会計を使用不可にします。
List	AAA 構成パラメーターを表示します。
Login	ログイン用の AAA を構成します。
Nets-info	ローカル PPP 認証に関する情報を表示します。
Password-rules	パスワード規則を構成します (使用可能または使用不可)。
PPP	PPP 用の AAA を構成します。
Quickset	認証方式を迅速に構成します。
サーバー	個々のリモート AAA サーバーを構成します。
Set	タイプに関係なく、認証パラメーターを構成します。
Tunnel	L2TP トンネル用の AAA を構成します。
User-profile	ローカル PPP ユーザーを構成します。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

### Disable

**disable** コマンドは、会計を使用不可にするのに使用します。

構文:

**disable** accounting

## List

**list** コマンドは、AAA パラメーターを表示するのに使用します。

構文:

```
list
    accounting
    authentication
    authorization
    all
    config
```

```
AAA Config> list all
ppp AAA configuration...
  ppp authentication      : Radius      serv01
    authorizeAuthent      YES
    Primary server address 1.1.1.1
    Secondary server address 2.2.2.2
    Request tries         3
    Request interval      3
    Key for encryption    <notSet>
  ppp authorization      : locallist
  ppp accounting         : Disabled
tunnel AAA configuration...
  tunnel authentication  : Radius      serv01
    authorizeAuthent      YES
    Primary server address 1.1.1.1
    Secondary server address 2.2.2.2
    Request tries         3
    Request interval      3
    Key for encryption    <notSet>
  tunnel authorization   : Radius      serv01
    authorizeAuthent      YES
    Primary server address 1.1.1.1
    Secondary server address 2.2.2.2
    Request tries         3
    Request interval      3
    Key for encryption    <notSet>
  tunnel accounting     : Disabled
login AAA configuration...
  login authentication   : Radius      serv01
    authorizeAuthent      YES
    Primary server address 1.1.1.1
    Secondary server address 2.2.2.2
    Request tries         3
    Request interval      3
    Key for encryption    <notSet>
  login authorization    : Radius      serv01
    authorizeAuthent      YES
    Primary server address 1.1.1.1
    Secondary server address 2.2.2.2
    Request tries         3
    Request interval      3
    Key for encryption    <notSet>
  login accounting      : Radius      serv01
    authorizeAuthent      YES
    Primary server address 1.1.1.1
    Secondary server address 2.2.2.2
    Request tries         3
    Request interval      3
    Key for encryption    <notSet>
```



```

AAA Config> list accounting all
accounting AAA configuration...
  accounting ppp          : Disabled
  accounting tunnel      : Disabled
  accounting login       : Radius      serv01
  authorizeAuthent       YES
  Primary server address 1.1.1.1
  Secondary server address 2.2.2.2
  Request tries          3
  Request interval       3
  Key for encryption     <notSet>
AAA Config> list accounting config
accounting ppp          : Disabled
accounting login       : Radius      serv01
accounting tunnel      : Disabled
AAA Config> list authentication all
authentication AAA configuration...
  authentication ppp     : Radius      serv01
  authorizeAuthent       YES
  Primary server address 1.1.1.1
  Secondary server address 2.2.2.2
  Request tries          3
  Request interval       3
  Key for encryption     <notSet>
  authentication tunnel : Radius      serv01
  authorizeAuthent       YES
  Primary server address 1.1.1.1
  Secondary server address 2.2.2.2
  Request tries          3
  Request interval       3
  Key for encryption     <notSet>

```

## Login

**login** コマンドは、ログイン用の AAA を構成するのに使用します。

表30 は、**login** コマンドと共に使用できるサブコマンドを示しています。

表 30. ログイン・サブコマンド

コマンド	機能
Disable	ログインの会計を使用不可にします。
List	ログイン用の AAA 構成パラメーターを表示します。
Set	ログイン用の AAA 構成パラメーターを設定します。

### Disable

**login disable** コマンドは、会計を使用不可にするのに使用します。

構文:

**login disable** accounting

### List

**login list** は、AAA 構成パラメーターを表示するのに使用します。

構文:

**login list** all  
accounting

authentication

authorization

config

### Set

**login set** コマンドは、認証パラメーターを構成するのに使用します。

構文:

```
login set          aaa  
                   accounting  
                   authentication  
                   authorization
```

#### **aaa** *authype*

認証、許可、および会計タイプを設定します。 *Authype* は、次のどれか 1 つです。

**local** 認証、許可、および会計タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

#### **remote**

認証、許可、および会計タイプを、リモート・ユーザー・データベースを使用するように設定します。

#### **server id**

リモート・データベースの識別子を指定します。

#### **accounting** *authype*

会計タイプを設定します。 *Authype* は、次のどれか 1 つです。

#### **remote**

認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

#### **server id**

リモート・データベースの識別子を指定します。

#### **authentication** *authype*

認証タイプを設定します。 *Authype* は、次のどれか 1 つです。

**local** 認証タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

#### **remote**

認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

#### **server id**

リモート・データベースの識別子を指定します。

#### **authorization** *authype*

許可タイプを設定します。 *Authype* は、次のどれか 1 つです。

**local** 許可タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

**remote**

許可タイプを、リモート・ユーザー・データベースを使用するように設定します。

**server id**

リモート・データベースの識別子を指定します。

## Nets-info

**nets-info** コマンドは、各 PPP インターフェースに現在構成されている PPP 認証プロトコルを表示します。

構文:

**nets-info**

## Password-rules

**password-rules** コマンドは、パスワードを構成する (使用可能または使用不可) のに使用します。

表31 は、**password-rules** コマンドと共に使用できるサブコマンドを示しています。

表 31. ログイン・サブコマンド

コマンド	機能
Disable	パスワード規則を使用不可にします。
Enable	パスワード規則を使用可能にします。
List	パスワード規則の現在の状態 (使用可能または使用不可) を表示します。

### Disable

**password-rules disable** コマンドは、任意のまたはすべてのパスワード規則を使用不可にするのに使用します。

構文:

**password-rules disable**     all  
                                   compare-ident-prev  
                                   change-days  
                                   first-non-numeric  
                                   ident-chars  
                                   last-non-numeric  
                                   lockout  
                                   minimum-length  
                                   one-alpha  
                                   one-nonalpha

prev-three

userid-contained

**compare-ident-prev**

前のユーザー識別とパスワード変更を要求しているユーザーとを比較しません。

**change-days**

パスワード変更が必要になる前の最大日数

有効値: 0 ~ 360

デフォルト値: 180

**first\_non-numeric**

パスワードの先頭文字で、数字は使えません。

有効値: 任意の非数字

デフォルト値: なし

**ident-chars**

前のパスワードの同じ位置に使用された文字が 3 字より多く含まれていてはなりません。

**last-non-numeric**

パスワードの最後の文字は数字であってはなりません。

有効値: 任意の非数字

デフォルト値: なし

**lockout**

ロックアウトされる前のパスワードの試行回数

有効値: 0 ~ 360

デフォルト値: 3

**minimum-length**

有効なパスワードに必要な最小文字数

有効値: 1 ~ 31

デフォルト値: 8

**maximum-length**

パスワードに含めることができる最大文字数

有効値: 1 ~ 31

デフォルト値: 8

**one-alpha**

パスワードの少なくとも 1 文字は英字でなければなりません。

**one-nonalpha**

パスワードの少なくとも 1 文字は数字でなければなりません。

**prev-three**

パスワードは、最後の 3 つのパスワードのどれとも同じであってはなりません。

### userid-contained

ユーザー ID をパスワードの一部として含めることはできません。

### Enable

**password-rules enable** コマンドは、任意のまたはすべてのパスワード規則を使用可能にするのに使用します。パスワード規則についての説明は、**disable** コマンドを参照してください。

構文:

```
password-rules enable    all
                        compare-ident-prev
                        change-days
                        first-non-numeric
                        ident-chars
                        last-non-numeric
                        lockout
                        minimum-length
                        one-alpha
                        one-nonalpha
                        prev-three
                        userid-contained
```

### List

**password-rules list** コマンドは、パスワード規則の現在の状態 (使用不可または使用可能) を表示するのに使用します。

構文:

```
password-rules list
```

## PPP

**ppp** コマンドは、PPP 用の AAA を構成するのに使用します。

表32 は、**ppp** コマンドと共に使用できるサブコマンドを示しています。

表 32. PPP サブコマンド

コマンド	機能
Disable	PPP の会計を使用不可にします。
List	PPP 用の AAA 構成パラメーターを表示します。
Set	PPP 用の AAA 構成パラメーターを設定します。

## Disable

**ppp disable** コマンドは、PPP の会計を使用不可にするのに使用します。

構文:

```
ppp disable                accounting
```

## List

**ppp list** コマンドは、PPP 用の AAA 構成パラメーターを表示するのに使用します。

構文:

```
ppp list                    all  
                             accounting  
                             authentication  
                             authorization  
                             config
```

## Set

**ppp set** コマンドは、PPP 用の AAA 構成パラメーターを表示するのに使用します。

構文:

```
ppp set                    aaa  
                             accounting  
                             authentication  
                             authorization
```

### **aaa** *authype*

認証、許可、および会計タイプを設定します。 *Authype* は、次のどれか 1 つです。

**local** 認証、許可、および会計タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

#### **remote**

認証、許可、および会計タイプを、リモート・ユーザー・データベースを使用するように設定します。

#### **server id**

リモート・データベースの識別子を指定します。

### **accounting** *authype*

会計タイプを設定します。 *Authype* は、次のどれか 1 つです。

#### **remote**

認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

#### **server id**

リモート・データベースの識別子を指定します。

**authentication** *authtype*

認証タイプを設定します。 *Authtype* は、次のどれか 1 つです。

**local** 認証タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

**remote**

認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

**server id**

リモート・データベースの識別子を指定します。

**authorization** *authtype*

許可タイプを設定します。 *Authtype* は、次のどれか 1 つです。

**local** 許可タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

**remote**

許可タイプを、リモート・ユーザー・データベースを使用するように設定します。

**server id**

リモート・データベースの識別子を指定します。

## Servers

**servers** コマンドは、個々のリモート AAA サーバーを構成するのに使用します。

表33 は、**servers** コマンドと共に使用できるサブコマンドを示しています。

表 33. サーバー・サブコマンド

コマンド	機能
Add	リモート AAA サーバー・プロファイルを追加します。
Change	リモート・サーバー・プロファイルを変更します。
Delete	リモート・サーバー・プロファイルを削除します。
Lists	AAA サーバー・プロファイル情報を表示します。

### Add

**servers add** コマンドは、リモート・サーバー・プロファイルを追加するのに使用します。

構文:

**servers add** name

**radius** 認証タイプを、Radius 認証サーバー・プロトコルを使用するように設定します。

次のパラメーターの値を設定できます。

**key-for-encryption:**

暗号化キーを指定します。

**有効値:** 最大 32 字の長さの任意の英数字列。

## 認証の構成

デフォルト値: なし。

### **primary-server-address:**

1 次認証サーバーのアドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

### **retries**

有効値: 1 ~ 100

デフォルト値: 3

### **retry-interval**

有効値: 1 ~ 60

デフォルト値: 3

### **secondary-server-address:**

2 次認証サーバーのアドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

### **Author-Authent**

認証時に許可属性を転送するかどうかを指定します。

有効値: yes、no

デフォルト値: yes

## **tacacs**

認証タイプを、TACACS 認証サーバー・プロトコルを使用するように設定します。

次のパラメーターの値を設定できます。

### **primary-server-address:**

1 次認証サーバーのアドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

### **retries**

有効値: 1 ~ 100

デフォルト値: 3

### **retry-interval**

有効値: 1 ~ 60

デフォルト値: 3

### **secondary-server-address:**

2 次認証サーバーのアドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0



**tacacsplus**

認証タイプを、TACACS+ 認証サーバー・プロトコルを使用するように設定します。

次のパラメーターの値を設定できます。

**encryption:**

暗号化を使用するかどうかを指定します。

有効値: yes、no

デフォルト値:

**key-for-encryption:**

使用する暗号化キーを指定します。

有効値: 任意の 16 進値

デフォルト値:

**primary-server-address:**

1 次認証サーバーのアドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

**privilege-level**

有効値: 0 ~ 15

デフォルト値: 0

**restarts**

リスタートの回数を設定します。このパラメーターには、タイムアウトによるリスタートは含まれず、サーバーによって要求されたりリスタートだけを対象にしています。

有効値: 0 ~ 3200

デフォルト値: 0

**time-to-connect**

サーバーから認証を得るために許容される時間数。

有効値: 1 ~ 60

デフォルト値: 9

**secondary-server-address:**

2 次認証サーバーのアドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

**Change**

**servers change** コマンドは、リモート・サーバー・プロファイルを変更するのに使われます。リモート・サーバー・プロファイルの説明は、**add** コマンドの項を参照してください。

構文:



**local** 認証、許可、および会計タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

**remote**

認証、許可、および会計タイプを、リモート・ユーザー・データベースを使用するように設定します。

**server id**

リモート・データベースの識別子を指定します。

**accounting** *authype*

ログイン、PPP、およびトンネルの会計タイプを設定します。 *Authype* は、次のどれか 1 つです。

**remote**

認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

**server id**

リモート・データベースの識別子を指定します。

**authentication** *authype*

ログイン、PPP、およびトンネルの認証タイプを設定します。 *Authype* は、次のどれか 1 つです。

**local** 認証タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

**remote**

認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

**server id**

リモート・データベースの識別子を指定します。

**authorization** *authype*

ログイン、PPP、およびトンネルの許可タイプを設定します。 *Authype* は、次のどれか 1 つです。

**local** 許可タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

**remote**

許可タイプを、リモート・ユーザー・データベースを使用するように設定します。

**server id**

リモート・データベースの識別子を指定します。

## Tunnel

**tunnel** コマンドは、L2TP トンネル用の AAA を構成するのに使用します。

262ページの表34 は、**tunnel** コマンドと共に使用できるサブコマンドを示しています。

表 34. トンネル・サブコマンド

コマンド	機能
Disable	L2TP トンネルの会計を使用不可にします。
List	L2TP トンネル用の AAA 構成パラメーターを表示します。
Set	L2TP トンネル用の AAA 構成パラメーターを設定します。

## Disable

**tunnel disable** コマンドは、L2TP トンネルの会計を使用不可にするのに使用します。

構文:

```
tunnel disable           accounting
```

## List

**tunnel list** コマンドは、L2TP トンネル用の AAA を表示するのに使用します。

構文:

```
tunnel list             all
                        accounting
                        authentication
                        authorization
                        config
```

## Set

**tunnel set** コマンドは、L2TP トンネル用の AAA 構成パラメーターを設定するのに使用します。

構文:

```
tunnel set             aaa
                        accounting
                        authentication
                        authorization
```

### aaa authtype

認証、許可、および会計タイプを設定します。 *Authtype* は、次のどれか 1 つです。

**local** 認証、許可、および会計タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

### remote

認証、許可、および会計タイプを、リモート・ユーザー・データベースを使用するように設定します。

### server id

リモート・データベースの識別子を指定します。

**accounting** *authype*

会計タイプを設定します。 *Authype* は、次のどれか 1 つです。

**remote**

認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

**server id**

リモート・データベースの識別子を指定します。

**authentication** *authype*

認証タイプを設定します。 *Authype* は、次のどれか 1 つです。

**local** 認証タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

**remote**

認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

**server id**

リモート・データベースの識別子を指定します。

**authorization** *authype*

許可タイプを設定します。 *Authype* は、次のどれか 1 つです。

**local** 許可タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

**remote**

許可タイプを、リモート・ユーザー・データベースを使用するように設定します。

**server id**

リモート・データベースの識別子を指定します。

## User-profiles

**user-profiles** コマンドは、`User profile config>` コマンド・プロンプトにアクセスするのに使用します。このプロンプトから、次のコマンドにアクセスできます。

表 35. ユーザー・プロファイル構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxiページの『ヘルプの入手』を参照してください。
Add	PPP ユーザー・プロファイルを追加します。
Change	PPP ユーザー・プロファイルを変更します。
Delete	PPP ユーザー・プロファイルを削除します。
Disable	PPP ユーザー・プロファイルを使用不可にします。
Enable	PPP ユーザー・プロファイルを使用可能にします。
List	PPP ユーザー・プロファイル情報を表示します。
Report	PPP ユーザー・プロファイル・レポートを生成します。
Reset-user	PPP ユーザー・プロファイルをリセットします。
Exit	直前のコマンド・レベルに戻ります。 xxxiiページの『下位レベル操作環境の終了』を参照してください。

## Add

**user profiles add** コマンドは、リモート・ルーターのユーザー・プロファイルをローカル PPP ユーザー・データベースに追加したり、IP ネットワークを通したルーターへのトンネル・ピア間アクセスを指定するのに使用します。

構文:

```
add                ppp-user
                    tunnel
```

### ppp-user

リモート・ルーターのユーザー・プロファイルを、ローカル PPP ユーザー・データベースに追加します。最大 500 のユーザーを追加できます。構成している装置に接続できる各リモート・ルーターまたは DIALS クライアントの PPP ユーザーを追加します。

コマンド構文およびオプションについては、*アクセス・インテグレーター・サービス ソフトウェア使用者の手引き* の “CONFIG プロセス (CONFIG - Talk 6) およびコマンド” の章の Add の項を参照してください。

例:

```
Config> add ppp-user
Enter name: [ ]? pppusr01
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [yes]
Will user be tunneled? (Yes, No): [No]
Number of days before account expiry[0-1000] [0]? 10
Number of grace logins allowed after an expiry[0-100] [0]? 5
IP address: [0.0.0.0]? 1.1.1.1
Set ECP encryption key for this user? (Yes, No): [No] no
Disable user ? (Yes, No): [No]
```

```
      PPP user name: pppusr01
      User IP address: 1.1.1.1
      Virtual Conn: disabled
      Encryption: disabled
      Status: enabled
      Login Attempts: 0
      Login Failures: 0
      Lockout Attempts: 0
      Account expires: Sun 17Feb2036 06:28:16
      Account duration: 10 days 00.00.00
      Password Expiry: <unlimited>
```

User 'pppusr01' has been added

例:

```
Config> add ppp-user
Enter name: [ ]? tunusr01
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [yes]
Will user be tunneled? (Yes, No): [No] yes
Enter hostname to use when connection to this peer: []? host01
Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1
```

```
--more--          PPP user name: tunusr01
--more--          Endpoint: 1.1.1.1
--more--          Hostname: host01
```

User 'tunusr01' has been added

**tunnel** IP ネットワークを通したルーターへのトンネル・ピア間アクセスを指定します。これにより、ピアはルーターへのトンネル PPP セッションを開始することが許可されます。

コマンド構文およびオプションについては、 *アクセス・インテグレーター・サービス ソフトウェア使用者の手引き* の “CONFIG プロセスの構成” の章の Add の項を参照してください。

例:

```
Config> add tunnel
Enter name: []? tunnel02
Enter hostname to use when connecting to this peer: []? host02
Set shared secret? (Yes, No): [No]? yes
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 2.2.2.22

Tunnel name: tunnel02
Endpoint: 2.2.2.22
```

## Change

**change** コマンドは、ユーザー・プロファイルを変更するのに使用します。

構文:

```
change                ppp-user
                        tunnel
```

## Delete

**delete** コマンドは、ユーザー・プロファイルを削除するのに使用します。

構文:

```
delete                ppp-user
                        tunnel
```

## Disable

**disable** コマンドは、ユーザー・プロファイルを使用不可にするのに使用します。

構文:

```
disable                name
```

## Enable

**enable** コマンドは、ユーザー・プロファイルを使用可能にするのに使用します。

構文:

```
enable                name
```

## List

**list** コマンドは、ユーザー・プロファイル情報を表示するのに使用します。

構文:

```
list                ppp-user
                    tunnel

User profile config> list ppp-user
List (Name, Verb, User, Addr, Encr, zdump): [Verb]
  PPP user name: ppp01
    Expiry: <unlimited>
  User IP address: Interface Default
    Encryption: Not Enabled
    Status: Enabled
  Login Attempts: 0
  Login Failures: 0
  Lockout Attempts: 0
1 record displayed.
```

**List** リスト情報にアクセスする方法を指定します。

有効値: name, verb, user, addr, encr, zdump

デフォルト値: verb

### PPP user name

ユーザー名を表示します。

### Expiry

有効期限を表示します。

### User IP address

ユーザー IP アドレスを表示します。

### Encryption

暗号化が使用可能か使用不可かを表示します。

### Status

状態が使用可能か使用不可かを表示します。

### Login attempts

ユーザーがログインを試行した回数を表示します。

### Login failures

ログインに失敗した試行回数を表示します。

### Lockout attempts

ロックアウトの試行回数を表示します。

## Report

**report** コマンドは、PPP ユーザー・プロファイル・レポートを生成するのに使用します。

構文:

```
report             addresses
                    all
```



```

        _callback
        _dump
        _encrypt
        _name
        _password
        _time
        _user
User profile config> report addresses
PPP user name      User IP address
-----
ppp01              Interface Default
1 record displayed.
User profile config> report all
  PPP user name: ppp01
    Expiry: <unlimited>
  User IP address: Interface Default
    Encryption: Not Enabled
    Status: Enabled
  Login Attempts: 0
  Login Failures: 0
  Lockout Attempts: 0
1 record displayed.
User profile config> report callback
PPP user name      Callback type      Phone Number
-----
ppp01
1 record displayed.
User profile config> report dump
Enter user name: []? user01
User profile config> report encrypt
PPP user name      Encryption
-----
ppp01              Not Enabled
1 record displayed.
User profile config> report name
PPP user name
-----
ppp01
1 record displayed.
User profile config> report password
PPP user name      Expiry      Grace
-----
ppp01              <unlimited>
1 record displayed.
User profile config> report time
PPP user name      Time allotted
-----
ppp01
1 record displayed.
User profile config> report user
Enter user name: []? login01
  PPP user name: login01
    Expiry: <unlimited>
  User IP address: Interface Default
  Encryption: Not Enabled

```

## 認証の構成

### Reset-user

**reset-user** コマンドは、ユーザー・プロフィールをリセットするのに使用します。

構文:

**reset-user** *name*

## 第17章 暗号化プロトコルの使用および構成

注: 暗号化サポートは任意選択なので、**load add** コマンドを使用してソフトウェア・ロードに追加する必要があります。アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の CONFIG プロセス **load** コマンドの項を参照してください。

ルーター内での多重暗号化の使用 (IP セキュリティー・レイヤーとフレーム・リレーまたは PPP のデータ・リンク・レイヤーの両方で暗号化を使用すること) は、米国政府の輸出規制によって制限されます。多重暗号化は、厳密な輸出管理下にあるソフトウェア・ロード (128 ビット・キーと三重 DES を使用する RC4 をサポートするソフトウェア・ロード) だけでサポートされます。

暗号化の目的は、プライバシーを保証するために、データを読み取り不能な形にして転送することです。**暗号化された** データは、元のデータを入手するためには、暗号化解除する必要があります。

2212 は、次のものをサポートしています。

- PPP インターフェース上の Microsoft ポイント・ポイント暗号化 (MPPE) 用の 40 および 128 ビット・キーを備えた RC4 暗号化アルゴリズム
- RCF 1968 および 1969 に記述されている PPP 暗号制御プロトコルをサポートする 56 ビット・キーを備えた暗号化ブロック・チェーン方式のデータ暗号化規格 (DES-CBC) アルゴリズム
- フレーム・リレーの暗号化用の 40 ビット・キーを使用する商業データ・マスキング・ファシリティー (CDMF)。このサポートは専有です。
- フレーム・リレーは、三重 DES と 128 ビット・キーも使用します。

### 暗号化制御プロトコルを使用した PPP の暗号化

暗号化制御プロトコル (ECP) は、PPP プロトコルを使用したポイントツーポイント・リンク通信で、ルーターが暗号化の使用をネゴシエーションするのに使用します。暗号化制御プロトコルは、PPP リンク上で使用する暗号化および暗号化解除アルゴリズムをネゴシエーションするための汎用機構を提供します。PPP リンクの各方向でそれぞれ異なる暗号化アルゴリズムをネゴシエーションすることも可能です。

暗号化と暗号化解除の方式を**暗号化アルゴリズム**と言います。暗号化アルゴリズムは、キーを使用して、暗号化と暗号化解除を制御します。圧縮とは異なり、ルーターはリンクの両方向で暗号化を行います。一方向だけの暗号化はセキュリティ上の危険があるからです。ECP が両方向の暗号化アルゴリズムをネゴシエーションできない場合、リンクは終了します。

### PPP の ECP 暗号化の構成

データ・リンク・レイヤーで暗号化を使用するように装置を構成するには、次の手順で行います。

1. リモート装置およびローカル PPP インターフェースの暗号化キーを設定する。

リモート装置の暗号化キーは、Config > プロンプトで **add ppp-user** コマンドを使用して設定します。コマンド構文およびオプションについては、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの“CONFIG プロセスの構成”の章の **Add** コマンドの項を参照してください。

ローカル PPP インターフェースの暗号化キーは、**enable ecp** コマンドを使用して設定します (アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの talk 6 PPP Config> **enable** コマンドの項を参照してください)。

2. PPP Config> プロンプトで **enable ecp** コマンドを使用して、個々の PPP リンクが暗号化制御プロトコル (ECP) を使用するように構成する。
3. PAP、CHAP、または SPAP を使用可能にする。

暗号化を使用不可にする、ユーザーの暗号化キーを変更する、暗号化の状態をリストする、あるいは暗号化を要求するときに装置が使用する名前を設定するといったことも可能です。詳しくは、次を参照してください。

- 暗号化を使用不可にする方法については、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの PPP Config> **disable ecp** コマンドの項を参照してください。
- リモート・ユーザーの暗号化キーおよびパスワードを変更する方法については、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの Config> **change ppp-user** コマンドの項を参照してください。
- 暗号化の状況を表示する方法については、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの PPP Config> **list ecp** コマンドの項を参照してください。
- 装置の名前を設定する方法については、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの PPP Config> **set name** コマンドの項を参照してください。

## PPP の ECP 暗号化の監視

インターフェース上の各種の暗号化設定を監視するには、次のようにします。

1. **talk 5** コマンドを使用して、監視プロンプトにアクセスする。
2. **network** コマンドを使用して、監視するインターフェースを選択する。このコマンドを使用すると、PPP n> プロンプトが表示されます (ただし、n はネットワーク番号を表します)。 **network** コマンドの使用について詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの『ポイント・ポイント・プロトコル・インターフェースの構成および監視』を参照してください。

このプロンプトから、次のことが行えます。

- 暗号化の現行状態、最新の暗号化のネゴシエーション、暗号化状態変更以降の経過時間、および暗号化機能によって使用されているアルゴリズムを表示する。(アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの **list control ecp** コマンドの項を参照してください。)
- インターフェースで送受信された暗号化制御パケットを表示する。(アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの **list ecp** コマンドの項を参照してください。)
- インターフェースで送信または受信された、暗号化されたデータ・パケットを表示する。(アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの **list edp** コマンドの項を参照してください。)

---

## Microsoft ポイントツーポイント暗号化 (MPPE)

Microsoft ポイントツーポイント暗号化 (MPPE) は、Microsoft ダイアルアップ・ネットワークワーキング (DUN) クライアントと呼ばれる Windows ワークステーションが、それ自体と 2212 の間で PPP リンクを介して転送するデータを暗号化する手段を提供します。MPPE は、ルーターからルーターへ PPP リンクを介して転送されるデータを暗号化するのにも使用できます。MPPE は常に両方向でネゴシエーションされます。

MPPE は、シークレット・キー・アルゴリズムを使用して暗号化を行います。シークレット・キー・アルゴリズムは、暗号化と暗号化解除に同じキーを使用します。このキーはユーザーによって構成されませんが、送信側と受信側のワークステーション間での MPPE のネゴシエーションのプロセスで生成されます。MPPE を使用するには、認証プロトコルの Microsoft チャレンジ / ハンドシェイク認証プロトコル (MS-CHAP) を構成する必要があります。

PPP インターフェースを MS-CHAP で認証する場合、ルーターは『Microsoft モード』に入り、圧縮が使用可能な場合は MPPC だけをネゴシエーションし、暗号化が使用可能な場合は MPPE だけをネゴシエーションします。『Microsoft モード』では、ルーターは圧縮アルゴリズムの優先順位リストを無視し、ECP ネゴシエーションを使用不可にします。

### MPPE の構成

MPPE を構成するには、各インターフェースごとに次のステップを実行する必要があります。

1. MS-CHAP を構成する。MS-CHAP の使用および構成に関する情報は、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の『Microsoft PPP CHAP 認証 (MS-CHAP)』 および『ポイント・ポイント・プロトコル・インターフェースの構成および監視』を参照してください。
2. ルーターとルーターの間の接続を構成している場合は、**set name** コマンドを使用して、ローカル PPP インターフェースの名前を設定する (アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の PPP Config> **set name** コマンドの項を参照してください)。
3. データ圧縮が必要な場合は、PPP Config> プロンプトで talk 6 **enable ccp** コマンドを使用して、MPPC を使用可能にする。MPPE は、データ圧縮を必要としません。
4. MPPE を使用可能にする。PPP Config> プロンプトで **enable mppe** コマンドを使用します (アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の PPP Config> **enable** コマンドの項を参照してください)。
5. ルーターをリスタートして、構成を活動化する。

MPPE を使用不可にしたり、MPPE オプションをリストすることもできます。

- MPPE を使用不可にするには、PPP Config> プロンプトで talk 6 **disable mppe** コマンドを使用します。
- 構成された MPPE オプションを表示するには、PPP Config> プロンプトで talk 6 **list ccp** コマンドを使用します。

## MPPE の監視

270ページの『PPP の ECP 暗号化の監視』の説明に従って、PPP> プロンプトを立ち上げます。MPPE データ統計を見るには **list mppe** コマンドを使用し、MPPE 状況を見るには **list control ccp** コマンドを使用します。これらのコマンドの出力の例は、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の『ポイント・ポイント・プロトコル・インターフェースの構成および監視』の章に示されています。

---

## フレーム・リレー・インターフェース上の暗号化の構成

注: フレーム・リレーは、専有の暗号化方式を使用します。

データ暗号化は、暗号化が使用可能にされているすべてのインターフェースでサポートされます。暗号化が使用可能にされているインターフェース上の個々の回線を必要に応じて、暗号化を実行する、または実行しないとして個別に構成することができます。

フレーム・リレー・リンク上で暗号化を使用するように装置を構成するには、次の手順で行います。

1. **talk 6** コマンドを使用して、フレーム・リレー構成プロンプトにアクセスする。
2. **net #** コマンドを使用して、暗号化を可能にしたいフレーム・リレー・インターフェースを選択する。
3. **enable encryption** コマンドを使用して、フレーム・リレー・インターフェース上の暗号化を使用可能にする。アクセス・インテグレーター・サービス ソフトウェア使用者の手引き のフレーム・リレー構成コマンドの項を参照してください。
4. **add permanent-virtual-circuit** コマンドを使用して、暗号化が可能なパーマネント・バーチャル・サーキットを追加し、各 PVC ごとに暗号化キーを定義する。アクセス・インテグレーター・サービス ソフトウェア使用者の手引き のフレーム・リレー構成コマンドの項を参照してください。
5. 構成する各暗号化可能インターフェースごとに、ステップ 1 ~ 4 を繰り返す。

注: FR パーマネント・バーチャル・サーキットの暗号化が使用可能にされている場合、バーチャル・サーキットの反対側の装置との暗号化のネゴシエーションが正常に行われれない限り、データは回線上に流れません。暗号化キーを入力するためには PVC を構成する必要があるため、暗号化は孤立回線に対してはサポートされません。

インターフェースの暗号化を使用不可にする、PVC の暗号化の設定値を変更する、あるいは暗号化の状態を表示することもできます。詳しくは、次の個所を参照してください。

- インターフェースの暗号化を使用不可にする場合は、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き のフレーム・リレー構成 **disable encryption** コマンドの項を参照してください。
- PVC の暗号化の設定を変更する場合は、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き のフレーム・リレー構成 **change permanent-virtual-circuit** コマンドの項を参照してください。

- 暗号化の状態を表示する場合は、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き のフレーム・リレー構成 **list all**、**list lmi**、および **list permanent-virtual-circuit** コマンドの項を参照してください。

---

## フレーム・リレー・インターフェース上の暗号化の監視

インターフェース上の各種の暗号化設定を監視するには、次のようにします。

1. **talk 5** コマンドを使用して、監視プロンプトにアクセスする。
2. **network #** コマンドを使用して、監視したいインターフェースを選択する。このコマンドを使用すると、FR *x*> プロンプトが表示されます。

このプロンプトから、インターフェース、PVC、または回線の暗号化の現行状態を表示することができます。アクセス・インテグレーター・サービス ソフトウェア使用者の手引き のフレーム・リレー監視 **list** コマンドを参照してください。





## 第18章 ポリシー機能の使用

この章では、ポリシー機能と他のルーター・ソフトウェア・コンポーネントが相互作用して、QOS またはセキュリティ (あるいはその両方) に関する決定を行う方法を説明します。ポリシー機能に関連した概念と、それぞれの構成コマンドについても説明します。ポリシー機能では、LDAP ディレクトリー・サーバーをポリシー情報の中央リポジトリーとして使用することもできます。LDAP 機能を使用可能にするために必要な概念と構成手順についても、この章で説明されています。次に、これらの概念と、ルーターがポリシーを実施する方法を説明し、さらに例を示しています。

- 『ポリシーの概説』
- 283ページの『LDAP とポリシー・データベースの対話』
- 287ページの『規則の生成』
- 288ページの『構成例』

### ポリシーの概説

ポリシー機能を使用すれば、ネットワークの IPv4 トラフィックの管理が容易になります。ポリシーは、非常に単純なフィルター規則 (ドロップまたはパス) に従って構成することも、複雑なセキュリティと QOS のシナリオに従って構成することもできます。ポリシーの組み合わせによって、ルーターがネットワークの IPv4 トラフィックを処理する方法が決定されます。

### ポリシーの決定と実施

本ルーター・ファミリーでのポリシーの設定が、ポリシーの決定とその実施方法の基礎になっています。これらの概念は、ポリシー決定ポイント (PDP) およびポリシー実施ポイント (PEP) と呼ばれます。

ルーターのメモリーに常駐するポリシー・データベースは、ローカル構成からロードされたポリシーと、LDAP から読み取られたポリシーからなります。ポリシー・データベースは、次の条件によって構築されます。

- 装置の再ロードまたはリスタート
- Talk 5 **reset database** コマンド
- 自動リフレッシュ
- SNMP set 要求

ポリシー・データベースは、PDP として機能します。データベースは、ポリシー機能に関連したコンポーネントがパケットを処理する方法を決定する一連のポリシーで構成されます。ポリシーによって決定が下されると (時刻、IP パケット情報、識別のようなプロトコル固有の情報などに基づいて)、その決定はアクションを実行するために実施コンポーネント (PEP) にパスされます。276ページの図26 は、これらのコンポーネントの関係を示しています。

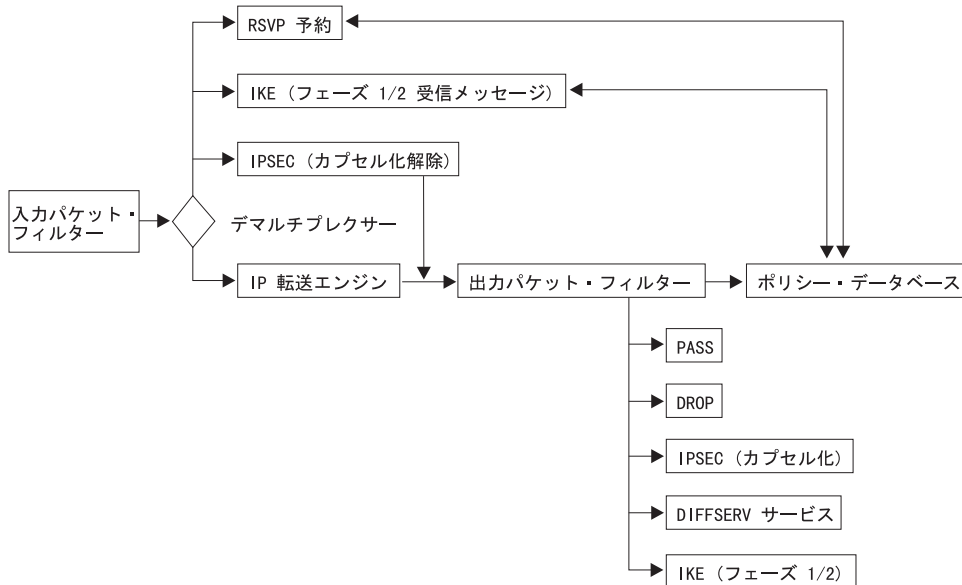


図 26. IP パケットのフローとポリシー・データベース

## ポリシーの決定とパケットのフロー

他のアクションが行われる前に、まず IP パケットは入力パケット・フィルタをパスする必要があります。入力パケット・フィルタに規則が存在する場合は、パケットに対して何らかのアクションが行われる場合があります。パケットを除外するフィルタがある場合、または入力パケット・フィルタに一致が検出されなかった場合は、パケットはドロップされます。

パケットが入力パケット・フィルタをパスすると、次は多重化解除フィルタに進み、パケットのあて先がローカルであるかどうかを検査されます。ローカルであれば、パケットはパケットのタイプに応じて他のモジュールにパスされます。これらのモジュールは、IPSec、IKE、RSVP などです。パケットのあて先がローカルの IPSec、IKE、または RSVP の場合、これらのモジュールはポリシー・データベースに照会して実行するアクションを決定します。

パケットのあて先がローカルでなければ、パケットは転送エンジンにパスされ、ルーティング決定が下されます。ルーティング決定によってパケットがドロップされない場合 (ポリシー・ベース・ルーティングによってパケットのドロップが決定される場合があります)、パケットは出力パケット・フィルタに進みます。出力パケットにフィルタ規則が存在する場合は、パケットに対してアドレス変換 (NAT) が実行されるか、パケットがパスされるか、またはドロップされます。フィルタ規則が存在しなければ、パケットはパスされます。フィルタ規則が存在し、一致が検出されない場合は、パケットはドロップされます。パケットが出力パケット・フィルタをパスした場合、IP エンジンはポリシー・データベースに照会して、このパケットに対して他のアクションを実行する必要があるかどうかを判別します。

**注:** インターフェースで入出力パケット・フィルタが使用可能になっていて、ポリシー・データベースによって制御されるパケットがこれらのインターフェースを通過する場合は、ポリシー・データベースが照会される前にパケットがドロップされないように、これらのパケットを含むフィルタ規則が入出力パケ

ット・フィルターに存在している必要があります。お勧めする方法の 1 つは、ポリシー・データベースを使用してパス/ドロップ規則をすべて構成し、パケット・フィルターを使用しないことです。

## IP のポリシー照会

IP 転送エンジンがポリシー・データベースを照会すると、次のような決定の組み合わせが戻されます。

- 一致が検出されない - パケットをパスする
- 一致が検出された - パケットをドロップする
- 一致が検出された - パケットをパスする
- 一致が検出された - IPSec 手動トンネル x によってパケットを保護する
- 一致が検出された - IKE ネゴシエーション・トンネル x によってパケットを保護する
- 一致が検出された - フェーズ 1 および 2 の ISAKMP ネゴシエーションを開始し、パケットをドロップする
- 一致が検出された - DiffServ QOS x を提供し、IPSec によってパケットを保護する

## IPSec のポリシー照会

IPSec がパケットを受け取った場合、IPSec はまずパケットのカプセル化を解除し、次にパケットが正しい IPSec トンネルに着信したかどうか判断する (よく適合性検査と呼ばれます) 必要があります。これは、ポリシー・データベースを照会することによって行われます。ポリシー・データベースは、この照会に対して次のような決定を戻します。

- 適合性検査を通過した - パケットを転送する
- 適合性検査に失敗した - パケットをドロップする

## IKE のポリシー決定

IKE がポリシー・データベースを照会すると、表36 に示すフェーズ 1 IP ポリシー決定を受け取ることができます。

表 36. IKE フェーズ 1 照会と、戻される決定

照会タイプ	決定
メッセージ 1 (メイン・モード)	一致が検出されず、パケットをドロップする
メッセージ 1 (メイン・モード)	一致が検出され、フェーズ 1 ポリシー x によってネゴシエーションする
メッセージ 5 (メイン・モード)	一致が検出されず、ピアとのネゴシエーションを停止して、パケットをドロップする
メッセージ 5 (メイン・モード)	一致が検出されず、ピアとのネゴシエーションを停止して、パケットをドロップする
メッセージ 5 (メイン・モード)	一致が検出され、ポリシー x と一致しており、フェーズ 1 を完了する
メッセージ 5 (メイン・モード)	一致が検出され、ポリシー y と一致しており、現在のフェーズ 1 を停止して、新しいポリシーを指定して新しいフェーズ 1 を開始する

## ポリシー機能の使用

表 36. IKE フェーズ 1 照会と、戻される決定 (続き)

照会タイプ	決定
メッセージ 1 (アグレッシブ・モード)	一致が検出されず、パケットをドロップする
メッセージ 1 (アグレッシブ・モード)	一致が検出され、ポリシー x と一致している

IKE がポリシー・データベースを照会すると、表37 に示すフェーズ 2 IP ポリシー決定を受け取ることができます。

表 37. IKE フェーズ 2 照会と、戻される決定

照会タイプ	決定
メッセージ 2 (応答側)	一致が検出されず、パケットをドロップする
メッセージ 2 (応答側)	一致が検出され、ポリシー x によってネゴシエーションする

### RSVP のポリシー決定

パケットが RSVP 制御メッセージならば、RSVP はポリシー・データベースを照会して、予約を受け入れるか拒否するかを決定します。予約を受け入れる場合は、RSVP はポリシーに基づいて予約のどの属性を制限するかを決定します。ポリシー・データベースのポリシーは、予約の期間、割り振る帯域幅の量、および保証する最小遅延を制御できます。

## ポリシー・オブジェクト

ポリシーはプロファイルからなっています。プロファイルは、決定の根拠となる一連のパケット属性、パケットの属性がプロファイルのものと一致した場合に実行するアクション、および決定を行いアクションを実行する期間である有効期間を指定します。これらの項目について、次に詳しく説明します。

ポリシーを構成するパーツは、個々の名前付きオブジェクトです。ポリシー・オブジェクトは互いを参照でき、関連した項目のグループとしてポリシーを構成します。構成情報を別々のオブジェクトに分離することによって、複数のポリシー定義でオブジェクトの多くを再使用できるので、時間の節約になり、保守作業が軽減されます。個々のポリシー・オブジェクトについて、次の項で詳しく説明します。

### ポリシー

ポリシー・オブジェクトは、チェックする条件、およびチェックが一致した場合に実行するアクションを記述します。ポリシーは、有効期間とプロファイルを名前によって参照します。ポリシーが有効であるためには、これらの参照が必要です。ポリシーは、IPSec 手動キー・トンネル・オブジェクト、IPSec アクション、ISAKMP アクション、RSVP アクション、または DiffServ アクションのうち、1 つまたは複数のアクションを名前によって参照する必要があります。有効な組み合わせは次のとおりです。

- IPSec 手動キー・トンネル
- パケットをドロップする IPSec アクション
- パケットをパスする IPSec アクション (セキュリティなし)
- パケットを保護する IPSec アクション、ISAKMP アクション
- DiffServ アクション (ドロップ)

- IPSec 手動キー・トンネルおよび DiffServ アクション (パス)
- パケットを保護する IPSec アクション、ISAKMP アクション、 DiffServ アクション (パス)
- RSVP アクション
- RSVP アクションと DiffServ アクション (パス)

**注:** これらの組み合わせのうち、IPSec 手動トンネルは IPSec アクション (IKE によってネゴシエーションされる IPSec トンネル) と同じポリシー定義に共存できず、RSVP アクションはどのような IPSec アクションとも関連付けてはなりません。パケットを保護する IPSec アクションをポリシーに関連付ける場合は、そのポリシーに ISAKMP アクションも関連付ける必要があります。

それぞれのポリシーには、優先順位番号も関連付けられています (優先順位属性の番号が大きいほど、優先順位が高くなります)。優先順位は、このポリシーが別のポリシーに優先されるかどうかを決定します。通常、優先順位を設定する必要があるのは、複数のポリシーのプロファイルが互いに何らかの競合を起こしている場合だけです。個別性の高いプロファイルをもつポリシーの優先順位を高くする必要があります。たとえば、あるポリシーはサブネット A からサブネット B へのトラフィックを IPSec (DES) によって保護するように指定していて、別のポリシーはポイント a' (サブネット A 内の特定のホスト) からサブネット B へのトラフィックを IPSec (3DES) によって保護するように指定しているとします。この場合、個別性の高いポリシー (a' から B) の優先順位を、A から B へのポリシーよりも高くする必要があります。

後で競合するポリシーに優先順位の値を追加指定するための余地ができるように、初期の優先順位の値は 5 つ以上離して指定することをお勧めします。それぞれのポリシーには使用可能属性もあります。これは、ポリシー・データベースにロードされたときにポリシーが使用可能になるかどうかを決定します。ポリシー・データベースの検索時に一致するポリシーが検出されても、ポリシーが使用不可になっている場合は、次に個別性の高いポリシーが実施されます。

## プロファイル

プロファイルは、特定のポリシーを選択するために使用する情報を決定します。プロファイルは、送信元アドレスとあて先アドレスの情報、プロトコル情報、および発信元とあて先のポート情報で構成されます。

**注:** IPSec/ISAKMP に関するポリシーを定義する際には、セキュリティーを提供するそれぞれのゲートウェイに、セキュリティーの関連を定義するポリシーが必要です。それぞれのゲートウェイのプロファイルは、送信元をあて先と関連付け、あて先を送信元と関連付ける必要があります。IPSec ポリシーのプロファイルは、トンネル内にカプセル化するトラフィックとして送信元アドレスを指定する必要があります。あて先アドレスはトンネルのリモート側になければなりません。

プロファイルは、サービス・タイプ (TOS) バイトと着発信 IP アドレスに基づいて選択を行うこともできます。デフォルトでは、任意の入力インターフェースに着信し、任意の出力インターフェースから発信するパケットが、他のセクターと突き合わせられます。場合によっては、パケットが着信するインターフェースと、パケ



## ポリシー機能の使用

ットが発信するインターフェースをはっきり指定できる柔軟さが必要になることがあります。この場合は、インターフェース・ペア・オブジェクトを追加して、インターフェース・ペア・オブジェクトのグループ名をプロファイルと関連付ける必要があります。インターフェース・ペア・オブジェクトをグループに割り当てるには、オブジェクトに同じ名前を指定します。こうすれば、(IPAddrX に着信し、任意のインターフェースから発信するパケット、または 任意のインターフェースに着信し、IPAddrX から発信するパケット) のような組み合わせを指定できます。これは、公衆インターフェースに一般的なドロップ規則を定義する場合に特に役立ちます。

**インターフェース・ペア:** 入力インターフェースと出力インターフェースを指定します。この選択対象のインターフェースの IP アドレスを指定します。値 255.255.255.255 は、任意のインターフェースを暗黙指定します。

プロファイルを使用して IPSec/ISAKMP ポリシーを選択する場合は、フェーズ 1 の間に送信するローカル ID と、フェーズ 1 ネゴシエーション時に受け入れ可能なリモート ID のリストを指定できます。デフォルトでは、ローカル ID は IPSec/IKE トラフィックのローカル・トンネル・エンドポイントで、リモート ID リストは任意です。オプションで、完全修飾ドメイン名 (FQDN)、ユーザー FQDN、およびキー ID を指定できます。ISAKMP フェーズ 1 ネゴシエーションの認証は、公用証明書、または事前に共有されているキーを使用して行われるので、通常はこれで十分です。ただし、リモート・アクセスのポリシーがあて先アドレスでないワイルドカードになっている状況では、ネットワーク資源へのアクセスを許可するリモート・アクセス・ユーザーのリストを指定した方がよい場合があります。

これらのユーザーは、通常の ISAKMP 認証方式によっても認証されます。ただしポリシー・データベースは、リモート・ピアによって送信されたローカル ID が、ポリシーのプロファイルのリモート・ユーザー・グループに指定された ID の 1 つと一致しているかどうかを確認する認証ステップを余分に実行します。これは、公用の認証局 (CA) が一般の人々の証明書を管理していて、ネットワーク管理者がこれらのユーザーのうち特定の集合 (たとえば、企業の従業員) だけにアクセスを許可したい場合に必要です。リモート・ユーザー・グループは、同じグループに属するユーザーのリストで構成されます。これらのユーザーは、1 つまたは複数の USER を追加することによってグループに入ります。ユーザーのグループが、それぞれのユーザーのグループ名を同じにしていることがあります。この場合、このグループをオプションでプロファイルに関連付けることができます。

### 有効期間

有効期間は、ポリシーが効力を持つ期間、つまりポリシーが有効である年、月、日、および時間を指定します。この柔軟さにより、たとえば『常時』、あるいは『今年だけ、1 月、2 月、3 月の間、月～金曜日、午前 9 時～午後 5 時』のように、ポリシーが有効になる時期を指定できます。ポリシー・データベースのポリシーが無効になると、次に個別性の高いポリシーが実施されます。したがって、月～金曜日の午前 9 時～午後 5 時まではサブネット A からサブネット B へのトラフィックをすべて保護し、その他の時間はサブネット A からサブネット B へのトラフィックをすべてドロップするように定義できます。この場合、最初のポリシーの優先順位を高くする必要があります (Talk 5 **add policy** コマンドを入力すると指定されます)。

## DiffServ アクション

DiffServ アクションは、DiffServ アクションを指定しているポリシーに一致したパケットに提供するサービス品質を記述します。パケットをドロップするように DiffServ アクションを構成することもでき、DiffServ アクションを使用して、関連したサービス品質にパケットをマップすることもできます。割り振る帯域幅は、出力帯域幅のパーセンテージとして構成するか、Kbps 単位の絶対値として構成できます。best effort/保証待ち行列、またはプレミアム待ち行列のどちらが帯域幅の割り振りを行うかを指定する必要があります。これらの待ち行列の詳細と定義方法については、385ページの『第22章 差別化サービス機能の使用』、および 391ページの『第23章 差別化サービスの構成と監視』を参照してください。

DiffServ アクションは、発信インターフェースから送信される前に TOS バイトにマークを付ける方法も指定します。デフォルトでは、TOS バイトにマークは付けられません。IP パケット・ヘッダーの情報に基づいて、ネットワーク内のある点でパケットにマークを付けると便利です。TOS バイトにすでにマークが付けられているので、種別が判別されたら、ネットワークの残りのホップでは新しい TOS バイトを探すだけでパケットに適用する QOS を判別できます。TOS バイトだけを探す方法は非常に効率的で、DiffServ バックボーンでハイパフォーマンスを実現するために必要です。

## RSVP アクション

RSVP アクションは、RSVP の予約が発生していて、予約要求がポリシーのプロファイルと一致している場合に、RSVP フローを許可するか拒否するかを指定します。予約を許可する場合、RSVP アクションは許可される予約期間、許可される帯域幅、および DiffServ アクションの参照 (オプション) も指定します。DiffServ アクションを参照すると、RSVP はルーターからパケットが発信される前に TOS バイトにマークを付ける方法を判別できます。これは、パケットが RSVP ネットワークから DiffServ ネットワークに渡される場合に役立ちます。RSVP は RSVP 境界まで QOS を提供でき、その後は TOS バイトに適切にマークを付ければ、DiffServ ネットワークが正しい帯域幅を適用できます。

## IPSec アクション

IPSec アクションは、ドロップ、パス、または保護のどれかのアクションを指定できます。アクションがドロップの場合は、このポリシーに一致するパケットがすべてドロップされます。アクションがセキュリティーなしのパスの場合は、パケットはすべてそのままパスされます。アクションがセキュリティーありのパスの場合は、パケットはこのアクションによって指定されたセキュリティー・アソシエーション (SA) によってすべて保護されます。IPSec アクションには、IPSec トンネルと IKE SA のトンネル・エンドポイントの IP アドレスも指定されます。

SA の属性は、IPSec アクションが参照する IPSec プロポーザルによって決定されます。IPSec アクションは複数の IPSec プロポーザルを指定でき、これらのプロポーザルは指定順に検査されます。IPSec アクションに複数のプロポーザルを指定することで、許容されるセキュリティーの組み合わせをすべて構成に含めることができるので、VPN ゲートウェイ間の構成の不一致を減らすことができます。

### IPSec プロポーザル

IPSec プロポーザルには、ESP または AH (またはその両方) のどの変換を提示するか、またはフェーズ 2 ISAKMP ネゴシエーション時に検査するかに関する情報があります。パーフェクト・フォワード・セクレシー (新規の Diffie Hellman 計算) が必要な場合、IPSec プロポーザルは使用する DH グループを指定します。IPSec プロポーザルが参照する変換は、指定順に送信または検査されます。使用するのがもっとも適切な ESP 変換または AH 変換をリストの最初にする必要があります。リストに複数の変換がある場合は、それぞれがピアの変換のリストと比較され、一致を検索されます。構成された変換がピアのリストと一致しない場合は、ネゴシエーションは失敗します。IPSec プロポーザルは、AH 変換と ESP 変換を組み合わせて表示できますが、有効な組み合わせは次のものだけです。

- AH だけのリスト (トンネル・モードまたはトランスポート・モード)
- ESP だけのリスト (トンネル・モードまたはトランスポート・モード)
- AH (トランスポート・モード) のリストと ESP (トンネル・モード) のリスト

### IPSec 変換

IPSec 変換の属性は、IPSec 暗号化に関する情報と、認証パラメーターを含んでおり、キーをリフレッシュする頻度も指定します。変換は、AH (認証だけ) または ESP (暗号化または認証、あるいはその両方) のどちらかであり、トンネル・モードまたはトランスポート・モードのどちらかで作動するように構成できます。

### ISAKMP アクション

ISAKMP アクションは、フェーズ 1 のキー管理情報を指定します。このアクションは、フェーズ 1 ネゴシエーションをメイン・モード (識別保護を提供する) で開始するか、アグレッシブ・モードで開始するかを指定します。フェーズ 1 セキュリティー・アソシエーションを装置の始動時にネゴシエーションするか、要求に応じてネゴシエーションするかも指定します。さらに ISAKMP アクションは、1 つまたは複数の ISAKMP プロポーザルを参照する必要があります。最初に参照するものは、もっとも望ましい ISAKMP プロポーザルでなければなりません。

### ISAKMP プロポーザル

ISAKMP プロポーザルは、フェーズ 1 セキュリティー・アソシエーションの暗号化と認証の属性を指定します。キーを生成するために使用する Diffie Hellman グループと、フェーズ 1 セキュリティー・アソシエーションの有効期間も指定します。ISAKMP プロポーザルの中で、認証方式を選択する必要があります。認証方式は、事前共有キー・モードまたは証明書モードのどちらかです。

### ユーザー

認証方式として事前共有キーを指定した ISAKMP ネゴシエーションを使用するポリシーに対しては、ユーザーを構成する必要があります。ユーザー構成は、ISAKMP ピアに対して使用する事前共有キーを指定します。ユーザー・オブジェクトには、リモート ISAKMP ピアの識別情報 (つまり IP アドレス)、FQDN、ユーザー FQDN またはキー ID、およびユーザーが認証に使用する方式が含まれています。認証方式は、事前共有キー・モードまたは証明書モードのどちらかです。事前共有キーを選択す

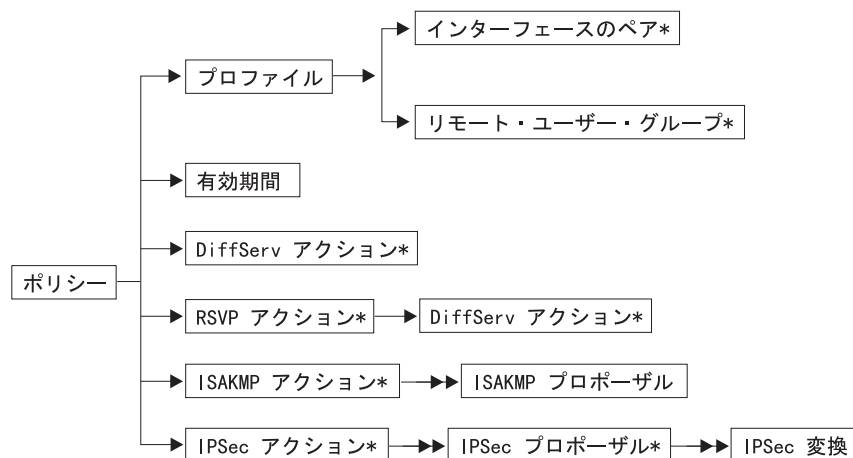


る場合は、事前共有キーを ASCII と 16 進数のどちらで入力するか、およびキーの値も指定する必要があります。ユーザーは、同じグループ名に割り当てることによってグループ化できます。オプションで、このグループをポリシーのプロファイルに関連付けると、フェーズ 1 のポリシー検索をより厳密に実行できます。

### IPSec 手動キー・トンネル

IPSec 手動キー・トンネルは、暗号化パラメーターと認証パラメーターの静的構成です。トンネルに対してネゴシエーションは実行されないため、両方のピアの構成はまったく同じでなければなりません。キーは実際にはこの構成の一部として入力され、トンネルの両側で一致している必要があります。このモードでは、ネゴシエーションは実行されないため、キーはリフレッシュされません。IPSec 手動キー・トンネルについて詳しくは、333ページの『第20章 IP セキュリティの使用』のIPSec機能の説明を参照してください。

図27 は、ポリシー構成オブジェクト間の関係を示しています。



注:

1. → は単一の参照を示します。
2. →▶ は複数の参照を示します。
3. \* はオプションの参照を示します。
4. ISAKMP/IPSec のセキュリティ・ポリシーでは、トラフィック・プロファイルがセキュア・トンネルに流れるトラフィックを定義します。

図 27. ポリシー構成オブジェクトの関係

## LDAP とポリシー・データベースの対話

本ルーター・ファミリーでは、LDAP サーバーをポリシー情報のリポジトリ (ポリシー・データベース) にすることができます。LDAP は、ディレクトリー・サーバーの検索と変更を可能にするプロトコルです。LDAP は X.500 標準の簡易バージョンです。ルーターは、ディレクトリー・サーバーの情報を検索する (ただし変更しない) 機能をサポートしています。ルーター内のポリシー検索エージェントが、その装置を対象にしたディレクトリー・サーバーにあるポリシー情報をすべて検索します。LDAP バージョン 2 または 3 で作動する LDAP サーバーはすべて、本ルーター内での設定に対応しています。構成をローカルに格納する従来の方法と比べて、ディレクトリー・サーバーを使用してポリシー情報を保管することの重要な利点は、変

## ポリシー機能の使用

更を 1 個所で行って、その変更を広いネットワークにあるすべての装置に適用できることです。これには、管理ドメインにある装置も、公衆境界を超えた装置も含まれます。

たとえば、ディレクトリーに IPSec 変換の定義が常駐しているとします。暗号化に関する企業のポリシーを DES から 3DES に変更する場合、通常はそれぞれのネットワーク構成にわたって、すべての装置構成を変更する必要があります。ディレクトリーを使用してポリシーを展開すれば、IPSec 変換を 1 つだけ変更すれば済みます。このとき、ネットワーク内のポリシーを使用可能にしているそれぞれの装置は、データベースを再作成する必要があります。別の例として、“GoldService” という名前の DiffServ アクションを変更して、帯域幅の値を帯域幅の 40% から 45% に増やしたいとします。LDAP サーバーとポリシー・インフラストラクチャーを使用すれば、これらのような構成変更をはるかに大規模に行うことができ、構成の不一致が減ります。

ネットワーク管理者ならば、毎日指定の時間にデータベースを自動リフレッシュする機能を利用することもできます。このオプションは、ポリシー機能の **set refresh** コマンドを入力することによって選択します。リフレッシュを使用可能にするか使用不可にするかを指定でき、使用可能にする場合は、データベースをリフレッシュする時刻を指定できます。このオプションは、変更を自動化する場合に便利です。たとえば、米国のマーケティング部門が日本の開発部門とインターネットを通じて話し合えるように新しいポリシーを追加する必要があり、セキュリティー・ゲートウェイは SG1 と SG2 であるとします。SG1 と SG2 の自動リフレッシュが使用可能になっていれば、この情報をディレクトリーに入力するだけで、真夜中に SG1 と SG2 は自動的にこの変更を選択します。

LDAP ポリシー検索エンジンを使用して、ポリシー・データベースの作成時に使用するセキュリティー・レベルを指定できます。これらのセキュリティー・オプションは、ポリシー機能の **set default** コマンドによって定義します。オプションは次のとおりです。

- 検索時にすべてのトラフィックをパスする (デフォルト)。
- LDAP ポリシー検索の要求と結果を除く すべてのトラフィックをドロップする。
- IPSec によって保護された LDAP ポリシー検索の要求と結果を除く すべてのトラフィックをドロップする。

状況によっては、最初の 2 つのオプションで十分な場合があります。ただし、LDAP トラフィックが公衆インフラストラクチャーを通過する場合は、3 番目のオプションを選択して情報を保護し、認証する必要があります。この場合、フェーズ 1 とフェーズ 2 の認証と暗号化のオプションを選択する必要があります。トンネル・エンドポイント (1 次と 2 次の LDAP サーバー) の IP アドレスも入力する必要があります。このブートストラップ IKE/IPSec トンネルは、LDAP トラフィックの送信前にネゴシエーションされます。この機能によって、285 ページの図 28 に示す構成を設定できます。

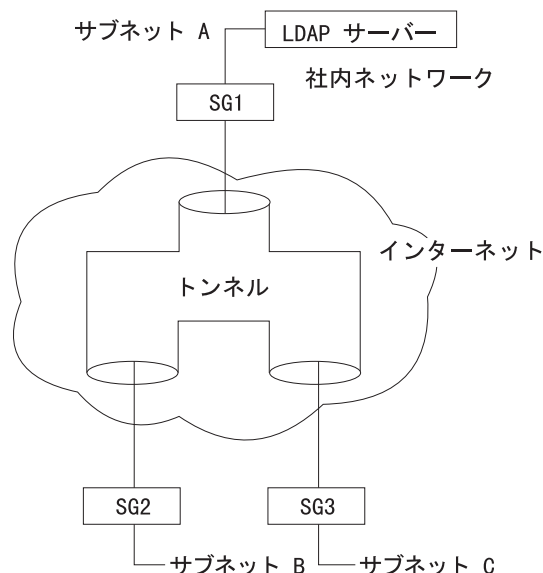


図 28. インターネットを経由するトラフィックの保護

この図は、社内ネットワークのサブネット A にある LDAP サーバーを示しています。SG1、SG2、および SG3 は、LDAP サーバーからポリシーを取り出します。SG2 と SG3 のポリシー検索はインターネット経由で行われ、IPSec によって保護されます。

ポリシー・データベースがディレクトリーからポリシーを正常に検索するために必要な構成情報は、次のとおりです。

- 1 次サーバーの IP アドレス (バックアップの 2 次サーバーも構成できます)
- サーバーが listen するポート番号 (注: SSL と TLS はサポートされません)
- ユーザー名とパスワード情報 (必要な場合)
- このルーター、またはルーターのクラスに対する DeviceProfile オブジェクトの基本識別名
- デフォルト・ポリシー情報

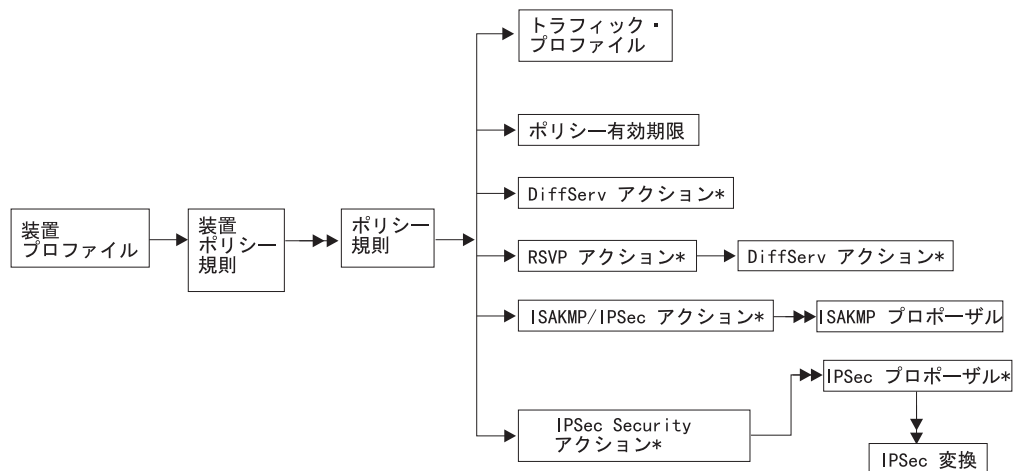
この構成情報を入力した後、次にポリシー・データベースがリフレッシュされるときに、ポリシー情報を得るためにディレクトリー・サーバーの照会が試行されます。ポリシー・データベースは、ローカルに構成されたポリシーと、LDAP サーバーから読み取られた規則の組み合わせができるようにします。2 つの規則が競合していることが検出され、これらの優先順位が同じである場合は、ローカル構成から読み取られた規則がディレクトリー・サーバーから読み取られた規則に優先されます。

## ポリシー・スキーマ

LDAP スキーマは、クラスを構成する規則と情報、およびディレクトリーのエントリーの内容を決定する属性定義のセットです。通常、LDAP スキーマは SNMP MIB と同様、ASN1 構文で作成されます。本ルーター・ファミリーがサポートするポリシー・スキーマは、IETF で行われている標準化前の段階の開発成果から構成されたものです。ポリシー・スキーマは、IPSec、IETF 内のポリシー・ワーキング・グループ、および DMTF 内のポリシー・ワーキング・グループによって行われている標準制定作業に基づいています。ポリシー・スキーマは、ルーターのポリシー機能にある既存

## ポリシー機能の使用

の構成オブジェクトに緊密に一致します。ポリシー・スキーマ定義ファイルと LDAP サーバー構成ファイルは、URL <http://www.networking.ibm.com/support> にアクセスすれば入手できます。お使いのルーター製品を選択してから、*Downloads* リンクを選択してください。図29 は、ポリシー・スキーマの全体的な構造を示しています。



注:

1. → は単一の参照を示します。
2. → は複数の参照を示します。
3. \* はオプションの参照を示します。
4. ISAKMP/IPSec のセキュリティー・ポリシーでは、トラフィック・プロファイルがセキュア・トンネルに流れるトラフィックを定義します。

図 29. ポリシー・スキーマの構造

DeviceProfile と DevicePolicyRules は、ポリシー・スキーマにある 2 つの重要なオブジェクトです。これらのオブジェクトによって、ポリシー検索エージェントは装置に必要なポリシーを見付けることができます。DeviceProfile には、装置の管理 IP アドレスに関する情報と、必須の DevicePolicyRules 参照があります。装置を 1 つの DeviceProfile にグループ化することも、ネットワーク内のそれぞれの装置が専用の DeviceProfile を持つこともできます。どちらを選択するかは、ネットワーク内の複数の装置が同じ規則のセットを取り出す必要があるかどうかによって決まります。通常、セキュリティー・ゲートウェイの場合は、すべてのゲートウェイのトンネル・エンドポイントが異なるので、これは当てはまりません。QOS だけの装置の場合は、グループ内のすべての装置が同じポリシーのセットを読み取ることが考えられます。

DevicePolicyRules オブジェクトは、装置のために取り出された DeviceProfile の値に基づいて検索されます。DevicePolicyRules オブジェクトが検出されたら、その装置の PolicyRules のリストを検索できます。オブジェクトが検出されなかった場合、またはオブジェクトに対する整合性検査中にエラーが検出された場合は、検索は打ち切れ、エラーを示すメッセージが ELS (PLCY メッセージ) に表示されます。エラーが発生した場合、ネットワーク管理者は次のどちらかの選択項目を構成して、エラーを処理できます。

- ローカルに読み取られたポリシーをすべて削除し、すべてドロップまたはすべてのパスの規則に復帰する

- ローカルに読み取られたポリシーをすべて保持する。このオプションは、ポリシー機能の **set default** コマンドと一緒に指定します。

どちらの場合も、構成された再試行間隔で検索が再度試みられます。1 次 LDAP サーバーと通信できない場合は、5 回の試行後に 2 次サーバーが試されます。2 次サーバーと通信できない場合は、5 回の試行後に 1 次サーバーが再度試されます。再試行間隔は、ポリシー機能の **set ldap retry-interval** コマンドを使用して指定できます。ネットワークの遅延のために検索が失敗する場合は、ポリシー機能の **set ldap search-timeout** コマンドを使用して、検索のタイムアウトをデフォルトの 3 秒から変更できます。

## 規則の生成

ネットワークの運用方法を指定するには、ポリシーを構成します。ルーターは、ポリシー情報を変換して、トラフィックのフローと比較する一連の規則にします。従来は、それぞれのトラフィック・パターンごとにインバウンドとアウトバウンドのパケット・フィルタを定義することによって、手作業でこれを行っていました。ポリシー・データベースを使用すれば、ただ 1 つのポリシーを構成するだけで済むので、この手間が省けます。

ほとんどの作業は、ポリシー・データベースが作成されるたびに内部で実行されます。場合によっては、ルーターがポリシーを単一の規則に直接変換します。ISAKMP/IPSec の場合は、ポリシーを 5 つの規則に変換します。5 つの規則は、トラフィックの方向 (着信と発信)、および IKE ネゴシエーションのフェーズ 1 とフェーズ 2 の間に発生する制御流れを記述するために必要です。ポリシーと規則との間の関係は、次のとおりです。

### 1 つの DiffServ ポリシー → 1 つの DiffServ 規則

### 1 つの RSVP ポリシー → 1 つの RSVP 規則

### 1 つの ISAKMP/IPSec ポリシー → 5 つの ISAKMP/IPSec 規則

例: サブネット A からサブネット B へのトラフィックを保護する。トンネル・エンドポイントは SGa と SGb

- フェーズ 1 インバウンド (プロファイル = SGb から SGa、Proto UDP、Src Port 500、Dst Port 500): この規則は、装置が ISAKMP 応答側として機能している場合に、リモート ISAKMP ピアから着信するフェーズ 1 ネゴシエーションをフィルタに掛けるために必要です。
- フェーズ 1 アウトバウンド (プロファイル = SGa から SGb、Proto UDP、Src Port 500、Dst Port 500): この規則は、トラフィックが ISAKMP フェーズ 1 ネゴシエーションを開始した場合に、フェーズ 1 情報をフィルタに掛けるために必要です。この場合、装置は ISAKMP 起動側として機能します。
- フェーズ 2 インバウンド (プロファイル = SGb から SGa、Proto UDP、Src Port 500、Dst Port 500): この規則は、リモート ISAKMP ピアから着信するフェーズ 2 トラフィックをフィルタに掛けるために必要です。このトラフィック



## ポリシー機能の使用

は、フェーズ 2 リフレッシュまたは初期ネゴシエーションを開始するリモート・ピアから生じます。アウトバウンド・トラフィック (規則 5) は、必要に応じて常にネゴシエーションを開始するので、フェーズ 2 アウトバウンド規則は必要ありません。

4. 保護トンネルへのトラフィック (プロファイル = サブネット A からサブネット B): この規則は、保護されないトラフィックを保護トンネルに入れるために必要です。セキュリティー・アソシエーションがネゴシエーション済みでない場合は、フェーズ 1 規則も収集され、IKE はフェーズ 1 とフェーズ 2 を開始します。SA が確立された後は、この規則に一致するパケットがカプセル化と伝送のために IPSec に渡されます。
5. 保護トンネルからのトラフィック (プロファイル = サブネット B からサブネット A): この規則は、保護トンネルに到着したはずのパケットが、実際に保護トンネルに到着したことを確認するために必要です。パケットが IPSec によってカプセル解除されていない場合にこの規則が適用されると、パケットはドロップされます。この規則は、ネットワーク内にスプーフィングされたトラフィックを処理します。

### 1 つの IPSec 手動キー・トンネル → 2 つの IPSec 規則

例: サブネット A からサブネット B へのトラフィックを保護する。トンネル・エンドポイントは SGa と SGb

1. 保護トンネルへのトラフィック (プロファイル = サブネット A からサブネット B): この規則は、保護されないトラフィックを保護トンネルに入れるために必要です。これは、静的に構成されたトンネルなので常に使用でき、この規則に一致するパケットは、カプセル化と伝送のために直接 IPSec に渡されません。
2. 保護トンネルからのトラフィック (プロファイル = サブネット B からサブネット A): この規則は、保護トンネルに到着したはずのパケットが、実際に保護トンネルに到着したことを確認するために必要です。パケットが IPSec によってカプセル解除されていない場合にこの規則が適用されると、パケットはドロップされます。この規則は、ネットワーク内にスプーフィングされたトラフィックを処理します。

これらの規則は、ポリシー機能の `Talk 5 list rule` コマンドを使用して表示できます。

---

## 構成例

次の例では、ポリシー機能を使用してネットワーク内のルーターを構成する方法を示します。まず、次のコマンドを入力してポリシー機能にアクセスします。

```
* talk 6
Config>feature policy
IP Network Policy configuration
```

## QOS を指定した IPSec/ISAKMP ポリシー

ポリシー情報は、2 つの方法のどちらかで入力できます。最初の方法は、個々のポリシー・オブジェクトを定義してから、それらをグループ化する方法です。この方法を使用するには、まず IPSec 変換を定義し、次に IPSec プロポーザル (IPSec 変換を

参照する) を定義します。その後、IPSec アクション (IPSec プロポーザルを参照する) を定義し、ポリシーの定義が完了するまで同様に行います。図30 を参照すると、この方法はポリシー・オブジェクトの右側から始まり、作業は左側に進みます。

2 番目の方法は、おそらくより簡単なもので、最初に高レベルのポリシー・オプションを定義し、プロンプトに応じて個々のポリシー・オブジェクトの定義を入力する方法です。構成手順の例は 図30 の後にあり、この図にある値に対応する値を使用しています。この方法は、左から右の方式を使用しており、**add policy** コマンドから始まります。

必要を満たすオブジェクトがすでに定義されている場合は、新しい定義を作成する代わりにそのオブジェクトを再利用できます。たとえば、以前のポリシー用に allTheTime の有効期間が構成されている場合は、それを再利用できます。次の手順は全体のプロセスを示していますが、すでに定義されたポリシー情報の再利用については説明していません。すでに定義された情報を使用する例については、297ページの『IPSec/ISAKMP だけのポリシー』を参照してください。

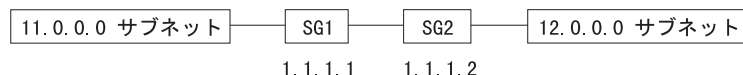


図30. QOS を指定した IPSec/ISAKMP の構成

次に説明するポリシー構成手順は、SG1 側から行います。ポリシーの記述は、次のとおりです。

トンネル・エンドポイントを SG1 と SG2 に指定してサブネット 11 からサブネット 12 へのトラフィックを保護し、DiffServ GoldService によってこのトンネルに QOS を提供する。

1. ポリシーを追加します。

```

Policy config>add policy
Enter a Name (1-29 characters) for this Policy []? examplePolicySecure11to12
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]? 10
  
```

2. プロファイルが構成されていないので、新しいものを定義する必要があります。

```

List of Profiles:
  0: New Profile

Enter number of the profile for this policy [0]?
  
```

3. 新規プロファイル定義。このケースでは、対象のトラフィックはサブネット 11 からサブネット 12 へのものです。

```

Enter a Name (1-29 characters) for this Profile []? trafficFrom11NetTo12Net
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]? 11.0.0.0
Enter IPV4 Source Mask [255.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]? 12.0.0.0
Enter IPV4 Destination Mask [255.0.0.0]?
  
```

```

Protocol IDs:
  1) TCP
  2) UDP
  3) All Protocols
  4) Specify Range
  
```

```

Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
  
```

## ポリシー機能の使用

```
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
Limit this profile to specific interface(s)? [No]:
```

Here is the Profile you specified...

```
Profile Name      = trafficFrom11NetTo12Net
sAddr:Mask=      11.0.0.0 : 255.0.0.0      sPort=   0 : 65535
dAddr:Mask=      12.0.0.0 : 255.0.0.0      dPort=   0 : 65535
proto            =                0 : 255
TOS              =                x00 : x00
Remote Grp=All Users
Is this correct? [Yes]:
```

4. プロファイル定義が完了し、ポリシー構成メニューに戻ります。

```
List of Profiles:
 0: New Profile
 1: trafficFrom11NetTo12Net
```

Enter number of the profile for this policy [1]? **1**

5. 有効期間が構成されていないので、新しいものを定義する必要があります。

```
List of Validity Periods:
 0: New Validity Period
```

Enter number of the validity period for this policy [0]?

6. 有効期間の構成に関する質問。この例では、有効期間は午前 9 時から午後 5 時、月～金曜日、1999 年のすべての月です。

```
Enter a Name (1-29 characters) for this Policy Valid Profile []?
MonToFri-9am:5pm-1999
```

Enter the lifetime of this policy. Please input the information in the following format:

```
yyymmddhhmmss:yyymmddhhmmss OR '*' denotes forever.
[*]? 19990101000000:19991231000000
```

During which months should policies containing this profile be valid. Please input any sequence of months by typing in the first three letters of each month with a space in between each entry, or type ALL to signify year round.

```
[ALL]?
```

During which days should policies containing this profile be valid. Please input any sequence of days by typing in the first three letters of each day with a space in between each entry, or type ALL to signify all week

```
[ALL]? mon tue wed thu fri
```

Enter the starting time (hh:mm:ss or \* denotes all day)

```
[*]? 00:00:00
```

Enter the ending time (hh:mm:ss)

```
[00:00:00]? 17:00:00
```

Here is the Policy Validity Profile you specified...

```
Validity Name     = MonToFri-9am:5pm-1999
Duration          = 19990101000000 : 19991231000000
Months           = ALL
Days             = MON TUE WED THU FRI
Hours            = 09:00:00 : 17:00:00
```

Is this correct? [Yes]:

7. 有効期間の定義が完了し、ポリシー構成メニューに戻りました。



List of Validity Periods:  
 0: New Validity Period  
 1: MonToFri-9am:5pm-1999

Enter number of the validity period for this policy [1]? **1**  
 Should this policy enforce an IPSEC action? [No]: **yes**

8. トンネル・エンドポイントは常に異なるので、常に新しい IPsec アクションを定義する必要があります。この例外は、同じ 2 つのゲートウェイ間に複数のトンネルがある場合と、トンネル・エンドポイントが不明であるワイルドカードを使用したリモート・アクセス構成の場合です。

IPSEC Actions:  
 0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?

9. IPsec アクションのメニュー。

Enter a Name (1-29 characters) for this IPsec Action []? **secure11NetTo12Net**  
 List of IPsec Security Action types:  
 1) Block (block connection)  
 2) Permit

Select the Security Action type (1-2) [2]? **2**  
 Should the traffic flow into a secure tunnel or in the clear:  
 1) Clear  
 2) Secure Tunnel

[2]?  
 Enter Tunnel Start Point IPV4 Address  
 [11.0.0.5]? **1.1.1.1**  
 Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)  
 [0.0.0.0]? **1.1.1.2**

Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:  
 Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?

Security Association Refresh Threshold, in percent (1-100) [85]?  
 Options for DF Bit in outer header (tunnel mode):  
 1) Copy  
 2) Set  
 3) Clear

Enter choice (1-3) [1]?  
 Enable Replay prevention (1=enable, 2=disable) [2]?  
 Do you want to negotiate the security association at  
 system initialization(Y-N)? [No]:  
 You must choose the proposals to be sent/checked against during phase 2  
 negotiations. Proposals should be entered in order of priority.

10. IPsec プロポーザルが定義されていないので、新しいものを定義する必要があります。いったん IPsec プロポーザルを定義すれば、複数の IPsec アクション間で再利用できることに注意してください。

List of IPSEC Proposals:  
 0: New Proposal

Enter the Number of the IPSEC Proposal [0]?

11. IPsec プロポーザルの構成。

Enter a Name (1-29 characters) for this IPsec Proposal []? **genP2Proposal**  
 Does this proposal require Perfect Forward Secrecy?(Y-N)? [No]:  
 Do you wish to enter any AH transforms for this proposal? [No]:  
 Do you wish to enter any ESP transforms for this proposal? [No]: **yes**

12. ESP 変換が構成されていないので、新しいものを定義する必要があります。いったん ESP 変換を定義すれば、任意の IPsec プロポーザルが変換を再利用できます。

## ポリシー機能の使用

```
List of ESP Transforms:  
  0: New Transform
```

```
Enter the Number of the ESP transform [0]? 0
```

### 13. IPSec 変換の構成。

```
Enter a Name (1-29 characters) for this IPsec Transform []? esp3DESswSHA
```

```
List of Protocol IDs:
```

- 1) IPSEC AH
- 2) IPSEC ESP

```
Select the Protocol ID (1-2) [1]? 2
```

```
List of Encapsulation Modes:
```

- 1) Tunnel
- 2) Transport

```
Select the Encapsulation Mode(1-2) [1]? 1
```

```
List of IPsec Authentication Algorithms:
```

- 0) None
- 1) HMAC-MD5
- 2) HMAC\_SHA

```
Select the ESP Authentication Algorithm (0-2) [2]? 2
```

```
List of ESP Cipher Algorithms:
```

- 1) ESP DES
- 2) ESP 3DES
- 3) ESP CDMF
- 4) ESP NULL

```
Select the ESP Cipher Algorithm (1-4) [1]? 2
```

```
Security Association Lifesize, in kilobytes (1024-65535) [50000]?
```

```
Security Association Lifetime, in seconds (120-65535) [3600]?
```

```
Here is the IPsec transform you specified...
```

```
Transform Name = esp3DESswSHA  
  Type =ESP   Mode =Tunnel   LifeSize=  50000 LifeTime=  3600  
  Auth =SHA   Encr =3DES
```

```
Is this correct? [Yes]:
```

### 14. IPSec プロポーザルのメニューに戻ります。

```
List of ESP Transforms:
```

- 0: New Transform
- 1: esp3DESswSHA

```
Enter the Number of the ESP transform [1]?
```

```
Do you wish to add another ESP transform to this proposal? [Yes]: no
```

```
Here is the IPsec proposal you specified...
```

```
Name = genP2Proposal  
  Pfs = N  
  ESP Transforms:  
    esp3DESswSHA
```

```
Is this correct? [Yes]:
```

### 15. IPSec アクションのメニューに戻ります。

```
List of IPSEC Proposals:
```

- 0: New Proposal
- 1: genP2Proposal

```
Enter the Number of the IPSEC Proposal [1]?
```

```
Are there any more Proposal definitions for this IPSEC Action? [No]:
```

```
Here is the IPsec Action you specified...
```

```
IPSECAction Name = secure11NetTo12Net  
  Tunnel Start:End = 1.1.1.1 : 1.1.1.2  
  Tunnel In Tunnel = No  
  Min Percent of SA Life = 75  
  Refresh Threshold = 85 %
```

```

Autostart                =                No
DF Bit                   =                COPY
Replay Prevention       =                Disabled
IPSEC Proposals:
genP2Proposal
Is this correct? [Yes]:

```

16. ポリシーのメニューに戻ります。

```

IPSEC Actions:
0: New IPSEC Action
1: secure11NetTo12Net

```

Enter the Number of the IPSEC Action [1]? 1

17. 保護タイプの IPSec アクションを指定したので、フェーズ 1 ネゴシエーションに対する ISAKMP アクションを指定する必要があります。何も定義されていないので、新しいものを入力する必要があります。ほとんどの場合、セキュリティー・ポリシーすべてに対して 1 つの ISAKMP アクションとプロポーザルで十分です。

```

ISAKMP Actions:
0: New ISAKMP Action

```

Enter the Number of the ISAKMP Action [0]?

18. ISAKMP アクションの構成。

Enter a Name (1-29 characters) for this ISAKMP Action []? genPhase1Action

List of ISAKMP Exchange Modes:

- 1) Main
- 2) Aggressive

Enter Exchange Mode (1-2) [1]?

Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?

ISAKMP Connection Lifesize, in kilobytes (100-65535) [5000]?

ISAKMP Connection Lifetime, in seconds (120-65535) [30000]?

Do you want to negotiate the security association at

system initialization(Y-N)? [Yes]: no

You must choose the proposals to be sent/checked against during phase 1 negotiations. Proposals should be entered in order of priority.

19. ISAKMP プロポーザルが構成されていないので、新しいものを作成する必要があります。

List of ISAKMP Proposals:

0: New Proposal

20. ISAKMP プロポーザルの構成。

Enter the Number of the ISAKMP Proposal [0]?

Enter a Name (1-29 characters) for this ISAKMP Proposal []? genP1Proposal

List of Authentication Methods:

- 1) Pre-Shared Key
- 2) RSA SIG

Select the authentication method (1-2) [1]? 2

List of Hashing Algorithms:

- 1) MD5
- 2) SHA

Select the hashing algorithm(1-2) [1]? 2

List of Cipher Algorithms:

- 1) DES
- 2) 3DES

## ポリシー機能の使用

```
Select the Cipher Algorithm (1-2) [1]? 2
Security Association Lifesize, in kilobytes (100-65535) [1000]?
Security Association Lifetime, in seconds (120-65535) [15000]?
```

```
List of Diffie Hellman Groups:
  1) Diffie Hellman Group 1
  2) Diffie Hellman Group 2
```

```
Select the Diffie Hellman Group ID from this proposal (1-2) [1]?
```

```
Here is the ISAKMP Proposal you specified...
```

```
Name = genP1Proposal
AuthMethod = Pre-Shared Key
LifeSize = 1000
LifeTime = 15000
DHGroupID = 1
Hash Algo = SHA
Encr Algo = 3DES CB
Is this correct? [Yes]:
```

### 21. ISAKMP アクションの構成に戻ります。

```
List of ISAKMP Proposals:
  0: New Proposal
  1: genP1Proposal
```

```
Enter the Number of the ISAKMP Proposal [1]?
Are there any more Proposal definitions for this ISAKMP Action? [No]:
```

```
Here is the ISAKMP Action you specified...
```

```
ISAKMP Name = genPhase1Action
Mode = Main
Min Percent of SA Life = 75
Conn LifeSize:LifeTime = 5000 : 30000
Autostart = No
ISAKMP Proposals:
  genP1Proposal
Is this correct? [Yes]:
```

### 22. ポリシーの構成に戻ります。

```
ISAKMP Actions:
  0: New ISAKMP Action
  1: genPhase1Action
```

```
Enter the Number of the ISAKMP Action [1]?
Do you wish to Map a DiffServ Action to this Policy? [No]: yes
```

### 23. DiffServ GoldService アクションを定義します。

```
DiffServ Actions:
  0: New DiffServ Action
```

```
Enter the Number of the DiffServ Action [0]?
```

### 24. DiffServ アクションの構成。

```
Enter a Name (1-29 characters) for this DiffServ Action []? GoldService
Enter the permission level for packets matching this DiffServ
Action (1. Permit, 2. Deny) [2]? 1
List of DiffServ Queues:
  1) Premium
  2) Assured/BE
Enter the Queue Number(1-2) for outgoing packets matching
this DiffServ Action [2]? 2
How do you want to specify the bandwidth allocated to this service?
Enter absolute kbps(1) or percentage of output bandwidth(2) [2]?
Enter the percentage of output bandwidth allocated to this service [10]? 40

Transmitted DS-byte mask [0]?
Transmitted DS-byte modify value [0]?
```

Here is the DiffServ Action you specified...

```
DiffServ Name = GoldService                               Type =Permit
                TOS mask:modify=x00:x00
                Queue:BwShare =Assured      : 40 %
Is this correct? [Yes]:
```

25. ポリシーの構成に戻ります。

```
DiffServ Actions:
  0: New DiffServ Action
  1: GoldService

Enter the Number of the DiffServ Action [1]? 1
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]:
```

Here is the Policy you specified...

```
Policy Name      = examplePolicySecure11to12
State:Priority   =Enabled      : 10
Profile         =trafficFrom10NetTo12Net
Valid Period    =MonToFri-9am:5pm-1999
IPSEC Action    =secure11NetTo12Net
ISAKMP Action   =genPhase1Action
DiffServ Action =GoldService
Is this correct? [Yes]:
```

26. DiffServ または IPSec が使用可能になっていない場合は、ポリシーを実施する前にまず DiffServ、IPSec、または両方 (DiffServ 機能または IPSec 機能) を使用可能にする必要があるというアラートが出されます。

```
You must enable and configure DiffServ in feature DS before
QoS can be ensured for this policy
```

27. このプロセスの最初のステップは、リモート ISAKMP ピアに対するユーザー・プロファイル定義の追加です。ISAKMP ネゴシエーションが公用証明書を使用してピアを認証する場合は、このステップは不要です。ただし、前の例では認証方式として事前共有キーを選択したので、ユーザーを指定し、ピアが使用しているものとして予期する事前共有キーを入力する必要があります。

```
Policy config>add user
Choose from the following ways to identify a user:
  1: IP Address
  2: Fully Qualified Domain Name
  3: User Fully Qualified Domain Name
  4: Key ID (Any string)
Enter your choice(1-4) [1]?
Enter the IP Address that distinguishes this user
[0.0.0.0]? 1.1.1.2
Group to include this user in []? peers
Authenticate user with 1:pre-shared key or 2: Public Certificate [1]?
Mode to enter key (1=ASCII, 2=HEX) [1]?
Enter the Pre-Shared Key (an even number of 2-128 ascii chars):
Enter the Pre-Shared Key again (10 characters) in ascii:
```

Here is the User Information you specified...

```
Name      = 1.1.1.2
Type      = IPV4 Addr
Group     =peers
Auth Mode =Pre-Shared Key
Key(Ascii)=exampleKey
Is this correct? [Yes]:
```

28. これで、ポリシー構成手順は完了しました。DiffServ、IPSec、またはネットワークや IP を構成する場合は、その構成を行わなければ IPSec トンネルが機能しません。次の list コマンドの例は、完了したばかりの構成を示しています。これ

## ポリシー機能の使用

らの変更をアクティブにするには、装置を再ロードするか、ポリシー機能の Talk 5 **reset database** コマンドを入力します。

```
Policy config>list all
```

```
Configured Policies....
```

```
Policy Name      = examplePolicySecure11to12
State:Priority   =Enabled      : 10
Profile          =trafficFrom11NetTo12Net
Valid Period    =MonToFri-9am:5pm-1999
IPSEC Action    =secure11NetTo12Net
ISAKMP Action   =genPhase1Action
DiffServ Action =GoldService
--More--
```

```
Configured Profiles....
```

```
Profile Name     = trafficFrom11NetTo12Net
sAddr:Mask=     11.0.0.0 : 255.0.0.0      sPort=    0 : 65535
dAddr:Mask=     12.0.0.0 : 255.0.0.0      dPort=    0 : 65535
proto           =                0 : 255
TOS             =                x00 : x00
Remote Grp=All Users
--More--
```

```
Configured Validity Periods
```

```
Validity Name   = MonToFri-9am:5pm-1999
Duration        = 19990101000000 : 19991231000000
Months         = ALL
Days           = MON TUE WED THU FRI
Hours          = 09:00:00 : 17:00:00
--More--
```

```
Configured DiffServ Actions....
```

```
DiffServ Name   = GoldService                Type =Permit
TOS mask:modify=x00:x00
Queue:BwShare   =Assured      : 40 %
--More--
```

```
Configured IPSEC Actions....
```

```
IPSECAction Name = secure11NetTo12Net
Tunnel Start:End =                1.1.1.1 : 1.1.1.2
Tunnel In Tunnel =                No
Min Percent of SA Life =                75
Refresh Threshold =                85 %
Autostart        =                No
DF Bit           =                COPY
Replay Prevention =                Disabled
IPSEC Proposals:
genP2Proposal
--More--
```

```
Configured IPSEC Proposals....
```

```
Name = genP2Proposal
Pfs = N
ESP Transforms:
esp3DESswSHA
--More--
```

```
Configured IPSEC Transforms....
```

```
Transform Name = esp3DESswSHA
Type =ESP      Mode =Tunnel      LifeSize= 50000 LifeTime= 3600
Auth =SHA      Encr =3DES
--More--
```

```
Configured ISAKMP Actions....
```

```

ISAKMP Name      = genPhase1Action
Mode              =                      Main
Min Percent of SA Life =              75
Conn LifeSize:LifeTime =            5000 : 30000
Autostart         =                      No
ISAKMP Proposals:
genP1Proposal
--More--

Configured ISAKMP Proposals....
Name = genP1Proposal
AuthMethod = Pre-Shared Key
LifeSize = 1000
LifeTime = 15000
DHGroupID = 1
Hash Algo = SHA
Encr Algo = 3DES CB
--More--

Configured Policy Users....
Name = 1.1.1.2
Type = IPV4 Addr
Group =peers
Auth Mode =Pre-Shared Key
Key(Ascii)=exampleKey
--More--

Configured Manual IPSEC Tunnels....

                                IPv4 Tunnels
-----
ID          Name          Local IPv4 Addr  Rem IPv4 Addr  Mode  State
-----

```

## IPSec/ISAKMP だけのポリシー

図31 の後にあるサンプル構成手順は、図の値に対応する値を使用しています。この手順は左から右への方式を使用しており、前のものが作成した情報を再利用することによって、前のサンプル手順を基にして構成を行う方法を説明しています。

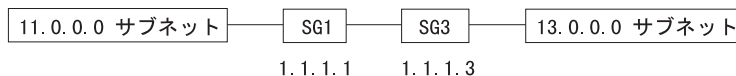


図 31. IPSec の構成と前の定義の再利用

次に説明するポリシー構成手順は、SG1 側から行います。この例のポリシー記述は、次のとおりです。

トンネル・エンドポイントを SG1 と SG3 に指定してサブネット 11 からサブネット 13 へのトラフィックを保護し、QOS を提供しない。

1. ポリシーを追加します。

```

Policy config>add policy
Enter a Name (1-29 characters) for this Policy []? examplePolicySecure11to13
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]? 10
List of Profiles:
0: New Profile
1: trafficFrom10NetTo12Net

Enter number of the profile for this policy [1]? 0
Enter a Name (1-29 characters) for this Profile []? trafficFrom11NetTo13Net
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]? 11.0.0.0

```

## ポリシー機能の使用

```
Enter IPV4 Source Mask [255.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]? 13.0.0.0
Enter IPV4 Destination Mask [255.0.0.0]?
```

```
Protocol IDs:
  1) TCP
  2) UDP
  3) All Protocols
  4) Specify Range
```

```
Select the protocol to filter on (1-4) [3]? 1
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
Limit this profile to specific interface(s)? [No]:
```

Here is the Profile you specified...

```
Profile Name      = trafficFrom11NetTo13Net
sAddr:Mask=      11.0.0.0 : 255.0.0.0      sPort=    0 : 65535
dAddr:Mask=      13.0.0.0 : 255.0.0.0      dPort=    0 : 65535
proto           =          6 : 6
TOS             =          x00 : x00
Remote Grp=All Users
Is this correct? [Yes]:
List of Profiles:
0: New Profile
1: trafficFrom10NetTo12Net
2: trafficFrom11NetTo13Net
```

```
Enter number of the profile for this policy [1]? 2
```

### 2. 有効期間を再利用します。

```
List of Validity Periods:
0: New Validity Period
1: MonToFri-9am:5pm-1999
```

```
Enter number of the validity period for this policy [1]?
Should this policy enforce an IPSEC action? [No]: yes
IPSEC Actions:
0: New IPSEC Action
1: secure11NetTo12Net
```

```
Enter the Number of the IPSEC Action [1]? 0
Enter a Name (1-29 characters) for this IPsec Action []? secure11To13
List of IPsec Security Action types:
  1) Block (block connection)
  2) Permit
```

```
Select the Security Action type (1-2) [2]?
Should the traffic flow into a secure tunnel or in the clear:
  1) Clear
  2) Secure Tunnel
```

```
[2]?
Enter Tunnel Start Point IPV4 Address
[11.0.0.5]? 1.1.1.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
[0.0.0.0]? 1.1.1.3
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA lifiesize/lifetime to use as the acceptable minimum [75]?
```



```
Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):
  1) Copy
  2) Set
  3) Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?
Do you want to negotiate the security association at
system initialization(Y-N)? [No]:
You must choose the proposals to be sent/checked against during phase 2
negotiations. Proposals should be entered in order of priority.
```

3. 前に定義した構成から IPsec プロポーザルを再利用します。

```
List of IPSEC Proposals:
0: New Proposal
1: genP2Proposal

Enter the Number of the IPSEC Proposal [1]?
Are there any more Proposal definitions for this IPSEC Action? [No]:
```

Here is the IPsec Action you specified...

```
IPSECAction Name = secure11To13
Tunnel Start:End      =      1.1.1.1 : 1.1.1.3
Tunnel In Tunnel      =      No
Min Percent of SA Life =      75
Refresh Threshold     =      85 %
Autostart              =      No
DF Bit                 =      COPY
Replay Prevention     =      Disabled
IPSEC Proposals:
genP2Proposal
Is this correct? [Yes]:
IPSEC Actions:
0: New IPSEC Action
1: secure11NetTo12Net
2: secure11To13
```

Enter the Number of the IPSEC Action [1]? 2

4. 前の構成から ISAKMP アクションを再利用します。

```
ISAKMP Actions:
0: New ISAKMP Action
1: genPhase1Action

Enter the Number of the ISAKMP Action [1]?
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?
```

Here is the Policy you specified...

```
Policy Name      = examplePolicySecure11to13
State:Priority   =Enabled      : 10
Profile         =trafficFrom11NetTo13Net
Valid Period    =MonToFri-9am:5pm-1999
IPSEC Action    =secure11To13
ISAKMP Action   =genPhase1Action
Is this correct? [Yes]:
```

## すべての公衆トラフィックをドロップする (フィルター規則)

このポリシー例は、IPSec によって保護されていないトラフィックをすべてドロップする公衆インターフェースに対して、単純な除去規則を構成する方法を説明します。この規則は非常に汎用的であり、構成される規則のうちで最低の優先順位を指定する必要があります。

1. ポリシーを追加します。

```
Policy config>add policy
Enter a Name (1-29 characters) for this Policy []? dropAllPublicTraffic
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
List of Profiles:
  0: New Profile
  1: trafficFrom10NetTo12Net
  2: trafficFrom11NetTo13Net

Enter number of the profile for this policy [1]? 0
```

2. 公衆インターフェース (1.1.1.1) を出入りするすべてのトラフィックを組み込んだ新しいプロファイルを定義します。

```
Enter a Name (1-29 characters) for this Profile []? allPublicTraffic
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]?
Enter IPV4 Source Mask [0.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]?
Enter IPV4 Destination Mask [0.0.0.0]?

Protocol IDs:
  1) TCP
  2) UDP
  3) All Protocols
  4) Specify Range

Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
```

3. 送信元とあて先 (またはその両方) の情報がワイルドカードになっているので、このトラフィックが発着信することが予期されるインターフェースを指定する必要があります。

```
The Source and/or Destination Address information you specified
includes all addresses. You must specify an Interface Pair
with this profile to further qualify what traffic you wish to filter
to this policy. The interface pair should at least specify the
Limit this profile to specific interface(s)? [No]: yes
Interface Pair Groups:
  0: New Ifc Pair

Number of Ifc Pair Group [1]? 0
```

4. 公衆インターフェースから発信するトラフィック用のインターフェース・ペアを追加します。

```

Enter a Group Name (1-29 characters) for this Interface Pair []? inOutPublic
Ingress Interface IP Address (255.255.255.255 = any ingress)
[255.255.255.255]?
Egress Interface IP Address (255.255.255.255 = any egress)
[255.255.255.255]? 1.1.1.1
Interface Pair Groups:
  0: New Ifc Pair
  1) Group Name: inOutPublic
      In:Out=255.255.255.255 : 1.1.1.1

```

Number of Ifc Pair Group [1]? **0**

5. 公衆インターフェースから着信するトラフィック用のもう 1 つのインターフェース・ペアを追加します。同じグループに割り当てられているために、前のインターフェース・ペアと同じ名前を指定します。

```

Enter a Group Name (1-29 characters) for this Interface Pair []? inOutPublic
Ingress Interface IP Address (255.255.255.255 = any ingress)
[255.255.255.255]? 1.1.1.1
Egress Interface IP Address (255.255.255.255 = any egress)
[255.255.255.255]?
Interface Pair Groups:
  0: New Ifc Pair
  1) Group Name: inOutPublic
      In:Out=255.255.255.255 : 1.1.1.1
      In:Out=      1.1.1.1 : 255.255.255.255

```

Number of Ifc Pair Group [1]?

Here is the Profile you specified...

```

Profile Name      = allPublicTraffic
sAddr:Mask=      0.0.0.0 : 0.0.0.0          sPort=      0 : 65535
dAddr:Mask=      0.0.0.0 : 0.0.0.0          dPort=      0 : 65535
proto            =          0 : 255
TOS              =          x00 : x00
Remote Grp=All Users
1. In:Out=255.255.255.255 : 1.1.1.1
2. In:Out=      1.1.1.1 : 255.255.255.255

```

Is this correct? [Yes]:

```

List of Profiles:
  0: New Profile
  1: trafficFrom10NetTo12Net
  2: trafficFrom11NetTo13Net
  3: allPublicTraffic

```

Enter number of the profile for this policy [1]? **3**

6. all the time を指定する有効期間を追加します。

```

List of Validity Periods:
  0: New Validity Period
  1: MonToFri-9am:5pm-1999

```

```

Enter number of the validity period for this policy [1]? 0
Enter a Name (1-29 characters) for this Policy Valid Profile []? allTheTime
Enter the lifetime of this policy. Please input the
information in the following format:
      yyyyymmddhhmmss:yyyyymmddhhmmss OR '*' denotes forever.

```

[\*]?

During which months should policies containing this profile be valid. Please input any sequence of months by typing in the first three letters of each month with a space in between each entry, or type ALL to signify year round.

[ALL]?

During which days should policies containing this profile

## ポリシー機能の使用

be valid. Please input any sequence of days by typing in the first three letters of each day with a space in between each entry, or type ALL to signify all week

[ALL]?

Enter the starting time (hh:mm:ss or \* denotes all day)

[\*]?

Here is the Policy Validity Profile you specified...

Validity Name = allTheTime

Duration = Forever

Months = ALL

Days = ALL

Hours = All Day

Is this correct? [Yes]:

List of Validity Periods:

0: New Validity Period

1: MonToFri-9am:5pm-1999

2: allTheTime

Enter number of the validity period for this policy [1]? 2

Should this policy enforce an IPSEC action? [No]: **yes**

IPSEC Actions:

0: New IPSEC Action

1: secure11NetTo12Net

2: secure11To13

7. トラフィックをすべてドロップする新しい IPsec アクションを追加します (フィルター・アクション)。

Enter the Number of the IPSEC Action [1]? 0

Enter a Name (1-29 characters) for this IPsec Action []? **dropTraffic**

List of IPsec Security Action types:

1) Block (block connection)

2) Permit

Select the Security Action type (1-2) [2]? 1

Here is the IPsec Action you specified...

IPSECAction Name = dropTraffic

Action = Drop

Is this correct? [Yes]:

IPSEC Actions:

0: New IPSEC Action

1: secure11NetTo12Net

2: secure11To13

3: dropTraffic

Enter the Number of the IPSEC Action [1]? 3

Do you wish to Map a DiffServ Action to this Policy? [No]:

Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

Here is the Policy you specified...

Policy Name = dropAllPublicTraffic

State:Priority =Enabled : 5

Profile =allPublicTraffic

Valid Period =allTheTime

IPSEC Action =dropTraffic

Is this correct? [Yes]:

## LDAP ポリシー検索エンジンの構成と使用可能化

この例は、LDAP ポリシー検索エンジンを構成し、使用可能にする方法を示しています。この例では、2 つの LDAP ディレクトリー (1 次と 2 次) があり、IP アドレスはそれぞれ 11.0.0.2 と 13.0.0.1 です。これらのディレクトリーは両方とも TCP ポート 389 を listen しており、cn=router、パスワード myPassWord を指定して装置を LDAP とバインドする必要があります。ルーターのポリシーに関するディレクトリー・ツリーの基本エントリーは、cn=RouterDeviceProfile,o=ibm,c=us です。

**注:** 現在、1 次と 2 次の LDAP サーバーは両方とも同じポートを listen する必要があります。ルーターに対して同じ認証証明書を持っている必要があります。ルーターに対する DeviceProfile は、両方のディレクトリー・サーバーで同じでなければなりません。

この例では、LDAP 通信が IPSec によって保護されるようにデフォルト・ポリシーを設定する方法も示します。この例は、ISAKMP 認証に対しては事前共有キーを使用し、フェーズ 1 とフェーズ 2 の認証と暗号化のパラメーターに対しては SHA と 3DES を使用しています。トンネルの開始点は、LDAP ポリシー検索を実行する装置の 1.1.1.4 で、トンネルの終点は、11.0.0.1 LDAP サーバーの 1.1.1.1 と、13.0.0.1 LDAP サーバーの 1.1.1.3 です。

1. LDAP ポリシー検索エンジンを構成して使用可能にし、結果を表示します。

```
Policy config>set ldap primary-server 11.0.0.1
Policy config>set ldap secondary-server 13.0.0.1
Policy config>set ldap port 389
Policy config>set ldap bind-name cn=router
Policy config>set ldap bind-pw myPassWord
Policy config>set ldap anonymous-bind no
Policy config>set ldap policy-base cn=RouterDeviceProfile,o=ibm,c=us
Policy config>enable ldap policy-search
Policy config>list ldap
LDAP CONFIGURATION information:

Primary Server Address:          11.0.0.1
Secondary Server Address:       13.0.0.1

Search timeout value:           3 sec(s)
Retry interval on search failures: 1 min(s)
Server TCP port number:        389
Server Version number:         2

Bind Information:
Bind Anonymously:               No
Device Distinguished Name:     cn=router
Device Password:               myPassWord

Base DN for this device's policies:  cn=RouterDeviceProfile,o=ibm,c=us

Search policies from LDAP Directory: Enabled
```

2. デフォルト・ポリシーを設定します。

```
Policy config>set default-policy
List of default policy rules:
1) Accept and Forward all IP Traffic
2) Permit LDAP traffic, drop all other IP Traffic
3) Permit and Secure LDAP traffic, drop all other IP Traffic
```

```
Select the default policy rule to use during policy refresh periods [1]? 3
List of default error handling procedures:
  1) Reset Policy Database to Default Rule
  2) Flush any rules read from LDAP, load local rules

Select the error handling behavior for when loading Policy Database [1]?

Please enter the set of Security Information for encrypting and
authenticating the LDAP traffic generated by the device when
retrieving policy information from the LDAP Server

Enter phase 1 ISAKMP negotiation parameters:

List of Diffie Hellman Groups:
  1) Diffie Hellman Group 1
  2) Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?

List of Hashing Algorithms:
  1) MD5
  2) SHA

Select the hashing algorithm(1-2) [1]? 2

List of Cipher Algorithms:
  1) DES
  2) 3DES

Select the Cipher Algorithm (1-2) [1]? 2
Authentication: (1)Pre-shared Key or (2)Certificate(RSA Sig) [2]? 1
Enter the Pre-Shared Key []? test

Enter phase 2 IPSEC negotiation parameters:
List of IPsec Authentication Algorithms:
  0) None
  1) HMAC-MD5
  2) HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [1]? 2
List of ESP Cipher Algorithms:
  1) ESP DES
  2) ESP 3DES
  3) ESP CDMF
  4) ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]? 2
Tunnel Start IPV4 Address (Primary LDAP Server)
[0.0.0.0]? 1.1.1.4
Tunnel End Point IPV4 Address (Primary LDAP Server)
[0.0.0.0]? 1.1.1.1
Tunnel Start IPV4 Address (Secondary LDAP Server)
[1.1.1.4]?
Tunnel End Point IPV4 Address (Secondary LDAP Server)
[1.1.1.1]? 1.1.1.3
Policy config>list default-policy

Default Policy Rule:                Drop All IP Traffic except secure LDAP
Default error handling procedure:    Reset Policy Database to Default Rule

Phase 1 ISAKMP negotiation parameters:
Diffie Hellman Group ID:            1
Hashing Algorithm:                  SHA
ISAKMP Cipher Algorithm:            ESP 3DES CBC
Per-shared key value:               test
```

```
Phase 2 IPSEC negotiation parameters:  
IPsec ESP Authentication Algorithm:  HMAC SHA  
ESP Cipher Algorithm:                3DES  
Local Tunnel Addr (Primary Server):  1.1.1.4  
Remote Tunnel Addr (Primary Server):  1.1.1.1  
Local Tunnel Addr (Secondary Server):  1.1.1.4  
Remote Tunnel Addr (Secondary Server): 1.1.1.3
```

この時点で、ポリシーを機能を使用してネットワーク内のルーターを管理する準備ができました。プロファイル、プロポーザル、変換、アクションなど、必要なポリシー・パラメーターを構成するために使用されるコマンドについて詳しくは、307ページの『ポリシー構成コマンド』、322ページの『LDAP ポリシー・サーバー構成コマンド』、および 327ページの『ポリシー監視コマンド』を参照してください。





## 第19章 ポリシー機能の構成と監視

この章では、ネットワーク内のルーター装置を構成し、操作するためにポリシー機能が用意している LDAP コマンドとポリシー・コマンドを説明します。この章には、次の内容が記載されています。

- 『ポリシー構成プロンプトへのアクセス』
- 『ポリシー構成コマンド』
- 322ページの『LDAP ポリシー・サーバー構成コマンド』
- 327ページの『ポリシー監視プロンプトへのアクセス』
- 327ページの『ポリシー監視コマンド』

### ポリシー構成プロンプトへのアクセス

ポリシー構成コマンドを入力する手順は、次のとおりです。

1. OPCON (\*) プロンプトで **talk 6** と入力する。
2. Config> プロンプトで **feature policy** と入力する。

Policy config> プロンプトが表示されます。これで、ポリシー構成コマンドを入力できるようになります。

### ポリシー構成コマンド

これらのコマンドを使用して、ポリシーに含まれる情報を構成できます。表38 はポリシー構成コマンドの要約を示し、ここでの残りの部分でこれらのコマンドについて説明します。コマンドは Policy config> プロンプトで入力します。コマンドとオプションを 1 行に入力することも、コマンドだけを入力してプロンプトに答えることもできます。有効なコマンド・オプションのリストを表示するには、オプションの代わりに疑問符 (?) を指定してコマンドを入力します。

表 38. ポリシー構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxi ページの『ヘルプの入手』を参照してください。
Add	ポリシーの作成に使用する情報を追加します。
Change	ポリシーを構成する情報を変更します。
Copy	ポリシー間で情報をコピーします。
Delete	ポリシーから情報を削除します。
Disable	ポリシーを使用不可にします。
Enable	ポリシーを使用可能にします。
List	ポリシーの情報を表示します。
Set	デフォルトとして使用するポリシーを指定します。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

## ポリシー構成コマンド (Talk 6)

### Add

**add** コマンドは、ポリシーに情報を追加するために使用します。

構文: add                                 diffserv-action  
  interface-pair  
  ipsec-action  
  ipsec-manual-tunn  
  ipsec-proposal  
  ipsec-transform  
  isakmp-action  
  isakmp-proposal  
  policy  
  profile  
  rsvp-action  
  user  
  validity-period

#### Diffserv-action

どの DiffServ-action 選択項目を適用するかについて情報を尋ねるプロンプトが出されます。

**Name** ポリシーの DiffServ アクションの固有な名前。

#### permission-level

ルーターがこの DiffServ アクションに一致するパケットを転送するかどうかを指定します。

1 許可

2 拒否

デフォルト値: 2

#### Queue-priority

この DiffServ アクションに一致する発信パケットを入れる待ち行列。

1 プレミアム (即時転送)

2 保証/Best Effort

デフォルト値: 2

#### bwshare-type

帯域幅共用割り振りのタイプ。

1 絶対 (Kbps)

2 パーセンテージ (合計出力帯域幅の)

デフォルト値: 2

**bwshare**

このサービスに割り振る帯域幅 (Kbps 単位、または出力帯域幅のパーセンテージとして指定)。

**ds-bytemask**

送信される ds バイトに適用するマスク。この値は、パケットの送信時に変更する必要のあるパケットの TOS バイトのビットを指定します。このバイトのどちらかのビット位置をゼロにすると、そのビットを変更してはならないことが指定されます。

デフォルト値:

00

(どのビットも変更しない)

**ds-bytemodify**

この装置によって転送されるパケットに適用する必要がある IP TOS バイトのマーキング。マスクにあるゼロは、対応するビットを変更しないことを指定します。1 は、そのビットをマーク・バイトのビット値によってマーク付けすることを指定します。演算は、 $\text{newTOSByte} = (\text{Mask} \wedge \text{receivedTOSByte}) \vee (\text{Mask} \wedge \text{Mark})$  となります。 $\wedge$  は、ビットに基づく補数です (Mask:Mark)。

例:

11111101:00000001

この例を使用すると、受信した値 0x07 は値 0x03 となって送信されます。

デフォルト値: X'00' (どのビットも変更しない)

**interface-pair**

インターフェース・ペアは、特定のインターフェース、またはインターフェースの集合と、プロファイルを関連付けます。デフォルトでは、プロファイル・オブジェクトはポリシーが任意のインターフェースに適用されることを制限しません。制限が必要な場合は、インターフェース・ペアを追加すれば制限を設けることができます。インターフェース・ペアは、トラフィックが着信するインターフェースの IP アドレスと、トラフィックを発信するインターフェースの IP アドレスを指定します。

次の例は、同じ名前の 2 つのインターフェース・ペアを示しています。これらは、任意のインターフェースから着信して公衆インターフェースから発信するトラフィックと、その逆を表しています。

```
1) Group Name: inOutPublic
   In:Out=255.255.255.255 : 1.1.1.1
   In:Out=1.1.1.1 : 255.255.255.255
```

**Name** インターフェース・ペアの名前。

**Ingress interface**

入力インターフェースの IPv4 アドレス。

デフォルト値: 255.255.255.255 (任意)

## ポリシー構成コマンド (Talk 6)

### Egress interface

出カインターフェースの IPv4 アドレス。

デフォルト値: 255.255.255.255 (任意)

### IPSec-action

フェーズ 2 トンネルを設定するための情報を尋ねるプロンプトが出され  
ます。

**Name** IPSec アクションの名前。

### Action type

このアクションを含むポリシーのプロファイルに一致するパケット  
に適用するアクション。

- 1 ブロック (接続をブロックする)
- 2 許可 (このアクションに一致するパケットを許可する)。 IPSec  
プロポーザルが存在しない場合は、パケットをパスします。  
IPSec プロポーザルが存在する場合は、パケットに IPSec セ  
キュリティー処理を適用します。

デフォルト値: 2

次のオプションは、アクション・タイプとしてパスを指定した場合だけ使用  
できます。

### Traffic flow type

トラフィック・フローのタイプ (保護トンネル、または暗号化なし)

- 1 暗号化なし
- 2 保護トンネル

デフォルト値: 2

次のオプションは、トラフィック・フローを保護に指定した場合だけ使用で  
きます。

### Tunnel start point

トンネル開始点の IPv4 アドレス。

### Tunnel end point

トンネル終点の IPv4 アドレス。(リモート・アクセスの場合は 0.0.0.0)

デフォルト値: 0.0.0.0

### Tunnel-in-tunnel

このトンネルによって保護されるトラフィックを、この装置で構成  
されている別のポリシーによってさらに保護するかどうかを指定し  
ます。

有効オプション: Yes または No

デフォルト値: No

**Percentage of SA liveness/lifetime to accept**

SA 存続サイズ/存続時間の最小 SA 存続サイズ/存続時間 (パーセンテージとして指定)。これより小さい値の SA 存続サイズ/存続時間の受信は受け入れられません。

デフォルト値: 75

**SA refresh threshold**

SA を自動的にリフレッシュする SA 存続時間または存続サイズ値のパーセンテージ。

デフォルト値: 85

**DF-Bit-Setting**

元のパケットから Don't Fragment ビットをコピーするかどうかを指定し、トンネル・モードで稼働している場合に、IPSec パケットの外部ヘッダーでそのビットをセットまたはクリアするかどうかを指定します。

- 1 コピー
- 2 セット
- 3 クリア

デフォルト値: 1

**Replay-Prevention**

IPSec が受信した IPSec パケットに対して、再生防止を実施するかどうかを指定します。このモードでは、IPSec は順序番号が有効であること、複数回受信されないことを保証します。

- 1 使用可能
- 2 使用不可

デフォルト値: 2

**Negotiate SA Automatically**

システム初期設定時にフェーズ 2 SA のネゴシエーションを自動的に行うかどうかを指定します。

Yes または No

デフォルト値: No

**IPSec proposal**

フェーズ 2 の間に送信またはチェックする IPSec プロポーザル (5 つまでのプロポーザルを指定できます) の名前。指定順序がプロポーザルの優先順位を決定し、最初のものが最高になります。

**IPSec-manual-tunn**

フェーズ 2 トンネルを手動で設定するための情報を尋ねるプロンプトが出されます。

**Tunnel name**

IPSec 手動トンネルの名前。

## ポリシー構成コマンド (Talk 6)

### Tunnel lifetime

トンネルの存続時間 (秒)。

デフォルト値: 46080

### Encapsulation mode

使用するカプセル化モード。

**tunn** トンネル・モード

**trans** トランスポート・モード

デフォルト値: tunn

### Policy

使用するトンネル・ポリシーのタイプ。

**AH** 認証ヘッダー

**ESP** カプセル化セキュリティー・ペイロード

#### AH-ESP

アウトバウンド・パケットの場合、認証の前に暗号化を実行することを指定します。

#### ESP-AH

アウトバウンド・パケットの場合、暗号化の前に認証を実行することを指定します。

デフォルト値: AH-ESP

### Local IP address

送信元 IPv4 アドレス。

デフォルト値: 11.0.0.5

### Local encryption SPI

送信元セキュリティー・パラメーター・インデックス値。

デフォルト値: 256

### Local encryption algorithm

送信元の暗号化アルゴリズム。

**Null** 暗号化なし。

**CDMF** 商用データ・マスキング機能。

#### DES-CBC

データ暗号化規格および暗号化ブロック・チェーン。

**3DES** 三重データ暗号化規格。

デフォルト値: DES-CBC

### Local encryption key

16 文字のキー。

### Padding

ローカル暗号化用の追加埋め込み。

デフォルト値: 0

**Local ESP authentication**

ローカル ESP 認証を使用するかどうかを指定します。

**Yes** または **No**

デフォルト値: Yes

**Remote IP address**

あて先 IPv4 アドレス。

デフォルト値: 0.0.0.0

**Remote encryption SPI**

あて先セキュリティー・パラメーター・インデックス値。

デフォルト値: 256

**Remote encryption algorithm**

あて先の暗号化アルゴリズム。

**Null** 暗号化なし。

**CDMF** 商用データ・マスキング機能。

**DES-CBC**

データ暗号化規格および暗号化ブロック・チェーン。

**3DES** 三重データ暗号化規格。

デフォルト値: DES-CBC

**Remote encryption key**

16 文字のキー。

**Verify remote encryption padding.**

リモート暗号化埋め込みを検査するかどうかを指定します。

**Yes** または **No**

デフォルト値: No

**Remote ESP authentication**

リモート ESP 認証を使用するかどうかを指定します。

**Yes** または **No**

デフォルト値: Yes

**DF bit**

Don't Fragment ビットを処理する方法を指定します。

**Copy** DF ビットをコピーします。

**Set** DF ビットをオンに設定します。

**Clear** DF ビットをオフに設定します。

デフォルト値: COPY

**Enable tunnel**

トンネルを作成時に使用可能にするかどうかを指定します。

**Yes** または **No**

## ポリシー構成コマンド (Talk 6)

デフォルト値: Yes

### IPSec-proposal

IPSec プロポーザルを作成するための情報を尋ねるプロンプトが出されます。

#### IPSec proposal name

IPSec プロポーザルの名前。

#### Perfect forward secrecy

以前に悪用されたキーから誰かが現行キーを判別するのを防ぐために、IKE を使用するかどうかを指定します。

Yes または No

デフォルト値: No

#### Diffie Hellman Group ID

Diffie Hellman グループのタイプ。

1 Diffie Hellman グループ 1

2 Diffie Hellman グループ 2

デフォルト値: 1

#### AH transform

このプロポーザルに対する AH 変換の名前 (5 つまでの変換を指定できます)。指定順序が変換の優先順位を決定し、最初のものが最高になります。

#### ESP transform

このプロポーザルに対する ESP 変換の名前 (5 つまでのプロポーザルを指定できます)。指定順序が変換の優先順位を決定し、最初のものが最高になります。

### IPSec-transform

IPSec 変換に関する情報を尋ねるプロンプトが出されます。

#### IPSec transform name

IPSec 変換の名前。

#### Protocol ID

使用するセキュリティー・プロトコル。

1 IPSec-AH

2 IPSec-ESP

デフォルト値: 1

#### AH Authentication Algorithm

使用する AH 認証アルゴリズム。

1 HMAC-MD5

2 HMAC-SHA

デフォルト値: 1

#### Encapsulation mode

使用するカプセル化モード。



- 1 トンネル
- 2 トランスポート

デフォルト値: 1

**ESP Authentication Algorithm**

使用する ESP 認証アルゴリズム。

- 0 なし
- 1 HMAC-MD5
- 2 HMAC-SHA

デフォルト値: 2

**ESP cipher algorithm**

使用する ESP 暗号アルゴリズム。

- 1 ESP DES
- 2 ESP 3DES
- 3 ESP CDMF
- 4 ESP Null (暗号化なし)

デフォルト値: 1

**SA lifiesize**

このプロポーザルに対する SA の存続サイズ (Kb)。

デフォルト値: 50000

**SA lifetime**

このプロポーザルに対する SA の存続時間 (秒)。

デフォルト値: 3600

**ISAKMP-Action**

適用する ISAKMP アクションに関する情報を尋ねるプロンプトが出されます。

**Name** ISAKMP アクションの名前。

**Exchange mode**

フェーズ 1 ネゴシエーションの交換モードのタイプ。

- 1 メイン
- 2 アグレッシブ

デフォルト値: 1

**Percentage of Minimum SA lifiesize/lifetime**

SA 存続サイズ/存続時間の最小 SA 存続サイズ/存続時間 (パーセンテージとして指定)。これより小さい値の SA 存続サイズ/存続時間は受け入れられません。

デフォルト値: 75

## ポリシー構成コマンド (Talk 6)

### ISAKMP connection lifeseize

フェーズ 1 接続の存続サイズ (Kb)。フェーズ 1 接続が満了すると、フェーズ 2 SA を次にリフレッシュする必要があるとき、フェーズ 2 を開始する前にフェーズ 1 はネゴシエーションを完全にやり直します。

デフォルト値: 5000

### ISAKMP connection lifetime

フェーズ 1 接続の存続時間 (秒)。フェーズ 1 接続が満了すると、フェーズ 2 を次にリフレッシュする必要があるとき、フェーズ 1 は完全にリスタートします。

デフォルト値: 5000

### Negotiate SA automatically

システム初期設定時に SA のネゴシエーションを自動的に行うかどうかを指定します。

Yes または No

デフォルト値: No

### ISAKMP proposal

フェーズ 2 高速モード時に送信またはチェックする ISAKMP プロポーザル (5 つまでのプロポーザルを指定できます) の名前。指定順序が変換の優先順位を決定し、最初のものが最高になります。

### ISAKMP-Proposal

ISAKMP ネゴシエーションで使用される ISAKMP プロポーザル情報を尋ねるプロンプトが出されます。

### ISAKMP proposal name

ISAKMP プロポーザルの名前。

### Authentication method

ISAKMP フェーズ 1 ネゴシエーション時に使用する認証のタイプ。

- 1 事前共有キー
- 2 RSA SIG (証明書モード)

デフォルト値: 1

### Hash algorithm

フェーズ 1 ネゴシエーション時に使用するハッシュ・アルゴリズムのタイプ。

- 1 MD5
- 2 SHA

デフォルト値: 1

### Cipher algorithm

フェーズ 1 ネゴシエーション時に使用する暗号アルゴリズムのタイプ。

- 1 DES

**2** 3DES

デフォルト値: 1

**Diffie Hellman Group ID**

フェーズ 1 ネゴシエーション時に使用する Diffie Hellman グループのタイプ。

**1** Diffie Hellman グループ 1**2** Diffie Hellman グループ 2

デフォルト値: 1

**SA lifeseize**

このプロポーザルに対する SA の存続サイズ (Kb)。

デフォルト値: 50000

**SA lifetime**

このプロポーザルに対する SA の存続時間 (秒)。

デフォルト値: 5000

**Policy** ポリシー構成に関する情報を尋ねるプロンプトが出されます。情報は、プロファイル名 (必須)、RSVP 名 (オプション)、DiffServ 名 (オプション)、IPSec 名 (オプション)、ISAKMP 名 (オプション)、および有効期間プロファイル (オプション) です。ポリシーを有効にするには、DiffServ、IPSec、ISAKMP、または RSVP のどれかを指定する必要があります。

デフォルト値: 常に有効

**Name** ポリシー構成の名前**Priority**

他のポリシーに対するこのポリシーの相対優先順位 (番号が大きいほど、優先順位が高くなります)。これは、複数のポリシーがパケットに適用される場合に、競合を解決するために使用されます。

デフォルト値: 5

**Profile**

このポリシーに対して使用する事前構成済みのデータ・トラフィック・プロファイルの名前。

**Validity period**

このポリシーに対して使用する事前構成済みの有効期間の名前。

**IPSec action**

このポリシーが IPSec アクションを実行する場合は、このポリシーに対して使用する事前構成済み IPSec アクションの名前。保護 IPSec アクションを指定した場合は、ISAKMP アクションも指定する必要があります。

**ISAKMP アクション**

このポリシーに対して使用する事前構成済みの ISAKMP アクションの名前。ISAKMP アクションを指定した場合は、IPSec アクションも指定する必要があります。

## ポリシー構成コマンド (Talk 6)

### Diffserv action

(このポリシーに DiffServ アクションをマップする場合) 事前構成済み DiffServ アクションの名前。

### RSVP action

このポリシーが実行する RSVP アクションの名前。

### Profile

アクションを実行する対象のポリシー・プロファイルに対し、セレクター (条件) のセットを定義するための情報を尋ねるプロンプトが出されます。

**name** ポリシー・プロファイルの名前。

### ipv4-src-address-format

IPv4 送信元アドレスの形式 (範囲、ネットマスク、単一のアドレス)。

### ipv4-src-address

IPv4 送信元アドレス (アドレス形式が *range* の場合は、低位アドレス)。

デフォルト値: 0.0.0.0

### ipv4-src-mask

IPv4 送信元マスク (アドレス形式が *range* の場合は、高位アドレス)。

デフォルト値: 255.0.0.0

### ipv4-dest-address-format

IPv4 あて先アドレスの形式 (範囲、ネットマスク、単一のアドレス)。

### ipv4-dest-address

IPv4 あて先アドレス (アドレス形式が *range* の場合は、低位アドレス)。

デフォルト値: 0.0.0.0

### ipv4-dest-mask

IPv4 あて先マスク (アドレス形式が *range* の場合は、高位アドレス)。

デフォルト値: 255.0.0.0

### protocol-id

フィルターに掛ける対象のプロトコル id。

- |   |           |
|---|-----------|
| 1 | TCP       |
| 2 | UDP       |
| 3 | すべてのプロトコル |
| 4 | 指定範囲      |

デフォルト値: 3

### src-port-start

送信元ポート番号範囲の最初のポート番号。

デフォルト値: 0

**src-port-end**

送信元ポート番号範囲の最後のポート番号。

デフォルト値: 65535

**dest-port-start**

あて先ポート番号範囲の最初のポート番号。

デフォルト値: 0

**dest-port-end**

あて先ポート番号範囲の最後のポート番号。

デフォルト値: 65535

**src-id-type**

リモート側に送信される送信元 ID タイプ。この値は、ISAKMP フェーズ 1 ネゴシエーション時に必要な ISAKMP 情報があるポリシーを判別するために使用されます。この値は、ISAKMP パケットの識別ペイロードの情報と比較されます。この情報は、リモート・ピアが IP アドレス以外の値を指定して装置を識別する必要がある場合に必要です。

- 1 ローカル・トンネル終点
- 2 ホストの完全修飾ドメイン名
- 3 ユーザーの完全修飾ドメイン名
- 4 キー ID

**any-user-access**

プロファイル定義内の任意のユーザーに対してアクセスを許可します。No を指定すると、このプロファイルに対するリモート・ユーザー・グループの名前を尋ねるプロンプトが出されます。この属性は、特定のポリシーに対するリモート・アクセス・ピアのアクセスを制限する場合にだけ必要です。

**Yes または No**

デフォルト値: Yes

**Received DS byte mask**

着信パケットの TOS バイトに適用する 8 ビットのマスク。

デフォルト値: 0

**Received DS byte match**

着信した TOS バイトと Received DS byte mask 値を AND 演算した結果と比較する、8 ビットのパターン。

デフォルト値: 0

**Interface pairs**

このポリシーが特定のインターフェースだけにトラフィック・フローを制限する必要がある場合、これはインターフェース・ペア・グループの名前です。

**RSVP-Action**

適用する RSVP アクションに関する情報を尋ねるプロンプトが出されます。

## ポリシー構成コマンド (Talk 6)

**Name** RSVP アクションの名前。

**Permission**

このアクションに一致する RSVP セッションの許可レベルを指定します。

1 許可

2 拒否

デフォルト値: 2

**Max token rate**

RSVP が個々のフローに割り振る帯域幅の最大量 (Kbps)。

デフォルト値: 100

**Max duration**

フローが存続できる最大時間 (秒)。

デフォルト値: 600

**RSVP-to-DS**

このアクションに一致する RSVP フローを、構成済みの DiffServ アクションにマップするかどうかを指定します。RSVP は、DiffServ アクションの情報を使用して、DiffServ を使用可能にした次の上流装置への TOS バイトにマークを付けます。これは、RSVP を使用可能にしたネットワークから、DiffServ を使用可能にしたネットワークに発信されるパケットがあるネットワークで使用します。

**Yes または No**

デフォルト値: No

### VALIDITY-PERIOD

ポリシーが有効である期間に関する情報を尋ねるプロンプトが出され、ポリシー・プロファイルが作成されます。

**Name** 有効期間プロファイルの名前。

**yyyymmddhhmmss:yyyymmddhhmmss**

この有効期間プロファイルを含むポリシーが有効である期間。

例:

19980101000000:19981231000000

**Months**

この有効期間プロファイルを含むポリシーが有効である月。それぞれの月の先頭 3 文字を使用して (例: jan, dec)、スペースで月を区切って任意の月の列を指定でき、all を指定してその年のすべての月を指定することもできます。

**Days**

この有効期間プロファイルを含むポリシーが有効である曜日。それぞれの曜日の先頭 3 文字を使用して (例: mon, fri)、スペースで曜日を区切って任意の曜日の列を指定でき、all を入力してその週のすべての曜日を指定することもできます。

**Starting time**

この有効期間プロファイルを含むポリシーが有効である時刻。この時刻は、hh:mm:ss の形式で指定するか、ポリシーを 1 日中有効にする場合は \* を指定します。

デフォルト値: \*

**Ending time**

この有効期間プロファイルを含むポリシーが満了する時刻。この時刻は、hh:mm:ss の形式で指定します。

デフォルト値: なし

## Change

**change** コマンドは、ポリシー・オブジェクト内の情報を変更するために使用します。使用できるオブジェクトについては、**add** コマンドの説明を参照してください。

## Copy

**copy** コマンドは、ポリシー・オブジェクト間で情報をコピーするために使用します。使用できるオブジェクトについては、**add** コマンドの説明を参照してください。(インターフェース・ペア、手動トンネル、およびユーザー・オプションは、**copy** コマンドの対象になりません。)

## Delete

**delete** コマンドは、ポリシー・オブジェクトから情報を削除するために使用します。使用できるオブジェクトについては、**add** コマンドの説明を参照してください。

## Disable

**disable** コマンドは、ポリシー構成を使用不可にするために使用します。

構文: disable policy

**Policy** 使用不可にするポリシー構成の名前を尋ねるプロンプトが出されます。

## Enable

**enable** コマンドは、ポリシー構成を使用可能にするために使用します。

構文: enable policy

**Policy** 使用可能にするポリシー構成の名前を尋ねるプロンプトが出されます。

## List

**list** コマンドは、ポリシー構成情報のどれか、またはすべてを表示するために使用します。

構文: list all  
default-policy

## ポリシー構成コマンド (Talk 6)

ldap

refresh

**All** ポリシー構成情報をすべて表示します。

### Default-policy

デフォルト・ポリシーの名前を表示します。

**LDAP** 定義済み LDAP 構成の名前を表示します。

### Refresh

ポリシーのリフレッシュ状況 (使用可能または使用不可) とリフレッシュ間隔を表示します。

---

## LDAP ポリシー・サーバー構成コマンド

LDAP ポリシー・サーバー構成コマンドを使用して、ポリシー情報を検索するための LDAP サーバー・オプションを指定できます。表39 は LDAP 構成コマンドの要約を示し、ここでの残りの部分でこれらのコマンドについて説明します。コマンドは Policy config> プロンプトで入力します。コマンドとオプションを 1 行に入力することも、コマンドだけを入力してプロンプトに答えることもできます。有効なコマンド・オプションのリストを表示するには、オプションの代わりに疑問符 (?) を指定してコマンドを入力します。

表 39. LDAP 構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxi ページの『ヘルプの入手』を参照してください。
Disable ldap	LDAP 構成オプションを使用不可にします。
Enable ldap	LDAP 構成オプションを使用可能にします。
Set ldap	LDAP 構成オプションを指定します。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

## Disable LDAP

**disable ldap** コマンドは、ディレクトリー内での LDAP ポリシー検索機能を使用不可にするために使用します。

構文: `disable ldap` `policy-search`

### policy-search

ディレクトリー内での LDAP のポリシー検索機能を実行不可にします。

## Enable LDAP

**enable ldap** コマンドは、ディレクトリー内での LDAP ポリシー検索機能を使用可能にするために使用します。

構文: `enable ldap` `policy-search`



**policy-search**

ディレクトリー内での LDAP のポリシー検索機能を実行可能にします。

**Set Default-Policy**

**set default-policy** コマンドは、ポリシー・データベースのリフレッシュ中に使用するポリシー・オプションを指定するために使用します。このコマンドは、エラー処理オプションと、LDAP ポリシー・サーバーへのアクセスに必要なデフォルト・セキュリティを設定します。

```
構文: set                default-policy
                                default-error-handling
                                default-security
```

**default-error-handling**

ポリシー・データベースのリフレッシュ中に使用するエラー処理オプションを指定します。

**注:** デフォルト・エラー処理の設定は、ポリシー・データベースの再作成中にエラーが発生した場合の装置の動作を決定します。エラーが発生した場合に、ユーザーは装置の動作を選択できます。このオプションは、次のとおりです。

1. ポリシー・データベースをデフォルト・セキュリティにリセットする。
2. LDAP から読み取った規則をすべてフラッシュし、ローカル規則とデフォルト・セキュリティをロードする。

これらの設定は、ポリシー・データベースの作成時にエラーがあった場合にだけ有効になります。どちらのオプションも、エラーが発生した場合はドロップまたはパスのデフォルト・セキュリティを継承します。オプション 2 を選択した場合は、トラフィックがローカルに定義されたポリシーと一致しなければ、すべてのトラフィックがドロップまたはパスされます。ポリシー・データベースが正常に作成された場合は、このオプションは使用されません。

**default-security**

ポリシー・データベースのリフレッシュ中に使用するセキュリティ・オプションを指定します。

**注:** ポリシー・データベースが正常に作成されると、デフォルト動作はパスに定義されます。このため、パケットがポリシー規則のどれかと一致しない場合は、パケットは暗号化されずにパスされます。規則と一致しないパケットをグローバルにドロップする場合、または特定のインターフェースの場合だけドロップする場合は、そのためのポリシーを定義する必要があります。

1. すべての IP トラフィックを受け入れて転送します。
2. LDAP トラフィックを許可し、その他の IP トラフィックをすべてドロップします。

## LDAP 構成コマンド (Talk 6)

このオプションを選択した場合、LDAP トラフィックを送受信する装置のローカル IP アドレスを尋ねるプロンプトが出されます。

- 3 LDAP トラフィックを許可して保護し、その他の IP トラフィックをすべてドロップします。

このオプションを選択した場合、次の情報を尋ねるプロンプトが出されます。

### DHGroupId

ISAKMP フェーズ 1 ネゴシエーション時に使用する Diffie-Hellman グループ Id。

- 1 DH グループ 1
- 2 DH グループ 2

### Phase1-Hash-Algorithm

フェーズ 1 ネゴシエーション時に使用するハッシュ・アルゴリズム。ハッシュ・アルゴリズムは、フェーズ 1 メッセージの認証を行います。

- 1 MD5
- 2 SHA

### Phase1-Cipher-Algorithm

フェーズ 1 ネゴシエーション時に使用する暗号アルゴリズム。暗号アルゴリズムは、フェーズ 1 ネゴシエーションの暗号化保護を行います。

- 1 DES
- 2 3DES

### Phase1-Authentication-Method

リモート・ピアに対して使用する認証方式。これは、ネゴシエーションの対象としてリモート・ピアが本当に正しい装置かどうかを ISAKMP が判別する方法を指定します。

- 1 事前共有キー
- 2 証明書 (RSA SIG)

### Pre-Shared-Key-Value

フェーズ 1 認証方式として事前共有キーを指定した場合は、キー値を ASCII 形式で入力するように求めるプロンプトが出されます。

### Phase2-ESP-Authentication-Algorithm

ESP は、デフォルト・セキュリティーとして許可される唯一の IPSec プロトコルです。フェーズ 2 ISAKMP ネゴシエーション時に使用する認証アルゴリズムを尋ねるプロンプトが出されます。

- 0 なし
- 1 HMAC-MD5
- 2 HMAC-SHA

**Phase2-ESP-Cipher-Algorithm**

ESP は、デフォルト・セキュリティーとして許可される唯一の IPSec プロトコルです。フェーズ 2 ISAKMP ネゴシエーション時に使用する暗号化アルゴリズムを尋ねるプロンプトが出されます。

- 1      ESP DES
- 2      ESP 3DES
- 3      ESP CDMF
- 4      ESP NULL

**Primary-Tunnel-Start**

装置と、1 次 LDAP サーバーを保護するセキュリティー・ゲートウェイとの間の、IKE トラフィックと IPSec トラフィック用に使用される装置の IP アドレス。

**Primary-Tunnel-End**

IKE トラフィックと IPSec トラフィック用に使用される 1 次 LDAP サーバーを保護するリモート・セキュリティー・ゲートウェイの IP アドレス。

**Secondary-Tunnel-Start**

装置と、2 次 LDAP サーバーを保護するセキュリティー・ゲートウェイとの間の IKE トラフィックと IPSec トラフィック用に使用される装置の IP アドレス。

**Secondary-Tunnel-End**

IKE トラフィックと IPSec トラフィック用に使用される 2 次 LDAP サーバーを保護するリモート・セキュリティー・ゲートウェイの IP アドレス。

**Set LDAP**

**set ldap** コマンドは、LDAP 操作パラメーターを構成するために使用します。

```
構文: set ldap          _anonymous-bind
                               yes
                               no
                               bind-name <name>
                               bind-pw <pw>
                               policy-base <string>
                               prietary <ip-address>
                               secondary <ip-address>
                               version <value>
```

**anonymous-bind [Yes または No]**

LDAP ディレクトリーに匿名でバインドするか、ユーザーが指定したバインド名とバインド・パスワードを使用してバインドするかを指定します。

## LDAP 構成コマンド (Talk 6)

デフォルト値: Yes

### **bind-name** <name>

LDAP サーバーのディレクトリーの検索を実行する前に、LDAP サーバーにバインドするために必要な情報を尋ねるプロンプトが出されます。*name* パラメーターは、ルーターが自身を識別するために使用する識別名を指定します。このパラメーターを入力しない場合、バインドは匿名の要求として出されます。

### **bind-pw** <pw>

LDAP サーバーのディレクトリーの検索を実行する前に、LDAP サーバーにバインドするために必要な情報を尋ねるプロンプトが出されます。*pw* パラメーターは、識別名に関連したパスワードです。このパラメーターを入力しない場合、バインドは匿名の要求として出されます。

### **policy-base** <string>

ルーターの SRAM と LDAP サーバーにあるポリシーを検索する範囲の定義に使用する文字列を入力するように、プロンプトが出されます。たとえば、このオプションを使用して、ルーター A、NHD、あるいは IBM-US だけに適用されるポリシーを得ることができます。*policy-base* は、LDAP サーバー内の DeviceProfile オブジェクトの識別名です。

### **primary** <ip-address>

ポリシーを検索する先の LDAP サーバーの IPv4 アドレスを尋ねるプロンプトが出されます。

### **secondary** <ip-address>

デフォルト・サーバーに到達できない場合に使用される、バックアップ LDAP サーバーの IPv4 アドレスを尋ねるプロンプトが出されます。

### **version** <value>

LDAP サーバーがサポートする LDAP バージョン番号を尋ねるプロンプトが出されます。

デフォルト値: 2 (許容値は 2 または 3 だけです)。

## Set Refresh

**set refresh** コマンドは、ポリシー・データベースの 1 日 1 回の自動リフレッシュを使用可能または使用不可にするために使用します。使用可能にすると、ポリシー・データベースは 1 日 1 回指定の時刻に自動的にリフレッシュされます。この機能を使用すれば、ネットワーク内のポリシーが使用可能になっているルーターが、LDAP ディレクトリー内で行われたポリシーの変更を自動的に取り込むことができます。このパラメーターをリセットするには、ポリシー機能の Talk 5 **reset refresh** コマンドを使用します。

構文: set refresh

enabled

yes

no

<time>

**enabled** [yes または no]

自動リフレッシュを実行するかどうかを指定します。

<time> enabled yes を指定した場合に、リフレッシュを実行する時刻 (24 時間形式) を指定します。

## ポリシー監視プロンプトへのアクセス

ポリシー機能のポリシー・コンソール部分を使用すれば、ポリシー・データベースにあるポリシーを表示して、個々のポリシーを使用可能または使用不可にすることができます。ポリシー監視環境にアクセスするには、OPCON プロンプト (\*) で **talk 5** と入力します。

\* t 5

次に、+ プロンプトで、次のコマンドを入力します。

```
+ feature policy
Policy>
```

## ポリシー監視コマンド

これらのコマンドを使用すれば、ポリシー・データベースに定義されているプロファイルを表示して、個々のポリシーを使用可能または使用不可にすることができます。表40 はポリシー監視コマンドの要約を示し、ここでの残りの部分でこれらのコマンドについて説明します。コマンドは Policy console> プロンプトで入力します。コマンドとオプションを 1 行に入力することも、コマンドだけを入力してプロンプトに答えることもできます。有効なコマンド・オプションのリストを表示するには、オプションの代わりに疑問符 (?) を指定してコマンドを入力します。

表 40. ポリシー監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxii ページの『ヘルプの入手』を参照してください。
使用不可	ポリシー・データベースにロードされたポリシーを使用不可にします。
Enable	ポリシー・データベースにロードされたポリシーを使用可能にします。
Reset	ポリシーに関連した基準をリフレッシュまたはリセットします。
Search	LDAP クライアントとサーバーとの間の活動をテストまたはデバッグします。
Status	ポリシー・データベースに関する情報を表示します。
List	LDAP 構成と定義済みポリシーに関する情報を表示します。
Test	ポリシー・エンジンを照会し、選択された規則を検索します。
Exit	直前のコマンド・レベルに戻ります。xxxii ページの『下位レベル操作環境の終了』を参照してください。

## Disable

**disable** コマンドは、ポリシー・データベースに現在ロードされているポリシーを使用不可にするために使用します。使用不可にしたポリシーの基準に一致するデータ・パケットには、デフォルト決定が適用されます。

## ポリシー監視コマンド (Talk 5)

構文: `disable` *<policy-name>*

## Enable

**enable** コマンドは、ポリシー・データベースに現在ロードされているポリシーを使用可能にするために使用します。使用可能にしたポリシーの基準に一致するデータ・パケットには、そのポリシーに対して構成された決定が適用されます。

構文: `enable` *<policy-name>*

## Reset

**reset** コマンドは、ポリシーに関連した基準をリフレッシュまたはリセットするために使用します。

構文: `reset` *ldap-config*  
*policy-database*  
*refresh-time*

### ldap-config

LDAP 構成 (**set ldap** コマンドで指定された) をメモリーに動的にロードします。変更内容は、次の検索操作時にアクティブになります。このコマンドは、ポリシー・データベースのリセットも強制的に出し、ポリシー・データベースのリフレッシュ時刻を非アクティブにします。

### policy-database

ポリシー・データベースをリフレッシュします。トンネル、フェーズ 1 とフェーズ 2 の SA をすべて停止し、RSVP と DiffServ のデータ構造をリセットし、ポリシー・データベースをフラッシュします。その後、ポリシーが LDAP サーバーからロードされ、自動開始が実行されます。データベースの再作成中は、LDAP サーバーとの間のパケットを除いて、パケットはルーターを出入りできません。

### refresh-time

ポリシー・データベースを 1 日 1 回自動的にリフレッシュする時刻を設定します。リフレッシュ時刻を使用不可にした場合、データベースはルーターがリブートまたはリスタートするまでリフレッシュされません。

## Search

**search** コマンドは、LDAP クライアントとサーバーとの間の活動をテストまたはデバッグするために使用します。ディレクトリーに対して検索を実行でき、検索結果を talk 5 で表示できます。

構文: `search` *filter*  
*ipaddress*

*filter* 検索操作のフィルター値を指定します。

*ipaddress* サーバーの IP アドレスを指定します。

## Status

**status** コマンドは、ポリシー・データベースに関する情報を表示するために使用します。

構文: `status`

**status** 最新のポリシー・データベースのリフレッシュ結果、リフレッシュ以後に経過した時間、および次回のリフレッシュがスケジュールされている時刻を表示します。

例:

```
Policy>status
Status of Last Search:      Failed
Time since last refresh:   4 seconds
Next Policy Refresh not scheduled
```

## List

**list** コマンドは、LDAP 構成とポリシーに関する情報を表示するために使用します。

構文: `list` `default-policy`  
`ldap`  
`policy`  
`refresh`  
`rule`  
`stats`

### default-policy

ポリシー・データベースのリフレッシュ時に使用するデフォルト・ポリシーをリストします。

**ldap** SRAM 内の LDAP 構成を表示します。

### policy

**basic** 論理ポリシー名によってポリシーのコンポーネントを表示します。ポリシーを 1 つ選択することも、すべてのポリシーを表示することもできます。リストは、Talk 6 での構成時に入力されたポリシーのコンポーネント名を表示します。

### complete

`list policy basic` と同じことを実行しますが、リストにはそれぞれの論理ポリシーごとにパラメーター値すべての完全リストが表示されます。

### generated

`list policy basic` と同じことを実行しますが、リストにはそれぞれの論理ポリシーごとに生成された規則すべての名前が表示されます。

### refresh

ポリシーのリフレッシュ状況 (使用可能または使用不可) とリフレッシュ間隔を表示します。

**rule** 次のオプションに従って、生成された規則に関する情報を表示します。

**basic** 生成された規則をすべて表示します。リストから規則を選択するこ



## ポリシー監視コマンド (Talk 5)

とも、すべての規則を表示することもできます。リストは、規則のコンポーネント名を表示します。コンポーネントには、次のものがあります。

**policy name**

**loaded from (LDAP or local)**

**state**

**priority**

**number of hits**

**profile**

**validity (次のものからなるアクション・リストが後に続く)**

IPSec (and, or)

ISAKMP (and, or)

DiffServ (and, or)

RSVP

### **complete**

rule basic と同じことを実行しますが、リストにはそれぞれのコンポーネントごとにパラメーターすべての名前が表示されます。

**stats** ヒットした規則とヒット数を表示します。規則には複数のアクションが存在する場合があります、すべてのアクションがヒットするとは限らないので、このオプションは規則のどのアクションがヒットしたか、およびその回数も表示します。

## Test

**test** コマンドは、ポリシー・データベースの動作を検査するために使用します。このコマンドを使用して、ポリシー・エンジンを照会して一致する規則を検索するセレクター・セットを入力できます。送信元アドレスとあて先アドレス、送信元ポートとあて先ポート、プロトコル ID、および TOS 値を尋ねるプロンプトが出されます。規則が一致した場合、コマンドは規則の名前を戻します。一致しなければ、*No match found* と表示します。

```
構文: test                               forwarder
                                           ISAKMP
                                           IPSec
                                           RSVP
```

### **forwarder**

IP 転送エンジンからのデータベース照会をシミュレートし、その照会から得られるポリシー決定を戻します。戻されるポリシーのタイプには、DiffServ 情報、IKE フェーズ 1 とフェーズ 1 情報、IPSec 手動トンネル ID などがあります。

### **ISAKMP**

フェーズ 1 ポリシー情報に対する IKE からのデータベース照会をシミュレートし、その照会から得られるポリシー決定を戻します。このオプションを使用する場合、送信元アドレスとあて先アドレスはトンネル終点 IP アドレスに設定し、プロトコルは 17 に、送信元ポートとあて先ポートは 500 に設定する必要があります。



## ポリシー監視コマンド (Talk 5)

| **IPSec** フェーズ 2 ポリシー情報に対する IKE からのデータベース照会をシミュレ  
| ートし、その照会から得られるポリシー決定を戻します。このオプションを  
| 使用する場合、送信元アドレスとあて先アドレスはトンネル・エンドポイン  
| ト IP アドレスに設定し、プロトコルは 17 に、送信元ポートとあて先ポート  
| は 500 に設定する必要があります。

| **RSVP** RSVP からのデータベース照会をシミュレートし、その照会から得られる  
| RSVP ポリシー決定を戻します。

## ポリシー監視コマンド (Talk 5)

## 第20章 IP セキュリティーの使用

この章では、IP セキュリティー機能の使用法について説明します。この章には、次の内容が記載されています。

- 『IP セキュリティーの概説』
- 334ページの『IP セキュリティーの概念』
- 343ページの『インターネット・キー交換の使用』
- 346ページの『公開キー・インフラストラクチャーの使用』
- 350ページの『手動 IP セキュリティーの使用 (IPv4)』
- 350ページの『手動 IP セキュリティーの使用 (IPv6)』

### IP セキュリティーの概説

ここでは、IPv4 と IPv6 の両方に使用できる IP セキュリティーの機能を概説します。

### 保護トンネルの使用

別のホスト、ルーター、またはファイアウォールに送信される IP パケットを保護するために、保護する必要のあるそれぞれの IP ルートごとに保護トンネルを構成できます。IPsec トンネルは、ローカル・ルーターが保護 IP パケットを転送するためのリモート・ホスト、ルーター、またはファイアウォールへの両方向の論理接続です。保護トンネルは、送信元ホストとあて先ホストのアドレス、ポート番号、トンネル ID などのパラメーターによって識別されます。

IPv4 では、ポリシー・データベースにトンネル・ポリシーを構成することによって、ネゴシエーションされたトンネルを定義でき、366ページの『ルーター A のトンネルの構成』に説明されているように `Talk 6 add tunnel` コマンドを使用して、手動トンネルを作成できます。IPv6 では、`Talk 6 add tunnel` コマンドを使用します。

保護 IPsec トンネルを確立するために、ポリシーは特殊な認証ヘッダーを付ける IP 認証ヘッダー (AH) 機能 (336ページの『IP 認証ヘッダー』を参照)、および IP カプセル化セキュリティ・ペイロード (ESP) 機能 (337ページの『IP カプセル化セキュリティ・ペイロード』を参照) を指定できます。ポリシーは、パケットに対して次のセキュリティ方式のどれを設定するかを決定します。

- AH アルゴリズムと AH 認証キー (356ページの『アルゴリズムの構成』、または 368ページの『アルゴリズムの構成』の該当する方を参照してください)。
- ESP 暗号化アルゴリズム、および ESP 暗号化キーと暗号化解除キー (356ページの『アルゴリズムの構成』、または 368ページの『アルゴリズムの構成』の該当する方を参照してください)。
- セキュリティー・パラメーター・インデックス (SPI) (338ページの『セキュリティ・アソシエーション』を参照してください)。

注: それぞれの保護トンネルの送信側と受信側は、同じオプションを選択する必要があります。

### IP セキュリティーの概念

インターネット・プロトコル (IP) を使用して送信されるパケットは、2212 の IP セキュリティー機能を使用して保護することができます。

セキュリティー (インターネット・プロトコルの RFC 2401 セキュリティー体系によって定義) は、次の機能で成り立っています。

**認証** 受信したデータは送信されたデータと同じであること、および提示された送信側が確かに実際の送信側であることが分かっている。

**健全性** データが変更されずに発信元からあて先に転送されることが保証される。

**機密性** 指定の受信側は何が送信されたのかを知っているが、当事者以外は何が送信されたのかを判別できないようにして通信する。

**非否認** 後で送信側がそのデータを送信したことを否定しても、受信側は送信側が確かに所定のデータを送信したことを証明できる方法で通信する。

**注:** 一部の国では、米国の輸出規制や暗号化パラメーターが表示されないなどの理由で、暗号化サポートが提供されない場合がありますが、ESP-NUL アルゴリズムは、どこでも利用可能です。ESP-NUL アルゴリズムの定義については、337 ページの『ESP 暗号化アルゴリズム』を参照してください。

### IP セキュリティー用語

IPv4 に関連した IPSec を説明するために、次の用語が使用されています。

#### 認証ヘッダー (AH)

データの発信元の認証、およびデータ健全性と再生保護を提供するパケット・ヘッダー情報があるデータ域。

**証明書** 終端エンティティーの ID をその公開キーと結び付ける ASN.1 コード化データ項目 (ITU X.509 標準に準拠)。(この場合、終端エンティティーは ISAKMP ネゴシエーション・エンティティーです。) 終端エンティティーは、認証要求を提出することによって、ID と公開キーを認証局 (CA) に登録する必要があります。CA は要求を検査し、要求に署名して、エンティティーに証明書を発行します。ISAKMP は、フェーズ 1 プロセス中に公開キー証明書を使用して、ルーター間のマスター機密 (暗号キー) を設定する初期メッセージ交換を認証します。

#### 認証局 (CA)

ネットワーク・ユーザーが ISAKMP を使用して保護ユーザー・データを交換するために使用する必要がある『署名入り』X.509 デジタル証明書を発行する信頼のおける公共機関。ISAKMP に対応した相手方との保護データ交換に参加するには、ルーターを CA に登録して、認証の際に使用する X.509 デジタル証明書を取得する必要があります。

#### デジタル署名

X.509 デジタル証明書の一部を構成するユーザーのコード化された ID を含むデータ項目。ユーザーは、フェーズ 1 ネゴシエーション時に証明書を交換して、互いを認証します。署名は、署名する入力データ域に対して公開キー操作を実行することによって生成されます。

**カプセル化セキュリティー・ペイロード (ESP)**

受信側以外がその内容を判別できないように、データグラムをカプセル化して暗号化する IPSec の機能。この機能は、データ保全性と再生保護を提供します。ESP は、データ発信元の認証も行います。この機能は、2 つのモードで稼働します。トランスポート・モードでは、元のデータグラムのペイロードだけを暗号化し、アドレス指定情報は無許可の相手方に見えます。トンネル・モードでは、ヘッダーを含む元のデータグラム全体が暗号化されます。このモードは、機密のアドレス情報を隠します。

**インターネット・キー交換 (IKE)**

ISAKMP プロトコルと Oakley プロトコルから派生したプロトコルで、インターネット・コミュニティーが暗号キーを交換し、通信の相手方を認証するために使用します。

**ISAKMP**

インターネット・セキュリティー・アソシエーションおよびキー管理プロトコル (Internet Security Association and Key Management Protocol)。この機能は、セキュリティー・アソシエーションを自動的に設定し、データ交換を行っている間パケットの暗号キーを管理します。

**管理情報ベース (MIB)**

ルーターの操作に関する統計情報を要求した信頼のおける中央の公的機関からの照会に応答して、ルーターが送信するデータ・ブロック。公的機関は、ネットワーク内の問題を検出して、担当者に修正処置を行うように連絡できます。

**Oakley**

ISAKMP が使用する暗号キー管理プロトコル。

**パーフェクト・フォワード・セクレシー (PFS)**

フェーズ 2 ネゴシエーションが、それぞれのネゴシエーションのたびに新しい暗号化キー情報を得る場合に得られるデータ・セキュリティーのレベル。ISAKMP は、通信者間で公開 Diffie Hellman 値を交換できるようにすることによって、これを実現しています。このセキュリティー機能は、以前に悪用されたキーから現行の暗号キーが判別されるのを防ぎます。

**フェーズ 1 ネゴシエーション**

フェーズ 2 ネゴシエーション時に交換される ISAKMP メッセージを保護する、ISAKMP セキュリティー・アソシエーションと暗号キーを確立する送信側と受信側との間の通信。フェーズ 1 はプロセッサに負担をかけるもので、通常は 1 日や 1 週間に 1 回だけのように、低い頻度で行われます。

**フェーズ 2 ネゴシエーション**

送信側と受信側との間で ISAKMP メッセージを交換する処理で、このときにユーザー・データの交換を保護するセキュリティー・アソシエーションと暗号キーがネゴシエーションされます。これらのネゴシエーションは、通常は 2 ～ 3 分間隔のように頻繁に行われ、ユーザーの介入なしで暗号キーを定期的に取りフレッシュするために使用されます。

**プロキシ**

別のネットワーク装置に代わって作動するように割り当てられたルーター。

## IP セキュリティーの使用

### 公開キー・インフラストラクチャー (PKI)

ユーザーの ID を公開キーと結合し、セキュリティーを保証しながら結合された公開キーを配布するために、CA が使用するフレームワーク。

### 高速モード

非 ISAKMP セキュリティー・アソシエーションを確立するためのフェーズ 2 ネゴシエーションを記述するために使われる用語。

**再生** データグラムを取り込んで、その内容を判別したり、データグラムを繰り返し再送してサービス妨害 (denial-of-service) 攻撃を仕掛けたりしようとする事。

### セキュリティー・アソシエーション (SA)

データ・パケットに関する情報 (暗号化アルゴリズムやキー情報など)、関係者の識別などを結び付けるデータ域。

**変換** 認証の構成と暗号化の選択に関する情報の名前付き集合。

## IP 認証ヘッダー

認証ヘッダー (AH) は、RFC 2402 IP Authentication Header に記述されています。このヘッダーには、IP データグラムの認証データが入っています。

ネゴシエーションされた IPSec を使用する IPv4 の場合、データグラムに割り当てられるポリシーは、インターネット・キー交換 (IKE) プロトコルと公開/プライベート・キーのペアに依存する暗号認証機能を設定しています。IPv4 手動トンネルと IPv6 の場合は、送信側は機密の認証キーに依存する暗号機能を使用します。どちらの場合も、暗号認証機能はデータグラムの内容に適用されます。AH は、単独で指定することも、ESP と一緒に指定することもできます。詳しくは、337ページの『AH と ESP の使用』を参照してください。

### AH 認証アルゴリズム

AH トンネル・ポリシーを使用する保護トンネルは、次の認証アルゴリズムのうちの 1 つを使用する必要があります。

- 再生防止付き HMAC-MD5 IP 認証
- 再生防止付き HMAC-SHA-1 IP 認証

これらの AH アルゴリズムは、暗号ハッシュ (ハッシュ・メッセージ認証コード、HMAC と省略される) を使用して、キーによるメッセージ認証機能とオプションの再生防止機能を結合します。再生防止機能は、AH に入っているシーケンス番号を使用して、パケットが以前に受信されていないかどうかを検査します。再生防止機能は、受信側をサービス妨害 (denial-of-service) 攻撃から保護します。この攻撃では、同じパケットが繰り返し送信されて、ルーターが重複パケットの処理に忙殺され、正当なトラフィックを処理できなくなります。認証コードは、機密暗号キーとデータに適用され、その後プライベート・キーの出力と最初の操作の出力に適用されます。HMAC-MD5 がこれを行う方法を、337ページの図32 に図示します。

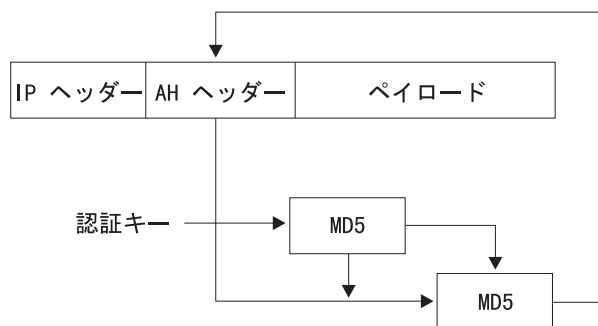


図 32. HMAC MD5 認証メッセージの作成

## IP カプセル化セキュリティー・ペイロード

IP カプセル化セキュリティー・ペイロード (ESP) は、RFC 2406 IP Encapsulating Security Payload に記述されています。ESP は、IP パケットの一部または全部を暗号化して、認証 (オプション) と保水性に加えて機密性を提供します。ただし、ESP-NULL アルゴリズムを選択した場合、ESP は認証と保水性の検査だけを実行します。ESP は、単独で指定することも、AH とともに指定することもできます。詳しくは、『AH と ESP の使用』を参照してください。

### ESP 認証アルゴリズム

ESP 認証に使用できるアルゴリズムは AH の場合と同じで、すでに 336 ページの『AH 認証アルゴリズム』に説明されています。

### ESP 暗号化アルゴリズム

ESP 暗号化ポリシーを使用する保護トンネルは、次の暗号化アルゴリズムのどれか 1 つ、または ESP-NULL アルゴリズムを使用する必要があります。

- 暗号化ブロック・チェーン方式のデータ暗号化規格 (DES-CBC)
- 商業データ・マスキング・ファシリティー (CDMF)
- トリプル DES (3DES)

**注:** ESP-NULL を除いて、ESP 暗号化アルゴリズムは米国の輸出規制の対象になっています。ご使用の 2212 で、これらのアルゴリズムの一部または全部を使用できない場合、これらのアルゴリズムの販売が禁止されている可能性があります。詳しくは、IBM 営業担当員にお尋ねください。

ESP-NULL アルゴリズムは、クリアテキスト・データは暗号化せず、すべての国で利用可能です。このアルゴリズムは、ESP 認証と保水性検査だけを使用可能にし、暗号化は行いません。ESP-NULL を使用する場合は、ESP 認証アルゴリズムのどれか 1 つを使用する **必要があります**。

## AH と ESP の使用

保護トンネルは、AH、ESP、AH-ESP、または ESP-AH のどれか 1 つの認証/暗号化を使用できます。AH と ESP を組み合わせて使用する場合は、次のことが当てはまります。



## IP セキュリティーの使用

- ポリシー AH-ESP は、アウトバウンド・パケットに対して認証の前に暗号化を実行することを示します。この場合、あて先ルーターでは AH 認証機能がまず実行され、インバウンド・パケットが検査されて、認証をパスしたパケットだけが ESP に転送されて暗号化解除されます。
- ポリシー ESP-AH は、アウトバウンド・パケットに対して暗号化の前に認証を実行することを示します。この場合、あて先ルーターでは ESP 機能がまずインバウンド・パケットを暗号化解除し、正常に暗号化解除されたパケットだけが AH 認証機能に転送されます。

## セキュリティー・アソシエーション

セキュリティー・アソシエーション (SA) は、伝送するトラフィックにセキュリティー・サービスを提供する単方向『接続』です。セキュリティー・サービスは、AH または ESP (ただし両方ではない) を使用して SA に提供されます。トラフィック・ストリームに AH と ESP の両方の保護が適用された場合は、2 つ (以上) の SA が作成されてトラフィック・ストリームを保護します。2 つのホスト間や 2 つのセキュリティー・ゲートウェイ間で通常の両方向通信を保護するには、2 つの SA (それぞれの方向に 1 つずつ) が必要です。

## トンネル・モードとトランスポート・モード

動作モード (トンネルまたはトランスポート) は、IPSec が IP パケットを処理する方法を決定します。トンネル・モードがデフォルトで、ルーターがセキュリティー・ゲートウェイとして動作している場合は、トンネル・モードが必須です。トンネル・モードは、ネットワーク内のパスの単一セグメント上でデータを保護します。トランスポート・モードは、ルーターがホストとして動作している場合にだけ使用でき、終端間でパス全体に沿ってデータを保護します。

### AH と動作モード

トンネル・モードでは、AH は IP パケットの前に置かれ、新しい IP ヘッダーが作成されて AH の前に置かれます。トンネル伝送されるパケットの IP ヘッダー (内部ヘッダー) には、パケットの最終的な発信元とあて先のアドレスが入ります。新規 IP ヘッダー (外部ヘッダー) には、セキュリティー・ゲートウェイ (トンネルのエンドポイント) のアドレスを入れることができます。AH は、新規 IP ヘッダー内の可変フィールドを除いて、新規 IP ヘッダーとトンネル伝送される IP パケットの両方を含めた新規パケット全体を保護します。

トランスポート・モードでは、AH は IP ヘッダーの後と高位レイヤー・プロトコル (TCP または UDP など) ヘッダーの前に挿入されます。このモードでは、AH は高位レイヤー・プロトコル・ヘッダーと IP パケットの内容を認証します。ただし、IP パケットの可変フィールド (たとえば、活動時間 [TTL]、チェックサム、フラグメント・フラグ、フラグメント・オフセット、およびサービス・タイプ [TOS] など) は除きません。

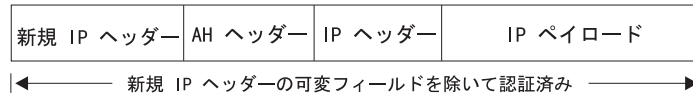
339ページの図33 は、AH によって保護されたデータグラムの形式を示しています。



オリジナル・データグラム



AH トンネル・モードによって保護されたオリジナル・データグラム



AH トランスポート・モードによって保護されたオリジナル・データグラム

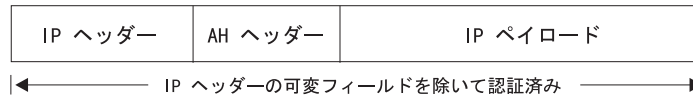


図 33. AH によって保護されたデータグラムの形式

## ESP と動作モード

トンネル・モードでは、ペイロード・データには IP パケット全体が入れられ、新規の IP ヘッダーが作成されて ESP ヘッダーの前に置かれます。トンネル伝送されるパケットの IP ヘッダー (内部ヘッダー) には、パケットの最終的な発信元とあて先のアドレスが入り、新規の IP ヘッダー (外部ヘッダー) には、セキュリティ・ゲートウェイのアドレスが入ります。ESP は、トンネル伝送 IP パケットを暗号化します。ESP 認証を使用すると、ESP ヘッダー、トンネル伝送 IP パケット、および ESP トレーラーが認証されます。

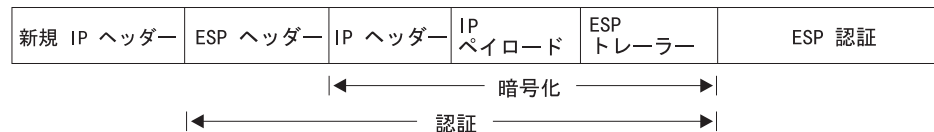
トランスポート・モードでは、ペイロード・データには、高位レイヤー・プロトコル・データ (TCP データや UDP データなど) が入れられます。認証を使用すると、ESP ヘッダー、高位レイヤー・プロトコル・データ、および ESP トレーラーが認証されます。

図 34 は、ESP によって保護されたデータグラムの形式を示しています

オリジナル・データグラム



ESP トンネル・モードによって保護されたオリジナル・データグラム



ESP トランスポート・モードによって保護されたオリジナル・データグラム

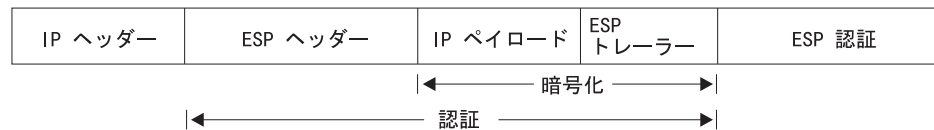
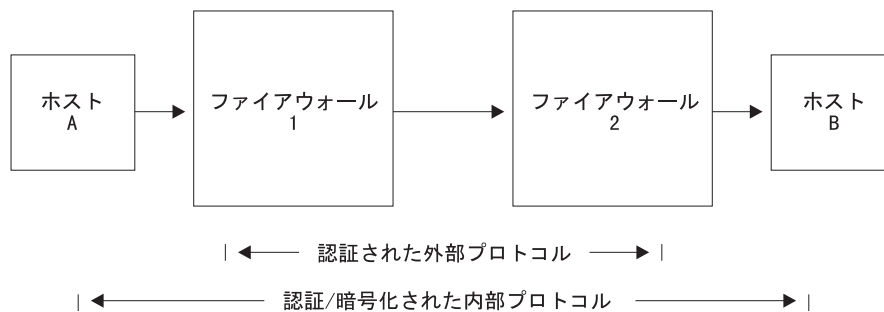


図 34. ESP によって保護されたデータグラムの形式

## IP セキュリティの使用

### AH と ESP のネスト

あるプロトコルをそれ自身の別のインスタンスの中にネストしたり、他のプロトコルの中にネストしたりすることができます。図35 は、ESP によって保護されたデータグラムを AH トンネルの中にネストした結果を示しています。



ホスト A は ESP トランスポートを使用する

IP ヘッダー	ESP ヘッダー	IP ペイロード	ESP トレーラー	ESP 認証
---------	----------	----------	-----------	--------

ファイアウォール 1 は AH トンネルを使用し、新規 IP ヘッダーを追加する

新規 IP ヘッダー	AH ヘッダー	IP ヘッダー	ESP ヘッダー	IP ペイロード	ESP トレーラー	ESP 認証
------------	---------	---------	----------	----------	-----------	--------

ファイアウォール 2 は AH トンネル・データグラムを受信し、認証して、外部ヘッダーと AH ヘッダーを取り除く

IP ヘッダー	ESP ヘッダー	IP ペイロード	ESP トレーラー	ESP 認証
---------	----------	----------	-----------	--------

図35. AH トンネル内での ESP のネスト

### L2TP パケットに対する IP セキュリティの使用

IPv4 では、IPSec を使用して L2TP パケットを保護することもできます。UDP パケット内の L2TP フレームをカプセル化することによって L2TP トンネルを作成した後、トンネルの両端点を定義する送信元アドレスと宛先アドレスをもつ IP パケット内に UDP パケットをカプセル化できます。その後、IP パケットに AH、ESP、および ISAKMP の各プロトコルを適用できます。図36 は、インターネット経由での伝送のために PPP とそのペイロード・プロトコルを組み込んでいる IP カプセル化された L2TP パケットを示しています。

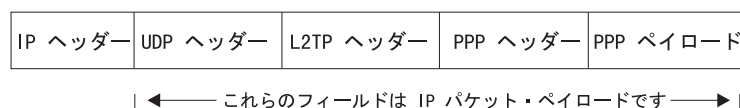


図36. IPSec によって保護された L2TP パケット

## トンネル内トンネル・モード

セキュリティ向上のために、前述したセキュリティ機能に加えて、トラフィック・ストリームのパケットを 2 回カプセル化し、まず 1 つの IPSec トンネルを通してパケットを伝送し、次に別のトンネルを通して伝送する (トンネル内トンネル) ことができます。

**注:** ルーター内での多重暗号化の使用 (暗号化が両方のトンネルに対して実行される場合に、トンネル内トンネル・モードを使用すること) は、米国政府の輸出規制によって制限されます。多重暗号化は、厳密な輸出管理下にあるソフトウェア・ロード (128 ビット・キーと三重 DES を使用する RC4 をサポートするソフトウェア・ロード) だけでサポートされます。

IPv4 では、ポリシー・データベースの規則が、第 1 のトンネルでカプセル化される (内側) パケットを指定します。そして、そのパケットが送信される前に、その規則によってパケットが第 2 のカプセル化 (外側) のために第 2 のトンネルに送られます。IPv6 では、パケット・フィルターのアクセス制御規則が、第 1 のトンネルでカプセル化される (内側) パケットを指定します。そして、そのパケットが送信される前に、第 2 の規則によってパケットが第 2 のカプセル化 (外側) のために第 2 のトンネルに送られます。

2 つの IPSec トンネルは同じルーターを起点とし、トンネルのリモート側は同じ物理位置にありますが、異なるマシン上にあります。最初のトンネルのリモート側は、保護ゲートウェイでもホストでも構いませんが、2 番目のトンネルのリモート側は保護ゲートウェイにする必要があります。トンネルのあて先が異なるので、トンネルのリモート IP アドレスは異ならなければなりません。トンネル内トンネル用に使用されるトンネルは、両方ともトンネル・モードに構成する必要があります。2 番目のトンネルでは追加埋め込みを使用できません。

パケットは、2 度カプセル化された後で、第 2 の (外側) トンネルを通して送信されます。そのトンネルの終端で、外側のカプセル化は除去され、最初のトンネルのカプセル化によって作成されたヘッダーの情報に基づいて、パケットは最初のトンネル (内側) に転送されます。このトンネルの終端で、内側のカプセル化が除去され、パケットはその最終あて先に転送されます。

## パス最大伝送単位ディスカバリー

IPv4 と IPv6 の両方とも、2212 がセキュリティ・ゲートウェイとして動作している場合に、IPSec はパス最大伝送単位 (PMTU) ディスカバリーをサポートします。PMTU ディスカバリーのサポートは、パケットを断片化できない場合に必要になります。IPv4 では、断片化不可 (DF) ビットがセットされているとパケットを断片化できません。IPv6 では、中間ルーターによってパケットを断片化できません。このような場合、パケットが保護トンネルの一端から他端までのパス内のリンクに収まらないと、『packet too big』という ICMP エラー・メッセージがパケットの発信元に送信されます。

ルーターはセキュリティ・ゲートウェイとして機能しているので、このエラー・パケットは、パケットの本当の発信元ではなく、発信側ルーターに戻されます。受信側ルーターは、本当の発信元に報告された MTU をパスする必要があります。こうすれば、発信元はパケットが最終あて先に到達するように、パケット・サイズを減

## IP セキュリティーの使用

らすことができます。PMTU ディスカバリーのサポートについては、インターネット・プロトコルに関する RFC 2401 - Security Architecture に記述されています。

IPv4 は、トンネル伝送されるパケットの外部ヘッダーの DF ビット設定として、次のオプションを備えています。

1. 内部ヘッダーからコピーする
2. 常にセットする
3. 常にクリアする

これらのオプションは、保護トンネル内トンネル・モードを構成する際に使用できます (たとえば、ポリシー機能の **add ipsec-manual-tunn** (IPv4)、または **Talk 6 add tunnel** (IPv6) コマンドを使用する場合)。DF ビットは選択されたオプションに応じて処理されますが、次の場合は例外です。

- トンネル MTU が最小 MTU に等しい。
- インバウンド・パケットのサイズが最小 MTU 以下である。
- カプセル化パケットのサイズが最小 MTU より大きい。

このような場合、IPv4 では構成に関係なく DF ビットはセットされず、保護パケットは受信側へのパス上で必要に応じて断片化できます。IPv6 では、セキュリティー・ゲートウェイを出たパケットは、トンネルの PMTU に収まるように必要に応じて断片化できます。インバウンド・パケットはすでに最小 MTU 以下であり、発信元ホストはサイズをそれ以上縮小できないので、この特別処置が必要になります。断片化ができないと、このパケットは永久に最終あて先に到着できないこととなります。

PMTU は、ネットワーク・トポロジーや構成の変更によって変更されることがあるので、PMTU 値を定期的にエージング処理して、最大値にリセットする必要があります。エージング・タイマーの値は、デフォルトでは 10 分で、**Talk 6 set path** コマンドを使用して構成できます。エージング・パラメーターを 0 に設定すると、PMTU エージングが使用不可になります。

## IP セキュリティー・トンネルを使用したネットワークの図

343ページの図37 は、ルーター A (IPSec を使用) をルーター B (IPSec と IPv4 用のネットワーク・アドレス変換の両方を使用) に接続する IPSec トンネルが 2 つあるネットワークの例です。

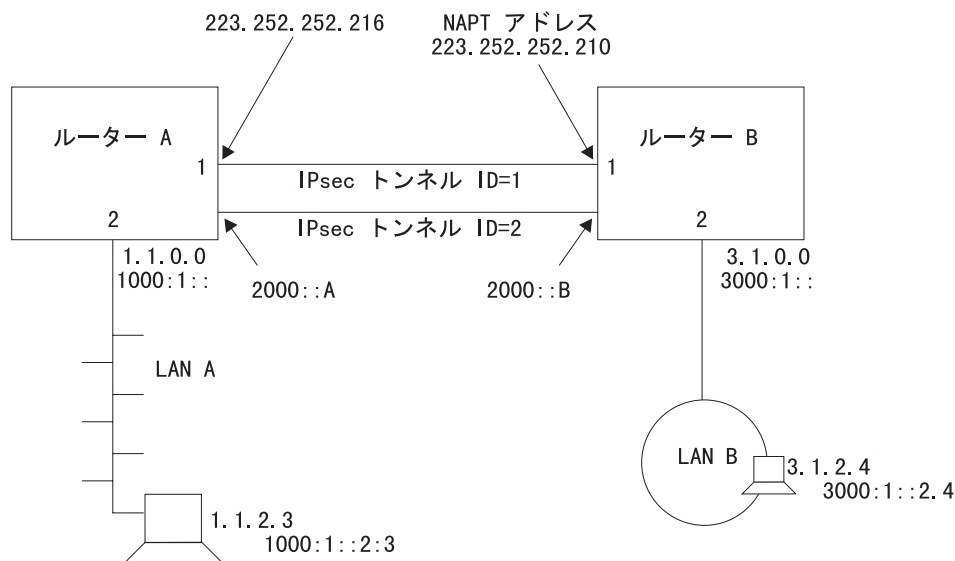


図 37. IPsec と NAT を使用したネットワーク

このネットワークでは、IPsec トンネル ID 1 をもつ IPsec トンネルが、ルーター A の IPv4 アドレス 223.252.252.216 からルーター B の IPv4 アドレス 223.252.252.210 に構成されています。ルーター A は IPsec 用に構成されています。ルーター B は、IPsec と NAT の両方用に構成されています。

このネットワークでは、IPsec トンネル ID 2 をもつ IPsec トンネルが、ルーター A の IPv6 アドレス 2000::A からルーター B の IPv6 アドレス 2000::B に構成されています。

IPv4 の場合、このネットワークを IKE 用に構成するには、351ページの『インターネット・キー交換の構成 (IPv4)』から始まる手順を実行します。手動 IPsec を使用する IPv4 の場合は、366ページの『手動トンネルの構成 (IPv4)』から始まる手順を実行します。IPv6 の場合は、369ページの『手動トンネルの構成 (IPv6)』から始まる手順を実行します。

**注:** ネットワークで NAT を使用しない場合でも、ルーター B の構成の説明をお読みになれば、IPsec トンネルの両端にあるパラメーターの関係を理解するのに役立ちます。

## インターネット・キー交換の使用

ここでは、インターネット・キー交換 (IKE) を使用して、IPsec セキュリティー・アソシエーションの定義と作成を自動化する方法を説明します。IKE は、IETF (RFC 2409) によってサポートされている標準で、ベンダーを問わず IPsec に対応した製品がセキュリティ要件に関する通信を行うための標準方式です。

IKE は、次のセキュリティ要件を満たすためのフレームワークを提供します。

## IP セキュリティーの使用

### リモート・ネゴシエーション・エンティティーの認証 (IKE ピア)

事前共有キーまたはデジタル証明書を使用して、エンティティーの身元を証明することによって、IKE は通信相手のエンティティーの識別を認証します。

### 両ピアでの同一キー・マテリアルの作成

Diffie-Hellman 公開/秘密キー・メカニズムを使用して、IKE は公開キー・コンポーネントの交換と、それぞれのピアによる同一キーの独立生成を実行します。

### IPSec セキュリティー・アソシエーションのネゴシエーションの保護を提供

IKE は、後述する 2 フェーズ・プロセスによって、IPSec トンネルのネゴシエーションを保護するためだけに使用されるセキュリティ・アソシエーションの作成と、IPSec がユーザー・データを保護するために使用するセキュリティ・アソシエーションの実際のネゴシエーションと作成を実行します。

## インターネット・キー交換フェーズ

IKE は、2 つの別個なネゴシエーション交換、フェーズ 1 とフェーズ 2 を定義しています。フェーズ 1 は、IKE ピア間の保護トンネルを設定します。このトンネルは、後続の IPSec トンネルのネゴシエーションを保護します。フェーズ 1 の間には、次の処理が示された順序で実行されます。

1. フェーズ 1 セキュリティー・アソシエーションの特性が、IKE ピアによってネゴシエーションされ、承認される。この特性には、IKE 通信を暗号化するために使用される暗号化アルゴリズム、使用されるハッシュ・アルゴリズム、認証方式、キーの生成時に使用される Diffie-Hellman グループなどがあります。
2. Diffie-Hellman キーが生成され、公開部分が IKE ピアと交換される。これらのキーは、両方のフェーズ 1 ネゴシエーションを暗号化する暗号化キーの生成に使用され、IPSec トンネルによって使用されるキーの生成も可能にします。
3. サポートされる 2 方式 (事前共有キー・モードと署名モード) のどちらかを使用して、IKE ピアが認証される。

事前共有キー・モードでは、事前のオフライン・プロセスによって両方の IKE ピアがキーを交換しており、このキーはフェーズ 1 の間にピアを認証するために使用されます。事前共有キーは、ポリシー機能の **add user** コマンドを使用して構成します。

署名モードでは、フェーズ 1 メッセージのペイロードの暗号化と暗号化解除に使用するキーを作成するために、署名入りの X.509 デジタル証明書が使用されます。署名と検証が正常に行われれば、ピアは認証されます。署名モードと X.509 デジタル証明書の使用について詳しくは、346ページの『公開キー・インフラストラクチャーの使用』を参照してください。

フェーズ 1 ネゴシエーションは、次に示す 2 つの交換モードのどちらかを使用して実行できます。

- メイン・モードは、6 つのメッセージを使用してフェーズ 1 ネゴシエーションを実行し、ネゴシエーション対象のピアの識別情報を暗号化します。
- アグレッシブ・モードは、3 つのメッセージを使用してフェーズ 1 ネゴシエーションを実行します。ピアは、最初の 2 つのメッセージ内で無保護の識別情報を交換します。



## IP セキュリティー・トンネルのネゴシエーション

ここで説明する処理は、ポリシー・データベースで定義された規則に一致する属性を持つパケットの送信をルーターが準備する際に行われます。トンネルのネゴシエーションは、2つのフェーズで行われます。フェーズ 1 では、送信側のルーターが 6つのメッセージ交換のうち最初のメッセージを送信することによって通信を開始します。このメッセージは、フェーズ 2 で使用されるセキュリティー・オプションを設定します。受信側は応答し、両者は ISAKMP セキュリティー・アソシエーション (SA) 特性と、使用する認証と暗号化のアルゴリズムをネゴシエーションし、互いの識別を認証します。フェーズ 2 では、両者は合計 3つのメッセージを交換して、両者間で送信される IP データグラムの保護に使用する SA とキーをネゴシエーションします。フェーズ 1 は、次のように進行します。

1. メッセージ 1: 送信側は、通信活動を実行する方法を提案する。提案されるのは、認証方式 (例: デジタル証明書)、認証アルゴリズム (例: HMAC-MD5)、および使用される暗号化アルゴリズム (例: DES-CBC) です。
2. メッセージ 2: 受信側は、サポートするセキュリティー・オプション (存在する場合) を送信側に示す。
3. メッセージ 3: 送信側は、自身の Diffie Hellman 公開値と、暗号化キーの作成に使用されるランダムな値を送信する。
4. メッセージ 4: 受信側は、自身の Diffie Hellman 公開値と、暗号化キーの作成に使用されるランダムな値を送信する。この時点で、両者は ISAKMP メッセージ交換の際に使用される公開キーとプライベート・キー、およびキーに関連した情報を作成します。
5. メッセージ 5: 送信側がデジタル署名を送信する。送信側は、信頼のおける認証局 (CA) によって署名された X.509 デジタル証明書を組み込む場合もあります。送信側が有効な証明書を組み込まなかった場合、受信側は LDAP プロトコルを使用して、信頼のおける CA、保護 DNS サーバー、またはすでに使用済みの証明書をそれぞれの ID 値にマップする保護ローカル・キャッシュから証明書を取得する必要があります。送信側に証明書を要求することもでき、送信側は即時に証明書を送信する必要があります。
6. メッセージ 6: 送信側のデジタル署名を検証した後、受信側は自身に関する同様な識別情報を送信側に送信する。

この時点では、両者は互いを認証し、SA の特性について合意し、ISAKMP SA を処理するためのキーとキーに関連した情報を得ました。次に両者はフェーズ 2 に入り、両者間で交換される IP データグラムの保護に使用する 非 ISAKMP SA とキーをネゴシエーションします。フェーズ 2 は、次のように進行します。

1. メッセージ 1: 送信側は、AH または ESP のアルゴリズム選択項目を送信して非 ISAKMP SA を提案し、その他のセキュリティー関連情報も含める。
2. メッセージ 2: 受信側は、選択したプロポーザルを送信側に示し、セキュリティー関連情報も含める。
3. メッセージ 3: 送信側は、数項目のハッシュ・レコードを送信して、ネゴシエーションされたセキュリティー・プロトコルを使用して続行する準備ができたことを受信側に示す。受信側が情報を検証すると、リンクが完了し、両者は保護データ・ストリームの交換を開始できます。

## 公開キー・インフラストラクチャーの使用

ここでは、公開キー・インフラストラクチャー (PKI) を使用する方法を説明します。PKI を使用して、IKE は IKE エンティティーを認証する公開キー署名モードをサポートします。本リリースは、PKI サポートを必要としない事前共有キー・モードをサポートしていますが、このモードには固有の欠点があります。このモードでは認証のために、各 IKE エンティティーをそのピアそれぞれの事前共有キーを使用して構成する必要があります。このことは、IKE 操作のスケラビリティを大きく制限します。公開キーに基づいた署名や、公開暗号化モードを使用すれば、はるかに高いスケラビリティが得られます。本リリースでは、IKE エンティティーを認証するために、署名モードの IKE フェーズ 1 ネゴシエーションで X.509 デジタル証明書を使用しています。

ユーザーは、IKE ネゴシエーションに関係させるそれぞれの IKE エンティティーに識別を割り当てます。このためには、エンティティーのユーザー・ポリシー・プロファイルの構成時に、ISAKMP ID フィールドに固有な値を指定します。それぞれの IKE エンティティーは、そのピアを使用して識別を認証します。

PKI は、公開キー操作をサポートするために現在定義、開発中です。PKI では、X.509 デジタル証明書が、エンティティーの公開キーとエンティティーが要求した識別を結び付けます。IKE エンティティーは、証明書に含まれている公開キーを取り出すことができ、その後公開キー操作を実行して、IKE ネゴシエーションに関係するピアの識別を認証できます。公開キーは、IKE 署名モードで使用されます。このモードでは、署名者はプライベート・キーを使用してデジタル署名を行います。受信側は、証明書から署名者の公開キーを取り出し、公開キーを使用して署名を検証します。デジタル証明書機能は、一方の IKE エンティティーが他方の IKE エンティティーの識別を認証するための、スケラブルな方式です。

## PKI の構成

本リリースは、ネゴシエーションに関係する両方の IKE エンティティーが同じ CA を使用することを前提としています。署名を使用して IKE ネゴシエーションを開始する前に、ルーター用に PKI を構成する必要があります。ルーターのプライベート・キーとルーター証明書を生成し、ルート CA の証明書をダウンロードする必要があります。次の手順では、PKI を構成する方法を説明します。

### 1. キー・ペアを生成し、証明書を要求する。

公開キー操作にはキー・ペアが必要なので (署名モードは、署名にプライベート・キーを使用し、検証に公開キーを使用します)、ルーター用のキー・ペアを生成する必要があります。証明書を要求するには、X.509 デジタル証明書に入れる生成された公開キーを CA に送信する必要があります。この後、すべての IKE ピアが、CA が発行した証明書からこの公開キーを取り出すことができます。プライベート・キーはルーターに常駐し、機密を保持されます (ルーターだけに知られている)。

本バージョンでは、次のことを行う **certificate request** コマンドを出すことができます。

- a. キー・ペアを生成する。キーの長さは、512 ビット、768 ビット、または 1024 ビットに指定できます。生成されたプライベート・キーはキャッシュ内に留まります。



- b. 証明書要求に含める情報を入力するようにユーザーに要求する (たとえば、IP アドレス形式のルーター ID、ドメイン名、電子メール名)。
  - c. 生成された公開キーとユーザーが入力した情報が入った証明書要求を作成する (PKCS#10 形式で)。
  - d. 証明書要求をホスト・マシンに TFTP によって送信する。
2. 証明書を発行する (ルーターの外部)

CA は、PKCS#10 証明書要求を受け取ります。CA は手作業で要求を検証して、証明書を発行できます。証明書には、ルーターの公開キーと、ユーザーが入力した情報が含まれています。CA はプライベート・キーを使用して証明書に署名するので、署名した CA をユーザーが信頼しているかぎり、証明書は信頼されたデジタル情報になります。これで、証明書を IKE ネゴシエーションに使用できるようになります。(この処理はルーターの操作の範囲外で、本書では詳しく説明しません。)

3. ルーター証明書をダウンロードする。

CA が証明書を発行したら、PKI は証明書をルーターにダウンロードできます。CA が証明書を発行する方法によって、PKI は TFTP または LDAP のどちらかを使用してダウンロードを実行できます。

デジタル署名などの公開キー操作を実行するために、ルーター証明書のプライベート・キーと公開キーは一致している必要がありますので注意してください。PKI が証明書をルーターにダウンロードする際には、公開キーを使用して生成されたプライベート・キーが、ルーターのキー・キャッシュ内になければなりません。一致するプライベート・キーがなければ、ダウンロードされた証明書は使用できません。このため、証明書要求を発行するときから証明書をダウンロードするときまで、ルーターをリスタートまたは再ロードしたり、キャッシュを消去したり、新しい証明書要求を発行したりしてはなりません。これらの操作のどれかを行うと、ルーターの実行キャッシュにあるプライベート・キーが破棄されます。

4. CA 証明書をダウンロードする。

IKE ピアの証明書を検証するために、PKI はピアのルート CA 証明書を取得する必要があります。本リリースは単一レベルの CA 操作をサポートしているので、IKE エンティティーは同じ CA に割り当てる必要があります。それぞれの IKE エンティティー (この場合は、それぞれのルーター) は、ピアから受け取った証明書が有効であることを検証するために、CA の証明書をダウンロードする (TFTP または LDAP のどちらかを使用して) 必要があります。

5. 証明書を保管し、再ロードする。

証明書、一致するプライベート・キー、および CA の証明書をルーターが取得した後、ユーザーは IKE ネゴシエーションを開始できます。通常証明書は数か月～数年間有効なので、ルーターを再ロードまたはリスタートするたびに証明書要求を発行し、ダウンロードを実行しなくて済むように、証明書とプライベート・キーを SRAM に保管できます。本バージョンは、証明書とプライベート・キーを SRAM に保管したり、SRAM から検索したりするための **cert save** コマンドと **cert load** コマンドを用意しています。

ルーター証明書とプライベート・キーはペアとして処理する必要がありますので注意してください (たとえば、これらは必ず一緒に SRAM に保管され、SRAM から検索されます)。

## IP セキュリティーの使用

次の例に示すように、TFTP と LDAP の両サーバーの情報を構成し、表示するには、Talk 6 コマンドを使用します。

### 例: サーバーの追加 (T6)

```
Config>f ipsec
IP Security feature user configuration
IPsec config>pki
PKI config>add server
Name ? (max 65 chars) []? test
Enter server IP Address []? 8.8.8.8
Transport type (Choices: TFTP/LDAP) [TFTP]?
PKI config>
```

### 例: サーバー構成のリスト (T6)

```
PKI config>li server

1) Name: SERVER1
   Type: TFTP
   IP addr: 8.8.8.8

2) Name: TEST
   Type: TFTP
   IP addr: 8.8.8.8
```

### 例: ルート証明書のリスト (T6)

```
PKI config>li cert

Root CA certificate:
  SRAM Name: R1
  Subject Name: /c=US/o=ibm/ou=nhd
  Issuer Name: /c=US/o=ibm/ou=nhd
  Validity: 1998/12/19 -- 2018/12/19
  Default Root Cert: No

  SRAM Name: R2
  Subject Name: /c=US/o=ibm/ou=nhd
  Issuer Name: /c=US/o=ibm/ou=nhd
  Validity: 1998/12/19 -- 2018/12/19
  Default Root Cert: Yes

Router Certificate:
  SRAM Name: B1
  Subject Name: /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
  Issuer Name: /c=CA/o=Entrust Technologies/ou=PartnerCA
  Subject alt Name: 1.1.1.1
  Key Usage: Sign & Encipherment
  Validity: 1998/10/29 -- 2001/10/29
  Default Cert: No

  SRAM Name: B2
  Subject Name: /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
  Issuer Name: /c=CA/o=Entrust Technologies/ou=PartnerCA
  Subject alt Name: 1.1.1.1
  Key Usage: Sign & Encipherment
  Validity: 1998/10/29 -- 2001/10/29
  Default Cert: Yes

  SRAM Name: B3
  Subject Name: /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
  Issuer Name: /c=CA/o=Entrust Technologies/ou=PartnerCA
  Subject alt Name: 1.1.1.1
  Key Usage: Sign & Encipherment
  Validity: 1998/10/29 -- 2001/10/29
  Default Cert: No

  SRAM Name: YYY
  Subject Name: /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
  Issuer Name: /c=CA/o=Entrust Technologies/ou=PartnerCA
  Subject alt Name: 1.1.1.1
```

```

Key Usage: Sign & Encipherment
Validity: 1998/10/29 -- 2001/10/29
Default Cert: No

```

### 例: 証明書要求 (T5)

```

PKI Console>cert-req
Enter the following part for the subject name
Country Name(Max 16 characters) []? us
Organization Name(Max 32 characters) []? IBM
Organization Unit Name(Max 32 characters) []? NHD
Common Name(Max 32 characters) []? router1
Key modulus size
[512]?
Certificate subject-alt-name type:
1--IPv4 Address
2--User FQDN
3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 12.1.1.1
Generating a key pair. This may take some time. Please wait ...
PKCS10 message successfully generated
Enter tftp server IP Address []? 8.8.8.8
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]?
Memory transfer starting.
.Memory transfer completed - successfully.
Certificate request TFTP to remote host successfully.
Private Key Alias [ROUTER KEY]? local
Generated private key LOCAL stored into cache

```

### 例: ルーター証明書のリスト (T5)

```

PKI Console>li cert
Router certificate
Serial Number: 909343811
Subject Name: /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
Issuer Name: /c=CA/o=Entrust Technologies/ou=PartnerCA
Subject alt Name: 1.1.1.1
Key Usage: Sign & Encipherment
Validity: 1998/10/29 -- 2001/10/29

Root CA certificate
Serial Number: 914034740
Subject Name: /c=US/o=ibm/ou=nhd
Issuer Name: /c=US/o=ibm/ou=nhd
Validity: 1998/12/19 -- 2018/12/19

```

### 例: Cert Save (T5)

```

PKI Console>cert-save
Enter type of certificate to be stored into SRAM:
1)Root certificate;
2)Box certificate with private key;
Select the certificate type (1-2) [2]?
SRAM Name for certificate and private key []? yyy
Load as default router certificate at initialization?? [No]:
Private key YYY written into SRAM
Both Certificate and private key saved into SRAM successfully
PKI Console>

```

### 例: Cert Load (T5)

```

PKI Console>cert-load
Enter type of certificate to be stored into SRAM:
1)Root certificate;
2)Box certificate with private key;
Select the certificate type (1-2) [2]?
Name []? yyy
Box certificate and private key saved into cache successfully
PKI Console>

```

### 手動 IP セキュリティーの使用 (IPv4)

2212 用の IPv4 に備わっている IP セキュリティー機能は、ポリシー機能などの IPSec 関連処理と連携して、認証、保全性、機密性、および非否認を実現します。IPSec を手作業で設定するには、ポリシー・データベースに IPSec オプションのサブセットを含むポリシーを事前に構成して、手動トンネルのプロファイルと有効期間を定義します。ポリシーを使用可能にしているルーターが IPSec パケットの送信準備を行うときに、ポリシーの内容に基づいて、ルーターがあて先ルーターと動的にネゴシエーションして IPSec オプションを設定するように、データベースに IPSec オプション (ポリシー) の完全セットを事前に構成することもできます。手動トンネルの定義については、355ページの『手動 IP セキュリティーの構成 (IPv4)』を参照してください。ポリシー・オプションの説明は、275ページの『第18章 ポリシー機能の使用』を参照してください。

---

### 手動 IP セキュリティーの使用 (IPv6)

2212 用の IPv6 が備えている IP セキュリティー機能は、認証、保全性、および機密性を実現します。手動トンネルの定義については、367ページの『手動 IP セキュリティーの構成 (IPv6)』を参照してください

---

## 第21章 IP セキュリティーの構成および監視

この章では、IP セキュリティーの構成および監視の方法、および IP セキュリティー監視コマンドの使用法について説明します。IPv4 の場合は、275ページの『第18章 ポリシー機能の使用』と 307ページの『第19章 ポリシー機能の構成と監視』に、IP セキュリティー・ポリシーの構成と監視に関する追加情報があります。この章には、次の内容が記載されています。

- 『インターネット・キー交換の構成 (IPv4)』
- 352ページの『公開キー・インフラストラクチャーの構成 (IPv4)』
- 352ページの『証明書の取得』
- 353ページの『公開キー・インフラストラクチャー構成コマンド』
- 355ページの『手動 IP セキュリティーの構成 (IPv4)』
- 356ページの『IP セキュリティー構成環境へのアクセス』
- 357ページの『手動 IP セキュリティー構成コマンド』
- 366ページの『手動トンネルの構成 (IPv4)』
- 367ページの『手動 IP セキュリティーの構成 (IPv6)』
- 368ページの『IP セキュリティー構成環境へのアクセス』
- 368ページの『手動 IP セキュリティー構成コマンド』
- 369ページの『手動トンネルの構成 (IPv6)』
- 373ページの『手動 IP セキュリティーの監視 (IPv4)』
- 383ページの『手動 IP セキュリティーの監視 (IPv6)』

注: TN3270、APPN-ISR、または APPN-HPR トラフィックを伝送するために IPSec トンネルを作成し、BRS を使用してそのトラフィックに優先順位を付ける計画の場合は、BRS の IPv4 優先順位ビット設定フィーチャーを使用することが必要です。詳しくは、10ページの『IP 保護トンネルおよび 2 次フラグメント内の SNA トラフィック用の IP バージョン 4 優先順位ビット処理の使用』を参照してください。

---

### インターネット・キー交換の構成 (IPv4)

ここでは、インターネット・キー交換 (IKE) を構成する方法を説明します。

IPSec トンネルを確立するには、まず次のことを行う必要があります。

1. トンネルを使用するパケットの属性と、結果として行われる処理 (ポリシー) を構成する。
2. 必要な暗号化オプションと認証オプションを構成する。

これらの作業を行う方法について詳しくは、275ページの『第18章 ポリシー機能の使用』、307ページの『第19章 ポリシー機能の構成と監視』、および 352ページの『公開キー・インフラストラクチャーの構成 (IPv4)』を参照してください。

## 公開キー・インフラストラクチャーの構成 (IPv4)

ここでは、IPv4 で公開キー・インフラストラクチャー (PKI) を構成する方法を説明します。

IPSec トンネルを確立するには、まず次のことを行う必要があります。

1. 公開/プライベート暗号キーのペアを作成し、信頼のおける認証局 (CA) からデジタル証明書を取得する。詳しくは、『証明書の取得』を参照してください
2. ポリシーを構成する対象のルーターに対して使用する IPSec アルゴリズム、SA などのオプションを決定する。詳しくは、345ページの『IP セキュリティー・トンネルのネゴシエーション』以降の項目を参照してください。
3. IKE とポリシー・データベースを構成する。詳しくは、351ページの『インターネット・キー交換の構成 (IPv4)』、275ページの『第18章 ポリシー機能の使用』、および 307ページの『第19章 ポリシー機能の構成と監視』を参照してください。

## 証明書の取得

IPSec トンネルを確立する前に、346ページの『公開キー・インフラストラクチャーの使用』に説明されているように、信頼のおける認証局 (CA) を選択し、CA に登録する必要があります。CA は署名入りの X.509 デジタル証明書を返し、ユーザーはこの証明書を使用して、ネットワーク内の相手方に対して自身を識別し、認証することができます。証明書は、コード化されたデジタル ID (署名) と、公開/プライベート暗号キーのペアで構成されます。次のことを行います。

1. CA を識別し、そのサーバー・アドレスを入手する。
2. 353ページの『公開キー・インフラストラクチャー構成コマンド』に説明されている、PKI Talk 6 **add ldapserver** コマンド、または **add ftpserver** コマンドのどちらかを使用して、証明書リポジトリ検索オプションを構成する。
3. 375ページの『公開キー・インフラストラクチャー監視コマンド』に説明されている PKI Talk 5 **certificate request** コマンドを使用して、公開/プライベート・キーのペアを作成する。これは、ルーター内で行うことも、リモート側で (たとえば、バーチャル私設ネットワーク (VPN) 管理者として) 行うこともできます。リモート側で行う場合は、キー・ペアを暗号化して、ルーターに安全に転送する必要があります。
4. 375ページの『公開キー・インフラストラクチャー監視コマンド』に説明されている PKI Talk 5 **certificate request** コマンドを使用して、初期の証明書要求を CA に提出する。要求は、電子メールまたは FTP のどちらかを經由して、PKCS#10 メッセージ形式で送信されます。CA は、キー・ペアを証明書に結合し、CA のプライベート・キーを使用して証明書に署名して、証明書を中央 (LDAP または FTP) リポジトリに保管するか、PKCS#7 メッセージ形式でユーザーに戻します。通常、証明書は数か月以上有効で、その後更新されます。更新は、ネットワーク内のどの相手方を引き続き信頼できるかを確認します。
5. 375ページの『公開キー・インフラストラクチャー監視コマンド』に説明されている PKI Talk 5 **certificate save** コマンドを使用して、ルーターの SRAM に証明書を保管する。

注:

1. SRAM 内の証明書レコードのリストを表示するには、『公開キー・インフラストラクチャー構成コマンド』に説明されている PKI Talk 6 **list certificate** コマンドを使用します。
2. SRAM から証明書レコードのリストを削除するには、『公開キー・インフラストラクチャー構成コマンド』に説明されている PKI Talk 6 **delete certificate** コマンドを使用します。
3. 以後の IPSec ネゴシエーション時に証明書要求を再発行する必要をなくするには、375ページの『公開キー・インフラストラクチャー監視コマンド』に説明されている PKI Talk 5 **certificate load** コマンドを使用して、受け取った証明書をキャッシュにロードします。

---

## 公開キー・インフラストラクチャー構成コマンド

### Add

PKI Talk 6 **add** コマンドは、証明書リポジトリ・サーバーとその場所を構成するために使用します。

構文:

```
add server
```

**server** 追加操作の対象がサーバーであることを指定します。

#### 例 1: サーバーの追加

```
PKI config>add server
Name ? (max 65 chars) []? myldap
Enter server IP Address []? 8.8.8.9
Transport type (Choices: TFTP/LDAP) [TFTP]? ldap
LDAP search timeout value [3]?
LDAP retry interval (mins) [1]?
LDAP server port number [389]?
LDAP version [2]?
Bind to the server anonymously? [No]:
Enter your bind DN: []? c=us o=ibm
Enter your bind PW: []? testldap
```

### Change

PKI Talk 6 **change** コマンドは、証明書リポジトリ・サーバーとその場所を変更するために使用します。

構文:

```
change server
```

**server** 追加操作の対象がサーバーであることを指定します。

#### 例 1: サーバーの変更

```
PKI config>change server
Name []? myldap
Enter server IP Address []? 8.8.8.7
Server type will continue to be LDAP
LDAP search timeout value [3]?
LDAP retry interval (mins) [1]?
LDAP server port number [389]?
```



## 公開キー・インフラストラクチャー構成コマンド

```
LDAP version [2]?
Enter your bind DN: [c=us o=ibm]?
Enter your bind PW: [testldap]?
```

## Delete

PKI Talk 6 **delete** コマンドは、ルーターの SRAM から証明書レコードまたはプライベート・キー・レコードを削除するため、またはサーバーを削除するために使用します。

構文:

```
delete          証明書
                 private-key
                 server
```

### certificate

削除操作の対象が証明書レコードであることを指定します。

**all** すべての証明書レコードを削除することを指定します。

**id** 削除する証明書レコードの ID を指定します。

#### 例 1: 証明書の削除

```
PKI config>delete certificate
Cert Name []? test
Enter the type of the certificate:
Choices: 1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]?
Box Certificate [TEST] deleted successfully
Corresponding private Key [TEST] deleted successfully
```

#### 例 2: プライベート・キーの削除

```
PKI config>delete private-keys
Private Key Name []? test
Private Key [TEST] deleted successfully
Corresponding box certificate [TEST] deleted successfully
```

#### 例 3: サーバー・レコードの削除

```
PKI config>delete server
Name []? myldap
Server MYLDAP deleted successfully
```

### private-key

削除操作の対象がプライベート・キー・レコードであることを指定します。

**server** 削除操作の対象がサーバーであることをしています。

## List

PKI Talk 6 **list** コマンドは、ルーターの SRAM 内にある証明書またはキー・レコードを表示するために使用します。

構文:

```
list          certificates
               private-keys
               servers
```



**certificates**

リスト操作の対象が証明書レコードであることを指定します。

**private-keys**

リスト操作の対象が秘密キー・レコードであることを指定します。

**servers**

リスト操作の対象がサーバー・レコードであることを指定します。

**例 1: 証明書のリスト**

```
PKI config>list certificates
```

```
Root CA certificate:
  SRAM Name: B
  Subject Name: /c=US/o=ibm/ou=nhd
  Issuer Name: /c=US/o=ibm/ou=nhd
  Validity: 1998/12/19 2:2:21 -- 2018/12/19 2:32:21
  Default Root Cert: Yes

Router Certificate:
  SRAM Name: W
  Subject Name: /c=US/o=ibm/ou=nhd/cn=testip
  Issuer Name: /c=US/o=ibm/ou=nhd
  Subject alt Name: 1.1.1.1
  Key Usage: Sign & Encipherment
  Validity: 1999/1/19 23:24:27 -- 2002/1/19 23:54:27
  Default Cert: No
```

**例 2: プライベート・キーのリスト**

```
PKI config>list private-keys
```

```
Private Keys In SRAM:
```

```
1) Name W
```

**例 3: サーバー・レコードのリスト**

```
PKI config>list servers
```

```
1) Name: SERVER1
   Type: LDAP
   IP addr: 1.1.1.2
     LDAP search timeout (secs): 10
     LDAP retry interval (mins): 3
     LDAP server port number: 390
     LDAP version: 2
     Anonymous bind ?: y

2) Name: TEST
   Type: TFTP
   IP addr: 8.8.8.8
```

---

## 手動 IP セキュリティーの構成 (IPv4)

ここでは、IPv4 での手動 IPSec 用に使用できる構成オプションを説明します。IPv4 には、すべての IPSec 機能が適用されます。

IPSec 手動トンネルを構成するには、次の手順を実行します。

1. IPSec トンネルを作成する。
2. IPSec をリセットする。
3. 手動トンネルのポリシーを構成する (プロファイル、有効性、ポリシー)。
4. ポリシーをリセットする。

## 手動 IP セキュリティーの構成 (IPv4)

### アルゴリズムの構成

表41 に示すアルゴリズムを使用して、トンネル・ポリシーを構成できます。

表 41. 各種のトンネル・ポリシーを使用して構成されたアルゴリズム

トンネル・ポリシー	アルゴリズム
AH, AH-ESP, または ESP-AH	<ul style="list-style-type: none"><li>ローカル AH 認証アルゴリズム - 必須</li><li>リモート AH 認証アルゴリズム - オプション</li></ul>
ESP, AH-ESP, または ESP-AH	<ul style="list-style-type: none"><li>ローカル暗号化アルゴリズム - 必須</li><li>リモート暗号化アルゴリズム - オプション</li><li>ローカル ESP 認証アルゴリズム - オプション</li><li>リモート ESP 認証アルゴリズム - オプション</li></ul> <p>注: ソフトウェア・ロードに暗号化が含まれていない場合は、暗号化関連のパラメーターは表示されません。</p>

トンネル・ポリシーは、アウトバウンド・パケットに対してローカル・アルゴリズムを使用し、インバウンド・パケットに対してリモート・アルゴリズムを使用します。トンネルのこちら側の端にあるルーターのローカル・アルゴリズムは、トンネルのあちら側の端にあるルーターのリモート・アルゴリズムと一致している必要があります。リモート・アルゴリズムの値はオプションで、デフォルトでは対応するローカル・アルゴリズムの値をとります。ESP 認証はオプション機能なので、ローカル ESP 認証アルゴリズムはオプションです。

### 暗号化キーの構成

構成するそれぞれのローカル・アルゴリズムに対して、リモート・ホストの対応するアルゴリズムに対するキーと同じキーも構成する必要があります。357ページの『手動 IP セキュリティー構成コマンド』に記載されている、**add tunnel** コマンドのキーの説明を参照してください。

---

## IP セキュリティー構成環境へのアクセス

IP セキュリティー構成環境にアクセスするには、OPCON プロンプト (\*) で **t 6** と入力し、次に Config> プロンプトで次のコマンド列を入力します。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config>ipv4
IPV4-IPsec config>
```

## 手動 IP セキュリティー構成コマンド

この節では、IP セキュリティー構成コマンドについて説明します。これらのコマンドは、IPV4-IPsec config> プロンプトで入力します。

表 42. IP セキュリティー構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxi ページの『ヘルプの入手』を参照してください。
Add tunnel	保護トンネルを追加します。
Change tunnel	保護トンネル構成パラメーター値を変更します。
Delete tunnel	保護トンネルを削除します。
Disable	安全な方法でのすべての IP セキュリティー処理 (パケット・フィルタに一致するパケットをドロップする) を使用不可にする、無保護な方法でのすべての IP 処理 (パケット・フィルタに一致するパケットをパスさせる) を使用不可にする、または保護トンネルを使用不可にします。
Enable	すべての IP セキュリティー処理を使用可能にする、または保護トンネルを使用可能にします。
List	グローバル IP セキュリティー情報、または定義済みのトンネルに関する情報を表示します。
Set	各種の IPSec オプションを設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

## Add Tunnel

**add tunnel** コマンドは、IPSec トンネルを定義するためのパラメーターを追加するのに使用します。

構文:

**add tunnel...**

**tunnel-name**

トンネルにラベルを付けるための任意指定パラメーター。これは 2212 内で固有でなければなりません。

**有効値:** 最大 15 文字。最初の字は文字でなければなりません。空白は使用できません。

**デフォルト値:** なし

**lifetime**

トンネルが活動状態でいられる時間数 (分)。値 0 は、トンネルの存続時間は満了しないことを示します。

**有効値:** 0 ~ 525600 (0 = 満了しない、525600 = 365 日)

**デフォルト値:** 46080 (32 日)

**encapsulation-mode**

IP パケットをカプセル化する方法。トンネル・モードでは、IP パケット全体がカプセル化され、新規の IP ヘッダーが作成されます。トランスポート・モードでは、IP ヘッダーはカプセル化されません。保護トンネルの一端がルー

## 手動 IP セキュリティー構成コマンド

ターの場合は、インターネット技術特別調査委員会 (IETF) セキュリティー体系草案に準拠して、トンネル・モードを使用することが**必要**です。

**有効値:** トンネル (*TUNN*) またはトランスポート (*TRANS*)

**デフォルト値:** トンネル (*TUNN*)

### tunnel-policy

トンネル・ポリシーを定義する 4 つの選択項目のうちの 1 つ。すなわち、IP 認証ヘッダー (AH)、IP カプセル化セキュリティー・ペイロード (ESP)、またはこれらのプロトコルの組み合わせ (AH-ESP および ESP-AH)。AH-ESP では、アウトバウンド・パケットで ESP 暗号化が最初に行われます。ESP-AH では、アウトバウンド・パケットで AH 認証が最初に行われます。一部のパラメーターは、ESP または AH のどちらかに固有です。暗号化パラメーターは、ESP、AH-ESP、または ESP-AH を選択した場合にだけ構成します。認証パラメーターは、AH、AH-ESP、または認証付き ESP を選択した場合にだけ構成します。

**有効値:** AH、ESP、AH-ESP、ESP-AH

**デフォルト値:** AH-ESP

### local-IP-address

トンネルのこちら側の IP アドレス。

**有効値:** インターフェースに構成された、または 2212 の内部アドレスとして構成された、有効な IP アドレス

**デフォルト値:** ルーターに構成された IP アドレスの 1 つ

### local-spi

セキュリティー・アソシエーションとは、AH または ESP を使用して接続のトラフィックを保護する単方向セキュリティー接続です。セキュリティー・パラメーター・インデックス (SPI) は、この保護トンネルに対応する 2 つのセキュリティー・アソシエーション (インバウンドまたはアウトバウンド) の 1 つを固有に識別する任意の 32 ビット値です。このパラメーターは必須であり、トンネルのローカル側で受信されるインバウンド・パケットに対してこのトンネルで期待される SPI を識別します。この値は、同じローカル IP アドレスをもつ別のトンネルのローカル SPI と一致してはなりません。トンネル・ポリシー (ESP、AH、AH-ESP、または ESP-AH) に関係なく、1 つの保護トンネルのインバウンド・トラフィックに対して 1 つだけローカル SPI を構成します。

**有効値:** 255 より大きい任意の 32 ビット値。

**デフォルト値:** 256

### local-encryption-algorithm

ローカル・ルーターから送信されるアウトバウンド・パケットの ESP に使用される暗号化アルゴリズム。ESP を構成する場合は必須です。一部の国では、米国の輸出規制のため、このアルゴリズムの一部または全部を使用できない場合があります。この暗号化アルゴリズムは、リモート側の暗号化アルゴリズムと一致していなければなりません。

## 手動 IP セキュリティー構成コマンド

ESP-NULL アルゴリズムは、ESP が暗号化を実行するのを防止します。このアルゴリズムは、すべての国で利用可能です。ESP-NULL を選択した場合は、認証アルゴリズム HMAC-MD5 または HMAC-SHA-1 を選択して、認証を自動化しておく必要があります。

有効値: DES-CBC、CDMF、3DES、または ESP-NULL

デフォルト値: DES-CBC

### local-encryption-key

ローカル ESP 暗号化アルゴリズムで使用される 1 つまたは複数のキー。これらは、保護トンネルの反対側に構成された対応するキーと一致していなければなりません。ESP-NULL 暗号化アルゴリズムを選択した場合は、このキーは構成しません。

有効値:

- DES-CBC の場合: 16 桁の 16 進文字 (0 ~ 9, a ~ f, A ~ F)
- CDMF の場合: 16 桁の 16 進文字 (0 ~ 9, a ~ f, A ~ F)
- 3DES の場合: どれも同じでない 3 つの別々のキー、それぞれ 16 桁の 16 進文字 (0 ~ 9, a ~ f, A ~ F)

デフォルト値: なし

### padding-for-local-encryption

アウトバウンド ESP パケットに追加される追加埋め込みのサイズ (バイト)。追加埋め込みは、暗号化アルゴリズムの結果、暗号化されたパケットが元のパケットと同じサイズになる場合、暗号化される IP パケットのサイズを偽装するために使用できます。ESP 埋め込み値は 8 の倍数でなければなりません。

暗号化アルゴリズムが ESP-NULL の場合は、埋め込みは必要ありません。ESP-NULL アルゴリズムは元のパケット・サイズに 1 バイトを追加するからです。ローカル暗号化の埋め込みを構成した場合、その値は無視されます。

有効値: 0 ~ 120

デフォルト値: 0

### local-ESP-authentication

ローカル ESP 認証を選択します (必要な場合)。暗号化アルゴリズムが ESP-NULL の場合、認証の指定は必須です。

有効値: Yes または No

デフォルト値: Yes

### local-authentication-algorithm

アウトバウンド・パケットで使用される認証アルゴリズム。ESP の場合、これは任意指定パラメーターで、ESP 認証を選択しない限り必要ではありません。AH、AH-ESP、または ESP-AH の場合、このパラメーターは必須です。使用する認証アルゴリズムは、IPSec トンネルの反対側で使用されるリモート認証アルゴリズムと一致していなければなりません。

有効値: HMAC-MD5 または HMAC-SHA

デフォルト値: HMAC-MD5

## 手動 IP セキュリティー構成コマンド

### local-authentication-key

ローカル認証アルゴリズムで使用されるキー。これは、IPSec トンネルの反対側に構成された等価キーと一致していなければなりません。ポリシーが AH、AH-ESP、または ESP-AH の場合、またはポリシーが ESP でローカル ESP 認証アルゴリズムが構成されている場合には、このパラメーターは必須です。

有効値:

- HMAC-MD5 の場合: 32 桁の 16 進文字 (0 ~ 9, a ~ f, A ~ F)
- HMAC-SHA の場合: 40 桁の 16 進文字 (0 ~ 9, a ~ f, A ~ F)

デフォルト値: なし

### remote-IP-address

トンネルのリモート側の IP アドレス。これは必須パラメーターです。

有効値: 有効な IP アドレス

デフォルト値: なし

### remote-spi

セキュリティー・アソシエーションとは、AH または ESP を使用して接続のトラフィックを保護する単方向セキュリティー接続です。セキュリティー・パラメーター・インデックス (SPI) は、この保護トンネルに対応する 2 つのセキュリティー・アソシエーション (インバウンドまたはアウトバウンド) の 1 つを固有に識別する任意の 32 ビット値です。このパラメーターは必須であり、リモート・ホスト側のアウトバウンド・パケットの ESP または AH に期待される SPI を識別します。この値は、同じリモート IP アドレスをもつ別のトンネルのリモート SPI と一致してはなりません。トンネル・ポリシー (ESP、AH、AH-ESP、または ESP-AH) に関係なく、1 つの IPSec トンネルのアウトバウンド・トラフィックに対して 1 つだけローカル SPI を構成します。

有効値: 255 より大きい任意の 32 ビット値。

デフォルト値: 256

### remote-encryption-algorithm

リモート・ホストから受信するインバウンド・パケットで使用される暗号化解除アルゴリズム。これはローカル側の暗号化アルゴリズムと一致していなければなりません。

ESP-NULL アルゴリズムは、ESP が暗号化を実行するのを防止します。ESP-NULL を選択した場合は、認証アルゴリズム HMAC-MD5 または HMAC-SHA-1 を選択して、認証を活動化しておく必要があります。

有効値: DES-CBC、CDMF、3DES、または ESP-NULL

デフォルト値: ローカル側の暗号化アルゴリズムの値

### remote-encryption-key

リモート側の ESP 暗号化アルゴリズムで使用される 1 つまたは複数のキー。これらは、保護トンネルの反対側に構成された等価キーと一致していなければなりません。ESP-NULL 暗号化アルゴリズムを選択した場合は、このキーは構成しません。

有効値:

## 手動 IP セキュリティー構成コマンド

- DES-CBC の場合: 16 桁の 16 進文字 (0 ~ 9, a ~ f, A ~ F)
- CDMF の場合: 16 桁の 16 進文字 (0 ~ 9, a ~ f, A ~ F)
- 3DES の場合: どれも一致しない 3 つの別々のキー、それぞれ 16 桁の 16 進文字 (0 ~ 9, a ~ f, A ~ F)

デフォルト値: なし

### verification-of-remote-encryption-padding

受信パケットの暗号化埋め込みのサイズを検査するかどうかを決めます。

有効値: Yes または No

デフォルト値: No

### padding-for-remote-encryption

受信 ESP パケットに期待される追加埋め込みのサイズ (バイト)。このパラメーターは、*verification-of-remote-encryption-padding* の値が Yes の場合にだけ必須であり、有効です。ESP 埋め込み値は 8 の倍数でなければなりません。8 で割り切れない値が構成されている場合、その値は 8 で割り切れる次の値に切り上げられます。

有効値: 0 ~ 120

デフォルト値: 0

### remote-ESP-authentication

インバウンド・パケットのリモート ESP 認証を選択します (必要な場合)。

有効値: Yes または No

デフォルト値: Yes

### remote-authentication-algorithm

インバウンド・パケットに使用される認証アルゴリズム。ESP の場合、これは任意指定パラメーターで、ESP 認証を選択しない限り必要ではありません。AH または AH と ESP の組み合わせ (AH-ESP または ESP-AH) の場合、このパラメーターは必須です。使用する認証アルゴリズムは、IPSec トンネルの反対側で使用されるローカル認証アルゴリズムと一致していなければなりません。

有効値: HMAC-MD5 または HMAC-SHA

デフォルト値: HMAC-MD5

### remote-authentication-key

リモート側の認証アルゴリズムで使用されるキー。これは、保護トンネルの反対側に構成された等価キーと一致していなければなりません。これは、AH、AH-ESP、ESP-AH、および ESP (リモート ESP 認証アルゴリズムが構成されている場合) で必須です。

有効値:

- HMAC-MD5 の場合: 32 桁の 16 進文字 (0 ~ 9, a ~ f, A ~ F)
- HMAC-SHA の場合: 40 桁の 16 進文字 (0 ~ 9, a ~ f, A ~ F)

デフォルト値: なし

### enable-replay-prevention

再生防止が使用可能かどうかを指定します。再生防止が使用可能の場合、IP セキュリティー・ヘッダー内のシーケンス番号を監視して、トンネルの受信



## 手動 IP セキュリティー構成コマンド

側によって重複パケットが処理されるのを防止します。再生防止の使用はお勧めできません。送信側のシーケンス番号カウンターが限界に達すると、トンネル・セキュリティー・アソシエーションを非活動化しなければならないからです。この状態が起きた場合、手動で介入して、既存のセキュリティー・アソシエーションをリスタートするか、新規に作成することが必要になります。

再生防止が使用可能の場合、**reset ipsec** コマンドを使用して IPsec をリセットした場合は、必ず IPsec トンネルの反対側のルーター上の IPsec もリセットする必要があります。これは、トンネルの両側でシーケンス番号を再初期設定するために必要です。トンネルの一端で IPsec がリセットされ、他端はリセットされていない場合、トンネルの各端のルーターは、シーケンス番号ミスマッチによりパケットを廃棄する可能性があります。

有効値: Yes または No

デフォルト値: No

**DF-bit** トンネル・モードの保護トンネルの外部ヘッダー内の断片化不可 (DF) ビットの扱いを指定します。パケットを断片化できないことを指定するために、IPv4 ヘッダー内にこのビットをセットすることができます。DF ビット・パラメーターは、インバウンド・パケット内の DF ビットの扱い方を 2212 に知らせます。すなわち、内部ヘッダー内に見つかった DF ビットを外部ヘッダーにコピーするか、外部ヘッダーにビットをセットするか、あるいは外部ヘッダー内のビットをクリアするかどうかを指示します。

DF ビットがセットされており、パケットを断片化できない場合、IPsec はパス MTU (PMTU) ディスカバリー機能を使用します。詳しくは、341ページの『パス最大伝送単位ディスカバリー』を参照してください。

有効値: コピー、セット、クリア

デフォルト値: コピー

### **enable-tunnel**

このトンネルが使用可能かどうかを指定します。パケット・フィルターを構成して、この IPsec トンネルで使用するインターフェースを定義し、IP をリセットするか 2212 をリスタートするまでは、使用可能にされたトンネルはパケットをフィルターに掛けません。IP をリセットするには、**reset ip** コマンドを使用します。

有効値: Yes または No

デフォルト値: Yes

## Change Tunnel

**change tunnel** コマンドは、**add tunnel** コマンドを使用して以前に構成した IPsec トンネル・パラメーターを変更するのに使用します。

構文:

**change tunnel ...** 変更できるパラメーターの表示については、**add tunnel** コマンドの項を参照してください。



## Delete Tunnel

Talk 6 **delete tunnel** コマンドは、IPSec トンネルを削除するために使用します。

構文:

```
delete tunnel          tunnel-id
                        tunnel-name
                        all
```

**tunnel-id**

削除する IPSec トンネルの識別子を指定します。

有効値: 1 ~ 65535

デフォルト値: 1

**tunnel-name**

削除する IPSec トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

**all** このインターフェース上のすべての IPSec トンネルを削除することを指定します。

## Disable

**disable** コマンドは、IPSec トンネルを使用不可にするか、あるいはすべての IPSec トンネルを安全な方法 (IPSec フィルターに一致するパケットをドロップする) または無保護な方法 (IPSec フィルターに一致するパケットをパスさせる) で使用不可にするのに使用します。

構文:

```
disable                ipsec drop
                        ipsec pass
                        tunnel ...
```

**ipsec drop**

ルーター上の IP セキュリティーを安全な方法で使用不可にします。すべての IPSec トンネルが使用不可にされますが、パケット・フィルタ規則の保護トンネル情報を使用して、IPSec トンネル・パケット・フィルタに一致するパケットを識別します。一致するパケットはドロップされます。

**ipsec pass**

ルーター上の IP セキュリティーを無保護な方法で使用不可にします。すべての IPSec トンネルが使用不可にされます。IPSec トンネル・パケット・フィルタに一致するパケットは、通常のトラフィックとして転送されます。

**tunnel tunnel-id tunnel-name all**

指定されたトンネルまたはすべてのトンネル上の IP セキュリティーを使用不可にします。

**tunnel-id**

使用不可にする保護トンネルの識別子を指定します。

## 手動 IP セキュリティー構成コマンド

有効値: 1 ~ 65535

デフォルト値: 1

### tunnel-name

使用不可にする保護トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

**all** すべてのトンネル

## Enable

**enable** コマンドは、すべてのインターフェースまたは 1 つのトンネルの IP セキュリティー・プロトコルを使用可能にするのに使用します。ルーター上の IPsec をグローバルに使用可能にしないと、個別に使用可能にされた IPSec トンネルは活動状態になりません。

構文:

```
enable                ipsec  
                        tunnel ...
```

**ipsec** ルーター全体の IP セキュリティーを使用可能にします。

**tunnel** *tunnel-id tunnel-name all*

指定されたトンネルまたはすべてのトンネル上の IP セキュリティーを使用可能にします。

### tunnel-id

使用可能にする保護トンネルの識別子を指定します。

有効値: 1 ~ 65535

デフォルト値: 1

### tunnel-name

使用可能にする保護トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

**all** すべてのトンネル

## List

**list** コマンドは、現行の IP セキュリティー構成を表示するのに使用します。グローバル・トンネル (global tunnels) には、ルーター上のすべてのトンネル (活動および定義済みの両方) が含まれます。すべてのトンネル (all tunnels) には、このインターフェースに構成されたすべてのトンネル (活動および定義済みの両方) が含まれます。活動トンネル (active tunnels) は、現在活動状態のトンネルです。定義済みトンネル (defined tunnels) は、定義されているが活動状態ではないトンネルです。IPv4 の場合は、ルーターの SRAM 内にある選択した証明書も表示されます。

構文:

```
list ...                all
```

## 手動 IP セキュリティー構成コマンド

```
status
tunnel
active tunnel-id tunnel-name all
defined tunnel-id tunnel-name all
```

### 例 1: すべての IPSec トンネルのリスト

```
IPsec config>list all
```

```
IPsec is ENABLED
```

```
IPsec Path MTU Aging Timer is 20 minutes
```

```
Defined Manual Tunnels:
```

ID	Name	Local IP Addr	Remote IP Addr	Mode	State
1	test	1.1.1.1	2.1.1.1	TUNN	Enabled
2	test2	1.1.1.1	1.1.1.3	TRANS	Enabled

```
Tunnel Cache:
```

ID	Local IP Addr	Remote IP Addr	Mode	Policy	Tunnel Expiration
2	1.1.1.1	1.1.1.3	TRANS	ESP	*****
1	1.1.1.1	2.1.1.1	TUNN	AH	*****

### 例 2: ESP ポリシーと ESP-NULL アルゴリズムを使用する IPSec トンネルのリスト

```
IPsec config>li tun 1000
```

Tunnel ID	Name	Mode	Policy	Life	Replay Prev	Rcv Win	IPsec Vers	State
1000	t1000	TUNN	ESP	46080	No	---	V2	Enabled

```
Handling of DF bit in outer header: COPY
```

```
Local Information:
```

```
IP Address: 10.11.12.10
Authentication: SPI: ----- Algorithm: -----
Encryption: SPI: 1234 Encryption Algorithm: NULL
Extra Pad: 0
ESP Authentication Algorithm: HMAC-MD5
```

```
Remote Information:
```

```
IP Address: 10.11.12.11
Authentication: SPI: ----- Algorithm: -----
Encryption: SPI: 1234 Encryption Algorithm: NULL
Verify Pad?: No
ESP Authentication Algorithm: HMAC-MD5
```

## Set

**set** コマンドは、トンネルの PMTU 値を制御するために使用します。

構文:

```
set path-mtu-age-timer
```

**path-mtu-age-timer**

2212 がトンネルの PMTU 値を最大値に戻すまでに経過する時間 (分) を指定します。

デフォルト値: 10 (0 は使用不可を意味します)

### 手動トンネルの構成 (IPv4)

ここでは、343ページの図37 に示すネットワークに対する手動 IPv4 トンネルの構成について説明します。

#### ルーター A のトンネルの構成

次の例では、IPv4 を使用して、343ページの図37 に示すネットワーク内のルーター A 用に IPsec 手動トンネルを構成する方法を説明します。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config>ipv4
IPv4-IPsec config>add tunnel
Adding tunnel 1
Tunnel Name (optional)? tunnelone
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH, ESP, AH-ESP, ESP-AH) [AH-ESP]? AH
Local IP Address [1.1.1.1]? 223.252.252.216
Local Authentication SPI (256-65535) [256]?
Local Authentication Algorithm (HMAC-MD5, HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 223.252.252.210
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5, HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Copy, set, or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPv4-IPsec config>
```

この例から分かるように、ユーザーが提供する必要があるパラメーターはプロンプトで指示されます。ESP、AH-ESP、または ESP-AH 保護トンネルの構成でも、同様のパラメーターが要求されます。

注: キーの値は、入力したときには表示されないため、この例には示されていません。HMAC-MD5 認証のキーが表示されるとすれば、32 桁の 16 進文字で示されます。たとえば、キーは 'X'1234567890ABCDEF1234567890ABCDEF' のような値を持っています。

#### ルーター B のトンネルの構成

ルーター B 内に、ルーター A に構成したトンネル (IPsec トンネル 1) と同じ IPsec 手動トンネルを構成する必要があります。ルーター B 内のこのトンネルのローカル IP アドレスは 223.252.252.210 で、リモート IP アドレスは 223.252.252.216 です。その他のすべての IPsec トンネル・パラメーターは、ルーター A に構成されたパラメーターと一致していなければなりません。

#### 例: ESP を使用した IP セキュリティー・トンネルの手動構成

トンネルがトンネル・モードにあり、トンネル・ポリシーが ESP である場合、DF ビットをセットするように求めるプロンプトが出ます。この例には、IPsec トンネルの構成だけを示します (パケット・フィルターの構成は示しません)。

```

IPV4-IPsec config>add tunnel
Adding tunnel 2
Tunnel Name (optional)? tunneltwo
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]? ESP
Local IP Address [1.1.1.1]?
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES, NULL) [DES-CBC]?
Do you wish to change the Local Encryption Key? [No]:
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [Yes]:
Remote IP Address [0.0.0.0]?
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF) [DES-CBC]?
Do you wish to change the Remote Encryption Key? [No]:
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPV4-IPsec config>

```

## 例: ESP と ESP-NUL を使用した IP セキュリティー・トンネルの手動構成

認証が必要であることに注意してください。

```

IPV4-IPsec config>add tunnel
Adding tunnel 3
Tunnel Name (optional)? tunnel13
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]? ESP
Local IP Address [1.1.1.1]?
Local Encryption SPI (256-65535) [256]? 1234
Local Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [DES-CBC]? null
Additional Padding for Local Encryption (0-120) [0]?
Local ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 10.11.12.11
Remote Encryption SPI (1-65535) [1234]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [NULL]?
Do you wish to perform verification of remote encryption padding? [No]:
Remote ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPV4-IPsec config>

```

## 手動 IP セキュリティーの構成 (IPv6)

ここでは、IPv6 での手動 IPSec 用に使用できる構成オプションを説明します。IPv6 には、すべての IPSec 機能が適用されます。IPv6 用の IPSec を構成する場合は、IPSec 構成の質問が次のように変更されるので注意してください。

- アドレスは IPv6 アドレス形式で入力します (たとえば、8:0:9:8::1)。
- DF ビットの設定についての問い合わせはありません。

IPSec 手動トンネルを構成するには、次の手順を実行します。

1. IPSec トンネルを作成する。
2. IPSec をリセットする。
3. フィルター規則を構成する。
4. IPV6 をリセットする。

## 手動 IP セキュリティーの構成 (IPv6)

### アルゴリズムの構成

表43 に示すアルゴリズムを使用して、トンネル・ポリシーを構成できます

表 43. 各種のトンネル・ポリシーを使用して構成されたアルゴリズム

トンネル・ポリシー	アルゴリズム
AH、AH-ESP、または ESP-AH	<ul style="list-style-type: none"><li>ローカル AH 認証アルゴリズム - 必須</li><li>リモート AH 認証アルゴリズム - オプション</li></ul>
ESP、AH-ESP、または ESP-AH	<ul style="list-style-type: none"><li>ローカル暗号化アルゴリズム - 必須</li><li>リモート暗号化アルゴリズム - オプション</li><li>ローカル ESP 認証アルゴリズム - オプション</li><li>リモート ESP 認証アルゴリズム - オプション</li></ul> <p>注: ソフトウェア・ロードに暗号化が含まれていない場合は、暗号化関連のパラメーターは表示されません。</p>

トンネル・ポリシーは、アウトバウンド・パケットに対してローカル・アルゴリズムを使用し、インバウンド・パケットに対してリモート・アルゴリズムを使用します。トンネルのこちら側の端にあるルーターのローカル・アルゴリズムは、トンネルのあちら側の端にあるルーターのリモート・アルゴリズムと一致している必要があります。リモート・アルゴリズムの値はオプションで、デフォルトでは対応するローカル・アルゴリズムの値をとります。ESP 認証はオプション機能なので、ローカル ESP 認証アルゴリズムはオプションです。

### 暗号化キーの構成

構成するそれぞれのアルゴリズムに対して、リモート・ホストの対応するアルゴリズムに対するキーと同じキーも構成する必要があります。357ページの『手動 IP セキュリティー構成コマンド』に記載されている、**add tunnel** コマンドのキーの説明を参照してください。

---

## IP セキュリティー構成環境へのアクセス

IP セキュリティー構成環境にアクセスするには、OPCON プロンプト (\*) で **t 6** と入力し、次に `Config>` プロンプトで次のコマンド列を入力します。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config> ipv6
IPV6-IPsec config>
```

---

## 手動 IP セキュリティー構成コマンド

IPv6 で使用できる IP セキュリティー構成コマンドについては、357ページの『手動 IP セキュリティー構成コマンド』を参照してください。IPv6 用のコマンドは、特に指示のない限り IPv4 用に使用されるものと同じです。コマンドは `IPV6-IPsec config>` プロンプトで入力します。

## 手動トンネルの構成 (IPv6)

ここでは、343ページの図37 のネットワーク例を参照しながらお読みください。IPSec トンネル 1 のエンドポイントは、ルーター A のインターフェース 1 上にあります。ルーター A は、IPsec 用に構成します。ルーター A を手作業で構成するには、次の手順を実行します。

1. IPSec トンネルを作成する。
2. IPSec トンネルのエンドポイントであるルーター・インターフェース上に、アウトバウンド・パケット・フィルタを 1 つ作成する。
3. パケット・フィルタのアクセス制御規則を作成する。
4. IPSec をリセットする。
5. IPv6 をリセットする。

## ルーター A の IP セキュリティ・トンネルの作成

次の例では、ルーター A 用に IPSec トンネル 1 を作成する方法を説明します。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config> ipv6
IPv6-IPsec config> add tunnel
IPsec Tunnel ID (1 - 65535) [1]
Tunnel Name (optional)? tunnelone
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH, ESP, AH-ESP, ESP-AH) [AH-ESP]? AH
Local IP Address [1000:1::1]? 2000::A
Local Authentication SPI (256-65535) [256]?
Local Authentication Algorithm (HMAC-MD5, HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0::0]? 2000::B
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5, HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
IPv6-IPsec config>
```

この例から分かるように、ユーザーが提供する必要があるパラメーターはプロンプトで指示されます。ESP、AH-ESP、または ESP-AH 保護トンネルの構成でも、同様のパラメーターが要求されます。

**注:** キーの値は、入力したときには表示されないため、この例には示されていません。HMAC-MD5 認証のキーが表示されるとすれば、32 桁の 16 進文字で示されます。たとえば、キーは X'1234567890ABCDEF1234567890ABCDEF' のような値を持っています。

## ルーター A のパケット・フィルタの構成

ルーター A の IPSec トンネルを作成した後で、IP パケット・フィルタを 1 つ設定する必要があります。次の例は、パケット・フィルタ *out-router-A* の作成方法を示しています。IPv6 パケット・フィルタとアクセス制御規則の構成については、プロトコル構成および監視 参照資料 第 1 巻 の IPv6 の使用の章にある、IPv6 のフィルター化とアクセス制御の項を参照してください。



## 手動トンネルの構成 (IPv6)

```
* talk 6
Config> Protocol IPv6
Internet protocol user configuration
IPv6 Config> set access-control on
IPv6 Config> add packet-filter
Packet-filter name [ ]? out-router-A
Filter incoming or outgoing traffic? [IN]? OUT
Which interface is this filter for [0]? 1
IPv6 Config> update packet-filter
Packet-filter name [ ]? out-router-A
Packet-filter 'out-router-A' Config>
```

## ルーター A のパケット・フィルター・アクセス制御規則の構成

次のステップは、パケット・フィルター・アクセス制御規則を構成することです。アウトバウンド・パケット・フィルター *out-router-A* に関するアクセス制御規則を 2 つ作成します。

アウトバウンド・パケット・フィルターのアクセス制御規則は、次の機能を実行します。

- 1 つのアクセス制御規則は、IPSec トンネルにパスされるパケットの発信元およびあて先アドレスの範囲を定義します。
- もう 1 つのアクセス制御規則は、パケット・フィルターを通して IPSec トラフィックをパスすることを許可します。

パケット・フィルター *out-router-A* の最初のアクセス制御規則を構成します。このアクセス制御規則は、ネットワーク 1000:1:: から、ルーター B に接続されたあて先ネットワーク 3000:1:: にパケットをパスします。

```
IPv6 Config> update packet-filter
Packet-filter name [ ]? out-router-A
Packet-filter 'out-router-A' Config> add access
Enter type [E]? IS
Internet source [0::0]? 1000:1::
Prefix Length [64]? 64
Internet destination [0::0]? 3000:1::
Prefix Length [64]? 64
Enter IPsec Tunnel ID [1]? 2
Packet-filter 'out-router-A' Config>
```

*out-router-A* の 2 番目のアクセス制御規則は、IPSec トンネルの両端間で保護されたパケットをパスすることを許可します。

```
Packet-filter 'out-router-A' Config> add access
Enter type [E]? I
Internet source [0::0]? 2000::A
Prefix Length [64]? 64
Internet destination [0::0]? 2000::B
Prefix Length [64]? 64
Packet-filter 'out-router-A' Config>
```

他のパケット・フィルターと同様に、*out-router-A* に対してワイルドカード・アクセス制御規則を構成して、どのアクセス制御規則にも一致しないトラフィックをパスするようにすることも可能です。

## ルーター A の IP セキュリティと IP のリセット

ポリシーの構成が完了したら、Talk 5 **reset ipsec** コマンドを使用して、新しい IPSec 構成のある SRAM を再ロードします。**reset ipsec** コマンドは、IP 構成には影響しません。その後、Talk 5 **reset ipv6** コマンドを使用して、ルーター内の IPv6 を動



的にリセットします。代わりに、各コンポーネントをリセットするために、ルーターをリスタートすることもできます。フィルター規則が再ロードされるように、IPSec と IPv6 をリセットするか、ルーターをリスタートする必要があります。そうしないと、構成がインターフェース上で正しくサポートされない可能性があります。詳しくは、351ページの『第21章 IP セキュリティーの構成および監視』、および **プロトコル構成および監視 参照資料 第 2 巻** の **reset ipv6** コマンドの項を参照してください。

343ページの図37 に示されているように、IPSec トンネル 2 のエンドポイントは、ルーター B のインターフェース 1 にあります。次の手順を実行して、ルーター B を手作業で構成します。

1. IPSec トンネルを作成する。
2. IPSec トンネルのエンドポイントであるルーター・インターフェース上に、アウトバウンド・フィルターを 1 つ作成する。
3. パケット・フィルターのアクセス制御規則を作成する。
4. IPSec をリセットする。
5. IPv6 をリセットする。

## ルーター B の IP セキュリティー・トンネルの作成

ルーター B 内に、ルーター A 内に作成したものと同一 IPSec トンネル (IPSec トンネル 2) を作成する必要があります。ルーター B 内のこのトンネルのローカル IP アドレスは 2000::B で、リモート IP アドレスは 2000::A です。その他の IPSec トンネル・パラメーターは、すべてルーター A に対して指定したものと一致する必要があります。

## ルーター B のパケット・フィルターの構成

ルーター A に対して行ったのと同様に、インターフェース 1 (IPSec トンネル 1 のエンドポイントであるルーター B 内のインターフェース) に、アウトバウンド・パケット・フィルター (*out-router-B*) を構成します。

## ルーター B のパケット・フィルター・アクセス制御規則の構成

*out-router-B* に対するアクセス制御規則を構成して、ネットワーク 3000:1:: から IPSec にアウトバウンド・パケットをパスし、IPSec トンネル 2 を通して処理および伝送するようにします。このアクセス制御規則は、タイプ I および S です。

```
Packet-filter name [ ]? out-router-B
Packet-filter 'out-router-B' Config> add access
Enter type [E]? IS
Internet source [0::0]? 3000:1::
Prefix Length [64]? 64
Internet destination [0::0]? 1000:1::
Prefix Length [64]? 64
Enter IPsec Tunnel ID [1]? 2
Packet-filter 'out-router-B' Config>
```

ここで、*out-router-B* に対して包括的アクセス制御規則を作成して、IPSec によって処理されたパケットを IPSec トンネル 2 を通してパスするようにします。

```
Packet-filter 'out-router-B' Config> add access
Enter type [E]? I
Internet source [0::0]? 2000::B
```

## 手動トンネルの構成 (IPv6)

```
Prefix Length [64]? 64
Internet destination [0::0]? 2000::A
Prefix Length [64]? 64
Packet-filter 'out-router-B' Config>
```

*out-router-B* に対して、2つのアクセス制御規則のどれにも一致しないパケット (たとえば、IPSec トンネル 2 であてでないトラフィック) をドロップせずにパスさせたい場合は、包括的ワイルドカード・アクセス制御規則を作成します。

## ルーター B の IP セキュリティーと IPv6 のリセット

IPSec 機能を作動させ、フィルターをアクティブにするには、まず IPSec と IPv6 をリセットする必要があります。IPSec と IPv6 をリセットするには、talk 5 **reset IPSec** コマンドを使用します。IPSec のリセットについては、370ページの『ルーター A の IP セキュリティーと IP のリセット』を参照してください。IPSec をリセットした後、talk 5 **reset IPv6** コマンドを使用して IPv6 をリセットします。代わりに、各コンポーネントをリセットするために、ルーターをリスタートすることもできます。

## 例: ESP を使用した IP セキュリティー・トンネルの構成

この例には、IPSec トンネルの構成だけを示します (パケット・フィルターの構成は示しません)。

```
IPV6-IPsec config>add tun
Tunnel ID or Tunnel Name [ ]? 2
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [ESP]?
Local IP Address [0::0]? 2000::A
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES, NULL) [DES-CBC]?
Do you wish to change the Local Encryption Key? (Yes or [No]):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [Yes]:
Remote IP Address [0::0]? 2000::B
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF) [DES-CBC]?
Do you wish to change the Remote Encryption Key? (Yes or [No]):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No][No]:
Do you wish to enable this tunnel? [Yes]:
IPV6-IPsec config>
```

## 例: ESP と ESP-NUL を使用した IP セキュリティー・トンネルの構成

認証が必要であることを注意してください。

```
IPV6-IPsec config>add tun
Tunnel ID or Tunnel Name [ ]? 2
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [ESP]?
Local IP Address [0::0]? 2000::A
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [DES-CBC]? null
Additional Padding for Local Encryption (0-120) [0]?
Local ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0::0]? 2000::B
Remote Encryption SPI (1-65535) [1234]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [NULL]?
Do you wish to perform verification of remote encryption padding? [No]:
Remote ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
```

```

Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
IPV6-IPsec config>

```

## 手動 IP セキュリティーの監視 (IPv4)

ここでは、IPv4 を使用して手動 IPsec を監視する方法を説明します。この説明では、インターネット・キー交換環境にアクセスする方法と、使用できるコマンドについて記述します。

### インターネット・キー交換環境へのアクセス

ここでは、IPv4 でインターネット・キー・プロトコル (IKE) を使用する方法を説明します。

IP セキュリティー IKE 監視環境にアクセスするには、**+** プロンプトで次のコマンド列を入力します。

```

+ feature ipsec
IPSP>ike
IKE>

```

### インターネット・キー交換監視コマンド

ここでは、IKE 監視コマンドについて説明します。

表 44. IKE 監視コマンドの一覧

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxiページの『ヘルプの入手』を参照してください。
Delete	特定のトンネルの ISAKMP フェーズ 1 SA を動的に削除するか、フェーズ 1 SA をすべて削除します。
List	特定のトンネルのフェーズ 1 SA、またはすべてのフェーズ 1 SA に関する情報を表示します。
Stats	トンネルの統計値を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxiiページの『下位レベル操作環境の終了』を参照してください。

#### Delete

IKE **delete** コマンドは、特定のトンネルのフェーズ 1 SA、またはすべてのフェーズ 1 SA を削除します。

構文:

```

delete          tunnel
                _
                all

```

**tunnel** 特定のトンネルのフェーズ 1 SA を削除することを指定します。

**all** 全てのフェーズ 1 SA を削除することを指定します。

例: トンネルの削除

## IKE 監視コマンド (Talk 5)

```
PKI config>delete tunnel
Peer address [10.0.0.3]?
```

### List

IKE **list** コマンドは、特定のトンネルのフェーズ 1 SA、またはすべての SA に関する情報を表示するために使用します。

構文:

```
list                tunnel
_                    all
```

**tunnel** 特定のトンネルの SA に関する情報を表示することを指定します。

**all** すべての SA に関する情報を表示することを指定します。

### 例: すべての SA に関する情報のリスト

```
IKE>list all
```

```
Phase 1 ISAKMP Tunnels for IPv4:
```

Peer Address	I/R	Mode	Auto	State	Auth
10.0.0.3	R	Aggr	N	QM_IDLE	pre-shared

```
IKE>LIST TUNNEL 10.0.0.3
```

```
Peer IKE address: 10.0.0.3
Local IKE address: 10.0.0.1
Role: Responder
Exchange: Aggr
Autostart: No
Oakley State: QM_IDLE
Authentication Method: Pre-shared Key
Encryption algorithm: des3
Hash function: md5
Diffie-Hellman group: 1
Refresh threshold: 85
Lifetime (secs): 15000
```

### Stats

IKE **stats** コマンドは、トンネルの統計を表示するために使用します。

構文:

```
stats                tunnel
```

**tunnel** トンネルの SA に関する統計情報を表示します。

**有効値:** 任意の構成済みトンネル名またはトンネル ID

### 例: トンネルの SA 統計の表示

```
IKE>stats
```

```
Peer address [10.0.0.3]?
```

```
Peer IP address.....: 10.0.0.3
Active time (secs)...: 187

In      Out
---    ---
Octets.....: 1229 1248
Packets.....: 14 16
Drop pkts.....: 0 1
Notifys.....: 6 0
```

```

Deletes.....:          0          0
Phase 2 Proposals....:    16         18
Invalid Proposals....:     0          0
Rejected Proposals...:     0          0

```

## 公開キー・インフラストラクチャー環境へのアクセス (IPv4)

ここでは、IPv4 で公開キー・インフラストラクチャー (PKI) を使用方法を説明します。

IP セキュリティー PKI 監視環境にアクセスするには、+ プロンプトで次のコマンド列を入力します。

```

+ feature ipsec
IPSP>pki
PKI>

```

## 公開キー・インフラストラクチャー監視コマンド

ここでは、公開キー・インフラストラクチャー (PKI) 監視コマンドについて説明します。

表 45. PKI 監視コマンドの一覧

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxi ページの『ヘルプの入手』を参照してください。
Cert-load	ルーターの SRAM に証明書をロードします。
Cert-req	CA に証明書要求を提出します。
Cert-save	将来の利用のために証明書をキャッシュに保管します。
List certificate	証明書に関する情報を表示します。
List configured-servers	構成済みサーバーに関する情報を表示します。
Load certificate	証明書の入ったレコードを SRAM から実行時キャッシュにロードします。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

### Cert-load

PKI **cert-load** コマンドは、証明書とプライベート・キーが入ったレコードを、SRAM から実行時証明書キャッシュにロードするために使用します。

構文:

**cert-load**

例: **SRAM** からキャッシュへの証明書レコードのロード

```

Enter type of certificate to be stored into SRAM:
  1)Root certificate;
  2)Box certificate with private key;
Select the certificate type (1-2) [2]?
Name []? test
mystr=1.1.1.1
Box certificate and private key saved into cache successfully

```

## PKI 監視コマンド (Talk 5)

### Cert-req

PKI **cert-req** コマンドは、CA から証明書を要求するために使用します。

構文:

**cert-req**

例: CA からの証明書の要求

```
Enter the following part for the subject name
Country Name(Max 16 characters) []? us
Organization Name(Max 32 characters) []? ibm
Organization Unit Name(Max 32 characters) []? nhd
Common Name(Max 32 characters) []?
Key modulus size (512|768|1024)
[512]?
Certificate subject-alt-name type:
1--IPv4 Address
2--User FQDN
3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 1.1.1.1
Generating a key pair. This may take some time. Please wait ...
PKCS10 message successfully generated
Enter tftp server IP Address []? test
Bad address, try again
Enter tftp server IP Address []? 8.8.8.8
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]?
Certificate request TFTP to remote host successfully.
```

### Cert-save

PKI **cert-save** コマンドは、証明書とプライベート・キーが入ったレコードを SRAM に保管するために使用します。

構文:

**cert-save**

例: SRAM への証明書レコードの保管

```
Enter type of certificate to be stored into SRAM:
1)Root certificate;
2)Box certificate with private key;
Select the certificate type (1-2) [2]?
SRAM Name for certificate and private key []? test
Load as default router certificate at initialization? [No]:
Private key TEST written into SRAM
Both Certificate and private key saved into SRAM successfully
```

### List Certificate

PKI **list certificate** コマンドは、X.509 デジタル証明書に関する情報を表示するために使用します。

構文:

**list certificate**

例: 証明書情報のリスト

```
Router certificate
Serial Number: 914034877
Subject Name: /c=US/o=ibm/ou=nhd/cn=testip
Issuer Name: /c=US/o=ibm/ou=nhd
```

```
Subject alt Name: 1.1.1.1
Key Usage: Sign & Encipherment
Validity: 1999/1/19 23:24:27 -- 2002/1/19 23:54:27
```

## List Configured-servers

PKI **list configured-servers** コマンドは、構成済みサーバーに関する情報を表示するために使用します。

構文:

**list configured-servers**

例: 構成済みサーバーに関する情報のリスト

```
1) Name: SERVER1
   Type: LDAP
   IP addr: 0.0.0.0
      LDAP search timeout (secs): 0
      LDAP retry interval (mins): 0
      LDAP server port number: 0
      LDAP version: 0
      LDAP version: 0
      Anonymous bind ?: y

2) Name: TEST
   Type: TFTP
   IP addr: 9.9.9.9

3) Name: TFTP
   Type: TFTP
   IP addr: 2.2.2.2
```

## Load Certificate

PKI **load certificate** コマンドは、証明書を SRAM から実行時キャッシュにロードするために使用します。

構文:

**load certificate**

例: キャッシュへの証明書のロード

```
Enter the type of the certificate:
Choices: 1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]?
Encoding format:
Choices: 1-DER 2-PEM
Enter (1-2): [1]?
Server info name []? test
Remote file name on tftp server (max 63 chars) [/tmp/default_file]? /tmp/test.cert

Attempting to load certificate file. Please wait ...
Router Certificate loaded into run-time cache
```

## IP セキュリティー監視環境へのアクセス (IPv4)

IPv4 IP セキュリティー監視環境にアクセスするには、OPCON プロンプト (\*) で **t 5** と入力します。

```
* t 5
```

次に、+ プロンプトで、次のコマンド列を入力します。

## IP セキュリティー監視環境へのアクセス (IPv4)

```
+ feature ipsec
IPSP>ipv4
IPV4-IPsec>
```

## IP セキュリティー監視コマンド (IPv4)

ここでは、IP セキュリティー監視コマンドについて説明します。

表 46. IP セキュリティー監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxi ページの『ヘルプの入手』を参照してください。
Change tunnel	保護トンネル構成パラメーター値を動的に変更します。
Delete tunnel	保護トンネルを動的に削除します。
Disable	安全な方法でのすべての IP セキュリティー処理 (パケット・フィルタに一致するパケットをドロップする) を動的に使用不可にする、無保護な方法でのすべての IP セキュリティー処理 (パケット・フィルタに一致するパケットをパスさせる) を動的に使用不可にする、または特定の保護トンネルを動的に使用不可にします。
Enable	すべての IP セキュリティー処理を動的に使用可能にする、または保護トンネルを動的に使用可能にします。
List	IP セキュリティー、アクティブなトンネル、および定義済みトンネルに関するグローバルな情報を表示します。
Reset	IP セキュリティーをリセットするか、または保護トンネルをリセットします。このコマンドは、Talk 6 で作成された構成を再ロードします。リセットすると、Talk 5 を使用して構成されたパラメーター値は、Talk 6 を使用して構成されたパラメーター値でオーバーライドされます。
Set	パス MTU (PMTU) 経時タイマーを動的に設定します。
Stats	すべてのトンネルまたは活動トンネルの統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

### Change Tunnel

保護トンネルを動的に変更します。

構文:

**change tunnel ...**

パラメーターの説明は、357 ページの『手動 IP セキュリティー構成コマンド』の **add tunnel** コマンドの項を参照してください。

### Delete Tunnel

**delete** は、1 つの保護トンネルまたはすべての保護トンネルを動的に削除するのに使用します。

構文:

**delete tunnel**

*tunnel-id*  
*tunnel-name*



**all****tunnel-id**

削除する IPSec トンネルの識別子を指定します。

有効値: 1 ~ 65535

デフォルト値: 1

**tunnel-name**

削除する IPSec トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

**all** このインターフェース上のすべての IPSec トンネルを削除することを指定します。**Disable****disable** コマンドは、すべてのインターフェースまたは 1 つのトンネルの IP セキュリティー・プロトコルを動的に使用不可にするのに使用します。

構文:

```
disable                ipsec drop
                        ipsec pass
                        tunnel ...
```

**ipsec drop**

ルーター上の IP セキュリティーを安全な方法で使用不可にします。すべての IPSec トンネルが使用不可にされますが、パケット・フィルタ規則の保護トンネル情報を使用して、IPSec トンネル・パケット・フィルタに一致するパケットを識別します。一致するパケットはドロップされます。

**ipsec pass**

ルーター上の IP セキュリティーを非安全な方法で使用不可にします。すべての IPSec トンネルが使用不可にされます。IPSec トンネル・パケット・フィルタに一致するパケットは、通常のトラフィックとして転送されます。

**tunnel tunnel-id all**

指定されたトンネルまたはすべてのトンネル上の IP セキュリティーを使用不可にします。

**tunnel-id**

使用不可にする保護トンネルの識別子を指定します。

有効値: 1 ~ 65535

デフォルト値: 1

**all** すべてのトンネル

## IP セキュリティー監視コマンド (Talk 5)

### Enable

**enable** コマンドは、すべてのインターフェースまたは 1 つのトンネルの IP セキュリティー・プロトコルを動的に使用可能にするのに使用します。ルーター上の IPsec をグローバルに使用可能にしないと、個別に使用可能にされた IPsec トンネルは活動状態になりません。

**注:** IPsec を使用不可に設定してルーターをリスタートした場合は、IPsec を動的に使用可能にすることはできません。

構文:

```
enable                ipsec
                        tunnel ...
```

**ipsec** ルーター全体の IP セキュリティーを使用可能にします。

**tunnel** *tunnel-id* | **all**

**tunnel-id**

使用可能にする保護トンネルの識別子を指定します。

有効値: 1 ~ 65535

デフォルト値: 1

**all** すべてのトンネル

### List

**list** コマンドは、現行の IP セキュリティー構成を表示するのに使用します。グローバル・トンネル (global tunnels) には、ルーター上のすべてのトンネル (活動および定義済みの両方) が含まれます。すべてのトンネル (all tunnels) には、このインターフェースに構成されたすべてのトンネル (活動および定義済みの両方) が含まれます。活動トンネル (active tunnels) は、現在活動状態のトンネルです。定義済みトンネル (defined tunnels) は、定義されているが活動状態ではないトンネルです。

構文:

```
list ...              all
                        global
                        tunnel
                        active tunnel-id tunnel-name all
                        defined tunnel-id tunnel-name all
```

**例 1:** すべての活動トンネルのリスト

```
IPV6-IPsec>li tunnel ?
ACTIVE
DEFINED
IPsec>li tunnel active
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? all
```

Tunnel Cache:

ID	Local IP Addr	Remote IP Addr	Mode	Policy	Tunnel Expiration
2	1.1.1.1	1.1.1.3	TRANS	ESP	*****
1	1.1.1.1	2.1.1.1	TUNN	AH	*****

例 2: 『パケットが大き過ぎる』 メッセージを受け取った 1 つの活動トンネルのリスト

```
IPV6-IPsec>li tun act 1
```

Tunnel ID	Name	Mode	Policy	Life	Replay Prev	Tunnel Expiration	PMTU
1	tofran2	TUNN	AH	46080	No	10:49 May 8 1998	1420 <b>1</b>

Local Information:

```

IP Address: 2001:1::6101 2
Authentication: SPI: 257 Algorithm: HMAC-MD5
Encryption: SPI: ----- Encryption Algorithm: -----
Extra Pad: ---
ESP Authentication Algorithm: -----

```

Remote Information:

```

IP Address: 2001.1..86
Authentication: SPI: 257 Algorithm: HMAC-MD5
Encryption: SPI: ----- Encryption Algorithm: -----
Verify Pad?: ---
ESP Authentication Algorithm: -----

```

**1** 「パケットが大き過ぎる」を受け取ったパケットがない場合、PMTU は n/a として表示されます。

**2** これは IPv6 アドレスです。IP バージョンが IPv4 の場合、DF ビットの扱い方 (COPY、SET、または CLEAR) を定義するメッセージが表示されます。

例 3: すべてのトンネルのリスト

```
IPV6-IPsec>li all
```

IPsec is ENABLED

IPsec Path MTU Aging Timer is 30 minutes

Defined Manual Tunnels for IPv4:

ID	Name	Local IP Addr	Remote IP Addr	Mode	State
1	tofran2	2001:1::6101	2001:1::86	TUNN	Enabled

Defined Manual Tunnels for IPv6:

```

ID= 1 Name= tofran2 Mode= TUNN State= Enabled
Local IP address= 2001:1::6101
Remote IP address= 2001:1::86

```

Tunnel Cache for IPv4:

ID	Local IP Addr	Remote IP Addr	Mode	Policy	Tunnel Expiration
1	2001:1::6101	2001:1::86	TUNN	AH	10:49 May 8 1998

Tunnel Cache for IPv6:

```

ID= 1 Mode= TUNN Policy= AH Expiration= 10:49 May 8 1998
Local IP Address= 2001:1::6101
Remote IP Address= 2001:1::86

```

## Reset

**reset** コマンドは、ルーター上または 1 つのトンネル上の IP セキュリティーを動的にリセットするのに使用します。IPSec またはトンネルをリセットした後で、必ず **reset IP** コマンドを使用して、IP 構成をリセットしてください。これは、パケット・フィルタやそのアクセス制御規則などのアクセス制御情報を再ロードするために

## IP セキュリティー監視コマンド (Talk 5)

必要です。IP をリセットしないと、パケット・フィルタおよびアクセス制御規則が、新規の IPSec 構成をサポートしない可能性があります。

**reset** コマンドを使用する代わりに、ルーターをリブートすることもできます。ただし、ルーターをリブートするとネットワークがしばらく切断されますが、**reset** コマンドは IP 機能だけを中断します。

構文:

```
reset                ipsec  
                    tunnel tunnel-id tunnel-name all
```

**ipsec** 2212 上の IP セキュリティーをリセットします。IP セキュリティーは一時的に使用不可になった後、リスタートします。IP セキュリティーが使用不可の間、通常は IPSec トンネルによって処理されるパケットは、リセットが完了するまでドロップされます。IP セキュリティーをリセットしても、2212 上の他の機能には影響を与えません。このコマンドは、Talk 6 を使用して作成された IP セキュリティー構成をアクティブにします。Talk 6 IP セキュリティー構成は Talk 5 構成を上書きします。

**tunnel** 指定されたトンネルの IP セキュリティーをリセットします。リセット時にトンネルが使用不可にされている場合、トンネル構成は SRAM 構成から再作成されますが、リセット後もトンネルは使用不可のままです。

**tunnel-id**

リセットする保護トンネルの識別子を指定します。

有効値: 1 ~ 65535

デフォルト値: 1

**tunnel-name**

リセットする保護トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

**all** すべてのトンネル

## Set

パス MTU (PMTU) 経時タイマーを動的に設定します。

構文:

```
set                path
```

パス (path)

このパラメーターは、2212 がトンネル MTU を最大値に戻す前に経過する時間 (分) を定義します。

デフォルト値: 10 (0 は使用不可を意味します)

## Stats

**stats** コマンドは、特定のトンネルまたはすべてのトンネルに関する統計を表示するのに使用します。たとえば、**stats** コマンドは、送受信されたパケットを表示します。

構文:

```
stats                tunnel-id
                    tunnel-name
                    all
```

**tunnel-id**

保護トンネルの識別子を指定します。

有効値: 1 ~ 65535

デフォルト値: 1

**tunnel-name**

構成された保護トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

**all** 2212 上に構成されたすべてのトンネルの統計を表示します。

例:

```
IPV6-IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? all

Global IPSec Statistics

Received:
total pkts  AH packets  ESP packets  total bytes  AH bytes  ESP bytes
-----
0           0           0           0           0           0

Sent:
total pkts  AH packets  ESP packets  total bytes  AH bytes  ESP bytes
-----
0           0           0           0           0           0

Receive Packet Errors:
total errs  AH errors  AH bad seq  ESP errors  ESP bad seq
-----
0           0           0           0           0

Send Packet Errors:
total errs  AH errors  ESP errors
-----
0           0           0
```

## 手動 IP セキュリティーの監視 (IPv6)

ここでは、IPv6 を使用して手動 IPSec を監視する方法を説明します。この説明では、IP セキュリティー環境にアクセスする方法と、使用できるコマンドについて記述します。

## IP セキュリティー監視環境へのアクセス

IP セキュリティー監視環境にアクセスするには、OPCON prompt (\*) プロンプトで **t 5** と入力します。

```
* t 5
```

次に、+ プロンプトで、次のコマンド・シーケンスを入力します。

## IP セキュリティー監視環境へのアクセス

```
+ feature ipsec
IPSP>ipv6
IPV6-IPsec>
```

## IP セキュリティー監視コマンド (IPv6)

IPv6 用の IP セキュリティー監視コマンドは、特に指示のないかぎり IPv4 用に使用されるものと同じです。コマンドの説明は、378ページの『IP セキュリティー監視コマンド (IPv4)』を参照してください。コマンドは IPV6-IPsec> プロンプトで入力します。

## 第22章 差別化サービス機能の使用

この章では、差別化サービス (DiffServ) 機能を使用して、ルーターが適切な IP データ・パケットに優先サービスを提供できるようにする方法を説明します。ルーターは、IP ヘッダーの情報に基づいてパケットをポリシー・データベース内の定義済み構成 (ポリシー機能を使用して作成された) と突き合わせることによって、パケットを分類します。詳しくは、275ページの『第18章 ポリシー機能の使用』を参照してください。この結果、一部のパケットは優先サービスを受けることができます。この章には、次の内容が記載されています。

- 『差別化サービスの概説』
- 388ページの『差別化サービスの用語』
- 388ページの『差別化サービスの構成』

### 差別化サービスの概説

今日 IP ネットワークにインストールされている転送装置のほとんどは、最初に着信したものに最初にサービスを提供するという基準で、データ・パケットに標準の best-effort サービスを提供しています。この送達方式はほとんどのトラフィックに適していますが、最近の新しいアプリケーションでは、特定のパケットを先に速く伝送する要求が増大しつつあります。

差別化サービス (DiffServ) 機能は、ルーターが伝送のために IP パケットを処理する際に、IP パケットに異なるサービス・レベルを提供します。DiffServ は、システム資源 (バッファ) とリンク資源 (帯域幅) を一部のパケットのために予約することによって、一部のパケットに優先サービスを提供します。DiffServ 分類機能は、IP ヘッダー内の各種フィールド (例: 送信元と宛先の IP アドレスとポート番号の範囲、プロトコル・タイプ、着信 TOS バイト) を検査することによって、IP パケットに提供するサービスのタイプを決定します。この機能をスケーラブルに実現するために、個々のフローはストリームに集約されます。ストリームは、DiffServ がバッファと帯域幅の使用を管理するために使用するエンティティです。図38 は、DiffServ がストリームのパケットをどのように処理するかを示しています。

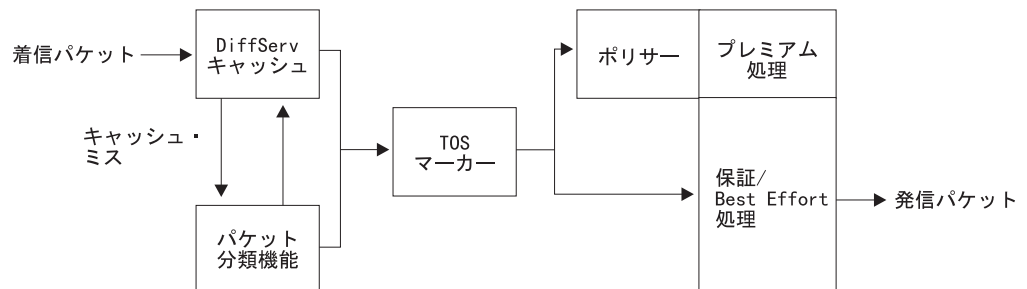


図 38. DiffServ データ・パケットのパス

従来の best-effort サービスに加えて、DiffServ は次のようなサービスを提供します。

#### 急送フォワーディング (EF)

急送フォワーディング・サービスは、DiffServ によるプレミアム・サービスの

## 差別化サービスの使用

設定で、次の説明ではどちらの用語も同じ意味で使われます。このサービスは、特定の転送速度と、保証フォワーディングまたは best effort サービスよりも低い遅延を保証します。余分なトラフィックが発生した場合、DiffServ は余分なトラフィックをドロップします。プレミアム待ち行列は EF サービスを提供し、387ページの図39 には EF 待ち行列として示されています。

### 保証フォワーディング転送 (AF)

保証フォワーディング・サービスは、DiffServ による保証サービスの設定で、次の説明ではどちらの用語も同じ意味で使われます。このサービスは、特定の転送速度を保証しますが、遅延の保証はありません。使用されていない資源が存在する場合、DiffServ は余分なトラフィックを高い速度で送信することができます。387ページの図39 に示されている AF/BE 待ち行列は、AF サービスを提供します。

### Best Effort (BE)

これは標準の best-effort サービスで、サービスや遅延の保証は提供しません。EF サービスと AF サービスのために資源を予約することと、best effort トラフィックが十分なサービスを受けられるだけの資源を残しておくことのバランスをよく考える必要があります。387ページの図39 に示されている AF/BE 待ち行列は、BE サービスを提供します。

ローカル・ルーターは制御パケットを作成して送信するので、制御パケットが十分なサービスを受けられるだけの資源も残しておく必要があります。

DiffServ は現在 PPP リンクとフレーム・リレー・リンク上に設定されており、RSVP サブシステムが使用できます。385ページの図38 は、ストリームのパケットがどのように処理されるかを示しています。ルーターがフローの最初のパケットを受信したときは (プレミアム・サービスを指定されていると仮定します)、高速パス・キャッシュにそのサービス・カテゴリーの指示が存在しないので、パケットは低速パスによって処理されます。DiffServ は、ポリシー・データベースの検索を起動して、パケット処理基準 (ポリシー) を取得します。ポリシーに定義されたアクションは、高速パス・キャッシュに保管されます。ルーターがこのフローの後続のパケットを受け取ると、高速パス・キャッシュにそのフローのエントリーがすでに存在することが検出されるので、ポリシーに定義されたアクションが適用され、パケットは高速パスに進みます。こうして、このフローの後続のパケットはプレミアム・サービスを受けます。

387ページの図39 は、ポリサー、バッファ管理、待ち行列、およびスケジューラーの関係を示しています。これらは、異なるサービス品質レベルを提供する基本コンポーネントの一部です。



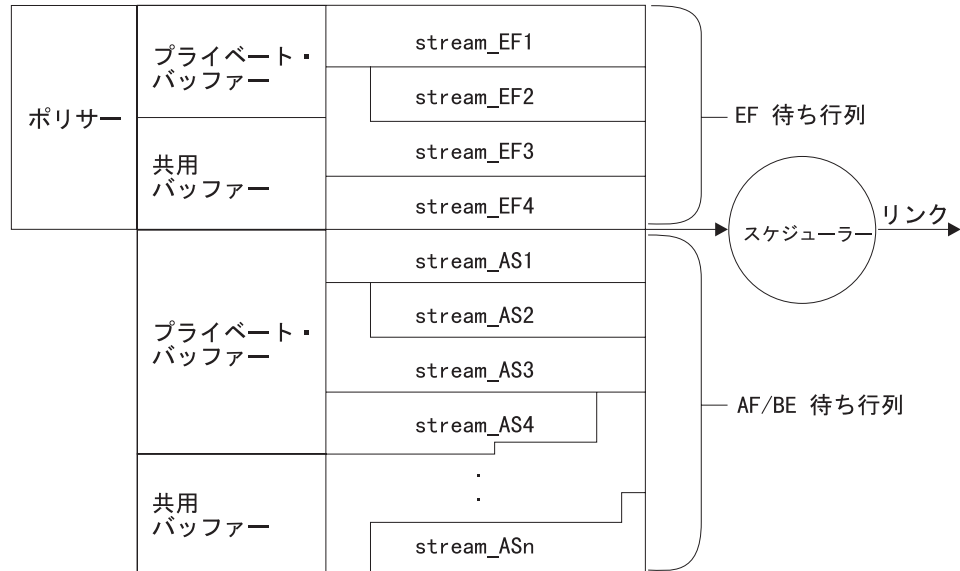


図 39. バッファ、待ち行列、およびスケジューラの関係

急送フォワーディング (EF) サービスと保証フォワーディング (AF) サービスは異なる特性を持っており、これらの特性はルーターにある (1) ポリサー、(2) バッファ管理、および (3) スケジューラの 3 つの機能によってサポートされます。これらの機能は、従来の BE ルーター装置よりも高度なトラフィック制御を実行します。

トラフィックが EF 処理を必要とする場合、余分なトラフィックはドロップする必要があります。DiffServ ポリサー 機能は、トークン・バケットを使用して EF トラフィックを検査し、パケットが余分であるかどうかを判別します。パケットが余分ならば、ポリサーはそのパケットをドロップします。

トラフィックが AF または BE 用の場合、またはポリサーが許可した EF トラフィックの場合は、速度に基づいたバッファ管理 機能がトラフィックを処理します。この機能は、インターフェースのプライベート・プール、または全インターフェース用の共用プールからバッファを割り振ります。インターフェースが使用できる物理バッファ・スペースの合計量を指定するには、Talk 6 **set receive-buffers** 構成コマンド (アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の **set receive-buffers** コマンドの項を参照) を使用します。プレミアム待ち行列と保証待ち行列の発信バッファ・サイズを設定するには、DiffServ Talk 6 **set interface** コマンドを使用します。これは、DiffServ が管理するバッファ・スペースです。(DiffServ は、別個のプールを 2 つ管理します。1 つはプレミアム (EF) 待ち行列用、1 つは保証フォワーディング (AF) 待ち行列用です。指定するバッファ・スペースは、システム内で使用できるバッファ・スペースの実際の量を反映するようにしてください。) バッファ管理は、パケット用に使用できるバッファが、そのインターフェースのプライベート・プールにあるかどうかを判別します。ある場合は、パケットを受け入れ、待ち行列に入れます。バッファがない場合は、共用プールからバッファ・スペースを割り振ることを試み、割り振ることができれば、パケットを待ち行列に入れます。共有バッファ・スペースがない場合は、バッファ管理はパケットをドロップします。

## 差別化サービスの使用

スケジューラー機能は、待ち行列を定期的に検査し、待ち行列に入っているパケットを待ち行列から出して、伝送のためにインターフェース・アダプターに送ります。この機能は、自己クロックを備えたフェア・キューイング・スケジューラーで、重み付けされたフェア・キューイングの一種です。スケジューラーの重みを構成でき、スケジューラーが待ち行列を検査する頻度を指定できます。

**注:** 資源を過剰に割り当てたりオーバー・ブッキングしたりする (つまり、実際よりも多くの帯域幅やバッファがあるかのようにトラフィックの条件制御を構成する) ような DiffServ オプションを構成することが可能です。DiffServ はオーバー・ブッキングをサポートしません。

DiffServ ストリームが活動停止状態 (ストリーム上でパケットが一定期間送信されなかった) になった場合、システムは他のストリームが使用できるように資源を再利用します。ストリームが再度アクティブになった場合は、資源がストリームに戻されます。過剰予約が原因で資源が使用できなくなった場合、DiffServ は定期的に資源の再割り当てを試みます。

ポリシー機能を使用して適切なポリシーを構成した後、DiffServ を設定するために最初に行うステップは、DiffServ **set** コマンドを使用して DiffServ が使用できるシステム資源を定義するオプションを構成することです。次に、**enable ds** コマンドを使用して DiffServ 機能を使用可能にし、**enable interface** コマンドを使用して発信インターフェースを使用可能にします。

---

## 差別化サービスの用語

DiffServ を説明するために、次の用語が使用されています。

### DiffServ キャッシュ

このキャッシュには、ルーターによってサービスを受けている最新のアクティブな IP フローのトラフィックとサービスのプロファイルが入っています。

**フロー** 同じ送信元アドレスとポート、IP プロトコル、および先アドレスとポートをもつ一連のパケット。

### ストリーム

フローの集まり。

### バーチャル・インターフェース (VIF)

フレーム・リレー・リンクの場合、それぞれの DLCI 接続はバーチャル・インターフェースと見なされます。

---

## 差別化サービスの構成

次の手順では、選択したパケットに優先サービスを提供するように DiffServ を構成する方法を、高いレベルで説明します。まず、次のようにして DiffServ 機能にアクセスします。

1. \* プロンプトで、**talk 6** と入力する。
2. Config> プロンプトで、**feature ds** と入力する。DS config> プロンプトが表示され、構成ダイアログが開始されます。

```
* talk 6
Config>feature ds
DS config>
```

3. ルーター上で DiffServ 機能を使用可能にする。

```
DS config>enable ds
DiffServ enabled
```

4. インターフェース・パラメーターを使用可能にし、設定する。

```
DS config>set interface
Enter Diffserv Interface number [0]? 2
Set Premium Queue Bandwidth (%) (1 - 99) [20]?
Assured Queue Bandwidth (%) = 80
Configure Advanced setting (y/n)? [No]: no
Accept input (y/n)? [Yes]:
```

**注:** Configure Advanced setting プロンプトに対して no を指定した場合は、プレミアム待ち行列と保証/BE 待ち行列のデフォルト・パラメーターが使用されません。

```
Configure Advanced setting (y/n)? [No]: yes
Set Premium Queue Weight (%) (20 - 99) [90]?
Assured Queue Weight (%) = 10
EGRESS BufSize for Premium Queue (in bytes) (550 - 16500) [5500]?
Max EGRESS QoS Allocation for Premium Queue (%) (1 - 99) [95]?
EGRESS BufSize for Assured/BE Queue (in bytes) (5500 - 140800) [27500]?
Max EGRESS QoS Allocation for Assured/BE Queue (%) (1 - 99) [80]?
```

この例では、回線帯域幅の 20 パーセントと、スケジューラ重みの 90 パーセントが EF 待ち行列に提供されます。EF 待ち行列の発信バッファ・サイズは 5500 (単位はバイト) で、そのうち 95 パーセントは QOS ストリームに割り当てることができます。AF/BE 待ち行列の発信バッファ・サイズは 27500 (単位はバイト) で、そのうち 80 パーセントは QOS ストリームに割り当てることができます。

5. ルーター上で DiffServ を使用可能にして、インターフェース・パラメーターの設定が完了したら、**Ctrl-P** を入力して \* プロンプトに戻る。

DiffServ を使用可能にして、インターフェース・パラメーターを設定した後、DiffServ をアクティブにするためにルーターをリスタートまたは再ロードする必要があります。DiffServ コマンドの指定について詳しくは、391ページの『第23章 差別化サービスの構成と監視』を参照してください。



## 第23章 差別化サービスの構成と監視

この章では、選択したデータ・パケットに優先サービスを提供するようにルーターとインターフェースを構成するために、差別化サービス (DiffServ) 機能が用意しているコマンドについて説明します。この章には、次の内容が記載されています。

- 『差別化サービス構成プロンプトへのアクセス』
- 『差別化サービス構成コマンド』
- 396ページの『差別化サービス監視環境へのアクセス』
- 396ページの『差別化サービス監視コマンド』

### 差別化サービス構成プロンプトへのアクセス

DiffServ 構成コマンドを入力する手順は、次のとおりです。

1. OPCON (\*) プロンプトで **talk 6** と入力する。
2. Config> プロンプトで **feature ds** と入力する。

DS Config> プロンプトが表示されます。これで、DiffServ 構成コマンドを入力できるようになります。

### 差別化サービス構成コマンド

これらのコマンドを使用して、選択したデータ・パケットに優先サービスを指定する DiffServ オプションを構成できます。表47 は DiffServ 構成コマンドの要約を示し、ここでの残りの部分でこれらのコマンドについて説明します。コマンドは DS Config> プロンプトで入力します。コマンドとオプションを 1 行に入力するか、コマンドだけを入力してプロンプトに答えます。有効なコマンド・オプションのリストを表示するには、オプションの代わりに疑問符 (?) を指定してコマンドを入力します。

表 47. DiffServ 構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxii ページの『ヘルプの入手』を参照してください。
Delete	ルーターの SRAM から DiffServ 構成レコードを削除します。
Disable	ルーター内の、または特定の発信インターフェースに対する DiffServ を使用不可にします。
Enable	ルーター内の、または特定の発信インターフェースに対する DiffServ を使用可能にします。
List	ルーターの DiffServ システムに関する情報と、インターフェース関連の設定値を表示します。
Set	ルーターの DiffServ 関連の設定値を指定します。
Exit	直前のコマンド・レベルに戻ります。xxxiii ページの『下位レベル操作環境の終了』を参照してください。



**interface** 使用可能にするインターフェースの番号を入力するプロンプトが  
出されます。

**例:**

```
DS Config> enable interface
Enter Interface number [0]? 2
DiffServ interface enabled
```

**注:** DiffServ は、PPP リンクとフレーム・リレー・リンク上でだけ使用可能に  
することができます。

## List

**list** コマンドは、ルーターの DiffServ システムに関する情報と、インターフェース  
関連の設定値を表示するために使用します。

**構文:** `list` all  
ds  
interface

**all** ルーターの DiffServ に関する情報とインターフェース構成を表示しま  
す。

**ds** ルーターの DiffServ 構成を表示します。

**例:**

```
DS Config> list ds
System Parameters:
    DiffServ:          ENABLED
    Packet_size:      550
    Min BE Alloc (%): 10
    Min CTL Alloc (%): 5
    Number_of_Q:      2
```

**interface** ルーター内のインターフェース、DiffServ の使用可能/使用不可の状  
況、およびそれぞれのインターフェースと待ち行列のパラメーター  
を表示します。

**例:**

```
DS Config> list interface
-----
Net If      Status NumQ Bwdth Wght OutBuf MaxQos Bwdth Wght OutBuf MaxQos
Num         (%)  (%) (bytes) (%) (%)  (%) (%)  (bytes) (%)
-----
2 PPP Enabled 2 20 90 5500 95 80 10 27500 80
3 PPP Enabled 2 20 90 5500 95 80 10 55000 80
```

## Set

**set** コマンドは、ルーターの DiffServ システムとインターフェース関連のパラメーター  
を設定するために使用します。

**構文:** `set` be-alloc-min  
ctl-alloc-min  
interface  
pkt-size

## DiffServ 構成コマンド (Talk 6)

**be-alloc-min** best effort サービスに割り振る合計出力バッファ・スペースの最小パーセンテージを指定します。

**デフォルト値: 10**

**例:**

```
DS Config> set be-alloc-min
Enter Minimum percent output BW allocated to BE service (10 - 50) [10]?
```

**ctl-alloc-min** ネットワーク制御サービスに割り振る合計出力バッファ・スペースの最小パーセンテージを指定します。

**デフォルト値: 5**

**例:**

```
DS Config> set ctl-alloc-min
Enter Minimum percent output BW allocated to CTL service (5 - 20) [5]?
```

**interface** DiffServ を使用可能にするインターフェースを指定し、インターフェース固有のパラメーターをユーザーに尋ねるプロンプトを出します。

### Queue bandwidth

プレミアム待ち行列用に使用する出力リンクのパーセンテージを指定します。残りのパーセンテージは、保証待ち行列の値として使用されます。

**デフォルト値: 20**

### Queue weight

スケジューラーがプレミアム待ち行列を監視する時間のパーセンテージを指定します。残りのパーセンテージは、保証待ち行列の値として使用されます。待ち行列の重みは、スケジューラーが EF トラフィックにすぐに応答できるように、デフォルトでは 90 パーセントになっています。

**デフォルト値: 90**

### Egress buffer size

プレミアム待ち行列と保証待ち行列に入れることができるデータの量 (単位はバイト) を指定します。

プレミアム待ち行列の場合、このパラメーターはプレミアム待ち行列に入れることができるデータの量 (単位はバイト) を制御します。このパラメーターの値が大きすぎると、プレミアム・トラフィックの待ち行列化遅延が大きくなる可能性があります。たとえば、この値を 25 K バイトに設定すると、出力リンク速度が 1.5 Mbps (T1 速度) の場合、133 ミリ秒 (25000 バイト \* 8 ビット/バイト)/1500000 bps、あるいは .133 秒 (133 ミリ秒) の待ち行列化遅延が生じる可能性があります。このパラメーターの値が小さすぎると、小さいバーストをバッファに入れることができなくなる可能性があります。たとえば、これを 2 Kb に設定すると、1500 バイトのパケット 2 つのバーストに対して十分なバッファがないこととなります (パケットが 3000 バイトのバッファ・スペースを必要とするため)。



## DiffServ 構成コマンド (Talk 6)

これらの両極間の妥協案として、デフォルト設定は 5500 バイトになっています。これは、デフォルト・パケット・サイズである 550 の 10 倍です。

### デフォルト値: 5500 (プレミアム待ち行列)

保証待ち行列の場合、このパラメーターは保証待ち行列に入れることができるデータの量 (単位はバイト) を制御します。このパラメーター値に関する考慮事項は、プレミアム待ち行列の場合と同じですが、保証待ち行列のトラフィックにはあまり厳密な遅延要求がないという点が異なります。その代わりに、保証待ち行列トラフィックは TCP フローで構成されている場合が多く、TCP フローはバースト性が高いという性質があります。このため、複数のフローからのバーストに対応するために十分なバッファ・スペースを定義する必要があります。

値 27500 は、デフォルト・パケット・サイズである 550 の 50 倍です。

### デフォルト値: 27500 (保証待ち行列)

## Egress QoS allocation

すべての DiffServ ストリームが予約できる発信バッファ・サイズ値の量 (パーセンテージ) を指定します。残りのパーセンテージは、共用プールの最小サイズとして使用されます。

### デフォルト値: 95 (プレミアム待ち行列)

### デフォルト値: 80 (保証待ち行列)

### 例:

```
DS Config> set interface
Enter Diffserv Interface number [0]? 2

DiffServ Interface enabled

Set Premium Queue Bandwidth (%) (1 - 99) [20]?
Assured Queue Bandwidth (%) = 80

Configure Advanced setting (y/n)? [No]: y

Set Premium Queue Weight (%) (20 - 99) [90]?
Assured Queue Weight (%) = 10

EGRESS BufSize for Premium Queue (in bytes) (550 - 16500) [5500]?
Max EGRESS QoS Allocation for Premium Queue (%) (1 - 99) [95]?

EGRESS BufSize for Assured/BE Queue (in bytes) (5500 - 140800) [27500]?
Max EGRESS QoS Allocation for Assured/BE Queue (%) (1 - 99) [80]?

DiffServ Interface: ENABLED
PREMIUM Queue Bandwidth (%) = 20
PREMIUM Queue Weight (%) = 80
PREMIUM Queue EGRESS BufSize in bytes = 5500
PREMIUM Queue Max EGRESS QoS allocation (%) = 95
ASSURED/BE Queue Bandwidth (%) = 80
ASSURED/BE Queue Weight (%) = 20
ASSURED/BE Queue EGRESS BufSize in bytes = 27500
ASSURED/BE Queue Max EGRESS QoS allocation (%) = 80
Accept input (y/n)? [Yes]:
```

### pkt-size

トラフィック・フローの平均パケット・サイズを指定します (単位はバイト)。この指定によって、DiffServ は着信インターフェースと発信インターフェースに対して使用できるバッファ・スペースを決定

## DiffServ 構成コマンド (Talk 6)

できます。この値が変更された場合、ルーターをリスタートして、DiffServ **set interface** コマンドの値を検討し、必要に応じて変更する必要があります。

デフォルト値: 550

例:

```
DS Config> set pkt-size
Average packet size (64 - 64000) [550]?
```

---

## 差別化サービス監視環境へのアクセス

DiffServ 機能のコンソール部分を使用して、DiffServ 関連の設定値を表示および管理できます。DiffServ 監視環境にアクセスするには、次のように OPCON プロンプト(\*) で **talk 5** と入力します。

```
* t 5
```

次に、+ プロンプトで、次のコマンドを入力します。

```
+ feature ds
DS Console>
```

---

## 差別化サービス監視コマンド

これらのコマンドを使用して、DiffServ 関連の設定値を表示できます。表48 は DiffServ 監視コマンドの要約を示し、ここでの残りの部分でこれらのコマンドについて説明します。コマンドは DS Console> プロンプトで入力します。コマンドとオプションを 1 行に入力するか、コマンドだけを入力してプロンプトに答えます。有効なコマンド・オプションのリストを表示するには、オプションの代わりに疑問符 (?) を指定してコマンドを入力します。

表 48. DiffServ 監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxii ページの『ヘルプの入手』を参照してください。
Clear	着信インターフェースと発信インターフェースの特定ペア間のストリームに関する統計を消去します。
DScache	ルーターの DiffServ キャッシュにある情報を消去または表示します。
List	ルーターの DiffServ システムに関する情報と、インターフェース関連の設定値を表示します。
Exit	直前のコマンド・レベルに戻ります。xxxiii ページの『下位レベル操作環境の終了』を参照してください。

### Clear

**clear** コマンドは、着信インターフェースと発信インターフェースの特定ペア間のストリームに関する統計を消去するために使用します。

構文: clear stream-stats

例:

```
DS Console> clear stream-stats
Incoming Network number : 0
Outgoing Network number : 2
IN Net 0 DiffServ not enabled.
Net 0->2 stream stats cleared at sysclock 85327 Second.
```

## DScache

**dscache** コマンドは、ルーターの DiffServ キャッシュにある情報を消去または表示するために使用します。

構文: **dscache** actions  
clear  
nexthop  
order  
sats

**actions** 指定の IP 送信元から指定の IP へ先に送信されるパケットに対して行うアクションを表示し、存在すれば DiffServ ストリーム ID を表示します。

例:

```
DS Console> dscache actions
Source Address to list []?
Destination Address to list []?
Source      Destination      Pro ProtocolInf Net TosIn/Out Action StrmID
10.1.100.1  9.1.140.1       1 T:x08 C:x00  0 x00->x15 PASS 85
9.1.140.1   10.1.100.1     1 T:x00 C:x00  1 x00->x15 PASS null
```

**clear** DiffServ キャッシュ全体の消去を指定します。

**nexthop** ネクスト・ホップ IP アドレスを表示します。

例:

```
DS Console> dscache nexthop
Source Address to list []? 5.0.13.248
Destination Address to list []? 5.0.11.249
Source      Destination      Pro ProtocolInf Net Tos NextHop
5.0.13.248  5.0.11.249      17 1031> 1031 0 x00 5.0.61.7 (PPP/1)
5.0.13.248  5.0.11.249      17 1032> 1032 0 x00 5.0.61.7 (PPP/1)
5.0.13.248  5.0.11.249      17 1033> 1033 0 x00 5.0.67.1 (PPP/1)
```

**order** パケットの到着順序を表示します。

例:

```
DS Console> dscache order
Order Source      Destination      Pro ProtocolInf Net Tos
1 5.0.16.246      5.0.13.248      1 T:x03 C:x03 2 x00
2 5.0.13.248      5.0.16.246      17 4000> 5678 0 x00
3 5.0.16.246      5.0.13.244      1 T:x03 C:x03 1 x00
4 5.0.13.248      5.0.15.243      17 123> 123 0 x00
```

**stats** 指定の IP 送信元から指定の IP へ先に送信されたパケットに関する統計を表示します。

例:

```
DS Console> dscache stats
Source Address to list []? 5.0.13.248
Destination Address to list []? 5.0.11.249
Source      Destination      Pro ProtocolInf Net Tos RxPkts RxBytes
```

## DiffServ 監視コマンド (Talk 5)

```
5.0.13.248    5.0.11.249    17 1031> 1031    0 x00    432    444096
5.0.13.248    5.0.11.249    17 1032> 1032    0 x00    432    444096
5.0.13.248    5.0.11.249    17 1033> 1033    0 x00    437    459516
```

## List

**list** コマンドは、ルーターの DiffServ システムに関する情報と、インターフェース関連の設定値を表示するために使用します。

構文: **list** interface  
queue  
stream  
vifs

**interface** ルーター内のインターフェース、DiffServ の使用可能/使用不可の状況、着信バッファの割り当てなどの情報を表示します。

**Net** インターフェース番号を表示します。

### Status

DiffServ 状況を表示します。

**KB/s** リンク速度を Kb/秒単位で表示します。

### VirtTime

スケジューラーによって使用されている仮想の時刻を表示します (非 DiffServ リンクの場合は n/a を表示し、進行中のパケットがない場合は 0 を表示します)。

**InMax** 保証転送に対して構成された最大バッファ・サイズを表示します。

**InCurr** 入力ストリームに対して現在使用されているバッファ・スペースの量を表示します。バッファには、進行中のパケットが入ります。

### InShar

この発信インターフェース用に使用できる共用バッファ・スペースの量を表示します。

### InMaxA

すべての QoS ストリーム全体に割り振ることができるバッファ・スペースの最大量を表示します。

### InCurA

入力ストリームが使用できる割り振りバッファ・スペースの量を表示します。

**NumI** 入力ストリームの数を表示します。

**NumO** 出力ストリームの数を表示します。

### 例:

```
DS Console> list interface
DiffServ interfaces:
Net Status  KB/s  VirtTime  InMax  InCurr  InShar  InMaxA  InCurA  NumI  NumO
-----
0 Disabled 1250    n/a    55000    550    49775  44000    5225    22  n/a
1 Disabled 1250    n/a    27500     0    27500  22000     0    20  n/a
```

## DiffServ 監視コマンド (Talk 5)

2 Enabled	256	0	27500	0	27500	22000	0	20	3
3 Enabled	256	0	55000	0	55000	44000	0	20	3
4 Disabled	0	n/a	550000	0	550000	550000	0	20	n/a
5 Disabled	0	n/a	550000	0	550000	550000	0	20	n/a
6 Disabled	0	n/a	550000	0	550000	550000	0	20	n/a
7 Disabled	0	n/a	550000	0	550000	550000	0	20	n/a
8 Disabled	2000	n/a	27500	0	27500	22000	0	20	n/a
9 Disabled	0	n/a	550000	0	550000	550000	0	20	n/a

### queue

DiffServ 発信待ち行列に割り当てられた重みと、発信インターフェースのバッファ割り振り状況を表示します。

#### Queued packets

現在待ち行列に入れられているパケットの数を表示します (0 は、現在待ち行列に入っているパケットがないことを示します)。

#### Svc Tag

この待ち行列が次にサービスを受ける必要がある仮想時刻を表示します。

#### Weight

この待ち行列のスケジューラーの重みを表示します。

#### out\_max\_alloc

DiffServ ストリームに割り振ることができるバッファ・スペースの最大量を表示します。

#### out\_curr\_alloc

割り振り済みバッファ・スペースの現在の量を表示します。

#### out\_max\_buff

この待ち行列用のバッファ・スペースの最大量を表示します。

#### out\_curr\_buff

パケット用に使用されている現在の割り振り済みバッファ・スペースの量を表示します。

#### out\_share\_buff

現在共用プールにあるバッファ・スペースの量を表示します。

#### 例:

```
DS Console> list queue
OUT Network number : 1
```

##### Premium Queue:

```
Queued packets: 0
Svc Tag:        4294967295
Weight: 20
out_max_alloc: 5225 (Bytes)
out_curr_alloc: 0 (Bytes)
out_max_buff:   5500 (Bytes)
out_curr_buff:  0 (Bytes)
out_share_buff: 5500 (Bytes)
```

##### Assured Queue:

```
Queued packets: 0
Svc Tag:        4294967295
Weight: 80
out_max_alloc: 22000 (Bytes)
out_curr_alloc: 4125 (Bytes)
```

## DiffServ 監視コマンド (Talk 5)

```
out_max_buff: 27500 (Bytes)
out_cur_buff: 0 (Bytes)
out_share_buff: 23375 (Bytes)
```

### stream

ストリームに関する情報を表示します。

**Id** ストリーム識別番号

**t** ストリーム・タイプ

**D** DiffServ ストリーム

**B** 最善的ストリーム

**C** ネットワーク制御ストリーム

**R** RSVP ストリーム

**I/o q** 待ち行列タイプ

**q1** プレミアム待ち行列

**q2** 保証/BE 待ち行列

**allo/cur(K)**

このストリームによって割り振られた合計バッファ・スペース (K バイト)。

**tot pkt**

このストリームが送信のために受信した合計パケット数。

**tot Kby**

このストリームが送信のために受信した合計 K バイト数。

**pkt snt**

このストリームが送信した合計パケット数。

**Kby snt**

このストリームが送信した合計 K バイト数。

**ovr snt**

共用バッファを使用して送信されたパケットの数。

**buf drp**

バッファ・スペースがなかったためにこのストリームからドロップされたパケットの数。

**policed**

プレミアム待ち行列に対するポリサーによってドロップされたパケットの数。

例:

```
DS Console> list stream
Incoming Network number : 0
Outgoing Network number : 2
At interface 0, 22 in-streams; clock=904 sec.
Streams from net 0 to net 2:
  Id  t I/o q  allo/cur(K)  tot pkt  tot Kby  pkt snt  Kby snt  ovr snt  buf drp  policed
-----
(policy name)
85  D  in  5.2/  0.0  82384  43828  48653  25883  0  0
    o-q1 5.2/  1.1  48653  25883  0  0  732
(-)
55  B  in  0.0/  0.0  0  0  0  0  0  0  0
    o-q2 2.8/  0.0  263  21  0  0  0
```

```
(-)
44 C in 0.0/ 0.0      0      0      0      0      0      0
   o-q2 1.4/ 0.0      79     6      0      0      0
```

**vifs**

フレーム・リレー・バーチャル・インターフェースに関する情報を表示します。

**例:**

```
DS Console> list vifs 1
```

```
DiffServ virtual interface for dlci: 17
  Status: Inactive - no packets queued for transmission
  CIR: 64000 (bits/sec)
  Virtual Time: 0
  Service Tag: 0
```

```
DiffServ virtual interface for dlci: 16
  Status: Inactive - no packets queued for transmission
  CIR: 64000 (bits/sec)
  Virtual Time: 0
  Service Tag: 0
```

## DiffServ 監視コマンド (Talk 5)



---

## 第24章 レイヤー 2 トンネルの使用 (L2TP、PPTP、L2F)

レイヤー 2 トンネル (L2T) は、L2TP、L2F、および PPTP の各トンネル・プロトコルで構成されます。

レイヤー 2 トンネル・プロトコル (L2TP) は、UDP/IP のようなパケット・ネットワークを通して PPP をトンネル伝送するための IETF 標準トラック・プロトコルです。L2TP は接続型です。

レイヤー 2 転送 (L2F) とポイントツーポイント・トンネル・プロトコル (PPTP) は、IP ネットワークを通じて PPP のトンネル伝送を行うための IETF 情報プロトコルです。

---

### L2TP の概説

L2TP は、多数の個別の自立走行式プロトコル・ドメインが、モデム、アクセス・サーバー、および ISDN ルーターを含む共通のアクセス・インフラストラクチャーを共用することを可能にします。L2TP は、PPP リンク・レイヤー (たとえば、HDLC および非同期 HDLC) のトンネル伝送を許します。このようなトンネルを使用すると、接続するダイヤルアップ・サーバーの場所とネットワークへのアクセスを提供する場所とを分離することが可能になります。

従来のインターネット上のダイヤルアップ・ネットワーク・サービスは、登録された IP アドレスに対してだけ提供されています。L2TP は、インターネット上の複数プロトコルおよび未登録 IP アドレスを許容する新しいクラスのバーチャル・ダイヤルアップ・アプリケーションを定義しています。このクラスのネットワーク・アプリケーションは、既存のインターネット・インフラストラクチャーを利用して PPP 経由で私設アドレス IP、IPX、および AppleTalk ダイヤルアップをサポートするのに便利です。

このようなマルチプロトコル・バーチャル・ダイヤルアップ・アプリケーションに対するサポートは、アクセスおよびコア・インフラストラクチャーへの巨額の投資を分担することができ、エンド・ユーザーはローカル・コールを使用してサービスにアクセスできるなど、エンド・ユーザー、企業、およびインターネット・サービス提供者のどちらにとっても有益です。

L2TP では、既存のインターネット・インフラストラクチャーの IP 以外のプロトコル・アプリケーションへの現行投資も活用できることが保証されます。

404ページの図40 は、ISDN を使用した L2TP ネットワークの例を示しています。このネットワークでは、L2TP ネットワーク・アクセス・コンセントレーター (LAC) と L2TP ネットワーク・サーバー (LNS) の間に、任意の媒体タイプを使用することができます。

## レイヤー 2 トンネルの使用

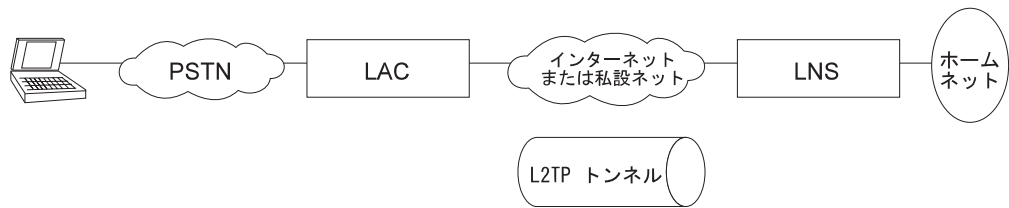


図 40. L2TP ネットワークの例

## L2TP の用語

L2TP を説明するために、次の用語が使用されています。

### 属性値ペア (AVP)

メッセージ・タイプと本文をコード化するための統一方式。この方式により、L2TP の拡張性が最大化され、相互運用も可能になります。

### L2TP アクセス・コンセントレーター (LAC)

PPP 運用と L2TP プロトコルの両方を扱える、1 つまたは複数の公衆電話網 (PSTN) または ISDN 回線に接続された装置。LAC は、L2TP を運用する媒体を設定しています。L2TP は、トラフィックを 1 つまたは複数の L2TP ネットワーク・サーバー (LNS) にパスします。L2TP は PPP ネットワークによって運ばれたプロトコルをトンネル伝送することができます。

### L2TP ネットワーク・サーバー (LNS)

LNS は、PPP エンド・ステーションとして使用できる任意のプラットフォーム上で稼働します。LNS は、L2TP プロトコルのサーバー側を扱います。L2TP は単一媒体にだけ依存して L2TP トンネル伝送を行うので、LNS は 1 つの LAN または WAN インターフェースしか持つことができませんが、LAC がサポートする任意の PPP インターフェースから着いたコールを終了させることができます。

### ネットワーク・アクセス・サーバー (NAS)

ユーザーに一時的なオンデマンド・ネットワーク・アクセスを提供する装置。このアクセスは、PSTN または ISDN 回線を使用するポイントツーポイントです。

### セッション (コール)

L2TP は、ダイヤル・ユーザーと LNS 間でエンド・エンド PPP 接続が試みられると、セッションを作成します。セッションのデータグラムは、LAC と LNS 間のトンネルを介して伝送されます。LNS と LAC は、LAC に接続された各ユーザーの状態情報を維持します。

### トンネル

トンネルは LNS と LAC の対によって定義されます。トンネルは、LAC と LNS 間で PPP データグラムを伝送します。1 つのトンネルが多数のセッションを多重化することができます。同じトンネルを介して作動する制御接続が、すべてのセッションおよびトンネル自体の確立、解放、保守を制御します。

## サポートされるフィーチャー

L2TP は UDP/IP を介して稼働し、次の機能をサポートします。

- 単一ユーザー・ダイヤルイン・クライアントのトンネル伝送
- 小規模ルーター (たとえば、認証ユーザーのプロファイルに基づいて単一静的ルートを確認するルーター) のトンネル伝送
- コールは、LAC から LNS へ (インバウンド)、LNS から LAC へ (アウトバウンド)、またはどちらかのピアによって (両方) 開始することができます。アウトバウンド・コールは、固定 (常にアップ) または要求に基づいた L2 トンネル・セッションのどちらかです。
- 1 つのトンネルでの複数のコール
- PAP、CHAP、および MS-CHAP のプロキシー認証
- プロキシー LCP
- プロキシー LCP が LAC で使用されない場合の LCP のリスタート
- トンネル・エンドポイント認証
- プロキシー PAP パスワードを転送するための隠し AVP
- ローカル rhelm (つまり、user@rhelm) ルックアップ・テーブルを使用したトンネル伝送
- AAA サブシステム内の PPP ユーザー名ルックアップを使用したトンネル伝送
- SNMP を使用した L2TP トンネルの管理。プロトコル構成および監視 参照資料 第 1 巻の『SNMP 管理』の項を参照してください。

注: Rhelm トンネル伝送では、*name@rhelm* 形式のユーザー名が必要です。この方式のトンネル伝送では、ソフトウェアは 2 つのテーブルを使用して、ダイヤルイン・ユーザーのトンネル伝送のあて先を解決する必要があります。このトンネル伝送方式の利点は、ユーザーは rhelm を定義するだけで済み、その rhelm に一致するすべてのユーザー名が同じあて先にトンネル伝送されます。

ユーザー・ベースのトンネル伝送の場合は、1 つのテーブルで解決されます。この方式では、各ユーザーを個別に固有のあて先にトンネル伝送することができます。

- LNS 用の BRS (PPP エンドポイントとして)
- **delete interface** コマンドを使用して L2TP 装置を削除する機能
- 動的に L2TP 装置を再構成する機能
- 順序制御、待ち行列化、再送、およびフロー制御チャネルの設定。L2TP はデータ・チャネルの順序制御、待ち行列化、およびフロー制御も行います。
- ユーザーが UDP ポートに基づいて IP セキュリティー・フィルターを作成できるように L2TP UDP ポート (1701) を固定する機能。
- L2TP ルーター・クライアント。L2TP ルーター・クライアントは、『クライアント開始』(ボランティア・トンネル伝送とも呼ばれます) モデルです。この機能は、サービス提供者のトポロジーとは無関係に、保護された、トンネル伝送による、マルチプロトコル・バーチャル私設ネットワーク (VPN) サービスを提供します。この機能により、クライアントと LAC を 1 つの物理ハードウェアに結集することができます。

## レイヤー 2 トンネルの使用

- インバウンド・コールをリモート・ホスト名に照合して、該当するインターフェースに接続。リモート・ホスト名が、ホスト名照合用に構成されたインターフェースのどれにも一致しない場合、そのコールは、リモート・ホスト名照合を使用しないインバウンド・インターフェース上で終了します。

注: 同じ LAC と LNS の対に対して複数のネット・マッピングを構成した場合、各マッピングにつき 1 つだけトンネルが存在することを確認してください。

- リモート・ホスト名照合を使用しないインバウンド・ネットの自動 IP、IPX、およびブリッジング構成。リモート・ホスト名照合を使用するアウトバウンド・ネットおよびインバウンド・ネットは、手動で構成する必要があります。

サポートされているその他のレイヤー 2 トンネル・プロトコルには、次のものがあります。

- L2F- NAS とゲートウェイの両機能がサポートされます。
- PPTP- ルーター・クライアント、PAC (PPTP アクセス・コンセントレーター)、および PNS (PPTP ネットワーク・サーバー) がサポートされます。

L2F は、L2TP をサポートしていないネットワーク装置に接続する場合に、相互運用可能なレイヤー 2 トンネルを提供します。

PPTP は、L2TP をサポートしていないネットワーク装置に接続する場合に、相互運用可能なレイヤー 2 トンネルを提供します。具体的には、PPTP は Microsoft Windows 95 (DUN 1.2 以上)、Windows 98、および Windows NT から IBM ルーターへの VPN サービス用に使用できます。

注: L2F と PPTP は、両方ともレイヤー 2 トンネル機能の中で構成されます。

---

## タイミングに関する考慮事項

ルーティング・ネットワークを介した PPP パケットのトンネル伝送は、その性質上、タイミングに関するいくつかの問題を考慮する必要があります。L2TP では、LAC と LNS の間の接続には、トンネル伝送のピアがタイムアウトになるほどの遅延はないものと想定しています。ピア間の待ち時間が PPP 状態遷移タイムアウト (通常は 3 秒) に達したり、それを超える状態が繰り返される場合は、接続性が妨げられる可能性があります。LAC と LNS 間の待ち時間がこのように悪い場合、接続全般が悪い状況になり、PPP 状態遷移を人為的に活動状態に維持しても、適正な接続が得られなくなります。接続の両側に PPP タイムアウトを延長する機能が備わっている場合は、これを使用すると、接続が非常に悪い状況でも接続できることがあります。

待ち時間の他に、LAC/LNS のペアと LAC/クライアントのペアの間の帯域幅の不一致も問題の原因になることがあります。たとえば、LAC と LNS の実際の帯域幅が PPP クライアントの帯域幅を大きく下回っている場合、LAC は LNS にパケットを送信するのに長時間かかる可能性があります。一方、LNS と LNS ホーム・ネットワーク上のホストとの間の接続が、ダイヤルイン・クライアントに比べて極端に速い場合、LNS は LAC にデータを送信するのに過剰な負担がかかる可能性があります。L2TP は、このような状況に対処するために、一連の内部および外部フロー制御を設定しています。

## LCP に関する考慮事項

プロキシー LCP を使用している場合、LAC が LCP とネゴシエーションし、PPP は LNS で処理を継続します。LAC は LCP オプションを LNS に転送するので、LNS はネゴシエーションの結果を知ることができます。LNS は、クライアントと LAC 間でネゴシエーションされるパラメーターに対して柔軟であることが必要です。LNS に受け入れられないパラメーターがあった場合、L2TP はトンネルを介してクライアントに *LCP 構成要求* を送って LCP と再ネゴシエーションします。

LNS が柔軟性を保つという要件は、MRU については特に重要です。IBM LNS では、構成された MRU は、プロキシー LCP に許容される最大値です。LAC からのプロキシー LCP メッセージの値が、LNS に構成された MRU 値より大きい場合、L2TP は LCP と再ネゴシエーションして、LAC からの他の LCP オプションは変更せずに、MRU を構成された MRU 値に等しくしようと試みます。

## レイヤー 2 トンネルの構成

L2T を構成するには、次のようにします。

1. **feature** コマンドを使用して、レイヤー 2 トンネル機能にアクセスする。

```
Config> feature layer-2-tunneling
Layer-2-Tunneling config>
```

2. 必要に応じ、L2TP、L2F、および PPTP を使用可能にする。

```
Layer-2-Tunneling config> enable L2TP
```

```
Layer-2-Tunneling config> enable L2F
```

```
Layer-2-Tunneling config> enable pptp
```

3. 必要な L2T ネットワークを追加する。LAC、L2F NAS、または PPTP PAC だけに限定される場合は、L2T ネットを追加する必要はありません。同時にトンネル伝送されるそれぞれの PPP 接続に対し、L2T ネットを 1 つずつ定義する必要があります。

```
Layer-2-Tunneling Config>ADD L2-NETS
Additional L2 nets: [0]? 10
Add unnumbered IP addresses for each L2 net? [Yes]: yes
Adding device as interface 31
Defaulting Data-link protocol to PPP
Adding device as interface 32
Defaulting Data-link protocol to PPP
Adding device as interface 33
Defaulting Data-link protocol to PPP
Adding device as interface 34
Defaulting Data-link protocol to PPP
Adding device as interface 35
Defaulting Data-link protocol to PPP
Adding device as interface 36
Defaulting Data-link protocol to PPP
Adding device as interface 37
Defaulting Data-link protocol to PPP
Adding device as interface 38
Defaulting Data-link protocol to PPP
Adding device as interface 39
Defaulting Data-link protocol to PPP
Adding device as interface 40
Defaulting Data-link protocol to PPP
```

- a. L2TP、L2F、または PPTP のトンネルを構成する。

AAA ローカル・リストを使用して L2TP トンネルを構成するには、次のように指定します。

## レイヤー 2 トンネルの使用

```
Config> add tunnel-profile
Enter name: []? lns.org
Tunneling Protocol? (PPTP, L2F, L2TP): L2TP
Enter local hostname: []? lac.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 11.0.0.1

      PPP user name: lns.org
      Tunnel Server: 11.0.0.1
      Hostname: lac.org

User 'lns.org' has been added
Config>
```

上の例を使用して、LAC 上のトンネル認証、および『user@lns.org』形式の『rhelm』トンネル伝送を構成することができます。

トンネル認証を特定の RADIUS サーバーで実行するように設定することも可能です。AIS 機構の使用と構成の『認証、許可、および会計 (AAA) セキュリティの使用』を参照してください。

LNS を構成していて、トンネル認証が LAC と LNS の両方で使用不可になっている場合は、トンネル・プロファイルを構成する必要はありません。

AAA ローカル・リストまたは RADIUS を使用して、LAC 上の PPP ユーザー名に基づいてトンネル伝送する場合は、次のように指定します。

```
Config> add ppp-user
Enter name: []? peter
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will 'peter' be tunneled? (Yes, No): [No] Y
Tunneling Protocol (PPTP, L2F, L2TP): [L2TP] L2TP
Enter local hostname: []? lac.org
Tunnel-Server endpoint address: [0.0.0.0]? 11.0.0.1

      PPP user name: peter
      Tunnel Server: 11.0.0.1
      Hostname: lac.org

Is information correct? (Yes, No, Quit): [Yes]

User 'peter' has been added
Config>
```

- b. インバウンド・トンネルのリモート・ホスト名照合を構成します (必要な場合)。

ただし、クライアント・ダイヤルインの構成手順の場合は、このステップは通常必要ありません。このオプションは、接続が特定のネットを使用する必要がある場合に使用します。

前の構成はネット 10 に対するものと想定します。

```
Config> net 10
L2TP 10> set remote-hostname
Remote Tunnel Hostname: [] ibm.com
```

**注:** リモート・ホスト名照合をオフにするには、次のコマンドを使用します。

```
Config> net 10
L2TP 10> set any-remote-hostname
```

4. L2TP 発信コールを構成します。次の例は、IP アドレス 1.1.1.1 を持つ LAC および IP アドレス 1.1.1.2 を持つ LNS を示しています。LNS は、LAC から 5552160 へのダイヤル・オンデマンド ISDN コールを発信するように構成されています。



**LNS 構成:**

```

Config> add tunnel-profile
Enter name: []? lac.org
Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
Enter local hostname: []? lns.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

      Tunnel name: lac.org
      TunnType: L2TP
      Endpoint: 1.1.1.1
      Hostname: lns.org

User 'lac.org' has been added
Config>
Config> add dev layer-2-tunneling
Config> net 10
L2TP 10> set connection-direction outbound
L2TP 10> set idle 30
L2TP 10> set remote-hostname lac.org
L2TP 10> enable outbound-call-from-lac
      Outbound Call Type (ISDN)? [ISDN]
      Outbound calling address: 5552160
      Outbound calling subaddress:
L2TP 10>
L2TP 10> encapsulator
PPP 10> set name vickie a
L2TP 10>
L2TP 10> exit
Config> add ppp-user larry b

```

**注:**

- a. LNS 装置が認証される場合は、認証名を設定します。この例には示されていない追加のプロンプトが出ます。詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの“ポイント・ポイント・プロトコル・インターフェースの使用”の章にある『PPP 認証の構成』を参照してください。
- b. LNS で認証されるユーザーを追加します。この例には示されていない追加のプロンプトが出ます。コマンド構文およびオプションについては、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの“CONFIG プロセス (CONFIG - Talk 6) およびコマンド”の章の Add の項を参照してください。

**LAC 構成:**

```

Config> add tunnel-profile
Enter name: []? lns.org
Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
Enter local hostname: []? lac.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.2

      Tunnel name: lns.org
      TunnType: L2TP
      Endpoint: 1.1.1.1
      Hostname: lac.org

User 'lns.org' has been added
Config>
Config> add dev dial-in a

```

## レイヤー 2 トンネルの使用

注:

- a. 物理的にコールするのに使用されます。
5. L2TP ルーター・クライアントを構成する。次の例は、L2TP ルーター・クライアント機能を使用した L2TP ボックス・ボックス接続を示しています。この接続は単方向に設定されており、要求ベースです。

クライアント構成:

```
Config> add tunnel-profile
Enter name: []? lns.org
Tunnel Protocol? (PPTP, L2T, L2TP): [L2TP]
Enter local hostname: []? client.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

Tunnel name: lns.org
TunnType: L2TP
Endpoint: 1.1.1.1
Hostname: client.org

User 'lns.org' has been added
Config>
Config> add dev layer-2-tunneling
Config> net 10
L2TP 10> set connection-direction outbound
L2TP 10> set idle 30
L2TP 10> set remote-hostname lns.org
L2TP 10> encapsulator
PPP 10> set name donald a
PPP 10> exit
L2TP 10> exit
Config>
```

注: a -- クライアント装置が認証される場合は、認証名を設定します。この例には示されていない追加のプロンプトが出ます。詳しくは、アクセス・インテグレーション ルーター・サービス ソフトウェア使用者の手引き の『PPP 認証の構成』を参照してください。

LNS 構成:

```
Config> add tunnel-profile
Enter name: []? client.org
Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
Enter local hostname: []? lns.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.2

Tunnel name: client.org
TunnType: L2TP
Endpoint: 1.1.1.2
Hostname: lns.org

User 'client.org' has been added
Config>
Config> add dev layer-2-tunneling
Config> net 10
L2TP 10> set connection-direction inbound
L2TP 10> set remote-hostname client.org
```



```
L2TP 10> encapsulator
Config>
Config> add ppp-user donald b
Config>
```

注: **b**-- LNS で認証されるユーザーを追加します。この例には示されていない追加のプロンプトが出ます。詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の『**add** 構成コマンド』の項を参照してください。

6. **set** コマンドと **enable** コマンドを使用して、各種機能の L2T パラメーターを構成する (必要な場合)。

```
Layer-2-Tunneling Config>set ?
Layer-2-Tunneling Config>enable ?
```

7. **encapsulator** コマンドを使用して、インバウンドおよび *\*any\** インバウンド・トンネル・ホスト名を設定されたすべての L2 ネットの PPP パラメーターを構成する (必要な場合)。

```
Layer-2-Tunneling Config>encapsulator
PPP-L2TP Config>
```

PPP の構成が完了したら、**exit** を入力して、L2T 機能の構成環境に戻ります。

## レイヤー 2 トンネルの使用

## 第25章 レイヤー 2 トンネル・プロトコルの構成と監視

この章では、レイヤー 2 トンネル (L2T) の構成コマンドと操作コマンドについて説明します。L2T は、レイヤー 2 トンネル・プロトコル (L2TP)、レイヤー 2 転送プロトコル (L2F)、およびポイントツーポイント・トンネル・プロトコル (PPTP) を組み込んでいます。この章には、次の内容が記載されています。

- 『L2T インターフェース構成プロンプトへのアクセス』
- 『L2 トンネル・インターフェース構成コマンド』
- 415ページの『L2 トンネル機能構成プロンプトへのアクセス』
- 416ページの『L2 トンネル機能構成コマンド』
- 421ページの『L2 トンネル監視プロンプトへのアクセス』
- 421ページの『L2 トンネル監視コマンド』

### L2T インターフェース構成プロンプトへのアクセス

L2T インターフェース構成プロンプトにアクセスする手順は、次のとおりです。

1. OPCON (\*) プロンプトで **talk 6** と入力する。
2. Config> プロンプトで **add dev layer-2-tunneling** と入力する (または、**add l2-nets** コマンドを使用する。416ページの『Add』を参照してください)。
3. Config> プロンプトで **n interface#** と入力する。

```
Config> add device layer-2-tunneling
Enter the number of Layer-2-Tunneling interfaces [1]
Adding device as interface 8
Defaulting Data-link protocol to PPP
Config> n 8
Session configuration
L2T config: 8>
```

### L2 トンネル・インターフェース構成コマンド

表49 は、L2T インターフェース構成コマンドの一覧です。これらのコマンドは L2T Config n> プロンプトで入力します (ただし、n はネット番号)。

表49. L2 トンネル・インターフェース構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxii ページの『ヘルプの入手』を参照してください。
Disable	発信コールを使用不可にします。
Enable	発信コールを使用可能にします。
Encapsulator	L2T インターフェースの PPP パラメーターを構成できます。 <b>注:</b> encapsulator オプションは、インターフェースに構成済みリモート・ホスト名がある場合だけ使用できます。
List	L2T インターフェースに関する情報を表示します。
Set	各種の L2T インターフェース・パラメーターを設定できます。

## L2 トンネル・インターフェース構成コマンド (Talk 6)

表 49. L2 トンネル・インターフェース構成コマンド (続き)

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

### Disable

**disable** コマンドは、L2TP アクセス・コンセントレーター (LAC) からのアウトバウンド・コールを使用不可にするために使用します。

構文: `disable` `outbound-calls-from-lac`

#### **outbound-calls-from-lac**

LNS が L2TP トンネルを経由して LAC からのダイヤル信号を開始しないようにします。

### Enable

**enable** コマンドは、L2TP アクセス・コンセントレーター (LAC) からのアウトバウンド・コールを使用可能にするために使用します。このコマンドは、L2TP に対してだけ使用する必要があります。

構文:

`enable` `outbound-calls-from-lac`

#### **outbound-calls-from-lac**

LNS が L2TP トンネルを経由して LAC からのダイヤル信号を開始できるようにします。

例:

```
L2T 10> enable outbound-call-from-lac
Outbound Call Type (ISDN)? [ISDN]
Outbound calling address: 1234
Outbound calling subaddress:
L2T 10>
```

### Encapsulator

**encapsulator** コマンドは、L2T インターフェースの PPP パラメーターを構成するのに使用します。

構文: `encapsulator`

このコマンドは、リモート・ホスト名が構成済みの場合にだけ使用できます。

ppp-L2tp config>プロンプトで使用できるコマンドの一覧は、

419ページの『Encapsulator』を参照してください。

### List

**list** コマンドは、種々の L2T インターフェース構成パラメーターの状態を表示するのに使用します。

構文: `list`

## L2 トンネル・インターフェース構成コマンド (Talk 6)

```
Layer-2-Tunneling Config>list
CONNECTION TYPE
-----
Connection Direction      INBOUND
Remote Tunnel Hostname    *ANY*
```

### Set

set コマンドは、L2T インターフェース動作パラメーターを構成するのに使用します。

構文: `set`      `any-remote-hostname`  
                  `connection-direction`  
                  `idle`  
                  `remote-hostname`

#### **any-remote-hostname**

このネット上のアウトバウンド・リモート・ホスト名をクリアし、インバウンド・リモート・ホスト名照合を使用不可にします。

#### **connection-direction [inbound] or [outbound] or [both]**

接続を開始できるのは、このネット上のピア (インバウンド)、ローカル装置 (アウトバウンド)、あるいはピアまたはローカル装置のどちらか (両方) のどれであるかを指定します。「両方」を指定した場合は、アイドル時間を 0 に指定することはできません。

デフォルト値: インバウンド

#### **idle-time** *seconds*

L2 トンネルがこのネット上のトンネル・セッションを切断するまでの非活動状態の秒数を指定します。ゼロの値は、そのトンネルは固定であり、切断してはならないことを示します。

有効値: 0 ~ 1024

デフォルト値: 0

#### **remote-hostname** *hostname*

ピアのトンネル・ホスト名を指定します。

アウトバウンド・トンネルの場合、ホスト名は AAA サブシステム内に構成されているトンネル・プロファイルを指定します。この名前は、ピアが自身を識別するために使用するトンネル・ホスト名でなければなりません。

インバウンド・トンネルの場合、このホスト名によって自身を識別するトンネル・ピアだけが、このインターフェースに接続できます。

有効値: 1 ~ 64 桁の ASCII 文字から成る任意の名前

デフォルト値: 名前

---

## L2 トンネル機能構成プロンプトへのアクセス

L2 トンネル機能構成プロンプトにアクセスする手順は、次のとおりです。

1. OPCON (\*) プロンプトで **talk 6** と入力する。
2. Config> プロンプトで **feature layer-2-tunneling** と入力する。

## L2 トンネル機能構成コマンド

表50 は、L2 トンネル機能構成コマンドの要約を示し、ここでの残りの部分で、これらのコマンドについて説明します。次のコマンドは Layer-2-Tunneling Config> プロンプトで入力します。

表 50. L2 トンネル機能構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxii ページの『ヘルプの入手』を参照してください。
Add	L2 トンネルのネットとピアを追加します。
Disable	L2 トンネル機能を使用不可にします。
Enable	L2 トンネル機能を使用可能にします。
Encapsulator	リモート・ホスト名を構成されていない (ANY) すべての L2 トンネル・ネットの PPP パラメーターを構成できます。
List	L2 トンネル構成に関する情報を表示します。
Set	バッファ、コール受信ウィンドウ、およびその他の L2 トンネル・パラメーターを設定することができます。
Exit	直前のコマンド・レベルに戻ります。xxxiii ページの『下位レベル操作環境の終了』を参照してください。

## Add

**add** コマンドは、L2 ネットを追加するために使用します。このルーターで終端する各並行 PPP セッションごとに 1 つの L2 ネットが必要です。トンネル伝送 PPP セッションの終端は、トンネルの LNS エンドポイントです。

構文: **add**

          
L2-nets

## L2-nets

**注:** このコマンドは、すべて小文字で入力できます。分かりやすくするために、最初の文字は大文字で示してあります。

L2 トンネル構成に L2 ネットを追加します。このルーターで転送される各並行 PPP セッションごとに 1 つの L2 ネットが必要です。このルーターを LAC としてだけ使用する場合は、バーチャル L2 ネットは必要ありません。このコマンドを入力すると、追加するネットの数および各 L2 ネットの無番号 IP アドレスを追加するかどうかを尋ねるプロンプトが出ます。

追加するネットの数は、今回自動的に追加されるネットの数を指しています。これらのネットは、既存の L2 ネットに追加されます。

各 L2 ネットの無番号 IP アドレスを追加すると、各 L2 ネットの IP ルーティング・テーブルに無番号 IP エントリが自動的に追加されます。無番号 IP アドレスは、お勧めしている運用方式です。L2 ネットで番号付きアドレスを使用する必要がある場合は、IP プロトコル構成環境で変更することができます (プロトコル構成および監視 参照資料 第 1 巻の『IP の構成』の章を参照してください)。

## Disable

**disable** コマンドは、L2 トンネル機能を使用不可にするために使用します。

構文: disable call-rcv-window  
fixed-udp-source-port  
force-chap-challenge  
hiding-for-pap-attributes  
L2f  
L2tp  
pptp  
proxy-auth  
proxy-lcp  
tunnel-auth

### call-rcv-window

L2 トンネルは、順序制御および輻輳 (ふくそう) 制御を行うために、各コールの packets を待ち行列化することができます。それぞれのコールには固有のウィンドウがあります。このウィンドウは、ACK を受信する前に送信できる packets の数です。*call-rcv-window* を使用不可にすると、全セッションのフロー制御と順序付けがオフになります。LAC と LNS 間の接続が高品質で、十分な帯域幅があり、packet 再配列があまり行われないことが分かっている場合は、これを設定しても構いません。

### fixed-udp-source-port

固定 UDP ポートの使用をクリアします。このパラメーターを使用不可にした場合、ユーザーは LAC と LNS の間に IP アドレスによる IP セキュリティー・フィルターを構成することを強制されます。

### force-chap-challenge

クライアントの LNS CHAP 再チャレンジを使用不可にします。PPP クライアントによる CHAP 再チャレンジが困難な場合、CHAP 再チャレンジを使用不可にすることが必要になります。

### hiding-for-pap-attributes

LAC と LNS の間のプロキシー PAP 情報の暗号化を使用不可にします。

**L2f** このルーター上の L2F プロトコルを使用不可にします。

**L2tp** このルーター上の L2TP プロトコルを使用不可にします。

**pptp** このルーター上の PPTP プロトコルを使用不可にします。

### proxy-auth

LAC から LNS へ PPP プロキシー認証を送信するのを使用不可にします。

### proxy-lcp

LAC から LNS へ LCP 情報を送信するのを使用不可にします。

### tunnel-auth

このルーターに共有の秘密情報に基づくトンネル・ピアの認証を使用不可にします。

## L2 トンネル機能構成コマンド (Talk 6)

### Enable

**enable** コマンドは、L2 トンネル機能を使用可能にするために使用します。

構文:

```
enable fixed-udp-source-port  
force-chap-challenge  
hiding-for-pap-attributes  
L2f  
L2tp  
pptp  
proxy-auth  
proxy-lcp  
tunnel-auth
```

#### **fixed-udp-source-port**

このパラメーターを使用可能にすると、L2 に対して UDP ポートに基づく IP セキュリティー・フィルターを構成することが可能になり、L2 トラフィックの暗号化または認証を容易に行うことができます。L2TP の場合は、UDP ポートを 1701 に設定します。

#### **force-chap-challenge**

LNS がプロキシー CHAP を受信する場合も、クライアントの LNS CHAP 再チャレンジを使用可能にします。クライアントがこのような再チャレンジを問題なく扱えることが分かっている場合には、セキュリティの観点から、これを使用可能にすることが望まれます。

#### **hiding-for-pap-attributes**

LAC と LNS の間のプロキシー PAP 情報の暗号化を使用可能にします。

**L2f** このルーター上の L2F を使用可能にします。

**L2tp** このルーター上の L2TP を使用可能にします。

**pptp** このルーター上の PPTP を使用可能にします。

#### **proxy-auth**

LAC から LNS へ PPP プロキシー認証を送信するのを使用可能にします。

#### **proxy-lcp**

LAC から LNS へ LCP 情報を送信するのを使用可能にします。

#### **tunnel-auth**

このルーターに共有の秘密情報に基づくトンネル・ピアの認証を使用可能にします。



## Encapsulator

**encapsulator** コマンドは、`ppp-L2tp config>` プロンプトにアクセスするために使用します。このプロンプトは、インバウンドおよび `*any*` リモート・ホスト名を指定して構成された、レイヤー 2 トンネル・インターフェースすべての PPP パラメータを構成するためのものです。

**構文:**            `encapsulator`

## List

**list** コマンドは、種々の L2 トンネル構成パラメータの状態を表示するのに使用します。

**構文:**            `list`

```
Layer-2-Tunneling Config>list
GENERAL ADMINISTRATION
-----
L2TP                               = Enabled
L2F                                 = Disabled
PPTP                                = Disabled
Maximum number of tunnels          = 20
Maximum number of calls (total)    = 50
Buffers Requested                   = 300

CONTROL CHANNEL SETTINGS
-----
Tunnel Auth                         = Enabled
Tunnel Rcv Window                   = 4
Retransmit Retries                  = 6
Local Hostname                      = Host6

DATA CHANNEL SETTINGS
-----
Force CHAP Challenge (extra security) = Disabled
Hiding for PAP Attributes            = Disabled
Hardware Error Polling Period (Sec)  = 120
Call Rcv Window                     = 6

MISCELLANEOUS
-----
SEND PROXY-LCP FROM LAC              = Enabled
SEND PROXY-AUTH FROM LAC             = Enabled
Fixed UDP Source Port (1701)         = Disabled
```

## Set

**set** コマンドは、L2 トンネルの動作パラメータを構成するのに使用します。

**Syntax:** `set`    `buffers`  
           `call-rcv-window`  
           `error-check-direction`  
           `host-lookup-password`  
           `local-hostname`  
           `max-calls`  
           `max-tunnels`  
           `transmit-retries`  
           `tunnel-rcv-window`

## L2 トンネル機能構成コマンド (Talk 6)

### buffers

要求された内部 L2 トンネル・バッファの数を指定します。要求を満たすのに十分なメモリーがない場合、リブートするとバッファの一部が利用可能になります。L2T が活動状態のときにメモリーの量を確認するには、**memory** コマンドを使用します (424ページの『Memory』を参照してください)。

有効値: 1 ~ 1000

デフォルト値: 200

### call-rcv-window

受信ウィンドウとして使用するパケットの数を指定し、**call-rcv-window** を使用可能にします。データ・チャネルのフロー制御が使用可能にされている場合、ルーター上のプロトコルが使用するため、および開始メッセージを使用してピアに通信するのに使用するための受信ウィンドウ・サイズを指定する必要があります。構成された値は、このルーターによって開始されるすべてのコールに適用されます。ゼロの値は、順序付けだけ (フロー制御なし) を指定します。

有効値: 0 ~ 100

デフォルト値: 0

### error-check-period [seconds]

LAC のハードウェア・エラーのポーリング期間を指定します。それぞれのポーリング期間には、LAC から LNS に WAN エラー通知メッセージが送信されます。範囲は 60 ~ 65000 秒です。

デフォルト値: 120 秒

### host-lookup-password

RADIUS トンネル認証に共有の機密情報を指定します。これは、サーバー上で構成されている機密情報と一致している必要があります。

デフォルト値: なし。

### local-hostname

トンネル・セットアップ・メッセージに入って送信される、ローカル・ルーターを識別するホスト名文字列を指定します。

デフォルト値: IBM

### max-calls

LAC または LNS として同時に活動状態にできるすべてのトンネルを通るコールの最大数を指定します。

有効値: 1 ~ 500

デフォルト値: 100

### max-tunnels

LAC または LNS として同時に活動状態にできるトンネルの最大数を指定します。

有効値: 1 ~ 100

デフォルト値: 30

**transmit-retries**

セッションまたはトンネルが非活動状態として宣言されて遮断される前に、制御チャネル上で L2TP パケットが再送される回数を指定します。

有効値: 2 ~ 100

デフォルト値: 6

**tunnel-rcv-window**

高信頼制御接続トランスポートの L2TP 受信ウィンドウ・サイズを指定します。このトランスポートでは、トンネルまたはセッションの設定、切断、および保守のために必要なメッセージを送受信します。

有効値: 1 ~ 100

デフォルト値: 4

---

## L2 トンネル監視プロンプトへのアクセス

L2 トンネル監視プロンプトにアクセスする手順は、次のとおりです。

1. OPCON (\*) プロンプトで **talk 5** と入力する。
2. GWCON (+) プロンプトで **feature layer-2-tunneling** コマンドを入力する。

---

## L2 トンネル監視コマンド

ここでは、L2 トンネル監視コマンドの要約を示し、個々のコマンドについて説明します。コマンドは Layer-2-Tunneling Console> プロンプトで入力します。

表51 は、L2 トンネル監視コマンドの一覧です。

表 51. L2 トンネル監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxii ページの『ヘルプの入手』を参照してください。
Call	コール設定中の各コールに関する統計と情報を表示します。
Kill	トンネルを即時に終了します。
Memory	現在の L2 トンネル・バッファの割り振りと使用状況を表示します。
Start	別のピアとのトンネル伝送を開始します。
Stop	トンネル伝送を停止し、各ピアが必要な管理を実行できるようにします。
Tunnel	既存の各トンネルに関する統計と情報を表示します。
Exit	直前のコマンド・レベルに戻ります。xxxiii ページの『下位レベル操作環境の終了』を参照してください。

## Call

**call** コマンドは、コールの統計と情報を表示するのに使用します。

構文: call      errors  
                      physical-errors  
                      queue

## L2 トンネル監視コマンド (Talk 5)

state

statistics

**errors** このコールで発生した一般的な伝送エラーを表示します。

例:

```
Layer-2-Tunneling Console> call errors
CallID | Serial # | ACK-timeout | Dropped pkts
56744 | 1 | 0 | 0
```

**CallID** このコールに対応するローカル識別子

**Serial #**

このコールをログに記録するのに使用された番号

**ACK-timeout**

ピアからタイムアウト通知を受信した回数

**Dropped pkts**

このコールで紛失を宣言されたパケットの数。これは、受信するはずであったが、ピアによって紛失として通知されたパケットです。

**physical-errors**

コールで発生したデータ・エラーを表示します。

例:

```
Layer-2-Tunneling Console> call physical-errors
CallID | Serial# | CRC Errors | framing Errors | HW overrun | buffer overrun | timeout Errors | alignment | time since updated
56744 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0
```

**CallID** このコールに対応するローカル識別子

**Serial #**

このコールをログに記録するのに使用された番号

**CRC Errors**

CRC が一致しなかったパケットの数

**framing errors**

フレーム・エラーを含むパケットの数

**HW overrun**

ハードウェア・オーバーランが発生した回数

**buffer overrun**

バッファ・オーバーランが発生した回数

**timeout errors**

インターフェースがタイムアウトになった回数

**alignment**

配列エラーが発生した回数

**time since updated**

前回のエラーのポーリングからの経過時間

**queue** 各コールの待ち行列に関する情報を表示します。

例:

```
Layer-2-Tunneling Console> call queue
CallID | Serial # | Tx Win | Rx Win | Ns | Nr | Rx Q | Tx Q | priority | out Q
56744 | 1 | 4 | 4 | 100 | 200 | 0 | 0 | 0 | 0
```

## L2 トンネル監視コマンド (Talk 5)

**CallID** このコールに対応するローカル識別子

**Serial #**

このコールをログに記録するのに使用された番号

**Tx Win**

ピアのデータの最大受信ウィンドウ

**Rx Win**

ローカル最大送信ウィンドウ

**Ns** このコールで送信される次のパケット・シーケンス番号

**Nr** このコールで受信が期待されている次のパケット・シーケンス番号

**Rx Q** 受信待ち行列の現在のパケット数

**Tx Q** 送信待ち行列の現在のパケット数

**priority**

L2TP による送信を待っている優先順位 PPP パケットの数

**out Q** L2TP による送信を待っている通常の PPP パケットの数

**state** 各コールの現在の状態を表示します。

例:

```
Layer-2-Tunneling Console> call state
CallID | Serial # | Net # | State | Time Since Chg | PeerID | TunnelID
56744 | 1 | 2 | Established | 00:00:00 | 345 | 45678
```

**CallID** このコールに対応するローカル識別子

**Serial #**

このコールをログに記録するのに使用された番号

**Net #** このコールに対応する装置番号。LNS のコールの場合、これは L2 ネットです。LAC のコールの場合、これは最初のコールを受信した PPP 装置です。

**State** 現在のコールの状態。有効なコールの状態は、次のとおりです。

**Established**

トンネル・ネットワーク・トラフィックの伝送準備完了。

**Idle** コールはアイドル状態です。

**Wait Cs Answer**

通信リンクがオープンするのを待っています。

**Wait Reply**

ピアからの応答を待っています。

**Wait Tunnel**

トンネルの確立を待っています。

**Time since chg**

前回の状態変更からの経過時間

**PeerID**

ピアのコール ID

**TunnelID**

このコールに対応するローカル・トンネル。

## L2 トンネル監視コマンド (Talk 5)

### statistics

各コールのデータ伝送に関する統計を表示します。

例:

```
Layer-2-Tunneling Console> call statistics
CallID | Serial # | Tx Pkts | Tx Bytes | Rx Pkts | Rx Bytes | RTT | ATO
56744 | 1 | 34 | 1056 | 45 | 1567 | 10 | 34
```

**CallID** このコールに対応するローカル識別子

**Serial #**

このコールをログに記録するのに使用された番号

**Tx Pkts**

このコールの送信されたパケット数

**Tx Bytes**

このコールの送信されたバイト数

**Rx Pkts**

このコールの受信されたパケット数

**Rx Bytes**

このコールの受信されたバイト数

**RTT** このコールの現行の算定一巡時間

**ATO** このコールの現行の算定適応タイムアウト

## Kill

**kill** は、トンネルを即時に終了するのに使用します。このコマンドは、トンネルのすべてのローカル資源を解放して、強制的に接続を終了させます。トンネルの終了はピアに通知されません。

注: このコマンドを使用するのは、**stop** コマンドではトンネルを終了させることができない場合だけに限ってください。

構文: `kill tunnel tunnelid`

**tunnel tunnelid**

終了させるトンネルを指定します。

## Memory

**memory** コマンドは、L2TP の現在のメモリーの使用状況を表示するのに使用します。

構文: `memory`

例:

```
Layer-2-Tunneling Console> mem
Number of layer-2-tunneling buffers: Requested = 2000, Total = 1200, Free = 1000
```

この例では、ユーザーは 2000 のバッファを構成しましたが、1200 しか割り当てることができませんでした。現在、200 のバッファが使用中で、1000 が空いています。

## Start

**start** コマンドは、別のピアとのトンネル伝送を開始するのに使用します。

構文: `start` (パラメーターを付けないと、ホスト名の入力を求められます。)

`tunnel hostname`

**hostname**

L2T がトンネルを確立する相手のホストの名前

## Stop

**stop** コマンドは、トンネル伝送を停止するのに使用します。トンネルを終了する前に、必要な終結処置を完了させます。

構文: `stop tunnel tunnelid`

**tunnel tunnelid**

終了させるトンネルを指定します。

## Tunnel

**tunnel** コマンドは、すべてのトンネルに関する統計と情報を表示するのに使用します。

構文: `tunnel` call  
errors  
peer  
queue  
state  
statistics  
transport

**calls** すべてのトンネルと、各トンネル内の各コールの状態を表示します。

**errors** トンネル上で発生したエラーを表示します。

例:

```
Layer-2-Tunneling Console> tunnel errors
Tunnel ID | Type | ACK-timeouts
96785     | L2TP | 0
43690     | PPTP | 2
96785     | L2F  | 0
```

**Tunnel ID**

このコールに対応するローカル識別子

**Type** 使用されているトンネル・プロトコルのタイプ。

**ACK-timeouts**

ピアからタイムアウト通知を受信した回数

**peer** トンネルとそのトンネルに対応するピアを表示します。

例:

## L2 トンネル監視コマンド (Talk 5)

```
Layer-2-Tunneling Console> tunnel peer
Tunnel ID | Type | Peer ID | Peer Hostname
96785     | L2TP | 89777   | peer1
11264     | L2F  | 46538   | peer2
34653     | L2F  | 11209   | peer3
87511     | PPTP | 55377   | peer4
```

### Tunnel ID

このコールに対応するローカル識別子

**Type** 使用されているトンネル・プロトコルのタイプ。

### Peer ID

このトンネルに割り当てられたピアのトンネル識別子

### Peer Hostname

ローカル・データベースに表示されるピアのホスト名

**queue** 各トンネルの待ち行列に関する情報を表示します。

例:

```
Layer-2-Tunneling Console> tunnel queue
Tunnel ID | Type | Rx Win | Tx Win | Ns | Nr | Rx Q | Tx Q
96785     | L2TP | 4       | 4       | 5  | 6  | 0     | 0
76488     | L2F  | 4       | 4       | 5  | 6  | 0     | 0
22209     | PPTP | 4       | 4       | 5  | 6  | 0     | 0
```

### Tunnel ID

このコールに対応するローカル識別子

**Type** 使用されているトンネル・プロトコルのタイプ。

### Rx Win

ローカルの受信ウィンドウを構成するパケットの最大数

### Tx Win

ピアの受信ウィンドウを構成するパケットの最大数

**Ns** 送信する次のパケットのシーケンス番号

**Nr** 受信する次のパケットのシーケンス番号

**Rx Q** 現在受信待ち行列にあるパケットの数

**Tx Q** 現在送信待ち行列にあるパケットの数

**state** すべてのトンネルの現在の状態を表示します。

例:

```
Layer-2-Tunneling Console> tunnel state
Tunnel ID | Type | Peer ID | State | Time Since Chg | # Calls | Flags
17404     | PPTP | 0       | Established | 00:00:00 | 1 | 0
96785     | L2TP | 0       | Established | 00:02:05 | 2 | 0
38237     | L2F  | 0       | Established | 00:00:00 | 1 | 0
```

### Tunnel ID

このコールに対応するローカル識別子

**Type** 使用されているトンネル・プロトコルのタイプ。

### Peer ID

このトンネルに割り当てられたピアのトンネル識別子

**State** 現在のトンネルの状態。有効なトンネル状態は、次のとおりです。

### Established

トンネルは確立されました。



## L2 トンネル監視コマンド (Talk 5)

**Idle** トンネルはアイドル状態です。

**Wait Ctrl Reply**

ホストはピアからの応答を待っています。

**Wait Ctrl Conn**

ホストはピアからの接続標識を待っています。

**Time since chg**

前回の状態変更からの経過時間

**# Calls**

このトンネル上の活動状態のコールの数

**Flags** このトンネル上の接続メッセージを制御するのに使用されたフラグ。

### statistics

トンネルに関連する統計を表示します。

例:

```
Layer-2-Tunneling Console> tunnel statistics
Tunnel ID | Type | Tx Pkts | Tx Bytes | Rx Pkts | Rx Bytes | RTT | ATO
96785     | L2TP | 4       | 78       | 5       | 89       | 10  | 31
96366     | L2F  | 9344    | 34578    | 305     | 4300     | 10  | 31
12344     | PPTP | 24      | 478      | 115     | 2745     | 10  | 31
```

**Tunnel ID**

このコールに対応するローカル識別子

**Type** 使用されているトンネル・プロトコルのタイプ。

**Tx Pkts**

送信されたパケット数

**Tx Bytes**

送信されたバイト数

**Rx Pkts**

受信されたパケット数

**Rx Bytes**

受信されたバイト数

**RTT** トンネル制御接続メッセージの現行の算定一巡時間

**ATO** トンネル制御接続メッセージの現行の算定適応タイムアウト

### transport

トンネルに関する UDP 情報を表示します。

例:

```
Layer-2-Tunneling Console> tunnel transport
Tunnel ID | Type | Peer IP Address | UDP Src | UDP Dest
96785     | L2TP | 11.0.0.102      | 1056    | 1089
30000     | L2F  | 11.0.0.104      | 1058    | 1090
45772     | PPTP | 11.4.4.027      | 1345    | 1020
```

**Tunnel ID**

このコールに対応するローカル識別子

**Type** 使用されているトンネル・プロトコルのタイプ。

**Peer IP address**

このトンネルのピアの IP アドレス

## L2 トンネル監視コマンド (Talk 5)

### UDP Src

このトンネルの UDP 発信元ポート

### UDP Dest

このトンネルの UDP あて先ポート

## 第26章 ネットワーク・アドレス変換の使用

ネットワーク・アドレス変換 (NAT) とその拡張機能であるネットワーク・アドレスおよびポート変換 (NAPT) は、組織の利用可能な IP アドレスの数を拡張することができ、公衆ネットワークのユーザーに私設ネットワークの一部のアドレスを知られるのを防止することができます。NAT では、公衆 IP アドレスを使用して私設 IP アドレスを表します。

公衆 IP アドレスとは、IP 公衆ネットワークのホストの有効なアドレスであり、公衆ネットワーク内で固有であることが必要です。公衆ネットワークがインターネットの場合、公衆 IP アドレスは、ネットワーク情報センター (NIC) によって提供される固有の IP アドレスでなければなりません。

私設アドレスはルーターには分かりますが、公衆ネットワークには分かりません。各私設ネットワーク内ではアドレスは固有であることが必要ですが、2 つの異なる私設ネットワークに同じアドレスが重複して存在しても構いません。私設アドレスは、スタブ・ネットワーク内のホストに割り当てられます。スタブ・ネットワークというのは、1 つのルーターだけを通して公衆ネットワークにアクセスできるネットワークのことです。

NAT は、いくつかの方法で、利用可能な IP アドレスを拡張します。

- 公衆アドレスを回転して使用することにより、1 つの公衆アドレスで複数の私設アドレスを表すことができる。
- アドレスの重複が可能である (重複アドレスがそれぞれ異なる私設ネットワークで使用されている場合に限られる)。
- ネットワーク管理者が、資源が限られてきている NIC アドレスの代わりに、任意の IP アドレスを私設ネットワークで使用することができる。

私設アドレスを使用すれば、アドレスを外界から隠すこともできます。NAT のこのフィチャーは、私設アドレスが知られるのを防止するための一種のファイアウォールとしての役目を果たします。

**重要:** NAT を定義しているインターネット草案のセクション 5.4 に、“アプリケーション内の IP アドレス (および、NAPT の場合は、TCP/UDP ポート) を持つ (および、使用する) アプリケーションは、NAT を通すと機能しない...” と記述されています。DLSw および XTP は、エンドポイント IP アドレスに基づいて (特に、どの相手がより高いアドレスを持っているかに基づいて) 決定を下すことに注意する必要があります。NAT を通して実行されているアプリケーション (DLSw や XTP など) は、そのアドレスは私設アドレスであると考えているのに対して、他のルーター内の相手のアプリケーションは、そのアプリケーションのアドレスは公衆アドレスであると考えてるので、間違った決定がなされる可能性があります。

430ページの図41 に示されているスタブ・ネットワーク内のワークステーションの図を見てください。この例では、スタブ・ネットワークは IP アドレスが 10.33.96.0、サブネット・マスクが 255.255.255.0 の IP サブネットから構成されています。

## ネットワーク・アドレス変換の使用

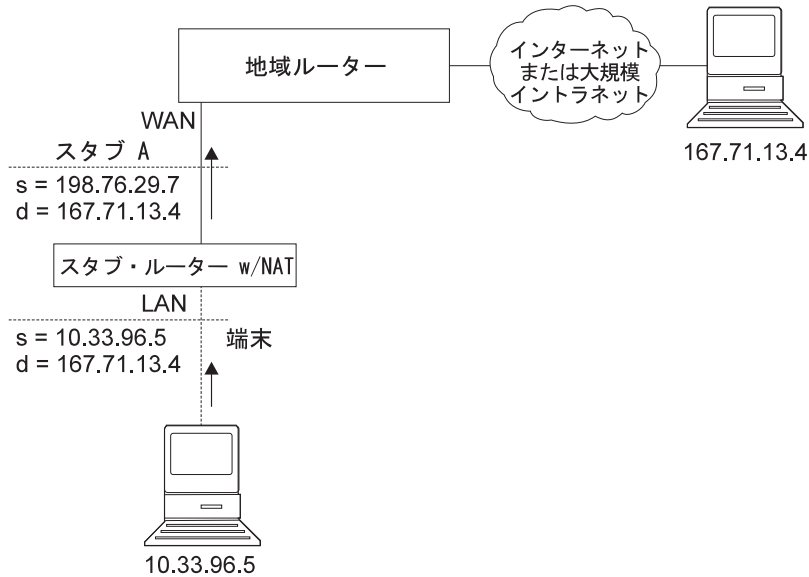


図 41. NAT を実行するネットワーク

NAT を使用するには、ネットワーク管理者は 1 つまたは複数の公衆 IP アドレスを 2212 内の公衆アドレス・プールに割り当て、私設 IP アドレスをスタブ・ネットワーク内の各ワークステーションに割り当てます。公衆 IP アドレスは *reserve pool* に割り当て、私設 IP アドレスは *translate range* に割り当てます。

NAT 機能は、最初に私設ネットワーク内のステーションの私設アドレスを公衆アドレスの 1 つに結合します。結合とは、その私設アドレスをもつパケットはすべて、パケットが発信されるたびに、その公衆 IP アドレスに変換されることを意味しています。インバウンド・パケットは、あて先として公衆 IP アドレスを持っています。NAT は公衆アドレスを認知し、それを私設 IP アドレスに変換して、パケットを転送します。トラフィックが停止した後、ユーザーが設定できるタイマーがタイムアウトになるまで、結合は維持されます。タイムアウトになった時点で、NAT は結合を終了し、その公衆アドレスを再利用できるようにします。

この例では、パケットは、発信元私設アドレス 10.33.96.5 からインターネット内のあて先アドレス 167.71.13.4 に転送されます。2212 内の NAT は、私設アドレス 10.33.96.5 を公衆アドレス 198.76.29.7 に変換します。この変換によって、私設アドレス 10.33.96.5 は公衆ネットワークから隠されるので、私設アドレス 10.33.96.5 を直接アドレス指定する着信パケットはありません。代わりに、167.71.13.4 からの着信パケットは公衆アドレス 198.76.29.7 あてに送られます。NAT ルーターは 198.76.29.7 をアドレス指定したパケットを受信すると、そのあて先公衆アドレスを私設アドレス 10.33.96.5 に変換し、パケットを転送します。

## ネットワーク・アドレス・ポート変換

NAPT は、TCP および UDP トラフィックにだけ使用できます。NAPT では、複数の私設アドレスが 1 つの公衆アドレスを同時に使用することができます。NAT は、1 つの公衆アドレスを 1 つの私設アドレスにマップするのに対して、NAPT は、NAPT 公衆アドレスおよび 公衆ポート番号を、私設アドレスおよび私設ポート番号にマップします。各公衆アドレス・プールにつき 1 つの NAPT アドレスしか構成できません。

NAPT の構成は、NAPT トラフィックに使用する 1 つの公衆アドレスまたは動的アドレス・インターフェース (PPP/PCP を使用して公衆アドレスを検索する) を指定するだけで済みます。NAPT の利点は、公衆 IP アドレス・プールからの 1 つのアドレスが、複数の私設 IP アドレスを同時にサポートできることです。

## 静的アドレス・マッピング

ときには、公衆ネットワークから直接アクセスできるステーションまたはサーバーを私設ネットワーク内に構成したい場合があります。その場合は、ステーションの私設アドレスを特定の公衆アドレスに静的にマッピングする必要があります。私設アドレスから発信されるすべてのメッセージは、あて先の公衆アドレスに変換され、公衆アドレスあてのインバウンド・メッセージはすべて、対応する私設アドレスに自動的に転送されます。静的アドレス・マッピングには、NAT と NAPT の 2 種類があります。

### NAT 静的アドレス・マッピング

NAT マッピングでは、すべての IP プロトコルがホストにアクセスできます。次に示すのは、NAT マッピングの構成例です。

私設アドレス	10.1.1.2
私設ポート	0
公衆 NAT アドレス	9.67.1.1
公衆ポート	0

### NAPT 静的アドレス・マッピング

TCP または UDP アプリケーションを指定する場合、事前割り当てされた私設ポートを組み込んだ NAPT マッピングを指定するオプションがあります。NAPT 静的アドレス・マッピングでは、NAPT 公衆アドレスを構成する必要があります。たとえば、私設アドレス 10.1.1.1 の Telnet ホストが NAPT 公衆アドレス 9.67.1.2 を使用するように構成する場合、静的マッピングは次のように構成します。

私設アドレス	10.1.1.1
私設ポート	23
公衆 NAPT アドレス	9.67.1.2
公衆ポート	23

私設ポートと公衆ポートは、Telnet 用に事前割り当てされたポートであるポート 23 にマップされます。この管理者は、同じ私設アドレス 10.1.1.1 に FTP サーバー (事前

## ネットワーク・アドレス変換の使用

割り当てアドレス 21) も持っており、これを NAPT 公衆アドレス 9.67.1.2 にマップする場合、このマッピングは次のようになります。

私設アドレス	10.1.1.1
私設ポート	21
公衆 NAPT アドレス	9.67.1.2
公衆ポート	21

アドレス 10.1.1.1 のサーバーは、両方のアプリケーションに同じ NAPT 公衆アドレス (9.67.1.2) を使用していますが、NAPT は異なるポート番号 (23 と 21) を使用することによって、この 2 つを区別することができます。しかし NAPT は、2 つのサーバーが同じ NAPT 公衆アドレスを使用し、同じアプリケーションおよびポート番号を持っている場合は、それらを区別することはできません。たとえば、NAPT 公衆アドレスと事前割り当てポート番号が、10.1.1.3 ポート 21 と 10.1.1.1 ポート 21 で同じである場合、NAPT は着信 FTP トラフィックをサーバー 10.1.1.3 と 10.1.1.1 のどちらに送るのか判断できません。同じ NAPT アドレスとアプリケーションを使用するサーバーを複数構成する場合は、サーバーの事前割り当てポート以外のポートを使用する必要があります (たとえば、FTP デーモンをポート 200 で開始するなど)。

---

## NAT 用のパケット・フィルターおよびアクセス制御規則の設定

管理者は、NAT または NAPT によって変換される私設アドレスの範囲を識別するのに加えて、2212 内の IP 用のパケット・フィルターとアクセス制御規則も設定する必要があります。NAT 構成では、公衆ネットワークに接続されているインターフェースに、1 つのインバウンド・パケット・フィルターと 1 つのアウトバウンド・パケット・フィルターを構成することが必要です。インバウンド・パケット・フィルターに対して 1 つまたは複数のアクセス制御規則を構成し、アウトバウンド・パケット・フィルターに対しても 1 つまたは複数のアクセス制御規則を構成することも必要です。インバウンド・フィルター・アクセス制御規則は、該当する定義済み公衆アドレスをもつインバウンド・パケットを NAT にパスします。アウトバウンド・フィルター・アクセス制御規則は、該当する定義済み私設アドレスをもつアウトバウンド・パケットを NAT にパスします。

NAT に適用されるアクセス制御規則は、アクセス制御規則タイプ **I** (包括的) および **N** (NAT) を持っています。IP アクセス制御の構成については、[プロトコルの構成と監視 解説書、第 1 巻](#) を参照してください。

**注:** NAT は、IPsec トンネルと合わせて構成することもできます。この構成の例は、370ページの『[ルーター A のパケット・フィルター・アクセス制御規則の構成](#)』にあります。

### 例: IP フィルターとアクセス制御規則をもつ NAT の構成

この例は、433ページの図42 に示したネットワーク内のスタブ・ルーターの NAT を構成する方法を示しています。コマンドの説明は、437ページの『[第27章 ネットワーク・アドレス変換の構成および監視](#)』を参照してください。

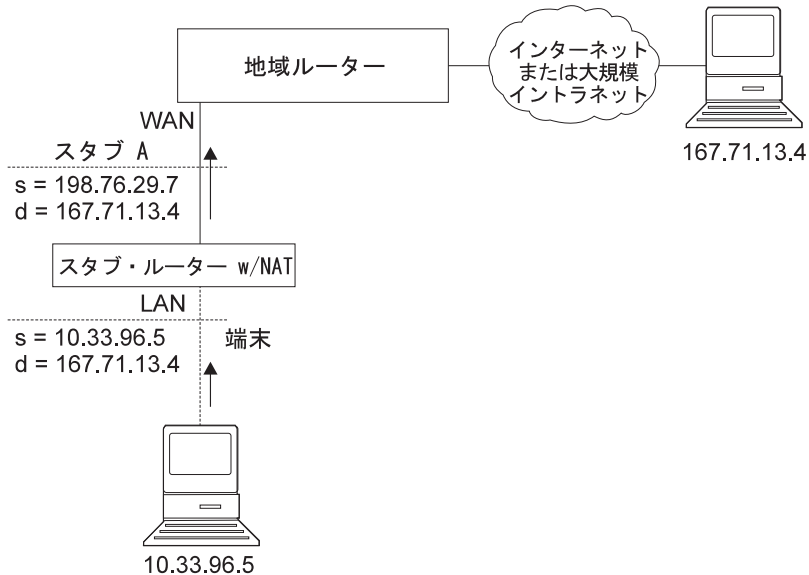


図 42. NAT を実行するネットワーク

次の手順で行います。

1. NAT および NAPT によって使用される公衆アドレスのプールを設定します。これには **reserve** コマンドを使用します。

```
NAT config> reserve No 198.76.29.7 255.255.255.0 6 pool1 198.76.29.7
NAT config> reserve No 198.76.29.15 255.255.255.0 3 pool1 0.0.0.0
```

この例では、*pool1* と呼ばれるプールが設定されました。プール内の NAPT アドレスは 198.76.29.7 です。アドレス 198.76.29.13 および 198.76.29.14 は利用不能なので、プールはそれら除外するように設定されています。入力するパラメーターは *public-address*、*mask*、*number-in-group*、*name*、および *napt-address* です。NAPT アドレスの値 0.0.0.0 は、このグループ内のアドレスはどれも NAPT アドレスではないことを意味しています。プールに NAPT を構成しない場合は、すべてのグループに NAPT アドレス 0.0.0.0 を使用します。

2. **translate** コマンドを使用して、*pool1* 内の公衆アドレスに変換される私設アドレスの範囲を設定します。入力するパラメーターは、*private-address*、*mask*、および *name* です。

```
NAT config> translate 10.33.96.0 255.255.255.0 pool1
```

3. 公衆アドレスの 1 つに固定的にマップする、私設ネットワーク内部のステーションの静的マッピングを設定します。次のコマンドは、公衆ネットワークから任意のタイプのトラフィックを受信するマシン (10.33.96.5) を識別します。2 番目のマシン (10.33.96.4) は、Telnet サーバーと HTTP サーバーの両方の役目を果たします。パラメーターは、*private-address*、*private-port-number*、*public-address*、および *public-port-number* です。*pool1* の NAPT アドレスは、2 つのポート番号を持つように構成されているホストの公衆アドレスとして使用されていることに注意してください。

```
NAT config> map 10.33.96.5 0 198.76.29.8 0
NAT config> map 10.33.96.4 23 198.76.29.7 23
NAT config> map 10.33.96.4 80 198.76.29.7 80
```

4. NAT を使用可能にします。

```
NAT config> enable NAT
```



## ネットワーク・アドレス変換の使用

- 2つのIPパケット・フィルタを作成して、IPがパケットをNATにパスするようにします。これらは、インターフェース0（公衆ネットワークに接続されているインターフェース）のインバウンド・パケット・フィルタとアウトバウンド・パケット・フィルタです。

```
IP Config> add packet-filter outbound out-0 0
IP Config> add packet-filter inbound in-0 0
```

- update** コマンドを使用して、packet-filter '*filter-name*' Config> プロンプトを表示します。NAT用のアクセス制御規則をインバウンド・フィルタに追加します。公衆インターフェース（ネット0）を介して受信したNATの予約済み公衆アドレス・プールあてのパケットを、NATにパスする必要があります。NATは公衆アドレス（および、パケットがNAPTアドレスあての場合は、公衆ポート）を正しい私設アドレス（および、パケットがNAPTアドレスあての場合は、私設ポート）で置き換えます。インターネット発信元の0.0.0.0のアドレスとマスクは、公衆ネットワークからのすべての発信元アドレスをNATにパスすることを示しています。

```
IP Config> update packet-filter
Packet-filter name [ ]? in-0
Packet-filter 'in-0' Config> add access
Enter type [E]? IN
Internet source [0.0.0.0]?
Source mask [255.255.255.255]? 0.0.0.0
Internet destination [0.0.0.0]? 198.76.29.0
Destination mask [255.255.255.255]?255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'in-0' Config>
```

アクセス制御規則の範囲は、pool1に定義されたアドレスの範囲より大きくなっています。NATにパスされたパケットのアドレスが、アクセス制御規則に定義された範囲内であるが、公衆アドレス・プール内のアドレスの1つではない場合、NATはそのパケットを変更せずにIPに戻します。

- ルーターが、アクセス制御規則に一致しないパケットをドロップせずにパスするようにしたい場合は、ワイルドカード・アクセス制御規則を作成することができます。次の例は、このようなアクセス制御規則を示しています。

```
Packet-filter 'in-0' Config> add access
Enter type [E]? I
Internet source [0.0.0.0]? 0.0.0.0
Source mask [255.255.255.255]? 0.0.0.0
Internet destination [0.0.0.0]? 0.0.0.0
Destination mask [255.255.255.255]?0.0.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'in-0' Config>
```

- NAT用のアクセス制御規則をアウトバウンド・パケット・フィルタに追加します。ネット0インターフェースから転送された私設ネットワーク上の発信元アドレスを持っているパケットを識別し、IPがそれらをNATにパスできるようにします。NATは私設アドレスをpool1内の公衆アドレスの1つで置き換えます。

```
Packet-filter 'out-0' Config> add access
Enter type [E]? IN
Internet source [0.0.0.0]? 10.33.96.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]?
Destination mask [255.255.255.255]?0.0.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'out-0' Config>
```



## ネットワーク・アドレス変換の使用

アクセス制御規則に一致しないパケットを転送する計画の場合は、フィルター *in-0* の場合と同様に、このパケット・フィルターを使用して、ワイルドカード包括的アクセス制御規則を最後のアクセス制御規則として追加することができます。

9. IP Config> プロンプトから **list packet-filter filter-name** コマンドを使用して、各パケット・フィルターのアクセス制御規則の正確性とシーケンスを検査できます。
10. IP 用のアクセス制御を使用可能にします。

```
IP Config> set access-control on
```

11. **talk 5** を使用して、IP および NAT をリセットします。ここまでは、ルーター構成の変更を作成してきましたが、これらの変更はルーターには影響を与えていません。IP および NAT の **reset** コマンドにより、ルーターは新規構成を読み取り、構成に定義された規則を使用して稼働するようになります。

```
NAT> reset NAT  
IP> reset IP
```

## ネットワーク・アドレス変換の使用

## 第27章 ネットワーク・アドレス変換の構成および監視

この章では、ネットワーク・アドレス変換 (NAT) 構成コマンドおよび監視コマンドについて説明し、次の内容が記載されています。

- 『ネットワーク・アドレス変換の構成環境へのアクセス』
- 『ネットワーク・アドレス変換構成コマンド』
- 444ページの『ネットワーク・アドレス変換監視環境へのアクセス』
- 445ページの『ネットワーク・アドレス変換監視コマンド』

### ネットワーク・アドレス変換の構成環境へのアクセス

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

```
Config> feature nat
Network Address Protocol user configuration
NAT config>
```

### ネットワーク・アドレス変換構成コマンド

ここでは、ネットワーク・アドレス変換 (NAT) 構成コマンドについて説明します。NAT を構成するには、これらのコマンドを NAT config> プロンプトで入力します。

表 52. NAT 構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxiiページの『ヘルプの入手』を参照してください。
Change	公衆 IP アドレス予約プール、私設アドレス変換範囲、および静的マッピングを変更します。
Delete	公衆 IP アドレス予約プール、私設アドレス変換範囲、および静的マッピングを削除します。
Disable	NAT を使用不可にします。
Enable	NAT を使用可能にします。
List	NAT 構成に関する情報を表示します。
Map	ステーションまたはサーバーの静的 NAT または NAPT 結合を作成します。
Reserve	公衆 IP アドレス・プールを作成し、そのプールにアドレスを追加します。
Reset	ルーターが NAT 構成を読み込み、構成された NAT 規則に従って稼働するようにします。
Set	タイムアウトを設定します。
Translate	NAT 公衆アドレス・プールによって変換される私設 IP アドレスを識別します。
Exit	直前のコマンド・レベルに戻ります。 xxxiiページの『下位レベル操作環境の終了』を参照してください。

## ネットワーク・アドレス変換の構成 (Talk 6)

### Change

**change** コマンドは、公衆 IP アドレス予約プール、私設 IP アドレス変換範囲、および静的マッピングを変更するのに使用します。

構文:

```
change                reserve
                        translate
                        mappings
```

#### **reserve** *pools*

公衆 IP アドレス予約プールの特性 (IP アドレスおよびマスクなど) を変更することができるプロンプトを表示します。

**有効値:** 構成されたプールを識別するインデックス番号。この番号は **list reserve pools** コマンドを入力すると表示されます。

**デフォルト値:** なし

#### **translate** *ranges*

私設 IP アドレス変換範囲の特性 (IP アドレスおよびマスクなど) を変更することができるプロンプトを表示します。

**有効値:** 構成された変換範囲を識別するインデックス番号。この番号は **list translate** コマンドを入力すると表示されます。

**デフォルト値:** なし

#### **mappings**

静的アドレス・マッピングの特性 (IP アドレスおよびポートなど) を変更することができるプロンプトを表示します。

**有効値:** 構成されたマッピングを識別するインデックス番号。この番号は **list mappings** コマンドを入力すると表示されます。

**デフォルト値:** なし

### Delete

**delete** コマンドは、公衆 IP アドレス予約プール、私設 IP アドレス変換範囲、およびマッピングを削除するのに使用します。

構文:

```
delete                reserve
                        translate
                        mappings
```

#### **reserve** *pools*

公衆 IP アドレス予約プールを削除することができるプロンプトを表示します。

**有効値:** 構成されたプールを識別するインデックス番号。この番号は **list reserve pools** コマンドを入力すると表示されます。

デフォルト値: なし

#### **translate** *ranges*

私設 IP アドレス変換範囲を削除することができるプロンプトを表示します。

**有効値:** 構成された変換範囲を識別するインデックス番号。この番号は **list translate** コマンドを入力すると表示されます。

デフォルト値: なし

#### **mappings**

静的アドレス・マッピングを削除することができるプロンプトを表示します。

**有効値:** 構成されたマッピングを識別するインデックス番号。この番号は **list mappings** コマンドを入力すると表示されます。

デフォルト値: なし

## Disable

**disable** コマンドは、NAT を使用不可にするのに使用します。変換を必要とするパケットをドロップさせて NAT を使用不可にすることも、変換を必要とするパケットをパスさせて NAT を使用不可にすることもできます。

構文:

**disable** n**at**

d**rop**

p**ass**

**drop** 変換を必要とするパケットをドロップさせて NAT を使用不可にします。

**pass** 変換を必要とするパケットをパスさせて NAT を使用不可にします。

## Enable

**enable** コマンドは、NAT を使用可能にするのに使用できます。NAT を使用可能にすると、実行の準備が整いますが、**reset** コマンドを使用するか、ルーターをリスタートするまでは実行されません。

構文:

**enable** n**at**

## List

**list** コマンドは、公衆 IP アドレス予約プール、私設 IP アドレス変換範囲、マッピング、グローバル設定値、またはすべての NAT 情報をリストするのに使用します。

構文:

**list**

r**eserve**

a**ddresses**

p**ools**

## ネットワーク・アドレス変換の構成 (Talk 6)

translate  
mappings  
global  
all

次の例では、時間は、時、分、および秒で表示されます。エントリー経過時間は、そのエントリーが最後に使用されてから経過した時間です。結合は、これらの 2 つのアドレス間をトラフィックが流れることを意味しています。タイムアウトは、結合をドロップする前の、最後の通信後に経過する時間を決めます。タイムアウトについて詳しくは、**set** コマンドの項を参照してください。

### 例:

```
NAT config>list all
NAT Globals:
NAT is ENABLED
Tcp Timeout....: 24:00:00
Non-Tcp Timeout: 0:01:00
NAT Reserved Address Pool(s):
Index First Address Mask Count NAPT Address Pool Name
1 9.8.7.1 255.255.255.0 3 0.0.0.0 pool1
2 9.8.7.6 255.255.255.0 12 9.8.7.9 pool1
NAT Translate Range(s):
Index IP Address IP Mask Associated Pool Name
1 7.1.1.0 255.255.255.0 pool1
2 10.0.0.0 255.0.0.0 pool1
NAT Static Mapping(s):
Index Private Address:Port Public Address.:Port
1 10.1.2.3 0 9.8.7.1 0
2 7.1.1.1 21 9.8.7.9 21
```

## Map

**map** コマンドは、私設ネットワーク内のホストまたはサーバーを公衆アドレスに静的に結合するのに使用します。このコマンドは、私設ネットワークのサーバーを設定するのに使用することができ、NAT の始動時のアソシエーションを確立します (これは、決して変更されることはありません)。

公衆および私設ポート番号 0 をもつ静的マッピングは NAT マッピングです。ポート番号に他の値をもつ静的マッピングは NAPT マッピングです。

### 構文:

```
map private-address private-port-number public-address  
public-port-number
```

### private-address

ワークステーションの私設アドレス。

**有効値:** 有効な IP フォーマットのインターネット・ホスト・アドレス。これは、公衆ネットワークから永続的にアクセスする必要があるスタブ・ネットワーク内のステーション (サーバーなど) に割り当てられたアドレスでなければなりません。

**デフォルト値:** なし

### private-port-number

私設アドレスをもつ装置で実行されているアプリケーションの TCP/UDP ポ

## ネットワーク・アドレス変換の構成 (Talk 6)

ート番号。0 を入力すると NAT 結合が作成され、それ以外の値を入力すると NAPT 結合が作成されます。NAPT の一般的なポート値は、Telnet は 23、FTP は 21、HTTP は 80 です。

有効値: 0 ~ 65535

デフォルト値: 0

### public-address

この私設アドレスがマップされる公衆 IP アドレス。これは、NAPT マッピングの場合は NAPT アドレス、NAT マッピングの場合は NAT アドレスでなければなりません。

有効値: 公衆ネットワークに固有の有効な IP アドレス。公衆ネットワークは、ネットワークの設計に応じて、インターネットまたはイントラネットが可能です。

デフォルト値: なし

### public-port-number

公衆アドレスで変換されるパケットのポート番号。値 0 は、すべてのポートを表します。一般的な値は、Telnet は 23、FTP は 21、HTTP は 80 です。

有効値: 0 ~ 65535

デフォルト値: 0

この例では、私設 IP アドレス 10.11.12.200 をもつサーバーは、インターネットからのすべてのトラフィックを受け入れます。私設アドレス 10.11.12.199 をもつサーバーは、Telnet サーバーおよび FTP サーバーです。

例:

```
map 10.11.12.200 0 9.8.7.2 0
map 10.11.12.199 23 9.8.7.9 23
map 10.11.12.199 21 9.8.7.9 21
```

## Reserve

**reserve** コマンドは、一定範囲の IP アドレスを作成し、公衆アドレス・プールに追加するのに使用します。公衆アドレス・プールに動的 IP アドレスを追加するためにも使用できます。

構文:

**reserve**

*dynamic*

*[interface][public-address][mask][number-in-group] name  
[napt-address]*

注: 大括弧の中に示されている値は、現在はオプションで表示されます。

- **Dynamic** - このエントリが、公衆アドレスのグループに対するものであるか、または IPCP を使用する PPP 接続から IP アドレスを検索する動的アドレス・インターフェースに対するものであるかを指定します。有効値は *yes* または *no* です。デフ

## ネットワーク・アドレス変換の構成 (Talk 6)

ォルトは *no* です。Dynamic=*yes* の場合は、指定する必要があるのはインターフェースと名前だけです。Dynamic=*no* の場合は、インターフェースは指定しませんが、その他の値をすべて指定する必要があります。

- Interface - IP 内で構成された動的アドレス・インターフェースを指定します。任意の有効インターフェース番号を指定できます。デフォルトはゼロです。

### public-address

プール内のこの範囲またはグループを構成する一連のアドレスの最初の公衆 IP アドレス。たとえば、プール内のこのグループに 9.8.7.6 ~ 9.8.7.17 の一連の 12 個のアドレスが含まれている場合、この値は 9.8.7.6 になります。

注: 別の範囲のアドレスを公衆アドレス・プールに追加するには、各グループごとに別々に **reserve** コマンドを使用し、同じプール名を使用して各グループを対応付けます。たとえば、9.8.7.6 ~ 9.8.7.17 のアドレスを pool1 内の 1 つのグループとして構成し、アドレス 9.8.7.1 ~ 9.8.7.3 を同じプール内の別のグループとして構成するといったことが可能です。この場合、アドレス 9.8.7.4 と 9.8.7.5 は構成されず、そのプールでは使用されません。

有効値: 公衆ネットワークに固有の有効な IP アドレス。

デフォルト値: なし

**mask** IP アドレスからビットを選択するマスク。このマスクは、IP アドレスと同様に、32 ビットの長さです。マスク内の 1 は、アドレスのネットワークまたはサブネット部分を選択します。0 はホスト部分を選択します。たとえば、アドレスが 9.8.7.6 でマスクが 255.255.0.0 の場合は、最初の 2 バイトが 9.8 であるすべてのアドレス範囲 (つまり、9.8.0.0 ~ 9.8.255.255) が含まれます。

有効値: 任意の有効な IP マスク

デフォルト値: なし

### number-in-group

グループ内に *public-address* から始まる順次アドレスがいくつ含まれるかを指定します。アドレス 9.8.7.6 ~ 9.8.7.17 の場合、この値は 12 です。

有効値: 1 ~ IP マスクによって定義できる値

デフォルト値: なし

**name** 公衆アドレス予約プールの名前。この文字列は、対応する **translate** コマンドのプール名と一致している必要があります。

有効値: 最大 16 字の印刷可能文字を使用した任意の名前。先頭と末尾のブランクは無視されます。

デフォルト値: なし

### napt-address

ネットワーク・アドレス・ポート変換 (NAPT) によって使用される公衆アドレス・プールからの 1 つの IP アドレス。このアドレスは、TCP および UDP トラフィックで、プロトコル・ポート番号に従って複数の私設アドレスを 1



## ネットワーク・アドレス変換の構成 (Talk 6)

つの NAPT アドレスにマップするのに使用されます。NAPT の使用はオプションです。これを使用する場合、1 つの公衆アドレス・プールには 1 つの NAPT アドレスしか入れることができません。プールまたはグループに NAPT アドレスが存在しない場合は、値 **0.0.0.0** を入力します。NAPT アドレスは 1 回だけプールに入力すれば済みます。

**有効値:** 公衆 IP アドレスの 1 つ。必ずしも公衆アドレス・プールに定義された値の範囲に含まれている必要はありませんが、同じサブネット内に存在する必要があります。

**デフォルト値:** 0.0.0.0 (NAPT がないことを意味します)

例:

```
reserve no 9.8.7.1 255.255.255.0 3 pool1 0.0.0.0
reserve no 9.8.7.6 255.255.255.0 12 pool1 9.8.7.9
reserve yes 2 dynamic_ip_pool
```

## Reset

**reset** コマンドは、NAT をリセットするのに使用します。このコマンドは、すべての結合を削除し、NAT が使用しているすべてのメモリーを解放し、現行の Talk 6 構成に基づいて NAT をリスタートします。NAT をリセットしても、2212 の他のコンポーネントを中断させることはありません。

**構文:**

**reset nat**

NAT が無効な構成を検出すると、それを知らせるメッセージを出します。NAT ELS メッセージを検討して、NAT 初期設定に失敗した理由を調べてください。

## Set

**set** コマンドは、TCP および非 TCP タイムアウトを設定するのに使用します。

**構文:**

**set** **tcp**  
**nontcp**

**tcp timeout**

2 つの結合されたワークステーション間で最後のメッセージをパスした後、NAT が TCP 結合を保持する時間。結合とは、私設アドレスと公衆 IP アドレスの 1 つとの間の関係を保持することです。

**有効値:** 0 ~ 65535 分 (0 分 ~ 約 45 日間)

**デフォルト値:** 1440 分 (24 時間)

**nontcp timeout**

2 つの結合されたワークステーション間で最後のメッセージをパスした後、NAT が非 TCP 結合を保持する時間。結合とは、私設アドレスと公衆 IP アドレスの 1 つとの間の関係を保持することです。

**有効値:** 0 ~ 65535 分 (0 分 ~ 約 45 日間)

## ネットワーク・アドレス変換の構成 (Talk 6)

デフォルト値: 1 分

### Translate

**translate** コマンドは、NAT が変換するアドレスのリストにサブネットを追加するのに使用します。各サブネットは、1 つの変換範囲です。NAT が知っている必要がある各変換範囲ごとに、このコマンドを 1 回入力する必要があります。任意の個数の変換範囲が、1 つの公衆アドレス予約プールを使用できます。

構文:

```
translate private-address mask name
```

#### **private-address**

変換する必要がある IP ホストまたはサブネットのアドレス。

**有効値:** 有効な小数点付き 10 進数の IP フォーマットのアドレス。サブネット・マスクと AND すると、このアドレスはスタブ・サブネット内のすべてのアドレスを識別します。スタブ・サブネットとは、そのルーターを介してだけ公衆ネットワークにアクセスするネットワークのことです。

**デフォルト値:** なし

**mask** **有効値:** 変換するスタブ・ネットワークに対応したネットワーク・マスクまたはサブネット・マスク

**デフォルト値:** 私設アドレスのクラス・マスク

**name** この範囲の私設アドレスのために NAT が使用する必要がある公衆アドレス・プールの名前

**有効値:** 最大 16 字の印刷可能文字を使用した任意の名前。これは **reserve** コマンドによって作成された公衆アドレス・プール名と一致していることが必要です。

**デフォルト値:** なし

---

## ネットワーク・アドレス変換監視環境へのアクセス

NAT 監視環境にアクセスするには、次のように入力します。

```
* t 5
```

次に、+ プロンプトで、次のコマンドを入力します。

```
+ feature NAT  
NAT>
```

NAT> プロンプトが表示されます。

## ネットワーク・アドレス変換監視コマンド

ここでは、IP セキュリティー監視コマンドについて説明します。次のコマンドは NAT> プロンプトで入力します。

表 53. NAT 監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxii ページの『ヘルプの入手』を参照してください。
List	NAT に関する情報を表示します。
Reset	ルーターが NAT 構成を読み込み、構成された NAT アクセス規則に従って稼働するようにします。 <b>reset NAT</b> コマンドを入力するまでは、NAT はルーターの稼働に影響を与えません。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

### List

**list** コマンドは、NAT 構成に関する情報を表示するのに使用します。

構文:

```
list
    all
    binding
    fragment
    global
    reserve
    pools
    addresses
    statistics
    translate
```

次の例では、時間は、時、分、および秒で表示されます。エントリー経過時間は、そのエントリーが最後に使用されてから経過した時間です。結合は、これらの 2 つのアドレス間にセッションが確立されることを意味しています。タイムアウトは、結合をドロップする前の、最後の通信後に経過する時間を決めます。タイムアウトについて詳しくは、Talk 6 の **set** コマンドの項を参照してください。

例:

```
NAT>list all
NAT Globals:
Current State   Tcp Timeout   Non-Tcp Timeout   Memory Usage (in bytes)
ENABLED        24:00:00      0:01:00           408

NAT Statistics:
Requests :    Passes    Drops    Holds
0 :         0         0         0

NAT Address Binding(s):
Private Address//Port   Public Address//Port   Bind Type   Entry Age
7.1.1.1    21    9.1.1.1    21    STATIC    0:00:13
```

## ネットワーク・アドレス変換の監視

```
10.1.2.3    0      9.1.1.2    0  STATIC    0:00:13

NAT TCP Session Information:
Private Address//Port  Public Address//Port  Tcp State  Data Delta  Entry Age
7.1.1.1    21      9.1.1.1    21  ESTAB'ED   0      0:00:56

NAT Translate Range(s):
Base Ip Address      Range Mask      Associated Reserve Pool
7.1.1.0             255.255.255.0  carol
10.0.0.0            255.0.0.0      carol

NAT Reserve Pool(s):
Reserve Pool      Pool Size      NAPT Address    1st Available Address
carol             21             9.1.1.1         9.1.1.12
-----
Number of Reserve Pools using NAPT.....: 1
Number of configured Reserved Addresses: 21

NAT Fragment Information:
Number of Entries      Number of Saved Fragments
0                      0
```

## Reset

**reset** コマンドは、NAT をリセットするのに使用します。このコマンドは、すべての結合を削除し、NAT が使用しているすべてのメモリーを解放し、現行の Talk 6 構成に基づいて NAT をリスタートします。NAT をリセットしても、2212 の他のコンポーネントを中断させることはありません。

構文:

**reset nat**

---

## 第28章 LAN へのダイヤルイン・アクセス (DIALs) サーバーの使用

DIALs サーバーを使用すると、リモート・ユーザーが LAN にダイヤルインし、LAN アダプターによってローカル接続されている場合と同じ方法で LAN の資源にアクセスすることが可能になります。同様に、DIALs サーバーを使用すると、LAN に接続されたユーザーがダイヤルアウトして WAN の資源 (電子掲示板、FAX 装置、インターネット・サービス提供者 (ISP)、およびその他のオンライン・サービス) にアクセスすることも可能になり、ワークステーション上にアナログ電話回線とモデムを装備する必要がなくなります。

DIALs サーバーは、同時にダイヤルイン・ユーザーとダイヤルアウト・ユーザーの両方として構成することができます。IBM DIALs ダイヤルイン・クライアントは、リモート・ワークステーション上で稼働し、ダイヤルイン機能を提供します。448ページの図43 は、ダイヤルイン機能をサポートする DIALs サーバーとして使用される装置の例を示しています。

## DIALs の使用

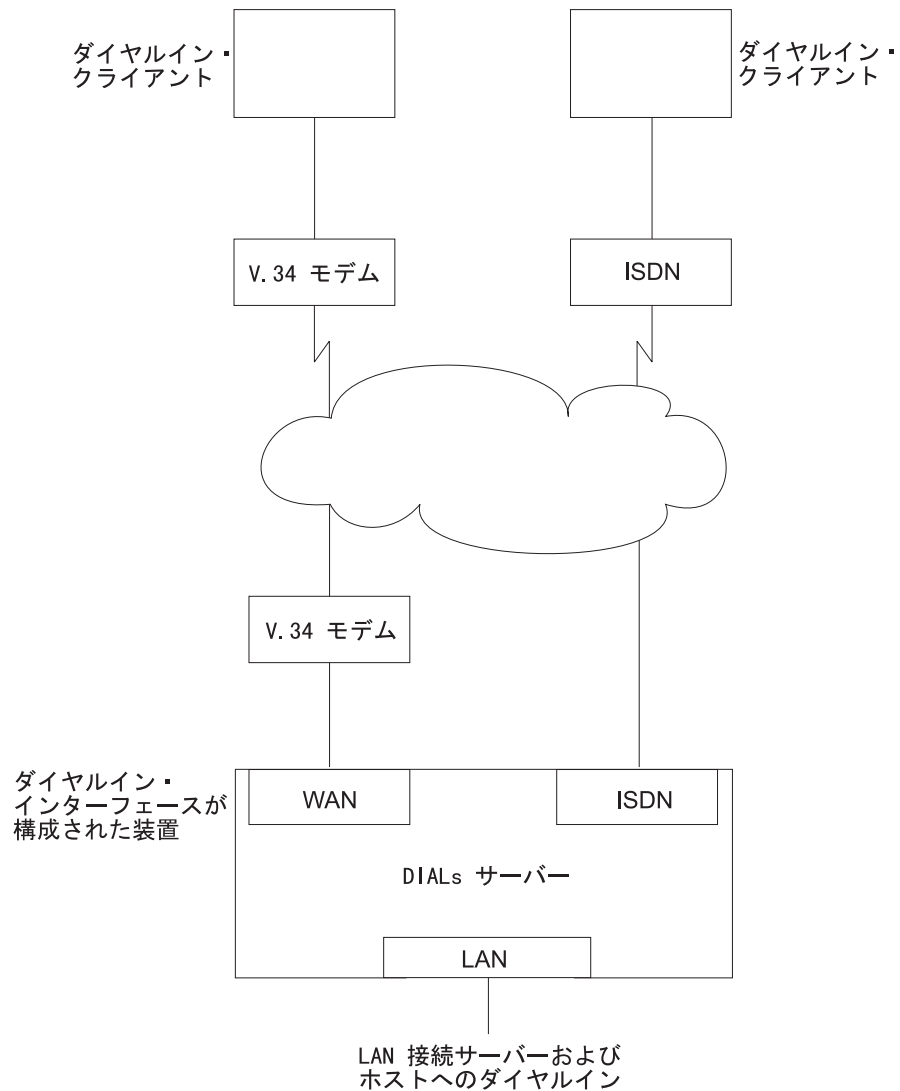


図43. ダイヤルインをサポートする DIALs サーバーの例

IBM DIALs ダイヤルアウト・クライアントは、ネットワークに接続されたワークステーション上で稼働し、ダイヤルアウト機能を提供します。449ページの図44 は、ダイヤルアウト機能をサポートする DIALs サーバーとして使用されている 2212 の例を示しています。

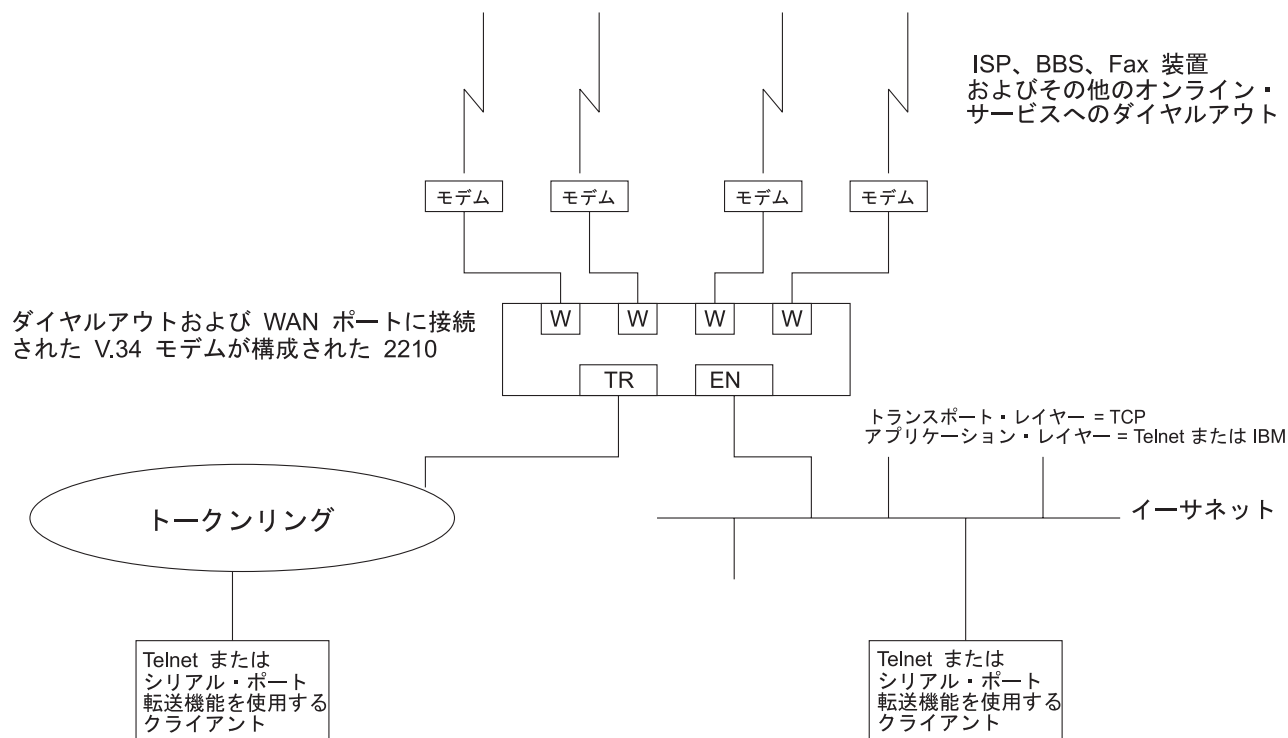


図 44. ダイヤルアウトをサポートする DIALs サーバーの例

## ダイヤルイン・アクセスを使用する前に

ダイヤルイン・アクセスを使用する前に、次の要件を満たしていることが必要です。

- ワークステーションで、IBM DIALs ダイヤルイン・クライアントまたは別の PPP ダイヤルイン・クライアント (以降では、**ダイヤルイン・クライアント** または **PPP ダイヤルイン・クライアント** と呼びます) が稼働している。
- クライアント・マシンのプロトコル構成が完了している。
- 単一ユーザー・ダイヤルインに使用する 2212 の WAN ポートに、ISDN および ISDN/デジタル・モデム・インターフェース、内蔵モデム・インターフェース、ヌル・モデム・インターフェース、または外付け V.34 モデムが接続されている。
- LAN に DIALs サーバーが完全に構成されている。

## ダイヤルイン・アクセスの構成

ここでは、DIALs サーバー上のダイヤルイン機能とダイヤルアウト機能両方を構成する方法について説明します。ダイヤルイン・アクセスを使用するためのクライアントの構成方法は、ワークステーションが使用するクライアントに付いている資料に記載されています。

## ダイヤルイン・インターフェースの構成

2212 上のダイヤルイン・インターフェースは、ダイヤル回線の特殊なタイプです。通常のダイヤル回線の設定値のほとんどは、単一ユーザー・ダイヤルイン・アプリケ

ーションには該当しないので、**ダイヤルイン** という名前の新しい装置タイプを追加して、このダイヤル回線用の適切なデフォルト値を設定することができます。ダイヤルイン装置を追加すると、IBM DIALs ダイヤルイン・クライアントを含めた大多数の PPP ダイヤルイン・クライアントに適用できる PPP カプセル化機能構成のデフォルト値も設定されます。これらのデフォルト値については、『ダイヤルイン・インターフェースのダイヤル回線パラメーターのデフォルト値』、および 451 ページの『ダイヤルイン回線のダイヤル回線 PPP カプセル化機能パラメーター』で説明します。

注: DIALs 機能は、ダイヤルイン回線でしか使用可能にできません。ダイヤルイン回線は、基本ネットが V.34、ISDN、および ISDN/デジタル・モデムの場合にだけサポートされます。

### ダイヤルイン・インターフェースのダイヤル回線パラメーターのデフォルト値

注:

1. ここで説明するパラメーターは、オーバーライドしてはなりません。オーバーライドすると、ダイヤルイン機能が正しく動作しなくなります。
2. 一部のパラメーターは、表示されなかったり、構成できない場合があります。パラメーターについての詳しい説明は、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの『ダイヤル回線の構成および監視』の章を参照してください。

ダイヤルイン・インターフェースを追加すると、次のデフォルト値が設定されます。

- **Idle time** は 0 に設定されます。標準回線は、アイドル・タイマーが意味をもたない回線として定義されていることに注意してください。これは、自動的にダイヤルアウトする固定回線ではありません。この回線がダイヤルアウトするのは、PPP コールバックがネゴシエーションされた場合、あるいはこの回線でマルチリンク PPP が使用可能にされている場合だけです。アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの『Shiva パスワード認証プロトコル (SPAP)』および『マルチリンク PPP プロトコルの使用』の項を参照してください。
- **Inbound calls** は可能です。PPP ダイヤルイン・クライアントは Nways ダイヤル回線によって実現された LID 交換を使用しないので、任意の着信を設定することができます。
- **Outbound calls** は可能です。

注: ダイヤルイン回線の『アウトバウンド』は、ダイヤルアウト回線と同じではありません。452 ページの『ダイヤルアウト・インターフェースを構成する前に』を参照してください。

- 『default\_address』に対してデフォルトのあて先アドレスが設定されます。このアドレスは、V.34 アドレスのリストに追加されます。これらのコールはインバウンドであり、アウトバウンドはコールバックまたはマルチリンク PPP 交換の結果だけになるので、あて先アドレスは無意味になります。ただし、このアドレスは、回線パラメーター用として必要です。このアドレスは削除してはなりません。削除すると、回線が使用不能になります。



## ダイヤルイン回線のダイヤル回線 PPP カプセル化機能パラメーター

注: パラメーターについての詳しい説明は、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の『ポイントツーポイント・プロトコル・インターフェースの使用』の章を参照してください。

ダイヤルイン・インターフェースを追加すると、次のデフォルト値が設定されます。

- SPAP、CHAP、および PAP に対する認証は使用可能です。
- PPP MRU は 1522 に設定されます。この MRU サイズは、Windows 3.1、OS/2、および DOS バージョンの IBM DIALs ダイヤルイン・クライアント用に必要です。これらのクライアントを使用していないことが明らかでない限り、この設定値を変更しないでください。
- PPP カプセル化機能上の DIALs を自動的に使用可能にします。これにより、NetBIOS 制御プロトコル、NetBIOS フレーム制御プロトコル、残り時間、SPAP 認証、コールバック、LCP 識別、およびクライアントへの IP 静的ルートの自動追加と削除など、LAN へのダイヤルイン・アクセスのユーザーにとって重要な機能がオンになります。DIALs 機能について詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の『ポイントツーポイント・プロトコル・インターフェースの使用』の章を参照してください。

## ダイヤルイン・インターフェースの追加

ダイヤルイン・インターフェースを追加するには、次のようにします。

1. 2212 上で V.34、ISDN、または ISDN/デジタル・モデム・インターフェースを構成する。構成についての詳しい説明は、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の『V.34 ネットワーク・インターフェースの使用』の章を参照してください。ISDN とデジタル・モデム・インターフェースについては、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の『ISDN インターフェースの使用』を参照してください。
2. **talk 6** コマンドを入力して、Config > プロンプトにアクセスする。
3. Config > プロンプトで **add device dial-in** と入力して、ダイヤルイン・インターフェースを追加する。ダイヤルイン回線をいくつ追加するかを尋ねられます。このコマンドは、新しいネットワークを作成し、それぞれのネットワーク番号を報告し、基本ネットワークの番号の入力を求め、マルチリンク PPP の場合は、使用可能にするように指示するプロンプトを出します。

例: 現行の最大ネットが 3 で、基本 2 ネットにダイヤルイン・ネットを 1 つ追加したいと想定します。

図45 は、ダイヤルイン・インターフェースの定義例です。

図45. ダイヤルイン・インターフェースの追加

```
Config>add dev dial-in
Adding device as interface 4
Defaulting Data-link protocol to PPP
Use "net 4" command to configure circuit parameters
Base net for this circuit [0]? 2

Enable as a Multilink PPP link? [no]
```

## DIALs の使用

Disabled as a Multilink PPP link.

```
Use "set data-link" command to change the data-link protocol
Use "net " command to configure dial circuit parameters.
Config>li dev
Ifc 0 Ethernet CSR 81600, CSR2 80C00, vector 94
Ifc 1 V.34 Base Net CSR 81620, CSR2 80D00, vector 93
Ifc 2 V.34 Base Net CSR 81640, CSR2 80E00, vector 92
Ifc 3 PPP Dial-in Circuit
Ifc 4 PPP Dial-in Circuit
```

## ダイヤルアウト・インターフェースを構成する前に

2212 上でダイヤルアウト・インターフェースを構成し、それを使用する前に、次の要件を満たしていることが必要です。

- DIALs サポートを備えた IBM ソフトウェアが 2212 にロードされている。
- 外付け V.34 モデム、内蔵モデム、またはヌル・モデム (2212 上の利用可能な WAN ポートに接続する場合)。構成情報については、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの『V.34 ネットワーク・インターフェースの使用』の章を参照してください。
- ワークステーションが 2212 DIALs サーバーへのアクセスをもつ LAN に接続されている。
- クライアントに telnet、telnet 転送機能、または IBM DIALs ダイヤルアウト・クライアントなどのソフトウェアがインストールされている。ダイヤルアウト・クライアントが正しく機能するためには、クライアントに IP が正しく構成されていることが必要です。

## ヌル・モデムの使用

ヌル・モデムを使用する場合は、D25NM-3 フル・ハンドシェイクを使用します。

ピン・マッピング:

1 から 1	1 から 1
2 から 3	3 から 2
4 から 5	5 から 4
6 から 8、20	8、20 から 6
7 から 7	7 から 7

## ダイヤルアウト・インターフェースの構成

次のステップでは、装置上のダイヤルアウト・インターフェースの構成方法について説明します。

1. V.34 モデムを、ダイヤルアウト・インターフェースとして使用する WAN ポートに接続する。
2. 2212 DIALs サーバーのコンソールに接続する。
3. \* プロンプトで **talk 6** と入力する。

4. V.34 インターフェースを設定する。詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の『V.34 ネットワーク・インターフェースの使用』の章を参照してください。
5. **add device dial-out** コマンドを使用して、ダイヤルアウト・インターフェースを追加する。インターフェースの入力を求められたら、利用可能な V.34 インターフェース番号を入力します。

**注:**

- a. V.34 基本ネットワーク上に複数の回線を構成することができます。ただし、同時に活動状態にできる回線は 1 つだけです。
  - b. ソフトウェアは、**default address** と呼ばれる V.34 アドレスを定義します。このアドレスはダイヤルアウトに必要なので、削除しないでください。これがないと、ダイヤルアウトは機能しなくなります。
6. PPP 認証サーバーを構成し (IBM DIALs ダイヤルアウト・クライアントを使用している場合)、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の『PPP 認証プロトコル』の項で説明しているように、PPP ユーザーを追加する。追加する PPP ユーザーは、ダイヤルアウトが使用可能でなければなりません。telnet を使用するダイヤルアウトは認証の必要がないので、telnet セッションの場合は認証を構成しないでください。
  7. **feature dials** コマンドを使用して、グローバル・ダイヤルアウト・パラメーターを構成する。アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の **feature** コマンドの項を参照してください。  
この環境で、ダイヤルアウト非活動タイマー、ダイヤルアウト・サーバー名、モデム・プール、およびその他のパラメーターを構成することができます。
  8. IBM DIALs ダイヤルアウト・クライアントが正しく機能させるためには、SNMP コミュニティーの定義の中で、ダイヤルアウト・サーバーを使用するすべてのダイヤルアウト・クライアントに対して読み取りアクセス許可を与えることが必要です。これは、ダイヤルアウト選択アプリケーションがネットワーク上のダイヤルアウト・サーバーを見付けるために必要です。SNMP コミュニティーの構成方法については、プロトコル構成および監視 参照資料 第 1 巻 の『SNMP 管理』の項を参照してください。
  9. 装置をリスタートする。

## モデム・プールの構成

モデム・プールとは、ユーザーからは 1 つのモデムに見えるモデムの集合です。ユーザーがダイヤルアウトすることが必要になると、このプールの中の最初の利用可能なモデムが使用されます。モデム・プールは、同じポート名をもつダイヤルアウト・インターフェースのグループを定義することによって、2212 DIALs 内に作成します。デフォルトでは、すべてのダイヤルアウト・インターフェースは

『ALL\_PORTS』という名前になり、これがモデム・プールを形成します。ダイヤルアウト・インターフェースを個別に命名すれば、ユーザーはダイヤルアウトに使用する特定のモデムを選択することが可能になります。

モデム・プールを構成するには、次のようにします。

1. \* プロンプトで **talk 6** と入力する。

## DIALs の使用

2. **net n** と入力する。ここで、**n** は、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの『V.34 ネットワーク・インターフェースの使用』の章に定義されているダイヤルアウト・インターフェースの番号です。これにより、このインターフェースの構成環境に入ります。
3. Circuit Config> プロンプトで **encapsulator** と入力する (アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの『ダイヤル回線の構成および監視』の章を参照してください)。これにより、ダイヤルアウト構成環境に入ります。
4. Dial-out Config> プロンプトで **set portname** と入力する。ポートの番号 (30 文字まで) の入力を求めるプロンプトが出ます。既存のポート名を指定すると、モデムはその名前のプールに追加されます。
5. 2212 をリスタートする。

---

## グローバル DIALs パラメーターを構成する前に

ここでは、グローバル DIALs サーバー・パラメーターについて説明します。

### サーバー提供の IP アドレス

ルーターを構成して、ダイヤルイン・クライアントが接続期間中に使用する IP アドレスを提供できるようにすることが可能です。ルーターがクライアントに割り当てるアドレスは、4 通りの方法で取り出すことができます。その方法を次に優先順に示します。

#### 1. ユーザー ID

IP アドレスを、各クライアントの PPP ユーザー・プロファイルに保管することができます。クライアントが接続して IP アドレスを要求したときに、ルーターはそのユーザーの PPP ユーザー・プロファイルに構成されているアドレスを取り出します。この方法では、ユーザーは毎回同じ IP アドレスを入手することができますが、各ユーザーごとに固有の IP アドレスが必要です。

PPP ユーザー・プロファイルに IP アドレスを構成するには、Config> **add ppp-user** コマンドを使用します。

#### 2. インターフェース

IP アドレスを、ダイヤルイン・インターフェース構成に保管することができます。クライアントが接続して IP アドレスを要求したときに、ルーターは接続に使用されたインターフェースからアドレスを取り出します。この方法は、各ダイヤルイン・インターフェースごとに固有の IP アドレスが必要です。

インターフェース IP アドレスを設定するには、次のようにします。

- Config> **list devices** コマンドを使用して、ハードウェア・インターフェースに割り当てられているインターフェース番号を表示する。
- Config> **net 'x'** コマンド ('x' は、構成されたインターフェース番号) を使用して、インターフェースのコマンド・プロンプトにアクセスする。
- PPP Config> **set ipcp** コマンドを使用して、インターフェース IP アドレスを設定する。

#### 3. プール

IP アドレスの集合を、IP アドレス・プールに保管することができます。クライアントが接続してアドレスを要求したときに、ルーターはプールからアドレスを取り出します。クライアントが切断すると、アドレスはプールに戻されます。この方法は、ダイヤルイン・クライアントの IP アドレスを構成するための単一の場所を提供するので、アドレス・サーバーは必要ありません。

IP アドレスのプールを追加するには、DIALs config> **add ip-pool** コマンドを使用します。

#### 4. DHCP プロキシ

IP アドレスを DHCP サーバーからリースすることができます。クライアントが接続してアドレスを要求したときに、ルーターはクライアントの代わりに DHCP サーバーからアドレスを要求します。この方法は、DHCP サーバーが LAN 上に存在するか、ルーター内で構成されていることが必要です。1 つの DHCP サーバーが、複数のルーター上のクライアントのアドレスを提供することができます。詳しくは、『動的ホスト構成プロトコル (DHCP)』を参照してください

DHCP サーバーを追加するには、DIALs config> **add dhcp-server** コマンドを使用します。

## IP アドレス割り当て方式

接続期間中にダイヤルイン・クライアントが使用する IP アドレスは、5 つの異なるソースから入手できます。ソースを優先順に示すと、次のようになります。

1. クライアント提供
2. ユーザー ID 割り当て
3. インターフェース割り当て
4. アドレス・プール
5. DHCP サーバー

ダイヤルイン・クライアントが接続すると、ルーターはアドレスが見つかるまで、またはすべてのソースがなくなるまで、これらのソースを順次に検索します。IP アドレスが見つからなかった場合、IPCP ネゴシエーションは失敗します。これらの方式は、任意の組み合わせで使用できます。

デフォルト構成は、次のとおりです。

```
Client      : Enabled
UserID      : Enabled
Interface   : Enabled
Pool        : Enabled
DHCP Proxy  : Disabled
```

注: デフォルトでは、PPP ユーザー・プロファイル、インターフェース、または IP アドレス・プールには、アドレスは構成されていません。

## 動的ホスト構成プロトコル (DHCP)

動的ホスト構成プロトコル (DHCP) は、ネットワーク上のホストに構成パラメーターを提供するために開発されたものです。DHCP は、他の構成パラメーターと一緒に、ネットワーク・アドレスをホストに割り当てる機構を備えています。

## DIALs の使用

プロキシ DHCP フィーチャーは、ダイヤルイン PPP ユーザーに代わって、クライアントとしての役目を果たします。これによって、装置はダイヤルイン・セッションの期間、またはリース期間が満了するまでの間、IP アドレスのリースを受けることができます。DHCP サーバーから割り当てられる IP アドレスは、PPP IPCP を通してダイヤルイン・クライアントに通知されます (IPCP についての説明は、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの『IP 制御プロトコル』の項を参照してください)。ダイヤルイン・クライアント・ソフトウェアは、IP アドレスを割り当てるために DHCP が使用されたことは知らないため、DHCP を活動化する必要はまったくありません。

プロキシ DHCP を使用するためには、少なくとも 1 つの DHCP サーバーが構成されており、ルーターからアクセス可能であることが必要です。

プロキシ DHCP では、ダイヤルイン・ユーザーに割り当てられるアドレスは、直接接続された LAN の同じサブネット内に存在する必要があります。標準的な構成では、プロキシ ARP サブネット・ルーティングを使用可能にし、ルーターがダイヤルイン・クライアントに代わってローカル・ネットワーク上のホストへの ARP 要求に回答できるようにする必要があります。

### 基本 DHCP の設定

最も基本的な構成では、ルーターと同じネットワーク上に 1 つの DHCP サーバーが存在し、リースされるダイヤルイン・アドレスがこの LAN と同じサブネット内に存在することが必要です。

クライアントはダイヤルインするときに、DHCP サーバーから IP アドレスをリースし、クライアントとの IPCP ネゴシエーションに使用します。

1. 2212 と DHCP を同じ LAN に接続する。
2. DHCP サーバーを構成して、開始する (IP アドレスをリースするためのサーバーの設定方法については、DHCP サーバーの資料を参照してください。リースする IP アドレスは、直接接続された LAN のサブネット内に存在しなければならず、プロキシ ARP が 2212 上で使用可能にされていないことを覚えておいてください。)
3. プロキシ DHCP の標準的な設定では、Client-Specified、Userid、Interface、および Pool の IP アドレス・ネゴシエーション・オプションを使用不可にします。

```
Dials Config>list ip
DIALs client IP address specification:
Client : disabled
UserID : disabled
Interface : disabled
DHCP Proxy : enabled
```

4. DHCP サーバーを追加する (Dials Config> **add dhcp 10.0.0.111**)。
5. ダイヤルイン・クライアント・ソフトウェアを *Server assigned* に設定する。

#### 注:

- a. *Server assigned* 構成は、ダイヤルイン・クライアントの実現によって異なります。
- b. クライアント・ソフトウェアは、そのアドレスを DHCP から入手するように構成してはなりません。クライアントのアドレスは、初期構成要求時に、アドレス 0.0.0.0 を IPCP に送信して入手することが必要です。



6. この設定では、DHCP GATEWAY ADDRESS はデフォルトの 0.0.0.0 にします。

## DHCP サーバーへの複数のホップ

構成された DHCP サーバーは、接続されたルーターから到達可能な IP アドレスに存在しなければなりません。常にリモート・アクセス・ボックスからサーバーに PING できることが必要です。

DHCP サーバーが複数ホップ離れた場所にある場合、サーバーは応答の送信先のアドレスを知っている必要があります、どのプールから IP アドレスを割り当てるかを示すことも必要です。DHCP サーバーを利用して多数のサブネットにアドレスを提供できるようにする上で、IP を割り当てるプールは重要であり、どのアドレス・プールから選択するかについて何らかの指示をする必要があります。そのために、DHCP ゲートウェイ・アドレス (*giaddr*) が使用されます (この用語は RFC 2131 の定義に準拠しています)。*giaddr* は、2212 にローカルのアドレス (たとえば、トークンリングまたはイーサネット LAN ポートなど) でなければなりません。*giaddr* は DHCP サーバーが応答に使用するアドレスなので、DHCP サーバー自体からこのアドレスに PING できることも確認する必要があります。

## 複数 DHCP サーバー・ネットワーク

冗長性のために、複数の DHCP サーバーを構成することも可能です。複数のサーバーを構成した場合、プロキシ DHCP クライアントはすべてのサーバーにアドレスを尋ね、最初に受信した応答を受け入れます。DHCP サーバーのどれかが 2 ホップ以上離れていたり、プール内のアドレスに対応していないサブネットに接続されている場合には、*giaddr* を構成する必要があります。『DHCP サーバーへの複数のホップ』を参照してください。

複数の DHCP サーバーがアドレスを提供する可能性があるため、各サーバーに構成するアドレス・プールはオーバーラップしないようにすることが重要です。DHCP サーバーが応答および検索を行う *giaddr* は 1 つしかないので、各アドレス・プールはお互いに同じサブネット内に存在することが必要です。

## 動的ドメイン名サーバー (DDNS)

ドメイン名サーバー (DNS) は、IP アドレスをホスト名にマップするもので、通常は静的な性質を持っています。動的 DNS フィーチャーというのは、DDNS DHCP サーバーおよび DNS サーバーと一緒に使用した場合、DHCP が IP アドレスとホスト名のマッピングを用いて DNS サーバーを動的に更新することができるフィーチャーをいいます。このフィーチャーは、プロキシ DHCP と一緒にしか使用できません。

2212 上の DNS を使用可能にし、ユーザー・プロファイルにホスト名を構成すると (アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの『PPP 認証プロトコル』の項を参照)、このホスト名がオプション 81 (DDNS) として DHCP サーバーにパスされます。DDNS に対して DHCP サーバーが正しく構成されている場合、DHCP サーバーは、ルーターにリースされた IP アドレスと、ルーターが送信したホスト名を使用して、DDNS サーバーを更新します。これにより、他のユーザーはホスト名を使用してダイヤルイン・クライアントにアクセスすることが可能になり、クライアントは動的に選択された IP アドレスを知っている必要はありません。

## DIALs の使用



## 第29章 DIALs の構成

この章では、DIALs 構成コマンドおよび動作コマンドについて説明します。この章には、次の内容が記載されています。

- 『DIALs グローバル構成環境へのアクセス』
- 『DIALs グローバル構成コマンド』
- 468ページの『DIALs グローバル監視環境へのアクセス』
- 468ページの『DIALs グローバル監視コマンド』
- 472ページの『ダイヤルイン・インターフェースの監視』
- 472ページの『ダイヤルアウト・インターフェースの監視』

### DIALs グローバル構成環境へのアクセス

グローバル構成プロセスにアクセスするには、次の手順を使用します。

1. OPCON プロンプトで、**talk 6** と入力する。(このコマンドについて詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の *OPCON* プロセスおよびコマンド の章を参照してください。) たとえば、次のように入力します。

```
* talk 6
Config>
```

**talk 6** コマンドを入力すると、CONFIG プロンプト (Config>) が端末に表示されます。最初に構成に入ったときにプロンプトが表示されない場合は、**Return** をもう一度押してください。

2. CONFIG プロンプトで **feature dials** コマンドを入力して DIALs Config> プロンプトを表示し、DIALs グローバル・パラメーター構成環境にアクセスします。

### DIALs グローバル構成コマンド

表 54. DIALs グローバル構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxiページの『ヘルプの入手』を参照してください。
Add	DHCP (動的ホスト構成プロトコル) サーバーを DHCP サーバーのリストに追加するか、または IP アドレス・プールを追加します。
Delete	DHCP サーバーをリストから削除するか、またはアドレス・ブロックを IP アドレス・プールから除去します。
Disable	IP アドレス割り当て方式、ダイヤルアウト・プロトコル、マルチシャシー MP、SPAP バナー、および動的 DNS を使用不可にします。
Enable	各種の IP アドレス割り当て方式、ダイヤルアウト・プロトコル、マルチシャシー MP、SPAP バナー、および動的 DNS を使用可能にします。
List	グローバル DIALs パラメーターとその値を表示します。

## DIALs の構成

表 54. DIALs グローバル構成コマンド (続き)

コマンド	機能
Set	許容時間、dhcp ゲートウェイ・アドレス、NetBIOS ネーム・サーバー・アドレス、ローカル割り当て MAC アドレス、バーチャル接続 (VC)、動的ネーム・サーバー・アドレス、ダイヤルアウト非活動タイマー、およびダイヤルアウト・サーバー名を設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

## Add

**add** コマンドは、新しいプロキシ DHCP サーバーをサーバーのリストに追加するか、または IP アドレス・プールを追加するのに使用します。

プロキシ DHCP サーバー・リストには DHCP サーバーの IP アドレスが入っており、この IP アドレスがダイヤルイン・クライアントにリースされます。冗長さのために、複数のサーバーを追加することも可能です。サーバーの最大数は 20 です。

IP アドレス・プール・フィーチャーは、ルーターがローカル定義されたアドレス・プールからダイヤルイン・クライアントへの IP アドレスを取り出すことができる方法を提供します。クライアントは、ルーターへの接続期間中、このアドレスを使用することができます。プールは、1 つまたは複数のブロックの IP アドレスから構成されます。ブロックの最大数は 20 です。各ブロックは、基本 IP アドレスとブロック内のアドレスの個数によって定義されます。各ブロック内のアドレスは、基本アドレスから始まって、昇順に連続しています。

構文:

```
add                dhcp-server ipaddress
                   ip-pool baseaddress #addresses
```

**dhcp-server** *ipaddress*

指定の IP アドレスをもつ dhcp サーバーを追加します。

例:

```
DIALs Config> add dhcp-server
DIALs Proxy DHCP server address [0.0.0.0]? 10.0.0.1
```

**ip-pool** *baseaddress* *#addresses*

アドレス・ブロックを IP プールに追加します。

例:

```
DIALs Config> add ip-pool
Base address []? 192.1.100.18
Number of addresses [1]? 57
DIALs config>add ip-pool
Base address []? 192.2.200.1
Number of addresses [1]? 250
DIALs config>list ip-pools
Configured IP address pools:
  Base Address      Last Address      Number
  -----
  192.1.100.18     192.1.100.74     57
  192.2.200.1      192.2.200.250    250
```

## Delete

**delete** コマンドは、サーバーのリストから既存のプロキシ DHCP サーバーを削除するか、または IP アドレス・プールからアドレス・ブロックを削除するのに使用します。

構文:

```
delete                dhcp-server ip address
                        ip-pool baseaddress #addresses
```

**dhcp-server** *ipaddress*

指定の IP アドレスをもつ dhcp サーバーを削除します。

例:

```
DIALs Config> delete dhcp-server
Enter the address to be deleted [0.0.0.0]? 10.0.0.1
```

**ip-pool** *baseaddress #addresses*

IP プールからアドレス・ブロックを削除します。

例:

```
DIALs Config> delete ip-pool
Base IP address of the block to be removed []? 192.2.200.1
```

## Disable

**disable** コマンドは、IP アドレス割り当て方式、ダイヤルアウト・プロトコル、SPAP バナー、および動的 DNS を使用不可にするのに使用します。

構文:

```
disable                dynamic-dns
                        dial-out
                        ip-address-assignment type
                        spap-banner
```

**dial-out** *type*

telnet または IBM DIALs ダイヤルアウト・クライアントとのダイヤルアウトを使用不可にします。次のものを指定することができます。

**dials** すべての IBM DIALs ダイヤルアウト・クライアントを使用不可にします。

**telnet** すべての telnet クライアントを使用不可にします。

両方のタイプのクライアントを使用不可にするためには、各タイプごとに **disable dial-out** コマンドを入力する必要があります。両方のタイプのクライアントを使用不可にすると、2212 上のダイヤルアウトが使用不可になります。

**dynamic-dns**

ユーザーのホスト名の DHCP オプション 81 を送信するのを使用不可にします。詳しくは、457ページの『動的ドメイン名サーバー (DDNS)』を参照してください。

## DIALs の構成

### IP-address-assignment *type*

各種の IPCP アドレス割り当て方式を使用不可にします。次のすべてが指定できます。

- Client - クライアント指定 IP アドレス割り当てを防止します。
- Userid - 認証ユーザー・プロファイルを使用して IP アドレスを調べるのを防止します。
- Interface - ルーターがインターフェースの IPCP 設定値を使用するのを防止します。
- Pool - ルーターが IP アドレス・プールを使用してクライアントにアドレスを割り当ててるのを防止します。
- DHCP-proxy - ルーターが DHCP サーバーからアドレスをリースするのを防止します。

割り当て方式については、454ページの『サーバー提供の IP アドレス』を参照してください。

### spap-banner

SPAP バナーを SPAP によって認証されたりリモート・ユーザーに送信するのを使用不可にします。

注: \n を入力すると、バナーの改行文字がクライアントに表示されます。

## Enable

**enable** コマンドは、IP アドレス割り当て方式、ダイヤルアウト・プロトコル、SPAP バナー、および動的 DNS を使用可能にするのに使用します。

構文:

```
enable                               dynamic-dns  
                                       ip-address-assignment . . .  
                                       spap-banner
```

### dial-out *type*

telnet または IBM DIALs ダイアルアウト・クライアントとのダイヤルアウトを使用可能にします。デフォルトでは、両方のタイプのクライアントが使用可能になります。次のものを指定することができます。

**dials** すべての IBM DIALs ダイアルアウト・クライアントを使用可能にします。

**telnet** すべての telnet クライアントを使用可能にします。

### dynamic-dns

ユーザーのホスト名の DHCP オプション 81 を送信するのを使用可能にします。詳しくは、457ページの『動的ドメイン名サーバー (DDNS)』を参照してください。

### IP-address-assignment *type*

各種の IPCP アドレス割り当て方式を使用可能にします。ルーターは使用可能にされている各方式をリスト順に試行します。次のすべてが指定できません。

- クライアント - クライアントは、使用するアドレスを指定することができます。
- Userid - ルーターは認証された PPP ユーザー・プロファイルで IP アドレスを調べます。アドレスが非ゼロの場合、そのアドレスがクライアントに提供されます。
- Interface - ルーターはインターフェースに構成された IP アドレスを調べます。アドレスがゼロでない場合、そのアドレスがクライアントに提供されます。
- Pool - ルーターは IP アドレス・プールからアドレスを要求します。アドレスが利用可能な場合、それがクライアントに提供されます。
- DHCP-proxy - ルーターは DHCP からアドレスのリースを試みます。成功した場合、そのアドレスがクライアントに提供されます。

割り当て方式については詳しくは、454ページの『サーバー提供の IP アドレス』を参照してください。

### spap-banner

SPAP バナーを SPAP によって認証されたリモート・ユーザーに送信するのを使用可能にします。SPAP バナーのテキストを入力するには、465ページの『Set』に説明されている **set spap-banner** コマンドを使用します。詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの『Shiva パスワード認証プロトコル (SPAP)』を参照してください。

## List

**list** コマンドは、現行の構成を表示するのに使用します。ポイントツーポイント・コンソールから、各ネットワークの DHCP 状態およびリース時間を監視することができます。例については、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの **listipcp** コマンドの項を参照してください。

### 構文:

```
list all
      dhcp-servers
      dial out
      dynamic-dns
      ip-address-assignment
      ip-pools
      name-servers
      spap-banner
      time-allowed
      vc-parameters
```

### 例:

```
DIALs config>li all
DIALs client IP address assignment:
Client      : Enabled
```

## DIALs の構成

```
UserID      : Enabled
Interface   : Enabled
Pool        : Enabled
DHCP Proxy  : Disabled
```

### Configured IP address pools:

Base Address	Last Address	Number
11.0.0.100	11.0.0.129	30
11.0.0.210	11.0.0.229	20

```
Configured DHCP servers:      11.0.0.2      11.0.0.50
```

```
Proxy DHCP is currently disabled
```

```
DHCP gateway address (giaddr): 11.0.0.10
```

```
Dynamic DNS: Enabled
```

```
Primary Domain Name Server   (DNS): 11.0.0.2
```

```
Secondary Domain Name Server (DNS): None
```

```
Primary NetBIOS Name Server  (NBNS): 11.0.0.2
```

```
Secondary NetBIOS Name Server (NBNS): None
```

```
Time allowed for connections: Unlimited
```

```
SPAP banner :Enabled
```

```
Welcome to the network...
```

### Box-level dial-out settings

```
Inactive timer:
```

```
15
```

```
LAN Protocols enabled for dial-out:
```

```
TELNET DIALs
```

```
Server name:
```

```
DIALOUT_SERVER
```

```
Number of Mac Addresses defined = 0
```

```
Base MAC Address: 000000000000
```

```
VC: Maximum Virtual Connections = 50
```

```
VC: Maximum suspend time (hours) (0 is unlimited) = 12
```

```
VC: Idle timeout period (seconds) = 30
```

```
Multi-chassis MP: Endpoint discriminator (0 means use box s/n) = 0
```

```
DIALs config>
```

この例は、次のことを示しています。

### DIALs client IP address specification

IP アドレス割り当て方式とそれが使用可能かどうかを表示します。このセクションおよびボックス・レベル・ダイヤルアウト設定値が入っているセクションの表示は、**list ip-address-assignment** コマンドへの応答として受け取ります。

### IP address pools

構成された IP アドレス・プールを表示します。このセクションの表示は、**list ip-pool** コマンドへの応答として受け取ります。

### Configured DHCP servers

現在 DHCP サーバーとして構成されている IP アドレスのリストを表示します。このセクションには、DHCP ゲートウェイとして使用されているインターフェースも表示されます。このセクションの表示は、**list dhcp-servers** コマンドへの応答として受け取ります。

### Dynamic Name Servers

動的 DNS が使用可能かどうかを表示します。このセクションの表示は、**list dynamic-dns** コマンドへの応答として受け取ります。

**primary domain server (dns)**

この行とその下の数行は、構成されている 1 次および 2 次ネーム・サーバーを表示します。このセクションの表示は、**list name-servers** コマンドへの応答として受け取ります。

**time allowed**

このユーザーの最大時間 (分) を表示します。このセクションの表示は、**list time-allowed** コマンドへの応答として受け取ります。

**spap banner**

spap バナーの内容を表示します。このセクションの表示は、**list spap-banner** コマンドへの応答として受け取ります。

**vc connections**

構成されたバーチャル・接続に関する情報を表示します。

**multi-chassis mp**

構成されたエンドポイント識別子を表示します。

## Set

**set** コマンドを使用して、許容時間、dhcp ゲートウェイ・アドレス、NetBIOS ネーム・サーバー・アドレス、動的ネーム・サーバー・アドレスおよびダイヤルアウト非活動タイマーとダイヤルアウト・サーバー名を設定します。

**構文:**

```

set
    dhcp-gateway-address
    dial-out . . .
    dns . . .
    laa
    multi-chassis-mp
    nbns . . .
    spap-banner . . .
    time-allowed
    vc-parameters

```

**dhcp-gateway-address interface# ipaddress**

DHCP ゲートウェイに対応する IP アドレスを設定します。DHCP はアドレスを次の目的で使用します。

1. DHCP の応答先のアドレス。
2. DHCP が割り当てる IP アドレスが入っているアドレス・プールの指示。

DHCP サーバーが LAN インターフェースに直接接続されていない場合、このアドレスは、DHCP サーバーへの IP 接続を持つ LAN インターフェースのうちの 1 つのアドレスとして構成する必要があります。詳しくは、455ページの『動的ホスト構成プロトコル (DHCP)』、および RFC 1541 の『giaddr』の定義を参照してください。

## DIALs の構成

### **dial-out parameter**

ダイヤルアウト・ネットワークの非活動タイマーまたはサーバー名を設定します。**Parameter** は、次のどちらかを使用できます。

#### **inactivity-timer**

ダイヤルアウト・ネットワークのダイヤルアウト非活動タイマーを設定します。これは、ユーザーがデータ・トラフィックなしに接続していられる時間 (分) として定義されます。たとえば、非活動タイマーが 5 分に設定されている場合、5 分間データの送受信がないと、その接続はドロップされ、モデムが利用可能になります。デフォルト値は 0 です。これは非活動タイマーは使用不可にされ、接続は無限に保持されることを意味しています。

#### **servername**

ダイヤルアウト・サーバーの名前を設定します。30 文字までの長さの任意の文字列を使用できます。デフォルト値は

『2210\_DIALS\_SERVER』です。これは、IBM DIALs ダイヤルアウト・クライアントが『Chooser』アプリケーションを使用してダイヤルアウト・サーバーを見つけるときに表示される名前です。このパラメーターは、telnet ダイヤルアウト・クライアントに対しては意味を持ちません。

### **dns type ipaddress**

1 次および 2 次ドメイン名サーバー (DNS) を構成します。**Type** は、次のどちらかを使用できます。

#### **primary**

使用するダイヤルイン・クライアントの 1 次 DNS サーバーの IP アドレスを設定します。一部のダイヤルアウト・クライアントでは (特に、Windows 95)、この値は IPCP 時にネゴシエーションされます。

#### **secondary**

使用するダイヤルイン・クライアントの 2 次 DNS サーバーの IP アドレスを設定します。一部のダイヤルアウト・クライアントでは (特に、Windows 95)、この値は IPCP 時にネゴシエーションされます。

### **laa #MAC\_addresses MAC\_address\_base**

ローカル管理アドレス (LAA) テーブルの MAC アドレスおよび基本アドレスの数を設定します。LAA アドレスを使用するのは、レイヤー 2 トンネル・ネットワークだけです。

#### **#MAC\_addresses**

MAC\_Address\_Base から始まる LAA テーブルに追加する MAC アドレスの数を指定します。

有効値: 0 ~ 256

デフォルト値: 0

#### **MAC\_address\_base**

LAA テーブルの基本 MAC アドレスを指定します。

有効値: 任意の有効な MAC アドレス

デフォルト値: 000000000000



例:

```
DIALs config>set 1aa
Number of Mac Addresses: [0]? 20
Locally Administered Mac Address Base (hex) [000000000000]? 002210aaaaaa
DIALs Config>
```

### multi-chassis-mp

使用するエンドポイント識別子を設定します。同じバンドルに結合するすべてのリンクは、同じエンドポイント識別子を持っていなければなりません。

例:

```
DIALs Config> set multi-chassis-mp
Enter Endpoint Discriminator to use from stacked group (0 for box S/N): 2345
```

### nbns type ipaddress

1 次および 2 次 NetBIOS ネーム・サーバーを構成します。**Type** は、次のどちらかを使用できます。

#### primary

1 次 NetBIOS ネーム・サーバーの IP アドレスを設定します。

#### secondary

2 次 NetBIOS ネーム・サーバーの IP アドレスを設定します。

### spap-banner

SPAP 認証を正常に完了したすべてのクライアントに送信するメッセージを構成することができます。

例:

```
DIALs config>set spap-banner
SPAP banner :Disabled

Enter Banner: Welcome to the network...
```

### time-allowed

PPP ダイアルイン・ユーザーおよびダイヤルアウト・ユーザーに許容される時間を設定します。このパラメーターは、ユーザーが接続を維持できる最大時間 (分) を定義します。デフォルト値は 0 で、これはユーザーが無限に接続していただけることを意味します。

### vc-parameters

このパラメーターは、デフォルトのグローバル・バーチャル接続属性を設定するのに使用します。システムは、接続の最大数、最中断時間、および非活動タイムアウト値の入力を求めるプロンプトを出します。

例:

```
Config> feature DIALs
DIALs Config> set vc-parameters
Maximum Virtual Connections [50]? 40
Maximum suspended time (hours) (0 is unlimited) [10]? 18
Inactivity Timeout (seconds) [30]? 60
DIALs Config>
```

#### Maximum Virtual Connections

活動状態または中断状態にできるバーチャル接続の最大数。MP で VC を使用する場合、この値は物理接続の数より 1 だけ大きい値に構成してください。

有効値: 0 ~ 255

デフォルト値: 50

## DIALs の構成

### Maximum suspended time

システムが接続を終了する前に、バーチャル接続を中断状態における最大時間。このパラメーターを 0 に指定すると、バーチャル接続は無限に中断状態でいられます。

有効値: 0 ~ 48

デフォルト値: 12

### Inactivity Timeout

中断する前に、バーチャル接続を非活動状態における秒数。

有効値: 10 ~ 1024

デフォルト値: 30

---

## DIALs グローバル監視環境へのアクセス

DIALs 監視コマンドにアクセスするには、次の手順を使用します。

1. OPCON プロンプトで **talk 5** を入力する。(このコマンドについて詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の“OPCON プロセスおよびコマンド”の章を参照してください。)たとえば、次のように入力します。

```
* talk 5
+
```

**talk 5** コマンドを入力すると、端末に GWCON プロンプト (+) が表示されます。最初に構成に入ったときにプロンプトが表示されない場合は、**Return** をもう一度押してください。

2. + プロンプトで **feature dials** コマンドを入力して DIALS Console> プロンプトを表示して、グローバル監視環境にアクセスします。

例:

```
+ feature dials
DIALS Console>
```

---

## DIALs グローバル監視コマンド

表 55. DIALs グローバル監視コマンド

コマンド	機能
Clear	特定の中断されたバーチャル接続をクリアします。
List	各種のバーチャル接続の状態、またはすべてのバーチャル接続を表示します。
Reset	DIALS パラメーターを動的に活動化します。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

### Clear

**clear** コマンドは、特定の中断されたバーチャル接続をクリアするのに使用します。

構文:

```
clear vc connection_id
```

**vc connection\_id**

終了する中断バーチャル接続を指定します。 *connection\_id* を入手するには、**list all-vc** または **list suspended-vc** コマンドを入力します。

## List

**list** コマンドは、すべてのバーチャル接続、活動状態のバーチャル接続、中断されたバーチャル接続、または *vc-parameters* の値を表示するのに使用します。

構文:

```
list
    all
    active-vc
    all-vc
    dhcp-servers
    ip-address-assignment
    ip-pool
    suspended-vc
```

**active-vc**

すべての活動状態のバーチャル接続の属性を表示します。属性の説明については、**all-vc** パラメーターの項を参照してください。

**all-vc**

すべての活動状態および中断状態のバーチャル接続の属性を表示します。この表示は、**list active-vc** コマンドと **list suspended-vc** コマンドの表示を組み合わせたものです。

例:

```
+ feature dials
DIALS console> list all
DIALS client IP address assignment:
Client      : Enabled
UserID     : Enabled
Interface  : Enabled
Pool       : Enabled
DHCP Proxy : Disabled

Current IP address pools:
      Base Address      Last Address      Total      Free
      -----      -
*      11.0.0.100      11.0.0.129      30      30
      11.0.0.210      11.0.0.229      20      19

Current DHCP servers:      11.0.0.2      11.0.0.50
Proxy DHCP is currently disabled
DHCP gateway address (giaddr): 11.0.0.10

Active VCs:
Conn ID      Interface      Idle-Timeout      Connected      Username
-----      -
1656494850      8      30      0:26:15      don
7293521502      9      30      1:41:57      jane

Suspended VCs:
```

## DIALs の構成

```
          Hrs.Max
Conn ID   Suspend Suspended Username
=====  =====  HH:MM:SS =====
9256166098    12    0: 4:13  joe
```

活動および中断 VC の属性は、次のとおりです。

### Conn ID

バーチャル接続の接続 ID。システムは、接続を確立するときに ID を割り当てます。

### Username

AAA、RADIUS、またはバーチャル接続を確立するローカル・リスト・ユーザー

活動 VC の場合:

### Interface

バーチャル接続を管理しているネットワーク・インターフェース。

**注:** VC が中断したこのインターフェースを使用している他のユーザーが問題を起こすのを避けるために、インターフェース割り当てを使用しているダイヤルアップ・クライアントには、IP アドレスを割り当てないでください。

### Idle Timeout

システムが VC を中断する前に非活動状態になっている時間数 (分)。これは **set** コマンドの非活動タイマーの値に一致しています。

### Connected HHH:MM:SS

VC がインターフェースに接続されていた時間数 (時間、分、秒)

中断 VC の場合:

### Hrs. Max Suspended

システムが接続を終了する前に VC が中断状態でいられる最大時間。これは **set** コマンドの最大中断時間の値に一致します。

### Suspended HH:MM:SS

VC が中断されていた合計時間数 (時間、分、秒)

## dhcp-servers

DHCP サーバーとその IP アドレスについて構成された情報を表示します。

## ip-address-assignment

IP アドレスをクライアントに割り当てるのに使用できる方式を表示します。

## ip-pool

現在のプールの使用状況を表示します。

例:

```
DIALs Console> list ip-pool
Current IP address pools:
  Base Address      Last Address      Total      Free
  -----
*  192.1.100.18     192.1.100.74     57         57
   192.2.200.1     192.2.200.250   250        250
```

Note: The \* indicates from which block the next address will be retrieved.

**suspended-vc**

すべての中断状態のバーチャル接続の属性を表示します。属性の説明については、**all-vc** パラメーターの項を参照してください。

**vc-parameters**

**set vc-parameters** コマンドを使用して設定された **vc-parameters** の値を表示します。

**Reset**

**reset** コマンドは、talk 6 で DIALs インターフェースに加えられた構成変更を動的に活動化するのに使用します。

構文:

**reset** all

dhcp-parameters

ip-address-assignment

ip-pool

vc-parameters

**all** DHCP、IP アドレス割り当て、および IP プールの構成変更を動的に活動化します。

**dhcp-parameters**

DHCP 構成を動的に活動化します。

**ip-address-assignment**

IP アドレス割り当て方式の構成を動的に活動化します。

**ip-pool**

IP アドレス・プールの構成を動的に活動化します。

**vc-parameters**

VC 構成変更を動的に更新します。

**ダイヤルアウト・インターフェース構成コマンド**

ダイヤルアウト・インターフェース・パラメーター環境にアクセスするには、次のようにします。

1. \* プロンプトで **talk 6** と入力する。
2. Config > プロンプトで **net n** と入力する。
3. Circuit config: n> プロンプトで **encapsulator** と入力する。

表56 は、dial-out config> プロンプトから利用可能なコマンドを示しています。

表 56. ダイヤルアウト・インターフェース構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxiページの『ヘルプの入手』を参照してください。
Set	モデムに対応するポート名を定義します。

## DIALs の構成

表 56. ダイアルアウト・インターフェース構成コマンド (続き)

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

## Set

**set** コマンドは、モデムのポート名を定義するのに使用します。

構文:

**set** portname *name*

**portname**

モデムに対応するポートの名前を定義します。この名前は、**モデム・プールを定義するのに使用します**。 名前の長さは最大 30 文字までです。

デフォルト値: ALL\_PORTS

例: dial-out config>set portname localcalls

---

## ダイアルイン・インターフェースの監視

ダイアルイン・インターフェースの監視は、他の PPP ダイアル回線の監視と同様です。詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きの『ポイントツーポイント・プロトコル・インターフェースの構成および監視』の章を参照してください。

---

## ダイアルアウト・インターフェースの監視

表57 は、ダイアルアウト・インターフェースを監視するのに使用できるコマンドを示しています。

表 57. ダイアルアウト・インターフェース監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxiページの『ヘルプの入手』を参照してください。
Clear	このダイアルアウト・インターフェースの統計をリセットします。
List	ダイアルアウト・インターフェースの現在の状態、このインターフェース上で送受信されたバイト数、およびクライアントの現行パラメーターを表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxiiページの『下位レベル操作環境の終了』を参照してください。

## Clear

**clear** コマンドは、このインターフェースによって送受信されたオクテット数の統計をリセットするのに使用します。

構文:

**clear**

例:

```
clear
Statistics reset.
```

**List**

**list** コマンドは、ダイヤルアウト・インターフェースの現在の状態を表示するのに使  
用します。**list** コマンドは常に、ダイヤルアウト・ネットワークの現在の状態、その  
状態に変更されてから経過した時間、および送受信したバイト数を表示します。

構文:

**list**

非活動インターフェースの例:

```
list
Dial-out Settings for current session:

Dial-out state is DOWN
Time since change          = 52 minutes and 34 seconds

Dial-out Octets transmitted = 0
Dial-out Octets received   = 0

Session down, no valid settings
```

注: クライアントが telnet を使用してダイヤルアウト・ポートに接続している場合、  
サーバーは認証を行わなかったため、ユーザー名は存在しません。

活動インターフェースの例:

```
list
Dial-out Settings for current session:

Dial-out state is UP
Time since change          = 3 seconds

Dial-out Octets transmitted = 14
Dial-out Octets received   = 765

Current user                = not available
Time allowed for user       = unlimited
Inactivity timer for port   = 10 minutes
Line speed                  = 57600
Current DTR state           = DTR ON
Current dial-out protocol   = TELNET
Options negotiated:
  Will Suppress Go Ahead
  Wont' Echo characters
```

活動 IBM DIALs ダイヤルアウト・クライアントの例:

```
list
Dial-out Settings for current session:

Dial-out state is UP
Time since change          = 12 seconds

Dial-out Octets transmitted = 11
Dial-out Octets received   = 756

Current user                = ebooth
Time allowed for user       = unlimited
```

## DIALs の構成

Inactivity timer for port = 10 minutes  
Line speed = 57600  
Current DTR state = DTR ON  
Current dial-out protocol = DIALs



---

## 第30章 DHCP サーバーの使用

この章では、DHCP サーバーの使用法について説明します。この章には、次の内容が記載されています。

- 『DHCP の概要』
- 480ページの『概念と用語』
- 483ページの『DHCP サーバーとリースのパラメーター』
- 483ページの『DHCP オプション』
- 496ページの『DHCP 用の IP の構成』
- 498ページの『DHCP サーバーのサンプル構成』

---

### DHCP の概要

動的ホスト構成プロトコル (DHCP) は、ブートストラップ・プロトコル (BOOTP) に基づいたクライアント/サーバー・プロトコルです。DHCP サーバーは、中央制御される再使用可能 IP アドレスなどの TCP/IP 構成情報を DHCP クライアントに提供します。DHCP サーバーの機能は、ネットワーク管理者が構成情報を新規ユーザーと既存ユーザーに配布する負担を軽減します。この機能は、RFC 2131 に準拠していますが、その資料に記載されていない追加機能を多数サポートしています。RFC 951 に定義されている BOOTP クライアントもサポートしています。

DHCP を使用すれば、対応するクライアントは同報通信 DISCOVER メッセージを送信してネットワーク内の DHCP サーバーを検出でき、その後ネットワークからクライアントの構成データを動的に取得できます。DHCP は、よく知られている BOOTP UDP ポート (サーバーは 68、クライアントは 67) を使用して、要求と応答をやり取りします。DHCP クライアントとサーバーは、既存の BOOTP リレー・エージェントを使用して、サービス範囲を拡張できます。DHCP は、変化するネットワークに対応する機能など、静的に構成されるネットワークを上回る数多くの利点を備えています。クライアントは IP アドレスのリースを受けるだけなので、アドレスがなくなったり、クライアントが別のサブネットに移動した場合に、アドレスを解放して他のクライアントが使用できるようにすることができます。

### DHCP の動作

DHCP を使用すれば、クライアントは IP ネットワーク構成情報 (IP アドレスなど) を中央の DHCP サーバーから入手できます。DHCP サーバーは、クライアントに提供するアドレスを永続的に割り振るか、特定の時間枠の間リースするかを制御します。クライアントがリースされたアドレスを受け取った場合は、アドレスの再検討とリースの更新をサーバーに定期的に要求する必要があります。

アドレス割り振り、リース、およびリース更新の処理は、すべてエンド・ユーザーには見えない DHCP クライアント・プログラムとサーバー・プログラムによって処理されます。クライアントは、RFC の設計によるメッセージを使用して、DHCP サーバーから提供されるオプションを受け入れて使用します。例を次に示します。

## DHCP サーバーの使用

1. クライアントは、メッセージ (クライアント ID を含む) を同報通信します。このメッセージは、クライアントの存在を公示し、IP アドレス (DHCPDISCOVER メッセージ) と、サブネット・マスク、ドメイン名サーバー、ドメイン名、静的ルートなどの必要なオプションを要求します。
2. (オプション) ネットワーク内のルーターが DHCP メッセージと BOOTP メッセージ (BOOTP リレーを使用) を転送するように構成されている場合は、同報通信メッセージは接続されたネットワークの DHCP サーバーに転送されます。
3. クライアントの DHCPDISCOVER メッセージを受け取った各 DHCP サーバーは、IP アドレスを提示する DHCPOFFER メッセージを送信します。DHCP サーバーは、アドレスを提示する前に、ネットワークに重複する IP アドレスがないかどうか検査します。サーバーは、構成ファイルを検査して、このクライアントに静的アドレスまたは動的アドレスのどちらを割り当てるか判断します。動的アドレスの場合は、サーバーはアドレス・プールからアドレスを選択し、もっとも古く使用されたアドレスを選びます。アドレス・プールは、クライアントにリースする IP アドレスの集まりです。静的アドレスの場合は、サーバーは DHCP サーバー構成の Client ステートメントを使用して、クライアントにオプションを割り当てます。提示の際に、DHCP サーバーは提示されるアドレスを予約します。
4. クライアントは、提示メッセージを受け取り、使用するサーバーを選択します。DHCP クライアントは提示を受け取ると、その提示に要求したオプションがいくつか含まれているかを記録します。DHCP クライアントは、最初の提示を受け取った後 4 秒間、DHCP サーバーから引き続き提示を受け取り、それぞれの提示に含まれている要求したオプションの数を記録します。その時間が終了すると、DHCP クライアントはすべての提示を比較し、基準を満たすものを 1 つ選択します。
5. クライアントは、選択したサーバーを示すメッセージを同報通信し、そのサーバーが提示した IP アドレスの使用を要求します (DHCPREQUEST メッセージ)。
6. サーバーが、サーバーの提示をクライアントが受け入れたことを示す DHCPREQUEST メッセージを受け取った場合、サーバーはそのアドレスにリース済みのマークを付けます。サーバーが、別のサーバーからの提示をクライアントが受け入れたことを示す DHCPREQUEST メッセージを受け取った場合、サーバーはアドレスを使用可能プールに戻します。指定時間内にメッセージを受け取らなかった場合は、サーバーはアドレスを使用可能プールに戻します。選択されたサーバーは、追加の構成情報を含む肯定応答をクライアントに送信します (DHCPACK メッセージ)。
7. クライアントは、構成情報が有効であるかどうかを判別します。DHCPACK メッセージを受け取ると、DHCP クライアントは提供された IP アドレスにアドレス解決プロトコル (ARP) 要求を送信し、すでに使用中でないかどうか調べます。クライアントが ARP 要求に対する応答を受け取った場合、クライアントは提示を辞退し (DHCPDECLINE メッセージ)、処理を再度開始します。そうでなければ、クライアントは構成情報を受け入れます。
8. 有効なリースを受け入れると、クライアントは DHCP サーバーとの BINDING 状態に入り、IP アドレスとオプションの使用を開始します。DHCP クライアントが動的アドレス・クライアントである場合、DHCP クライアントは、ホスト名と IP アドレスのマッピングを動的ドメイン名サーバーに通知します。

オプションを要求する DHCP クライアントに対して、通常 DHCP サーバーは、サブネット・マスク、ドメイン名サーバー、ドメイン名、静的ルート、クラス ID (特定のベンダーを識別する)、ユーザー・クラスなどのオプションを提供します。

ただし DHCP クライアントは、独自に固有なオプションのセットを要求できます。たとえば、Windows NT 3.5.1 DHCP クライアントはこのようなオプションを要求する必要があります。クライアントが要求する DHCP オプションの IBM 提供のデフォルト・セットは、サブネット・マスク、ドメイン名サーバー、静的ルートなどです。オプションの説明は、483ページの『DHCP オプション』を参照してください。

## リースの更新

DHCP クライアントは、リースの残り時間を常に監視しています。リース満了の指定時間前 (通常は、リース時間の半分が経過したとき) に、クライアントは更新要求をリース側のサーバーに送信します。更新要求には、クライアントの現行 IP アドレスと構成情報が入っています。サーバーがリースの提示に応答した場合は、DHCP クライアントのリースが更新されます。

DHCP サーバーが明示的に要求を拒否した場合は、DHCP クライアントは引き続き IP アドレスをリース時間満了まで使用でき、それからアドレス要求処理 (同報通信、アドレス要求など) を開始します。サーバーが到達不能になっている場合、クライアントはリースが満了するまで引き続き割り当てられたアドレスを使用できます。

## クライアントの移動

DHCP の利点の 1 つは、クライアント・ホストが新しいサブネットで必要な IP 構成情報を前もって知らなくても、サブネット間を自由に移動できることです。ホストを再配置する先のサブネットが DHCP サーバーにアクセスできるかぎり、DHCP クライアントはこれらのサブネットにアクセスできるように自身を正しく自動構成します。

新しいサブネットにアクセスするために DHCP クライアントを再構成するには、クライアント・ホストをリブートする必要があります。ホストが新しいサブネット上でリスタートすると、DHCP クライアントはアドレスを割り当てた元の DHCP サーバーに対して、以前のリースの更新を試みます。そのアドレスは新しいサブネットでは無効なので、サーバーは要求の更新を拒否します。DHCP サーバーからのサーバー応答や命令を受け取らなかったクライアントは、IP アドレス要求処理を開始して新しい IP アドレスを取得し、ネットワークにアクセスします。

## サーバー・オプションの変更

DHCP を使用すれば、サーバーで変更を行って、サーバーを再初期設定し、該当するクライアントにその変更内容を配布することができます。DHCP クライアントは、リースの期間中は DHCP サーバーによって割り当てられた DHCP オプション値を保存します。クライアントがすでに稼働しているときにサーバーで構成変更を実行した場合、DHCP クライアントはリースの更新を試みるまで、またはリスタートするまでこの変更を処理しません。

**注:** サーバーを再初期設定すると (t 5 `reset dhcp` コマンドを使用して)、DHCP サーバーがリースを更新するまで、ルーターによって表示されていたリース時間の情報は失われます。

### DHCP サーバーの数

必要なサーバーの数は、使用しているサブネットの数、サポートする予定の DHCP クライアントの数、BOOTP リレーを使用するかどうか、および選択するリース時間によって大きく異なります。DHCP プロトコルは現在サーバー間通信を定義していないことに注意してください。このため、サーバーは情報を共有できず、他のサーバーが故障したときに DHCP サーバーを「ホット・バックアップ」として機能させることもできません。DHCP クライアントは、同報通信メッセージを送信します。設計により、同報通信メッセージはサブネットをまたがる境界を超えません。クライアントのメッセージをサブネットの外に転送できるようにするには、BOOTP リレー・エージェントを使用して、DHCP 要求を転送するために追加のルーターを構成する必要があります。そうでなければ、DHCP サーバーをそれぞれのサブネット上で構成する必要があります。

#### 1 台の DHCP サーバー

1 台の DHCP サーバーを使用してサブネット上のホストにサービスを提供する場合は、1 台のサーバーが故障した場合の影響を考慮してください。一般に、サーバーの故障は、ネットワークに参加しようとしている DHCP クライアントだけに影響します。通常、すでにネットワーク上にある DHCP クライアントは、リースが満了するまでは影響なく作動を続行します。ただし、リース時間の短いクライアントは、サーバーがリスタート可能になる前にネットワークへのアクセスを失う可能性があります。サーバーのダウン時間の影響を最小限にするために、サブネットに対して DHCP サーバーを 1 台だけ使用する場合は、十分に長いリース時間を選択して故障した DHCP サーバーにリスタートまたは応答する時間を与える必要があります。

#### 複数の DHCP サーバー

単一障害点を避けるために、同じサブネットに複数の DHCP サーバーがサービスを提供するように構成できます。1 台のサーバーが故障した場合は、他のサーバーがサブネットへのサービスを続行できます。それぞれの DHCP サーバーは、サブネットへの直接接続によって、または BOOTP リレー・エージェントを使用してアクセス可能にする必要があります。

2 台の DHCP サーバーが同じアドレスにサービスを提供することはできないので、サブネットに対して定義されるアドレス・プールは DHCP サーバー間で固有でなければなりません。このため、複数の DHCP サーバーを使用して特定のサブネットにサービスを提供する場合は、そのサブネットの全アドレスのリストをサーバー間で分割する必要があります。たとえば、一方のサーバーは、サブネットの使用可能アドレスの 70% で作動できるアドレス・プールを指定して構成し、他方のサーバーは、使用可能アドレスの残り 30% で作動できるアドレス・プールを指定して構成します。

複数の DHCP サーバーを使用すれば、DHCP 関連のネットワーク・アクセス障害が起こる可能性が減りますが、確実に障害がなくなることはありません。あるサブネットの DHCP サーバーが故障した場合に、他の DHCP サーバーが新しいクライアントからの要求に対応できない場合があります。たとえば、サーバーの限られた使用可能アドレス・プールを使いきってしまうような要求があった場合です。

ただし、どちらの DHCP サーバーがアドレスのプールを最初に使いきってしまうかを偏らせることができます。DHCP クライアントは、オプションを多く提示する DHCP サーバーを選択する傾向があります。70% の使用可能アドレスを持つ DHCP サーバーにサービスを偏らせるには、サブネットの使用可能アドレスの 30% を持つサーバーからは DHCP オプションを少なく提示するようにします。

## BOOTP サーバー

ネットワークに BOOTP クライアントとサーバーがすでにある場合は、BOOTP サーバーを DHCP サーバーに置き換えることも検討できます。DHCP サーバーは、オプションで現行の BOOTP サーバーと同じ IP 構成情報を BOOTP クライアントに提供できます。BOOTP サーバーを DHCP サーバーに置き換えることができず、両方がネットワークにサービスを提供するようにしたい場合は、次の予防策をとることをお勧めします。

- DHCP サーバー内で BOOTP サポートをオフにする。
- BOOTP サーバーと DHCP サーバーが同じアドレスを提供していないことを確認する。
- 適切な BOOTP サーバーと DHCP サーバーの両方に BOOTP 同報通信を転送するように、ルーター内の BOOTP リレー・サポートを構成する。

DHCP サーバーは、BOOTP クライアントに永続 IP アドレスを割り振ります。サブネットの再番号付けによって、BOOTP の割り当てたアドレスが使用できなくなった場合は、BOOTP クライアントを再始動して新しい IP アドレスを取得する必要があります。

## 特殊な DHCP クライアント

次のように、管理用の特殊な用途を持った DHCP クライアントやネットワーク・サーバーを使用できます。

- 永久リース:  
無限のリース時間を指定することによって、指定のホストに永久リースを割り当てることができます。DHCP サーバーは、明示的に要求した BOOTP クライアントにも、BOOTP クライアントのサポートが使用可能になっているかぎり永久リースを割り振ります。DHCP サーバーは、明示的に要求した DHCP ホストにも永久リースを割り振ります。
- 特定の IP アドレス:  
特定のサブネットにある特定の DHCP または BOOTP クライアント・ホストのために、特定のアドレスと構成パラメーターを予約できます。
- 特定の構成パラメーター:  
所属するサブネットに関係なく、クライアントに特定の構成情報を割り振ることができます。
- ワークステーションの手動定義:  
IP ネットワーク・アクセスの構成に DHCP または BOOTP を使用しない既存ホストに対しては、DHCP サブネットからアドレスを明示的に除外する必要があります。DHCP サーバーとクライアントは、IP アドレスの割り振りまたは使用前に、その IP アドレスが使用中でないかどうか自動的に検査しますが、オフになってい



## DHCP サーバーの使用

たり一時的にネットワークから外れたりしている手動定義されたホストのアドレスは検出できません。この場合、そのホストの IP アドレスを明示的に除外しなければ、手動定義されたホストがネットワークに再度アクセスするときに、アドレス重複の問題が起こる場合があります。

## リース時間

デフォルト・リース時間は 24 時間です。DHCP リース時間は、ネットワークの動作とパフォーマンスに影響する可能性があるので注意してください。

- リース時間が短いと、DHCP のリース更新要求が原因で、ネットワーク・トラフィックの量が増えます。たとえば、リース時間を 5 分に設定した場合は、それぞれのクライアントが約 2.5 分ごとに更新要求を送信します。
- リース時間が長すぎると、IP アドレスを再使用する機能が制限されることがあります。さらに、リース時間が非常に長いと、クライアントのリスタート時またはリースの更新時に行われる構成変更が遅れます。

選択するリース時間は、次のようにユーザーのニーズによって大きく異なります。

- 使用可能アドレス数と比較したサポートするホストの数。アドレス数よりホスト数の方が多い場合は、1 ～ 2 時間の短いリース時間を選択すると良いでしょう。こうすれば、未使用のアドレスをできるだけ早くプールに戻すことができます。
- ネットワークの変更に費やすことができる時間。ホストは、リスタート時、またはリースの更新時に、構成情報の変更内容を受け取ります。これらの変更を行うために、タイミングの良い十分な時間枠を割り当ててください。たとえば、通常は夜間に変更を行う場合は、12 時間のリース時間を割り当てます。
- 使用できる DHCP サーバーの数。大規模ネットワークに少数の DHCP サーバーしかない場合は、サーバーのダウン時間の影響を最小限にするために、長いリース時間を選択すると良いでしょう。

ホストのリース要件を組み合わせる必要がある複雑なネットワークの場合は、DHCP クラスを定義できます。

---

## 概念と用語

DHCP サーバーの機能を説明するために、次の概念が使用されています。

### スコープ

スコープという用語は、DHCP サーバー構成を説明する際には、特定のパラメーター値が関係するものを示すために使用されます。481ページの図46は、次のスコープを図示しています。

- グローバル・オプション 1
- グローバル・オプション 3
- グローバル・クラス ClassA

ClassA はオプション 1 を再定義しますが、グローバル・スコープからオプション 3 の値を継承します。

- グローバル・クライアント ClientA

ClientA はオプション 3 を再定義しますが、グローバル・スコープからオプション 1 の値を継承します。

- サブネット SubA
  - オプション 1 を再定義する。
  - グローバル・スコープからオプション 3 の値を継承する。
  - SubA のスコープ内に ClassB を定義する。  
ClassB はオプション 1 の値を再定義しますが、SubA からオプション 3 の値を継承します (これは、グローバル・スコープからも継承されません)。
  - SubA のスコープ内に ClientB を定義する。  
ClientB はオプション 3 を再定義しますが、SubA からオプション 1 の値を継承します。
- ベンダー・オプション vendorA  
ベンダー・オプションは例外です。ベンダー・オプションは独立しており、ベンダー・オプション・スコープの外側からは継承されません。

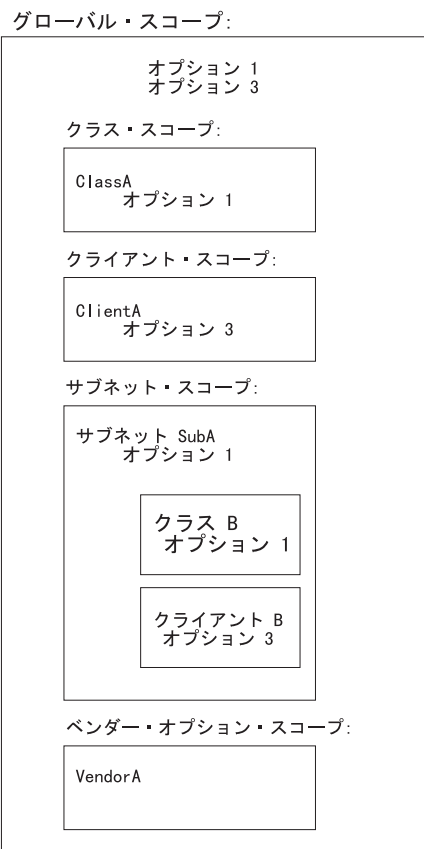


図 46. スコープの概念

### サブネット

サブネットは、DHCP サーバーによって管理されるアドレス・プールのパラメーターを定義します。アドレス・プールは、クライアントにリースする IP アドレスの集まりです。指定できるパラメーターには、リース時間など、アドレス・プールを使用するクライアントに関するオプションが含まれます。リース時間などのオプションは、グローバル・スコープから継承できます。

### サブネット・グループ

サブネット・グループは、同じインターフェース上で一緒にグループ化された複数のサブネットを識別するためのものです。あるグループに含まれるすべてのサブネットに、同じサブネット・グループ名と固有な優先順位が与えられます。優先順位は、グループが関連付けられているアドレス・ポリシーに従ってアドレスを提供する順序を決定するために使用されます。サブネットは、次の 2 つのアドレス・ポリシーのどちらかに属します。

- Inorder

このポリシーはデフォルトです。inorder ポリシーは、最低の優先順位をもつサブネットのアドレスを最初に、最高の優先順位をもつサブネットのアドレスを最後に管理します。

- Balance

balance ポリシーは、定義されたサブネットのグループのアドレスを、ラウンドロビン順序で管理します。最初に管理されるアドレスは、最低の優先順位をもつサブネットのもので、2 番目に管理されるアドレスは、次に低い優先順位をもつサブネットのもので、以降も同様です。最高の優先順位をもつサブネットのアドレスが管理されると、グループ内のすべてのサブネットが全アドレスを使いきるまで、ポリシーは最低の優先順位をもつサブネットに戻ります。

**クラス** クラスは、DHCP サーバーによって管理されるユーザー定義のクライアント・グループのパラメーターを定義します。クラスは、グローバル・スコープまたはサブネット・スコープの下に定義できます。サブネット・スコープ内にクラスを定義した場合、DHCP サーバーは、指定のサブネット内にあって、かつそのクラスを要求したクライアントだけにサービスを提供します。サブネットの範囲内に定義されたクラスだけが、アドレスの範囲を指定できます。範囲としては、サブネット範囲のサブセット、またはサブネット範囲と等しい範囲のどちらも指定できます。範囲を使いきったクラスからの IP アドレスを要求したクライアントは、サブネット範囲からの IP アドレスを提示されます (使用可能ならば)。クライアントは、使いきってしまったクラスに関連したオプションを提示されます。

### クライアント

クライアントは、次の目的で使用できます。

- 特定のエンド・ステーションに対して静的 IP アドレスと DHCP オプションを定義する
- サービスから特定のエンド・ステーションを除外する
- 使用可能な IP アドレスの範囲から IP アドレスを除外する

それぞれのクライアントには、指定されたハードウェア・タイプ、クライアント ID、および IP アドレスがあります。ハードウェア・タイプは、RFC 1340 に定義されており、次に示されています。0 を除くすべてのハードウェア・タイプの場合、クライアント ID はエンド・ステーションのハードウェア・アドレス (または MAC アドレス) です。ハードウェア・タイプ 0 の場合、クライアント id は文字列です。通常、これはドメイン名です。

クライアントを定義する際に、IP アドレス、*any*、または *none* のどちらかを尋ねるプロンプトが出されます。IP アドレスを定義すると、その IP アドレスはそのクライアント用に予約されます。*any* を選択した場合、そのクライア



ントにはそのサブネット内で使用可能な任意の IP アドレスが与えられます。同じサブネット内に、それぞれ固有な範囲をもつ複数のサブネット・レコードがある場合、*any* を指定して構成されたクライアントは、サブネット内で使用可能な最初のアドレスを取得します。このアドレスは、必ずしもクライアントが定義されている特定のサブネット・レコードの範囲にあるとは限りません。*none* を選択した場合は、そのエンド・ステーションには IP アドレスはまったく提供されません。IP アドレスを管理対象から除外するには、ハードウェア・タイプとクライアント ID を 0 に指定したクライアント・レコードを定義します。

RFC1340 によって定義されていて、IBM 2212 に関係のあるハードウェア・タイプは、次のとおりです。

ハードウェア・タイプ	値
-----	-----
予約済み	0
イーサネット	1
IEEE 802 ネットワーク (トークンリングなど)	6

完全なリストについては、RFC 1340 を参照してください。

---

## DHCP サーバーとリースのパラメーター

グローバル・レベルで、次の DHCP サーバー・パラメーターを定義できます。

- bootstrapservers
- canonical
- lease expire interval
- lease time default
- ping time
- support unlisted clients
- support bootp
- used ip address expire interval

これらのパラメーターについての説明は、525ページの『Set』を参照してください。

---

## DHCP オプション

DHCP では、クライアントに追加の構成情報を提供するオプションを指定できます。オプションは、RFC 2132 とその他のさまざまな RFC に定義されています。

### オプションの形式

すべてのオプションの構成データは、次の形式のどれか 1 つに従っている必要があります。

形式	定義
IP アドレス	小数点表記法による単一の IP アドレス。
複数の IP アドレス	空白で区切られた、小数点表記法による 1 つまたは複数の IP アドレス。

## DHCP サーバーの使用

IP アドレス・ペア	空白で区切られた、小数点表記法による 2 つの IP アドレス。
複数の IP アドレス・ペア	それぞれのペア間が空白によって区切られた、1 つまたは複数の IP アドレス・ペア。
ブール	0 または 1 (真または偽)。
バイト	-128 ~ 127 (両極の値を含む) の 10 進数。
符号なしバイト	0 ~ 255 (両極の値を含む) の 10 進数。符号なしバイトに負の値を指定することはできません。
符号なしバイトのリスト	空白で区切られた、1 つまたは複数の 0 ~ 255 (両極の値を含む) の 10 進数。符号なしバイトに負の数値を指定することはできません。
ショート (メッセージ長)	-32768 ~ 32767 (両極の値を含む) の 10 進数。
符号なしショート (メッセージ長)	0 ~ 65535 (両極の値を含む) の 10 進数。符号なしショート (メッセージ長) に負の数値を指定することはできません。
符号なしショート (メッセージ長) のリスト	空白で区切られた、1 つまたは複数の 0 ~ 65535 (両極の値を含む) の 10 進数。符号なしショート (メッセージ長) に負の数値を指定することはできません。
ロング (メッセージ長)	-2147483648 ~ 2147483647 (両極の値を含む) の 10 進値。
符号なしロング (メッセージ長)	0 ~ 4294967295 (両極の値を含む) の 10 進数。符号なしロング (メッセージ長) に負の数値を指定することはできません。
文字列	一連の文字。
N/A	クライアントがこの情報を生成するので、指定は不要であることを示します。

それぞれの DHCP オプションは、数字コードで識別されます。

設計済みオプション 0 ~ 127 とオプション 255 は、RFC による定義用に予約済みです。DHCP サーバー、DHCP クライアント、またはサーバーとクライアントの両方が、この中のオプションを使用します。設計済みオプションの一部は、管理者が変更できます。その他のオプションは、クライアントとサーバー専用です。

**注:** 既知の形式をもつ設計済みオプションに対しては、16 進値は使用できません。

管理者が DHCP サーバーで構成できない、または構成してはならないオプションには、次のものがあります。

- 52 オプション・オーバーロード
- 53 DHCP メッセージ・タイプ

- 54 サーバー ID
- 55 パラメーター要求リスト
- 56 メッセージ
- 57 最大 DHCP メッセージ・サイズ
- 60 クラス ID

オプション 128 ~ 254 はユーザー定義オプションで、管理者が DHCP クライアントに情報を渡すために定義して、サイト固有の構成パラメーターを設定できます。

IBM は、オプション 192: TXT RR など IBM 固有の一連のオプションを追加で提供しています。

ユーザー定義オプションの形式は次のとおりです。

構文:

**option**            *code value*

ただし、

**code** 1 ~ 254 の任意のオプション・コード (すでに RFC で定義されているコードを除く)。

**value** 必ず文字列でなければなりません。サーバー側では、これは ASCII 文字列または 16 進数文字列のどちらかです。ただしクライアント側では、これは処理プログラムに渡された 16 進数文字列として常に表示されます。

サーバーは、指定された値をクライアントにパスします。ただし、値を処理するためには、プログラムまたはコマンド・ファイルを作成する必要があります。

## クライアントに対して提供されている基本オプション

次の基本オプションがクライアントに対して提供されています。構成形式については、483ページの『オプションの形式』を参照してください。

- 1 **サブネット・マスク** このオプションは、DHCP サーバーだけで指定されます。32 ビット小数点表記法で指定されるクライアントのサブネット・マスク。必須ではありませんが、ほとんどの構成で DHCP サーバーはオプション 1 (サブネット・マスク) を DHCP クライアントに送信する必要があります。クライアントが DHCP サーバーからサブネット・マスクを受け取らず、サブネットに適切でないサブネット・マスクを想定した場合、クライアントの動作は予期できなくなります。指定されなかった場合、クライアントは次のデフォルト・サブネット・マスクを使用します。

- クラス A ネットワーク 255.0.0.0
- クラス B ネットワーク 255.255.0.0
- クラス C ネットワーク 255.255.255.0

オプション形式: 複数の IP アドレス

- 2 **時刻オフセット** このオプションは、DHCP サーバーだけで指定されます。クライアントのサブネットの、協定世界時 (CUT) からのオフセット (秒)。オフセットは符号付き 32 ビット整数です。

## DHCP サーバーの使用

オプション形式: ロング (メッセージ長)

- 3 ルーター** このオプションは、DHCP サーバーだけで指定されます。クライアントのサブネットにあるルーターの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 4 時刻サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる時刻サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 5 ネーム・サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる IEN 116 ネーム・サーバーの IP アドレス (優先順)。

**注:** これは、ドメイン名サーバーのオプションではありません。ドメイン名サーバーを指定するには、オプション 6 を使用します。

オプション形式: 複数の IP アドレス

- 6 ドメイン名サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できるドメイン・ネーム・システムの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

**注:** PPP インターフェース上で動的アドレスが構成されている場合は、インターネット・サービス・プロバイダー (ISP) の IPCP を使用して、1 次と 2 次の DNS アドレスを検索できます。オプション 6 でこれらの DNS アドレスを DHCP クライアントにパスするには、動的アドレス・インターフェースに対応する無番号の IP インターフェース・アドレス (0.0.0.n など) を構成する必要があります。DHCP サーバーは、クライアントが要求を送信すると、この値を検索されたアドレスに変換します。DHCP クライアントが、PPP インターフェースがアクティブになる前にサーバーから構成情報を要求した場合は、検索された DNS アドレスを受け取るために、クライアントはリスタートするか、リースを更新する必要があります。

- 7 ログ・サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる MIT-LCS UDP ログ・サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 8 Cookie サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる Cookie (あるいは quote-of-the-day サーバー) の IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 9 LPR サーバー** このオプションは、DHCP クライアントと DHCP サーバーの両方で指定できます。ただし、DHCP クライアントだけで指定した場合、構成は不完全になります。クライアントが使用できるライン・プリンター・サーバーの IP アドレス (優先順)。オプション 9 を使用すると、クライアントが LPR\_SERVER 環境変数を指定する必要がなくなります。

オプション形式: 複数の IP アドレス

- 10 **Impress サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる Imagen Impress サーバーの IP アドレス (優先順)。オプション形式: 複数の IP アドレス
- 11 **リソース・ロケーション・サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できるリソース・ロケーション (RLP) サーバーの IP アドレス (優先順)。RLP サーバーを使用すると、クライアントはドメイン名サーバーなど、指定のサービスを提供するリソースを見付けることができます。オプション形式: 複数の IP アドレス
- 12 **ホスト名** このオプションは、DHCP クライアントと DHCP サーバーの両方で指定できます。DHCP クライアントがホスト名を指定しない場合、DHCP サーバーはオプション 12 を無視します。クライアントのホスト名 (ローカル・ドメイン名を含む場合もある)。ホスト名の最小の長さは 1 オクテットで、最大の長さは 32 文字です。文字セットの制約事項については、RFC 1035 を参照してください。オプション形式: 文字列
- 13 **ブート・ファイル・サイズ** このオプションは、DHCP サーバーだけで指定されます。クライアントのデフォルト・ブート構成ファイルの長さ (512 オクテット・ブロック単位)。オプション形式: 符号なしショート (メッセージ長)
- 14 **メリット・ダンプ・ファイル** このオプションは、DHCP サーバーだけで指定されます。クライアントがクラッシュした場合に、クライアントのコア・イメージを保管するメリット・ダンプ・ファイルのパス名。パスの形式は、ネットワーク・バーチャル端末 (NVT) ASCII 文字セットの文字で構成される文字列です。最小長さは 1 オクテットです。オプション形式: 文字列
- 15 **ドメイン名** このオプションは、DHCP クライアントと DHCP サーバーの両方で指定されます。DHCP サーバーでオプション 15 に値を指定しない場合、クライアントはオプション 12 (ホスト名) とオプション15 (ドメイン名) に値を指定する必要があります。このステートメントは、グローバル・スコープ内で指定するか、サブネット、クラス、またはクライアントのスコープ内で指定できます。オプション形式: 文字列
- 16 **スワップ・サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントのスワップ・サーバーの IP アドレス。オプション形式: IP アドレス
- 17 **ルート・パス** このオプションは、DHCP サーバーだけで指定されます。クライアントのルート・ディスクがあるパス。パスの形式は、NVT ASCII 文字セットの文字で構成される文字列です。最小長さは 1 オクテットです。オプション形式: 文字列
- 18 **拡張パス** このオプションは、DHCP サーバーだけで指定されます。拡張パ

## DHCP サーバーの使用

ス・オプションは、トリビアル・ファイル転送プロトコル (TFTP) を使用して検索できるファイルの識別に使用できる文字列を指定します。最小の長さは 1 オクテットです。

オプション形式: 文字列

## ホストに対する IP レイヤー・パラメーターのオプション

- 19 IP 転送** このオプションは、DHCP サーバーだけで指定されます。IP レイヤー・パケットのクライアントによる転送を使用可能 (1) または使用不可 (0) にします。

オプション形式: ブール

- 20 非ローカル・ソース・ルーティング** このオプションは、DHCP サーバーだけで指定されます。非ローカル・ソース・ルートを用いた IP レイヤー・データグラム of クライアントによる転送を使用可能 (1) または使用不可 (0) にします。

オプション形式: ブール

- 21 ポリシー・フィルター** このオプションは、DHCP サーバーだけで指定されます。IP アドレスとネット・マスクのペアは、非ローカル・ソース・ルートを用いたデータグラムをフィルターに掛けるために使用されます。ネクスト・ホップ・アドレスがフィルター・ペアのどれとも一致しないデータグラムは、クライアントによって廃棄されます。ポリシー・フィルター・オプションの最小長さは、8 オクテットです。

オプション形式: 複数の IP アドレス・ペア

- 22 最大データグラム再組み立てサイズ** このオプションは、DHCP サーバーだけで指定されます。クライアントが再組み立てするデータグラムの最大サイズ。最小値は 576 です。

オプション形式: 符号なしショート (メッセージ長)

- 23 デフォルト IP 存続時間** このオプションは、DHCP サーバーだけで指定されます。クライアントが発信データグラムに対して使用するデフォルト存続時間 (TTL)。TTL は、1 ~ 255 の値をもつオクテットです。

オプション形式: 符号なしバイト

- 24 パス MTU エージング・タイムアウト** このオプションは、DHCP サーバーだけで指定されます。RFC 1191 に記述されているメカニズムによって検出されるパス最大伝送単位 (MTU) のエージングに使用されるタイムアウト (秒)。

オプション形式: 符号なしロング (メッセージ長)

- 25 パス MTU プラトール・テーブル** このオプションは、DHCP サーバーだけで指定されます。RFC 1191 で定義されているパス MTU ディスカバリーで要求する MTU サイズのテーブル。最小 MTU 値は 68 です。パス MTU プラトール・テーブル・オプションの最小の長さは 2 オクテットです。長さは 2 の倍数でなければなりません。

オプション形式: 符号なしショート (メッセージ長)



## インターフェースに対する IP レイヤー・パラメーターのオプション

- 26 **インターフェース MTU** このオプションは、DHCP サーバーだけで指定されます。このインターフェースに対して要求する最大伝送単位 (MTU)。最小 MTU 値は 68 です。  
オプション形式: 符号なしショート (メッセージ長)
- 27 **全サブネットがローカル** このオプションは、DHCP サーバーだけで指定されます。クライアントは、すべてのサブネットが同じ最大伝送単位 (MTU) を使用することを前提とする (1) か、前提としません (0)。値 0 を指定すると、クライアントは一部のサブネットの MTU が小さいことを前提とします。  
オプション形式: ブール
- 28 **同報通信アドレス** このオプションは、DHCP サーバーだけで指定されます。クライアントのサブネットで使用される同報通信アドレス。  
オプション形式: IP アドレス
- 29 **マスク・ディスカバリーの実行** このオプションは、DHCP サーバーだけで指定されます。クライアントは、インターネット制御メッセージ・プロトコル (ICMP) を使用してサブネット・マスクのディスカバリーを実行する (1) か、実行しません (0)。  
オプション形式: ブール
- 30 **マスク提供** このオプションは、DHCP サーバーだけで指定されます。クライアントは、インターネット制御メッセージ・プロトコル (ICMP) を使用してサブネット・マスクの要求に応答する (1) か、応答しません (0)。  
オプション形式: ブール
- 31 **ルーター・ディスカバリーの実行** このオプションは、DHCP サーバーだけで指定されます。クライアントは、RFC 1256 に定義されているルーター・ディスカバリーを使用してルーターを送信請求する (1) か、送信請求しません (0)。  
オプション形式: ブール
- 32 **ルーター勧誘アドレス** このオプションは、DHCP サーバーだけで指定されます。クライアントがルーター送信請求の要求を送信するアドレス。  
オプション形式: IP アドレス
- 33 **静的ルート** このオプションは、DHCP サーバーだけで指定されます。クライアントがルーティング・キャッシュにインストールする静的ルート (優先順のあて先アドレスとルーターのペア)。最初のアドレスはあて先アドレスで、2 番目のアドレスはあて先に対するルーターです。デフォルト・ルートあて先として 0.0.0.0 を指定しないでください。  
オプション形式: 複数の IP アドレス・ペア

## インターフェースに対するリンク・レイヤー・パラメーターのオプション

- 34 **トレーラー・カプセル化** このオプションは、DHCP サーバーだけで指定されます。クライアントは、アドレス解決プロトコル (ARP) を使用する際に、ト

## DHCP サーバーの使用

レーラーの使用をネゴシエーションする (1) か、ネゴシエーションしません (0)。詳しくは、RFC 893 を参照してください。

オプション形式: ブール

- 35 ARP キャッシュ・タイムアウト** このオプションは、DHCP サーバーだけで指定されます。アドレス解決プロトコル (ARP) キャッシュ・エントリーのタイムアウト (秒)。

オプション形式: 符号なしロング (メッセージ長)

- 36 イーサネット・カプセル化** このオプションは、DHCP サーバーだけで指定されます。イーサネット・インターフェースに対して、クライアントは RFC 1042 に記述されている IEEE 802.3 (1) イーサネット・カプセル化、または RFC 894 に記述されているイーサネット V2 (0) カプセル化を使用します。

オプション形式: ブール

## TCP パラメーター・オプション

- 37 TCP デフォルト TTL** このオプションは、DHCP サーバーだけで指定されます。クライアントが TCP セグメントの送信に使用するデフォルト存続時間 (TTL)。

オプション形式: 符号なしバイト

- 38 TCP キープアライブ間隔** このオプションは、DHCP サーバーだけで指定されます。TCP 接続に対してキープアライブ・メッセージを送信する前に、クライアントが待機する間隔 (秒)。値 0 は、アプリケーションによって要求されるまで、クライアントはキープアライブ・メッセージを送信しないことを指示します。

オプション形式: 符号なしロング (メッセージ長)

- 39 TCP キープアライブ不要情報** このオプションは、DHCP サーバーだけで指定されます。クライアントは、以前のインプリメンテーションとの互換性のために、不要情報のオクテットを含む TCP キープアライブ・メッセージを送信する (1) か、送信しません (0)。

オプション形式: ブール

## アプリケーションおよびサービス・パラメーターのオプション

- 40 ネットワーク情報サービス・ドメイン** このオプションは、DHCP サーバーだけで指定されます。クライアントのネットワーク情報サービス (NIS) ドメイン。ドメインの形式は、NVT ASCII 文字セットの文字で構成される文字列です。最小の長さは 1 オクテットです。

オプション形式: 文字列

- 41 ネットワーク情報サービス・ドメイン** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できるネットワーク情報サービス (NIS) サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 42 ネットワーク・タイム・プロトコル・サーバー** このオプションは、DHCP サ



サーバーだけで指定されます。クライアントが使用できるネットワーク・タイム・プロトコル (NTP) サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

**43 ベンダー固有情報** オプション 43 は、DHCP サーバーだけで指定され、サーバーはオプション 60 (クラス ID) を送信するクライアントにこのオプションを戻します。この情報オプションは、クライアントとサーバーがベンダー固有情報 (ベンダー・オプション定義で指定された) を交換するために使用します。ベンダー・オプションをカプセル化するためにオプション 43 を使用する際には、次の考慮事項があります。

- さまざまなベンダーのクライアントとサーバー間の相互運用を可能にするために、各ベンダーは RFC 2132 の標準形式を使用して、オプション 43 の内容を明確に文書化する必要があります。
- 各ベンダーは、オプション 43 にカプセル化できる個々のオプションを、別のベンダーの DHCP サーバーが簡単に設定できる形式で指定する必要があります。たとえば、ベンダーは次のことを行う必要があります。
  - DHCP オプションに対してすでに定義されているデータ・タイプ、またはその他のよく定義されたデータ・タイプのどちらかで、これらのオプションを表現する。
  - 他のベンダーが提供するサーバーとの交換のために、構成ファイル内に容易にコード化できるオプションを選択する。
  - すべてのサーバーが容易にサポートできるようにする。

クライアントから送信されたベンダー固有の情報を解釈できないサーバーは、その情報を無視する必要があります。必要なベンダー固有情報を受け取ることができないクライアントは、ベンダー固有情報なしでの動作を試みる必要があります。このオプションについて詳しくは、RFC 2131 と RFC 2132 を参照してください。

**注:** これらの考慮事項があるため、IBM は IBM 固有のオプション用に代わりに 192 と 200 を使用しています。

オプション形式: 文字列

**44 NetBIOS over TCP/IP ネーム・サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる NetBIOS ネーム・サーバー (NBNS) の IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

**45 NetBIOS over TCP/IP データグラム配布サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる NetBIOS データグラム配布 (NBDD) ネーム・サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

**46 NetBIOS over TCP/IP タイプ** このオプションは、DHCP サーバーだけで指定されます。RFC 1001 と RFC 1002 に記述されている、NetBIOS over TCP/IP 構成可能クライアント用に使用されるノード・タイプ。クライアント・タイプを指定するための値には、次のものがあります。

- 0x1 B ノード

## DHCP サーバーの使用

- 0x2 P ノード
- 0x4 M ノード
- 0x8 H ノード

オプション形式: 符号なしバイト

- 47 NetBIOS over TCP/IP スコープ** このオプションは、DHCP サーバーだけで指定されます。クライアントに対する NetBIOS over TCP/IP スコープ・パラメーター (RFC 1001/1002 に指定)。最小の長さは 1 オクテットです。

オプション形式: 符号なしバイト

- 48 X Window システム・フォント・サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる X Window システム・フォント・サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 49 Window システム・ディスプレイ・マネージャー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる X Window システム・ディスプレイ・マネージャーを実行するシステムの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

## DHCP 拡張オプション

- 50 要求 IP アドレス** このオプションは、DHCP サーバーだけで指定されます。DHCP サーバーは、特定の IP アドレスに対する DHCP クライアントの要求を拒否できます。クライアントが特定の IP アドレスを要求 (DHCPDISCOVER) できるようにします。

オプション形式: N/A

- 51 IP アドレス・リース時間** このオプションは、DHCP クライアントと DHCP サーバーの両方で指定できます。DHCP クライアントは、オプション 51 を使用して、DHCP サーバーが提示した defaultLeaseInterval 値をオーバーライドできます。クライアントが IP アドレスに対してリース時間を要求 (DHCPDISCOVER または DHCPREQUEST) できるようにします。応答 (DHCPOFFER) の中で、DHCP サーバーはこのオプションを使用してリース時間を提示します。このオプションは、グローバル、サブネット、クラス、またはクライアントの範囲内で指定できます。無限の (永久) リースを指定するには、X'ffffffff' を使用します。

オプション形式: 符号なしロング (メッセージ長)

- 58 更新 (T1) 時間値** このオプションは、DHCP サーバーだけで指定されます。サーバーがアドレスを割り当てる時刻と、クライアントが更新状態に移行する時刻との間の間隔 (秒)。

オプション形式: 符号なしロング (メッセージ長)

- 59 再バインド (T2) 時間値** このオプションは、DHCP サーバーだけで指定されます。サーバーがアドレスを割り当てる時刻と、クライアントが再バインド状態に入る時刻との間の間隔 (秒)。

オプション形式: 符号なしロング (メッセージ長)

- 60 **クラス ID** このオプションは、DHCP サーバーだけで指定されます。この情報は、クライアントによって生成されるもので、指定する必要はありません。クライアントによってサーバーに提供される、クライアントのタイプと構成。たとえば、ID はクライアントのベンダー固有のハードウェア構成をコード化します。情報は、サーバーによって解釈される  $n$  オクテットの列です。(例: hex: X'01' X'02' X'03'.) クライアントから送信されたクラス固有の情報を解釈する装備がないサーバーは、その情報を無視する必要があります。最小の長さは 1 オクテットです。
- オプション形式: N/A
- 61 **クライアント ID** このオプションは、DHCP クライアントと DHCP サーバーの両方で指定できます。DHCP クライアントは、オプション 61 を使用して、固有なクライアント ID を指定できます。DHCP サーバーは、オプション 61 を使用して、アドレス・バインドのデータベースに索引を付けることができます。この値は、管理ドメイン内のクライアントすべてに対して固有であることが要求されます。
- オプション形式: 文字列
- 62 **NetWare/IP ドメイン名** このオプションは、DHCP サーバーだけで指定されます。Netware/IP ドメイン名。最小の長さは 1 オクテット、最大の長さは 255 です。
- オプション形式: 文字列
- 63 **NetWare/IP** このオプションは、DHCP サーバーだけで指定されます。NetWare/IP ドメイン名を除くすべての NetWare/IP 関連情報を伝達するために使用される汎用オプション・コード。NetWare/IP サブオプションの数は、このオプション・コードを使用して伝達されます。最小の長さは 1、最大の長さは 255 です。
- オプション形式: 文字列
- 64 **NIS ドメイン名** このオプションは、DHCP サーバーだけで指定されます。ネットワーク情報サービス (NIS)+ V3 クライアント・ドメイン名。ドメインの形式は、NVT ASCII 文字セットの文字で構成される文字列です。最小の長さは 1 です。
- オプション形式: 文字列
- 65 **NIS サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できるネットワーク情報サービス (NIS)+ V3 サーバーの IP アドレス (優先順)。
- オプション形式: 複数の IP アドレス
- 66 **サーバー名** このオプションは、DHCP サーバーだけで指定されます。DHCP ヘッダーの『sname』フィールドが DHCP オプションに対して使われた場合に使用されるトリビアル・ファイル転送プロトコル (TFTP) サーバー名。
- オプション形式: 文字列
- 67 **ブート・ファイル名** このオプションは、DHCP サーバーだけで指定されます。DHCP ヘッダーの file フィールドが DHCP オプションに対して使われた場合のブート・ファイルの名前。最小の長さは 1 です。

**注:** このオプションは、ブート・ファイル名を DHCP クライアントにパスするためを使用します。ブート・ファイル名は、完全修飾パス名を含んでいる必要があり、128 文字より短くなければなりません。(例: オプション 67 c:\path\boot\_file\_name。)このファイルには、BOOTP 応答内の 64 オクテットのベンダー拡張フィールドと同じ方法で解釈できる情報が含まれていますが、ファイルの長さが BootP ヘッダーによって 128 文字に制限されている点が異なります。

オプション形式: 文字列

- 68 ホーム・アドレス** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できるモバイル IP ホーム・エージェントの IP アドレス (優先順)。このオプションを使用すると、モバイル・ホストがモバイル・ホーム・アドレスを得ることができ、ホーム・ネットワークのサブネット・マスクを判別できます。通常の長さは 4 オクテットで、単一のホーム・エージェントのホーム・アドレスが入っていますが、長さをゼロにすることもできます。ゼロの長さは、ホーム・エージェントが使用できないことを示します。

オプション形式: 複数の IP アドレス

- 69 SMTP サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる SMTP サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 70 POP3 サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる POP サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 71 NNTP サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる NNTP サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 72 WWW サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる WWW サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 73 Finger サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる Finger サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 74 IRC サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できるインターネット・リレー・チャット (IRC) サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 75 StreetTalk サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる StreetTalk サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 76 STDA サーバー** このオプションは、DHCP サーバーだけで指定されます。クライアントが使用できる StreetTalk Directory Assistance (STDA) サーバーの IP アドレス (優先順)。

オプション形式: 複数の IP アドレス

- 77 ユーザー・クラス** このオプションは、DHCP サーバーだけで指定されます。DHCP クライアントは、オプション 77 を使用して、ホストがメンバーになっているクラスを DHCP サーバーに示します。DHCP サーバーでそのクラスに対して定義されたパラメーターを受け取るには、オプション 77 の値として \DHCPD.CFG ファイルにユーザー・クラスを手作業で入力する必要があります。DHCPD.CFG ファイルは、ONDEMAND\SERVER\ETC ディレクトリーにあります。

オプション形式: 文字列

- 78 ディレクトリー・エージェント** このオプションは、DHCP サーバーだけで指定されます。動的ホスト構成プロトコルは、TCP/IP ネットワーク上のホストに構成パラメーターをパスするためのフレームワークです。サービス・ロケーション・プロトコルを使用するエンティティーは、メッセージをやり取りするために、ディレクトリー・エージェントのアドレスを知る必要があります。場合によっては、サービス・ロケーション・プロトコルを使用して交換するサービス属性および URL と関連して使用する正しいスコープと命名機関を知る必要があります。ディレクトリー・エージェントには特定のスコープがあり、特定の命名機関によって定義されたスキームに関する知識を備えている場合もあります。

オプション形式: IP アドレス

- 79 サービス・スコープ** このオプションは、DHCP サーバーだけで指定されます。この拡張オプションは、サービス・ロケーション・プロトコルによって指定されたサービス要求メッセージに応答する際に、サービス・エージェントが使用すべきスコープを指示します。

オプション形式: 文字列

- 80 命名機関** このオプションは、DHCP サーバーだけで指定されます。この拡張オプションは、命名機関を指示します。命名機関は、サービス・ロケーション・プロトコルを備えたエンティティーによって使用される URL に使用できるスキームの構文を指定します。

オプション形式: 文字列

## IBM 固有のオプション

IBM は、ユーザー定義範囲 (128 ~ 254) 内にオプションを定義して、IBM 固有のオプションのセットを提供しています。これらのオプションは、IBM のベンダー・オプション (オプション 43) を定義する代わりに使用されます。これらのオプションは再定義しないことをお勧めします。

- 192 TXT RR** DHCP サーバーでこのオプションを指定した場合、DHCP クライアントのユーザーは、システム管理者情報フィールドへの入力を要求されません。



## DHCP サーバーの使用

**注:** このオプションは、OS/2 クライアント用の TCP/IP バージョン 4.1 だけがサポートしています。このオプションを使用すると、4 つまでの必須テキスト・ラベルまたは入力フィールド (ユーザーの名前、ユーザーの電話番号など、DDNS クライアント構成プログラムがユーザーに尋ねるフィールド) をシステム管理者が指定できます。これらのフィールドによって、システム管理者はホスト名などのデータを実際に構成した人を識別できます。DDNS 構成プログラムは、システム管理者が指定しないかぎり、これらのフィールドを表示しません。この情報は、DNS 内のテキスト・レコードに保管されます。フィールド・ラベルとデータのペアは、1 つの TXT 資源レコードに収まる必要があります。使用可能なスペースは、ペア間で均等に分割されます。値は、動的アドレス・クライアントのファイル DDNSCLI.CFG でも更新されます。

オプション形式: 文字列

## ベンダー・オプション

DHCP プロトコルは、RFC 設計済みオプション 43 と 60 を使用して、ベンダー固有の情報を DHCP クライアントに提供する手段を提供しています。

**60** オプション 60 は、クライアントが特定のベンダー製のものであることを示すために、DHCP クライアントで構成され、DHCP サーバーに送信されます。

**43** オプション 43 は、DHCP サーバーで構成され、クライアントのオプション 60 要求に回答してクライアントに戻すベンダー固有情報を定義します。共通コード DHCP サーバーの場合、オプション 43 は `add vendor-option` コマンドを使用して構成されます。ベンダー・オプションは、グローバル・スコープ内だけで定義されます。ベンダー・オプションは、ベンダーの名前とオプション・データで構成されます。オプション・データには次の 2 形式があります。

### 16 進データ

`add vendor-option` コマンドを出すときに、ベンダー名とともに入力されます。16 進データは、バイト間に空白を入れた 16 進文字列として入力する必要があります (『01 AA 55』)。

### オプション

`add option` コマンドによって、ベンダー・オプション・スコープに任意の DHCP オプションを追加できます。

**注:** 16 進データとオプションは、ベンダー定義内で排他的に定義されます。どちらか一方を定義できますが、両方はできません。

---

## DHCP 用の IP の構成

追加されたサブネット上のクライアントに対して、DHCP サーバーが IP アドレスと構成情報を正常に割り当てるためには、IP を適切に構成する必要があります。このことは、サポート対象として構成されているサブネットに DHCP サーバーが直接接続されている場合に必要になります。

BOOTP リレー・エージェントを使用してこの DHCP サーバーに DHCP 要求メッセージを転送している場合は、サーバーに直接接続されていないサブネットをサポートするために必要な IP 構成はありません。

## IP アドレスの追加

接続中のインターフェースには、DHCP 構成済みサブネット内にある IP アドレスを追加する必要があります。そのインターフェースに複数のアドレスが定義されている場合、DHCP に追加するアドレスは最後に追加されたものでなければなりません。IP は、そのインターフェースで最初に検出されたアドレスにメッセージが着信した場合と同様に、同報通信 DHCP DISCOVER メッセージをサーバーに提示するだけです。

**注:** インターフェースで最初に検出されるアドレスは、インターフェースに最後に追加されたアドレスです。

例:

- DHCP は、サブネットを次のように追加しました。

```
DHCP Server config>list subnet all
subnet      subnet      subnet      starting    ending
name        address     mask        IP Addr     IP Addr
-----
net-one     192.168.8.0 255.255.255.0 192.168.8.2 192.168.8.50
```

- IP は次を必要とします。

```
IP config>add address
Which net is this address for [0]? 0
New address []? 192.168.8.1
Address mask [255.255.255.0]?
```

```
IP config>list add
IP addresses for each interface:
intf  0  192.168.8.1  255.255.255.0  Local wire broadcast, fill 1
intf  1  IP disabled on this interface
intf  2  0.0.0.2      255.255.255.255  Local wire broadcast, fill 1
intf  3  IP disabled on this interface
```

## IP シンプル・インターネット・アクセスの使用

IP 内でシンプル・インターネット・アクセスが使用可能になっていて、DHCP がまだ構成されていない場合は、DHCP サーバー内に次の構成が自動的に生成されます。シンプル・インターネット・アクセスは、NAT 機能やその他の IP フィルターとアクセス制御も自動的に構成します。DHCP がすでに構成済みの場合は、DHCP 構成に変更/追加はありません。詳細と制約事項については、[プロトコル構成および監視 参照資料 第 1 巻の『IP の使用』の章にあるシンプル・インターネット・アクセスの使用を参照してください。](#)

- IP が次のように構成された場合:

```
IP config>enable simple-internet-access
Interface to Service Provider [0]? 3
SIMPLE-INTERNET-ACCESS enabled on interface 3
```

```
IP config>add address
Which net is this address for [0]? 0
New address []? 192.168.8.1
Address mask [255.255.255.0]?
```

## DHCP サーバーの使用

```
IP config>list add
IP addresses for each interface:
intf    0  192.168.8.1      255.255.255.0  Local wire broadcast, fill 1
intf    1
intf    2
intf    3  0.0.0.3              255.255.255.255  Local wire broadcast, fill 1
                                           SIMPLE-INTERNET-ACCESS Enabled
```

- DHCP サーバーには次の構成が生成されます。

```
DHCP Server config> list global
.
.
DHCP Server enabled: Yes
.
.
DHCP Server config>list subnet all
subnet      subnet      subnet      starting      ending
name        address      mask        IP Addr       IP Addr
-----
simple-net   192.168.8.0  255.255.255.0  192.168.8.2   192.168.8.50

DHCP Server config> list option subnet
Enter the subnet name []? simple-net
option      option
code        data
-----
1           255.255.255.0
3           192.168.8.1
6           0.0.0.3
```

---

## DHCP サーバーのサンプル構成

### ASCII テキスト・ファイル

ここでは、ASCII テキスト形式の代表的な DHCP サーバー構成を示します。この例は、ユーザーに分かりやすい形式で構成を示すための例示用のものに過ぎません。IBM 2212 は ASCII 構成をサポートしません。

ブロック番号 (**1**) を使用すれば、この ASCII 例で説明する機能を、499ページの『OPCON (Talk 6) 構成』に説明する同等な talk 6 構成と関連付けることができます。

#### **1** サーバー・パラメーターの構成

```
leaseTimeDefault      120                # 120 minutes
leaseExpireInterval   20 seconds
supportBOOTP          yes
supportUnlistedClients yes
```

**2** グローバル・オプション。低位のスコープでオーバーライドされないかぎり、すべてのクライアントに渡されます。

```
option 15      "raleigh.ibm.com"      # domain name
option 6       9.67.1.5          # dns server
class manager
{
  option 48    6.5.4.3
  option 9     9.37.35.146
  option 210   "manager_authority" # site specific option given to all managers
}
```



**3** ベンダー・オプション

```

vendor XI-clients hex"01 02 03"
vendor XA-clients
{
  option 23 100 # IP TTL
}

```

**4** 代表的なサブネット

```

subnet 9.2.23.0 255.255.255.0 9.2.23.120-9.2.23.126
{
  option 28 9.2.23.127 # broadcast address
  option 9 5.6.7.8
  option 51 200
}

```

**5** サブネット・スコープで定義されたクラス・マネージャー。  
このオプション 9 は、グローバル・マネージャー・クラスで指定された  
オプション 9 をオーバーライドします。

```

class manager
{
  option 9 9.2.23.98
}

```

**6** プログラマーが独自のサブネット範囲を所有している

```

class developers 9.2.23.125-9.2.23.126
{
  option 51 -1 # infinite lease.
  option 9 9.37.35.1 # printer used by the developers
}
}

```

**7** 任意のアドレスを受け入れるが、固有のオプションのセットを  
持つクライアントの例。

```

client 6 0x10005aa4b9ab ANY
{
  option 51 999
  option 1 255.255.255.0
}

```

**8** サービスからアドレスを除外する。

```

client 0 0 9.2.23.121

```

**OPCON (Talk 6) 構成**

次は、talk 6 を使用した同じ構成の例です。

**1** サーバー・パラメーターの構成

```

Config>f dhcp-server
DHCP server user configuration
DHCP Server config> enable dhcp
DHCP Server config>
DHCP Server config> set lease-time-default hours 2
DHCP Server config>set lease-expire-interval seconds 20
DHCP Server config>set support-bootp yes
DHCP Server config>set support-unlisted-clients global yes

```

```

DHCP Server config>li glob
DHCP server Global Parameters
=====

```

```

DHCP server enabled: Yes

```

## DHCP サーバーの使用

```
Balance: No subnet groups defined
Inorder: No subnet groups defined
Canonical: No
Lease Expire Interval: 20 second(s)
Lease Time Default: 2 hour(s)

Support BOOTP Clients: Yes
Bootstrap Server: Not configured

Support Unlisted Clients: Yes

Ping Time: 1 second(s)
Used IP Address Expire Interval: 15 minute(s)
```

**2** グローバル・オプション。低位のスコープでオーバーライドされないかぎり、すべてのクライアントに渡されます。

```
DHCP Server config>add option global 15 raleigh.ibm.com
DHCP Server config>add option global 6 9.67.1.5
```

```
DHCP Server config>li option global
option option
code data
```

```
-----
15 raleigh.ibm.com
6 9.67.1.5
```

```
DHCP Server config> add class global
Enter the class name []? manager
Class record with name manager has been added
```

```
DHCP Server config> add option class-global
Enter the class name []? manager
Enter the option code [1]? 48
Enter the option data []? 6.5.4.3
```

```
DHCP Server config>add option class-global 9 9.37.35.146
DHCP Server config>add option class-global manager 210 manager_authority
```

```
DHCP Server config>li class global manager
class
name
```

```
-----
manager
```

```
Number of Options: 3
option option
code data
-----
48 6.5.4.3
9 9.37.35.146
210 manager_authority
```

**3** ベンダー・オプション

```
DHCP Server config>add vendor-option XI-client
Enter the vendor hex data []? 01 02 03
Vendor-option record with name XI-client has been added
```

```
DHCP Server config> add vendor-option XA-client
Enter the vendor hex data []?
Vendor-option record with name XA-client has been added
```

```
DHCP Server config> add option vendor-option XA-client 23 100
```

```
DHCP Server config>li vendor-option all
```

```
vendor      hex
name        data
```

```
-----
XI-client   01 02 03
```

```
XA-client
```

```
DHCP Server config>li vendor-option det XA-client
```

```
vendor      hex
name        data
```

```
-----
XA-client
```

```
Number of Options: 1
```

```
option      option
code        data
```

```
-----
23          100
```

#### 4 代表的なサブネット

```
DHCP Server config>add subnet
```

```
Enter the subnet name []? sub1
```

```
Enter the IP subnet []? 9.2.23.0
```

```
Enter the IP subnet mask [255.255.255.0]?
```

```
Enter start of IP address range [9.2.23.1]? 9.2.23.120
```

```
Enter end of IP address range [9.2.23.150]? 9.2.23.126
```

```
Enter the subnet group name []?
```

```
Subnet record with name sub1 has been added
```

```
DHCP Server config>
```

```
DHCP Server config> add option subnet
```

```
Enter the subnet name []? sub1
```

```
Enter the option code []? 28
```

```
Enter the option data []? 9.2.23.127
```

```
DHCP Server config> add option subnet 9 5.6.7.8
```

```
DHCP Server config>add option subnet sub1 51 200
```

```
DHCP Server config>add class subnet
```

```
Enter the subnet name []? sub1
```

```
Enter the class name []? manager
```

```
Enter start of IP address range []?
```

```
Class record with name manager has been added
```

```
DHCP Server config>add option class-subnet sub1 manager
```

```
Enter the option code [1]? 9
```

```
Enter the option data []? 9.2.23.98
```

#### 6 プログラマーが独自のサブネット範囲を所有している

```
DHCP Server config>add class subnet
```

```
Enter the subnet name []? sub1
```

```
Enter the class name []? developers
```

```
Enter start of IP address range []? 9.2.23.125
```

```
Enter end of IP address range []? 9.2.23.126
```

```
Class record with name developers has been added
```

```
DHCP Server config>add option class-subnet sub1 developers 51 -1
```

```
DHCP Server config>add option class-subnet sub1 developers 9 9.37.35.1
```

```
DHCP Server config>li subnet detailed sub1
```

subnet name	subnet address	subnet mask	starting IP Addr	ending IP Addr
sub1	9.2.23.0	255.255.255.0	9.2.23.120	9.2.23.126

```
Number of Classes: 2
```

## DHCP サーバーの使用

```
class
name
-----
manager

Number of Options: 1
option option
code    data
-----
9       9.2.23.98
developers
starting IP address: 9.2.23.125
ending   IP address: 9.2.23.126

Number of Options: 2
option option
code    data
-----
51      -1
9       9.37.35.1

Number of Options: 3
option option
code    data
-----
28      9.2.23.127
9       5.6.7.8
51      200
```

**7** 任意のアドレスを受け入れるが、固有のオプションのセットを持つクライアントの例。

```
DHCP Server config>add client global
Enter the client name []? any-addr
Enter the client's hardware type (0 - 21) [1]? 6
Enter the client ID (MAC address or string) []? 10005aa4b9ab
Enter the client's IP address (IP address, any, none) []? any

DHCP Server config>add option client-global any-addr 51 999
DHCP Server config>add option client-global any-addr 1 255.255.255.0
```

**8** サービスからアドレスを除外する。

```
Enter the client name []? excl-addr
Enter the client's hardware type (0 - 21) [1]? 0
Enter the client ID (MAC address or string) []? 0
Enter the client's IP address (IP address, any, none) []? 9.2.23.121
```

```
DHCP Server config>li cli all
client      client client      attached      IP
name        type  identifier  to subnet    address
-----
any-addr    6     10005aa4b9ab          Any
excl-addr   0     0                    9.2.23.121
```

```
DHCP Server config>li client global any-addr
client      client client      IP
name        type  identifier  address
-----
any-addr    6     10005aa4b9ab          Any
```

```
Number of Options: 2
option option
code    data
-----
51      999
1       255.255.255.0
```

## 第31章 DHCP サーバーの構成と監視

この章では、DHCP サーバーの構成コマンドと操作コマンドの使用法について説明します。この章には次の内容が記載されています。

- 『DHCP サーバー構成環境へのアクセス』
- 『DHCP サーバー構成コマンド』
- 533ページの『DHCP サーバー監視環境へのアクセス』
- 533ページの『DHCP サーバー監視コマンド』

### DHCP サーバー構成環境へのアクセス

DHCP サーバー構成 プロセスにアクセスするには、次の手順を使用します。

1. OPCODE プロンプトで、**talk 6** と入力する。たとえば、次のように入力します。

```
* talk 6
Config>
```

**talk 6** コマンドを入力すると、Config プロンプト (Config>) が端末に表示されます。最初に構成に入ったときにプロンプトが表示されない場合は、**Return** をもう一度押してください。

2. Config プロンプトで、**feature dhcp-server** コマンドを入力して DHCP Server config> プロンプトを表示する。

### DHCP サーバー構成コマンド

表 58. DHCP サーバー構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxiページの『ヘルプの入手』を参照してください。
Add	クラス、クライアント、サブネット、またはベンダー・オプションを追加します。
Change	クラス、クライアント、サブネット、またはベンダー・オプションの定義を変更します。
Default	特定のグローバル変数をデフォルト値に戻します。
Delete	クラス、サブネット、またはベンダー・オプションを削除します。
Disable	DHCP サーバーをグローバルに使用不可にします。
Enable	DHCP サーバーをグローバルに使用可能にします。
List	クラス、クライアント、グローバル、サブネット、またはベンダー・オプションの定義を表示します。
Set	指定のスコープにあるグローバル・パラメーターまたはオプションの定義を設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxiiページの『下位レベル操作環境の終了』を参照してください。

## DHCP サーバー構成コマンド (Talk 6)

### Add

**add** コマンドは、クラス、サブネット、またはベンダー・オプションを追加するために使用します。

構文:

```
add                                class
                                     client
                                     option
                                     subnet
                                     vendor-option
```

**class** *scope* [*subnet\_name*] *class\_name* [*range\_start*] [*range\_end*]  
クラスを定義します。

**scope** クラスを追加する先のスコープを指定します。

有効値: global または subnet

デフォルト値: なし

**subnet\_name**

これは、**scope** が *subnet* の場合だけ有効です。クラスを追加する先のサブネット名を指定します。

有効値: 任意の既存サブネット名

デフォルト値: なし

**class-name**

クラスの名前を指定します。

有効値: 長さ 40 文字までの ASCII 文字列

デフォルト値: なし

**range-start**

これは、**scope** が *subnet* の場合だけ有効です。クライアントに割り当てる IP アドレスの開始 IP アドレスを指定します。

有効値: クラスを追加する先のサブネットの範囲内にある任意の有効 IP アドレス

デフォルト値: 指定のサブネットに属するサブネット範囲の最初の IP アドレス

**range-end**

これは、**scope** が *subnet* の場合だけ有効です。クライアントに割り当てる IP アドレスの終了 IP アドレスを指定します。

有効値: クラスを追加する先のサブネットの範囲内にある任意の有効 IP アドレスこの値は、**range-start** に指定した値より大きくなければなりません。

## DHCP サーバー構成コマンド (Talk 6)

**デフォルト値:** 指定のサブネットに属するサブネット範囲の開始 IP アドレスに 5 を足した値。得られる IP アドレスがサブネット範囲にない場合、デフォルトはサブネット範囲の終了 IP アドレスになります。

例:

```
DHCP Server config> add class global
Enter class name? ClassA

DHCP Server config> add class subnet
Enter the subnet name[]? subA
Enter class name[]? C1aA
Enter start of IP address range[10.1.1.1]?
Enter end of IP address range[10.1.1.6]?
```

**client** *scope [subnet\_name] client\_name id-type id-value address*

クライアントを定義します。

**scope** クライアントを追加する先のスコープを指定します。

**有効値:** global または subnet

**デフォルト値:** なし

**subnet-name**

**scope** が *subnet* の場合だけ有効です。クライアントを追加する先のサブネット名を指定します。

**有効値:** 任意の既存サブネット名

**デフォルト値:** なし

**client-name**

クライアントの名前を指定します。

**有効値:** 任意の 10 文字の ASCII 文字列

**デフォルト値:** なし

**id-type**

クライアントのハードウェア・タイプを指定します。IBM 2212 に適用できる RFC 1340 に定義されたハードウェア・タイプを、有効値として次に示します。

**有効値:**

**0** 指定なし。クライアントの記号名を指定します。

**1** イーサネット

**6** IEEE 802 ネットワーク (802.5 トークンリングなど)

**デフォルト値:** 1

**id-value**

クライアント ID を指定します。**id-type** が 0 の場合、**id-value** は 64 文字の文字列です。そうでなければ、**id-value** は MAC アドレスです。

**注:** **id-type** の 0 と **id-value** の 0 は、指定の IP アドレスをサーバーによって配布しないことを指定します。

## DHCP サーバー構成コマンド (Talk 6)

有効値: 0 または任意の有効 MAC アドレス (12 桁の 16 進数字)

デフォルト値: なし

### address

クライアントに提供する IP アドレス、またはクライアントにサービスを提供しないこと、あるいはクライアントに IP アドレス・プールから任意のアドレスを提供できることを示す文字列を指定します。

有効値:

#### 任意の有効 IP アドレス

ドット 10 進数形式。クライアントがサブネット・スコープ内に定義されている場合は IP アドレスはサブネット範囲内になければなりません。

**none** 一致するクライアントにサービスを提供しないことを指定します。

**any** サブネット・プール内の任意の IP アドレスをクライアントに提供できることを指定します。

デフォルト値: なし

注: **id-type** の 0 と **id-value** の 0 は、指定の IP アドレスをサーバーによって配布しないことを指定します。

例:

```
DHCP Server config> add client global
Enter the client name []? ClientA
Enter the client's hardware type (0 - 21) [1]? 0
Enter the client ID (MAC address or string) []? ClientA
Enter the client's IP address (IP address, any, none) []? 9.1.1.1
Client record with name ClientA has been added
```

```
DHCP Server config> add client subnet
Enter the subnet name []? subA
Enter the client name []? CliA
Enter the client's hardware type (0 - 21) [1]? 1
Enter the client ID (MAC address or string) []? 400000000010
Enter the client's IP address (IP address, any, none) []? 10.1.1.10
Client record with name CliA has been added
```

**option** *scope [subnet-name] [class-name] [client-name] [vendor-name] code data*  
オプションを定義します。オプションは、グローバルに定義することも、サブネット、クラス、クライアント、またはベンダー・オプションの範囲内に定義することもできます。

**scope** オプションを追加する先のスコープを指定します。

有効値:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option



デフォルト値: なし

#### subnet-name

**scope** が *subnet*、*class-subnet*、または *client-subnet* の場合だけ有効です。クライアントを追加する先のサブネット名を指定します。

有効値: 任意の既存サブネット名

デフォルト値: なし

#### class-name

**scope** が *class-global* または *class-subnet* の場合だけ有効です。オプションを追加する先のクラス名を指定します。

有効値: 既存のクラス名

デフォルト値: なし

#### client-name

**scope** が *client-global* または *client-subnet* の場合だけ有効です。オプションを追加する先のクライアント名を指定します。

有効値: 任意の既存クライアント名

デフォルト値: なし

#### vendor-name

**scope** が *vendor-option* の場合だけ有効です。オプションを追加する先のベンダー名を指定します。

有効値: 任意の既存ベンダー名

デフォルト値: なし

#### code

オプション・コードを指定します。DHCP オプションは RFC 2132 に定義されています。オプションとその形式についての説明は、483ページの『DHCP オプション』を参照してください。

有効値: 1 ~ 255

デフォルト値: 1

#### data

オプション・データを指定します。オプション・データは 3 つの方法で定義できます。

- RFC 2132 に定義されている特定の形式に合わせた ASCII 文字列。
- 初期設定時の 16 進数変換。データは *hex: 01 aa 04* のように入力する必要があります。
- 文字列。データは *abcdef* のように入力する必要があります。

例:

```
DHCP Server config> add option global
Enter the option code [1]? 3
Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option subnet
Enter the subnet name []? subA
Enter the option code [1]? 3
Enter the option data []? 9.167.100.1
```

例:

## DHCP サーバー構成コマンド (Talk 6)

```
DHCP Server config> add option class-global
Enter the class name []? ClassA
Enter the option code [1]? 3
Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option client
Enter the client name []? ClientA
Enter the option code [1]? 3
Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option class-subnet
Enter the subnet name []? subA
Enter the class name []? ClaA
Enter the option code [1]? 3
Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option client-subnet
Enter the subnet name []? subA
Enter the client name []? CliA
Enter the option code [1]? 3
Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option vendor-option
Enter the vendor name []? 200
Enter the option code [1]? 85
Enter the option data []? hex:01 AA 04
```

例:

```
DHCP Server config> add option vendor-option
Enter the vendor name []? 200
Enter the option code [1]? 86
Enter the option data []? 9.67.85.4
```

**subnet** *subnet\_name subnet-address subnet-mask range-start range-end [subnet\_group\_name]*  
*[subnet\_group\_priority] [policy-list]*

サブネットを定義します。

### subnet-name

サブネットの名前を指定します。

**有効値:** 任意の 10 文字の ASCII 文字列

**デフォルト値:** なし

### subnet-address

サブネットのアドレスを指定します。アドレスはドット 10 進数形式で指定します。

**有効値:** 任意の有効な IP サブネット・アドレス

**デフォルト値:** なし

### subnet-mask

サブネット・アドレス・マスクを指定します。サブネット・アドレス・マスクは、サブネット・マスク内になければならず、マスクより多いビット数を含むことはできません。

**有効値:** ドット 10 進数形式の任意の有効 IP マスク

**デフォルト値:** サブネット・アドレスに基づいて計算される

**range-start**

このサーバーがこのサブネットのために管理する IP アドレス・プールの開始 IP アドレスを指定します。*range-start* を指定しない場合は、サブネット内のアドレスすべてがサーバーによって管理されません。

**有効値:** 指定のサブネット内にある、ドット 10 進数形式の任意の有効 IP アドレス

**デフォルト値:** サブネットの最初の IP アドレス

**range-end**

このサーバーがこのサブネットのために管理する IP アドレス・プールの終了 IP アドレスを指定します。

**有効値:** 指定のサブネット内にある、ドット 10 進数形式の任意の有効 IP アドレス

**デフォルト値:** **range-start** に 50 を足した値。得られる IP アドレスがサブネット内でない場合、デフォルトはサブネット内の最終 IP アドレスになります。

**subnet-group-name**

このサブネットが属するサブネット・グループ名を指定します。

**有効値:** 長さ 64 文字までの ASCII 文字列

**デフォルト値:** なし

**subnet-group-priority**

サブネット・グループ内でのこのサブネットの優先順位を指定します。この優先順位は、指定のサブネット・グループ内でアドレスを割り当てる順序を決定するために使用されます。

**有効値:** 1 ~ 65535

**デフォルト値:** 1

**policy-list**

サブネット・グループを追加する先のポリシー・アドレス・リスト (Balance または Inorder) を指定します。あるリストにサブネット・グループがすでに存在していて、他のリストが指定された場合、サブネット・グループは新しいリストに移動します。

**有効値:** Inorder または Balance

**デフォルト値:** これが新規サブネットの場合、デフォルトは Inorder です。そうでなければ、デフォルトはサブネット・グループが属する新規ポリシー・リストです。

**例:**

```
DHCP Server config> add subnet
Enter the subnet name []? subA
Enter the IP subnet []? 10.1.1.0
Enter the IP subnet mask [255.255.255.0]?
Enter start of IP address range [10.1.1.1]?
Enter end of IP address range [10.1.1.31]?
Enter the subnet group name []? group1
Enter the subnet group priority (1 - 65535) [1]?
```

## DHCP サーバー構成コマンド (Talk 6)

```
Enter the access policy list (Inorder or Balance) [Inorder]?  
Subnet record with name sub1 has been added  
Subnet group group1 is being added to the Inorder List
```

### **vendor-option** *vendor\_name* [*hex\_value*]

ベンダー・オプションを追加します。ベンダー・オプション・データを指定する方法は次の 2 つです。

- プロンプトが出たら 16 進データを入力する
- **add option vendor** コマンドを使用して、ベンダーに特定のオプションを追加する。オプションについては、506 ページを参照してください。

#### *vendor\_name*

ベンダーの名前を指定します。

**有効値:** 長さ 40 文字までの ASCII 文字列

**デフォルト値:** なし

#### *hex-value*

オプションのデータ部分の値を表現する 16 進 ASCII 文字列を指定します。

**有効値:** *01 aa 04* のような形式の任意の有効 16 進文字列。

**デフォルト値:** なし

例:

```
DHCP Server config> add vendor-option  
Enter the vendor name []? XA-client  
Enter the vendor hex data [] 01 aa 04?  
Vendor-option record with name XA-client has been added
```

## Change

**change** コマンドは、クラス、クライアント、サブネット、またはベンダー・オプションの構成を変更するために使用します。

構文:

```
change class client subnet vendor-option
```

**class** *scope* [*subnet\_name*] *class\_name* *new\_class\_name* [*new\_range\_start*] [*new\_range\_end*]

クラスを変更します。

**scope** 変更するクラスの範囲を指定します。

**有効値:** global または subnet

**デフォルト値:** なし

#### **subnet-name**

**scope** が *subnet* の場合だけ有効です。クラスが属するサブネットの名前を指定します。

**有効値:** 任意の既存サブネット名

デフォルト値: なし

**class-name**

クラスの名前を指定します。

有効値: 既存のクラス名

デフォルト値: なし

**new-class-name**

クラスの新しい名前を指定します。

有効値: 長さ 40 文字までの ASCII 文字列

デフォルト値: 既存のクラス名

**new-range-start**

**scope** が *subnet* の場合だけ有効です。クライアントに割り当てる IP アドレスの新しい開始 IP アドレスを指定します。

有効値: サブネット範囲内にある任意の IP アドレス

デフォルト値: 既存の range-start

**new-range-end**

クライアントに割り当てる IP アドレスの新しい終了 IP アドレスを指定します。

有効値: サブネット範囲内にある **new-range-end** より大きい任意の有効 IP アドレス

デフォルト値: 既存の range-end

例:

```
DHCP Server config> change class global
Enter the class name []? ClassA
Enter the new class name [ClassA]?
```

例:

```
DHCP Server config> change class subnet
Enter the subnet name []? subA
Enter the class name []? ClaA
Enter the new class name [ClaA]?
Enter start of IP address range [10.1.1.1]?
Enter end of IP address range [10.1.1.6]?
```

**client** *scope* [*subnet\_name*] *client\_name* *new-client\_name* *new-id-type* *new-id-value*  
*new-address*

クライアントを変更します。

**scope** 変更するクライアントのスコープを指定します。

有効値: global または subnet

デフォルト値: なし

**subnet-name**

**scope** が *subnet* の場合だけ有効です。クライアントが属するサブネットの名前を指定します。

有効値: 任意の既存サブネット名

デフォルト値: なし

## DHCP サーバー構成コマンド (Talk 6)

### client-name

クライアントの名前を指定します。

有効値: 既存のクライアント名

デフォルト値: なし

### new-client-name

クライアントの新しい名前を指定します。

有効値: 長さ 10 文字までの ASCII 文字列

デフォルト値: 既存のクライアント名

### new-id-type

クライアントの新しいハードウェア・タイプを指定します。

有効値: 0 ~ 21 (505 ページを参照)。

デフォルト値: クライアントの既存ハードウェア・タイプ

### new-id-value

新しいクライアント ID を指定します。

有効値: 0 または任意の有効 MAC アドレス (12 桁の 16 進数字)

デフォルト値: 既存のクライアント ID タイプ

注: **id-type** の 0 と **id-value** の 0 は、指定の IP アドレスをサーバーによって配布しないことを指定します。

### new-address

クライアントに提供する新しい IP アドレス、またはクライアントにサービスを提供しないこと、あるいはクライアントに IP アドレス・プールから任意のアドレスを提供できることを示す文字列を指定します。

有効値:

任意の有効 IP アドレス

**none** 一致するクライアントにサービスを提供しないことを指定します。

**any** サブネット・プール内の任意の IP アドレスをクライアントに提供できることを指定します。

デフォルト値: なし

注: **id-type** の 0 と **id-value** の 0 は、指定の IP アドレスをサーバーによって配布しないことを指定します。

例:

```
DHCP Server config> change client global
Enter the client name []? ClientA
Enter the new client name [ClientA]?
Enter the new client hardware type (0 - 21) [0]?
Enter the new client ID [ClientA]?
Enter the client's new IP address (IP address, any, none) [9.1.1.1]?
Client ClientA has been changed
```

例:

```

DHCP Server config> change client subnet
Enter the subnet name []? subA
Enter the client name []? CliA
Enter the new client name [ClientA]?
Enter the new client hardware type (0 - 21) [1]?
Enter the new client ID [400000000010]?
Enter the client's new IP address (IP address, any, none) [10.1.1.10]?
Client CliA has been changed

```

**subnet** *subnet\_name new\_subnet\_name new\_subnet\_address new\_subnet\_mask  
new-range\_start new-range\_end*

サブネットを変更します。

#### **subnet\_name**

変更する特定のサブネット名を指定します。

**有効値:** 既存のサブネット名

**デフォルト値:** なし

#### **new\_subnet\_name**

指定のサブネットの新しい名前を指定します。

**有効値:** 任意の 10 文字の ASCII 文字列

**デフォルト値:** 元のサブネット名

#### **new\_subnet\_addresses**

サブネットの新しいアドレスを指定します。アドレスはドット 10 進表記で指定します。

**有効値:** 任意の有効な IP サブネット・アドレス

**デフォルト値:** 既存のサブネット・アドレス

#### **new\_subnet\_mask**

新しいサブネット・アドレス・マスクを指定します。サブネット・アドレス・マスクは、サブネット・マスク内になければならず、マスクより多いビット数を含むことはできません。

**有効値:** 任意の有効な IP マスク

**デフォルト値:** 既存のサブネット・マスク

#### **new-range-start**

このサーバーがこのサブネットのために管理する IP アドレス・プールの新しい開始 IP アドレスを指定します。*range-start* を指定しない場合は、サブネット内のアドレスすべてがサーバーによって管理されます。

**有効値:** サブネット範囲内にある任意の有効 IP アドレス

**デフォルト値:** 既存のプール開始アドレス

#### **new-range-end**

このサーバーがこのサブネットのために管理する IP アドレス・プールの新しい終了 IP アドレスを指定します。

**有効値:** サブネット範囲内にあり、開始プール・アドレスより大きい任意の有効 IP アドレス

**デフォルト値:** 既存のプール終了アドレス

## DHCP サーバー構成コマンド (Talk 6)

例:

```
DHCP Server config> change subnet
Enter the subnet name []? subA
Enter the new subnet name [subA]?
Enter the new IP subnet [10.1.1.0]?
Enter the new IP subnet mask [255.255.0.0]?
Enter new start of IP address range [10.1.1.1]?
Enter new end of IP address range [10.1.1.31]?
Enter the new subnet group name [group11]?
Enter the new subnet group priority [1]?
Enter the new access policy list (Inorder or Balance) [Inorder]?
```

**vendor-option** *vendor\_name new\_vendor\_name [new\_hex\_value]*

ベンダー・オプションを変更します。

**vendor\_name**

ベンダー・オプションの新しい名前を指定します。

有効値: 既存のベンダー名

デフォルト値: なし

**new\_vendor\_name**

ベンダー・オプションの新しい名前を指定します。

有効値: 長さ 40 文字までの ASCII 文字列

デフォルト値: 既存のベンダー・オプション名

**new\_hex\_value**

オプションのデータ部分の値を表現する新しい 16 進 ASCII 文字列を指定します。このベンダー・オプションに特定のオプションが追加されている場合は、16 進値は追加できません。

有効値: 任意の有効な 16 進数文字列

デフォルト値: 既存の 16 進数文字列

例:

```
DHCP Server config> change vendor-option
Enter the vendor name []? XA-clients
Enter the new vendor name [XA-clients]?
Enter the new vendor data [01 aa 04]?
```

## Delete

**delete** コマンドは、クラス、クライアント、オプション、サブネット、サブネット・グループ、またはベンダー・オプションを削除するために使用します。

構文:

<b>delete</b>	class
	client
	option
	subnet
	subnet-group
	vendor-option



**class** *scope* [*subnet\_name*] *class\_name*

クラスと、そのスコープの下に定義されているすべてのオプションを削除します。

**scope** クラスを削除するスコープを指定します。

有効値: global または subnet

デフォルト値: なし

**subnet-name**

**scope** が *subnet* の場合だけ有効です。クラスを削除するサブネットの名前を指定します。

有効値: 任意の既存サブネット名

デフォルト値: なし

**class-name**

削除するクラスの名前を指定します。

有効値: 既存のクラス名

デフォルト値: なし

例:

```
DHCP Server config> delete class global
Enter the class name []? ClassA
```

例:

```
DHCP Server config> delete class subnet
Enter the subnet name []? subA
Enter the class name []? ClaA
```

**client** *scope* [*subnet\_name* ] *client\_name*

クライアントと、そのスコープの下に定義されているすべてのオプションを削除します。

**scope** クライアントを削除するスコープを指定します。

有効値: global または subnet

デフォルト値: なし

**subnet\_name**

**scope** が *subnet* の場合だけ有効です。クライアントを削除するサブネットの名前を指定します。

有効値: 既存のサブネット名

デフォルト値: なし

**client\_name**

削除するクライアントの名前を指定します。

有効値: 既存のクライアント名

デフォルト値: なし

例:

```
DHCP Server config> delete client global
Enter the client name []? ClientA
```

例:

## DHCP サーバー構成コマンド (Talk 6)

```
DHCP Server config> delete client subnet
Enter the subnet name []? subA
Enter the client name []? CliA
```

**option** *scope* [*subnet\_name*] [*class\_name*] [*client\_name*] [*vendor\_name*] *code*

指定の範囲内にあるオプションを削除します。

**scope** オプションを削除する範囲を指定します。

有効値:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

デフォルト値: なし

**subnet-name**

**scope** が *subnet*、*class-subnet*、または *client-subnet* の場合だけ有効です。クライアントを削除するサブネットの名前を指定します。

有効値: 任意の既存サブネット名

デフォルト値: なし

**class-name**

**scope** が *class-global* または *class-subnet* の場合だけ有効です。オプションを削除するクラス名を指定します。

有効値: 既存のクラス名

デフォルト値: なし

**client-name**

**scope** が *client-global* または *client-subnet* の場合だけ有効です。オプションを削除するクライアント名を指定します。

有効値: 任意の既存クライアント名

デフォルト値: なし

**vendor-name**

**scope** が *vendor-option* の場合だけ有効です。オプションを削除するベンダー名を指定します。

有効値: 任意の既存ベンダー名

デフォルト値: なし

**code** オプション・コードを指定します。DHCP オプションは RFC 2132 に定義されています。オプションとその形式についての説明は、483ページの『DHCP オプション』を参照してください。

有効値: 1 ~ 255

デフォルト値: 1

例:

```
DHCP Server config> delete option global
Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option subnet
Enter the subnet name []? subA
Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option class-global
Enter the class name []? ClassA
Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option client
Enter the client name []? ClientA
Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option class-subnet
Enter the subnet name []? subA
Enter the class name []? ClaA
Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option client-subnet
Enter the subnet name []? subA
Enter the client name []? CliA
Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option vendor-option
Enter the vendor name []? XI-clients
Enter the option code [1]? 85
```

例:

```
DHCP Server config> delete option vendor-option
Enter the vendor name []? 200
Enter the option code [1]? 86
```

**subnet** *subnet\_name*

サブネットと、そのスコープの下に定義されているすべてのクラス、クライアント、およびオプションを削除します。

**subnet\_name**

削除するサブネットの名前を指定します。

**有効値:** 任意の既存サブネット名

**デフォルト値:** なし

例:

```
DHCP Server config> delete subnet
Enter the subnet name []? subA
You are about to delete a subnet subA
and all the associated class, client, and option records associated with it
Are you sure you want to continue? [No]:
```

**subnet-group** *subnet\_group\_name*

特定のサブネット・グループに関連したすべてのサブネット、およびサブネット・スコープの下に定義されているすべてのクラス、クライアント、およびオプションを削除します。

## DHCP サーバー構成コマンド (Talk 6)

### **subnet\_group\_name**

サブネット・グループを識別する名前を指定します。

**有効値:** 既存のサブネット・グループ名

**デフォルト値:** なし

**例:**

```
DHCP Server config> delete subnet-group
Enter the subnet group name []? group2
You are about to delete a all subnets in group group2
and all the associated class, client, and option records associated with them
Are you sure you want to continue? [No]:
```

### **vendor-option vendor\_name**

ベンダー・オプションと、そのスコープの下に定義されているすべてのオプションを削除します。

*vendor\_name*

ベンダーの名前を指定します。

**有効値:** 長さ 40 文字までの ASCII 文字列

**デフォルト値:** なし

**例:**

```
DHCP Server config> delete vendor-option
Enter the vendor name []? XA-clients
```

## Disable

**disable** コマンドは、DHCP サーバーをグローバルに使用不可にするために使用します。

**構文:**

```
disable dhcp-server
```

**例:**

```
DHCP Server config> disable dhcp-server
```

## Enable

**enable** コマンドは、DHCP サーバーをグローバルに使用可能にするために使用します。

**構文:**

```
enable dhcp-server
```

**例:**

```
DHCP Server config> enable dhcp-server
```

## List

**list** コマンドは、クラス、クライアント、グローバル・パラメーター、サブネット、またはベンダー・オプションに関する構成情報と、関連したオプションを表示するために使用します。

**構文:**

```
list
_
class
client
global
option
subnet
vendor-option
```

```
class all
    global class-name
    subnet class-name
```

構成されたすべてのクラスの要約、または特定のクラスの詳細を表示します。

**class-name**

表示するクラスの名前を指定します。

**有効値:** 既存のクラス名

**デフォルト値:** なし

**例:**

```
DHCP Server config> list class all
```

```
class          attached
name           to subnet
-----
ClassA
ClaA           subA
```

**例:**

```
DHCP Server config> list class global
Enter the class name []? ClassA
```

```
class
name
-----
ClassA
Bootstrap Server: 100.100.100.100
Canonical: Yes
Support Unlisted Clients: Yes
Number of Options: 1
option  option
code   data
-----
1      255.255.0.0
```

**例:**

## DHCP サーバー構成コマンド (Talk 6)

```
DHCP Server config> list class subnet
Enter the subnet name []? subA
Enter the class name []? ClaA

class
name
-----
ClaA
starting IP address: 10.1.1.3
ending IP address: 10.1.1.5
Bootstrap Server: 100.100.100.100
Canonical: Yes
Support Unlisted Clients: DHCP

Number of Options: 1
option      option
code        data
-----
6           9.67.100.1

client all

global client-name

subnet client-name
```

構成されたすべてのクライアントの要約、または特定のクライアントの詳細を表示します。

### client-name

表示するクライアントの名前を指定します。

**有効値:** 既存のクライアント名

**デフォルト値:** なし

例:

```
DHCP Server config> list client all
client client client attached IP
name type identifier to subnet address
-----
ClientA 0 ClientA 9.1.1.1
CliA 1 400000000010 subA 10.1.1.10
```

例:

```
DHCP Server config> list client global
Enter the client name []? ClientA
```

例:

```
DHCP Server config> list client subnet
Enter the subnet name []? subA
Enter the client name []? CliA

client client client IP
name type identifier address
-----
CliA 1 400000000010 10.1.1.10
Bootstrap Server: 200.200.200.200
Canonical: Yes

Number of Options: 1
```

option code	option data
6	9.67.100.1

**global**

グローバル・パラメーターを表示します。

例:

DHCP Server config> **list global**

```
DHCP server Global Parameters
=====
DHCP server enabled: Yes

Balance: group2

Inorder: group1

Canonical: No

Lease Expire Interval: 1 minute(s)
Lease Time Default: 1 day(s)

Support BOOTP Clients: No
Bootstrap Server: Not configured

Support Unlisted Clients: Yes
Ping Time: 1 second(s)
Used IP Address Expire Interval: 15 minute(s)
```

**option** *scope* [*subnet-name*] [*class-name*] [*client-name*] [*vendor-name*] *code*

**scope** オプションを表示するスコープを指定します。

有効値:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

デフォルト値: なし

**subnet-name**

**scope** が *subnet*、*class-subnet*、または *client-subnet* の場合だけ有効です。表示するオプションが属するサブネットの名前を指定します。

有効値: 任意の既存サブネット名

デフォルト値: なし

**class-name**

**scope** が *class-global* または *class-subnet* の場合だけ有効です。表示するオプションが属するクラスの名前を指定します。

## DHCP サーバー構成コマンド (Talk 6)

有効値: 既存のクラス名

デフォルト値: なし

### client-name

**scope** が *client-global* または *client-subnet* の場合だけ有効です。表示するオプションが属するクライアントの名前を指定します。

有効値: 任意の既存クライアント名

デフォルト値: なし

### vendor-name

**scope** が *vendor-option* の場合だけ有効です。表示するオプションが属するベンダーの名前を指定します。

有効値: 任意の既存ベンダー名

デフォルト値: なし

**code** オプション・コードを指定します。DHCP オプションは RFC 2132 に定義されています。オプションとその形式についての説明は、483ページの『DHCP オプション』を参照してください。

有効値: 1 ~ 255

デフォルト値: 1

例:

```
DHCP Server config> list option global
```

option code	option data
3	9.67.100.1

例:

```
DHCP Server config> list option class-global
```

```
Enter the class name []? ClassA
option code    option data
-----
3              9.67.100.1
```

例:

```
DHCP Server config> list option class-subnet
```

```
Enter the subnet name []? subA
Enter the class name []? claA
option code    option data
-----
3              9.67.100.1
```

例:

```
DHCP Server config> list option client-global
```



```

Enter the client name []? ClientA
option   option
code    data
-----
3        9.67.100.1

```

例:

```

DHCP Server config> list option client-subnet
Enter the subnet name []? subA
Enter the client name []? cliA

```

```

option   option
code    data
-----
3        9.67.100.1

```

例:

```

DHCP Server config> list option subnet
Enter the subnet name []? subA

```

```

option   option
code    data
-----
6        9.67.100.1

```

例:

```

DHCP Server config> list option vendor-option
Enter the vendor name []? XI-clients

```

```

option   option
code    data
-----
85       hex:01 aa 04
86       9.67.85.4

```

### subnet

all

detailed *subnet-name*

構成されたすべてのサブネットの要約、または特定のサブネットの詳細を表示します。

### subnet-name

表示するサブネットの名前を指定します。

**有効値:** 既存のサブネット名

**デフォルト値:** なし

例:

```

DHCP Server config> list subnet all

```

```

name     address      mask          IP Addr   IP Addr
-----
subA     10.1.1.0    255.255.0.0  10.1.1.1 10.1.1.31
subB     11.1.1.0    255.255.0.0  11.1.1.1 11.1.1.31

```

## DHCP サーバー構成コマンド (Talk 6)

例:

```
DHCP Server config> list subnet detailed
Enter the subnet name []? subA
```

subnet name	subnet address	subnet mask	starting IP Addr	ending IP Addr
subA	10.1.1.0	255.255.0.0	10.1.1.1	10.1.1.31

Subnet Group: group1/1

Number of Classes: 1

class name

-----  
ClaA

starting IP address: 10.1.1.1

ending IP address: 10.1.1.6

Bootstrap Server: 100.100.100.100

Canonical: Yes

Support Unlisted Clients: DHCP

Number of Options: 1

option option  
code data

-----  
6 9.67.100.1

Number of Clients: 1

client name	client type	client identifier	IP address
Clia	1	400000000010	10.1.1.10

-----  
Clia 1 400000000010 10.1.1.10

Bootstrap Server: 200.200.200.200

Canonical: Yes

Number of Options: 1

option option  
code data

-----  
6 9.67.100.1

Number of Options: 1

option option  
code data

-----  
1 255.255.255.0

**vendor-option**

all

detailed *vendor-name*

構成されたすべてのベンダーの要約、または特定のベンダー・オプションの詳細を表示します。

**vendor-name**

表示するベンダー・オプションの名前を指定します。

**有効値:** 既存のベンダー名

**デフォルト値:** なし

例:

```
DHCP Server config> list vendor-option all
```

```

vendor      hex
name        data
-----
XA-clients  01 AA 04
XI-clients

DHCP Server config> list vendor-option detailed
Enter the vendor name []? XI-clients
vendor      hex
name        data
-----
XI-clients

Number of Options: 2
option      option
code        data
-----
85          hex:01 AA 04
86          9.67.85.4

```

## Set

**set** コマンドは、グローバル・パラメーターの値を指定するため、および Balance リストと Inorder リストにサブネット・グループを追加するために使用します。

構文:

```

set
_
balance
bootstrapservers
canonical
inorder
lease-expire-interval
lease-time-default
ping-time
support-bootp
support-unlisted-clients
used-ip-address-expire-interval

```

**balance** *subnet\_group\_name*

Balance リストにサブネット・グループを追加または移動します。アドレスは、優先順位に応じ、サブネット・グループ内に定義されているグループに関連付けられたすべてのサブネットから、ラウンドロビン方式で割り当てられます。

**subnet\_group\_name**

このサブネットが属するサブネット・グループの名前を指定します。

**有効値:** 既存のサブネット・グループ名

**デフォルト値:** なし

## DHCP サーバー構成コマンド (Talk 6)

例:

```
DHCP Server config> set balance
Enter the subnet group name []? group1
```

**bootstrapserver** *scope* [*subnet-name*] [*class-name*] [*client-name*] *address*

DHCP サーバーがクライアントに対してブートストラップ・サーバーを指定するかどうかを指定します。DHCP サーバーがブートストラップ・サーバーを指定するようにしたい場合は、サーバーの IP アドレスを定義する必要があります。このパラメーターは、グローバル、サブネット、クラス、またはクライアントの範囲内で指定できます。

**scope** bootstrapserver パラメーターの範囲を指定します。

有効値:

- class-global
- class-subnet
- client-global
- client-subnet
- global
- subnet

デフォルト値: なし

**subnet-name**

範囲が *subnet*、*class-subnet*、または *client-subnet* の場合に有効です。ブートストラップ・サーバーを指定する対象のサブネット名を指定します。

有効値: 既存のサブネット名

デフォルト値: なし

**class-name**

範囲が *class-global* または *class-subnet* の場合に有効です。ブートストラップ・サーバーを指定する対象のクラス名を指定します。

有効値: 既存のクラス名

デフォルト値: なし

**client-name**

範囲が *client-global* または *client-subnet* の場合に有効です。ブートストラップ・サーバーを指定する対象のクライアント名を指定します。

有効値: 既存のクライアント名

デフォルト値: なし

**サーバーの IP アドレス**

ブートストラップ・サーバーの IP アドレスを指定します。

有効値: ドット 10 進形式の任意の有効 IP アドレス

デフォルト値: なし

例:

## DHCP サーバー構成コマンド (Talk 6)

```
DHCP Server config> set bootstrap-server class-global
Enter the class name []? ClassA
Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server class-subnet
Enter the subnet name []? subA
Enter the class name []? ClassA
Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server client-global
Enter the client name []? ClientA
Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server client-subnet
Enter the subnet name []? subA
Enter the client name []? ClientA
Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server global
Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server subnet
Enter the subnet name []? subA
Enter the IP address of the server []? 100.100.100.100
```

**canonical** *scope [subnet-name] [class-name] [client-name] value*

DHCP サーバーが MAC アドレスを標準形式に変換するかどうかを指定します。

イーサネット/802.3 クライアントの MAC アドレスは、標準 (バイトが最下位ビットから始まる) 形式で保管されます。トークンリング・クライアントの MAC アドレスは、非標準 (バイトが最上位ビットから始まる) 形式で保管されます。このパラメーターは、DHCP サーバーが一方の媒体タイプ (トークンリングまたはイーサネット/802.3)、クライアントが他方の媒体タイプに基づいていて、両者間に中継ブリッジがある場合に使用する必要があります。このパラメーターを *yes* に設定すると、DHCP サーバーはクライアントの MAC アドレスを標準から非標準に、または非標準から標準に反転します。DHCP サーバーは MAC アドレスの元の形式を知らないため、このパラメーターを *yes* に設定すると単にアドレスが反転されます。Canonical は、グローバル、サブネット、クラス、またはクライアントの各スコープ内で設定できます。

**scope** bootstrapservers パラメーターのスコープを指定します。

**有効値:**

- class-global
- class-subnet
- client-global
- client-subnet
- global
- subnet

**デフォルト値:** なし

## DHCP サーバー構成コマンド (Talk 6)

### subnet-name

スコープが *subnet*、*class-subnet*、または *client-subnet* の場合に有効です。canonical を指定する対象のサブネットの名前を指定します。

有効値: 既存のサブネット名

デフォルト値: なし

### class-name

スコープが *class-global* または *class-subnet* の場合に有効です。canonical を指定する対象のクラスのクラスの名前を指定します。

有効値: 既存のクラス名

デフォルト値: なし

### client-name

スコープが *client-global* または *client-subnet* の場合に有効です。canonical を指定する対象のクライアントの名前を指定します。

有効値: 既存のクライアント名

デフォルト値: なし

**value** MAC アドレスを標準形式に変換するかどうかを指定します。

有効値: yes, no

デフォルト値: **scope** が *global* の場合は、no。そうでなければ、デフォルト値はスコープ階層によって決まります。スコープについての説明は、480ページの『概念と用語』を参照してください。

例:

```
DHCP Server config> set canonical class-global
Enter the class name []? ClassA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical class-subnet
Enter the subnet name []? subA
Enter the class name []? ClassA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical client-global
Enter the client name []? ClientA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical client-subnet
Enter the subnet name []? subA
Enter the client name []? ClientA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical global
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical subnet
Enter the subnet name []? subA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

**inorder** *label-list*

Inorder リストにサブネット・グループを追加または移動します。アドレスは、サブネット・グループ内のサブネットから、そのサブネットに割り当てられた優先順位順に割り当てられます。

**subnet\_group\_name**

このサブネットが属するサブネット・グループを指定します。

**有効値:** 既存のサブネット・グループ名

**デフォルト値:** なし

例:

```
DHCP Server config> set inorder
Enter the subnet group name []? g2
```

**lease-expire-interval** *time length*

アドレス・プール内のアドレスすべてのリース条件を検討して、有効期限が切れたリースを判別する間隔を指定します。リース満了間隔は、グローバル・レベルでだけ設定できます。

**time** 時間測定の単位を指定します。

**有効値:** seconds、minutes、hours

**デフォルト値:** なし

**length** 間隔の長さを指定します。

**有効値:** 15 秒 ~ 12 時間

**デフォルト値:**

- 15 (時間単位が秒の場合)
- 1 (時間単位が分の場合)
- 1 (時間単位が時の場合)

例:

```
DHCP Server config> set lease-expire-interval seconds
How long is the interval in seconds (max:59) [15]? 59
```

例:

```
DHCP Server config> set lease-expire-interval minutes
How long is the interval in minutes (max:59) [1]? 45
```

例:

```
DHCP Server config> set lease-expire-interval hours
How long is the interval in hours (max:12) [1]? 2
```

**lease-time-default** *time length*

DHCP サーバーによって出されるリースのデフォルト・リース期間を指定します。無限大の間隔は、リースが永久に満了しないことを意味します。リース時間のデフォルトは、グローバル・レベルでだけ設定できます。

**time** 時間測定の単位を指定します。

**有効値:** minutes、hours、days、weeks、months、years、infinity

**デフォルト値:** なし

**length** 間隔の長さを指定します。

**有効値:** 3 分 ~ 無限大

## DHCP サーバー構成コマンド (Talk 6)

デフォルト値:

- 3 (時間単位が分の場合)
- 1 (時間単位が時の場合)
- 1 (時間単位が日の場合)
- 1 (時間単位が月の場合)
- 1 (時間単位が年の場合)

例:

```
DHCP Server config> set lease-time-default minutes
How long is the interval in minutes (max:59) [3]? 2
```

例:

```
DHCP Server config> set lease-time-default hours
How long is the interval in hours (max:23) [1]? 45
```

例:

```
DHCP Server config> set lease-time-default days
How long is the interval in days (max:6) [1]? 2
```

例:

```
DHCP Server config> set lease-time-default weeks
How long is the interval in weeks (max:3) [1]? 1
```

例:

```
DHCP Server config> set lease-time-default months
How long is the interval in months (max:11) [1]? 3
```

例:

```
DHCP Server config> set lease-time-default years
How long is the interval in years (max:10) [1]? 3
```

例:

```
DHCP Server config> set lease-time-default infinity
```

### **ping-time** *time length*

IP アドレスを割り当てる前に、DHCP サーバーは IP アドレスが使用中でないことをテストして確認します。この値は、DHCP サーバーがアドレスに使用可能なマークを付ける前に、ping 応答を待機する時間を指定します。値 0 は ping を使用不可にし、この場合 DHCP サーバーは割り当ての前にアドレスをテストしません。

**time** 時間測定の単位を指定します。

有効値: seconds

デフォルト値: なし

**length** 間隔の長さを指定します。

有効値: 0 ~ 5 秒

デフォルト値: 1

例:

```
DHCP Server config> set ping-time seconds
How long is the interval in seconds (max:5) [1]? 10
```



**support-bootp** *value*

サーバーが BOOTP クライアントからの要求に応答するかどうかを指定します。DHCP サーバーが以前に BOOTP クライアントをサポートするように構成されていて、BOOTP クライアントをサポートしないように再構成された場合、再構成前に確立されていた BOOTP クライアントへのアドレス・バインドは、BOOTP クライアントが別の要求を出す (リスタート時に) までは保持されます。別の要求を出したときには、サーバーは応答しないので、バインドは消去されます。このパラメーターは、グローバル・レベルでだけ設定できます。

**有効値:** yes または no

**デフォルト値:** no

**例:**

```
DHCP Server config> set support-bootp
Would you like the server to support BOOTP clients? [No] 10
```

**support-unlisted-clients** *scope [subnet-name] [class-name] value*

この構成に明示的に表示されているクライアント ID をもつもの以外の DHCP クライアントからの要求に、サーバーが応答するかどうかを指定します。このパラメーターには、指定可能な値がいくつかあります。

**scope support-unlisted-clients** パラメーターのスコープを指定します。

**有効値:**

- class-global
- class-subnet
- global
- subnet

**デフォルト値:** なし

**subnet-name**

スコープが *subnet*、*class-subnet*、または *client-subnet* の場合に有効です。このパラメーターを指定する対象のサブネットの名前を指定します。

**有効値:** 既存のサブネット名

**デフォルト値:** なし

**class-name**

スコープが *class-global*、または *class-subnet* の場合に有効です。このパラメーターを指定する対象のクラスの名前を指定します。

**有効値:** 既存のクラス名

**デフォルト値:** なし

**value**

**yes** DHCP サーバーは、タイプや構成済みであるかどうかに関係なく、すべてのクライアントに応答する必要があります。

**no** DHCP サーバーは、構成済みの DHCP クライアントからの要求だけに応答します。

## DHCP サーバー構成コマンド (Talk 6)

**bootp** DHCP サーバーは、表示されていない BOOTP クライアントをサポートしますが、表示されていない DHCP クライアントはサポートしません。

**dhcp** DHCP サーバーは、表示されていない DHCP クライアントに応答しますが、表示されていない BOOTP クライアントには応答しません。

**有効値:** yes、no、bootp、dhcp

**デフォルト値:** **scope** が *global* の場合は、yes。そうでなければ、デフォルト値はスコープ階層によって決まります。スコープについての説明は、480ページの『概念と用語』を参照してください。

例:

```
DHCP Server config> set support-unlisted-clients class-global yes
Enter the class name []? ClassA
```

例:

```
DHCP Server config> set support-unlisted-clients class-subnet no
Enter the subnet name []? subA
Enter the class name []? ClassA
```

例:

```
DHCP Server config> set support-unlisted-clients global bootp
```

例:

```
DHCP Server config> set support-unlisted-clients subnet dhcp
Enter the subnet name []? subA
```

### **used-ip-address-expire-interval** *time length*

サーバーがアドレスを割り当て可能にする前に、使用中の IP アドレスを保持する間隔を指定します。サーバーは、IP アドレスを割り振る前にアドレスを ping して、そのアドレスがネットワーク上ですでに使用されていないことを確認します。その後サーバーは、使用中のアドレスに予約済みのマークを付けます。このパラメーターは、アドレスを割り当て可能にする前に、使用中のアドレスを予約済みとして保持する期間を指定します。このパラメーターは、グローバル・レベルでだけ設定できます。

**time** 時間測定の単位を指定します。

**有効値:** seconds、minutes、hours、days、weeks、months、years、infinity

**デフォルト値:** なし

**length** 間隔の長さを指定します。

**有効値:** 30 秒～ infinity

**デフォルト値:**

- 30 (時間単位が秒の場合)
- 15 (時間単位が分の場合)
- 1 (時間単位が時の場合)
- 1 (時間単位が日の場合)
- 1 (時間単位が月の場合)
- 1 (時間単位が年の場合)

例:

```
DHCP Server config> set used-ip-address-expire-interval seconds
How long is the interval in seconds (max:59) [30]? 2
```

例:

```
DHCP Server config> set used-ip-address-expire-interval minutes
How long is the interval in minutes (max:59) [15]? 2
```

例:

```
DHCP Server config> set used-ip-address-expire-interval hours
How long is the interval in hours (max:23) [1]? 5
```

例:

```
DHCP Server config> set used-ip-address-expire-interval days
How long is the interval in days (max:6) [1]? 2
```

例:

```
DHCP Server config> set used-ip-address-expire-interval weeks
How long is the interval in weeks (max:3) [1]? 1
```

例:

```
DHCP Server config> set used-ip-address-expire-interval months
How long is the interval in months (max:11) [1]? 3
```

例:

```
DHCP Server config> set used-ip-address-expire-interval years
How long is the interval in years (max:10) [1]? 3
```

例:

```
DHCP Server config> set used-ip-address-expire-interval infinity
```

## DHCP サーバー監視環境へのアクセス

DHCP サーバー監視 プロセスにアクセスするには、次の手順を使用します。

1. OPCON プロンプトで **talk 5** を入力する。たとえば、次のように入力します。

```
* talk 5
Config>
```

**talk 5** コマンドを入力すると、端末に CONFIG プロンプト (+) が表示されます。最初に構成に入ったときにプロンプトが表示されない場合は、**Return** をもう一度押してください。

2. + プロンプトで、**feature dhcp-server** コマンドを入力して、DHCP Server> プロンプトを表示する。

## DHCP サーバー監視コマンド

表 59. DHCP サーバー監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxixページの『ヘルプの入手』を参照してください。
Disable	DHCP サーバーを動的に使用不可にします。
Enable	DHCP サーバーを動的に使用可能にします。
List	クラス、クライアント、グローバル、サブネット、およびベンダー・オプションのパラメーターを表示します。

## DHCP サーバー監視コマンド (Talk 6)

表 59. DHCP サーバー監視コマンドの要約 (続き)

コマンド	機能
Reset	DHCP サーバー構成を動的にリセットします。
Request	
Exit	直前のコマンド・レベルに戻ります。 xxxiiページの『下位レベル操作環境の終了』を参照してください。

### Disable

**disable** コマンドは、DHCP サーバーを動的に使用不可にするために使用します。

構文:

```
disable                dhcp
```

### Enable

**enable** コマンドは、DHCP サーバーを動的に使用可能にするために使用します。

構文:

```
enable                dhcp
```

### List

**list** コマンドは、クラス、クライアント、グローバル・パラメーター、サブネット、またはベンダー・オプションに関する構成情報と、関連したオプションを表示するために使用します。**list** コマンドの例については、519ページの『List』を参照してください。

構文:

```
list                  class  
                        client  
                        global  
                        option  
                        subnet  
                        vendor-option
```

### Reset

**reset** コマンドは、DHCP サーバー構成を動的にリセットするために使用します。

構文:

```
reset                dhcp
```

例:

```
DHCP Server> reset dhcp
You are about to reset the DHCP Server. Clients who have been granted a lease by this
server will need to renew it.
Are you sure you want to continue? [No]: y
DHCP Server has been reset
DHCP Server>
```

## Request

**request** コマンドは、管理情報を表示するために使用します。

構文:

```
request                clientid
                        delete
                        ipquery
                        poolquery
                        stats
                        status
```

**clientid** *client\_id*

クライアントに関する情報を表示します。

**client\_id**

クライアントの ID を指定します。

**有効値:** 既存のクライアント ID

**デフォルト値:** なし

**例:**

```
DHCP Server> request clientid
Enter the client name []? 0020351FB371

Client id: 1-0x0020351FB371
Status: BOUND
Address last assigned: 192.9.200.10
Most recent lease time: 16:41:25 December 3, 1998
Proxy flag: FALSE
Hostname: Win-XY-1
Domain name: city.net
```

**delete** *address*

特定のクライアントの IP アドレスに対するリースを削除します。

**address**

削除するクライアントの IP アドレスを指定します。

**有効値:** 既存クライアントの任意の有効 IP アドレス

**デフォルト値:** なし

**例:**

```
DHCP Server> request delete
Enter the client's IP address []? 194.3.200.10
```

**ipquery** *address*

IP アドレスに関する情報を表示します。

**例:**

## DHCP サーバー監視コマンド (Talk 6)

```
DHCP Server>req ipquery 192.168.8.3
IP address:      192.168.8.3
Status:          RECLAIMED
Lease time:      86400 seconds
Start time:      Not Leased
Last time leased: 04:16:33 March 9, 1999
DHCP Server>
```

### **poolquery** *address*

IP アドレスのプールに関する情報を表示します。

#### **address**

表示するプール内の IP アドレスを指定します。

**有効値:** 表示するプール内にある任意の有効 IP アドレス

**デフォルト値:** なし

#### **例:**

```
DHCP Server> request poolquery
```

```
Enter the client's IP address []? 194.3.200.10
IP address:      194.3.200.10
Status:          LEASED
Lease time:      86400 seconds
Start time:      16:41:25 December 3, 1998
Last time leased: 16:41:25 December 3, 1998
Client id:       1-0x0020351FB371
Hostname:        Win-XY-1
Domain name:     city.net
IP address:      194.3.200.11
Status:          STOCKED
IP address:      194.3.200.12
Status:          STOCKED
```

**stats** サーバーによって管理されているアドレス・プールに関する統計情報を表示します。統計情報には、処理されたディスカバリー・パケット数、無応答のディスカバリー・パケット数、行われた提示数、許可されたリース数、否定応答 (NAK) 数、処理された通知数 (肯定応答 (ACK) を含む)、更新数、解放数、処理された BOOTP クライアント数、proxyARec 更新の試行数、サポートされないパケット数などがあります。

#### **構文:**

```
request                                stats
```

#### **例:**

```
DHCP Server> request stats
Number of DISCOVER requests received:      8
Number of OFFER responses sent:            4
Number of ACK responses sent:              3
Number of NACK responses sent:             0
Number of RELEASE requests received:      0
Number of DECLINE packets received:       0
Number of INFORM requests received:       0
Number of BOOTP requests received:        0
Number of requests received via proxy:    0
Number of UNSUPPORTED requests received:  0
Total number of request/responses:        15
Number of lease expirations:              0
```

**status** アドレス・プールに関する情報を表示します。

#### **例:**

```
DHCP Server> request status
IP address:      194.3.200.10
Status:          LEASED
Lease time:      86400 seconds
```

## DHCP サーバー監視コマンド (Talk 6)

```
Start time:          16:41:25 December 3, 1998
Last time leased:   16:41:25 December 3, 1998
Client id:          1-0x0020351FB371
Hostname:           Win-XY-1
Domain name:        city.net

IP address:         194.3.200.11
Status:             STOCKED

IP address:         194.3.200.12
Status:             STOCKED

IP address:         194.3.200.10
Status:             STOCKED
```

## DHCP サーバー監視コマンド (Talk 6)



## 第32章 シン・サーバー・フィーチャーの使用

この章では、IBM 2212 のシン・サーバー・フィーチャー (TSF) の使用法について説明します。

### ネットワーク・ステーションの概説

ネットワーク・ステーションは、パーソナル・コンピュータ (PC) に似ており、キーボード、ディスプレイ、およびマウスを備えています。ネットワーク・ステーションと PC の主な相違点は、ネットワーク・ステーションのファイルは、マシン内部のハード・ディスク上ではなく、ネットワーク・サーバー上に常駐することです。ネットワーク・ステーションはグラフィカル・ユーザー・インターフェース (GUI) を提供し、ユーザーはこれを使用してエミュレーター、リモート X アプリケーション、Web ブラウザー、アプリケーション、およびプリンターなど、さまざまなリソースにアクセスできます。

ネットワーク・ステーションは、トークンリングまたはイーサネット接続を介し、TCP/IP を使用して、サーバーと通信します。ネットワーク・ステーションの電源オン・プロセスは、次のとおりです。

- 不揮発性ランダム・アクセス・メモリーに常駐するブート・モニター・プログラムが始動し、電源オン自己テストが実行されます。
- ネットワーク・ステーションが、IP アドレス、サーバー・アドレス、およびブート・ファイルのパスと名前などの情報をネットワーク・ステーションに提供する BootP または DHCP サーバーに接続します。代わりに、ネットワーク・ステーションは、不揮発性ランダム・アクセス・メモリーに保管されている値からこの情報を取り出すこともできます。
- ネットワーク・ステーションが、トリビアル・ファイル転送プロトコル (TFTP)、リモート・ファイル・システム/400 (RFS/400)、またはネットワーク・ファイル・システム (NFS) を使用して、オペレーティング・システム、ハードウェア構成ファイル、およびアプリケーション・プログラムなどの基本コードを、基本コード・サーバーからダウンロードします。
- ネットワーク・ステーションが、ネットワーク・ステーションに接続されているプリンターの構成やネットワーク・ステーションのキーボード言語などの端末ベースの構成情報を、端末構成サーバーからダウンロードします。
- ネットワーク・ステーションがログオン画面を表示します。ここで、ユーザー ID とパスワードを入力することができます。
- 認証サーバーがユーザー ID とパスワードの妥当性検査を行い、パーソナル・ユーザー・ファイルへのアクセスを許可します。
- ユーザーの個別設定環境の変更がダウンロードされます。
- ネットワーク・ステーションが個別設定デスクトップを表示します。

ネットワーク・ステーションについて詳しくは、*IBM Network Station Manager Installation and Use*, SC41-0664 を参照してください。

## シン・サーバー・フィーチャーの概説

1 台の物理装置が BootP/DHCP サーバー、ブート・サーバー、端末構成サーバー、および認証サーバーとして機能することも、それぞれのサーバーを別々の装置にすることもできます。たとえば、ネットワーク・ステーションを AS/400 に接続し、AS/400 が BootP サーバー、基本コード・サーバー、端末構成サーバー、および認証サーバーの役割を果たすことができます。代わりに、各サーバーを別々の物理装置にすることもできます。たとえば、NT サーバーが DHCP サーバーとして働き、AS/400 が基本コード・サーバー、別の AS/400 が端末構成サーバー、さらに別の AS/400 が認証サーバーとして働くネットワークにネットワーク・ステーションを接続するといったことが可能です。

シン・サーバー・フィーチャーを使用すると、2212 を基本コード・サーバーにすることができます。TSF の使用が望ましい理由を示す 1 つの例を、541ページの図47 と 541ページの図48 に示します。541ページの図47 では、ネットワーク・ステーションに必要なファイルはすべて単一のサーバーからダウンロードされます。ネットワーク・ステーションの電源オン時には、ダウンロードは数メガバイトに達します。これは、特に多数のネットワーク・ステーションが同時に電源を入れた場合、ネットワーク・インフラストラクチャーだけではなく、基本コード / 端末構成サーバーまたは認証サーバーとして働く装置にとっても非常に大きな負担がかかる可能性があります。541ページの図48 は、リモート側でシン・サーバーが使用されているネットワークを示しています。ネットワーク・ステーションのブート・コードに関連するファイルの多くは、シン・サーバーによってキャッシュされます。ネットワーク・ステーションの電源をオンにしたとき、ほとんどのブート・コードはシン・サーバーからロードされ、ネットワーク・インフラストラクチャーを通してトランスポートする必要があるデータはわずかな量だけになります。このように 1 つのサーバーの処理が減ることにより、ネットワーク・トラフィックが減少し、ネットワーク・ステーションの電源オンを完了させるのに必要な時間を短縮することができます。

シン・サーバーによってキャッシュされるファイルは、マスター・ファイル・サーバーに常駐するファイルのコピーなので、マスター・ファイル・サーバー上のバージョンが変更された場合、シン・サーバーはそのファイルのバージョンを更新する必要があります。次の時点で、シン・サーバーは、すべてのキャッシュ・ファイルがマスター・ファイル・サーバーのバージョンと同一であることを確認します。

1. IBM 2212 の電源オン時
2. IBM 2212 の再ロードまたはリスタート時
3. TSF のリスタート時
4. TSF 構成で指定された時間間隔に達したとき
5. SNMP MIB アクション・パラメーターによって起動されたとき
6. TSF talk 5 **refresh** コマンドが出されたとき
7. ファイルにアクセスするたびに (TFTP を除く)。TSF は、アクセスした各ファイルが、マスター・ファイル・サーバー上のバージョンに一致していることを確認します。相違が検出された場合、ファイルは更新されます。その後で TSF は、残りのファイルもマスター・ファイル・サーバーに一致していることを確認します。

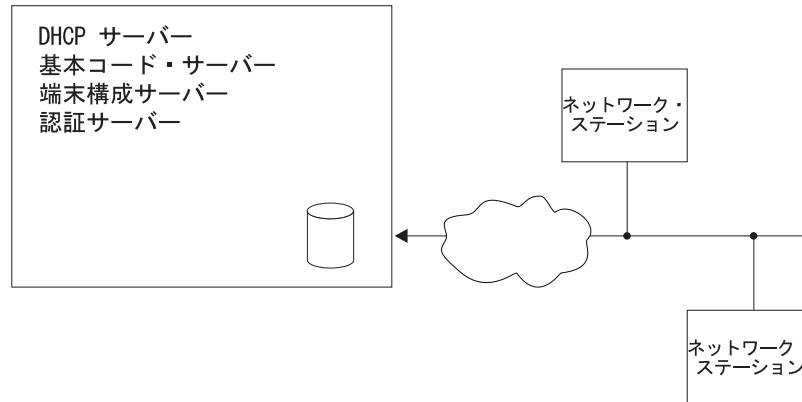


図 47. シン・サーバーのないリモート・ネットワーク・ステーション

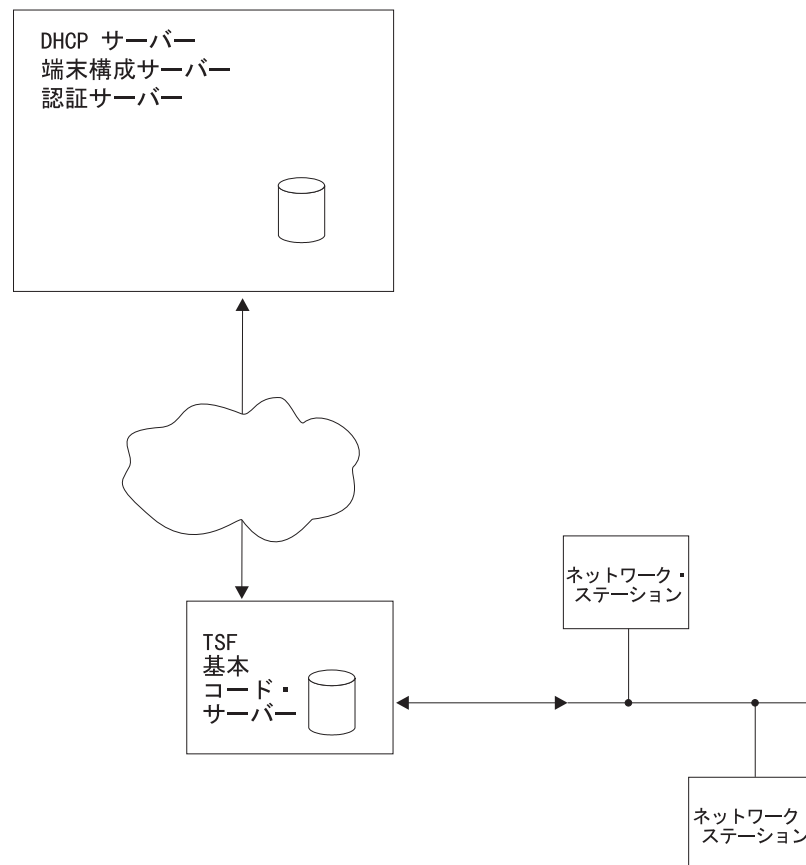


図 48. シン・サーバーのあるリモート・ネットワーク・ステーション

## BootP/DHCP サポート

BootP/DHCP サーバー・サポートには、次の 2 つのオプションがあります。

- IBM 2212 DHCP サーバー・サポートを使用する。475ページの『第30章 DHCP サーバーの使用』を参照してください。

## TSF の使用

- BootP/DHCP 要求のリレー・エージェントとして機能するように IBM 2212 を構成する。詳しくは、*プロトコル構成および監視 参照資料 第 1 巻* を参照してください。

複数サーバー環境について詳しくは、*IBM Network Station Manager Installation and Use*, SC41-0664 を参照してください。

---

## ネットワーク・ステーションとの通信に使用するプロトコル

ネットワーク・ステーションとそのサーバー間の通信に使用するプロトコルは、BootP/DHCP の構成またはネットワーク・ステーション NVRAM の構成のどちらかで決めます。どちらの場合も、ネットワーク・ステーションが使用するプロトコルは、TSF の構成と互換性がなければなりません。

TSF がマスター・ファイル・サーバーとの通信に RFS を使用するように構成されている場合、TSF はネットワーク・ステーションからの RFS および TFTP 要求は受け入れませんが、ネットワーク・ステーションからの NFS 要求には応答しません。

同様に、TSF がマスター・ファイル・サーバーとの通信に NFS を使用するように構成されている場合、TSF はネットワーク・ステーションからの NFS および TFTP 要求は受け入れませんが、ネットワーク・ステーションからの RFS 要求には応答しません。

## RFS の使用

TSF は、RFS を使用して AS/400 への接続を確立します。ネットワーク・ステーションがファイルのオープンを要求すると、TSF は認証のためにその要求を AS/400 に転送します。ネットワーク・ステーションが認証されなかった場合、TSF は要求されたファイルをネットワーク・ステーションに送りません。ネットワーク・ステーションが認証され、AS/400 上の要求されたファイルのバージョンが IBM 2212 TSF に保管されているバージョンと異なっている場合、ネットワーク・ステーションの要求は AS/400 に渡されます。AS/400 上のファイルが、TSF がキャッシュしたファイルと同じバージョンの場合には、TSF はそのファイルをネットワーク・ステーションに提供します。

TSF から AS/400 への接続が利用不能の場合は、TSF は現在キャッシュされているファイルをネットワーク・ステーションに提供します。

## TFTP の使用

ネットワーク・ステーションと TSF の間の通信に TFTP が使用されている場合、ファイルが利用可能であれば、TSF はネットワーク・ステーションからのファイルの要求に応じます。TSF とマスター・ファイル・サーバーの間のバージョンの確認は行われません。ファイルが TSF キャッシュ内にはない場合には、ネットワーク・ステーションからの要求はマスター・ファイル・サーバーに転送されます。

## NFS の使用

ネットワーク・ステーションと TSF の間の通信に NFS が使用されている場合、ネットワーク・ステーションからファイルの要求があると、TSF はそのファイルがキャッシュ内にある場合は、ファイルのサービスを開始します。同時に、そのファイルがマスター・ファイル・サーバー内のものと同じバージョンであるかどうかを確認します。同じでない場合、TSF はファイルのサービスを打ち切り、ただちにマスター・ファイル・サーバーから新しいバージョンのダウンロードを開始します。

TSF がそのファイルをキャッシュしていない場合、TSF は "ファイルが見つからない" というメッセージを戻します。要求されたファイルが、サブディレクトリー組み込みとして構成されているディレクトリー内に常駐している場合、またはそのような構成のディレクトリー下のサブディレクトリー内に常駐している場合、ファイルがマスター・ファイル・サーバー内に存在すれば、TSF はファイルのキャッシュを開始します。

---

## ファイル・キャッシュの更新

IBM 2212 のファイル・キャッシュに使用するプロトコルは、TSF の構成によって決まります。**add master-file-server** コマンドを使用して、マスター・サーバーを指定します。

*nfs* を指定すると、事前ロード・リスト・ファイル名の入力を求めるプロンプトが出ます。事前ロード・リストとは、TSF がキャッシュする必要があるファイルの完全修飾ファイル名を指定する ASCII ファイルです。

*nfs* を指定すると、キャッシュするディレクトリー名の入力を求めるプロンプトが出ます (いくつかのデフォルト値が提供される場合もあります)。ディレクトリーを指定すると、サブディレクトリーを組み込むかどうかを尋ねるプロンプトが出ます。*no* (サブディレクトリーを組み込まない) を指定すると、TSF は指定されたディレクトリー内のすべてのファイルを TSF キャッシュに事前ロードします。*yes* (サブディレクトリーを組み込む) を指定すると、TSF はそのディレクトリーからはどのファイルも事前ロードせず、ネットワーク・ステーションがファイルを要求した時点で、そのディレクトリーとサブディレクトリーから動的にファイルを取り出します。

更新処理が進行中のファイルは、処理中はネットワーク・ステーションに送られません。

---

## シン・サーバー環境の構成

TSF をインストールする場合、TSF 自体の他にいくつかの構成を考慮することが必要になります。ここでは、BootP/DHCP サーバー、マスター・ファイル・サーバー、IBM 2212 BootP リレー、IBM 2212 内部 IP アドレス、および IBM 2212 TSF 構成に加える必要がある変更について説明します。Network Station Manager Release 2.5 を実行している AS/400 に接続されたシン・サーバーの例を 546ページの『サンプル構成』に示します。

シン・サーバー環境の構成プロセスについては、次で説明しています。

## TSF の使用

- 『構成に関する推奨事項』
- 545ページの『BootP/DHCP サーバーの構成』
- 545ページの『シン・サーバー環境用のサーバーの構成』
- 545ページの『BootP リレーの構成』
- 546ページの『内部 IP アドレスの構成』
- 546ページの『TSF の構成』
- 546ページの『サンプル構成』

## 構成に関する推奨事項

TSF を最大限に活用するのに役立つ、構成に関する推奨事項を次に示します。

- ハード・ディスクを使用する。

TSF は必ずしもハード・ディスクを必要としませんが、構成されている TSF メモリー・キャッシュが小さ過ぎる場合 (または、2212 内の他の機能のために十分な大きさに構成できない場合)、これを使用すると効率を高めることができます。ハード・ディスクを使用すると、TSF や 2212 をリスタートまたは再ロードした場合にも、効率が改善されます。

- ネットワーク・ステーションの最大数。

TSF は、同時に最大 200 の RFS ネットワーク・ステーション接続ができます。同時に 30 ~ 40 台のネットワーク・ステーションの電源をオンにすると、ネットワーク・ステーションのタイムアウト値を超える遅延が生じる場合があります。回復のためには、ネットワーク・ステーションの電源を再度オンにする必要が生じる場合があります。

- マスター・ファイル・サーバーは、Network Station Manager を稼働するサーバーにする。

TSF では、マスター・ファイル・サーバー IP アドレスは任意の値にすることができますが、これは Network Station Manager (NSM) を稼働する装置のアドレスに設定することをお勧めします。これにより、ファイル構造がネットワーク・ステーションと互換性を持ち (つまり、TSF とも互換性を持ち)、TSF が要求するファイルを提供できるようになります。

- すべてのキャッシュ・ファイルをメモリーに保管できる十分な量のメモリーを定義する。

ハード・ディスクを使用しない場合は、これは必須の要件です。ハード・ディスクを使用する場合でも、メモリーへのアクセスはハード・ディスクへのアクセスよりはるかに高速です。必要なメモリーの量は、ユーザーの環境によって異なります。Talk 5 **list config** コマンドを使用して、ユーザーの特定状況下でのファイル・セットの大きさを調べてください。Hard File storage being used for Thin Server (シン・サーバー用に使用されているハード・ディスク記憶域) に表示される値は、ファイル・セットのサイズを KB 単位で示しています。ただし、異なるタイプのネットワーク・ステーションまたはアプリケーションをユーザー環境に追加または削除した場合、この値は変更される可能性があります。

- NFS を使用している場合、TSF は必要なファイルを動的に確認する。

この確認プロセスでは、TSF がすべての必要なファイルを識別するために、ネットワーク・ステーション電源オン・シーケンスを数回実行することが必要になる場合があります。



## BootP/DHCP サーバーの構成

Network Station Manager Release 3 を稼働している場合、シン・サーバーを使用するためには DHCP が必要です。AS/400 をマスター・ファイル・サーバーとして使用している場合は、Network Station Manager Release 2.5 を使用することも可能で、その場合は DHCP の代わりに BootP を使用できます。

BootP の場合は、1 つのサーバー・アドレスしか指定できません。そのアドレスは **sa** タグを使用して指定します。このタグは、ネットワーク・ステーションの BootP レコード内にすでに存在する場合も、存在しない場合もあります。存在しない場合は、タグを作成し、その値を 2212 の内部 IP アドレスに設定してください。すでに存在する場合は、その値を 2212 の内部 IP アドレスに変更してください。

DHCP では、シン・サーバーを使用する場合に変更が必要になるフィールドは、次のとおりです。

- オプション 66 またはブートストラップ・サーバー - 基本コード・サーバー IP アドレス

この値は、IBM 2212 内部 IP アドレスに設定する必要があります。

- オプション 211 - 基本コード・サーバーに使用するプロトコル

シン・サーバーのマスター・ファイル・サーバー・タイプを NFS に構成する場合、これは *nfs* または *tftp* のどちらかでなければなりません。シン・サーバーのマスター・ファイル・サーバー・タイプを RFS に構成する場合、これは *rfs/400* または *tftp* のどちらかでなければなりません。

- オプション 212 - 端末構成サーバー

このアドレスは、マスター・ファイル・サーバー IP アドレスと同じでなければなりません。このアドレスはシン・サーバーの IP アドレスであってはなりません。

NS と BootP および DHCP の関係について詳しくは、*IBM Network Station Manager Installation and Use*、SC41-0664 を参照してください。

## シン・サーバー環境用のサーバーの構成

RFS の場合、事前ロード・リストを AS/400 にインストールする必要があります。事前ロード・リストは、インターネットの

<http://www.networking.ibm.com/netprod.html#routers> から入手できます。このサイトから LoadList.file をファイル転送し、それを AS/400 上の /QIBM/ProdData/ OS400/NetStationRmtController に入れます。NetStationRmtController ディレクトリーを作成することが必要になる場合があります。

NFS の場合は、シン・サーバー用の特別な変更は必要ありません。

## BootP リレーの構成

IBM 2212 の BootP リレー・エージェントを使用可能にし、適切な BootP および DHCP サーバーを構成しないと、BootP リレーはこれらのサーバーに転送されません。詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きを参照してください。

## TSF の使用

### 内部 IP アドレスの構成

内部 IP アドレスがすでに存在する場合は、特別な変更は必要ありません。現在、内部 IP アドレスが指定されていない場合は、指定する必要があります。詳しくは、プロトコル構成および監視 参照資料 第 1 巻 を参照してください。

### TSF の構成

553ページの『第33章 シン・サーバー機能の構成および監視』に説明されているコマンドを使用して、シン・サーバーを構成します。

最小限、次のコマンドを入力しなければなりません。

1. **load add package thin-server**
2. **set mode enable**
3. **add master-server**

---

### サンプル構成

次の例は、Network Station Manager R2.5 を稼働する AS/400 に接続する TSF を構成します。

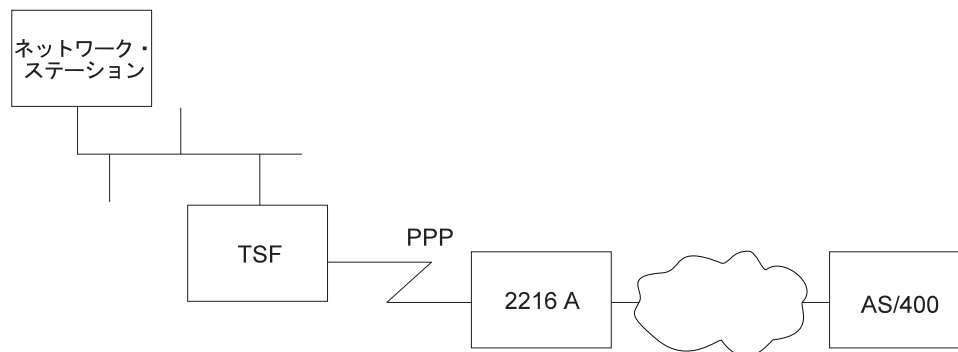


図 49. TSF サンプル構成

次の説明は、上記のネットワークに基づき、次の条件を想定してシン・サーバー・フィーチャーを構成する場合を示しています。

- AS/400 は BootP サーバーである。
- 2216 A はルーターである (TSF は構成されず、TSF 用の特別な構成もない)。
- ネットワーク IP 接続性は確認済みである。つまり、AS/400 は IBM 2212 (TSF) に PING でき、IBM 2212 は AS/400 に PING できる。
- BootP リレーは現在、IBM 2212 (TSF) で使用可能にされていない。
- IP 内部アドレスは現在、IBM 2212 (TSF) に構成されていない。

### AS/400 の構成

#### BootP (NSM リリース 2.5)

1. NSM を使用して、NS を定義する。



2. BootP テーブルを、ASCII エディターを備えたシステムに ftp (ファイル転送) する。

```
c:\>ftp as400a
Connected to as400a.raleigh.ibm.com.
220-QTCP at AS400A.RALEIGH.IBM.COM.
220 Connection will close if idle more than 5 minutes.
Name (as400a:goofy): qsecofr
331 Enter password. Password:
230 QSECOFR logged on.
ftp> ascii
ftp> get qusrsys/qatodbtp.bootptab bootptab
ftp> quit
```

3. ASCII エディターを使用してファイルを編集し、"sa" タグを指定された 2212 (TSF) の内部 IP アドレスに追加する。

```
OLD LINE
-----
NSEN106:ip=192.9.250.36:bt=IBMNSM:ht=1:ha=00.00.A7.01.2E.35:
sm=255.255.248.0:gw=192.9.250.6:bf=KERNEL:
hd=/QIBM/PRODDATA/NETWORKSTATION

MODIFIED LINE
-----
NSEN106:ip=192.9.250.36:bt=IBMNSM:ht=1:ha=00.00.A7.01.2E.35:
sm=255.255.248.0:gw=192.9.250.6:bf=KERNEL:
hd=/QIBM/PRODDATA/NETWORKSTATION:sa=192.9.250.6
```

ここで、192.9.250.6 は 2212 (TSF) の内部 IP アドレスです。

4. BootP テーブルを ftp (ファイル転送) して AS/400 に戻す。

```
c:\> ftp as400a
Connected to as400a.raleigh.ibm.com.
220-QTCP at AS400A.RALEIGH.IBM.COM.
220 Connection will close if idle more than 5 minutes.
Name (as400a:goofy): qsecofr
331 Enter password.
Password:
230 QSECOFR logged on.
ftp> ascii
ftp> put bootptab qusrsys/qatodbtp.bootptab
ftp> quit
```

## 事前ロード・リストの設定

事前ロード・リストは、インターネット

<http://www.networking.ibm.com/netprod.html#routers> から入手できます。

事前ロード・リストを入手したら、それを AS/400 に "ftp" することができます。

1. ローカル・ディレクトリーが "LoadList.file" の場所に設定されていることを確認する。
2. AS/400 に ftp する - "test400" は、この例の AS/400 の名前です。

```
ftp test400
Connected to test400.raleigh.ibm.com.
Name (test400:root): qsecofr
Enter password.
Password:
QSECOFR logged on.
```

3. ターゲット AS/400 上の正しいディレクトリーに変更する。

## TSF の使用

```
ftp> cd /
Current directory changed to /.
ftp> cd qibm/proddata/os400/
Current directory changed to /qibm/proddata/os400.
ftp> dir
PORT subcommand request successful.
List started.
QTCP          34816 04/30/97 02:50:36 *DIR    REXEC/
QSECOFR       33792 07/24/98 08:04:55 *DIR    NetStationRmtController/
List completed.
```

- ディレクトリー "NetStationRmtController" が存在しない場合は、それを作成することが必要になります。

```
ftp> MKD
(directory - name) NetStationRmtController
Created directory /qibm/proddata/os400/netstationrmtcontroller
```

- NetStationRmtController ディレクトリーに変更する。

```
ftp> cd NetStationRmtController
Current directory changed to /qibm/proddata/os400/Netstationrmtcontroller.
```

- ファイルを AS/400 に転送する。

```
ftp> ascii
Representation type is ASCII nonprint.
ftp> put LoadList.file
PORT subcommand request successful.
Sending file to /qibm/proddata/os400/Netstationrmtcontroller
File transfer completed successfully.
```

## TCP/IP の構成

TCP/IP 構成は、ユーザー特定の環境に依存します。

## IBM 2212 (TSF) の構成

### BootP リレー

- BootP リレーがすでに構成されているかどうかを調べる。

```
*
*
t 6
Config>protocol ip
Internet protocol user configuration
IP config>list bootp
BOOTP forwarding: enabled
Max number of BOOTP forwarding hops: 4
Min secs of retry before forwarding: 0
Configured BOOTP servers:      192.9.220.21
IP config>
```

- すでに使用可能にされていない場合は、それを使用可能にする。

```
IP config>enable bootp
Maximum number of forwarding hops [4]?
Minimum seconds before forwarding [0]?
IP config>
```

- ネットワーク・ステーション BootP または DHCP サーバーが、構成されたサーバーのリストに含まれていない場合は、それを追加する。

```
IP config>add bootp-server
BOOTP server address [0.0.0.0]? 9.37.121.6
IP config>
```

## 内部 IP アドレス

1. 内部 IP アドレスがすでに構成されているかどうかを調べる。

```
Config>protocol ip
Internet protocol user configuration
IP config>list addresses
IP addresses for each interface:
  intf    0   9.37.177.97      255.255.248.0   Local wire...
  intf    1  192.9.220.2          255.255.255.0   Local wire...
  intf    2  192.9.250.6           255.255.255.0   Local wire...
  intf    3  192.9.222.2           255.255.255.0   Local wire...
  intf    4
  intf    5
  intf    6  192.9.223.2           255.255.255.0   Local wire...
IP config>
```

2. 内部 IP アドレスを構成する。

```
IP config>set internal-ip-address
Internal IP address [192.9.223.2]? 192.9.250.6
IP config>
```

3. 再度、アドレスを表示する。

```
IP config>list addresses
IP addresses for each interface:
  intf    0   9.37.177.97      255.255.248.0   Local wire
  intf    1  192.9.220.2          255.255.255.0   Local wire
  intf    2  192.9.250.6           255.255.255.0   Local wire
  intf    3  192.9.222.2           255.255.255.0   Local wire
  intf    4
  intf    5
  intf    6  192.9.223.2           255.255.255.0   Local wire
Internal IP address: 192.9.250.6
IP config>
```

## シン・サーバー・フィーチャー

1. ロード・パッケージ thin-server を追加する。

ロード・パッケージを追加しておかないと、シン・サーバー・フィーチャーを構成することができません。

最初にシン・サーバー・パッケージが利用可能であることを確認します。

```
Config>load list available
Available Packages
-----
appn package
tn3270e package
thin-server package
Config>
```

利用可能でない場合は、先に進む前に、正しいソフトウェア・バージョンを入手する必要があります。

利用可能な場合は、パッケージがすでにロードされていないことを確認します。

```
Config>load list configured
Configured Packages
-----
thin-server package
Config>
```

すでにロード / 構成されている場合は (上記のように)、TSF の構成に進むことができます。まだロードされていない場合は、シン・サーバー・パッケージを追加する必要があります。

```
Config>load add package thin-server
thin-server package configured successfully
This change requires a reload.
Config>
```

- 再ロードする。

シン・サーバー・パッケージを追加しなければならなかった場合は、ここで構成を書き込み、IBM 2212 を再ロードする必要があります。

- モードを使用可能に設定する。

パッケージをロードした場合、初期時にはシン・サーバーは使用不可になっています。モードを使用可能に設定しないと、他のシン・サーバー・パラメーターを構成できません。

```
*
*
t 6
Config>feature tsf
Thin server config>set mode enable

Thin server feature (TSF) is fully enabled once
you have entered a Master File Server for either
RFS or NFS. Please add a master-file-server if
one is not already configured.
Thin server config>
```

- master-file-server を追加する。

シン・サーバー・フィーチャーを使用可能にしたら、マスター・ファイル・サーバーを構成する必要があります。この例の場合、マスター・ファイル・サーバーは AS/400 なので、RFS マスター・ファイル・サーバーを追加します。このネットワークの場合は、デフォルトの TFTP タイムアウトおよび再試行パラメーターが適当です。

```
Thin server config>add master-file-server rfs-as400
File Server IP address [0.0.0.0]? 9.37.100.68
TFTP Packet Timeout in seconds (5 - 10) [5]?
TFTP Max Retry Limit (1 - 10) [1]? 7
TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192)
[8192]?
Pre-load File name
[/QIBM/ProdData/OS400/NetstationRmtController/Load list.file]?
Thin server config>
```

トークンリング・インターフェース上の AS/400 の IP アドレスは 9.37.100.68 です。事前ロード・リスト・ファイルを AS/400 にインストールしたときに、その名前をシン・サーバーのデフォルト名に一致するように指定したので、変更する必要はありません。

- time-to-refresh-pre-load-list を設定する (任意選択)。

リフレッシュを実行する時間のデフォルト値は 1:00 AM です。この時間は、大きなファイルが変更され、Thin サーバーがダウンロードすることが必要になった場合、パフォーマンスへの影響を最小限にするために選択されたものです。

- interval-pre-load-list を設定する (任意選択)。

キャッシュ・ファイルを検査する間隔のデフォルト値は、master-file-server と同じレベルで、毎日です。このパラメーターの値と time-to-refresh-pre-load-list パラメーターの値によって、ファイルを検査する頻度が決まります。ネットワーク・ステーションのファイルの変更が頻繁に行われない場合、これらの値は、1 週間に 1 回、または 1 か月に 1 回更新するように設定することができます。

7. メモリーを設定する (任意選択)。

ファイル・キャッシュ用のデフォルト・メモリーは 16 MB RAM キャッシュで、これで十分のはずです。複数のネットワーク・ステーションが TSF を使用している場合は、544ページの『構成に関する推奨事項』の推奨値を参照してください。

8. ハード・ディスクを設定する (任意選択)。

ハード・ディスクの使用をお勧めします。ハード・ディスクを使用しない場合は、このパラメーターを *no* に設定します。



---

## 第33章 シン・サーバー機能の構成および監視

この章では、シン・サーバー機能 (TSF) の構成および動作コマンドの使用方法について説明し、次の内容が記載されています。

- 『TSF 構成環境へのアクセス』
- 『TSF 構成コマンド』
- 562ページの『TSF 監視環境へのアクセス』
- 562ページの『TSF 監視コマンド』

---

### TSF 構成環境へのアクセス

TSF 構成プロセスにアクセスするには、次の手順を使用します。

1. OPCON プロンプトで、**talk 6** と入力する。(このコマンドについて詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の“OPCON プロセスおよびコマンド”の章を参照してください。)たとえば、次のように入力します。

```
* talk 6
Config>
```

**talk 6** コマンドを入力すると、CONFIG プロンプト (Config>) が端末に表示されます。最初に構成に入ったときにプロンプトが表示されない場合は、**Return** をもう一度押してください。

2. CONFIG プロンプトで **feature tsf** コマンドを入力して Thin server config> プロンプトを表示する。

---

### TSF 構成コマンド

TSF を構成するには、Thin server config> プロンプトでコマンドを入力します。

表 60. TSF 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxiiページの『ヘルプの入手』を参照してください。
Add	Adds マスター・ファイル・サーバー (RFS または NFS) を追加します。
Delete	Deletes マスター・ファイル・サーバー (RFS または NFS) を削除します。
List	シン・サーバー構成を表示します。
Modify	Modifies マスター・ファイル・サーバー (RFS または NFS) を変更します。
Set	シン・サーバー・パラメーターを設定します。
Exit	直前のコマンド・レベルに戻ります。xxxiiページの『下位レベル操作環境の終了』を参照してください。

#### Add

**add** コマンドは、マスター・ファイル・サーバー構成を追加するのに使用します。

## TSF 構成コマンド (Talk 6)

master-file-server タイプとして *nfs* を選択した場合、シン・サーバーは NFS を使用してマスター・ファイル・サーバーと通信してファイルを同期化し、NS は TFTP または NFS を使用してシン・サーバーと通信することができます。master-file-server タイプとして *rfs* を選択した場合、シン・サーバーは RFS を使用してマスター・ファイル・サーバーと通信してファイルを同期化し、NS は TFTP または RFS を使用してシン・サーバーと通信することができます。

構文:

```
add master-file-server      nfs-s390  
                             nfs-nt  
                             nfs-aix  
                             nfs-other  
                             rfs-as400
```

### **nfs-s390**

TSF が S/390 に接続されている場合に使用します。

#### **file server IP address**

有効値: 任意の有効な IP アドレス

デフォルト値: なし

#### **tftp packet timeout**

有効値: 5 ~ 10 秒

デフォルト値: 5

#### **tftp maximum retry limit**

有効値: 1 ~ 10

デフォルト値: 1

#### **maximum segment size**

最大パケット・セグメント・サイズを指定します。

有効値: 512、1024、2048、4096、8192 (バイト)

デフォルト値: 8192

#### **additional include subdirectories**

組み込みサブディレクトリーを追加するかどうかを指定します。追加のサブディレクトリーは、TSF がデフォルト・ディレクトリー内に存在しないファイルをキャッシュする必要がある場合に指定できます。

有効値: yes または no

デフォルト値: yes

#### **additional include subdirectory path**

追加する組み込みサブディレクトリーのパスを指定します。

有効値: a ~ z、A ~ Z、0 ~ 9、., \_、--, /

デフォルト値: なし



**include all subdirectories under this directory**

指定した追加サブディレクトリー・パス内のすべてのネストされたサブディレクトリーを含めるかどうかを指定します。

有効値:

- No

TSF は、指定されたディレクトリー内のすべてのファイルを事前ロードします。

- Yes

TSF は、指定されたディレクトリー内のファイルを事前ロードしません。代わりに、TSF は必要になった時点で、ディレクトリーとそのサブディレクトリーからファイルをロードします。

デフォルト値: no

**nfs-nt** TSF が Windows-NT に接続されている場合に使用します。

**file server IP address**

有効値: 任意の有効な IP アドレス

デフォルト値: なし

**tftp packet timeout**

有効値: 5 ~ 10 秒

デフォルト値: 5

**tftp maximum retry limit**

有効値: 1 ~ 10

デフォルト値: 1

**maximum segment size**

最大パケット・セグメント・サイズを指定します。

有効値: 512、1024、2048、4096、8192 (バイト)

デフォルト値: 8192

**additional include subdirectories**

組み込みサブディレクトリーを追加するかどうかを指定します。

有効値: yes または no

デフォルト値: yes

**additional include subdirectory path**

追加する組み込みサブディレクトリーのパスを指定します。

有効値: a ~ z、A ~ Z、0 ~ 9、., \_、--, /

デフォルト値: なし

**include all subdirectories under this directory**

指定した追加サブディレクトリー・パス内のすべてのネストされたサブディレクトリーを含めるかどうかを指定します。

有効値:

- No

## TSF 構成コマンド (Talk 6)

TSF は、指定されたディレクトリー内のすべてのファイルを事前ロードします。

- Yes

TSF は、指定されたディレクトリー内のファイルを事前ロードしません。代わりに、TSF は必要になった時点で、ディレクトリーとそのサブディレクトリーからファイルをロードします。

デフォルト値: no

### nfs-aix

TSF が AIX に接続されている場合に使用します。

#### file server IP address

有効値: 任意の有効な IP アドレス

デフォルト値: なし

#### tftp packet timeout

有効値: 5 ~ 10 秒

デフォルト値: 5

#### tftp maximum retry limit

有効値: 1 ~ 10

デフォルト値: 1

#### maximum segment size

最大パケット・セグメント・サイズを指定します。

有効値: 512、1024、2048、4096、8192 (バイト)

デフォルト値: 8192

#### additional include subdirectories

組み込みサブディレクトリーを追加するかどうかを指定します。

有効値: yes または no

デフォルト値: yes

#### additional include subdirectory path

追加する組み込みサブディレクトリーのパスを指定します。

有効値: a ~ z、A ~ Z、0 ~ 9、.. \_、--、/

デフォルト値: なし

#### include all subdirectories under this directory

指定した追加サブディレクトリー・パス内のすべてのネストされたサブディレクトリーを含めるかどうかを指定します。

有効値:

- No

TSF は、指定されたディレクトリー内のすべてのファイルを事前ロードします。

- Yes

## TSF 構成コマンド (Talk 6)

TSF は、指定されたディレクトリー内のファイルを事前ロードしません。代わりに、TSF は必要になった時点で、ディレクトリーとそのサブディレクトリーからファイルをロードします。

デフォルト値: no

### nfs-other

手動ですべてのサブディレクトリーを指定したい場合に使用します。

#### file server IP address

有効値: 任意の有効な IP アドレス

デフォルト値: なし

#### tftp packet timeout

有効値: 5 ~ 10 秒

デフォルト値: 5

#### tftp maximum retry limit

有効値: 1 ~ 10

デフォルト値: 1

#### maximum segment size

最大パケット・セグメント・サイズを指定します。

有効値: 512、1024、2048、4096、8192 (バイト)

デフォルト値: 8192

#### additional include subdirectories

組み込みサブディレクトリーを追加するかどうかを指定します。

有効値: yes または no

デフォルト値: yes

#### additional include subdirectory path

追加する組み込みサブディレクトリーのパスを指定します。

有効値: a ~ z、A ~ Z、0 ~ 9、.. \_、--、 /

デフォルト値: なし

#### include all subdirectories under this directory

指定した追加サブディレクトリー・パス内のすべてのネストされたサブディレクトリーを含めるかどうかを指定します。

有効値:

- No

TSF は、指定されたディレクトリー内のすべてのファイルを事前ロードします。

- Yes

TSF は、指定されたディレクトリー内のファイルを事前ロードしません。代わりに、TSF は必要になった時点で、ディレクトリーとそのサブディレクトリーからファイルをロードします。

デフォルト値: no

## TSF 構成コマンド (Talk 6)

### rfs-as400

TSF が AS/400 に接続されている場合に使用します。

#### file server IP address

有効値: 任意の有効な IP アドレス

デフォルト値: なし

#### tftp packet timeout

有効値: 5 ~ 10 秒

デフォルト値: 5

#### tftp maximum retry limit

有効値: 1 ~ 10

デフォルト値: 1

#### maximum segment size

最大パケット・セグメント・サイズを指定します。

有効値: 512、1024、2048、4096、8192 (バイト)

デフォルト値: 8192

#### pre-load file name

事前ロード・ファイルの名前とパスを指定します。

有効値: a ~ z、A ~ Z、0 ~ 9、., \_、--, /

デフォルト値:

/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file

### 例: NFS の場合

```
Thin server config> add master-file-server nfs
File Server IP address [0.0.0.0]? 10.22.55.94
TFTP Packet Timeout in seconds (5 - 10) [5]? 6
TFTP Max Retry Limit (1 - 10) [1]? 7
TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192) [8192]? 512
```

Default Include Directories:

Include Directory List Follows:

Include

all

Subdirs? Directory Names

```
-----
N /hfs/usr/lpp/nstation/standard
Y /hfs/usr/lpp/nstation/standard/mods
Y /hfs/usr/lpp/nstation/standard/nls
Y /hfs/usr/lpp/nstation/standard/fonts
Y /hfs/usr/lpp/nstation/standard/java
Y /hfs/usr/lpp/nstation/standard/keyboards
Y /hfs/usr/lpp/nstation/standard/proms
Y /hfs/usr/lpp/nstation/standard/X11
Y /hfs/usr/lpp/nstation/standard/configs
Y /hfs/usr/lpp/nstation/standard/SysDef
Y /hfs/usr/lpp/nstation/standard/zoneinfo
```

Do you want additional Include Subdirectories (Y)es (N)o? [y]

```
Include Subdirectory [ ]? /usr/lpp/nstation/standard/whatever
Include all subdirectories under this directory (Y)es or (N)o? [n]
```

Do you want additional Include Subdirectories (Y)es (N)o? []

### 例: RFS の場合

```
Thin server config> add master-file-server rfs
File Server IP address [0.0.0.0]? 01.01.01.98
TFTP Packet Timeout in seconds (5-10) [5]? 6
TFTP Max Retry Limit (1-10) [1]? 7
TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192) [8192]? 512

Pre-Load File name
[/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file]?
```

## Delete

**delete** コマンドは、マスター・ファイル・サーバー構成を削除するのに使用します。

構文:

```
delete master-file-server      nfs
                                     rfs
```

**nfs** NFS マスター・ファイル・サーバーが構成されている場合に使用します。

**rfs** TSF が RFS マスター・ファイル・サーバー用に構成されている場合に使用します。

## List

**list** コマンドは、TSF 構成を表示するのに使用します。

構文:

```
list all
```

例:

```
Thin server config> list all
```

```
Thin Server Feature:
Enabled
Interval to refresh cache in day(s): 2
Time of day (military time) to refresh cache: 0800
Megabytes used for Thin Server RAM cache: 4
Use Hard File: YES
```

```
Master Thin Server list:
Server IP Address: 9.37.111.12
Server Protocol: NFS
TFTP Packet Timeout in seconds: 10
TFTP Retry Limit                : 6
TFTP Max Segment Size in bytes: 512
```

Initial directories setup for server type: NFS-AIX

NFS Include Directory List Follows:

```
Include
all
subdirs?  Directory Names
-----  -----
N         /usr/netstation
Y         /usr/netstation/mods
Y         /usr/netstation/nls
Y         /usr/netstation/fonts
Y         /usr/netstation/java
Y         /usr/netstation/keyboards
```

## TSF 構成コマンド (Talk 6)

```
Y      /usr/netstation/proms
Y      /usr/netstation/X11
Y      /usr/netstation/configs
Y      /usr/netstation/SysDef
Y      /usr/netstation/zoneinfo
```

## Modify

**modify** コマンドは、マスター・ファイル・サーバー構成を変更するのに使用します。

構文:

```
modify master-file-server   nfs
                               rfs
```

**nfs** NFS マスター・ファイル・サーバーの 1 つが構成された場合に使用します。

**rfs** TSF が RFS マスター・ファイル・サーバー用に構成されている場合に使用します。

例: **NFS** の場合

```
Thin server config> modify master-file-server nfs
File Server IP address [          ]? 10.22.55.94
TFTP Packet Timeout in seconds (5 - 10) [5 ]? 10
TFTP Max Retry Limit (1 - 10) [1]? 6
TFTP Max Segment Size in bytes valid values are 512, 1024, 2048, 4096,
8192) [8192]? 1024

Include subdirectory [/usr/lpp/tcpip/nstation/standard, (Y)es or (N)o [Y]?
Include all subdirectories under this directory (Y)es or (N)o [N]?

Include subdirectory [/usr/lpp/tcpip/nstation/standard/mods], (Y)es or (N)o [Y]?
Include all subdirectories under this directory (Y)es or (N)o [N]?

Include subdirectory [/usr/lpp/tcpip/nstation/standard/nls], (Y)es or (N)o [Y]?
Include all subdirectories under this directory (Y)es or (N)o [N]?

Include subdirectory [/usr/lpp/tcpip/nstation/standard/fonts], (Y)es or (N)o [Y]?
Include all subdirectories under this directory (Y)es or (N)o [N]?

Include subdirectory [/usr/lpp/tcpip/nstation/standard/java], (Y)es or (N)o [Y]?
Include all subdirectories under this directory (Y)es or (N)o [N]?

Include subdirectory [/usr/lpp/tcpip/nstation/standard/keyboards], (Y)es or (N)o [Y]?
Include all subdirectories under this directory (Y)es or (N)o [N]?

Do you want additional Include Subdirectories (Y)es or (N)o? n
```

例: **RFS** の場合

```
Thin server config> modify master-file-server rfs
File Server IP address [09.09.255.253 ]? 01.01.01.98
TFTP Packet Timeout in seconds [5 ]? 10
TFTP Retry Limit [5 ]? 6
TFTP Max Segment Size in bytes [8192]? 512

Pre-Load File name
[/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file]?
```

## Set

**set** コマンドは、TSF 構成パラメーターを設定するのに使用します。

構文:

```
set mode
      interval-pre-load-list
      time-to-refresh-pre-load-list
      memory-cache
      hard-file
```

**mode** TSF のモードを指定します。

有効値:

- enable

enable モードは、TSF は完全に機能し、キャッシュ・ファイルをネットワーク・ステーションに提供することを意味しています。

- disable

disable モードは、TSF は活動状態でなく、ネットワーク・ステーションに応答しないことを意味しています。ネットワーク・ステーションはサーバーに直接接続するように構成する必要があります。

- passthru

passthru モードは、RFS を使用している場合にだけ有効です。Passthru では、ネットワーク・ステーションは TSF に接続できますが、ファイルは常にマスター・ファイル・サーバーから入手されます。

デフォルト値:

#### **interval-pre-load-list**

事前ロード・リストを更新する間隔を日数で指定します。

有効値: 00 ~ 365

デフォルト値: 01

#### **time-to-refresh-pre-load-list**

キャッシュをリフレッシュする時刻を軍用表示 (24 時間) で指定します。

有効値: 0001 ~ 2400

デフォルト値: 0100

#### **memory-cache**

シン・サーバー RAM キャッシュのメモリー量を MB 単位で指定します。ハード・ディスクを使用する場合、TSF の効率と IBM 2212 内の他の機能とのバランスが取れる値を選択することが必要です。ハード・ディスクを使用しない場合、この値はすべてのキャッシュ・ファイルを保持できる十分な大きさにする必要があります。詳しくは、544ページの『構成に関する推奨事項』を参照してください。

有効値: 8 ~ 64 MB

デフォルト値: 16

## TSF 構成コマンド (Talk 6)

### hard-file

ハード・ディスクを使用するかどうかを指定します。

有効値: yes または no

デフォルト値: yes

### 例:

```
Thin server config> set mode passthru
This server feature (TSF) is passthru
Thin server config> set interval-pre-load-list
Interval to refresh the Pre-Load list in days (00-365) [01]? 1
Thin server config> set time-to-refresh-pre-load-list
Time of day to refresh cache in military time (0001-2400) [0100] 0800
Thin server config> set memory-cache
Amount of memory in megabytes for Thin Server RAM cache (8-64MB) [8]
Thin server config> set hard-file
Use the Hard File (Y)ex N(o) [Y]? yes
```

---

## TSF 監視環境へのアクセス

TSF 監視コマンドにアクセスするには、次の手順を使用します。このプロセスにより TSF 監視 プロセスにアクセスできます。

1. OPCON プロンプトで **talk 5** を入力する。(このコマンドについて詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の *OPCON* プロセスおよびコマンド の章を参照してください。) たとえば、次のように入力します。

```
* talk 5
+
```

**talk 5** コマンドを入力すると、端末に GWCON プロンプト (+) が表示されます。最初に構成に入ったときにプロンプトが表示されない場合は、**Return** をもう一度押してください。

2. + プロンプトで **f tsf** コマンドを入力して Thin-Server> プロンプトを表示する。

### 例:

```
+ f tsf
Thin-Server>
```

---

## TSF 監視コマンド

ここでは、TSF 監視コマンドについて説明します。

表 61. TSF 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxiページの『ヘルプの入手』を参照してください。
Delete	シン・サーバー・フィーチャー・ファイル・キャッシュからファイルを削除します。
Flush	シン・サーバー・フィーチャー・ファイル・キャッシュをフラッシュします。
List	シン・サーバーの設定および値を表示します。
Refresh	キャッシュをリフレッシュします。



表 61. TSF 監視コマンドの要約 (続き)

コマンド	機能
Reset	カウンターをリセットします。
Restart	シン・サーバー・プロセスをリスタートします。
Set	シン・サーバー・フィーチャーの設定を変更します。
Exit	直前のコマンド・レベルに戻ります。 xxxiiページの『下位レベル操作環境の終了』を参照してください。

## Delete

**delete** コマンドは、シン・サーバー・フィーチャー・ファイル・キャッシュからファイルを削除するのに使用します。

構文:

**delete** *filename*

**filename**

ファイル・キャッシュから除去するファイルの名前を指定します。

有効値:

デフォルト値: なし

例:

```
Thin-Server> delete
Enter filename to delete from the File Cache: /ibm/prod/ns/5494.dat
Are you sure that you want to delete this file? (Y/ [N]): y
File successfully deleted
```

## Flush

**flush** コマンドは、TSF メモリーおよびハード・ディスクのキャッシュ・スペースをフラッシュするのに使用します。**flush** コマンドは、すべてのキャッシュ・ファイルを消去します。シン・サーバー・キャッシュは、マスター・サーバーからの次のリフレッシュ時に更新されます。リフレッシュが完了するまで、ネットワーク・ステーションに遅延が生じることがあります。

構文:

**flush**

例:

```
Thin-Server> flush
The FLUSH command will erase all cached files.
The Thin Server cache will be updated on the next refresh
from the Master Server. Network Stations may experience
delays until the refresh is completed.
Are you sure you really want to do this? (Y/ [N]): y
All Thin Server cached files have been flushed
```

## List

**list** コマンドは、TSF パラメーター設定値を表示するのに使用します。

構文:

**list** cached-files

## TSF 監視コマンド (Talk 5)

```
config
file-access-counters
file-refresh-counters
pre-load-list
tftp-counters
ts-counters
```

例:

```
Thin-Server> list cached-files
```

```
Cached
File Name      File Size  Time Stamp      Flags  Host File Name
-----
00000026.DAT   2729      04/08/98 13:35:07    RYY   /QIBM/ProdData/OS400/Netstat
ionRmtController/Loadlist.file
00000002.DAT  2049220   09/16/97 08:55:39    RYU   /QIBM/PRODDATA/NETWORKSTATIO
N/KERNEL
                10060     03/04/97 16:12:44    RY-   /QIBM/PRODDATA/NETWORKSTATIO
N/FONTS/PCF/MISC/7X14B.PCF
List is Complete
```

フラグの意味は次のとおりです。

- WhereFrom
  - R = RFS クライアント
  - N = NFS クライアント
  - - = なし
- InTable
  - - = テーブル内に存在しない
  - u (または m) = 更新開始
  - Y = テーブル内に存在
- FileState
  - - = ディスク上に存在しない
  - D = ダーティー
  - A = 更新中止
  - u = 更新開始
  - U = 更新中
  - Y = ディスク上に存在し利用可能

最後の 2 つのフラグの一般的な組み合わせは、次のとおりです (分かりやすいように、3 つのフラグすべてを表示)。

- RYY - 正常なファイル。
- RuY - 完全リフレッシュが進行中で、このファイルはまだ検証されていません。
- RYU - このファイルは更新中です。

例: RFS の場合

```
Thin-Server> list config
Thin Server Configuration
Thin Server feature is: Enabled
Thin Server feature state is: Active, initializing file structure
Interval to refresh Pre-Load List (#days): 1
Time of day (Military) to refresh Pre-Load List: 01:00:00
```

```

Memory (KB) currently using for RAM cache: 25600
Maximum memory (KB) configured for RAM cache: 25600
Currently using Hard File?: Yes
Hard File storage defined for Thin Server: 942752
Hard File storage being used for Thin Server: 0
Number of Files Cached: 0
Master Server IP address: 9.37.177.61
TFTP Packet Timeout Value: 5
TFTP Max Retries: 1
TFTP Max Segment Size: 8192

Thin Server Sync Protocol: RFS
Name of Pre-Load List file:
/QIBM/ProdData/OS400/NetstationRmtController/Loadlist.file
Thin Server>

```

**例: NFS の場合**

Thin-Server> **list config**

```

Thin Server Configuration
Thin Server feature is: Enabled
Thin Server Feature state is: Active, initializing file structure
Interval to refresh Pre-Load List (#days): 1
Time of day (Military) to refresh Pre-Load List: 01:00:00
Memory (KB) currently using for RAM cache: 25600
Maximum memory (KB) configured for RAM cache: 25600
Currently using Hard File?: Yes
Hard File storage defined for Thin Server: 915424
Hard File storage being used for Thin Server: 27328
Number of Files Cached: 82
Master Server IP address: 9.37.181.47
TFTP Packet Timeout Value: 5
TFTP Max Retries: 1
TFTP Max Segment Size: 8192

Thin Server Sync Protocol: NFS
Include Directory List Follows:

Include
all
Subdirs? Directory Names
-----
N /usr/netstation
Y /usr/netstation/mods
Y /usr/netstation/nls
Y /usr/netstation/fonts
Y /usr/netstation/java
Y /usr/netstation/keyboards
Y /usr/netstation/proms
Y /usr/netstation/X11
Y /usr/netstation/configs
Y /usr/netstation/SysDef
Y /usr/netstation/zoneinfo
Thin Server>

```

**例:**

Thin-Server> **list file-access-counters**

```

Disk Statistics/Counters:
Number of files currently open: 20
Number of Total File Opens: 23
Number of Open Fails when File is Locked: 1
Number of Read misses - Version Mismatch: 4
Number of Read misses - File Not Present: 3
Number of Write misses - Hard File Full: 4

```

**例:**

Thin-Server> **list file-refresh-counters**

```

File Refresh Statistics/Counters
Number of Files Updated during last refresh: 0
Number of Update Failures during last refresh: 0
Number of Refreshes: 0
Number of Refresh Failures: 1
Number of Files Refreshed: 30

```

## TSF 監視コマンド (Talk 5)

```
Date/Time of Last File Update:          has not occurred since last reset
Date/Time of Last File Download:       has not occurred since last reset
```

Thin Server>

**例:**

```
Thin-Server> list pre-load-list
<display of pre-load list raw file>
List of Pre-Load List File is Complete
```

**例:**

```
Thin-Server> list tftp-counters
```

```
TFTP Statistics/Counters
Number of Total TFTP Clients:          3
Number of Current TFTP Clients:        2
Number of Files Served:                22
Number of Files Served by Master Server: 22
```

**例: RFS の場合**

```
Thin-Server> list ts-counters
```

```
Thin Server Statistics/Counters
Relay to Master File Server:          Available
Number of Total RFS Clients:          0
Number of Current RFS Clients:        0
Number of Files Served:                0
Number of Files Served by Master Server: 0
Number of NS Port Mapper socket accepts: 0
Number of NS Port Mapper sockets currently active/open: 0
Number of NS Server socket accepts:   0
Number of NS 8473 sockets currently active/open: 0
Number of NS Login sock accepts:      0
Number of NS 8476 sockets currently active/open: 0
Number of RFS writes to a Thin Server cached file: 0
```

Thin Server>

**例: NFS の場合**

```
Thin-Server> list ts-counters
```

```
Thin Server Statistics/Counters
Number of NFS Server Reads:           13
Number of NFS Server Read Directories: 8
Number of Unsupported NFS Requests:    2
Number of total NFS Mounts:           22
Number of current NFS Mounts:          7
Number of total NFS clients:           15
Number of current NFS Clients:         4
```

## Refresh

**refresh** コマンドは、キャッシュを強制的にリフレッシュするのに使用します。

構文:

**refresh**

例:

```
Thin-Server> refresh
```

```
Force a refresh of the cache ? (Y/ [N]): y
```

```
Thin Server cache has been refreshed
```

## Reset

**reset** コマンドは、カウンターを動的にリセットするのに使用します。

構文:

```
reset                all
                        file-access-counters
                        file-refresh
                        tftp-counters
                        ts-counters
```

例:

```
Thin-Server> reset all
```

```
All Thin Server feature counters have been reset
```

## Restart

**restart** コマンドは、TSF プロセスをリスタートするのに使用します。

構文:

**restart**

例:

```
Thin-Server> restart
```

```
Restart Thin Server? (Y/ [N]): y
```

```
Thin Server has been restarted
```

## Set

**set** コマンドは、TSF キャッシュ・モードを設定するのに使用します。

構文:

```
set                mode
```

**mode** TSF のモードを指定します。 561ページの『Set』を参照してください

有効値:

## TSF 監視コマンド (Talk 5)

- enable
- disable
- passthru

例:

```
Thin-Server> set mode ?
```

```
DISABLED  
ENABLED  
PASSTHRU
```

```
Thin-Server> set mode disable
```

```
Thin Server caching is now disabled
```

---

## 第34章 VCRM の構成および監視

バーチャル・サーキット・リソース・マネージャー (VCRM) は、リソース ReSerVation プロトコル (RSVP) をサポートする機能です。このプロトコルについては、プロトコル構成および監視 参照資料 第 1 巻の『RSVP の使用』および『RSVP の構成および監視』の章で説明しています。RSVP からの予約要求に基づいて、VCRM は物理インターフェースを介したデータ・フローのための接続を作成します。その場合、最初に VCRM は予約を収容できる十分な帯域幅が得られるかどうかを調べることが必要です。

**注:** フレーム・リレーや X.25 のような WAN インターフェースを使用している場合、利用可能な帯域幅の量が VCRM に分かるようにするために、回線速度を設定する必要があります。回線速度の設定手順は、アクセス・インテグレーション・サービス ソフトウェア使用者の手引きのフレーム・リレーおよび X.25 インターフェースの構成および監視の章で説明しています。

インターフェースが PPP リンク、LAN、または WAN の場合、VCRM は QoS のソフトウェア待ち行列化および best-effort パケットを使用して、アウトバウンド・リンク上のパケットを優先順位付けします。

この章には、次の内容が記載されています。

- 『VCRM 構成環境へのアクセス』
- 『VCRM 監視環境へのアクセス』
- 570ページの『VCRM 監視コマンド』

---

### VCRM 構成環境へのアクセス

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

```
Config> feature vcrm
VC & Resource Management config console
--Currently no configurable objects.
Config>
```

表示されるメッセージの目的は、VCRM は別個には構成できないことを示すことです。RSVP を使用可能にすると VCRM も使用可能になり、そのパラメーターを RSVP 構成から入手します。

---

### VCRM 監視環境へのアクセス

VCRM 監視環境にアクセスするには、次のように入力します。

```
* t 5
```

次に、+ プロンプトで、次のコマンドを入力します。

```
+ feature VCRM
VCRM console
VCRM Console>
```

VCRM Console> プロンプトが表示されます。

## VCRM 監視コマンド

ここでは、VCRM 監視コマンドについて説明します。次のコマンドは VCRM> プロンプトで入力します。

表 62. VCRM 監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxix ページの『ヘルプの入手』を参照してください。
Clear	待ち行列統計をリセットします。
Queue	ソフトウェア待ち行列統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxix ページの『下位レベル操作環境の終了』を参照してください。

### Clear

**clear** コマンドは、ソフトウェア待ち行列統計をリセットするのに使用します。

構文:

**clear**

**clear** コマンドの例は、**queue** コマンドの項を参照してください。

### Queue

**queue** コマンドは、トラフィック・フローのソフトウェア待ち行列を表示するのに使用します。

構文:

**queue**

ソフトウェア待ち行列の表示に使用される用語の定義を次に示します。

**Quota** 予約された帯域幅の量。当初は、best-effort (B.E.) がすべての quota (割り当て量) を所有します。予約されると、予約帯域幅 (b/w) が B.E. quota から QoS quota にシフトします。

**Max-q** パケットに記述されている最大待ち行列の長さ。

**Curr-q**

パケットに記述されている現行の待ち行列の長さ。

**In quota**

割り当てられた帯域幅内で送信されたパケット数または K バイト数。

**Outside quota**

割り当てられた帯域幅外で送信されたパケット数または K バイト数 (アイドル帯域幅が利用可能な場合)。

**Packets/bytes dropped**

ソフトウェア待ち行列によってドロップされたパケット数またはバイト数



**DLC packets/bytes dropped**

パケットがソフトウェア待ち行列を通過した後で DLC によってドロップされたパケット数またはバイト数

例:

```
*t 5

+feature vcrm
VCRM console
VCRM Console>?
CLEAR
QUEUE
EXIT
VCRM Console>queue
Flow-control Queues at sys-clock 346781 Second:
-----
Intf   B.E. Quota:      10000 Kbps      QoS Quota:      0      Kbps
0/Eth  B.E. Max-q      0
      B.E. curr-q   0
      B.E. pkts/Kbytes sent:
      in quota:    54169/ 3926      QoS pkts/Kbytes sent:
      outside quota: 0/ 0      in quota:      0/      0
      B.E. pkts/bytes dropped: 0/0      QoS pkts/bytes dropped: 0/0
      DLC pkts/bytes dropped: B.E.: 0/0      QoS: 0/0
Intf   B.E. Quota:      2048 Kbps      QoS Quota:      0      Kbps
2/PPP  B.E. Max-q      0
      B.E. curr-q   0
      B.E. pkts/Kbytes sent:
      in quota:    62/ 6      in quota:      0/      0
      outside quota: 0/ 0      outside quota: 0/      0
      B.E. pkts/bytes dropped: 0/0      QoS pkts/bytes dropped: 0/0
      DLC pkts/bytes dropped: B.E.: 0/0      QoS: 0/0
Intf   B.E. Quota:      2032 Kbps      QoS Quota:      16     Kbps
3/FR   B.E. Max-q      1
      B.E. curr-q   0
      B.E. pkts/Kbytes sent:
      in quota:    53160/ 4920      QoS pkts/Kbytes sent:
      outside quota: 0/ 0      in quota:      346596/ 31886
      B.E. pkts/bytes dropped: 0/0      QoS pkts/bytes dropped: 0/0
      DLC pkts/bytes dropped: B.E.: 0/0      QoS: 0/0
Intf   B.E. Quota:      2048 Kbps      QoS Quota:      0      Kbps
4/PPP  B.E. Max-q      1
      B.E. curr-q   0
      B.E. pkts/Kbytes sent:
      in quota:    66/ 6      in quota:      109/ 1
      outside quota: 0/ 0      outside quota: 0/
      B.E. pkts/bytes dropped: 0/0      QoS pkts/bytes dropped: 0/0
      DLC pkts/bytes dropped: B.E.: 0/0      QoS: 0/0

Max total queue length=1; current total length=0
VCRM Console>clear
Flow-control Queues cleared at sys-clock 346786 Second:
-----
VCRM Console>
```

## VCRM の監視 (Talk 5)

---

## 第35章 音声アダプターの使用

この章では、音声アダプターについて説明し、Nuera F200 フレーム・リレー・アクセス装置 (FRAD) と組み合わせて音声アダプターを使用する方法を説明します。ダイヤル・プランと構成の大部分は、F200 上で行います。F200 は、2212 ポート間の接続をすべて処理します。2212 ポート構成には、F200 に到達するために必要な情報だけが組み込まれます。

この章には、次の内容が記載されています。

- 『音声アダプターの概説』
- 574ページの『2212 音声ポートと通信するための Nuera F200 の構成』
- 577ページの『Nuera F200 と通信するための 2212 音声ポートの構成』
- 578ページの『Nuera F200 を使用しない通信』

---

### 音声アダプターの概説

574ページの図50 は、2 台の 2212 が Nuera F200 FRAD に接続されているネットワークの図です。それぞれの 2212 には、音声アダプター・カードを 4 枚まで取り付けることができ、それぞれのカードには 2 つの音声ポートがあるので、ポートは合計 8 つまでです。ポートは、FXS、FXO、または E&M のインターフェースを使用できます。それぞれの音声ポートは、構内交換機 (PBX)、別の電話機、またはキー・システムに直接接続できます。それぞれの音声ポートは、最大 8 台の F200 へのフレーム・リレー接続をサポートできます。音声ポートは、同じ 2212 内の他の音声ポートに接続することもできます。これは、ローカル・コール・ルーティング と呼ばれます。

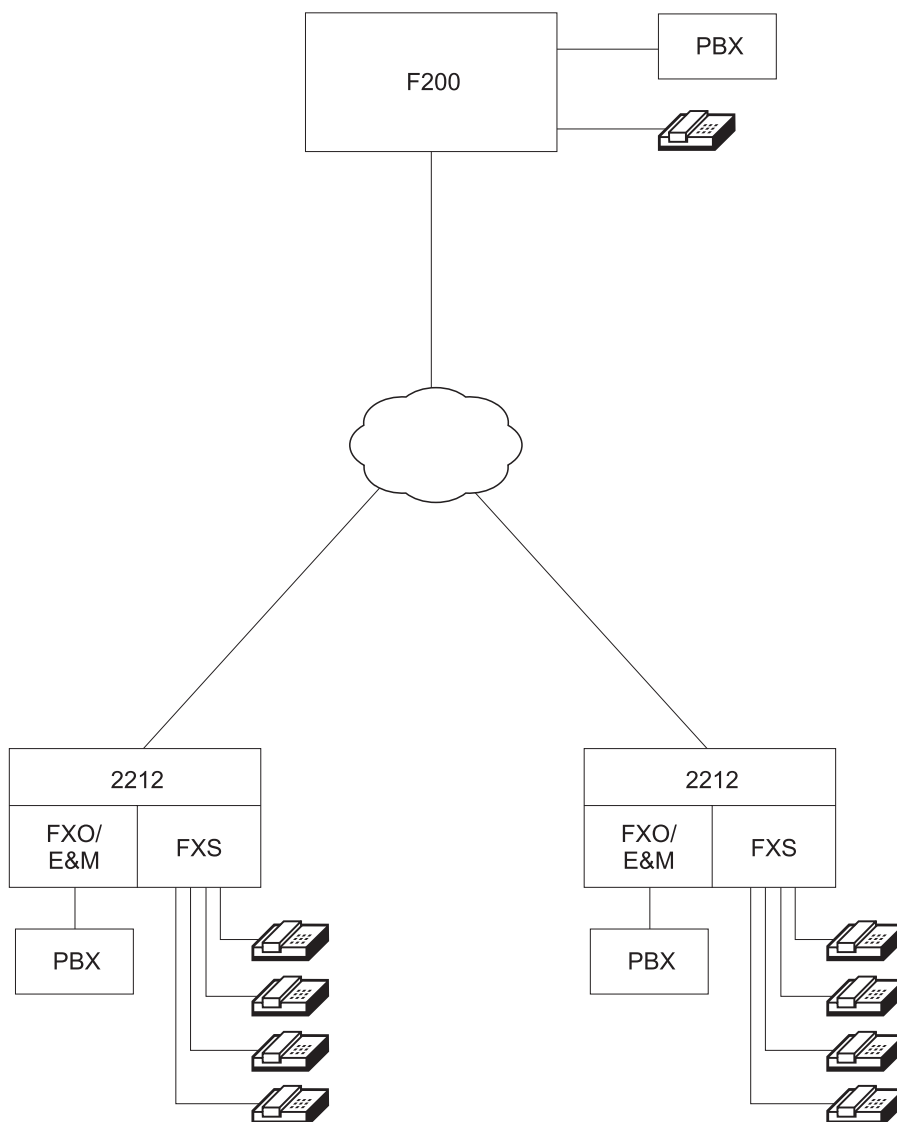


図 50. F200 と 2212 音声ポートの通信

音声アダプターの定義は、2つのステップからなる構成プロセスです。まず、2212 音声ポートと通信するように F200 を定義する必要があり、次に F200 と通信するように 2212 音声ポートを同様に定義します。

コール処理規則、ダイヤル・マッチング規則、ネットワーク出力規則、および電話回線出力規則の定義例については、579ページの『第36章 音声アダプターの構成と監視』を参照してください。

## 2212 音声ポートと通信するための Nuera F200 の構成

2212 音声アダプターと通信するために F200 を構成するには、ダイヤル・プラン と呼ばれる一連のパラメーターを定義する必要があります。F200 ダイヤル・プランには、次の情報が含まれています。

- 回線グループ

・ 回線記述子

図51 は、2212A と 2212B の音声ポート間の通信に必要なルーティング情報を示しています。

F200 0.0.0.1 回線グループ (ダイヤル・プラン)

回線グループ #	回線 (記述)	DLCI	サブチャンネル
1	プロセス 5	16	4
		16	5
2	プロセス 5	17	4
		17	5
3	プロセス 7	17	6
		17	7

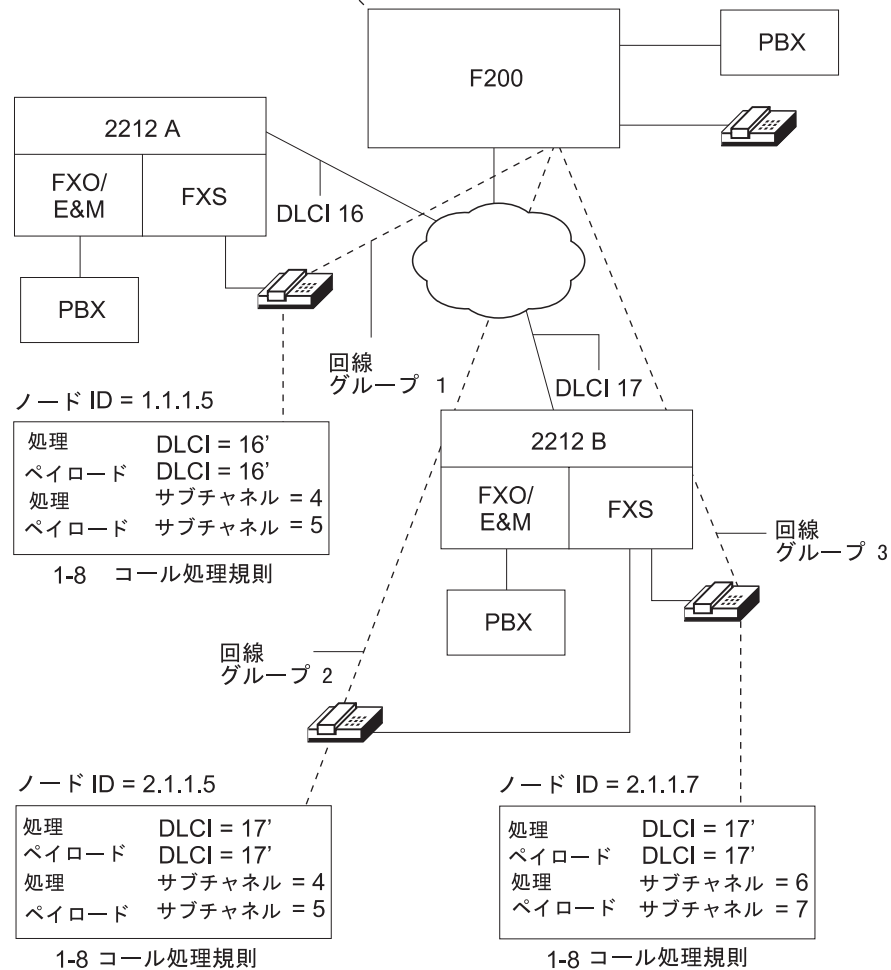


図 51. 音声ポートのコール処理情報の構成

F200 回線グループは、F200 とリモート・ノードとの間にバーチャル音声ネットワーク・トランク を定義します。F200-F200 回線グループには別個の回線が多数含まれていることがありますが、F200-2212 音声アダプター回線グループには PVC 回線が 1 つ だけあります。回線グループは、リモート・ノード (F200 または 2212 音声ポート) に接続します。図51 では、回線グループ 1 はノード ID 1.1.1.5 の 2212A 音声

## 音声アダプターの使用

ポートに接続します。回線グループ 2 は、ノード ID 2.1.1.5 の 2212B 音声ポートに接続します。回線グループ 3 は、ノード ID 2.1.1.7 の 2212B 音声ポートに接続します。それぞれの 2212 音声ポートは、同じ 2212 上のポートであっても、固有なノード ID を持っている必要があります。このため、それぞれの 2212 音声ポートごとに、F200 への固有な回線グループを定義する必要があります。

F200 回線記述子は、それぞれの回線グループ内にある個々の回線を定義します。1 つの F200-F200 回線グループに対して、複数の回線記述子を指定できます (グループ内のそれぞれの回線に対して 1 つずつ)。F200-2212 音声アダプター回線グループにある回線は 1 つだけなので、F200-2212 音声アダプター回線グループには回線記述子が 1 つだけあります。

回線記述子には、処理回線とペイロード回線の両方の情報が含まれています。処理回線は、呼び出しの確立と呼び出しの終了に必要なパケットを転送するために使用されます。このパケットは、Nuera 固有の CALL SETUP、CONNECT、ANSWER、および RELEASE の各パケットです。ペイロード回線は、実際の圧縮音声データが入ったパケットを転送するために使用されます。

575ページの図51 では、F200 には回線グループを 3 つ (それぞれの 2212 音声ポートに 1 つずつ) 指定したダイヤル・プランがあります。F200 が特定のノード ID との通信を確立するための要求を受け取ると、回線グループを使用してターゲット装置を見付けます。F200 回線グループには、次の情報が含まれています。

- 回線グループ番号
- Connect-to ノード (接続先のノード)
- 回線記述子 (処理およびペイロード)
  - DLCI (16-991)
  - サブチャンネル (処理およびペイロード)

**注:** F200-2212 音声アダプター回線に対する回線記述子を定義する際には、回線記述子とペイロード・サブチャンネル番号が一致している必要があります。指定できる最小のサブチャンネル値は 4 です。F200 と 2212 との間の回線グループは、すべて同じ DLCI を使用できます。

## ダイヤル・プランの構成

F200 のダイヤル・プランは、1 ~ 4 つの変換規則で構成されます。これらの規則は、装置が F200 と接続して通信する方法を制御します。それぞれの変換規則は、順序付きケースの番号 (1 ~ 100) で構成されます。それぞれの F200 回線グループは、特定の変換規則と関連付けられます。それぞれの変換規則は、次の要素で成り立っています。

### 送信元マッチング規則

送信元番号のダイヤル桁マッチング・パターン。

### あて先マッチング規則

あて先番号のダイヤル桁マッチング・パターン。

### ルート規則

回線グループ、回線グループのサブセット、またはローカル・ポートのリスト。

**送信元出力規則**

コール・セットアップ時に送信元番号を変換するための規則。

**あて先出力規則**

コール・セットアップ時、またはデータ伝送中に、あて先番号を変換するための規則。

コール・セットアップ時に、送信元番号とあて先番号が、それぞれの変換規則ケースにある対応するマッチング規則と比較されます。比較は、一致が検出されるまで昇順で行われます。一致が検出された場合は、一致したケースのルート規則がコールのルートを指定します。一致したケースの出力規則は、コール・セットアップ情報を変更したり、ダイヤル番号を生成したりします。

---

## Nuera F200 と通信するための 2212 音声ポートの構成

F200 と通信するために 2212 音声ポートを構成するには、次の規則を定義する必要があります。

- 電話回線出力規則 -- それぞれの音声ポートごとに 1 つの規則
- コール処理規則 -- それぞれの音声ポートごとに 8 つまでの規則

それぞれの 2212 に対して、電話回線出力規則を 8 つまで (それぞれの音声ポートごとに 1 つの規則) 定義できます。電話回線出力規則は、電話回線インターフェースにダイヤル桁を送信する方法を決定します。それぞれの電話回線規則は、あて先ダイヤル桁、送信元ダイヤル桁、定数、および休止の組み合わせからなります。

それぞれの音声ポートに対して、コール処理規則を 8 つまで定義できます。それぞれの規則は、接続を確立する方法を決定する一連の接続パラメーターを指定します。コール処理規則には、次の情報が含まれています。

- 処理 DLCI (16 ~ 1007)
- ペイロード DLCI (16 ~ 1007)
- 処理サブチャネル (4 ~ 254)
- ペイロード・サブチャネル (4 ~ 254)
- ダイヤル桁マッチング規則番号 (1 ~ 64)
- ネットワーク出力規則番号 (1 ~ 64)

**注:** 音声ポートに対して定義されたペイロード・パラメーターと処理パラメーターは、音声ポートに接続できる F200 に対して定義されたペイロード・パラメーターと処理パラメーターに対応する必要があります。

ダイヤル桁マッチング規則を使用すると、ダイヤル桁シーケンスのそれぞれの桁で許容される桁の範囲を指定できます。複数桁ワイルドカードや、『オフフック』状態のときに即時に接続を開始させるシーケンスを指定できます。最大 64 の規則からなるプールを定義して、それぞれのコール処理規則の中でダイヤル桁規則を指定できます。

ネットワーク出力ファイルを使用すると、コール・セットアップ用のフレーム・リレー・パケットにあて先番号を出力する方法を指定できます。この規則は、あて先番号の桁と定数の組み合わせからなります。

## 音声アダプターの使用

2212 音声ポートがコールを開始すると、あて先番号がそのポートのダイヤル桁マッチング規則と比較されます。これらの規則は、そのポートのコール処理規則の中で定義されています。一致が検出されると、一致するコール処理規則の DLCI とサブチャネルがあて先ノードを決定します。あて先番号を変更する必要がある場合は、ネットワーク出力規則が番号の変更方法を決定します。

2212 がコールを受信すると、DLCI とサブチャネルのペアがコールを受信する音声ポートを決定します。それぞれの音声ポートは、コール処理規則の 1 つに定義されている任意の DLCI とサブチャネルのペアからのコールを受け入れます。あて先音声ポートの電話回線出力規則があて先番号に対して使用され、ダイヤル桁出力パルス・シーケンスを生成します (必要な場合)。

---

## Nuera F200 を使用しない通信

限られたネットワーク・アクセス機能だけが必要な場合は、次の方法を使用することによって、Nuera F200 を使用せずに 2 つの音声ポート間で通信できます。

- 別々の 2212 の音声ポート間で通信する
- 同じ 2212 の音声ポート間で通信する (ローカル・コール・ルーティング)

## 2212 間の通信

それぞれの音声ポートに対して対応するコール処理規則を定義すれば、F200 を使用せずに別々の 2212 にある 2 つの音声ポート間でコールを行うことができます。これらの規則はそれぞれ、同じペイロード・サブチャネルとコール処理サブチャネル、および対応するペイロード DLCI とコール処理 DLCI を指定する必要があります。F200 を使用せずに通信する場合、ノード ID フィールドは使用されません。

**注:** F200 に接続せずに、それぞれの音声ポートを最大 8 つのリモート音声ポートに接続できます。音声ポートのローカル・コール・ルーティングを使用可能にしている場合、そのポートは 7 つのリモート音声ポートだけに接続できます。

## ローカル・コール・ルーティング

F200 を使用せずに、同じ 2212 にある 2 つの音声ポート間でコールを行うことができます。このためには、それぞれのポートに対する 8 つのコール処理規則のうち、1 つをローカル・コール・ルーティング用に構成します。ローカル・コール・ルーティングは、ローカル・コール規則を定義したそれぞれの音声ポートに構成されたローカル番号と、あて先番号を比較します。各ポートのローカル番号の中で、比較対象になる先頭桁数を指定できます。

ネットワーク出力ファイル (ローカル・ルート・コール規則で指定される) は、コールを正しくルート指定できるように、十分な桁数のあて先番号を指定する必要があります。

送信元音声ポートとあて先音声ポートは同じ 2212 内にあるので、ローカル・ルーティング・コール規則には DLCI 情報とサブチャネル情報はありません。



## 第36章 音声アダプターの構成と監視

この章では、音声アダプターの構成コマンドと操作コマンドの使用方法について説明します。この章には、次の内容が記載されています。

- 『音声機能構成環境へのアクセス』
- 『音声アダプター構成コマンド』
- 589ページの『音声ネットワーク構成コマンド』
- 592ページの『音声アダプター監視環境へのアクセス』
- 592ページの『音声アダプター監視コマンド』

### 音声機能構成環境へのアクセス

音声アダプター構成プロセスにアクセスするには、次の手順を使用します。

1. OPCON プロンプトで、**talk 6** と入力する。(このコマンドについて詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の *OPCON* プロセスおよびコマンド の章を参照してください。) たとえば、次のように入力します。

```
* talk 6
Config>
```

**talk 6** コマンドを入力すると、CONFIG プロンプト (Config>) がコマンド行に表示されます。最初に構成に入ったときにプロンプトが表示されない場合は、**Return** をもう一度押してください。

2. CONFIG プロンプトで、**feat voice** コマンドを入力して Voice Config> プロンプトを表示する。

### 音声アダプター構成コマンド

ここでは、2212 ダイアル・プランを構成する方法を説明します。タイマーとトーンを設定する方法も説明します。これらは、2212 に対して一度構成されると、2212 の音声ポートすべてに適用されます。

音声アダプターを構成するには、Voice Config> プロンプトで次のコマンドを入力します。

表 63. 音声構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxx iページの『ヘルプの入手』を参照してください。
Add	コール処理規則、ダイヤル・マッチング規則、または出力規則を追加します。
Delete	コール処理規則、ダイヤル・マッチング規則、または出力規則を削除します。
List	各種のタイマーとトーンの設定値を表示します。

## 音声アダプター構成コマンド (Talk 6)

表 63. 音声構成コマンドの要約 (続き)

コマンド	機能
Modify	コール処理規則、ダイヤル・マッチング規則、または出力規則を更新します。
Reorder-Call-Rule Set	コール処理規則の検索順序を変更します。
Set	タイマー、トーン、および FR-Net (フレーム・リレー・ネット) を設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

## Add

**add** コマンドは、音声アダプターに対するコール処理規則、ダイヤル桁マッチング規則、および出力規則を追加するために使用します。

構文:

```
add call-processing-rule  
dial-matching-rule  
network-output-rule  
telco-output-rule
```

### call-processing-rule

コール処理規則を指定します。発信コールの場合、それぞれのコール処理規則に関連したダイヤル桁マッチング規則と、ダイヤルされた番号を比較することによって、コール処理規則は昇順に評価されます。一致が検出された場合は、コール処理規則にあるネットワーク出力規則とコール・ルーティング情報が、コールの処理に使用されます。音声ポートは、任意の関連したコール・ルーティング規則に指定された、任意のあて先からのコールを受け入れることができるので、この規則は効果がありません。それぞれの音声ポートに対し、8 つまでのコール処理規則を定義できます。

**注:** コール処理規則は、Nuera F200 の変換規則と類似しています。変換規則は、ネットワーク出力規則とダイヤル・マッチング規則を、コール・ルーティング情報 (リモート・コール・ルートの場合は DLCI とサブチャネルの指定、ローカル・コール・ルートの場合はローカル番号と比較するあて先番号の桁数) と組み合わせたものです。

```
Voice config>add call  
Voice Net [0]? 5  
Define Call Processing Rule #1  
Destination Type (Local or Remote)(Remote?)?  
Call Processing DLCI (16 to 1007)[16]?  
Payload DLCI (16 to 1007)[16]? 17  
Call Processing Subchannel (4 to 254)[4]?  
Payload Subchannel (4 to 254)[4]? 5  
Dial Digit Matching Rule (0 to 4)[1]?  
Network Output Rule Number (0 to 2)[1]?
```

#### Destination Type

あて先ノードが 2212/F200 (Remote) または同じ 2212 上の別の音声ポート (Local) のどちらであるかを指定します。

#### Call Processing DLCI

コールをセットアップし、その後終了するために使用される DLCI を指定します。

**Payload DLCI**

圧縮音声データ・パケットを送受信するために使用される DLCI を指定します。

**Call Processing Subchannel**

コールをセットアップし、その後終了するために使用されるサブチャネルを指定します。

**Payload Subchannel**

圧縮音声データ・パケットを送受信するために使用されるサブチャネルを指定します。

**Dial Digit Matching Rule**

このコール処理規則に対して使用するダイヤル桁マッチング規則の番号を指定します。

**Network Output Rule**

このコール処理規則に対して使用するネットワーク出力規則の番号を指定します。

**dial-matching-rule**

ダイヤル桁パターン・マッチング・シーケンスを指定します。このシーケンスの各要素は、その位置で許容される桁の範囲を指定します。

**注:** ダイヤル・マッチング規則は、Nuera F200 のあて先マッチング規則と類似しています。

```
Voice config>add dial
```

```
Define Dial Digit Matching Rule #4
```

```
Dial Mask 1: Digit String (0-9, A-D, *, #), [W]ildcard, [N]umeric Wildcard,
             [M]ultidigit Wildcard
             [MultiDigit Wildcard]? 456 /* match 4 or 5 or 6 */
Dial Mask 2: Digit String (0-9, A-D, *, #), [W]ildcard, [N]umeric Wildcard,
             [M]ultidigit Wildcard, or [E]nd
             [End]? m
Dial Mask 3: Digit String (0-9, A-D, *, #), [W]ildcard, [N]umeric Wildcard,
             [M]ultidigit Wildcard
             [MultiDigit Wildcard]? e
```

```
Matching Rule contains Multidigit Wildcard(s)
```

```
Minimum number of digits accepted for Multidigit Wildcard [1]? (specify either 0 or 1)
```

**Dial Mask #**

1 ~ 20 のダイヤル桁マスクのセットから 1 つを指定します。それぞれのマスクは、20 桁のダイヤル・シーケンス内のその位置で許容される桁の範囲を指定します。

**Digit String**

選択される桁が含まれている必要がある桁の集合を指定します。

**Wildcard**

その桁が 0 ~ 9、A ~ D、#、または \* のどれか 1 つでなければならないことを指定します。

**Numeric Wildcard**

その桁が 0 ~ 9 でなければならないことを指定します。

**Multidigit Wildcard**

指定の位置で複数の桁が許容されることを指定します。複数桁ワイルドカード・マスクがダイヤル・マッチング規則の最

## 音声アダプター構成コマンド (Talk 6)

後にある場合は、シーケンス内のこのポイントに任意の桁 (0 ~ 9、A ~ D、#、\*) を入力できます。この場合、20 桁が入力されるか、追加の桁が入力されずに Interdigit Timeout が満了するまで、音声ポートは桁の収集を続行します。複数桁ワイルドカードの後にマスクがある場合、音声ポートは複数桁ワイルドカード・マスクの後にあるマスクを満たす桁が入力されるまで、複数桁マスクを満たす桁の収集を続行します。

### network-output-rule

フレーム・リレー・コール・セットアップ・パケットにパスするあて先番号の桁を指定します。シーケンスは、送信元電話回線ポートで受け取ったダイヤルされた桁と、定数の組み合わせとして指定されます。

**注:** ネットワーク出力規則は、フレーム・リレー・ポートに対する Nuera F200 のあて先出力規則と類似しています。

```
Voice config>add network
Define Network Output Rule #5
Digit 1: (Destination/Constant/End) [End]? c
          (0-9, A-D, *, #) [0]? 1
Digit 2: (Destination/Constant/End) [End]?
          (1-20) [1]?
Digit 3: (Destination/Constant/End) [End]?
          (1-20) [2]?
Digit 4: (Destination/Constant/End) [End]?
          (1-20) [3]?
Digit 5: (Destination/Constant/End) [End]? e
```

#### Digit #

特定のダイヤル桁を決定する方法を指定します。

#### Destination

あて先電話番号の指定の位置からの桁を使用することを指定します。

#### Constant

指定の位置で常に定数桁 (0 ~ 9、A ~ D、#、\*) を使用することを指定します。

**End** 桁シーケンスの終了を指定します。

### telco-output-rule

電話回線ポートが呼び出しのあて先ならば電話回線ポートから送出するダイヤル桁のシーケンスを指定します。シーケンスは、コール・セットアップ時にパスされるあて先番号と送信元番号のダイヤル桁、定数、および休止文字の組み合わせとして指定されます。

**注:** 電話回線出力規則は、音声ポートに対する Nuera F200 のあて先出力規則と類似しています。

```
Voice config>add telco
Define Telco Output Rule #4
Digit 1: (Source/Destination/Constant/Pause/End) [Destination]? c
          (0-9, A-D, *, #) [0]? 9
Digit 2: (Source/Destination/Constant/Pause/End) [Destination]? p
Digit 3: (Source/Destination/Constant/Pause/End) [Destination]?
          (1-40) [1]?
Digit 4: (Source/Destination/Constant/Pause/End) [Destination]?
          (1-40) [2]?
```

## 音声アダプター構成コマンド (Talk 6)

Digit 5: (Source/Destination/Constant/Pause/End) [Destination]?  
(1-40) [3]?  
Digit 6: (Source/Destination/Constant/Pause/End) [Destination]? e

### Digit #

特定のダイヤル桁を決定する方法を指定します。

#### Source

送信先電話番号の指定の位置からの桁を使用することを指定します。

#### Destination

あて先電話番号の指定の位置からの桁を使用することを指定します。

#### Source

送信先電話番号の指定の位置からの桁を使用することを指定します。

#### Constant

指定の位置で常に定数桁 (0 ~ 9、A ~ D、#、\*) を使用することを指定します。

**Pause** ダイヤル桁シーケンスのこのポイントに休止インターバルを挿入することを指定します。

**End** 桁シーケンスの終了を指定します。

## Delete

**delete** コマンドは、音声アダプターに対するコール処理規則、ダイヤル桁マッチング規則、および出力規則を削除するために使用します。

構文:

```
delete                call-processing-rule  
                        dial-matching-rule  
                        network-output-rule  
                        telco-output-rule
```

コール処理規則、ダイヤル・マッチング規則、および出力規則については、580ページの『Add』を参照してください。

## List

**list** コマンドは、規則、タイマー遅延、およびトーン設定に関する情報を表示するために使用します。

構文:

```
list  
call-processing-rule  
dial-matching-rule  
network-output-rule  
telco-output-rule  
timers  
tones
```

## 音声アダプター構成コマンド (Talk 6)

### call processing rule

指定の音声ポートに対するコール処理規則を表示します。特定のポート番号が指定されていない場合は、ポート番号を指定できる Voice Net [0] プロンプトが表示されます。

```
Voice config>list call
Voice Net [0]? 5
Call Processing Rule #1
Call Processing DLCI      =16
Payload DLCI              =17
Call Processing Subchannel = 4
Payload Subchannel        = 5
Dial Digit Matching Rule  = 1
Network Output Rule       = 1
```

### Call processing DLCI

このポートに対して定義されているコール処理 DLCI を示します。

### Payload DLCI

このポートに対して定義されているペイロード DLCI を示します。

### Call processing subchannel

このポートに対して定義されているコール処理サブチャネルを示します。

### Payload subchannel

このポートに対して定義されているペイロード・サブチャネルを示します。

### Dial digit matching rule

このポートが現在使用しているダイヤル桁マッチング規則を示します。

### Network output rule

このポートが現在使用しているネットワーク出力規則を示します。

### dial matching rule

指定の音声ポートに対するダイヤル桁マッチング規則を表示します。特定のポート番号が指定されていない場合は、ポート番号を指定できる Voice Net [0] プロンプトが表示されます。

```
Voice config>list dial 4
Dial Digit Matching Rule #4
Dial Mask 1:Match Digits=456
Dial Mask 2:Match Digits=MultiDigit Wildcard
```

### network-output-rule

指定の音声ポートに対するネットワーク処理規則を表示します。

### telco-output-rule

指定の音声ポートに対する電話回線出力規則を表示します。

**timers** この音声アダプターに関連した遅延とタイムアウト (ミリ秒) をすべて表示します。パラメーターについての説明は、586 ページを参照してください。

```
Voice config>list timers
Seize Detect Delay      :50 ms   First Digit Timeout    :10000 ms
Answer Detect Delay     :10 ms   Inter Digit Timeout    :5000 ms
Discon Detect Delay     :200 ms  Start Dial Delay       :500 ms
Glare Detect Delay      :500 ms  Ring No Answer Timeout :30000 ms
```

## 音声アダプター構成コマンド (Talk 6)

```
Wink Detect Timeout :2000 ms Ring on Detect Timeout :400 ms
Wink Start Delay :50 ms Ring Off Detect Timeout :6000 ms
Wink Duration :200 ms Warble Timeout :10000 ms
```

**tones** この音声アダプターに関連したトーンをすべて表示します。パラメーターについての説明は、587 ページを参照してください。

```
Voice config>list tones
```

Tone	On1	Off1	On2	Off2	Freq1	Freq2	Level1	Level2
	ms	ms	ms	ms	Hz	Hz	dB	dB
Dial	0	0	0	0	350	440	-16	-16
Ring Back	2000	4000	2000	4000	440	480	-22	-22
Busy	500	500	500	500	480	620	-20	-20
Fast Busy	300	300	300	300	480	620	-16	-16
Warble	100	100	100	100	1400	2060	-16	-16
Dtmf	100	100					-7	

## Modify

**modify** コマンドは、音声アダプターに対するコール処理規則、ダイヤル・マッチング規則、および出力規則を更新するために使用します。

構文:

```
modify                call-processing-rule
                        dial-matching-rule
                        network-output-rule
                        telco-output-rule
```

コール処理規則、ダイヤル・マッチング規則、および出力規則については、580ページの『Add』を参照してください。

## Reorder-Call-Rule

**reorder-call-rule** コマンドは、コール処理規則の検索順序を変更するために使用します。

構文:

```
reorder-call-rule    net_number old_rule# new_rule#
```

**net\_number**

コール処理規則の順序を変更するネットワークの番号を指定します。

**old\_rule#**

順序を変更するコール規則の現行番号 (1 ~ 8) を指定します。

**new\_rule#**

順序を変更した規則が新しいコール処理規則リストに現れる位置 (1 ~ 8) を指定します。

次の例では、現在ネットワーク 5 のコール処理リストの 6 番目にあるコール処理規則が、リストの最初の規則に上がります。

```
Voice config>reorder call-rule 5 6 1
```

### Set

**set** コマンドは、各種の遅延とタイムアウトの値を指定するために使用します。

構文:

```
set                fr-net net-number  
                    timer ...  
                    tone ...
```

**fr-net** **set fr-net** コマンドは、VoFR (音声フレーム) パケットのルートとして使用するフレーム・リレー・ネットの番号を指定するために使用します。任意の構成済みネット番号、または 0X'FFFF' (ネットを指定しない場合) を指定します。

**timer** **set timer** コマンドは、次のタイマー・パラメーターを設定するために使用します。

#### **answer-detect-delay**

応答信号が認識されるまでの時間 (ミリ秒) を指定します。範囲は 0 ~ 500 ミリ秒です。デフォルトは 10 ミリ秒です。

#### **disconnect-detect-delay**

切断信号が認識されるまでの時間 (ミリ秒) を指定します。範囲は 0 ~ 500 ミリ秒です。デフォルトは 200 ミリ秒です。

#### **first-digit-timeout**

最初の桁を受け取る必要がある時間 (ミリ秒) を指定します。範囲は 0 ~ 10 000 ミリ秒です。デフォルトは 10 000 ミリ秒です。

#### **glare-detect-delay**

ポートがチャネルを捕そくできるようになるまでの時間 (ミリ秒) を指定します。範囲は 0 ~ 500 ミリ秒です。デフォルトは 500 ミリ秒です。

#### **inter-digit-timeout**

最初の桁を受け取った後に桁を受け取る必要がある時間 (ミリ秒) を指定します。範囲は 0 ~ 10 000 ミリ秒です。デフォルトは 500 ミリ秒です。

#### **ring-no-answer-timeout**

応答を待機している間、コールを中止するまでに、音声チャネルが FXO ポートを呼び出す時間 (ミリ秒) を指定します。範囲は 0 ~ 64 000 ミリ秒です。デフォルトは 30 000 秒です。

#### **ring-off-detect-timeout**

呼び出しが停止したことをサーバーが判断するまでの FXO ポートの呼び出しがない時間 (ミリ秒) を指定します。範囲は 0 ~ 64 000 ミリ秒です。デフォルトは 6000 ミリ秒です。

#### **ring-on-detect-timeout**

呼び出しが認識されるまでの、FXO ポートの呼び出しが発生している時間 (ミリ秒)。範囲は 0 ~ 64 000 ミリ秒です。デフォルトは 400 ミリ秒です。



**seize-detect-delay**

捕そく信号が認識されるまでの時間 (ミリ秒) を指定します。範囲は 0 ~ 500 ミリ秒です。デフォルトは 50 ミリ秒です。

**start-dial-delay**

ダイヤル信号の受信後、桁が送信されるまでの時間 (ミリ秒) を指定します。範囲は 0 ~ 64 000 ミリ秒です。デフォルトは 500 ミリ秒です。

**warble-timeout**

切断後、震音信号を生成する前に必要な無音の時間 (ミリ秒) を指定します。範囲は 0 ~ 64 000 ミリ秒です。デフォルトは 10 000 ミリ秒です。

**wink-detect-timeout**

ウィンクを受信しなかった場合に、コールが終了するまでの時間 (ミリ秒)。範囲は 0 ~ 64 000 ミリ秒です。デフォルトは 2000 ミリ秒です。

**wink-duration**

ウィンク信号の持続時間 (ミリ秒) を指定します。範囲は 0 ~ 10 000 ミリ秒です。デフォルトは 200 ミリ秒です。

**wink-start-delay**

着信捕そく信号の受信後、ウィンク信号が生成されるまでの時間 (ミリ秒) を指定します。範囲は 0 ~ 64 000 ミリ秒です。デフォルトは 50 ミリ秒です。

**tone set tone** コマンドは、次のトーン・パラメーターを設定するために使用します。

**busy** ビジー信号を生成するために使用される 2 つまでの周波数の特性を指定します。set tone busy コマンドを入力すると、次の情報を尋ねられます。

**on1** *freq1* が『オン』(アクティブ) である時間 (ミリ秒) を指定します。ゼロを指定すると、関連したトーンは常にオンになり、結果として連続トーンになります。範囲は 0 ~ 32767 ミリ秒です。デフォルトはゼロです。

**off1** *freq1* が『オフ』(非アクティブ) である時間 (ミリ秒) を指定します。ゼロを指定すると、関連したトーンは常にオンになり、結果として連続トーンになります。範囲は 0 ~ 32767 ミリ秒です。デフォルトはゼロです。

**on2** *freq2* が『オン』(アクティブ) である時間 (ミリ秒) を指定します。ゼロを指定すると、関連したトーンは常にオンになり、結果として連続トーンになります。範囲は 0 ~ 32767 ミリ秒です。デフォルトはゼロです。

**off2** *freq2* が『オフ』(非アクティブ) である時間 (ミリ秒) を指定します。ゼロを指定すると、関連したトーンは常にオンになり、結果として連続トーンになります。範囲は 0 ~ 32767 ミリ秒です。デフォルトはゼロです。

## 音声アダプター構成コマンド (Talk 6)

**freq1** ビジー信号の第 1 トーンの周波数 (ヘルツ) を指定します。範囲は 0 ~ 3000 ヘルツです。デフォルトは 350 ヘルツです。

**freq2** ビジー信号の第 2 トーンの周波数 (ヘルツ) を指定します。範囲は 0 ~ 3000 ヘルツです。デフォルトは 440 ヘルツです。

**level1** 増分 .5 dB で *freq1* の dB ゲイン・レベルを指定します。範囲は -13dB ~ -40 dB です。デフォルトは -16 dB です。

**level2** 増分 .5 dB で *freq2* の dB ゲイン・レベルを指定します。範囲は -13 dB ~ -40 dB です。デフォルトは -16 dB です。

**dial** ダイヤル音を生成するために使用される 2 つまでの周波数の特性を指定します。**set tone dial** を入力すると、*on1*、*off1*、*on2*、*off2*、*freq1*、*freq2*、*level1*、および *level2* を尋ねられます。パラメーターについての説明は、587 ページを参照してください。

**dtmf** デュアル・トーン複数周波数 (DTMF) 信号の特性を指定します。**set tone dtmf** コマンドを入力すると、次の情報を尋ねられます。

### **ontime**

DTMF の『オン時間』を指定します。ゼロを指定すると、DTMF 信号は生成されません。通常、40 ミリ秒以下の *ontime* を指定してはなりません。このように設定すると、12.5 トーン/秒の信号が生成されます。範囲は 0 ~ 32767 ミリ秒です。デフォルトは 100 ミリ秒です。

### **offtime**

DTMF の『オフ時間』を指定します。ゼロを指定すると、DTMF 信号は生成されません。範囲は 0 ~ 32767 ミリ秒です。デフォルトは 100 ミリ秒です。

**level** 増分 .5 dB で DTMF 信号の dB ゲイン・レベルを指定します。範囲は -7 dB ~ -25 dB です。デフォルトは -7 dB です。

### **fast busy**

ファースト・ビジー信号を生成するために使用される 2 つまでの周波数の特性を指定します。**set tone fast busy** を入力すると、*on1*、*off1*、*on2*、*off2*、*freq1*、*freq2*、*level1*、および *level2* を尋ねられます。パラメーターについての説明は、587 ページを参照してください。

### **ring-back**

リングバックを生成するために使用される 2 つまでの周波数の特性を指定します。**set tone ring-back** を入力すると、*on1*、*off1*、*on2*、*off2*、*freq1*、*freq2*、*level1*、および *level2* を尋ねられます。パラメーターについての説明は、587 ページを参照してください。

### **warble**

ダイヤル音を生成するために使用される 2 つまでの周波数の特性を指定します。**set tone warble** を入力すると、*on1*、*off1*、*on2*、*off2*、*freq1*、*freq2*、*level1*、および *level2* を尋ねられます。パラメーターについての説明は、587 ページを参照してください。

## 音声ネットワーク構成コマンド

音声ネットワークを構成するには、**network** コマンドと音声ポートの番号を入力します。

```
Config> network 5
Voice 5 Config>
```

音声アダプターを構成するには、Voice n Config> プロンプトで次のコマンドを入力します。

表 64. 音声ポート・コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxi ページの『ヘルプの入手』を参照してください。
List	音声ポートの各種設定値を表示します。
Set	音声ポートの各種パラメーターを設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxii ページの『下位レベル操作環境の終了』を参照してください。

## List

**list** コマンドは、音声ポートの現行設定値を表示するために使用します。

構文:

**list**

たとえば、音声ポートの現行構成を表示するには、次のように入力します。

```
Voice 5 config>list
NodeID: 1.2.3.4
Local Phone Number:1234567
Telco Output Rule Number: 0
Telco Parameters
Tx Gain   :-4 dB      E&M Type :1
Rx Gain   :-4 dB      E&M Wire :4
OOS Signal:Busy     E&M Start:Immediate
Dsp Parameters
Vocoder Suite :Nuera  VAD Mode      :Off
Vocoder Rate  :9600   VAD Hangover  :255 ms
Frame Packing :1      VAD Threshold :-45 dB
Echo Cancel  :0n      Fax           :0n
NLP          :0n      NSF           :0n
2100Hz Detect :0n
```

### Node ID

音声ポートの Nuera ノード ID を示します。

### Local Telephone Number

音声ポートのローカル電話番号を示します。

### Telco Output Rule

音声ポートが現在使用している電話回線出力規則を示します。



frame-packing  
local-number  
node-id  
oos  
output-rule  
rate  
rx-gain  
start  
suite  
tx-gain  
vad  
wire

**set** コマンドでは、次のパラメーターを設定できます。

#### **echo-cancel**

エコー消去を使用可能にするかどうかを指定します。 *yes* (1) または *no* (2) のどちらかを選択できます。デフォルトは *yes* です。

#### **frame-packing**

1 つのフレーム・リレー・パケットにパックされる音声フレームの数を指定します。範囲は 1 ~ 5 で、デフォルトは 1 です。

#### **local-number**

指定の音声ポートのローカル電話番号を示します。範囲は任意の 20 桁 (0 ~ 9、A ~ D、\*、#) の番号です。デフォルトは 0 です。

#### **node-id**

ポートの Nuera ノード ID を指定します。デフォルトは 0.0.0.0 です。

#### **oos**

指定の音声ポートが作動不能であることを示すために使用するトーンのタイプを指定します。 *idle* (1) または *busy* (2) のどちらかを選択できます。デフォルトは *busy* です。

#### **output-rule**

使用する電話回線出力規則を指定します。範囲は 0 ~ 8 です。(上限は、定義されている電話回線出力規則の数によって決まります。) デフォルトは 0 です。

#### **rate**

音声ポートの伝送速度を指定します。 *suite* パラメーターとして Nuera を指定する場合は、4.8 KB、7.47 KB、9.6 KB、または 32 KB を選択できます。 *suite* パラメーターとして ITU を指定する場合は、8 KB、16 KB、または 32 KB を選択できます。デフォルトは 9.6 KB です。

#### **rx-gain**

音声ポートが受信信号を減衰 (または増幅) させる量を指定します。範囲は -16 dB ~ +7 dB です。デフォルトは -4 dB です。

#### **start (E&M だけ)**

音声ポートが伝送を開始する方法を指定します。 *immediate start* (1) または *wink start* (2) のどちらかを選択できます。デフォルトは *immediate start* です。

#### **suite**

音声ポートが使用するプロトコルのタイプを指定します。  
*NUERA -- ECELP/G.726* (2) または *ITU -- G.729/G728/G.726* (3) のどちらかを選択できます。デフォルトは *NUERA* です。

## 音声アダプター構成コマンド (Talk 6)

### tx-gain

音声ポートが送信信号を減衰 (または増幅) させる量を指定します。範囲は -16 dB ~ +7 dB です。デフォルトは -4 dB です。

### type (E&M だけ)

指定の音声ポートに対して電話回線 E&M インターフェースを指定します。1、2、または 5 のどれかを選択できます。デフォルトは 1 です。

**vad** VAD モードを指定します。fixed (1)、adaptive (2)、または none (3) を選択できます。デフォルトは adaptive です。

### wire (E&M だけ)

2 線式または 4 線式のどちらの電話回線接続を使用するかを指定します。2 (2 線式) または 4 (4 線式) のどちらかを選択できます。デフォルトは 4 です。

---

## 音声アダプター監視環境へのアクセス

音声アダプター監視コマンドにアクセスするには、次の手順を使用します。この手順により、音声アダプター監視 プロセスにアクセスできます。

1. OPCON プロンプトで **talk 5** を入力する。(このコマンドについて詳しくは、アクセス・インテグレーター・サービス ソフトウェア使用者の手引き の *OPCON* プロセスおよびコマンド の章を参照してください。) たとえば、次のように入力します。

```
* talk 5
+
```

**talk 5** コマンドを入力すると、コマンド行に GWCON プロンプト (+) が表示されます。最初に構成に入ったときにプロンプトが表示されない場合は、**Return** をもう一度押してください。

2. + プロンプトで **network n** コマンドを入力して Voice n Console > プロンプトを表示する。

例:

```
+ network 2
Voice 2 Console>
```

---

## 音声アダプター監視コマンド

ここでは、音声アダプター監視コマンドについて説明します。

表 65. 音声アダプター監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。xxxページの『ヘルプの入手』を参照してください。
Calls	指定の音声ポートに関連した各種のイベントとメッセージ・カウンターを表示する。
Status	音声ポートの各種設定値、および送受信エラー情報を表示する。
Trace call	ターゲット・インターフェースに関する各種のトレース情報を表示する。

表 65. 音声アダプター監視コマンドの要約 (続き)

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

## Calls

**calls** コマンドは、コール処理メッセージとイベント・カウンターを表示するために使用します。

### 構文:

#### **calls**

### 例:

```
Voice 1 Console> calls
```

#### Event Counters

Seize Detected	5	Digit Detected	4
Seize Applied	0	Digit Generated	0

#### Message Counters

Setup Sent	1	Setup Received	0
Connect Sent	0	Connect Received	1
Answer Sent	0	Answer Received	1
Release Sent	2	Release Received	0

#### Release Cause Counters

Normal	1	Response	0
Busy	1	OOS	0
Local Bandwidth	0	Incompatible	0
Remote Bandwidth	0		

### Event Counters

電話回線インターフェース上で発生したイベントの数を示します。

#### Seize Detected

Seize In イベント (音声ポートに接続された電話がオフフックになった) の数を示します。

#### Seize Applied

Seize Out イベント (音声ポート自体がオフフックになった) の数を示します。

#### Digit Detected

電話回線インターフェース上の加入者から受信したダイヤル桁数を示します。

#### Digit Generated

電話回線インターフェース上の加入者に送信したダイヤル桁数を示します。

### Message Counters

フレーム・リレー回線を通じて音声ポートとの間で送受信されたコール処理メッセージの数を示します。セットアップ・メッセージ、接続メッセージ、および応答メッセージが、コールの確立時に 2 つのエンド・ノード間を流れます。コールの起動側がリモート側にセットアップ・メッセージを送信すると、リモート側は接続メッセージによって応答し、その後コールが成功した



## 音声アダプター監視コマンド (Talk 5)

場合は応答メッセージを送信します。コールを完了できなかった場合は、リモート・ノードによって解放メッセージが送信されます。解放メッセージは、成功したコールが正常に終了した (両端のノードがオンフックになった) ときにも、それぞれの終端によって送信されます。

### Setup Sent

送信したセットアップ・メッセージの数を示します。

### Connect Sent

送信した接続メッセージの数を示します。

### Answer Sent

送信した応答メッセージの数を示します。

### Release Sent

送信した解放メッセージの数を示します。

### Setup Received

受信したセットアップ・メッセージの数を示します。

### Connect Received

受信した接続メッセージの数を示します。

### Answer Received

受信した応答メッセージの数を示します。

### Release Received

受信した解放メッセージの数を示します。

## Release Cause Counters

解放メッセージの理由を表示します。

### Normal

こちら側の (ローカル) ノードによって開始された通常ハングアップの数を示します。

**Busy** チャンネルが使用中のために生じたハングアップの数を示します。

### Local Bandwidth

ローカル帯域幅の不足が原因で生じたハングアップの数を示します。

### Remote Bandwidth

リモート帯域幅の不足が原因で生じたハングアップの数を示します。

### Response

相手側の (リモート) ノードによって開始された通常ハングアップの数を示します。

**OOS** 相手側がサービス不能になっているために生じたハングアップの数を示します。

### Incompatible

エンド・ノード間の非互換性が原因で生じたハングアップの数を示します。



## Status

**status** コマンドは、特定の音声ポートに関する情報を表示するために使用します。

構文:

**status**

例:

```
Voice 1 Config> status
```

```
Node ID           :0.0.0.0
Absolute Port Address :01
```

Vocoder Suite	Nuera	Echo Canceller	Filter
Vocoder Active	ECELP	Fax Demodulation	Idle
Vocoder Rate	9600	Fax Modulation	Idle
Vocoder Packet Size	18	Fax Type	V.27 at 9600 bps
Vocoder Frame Size	120	Fax Last FCF	0

```
Last Received Dial Sequence :8675309
Last Transmitted Dial Sequence :911
```

Transmit Packets		Receive Packets	
Total	179	Total	184
Voice	169	Voice	167
CAS	0	CAS	11
DTMF	0	DTMF	0
FAX	0	FAX	0
Lost	0	Lost	0

### Node ID

音声ポートの Nuera ノード ID を示します。

### Absolute Port Address

F200 コール会計に使用される 2212 音声ポート ID を示します。このアドレスは、2212 ソフトウェアによって自動生成され、特定の 2212 にあるそれぞれの音声ポートに固有です。

### Vocoder Suite

音声ポートに対して現在使用できる vocoder suite (ITU または NUERA のどちらか) を示します。

### Vocoder Rate

現在の vocoder rate を示します。

### Vocoder Packet Size

それぞれの vocoder packet のバイト数を示します。これは生の圧縮出力のサイズで、フレーム・リレー・ヘッダーは含みません。

### Vocoder Frame Size

それぞれの vocoder frame にある PCM サンプルの数を示します。

### Echo Canceller

エコー消去の現在の状態を示します。

### FAX Demodulation

FAX 復調の現在の状況を示します。状況は、Active または Idle のどちらかです。

## 音声アダプター監視コマンド (Talk 5)

### FAX Modulation

FAX 変調の現在の状況を示します。状況は、Active または Idle のどちらかです。

### FAX Type

使用されている変調のタイプを示します。

### FAX Last FCF

最後に復調されたファクシミリ制御フィールドを示します。

### Last Received Dial Sequence

電話回線インターフェース上の加入者から最後に受信したダイヤル桁シーケンスを示します。

### Last Received Dial Sequence

電話回線インターフェース上の加入者に最後に送信したダイヤル桁シーケンスを示します。

### Transmit Packets/ Receive Packets

送信または受信したフレーム・リレー・パケットに関する各種の情報を示します。送信パケットは、音声ポートによって生成され、フレーム・リレー・リンクを経由して送信されたパケットです。受信パケットは、音声ポートによってフレーム・リレー・リンクを経由して受信されたパケットです。

**Total** 受信または送信したパケットの合計数を示します。

**Voice** 受信または送信した圧縮音声パケットの数を示します。

**CAS** 受信または送信した CAS パケットの数を示します。

**DTMF** 受信または送信した DTMF パケットの数を示します。

**FAX** 受信または送信した FAX パケットの数を示します。

**Lost** ローカル・ノードによって送信され、リモート・ノードによって受信されなかったパケットの数 (送信パケット)、またはリモート・ノードによって送信され、ローカル・ノードによって受信されなかったパケットの数 (受信パケット) を示します。

## Trace Call

**trace call** コマンドは、ターゲット・インターフェースに関する、すべてのセットアップ・メッセージまたは構成制御コマンドをトレースするために使用します。トレース・イベントは、ELS (talk 2) を使用して表示できます。

構文:

**trace call**

---

## 付録. リモート AAA 属性

ここでは、Radius、TACACS、および TACACS+ サーバーによって使用されるリモート AAA 属性が収められています。

---

### Radius

IBM ベンダー ID: 211

#### 認証属性

##### 標準の草案

TUNNEL_TYPE	64
TUNNEL_MEDIUM_TYPE	65
TUNNEL_CLIEN_TYPE	66
TUNNEL_SERVER_EP	67
TUNNEL_CONN_ID	68
TUNNEL_PASSWORD	69

値

TUNNEL_TYPE	3	L2TP	整数
TUNNEL_MEDIUM_TYPE	1	IP	整数
TUNNEL_SERVER_EP		IP アドレス	文字列

#### IBM ベンダー特定

NAS_TUNNEL_PASSWORD	101
CALLBACK_FLAGS	210
ENCRYPTION	211
HOSTNAME	213
SUBNETMASK	215
PRIVILEGE	216

### キーワード

Radius サーバーでは、ベンダー特定のフィールド <keyword>=<value> に入力できるキーワードが使用されます。

KWD_CALLBACK_FLAGS	CBF
KWD_ENCRYPTION	ENC
KWD_HOSTNAME	HSN
KWD_SUBNETMASK	SNM

KWD_PRIVELGE	PRV
値	
PRIVILEGE:	
ADMIN	
OPER	
MONITOR	
CALLBACKFLAGS	
REQ	必須コールバック
ROAM	ローミング・コールバック

---

## TACACS+

### 認証

### 承認

```
PPP service=ppp protocol=ip
LOGIN service=shell cmd=null pri_lvl*0
```

### 標準 TACACS+ 属性

```
service
protocol
cmd
addr
timeout
priv_lvl
callback-dialstring
```

### IBM 特定の属性

```
encryption_key    16 進文字
dial_out           TRUE FALSE ONLY
```

### 会計

```
task_id
start_time
stop_time
elapsed_time
timezone
event
reason
bytes
bytes_in
bytes_out
paks
paks_in
```

paks\_out  
status  
err\_msg



## 略語集

- AAL** ATM アダプテーション・レイヤー (ATM Adaptation Layer)
- AAL-5** ATM アダプテーション・レイヤー 5 (ATM Adaptation Layer 5)
- AARP** AppleTalk アドレス解決プロトコル (AppleTalk Address Resolution Protocol)
- ABR** エリア・ボーダー・ルーター (area border router)
- ack** 確認応答 (acknowledgment)
- AIX** 拡張対話式エグゼクティブ (Advanced Interactive Executive)
- AMA** 任意 MAC アドレス指定 (arbitrary MAC addressing)
- AMP** アクティブ・モニター・プレゼント (active monitor present)
- ANSI** 米国規格協会 (American National Standards Institute)
- AP2** AppleTalk フェーズ 2 (AppleTalk Phase 2)
- APPN** 拡張ピアツーピア・ネットワーキング機能 (Advanced Peer-to-Peer Networking)
- ARE** 全ルート探索 (all-routes explorer)
- ARI** ATM 実インターフェース (ATM real interface)
- ARI/FCI**  
アドレス認知標識 / フレーム複写標識 (address recognized indicator/frame copied indicator)
- ARP** アドレス解決プロトコル (Address Resolution Protocol)
- AS** 自律システム (autonomous system)
- ASBR** 自律システム境界ルーター (autonomous system boundary router)
- ASCII** 情報交換用米国標準コード (American National Standard Code for Information Interchange)
- ASN.1** 抽象構文表記法 1 (abstract syntax notation 1)
- ASRT** 適応ソース・ルーティング透過型 (adaptive source routing transparent)
- ASYNC**  
非同期 (asynchronous)
- ATCP** AppleTalk 制御プロトコル (AppleTalk Control Protocol)
- ATM** 非同期転送モード (Asynchronous Transfer Mode)
- ATMARP**  
クラシカル IP 中の ARP (ARP in Classical IP)
- ATP** AppleTalk トランザクション・プロトコル (AppleTalk Transaction Protocol)
- AUI** 接続ユニット・インターフェース (attachment unit interface)
- AVI** ATM バーチャル・インターフェース (ATM virtual interface)
- ayt** are you there (相手確認)
- BAN** 境界アクセス・ノード (Boundary Access Node)
- BBCM** ブリッジング・ブロードキャスト・マネージャー (Bridging Broadcast Manager)

**BCM** ブロードキャスト・マネージャー (BroadCast Manager)

**BECN** 逆方向明示的輻輳 (ふくそう)通知 (backward explicit congestion notification)

**BGP** ボーダー・ゲートウェイ・プロトコル (Border Gateway Protocol)

**BGP** ボーダー成長プロトコル (Border Growth Protocol)

**BNC** Bayonet Niell-Concelman

**BNCP** ブリッジング・ネットワーク制御プロトコル (Bridging Network Control Protocol)

**BOOTP**  
BOOT プロトコル (BOOT protocol)

**BPDU** ブリッジ・プロトコル・データ単位 (bridge protocol data unit)

**bps** ビット / 秒 (bits per second)

**BR** ブリッジング / ルーティング (bridging/routing)

**BRS** 帯域幅予約 (bandwidth reservation)

**BSD** Berkeley ソフトウェア配布 (Berkeley software distribution)

**BTP** BOOTP リレー・エージェント (BOOTP relay agent)

**BTU** 基本伝送単位 (basic transmission unit)

**CAM** コンテンツ・アドレス可能メモリー (content-addressable memory)

**CCITT** 国際電信電話諮問委員会 (Consultative Committee on International Telegraph and Telephone)

**CD** 衝突検出 (collision detection)

**CGWCON**  
ゲートウェイ・コンソール (Gateway Console)

**CIDR** 無クラス・ドメイン間ルーティング (Classless Inter-Domain Routing)

**CIP** クラシカル IP (Classical IP)

**CIR** 認定情報速度 (committed information rate)

**CLNP** コネクションレス型モード・ネットワーク・プロトコル (Connectionless-Mode Network Protocol)

**CPU** 中央演算処理装置 (central processing unit)

**CRC** 巡回冗長検査 (cyclic redundancy check)

**CRS** 構成報告サーバー (configuration report server)

**CTS** 送信可 (clear to send)

**CUD** コール・ユーザー・データ (call user data)

**DAF** あて先アドレス・フィルター (destination address filtering)

**DB** データベース (database)

**DBsum**  
データベース要約 (database summary)

**DCD** データ・チャネル受信回線信号検出器 (data channel received line signal detector)



**DCE** データ回線終端装置 (data circuit-terminating equipment)  
**DCS** 直接接続サーバー (Directly connected server)  
**DDLC** デュアル・データ・リンク制御装置 (dual data-link controller)  
**DDN** 防衛データ・ネットワーク (Defense Data Network)  
**DDP** データグラム送達プロトコル (Datagram Delivery Protocol)  
**DDT** 動的デバッグ・ツール (Dynamic Debugging Tool)  
**DHCP** 動的ホスト構成プロトコル (Dynamic Host Configuration Protocol)  
**dir** 直接接続 (directly connected)  
**DL** データ・リンク (data link)  
**DLC** データ・リンク制御 (data link control)  
**DLCI** データ・リンク接続識別子 (data link connection identifier)  
**DLS** データ・リンク交換 (data link switching)  
**DLSw** データ・リンク交換 (data link switching)  
**DMA** 直接メモリー・アクセス (direct memory access)  
**DNA** デジタル・ネットワーク体系 (Digital Network Architecture)  
**DNCP** DECnet プロトコル制御プロトコル (DECnet Protocol Control Protocol)  
**DNIC** データ・ネットワーク識別コード (Data Network Identifier Code)  
**DoD** 米国国防総省 (Department of Defense)  
**DOS** ディスク・オペレーティング・システム (Disk Operating System)  
**DR** 指定ルーター (designated router)  
**DRAM** 動的ランダム・アクセス・メモリー (Dynamic Random Access Memory)  
**DSAP** あて先サービス・アクセス・ポイント (destination service access point)  
**DSE** データ交換装置 (data switching equipment)  
**DSE** データ交換機 (data switching exchange)  
**DSR** データ・セット・レディー (data set ready)  
**DSU** データ・サービス装置 (data service unit)  
**DTE** データ端末装置 (data terminal equipment)  
**DTR** データ端末レディー (data terminal ready)  
**Dtype** あて先タイプ (destination type)  
**DVMRP**  
 距離ベクトル・マルチキャスト・ルーティング・プロトコル (Distance Vector Multicast Routing Protocol)  
**E1** 2.048 Mbps 伝送速度 (2.048 Mbps transmission rate)  
**EDEL** 終了区切り文字 (end delimiter)  
**EDI** エラー検出標識 (error detected indicator)  
**EGP** 外部ゲートウェイ・プロトコル (Exterior Gateway Protocol)

**EIA** 米国電子工業会 (Electronics Industries Association)

**ELAN** エミュレート LAN (Emulated LAN)

**ELAP** EtherTalk リンク・アクセス・プロトコル (EtherTalk Link Access Protocol)

**ELS** イベント・ログ・システム (Event Logging System)

**ELSCon**  
2 次 ELS コンソール (Secondary ELS Console)

**ESI** エンド・システム識別子 (End system identifier)

**EST** 東部標準時 (Eastern Standard Time)

**Eth** イーサネット (Ethernet)

**fa-ga** 機能アドレス・グループ・アドレス (functional address-group address)

**FCS** フレーム検査シーケンス (frame check sequence)

**FECN** 順方向明示的輻輳 (ふくそう) 通知 (forward explicit congestion notification)

**FIFO** 先入れ先出し (first in, first out)

**FLT** フィルター・ライブラリー (filter library)

**FR** フレーム・リレー (Frame Relay)

**FRL** フレーム・リレー (Frame Relay)

**FTP** ファイル転送プロトコル (File Transfer Protocol)

**GMT** グリニッジ標準時 (Greenwich Mean Time)

**GOSIP**  
米国政府 OSI 調達仕様 (Government Open Systems Interconnection Profile)

**GTE** 一般電話会社 (General Telephone Company)

**GWCON**  
ゲートウェイ・コンソール (Gateway Console)

**HDLC** ハイレベル・データ・リンク制御 (high-level data link control)

**HEX** 16 進法 (hexadecimal)

**HPR** 高性能ルーティング (high-performance routing)

**HST** TCP/IP ホスト・サービス (TCP/IP host services)

**HTF** ホスト・テーブル形式 (host table format)

**IBD** 統合ブート装置 (Integrated Boot Device)

**ICMP** インターネット制御メッセージ・プロトコル (Internet Control Message Protocol)

**ICP** インターネット制御プロトコル (Internet Control Protocol)

**ID** 識別 (identification)

**IDP** イニシアル・ドメイン・パート (Initial Domain Part)

**IDP** インターネット・データグラム・プロトコル (Internet Datagram Protocol)

**IEEE** 米国電気電子学会 (Institute of Electrical and Electronics Engineers)

**IETF** インターネット技術特別調査委員会 (Internet Engineering Task Force)

<b>lfc#</b>	インターフェース番号 (interface number)
<b>IGP</b>	内部ゲートウェイ・プロトコル (interior gateway protocol)
<b>ILMI</b>	インターリム・ローカル管理インターフェース (Interim Local Management Interface)
<b>InARP</b>	逆アドレス解決プロトコル (Inverse Address Resolution Protocol)
<b>IP</b>	インターネット・プロトコル (Internet Protocol)
<b>IPCP</b>	IP 制御プロトコル (IP Control Protocol)
<b>IPPN</b>	IP プロトコル・ネットワーク (IP Protocol Network)
<b>IPX</b>	インターネットワーク・パケット交換 (Internetwork Packet Exchange)
<b>IPXCP</b>	IPX 制御プロトコル (IPX Control Protocol)
<b>ISDN</b>	サービス総合デジタル網 (integrated services digital network)
<b>ISO</b>	国際標準化機構 (International Organization for Standardization)
<b>Kbps</b>	キロビット / 秒 (kilobits per second)
<b>LAC</b>	L2TP ネットワーク・アクセス集線装置 (L2TP Network Access Concentrator)
<b>LAN</b>	ローカル・エリア・ネットワーク (local area network)
<b>LAPB</b>	平衡型リンク・アクセス・プロトコル (link access protocol-balanced)
<b>LAT</b>	ローカル・エリア・トランスポート (local area transport)
<b>LCS</b>	LAN チャネル・ステーション (LAN Channel Station)
<b>LCP</b>	リンク制御プロトコル (Link Control Protocol)
<b>LE</b>	LAN エミュレーション (LAN Emulation)
<b>LEC</b>	LAN エミュレーション・クライアント (LAN Emulation Client)
<b>LED</b>	発光ダイオード (light-emitting diode)
<b>LECS</b>	LAN エミュレーション構成サーバー (LAN Emulation Configuration Server)
<b>LES</b>	LAN エミュレーション・サーバー (LAN Emulation Server)
<b>LES-BUS</b>	LAN エミュレーション・サーバー - 同報通信および未知サーバー (LAN Emulation Server - Broadcast and Unknown Server)
<b>LF</b>	最大フレーム、改行 (largest frame; line feed)
<b>LIS</b>	論理 IP サブネット (Logical IP subnet)
<b>LLC</b>	論理リンク制御 (logical link control)
<b>LLC2</b>	論理リンク制御 2 (論理リンク制御 2)
<b>LMI</b>	ローカル管理インターフェース (local management interface)
<b>LNS</b>	L2TP ネットワーク・サーバー (L2TP Network Server)
<b>LRM</b>	LAN 報告機構 (LAN reporting mechanism)
<b>LS</b>	リンク状態 (link state)
<b>LSA</b>	リンク状態公示 (link state advertisement)

**LSA** リンク・サービス体系 (Link Services Architecture)

**LSB** 最下位ビット (least significant bit)

**LSI** LAN ショートカット・インターフェース (LAN shortcuts interface)

**LSreq** リンク状態要求 (link state request)

**LSrxl** リンク状態再送リスト (link state retransmission list)

**LU** 論理装置 (logical unit)

**MAC** 媒体アクセス制御 (medium access control)

**Mb** メガビット (megabit)

**MB** メガバイト (megabyte)

**Mbps** メガビット / 秒 (megabits per second)

**MBps** メガバイト / 秒 (megabytes per second)

**MC** マルチキャスト (multicast)

**MCF** MAC フィルター (MAC filtering)

**MIB** 管理情報ベース (Management Information Base)

**MIB II** 管理情報ベース II (Management Information Base II)

**MILNET**  
軍事ネットワーク (military network)

**MOS** マイクロ・オペレーティング・システム (Micro Operating System)

**MOSDBG**  
マイクロ・オペレーティング・システム・デバッグ・ツール (Micro Operating System Debugging Tool)

**MOSDDT**  
マイクロ・オペレーティング・システム動的デバッグ・ツール (Micro Operating System Dynamic Debugging Tool)

**MOSPF**  
マルチキャスト拡張付き最短パス最優先オープン (Open Shortest Path First with multicast extensions)

**MPC** マルチパス・チャネル (Multi-Path Channel)

**MPC+** ハイパフォーマンス・データ転送 (HPDT) マルチパス・チャネル (High performance data transfer (HPDT) Multi-Path Channel)

**MSB** 最上位ビット (most significant bit)

**MSDU** MAC サービス・データ単位 (MAC service data unit)

**MSS** マルチプロトコル・スイッチ・サービス (Multiprotocol Switched Services)

**MRU** 最大受信単位 (maximum receive unit)

**MTU** 最大伝送単位 (maximum transmission unit)

**nak** 否定応答 (not acknowledged)

**NAS** Nways スイッチ管理ステーション (Nways Switch Administration station)

**NBMA** 非同報通信マルチアクセス (Non-Broadcast Multiple Access)

**NBP** ネーム・バインディング・プロトコル (Name Binding Protocol)

**NBR** 近隣、ネイバー (neighbor)

**NCP** ネットワーク制御プロトコル (Network Control Protocol)

**NCP** ネットワーク・コア・プロトコル (Network Core Protocol)

**NDPS** 非介入パス・スイッチ (non-disruptive path switching)

**NetBIOS**  
ネットワーク基本入出力システム (Network Basic Input/Output System)

**NHRP** ネクスト・ホップ解決プロトコル (Next Hop Resolution Protocol)

**NIST** 米国連邦情報技術局 (National Institute of Standards and Technology)

**NPDU** ネットワーク・プロトコル・データ単位 (Network Protocol Data Unit)

**NRZ** 非ゼロ復帰 (non-return-to-zero)

**NRZI** 非ゼロ復帰反転 (non-return-to-zero inverted)

**NSAP** ネットワーク・サービス・アクセス・ポイント (Network Service Access Point)

**NSF** 国立科学財団 (National Science Foundation)

**NSFNET**  
国立科学財団ネットワーク (National Science Foundation NETwork)

**NVCNFG**  
不揮発性構成 (nonvolatile configuration)

**OPCON**  
オペレーター・コンソール (Operator Console)

**OSI** 開放型システム間相互接続 (open systems interconnection)

**OSICP**  
OSI 制御プロトコル (OSI Control Protocol)

**OSPF** 最短パス最優先オープン (Open Shortest Path First)

**OUI** 組織固有識別子 (organization unique identifier)

**PC** パーソナル・コンピューター (personal computer)

**PCA** 並列チャネル・アダプター (parallel channel adapter)

**PCR** ピーク・セル速度 (peak cell rate)

**PDN** 公衆データ網 (public data network)

**PING** パケット・インターネット・グローパー (Packet internet groper)

**PDU** プロトコル・データ単位 (protocol data unit)

**PID** プロセス識別子 (process identification)

**P-P** ポイント・ポイント (Point-to-Point)

**PPP** ポイント・ポイント・プロトコル (Point-to-Point Protocol)

**PROM** プログラム式読み取り専用メモリー (programmable read-only memory)

**PU** 物理装置 (physical unit)

**PVC** パーマネント・バーチャル・サーキット (permanent virtual circuit)

<b>Qos</b>	サービス品質 (Quality of Service)
<b>RAM</b>	ランダム・アクセス・メモリー (random access memory)
<b>RD</b>	ルート記述子 (route descriptor)
<b>REM</b>	リング・エラー監視 (ring error monitor)
<b>REV</b>	受信 (receive)
<b>RFC</b>	コメント要求 (Request for Comments)
<b>RI</b>	リング標識、ルーティング情報 (ring indicator; routing information)
<b>RIF</b>	ルーティング情報フィールド (routing information field)
<b>RII</b>	ルーティング情報標識 (routing information indicator)
<b>RIP</b>	ルーティング情報プロトコル (Routing Information Protocol)
<b>RISC</b>	縮小命令セット・コンピューター (reduced instruction-set computer)
<b>RNR</b>	受信不可 (receive not ready)
<b>ROM</b>	読み取り専用メモリー (read-only memory)
<b>ROpcon</b>	リモート・オペレーター・コンソール (Remote Operator Console)
<b>RPS</b>	リング・パラメーター・サーバー (ring parameter server)
<b>RTMP</b>	ルーティング・テーブル保守プロトコル (Routing Table Maintenance Protocol)
<b>RTP</b>	ルーティング更新プロトコル (RouTing update Protocol)
<b>RTS</b>	送信要求 (request to send)
<b>Rtype</b>	ルート・タイプ (route type)
<b>rxmits</b>	再送 (retransmissions)
<b>rxmt</b>	再送する (retransmit)
<b>s</b>	秒 (second)
<b>SAF</b>	発信元アドレス・フィルター (source address filtering)
<b>SAP</b>	サービス・アクセス・ポイント (Service access point)
<b>SAP</b>	サービス公示プロトコル (Service Advertising Protocol)
<b>SCR</b>	持続セル速度 (Sustained cell rate)
<b>SCSP</b>	サーバー・キャッシュ同期プロトコル (Server Cache Synchronization Protocol)
<b>sdel</b>	開始区切り文字 (start delimiter)
<b>SDLC</b>	SDLC リレー、同期データ・リンク制御 (SDLC relay, synchronous data link control)
<b>SDU</b>	サービス・データ単位 (Service Data Unit)
<b>seqno</b>	シーケンス番号 (sequence number)
<b>SGID</b>	サーバー・グループ ID (sever group id)
<b>SGMP</b>	シンプル・ゲートウェイ監視プロトコル (Simple Gateway Monitoring Protocol)
<b>SL</b>	シリアル・ライン (serial line)

<b>SLIP</b>	シリアル・ライン IP (Serial Line IP)
<b>SMP</b>	待機モニター・プレゼント (standby monitor present)
<b>SMTP</b>	シンプル・メール転送プロトコル (Simple Mail Transfer Protocol)
<b>SNA</b>	システム・ネットワーク体系 (Systems Network Architecture)
<b>SNAP</b>	サブネットワーク・アクセス・プロトコル (Subnetwork Access Protocol)
<b>SNMP</b>	シンプル・ネットワーク管理プロトコル (Simple Network Management Protocol)
<b>SNPA</b>	サブネットワーク接続ポイント (subnetwork point of attachment)
<b>SPF</b>	OSPF エリア内ルート (OSPF intra-area route)
<b>SPE1</b>	OSPF 外部ルート・タイプ 1 (OSPF external route type 1)
<b>SPE2</b>	OSPF 外部ルート・タイプ 2 (OSPF external route type 2)
<b>SPIA</b>	OSPF エリア間ルート・タイプ (OSPF inter-area route type)
<b>SPID</b>	サービス・プロファイル ID (service profile ID)
<b>SPX</b>	順次パケット交換 (Sequenced Packet Exchange)
<b>SQE</b>	信号品質エラー (signal quality error)
<b>SRAM</b>	静的ランダム・アクセス・メモリー (static random access memory)
<b>SRB</b>	ソース・ルーティング・ブリッジ (source routing bridge)
<b>SRF</b>	特定ルート・フレーム (specifically routed frame)
<b>SRLY</b>	SDLC リレー (SDLC relay)
<b>SRT</b>	ソース・ルーティング透過型 (source routing transparent)
<b>SR-TB</b>	ソース・ルーティング - 透過型ブリッジ (source routing-transparent bridge)
<b>STA</b>	静的 (static)
<b>STB</b>	スパンニング・ツリー・ブリッジ (spanning tree bridge)
<b>STE</b>	スパンニング・ツリー探索 (spanning-tree explorer)
<b>STP</b>	シールド付き対より線、スパンニング・ツリー・プロトコル (shielded twisted pair; spanning tree protocol)
<b>SVC</b>	スイッチド・バーチャル・サーキット (switched virtual circuit)
<b>SVN</b>	スイッチド・バーチャル・ネットワーキング (Switched Virtual Networking)
<b>TB</b>	透過型ブリッジ (transparent bridge)
<b>TCN</b>	トポロジ変更通知 (topology change notification)
<b>TCP</b>	伝送制御プロトコル (Transmission Control Protocol)
<b>TCP/IP</b>	伝送制御プロトコル / インターネット・プロトコル (Transmission Control Protocol/Internet Protocol)
<b>TEI</b>	端末終端点識別子 (terminal point identifier)
<b>TFTP</b>	トリビアル・ファイル転送プロトコル (Trivial File Transfer Protocol)
<b>TKR</b>	トークンリング (token ring)

<b>TLV</b>	タイプ/長さ/値 (Type/Length/Value)
<b>TMO</b>	タイムアウト (timeout)
<b>TOS</b>	サービスのタイプ (type of service)
<b>TSF</b>	透過型スパンニング・フレーム (transparent spanning frames)
<b>TTL</b>	活動回数 (time to live)
<b>TTY</b>	テレタイプライター (teletypewriter)
<b>TX</b>	送信 (transmit)
<b>UA</b>	非番号制確認 (unnumbered acknowledgment)
<b>UDP</b>	ユーザー・データグラム・プロトコル (User Datagram Protocol)
<b>UI</b>	非番号制情報 (unnumbered information)
<b>UNI</b>	ユーザー・ネットワーク・インターフェース (User-Network Interface)
<b>UTP</b>	シールドなし対より線 (unshielded twisted pair)
<b>VCC</b>	バーチャル・チャネル・コネクション (Virtual Channel Connection)
<b>VINES</b>	バーチャル・ネットワーキング・システム (VirtuAl NETworking System)
<b>VIR</b>	可変情報速度 (variable information rate)
<b>VL</b>	バーチャル・リンク (virtual link)
<b>VNI</b>	バーチャル・ネットワーク・インターフェース (Virtual Network Interface)
<b>VR</b>	バーチャル・ルート (virtual route)
<b>WAN</b>	広域ネットワーク (wide area network)
<b>WRS</b>	WAN 復元 / 再ルート (WAN restoral/reroute)
<b>X.25</b>	パケット交換網 (packet-switched networks)
<b>X.251</b>	X.25 物理レイヤー (X.25 physical layer)
<b>X.252</b>	X.25 フレーム・レイヤー (X.25 frame layer)
<b>X.253</b>	X.25 パケット・レイヤー (packet layer)
<b>XID</b>	交換 ID (exchange identification)
<b>XNS</b>	Xerox ネットワーク・システム (Xerox Network Systems)
<b>XSUM</b>	チェックサム (checksum)
<b>ZIP</b>	AppleTalk ゾーン情報プロトコル (AppleTalk Zone Information Protocol)
<b>ZIP2</b>	AppleTalk ゾーン情報プロトコル 2 (AppleTalk Zone Information Protocol 2)
<b>ZIT</b>	ゾーン情報テーブル (Zone Information Table)



## 用語集

この用語集には、以下からの用語および定義が含まれています。

- *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990 (米国規格協会 (ANSI) が 1990 年に著作権を取得)。この複写版が米国規格協会 (ANSI: 11 West 42nd Street, New York, New York 10036) から発売されています。定義の後に記号 (A) を付けて出典を示してあります。
- ANSI/EIA Standard--440-A, *Fiber Optic Terminology*。この複写版が米国電子工業会 (2001 Pennsylvania Avenue, N.W., Washington, DC 20006) から発売されています。定義の後に記号 (E) を付けて出典を示してあります。
- *Information Technology Vocabulary*。国際標準化機構および国際電気標準会議の第 1 合同技術委員会第 1 分科会 (ISO/IEC JTC1/SC1) によって編さんされたものです。この語い集の刊行部分から転載した定義については、その後に記号 (I) を付けて示してあります。また、ISO/IEC JTC1/SC1 で編さん中の国際規格草案、分科会草案、および作業文書から採用した定義については、その後に記号 (T) を付けて、SC1 の加盟各国諸団体間で最終合意がなされていないことを示してあります。
- *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users' Glossary*
- *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

この用語集では、以下の形で相互参照しています。

### と対比:

反対の意味または実質的に異なる意味をもつ用語を示します。

### の同義語:

この用語集の該当箇所に記述されている、優先的に使用してほしい、同じ意味をもつ用語を示します。

### と同義:

逆方向参照として、定義の対象となっている用語から、同じ意味をもつ他の用語をすべて参照します。

### を参照:

一部の語 (特に最後の語) が同じ複数語からなる用語を参照します。

### も参照:

関連する意味 (同義ではない) をもつ用語を参照します。

## A

**AAL.** ATM アダプテーション・レイヤー (ATM Adaptation Layer)。ヘッダーを追加/除去し、セルへからのデータを細分化/再組み立てすることにより、ATM ネットワークへからのユーザー・データを適応させるレイヤー。

**AAL-5.** ATM アダプター・レイヤー 5 (ATM Adaptation Layer 5)。複数ある標準 AAL の 1 つ。AAL-5 はデータ通信に設計されたもので、LAN エミュレーションおよびクラシカル IP によって使用される。

**抽象構文 (abstract syntax).** データ伝送に必要な特性はすべて含んでいるが、その他の明細 (たとえば、特定のコンピューター・アーキテクチャーに依存する明細など) は省略 (抽象化) されているデータ仕様。抽象構文表記法 (ASN.1) (*abstract syntax notation 1 (ASN.1)*) および基本符号化規則 (BER) (*basic encoding rules (BER)*) も参照。

**抽象構文表記法 1 (ASN.1) (abstract syntax notation 1 (ASN.1)).** 次の標準で指定されている抽象構文の開放型システム間相互接続 (OSI) 方式。

- ITU-T 勧告 X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T 勧告 X.680 (1994) | ISO/IEC 8824-1: 1994

基本符号化規則 (BER) (*basic encoding rules (BER)*) も参照。

**ACCESS.** シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、管理ノードがオブジェクトに対して提供する最小レベルのサポートを定義する、管理情報ベース (MIB) モジュール内の文節。

**確認応答 (acknowledgment).** (1) 受信側が送信側に肯定応答として確認応答文字を伝送すること。(T) (2) 送信された項目が受信されたことを示すこと。

**アクティブ (active).** (1) 運用可。(2) 別のノードまたは装置に接続された、またはそれへの接続が利用可能なノードまたは装置に関する用語。

**アクティブ・モニター (active monitor).** トークンリング・ネットワークにおいて、一度に 1 つのリング・ステーションによって実行される機能で、トークンの伝送を開始し、トークン誤り回復機能を提供する。現在のアクティブ・モニターに障害が起こった場合、リング上の任意のアクティブ・アダプターが、アクティブ・モニター機能を提供することができる。

**アドレス (address).** データ通信において、通信ネットワークに接続された各装置、ワークステーション、またはユーザーに割り当てられる固有のコード。

**アドレス・マッピング・テーブル (AMT) (address mapping table (AMT)).** 現在のノード・アドレスとハードウェア・アドレスのマッピングを提供する、AppleTalk ルーター内に維持されているテーブル。

**アドレス・マスク (address mask).** インターネット・サブネットワークにおいて、IP アドレスのホスト部分のサブネットワーク・アドレス・ビットを識別するために使用される、32 ビットのマスク。サブネット・マスク (*subnet mask*) およびサブネットワーク・マスク (*subnetwork mask*) と同義。

**アドレス解決 (address resolution).** (1) ネットワーク・レイヤー・アドレスを媒体特有アドレスにマッピングする方法。(2) アドレス解決プロトコル (*ARP*) (*Address Resolution Protocol (ARP)*) および *AppleTalk* アドレス解決プロトコル (*AARP*) (*AppleTalk Address Resolution Protocol (AARP)*) も参照。

**アドレス解決プロトコル (ARP) (Address Resolution Protocol (ARP)).** (1) インターネット・プロトコルにおいて、サポートされる大都市圏ネットワークやローカル・エリア・ネットワーク (イーサネットやトークンリングなど) が使用するアドレスに、IP アドレスを動的にマップするプロトコル。(2) 逆アドレス解決プロトコル (*RARP*) (*Reverse Address Resolution Protocol (RARP)*) も参照。

**アドレッシング (addressing).** データ通信において、端末局がデータの送信先の端末局を選択する方法。

**隣接ノード (adjacent nodes).** 他のノードとは接続していない少なくとも 1 つのパスによって相互に接続されている 2 つのノード。(T)

**管理ドメイン (Administrative Domain).** 1 つの管理機能によって管理される、ホストとルーターおよび相互接続ネットワークの集合。

**拡張ピアツーピア・ネットワーキング機能 (Advanced Peer-to-Peer Networking) (APPN).** SNA の拡張機能で、次の特長を備えている。(a) 重大な階層間の依存関係を回避することによって、単一点の障害の影響を分離できるようにした、分散ネットワーク制御の機能強化。(b) 接続、再構成、および柔軟なルート選択を容易に実現できる、動的なネットワーク・トポロジー情報の交換。(c) ネットワークの資源の動的定義。(d) 資源の登録およびディレクトリー検索の自動化。APPN は、エンド・ユーザー・サービス向けの LU 6.2 ピア間通信機能をネットワークの制御に拡張し、LU 2、LU 3、および LU 6.2 を含む複数の LU タイプをサポートする。

**拡張ピアツーピア・ネットワーキング機能 (APPN) エンド・ノード (Advanced Peer-to-Peer Networking (APPN) end node).** 広範囲のエンド・ユーザー・サービスを提供し、そのローカル・コントロール・ポイント (CP) と隣接するネットワーク・ノード内の CP との間のセッションをサポートするノード。このノードは、これらのセッションを使用して、隣接 CP (ネットワーク・ノード・サーバー) に資源を動的に登録し、ディレクトリー検索要求を送受信し、管理サービスを受ける。APPN エンド・ノードは、サブエリア・ネットワークに周辺ノードまたは他のエンド・ノードとして接続することもできる。

**拡張ピアツーピア・ネットワーキング機能 (APPN) ネットワーク (Advanced Peer-to-Peer Networking (APPN) network).** 相互接続されたネットワーク・ノードとそれらのクライアント・エンド・ノードの集合。

**拡張ピアツーピア・ネットワーキング機能 (APPN) ネットワーク・ノード (Advanced Peer-to-Peer Networking (APPN) network node).** 広範囲のエンド・ユーザー・サービスを提供するノードで、次のものを提供することができる。

- 分散ディレクトリー・サービス (中央ディレクトリー・サーバーへのドメインの資源の登録を含む)
- トポロジー・データベースは他の APPN ネットワーク・ノードと交換し、そのネットワーク内のネットワークが、要求されたサービス・クラスに基づいて LU-LU セッションの最適ルートを選択できるようにする。
- そのローカル LU とクライアント・エンド・ノードのセッション・サービス
- APPN ネットワークの中間ルーティング・サービス

**拡張ピアツーピア・ネットワーキング機能 (APPN) ノード (Advanced Peer-to-Peer Networking (APPN) node).** APPN ネットワーク・ノードまたは APPN エンド・ノード。

**エージェント (agent).** エージェントの役割を果たすシステム。

**アラート (alert).** 問題または切迫した問題を識別するためにネットワーク内の管理サービス中心拠点に送られるメッセージ。

**全ステーション・アドレス (all-stations address).** 通信において、同報通信アドレス (*broadcast address*) の同義語。

**米国規格協会 (ANSI) (American National Standards Institute (ANSI)).** 認定組織が米国の自主業界標準を作成して維持するための手順を決める、生産者、消費者、および一般の関係団体から構成される組織。(A)

**アナログ (analog).** (1) 連続的に変化する物理量から構成されるデータに関する用語。(A) (2) デジタル (*digital*) と対比。

**AppleTalk.** Apple Computer, Inc. によって開発されたネットワーク・プロトコル。このプロトコルは、ネットワーク上の装置を相互接続するために使用される。装置は、Apple 製品と非 Apple 製品を混合して使用できる。

**AppleTalk アドレス解決プロトコル (AARP) (AppleTalk Address Resolution Protocol (AARP)).** AppleTalk ネットワークにおいて、(a) AppleTalk ノード・アドレスをハードウェア・アドレスに変換し、(b) 複数のプロトコルをサポートするネットワーク内のアドレッシングの矛盾を調整するプロトコル。

**AppleTalk トランザクション・プロトコル (ATP) (AppleTalk Transaction Protocol (ATP)).** AppleTalk ネットワークにおいて、ゾーン情報を得るためにゾーン情報プロトコル (ZIP) にアクセスするホストに対して、クライアント/サーバー要求・応答機能を提供するプロトコル。

**APPN ネットワーク (APPN network).** 拡張ピアツーピア・ネットワーク機能 (*APPN*) ネットワーク (*Advanced Peer-to-Peer Networking (APPN) network*) を参照。

**APPN ネットワーク・ノード (APPN network node).** 拡張ピアツーピア・ネットワーク機能 (*APPN*) ネットワーク・ノード (*Advanced Peer-to-Peer Networking (APPN) network node*) を参照。

**任意 MAC アドレッシング (AMA) (arbitrary MAC addressing (AMA)).** DECnet 体系において、出荷時設定アドレスとローカル管理アドレスをサポートする、DECnet フェーズ IV-Prime によって使用されるアドレッシング機構。

**エリア、区域 (area).** インターネットおよび DECnet ルーティング・プロトコルにおいて、ネットワークの通信事業者の定義によってグループ化された、ネットワークまたはゲートウェイのサブセット。各エリアは自己完結型で、あるエリアのトポロジーは他のエリアからは見えない。

**非同期 (ASYNC) (asynchronous (ASYNC)).** 共通タイミング信号のような特定の事象の発生に依存しない 2 つ以上のプロセス。(T)

**ATM.** 非同期転送モード (*Asynchronous Transfer Mode*)。セル交換を基礎とした、コネクション型高速ネットワーク・テクノロジー。

**ATMARP.** クラシカル IP 内の ARP。

**接続ユニット・インターフェース (AUI) (attachment unit interface (AUI)).** ローカル・エリア・ネットワークにおいて、媒体接続ユニットとデータ・ステーション内のデータ端末装置間のインターフェース。(I) (A)

**属性値ペア (AVP) (Attribute Value Pair (AVP)).** メッセージ・タイプおよび本文をコード化する一律的な方法。この方式は、L2TP のインターオペラビリティを可能にすると同時に、拡張性を最大化する。

**認証障害 (authentication failure).** シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、要求側クライアントが SNMP コミュニティーのメンバーでない場合に、認証エンティティーが生成するトラップ。

**自律システム (autonomous system).** TCP/IP において、1 つの管理機関の下にあるネットワークとルーターの集まり。このようなネットワークとルーターは緊密に協力し、自ら選択した内部ゲートウェイ・プロトコルを使用して、相互にネットワークの到達可能性とルーティングの情報を伝送する。

**自律システム番号 (autonomous system number).** TCP/IP において、IP アドレスの割り当てを行うのと同じ中央電気通信事業者が自律システムに割り当てる番号。自律システム番号により、自動ルーティング・アルゴリズムは、自律システムを区別することができる。

## B

**BCM.** ブロードキャスト・マネージャー (*BroadCast Manager*)。同報通信フレームの効果を制限するために設計された、LAN エミュレーションの IBM 拡張版。

**バックボーン (backbone).** (1) ローカル・エリア・ネットワークのマルチ・ブリッジ・リング構成において、ブ



リッジまたはルーターを用いてリングが接続されている高速リンク。バックボーンは、バスまたはリングとして構成することができる。(2) 広域ネットワークにおいて、ノードまたはデータ交換機 (DSE) が接続されている高速リンク。

**バックボーン・ネットワーク (backbone network).** より小規模の (通常は、より低速の) ネットワークを接続する中央のネットワーク。バックボーン・ネットワークは通常、相互接続するネットワークよりもはるかに高容量の通信ネットワーク、あるいは公用パケット交換データグラム・ネットワークのような広域ネットワーク (WAN) である。

**バックボーン・ルーター (backbone router).** (1) エリア間でデータを転送するのに使用されるルーター。(2) ネットワークをより大規模なインターネットに接続するのに使用される、一連のルーターの中の 1 つ。

**帯域幅 (Bandwidth).** 光リンクの帯域幅は、リンクが情報を運ぶ容量を表し、光リンクがサポートできる最大ビット・レートを示す。

**基本伝送単位 (BTU) (basic transmission unit (BTU)).** SNA において、バス制御コンポーネント間で受け渡されるデータと制御情報の単位。BTU は、1 つまたは複数のバス情報単位 (PIU) から構成される。

**ポー (baud).** 非同期伝送において、1 秒当りの変調速度の単位。つまり、サイクル間隔が 20 ミリ秒の場合、変調速度は 50 ポーになる。(A)

**ブートストラップ (bootstrap).** (1) コンピューター・プログラムが完全に記憶装置に入り終わるまで、後に続く命令をロードして実行させる一連の命令。(T) (2) それ自体の働きによって望ましい状態に到達するように設計された技法または装置。たとえば、最初の幾つかの命令が、残りの命令を入力装置からコンピューターに読み込むようになっている機械ルーチン。(A)

**ボーダー・ゲートウェイ・プロトコル (BGP) (Border Gateway Protocol (BGP)).** ドメインと自律システムの間で使用されるインターネット・プロトコル (IP) ルーティング・プロトコル。

**ボーダー・ルーター (border router).** インターネット通信において、自律システムの端に位置し、別の自律システムの端にあるルーターと通信するルーター。

**ブリッジ (bridge).** 複数の LAN を (ローカルまたはリモート側で) 相互接続する機能を持った装置で、同じ論理リンク制御プロトコルを使用するが、異なる媒体アクセス制御プロトコルを使用することができる。ブリッジは、媒体アクセス制御 (MAC) アドレスに基づいてフレームを別のブリッジに転送する。

**ブリッジ識別子 (bridge identifier).** スパニング・ツリー・プロトコルで使用される、最下位ポート識別子をもつポートの MAC アドレスとユーザー定義の値から構成される 8 バイトのフィールド。

**ブリッジング (bridging).** LAN では、フレームを 1 つの LAN セグメントから別のセグメントに転送すること。着側は、フレーム・ヘッダーの着信アドレス・フィールドに符号化された媒体アクセス制御 (MAC) サブレイヤー・アドレスによって指定される。

**同報通信 (broadcast).** (1) すべてのあて先に同じデータを伝送すること。(T) (2) 複数のあて先に同時にデータを伝送すること。(3) マルチキャスト (*multicast*) と対比。

**同報通信アドレス (broadcast address).** 通信において、リンク上のすべてのステーションに共通のアドレスとして確保されているステーション・アドレス (8 桁の 1 で構成)。全ステーション・アドレス (*all-stations address*) と同義。

**BUS.** 同報通信および未知サーバー (Broadcast and Unknown Server)。マルチキャスト・フレームおよび不明ユニキャスト・フレームの送達を担当する LAN エミュレーション・サービス・コンポーネント。

## C

**キャッシュ (cache).** (1) 主記憶装置から読み出した、プロセッサが次に必要になる可能性がある命令とデータのコピーを入れておくために使用される、主記憶装置より小さくて高速の特殊用途バッファ記憶装置。(T) (2) 頻繁にアクセスされる命令とデータを入れておくバッファ記憶装置。アクセス時間を短縮するために使用される。(3) ディレクトリーの検索速度を上げるために、頻繁に使用されるディレクトリー情報を入れておくことができる、ネットワーク・ノード内のディレクトリー・データベースのオプション部。(4) キャッシュに入れる、または保管すること。

**コール・リクエスト・パケット (call request packet).** (1) コールのための接続を確立することを要求するために、データ端末装置 (DTE) がネットワーク全体に伝送するコール監視パケット。(2) X.25 通信において、ネットワークを通してコール設定を要求するために、DTE によって伝送されるコール監視パケット。

**標準アドレス (canonical address).** LAN において、トークンリングまたはイーサネット・アダプターの媒体アクセス制御 (MAC) アドレスを伝送するための IEEE 802.1 形式。標準形式では、各アドレス・バイトの最下位 (右端) ビットが最初に伝送される。非標準アドレス (*noncanonical address*) と対比。

**キャリア (carrier).** 通信システムを介して伝送される情報を運ぶ信号によって変化する電波、電磁波、またはパルス列。(T)

**キャリア検出 (carrier detect).** 受信回線信号検出器 (RLSD) (received line signal detector (RLSD)) の同義語。

**キャリア・センス (carrier sense).** ローカル・エリア・ネットワークにおいて、別のステーションが伝送中であるかどうかを検出する、データ・ステーションの機能。(T)

**搬送波検知多重アクセス/衝突検出 (CSMA/CD) (carrier sense multiple access with collision detection (CSMA/CD)).** キャリア・センスを必要とするプロトコル。送信側データ・ステーションは、伝送中に別の信号を検出すると、送信を停止し、ジャム信号を送り、可変時間待ってから再試行する。(T) (A)

**CCITT.** 国際電信電話諮問委員会 (International Telegraph and Telephone Consultative Committee)。以前は国際電気通信連合 (ITU) の組織であったが、1993年3月1日にITUは再編成され、標準化の任務は、電気通信連合の電気通信標準化部門 (ITU-TS) という名前の下部組織に移管された。『CCITT』という用語は、再編成の前に承認された勧告を表すのに引き続き使用される。

**チャンネル (channel).** (1) 信号を送ることができるパス。たとえば、データ・チャンネル、出力チャンネル。(A) (2) 主記憶装置とローカル周辺装置との間のデータ転送を扱う、処理装置によって制御される装置。

**チャンネル・サービス・ユニット (CSU) (channel service unit (CSU)).** デジタル・ネットワークへのインターフェースを提供する装置。CSUは、チャンネル帯域幅内で信号の効率を一定に保つ伝送路調整 (等化) 機能、バイナリー・パルス・ストリームを構成する信号再編成機能、およびCSUと通信事業者のオフィス・チャンネル装置間のテスト信号伝送を含めたループバック・テスト機能を提供する。データ・サービス装置 (DSU) (data service unit (DSU)) も参照。

**チャンネル化 (channelization).** 通信回線上の帯域幅を多数のチャンネル (サイズが異なる場合もある) に分割するプロセス。**時分割多重方式 (time division multiplexing) (TDM)** と呼ばれる。

**チェックサム (checksum).** (1) グループに関連し、検査目的で使用される、データのグループの合計。(T) (2) 誤り検出において、ブロック内の全ビットを対象とする。書き込まれて計算された合計に一致しない場合は、誤りが指示される。(3) ディスクットにおいて、誤り検出の目的でセクターに書き込まれるデータ。計算されたチェックサムが、セクターに書き込まれたデータのチェックサ

ムに一致しない場合は、不良セクターを示している。データは、数字またはチェックサムの計算では数字とみなされる他の文字列のいずれかである。

**CIP.** クラシカル IP (Classical IP)。

**CIPC.** クラシカル IP クライアント (Classical IP Client)。

**クラシカル IP (Classical IP).** ATM 上で IP を使用して通信するための ATM 接続ホストの IETF 標準。

**クラシカル IP クライアント (Classical IP Client).** 論理 IP サブネットのユーザーを表すクラシカル IP コンポーネント。

**サーキット交換 (circuit switching).** (1) 必要に応じて、2 つ以上のデータ端末装置 (DTE) を接続し、その接続が解放されるまで、それらの装置間のデータ回線を専用を使用することができるプロセス。(I) (A) (2) 回線交換 (line switching) と同義。

**クラス A ネットワーク (class A network).** インターネット通信において、IP アドレスの上位 (最上位) ビットが 0 に設定され、ホスト ID が下位の 3 オクテットを占めるネットワーク。

**クラス B ネットワーク (class B network).** インターネット通信において、IP アドレスの 2 つの上位 (最上位と最上位の次の) ビットがそれぞれ 1 と 0 に設定され、ホスト ID が下位の 2 オクテットを占めるネットワーク。

**サービス・クラス (COS) (class of service (COS)).** セッションのパートナー間のルートを確認するために使用される一組の特性 (ルートのセキュリティー、伝送の優先順位、帯域幅など)。サービス・クラスは、セッションの開始プログラムによって指定されたモード名から導出される。

**クライアント (client).** (1) サーバーから共用サービスを受け取る機能単位。(T) (2) ユーザーのこと。

**クライアント/サーバー (client/server).** 通信において、一方の側のプログラムが相手側のプログラムに要求を送信して応答を待つという、分散データ処理における対話のモデル。要求側プログラムをクライアントといい、応答側プログラムをサーバーという。

**クロッキング、刻時 (clocking).** (1) 2 進データ同期通信において、クロック・パルスを使用して、データおよび制御文字の同期を制御すること。(2) 一定時間に通信回線上で送信するデータ・ビット数を制御する方法。

**衝突 (collision).** チャンネル上の同時伝送によって生じる望ましくない状態。(T)

**衝突検出 (collision detection).** 搬送波検知多重アクセス/衝突検出 (CSMA/CD) において、2 台以上のステーションが同時に伝送していることを示す信号。

**認定情報速度 (Committed information rate).** ネットワークが送達することに同意した、ビットで表されたデータの最大量。

**コミュニティ (community).** シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、エンティティー間の管理関係。

**コミュニティ名 (community name).** シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、コミュニティを識別するオクテット列。

**圧縮 (compression).** (1) レコードまたはブロックの長さを短縮するために、ギャップ、空のフィールド、冗長要素、および不必要なデータを除去する処理。(2) メッセージまたは記録を表すのに使用するビット数を減らすために符号化すること。

**構成 (configuration).** (1) 情報処理システムのハードウェアとソフトウェアを編成し、相互に接続する方法。(T) (2) システム、サブシステム、またはネットワークを構成する装置とプログラム。

**構成データベース (CDB) (configuration database (CDB)).** 1 つまたは複数の装置の構成パラメーターを保管するデータベース。構成プログラムを使用して作成し、更新する。

**構成ファイル (configuration file).** システム装置またはネットワークの特性を指定するファイル。

**構成パラメーター (configuration parameter).** 構成定義内の変数で、その値により、あるプロダクトと同じネットワーク内の別のプロダクトの特性を表したり、プロダクト自体の特性を定義する。

**構成報告書サーバー (CRS) (configuration report server (CRS)).** IBM トークンリング・ネットワーク・ブリッジ・プログラムにおいて、LAN ネットワーク・マネージャー (LNM) からのコマンドを受け入れて、ステーション情報を入手する、ステーション・パラメーターを設定する、およびステーションをリングから除去するサーバー。また、このサーバーは、リング上のステーションによって生成された構成報告書の収集および転送も行う。構成報告書には、新しいアクティブ・モニター報告書および最近隣アクティブ・アップストリーム (NAUN) 報告書が含まれる。

**輻輳 (ふくそう) (congestion).** ネットワーク輻輳 (ふくそう) (*network congestion*) を参照。

**接続、コネクション (connection).** データ通信において、情報を伝達するために装置間に設定される関係。(I) (A)

**コントロール・ポイント (CP) (control point (CP)).** (1) ノードの資源を管理する、APPN ノードまたは LEN ノードのコンポーネント。APPN ノードでは、CP は他の APPN ノードとの CP-CP セッションを行うことができる。APPN ネットワーク・ノードでは、CP は APPN ネットワークの隣接エンド・ノードへのサービスも提供する。(2) ノードの資源を管理し、オプションでネットワークの他のノードにサービスを提供する、該当ノードのコンポーネント。その例としては、タイプ 5 サブエリア・ノードのシステム・サービス・コントロール・ポイント (SSCP)、APPN ネットワーク・ノードのネットワーク・ノード・コントロール・ポイント (NNCP)、および APPN または LEN エンド・ノードのエンド・ノード・コントロール・ポイント (ENCP) がある。SSCP および NNCP は、他のノードへのサービスを提供することができる。

**コントロール・ポイント管理サービス (CPMS) (control point management services (CPMS)).** 管理サービス機能から構成され、問題管理、効率および会計管理、変更管理、および構成管理を実行するのに役立つ機能を提供する、コントロール・ポイントの構成要素。CPMS によって提供される機能には、システム資源をテストするために要求を物理装置管理サービス (PUMS) に送信する機能、システム資源に関する統計情報 (たとえば、誤りデータやパフォーマンス・データ) を PUMS から収集する機能、およびテスト結果と収集されたシステム資源に関する統計情報を分析および表示する機能が含まれる。問題判別およびパフォーマンス監視を分析および表示する機能は、複数の CPMS 間に分散することができる。

**コントロール・ポイント管理サービス単位 (CP-MSU) (control point management services unit (CP-MSU)).** 管理サービス機能セット間を流れる、管理サービス・データが入っているメッセージ単位。このメッセージ単位は、汎用データ・ストリーム (GDS) 形式である。管理サービス単位 (MSU) (*management services unit (MSU)*) およびネットワーク管理ベクトル移送 (NMVT) (*network management vector transport (NMVT)*) も参照。

**CU 論理アドレス (CU Logical Address).** 2216 に対してホストによって定義された制御装置アドレス。この値は、ホスト出力構成プログラム (IOCP) の CNTLUNIT マクロ命令の CUADD ステートメントによって定義される。制御装置アドレスは、同じホスト上で定義された各論理区画ごとに固有でなければならない。



## D

**D ビット (D-bit).** 送達確認ビット (Delivery-confirmation bit)。X.25 通信において、受信側からのエンド・エンド確認 (送達確認) が必要な場合に 1 にセットされる、データ・パケットまたはコール・リクエスト・パケット内のビット。

**デーモン (daemon).** 標準サービスを行うために無人で実行されるプログラム。デーモンには、そのタスクを実行するために自動的に起動されるものと、定期的に動作するものがある。

**データ・キャリア検出 (DCD) (data carrier detect (DCD)).** 受信回線信号検出器 (RLSD) (received line signal detector (RLSD)) の同義語。

**データ回線 (data circuit).** (1) 両方向データ通信の手段を提供する、関連付けられた一対の送信チャネルと受信チャネル。(I) (2) SNA においては、リンク接続 (link connection) の同義語。(3) 物理回線 (physical circuit) およびバーチャル・サーキット (virtual circuit) も参照。

注:

1. データ交換装置相互間では、データ回線は、データ交換装置で使用するインターフェースのタイプによって、データ回線終端装置 (DCE) を含むことがある。
2. データ端末とデータ交換装置またはデータ集線装置との間では、データ回線は、データ装置側のデータ回線終端装置を含み、またデータ交換装置またはデータ集線装置側の DCE と類似の装置を含むことがある。

**データ回線終端装置 (DCE) (data circuit-terminating equipment (DCE)).** データ端末において、データ端末装置 (DTE) と回線の間で信号変換および符号化を行う装置。(I)

注:

1. DCE は、独立した機器であるか、DTE または中間装置に組み込まれている。
2. DCE は、伝送路のネットワーク側で一般的に必要とされる機能を果す。

**データ・リンク接続識別子 (DLCI) (data link connection identifier (DLCI)).** フレーム・リレー・サブポート、またはフレーム・リレー・ネットワークの PVC セグメントの数字識別子。1 つのフレーム・リレー・ポート内の各サブポートは、固有の DLCI を持っている。下表 (米国規格協会 (ANSI) 標準 T1.618 および国際電信電話諮問委員会 (ITU-T/CCITT) 標準 Q.922 から抜粋) は、特定の DLCI 値に関連する機能を示している。

DLCI 値	機能
0	チャネル内信号
1-15	未使用
16-991	フレーム・リレー接続手順を用いて割り当て
992-1007	フレーム・リレー・ベアラー・サービスのレイヤー 2 管理
1008-1022	未使用
1023	チャネル内のレイヤー管理

**データ・リンク制御 (DLC) (data link control (DLC)).** データ・リンク (SDLC リンクまたはトークンリングなど) 上のノードが、情報を正確に交換するために使用する規則。

**データ・リンク制御 (DLC) レイヤー (data link control (DLC) layer).** SNA において、2 つのノード間のリンクを介するデータ転送をスケジュールし、そのリンクの誤り制御を行うリンク・ステーションから構成されるレイヤー。データ・リンク制御の例としては、ビット順次リンク接続の SDLC や、システム/370 チャンネルのデータ・リンク制御がある。

注: 通常、DLC レイヤーは物理トランスポート機構から独立しており、上位レイヤーに送るデータの保全性が確保される。

**データ・リンク・レイヤー (data link layer).** 開放型システム間相互接続参照モデルにおいて、ネットワーク・レイヤー内のエンティティが通信リンクを通して相互にデータを転送するサービスを提供するレイヤー。データ・リンク・レイヤーは、物理レイヤーで発生した誤りを検出し、訂正する。(T)

**データ・リンク・レベル (data link level).** (1) データ・ステーションの階層構造において、ハイレベル論理とデータ・リンクの制御を維持するデータ・リンクとの間の、制御または処理論理の概念的レベル。データ・リンク・レベルは、送信ビットの挿入および受信ビットの削除、アドレス・フィールドおよび制御フィールドの解釈、コマンドとレスポンスの生成、送信、および解釈、フレーム・チェック・シーケンスの計算と解釈といった機能を実行する。パケット・レベル (packet level) および物理レベル (physical level) も参照。(2) X.25 通信において、フレーム・レベル (frame level) の同義語。

**データ・リンク交換 (DLSw) (data link switching (DLSw)).** IEEE 802.2 論理リンク制御 (LLC) タイプ 2 を使用する、ネットワーク・プロトコルの伝達方法。SNA および NetBIOS は、LLC タイプ 2 を使用する例である。カプセル化 (encapsulation) およびスプーフィング (spoofing) も参照。

**データ・パケット (data packet).** X.25 通信において、DTE/DCE インターフェースのパーチャル・サーキット上でユーザー・データを伝送するために使用されるパケット。

**データ・サービス装置 (DSU) (data service unit (DSU)).** データ端末装置にデジタル・データ・サービス・インターフェースを直接提供する装置。DSU は、ループ等化機能、リモートおよびローカル・テスト機能、および標準 EIA/CCITT インターフェース機構を提供する。

**データ・セット・レディー (DSR) (data set ready (DSR)).** DCE レディー (DCE ready) の同義語。

**データ交換機 (DSE) (data switching exchange (DSE)).** 1 つの場所に設置され、回線交換、メッセージ交換、およびパケット交換などの交換機能を提供する装置。(I)

**データ端末装置 (DTE) (data terminal equipment (DTE)).** データ・ステーションにおいて、データ送信側、データ受信側、またはその両方として動作する部分。(I) (A)

**データ端末レディー (DTR) (data terminal ready (DTR)).** EIA 232 プロトコルで使用されるモデムへの信号。

**データ転送速度 (data transfer rate).** データ伝送システムの通信している装置の間を単位時間に通過するビット、文字、またはブロックの数の平均値。(I)

注:

1. 速度は、秒、分、または時間当たりのビット数、文字数、またはブロック数で表す。
2. 通信する装置、たとえば、モデム、中間装置、または送信側と受信側を示す必要がある。

**データグラム (datagram).** (1) パケット交換において、発信データ端末装置 (DTE) から着信 DTE までのルーティングに必要な十分な情報を伝達し、前もって DTE とネットワーク・ノード間で情報交換をする必要がない、他のパケットから独立した自己完結型パケット。(I) (2) TCP/IP においては、インターネット環境で受け渡される情報の基本単位。データグラムには、データの他に発信元アドレスとあて先アドレスが入っている。インターネット・プロトコル (IP) データグラムは、IP ヘッダーと後続のトランスポート・レイヤー・データによって構成される。(3) パケット (packet) および セグメント (segment) も参照。

**データグラム送達プロトコル (DDP) (Datagram Delivery Protocol (DDP)).** AppleTalk ネットワーク・ノードにおいて、インターネット・レイヤーのコネクションレス・ソケット間送達サービスによってネットワークの接続性を提供するプロトコル。

**DCE レディー (DCE ready).** EIA 232 標準において、ローカル・データ回線終端装置 (DCE) が通信チャンネルに接続され、データ送信が可能になっていることを、データ端末装置 (DTE) に知らせる信号。データ・セット・レディー (DSR) (data set ready (DSR)) と同義。

**DECnet.** 通常は資源の共用、分散計算、またはリモート・システム構成の目的で、Digital Equipment Corporation のシステムを相互連結するのに使用される、一連のソフトウェア・モジュール、データベース、およびハードウェア・コンポーネント動作を定義するネットワーク体系。DECnet ネットワークの実現方式は、デジタル・ネットワーク体系 (DNA) モデルに準拠している。

**デフォルト (default).** 明示的に指定されていない場合に仮定される属性、状態、値、またはオプション。(I)

**従属 LU リクエスター (dependent LU requester (DLUR)).** APPN エンド・ノードまたは APPN ネットワーク・ノードで、従属 LU を所有するが、従属 LU サーバーがそれらの従属 LU に SSCP サービスを提供することを要求する。

**指定ルーター (designated router).** 他のルーターの存在とアイデンティティをエンド・ノードに知らせるルーター。指定ルーターの選択は、最高の優先順位をもつルーターに基づいて行われる。最高の優先順位をもつルーターが複数ある場合は、最高のステーション・アドレスをもつルーターが選択される。

**あて先ノード (destination node).** 要求またはデータの送信先のノード。

**あて先ポート (destination port).** 順次サービスを提供するコネクション・ポイントとして機能する 8 ポート非同期アダプター。

**あて先サービス・アクセス・ポイント (DSAP) (destination service access point (DSAP)).** SNA および TCP/IP において、システムがリモート装置からのデータを該当する通信サポートにルーティングするのに使用される論理アドレス。発信元サービス・アクセス・ポイント (SSAP) (source service access point (SSAP)) と対比。

**装置 (device).** 特定の目的をもつ機械的、電氣的、または電子的な仕組み。

**装置アドレス (device address).** 2216 装置を選択するためにチャンネル・バスで伝送される装置アドレス。S/370



入出力アーキテクチャーでは、サブチャネル番号とも呼ばれる。この値は、ホストIOCP 内の実装置に対する CNTLUNIT マクロ命令の UNITADD ステートメントによって定義される。

**デジタル (digital).** (1) 数字からなるデータを表わす用語。(T) (2) 数字の形をしたデータを表わす用語。(A) (3) アナログ (*analog*) と対比。

**デジタル・ネットワーク体系 (DNA) (Digital Network Architecture (DNA)).** すべての DECnet ハードウェアおよびソフトウェア実現モデル。

**直接メモリー・アクセス (DMA) (direct memory access (DMA)).** マイクロチャネル・バス上の装置が、システム処理装置を介さずに、システムまたはバス・メモリーに直接アクセスできるシステム機能。

**ディレクトリー (directory).** 識別子およびそれに対応するデータ項目への参照からなるテーブル。(I) (A)

**ディレクトリー・サービス (DS) (directory service (DS)).** アプリケーション・プロセスによって使用される記号名を、OSI 環境で使用される完全なネットワーク・アドレスに変換するアプリケーション・サービス要素。(T)

**ディレクトリー・サービス (DS) (directory services (DS)).** ネットワーク・リソースの場所に関する情報を維持する、APPN ノードのコントロール・ポイント・コンポーネント。

**使用不可 (disable).** 機能しないようにすること。

**使用不可の (disabled).** (1) 特定のタイプの割り込みの発生を防止する処理装置の状態を表わす用語。(2) 伝送制御装置または音声応答装置が線路上の着信コールを受け入れることができない状態を表わす用語。

**定義域、ドメイン (domain).** (1) データ処理資源が共通制御下に置かれているコンピューター・ネットワーク部分。(T) (2) 開放型システム間相互接続 (OSI) において、共通のポリシーが適用される、分散システムの部分または管理オブジェクトの集合。(3) 管理ドメイン (*Administrative Domain*) およびドメイン名 (*domain name*) を参照。

**ドメイン名 (domain name).** インターネット・プロトコルにおける、ホスト・システムの名前。ドメイン名は、区切り文字によって区切られた一連のサブネームから構成される。たとえば、ホスト・システムの完全修飾ドメイン名 (FQDN) が `ralvm7.vnet.ibm.com` である場合、以下がそれぞれドメイン名である。

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`

- `ibm.com`

**ドメイン名サーバー (domain name server).** インターネット・プロトコルにおいて、ドメイン名を IP アドレスにマップすることにより名前からアドレスへの変換を行うサーバー・プログラム。ネーム・サーバー (*name server*) と同義。

**ドメイン名システム (DNS) (Domain Name System (DNS)).** インターネット・プロトコルにおいて、ドメイン名を IP アドレスにマップするために使用される分散データベース・システム。

**ドット 10 進表記 (dotted decimal notation).** 基底を 10 とし、ピリオド (ドット) で相互を分離して書かれた、4 つの 8 ビット数字からなる 32 ビット整数の構文表記。IP アドレスを表すのに使用される。

**ダンプ (dump).** (1) ダンプしたデータ。(T) (2) 誤り情報を収集するために、バーチャル記憶装置のコンテンツの全部または一部をコピーすること。

**動的再構成 (DR) (dynamic reconfiguration (DR)).** 完全な構成テーブルを再生成したり、影響を受けるメジャー・ノードを停止せずに、ネットワーク構成 (周辺 PU および LU) を変更するプロセス。

**動的ルーティング (Dynamic Routing).** 初期化時に静的に構成されたルートではなく、動的に確認されたルートを使用するルーティング。

## E

**エコー (echo).** データ通信において、通信チャネル上の反射信号。たとえば、通信端末装置では各信号は 2 度表示される。ローカル端末に入ったときに一度表示され、通信リンクを経由して戻ってきたときに再度表示される。これにより、信号が正確であるかどうかを検査することができる。

**EIA 232.** データ通信において、順次 2 進データ交換を使用して、データ端末装置 (DTE) とデータ回線終端装置 (DTE) 間のインターフェースを定義する米国電子工業会 (EIA) の仕様。

**ELAN.** エミュレートされたローカル・エリア・ネットワーク (Emulated Local Area Network)。ATM 技術で実施された LAN セグメント。

**米国電子工業会 (EIA) (Electronic Industries Association (EIA)).** 業界の技術成長を促進し、各メンバーの意見を代表し、業界標準を開発するために組織された電子機器製造業者の団体。

**EIA 単位 (EIA unit).** 米国電子工業会で確立された測定単位で、44.45 mm (1.7 インチ) に等しい。

**カプセル化 (encapsulation).** (1) 通信において、階層化されたプロトコルによって使用される技法で、これを用いて各レイヤーはサポートするレイヤーからのプロトコル・データ単位 (PDU) に制御情報を追加する。この場合、このレイヤーは、サポートするレイヤーからのデータをカプセル化する。インターネット・プロトコルでは、たとえば、パケットには、物理レイヤーからの制御情報が入り、その後ネットワーク・レイヤーからの制御情報が続き、その後アプリケーション・プロトコル・データが入っている。(2) データ・リンク交換 (*data link switching*) も参照。

**コード化 (encode).** 元の形に再び変換できるような方法で、規則を使用してデータを変換すること。(T)

**エンド・ノード (EN) (end node (EN)).** (1) 拡張ピアツーピア・ネットワークング (*APPN*) エンド・ノード (*Advanced Peer-to-Peer Networking (APPN) end node*) およびローエントリー・ネットワークング (*LEN*) エンド・ノード (*low-entry networking (LEN) end node*) を参照。(2) 通信において、頻繁に 1 つのデータ・リンクに接続されるノードで、中間ルーティング機能を実行できないもの。

**入り口点 (EP) (entry point (EP)).** SNA において、分散ネットワーク管理サポートを提供する、タイプ 2.0、タイプ 2.1、タイプ 4、またはタイプ 5 ノード。それ自体に関するネットワーク管理データとそれが制御する資源を、集中処理のために中心拠点に送り、中心拠点が開始したコマンドを受け取って実行することによって、その資源を管理および制御する。

**等価容量 (equivalent capacity).** NBBS 体系において、パケット紛失率を限界値以下にするために、コネクシオンに必要な帯域幅の最少量。

**ESI.** エンド・システム識別子 (End System Identifier)。ATM アドレスの 6 バイトのコンポーネント。

**イーサネット(Ethernet).** 複数の端末が事前の調整なしに伝送媒体に自由にアクセスできる、10 Mbps のベースバンド・ローカル・エリア・ネットワーク。搬送波検知/延期を使用して競合を回避し、衝突検出/遅延再送を使用して競合を解決する。イーサネットは、搬送波検知多重アクセス/衝突検出 (CSMA/CD) を使用する。

**例外 (exception).** データ・セットまたはファイルの処理中に見付かった入出力誤りのような異常な状態。

**例外応答 (ER) (exception response (ER)).** SNA において、受信した要求が受付不能または処理不能の場合にのみ応答を戻すように受信側に指示する (つまり、否定応

答は戻すことができるが肯定応答は戻せない)、要求ヘッダーの「要求された応答形式」フィールドで指定されたプロトコル。固定応答 (*definite response*) および応答なし (*no response*) と対比。

**交換 ID (XID) (exchange identification (XID)).** 隣接ノード間でノードおよびリンクの特性を伝達するために使用される、基本リンク単位の 1 つのタイプ。XID は、リンク起動の前と起動中はリンクおよびノード特性の設定と交渉を行うためにリンク・ステーション間で交換され、またリンク起動後はそれらの特性の変更を通知する。

**明示ルート (ER) (explicit route (ER)).** SNA において、2 つのサブエリア・ノードを接続する 1 つまたは複数の伝送グループ。明示ルートは、発側サブエリア・アドレス、あて先サブエリア・アドレス、明示ルート番号、および逆明示ルート番号によって識別される。バーチャル・ルート (VR) (*virtual route (VR)*) と対比。

**探索フレーム (explorer frame).** 探索パケット (*explorer packet*) を参照。

**探索パケット (explorer packet).** LAN において、発信元ホストによって生成され、LAN のソース・ルーティング全体を探索して、ホストが利用可能なパスに関する情報を収集するパケット。

**外部ゲートウェイ (exterior gateway).** インターネット通信において、ある自律システム上の、別の自律システムと通信するゲートウェイ。内部ゲートウェイ (*interior gateway*) と対比。

**外部ゲートウェイ・プロトコル (EGP) (Exterior Gateway Protocol (EGP)).** インターネット・プロトコルにおいて、ドメインと自律システム間で使用され、ネットワーク到達可能性情報を公示および交換することができるプロトコル。ある自律システム内の IP ネットワーク・アドレスが、EGP に参加しているルーターによって、別の自律システムに公示される。EGP の例としては、ボーダー・ゲートウェイ・プロトコル (BGP) がある。内部ゲートウェイ・プロトコル (IGP) (*Interior Gateway Protocol (IGP)*) と対比。

## F

**ファックス (fax).** ファクシミリ機から受け取ったハードコピー。テレコピー (*telecopy*) と同義。

**ファイル転送プロトコル (FTP) (File Transfer Protocol (FTP)).** インターネット・プロトコルにおいて、TCP および Telnet サービスを使用して、計算機間またはホスト間で大量データ・ファイルを転送する、アプリケーション・レイヤー・プロトコル。

**フラッシュ・メモリー (flash memory).** プログラム式で、消去可能で、連続的な電力を必要としない、データ記憶装置。他のプログラム式、消去可能データ記憶装置と比べたフラッシュ・メモリーの主な長所は、回路ボードから取り外さずに再プログラムできることである。

**フロー制御 (flow control).** (1) SNA において、データ・トラフィックがネットワークのコンポーネント間を通過する速度を管理するプロセス。フロー制御の目的は、メッセージの流れを最適化してネットワーク輻輳 (ふくそう) を最小にすることである。つまり、受信側または中間ルーティング・ノードのバッファがオーバーフローせず、また受信側が追加メッセージ単位の到着を待つこともないようにする。(2) ペーシング (pacing) も参照。

**フラグメント (fragment).** 分割 (fragmentation) を参照。

**断片化 (fragmentation).** (1) 伝送する物理媒体の容量に合わせるために、データグラムをより小さい部分つまり断片に分割する処理。(2) 分割 (segmenting) も参照。

**フレーム (frame).** (1) ある特別な情報で構成されるデータ構造。特別な情報とは、いくつかのスロットで成り立ち、各スロット内の属性値を読むことにより適切な接続手順が決められる。(T) (2) IBM トークンリング・ネットワークなどのローカル・エリア・ネットワークにおける伝送単位。区切り文字、制御文字、情報、および検査文字が含まれる。(3) SDLC において、SDLC 手順を使用して伝送される、コマンド、レスポンス、およびすべての情報を運ぶ手段。

**フレーム・レベル (frame level).** データ・リンク・レベル (data link level) と同義。リンク・レベル (link level) を参照。

**フレーム・リレー (frame relay).** (1) ユーザーの装置と高速パケット・ネットワークの境界を記述したインターフェース標準。フレーム・リレー・システムでは、無効なフレームは廃棄される。回復はホップごとではなく、エンド・エンドで行われる。(2) サービス総合デジタル網 (ISDN) D チャネル標準から導出された技法。接続は高信頼性で、ネットワークの誤り検出と制御のオーバーヘッドはないものと想定している。

**フロントエンド・プロセッサ (front-end processor).** メインフレームの通信制御タスクを軽減する、IBM 3745 または 3174 のようなプロセッサ。

## G

**ゲートウェイ (gateway).** (1) ネットワーク体系が異なる 2 つのコンピューター・ネットワークを相互に接続する機能単位。ゲートウェイは、異なる体系をもつネットワークまたはシステムを接続する。ブリッジは、同一または

類似の体系をもつネットワークまたはシステムを接続する。(T) (2) IBM トークンリング・ネットワークにおいて、ローカル・エリア・ネットワークを、異なる論理リンク・プロトコルを使用する別のローカル・エリア・ネットワークまたはホストに接続する、装置と関連ソフトウェア。(3) TCP/IP においては、ルーター (router) の同義語。

**汎用データ・ストリーム (GDS) (general data stream (GDS)).** LU 6.2 セッション内の会話に使用されるデータ・ストリーム。

**汎用データ・ストリーム (GDS) 変数 (general data stream (GDS) variable).** 識別子と長さフィールドで始まり、アプリケーション・データ、ユーザー制御データ、または SNA 定義制御データのいずれかを持つ RU 副構造の 1 タイプ。

## H

**ヘッダー (header).** (1) ユーザー・データの前に置かれるシステムが定めた制御情報。(2) 1 つまたは複数のあて先フィールド、発信元ステーションの名前、入力シーケンス番号、メッセージのタイプを示す文字列、メッセージの優先順位レベルなどの制御情報が入っているメッセージの部分。

**ヒープ・メモリー (heap memory).** データ構造を動的に割り振るために使用される RAM の量。

**ハロー (Hello).** 協働する承認ルーターが最小遅延ルートを見付けるために使用するプロトコル。

**ハロー・メッセージ (hello message).** (1) ルーター相互間またはルーターとホスト間の到達可能性を設定し、テストするために定期的に送られるメッセージ。(2) インターネット・プロトコルにおいて、ハロー・プロトコルによって内部ゲートウェイ・プロトコル (IGP) として定義されるメッセージ。

**ヒューリスティック (heuristic).** 最終結果に向けての進展状況を評価することによって解答を見付けるといふ、問題解決の探索的方法を表わす用語。

**ハイレベル・データ・リンク制御 (HDLC) (high-level data link control (HDLC)).** データ通信において、HDLC 国際規格 ISO 3309 フレーム構造および ISO 4335 手順要素に準拠して、指定された一連のビットを使用してデータ・リンクを制御すること。

**高性能ルーティング (HPR) (high-performance routing (HPR)).** 特に高速リンクの使用時に、データ・ルーティングの効率と信頼性を高める、拡張ピアツーピア・ネットワークワーキング機能 (APPN) 体系の追加機能。



**ホップ (hop).** (1) APPN において、中間ノードを含まないルート部分。隣接ノード間を接続する 1 つの伝送グループだけで構成される。(2) ルーティング・レイヤーにおいては、ネットワークの 2 つのノード間の論理距離。

**ホップ・カウント (hop count).** (1) 2 点間の距離の尺度。(2) インターネット通信において、あて先までの線路でデータグラムが通過するルーターの数。(3) SNA において、あて先までのパスで通過するリンク数の尺度。

**ホスト (host).** インターネット・プロトコルにおいて、エンド・システムのこと。エンド・システムはどのワークステーションでも構わず、必ずしもメインフレームである必要はない。

**ホット・プラグ可能、常時交換可能 (hot pluggable).** 該当するコンポーネントに接続されていない、あるいは依存していない他のリソースの動作を妨害せずに、取り付けや取り外しを行うことができるハードウェア・コンポーネントを表す用語。

**ハブ (インテリジェント) (hub (intelligent)).** 異なるケーブルおよびプロトコルをもつ LAN に対してブリッジングおよびルーティング機能を提供する、IBM 8260 のような集線装置。

**ヒステリシス (hysteresis).** アラート条件がクリアされる前に、設定されたアラート限界値を超過して変化する必要がある温度の量。

## I

**I フレーム (I-frame).** 情報フレーム (Information frame)。

**IETF.** インターネット技術特別調査委員会 (Internet Engineering Task Force)。インターネット仕様を作成する機関。

**ILMI.** インターリム・ローカル管理インターフェース (Interim Local Management Interface)。ユーザー・ネットワーク・インターフェース (UNI) を管理するための SNMP ベースの手順。

**情報 (I) フレーム (information (I) frame).** 番号制情報転送に使用される I フォーマットのフレーム。

**入出力チャネル (input/output channel).** データ処理システムにおいて、内部機器と周辺機器の間のデータ転送を扱う装置。(I) (A)

**統合デジタル網交換機 (IDNX) (Integrated Digital Network Exchange (IDNX)).** 音声、データ、および画像アプリケーションを統合する処理装置。伝送資源の管

理や、マルチプレクサーおよびネットワーク管理支援システムへの接続も行う。異なるベンダーからの装置を統合することができる。

**サービス総合デジタル網 (ISDN) (integrated services digital network (ISDN)).** 音声やデータも含めた多数のサービスをサポートするデジタル・エンド・エンド通信ネットワーク。

**注:** ISDN は公衆網および私設網体系で使用される。

**インターフェース (interface).** (1) 機能特性、信号特性、またはその他の該当する特性によって定義された、2 つの機能単位間の共有された境界。この概念には、異なる機能をもつ 2 つの装置を接続するための仕様も含まれる。

(T) (2) システム、プログラム、または装置をつなぐハードウェア、ソフトウェア、またはその両方。

**内部ゲートウェイ (interior gateway).** インターネット通信において、専用の自律システムとのみ通信するゲートウェイ。外部ゲートウェイ (exterior gateway) と対比。

**内部ゲートウェイ・プロトコル (IGP) (Interior Gateway Protocol (IGP)).** インターネット・プロトコルにおいて、自律システム内部でネットワーク到達可能性およびルーティングに関する情報を伝送するのに使用されるプロトコル。IGP の例としては、ルーティング情報プロトコル (RIP) および最短パス最優先オープン (OSPF) がある。

**中間ノード (intermediate node).** 複数の分岐の終端にあるノード。(T)

**中間セッション・ルーティング (ISR) (intermediate session routing (ISR)).** そのノードを通過するが、エンドポイントは別の場所にあるすべてのセッションに対して、セッション・レベルのフロー制御と障害報告を提供する、APPN ネットワーク・ノード内のルーティング機能の 1 タイプ。

**国際標準化機構 (ISO) (International Organization for Standardization (ISO)).** 製品やサービスの国際的な交流を容易にするため、また知的、科学的、技術的、経済的活動の分野における相互協力を進めるための標準化を推進するために設立された国際的な組織。

**国際電気通信連合 (ITU) (International Telecommunication Union (ITU)).** 世界の周波数割り振りおよび無線規制を含めて、標準化された通信手順および実施要領を提供するために設立された米国の特殊通信機関。

**インターネット (internet).** 一組のルーターによって相互接続され、1つの大規模ネットワークとして機能することができるネットワークの集合体。インターネット (*Internet*) も参照。

**インターネット (Internet).** 世界中の大規模な国営バックボーン・ネットワークと、多数の地域や構内のネットワークから構成される、インターネット体系委員会 (IAB) によって管理されるインターネット。インターネットでは、1組のインターネット・プロトコルを使用する。

**インターネット・アドレス (Internet address).** IP アドレス (*IP address*) を参照。

**インターネット体系委員会 (IAB) (Internet Architecture Board (IAB)).** TCP/IP として知られるインターネット・プロトコルの開発を監督する技術団体。

**インターネット制御メッセージ・プロトコル (ICMP) (Internet Control Message Protocol (ICMP)).** インターネット・プロトコル (IP) レイヤーの誤りを処理し、メッセージを制御するために使用されるプロトコル。問題の報告と誤っているデータグラムあて先が、データグラムの発信元に戻される。ICMP は、インターネット・プロトコルの一部である。

**インターネット制御プロトコル (ICP) (Internet Control Protocol (ICP)).** 例外通知、メトリック通知、および PING サポートを提供するバーチャル・ネットワークング・システム (Virtual NEtworking System (VINES))。ルーティング更新プロトコル (*RTP*) (*RouTing update Protocol (RTP)*) も参照。

**インターネット技術特別調査委員会 (IETF) (Internet Engineering Task Force (IETF)).** インターネットの短期的な技術問題の解決を担当する、インターネット体系委員会 (IAB) の特別調査委員会。

**インターネットワーク・パケット交換機能 (IPX) (Internetwork Packet Exchange (IPX)).** (1) Novell のサーバー、または IPX を実装したワークステーションまたはルーターと、他のワークステーションを接続するために使用される、ネットワーク・プロトコル。IPX は、インターネット・プロトコル (IP) に類似しているが、異なるパケット・フォーマットおよび用語を採用している。(2) Xerox ネットワーク・システム (*XNS*) (*Xerox Network Systems (XNS)*)も参照。

**インターネット・プロトコル (IP) (Internet Protocol (IP)).** 1つのネットワークまたは相互接続ネットワークを通してデータをルーティングするコネクションレス・プロトコル。IP は、上位のプロトコル・レイヤーと物理ネットワークの間の中間層として働く。ただし、このプ

ロトコルは、誤り回復やフロー制御は行わず、また物理ネットワークの信頼性も保証しない。

**インターオペラビリティ (interoperability).** ユーザーが装置固有の特性をほとんど (または、まったく) 知らなくても、種々の機能単位間で通信したり、プログラムを実行したり、あるいはデータを転送できること。(T)

**エリア内ルーティング (intra-area routing).** インターネット通信において、エリア内部でデータをルーティングすること。

**逆アドレス解決プロトコル (InARP) (Inverse Address Resolution Protocol (InARP)).** インターネット・プロトコルにおいて、事前設定されたハードウェア・アドレスを使用してプロトコル・アドレスを見付けるために使用されるプロトコル。フレーム・リレー文脈において、データ・リンク・コネクション識別子 (DLCI) は、事前設定ハードウェア・アドレスと同義。

**IPPN.** 他のプロトコルが IP を通してデータをトランスポートする場合に使用するインターフェース。

**IP アドレス (IP address).** インターネット・プロトコル、標準 5、Request For Comments (RFC) 791 によって定義された 32 ビット・アドレス。通常は、ドット付き 10 進表記で示される。

**IP データグラム (IP datagram).** インターネット・プロトコルにおいて、インターネットを通して伝送される情報の基本単位。発信元とあて先先のアドレス、ユーザー・データ、および制御情報 (データグラムの長さ、ヘッダー・チェックサム、データグラムの分割が可能かどうか、あるいは分割されているかどうかを示すフラグなど) が入っている。

**IP ルーター (IP router).** ネットワーク上のトラフィックが流れるパスを決定する、IP インターネット内の装置。ルーティング・プロトコルを使用して、ネットワークに関する情報を収集し、データグラムを最終着側に転送する最善ルートを決める。データグラムは、IP あて先アドレスに基づいてルーティングされる。

**IPXWAN.** 広域ネットワーク (WAN) を介してインターネットワーク・パケット交換機能 (IPX) ルーティング情報を交換する前に、ルーター相互間で情報を交換するために使用される Novell プロトコル。

## J

**ジッター (jitter).** (1) デジタル信号の有意瞬間における、その理想位置からの短時間の非累積的な変動。(2) 伝送されたデジタル信号の好ましくない変動。(3) ネットワーク遅延の変動。

## L

**L2TP アクセス集線装置 (LAC) (L2TP Access Concentrator (LAC)).** PPP プロトコルと L2TP プロトコルの両方を扱うことができる 1 つまたは複数の公衆サービス電話網 (PSTN) 回線または ISDN 回線に接続される集線装置。装置には、L2TP が稼働するためのメディアをサポートする必要がある。L2TP はトラフィックを 1 つまたは複数の L2TP ネットワーク・サーバー (LNS) に渡す。L2TP は、PPP ネットワークによって搬送されたプロトコルをトンネルすることができる。

**L2TP ネットワーク・サーバー (LNS) (L2TP Network Server (LNS)).** LNS は PPP エンド・ステーションなど任意のプラットフォーム上で稼働する。LNS は L2TP プロトコルのサーバー側を扱う。L2TP は、L2TP トンネルを通じて到着する単一の媒体にだけ依存しているので、LNS は単一の LAN または WAN インターフェースだけをもつが、LAC によってサポートされる全範囲の PPP インターフェースのうちどのインターフェースから到着する呼び出しも着信する。これらには、非同期 ISDN、同期 ISDN、V.120、およびその他のタイプの接続が含まれる。

**LAN ブリッジ・サーバー (LBS) (LAN bridge server (LBS)).** IBM トークンリング・ネットワーク・ブリッジ・プログラムにおいて、2 つ以上のリング間で (ブリッジを介して) 転送されたフレームに関する統計情報を保持しているサーバー。LBS は、LAN 報告機構 (LRM) を通して、これらの統計を該当の LAN マネージャーに送信する。

**LAN エミュレーション (LE) (LAN Emulation (LE)).** ATM ネットワークの従来の LAN アプリケーションをサポートする ATM フォーラム標準。

**LAN エミュレーション・クライアント (LEC) (LAN Emulation Client (LEC)).** エミュレートされた LAN のユーザーを表す LAN エミュレーション・コンポーネント。

**LAN エミュレーション構成サーバー (LECS) (LAN Emulation Configuration Server (LECS)).** 構成データを中央に集めて広く配布する、LAN エミュレーション・サービス・コンポーネント。

**LAN エミュレーション・サーバー (LES) (LAN Emulation Server (LES)).** LAN あて先を ATM アドレスにする、LAN エミュレーション・サービス・コンポーネント。

**LAN ネットワーク管理プログラム (LNM) (LAN Network Manager (LNM)).** ユーザーが中央のワークステーションから LAN 資源を管理および監視できるようにする、IBM ライセンス・プログラム。

**LAN セグメント (LAN segment).** (1) 独立して動作することができるが、ブリッジによってネットワークの他の部分に接続されている LAN の部分 (たとえば、バスまたはリング)。(2) ブリッジのない環状ネットワークまたはバス・ネットワーク。

**レイヤー (layer).** (1) ネットワーク体系において、階層式に配列された一組のグループのうちの 1 つで、ネットワーク体系に一致するすべてのシステム間にまたがっている、概念的に完全なサービス・グループ。(T) (2) 開放型システム間相互接続参照モデルにおいて、7 つの概念的に完全な、階層式に配列されたサービス、機能、およびプロトコルのグループのうちの 1 つで、すべての開放型システム間にまたがっている。(T) (3) SNA において、他のグループの機能からは論理的に分離されている、関連する機能の集まり。あるレイヤーの機能の実現方式を変更しても、他のレイヤーの機能には影響を与えない。

**LE. LAN エミュレーション (LAN Emulation).** ATM ネットワークの従来の LAN アプリケーションをサポートする ATM フォーラム標準。

**LEC. LAN エミュレーション・クライアント (LAN Emulation Client).** エミュレートされた LAN のユーザーを表す LAN エミュレーション・コンポーネント。

**LECS. LAN エミュレーション構成サーバー (LAN Emulation Configuration Server).** 構成データを中央に集めて広く配布する、LAN エミュレーション・サービス・コンポーネント。

**LES. LAN エミュレーション・サーバー (LAN Emulation Server).** LAN あて先を ATM アドレスにする、LAN エミュレーション・サービス・コンポーネント。

**回線交換 (line switching).** サーキット交換 (circuit switching) の同義語。

**リンク (link).** リンク接続機構 (伝送媒体) と、2 つのリンク局 (リンク接続機構の両側に 1 つずつ) の組み合わせ。多地点構成またはトークンリング構成では、1 つのリンク接続を複数のリンクで共用できる。

**平衡型リンク・アクセス・プロトコル (LAPB) (link access protocol balanced (LAPB)).** リンク・レベルで X.25 ネットワークにアクセスするのに使用されるプロトコル。LAPB は、ポイント・ポイント通信に使用される全二重、非同期、対称プロトコルである。



**リンク・アドレス (Link Address).** ESCON チャンネル・アダプター付きの 2216 の場合は、次のように決められたポート番号である。つまり、通信パスに ESCD が 1 つある場合は、ホストに接続された ESCON ディレクター (ESCD) ポート番号。通信パスに ESCD が 2 つある場合は、動的接続で定義された ESCD のホスト側ポート番号。通信パスに ESCD がいない場合、この値は 'X'01' に設定する必要がある。

**リンク接続 (link-attached).** (1) データ・リンクによって制御装置に接続されている装置を表わす用語。(2) チャンネル接続 (*channel-attached*) と対比。(3) リモート (*remote*) と同義。

**リンク接続機構 (link connection).** (1) 1 つのリンク局と他の 1 つまたは複数のリンク局の間で両方向通信を提供する物理装置。たとえば、通信回線およびデータ回線終端装置 (DCE)。(2) SNA においては、データ回線 (*data circuit*) と同義。

**リンク・レベル (link level).** (1) 加入者の機械をネットワーク・ノードに接続する全二重リンクを通してネットワークとの間でデータを受け渡しするのに使用されるリンク・プロトコルを定義している X.25 勧告の部分。LAP および LAPB は、CCITT によって推奨されているリンク・アクセス・プロトコルである。(2) データ・リンク・レベル (*data link level*) も参照。

**リンク状態 (link-state).** ルーティング・プロトコルにおいて、ルーターまたはネットワークの使用可能なインターフェースおよび到達可能な近隣に関する、公示された情報。プロトコルのトポロジー・データベースは、収集されたリンク状態公示から作成される。

**リンク・ステーション (link station).** (1) 特定のリンクを介した隣接ノードへの接続を表す、ノード内のハードウェアおよびソフトウェア・コンポーネント。たとえば、ノード A が 3 つの隣接ノードに接続する多地点回線の 1 次エンドのとき、ノード A は隣接ノードへの接続を表す 3 つのリンク・ステーションをもつことになる。(2) 隣接リンク・ステーション (*ALS*) (*adjacent link station* (*ALS*)) も参照。

**LIS.** 論理 IP サブネット (Logical IP Subnet)。ATM 技術のスイッチド・バーチャル・ネットワークング (SVN) 構成で実現された IP サブネット。

**ローカル (local).** (1) 通信回線を使用しないで直接アクセスされる装置を表わす用語。(2) リモート (*remote*) と対比。(3) チャンネル接続 (*channel-attached*) の同義語。

**ローカル・エリア・ネットワーク (LAN) (local area network (LAN)).** (1) 地理的に限定された区域内にある、ユーザーの構内に置かれているコンピューター・ネット

ワーク。ローカル・エリア・ネットワーク内部の通信は、外部の規制の対象にはならないが、LAN の境界を越えた通信は、何らかの形で規制を受ける場合がある。(T) (2) 1 組の装置が相互通信を目的として接続されているネットワークで、さらに大きなネットワークに接続することができる。(3) イーサネット (*Ethernet*) およびトークンリング (*token ring*) も参照。(4) 大都市圏ネットワーク (*MAN*) (*metropolitan area network (MAN)*) および広域ネットワーク (*WAN*) (*wide area network (WAN)*) と対比。

**ローカル・ブリッジング (local bridging).** 通信リンクを使用せずに 1 つのブリッジが複数の LAN セグメントを接続することができるブリッジ・プログラムの機能。リモート・ブリッジング (*remote bridging*) と対比。

**ローカル管理インターフェース (LMI) (local management interface (LMI)).** ローカル管理インターフェース (*LMI*) プロトコル (*local management interface (LMI) protocol*) を参照。

**ローカル管理インターフェース (LMI) プロトコル (local management interface (LMI) protocol).** NCP において、DLCI 'X'00' を介して回線状況の情報を交換するために隣接フレーム・リレー・ノードが使用する、1 組のフレーム・リレー・ネットワーク管理手順とメッセージ。NCP は、米国規格協会 (ANSI) と国際電信電話諮問委員会 (ITU-T/CCITT) の両方のバージョンの LMI プロトコルをサポートする。これらの標準では、LMI プロトコルをリンク保全検査テスト (*LIVT*) (*link integrity verification tests (LIVT)*) として参照している。

**ローカル管理アドレス (locally administered address).** ローカル・エリア・ネットワークにおいて、出荷時設定アドレスを指定変更するためにユーザーが割り当てることができるアダプター・アドレス。出荷時設定アドレス (*universally administered address*) と対比。

**論理チャンネル (logical channel).** パケット交換モードの動作において、データ・リンクを介して同時にデータの送信と受信を行うために一緒に使用される、送信チャンネルと受信チャンネル。パケットの伝送をインターリーブすることにより、同じデータ・リンク上に複数の論理チャンネルを確立することができる。

**論理リンク (logical link).** 1 対のリンク・ステーション (2 つの隣接ノードのそれぞれに 1 つ) とその基礎になるリンク接続。2 つのノード間に 1 つのリンク・レイヤー接続機構を提供する。2 つのノードを接続する同一の物理媒体を共用しながら、複数の論理リンクを区別することができる。その例としては、ローカル・エリア・ネットワーク (LAN) ファシリティーで使用される 802.2 論理リンクと、2 つのノード間の同じポイント・ポイント物理リンクを使用する LAP E 論理リンクがある。論理リンク

という用語には、DTE から X.25 ネットワークへのアクセス・リンクを共用する複数の X.25 論理チャンネルも含まれる。

**論理リンク制御 (LLC) (logical link control (LLC)).** 情報を正確に交換するために、2 種類のデータ・リンク制御 (DLC) 動作を提供するデータ・リンク制御 (DLC) LAN サブレイヤー。最初のタイプはコネクションレス・サービスで、リンクを確立せずに情報を送受信することができる。コネクションレス・サービスの場合、LLC サブレイヤーは誤り回復またはフロー制御を行わない。2 番目のタイプはコネクション指向のサービスで、情報を交換する前にリンクを確立する必要がある。コネクション指向のサービスは、順序保存情報転送、フロー制御、および誤り回復を提供する。

**論理リンク制御 (LLC) プロトコル (logical link control (LLC) protocol).** ローカル・エリア・ネットワークにおいて、伝送媒体の共用方法からは独立して、データ・ステーション間の伝送フレームの交換を規定するプロトコル (T) LLC プロトコルは IEEE 802 委員会によって開発されたもので、すべての LAN 標準に共通である。

**論理リンク制御 (LLC) プロトコル・データ単位 (logical link control (LLC) protocol data unit).** 異なるノードのリンク・ステーション間で交換される情報の単位。LLC プロトコル・データ単位には、あて先サービス・アクセス・ポイント (DSAP)、発信元サービス・アクセス・ポイント (SSAP)、制御フィールド、およびユーザー・データが入っている。

**論理区画 (logical partition).** 論理区分 (LPAR) モードで動作できる、ホスト内の区画に割り当てられた番号。LPAR モードでは、ESCON アダプターは複数のホスト区画と論理ファイバー接続を共用することができる。

**論理区分 (LPAR) モード (Logically Partitioned (LPAR) mode).** 処理を論理区画 (LP) に分割して、複数のプロセッサがあるように見せる、一部のホスト・プロセッサの機能。LPAR モードでは、ESCON アダプターは複数のホスト区画と論理ファイバー接続を共用することができる。

**LP.** 論理区画 (logical partition)

**LP 番号 (LP number).** 論理区画番号 (Logical partition number)。これによって、複数の論理ホスト区画 (LP) が 1 つの ESCON ファイバーを共用することができる。この値は、ホスト入出力構成プログラム (IOCP) の RESOURCE マクロ命令によって定義される。ホストで EMIF を使用していない場合は、LP 番号としてデフォルト値 0 を使用する。

**LPAR.** 論理区分 (logically partitioned)。

**LPAR モード (LPAR mode).** 論理区分 (LPAR) モード。

**論理装置 (LU) (logical unit (LU)).** ユーザーがネットワーク・リソースにアクセスし、相互に通信することができる、ネットワーク・アクセス可能単位の一つ。

**ループバック・テスト (loopback test).** テスターからの信号をモデムや他のネットワーク要素でループさせてテスターに戻し、それを計測して通信パスの品質を調べたり、確認したりするテスト。

**ローエントリー・ネットワーキング (LEN) (low-entry networking (LEN)).** 論理装置間の複数の並列セッションをサポートするために、基本ピア間プロトコルを使用して相互に直接接続することができるノードの機能。

**ローエントリー・ネットワーキング (LEN) エンド・ノード (low-entry networking (LEN) end node).** 隣接 APPN ネットワーク・ノードからネットワーク・サービスを受ける LEN ノード。

**ローエントリー・ネットワーキング (LEN) ノード (low-entry networking (LEN) node).** 一連のエンド・ユーザー・サービスを行い、ピア・プロトコルを使用して他のノードと直接接続し、隣接 APPN ネットワーク・ノードから暗黙に (すなわち、CP-CP セッションを直接使用せずに) ネットワーク・サービスを受けるノード。

## M

**管理アクセス (management access).** ネットワーク管理ステーション、または変更制御サーバーを NBBS ネットワークに接続する Nways スイッチ。

**管理情報ベース (MIB) (Management Information Base (MIB)).** (1) ネットワーク管理プロトコルによってアクセスできるオブジェクトの集合。(2) ホストやゲートウェイから入手できる情報および許容される動作を指定する管理情報の定義。(3) OSI では、開放型システム内の管理情報の概念的リポジトリ。

**管理ステーション (management station).** インターネット通信において、ネットワーク全体 (または、一部) を管理するシステム。管理ステーションは、シンプル・ネットワーク・マネージメント・プロトコル (SNMP) のようなネットワーク管理プロトコルを使用して、被管理ノードに常駐するネットワーク管理エージェントと通信する。

**マッピング (mapping).** あるフォーマットで送信側から伝送されたデータを、受信側が受け入れられるデータ形式に変換するプロセス。



**マスク (mask).** (1) 他の文字パターンの一部を保持または削除することを制御するために使用する文字パターン。(I) (A) (2) 他の文字パターンの一部を保持または削除することを制御するために、文字パターンを使用すること。(I) (A)

**最大伝送単位 (MTU) (maximum transmission unit (MTU)).** LAN において、1 つのフレームに入れて所定の物理媒体で送信できる最大可能データ単位。たとえば、イーサネットの MTU は 1500 バイトである。

**媒体アクセス制御 (MAC) (medium access control (MAC)).** LAN において、媒体に依存する機能をサポートし、物理レイヤーのサービスを使用して論理リンク制御 (LLC) サブレイヤーにサービスを提供する、データ・リンク制御レイヤーのサブレイヤー。MAC サブレイヤーには、装置が伝送媒体にアクセスできる時期を判別する方法が含まれている。

**媒体アクセス制御 (MAC) プロトコル (medium access control (MAC) protocol).** ローカル・エリア・ネットワークにおいて、データ・ステーション間でデータを交換できるようにするために、ネットワークのトポロジを考慮に入れて、伝送媒体へのアクセスを規制するプロトコル。(T)

**媒体アクセス制御 (MAC) サブレイヤー (medium access control (MAC) sublayer).** ローカル・エリア・ネットワークにおいて、媒体アクセス方式に適用されるデータ・リンク・レイヤーの部分。MAC サブレイヤーは、トポロジー依存の機能をサポートし、物理レイヤーのサービスを使用して、論理リンク制御サブレイヤーにサービスを提供する。(T)

**メトリック (metric).** インターネット通信において、同じ自律システムへの複数の出入口ポイントを区別するために使用される、ルートに関連する値。最低のメトリックをもつルートが優先される。

**大都市圏ネットワーク (MAN) (metropolitan area network (MAN)).** 2 つ以上のネットワークを相互接続して形成された通信ネットワーク。個々のネットワークより高速で動作すること、行政の境界にまたがること、および複数のアクセス方式を使用することが可能になる。(T) ローカル・エリア・ネットワーク (*local area network (LAN)*) および広域ネットワーク (*wide area network (WAN)*) と対比。

**MIB.** (1) MIB モジュール。(2) 管理情報ベース (Management Information Base)。

**MIB オブジェクト (MIB object).** MIB 変数 (*MIB variable*) の同義語。

**MIB 変数 (MIB variable).** シンプル・ネットワーク・マネジメント・プロトコル (SNMP) において、MIB モジュールに定義されているデータの特定インスタンス。MIB オブジェクト (*MIB object*) と同義。

**MIB ビュー (MIB view).** シンプル・ネットワーク・マネジメント・プロトコル (SNMP) において、特定のコミュニティに見える、エージェントと呼ばれる管理オブジェクトの集合。

**MILNET.** 本来は ARPANET の一部であった軍用ネットワーク。1984 年に ARPANET から分割された。MILNET は、軍用施設に高信頼性のネットワーク・サービスを提供している。

**モデム (変復調装置) (modem (modulator/demodulator)).** (1) 信号を変調および復調する装置。モデムの機能の 1 つは、デジタル・データをアナログ伝送ファシリティを介して伝送できるようにすることである。(T) (A) (2) コンピュータからのデジタル・データを、通信回線上で伝送できるアナログ信号に変換し、また受信したアナログ信号をコンピュータのためのデータに変換する装置。

**モジュール (module).** Nways スイッチにおいて、論理カード、コネクタ、およびライトが含まれている、パッケージされたハードウェア装置。モジュールは、アダプター、回線インターフェース・カプラー、音声サーバー拡張、およびその他のコンポーネントをパッケージするのに使用される。すべてのモジュールが論理サブラックにホット・プラグ可能。

**モジュロ (modulo).** (1) モジュラスに関する用語。たとえば、9 は 4 モジュロ 5 と同等。(2) モジュラス (*modulus*) も参照。

**モジュラス (modulus).** 剰余を残さずに 2 つの関連する数値の差を除算する関係式における、正整数のような数。たとえば、9 と 4 はモジュラス 5 をもつ ( $9 - 4 = 5$ 、 $4 - 9 = -5$ 、かつ 5 は 5 と  $-5$  の両方とも割りきれぬ)。

**モニター (monitor).** (1) 分析するために、データ処理システムの中の選ばれた活動を監視し、記録する機能。基準から著しく逸脱していることを示すため、または特定の機能の利用度を測るために使用する。(T) (2) システムの操作を観察、監視、制御、検査するソフトウェアまたはハードウェア。(A) (3) リング上のトークンの伝送を開始し、トークンの紛失、フレームの循環、またはその他の問題が生じた場合にソフト誤り回復を提供するために必要な機能。この機能は、すべてのリング・ステーションに存在する。

**MSS.** マルチプロトコル交換サービス (Multiprotocol Switched Services)。IBM のスイッチド・バーチャル・ネットワークング (SVN) 構成のコンポーネント。

**マルチキャスト (multicast).** (1) 選択されたあて先グループに同じデータを伝送すること。(T) (2) パケットのコピーが可能ならすべてのあて先のサブセットだけに伝達される、特殊な形式の同報通信。

**マルチパス・チャネル (multipath channel) (MPC).** VTAM-VTAM 間両方向通信用として複数の単方向サブチャネルを使用するチャネル・プロトコル。

**マルチドメイン・サポート (MDS) (multiple-domain support (MDS)).** LU-LU および CP-CP セッションを介して管理サービス機能セット相互間で管理サービス・データを伝達する手法。マルチドメイン・サポート・メッセージ単位 (MDS-MU) (multiple-domain support message unit (MDS-MU)) も参照。

**マルチドメイン・サポート・メッセージ単位 (MDS-MU) (multiple-domain support message unit (MDS-MU)).** 管理サービス・データが入っているメッセージ単位で、マルチドメイン・サポートによって使用される LU-LU および CP-CP セッションを介して管理サービス機能セット相互間に流される。このメッセージ単位およびその中に入っている実際の管理サービス・データは、一般データ・ストリーム (GDS) 形式である。コントロール・ポイント管理サービス単位 (CP-MSU) (control point management services unit (CP-MSU))、管理サービス単位 (MSU) (management services unit (MSU))、およびネットワーク管理ベクトル伝達 (NMVT) (network management vector transport (NMVT)) も参照。

## N

**ネーム・バインディング・プロトコル (NBP) (Name Binding Protocol (NBP)).** AppleTalk ネットワークにおいて、AppleTalk エンティティ (資源) 名 (文字列) からトランスポート・レイヤーの AppleTalk IP アドレス (16 ビットの数字) へのネーム変換機能を提供するプロトコル。

**ネーム・レゾリューション (name resolution).** インターネット通信において、機械名を対応するインターネット・プロトコル (IP) アドレスにマップする処理。ドメイン名システム (DNS) (Domain Name System (DNS)) も参照。

**ネーム・サーバー (name server).** インターネット・プロトコルにおいて、ドメイン名サーバー (domain name server) の同義語。

**最近隣活動アップストリーム (NAUN) (nearest active upstream neighbor (NAUN)).** IBM トークンリング・ネットワークにおいて、リング上の所定のステーションにデータを直接送信するステーション。

**近隣 (neighbor).** ネットワーク管理者によってルーティング情報を受信するように指定された、共通サブネットワーク上のルーター。

**NetBIOS.** ネットワーク基本入出力システム (Network Basic Input/Output System)。メッセージ、プリンター・サーバー、およびファイル・サーバーの機能を提供するために LAN 上で使用される、ネットワーク、IBM パーソナル・コンピューター (PC)、および互換 PC への標準インターフェース。NetBIOS を使用するアプリケーション・プログラムは、LAN データ・リンク制御 (DLC) プロトコルの詳細を処理する必要がない。

**網、ネットワーク (network).** (1) 情報交換のために接続されたデータ処理装置とソフトウェアの構成。(2) ノードとそれを相互接続するリンクの集合。

**ネットワーク・アクセス・サーバー (Network Access Server) (NAS).** ユーザーに一時的なオンデマンド・ネットワーク・アクセスを提供する装置。このアクセスは、PSTN または ISDN 伝送路を使用するポイント・ポイントです。

**ネットワーク・アクセス可能単位 (NAU) (network accessible unit (NAU)).** 論理装置 (LU)、物理装置 (PU)、コントロール・ポイント (CP)、またはシステム・サービス・コントロール・ポイント (SSCP)。パス制御ネットワークによって伝送される情報の発側または着側となる。ネットワーク・アドレス可能単位 (network addressable unit) と同義。

**ネットワーク・アドレス (network address).** ISO 7498-3 によると、1 組のネットワーク・サービス・アクセス・ポイントを識別する、OSI 環境内であいまいさのない名前。

**ネットワーク・アドレス可能単位 (NAU) (network addressable unit (NAU)).** ネットワーク・アクセス可能単位 (network accessible unit) の同義語。

**ネットワーク体系 (network architecture).** コンピューター・ネットワークの論理構造と運用原則。(T)

**注:** 運用原則には、サービス、機能、およびプロトコルが含まれる。

**ネットワーク輻輳 (ふくそう) (network congestion).** 通信量がネットワークで処理できる量を上回ったことによって起こる望ましくない過負荷状態。

**ネットワーク制御 (network control).** 以下の目的のために Nways スイッチのコントロール・ポイントによって実行される NBBS 体系の機能。

- Nways スイッチ資源の割り振りと制御
- トポロジーおよびディレクトリー・サービスの提供
- ルートの選択
- 輻輳 (ふくそう) の制御

**ネットワーク識別子 (network identifier).** (1) TCP/IP において、ネットワークを定義する IP アドレスの部分。ネットワーク ID の長さは、ネットワーク・クラス (A、B、または C) のタイプによって異なる。(2) 特定のサブネットワークを固有に識別する、1~8 バイトのユーザーが選択した名前、または 8 バイトの IBM 登録名。

**ネットワーク情報センター(NIC) (Network Information Center (NIC)).** インターネット通信において、ユーザーに援助、資料、訓練、およびその他のサービスを提供する、全世界の局所的、地域的、および国家的なグループ。

**ネットワーク・レイヤー (network layer).** 開放型システム間相互接続 (OSI) 体系において、OSI 環境全体のルーティング、交換、およびリンク・レイヤー・アクセス機能を提供するレイヤー。

**ネットワーク管理 (network management).** 通信用のデータ処理または情報システムを計画、組織、および制御するプロセス。

**ネットワーク管理ステーション (NMS) (network management station (NMS)).** NetView/AIX および Nways スイッチ管理プログラムを稼働するステーション。NBBS ネットワーク・トポロジー、会計、効率、構成の更新、および問題分析を管理する。

ネットワーク管理ステーションは、イーサネット LAN を介して管理アクセス Nways スイッチに接続される。

**ネットワーク管理ステーション (network management station).** シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、ネットワーク要素を監視、制御する管理アプリケーション・プログラムを実行する端末。

**ネットワーク管理ベクトル転送 (NMVT) (network management vector transport (NMVT)).** 物理装置管理サービスとコントロール・ポイント管理サービス間のアクティブ・セッション (SSCP-PU セッション) を介して流される、管理サービス要求応答単位 (RU)。

**ネットワーク・マネージャー (network manager).** ネットワーク・ノードの問題を監視、管理、および診断するプログラムまたはプログラムの集まり。

**ネットワーク・ノード (NN) (network node (NN)).** 拡張ピアツー・ピア・ネットワーキング機能 (APPN) ネットワーク・ノード (Advanced Peer-to-Peer Networking (APPN) network node) を参照。

**ネクスト・ホップ解決プロトコル (NHRP) (Next Hop Resolution Protocol (NHRP)).** RFC としての認定を受けるために提出されている、インターネット草案バージョン 10 に指定されているルーティング・プロトコル。ネクスト・ホップ解決プロトコルでは、発信元ステーションが、あて先の方向にある『NBMA ネクスト・ホップ』の非同報通信マルチアクセス (NBMA) アドレスを判別する方式を定義する。NBMA ネクスト・ホップは、あて先自体である場合もあれば、NBMA ネットワーク内にあって、あて先に『最も近い』ルーターである場合もある。こうして、発信元ステーションは、あて先またはルーターとの間に直接 NBMA バーチャル・サーキットを確立し、NBMA ネットワーク上のルーティング・ホップの数を減らすことができる。

**ネットワーク・サポート・センター (Network Support Center).** IBM が NBBS ネットワークにリモート・サポートを提供する場所。

**ネットワーク・サポート・ステーション (network support station).** ローカルで動作し、Nways スイッチにサービスするために使用される処理装置。Nways スイッチの管理者または保守担当者が使用する。

**ネットワーク・ユーザー・アドレス (NUA) (network user address (NUA)).** X.25 通信において、最大 15 桁の 2 進コード数字を含む X.121 アドレス。

**ネットワーキング広帯域サービス (NBBS) (Networking BroadBand Services (NBBS)).** ATM 標準を補完して以下の機能を提供する、高速ネットワーキング用の IBM 体系。

- アクセス・サービス
- トランスポート・サービス
- ネットワーク制御

**NHRP.** ネクスト・ホップ解決プロトコル (Next Hop Resolution Protocol)。

**ノード (node).** (1) ネットワーク・ノードにおいて、1 台または複数の装置がチャネルまたはデータ回線を接続する点。(2) ネットワークに接続された、データを送受信する装置。

**非標準アドレス (noncanonical address).** LAN において、トークンリング・アダプターの媒体アクセス制御 (MAC) アドレスを伝送するためのフォーマットの 1 つ。非標準フォーマットでは、各アドレス・バイトの最上位



(左端) ビットが最初に伝送される。標準アドレス (*canonical address*) と対比。

**非ゼロ復帰 (1) 記録 (NRZ-1) (Non-Return-to-Zero Changes-on-Ones Recording (NRZ-1))**. 磁化状態の変化が 1 を表し、変化しないことが 0 を表す記録方式。1 の信号のみが明示的に記録される。(以前は**非ゼロ復帰反転 (NRZI)** 記録と呼ばれていた。)

**非シード・ルーター (nonseed router)**. AppleTalk ネットワークにおいて、同じネットワークに接続されているシード・ルーターからネットワーク番号範囲とゾーン・リスト情報を獲得するルーター。

**Nways スイッチ (Nways Switch)**. IBM 2220 Nways ブロードバンド・スイッチ (IBM 2220 Nways BroadBand Switch) と同義。

**Nways スイッチ構成端末 (Nways Switch configuration station)**. Nways Switch 構成ツール (NCT) の独立バージョンを稼働している専用 OS/2 端末。ネットワーク構成データベースを生成するのに使用され、リモート・コンソールに導入する必要がある。

## O

**最短パス最優先オープン (OSPF) (Open Shortest Path First (OSPF))**. インターネット・プロトコルにおいて、領域ドメイン内の情報転送を行う機能。ルーティング情報プロトコル (RIP) の代替として、OSPF は最低コストのルーティングが可能であり、大きい地域や企業ネットワークのルーティングを扱う。

**開放型システム間相互接続 (OSI) (Open Systems Interconnection (OSI))**. (1) 情報交換のための国際標準化機構 (ISO) の標準に準拠した開放型システムの相互接続。(T) (A) (2) データ処理システムの相互接続を可能にする標準的手順の使用。

注: OSI 体系は、コンピューター・システムの相互接続のための現在および将来の標準の開発を統合するための枠組みを設定している。ネットワーク機能は 7 つのレイヤーに分けられている。各レイヤーは、異なるアプリケーションをサポートする標準的方法で実行できる、関連したデータ処理および通信機能の集まりを表している。

**開放型システム間相互接続 (OSI) 体系 (Open Systems Interconnection (OSI) architecture)**. 開放型システム相互接続に関連する特定の一組の ISO 規格に準拠したネットワーク体系。(T)

**開放型システム間相互接続 (OSI) 参照モデル (Open Systems Interconnection (OSI))**. 開放型システム相互接続、およびその 7 つのレイヤーの目的と階層式配列の一般原則を記述したモデル。(T)

**発信元 (origin)**. メッセージまたはその他のデータが発信された外部論理装置 (LU) またはアプリケーション・プログラム。あて先 (*destination*) も参照。

**孤立回線 (orphan circuit)**. その利用可能性が動的に学習される未構成の回線。

## P

**ペーシング (pacing)**. (1) オーバーランまたは輻輳 (ふくそう) を防止するために、受信側コンポーネントが送信側コンポーネントの伝送速度を制御する方法。(2) フロー制御 (*flow control*)、受信ペーシング (*receive pacing*)、送信ペーシング (*send pacing*)、セッション・レベル・ペーシング (*session-level pacing*)、およびバーチャル・ルート (VR) ペーシング (*virtual route (VR) pacing*) も参照。

**パケット (packet)**. データ通信において、1 つのまとまりとして送信および交換される、データと制御信号を含む 2 進数の列。データ、制御信号、および誤り制御情報が、特定の形式に配列されている。(I)

**パケット・インターネット・グローパー (PING) (packet internet groper (PING))**. (1) インターネット通信において、インターネット制御メッセージ・プロトコル (ICMP) エコー要求をあて先に送って応答を待つことにより、あて先に到達できるかどうかをテストする、TCP/IP ネットワーク・ノードで使用されるプログラム。(2) 通信における、到達可能性のテスト。

**パケット損失率 (packet loss ratio)**. パケットが指定のあて先に到達しない、または指定された時間内に到達しない確率。

**パケット・モード動作 (packet mode operation)**. パケット交換 (*packet switching*) の同義語。

**パケット交換 (packet switching)**. (1) アドレス指定されたパケットを用いてデータのルーティングと転送を行うことによって、パケットの伝送中だけチャネルが占有されるようにする処理。伝送が完了すると、そのチャネルは他のパケットの伝送に利用可能になる。(I) (2) パケット・モード動作 (*packet mode operation*) と同義。回線交換 (*circuit switching*) も参照。

**並列ブリッジ (parallel bridges)**. 同じ LAN セグメントに接続され、そのセグメントへの冗長パスを形成する 1 対のブリッジ。

**並列伝送グループ (parallel transmission groups).** 各グループが異なるグループ番号をもつ、隣接ノード間の複数の伝送グループ。

**パス (path).** (1) 通信ネットワークにおける 2 つのノード間のルート。パスは複数の分岐を含むことができる。

(T) (2) 2 つのネットワーク・アクセス可能装置間で交換される情報が通る、一連の伝送ネットワーク・コンポーネント (パス制御およびデータ・リンク制御)。明示ルート (*ER*) (*explicit route (ER)*)、ルート拡張 (*route extension*)、およびバーチャル・ルート (*VR*) (*virtual route (VR)*) も参照。

**パス制御 (PC) (path control (PC)).** 通信ネットワークのネットワーク・アクセス可能装置間でメッセージをルーティングし、相互間のパスを提供する機能。伝送制御からの基本情報単位 (BIU) を (場合によっては分割して) パス情報単位 (PIU) に変換し、1 つまたは複数の PIU を含む基本伝送単位をデータ・リンク制御と交換する。パス制御はノード・タイプによって異なる。あるノード (たとえば、APPN ノード) は、ローカルに生成されたセッション識別子をルーティングに使用し、あるノード (サブエリア・ノード) は、ネットワーク・アドレスをルーティングに使用する。

**パス・コスト (path cost).** リンク状態ルーティング・プロトコルにおいて、2 つのノードまたはネットワーク・ノード間のパス上のリンク・コストの合計。

**パス情報単位 (PIU) (path information unit (PIU)).** 伝送ヘッダー (TH) のみから成る、または TH の後に基本情報単位 (BIU) または BIU セグメントが続いているメッセージ単位。

**パターン突き合わせ文字 (pattern-matching character).** 1 文字または複数の文字を表すために使用できる、アスタリスク (\*) や疑問符 (?) のような特殊文字。任意の 1 文字または一組の文字を、パターン突き合わせ文字と置き換えることができる。グローバル文字 (*global character*) およびワイルドカード文字 (*wildcard character*) と同義。

**パーマネント・バーチャル・サーキット (PVC) (permanent virtual circuit (PVC)).** X.25 およびフレーム・リレー通信で、各データ端末装置 (DTE) に論理チャネルが固定的に割り当てられているバーチャル・サーキット。コール設定プロトコルは不要である。スイッチド・バーチャル・サーキット (*SVC*) (*switched virtual circuit (SVC)*) と対比。

**物理回線 (physical circuit).** 多重化なしで確立されている回路。データ回線 (*data circuit*) も参照。バーチャル・サーキット (*virtual circuit*) と対比。

**物理レイヤー (physical layer).** 開放型システム間相互接続参照モデルにおいて、伝送媒体を介して物理接続を確立、維持、および解放するための機械的、電気的、機能的、および手順的な手段を提供するレイヤー。(T)

**物理装置 (PU) (physical unit (PU)).** (1) SSCP-PU セッションを介した SSCP の要求に応じて、ノードに関連する資源 (接続リンクや隣接リンク・ステーションなど) を管理および監視するコンポーネント。SSCP は、接続リンクのようなノードの資源を PU を介して間接的に管理するために、物理装置をもつセッションを起動する。この用語は、タイプ 2.0、タイプ 4、およびタイプ 5 ノードにのみ適用される。(2) 周辺 PU (*peripheral PU*) およびサブエリア PU (*subarea PU*) も参照。

**PING コマンド (ping command).** インターネット制御メッセージ・プロトコル (ICMP) エコー要求パケットをゲートウェイ、ルーター、またはホストに送信し、その応答を待つコマンド。

**ポイント・ポイント・プロトコル (PPP) (Point-to-Point Protocol (PPP)).** パケットをカプセル化し、シリアル・ポイント・ポイント・リンクを介して伝送する方法を提供するプロトコル。

**ポーリング (polling).** (1) 多地点接続またはポイント・ポイント接続において、データ・ステーションに対して一度に 1 台ずつ送信するように促す処理。(I) (2) 競合を避けるため、動作状況を調べるため、またはデータの送信または受信が可能かどうかを調べるための、装置に対する問い合わせ。(A)

**ポート (port).** (1) データを入出力するためのアクセス・ポイント。(2) 他の装置 (ディスプレイ、プリンターなど) のケーブルが接続される装置上のコネクタ。(3) リンク・ハードウェアへの物理接続の表現。ポートはアダプターと呼ばれることもあるが、アダプターは 2 つ以上のポートをもつことができる。単一の DLC プロセスで、1 つまたは複数のポートを制御することができる。(4) インターネット・プロトコルにおいて、TCP またはユーザー・データグラム・プロトコル (UDP) と、上位レベルのプロトコルまたはアプリケーションの間の通信に使用される 16 ビットの番号。ファイル転送プロトコル (FTP) やシンプル・メール転送プロトコル (SMTP) など一部のプロトコルでは、すべての TCP/IP 実装に同一の割り当て済みポート番号が使用される。(5) ホスト計算機内の複数のあて先を区別するために、トランスポート・プロトコルが使用する抽象概念。(6) ソケット (*socket*) と同義。

**ポート・アダプター (port adapter).** ポート回線に NBBS 体系のアクセス・サービスを提供するコードを実行している、Nways スイッチの 2216 以外の型式のモジュール。2216 では、ポート・アダプターとトランク・アダ

プター機能が結合された多重化ポート/トランク・アダプター (MPTA) が使用されている。

**ポート回線 (port line).** 外部ユーザー装置を Nways スイッチに接続し、それにより NBBS ネットワークへの接続を可能にする通信回線。回線エミュレーション・サービス (CES)、パルス符号変調 (PCM)、ハイレベル・データ・リンク制御 (HDLC)、またはフレーム・リレー (FR) など、各種のアクセス・サービスおよびインターフェースを使用できる。

Nways スイッチでは、各ポート回線は 1 つの (または、複数の) NBBS ポートに関連付けられている。

**ポート番号 (port number).** インターネット通信において、トランスポート・サービスに対してアプリケーション・エンティティーを識別するもの。

**ポテンシャル接続 (potential connection).** NBBS 体系において、NBBS ネットワークの外部の 2 つの装置間の事前定義された接続。エンドポイント Nways スイッチの 1 つに保管されている構成パラメーターによって定義される。

**構内交換機 (PBX) (private branch exchange (PBX)).** 公衆電話網と相互に呼を伝送する構内電話交換機。

**問題判別 (problem determination).** プログラムのコンポーネント、機械の障害、通信設備、ユーザー所有または外注のプログラムや機器、停電などの環境障害、あるいはユーザーの誤りなど、問題の原因を判別するプロセス。

**プログラム一時修正 (PTF) (program temporary fix (PTF)).** プログラムの未変更の現行リリースに含まれる、IBM によって診断された問題の一時的な解決策または迂回策。

**プロトコル (protocol).** (1) 機能単位が通信する方法を規定する、意味上および構文上の一組の規則。(I) (2) 開放型システム間相互接続体系において、同じレイヤー内のエンティティーが通信機能を実行する方法を規定する、1 組の意味上および構文上の規則。(T) (3) SNA において、ネットワーク管理、データ伝送、およびネットワーク・コンポーネントの状態の同期化を行うために使用する要求とレスポンスの意味と順序の規則。**回線制御規則 (line control discipline)** および**伝送制御手順 (line discipline)** と同義。**ブラケット・プロトコル (bracket protocol)** および**リンク・プロトコル (link protocol)** を参照。

**プロトコル・データ単位 (PDU) (protocol data unit (PDU)).** 特定のレイヤーのプロトコルに指定されており、このレイヤーのプロトコル制御情報 (および、このレ

イヤーのユーザー・データが含まれる場合もある) から構成されるデータの単位。(T)

**パルス符号変調 (PCM) (pulse code modulation (PCM)).** アナログ音声信号のデジタル化のために採用された標準。PCM では、音声は 8 kHz の速度でサンプリングされ、各サンプルは 8 ビット・フレームに符号化される。

NBBS ネットワークでは、PCM は音声および FAX データを運ぶための回線エミュレーション・サービス (CES) の代替である。

## Q

**サービス品質 (QOS) (quality of service (QoS)).** NBBS 体系では、サービス品質でネットワーク接続の特性を保証する。これは、エンド・エンド遅延、ジッター、およびパケット紛失率などを表わす。

**サービス品質 (QoS) (Quality of Service (QoS)).** 性能パラメーターを使用してアクセスされる、エンド・エンド・サービスのユーザー指向の性能。ATM ネットワークでは、セル損失比率、セル伝送遅延、およびセル遅延変動といった性能パラメーターによって、エンド・エンド ATM 接続の QoS が決まる。

## R

**高速トランスポート・プロトコル (RTP) コネクション (Rapid Transport Protocol (RTP) connection).** 高性能ルーティング (HPR) において、セッション・トラフィックを伝達するためにルートのエンドポイント間に確立される接続。

**到達可能性 (reachability).** ノードまたは資源が、別のノードまたは資源と通信できること。

**読み取り専用メモリー (ROM) (read-only memory (ROM)).** 特殊な条件下を除いて、保管されたデータをユーザーが変更できないメモリー。

**リアルタイム処理 (real-time processing).** 処理操作中に、ある処理が必要とするデータまたは生成するデータを処理すること。通常はその結果が、実行中の処理 (および、おそらく関連の処理にも) 使用され、それに影響を与える。

**再組み立て (reassemble).** 通信において、分割されたパケットを受信後に相互に結合して元に戻すプロセス。



**受信不可 (RNR) (receive not ready (RNR)).** 通信において、着信フレームを受け入れることができないという一時的な状態を示す、データ・リンク・コマンドまたはレスポンス。

**受信不可 (RNR) パケット (receive not ready (RNR) packet).** RNR パケット (*RNR packet*) を参照。

**受信回線信号検出器 (RLSD) (received line signal detector (RLSD)).** EIA 232 標準において、リモート・データ回線終端装置 (DCE) からの信号を受信中であることをデータ端末装置 (DTE) に示す信号。キャリア検出 (*carrier detect*) およびデータ・キャリア検出 (*DCD*) (*data carrier detect (DCD)*) と同義。

**認定私企業 (RPOA) (Recognized Private Operating Agency (RPOA)).** 電気通信サービスを提供し、国際電信電話諮問委員会の定める義務と規則に従う、政府省庁や機関以外の個人、会社、または組織。たとえば、通信事業者。

**縮小命令セット・コンピューター (RISC) (reduced instruction-set computer (RISC)).** 実行速度を上げるために、少数の単純化された頻繁に使用される命令セットを使用するコンピューター。

**リモート (remote).** (1) 通信回線を介してアクセスされるシステム、プログラム、または装置を表わす。(2) リンク接続 (*link-attached*) と同義。(3) ローカル (*local*) と対比。

**リモート・ブリッジング (remote bridging).** 2 つのブリッジが通信リンクを使用して複数の LAN を接続することができる、ブリッジの機能。ローカル・ブリッジング (*local bridging*) と対比。

**リモート・コンソール (remote console).** OS/2、TCP/IP、およびリモート Nways スイッチ資源制御プログラムを実行しているステーション。任意のネットワーク・サポート・ステーションに接続し、リモートから Nways スイッチの操作と保守を行うことができる。

接続は、以下を介して行う。

- モデムを使用して交換回線を介して
- NBBS ネットワークを介して (リモート・コンソールが、イーサネット LAN を通じてそのアクセス Nways スイッチに接続されている場合)

任意のネットワーク・サポート・ステーションを、別のネットワーク・サポート・ステーションのリモート・コンソールとして使用することができる。

**リモート実行プロトコル (REXEC) (Remote Execution Protocol (REXEC)).** ネットワーク・ノード内の任意のホストからコマンドまたはプログラムを実行することができるプロトコル。ローカル・ホストは、コマンドの実行結果を受け取る。

**コメント要求 (RFC)(Request for Comments (RFC)).** インターネット通信において、インターネット・プロトコルの一部とそれに関連する実験を記述した文書シリーズ。すべてのインターネット標準は、RFC として文書化されている。

**リセット (reset).** パーチャル・サーキットにおいて、データ・フロー制御を再初期化すること。リセットすると、転送中のデータはすべて削除される。

**リセット要求パケット (reset request packet).** X.25 通信において、パーチャル・コールまたはパーマネント・パーチャル・サーキットのリセットを要求するために、データ端末装置 (DTE) またはデータ回線終端装置 (DCE) に送信するパケット。要求の理由もパケットに指定することができる。

**資源 (resource).** Nways スイッチにおいて、ハードウェア要素または制御プログラムによって作成される論理エンティティ。たとえば、アダプター、LIC、および伝送路は物理資源である。コントロール・ポイント、NBBS 中継線、NBBS ポート、およびコネクションは論理資源である。

NBBS ネットワークでは、資源を活用する前に、それを構成しておくことが必要である。

**リング (ring).** 環状ネットワーク (*ring network*) を参照。

**環状ネットワーク (ring network).** (1) 各ノードに正確に 2 本の分岐が接続されており、任意の 2 つのノード間には正確に 2 つのパスがあるネットワーク・ノード。(T) (2) 装置が単方向伝送リンクで接続されて閉じたパスを形成しているネットワーク構成。

**リング・セグメント (ring segment).** リングの残りの部分から分離することができる (コネクタを引き抜くことによって) リングの区間。LAN セグメント (*LAN segment*) を参照。

**rlogin (リモート・ログイン) (rlogin (remote login)).** Berkeley UNIX ベースのシステムによって提供されるサービス。ある機械の許可ユーザーがインターネットを介して他の UNIX システムに接続し、相互の端末が直接接続されているかのようにして対話することができる。rlogin ソフトウェアは、ユーザーの環境に関する情報 (たとえば、端末タイプ) をリモートの機械に渡す。

**RNR パケット (RNR packet).** データ端末装置 (DTE) またはデータ回線終端装置 (DCE) が、バーチャル・コールまたはパーマネント・バーチャル・サーキットに対する追加パケットを一時的に受付不能であることを示すために使用するパケット。

**ルート (根) ブリッジ (root bridge).** ブリッジ・ネットワークにおいて、他のアクティブ・ブリッジとの間に形成されたスパンニング・ツリーのルート (根) となるブリッジ。ルート (根) ブリッジは、スパンニング・ツリー・トポロジーを維持するために、ブリッジ・プロトコル・データ単位 (BPDU) を発信し、他のアクティブ・ブリッジに転送する。これは、ネットワーク内の最高の優先順位をもつブリッジである。

**ルート (route).** (1) 発信ノードから着信ノードまでのパスを表し、相互間で交換されるトラフィックが通る、正しいシーケンスのノードと伝送グループ (TG)。 (2) ネットワークのトラフィックが発信元からあて先に達するために使用するパス。

**ルート (経路) ブリッジ (route bridge).** 2 つのブリッジ・コンピューターが通信リンクを使用して 2 つの LAN を接続することができる、IBM ブリッジ・プログラムの機能。各ブリッジ・コンピューターは LAN の 1 つに直接接続されており、通信リンクが 2 つのブリッジ・コンピューターを接続する。

**ルート拡張機能 (REX) (route extension (REX)).** SNA において、サブエリア・ノードと隣接周辺ノード内のネットワーク・アドレス可能単位 (NAU) 間のパス部分を形成する、周辺リンクを含めたバス制御ネットワーク・コンポーネント。明示ルート (ER) (*explicit route (ER)*)、パス (*path*)、およびバーチャル・ルート (VR) (*virtual route (VR)*) も参照。

**ルート選択制御ベクトル (RSCV) (Route Selection control vector (RSCV)).** APPN ネットワーク内のルートを記述する制御ベクトル。RSCV は、発信元ノードからあて先ノードまでのパスを形成する TG とノードを識別する、正しいシーケンスの制御ベクトルから構成される。

**ルーター (router).** (1) ネットワークのトラフィックの流れのパスを決めるコンピューター。パスの選択は、特定のプロトコル、最短または最善パスを識別するアルゴリズム、およびその他の基準 (メトリックやプロトコル特有のあて先アドレスなど) から得られた情報に基づいて、複数のパスから選ばれる。 (2) 参照モデル・ネットワーク・レイヤーにおいて、類似または異なる体系を使用する 2 つの LAN セグメントを接続する装置。 (3) OSI 用語では、エンティティーに到達できるパスを判別する機能。 (4) TCP/IP では、ゲートウェイ (*gateway*) と同義。 (5) ブリッジ (*bridge*) と対比。

**ルーティング (routing).** (1) メッセージをあて先に到達させるためのパスを割り当てること。 (2) SNA において、メッセージ単位で運ばれるパラメーター (伝送ヘッダー内のあて先ネットワーク・アドレスなど) によって決められた、ネットワークの特定パスを通してメッセージ単位を転送すること。

**ルーティング・ドメイン (routing domain).** インターネット通信において、ルーティング・プロトコルを使用してネットワーク全体の表示が各中間システム内で同一になるようにしている、中間システムのグループ。ルーティング・ドメインは、外部リンクによって相互に接続されている。

**ルーティング情報プロトコル (RIP) (Routing Information Protocol (RIP)).** インターネット・プロトコルにおいて、領域間のルーティング情報を交換し、インターネット・ホスト間の最適ルートを定めるために使用される、内部ゲートウェイ・プロトコル。RIP は、リンク伝送速度ではなく、ルート・メトリックに基づいて最適ルートを定める。

**ルーティング・ループ (routing loop).** コンバージェンスが起こるまで、あるいは関係のネットワークが到達不能とみなされるまで、ルーターが相互間で情報を循環するときに発生する状態。

**ルーティング・プロトコル (routing protocol).** ルーターが他のルーターを見付け、到達可能なネットワークに達する最善ルートに関する情報を最新に保つために使用される技法。

**ルーティング・テーブル (routing table).** データグラムを転送したり、接続を確立するために使用されるルートの集まり。この情報は、ネットワーク・トポロジーと着側への到達可能性を識別するために、ルーター間で受け渡される。

**ルーティング・テーブル保守プロトコル (RTMP) (Routing Table Maintenance Protocol (RTMP)).** AppleTalk ネットワークにおいて、AppleTalk ルーティング・テーブルを用いて、トランスポート・レイヤーでルーティング情報を生成し、保守する機能を提供するプロトコル。AppleTalk ルーティング・テーブルは、インターネットを通して、発信元ソケットからあて先ソケットにパケットを伝送する。

**ルーティング更新プロトコル (RTP) (Routing update Protocol (RTP)).** ルーティング・データベースを維持しているバーチャル・ネットワーク・システム (Virtual Networking System (VINES)) プロトコルで、VINES ノード間でのルーティング情報の交換を可能にする。インターネット制御プロトコル (ICP) (*Internet Control Protocol (ICP)*) も参照。



**rsh.** ログイン・ステップを完全に飛ばして、リモート UNIX 機械上のコマンド解釈プログラムを呼び出し、そのコマンド解釈プログラムにコマンド行引き数を渡す、`rlogin` コマンドの変数。

## S

**SAP.** サービス・アクセス・ポイント (service access point) を参照。

**シード・ルーター (seed router).** AppleTalk ネットワークにおいて、ネットワーク構成データ (たとえば、ネットワーク範囲の数やゾーン・リスト) を維持するルーター。各ネットワークには、少なくとも 1 つのシード・ルーターがある。シード・ルーターは、構成ツールを使用して、最初に設定する必要がある。非シード・ルーター (*nonseed router*) と対比。

**セグメント (segment).** (1) コンポーネント間または装置の相互間のケーブル区間。セグメントは、1 本のパッチ・ケーブル、相互接続された複数のパッチ・ケーブル、または相互接続された建物ケーブルとパッチ・ケーブルの組み合わせから成る。(2) インターネット通信において、異なる機械にある TCP 機能の間の転送単位。各セグメントには、制御フィールドとデータ・フィールドが入っており、現在のバイト・ストリーム位置、実際のデータ・バイト、および受信データを妥当性検査するためのチェックサムが付加されている。

**分割 (segmenting).** OSI において、サポートするレイヤーからの 1 つのプロトコル・データ単位 (PDU) を複数の PDU にマップするためにレイヤーが実行する機能。

**シーケンス番号 (sequence number).** 通信において、伝送の流れやデータの受信を制御するために、フレームまたはパケットに割り当てられる番号。

**シリアル・ライン・インターネット・プロトコル (Serial Line Internet Protocol) (SLIP).** シリアル・ライン (たとえば、シリアル・ケーブルまたは電話回線を介したモデムへの RS232 接続) を介した 2 つの IP ホスト間のポイント・ポイント接続上で使用されるプロトコル。

NBBS ネットワークでは、SLIP は、ネットワーク・サポート・ステーションと IBM ネットワーク・サポート・センター (NSC) の間の接続にまたがって使用される。

**サーバー (server).** 通信ネットワークを通してワークステーションに共有サービスを提供する機能。たとえば、ファイル・サーバー、プリント・サーバー、メール・サーバー。(T)

**サービス・アクセス・ポイント (SAP) (service access point (SAP)).** (1) 開放型システム間相互接続 (OSI) 体系において、あるレイヤーのサービスが、そのレイヤーのエンティティによって、すぐ上のレイヤーのエンティティに提供されるポイント。(T) (2) アダプターによって提供される、情報を送受信することができる論理ポイント。1 つのサービス・アクセス・ポイントで、多数のリンクを終端させることができる。

**サービス公示プロトコル (SAP) (Service Advertising Protocol (SAP)).** インターネットワーク・パケット交換機能 (IPX) において、以下を提供するプロトコル。

- インターネット上の IPX サーバーが、そのサービスの名前とタイプを公示することができる機構。このプロトコルを使用するサーバーの名前、サービス・タイプ、およびアドレスは、NetWare を稼働するすべてのファイル・サーバーに記録されている。
- ワークステーションが、すべてのタイプのすべてのサーバー、特定タイプのすべてのサーバー、または特定タイプの最近隣サーバーのアイデンティティを見付けるために、照会を同報通信できる機構。
- ワークステーションが、特定タイプのすべてのサーバーの名前とアドレスを見付けるために、NetWare を稼働するすべてのファイル・サーバーを照会することができる機構。

**セッション (session).** (1) ネットワーク体系において、装置間のデータ通信を目的として、接続の確立、維持、および解放の過程で生じるすべての活動。(T) (2) 要求に応じて、活動化し、さまざまなプロトコルを提供するように調整し、非活動化することができる、ネットワーク・アクセス可能単位 (NAU) 間の論理結合。各セッションは、セッション中に交換されるすべての伝送を伴う伝送ヘッダー (TH) の中で固有に識別される。(3) L2TP において、ダイヤル・ユーザーと LNS 間でエンドツーエンド PPP 接続が試行されるとき、ユーザーがセッションを開始したか、LNS がアウトバウンド・コールを開始したかどうかにかかわらず、L2TP はセッションを生成する。そのセッション用のデータグラムは、LAC と LNS 間のトンネルを通じて送信される。LNS および LAC は、LAC に接続された各ユーザーについての状態情報を保持する。

**シンプル・ネットワーク管理プロトコル (SNMP) (Simple Network Management Protocol (SNMP)).** インターネット・プロトコルにおいて、ルーターと接続ネットワークを監視するのに使用されるネットワーク管理プロトコル。SNMP は、アダプテーション・レイヤー・プロトコルである。管理される装置に関する情報が定義され、そのアプリケーションの管理情報ベース (MIB) に保管される。

**SLIP.** シリアル・ライン IP (Serial Line IP)。シリアル通信リンク上で実行中の IP に関する IETF 標準。

**SNA 管理サービス (SNA/MS) (SNA management services (SNA/MS)).** SNA ネットワークの管理を援助するために提供されるサービス。

**SNAP.** (1) サブネットワーク・アクセス・プロトコル (SubNetwork Access Protocol)。 (2) サブネットワーク接続点 (SubNetwork Attachment Point)。

**ソケット (socket).** (1) 処理間またはアプリケーション・プログラム間の通信のエンドポイント。 (2) カリフォルニア大学の Berkeley ソフトウェア配布 (一般には、 Berkeley UNIX または BSD UNIX と呼ばれる) によって提供される抽象概念で、プロセスまたはアプリケーション間の通信のエンドポイントとして働く。

**ソース・ルート・ブリッジング (source route bridging).** LAN において、フレームの IEEE 802.5 媒体アクセス制御 (MAC) ヘッダー内のルーティング情報を使用して、フレームが送信する必要があるリングまたはトークンリング・セグメントを判別するブリッジング方式。ルーティング情報は、発信元ノードによって MAC ヘッダーに挿入される。ルーティング情報フィールド内の情報は、発信元ホストが生成する探索パケットから取り出される。

**ソース・ルーティング (source routing).** LAN において、発信元ステーションがフレームの通るルートを決めて、そのルーティング情報をフレームに組み込む方式。ブリッジは、そのルーティング情報を読み取り、フレームを転送するかどうかを判別する。

**発信元サービス・アクセス・ポイント (SSAP) (source service access point (SSAP)).** SNA および TCP/IP において、システムがリモート装置にデータを送信することを可能にする論理アドレス。あて先サービス・アクセス・ポイント (DSAP) (destination service access point (DSAP)) と対比。

**スパンニング・ツリー (spanning tree).** LAN において、ブリッジが自動的にルーティング・テーブルを作成し、トポロジーの変更に応じてそのテーブルを更新することによって、ブリッジ・ネットワーク内の任意の 2 つの LAN 間に 1 つしかルートが存在しないようにする方式。この方式により、パケットがルートを循環して送信元ルーターに戻るといったパケットのループを防止することができる。

**制御範囲 (SOC) (sphere of control (SOC)).** 1 つの管理サービス中心拠点によってサービスされるコントロール・ポイント・ドメインの集合。

**制御範囲 (SOC) ノード (sphere of control (SOC) node).** 中心拠点の制御範囲内にあるノード。 SOC ノードは、その中心拠点と管理サービス機能を交換している。 APPN エンド・ノードは、管理サービス機能を交換する機能をサポートする場合は、SOC ノードになれる。

**水平分割 (split horizon).** ネットワークのコンバージェンスを達成する時間を最小化するための技法。 ルーターは特定のルート (経路) を受信したインターフェースを記録し、そのルートに関する情報は再び同じインターフェースに伝送しないようにする。

**スプーフィング (spoofing).** データ・リンクにおいて、エンド・ステーションから開始されたプロトコルが、最終あて先の代わりに中間ノードによって確認応答されて処理される技法。たとえば、IBM 6611 データ・リンク交換では、SNA フレームはカプセル化して TCP/IP パケットに入れられ、非 SNA 広域ネットワーク・ノードを通過して伝送され、別の IBM 6611 によってアンパックされて、最終あて先に渡される。スプーフィングの利点は、エンド・エンド・セッションのタイムアウトを防止できることである。

**標準 MIB (standard MIB).** シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、管理情報構造 (SMI) の管理の下に置かれ、インターネット技術作業部会 (IETF) によって標準とみなされている MIB モジュール。

**静的ルート (static route).** ルーティング・テーブルに手入力される、ホスト間、ネットワーク・ノード間、またはその両方のルート。

**ステーション (station).** 通信機能を使用するシステムの入力または出力ポイント。たとえば、通信回線を通してデータを送信または受信することができる、ある特定の場所にある 1 台または複数のシステム、コンピューター、端末、装置、および関連のプログラム。

**StreetTalk.** バーチャル・ネットワーキング・システム (VINES) において、利用者がネットワークのトポロジーを知らなくても、ネットワーク上の任意のリソースを見つけてアクセスすることができる、ネットワーク全体の固有のネーミング/アドレッシング・システム。インターネット制御プロトコル (ICP) (Internet Control Protocol (ICP)) および ルーティング更新プロトコル (RTP) (Routing update Protocol (RTP)) も参照。

**管理情報構造 (SMI) (Structure of Management Information (SMI)).** (1) シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、ネットワーク管理プロトコルを用いてアクセスできるオブジェクトを定義するのに使用される規則。 (2) OSI において、情報の管理に関連する標準の集合。この集合には、管理情

報モデル (*Management Information Model*)および管理オブジェクト定義の指針 (*Guidelines for the Definition of Managed Objects*)が含まれる。

**サブエリア (subarea).** サブエリア・ノード、接続された周辺ノード、および関連の資源から構成される SNA ネットワークの部分。サブエリア・ノード内では、すべてのネットワーク・アクセス可能単位 (NAU)、リンク、およびサブエリア内のアドレス可能な隣接リンク端末 (接続された周辺ノードまたはサブエリア・ノード内の) は、共通のサブエリア・アドレスを共用し、異なる要素アドレスを持っている。

**サブネット (subnet).** (1) TCP/IP において、IP アドレスの一部によって識別されるネットワークの部分。(2) サブネットワーク (*subnetwork*) の同義語。

**サブネット・アドレス (subnet address).** インターネット通信において、ホスト・アドレスの一部がローカル・ネットワーク・アドレスとして解釈される、基本 IP アドレスリング機構の拡張。

**サブネット・マスク (subnet mask).** アドレス・マスク (*address mask*) の同義語。

**サブネットワーク (subnetwork).** (1) 1 組の共通特性 (同一ネットワーク ID など) を持つノードの集まり。(2) サブネット (*subnet*) の同義語。

**サブネットワーク・アクセス・プロトコル (SNAP) (Subnetwork Access Protocol (SNAP)).** LAN において、パケットが属している非 IEEE 標準プロトコル・ファミリーを識別する、5 バイトのプロトコル識別子。SNAP 値を使用して、\$AA をサービス・アクセス・ポイント (SAP) 値として使用する各プロトコルを区別する。

**サブネットワーク接続点 (SubNetwork Attachment Point).** フレームのプロトコル・タイプを識別する LLC ヘッダー拡張部。

**サブネットワーク・マスク (subnetwork mask).** アドレス・マスク (*address mask*) の同義語。

**サブシステム (subsystem).** 制御システムから独立して、または非同期で、動作することができる、2 次的または従属的なシステム。(T)

**スイッチド・バーチャル・サーキット (SVC) (switched virtual circuit (SVC)).** 必要に応じて動的に確立される X.25 回線。交換回線と同等の X.25 回線。パーマナント・バーチャル・サーキット (PVC) (*permanent virtual circuit (PVC)*) と対比。

**同期 (synchronous).** (1) 共通タイミング信号のような特定の事象の発生に依存する 2 つ以上のプロセス。(T) (2) 規則的または予測可能な時間的關係をもって起こること。

**同期データ・リンク制御 (SDLC) (Synchronous Data Link Control (SDLC)).** (1) リンク接続上で同期、コード透過、ビット直列情報伝送を管理するための、米国規格協会 (ANSI) のアドバンスト・データ通信制御手順 (ADCCP) および国際規格のハイレベル・データ・リンク制御 (HDLC) のサブセットに従う規則。伝送交換は、交換回線または非交換回線上で、全二重または半二重で行われる。リンク接続の構成は、ポイント・ポイント、多地点、またはループのいずれかである。(I) (2) 2 進データ同期通信 (BSC) (*binary synchronous communication (BSC)*) と対比。

**同期光ネットワーク (synchronous optical network) (SONET).** 光インターフェースを介してデジタル情報を伝送するための米国標準。これは、同期デジタル階層 (SDH) 勧告と密接な関連がある。

**SYNTAX.** シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、管理オブジェクトに対応する抽象データ構造を定義する、MIB モジュール内の文節。

**システム (system).** データ処理において、特定の機能を達成するために組織された人間、機械、および方式の集まり。(I) (A)

**システム構成 (system configuration).** 特定のデータ処理システムを形成する装置とプログラムを指定するプロセス。

**システム・サービス・コントロール・ポイント (SSCP) (system services control point (SSCP)).** 構成の管理、ネットワーク運用者および問題判別の要求の調整、およびネットワーク利用者にディレクトリー・サービスやその他のセッション・サービスを提供するための、サブエリア・ネットワーク内のコンポーネント。相互に対等の立場で協働する複数の SSCP は、ネットワークを複数の制御領域に分割し、各 SSCP が自身の領域内の物理装置および論理装置に対して階層的な制御関係を持つようにすることができる。

**システム・ネットワーク体系 (SNA) (Systems Network Architecture (SNA)).** ネットワークを通して情報単位を伝送し、ネットワークの構成と運用を制御するための、論理構造、フォーマット、プロトコル、および動作手順の記述。SNA の階層化された構造により、情報の最終的な発信元とあて先 (つまり、利用者) が、情報交換に使用される SNA ネットワークの特定のサービスや機能から独立し、その影響を受けなくすることができる。



## T

**TCP/IP.** (1) 伝送制御プロトコル/インターネット・プロトコル (Transmission Control Protocol/Internet Protocol)。(2) 本来は米国国防総省によって開発された UNIX に似ている、イーサネットを基礎にしたシステム相互接続プロトコル。TCP/IP により、レイヤー 4 が TCP でレイヤー 3 が IP のパケット交換方式リサーチ・ネットワークである ARPANET (拡張研究プログラム機関ネットワーク (Advanced Research Projects Agency Network)) の利便性が向上した。

**Telnet.** インターネット・プロトコルにおいて、リモート端末接続サービスを提供するプロトコル。このプロトコルによって、あるホストのユーザーがリモート・ホストにログオンし、そのホストに直接接続されている端末ユーザーとして対話することができる。

**しきい値 (threshold).** (1) IBM ブリッジ・プログラムにおいて、『しきい値超過』 オカレンスがカウントされてネットワーク管理プログラムに通知される前に、誤りのためにブリッジを通過して転送されないフレームの最大数として設定される値。(2) そこからカウンターが 0 まで減分される初期値、または初期値からカウンターが増分または減分されて到達する値。

**スループット・クラス (throughput class).** パケット交換において、データ端末装置 (DTE) パケットがパケット交換ネットワークを通過する速度。

**時分割多重 (TDM) (time division multiplexing (TDM)).** チャンネル化 (*channelization*) を参照。

**活動回数 (TTL) (time to live (TTL)).** ベストエフォート送達プロトコルが、パケットの無限ループを禁止するために使用する技法。TTL カウンターが 0 に達すると、パケットは廃棄される。

**タイムアウト (timeout).** (1) 指定された事象の発生時から始まる事前定義された時間間隔の終了前に起こる別の事象。(2) システム操作を中断してリスタートすることが必要になる前の、ポーリングまたはアドレッシングに対するレスポンスのような、特定の動作を起こすために割り当てられた時間。

**TLV.** タイプ/長さ/値 (Type/Length/Value)。LAN エミュレーション・パケットの中の汎用情報要素。

**トークン (token).** (1) ローカル・エリア・ネットワークにおいて、あるデータ装置が一時的に伝送媒体を制御していることを示すために、そのデータ装置から別のデータ装置に連続的に渡される許可信号。各データ装置には、媒体を制御するためにトークンを獲得して使用する機会が与えられる。トークンというのは、伝送許可を示

す特別のメッセージまたはビット・パターンである。(T) (2) LAN において、伝送媒体上を、ある装置から別の装置に渡される一連のビット。トークンにデータが付加されるとフレームになる。

**トークンリング (token ring).** (1) IEEE 802.5 では、媒体に接続されたステーション間でトークン (特殊なパケットまたはフレーム) を渡すことによって媒体アクセスを制御するネットワーク技術。(2) ある接続リング・ステーション (ノード) から別のノードにトークンを渡すリング・トポロジーを持つ、FDDI または IEEE 802.5 ネットワーク。(3) ローカル・エリア・ネットワーク (LAN) (*local area network (LAN)*) も参照。

**トークンリング・ネットワーク (token-ring network).** (1) トークン・パッシング手順により、データ・ステーション間で単方向のデータ伝送を行い、伝送されたデータが送信元ステーションに戻ってくる構造の環状ネットワーク。(T) (2) ノードからノードへ順にトークンを渡すリング・トポロジーを使用するネットワーク。送信の準備ができていないノードは、トークンを取り込み、伝送するデータを挿入することができる。

**トポロジー (topology).** 通信において、ネットワーク・ノード内のノードの物理的または論理的な配置。特に、ノードとそれを結ぶリンクの関係を表す。

**トポロジー・データベース更新 (TDU) (topology database update (TDU)).** ネットワーク・トポロジー・データベースを維持するために、APPN ネットワーク・ノード間に同報通信され、各ネットワーク・ノードに完全に複写される、新規または変更されたリンクまたはノードに関するメッセージ。TDU には、以下のものを識別する情報が入っている。

- 送信元ノード
- ネットワークの各種資源のノード特性およびリンク特性
- 記述されている各資源の最新の更新のシーケンス番号

**トレース (trace).** (1) コンピューター・プログラムの実行の記録。命令が実行された順序を表す。(A) (2) データ・リンクの場合は、送信または受信されたフレームとバイトの記録。

**トランシーバー (送受信装置) (transceiver (transmitter-receiver)).** LAN において、ホスト・インターフェースをイーサネットのようなローカル・エリア・ネットワークに接続する物理装置。イーサネット・トランシーバーには、ケーブルに信号を送って衝突を検出する電子機器が内蔵されている。

**伝送制御プロトコル (TCP) (Transmission Control Protocol (TCP)).** インターネット、およびインターネットワーク・プロトコルに関する米国国防総省の規格に準拠するその他のすべての通信ネットワークで使用されている通信プロトコル。TCP は、パケット交換通信網のホストとそのネットワークの相互接続システムのホストとの間に、高信頼性ホスト間プロトコルを提供する。基礎となるプロトコルとして、インターネット・プロトコル (IP) を使用している。

**伝送制御プロトコル/インターネット・プロトコル (TCP/IP) (Transmission Control Protocol/Internet Protocol (TCP/IP)).** ローカル・エリア・ネットワークと広域ネットワーク・ノードの両方で、ピア間接続機能をサポートする一組の通信プロトコル。

**伝送グループ (TG) (transmission group (TG)).** (1) 伝送グループ番号によって識別された隣接ノード間の接続。(2) サブエリア・ネットワークにおいて、隣接ノード間の単一リンクまたはリンク群。伝送群がリンク群で構成される場合、リンクは単一の論理リンクと見なされ、伝送群はマルチリンク伝送群 (MLTG) と呼ばれる。混合媒体マルチリンク伝送群 (MMMLTG) とは、異なる媒体タイプのリンク (たとえば、トークンリング、交換 SDLC、非交換 SDLC、およびフレーム・リレー・リンク) を含むものを言う。(3) APPN ネットワークにおいて、隣接ノード間の 1 つのリンク。(4) 並列伝送群 (parallel transmission groups) も参照。

**伝送ヘッダー (transmission header) (TH).** パス制御が、メッセージ単位をルーティングし、ネットワークの中の流れを制御するために作成して使用する制御情報。オプションでその後に基本情報単位 (BIU) または BIU セグメントを続けることができる。パス情報単位 (path information unit) も参照。

**透過ブリッジング (transparent bridging).** LAN において、媒体アクセス制御 (MAC) レベルを通して、個々のローカル・エリア・ネットワークを相互に結合する方式。透過型ブリッジには MAC アドレスが入ったテーブルが保管されており、テーブルに指示されている場合は、ブリッジが検出したフレームを別の LAN に転送することができる。

**トランスポート・レイヤー (transport layer).** 開放型システム間相互接続参照モデルにおいて、高信頼性エンド・エンド・データ転送サービスを提供するレイヤー。パス内に中継開放型システムが存在する場合もある。(T) 開放型システム間相互接続参照モデル (Open Systems Interconnection reference model) も参照。

**トランスポート・サービス (transport services).** 以下の目的のために Nways スイッチのコントロール・ポイントによって実行される NBBS 体系の機能。

- トランク・ラインと Nways スイッチの接続サポート
- 帯域幅の使用率の最大化
- サービス品質の保証
- Nways スイッチ間のパケット転送
- 論理待ち行列の管理と、伝送のスケジューリング

**トラップ (trap).** シンプル・ネットワーク・マネジメント・プロトコル (SNMP) において、例外条件を報告するために、管理ノード (エージェント機能) が管理ステーションに送るメッセージ。

**トランク・アダプター (trunk adapter).** トランク・ラインに NBBS 体系のトランスポート・サービスを提供するコードを実行する、Nways スイッチの 2216 以外の型式のモジュール。2216 では、ポート・アダプターとトランク・アダプターの機能が結合された多重化ポート/トランク・アダプター (MPTA) が使用されている。

**トランク・ライン (trunk line).** 2 つの Nways スイッチを接続する高速伝送路。同軸ケーブル、ファイバー・ケーブル、または無線を使用でき、通信会社からリースすることもできる。

Nways スイッチでは、各トランク・ラインは 1 つの NBBS トランクに関連付けられている。

**トンネル (Tunnel).** トンネルとは、LNS-LAC の対によって定義されるもので、LAC と LNS の間で PPP データグラムを伝える。単一のトンネルで多くのセッションを多重化することができる。制御接続が同じトンネルを介して作動する場合は、すべてのセッションおよびトンネル自体の設定、解放、および保守を制御する。

**トンネル伝送 (tunneling).** トランスポート・ネットワークを、単一の通信リンクまたは LAN のように扱うこと。カプセル化 (encapsulation) も参照。

**T1.** 米国では、1.544-Mbps の公衆アクセス回線。24 個の 64 Kbps チャネルで利用可能。欧州方式 (E1) は 2.048 Mbps で伝送する。

## U

**出荷時設定アドレス (universally administered address).** ローカル・エリア・ネットワークにおいて、製造時にアダプターに永久的に符号化されるアドレス。出荷時設定アドレスは固有である。ローカル管理アドレス (locally administered address) と対比。

**ユーザー・データグラム・プロトコル (UDP) (User Datagram Protocol (UDP)).** インターネット・プロトコルにおいて、低信頼性のコネクションレス・データグラム・サービスを提供するプロトコル。このプロトコルを使用して、ある計算機またはプロセス上のアプリケーション

ョン・プログラムが、別の計算機またはプロセス上のアプリケーション・プログラムに、データグラムを送信することができる。UDP では、インターネット・プロトコル (IP) を使用してデータグラムを送達する。

## V

**V.24.** データ通信において、データ端末装置 (DTE) とデータ回線終端装置 (DCE) 間の交換回線の一連の定義を規定した CCITT の仕様。

**V.25.** データ通信において、手動および自動で設定されたコールのエコー制御装置を使用禁止にする手順を含めた、一般交換電話ネットワークの自動応答装置および並列自動コール装置を定義する CCITT の仕様。

**V.34.** 標準の市販の音声グレードの 33.6 Kbps (およびそれより低速の) チャネルを介してのモデム通信に関する ITU-T 勧告。

**V.35.** データ通信において、種々のデータ転送速度のデータ端末装置 (DTE) とデータ回線終端装置 (DCE) 間の交換回線の一連の定義を規定した CCITT の仕様。

**V.36.** データ通信において、48, 56, 64, または 72 キロビット/秒のデータ転送速度のデータ端末装置 (DTE) とデータ回線終端装置 (DCE) 間の交換回線の一連の定義を規定した CCITT の仕様。

**VCC.** バーチャル・チャンネル・コネクション (Virtual Channel Connection)。当事者 (通話者) 間の接続。

**バージョン (version).** 通常は重要な新しいコードまたは新しい機能を含む、別個のライセンス・プログラム。

**VINES.** バーチャル・ネットワーキング・システム (Virtual Networking System)。

**バーチャル・サーキット (virtual circuit).** (1) パケット交換で、実際の接続箇所をユーザーに見えるようにする、ネットワークによって提供される機能。(T) データ回線 (data circuit) も参照。物理回線 (physical circuit) と対比。(2) 2 台の DTE 間に確立された論理接続。

**バーチャル・コネクション (virtual connection).** フレーム・リレーにおいて、ポテンシャル接続の戻りパス。

**バーチャル・リンク (virtual link).** 最短パス最優先オープン (OSPF) において、非バックボーン中継エリアによって分離されたボーダー・ルーターに接続する、ポイント・ポイント・インターフェース。エリア・ルーターは OSPF バックボーンの一部なので、バーチャル・リンクはバックボーンに接続する。バーチャル・リンクは、OSPF バックボーンが不連続にならないようにする。

**バーチャル・ローカル・エリア・ネットワーク (VLAN) (Virtual Local Area Network (VLAN)).** プロトコルおよびサブネットに基づく、1 つまたは複数の LAN の論理的グループ化で、ネットワーク・トラフィックを、こうしてできるグループ内に分離する場合に使用される。

**バーチャル・ネットワーキング・システム (VINES) (Virtual Networking System (VINES)).** Banyan Systems, Inc. からのネットワーク運用システムとネットワーク・ソフトウェア。VINES ネットワークにおけるバーチャル・リンクでは、たとえ実際には数百マイル離れていても、すべての装置およびサービスが相互に直接接続されているように見える。StreetTalk も参照。

**バーチャル・ルート (VR) (virtual route (VR)).** (1) SNA において、次のような論理接続。(a) 特定の明示ルートとして物理的に実現されている 2 つのサブエリア・ノード間の論理接続。または (b) ノード内のセッション用のサブエリア・ノード内に完全に収まっている論理接続。別個のサブエリア・ノードの間のバーチャル・ルートは、使用する明示ルートに伝送優先順位を定め、バーチャル・ルート・ペーシングによってフロー制御を行い、パス情報単位 (PIU) にシーケンス番号を付けることによりデータ保全性を確保する。(2) 明示ルート (ER) (explicit route (ER)) と対比。パス (path) およびルート拡張 (REX) (route extension (REX)) も参照。

## W

**広域ネットワーク (WAN) (wide area network (WAN)).**

(1) ローカル・エリア・ネットワークや大都市圏ネットワークよりも広い地域に通信サービスを提供し、公衆通信施設を使用または提供することができるネットワーク。

(T) (2) 何百キロあるいは何千キロも離れた区域にサービスを行うように設計されたデータ通信ネットワーク。たとえば、公衆および私用パケット交換ネットワークや各国の電話網など。(3) ローカル・エリア・ネットワーク (local area network (LAN)) および大都市圏ネットワーク (metropolitan area network (MAN)) と対比。

**ワイルドカード文字 (wildcard character).** パターン突き合わせ文字 (pattern-matching character) の同義語。

## X

**X.21.** 公衆データ網上の同期動作のための、データ端末装置とデータ回線終端装置の間の汎用インターフェースに関する、国際電信電話諮問委員会 (CCITT) の勧告。

**X.25.** (1) データ端末装置とパケット交換データ網間のインターフェースに関する、国際電信電話諮問委員会 (CCITT) の勧告。(2) パケット交換 (packet switching) も参照。

**Xerox ネットワーク・システム (XNS) (Xerox Network Systems (XNS)).** Xerox Corporation によって開発された一組のインターネット・プロトコル。TCP/IP プロトコルに類似しているが、XNS は異なるパケット・フォーマットと用語を使用している。インターネットワーク・パケット交換機能 (*IPX*) (*Internetwork Packet Exchange (IPX)*) も参照。

## Z

**ゾーン (zone).** AppleTalk ネットワークにおいて、インターネット内部のノードのサブセット。

**ゾーン情報プロトコル (ZIP) (Zone Information Protocol (ZIP)).** AppleTalk プロトコルにおいて、セッション・レイヤーのインターネット全体のゾーン名とネットワーク番号のマッピングを維持してゾーン管理サービスを提供するプロトコル。

**ゾーン情報テーブル (ZIT) (zone information table (ZIT)).** インターネットのネットワーク番号と対応ゾーン・ネームのマッピングをリストしたもの。このリストは、AppleTalk インターネットの各インターネット・ルーターによって維持される。

## 特殊文字 (Special Characters)

**2216 Nways ブロードバンド・スイッチ (2216 Nways BroadBand Switch).** NBBS ネットワークでの高速通信を可能にする高速パケット交換機。2220 Nways ブロードバンド・スイッチでは、ネットワーキング・ブロードバンド・サービス体系で定義されている機能を実装している。**Nways スイッチ (Nways Switch)** と同義。





# 索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

## [ア行]

アクセス、認証構成プロンプトへの 249  
アクセス、ホスト・オンデマンド・クライアント・キャッシュに 149  
アクセス、Web サーバー・キャッシュへの 207  
圧縮  
  概説  
    フレーム・リレー 229  
    PPP 229  
アドバイザー  
  ネットワーク・ディスパッチャーの 101  
アルゴリズム、IP セキュリティーの (IPv4) 356  
アルゴリズム、IP セキュリティーの (IPv6) 368  
暗号化  
  監視  
    フレーム・リレーの 273  
    PPP の 270  
  構成 269  
    フレーム・リレーの 272  
    フレーム・リレー 269  
  ECP の構成  
    PPP の 269  
  MPPE の監視  
    PPP の 272  
  MPPE の構成  
    PPP の 271  
  PPP 269  
暗号化キー 351  
  IP セキュリティーの (IPv4)、構成 356  
暗号化制御プロトコル  
  PPP の 269  
依存関係テーブル 169  
インターネット・キー交換 343  
  監視コマンド  
    アクセス (IPv4) 373  
    監視コマンド (IPv4) 373  
    キー交換フェーズ 344  
  構成 351  
  構成、公開キー・インフラストラクチャーの 346  
  メッセージ交換 345  
インターフェース  
  帯域幅予約監視コマンド 47  
  帯域幅予約構成コマンド 37

インターフェース監視コマンド  
  ダイヤルアウト 472  
  ダイヤルイン 472  
インターフェース構成コマンド  
  ダイヤルアウト 471  
音声  
  構成コマンド、要約 579  
音声アダプター  
  概説 574  
  構成 577, 579  
  使用 573  
音声アダプター監視コマンド  
  アクセス 592  
音声監視コマンド  
  要約 592  
  calls 593  
  status 595  
  trace 596  
音声構成コマンド  
  アクセス 579  
  add 580  
  delete 583  
  list 583, 589  
  modify 585  
  reorder-call-rule 585  
  set 586, 590  
音声ネットワーク構成コマンド  
  アクセス 589

## [カ行]

会計  
  セキュリティ 241  
概説  
  圧縮 229  
  WAN 再ルート 65  
  WAN 復元 65  
外部キャッシュ制御プロトコル 170  
  構成 171  
外部キャッシュ制御プロトコル (ECCP) のベクトル形式  
  173  
  コマンド応答ベクトル 176  
  コマンド要求ベクトル 175  
  サブベクトルの形式 178  
  認証応答ベクトル 176  
  認証要求ベクトル 175  
  フィールドの説明 173  
外部キャッシュ制御マネージャー  
  削除、オブジェクトの 171

- 外部キャッシュ制御マネージャー (続き)
  - 使用、依存関係テーブルの 171
  - 使用、URL マスクの 173
  - 使用、統計の 172
  - 使用、ポリシーの 172
  - 照会、オブジェクトの 172
  - 使用可能/使用不可、区画の 172
  - 除去、区画の 172
  - 説明 171
  - 追加、オブジェクトの 171
- 外部キャッシュ制御マネージャーの概要 169
- 外部キャッシュ制御マネージャーの認証 170
- カプセル化セキュリティー・ペイロード (ESP) 337
- 監視 351
  - 暗号化
    - フレーム・リレーの 273
    - PPP の 270
  - 音声監視コマンド 592
  - 手動 IP セキュリティー (IPv6) 383
  - データ圧縮、フレーム・リレー・リンク上での 237
  - データ圧縮、PPP リンク上の 234
  - IP セキュリティー (IPv4) 373
  - MPPE
    - PPP の 272
  - TSF 監視コマンド 562
- 監視コマンド
  - ダイヤルアウト・インターフェース 472
  - ダイヤルイン・インターフェース 472
  - ポリシー
    - disable 327
    - enable 328
    - list 329
    - reset 328
    - search 328
    - status 329
    - test 330
  - DIALs グローバル 468
  - diffserv
    - clear 396
    - dscache 397
    - list 398
  - IPSec 351
    - change tunnel 378
    - delete 373
    - delete tunnel 378
    - disable 379
    - enable 380
    - IKE、アクセス (IPv4) 373
    - IPSec、アクセス (IPv4) 377
    - IPSec、アクセス (IPv6) 383
    - list 374, 380
    - PKI、アクセス (IPv4) 375
  - 監視コマンド (続き)
    - IPSec 351 (続き)
      - reset 381
      - set 382
      - stats 374, 382
  - キー 351
    - IP セキュリティーの (IPv4)、構成 356
    - IP セキュリティーの (IPv6)、構成 368
  - キーワード 597
  - 機能
    - 監視 21
    - シン・サーバー機能 (TSF) 539
    - 帯域幅予約 1
    - MAC フィルター 49, 53
  - キャッシュ 161
  - キャッシュ要求が検出された場合 166
  - キャッシュ・ヒットがある場合の Web サーバー・キャッシュを使用したネットワーク・ディスパッチャー 161
  - 許可
    - セキュリティー 241
  - グローバル監視コマンド
    - DIALs 468
  - グローバル構成コマンド
    - DIALs 459
  - コード化サブシステム
    - 監視 221, 223
    - 構成 221
  - 公開キー・インフラストラクチャー 346
    - アクセス、環境への (IPv4) 375
    - 監視コマンド 375
      - アクセス (IPv4) 375
      - cert-load (IPv4) 375
      - cert-req (IPv4) 376
      - cert-save (IPv4) 376
      - list certificate (IPv4) 376
      - list configured-servers (IPv4) 377
      - load certificate (IPv4) 377
    - 構成 346, 352
    - 構成、公開キー・インフラストラクチャーの 346
    - 構成コマンド 353
      - add server 353
      - change server 353
      - delete certificate 354
      - delete private-key 354
      - delete server 354
      - list certificates 355
      - list private-keys 355
      - list servers 355
  - 構成 351
    - 暗号化 269
      - フレーム・リレーの 272

構成 351 (続き)

- インターネット・キー交換 351
- 公開キー・インフラストラクチャー 352
- 手動 IP セキュリティー (IPv4) 355
- 手動トンネル (IPv4) 366
- 手動トンネル (IPv6) 369
- ダイヤルアウト・インターフェース 452
- ダイヤルイン・インターフェース 449
- データ圧縮、フレーム・リレー・リンク上での 237
- データ圧縮、PPP リンク上の 234
- 認証プロンプトへのアクセス 249
- ポリシー 307
- diffserv 391
- ECP 暗号化
  - PPP の 269
- IP セキュリティー (IPv6) 367
- L2 プロトコル 413
- LDAP 307
- MPPE
  - PPP の 271
- MS ポイント・ポイント暗号化 269
- WAN 復元 71

構成コマンド 351

- ダイヤルアウト・インターフェース 471
- トンネル
  - add 416
- 認証 249
- ポリシー 307
  - add 308
  - change 321
  - copy 321
  - delete 321
  - disable 321
  - enable 321
  - list 321
- default-policy
  - set 323
- DIALs 454
- DIALs グローバル 459
- diffserv 391
  - delete 392
  - disable 392
  - enable 392
  - list 393
  - set 393
- IPSec 351
  - アクセス (IPv4) 356
  - アクセス (IPv6) 368
  - add server 353
  - add tunnel 357
  - change server 353
  - change tunnel 362

構成コマンド 351 (続き)

- IPSec 351 (続き)
  - delete certificate 354
  - delete private-key 354
  - delete server 354
  - delete tunnel (IPv4) 363
  - disable 363
  - enable 364
  - list 364
  - list certificates 355
  - list private-keys 355
  - list servers 355
  - set 365
- L2 トンネル
  - set 415, 419
- L2F、要約 413, 416
- L2T
  - add 416
  - disable 414, 417
  - enable 414, 418
- L2TP
  - トンネル 425
  - call 421
  - encapsulator 414, 419
  - kill 424
  - list 414, 419
  - memory 424
  - start 425
  - stop 425
- L2TP の要約 413, 416
- LDAP 322
  - disable 322
  - enable 322
  - set 325
- PPTP、要約 413, 416
- refresh
  - set 326

構成と監視、Web サーバー・キャッシュの 201

コマンド

- ダイヤルアウト
  - インターフェース構成 471
  - インターフェースの監視 472
- ダイヤルイン
  - インターフェースの監視 472
- DIALs
  - グローバル監視 468
  - グローバル構成 459

コマンド応答ベクトル 174

## [サ行]

### サーバー

#### 認証

定義 245

#### ACE/サーバー

サポート 246

制約 247

#### DIALs

構成コマンド 454

使用 447

定義 447

要件 449

### サブフィールドの形式 195

依存関係サブフィールド 196

オブジェクト・サブフィールド 197

名前サブフィールド 197

パスワード要求サブフィールド 197

URL 要求サブフィールド 198

### サブベクトルの形式 178

add (force) object コマンド・サブベクトル 179

add (force) 応答サブベクトル 187

add object 応答サブベクトル 187

add object コマンド・サブベクトル 179

delete object 応答 サブベクトル 188

delete object コマンド・サブベクトル 179

dependency 応答サブベクトル 188

dependency コマンド・サブベクトル 180

disable command サブベクトル 181

disable 応答サブベクトル 189

enable 応答サブベクトル 189

enable コマンド・サブベクトル 181

policy 応答サブベクトル 189

policy コマンド・サブベクトル 182

purge 応答サブベクトル 192

purge コマンド・サブベクトル 185

query 応答サブベクトル 192

query コマンド・サブベクトル 185

statics コマンド・サブベクトル 186

URL mask 応答サブベクトル 195

URL mask コマンド・サブベクトル 186

### 実行プログラム

ネットワーク・ディスパッチャーの 100

### 手動 IP セキュリティー 351

監視 (IPv6) 383

構成コマンド (IPv4) 357

IPv4 350

IPv6 350

### 準備、ネゴシエーションされた IP セキュリティー操作の 351

### 使用

ダイヤルイン・アクセス・サーバー 447

使用、HTTP プロキシの 164

使用、WAN 復元の 65

### 証明書

取得 352

### シン・サーバー機能

構成 553

スケーラブル高可用性キャッシュ 165

静的アドレス・マッピング 431

### セキュリティー 170

会計 241

許可 241

認証 241

セキュリティー・アソシエーション (SA) 338

属性、リモート AAA 597

## [タ行]

### 帯域幅予約

監視プロンプトへのアクセス 43

構成 1

構成コマンド

要約 24

構成プロンプトへのアクセス 21

フィルター付き 7

フレーム・リレー上の 3

### 帯域幅予約監視コマンド

インターフェース 47

監視プロンプトへのアクセス 43

要約 44

circuit 45

clear 45

clear-circuit-class 45

counters 46

counters-circuit-class 46

last 47

last-circuit-class 47

### 帯域幅予約構成コマンド

インターフェース 37

サンプル構成 13

要約 22

activate-ip-precedence-filtering 26

add-circuit-class 26

add-class 26

assign 28

assign-circuit 30

BRS 構成プロンプトへのアクセス 21

change-circuit-class 31

change-class 31

circuit 31

clear-block 32

create-super-class 32

deactivate-ip-precedence-filtering 33

deassign 33

## 帯域幅予約構成コマンド (続き)

- deassign-circuit 33
- default-circuit-class 33
- default-class 34
- del-circuit-class 34
- del-class 34
- disable 35
- disable-hpr-over-ip-port-numbers 35
- enable 35
- enable-hpr-over-ip-port-numbers 36
- list 38
- queue-length 40
- set circuit defaults 41
- show 41
- tag 42
- untag 43
- use circuit defaults 43

## 帯域幅予約システム (BRS)

- 説明 1
- 廃棄可能性 (DE) 4
- IP バージョン 4 優先順位ビット処理の使用 10
- TCP/UDP ポート番号フィルター 9

## ダイヤルアウト

- インターフェース監視コマンド 472
- インターフェース構成コマンド 471

## ダイヤルアウト・インターフェース

- 構成 452
- モデム・プール 453

## ダイヤルイン

- インターフェース監視コマンド 472

## ダイヤルイン・アクセス・サーバー

- サーバー提供の IP アドレス 454
- IP アドレス割り当て方式 455

## ダイヤルイン・インターフェース

- 構成 449
- ダイヤル回線パラメーターのデフォルト値 450
- 追加 451
- PPP カプセル化機能パラメーターのデフォルト値 451

## ダイヤル回線

- パラメーターのデフォルト値
- ダイヤルイン・インターフェースの 450

## ダイヤル・オン・オーバーフロー 65

## ダイヤル・プラン (Nuera F200) 576

## データ圧縮

- 圧縮セッション
- 定義 233
- 概説 229
- 概念 229
- 基本 230
- 考慮事項 232
- データ内容 234

## データ圧縮 (続き)

- 考慮事項 232 (続き)
- メモリー使用量 233
- リンク・レイヤー圧縮 234
- CPU 負荷 232
- データ・ディクショナリー
- 定義 230
- ヒストリー
- 定義 230
- フレーム・リレー・リンク上での 237
- 監視 239
- 構成 237

## 定義、クラスターの

- ホスト・オンデマンド・クライアント・キャッシュ 113

## 動的ドメイン名サーバー (DDNS)

- 説明 457

## 動的ホスト構成プロトコル (DHCP)

- 基本的な設定 456
- サーバーへの複数ホップ 457
- 説明 455
- 複数サーバー・ネットワーク 457

## トランスポート・モード 338

## トンネル内トンネル、IP セキュリティの 341

## トンネル・モード 338

# [ナ行]

## 認証 241, 249

- 構成コマンド 249
- セキュリティ 241
- SecurID の使用 246
- 制約 247

## 認証構成プロンプト

- アクセス 249

## 認証サーバー

- 定義 245
- ACE/サーバー 246

## 認証ヘッダー (AH) 336

## ネゴシエーションされた IP セキュリティ 343

- 操作
- 準備 351

- メッセージ交換 345
- IKE キー交換フェーズ 344
- IKE メッセージ交換 345

## ネットワーク図

- IP セキュリティ・トンネル 342

## ネットワーク制御プロトコル (NCP)

- PPP インターフェースの
- 暗号化制御プロトコル 269

## ネットワーク・アドレス変換

- 監視コマンド 445
- 構成 437

ネットワーク・アドレス変換 (NAT)  
 使用 429  
ネットワーク・アドレス変換構成コマンド 437  
 list 439  
ネットワーク・アドレス変換コマンド  
 change 438  
 delete 438  
 disable 439  
 enable 439  
 map 440  
 reserve 441  
 reset 443  
 set 443  
ネットワーク・アドレス・ポート変換 (NAPT)  
 使用 431  
ネットワーク・ステーション 539  
ネットワーク・ディスパッチャー 99  
 アドバイザー 101  
 概説 99  
 高可用性 101  
 構成 104  
 構成コマンド 99, 117  
   アクセス 117, 137  
   要約 117, 137  
   add 118  
   clear 124  
   disable 125  
   enable 126  
   list 127, 138  
   quiesce 139  
   remove 129  
   report 140  
   set 131  
   status 141  
 実行プログラム 100  
 使用 99  
   ステップ 106  
 負荷の平衡化 100  
 マネージャー 101  
 SNMP 管理アプリケーション 100  
ネットワーク・ディスパッチャー、Web サーバー・キ  
 ャッシュを使用しない 160  
ネットワーク・ディスパッチャーと Web サーバー・キ  
 ャッシュ、キャッシュ・ヒットなし 160

## [八行]

バーチャル・サーキット・リソース・マネージャー  
 (VCRM)  
 構成と監視 569  
パス MTU ディスカバリー 341  
パラメーター  
 MAC フィルター 50

フィルター  
 および帯域幅予約 7  
 マルチキャスト・アドレッシング 8  
 優先順位 13  
 MAC アドレッシング 8  
負荷の平衡化  
 ネットワーク・ディスパッチャーによる 100  
ブリッジング機能  
 更新コマンド 58  
 MAC フィルター 53  
 update サブコマンド 51  
フレーム・リレー  
 暗号化 269  
 監視 273  
 構成 272  
 帯域幅予約 3  
フレーム・リレー・リンク  
 構成と監視、データ圧縮の 237  
プロトコル  
 音声アダプター 579  
ポイントツーポイント・プロトコル (PPP)  
 暗号化制御プロトコル 269  
保護トンネル 333  
ホスト・オンデマンド・クライアント・キャッシュ  
 構成と監視 145  
 定義、クラスターの 113  
ホスト・オンデマンド・クライアント・キャッシュ監視  
 コマンド  
   activate 154  
   clear 154  
   delete 155  
   disable 155  
   enable 155  
   list 156  
ホスト・オンデマンド・クライアント・キャッシュ構成  
 コマンド  
   activate 150  
   add 150  
   delete 150  
   list 151  
   modify 152  
ホスト・オンデマンド・クライアント・キャッシュ変更  
 コマンド  
   modify 158  
ポリシー 327  
 オブジェクト 278  
 概説 275  
 監視コマンド 327  
   disable 327  
   enable 328  
   list 329  
   reset 328

ポリシー 327 (続き)  
  search 328  
  status 329  
  test 330  
監視プロンプト  
  アクセス 327  
機能、概要 275  
決定と実施 275  
決定とパケットのフロー 276  
構成 307  
構成コマンド  
  要約 307  
  add 308  
  change 321  
  copy 321  
  delete 321  
  disable 321  
  enable 321  
  list 321  
構成プロンプト  
  アクセス 307  
構成例 288  
除去、すべての公衆トラフィックの 300  
スキーマ 285  
生成、規則の 287  
IKE の決定 277  
IP 照会 277  
IPSec の照会 277  
IPSec/ISAKMP だけのポリシー 297  
IPSec/ISAKMP ポリシー、QOS を指定した 288  
LDAP とポリシー・データベースの対話 283  
LDAP ポリシー検索エンジン  
  構成と使用可能化 303  
RSVP の決定 278

## [マ行]

マネージャー  
  ネットワーク・ディスパッチャーの 101  
モデム・プール  
  構成 453  
戻りコード 198  
  戻りコードと説明 198

## [ヤ行]

優先待ち行列  
  説明 6  
要求が担当のキャッシュに転送され、検出されなかった  
  場合 168  
要求が担当のキャッシュに転送される場合 167  
要求がバックエンド・サーバーに転送される場合 167

要件  
  ダイヤルイン・アクセス・サーバーの 449

## [ラ行]

リモート AAA 属性 597  
  キーワード 597  
  radius 597  
  TACACS 598

## A

AAA セキュリティー  
  セキュリティ 241  
AAA 属性、リモート 597  
ACE/サーバー  
  認証 246  
activate  
  ホスト・オンデマンド・クライアント・キャッシュ監  
  視コマンド 154  
  ホスト・オンデマンド・クライアント・キャッシュ構  
  成コマンド 150  
  Web サーバー・キャッシュ監視コマンド 215  
  Web サーバー・キャッシュ構成コマンド 208  
activate-ip-precedence-filtering  
  帯域幅予約構成コマンド 26  
add  
  音声構成コマンド 580  
  ホスト・オンデマンド・クライアント・キャッシュ構  
  成コマンド 150  
  DHCP サーバー構成コマンド 504  
  MAC フィルター更新コマンド 59  
  TSF 構成コマンド 553  
  WAN 復元構成コマンド 71  
  Web サーバー・キャッシュ構成コマンド 208  
add server  
  IP セキュリティー構成コマンド 353  
add tunnel  
  IP セキュリティー構成コマンド 357  
add-circuit-class  
  帯域幅予約構成コマンド 26  
add-class  
  帯域幅予約構成コマンド 26  
AH 336  
assign  
  帯域幅予約構成コマンド 28  
assign-circuit  
  帯域幅予約構成コマンド 30  
attach  
  MAC フィルター構成コマンド 54

## B

BOOTP サーバー 479

## C

calls

音声監視コマンド 593

cert-load

PKI 監視コマンド (IPv4) 375

cert-req

PKI 監視コマンド (IPv4) 376

cert-save

PKI 監視コマンド (IPv4) 376

change

ネットワーク・アドレス変換コマンド 438

DHCP サーバー構成コマンド 510

NAT コマンド 438

change server

IP セキュリティー構成コマンド 353

change tunnel

IP セキュリティー監視コマンド 378

IP セキュリティー構成コマンド 362

change-circuit-class

帯域幅予約構成コマンド 31

change-class

帯域幅予約構成コマンド 31

circuit

帯域幅予約監視コマンド 45

帯域幅予約構成コマンド 31

clear

帯域幅予約監視コマンド 45

ホスト・オンデマンド・クライアント・キャッシュ監視コマンド 154

MAC フィルター監視コマンド 62

VCRM 監視コマンド 570

WAN 復元監視コマンド 80

Web サーバー・キャッシュ監視コマンド 216

clear-block

帯域幅予約構成コマンド 32

clear-circuit-class

帯域幅予約監視コマンド 45

counters

帯域幅予約監視コマンド 46

counters-circuit-class

帯域幅予約監視コマンド 46

create

MAC フィルター構成コマンド 54

create-super-class

帯域幅予約構成コマンド 32

## D

deactivate-ip-precedence-filtering

帯域幅予約構成コマンド 33

deassign

帯域幅予約構成コマンド 33

deassign-circuit

帯域幅予約構成コマンド 33

default

MAC フィルター構成コマンド 55

default-circuit-class

帯域幅予約構成コマンド 33

default-class

帯域幅予約構成コマンド 34

delete

音声構成コマンド 583

ネットワーク・アドレス変換コマンド 438

ホスト・オンデマンド・クライアント・キャッシュ監視コマンド 155

ホスト・オンデマンド・クライアント・キャッシュ構成コマンド 150

DHCP サーバー構成コマンド 514

IP セキュリティー監視コマンド 373

MAC フィルター更新コマンド 60

MAC フィルター構成コマンド 55

NAT コマンド 438

TSF 構成コマンド 559

Web サーバー・キャッシュ監視コマンド 216

Web サーバー・キャッシュ構成コマンド 209

delete certificate

IP セキュリティー構成コマンド 354

delete private-key

IP セキュリティー構成コマンド 354

delete server

IP セキュリティー構成コマンド 354

delete tunnel

IP セキュリティー監視コマンド 378

IP セキュリティー構成コマンド (IPv4) 363

delete-file

TSF 監視コマンド 563

del-circuit-class

帯域幅予約構成コマンド 34

del-class

帯域幅予約構成コマンド 34

detach

MAC フィルター構成コマンド 56

DHCP サーバー 475, 503

オプション

アプリケーションおよびサービス・パラメーター  
490

基本、クライアントに対して提供されている 485

形式 483



DHCP サーバー 475, 503 (続き)

ベンダー 496

リンク・レイヤー・パラメーター、インターフェースに対する 489

DHCP 拡張 492

IBM 固有の 495

IP レイヤー・パラメーター、インターフェースに対する 489

IP レイヤー・パラメーター、ホストに対する 488

TCP パラメーター 490

概念 480

概要 475

数、DHCP サーバーの 478

クライアントの移動 477

サーバー・オプションの変更 477

サンプル構成 498

特殊な DHCP クライアント 479

用語 480

リース時間 480

リースの更新 477

BOOTP サーバー 479

DHCP サーバー、複数 478

DHCP サーバー、1 台 478

DHCP サーバーとリースの パラメーター 483

DHCP の動作 475

DHCP サーバー監視コマンド

アクセス 533

disable 534

enable 534

request 535

reset 534

DHCP サーバー構成コマンド

アクセス 503

add 504

change 510

delete 514

disable 518

enable 518

list 519, 534

set 525

DIALs

グローバル監視コマンド 468

グローバル構成コマンド 459

構成コマンド 454

使用 447

ダイヤルアウト・インターフェース  
構成 452

ダイヤルイン・インターフェース  
構成 449

定義 447

DIALs (続き)

動的ドメイン名サーバー (DDNS)

説明 457

動的ホスト構成プロトコル (DHCP)

基本的な設定 456

サーバーへの複数ホップ 457

説明 455

複数サーバー・ネットワーク 457

モデム・プール

構成 453

要件 449

DIALs 監視コマンド

アクセス 468

dials コマンド 459

diffserv 396

概説 385

監視コマンド 396

clear 396

dscache 397

list 398

監視プロンプト

アクセス 396

機能、概要 385

構成 388, 391

構成コマンド

要約 391

delete 392

disable 392

enable 392

list 393

set 393

構成プロンプト

アクセス 391

用語 388

disable

帯域幅予約構成コマンド 35

ネットワーク・アドレス変換コマンド 439

ホスト・オンデマンド・クライアント・キャッシュ監視  
コマンド 155

DHCP サーバー監視コマンド 534

DHCP サーバー構成コマンド 518

IP セキュリティー監視コマンド 379

IP セキュリティー構成コマンド 363

MAC フィルター監視コマンド 63

MAC フィルター構成コマンド 56

NAT コマンド 439

WAN 復元構成コマンド 73, 80

Web サーバー・キャッシュ監視コマンド 217

disable-hpr-over-ip-port-numbers

帯域幅予約構成コマンド 35

DLSw

MAC フィルター 49

## E

ECP 暗号化

構成

PPP の 269

enable

帯域幅予約構成コマンド 35

ネットワーク・アドレス変換構成コマンド 439

ホスト・オンデマンド・クライアント・キャッシュ監視コマンド 155

DHCP サーバー監視コマンド 534

DHCP サーバー構成コマンド 518

IP セキュリティー監視コマンド 380

IP セキュリティー構成コマンド 364

MAC フィルター監視コマンド 63

MAC フィルター構成コマンド 56

NAT 構成コマンド 439

WAN 復元監視コマンド 81

WAN 復元構成コマンド 74

Web サーバー・キャッシュ監視コマンド 216

enable-hpr-over-ip-port-numbers

帯域幅予約構成コマンド 36

ES

監視 221

構成 221

ESP 337

## F

feature コマンド 553

flush

TSF 監視コマンド 563

## I

IP セキュリティー 333

アルゴリズム (IPv6) 368

インターネット・キー交換 343, 346

監視コマンド (IPv4) 373

構成 351

概説 333

概念 334

カプセル化セキュリティ・ペイロード (ESP) 337

監視 (IPv4) 373

監視 (IPv6) 383

監視、インターネット・キー交換の (IPv4) 373

監視コマンド

アクセス (IPv4) 377

アクセス (IPv6) 383

change tunnel 378

delete 373

delete tunnel 378

disable 379

IP セキュリティー 333 (続き)

監視コマンド (続き)

enable 380

list 374, 380

reset 381

set 382

stats 374, 382

監視コマンド (IPv4) 378

監視コマンド (IPv6) 384

公開キー・インフラストラクチャー 346

監視コマンド 375

構成 352

構成コマンド 353

構成 (IPv6) 367

構成、アルゴリズムの (IPv6) 368

構成、暗号化キーの (IPv4) 356

構成、キーの (IPv6) 368

構成アルゴリズム (IPv4) 356

構成コマンド

アクセス (IPv4) 356

アクセス (IPv6) 368

add server 353

add tunnel 357

change server 353

change tunnel 362

delete 354

delete private-key 354

delete server 354

delete tunnel 363

disable 363

enable 364

list 364

list certificates 355

list private-keys 355

list servers 355

set 365

構成と監視 351

手動

監視 (IPv4) 383

構成 (IPv4) 355

手動 (IPv4) 350

手動 (IPv6) 350

手動トンネル

構成 (IPv4) 366

構成 (IPv6) 369

準備、ネゴシエーションされた IP セキュリティー操作の 351

使用 333

AH と ESP 337

証明書

取得 352

セキュリティ・アソシエーション (SA) 338

IP セキュリティー 333 (続き)  
と L2TP パケット 340  
トランスポート・モード 338  
トンネル  
ネットワーク図 342  
トンネル内トンネル 341  
トンネル・モード 338  
認証ヘッダー (AH) 336  
ネゴシエーションされた 343  
メッセージ交換 345  
ネスト、プロトコルの 340  
パス MTU ディスカバリー 341  
保護トンネル 333  
用語 334

## L

L2F  
構成 413  
L2T 403  
概説 403  
構成 407  
構成コマンド  
要約 413, 416  
add 416  
disable 414, 417  
enable 414, 418  
encapsulator 414, 419  
list 414, 419  
set 415, 419  
考慮事項  
タイミング 406  
LCP 407  
サポートされるフィーチャー 405  
用語 404  
L2TP  
監視コマンド 421  
トンネル 425  
call 421  
kill 424  
memory 424  
start 425  
stop 425  
構成 413  
L2TP パケット  
と IP セキュリティー 340  
last  
帯域幅予約監視コマンド 47  
last-circuit-class  
帯域幅予約監視コマンド 47  
LDAP  
構成 307

LDAP (続き)  
構成コマンド  
要約 322  
disable 322  
enable 322  
set 325  
set default-policy 323  
set refresh 326  
list  
音声構成コマンド 583, 589  
コード化サブシステムのパラメーター (talk 5) 224  
コード化サブシステムのパラメーター (talk 6) 222  
帯域幅予約構成コマンド 38  
ネットワーク・アドレス変換監視コマンド 445  
ネットワーク・アドレス変換構成コマンド 439  
ホスト・オンデマンド・クライアント・キャッシュ監視コマンド 156  
ホスト・オンデマンド・クライアント・キャッシュ構成コマンド 151  
DHCP サーバー構成コマンド 519, 534  
IP セキュリティー監視コマンド 374, 380  
IP セキュリティー構成コマンド 364  
MAC フィルター監視コマンド 63  
MAC フィルター更新コマンド 60  
MAC フィルター構成コマンド 57  
NAT 監視コマンド 445  
NAT 構成コマンド 439  
TSF 監視コマンド 563  
TSF 構成コマンド 559  
WAN 復元監視コマンド 85  
WAN 復元構成コマンド 75  
Web サーバー・キャッシュ監視コマンド 217  
Web サーバー・キャッシュ構成コマンド 210  
list certificate  
PKI 監視コマンド (IPv4) 376  
list certificates  
IP セキュリティー構成コマンド 355  
list configured-servers  
PKI 監視コマンド (IPv4) 377  
list devices コマンド 579  
list private-keys  
IP セキュリティー構成コマンド 355  
list servers  
IP セキュリティー構成コマンド 355  
load certificate  
PKI 監視コマンド (IPv4) 377

## M

MAC フィルター  
監視プロンプトへのアクセス 61  
構成 53

## MAC フィルター (続き)

構成プロンプトへのアクセス 53

説明 49

タグの使用 51

パラメーター 50

DLSw トラフィックの 49

update サブコマンド 51

## MAC フィルター監視コマンド

アクセス 61

要約 62

clear 62

disable 63

enable 63

list 63

reinit 64

## MAC フィルター構成コマンド

アクセス 53

更新コマンド

要約 58

add 59

delete 60

list 60

move 61

set-action 61

要約 53

attach 54

create 54

default 55

delete 55

detach 56

disable 56

enable 56

list 57

move 57

reinit 57

Set-cache 58

set-cache 58

update 58

update サブコマンド 51

## map

ネットワーク・アドレス変換構成コマンド 440

NAT 構成コマンド 440

## modify

音声構成コマンド 585

ホスト・オンデマンド・クライアント・キャッシュ構成コマンド 152

ホスト・オンデマンド・クライアント・キャッシュ変更コマンド 158

TSF 構成コマンド 560

Web サーバー・キャッシュ構成コマンド 211

Web サーバー・キャッシュ変更コマンド 220

## move

MAC フィルター更新コマンド 61

MAC フィルター構成コマンド 57

## MPPE

構成 269

PPP の 271

## MS ポイントツーポイント暗号化

構成 269

PPP の 271

## N

### NAPT

使用 431

### NAT

アクセス制御規則 432

監視コマンド 445

構成 437

サンプル構成 432

使用 429

静的アドレス・マッピング 431

パケット・フィルタ 432

NAT 構成コマンド 437

### NAT コマンド

change 438

delete 438

disable 439

enable 439

list 439

map 440

reserve 441

reset 443

set 443

NAT 用のアクセス制御規則 432

NAT 用のパケット・フィルタ 432

### NFS

TFTP の使用 543

### Nuera F200 マルチプレクサー

構成 574

## P

### PPP カプセル化機能

パラメーターのデフォルト値

ダイヤルイン・インターフェースの 451

### PPP リンク

構成と監視、データ圧縮の 234

### PPTP

構成 413

## Q

queue

VCRM 監視コマンド 570

queue-length

帯域幅予約構成コマンド 40

## R

radius 597

refresh

TSF 監視コマンド 567

reinit

MAC フィルター監視コマンド 64

MAC フィルター構成コマンド 57

remove

WAN 復元構成コマンド 75

reorder-call-rule

音声構成コマンド 585

request

DHCP サーバー監視コマンド 535

reserve

ネットワーク・アドレス変換コマンド 441

NAT コマンド 441

reset

ネットワーク・アドレス変換 446

ネットワーク・アドレス変換構成コマンド 443

DHCP サーバー監視コマンド 534

IP セキュリティー監視コマンド 381

NAT 構成コマンド 443, 446

TSF 監視コマンド 567

restart

TSF 監視コマンド 567

## S

SecurID

制約 247

説明 246

set

音声構成コマンド 586, 590

コード化サブシステムのパラメーター 222

ネットワーク・アドレス変換構成コマンド 443

DHCP サーバー構成コマンド 525

IP セキュリティー監視コマンド 382

IP セキュリティー構成コマンド 365

NAT 構成コマンド 443

TSF 監視コマンド 567

TSF 構成コマンド 561

WAN 再ルート構成コマンド 76, 82

set circuit defaults

帯域幅予約構成コマンド 41

set-action

MAC フィルター更新コマンド 61

show

帯域幅予約構成コマンド 41

stats

IP セキュリティー監視コマンド 374, 382

status

音声監視コマンド 595

## T

TACACS 598

tag

帯域幅予約構成コマンド 42

Talk

OPCON コマンド 503, 533, 579, 592

talk

OPCON コマンド 459, 468, 553, 562

TN3270E サーバー 145

trace

音声監視コマンド 596

translate

ネットワーク・アドレス変換構成コマンド 444

NAT 構成コマンド 444

TSF

概説 540

構成ステップ 543

サンプル構成 546

使用 539

ファイル・キャッシュの更新 543

BootP/DHCP サーバーの構成 545

RFS の使用 542

TFTP の使用 542

TSF 用のサーバー構成 545

tsf

構成 553

TSF 監視コマンド

アクセス 562

要約 562

delete-file 563

file 563

flush 563

refresh 567

reset 567

restart 567

set 567

TSF 構成コマンド

add 553

delete 559

list 559

modify 560

set 561

tsf 構成コマンド  
要約 553

## U

untag  
帯域幅予約構成コマンド 43  
update  
MAC フィルター構成コマンド 58  
update サブコマンド  
MAC フィルター構成コマンド 51  
use circuit defaults  
帯域幅予約構成コマンド 43

## V

VCRM  
構成と監視 569  
VCRM 監視環境  
アクセス 569  
VCRM 監視コマンド  
clear 570  
queue 570  
VOFR 28

## W

WAN 再ルート  
概説 65  
構成 93  
サンプル構成 93  
説明 91  
代替リンクの構成 96  
代替リンクの割り当て 96  
ダイヤル回線の構成 96  
フレーム・リレーの構成 95  
ISDN の構成 96  
WAN 再ルート構成コマンド  
set 76, 82  
WAN 復元  
概説 65  
構成手順 68  
2 次ダイヤル回線の構成 69  
WAN 復元監視コマンド  
アクセス 79  
要約 79  
clear 80  
disable 80  
enable 81  
list 85  
WAN 復元構成コマンド  
要約 71

WAN 復元構成コマンド (続き)

add 71  
disable 73  
enable 74  
list 75  
remove 75  
Web サーバー・キャッシュ  
定義、クラスターの 113  
Web サーバー・キャッシュ監視コマンド  
activate 215  
clear 216  
delete 216  
disable 217  
enable 216  
list 217  
Web サーバー・キャッシュ構成コマンド  
activate 208  
add 208  
delete 209  
list 210  
modify 211  
Web サーバー・キャッシュの概説 159  
Web サーバー・キャッシュのコマンド 207  
Web サーバー・キャッシュの使用 159  
Web サーバー・キャッシュ変更コマンド  
modify 220





Printed in Japan

SD88-6063-01



日本アイ・ビー・エム株式会社  
〒106-8711 東京都港区六本木3-2-12



Spine information:



アクセス・インテグレーター・  
サービス

AIS V3.3 機構の使用