

Nways
マルチプロトコル・ルーティング・サービス



ソフトウェア使用者の手引き
バージョン 3.3

Nways
マルチプロトコル・ルーティング・サービス



ソフトウェア使用者の手引き
バージョン 3.3

お願い

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

本書は、IBM Nways マルチプロトコル・ルーティング・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.co.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： SC30-3681-09
Nways Multiprotocol Routing Services
Software User's Guide
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	xxi
表	xxiii
特記事項	xxvii
本書のオンライン・バージョンのご使用条件	xxvii
商標	xxvii
まえがき	xxix
本書の対象読者	xxix
ソフトウェアについて	xxix
本書における表記法	xxx
IBM 2210 Nways マルチプロトコル・ルーターの資料	xxxi
IBM 2210 ソフトウェア・ライブラリーの変更の要約	xxxi

第1部 ソフトウェアの概要および使用 1

第1章 開始	3
始める前に	3
現行リリースへの移行	3
ローカルおよびリモート・コンソールを使用してのソフトウェアへのアクセス	4
ローカル・コンソール	4
リモート・コンソール	5
リモート・ログインまたはローカル・ログイン	5
装置の再ロード	6
装置の終了	6
ユーザー・インターフェース・システムの説明	7
第1レベル・ユーザー・インターフェースの定義	7
第2章 ソフトウェアの使用	11
コマンドの入力	11
プロセスへの接続	11
プロンプトの識別	12
ヘルプの入手	13
下位レベル環境の終了	13
OPCON に戻る方法	13
構成に関する推奨事項	13
初めて構成を作成する場合	14
既存の構成に基づいて構成する場合	14
第2レベルのプロセスへのアクセス	16
構成プロセスへのアクセス、CONFIG (Talk 6)	16
コンソール動作/監視プロセスへのアクセス、GWCON (Talk 5)	17
2次 ELS コンソール・プロセスへのアクセス、ELSCON (Talk 7)	18
第3レベルのプロセスへのアクセス	18
装置の追加	18
フィーチャーの構成プロセスおよび動作プロセスへのアクセス	24
プロトコルの構成プロセスおよび動作プロセスへのアクセス	25
コマンド完成	26
コマンド完成が使用可能にされたときのオンライン・ヘルプ	27

コマンド完成が使用不可にされたときのオンライン・ヘルプ	29
コマンド活動記録	30
コマンド活動記録内のコマンドの反復	30
コマンド活動記録内の一連のコマンドの反復	30
第3章 OPCON プロセスとコマンド	33
OPCON プロセスとは	33
OPCON プロセスへのアクセス	33
OPCON コマンド	34
Configuration	34
Console	35
Diags.	35
Divert	35
Els	36
Event.	36
Flush.	36
Halt	37
Intercept.	37
Logout	38
Memory.	38
Ping	39
Reload	40
Status.	40
Suspend.	41
Talk	42
Telnet	42

第2部 基本サービスの概要、構成、および使用. 45

第4章 CONFIG プロセス (CONFIG - Talk 6) およびコマンド	47
CONFIG とは	47
Config-Only モード	48
クイック構成.	48
ユーザー・アクセスの構成.	49
予備インターフェースの構成.	50
インターフェースのリセット.	54
システム・ダンプの使用	57
CONFIG への出入り	57
CONFIG コマンド	58
Add	59
Boot	66
Change	66
Clear	73
Delete	75
Disable	77
Enable	77
Event.	80
Feature	80
List	81
Load	84
Network.	85
Patch.	86

Performance	89
Protocol	89
Qconfig	89
Set	90
System Retrieve	95
System View	96
Time	97
Unpatch	98
Update	98
Write	98
第5章 ブート CONFIG プロセス	101
ブート CONFIG とは	101
ブートの構成	101
ブート・サーバーとしての装置の使用	102
BOOTP 転送プロセスの働き	102
BOOTP クライアントとしての装置	102
BOOTP リレー・エージェントとしての装置	103
BOOTP 転送の使用可能/使用不可	103
BOOTP サーバーの構成	104
トリビアル・ファイル転送プロトコル (TFTP) の使用	104
リモート・ホストまたはルーターからの構成ファイルへのアクセス	106
IBD のファイル名の定義	106
ファイル転送時の IBD に関する考慮事項	107
複数のファイルへの大量のデータの転送	107
受信側でファイルを転送するためにブロックの最大数を指定	108
構成ロードの妥当性検査	108
特定時刻にイメージをロード	108
ダンプの構成	109
ダンプ・ファイル	109
TFTP サーバー、ブートおよびダンプ・ディレクトリー	109
ソフトウェア / コードの導入	110
第6章 ブート CONFIG の構成	113
ブート CONFIG の開始と終了	113
ブート CONFIG コマンド	113
Add	114
Change	117
Copy	119
Delete	120
Describe	121
Disable	121
Enable	122
Erase	122
List	123
Load	125
Store	127
Timedload	127
TFTP	129
第7章 ブート・オプション	133
始める前に	133

コンソール端末を使用した統合ブート装置からのブート	134
コンソール端末を使用した BOOTP	134
コンソール端末を使用した TFTP ホスト・サーバーからのブート	135
使用可能なブート・オプション	135
ブート・オプションへのアクセス	135
ブート・オプション・プロンプト	137
B (ブート)	138
BC (Config-only モードでのブート)	138
BM (コンソール照会を使用したブート)	139
BN (コンソール照会を使用したブート、実行禁止)	141
BP (BootP を使用したブート)	141
D (保管済み構成を使用したダンプ)	142
DIAG (IBM 拡張診断プログラムの実行)	143
DM (コンソール照会を使用したダンプ)	144
UB (TFTP ブート構成の表示)	144
UC (ハードウェア構成の表示)	144
UG (RAM 内アドレスでの実行)	145
LC (構成メモリーのロード)	145
CC (構成メモリーの消去)	147
ZB (ZModem ブート)	147
ZC (ZModem 構成メモリーのロード)	147
2210 の構成	148
第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド	149
GWCON とは	149
GWCON の出入り	149
GWCON コマンド	150
Activate	150
Buffer	151
Clear	152
Configuration	152
Disable	156
Enable	156
Error	157
Event	157
Feature	158
Interface	158
Memory	159
Network	161
Performance	162
Protocol	162
Queue	162
Reset	164
Statistics	164
Test	165
Uptime	166
第9章 メッセージ処理 (MONITR - Talk 2) プロセス	167
メッセージ処理 (MONITR) とは	167
メッセージ処理に影響を与えるコマンド	167
メッセージ処理 (MONITR) プロセスへの出入り	167
メッセージの受信	168

第10章 イベント・ログ・システム (ELS) の使用	169
ELS とは	169
ELS 構成環境への出入り	170
イベント・ログの概念	170
イベントの原因	170
メッセージの解釈	171
ELS の使用	174
ELS メッセージの回転の管理	174
UNIX ホスト上の Telnet 接続を使用した ELS 出力の取り込み	175
イベント・メッセージを SNMP トラップで送信できるように ELS を構成	175
ELS を使用してのトラブルシューティング	176
ELS 例 1.	176
ELS 例 2.	176
ELS 例 3.	177
ELS リモート・ログ記録の使用および構成	177
Syslog ファシリティとレベル	178
リモート・ワークステーションの構成	178
リモート・ログ記録用の 2210 の構成	180
リモート・ログ記録の出力	182
その他の考慮事項	186
ELS メッセージ・バッファの使用	187
第11章 イベント・ログ・システム (ELS) の構成および監視	189
ELS 構成環境へのアクセス	189
ELS 構成コマンド	189
Add.	190
Advanced.	190
Clear	191
Default.	191
Delete	191
Display.	191
Filter	192
List	192
Nodisplay.	194
Noremote.	195
Notrace	196
Notrap	197
Remote.	198
Set	199
Trace	204
Trap.	205
ELS ネット・フィルター構成コマンド	206
ELS メッセージ・バッファ構成コマンド	209
ELS 動作環境への出入り	213
ELS 監視コマンド	213
Advanced.	214
Clear	214
Display.	215
Files Trace TFTP	215
Filter	216
List	216
Nodisplay.	219

Noremove	219
Notrace	220
Notrap	221
Packet Trace	222
Remote	222
Remove	224
Restore	224
Retrieve	224
Save	225
Set	225
Statistics	231
Trace	233
Trap	234
View	235
パケット・トレース監視コマンド	235
ELS ネット・フィルター監視コマンド	238
ELS メッセージ・バッファ監視コマンド	241
第12章 性能の構成および監視	247
性能の概要	247
性能報告の正確度	247
性能構成環境へのアクセス	247
性能構成コマンド	248
Disable	248
Enable	248
List	249
Set	249
性能監視環境へのアクセス	249
性能監視コマンド	249
Disable	250
Enable	250
List	250
Report	250
Set	251

第3部 インターフェースの概要、構成、および動作 253

第13章 ネットワーク・インターフェースの開始	255
先に進む前に	255
ネットワーク・インターフェースと GWCON インターフェース・コマンド	255
ネットワーク・インターフェースの構成プロセスおよびコンソール・プロセスへのアクセス	255
リンク・レイヤー・プロトコルの構成プロセスおよびコンソール・プロセスへのアクセス	256
予備インターフェースの定義	256
第14章 IEEE 802.5 トークンリング・ネットワーク・インターフェースの構成	257
トークンリング・インターフェース構成プロセスへのアクセス	257
トークンリング構成コマンド	257
List	258
LLC	258
Media	259

Packet-Size	259
Set	259
Source-routing	260
speed	261
インターフェース監視プロセスへのアクセス	261
トークンリング・インターフェース監視コマンド	261
Dump	262
LLC.	262
トークンリング・インターフェースと GWCON インターフェース・コマンド	263
802.5 トークンリング・インターフェースについて表示される統計	263
第15章 LLC インターフェースの構成および監視.	267
インターフェース構成プロセスへのアクセス	267
LLC 構成コマンド	267
List	268
Set	269
インターフェース監視プロセスへのアクセス	271
LLC 監視コマンド	271
Clear-Counters	271
List	271
Set	277
第16章 イーサネット・ネットワーク・インターフェースの使用	279
インターフェース・コマンドによるイーサネット統計の表示.	279
第17章 イーサネット・ネットワーク・インターフェースの構成および監視	283
イーサネット・インターフェース構成プロセスへのアクセス.	283
イーサネット構成コマンド	283
Connector-Type.	284
IP-Encapsulation	284
List	284
Physical-Address	284
イーサネット・インターフェース動作プロセスへのアクセス.	285
イーサネット・インターフェース監視コマンド.	285
Collisions	286
第18章 LAN エミュレーションの概説.	287
LAN エミュレーションの利点	287
LAN エミュレーションのコンポーネント.	288
ATM でのアドレッシング	289
ESI	290
LAN エミュレーション・コンポーネントの ATM アドレス	291
関連 ILMI 機能の概説.	291
信号バージョンの手動による構成.	292
ILMI の使用による LECS の探索.	292
LECS 機能の概説.	292
LECS 割り当てポリシーの使用例.	294
TLV に関するその他の情報.	296
LES への接続	297
アドレス登録	298
アドレス解決	298
BUS への接続.	299
BUS 機能	300

データ・ダイレクト VCC の確立	300
LAN エミュレーションの拡張機能の概説	301
ブロードキャスト・マネージャー	301
IP の BCM サポート	302
IPX の BCM サポート	302
NetBIOS の BCM サポート	303
ソース・ルート・ブリッジングの BCM サポート	303
LAN エミュレーションの信頼性	304
LAN エミュレーションのセキュリティー	305
LAN エミュレーションの主要な構成パラメーター	307
第19章 ATM の使用	309
ATM および LAN エミュレーション	309
アドレスを入力する方法	309
ATM-LLC 多重化	310
ATM バーチャル・インターフェースの概念	310
ATM バーチャル・インターフェースの使用による利点	311
ATM バーチャル・インターフェースの使用による不利益	312
第20章 ATM の構成および監視	313
ATM インターフェース構成プロセスへのアクセス	313
ATM 構成コマンド	314
ATM インターフェース構成コマンド	314
Add	315
List	315
QoS 構成	316
Remove	316
Set	316
Enable	320
Disable	321
バーチャル ATM インターフェース構成プロセスへのアクセス	321
ATM バーチャル・インターフェース構成コマンド	321
Add	322
List	322
Remove	322
ATM 監視プロセスへのアクセス	323
ATM 監視コマンド	323
Interface	323
ATM-LLC	324
ATM インターフェース監視コマンド (ATM INTERFACE+ プロンプト)	324
List	324
Trace	325
Wrap	326
ATM-LLC 監視コマンド	327
List	327
ATM バーチャル・インターフェース監視コマンド	327
第21章 LAN エミュレーション・クライアントの使用	329
LAN エミュレーション・クライアントの概要	329
第22章 LAN エミュレーション・クライアントの構成および監視	331
LAN エミュレーション・クライアントの構成	331
Add	331

Config	332
List	332
Remove	332
ATM フォーラム準拠 LE クライアントの構成	333
ARP Configuration	333
Frame	336
IP-Encapsulation (イーサネット ATM フォーラム準拠 LEC の場合のみ)	336
List	337
LLC.	337
QoS.	337
RIF-Timer (トークンリング・フォーラム準拠 LEC の場合のみ)	337
Set	337
Source-Routing (トークンリング・フォーラム準拠 LEC の場合のみ)	349
LLC 構成コマンド	350
List	350
Set	350
LEC 監視環境へのアクセス	351
LEC 監視コマンド	352
List	353
LLC.	356
MIB.	357
QoS Information	361
Trace	361
LLC 監視コマンド	362
List	362
Set	362
第23章 シリアル・ライン・インターフェースの構成	365
インターフェース構成プロセスへのアクセス	365
クロックおよびケーブルのタイプ	365
ネットワーク・インターフェースおよび GWCON インターフェース・コマンド	366
第24章 X.25 ネットワーク・インターフェースの使用	367
基本構成手順	367
ナショナル・パーソナリティの設定	368
X.25 のデフォルト値について	368
マルチカプセル化	370
制限	370
構成変更	370
マルチカプセル化および閉域ユーザー・グループ (CUG) の構成	371
閉域ユーザー・グループの概要	372
相互形閉域ユーザー・グループ	373
拡張閉域ユーザー・グループのタイプ	373
装置上に閉域ユーザー・グループをもつ X.25 回線の確立	373
X.25 閉域ユーザー・グループの構成	374
第25章 X.25 ネットワーク・インターフェースの構成および監視	377
X.25 構成コマンド	377
Set	378
Enable	383
Disable.	384
National Enable.	385

National Disable	387
National Set	388
National Restore	393
Add	394
Change	401
Delete	403
List	404
インターフェース監視プロセスへのアクセス	407
X.25 監視コマンド	407
List	408
Parameters	408
Reset	409
Statistics	410
X.25 ネットワーク・インターフェースおよび GWCON インターフェース・コ マンド	411
X.25 インターフェースに関して表示される統計	411
第26章 XTP の使用	415
X.25 トランスポート・プロトコル	415
構成情報	416
DTE アドレス・ワイルドカード	418
XTP バックアップ・ピア機能	418
リモート DTE の検索	418
接続要求タイマー	419
ローカル XTP	419
XTP と閉域ユーザー・グループ	420
XTP の構成	420
構成手順	420
データ・リンクの設定	421
IP インターフェースの構成	422
X.25 の構成	422
ナショナル・パーソナリティーの設定	424
IP アドレスの定義	424
内部 IP アドレスの設定	424
XTP の構成	424
リモート・ルーターのサンプル構成	426
第27章 XTP の構成および監視	429
XTP 構成コマンド	429
Add	429
Change	432
Delete	433
Enable	434
Disable	434
Set	434
List	434
XTP 監視コマンド	436
Add	437
Delete	437
List	438
第28章 フレーム・リレー・インターフェースの使用	443

フレーム・リレーの概説	443
フレーム・リレー・ネットワーク	444
フレーム・リレー・スイッチド・バーチャル・サーキット	445
フレーム・リレー・インターフェースの初期化	445
オーファン回線	447
フレーム・リレー・インターフェースの状態に影響を与える PVC 状態の構成	448
フレーム・リレーのフレーム	448
フレーム・リレー・ネットワークを介したフレーム転送	450
プロトコル・アドレス	451
マルチキャスト・エミュレーションとプロトコル・ブロードキャスト	451
フレーム・リレー・ネットワーク管理	452
管理状態報告書	452
全状態報告書	453
リンク整合性検証報告書	453
統合リンク・レイヤー・マネージメント (CLLM)	453
フレーム・リレー・データ速度	454
認定情報速度 (CIR)	454
オーファン・パーマネント・バーチャル・サーキットの CIR	454
認定バースト (Bc) サイズ	454
超過バースト (Be) サイズ	455
回線速度	455
最小情報速度	456
最大情報速度	456
可変情報速度	456
回線輻輳	457
CIR の監視	457
輻輳監視	457
輻輳通知と回避	458
フレーム・リレーを介する帯域幅予約	460
フレーム・リレー・インターフェースを介する断片化	460
フレーム・リレーを介しての音声転送	461
フレーム・リレー構成プロンプトの表示	462
フレーム・リレー基本構成手順	462
フレーム・リレー PVC マネージメントの使用可能化	463
フレーム・リレー SVC マネージメントの使用可能化	464
第29章 フレーム・リレー・インターフェースの構成および監視	465
フレーム・リレー構成コマンド	465
Add	466
Change	475
Disable	476
Enable	478
List	485
LLC	492
Remove	492
Set	494
フレーム・リレー監視プロンプトへのアクセス	500
フレーム・リレー監視コマンド	500
Clear	501
Disable	501
Enable	501

List	502
LLC	512
Notrace	512
Set	513
Trace	514
フレーム・リレー・インターフェースおよび GWCON インターフェース・コマンド	515
フレーム・リレー・インターフェースについて表示される統計	515
第30章 ポイント・ポイント・プロトコル・インターフェースの使用	519
PPP の概説	519
PPP データ・リンク・レイヤー・フレーム構造	520
PPP リンク制御プロトコル (LCP)	522
LCP パケット	523
リンク確立パケット	524
リンク終了パケット	526
リンク保守パケット	526
PPP 認証プロトコル	526
パスワード認証プロトコル (PAP)	527
チャレンジ/ハンドシェイク認証プロトコル (CHAP)	528
Microsoft PPP CHAP 認証 (MS-CHAP)	528
Shiva パスワード認証プロトコル (SPAP)	528
PPP 認証の構成	529
PPP コールバックの構成	530
PPP を用いた AAA の使用	531
PPP ネットワーク制御プロトコル	532
AppleTalk 制御プロトコル	532
Banyan VINES 制御プロトコル	532
Bridging Control Protocol	532
コールバック制御プロトコル	533
DECnet IV 制御プロトコル	533
IP 制御プロトコル	533
IPv6 制御プロトコル	534
IPX 制御プロトコル	535
OSI 制御プロトコル	535
APPN HPR 制御プロトコル	535
APPN ISR 制御プロトコル	535
バーチャル・コネクションの使用および構成	535
VC の考慮事項	535
VC の構成	536
第31章 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	539
インターフェース構成プロセスへのアクセス	539
PPP インターフェース構成プロンプトへのアクセス	540
ポイント・ポイント構成コマンド	540
Disable	540
Enable	542
List	544
LLC	549
Set	549
インターフェース監視プロセスへのアクセス	560

ポイント・ポイント監視コマンド	560
Clear	561
List	561
LLC	585
ポイント・ポイント・プロトコル・インターフェースと GWCON インターフェ ース・コマンド	585
第32章 マルチリンク PPP プロトコルの使用	589
MP の考慮事項	590
マルチシャシー MP	591
マルチリンク PPP インターフェースの構成	591
PPP ダイアル回線での MP の構成	591
PPP シリアル・リンクでの MP の構成	592
レイヤー 2 トンネル伝送ネット上での MP の構成	593
マルチシャシー MP の構成	593
第33章 マルチプロトコル PPP プロトコル (MP) の構成および監視	595
MP 構成プロンプトへのアクセス	595
マルチリンク PPP インターフェースの MP 構成コマンド	595
Disable	596
Enable	596
Encapsulator	596
List	596
Set	597
MP インターフェース状態の監視	599
MP 監視コマンドへのアクセス	599
マルチリンク PPP プロトコル監視コマンド	600
List	600
第34章 SDLC リレーの構成および監視	605
SDLC リレーの概要	605
基本構成手順	607
動的再構成	607
SDLC リレー構成環境へのアクセス	608
SDLC リレー構成コマンド	608
Add	608
Delete	610
Disable	610
Enable	611
List (ネットワーク SRLY の場合)	611
List (プロトコル SDLC リレーの場合)	612
Set	614
SDLC リレー監視環境へのアクセス	616
SDLC リレー監視コマンド	617
Clear-Port-Statistics	617
Disable	617
Enable	618
List	618
SDLC リレー・インターフェースおよび GWCON インターフェース・コマン ド	620
第35章 SDLC インターフェースの使用	621
基本構成手順	621

交換 SDLC コールイン・インターフェースの構成	621
SDLC 構成要件	623
第36章 SDLC インターフェースの構成および監視	625
SDLC 構成環境へのアクセス	625
SDLC 構成コマンド	626
Add	627
Delete	628
Disable	628
Enable	629
List	629
Set	632
SDLC 監視環境へのアクセス	639
SDLC 監視コマンド	640
Add	640
Clear	641
Delete	641
Disable	641
Enable	641
List	642
Msgsz	645
Set	645
Test	649
SDLC インターフェースおよび GWCON インターフェース・コマンド	650
SDLC インターフェースで表示される統計	650
第37章 バイナリー同期リレー (BRLY) の使用	653
BRLY の概要	653
BRLY 構成のサンプル	654
BRLY の考慮事項	657
第38章 BSC リレーの構成および監視	659
基本構成手順	659
BSC リレー構成コマンド	660
Add	660
Delete	662
Disable	663
Enable	663
List (ネットワーク BSC の場合)	664
List (プロトコル BRLY の場合)	665
Set	665
BSC リレー監視環境へのアクセス	668
BSC リレー監視コマンド	669
Clear	669
Disable	669
Enable	670
List	670
BSC リレー・インターフェースおよび GWCON インターフェース・コマンド	672
第39章 V.25bis ネットワーク・インターフェースの使用	673
始める前に	673
構成手順	673
V.25bis アドレスの追加	673

V.25bis インターフェースの構成	674
ダイヤル回線の追加	675
ダイヤル回線の構成	675
第40章 V.25bis ネットワーク・インターフェースの構成および監視	679
インターフェース構成プロセスへのアクセス	679
V.25bis 構成コマンド	679
List	680
Set	681
インターフェース監視プロセスへのアクセス	684
V.25bis 監視コマンド	684
Calls	684
Circuits	685
Parameters	686
Statistics	687
V.25bis と GWCON コマンド	689
V.25bis インターフェースおよびダイヤル回線の統計	689
第41章 V.34 ネットワーク・インターフェースの使用	693
始める前に	693
構成手順	693
V.34 アドレスの追加	693
V.34 インターフェースの構成	694
ダイヤル回線の追加	695
ダイヤル回線の構成	696
第42章 V.34 ネットワーク・インターフェースの構成および監視	699
インターフェース構成プロセスへのアクセス	699
V.34 構成コマンド	699
List	700
Set	701
インターフェース監視プロセスへのアクセス	703
V.34 監視コマンド	704
Calls	704
Circuits	705
Parameters	706
Statistics	707
V.34 と GWCON コマンド	709
V.34 インターフェースおよびダイヤル回線の統計	709
第43章 ISDN インターフェースの使用	713
ISDN の概説	713
ISDN アダプターとインターフェース	714
ダイヤル回線	714
アドレッシング	715
過剰加入および回線の競合	716
デマンド回線を介したコスト制御	716
コーラー ID および LID	716
ISDN 原因符号	717
サンプル ISDN 構成	719
ISDN を介するフレーム・リレー構成	719
WAN 復元の構成	719
チャンネル化 T1/E1	720

ISDN インターフェースの要件と制約	721
サポートされるスイッチ/サービス	721
ISDN インターフェースの制約事項	721
ダイヤル回線の構成要件	721
始める前に	721
構成手順	722
ISDN アドレスの追加	722
ISDN パラメーターの構成	722
ISDN インターフェースの構成	724
ダイヤル回線の追加	725
ダイヤル回線の構成	725
I.431 スwitchの機種	727
ネイティブ I.431 サポート	727
第44章 ISDN インターフェースの構成および監視	729
ISDN 構成コマンド	729
Block-Calls	729
List	730
Remove	730
Set	730
Cause Code	734
インターフェース監視プロセスへのアクセス	735
ISDN 監視コマンド	735
Block-Calls	736
Calls	736
Channels	737
Circuits	737
Dial-dump.	738
L2_Counters	738
L3_Counters	738
TEI	738
Parameters	739
Statistics	739
ISDN と GWCON コマンド	740
Interface -- ISDN インターフェースとダイヤル回線の統計	740
Configuration - ルーターのハードウェアおよびソフトウェアに関する情報	742
第45章 ダイヤル回線の構成および監視	743
ダイヤル回線構成コマンド	743
Delete	744
Encapsulator	744
List	745
Set	747
ダイヤル回線監視コマンド	750
Callback	750
第4部 付録および後付け	753
付録A. クイック構成リファレンス	755
クイック構成に関する注記	755
選択	755
終了とリスタート	756

完了	756
クイック構成プログラムの開始	756
LAN エミュレーションの構成	757
ブリッジングの構成	757
プロトコルの構成	759
IP の構成	759
IPX の構成	761
DECnet (DNA) の構成	764
IBM 2210 のリスタート	766
付録B. X.25 ナショナル・パーソナリティ	767
GTE-Telenet	767
DDN	767
付録C. 複数のディスクからのルーター・ロード・ファイルの作成	769
DOS でのロード・ファイルのアセンブル	769
UNIX でのロード・ファイルのアセンブル	769
DOS でのロード・ファイルの分割	770
UNIX でのロード・ファイルの分割	771
略語集	773
用語集	783
索引	815



1. マルチプロトコル・ルーティング・サービス	8
2. プロセスとコマンドの関係	8
3. メモリーの使用状況	39
4. イベントによって生成されるメッセージ	171
5. Syslog メッセージ記述	177
6. syslog.conf 構成ファイル	180
7. リモート・ログ記録用の 2210 の構成	181
8. リモート・ログ記録用のサブシステムおよびイベントの構成	182
9. Syslog News Info ファイルの内容の例	183
10. Talk 2 からの出力	184
11. Syslog_user_alert ファイルの内容の例	184
12. 静的 ARP 項目の設定例	185
13. Syslog 出力内の反復シーケンス番号の例	186
14. 単純な LAN エミュレーション・ネットワークの物理図と論理図	288
15. LE クライアントと LES 間のデフォルト接続	298
16. LE クライアント (LEC) と BUS 間のデフォルト接続	299
17. LAN エミュレーションの冗長度	304
18. 閉域ユーザー・グループのヌル・カプセル化	372
19. XTP の使用前と使用後の構成	416
20. サンプル XTP 構成	421
21. フレーム・リレー・ネットワーク内の DLCI	444
22. フレーム・リレー・ネットワーク内の DLCI	446
23. オーフアン回線	447
24. フレーム・リレーのフレーム・フォーマット	449
25. 輻輳通知と減速	459
26. ポイント・ポイント・リンクの例	520
27. PPP フレーム構造	521
28. LCP フレーム構造 (PPP 情報フィールド内の)	523
29. マルチシャシー MP	593
30. SDLC リレー構成の例	606
31. 物理 BSC リレー構成	653
32. バーチャル BSC リレー・マルチポイント構成	654
33. バーチャルおよび物理 BRLY マルチポイント構成の組み合わせ	654
34. ルーター A の BRLY 構成 (ルーター A で入力されたコマンド)	656
35. ルーター B の BRLY 構成 (ルーター B で入力されたコマンド)	657
36. ルーター C の BRLY 構成 (ルーター C で入力されたコマンド)	657
37. ISDN を介するフレーム・リレー構成	719
38. WAN 復元のための ISDN の使用	720

一 表

1. プロセス、目的、アクセスするコマンド	12
2. ネットワーク体系とサポートされるインターフェース	22
3. OPCON コマンド	34
4. Quick Config 機能	48
5. CONFIG コマンドの要約	58
6. アクセス許可	65
7. IBM 2210 フィーチャー番号と名前	80
8. Set Prompt Level コマンドによって提供される追加機能	94
9. インターフェースのデフォルトおよび最大設定値	95
10. ファイル名の拡張子に関する規則	107
11. ブート CONFIG コマンド	113
12. Add Boot Entry パラメーター	115
13. ブート方式の説明	133
14. ブート・オプション	136
15. ブート・オプション・プロンプト	137
16. GWCON コマンドの要約	150
17. ログ・レベル	172
18. パケット完了コード (エラー・コード)	173
19. ELS 構成コマンドの要約	189
20. ELS ネット・フィルタ構成コマンド	206
21. ELS メッセージ・バッファ構成コマンド	209
22. ELS 監視コマンドの要約	213
23. パケット・トレース監視コマンドの要約	235
24. ELS ネット・フィルタ監視コマンド	238
25. ELS メッセージ・バッファ監視コマンド	241
26. PERF 構成コマンドの要約	248
27. PERF 監視コマンドの要約	249
28. トークンリング構成コマンドの要約	257
29. トークンリング 4/16 の有効なパケット・サイズ	259
30. トークンリング監視コマンドの要約	261
31. LLC 構成コマンドの要約	267
32. LLC 監視コマンドの要約	271
33. イーサネット構成コマンドの要約	283
34. イーサネット構成コマンドの要約	285
35. ATM 構成コマンドの要約	314
36. ATM INTERFACE 構成コマンドの要約	315
37. ATM バーチャル・インターフェース構成コマンドの要約	321
38. ATM 構成コマンドの要約	323
39. ATM INTERFACE 監視コマンドの要約	324
40. ATM LLC 構成コマンドの要約	327
41. LAN EMULATION クライアント構成コマンドの要約	331
42. LAN エミュレーション・クライアントの構成コマンドの要約	333
43. ATM LAN エミュレーション・クライアント ARP 構成コマンドの要約	334
44. ATM LAN エミュレーション・クライアント ARP 構成コマンドの要約	335
45. LLC コマンドの要約	350
46. LE クライアント監視コマンドの要約	352
47. LLC 監視コマンドの要約	362
48. Set コマンド	368

49. National Enable パラメーター	369
50. National Set パラメーター	369
51. 閉域ユーザー・グループの着信 X.25 回線の確立	374
52. X.25 構成コマンドの要約	377
53. 内部クロックが 2210 インターフェースに使用されるとき の回線速度	382
54. 外部クロックが 2210 インターフェースに使用されるとき の回線速度	382
55. VC 定義の例	383
56. X.25 監視コマンドの要約	407
57. XTP 構成コマンドの要約	429
58. XTP 監視コマンドの要約	436
59. プロトコル・アドレス・マッピング	451
60. フレーム・リレー・マネージメント・オプション	463
61. フレーム・リレー構成コマンドの要約	465
62. 2210 インターフェースに内部クロックが使用されるとき の回線速度	498
63. 2210 インターフェースに外部クロックが使用されるとき の回線速度	498
64. フレーム・リレー・マネージメント・オプション	499
65. 2210 シリアル・インターフェースの転送遅延の単位と範囲	500
66. フレーム・リレー監視コマンドの要約	500
67. LCP パケット符号	523
68. ポイント・ポイント構成コマンドの要約	540
69. 2210 インターフェースのケーブル・タイプ	552
70. 2210 インターフェースに内部クロックが使用されるとき の回線速度	554
71. 2210 インターフェースに外部クロックが使用されるとき の回線速度	554
72. ポイント・ポイント監視コマンドの要約	561
73. MP 構成コマンド	595
74. MP 監視コマンド	600
75. SDLC リレー構成コマンドの要約	608
76. 2210 インターフェースのケーブル・タイプ	614
77. Set Frame-Size コマンドのフレーム・サイズの有効値	615
78. 2210 インターフェースに内部クロックが使用されるとき の回線速度	615
79. 2210 インターフェースに外部クロックが使用されるとき の回線速度	616
80. SDLC リレー監視コマンドの要約	617
81. SDLC 構成コマンドの要約	626
82. 2210 インターフェースのケーブル・タイプ	633
83. Link Frame-Size コマンドのフレーム・サイズの有効値	634
84. 2210 インターフェースに内部クロックが使用されるとき の回線速度	637
85. 2210 インターフェースに外部クロックを使用するとき の回線速度	637
86. SDLC 監視コマンドの要約	640
87. BSC リレー構成コマンドの要約	660
88. 2210 インターフェースのケーブル・タイプ	666
89. Set Frame-Size コマンドのフレーム・サイズの有効値	667
90. 2210 インターフェースに内部クロックが使用されるとき の回線速度	668
91. 2210 インターフェースに外部クロックが使用されるとき の回線速度	668
92. BSC リレー監視コマンドの要約	669
93. V.25bis 構成コマンドの要約	679
94. V.25bis 監視コマンドの要約	684
95. V.34 構成コマンドの要約	699
96. V.34 監視コマンドの要約	704
97. ISDN Q.931 原因符号	717
98. ISDN 構成コマンドの要約	729
99. ISDN Cause Codes コマンドの要約	734
100. ISDN 監視コマンドの要約	735

101. ダイヤル回線構成コマンドの要約	743
102. ダイヤル回線監視コマンドの要約	750

特記事項

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

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

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

本書のオンライン・バージョンのご使用条件

弊社は、お客様に対して以下のことを許諾します。

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

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

商標

以下の用語は、米国あるいはその他の国々における IBM 社の商標です。

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

UNIX は、米国およびその他の国における登録商標であり、X/Open Company Limited がライセンスを専有しています。

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、Nways 装置 に導入された マルチプロトコル・ルーティング・サービス の基本コード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。本書は、以下のプロセスおよび操作を行うのに役立ちます。

- マルチプロトコル・ルーティング・サービス の基本コードの構成、監視、および使用。
- Nways 装置 によってサポートされるインターフェースおよびリンク・レイヤー・ソフトウェアの構成、監視、および使用。

本書は、に説明されている 2210 用のソフトウェア・ライブラリーの第 1 巻です。特定の Nways 装置は、ライブラリー内で説明されているすべてのフィーチャーおよび機能をサポートしてはおりません。フィーチャーまたは機能が装置に固有である場合、その制限が、関係資料に示されているか、本書のまえがきの表に示されています。

本書では 2210 のことを“ルーター”または“装置”と呼んでいます。ライブラリーにある例は、2210 の構成を表していますが、実際の出力はライブラリーとは異なる場合があります。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・ネットワークのハードウェアおよびソフトウェアを扱った経験があれば役に立ちますが、プロトコル・ソフトウェアを使用する上では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。追加情報をご利用頂ける場合、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 Nways マルチプロトコル・ルーティング・サービスは、**** NOT 2210 **** (ライセンス・プログラム番号 5765-C90) をサポートするソフトウェアです。このソフトウェアには、以下に挙げる構成要素が含まれています。

- 基本コード (次のものからできています。)
 - 装置に対してブリッジング、データ・リンク・スイッチ、および SNMP エージェントの各機能を提供するコード
 - 装置に導入されているマルチプロトコル・ルーティング・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に、あるいは 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されます。

基本コードは工場で 2210 に導入済みです。

- IBM Nways マルチプロトコル・ルーティング・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びます)。これは、独立型ワークステーションから装置を構成できるようにするグラフィカル・ユーザー・インターフェースです。構成プログラムにはエラー検査およびオンライン・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はいません。ソフトウェア受注の一環として、装置とは別に出荷されます。

IBM Nways マルチプロトコル・ルーティング・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・ページから入手することもできます。サーバー・アドレスおよびディレクトリーについては、Nways マルチプロトコル / アクセス・サービス製品 構成プログラム使用者の手引き、GC88-6657 を参照してください。

本書における表記法

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

1. コマンドの省略形は、以下の例に示すように下線が付いています。

```
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、オプションの省略時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 UTP に省略時設定されます。

5. キーボードのキーの組み合わせは、以下のように表示されます。

- **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表します。状況によっては、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、次のように表示されます。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されます。たとえば、次のように入力します。

File Name: *filename.ext*

IBM 2210 Nways マルチプロトコル・ルーターの資料

ライブラリーの再編成: バージョン 3.2 から始まって、ライブラリーの編成への以下の変更が行なわれました。

- ソフトウェア使用者の手引き にあった**フィーチャーの理解、使用および構成**という表題の情報は、新しい資料である **フィーチャーの使用と構成** に移動しました。
- DIAL フィーチャーの使用、構成、および監視に関する章は、**フィーチャーの使用と構成** の資料に移動しました。

情報の更新と訂正: 資料が印刷された後に実施された技術変更、説明、および修正を常に把握しておくためには、以下のアドレスで IBM 2210 のホーム・ページをご覧ください。

<http://www.networking.ibm.com/220/220prod.html>

IBM 2210 ソフトウェア・ライブラリーの変更の要約

以下のリストは、バージョン 3.3 で行なわれたソフトウェアの変更に適用されます。変更の内容は、以下のとおりです。

• 新しい機能

- サブシステムの符号化 (ES)
- 動的ホスト構成プロトコル (DHCP) サービス
- 仮想私設ネットワーク (VPN)
 - ディレクトリー・サービス: Lightweight Directory Access Protocol (LDAP) サポート
 - ISAKMP/Oakley サポート
 - 層 2 転送 (L2F)
 - ポイント・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・パケット断片化
- フレーム・リレーを介しての音声パケット転送

• 拡張機能

- IP 拡張
 - 汎用 IPv4 ルーティング・ポリシー
 - IPv6 パケット・フィルター、動的再構成、および DHCP リレー・エージェント・サポート
- SDLC 拡張

変更の要約

- 1 次グループ・ポーリング
- 両方向同時通信
- ルーター内で待ち行列に入れられた非セッション・メッセージの制御を可能にする DLSw 構成パラメーター
- シン・サーバー機能用の性能拡張
- TN3270 拡張
 - IBM eNetwork ホスト・オンデマンド・クライアント・キャッシュ
 - ホストで開始される動的 LU 定義
 - DLSw を介しての複数の PU SAs
- ブリッジング拡張
 - IPX SR-TB サポート
- X.25 動的再構成サポート
- IPX 拡張
 - 構成可能な RIP ティック
 - フレーム・リレー SVC を介しての IPXWAN
- コマンド行インターフェースのコマンド完成機能
- Web サーバー・キャッシュ拡張
 - 外部キャッシュ制御マネージャー
 - 拡張容易性・可用性拡張

• 説明と訂正

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

第1部 ソフトウェアの概要および使用

第1章 開始

この章では、IBM 2210 Nways マルチプロトコル・ルーター (2210) およびマルチプロトコル・ルーティング・サービスに関連する以下のコンポーネントの使用を開始する方法について説明します。

- 装置コンソール端末
- 装置ソフトウェア (マルチプロトコル・ルーティング・サービス)
- 装置ソフトウェア・ユーザー・インターフェース

この章は、以下の節に分かれています。

- 『始める前に』
- 4ページの『ローカルおよびリモート・コンソールを使用してのソフトウェアへのアクセス』
- 7ページの『ユーザー・インターフェース・システムの説明』

始める前に

開始する前に、以下のチェックリストを参照して、装置が正しく導入されているかどうかを確認してください。

チェックリスト...

- 必要なハードウェアはすべて導入済みですか。
- コンソール端末 (ビデオ端末) は装置に接続してありますか。

重要: サービス・ポート接続端末を使用して IBM 2210 の構成または監視を行い、サービス端末が読み取り不能である場合は、構成の中のいくつかのパラメーターを変更する必要があります。

ハードウェア資料を参照してください。

- 装置は、該当するネットワーク・インターフェースやケーブルを使用してネットワークに接続してありますか。
- 必要なハードウェア診断はすべて実行しましたか。

これらの手順について詳しくは、*IBM 2210 Nways マルチプロトコル・ルーター 設置と初期構成の手引き*を参照してください。

現行リリースへの移行

新しいコード・レベルへの移行についての詳細は、*IBM 2210 Nways Multiprotocol Router Service and Maintenance Manual* を参照してください。

ローカルおよびリモート・コンソールを使用してのソフトウェアへのアクセス

装置コンソールから装置ユーザー・インターフェースを使用して、装置のネットワーク・ソフトウェアの機能の監視や変更を行うことができます。装置はローカル・コンソールおよびリモート・コンソールをサポートしています。

ローカル・コンソール

ローカル・コンソールは、EIA 232 (RS-232) ケーブルによって直接接続されるか、あるいはモデムを介して装置に接続されます。初期ソフトウェア導入時に、ローカル・コンソールを使用することが必要になる場合があります。初期セットアップ接続の後には、IP 転送が使用可能になっている限り、Telnet を介して接続することができます。(IP 転送を使用可能にする方法の詳細については、プロトコルの構成と監視解説書を参照してください。)

構成した装置を初めて始動すると、画面にブート・メッセージが表示され、続いてオペレーターのコンソール (OPERATOR'S CONSOLE) つまり OPCON プロンプト (*) が表示されます。* プロンプトは装置が OPCON コマンドを受信する準備ができていることを示しています。

2210 サービス・ポートに接続された ASCII 端末を使用して、最初にその構成を行う必要があります。

重要: 不要情報、ランダム文字、逆疑問符、または端末を 2210 サービス・ポートに接続できないなどの問題が生じる場合、さまざまな原因が考えられます。以下に、それらの原因の一部のものをリストします。

- サービス・コンソール上に不要情報またはランダム文字が生じる最も一般的な原因は、ボー・レートが IBM 2210 と同期していないことです。

2210 が特定のボー・レートに設定されている場合、端末または端末エミュレーターは、それと同じボー・レートに設定する必要があります。

IBM 2210 が通信速度自動選択 (これがデフォルト) に設定されている場合は、端末の break キー・シーケンスを押して **Enter** を押します。

PC 端末エミュレーターの一般的な BREAK キー・シーケンスは Alt-B です (端末エミュレーターの資料を参照してください)。ASCII 端末はほとんどに **Break** キーが付いています (しばしば **Ctrl** キーと一緒に使用されます)。

詳しくは、ハードウェアの資料を参照してください。

- 端末または装置 (AC) の接地の欠陥
- 端末と IBM 2210 間の EIA 232 (RS-232) ケーブルの欠陥、不適正なシールド、または不適正な接地
- 端末または端末エミュレーターの欠陥
- IBM 2210 システム・ボードの欠陥
- 高レベルの電磁気干渉 (EMI)
- 送電線外乱

2210 が初期構成された後は、IP が使用可能である限り、装置の操作にローカル・コンソールを使う必要はありません。

装置ソフトウェアによって、コンソールの活動は自動的に処理されます。ソフトウェアをアップグレードするときには、ローカル・コンソールを使用することが必要になる場合もあります。ローカル・コンソールの接続と構成についての情報は、*IBM 2210 Nways マルチプロトコル・ルーター 設置と初期構成の手引き*を参照してください。

リモート・コンソール

リモート・コンソールは、標準リモート端末プロトコルを使用して、装置に接続されます。リモート・コンソールの機能は、ローカル・コンソールの場合と同じですが、`configuration`. 1つの装置上で同時に2台までリモート・コンソールを使用することができます。リモート・コンソールはTelnet接続を介して装置に接続することができます。このフィーチャーの使用不可を選択できるオプションがあります。

Telnet 接続

装置は、Telnet クライアントと Telnet サーバーの両方をサポートします。装置上のリモート・コンソールが Telnet サーバーの役を務めます。OPCON (*) プロセスで `telnet` コマンドを使用して、装置から別の装置またはホストに接続するときは、装置は Telnet クライアントの役を務めます。

リモート・ログイン名およびパスワード

リモート・ログイン時には、装置はプロンプトによって、ログイン名およびパスワードの入力を指示します。リモート・コンソールから装置にログインするときは、装置の `status` コマンドを使用することによって、ログイン名を表示することができます。

リモート・ログインまたはローカル・ログイン

ローカル・コンソールへのログインは、ホスト・システム上で Telnet を開始し、装置に接続する必要がある点を除けば、リモート・コンソールへのログインの場合と同じです。リモート・ログインの場合は、1ステップから始めます。ローカル・ログインの場合は、3ステップから始めます。

リモート・コンソールからログインする場合は、次のようにします。

1. ホスト・システム上で Telnet を開始して、装置に接続する。ホスト・システムとは、リモート端末が接続されているシステムのことです。
2. 装置の名前またはインターネット・プロトコル (IP) アドレスを提供する。
装置名を使用する場合は、ネットワークにネーム・サーバーがあることが必要です。次の例に示すように、装置名または IP アドレスを出します。

```
% telnet brandenburg
```

または

```
% telnet 128.185.132.43
```

ここまでは、リモート・ログインとローカル・ログインには相違はありません。

3. プロンプトで指示されたら、ログイン名とパスワードを入力する。

Login:
Password:

ログイン名はあるがパスワードはないということもあり得ます。パスワードは、装置へのアクセスを制御します。パスワードが設定されていない場合は、Password: プロンプトで **Enter** キーを押します。ログインは自動的に設定されません。セキュリティのために、CONFIG プロセスで **add user** コマンドを使用して、ユーザー名とパスワードを設定することができます。詳細については、65 ページの **add user** 構成コマンドを参照してください。再ロードして、変更をアクティブにするのを忘れないでください。

注: 初期プロンプトが表示されてから 1 分以内にログイン名と有効なパスワードを入力しなかった場合、または間違ったパスワードを 3 回連続して入力した場合、装置は Telnet 接続を切断します。

4. **Enter** キーを押して、メイン・プロンプトのアスタリスク (*) を表示する。
Enter キーを数回押すか、または **Ctrl-P** を押さないと、* プロンプトが表示されないことがあります。

この段階に達すれば、キーボードからのコマンドの入力を始めることができます。コマンド行に入力した最後の文字を削除するときは **後退** キーを押します。コマンド行の入力全体を削除してコマンドを再入力できるようにするには、**削除** キーまたは **Ctrl-U** を押します。詳細については、26 ページの『コマンド完成』および 30 ページの『コマンド活動記録』を参照してください。

Telnet クライアント上でローカル Telnet コマンドを使用して、Telnet 接続をクローズすることもできます。

注: VT100 端末を使用している場合、**後退** キーを押すと目に見えない文字が挿入されるので、このキーは押さないようにしてください。その代わりに、**削除** キーを使用してください。

5. 『装置の終了』の説明に従って、装置を終了します。

装置の再ロード

reload コマンドは、メモリーから構成の新しいコピーをロードすることで、装置をリブートするのに使用します。動的に構成可能でない、ユーザーが構成可能なパラメーターを変更するたびに、その変更が有効になるには装置を再ロードする必要があります。たとえば、次のように入力します。

* **reload**

The configuration has been changed, save it? (Yes or [No] or Abort)

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

装置の終了

* プロンプトに戻り、**logout** コマンドを使用して、Telnet 接続をクローズします。たとえば、次のように入力します。

```
IP Config> exit  
Config> Ctrl-P  
* logout  
  
%
```


Telnet クライアント上でローカル Telnet コマンドを使用して、Telnet 接続をクローズすることもできます。

ユーザー・インターフェース・システムの説明

このソフトウェアは、さまざまなプロセスおよびハードウェア装置間の CPU の使用をスケジュールするマルチタスク処理システムです。装置ソフトウェアは、次のようなものです。

- タイミングおよびメモリ管理を行い、ユーザーが装置の動作パラメーターの表示および変更を行うことができる、ローカルとリモートの両方のオペレーター・コンソールをサポートします。
- さまざまなユーザー・インターフェース・プロセス、すべてのネットワーク・インターフェース・ドライバー、および装置と共に購入されたすべてのプロトコル転送プログラムを含む、機能モジュールで構成されます。

第 1 レベル・ユーザー・インターフェースの定義

ソフトウェアへのユーザー・インターフェースは、メイン・メニュー (プロセス) といくつかの補助メニュー (プロセス) で構成されます。これらのメニューは、ソフトウェアの複数のレベルのプロセスに関連しています。

第 1 レベルのプロセスは、OPCON プロセスと CONFIG-ONLY プロセスから成っています。ほとんどの場合、OPCON プロセスを使用して第 2 レベルにアクセスし、IBM 2210 で実行する基本サービス、フィーチャー、インターフェース、およびプロトコルを構成または操作します。

第 2 レベルには、構成 (CONFIG)、コンソール (GWCON)、およびイベント・ログ・システム (MONITR) などのプロセスが含まれます。これらの第 2 レベルのプロセスにアクセスするには、OPCON コマンドである **configuration**、**console**、または **event** を使用することもできます。あるいは、**status** コマンドを使用して、第 2 レベルのプロセスをリストしてから、**talk pid** コマンドを使用して第 2 レベルのプロセスにアクセスすることもできます。ソフトウェア内には使用できないプロセスもあります。プロセスの概要については、12ページの表1 を参照してください。

8ページの図1 は、各種のプロセスを示し、装置ソフトウェアの構造内でのそれらの配置を示しています。

ルーター・ソフトウェア・プロセス

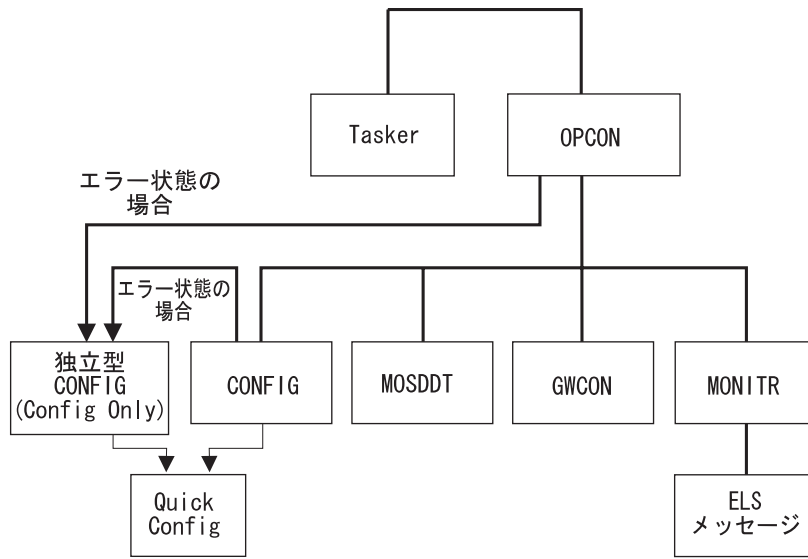


図1. マルチプロトコル・ルーティング・サービス

図2 は、さまざまなプロセス・レベル間の関係の例を示しています。

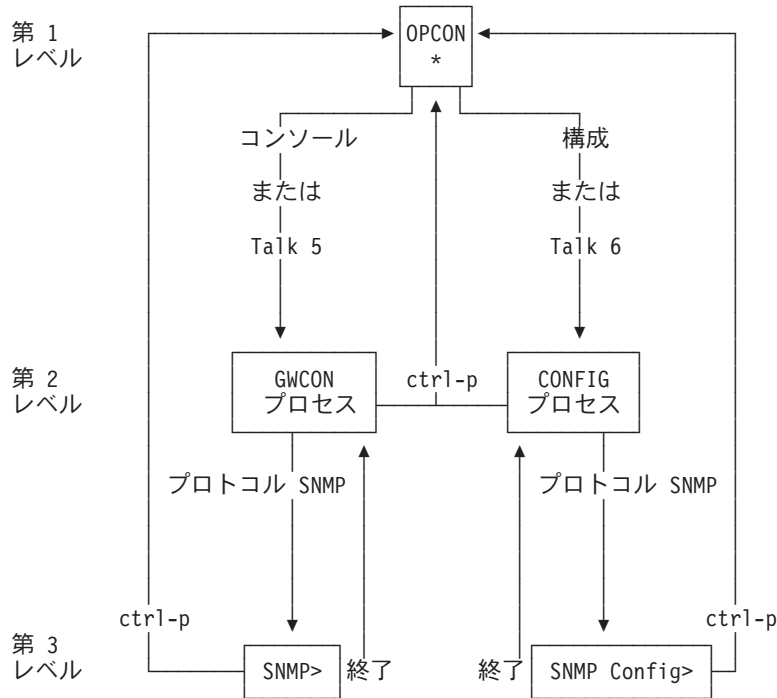


図2. プロセスとコマンドの関係

注: 図2 には、各プロセス・レベルにアクセスしたり、各プロセス・レベルから戻ったりするのに使用される種々のコマンドも示されています。

OPCON についての詳細は、33ページの『OPCON プロセスとは』を参照し、CONFIG-ONLY についての詳細は、48ページの『Config-Only モード』を参照してください。

ROPCON プロセスは、リモート・コンソールからの処理を行うもので、基本的には OPCON プロセスと同じです。

クイック構成プロセス

クイック構成 (つまり、Quick Config) では、特定のオペレーティング・システム・コマンドを処理しなくても、装置の部分を即時に構成することができます。構成をもたない装置を初期ロードまたは再ロードすると、Config-Only に入り、そのプロセスから Quick Config メニューにアクセスできます。装置に装置が構成されており、その装置にプロトコルが構成されていない場合、装置は自動的に Config-Only でスタートし、その後で Quick Config に入ります。

また、CONFIG プロセスから **qconfig** コマンドを使用して Quick Config に入ることもできます。

システム・セキュリティー

add user コマンドを使用して、ログイン許可をもつ複数のユーザーを追加することができます。セキュリティー問題についての詳細、および **set password** コマンドと **add user** コマンドの説明は、49ページの『ユーザー・アクセスの構成』を参照してください。

第2章 ソフトウェアの使用

この章では、ソフトウェアの使用法について説明します。この章は次の各節に分かれています。

- 『コマンドの入力』
- 『プロセスへの接続』
- 13ページの『構成に関する推奨事項』
- 16ページの『第 2 レベルのプロセスへのアクセス』
- 18ページの『第 3 レベルのプロセスへのアクセス』
- 26ページの『コマンド完成』
- 30ページの『コマンド活動記録』

コマンドの入力

コマンドを入力する場合は、以下の点に留意します。

- 入力できるコマンドの中で、そのコマンドを固有に識別するのに十分な文字数を順次に入力することもできます。たとえば、**reload** コマンドを実行する場合は、最小限として **rel** と入力する必要があります。コマンド構文について説明した章で、必要な最小文字数を下線で示してあります。
- コマンドは大文字・小文字の区別をしません。
- コマンド（および後続のオプション）の先頭文字を入力するだけで、コマンドを実行できる場合があります。たとえば、* プロンプトで **s** と入力し、その後続けて **Enter** キーを押すだけで、**status** コマンドが実行されます。
- コマンド完成が使用可能にされている場合、Esc を押して **?** を入力し、コマンドの入力についてのヘルプを入手することができます。詳細については、26ページの『コマンド完成』および 30ページの『コマンド活動記録』を参照してください。

プロセスへの接続

装置を開始すると、コンソールにブート・メッセージが表示されます。次に、OPCON プロンプト (*) が画面に表示され、これで OPCON プロセスに入ったので OPCON コマンドの入力を開始できることが示されます。これが異なるプロセスとの通信を行うコマンド・プロンプトになります。

頻繁に必要とされるコマンドは、『- - - -』の区切り記号の前に表示されます。OPCON プロンプト (*) で該当するコマンドを入力します。コマンドのリストについては、34ページの表3 を参照してください。

あるいは、次のようにすることができます。

1. * プロンプトで **status** コマンドを入力して、プロセスのプロセス ID (PID) 番号を見つける。

status コマンドは、プロセス ID (PID)、プロセス名、およびプロセスの状態など、装置プロセスに関する情報を表示します。 **status** コマンドを出すと、次の例のような表示が得られます。

```
* status
Pid Name      Status TTY  Comments
1  COpCn1    RDY   TTY0
2  Monitr    DET   --
3  Tasker    RDY   --
4  MOSDBG    DET   --
5  CGWCon    DET   --
6  Config    DET   --
7  ELScon    DET   --
8  ROpCn1    IDL   TTY1 128.185.210.125
9  ROpCn2    IDL   TTY2
```

2. **talk pid** コマンドを使用する。ただし、*pid* は、接続したいプロセスの番号です。(これらのコマンドおよび他の OPCON コマンドの詳細については、33ページの『OPCON プロセスとは』を参照してください。)

注: リストされたどのプロセスにもユーザー・インターフェースがあるとは限りません (たとえば、**talk 3** プロセス)。**talk 4** コマンドは、IBM サービス技術員が使用するためのものです。

プロンプトの識別

各プロセスは、それぞれ異なるプロンプトを使用します。プロンプトを見れば、コンソールが接続されているプロセスがわかります。(**talk pid** コマンドを入力したときにプロンプトが表示されない場合は、再度 **Enter** を押します。)

以下のリストは、5 つのメイン・プロセスのプロンプトを示しています。

表 1. プロセス、目的、アクセスするコマンド

プロセス	レベルと目的	アクセスするためのコマンド	入力プロンプト
OPCON	レベル 1 - すべての 2 次レベルへのアクセス	Ctrl-P	アスタリスク (*)
CONFIG	レベル 2 - 基本サービスの構成、および第 3 レベルの構成へのアクセス	Configuration または talk 6	Config >
GWCON	レベル 2 - 基本サービスの動作と監視、および第 3 レベルの動作と監視へのアクセス	Console または talk 5	正符号 (+)
MONITR	レベル 2 - メッセージの表示	Event または talk 2	(なし)
ELSCon	レベル 2 - 直接監視および ELS コンソールへのアクセス	els または talk 7	ELS Secondary Console>
MOSDBG	レベル 2 - 診断環境	talk 4	db>
DIAGS	レベル 2 - ハードウェア診断の実行	diags	

注: **talk 4** コマンドの入力は、サービス技術員の指示のもとで行ってください。

OPCON プロンプト・レベルで、キーボードからコマンドの入力を開始できます。コマンド行に入力した最後の文字を削除するときは **後退** キーを使用します。コマンド行の入力全体を削除してコマンドを再入力できるようにするには、**Ctrl-U** を使用しま

す。詳細については、26ページの『コマンド完成』および 30ページの『コマンド活動記録』を参照するか、**Escape ?** を押します。

ヘルプの入手

コマンド・プロンプトでは、そのレベルで利用可能なコマンドのリストという形でヘルプを得ることができます。このためには、**? (help コマンド)** を入力して、**Enter** を押します。**?** は、現行プロンプト・レベルから利用可能なコマンドをリストするのに使用します。通常は特定のコマンド名の後に **?** を入力すると、そのオプションをリストすることもできます。

下位レベル環境の終了

ソフトウェアは複数レベルの構造になっているので、2210 を構成または動作するときには、2 次、3 次、およびさらに下位レベルの環境に入ります。すぐ上のレベルに戻るためには、**exit** コマンドを入力します。2 次レベルに達するためには、2 次レベルのプロンプト (Config> または +) が得られるまで繰り返し **exit** を入力します。

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

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

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

OPCON に戻る方法

OPCON プロンプト (*) に戻るには、**Ctrl-P** を押します。OPCON に戻ってからでなければ、別のプロセスと通信することはできません。たとえば、コンソール (GWCON) プロセスに接続されているときに CONFIG プロセスに接続したい場合、まず **Ctrl-P** を押して OPCON に戻る必要があります。**Ctrl-P** キーの組み合わせは、デフォルトのインターセプト文字 です。

第 3 レベル以下のレベルのプロセスからインターセプト文字を使用して、* プロンプトに戻った場合、次回に **talk** コマンドを使用して同じプロセスとトークすると、再び同じレベルのメニューに入ります。装置を再初期化すると、このリンクはなくなります。

構成に関する推奨事項

2210 の構成は、初めて構成するのか、既存の構成に基づいて構成を作成するのか、あるいは構成を更新するだけなのかによって異なります。以下の節は、ユーザーのニーズに応じて、最良の手順を使用するためのガイドとして使用してください。

初めて構成を作成する場合

この手順は、構成する 2210 と似たような構成をもつ 2210 が他に存在しないものと想定しています。また、2210 を箱から取り出したばかりであることも想定しています。この手順は順序付けて示してありますが、実際の構成は (ステップ 3 以降) どのような順序で行っても構いません。

IBM 2210 を初めて構成する場合は、次のようにします。

1. 構成する 2210 を調べて、どのインターフェースを構成する必要があるか確認する。これは後で使用するので、メモしておいてください。
2. 4ページの『ローカルおよびリモート・コンソールを使用してのソフトウェアへのアクセス』の説明に従って、2210 に接続する。
3. 最初に、48ページの『クイック構成』または 755ページの『付録A. クイック構成リファレンス』で説明している Quick Config を使用して、2210 のポートと少なくとも装置の内部 IP アドレスを構成する。装置に Telnet 通信を行なうために必要な最小構成を行います。
4. 基本サービス (ブート・オプションなど) を構成する。16ページの『構成プロセスへのアクセス、CONFIG (Talk 6)』の説明に従って、構成プロセスにアクセスします。
5. インターフェースを構成する。19ページの『ネットワーク・インターフェース構成プロセスへのアクセス』の説明に従って、インターフェース構成プロセスにアクセスします。
6. 必要なフィーチャーを構成する。24ページの『フィーチャーの構成プロセスおよび動作プロセスへのアクセス』の説明に従って、フィーチャー構成プロセスにアクセスします。
7. この装置を通して実行するプロトコルを構成する。25ページの『プロトコルの構成プロセスおよび動作プロセスへのアクセス』の説明に従って、プロトコル構成プロセスにアクセスします。

注: 最小限として、このステップで IP を構成します。

8. 6ページの『装置の再ロード』の説明に従って、装置を再ロードする。

既存の構成に基づいて構成する場合

この節では、以下の方法について説明します。

- 稼働中の 2210 の構成に基づいて構成する
- 2210 の構成を永続的に更新する
- 2210 の稼働時に、2210 の構成を一時的に更新する

既存の構成に基づく構成

新規の 2210 に構成したいものと同じインターフェース、フィーチャー、およびプロトコルを使用している 2210 がすでに存在する場合は、既存の 2210 に基づいて構成することにより、時間を節約することができます。このタイプの構成は、コマンド行インターフェースまたは 2210 に付属の構成プログラムのいずれかを使用して行うことができます。いずれの場合も、2210 は実動ネットワークに組み込まれていないものと想定しています。

コマンド行インターフェースを使用して、既存の構成に基づいて構成する場合は、以下の手順で行います。

1. 使用したい構成のコピーを入手する。
 - a. OPCON (*) プロンプトで **talk 6** と入力する。
 - b. Config> プロンプトで **boot** と入力する。
 - c. Boot config> プロンプトで **copy configuration file** コマンドを入力する。詳細については、101ページの『第5章 ブート CONFIG プロセス』を参照してください。
2. 構成する 2210 に接続する。
3. 1ステップで入手した構成を、 TFTP GET を使用して 2210 にロードする。101ページの『第5章 ブート CONFIG プロセス』を参照してください。
4. 構成を更新する。
5. 構成を書き込む。47ページの『CONFIG とは』を参照してください。
6. 2210 を再ロードする。

構成プログラムを使用して、既存の構成に基づいて構成する場合は、以下の手順で行います。

1. 構成プログラムを開始する。
2. 新規の構成の基にする 2210 から構成を取り出す。
3. 新規の構成のために必要な変更を行う。この変更には、アドレス、ホスト名、ユーザー、およびその他の項目が含まれます。
4. 構成を、取り出した元の名前とは別の名前前で保管する。
5. この構成を、構成する 2210 に送信する。
6. 2210 を再ロードする。

構成プログラムの使用について詳しくは、*Nways* マルチプロトコル / アクセス・サービス製品 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。

構成の永続的な更新

構成を永続的に更新する場合は、以下の手順で行います。

1. 4ページの『ローカルおよびリモート・コンソールを使用してのソフトウェアへのアクセス』の説明に従って、更新する 2210 にアクセスする。* プロンプトが表示されます。
2. **talk 6** コマンドを入力して、構成プロセスにアクセスする。
3. 該当するコマンドを入力して、変更する領域の構成を行う第 3 レベルのプロセスにアクセスする。
4. **exit** を必要な回数入力して、構成プロセスに戻る。
5. 構成を書き込む。47ページの『CONFIG とは』を参照してください。
6. 2210 を再ロードする。

構成の一時的な更新

構成を永続的に更新できるようになるまで、2210 の一部の動作特性を変更できるように、構成を一時的に更新することができます。この機能により、ただちに変更を行

って、問題の解決や性能の向上を図り、ピーク期間中の停止を回避することが可能になります。後で構成の永続的な更新を行い、停止をスケジュールし、`reload`して、変更を有効にすることができます。

構成を一時的に更新するには、以下の手順で行います。

1. 4ページの『ローカルおよびリモート・コンソールを使用してのソフトウェアへのアクセス』の説明に従って、更新する 2210 にアクセスする。* プロンプトが表示されます。
2. **talk 5** コマンドを入力して、動作/監視プロセスにアクセスする。

注: すべてのインターフェース・タイプ、プロトコル、または機能で、`talk 5` コマンドを使って一時的構成変更を行うことができるわけではありません。

3. 該当するコマンドを入力して、変更する領域を監視する第 3 レベルのプロセスにアクセスする。
4. **exit** を必要な回数入力して、動作/監視プロセスに戻る。
5. **Ctrl-P** を入力して、* プロンプトに戻る。
6. 6ページの『装置の終了』の説明に従って、装置を終了する。

第 2 レベルのプロセスへのアクセス

すべてのインターフェース、フィーチャー、およびプロトコルには、以下のプロセスにアクセスするためのコマンドがあります。

- インターフェース、フィーチャー、またはプロトコルを初期構成して使用可能にしたり、後で構成変更を行うための構成プロセス
- 各インターフェース、フィーチャー、またはプロトコルに関する情報を表示したり、構成を一時的に変更したり、あるいは構成変更をアクティブにしたりするための動作/監視プロセス

また、一部の基本システム・サービスも、第 2 レベル・プロセスを通して構成または動作することができます。これらの機能を実行するためのコマンドについての説明は、47ページの『CONFIG とは』から始まります。

次の節では、第 2 プロセスにアクセスする手順について説明します。

構成プロセスへのアクセス、CONFIG (Talk 6)

各プロトコル構成プロセスには、装置の CONFIG プロセスを通してアクセスします。CONFIG は装置ユーザー・インターフェースの第 2 レベルのプロセスで、第 3 レベルのプロセスとの通信を可能にします。第 3 レベルのプロセスの例としては、プロトコル・プロセスがあります。

CONFIG コマンド・インターフェースは、いくつかのメニューで構成されています。プロトコル構成コマンド・インターフェースは、CONFIG インターフェースの内のメニューです。各プロトコル構成インターフェースには、それぞれ独自のプロンプトがあります。たとえば、SNMP プロトコル・コマンド・インターフェースのプロンプトは `SNMP config>` です。

以下の項では、これらの手順についてさらに詳細に説明します。

CONFIG プロセスに入る方法

OPCON から CONFIG プロセスに入り、CONFIG プロンプトを表示させるには、**configuration** コマンドを入力します。あるいは、OPCON **talk** コマンドと PID を入力して、CONFIG を表示させることもできます。CONFIG の PID は 6 です。

* **configuration**

または

* **talk 6**

コンソールに CONFIG プロンプト (Config>) が表示されます。このプロンプトが表示されない場合は、再度 **Enter** キーを押してください。

クイック構成プロセス: クイック構成 (つまり、Quick Config) では、特定のオペレーティング・システム・コマンドを処理しなくても、装置の部分を即時に構成することができます。CONFIG プロセスから **qconfig** コマンドを使用すると、Quick Config メニューに入ります (48ページの『クイック構成』を参照してください)。

装置の再ロード

CONFIG を介してプロトコル・パラメーターに対して行なわれる変更は、動的変更を含むネットを起動するか、あるいは装置ソフトウェアを再ロードするまでは、有効になりません。

注: 変更を装置のフラッシュ・メモリーに保管するには、**write** コマンドを入力する必要があります。

コンソール動作/監視プロセスへのアクセス、GWCON (Talk 5)

インターフェース、フィーチャー、またはプロトコルに関する情報を表示したり、実行中にパラメーターを変更したりするためには、動作 (監視) プロセスにアクセスし、これを使用して行うことが必要です。動作コマンド・インターフェースは、GWCON インターフェースのモードです。GWCON モード内では、各インターフェース、フィーチャー、またはプロトコル・インターフェースには、それぞれ独自のプロンプトがあります。たとえば、SNMP プロトコルのプロンプトは **SNMP>** です。

注: このプロセスで変更したパラメーターは、2210 の動作コードを再ロードすることが必要になったイベント (電源異常など) の後、あるいは**reload** コマンドを入力した後は、アクティブのままにはなりません。

以下の項では、これらの手順についてさらに詳細に説明します。

GWCON コマンド・プロセスに入る方法

OPCON から GWCON プロセスに入り、GWCON プロンプトを表示させるには、**console** コマンドを入力します。あるいは、**talk** コマンドと PID を入力して、GWCON を表示させることもできます。GWCON の PID は 5 です。たとえば、次のように入力します。

* **console**

または

* talk 5

これにより、GWCON プロンプト (+) がコンソールに表示されます。このプロンプトが表示されない場合は、再度 **Enter** を押してください。

2 次 ELS コンソール・プロセスへのアクセス、ELSCon (Talk 7)

2 次 ELS コンソールを使うと、GWCON の現行の状態を中断することなく GWCON talk 5 ELS に便利にアクセスすることができます。talk 5 で **ping** の最中であるか、talk 5 メニュー構造の奥深くで、GWCON の現行の状態を中断することなく、ELS を制御したいとします。2 次 ELS コンソール (Talk 7) は、この目的に役立ちます。

OPCON から2 次 ELS 制御 (ELSCon) プロセスに入り、2 次 ELS コンソール・プロンプトを表示させるには、**els** コマンドを入力します。あるいは、**talk 7** コマンドを入力することもできます。

次の例では、**ping** コマンドの実行中に別の ELS イベントが表示されます。

注: OPCON プロンプト (*) を表示させるには、インターセプト文字 (デフォルトでは Ctrl-P) が使用されます。

```
*talk 5
+protocol ip
IP>ping 10.0.0.9
PING 10.0.0.2 -> 10.0.0.9: 56 data bytes, ttl=64, every 1 sec.
```

*talk 7

```
ELS Secondary Console>display event ip.7
Complete
ELS Secondary Console>
*talk 2
00:20:48 IP.007: 10.0.0.2 -> 10.0.0.9
00:20:49 IP.007: 10.0.0.2 -> 10.0.0.9
```

第 3 レベルのプロセスへのアクセス

第 2 レベルにアクセスした後で、IBM 2210 のインターフェース、フィーチャー、およびプロトコルを構成または動作するために、第 3 レベルでコマンドを入力する必要があります。以下の節では、第 3 レベルのプロセスにアクセスする方法について説明します。

装置の追加

この節では、**add device** コマンドを使用してネットワーク・インターフェースを構成する方法について説明します。ネットワーク・インターフェースは、通常はアダプターですが、動作プロセスによって使用される定義である場合もあります。たとえば、1 つのポートに 2 つの IP アドレスを割り当てることができ、どちらのアドレスもインターフェースと見なされます。**add device** コマンドを使用してインターフェースを確立した後、ネットワーク・インターフェースの構成プロセスや動作プロセス (たとえば、Talk 5 監視プロセス) にアクセスすることができます。これらのプ

プロセスを使用して、装置内で使用されるネットワーク・インターフェースの、ソフトウェアで構成可能なパラメーターを変更したり、監視したりします。

ネットワーク・インターフェース構成プロセスへのアクセス

装置の構成プロセスにアクセスするには、以下の手順を使用します。このプロセスにより、特定のインターフェースの構成 プロセスにアクセスすることができます。

1. OPCODE プロンプトで、**configuration** コマンドを入力する。

```
* configuration
```

configuration コマンドを入力すると、CONFIG プロンプト (Config>) がコンソールに表示されます。最初に **configuration** と入力したときにこのプロンプトが表示されない場合は、**Enter** をもう一度押してください。

add device コマンドを使用して、ネットワーク・インターフェースを作成します。**add device** コマンドは、自動的にインターフェース番号を割り当てます。(add device ? と入力すると、サポートされる装置タイプのリストが表示されません。)

サポートされている装置のタイプは、次のとおりです。

- a. マルチポート・アダプター

add device コマンドを使ってマルチポート・アダプターの装置名を指定すると、アダプターのスロット番号およびインターフェース用に使用したいアダプターのポート番号を入力するよう求められます。

アダプター上の複数のポートを使用したい場合は、add device コマンドを複数回入力し、そのたびに異なるポート番号を指定する必要があります。

たとえば、スロット 7 内の 8 ポート X.21 アダプター上のポート 0 と 1 のインターフェースを作成するには、次のようなコマンドを入力することになります。

```
Config> add device x21
Device Slot #(1-8) [1]? 7
Device Port #(0-7) [0]? 0
Defaulting Data-link protocol to PPP
Adding X.21 PPP device in slot 7 port 0 as interface #6
Use "set data-link" command to change the data-link protocol
Use "net 6" to configure X.21 PPP parameters
```

```
Config> add device x21
Device Slot #(1-8) [1]? 7
Device Port #(0-7) [0]? 1
Defaulting Data-Link protocol to PPP
Adding X.21 PPP device in slot 7 port 1 as interface #7
Use "set data-link" command to change the data-link protocol
Use "net 7" to configure X.21 PPP parameters
```

注: シリアル・アダプターのポート番号は 0 ベースです。他のすべてのマルチポート・アダプターのポート番号は 1 ベースです。

4 ポート ISDN チャネル化 T1 および E1 アダプターでは、1 つの **add device** コマンドを使って複数のポートを構成することができます。これらのアダプターの 1 つを追加すると、ソフトウェアが、追加するポートの範囲を入力するよう促します。次の例は、ダイヤルイン・ネットを使用しているスロット 4 に 4 ポート ISDN チャネル化 T1 および E1 アダプターを追加する方法を示しています。

```

Device Slot #(1-8) [1]? 3
Device Port Range (1-8)
  Lowest Port #(1) [1]? 2
  Highest Port #(8) [8]? 2
Automatically add dial-in nets for this base net? (Yes or [No]): yes
Automatically enable IP for these dial-in nets?(Yes or [No]): yes
Enable as a Multilink PPP link?(Yes or [No]): yes
Adding 23 dial-in nets on top of base net 14
Adding 8-port ISDN Primary T1/J1 devices in slot 3 port 2 as interfaces #14.
Use "net 14" to configure 8-port ISDN Primary T1/J1 parameters.

```

b. 単一ポート・アダプター

add device コマンドを使って単一ポート・アダプターの装置名を指定すると、アダプターのスロット番号を入力するよう促されます。

次の例では、スロット 2 内の 1 ポート ISDN-PRI T1/J1 アダプターにインターフェースを追加します。

```

Config> add device t1-isdn
Device Slot #(1-8) [1]? 2
Adding ISDN Primary T1/J1 device in slot 2 port 1 as interface #7
Use "net 7" to configure ISDN Primary T1/J1 parameters

```

c. ダイヤル回線

次の例は、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
Enter the number of PPP Dial Circuit interfaces [1]?
Adding device as interface 8
Base net for this circuit[0]?4
Defaulting Data-link protocol to PPP
Use "set data-link" command to change the data-link protocol
Use "net 8" command to configure circuit parameters

```

d. 次の例は、ダイヤルイン回線を追加します。

```

Config>add device dial-in
Enter the number of dial-in interfaces [1]?
Adding device as interface 5
Base net for this circuit [0]? 5
Defaulting Data-link protocol to PPP
Use "set data-link" command to change the data-link protocol
Use "net 5" command to configure circuit parameters

```

e. マルチリンク PPP

次の例は、マルチリンク PPP インターフェースを追加します。

```

Config>add device multilink-ppp
Enter the number of Multilink PPP interfaces [1]?
Adding device as interface 7
Defaulting Data-link protocol to PPP
Use "net 7" command to configure circuit parameters

```

注:

- a. シリアル・アダプターまたはダイヤル回線用のインターフェースを作成する場合、デフォルトのデータ・リンク・タイプは PPP になりますが、**set data-link** コマンドを使用して、データ・リンク・タイプを変更することができます。シリアル・ポートおよびダイヤル回線でサポートされるデータ・リンク・タイプについては 22 ページの表 2 を参照し、90 ページの **set data-link** コマンドの説明をお読みください。

2. Config> プロンプトで、**list devices** コマンドを入力して、装置が現在構成されているネットワーク・インターフェース番号を次のように表示します。

```
Config> list devices
```

```

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
Ifc 6 Ethernet            Slot: 5 Port: 1
Ifc 7 Ethernet            Slot: 5 Port: 2

```

Ifc 8 Ethernet	Slot: 6	Port: 1
Ifc 9 Ethernet	Slot: 6	Port: 2
Ifc 10 V.35/V.36 Frame Relay	Slot: 8	Port: 0
Ifc 11 V.35/V.36 X.25	Slot: 8	Port: 1
Ifc 12 V.35/V.36 PPP	Slot: 8	Port: 2
Ifc 13 V.35/V.36 PPP	Slot: 8	Port: 3
Ifc 14 V.35/V.36 PPP	Slot: 8	Port: 4
Ifc 15 V.35/V.36 PPP	Slot: 8	Port: 5

3. インターフェース番号を記録する。
4. CONFIG **network** コマンドと、構成するインターフェースの番号を入力する。たとえば、次のように入力します。

```
Config> network 1
```

これで、該当する構成プロンプト（たとえば、トークンリングの場合は TKR Config>）がコンソールに表示されます。

注: ネットワーク・インターフェースは、すべてがユーザーによる構成が可能とは限りません。構成できないインターフェースの場合は、次のようなメッセージが出ます。

```
That network is not configurable
```

IBM 2216 装置サポートの制約事項: IBM 2216 に装置を追加するときは、以下の規則が適用されます。

- 2 つまでの ATM インターフェースを定義することができます。
- 8 つまでの ISDN-PRI インターフェースを定義できますが、次の制約があります。
 - 4 つ以下の 1 ポート・アダプターを使用することができる
 - 1 つ以上の 4 ポート ISDN チャネル化 T1 および E1 アダプターを使用することができる
- LAN 装置をスロット 3、4、7、または 8 に追加すると、ペアの他方のスロットは使用不可になります。たとえば、LAN 装置をスロット 4 に追加すると、スロット 3 は使用不可になります。同様に、装置をスロット 3 に追加すると、スロット 4 は使用不可にされます。LAN 装置をスロット 7 および 8 に追加するにも、同じ規則が適用されます。
- V.35/V.36 アダプターは V.35 ケーブルまたは V.36 ケーブルのいずれかを使用する必要があります。V.35/V.36 アダプターに接続される多分岐ケーブルのタイプは、どのタイプのケーブル (V.35 または V.36) を使用できるかを決定します。

インターフェース構成の表示: 同じインターフェース構成プロンプトから、**list** コマンドを使用して、選択したインターフェースに特定の構成情報をリストすることができます。たとえば、次のように入力します。

```
TKR Config> list
```

```
Token-Ring configuration:
```

```
PACKET SIZE (INFO FIELD): 4472
Speed: 16 Mb/sec
Media: Shielded
```

```
RIF Aging Timer: 120 Source Routing: Enabled
MAC Address: 000000000000
```

ネットワーク・インターフェースの構成: IBM 2210 のネットワーク・インターフェースの構成についての詳しい情報は、本書の該当する章を参照してください。

表2 は、ネットワーク体系と各体系でサポートされるインターフェースをリストしています。

表2. ネットワーク体系とサポートされるインターフェース

ネットワーク体系	サポートされるインターフェース
ATM	1 ポート ATM 25-Mbps MMF 1 ポート ATM 25-Mbps SMF
802.5 トークンリング	2 ポート・トークンリング
イーサネット	<ul style="list-style-type: none"> • 1 ポート 10/100-Mbps イーサネット • 2 ポート 10-Mbps イーサネット
ISDN	<ul style="list-style-type: none"> • 1 ポート ISDN-PRI (T1/J1) * • 1 ポート ISDN-PRI (E1) * • 4 ポート ISDN チャネル化 T1 および E1 * <p>注:</p> <p>1. アスタリスク (*) が付いているインターフェースは、ISDN またはチャネル化インターフェースとして使用できます。</p>
ポイント・ポイント	8 ポート V.24/EIA 232E、6 ポート V.35/V.36、8 ポート X.21、1 ポート HSSI、およびダイヤル回線インターフェース
フレーム・リレー	8 ポート V.24/EIA 232E、6 ポート V.35/V.36、8 ポート X.21、1 ポート HSSI、およびダイヤル回線インターフェース
X.25	8 ポート V.24/EIA 232E、6 ポート V.35/V.36、および 8 ポート X.21 アダプター
SDLC リレー	8 ポート V.24/EIA 232E、6 ポート V.35/V.36、および 8 ポート X.21
SDLC	8 ポート V.24/EIA 232E、6 ポート V.35/V.36、8 ポート X.21、およびダイヤル回線インターフェース
V.25bis	8 ポート V.24/EIA 232E
ダイヤルイン	PPP ダイアル回線インターフェース。構成パラメーターのデフォルトでは DIAL をサポートする
マルチリンク PPP (MP)	任意の PPP リンクでサポート
ESCON チャネル・アダプター	LAN チャネル・ステーション (LCS)、リンク・サービス・アーキテクチャー (LSA)、およびマルチ・パス・チャネル+ (MPC+)
並列チャネル・アダプター	LAN チャネル・ステーション (LCS)、リンク・サービス・アーキテクチャー (LSA)、およびマルチ・パス・チャネル+ (MPC+)
L2TP、L2F、および PPTP	レイヤー 2 トンネル・プロトコル (L2TP)、レイヤー 2 転送 (L2F)、およびポイント・ポイント・トンネル・プロトコル (PPTP) を通じてのバーチャル PPP DIAL 接続をサポートします。
FDDI	1 ポート FDDI

注:

1. PPP ダイアル回線インターフェースは、ISDNまたは V.25bis を基本ネットワーク・インターフェースとして使用できます。
2. FR ダイアル回線インターフェースは、ISDN または V.25bis ネットワークを基本ネットワーク・インターフェースとして使用できます。

3. ダイヤルイン回線インターフェースは、ISDN ネットワークを基本ネットワーク・インターフェースとして使用できます。
4. SDLC ダイヤル回線は、V.25bis を基本ネットワーク・インターフェースとして使用できます。

ネットワーク・インターフェース・コンソール・プロセスへのアクセス

特定の装置に関連する情報を監視する場合は、以下の手順を使用して、コンソール・プロセスにアクセスします。

1. OPCON プロンプトで、**console** コマンドを入力します。たとえば、次のように入力します。

```
* console
```

2. GWCON プロンプト (+) がコンソールに表示される。最初に GWCON に入ったときにこのプロンプトが表示されない場合は、**Enter** をもう一度押してください。
3. GWCON プロンプトで、**configuration** コマンドを入力します。たとえば、次のように入力します。

```
+configuration
```

```
Multiprotocol Access Services
```

```
2216-MAS Feature 2822 V3.2 Mod 0 PTF 0 RPQ 0 MAS.EF9 cc4_2a
```

```
Num Name Protocol
0 IP DOD-IP
3 ARP Address Resolution
4 DN DNA Phase IV
6 VIN Banyan Vines
7 IPX NetWare IPX
10 BGP Border Gateway Protocol
11 SNMP Simple Network Management Protocol
12 OSPF Open SPF-Based Routing Protocol
22 AP2 AppleTalk Phase 2
23 ASRT Adaptive Source Routing Transparent Enhanced Bridge
26 DLS Data Link Switching
27 XTP X.25 Transport Protocol
28 APPN Advanced Peer-to-Peer Networking [HPR]
30 APPN Advanced Peer-to-Peer Networking [ISR]
```

```
Num Name Feature
2 MCF MAC Filtering
```

```
16 Networks:
Net Interface MAC/Data-Link Hardware State
0 TKR/0 Token-Ring/802.5 Token-Ring Up
1 TKR/1 Token-Ring/802.5 Token-Ring Up
2 TKR/2 Token-Ring/802.5 Token-Ring Up
3 TKR/3 Token-Ring/802.5 Token-Ring Up
4 Eth/0 Ethernet/IEEE 802.3 Ethernet Up
5 Eth/1 Ethernet/IEEE 802.3 Ethernet Up
6 Eth/2 Ethernet/IEEE 802.3 Ethernet Up
7 Eth/3 Ethernet/IEEE 802.3 Ethernet Up
8 Eth/4 Ethernet/IEEE 802.3 Ethernet Up
9 Eth/5 Ethernet/IEEE 802.3 Ethernet Up
10 FR/0 Frame Relay V.35/V.36 Up
11 X25/0 X.25 V.35/V.36 Up
12 PPP/0 Point to Point V.35/V.36 Up
```

13	PPP/1	Point to Point	V.35/V.36	Up
14	PPP/2	Point to Point	V.35/V.36	Up
15	PPP/3	Point to Point	V.35/V.36	Up

4. GWCON **network** コマンドと監視したいインターフェースの番号を入力する。たとえば、次のように入力します。

```
+ network 11
X.25>
```

この例では、X.25 コンソール・プロンプトがコンソールに表示されます。ここで X.25 コンソール・コマンドを入力して、X.25 インターフェースに関する情報を表示させることができます。

ネットワーク・インターフェースの監視: 2210 のネットワーク・インターフェースの監視についての詳しい情報は、本書の該当する章を参照してください。

フィーチャーの構成プロセスおよび動作プロセスへのアクセス

マルチプロトコル・ルーティング・サービスのフィーチャーの構成プロセスおよび動作プロセスにアクセスするのに役立つように、この節ではこれらの手順の両方について概説します。

フィーチャー・プロセスへのアクセス

プロトコル構成プロセスおよびネットワーク・インターフェース構成プロセス以外の、マルチプロトコル・ルーティング・サービスの特定のフィーチャーに関する構成コマンドにアクセスする場合は、CONFIG プロセスから **feature** コマンドを使用します。

プロトコル・コンソール・プロセスおよびネットワーク・インターフェース・コンソール・プロセス以外の、特定のフィーチャーに関するコンソール・コマンドにアクセスする場合は、GWCON プロセスから **feature** コマンドを使用します。

使用しているソフトウェア・リリースで使用可能なフィーチャーのリストを表示させるには、**feature** コマンドの後に疑問符を入力します。たとえば、次のように入力します。

```
Config> feature ?
WRS
BRS
MCF
TSF
Feature name or number [1] ?
```

特定のフィーチャーの構成プロンプトまたは動作プロンプトにアクセスするには、それぞれ Config> または + (GWCON) プロンプトで、**feature** コマンドに続けて機能の番号または短縮名を入力します。たとえば、次のように入力します。

```
Config> feature mcf
MAC filtering user configuration
Filter Config>
```

80ページの表7 は、使用できるフィーチャーの番号と名前をリストしています。

フィーチャーの構成プロンプトまたは動作プロンプトにアクセスしたら、そのフィーチャーの特定コマンドの入力を開始することができます。直前のプロンプト・レベルに戻るには、フィーチャーのプロンプトで **exit** コマンドを入力します。

プロトコルの構成プロセスおよび動作プロセスへのアクセス

この節では、プロトコルの構成プロセスおよび動作プロセスにアクセスする方法について説明します。

プロトコル構成プロセスに入る方法

CONFIG> プロンプトから、必要なプロトコル構成プロセスに入るには、次のようになります。

1. CONFIG> プロンプトで **list configuration** コマンドを使用して、ソフトウェアのコピーとして購入したプロトコルの番号と名前を表示する。**list configuration** コマンドの出力例については、81 ページを参照してください。
2. Config> プロンプトで、構成したいプロトコルの番号と短縮名 (たとえば、SNMP) を指定して **protocol** コマンドを入力する。プロトコル番号と短縮名は **list configuration** コマンドの画面から入手します。次の例では、SNMP プロトコル構成プロセスにアクセスするためのコマンドが入力されています。

```
Config> protocol SNMP
```

または

```
Config> protocol 11  
SNMP user configuration
```

これにより、プロトコル構成プロンプトがコンソールに表示されます。次の例は、SNMP プロトコル構成プロンプトを示しています。

```
SNMP config>
```

これで、このプロトコルの構成コマンドの入力を開始することができます。特定のプロトコル構成コマンドの詳細については、**プロトコルの構成と監視 解説書** の該当するプロトコルのセクションを参照してください。

要約すると、**protocol** コマンドを使用すると、装置に導入されているプロトコル・ソフトウェアの構成プロセスに入ることができます。**protocol** コマンドは、プロトコルのコマンド・プロセスに入ります。**protocol** コマンドを入力すると、指定されたプロトコルのプロンプトが表示されます。このプロンプトから、そのプロトコル特定のコマンドを入力できます。

プロトコル動作プロセスに入る方法

GWCON プロンプトからプロトコル・コンソール・プロセスに入るには、次のようになります。

1. GWCON プロンプトで、**configuration** コマンドを入力して、装置に構成されているプロトコルとネットワークを表示する。たとえば、次のように入力します。

```
+configuration
```

```
Multiprotocol Access Services
```

```
2216-MAS Feature 2822 V3.2 Mod 0 PTF 0 RPQ 0 MAS.EF9 cc4_2a
```

```

Num Name Protocol
0 IP DOD-IP
3 ARP Address Resolution
4 DN DNA Phase IV
6 VIN Banyan Vines
7 IPX NetWare IPX
10 BGP Border Gateway Protocol
11 SNMP Simple Network Management Protocol
12 OSPF Open SPF-Based Routing Protocol
22 AP2 AppleTalk Phase 2
23 ASRT Adaptive Source Routing Transparent Enhanced Bridge
26 DLS Data Link Switching
27 XTP X.25 Transport Protocol
28 APPN Advanced Peer-to-Peer Networking [HPR]
30 APPN Advanced Peer-to-Peer Networking [ISR]

Num Name Feature
2 MCF MAC Filtering

16 Networks:
Net Interface MAC/Data-Link Hardware State
0 TKR/0 Token-Ring/802.5 Token-Ring Up
1 TKR/1 Token-Ring/802.5 Token-Ring Up
2 TKR/2 Token-Ring/802.5 Token-Ring Up
3 TKR/3 Token-Ring/802.5 Token-Ring Up
4 Eth/0 Ethernet/IEEE 802.3 Ethernet Up
5 Eth/1 Ethernet/IEEE 802.3 Ethernet Up
6 Eth/2 Ethernet/IEEE 802.3 Ethernet Up
7 Eth/3 Ethernet/IEEE 802.3 Ethernet Up
8 Eth/4 Ethernet/IEEE 802.3 Ethernet Up
9 Eth/5 Ethernet/IEEE 802.3 Ethernet Up
10 FR/0 Frame Relay V.35/V.36 Up
11 X25/0 X.25 V.35/V.36 Up
12 PPP/0 Point to Point V.35/V.36 Up
13 PPP/1 Point to Point V.35/V.36 Up
14 PPP/2 Point to Point V.35/V.36 Up
15 PPP/3 Point to Point V.35/V.36 Up

```

注: APPN[®] は IBM の登録商標です。

- 構成情報に表示されている必要なプロトコルのプロトコル番号と短縮名を指定して、GWCON **protocol** コマンドを入力する。

次の例では、SNMP プロトコル・コンソール・プロセスにアクセスするためのコマンドが入力されています。

```
+ protocol 11
```

または

```
+ protocol SNMP
```

これにより、プロトコル・コンソール・プロンプトがコンソールに表示されません。この例は、SNMP プロトコル・コンソール・プロンプトを示しています。

```
SNMP>
```

これで、このプロトコルのコマンドを入力し始めることができます。特定のプロトコル・コンソール・コマンドの詳細については、*Protocol Configuration and Monitoring Reference* の該当するプロトコルのセクションを参照してください。

コマンド完成

自動コマンド完成機能では、コマンド行で入力されたコマンドの構文を作成するのをお手伝いします。

コマンド完成の振る舞いを説明するために、ある一定のメニュー・コンテキストで以下のコマンドが許可されていると想定します。(これはメニューの例にすぎません。)

enable

auto-refresh

caching

set

cache-size

cache-timeout

priority

- **ena** と入力して、スペース・バーを押すと、フル・コマンドが **ENABLE** として示されます。**?** を入力すると、enable (使用可能) にするすべての可能な項目 (**auto-refresh** および **caching**) が示され、コマンド **ENABLE** がコマンド行に残っています。
- **ena** と入力して **Enter** と押すと、コマンドが完全には指定されていないというメッセージが印刷され、enable (使用可能) にする考えられる項目のリストが示され (**auto-refresh** および **caching**)、コマンド **ENABLE** がコマンド行に残っています。
- **ENABLE** コマンドは、使用可能にする項目を必要とするので、考えられるコマンド完成のリストが表示され、左端に『...』が付き、コマンドについてさらに入力が必要なことを示します。
- 入力が複数のコマンドと一致する場合、考えられる完成のリストが表示されます。新しいコマンド行での入力は、最も長い共通接頭部に拡張されます。たとえば、**set ca** と入力してから、スペース・バーを押すと、**CACHE-SIZE** および **CACHE-TIMEOUT** がリストされ、新しいコマンド行が **SET cache-** に拡張されます。これは、考えられる両方の完成について『cache-』が共通だからです。今度は文字『s』または文字『t』を入力して、考えられる完成の "size" または "timeout" を区別する必要があります。
- 共通のコマンドは、代替形式 (**SHOW**、**DISPLAY**、**LIST**) で表示されることがあります。コマンド完成が共通のコマンド (たとえば、**SHOW**) で一致を生じさせない場合には、代替 **DISPLAY** または **LIST** が表示されます (見付かる場合)。
- コマンド (および代替) の検索で、正確な一致が生じない場合、ユーザーの入力の一部を使用して、考えられる完成のリストが提示されます。たとえば、**enanle** に続けてスペース・バーを押すと、**ena** で置き換えられ、考えられる完成として **ENABLE** がリストされることとなります。
- 考えられるコマンドのリストが示される場合、Tab キーを使用して現行のコマンド行で一度に 1 つのコマンドずつ循環することができます。スペース・バーまたは Enter キーを使用して、示されているコマンドを選択することができます。

コマンド完成が使用可能にされたときのオンライン・ヘルプ

コマンド完成が使用可能にされるときは、次のオンライン・ヘルプが使用できます。

enable command-completion 構文については、77 ページを参照してください。

- **?** 疑問符は、考えられる完成のリストを表示します。コマンドがすでに完成している場合はメッセージが表示されます。

スペース・バー

コマンド行にある現行のワードを完成しようとします。固有な一致が見付からない場合、考えられる完成がリストされます。

Tab コマンド行にある現行のワードを完成しようとします。固有な一致が見付からない場合、考えられる完成がリストされ、Tab キーを使用してこれらの考えられる完成を通じて循環することができます。現在表示されているコマンドを選択するには、スペース・バーまたは Enter キーを使用します。

Enter コマンド行にある現行のワードを完成しようとします。コマンドが完成すると、Enter はコマンドを実行し、それをコマンド活動記録に保管します。コマンドが不完全である場合は、考えられる完成のリストが表示されます。

Ctrl-P MOS オペレーター・コンソール・プロンプト (*) に戻ります。(Ctrl-P は、デフォルトのインターセプト文字です。)

Backspace

コマンド行での最後の文字を削除します。

Ctrl-W コマンド行での最後のワードを削除します。

Ctrl-U 現行のコマンドを打ち切ります。

Ctrl-L 現行のコマンド行を最新表示して、その内容を表示します。

Ctrl-B 逆方向の検索。現行のコマンド行を、循環するコマンド活動記録内の前のコマンドで置き換えます。

Ctrl-F 順方向の検索。現行のコマンド行を、コマンド活動記録内の次のコマンドで置き換えます。

Ctrl-R コマンド活動記録内の反復シーケンスの開始をマーク付けします。 **Ctrl-N** 機能と一緒に使用してください。

Ctrl-N 現行のコマンド行を、開始コマンドが **Ctrl-R** でマーク付けされている反復シーケンス内の次のコマンドで置き換えます。

Ctrl-C Easy-Start を取り消します (アクティブである場合)。

Escape ?

Escape に続けて『?』を入力すると、このコマンド行ヘルプが印刷されます。

自動コマンド完成には、以下の規則が適用されます。

- 完成したコマンドは、コマンド行に英大文字で示されます。
- 共通のコマンドは、代替形式 (**ADD** 対 **CREATE**) で表示されることがあります。コマンド完成が共通のコマンドで一致を生じさせない場合には、代替コマンドがあればそれが表示されます。
- コマンド (および代替コマンド) の検索で、固有な一致が生じない場合、考えられる完成のリストが示され、最も長い共通接頭部が提示されます。
- 考えられる完成がリストされるとき、さらにコマンド入力が必要とするコマンドは左端に『...』を付けて示されます。
- コマンド活動記録検索キー (Ctrl-B、F、N) が押されるとき、コマンド活動記録が走査され、現行のコマンド・コンテキスト内で正常に構文解析されるコマンドがないか調べられます。そのようなコマンドが存在しない場合は、トーンが鳴りません。

- 一部のコマンド・メニューは動的に作成されます。コマンド完成は、いつでもこれらの動的リンクに従うとは限りません。これらの場合には、'?' を入力することができます。
- 1 つだけのコマンドに対し (コメントを入力するために) コマンド完成を使用不可にする場合、コマンド行の最初の文字として任意のコメント文字を入力します。コメント文字は !@\$%*:/" です。
- コマンド完成は、内部エラーの場合には使用不可にされます。画面上のデバッグ情報をカスタマー・サポートに報告します。
- コマンド完成は現在使用可能にされています。このオプションを使用不可にするには、Configuration talk 6 から **disable command-completion** コマンドを使用します。

コマンド完成が使用不可にされたときのオンライン・ヘルプ

コマンド完成が使用不可にされるときは、次のオンライン・ヘルプが使用できません。

? コマンド行の末尾に ? (疑問符) が入力される時、考えられる完成のリストが示されます。

Enter コマンドを実行して、それをコマンド活動記録に保管します。コマンドが完全には指定されていない場合は、メッセージが印刷されます。

Ctrl-P MOS オペレーター・コンソール・プロンプト (*) に戻ります。(Ctrl-P は、デフォルトのインターセプト文字です。)

Backspace

コマンド行での最後の文字を削除します。

Ctrl-U 現行のコマンドを打ち切ります。

Ctrl-B 逆方向の検索。現行のコマンド行を、循環するコマンド活動記録内の前のコマンドで置き換えます。

Ctrl-F 順方向の検索。現行のコマンド行を、コマンド活動記録内の次のコマンドで置き換えます。

Ctrl-R コマンド活動記録内の反復シーケンスの開始をマーク付けします。 **Ctrl-N** 機能と一緒に使用してください。

Ctrl-N 現行のコマンド行を、開始コマンドが **Ctrl-R** でマーク付けされている反復シーケンス内の次のコマンドで置き換えます。

Ctrl-C Easy-Start を取り消します (アクティブである場合)。

Escape ?

Escape に続けて『?』を入力すると、このコマンド行ヘルプが印刷されます。

自動コマンド完成には、以下の規則が適用されます。

- コマンド完成は現在使用不可にされています。このオプションを使用可能にするには、Configuration talk 6 から **enable command-completion** コマンドを使用します。

コマンド活動記録

コマンド活動記録には、OPCON、GWCON (Talk 5)、または CONFIG (Talk 6) コマンド行メニューでユーザーによって入力された最後の最大50 までのコマンドが含まれます。

逆方向および順方向の検索キーを使用して、以前に入力したコマンドを再度呼び出すことができます。また、熟練したユーザー向けに、一連の特定コマンドを反復して使用できる機能も用意されています。

コマンド活動記録内のコマンドの反復

OPCON、GWCON、または CONFIG メニュー内の任意のコマンド行プロンプトで **Ctrl-B** (backward) または **Ctrl-F** (forward) を押すと、現行のコマンド行が、コマンド活動記録内の前のコマンドまたは次のコマンドと置き換わります。コマンド活動記録は、コマンド行インターフェースを通じて共通です。つまり、GWCON メニューで入力したコマンドを CONFIG 内から検索したり、CONFIG メニューで入力したコマンドを GWCON から検索するといったことが可能です。

自動コマンド完成が使用可能にされ (26ページの『コマンド完成』を参照)、コマンド活動記録検索キー (Ctrl-B、F、N) が押されると、コマンド活動記録が走査され、現行のコマンド・コンテキスト内で正常に構文解析されるコマンドがないか調べられます。そのようなコマンドが存在しない場合は、トーンが鳴ります。

コマンド活動記録には、最新に入力されたコマンドが、最大で最後の 50 個が入っています。リスタート後に 3 つのコマンドしか入力していない場合、**Ctrl-F** または **Ctrl-B** を押すと、この 3 つのコマンドだけが循環します。それまでにコマンドが入力されていない場合、**Ctrl-F** または **Ctrl-B** を押すと、トーンが鳴ります。

注: **Ctrl-U** を押して打ち切られたコマンドは、コマンド活動記録には入力されません。コマンド完成が使用可能にされると、コマンド活動記録には完全なコマンドだけが入力されます。

2 つの類似したコマンドを入力する場合は、

```
display sub les  
display sub lec
```

次のようにします。

display sub les と入力して、**Enter** を押します。

Ctrl-B (Backward) を押すと、現在の行が次の行で置き換えられます。

```
display sub les
```

Backspace を押して、『s』を『c』で置き換えます。

display sub lec となるので、**Enter** を押します。

コマンド活動記録内の一連のコマンドの反復

上級のユーザー向けに、特定の一連の GWCON または CONFIG コマンドを簡単に反復使用することができる追加機能が提供されています。コマンド活動記録

の中の C1, C2,...,Cn を反復シーケンスと呼びます。このフィーチャーは、あるタスクの中で複数のコマンドを反復して使用する必要がある場合に、単に **Ctrl-B** および **Ctrl-F** だけを使うよりも便利なことがあります。コマンド C1 で **Ctrl-R** (repeat) を入力して、反復シーケンスの開始をセットします。続いて **Ctrl-N** (next) を入力して、反復シーケンス内の次のコマンドを取り出します。コマンドは自動的に入力されるのではなく、現行のコマンド行に置かれるので、ユーザーはそのコマンドを修正したり、入力したりすることができます。

必要な動作を実行する反復シーケンスを作成するために、初めに **Ctrl-N** (next) を使用して取り出される最初のコマンドは、**Ctrl-R** (repeat) を使用してセットされた反復シーケンスの開始方法によって異なったものになります。

Ctrl-R を使用して反復シーケンスの開始をセットするには、次の 2 通りの方法があります。

1. C1 を最初に入力するときにセットする
2. **Ctrl-B** または **Ctrl-F** を使用してコマンド活動記録から C1 を取り出したときにセットする。

コマンドの入力時に反復シーケンスを開始

コマンド C1 を入力するときに **Ctrl-R** を入力し、次にコマンド C2, C3... Cn を入力した場合、**Ctrl-N** を入力すると、コマンド C1, C2, ... Cn, C1, C2, ... Cn, C1, ... が連続的にコマンド行に置かれます。

例 1 では、反復シーケンスの開始は、最初のコマンドの入力時にセットされています。ユーザーは事前に、GWCON に入力するのと同じコマンドを CONFIG で反復する必要があることを知っています。

例 1

1. シーケンスの最初のコマンドを入力するときに、**Ctrl-R** (repeat) を使用して、反復シーケンスの開始をセットする。

```
*console
+event Ctrl-R
```

ここで **Enter** を押して、反復シーケンスをセットします。

2. シーケンス内の後続のコマンドを入力する。

```
Event Logging System user console
ELS>display sub les
ELS>display sub lec
ELS>exit
+
```

3. これと同じコマンドを CONFIG に入力するために、

Ctrl-P (デフォルトの OPCON インターセプト文字) を押して、CONFIG に行く。

```
+--press Ctrl-P-
*configuration
Config>Ctrl-N for NEXT to retrieve the start of this sequence-
Config>event Enter
Event Logging System user configuration
ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
ELS config>display sub les Enter
ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
```

```
ELS config>display sub lec Enter
ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
ELS config>exit Enter
Config>
```

すべてのコマンドの入力後に反復シーケンスを開始

一方、最初に C1, C2, ... Cn を入力した場合は、**Ctrl-B** または **Ctrl-F** を使用して C1 を取り出します。**Ctrl-R** を入力し、**Ctrl-N** を入力すると、コマンド C2,..., Cn, C1, C2,..., Cn, C1,...,Cn がコマンド行に連続して置かれます (例 2 を参照)。C1 が取り出されたときには、C1 はすでにコマンド行に置かれており、最初の **Ctrl-N** で再度呼び出す必要はないので、最初の C1 はバイパスされます。

例 2 では、すべてのコマンドを入力した後で、反復するシーケンスの最初のコマンドを取り出します。一連のコマンドが GWCON で入力されており、同じシーケンスを CONFIG で反復する必要があります。

例 2

1. 以下のコマンドを GWCON に入力する。

```
*console
+event
Event Logging System user console
ELS>display sub les
ELS>display sub lec
ELS>exit
+
```

2. これと同じコマンドを CONFIG に入力するために、**Ctrl-P** (デフォルトの OPCON インターセプト文字) を押して、CONFIG に行く。

```
+Ctrl-P-
*configuration
Config>Ctrl-B four times to retrieve the start of
the four command sequence in this example-
Config>event
Config>event Ctrl-R for REPEAT to set the start of the repeat sequence-
Config>event Enter
Event Logging System user configuration
ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
ELS config>display sub les Enter
ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
ELS config>display sub lec Enter
ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
ELS config>exit Enter
Config>
```

第3章 OPCON プロセスとコマンド

この章では、OPCON インターフェースの構成コマンドおよびオペレーショナル・コマンドについて説明します。この章は、次の節に分かれています。

- 『OPCON プロセスとは』
- 『OPCON プロセスへのアクセス』
- 34ページの『OPCON コマンド』

OPCON プロセスとは

オペレーター・コンソール・プロセス (OPCON) は、装置ソフトウェア・ユーザー・インターフェースのルート・レベルのプロセスです。OPCON の主な機能は、2 次レベルのプロセス (構成、コンソール、およびイベント・ログ) と通信することです。OPCON コマンドを使用して、以下のことも行えます。

- 装置メモリーの使用量に関する情報を表示する
- 装置ソフトウェアを再ロードする (リブート)
- 他の装置またはホストに Telnet でログインまたは ping する
- すべての装置プロセスに関する情報を表示する
- プロセスからの出力を操作する
- OPCON インターセプト文字を変更する

OPCON プロセスへのアクセス

初めて装置を開始すると、コンソールにブート・メッセージが表示されます。次に、OPCON プロンプト (*) がコンソールに表示され、OPCON プロセスがアクティブになり、OPCON コマンドを受け入れる準備が整ったことを示します。

OPCON プロセスでは、装置の動作パラメーターのすべてを構成、変更、および監視することができます。OPCON プロセスにいるときは、装置はデータを転送しています。装置がブートされて OPCON に入ると、著作権ロゴとアスタリスク (*) プロンプトが、ローカル接続されたコンソール端末に表示されます。これが OPCON (OPERATOR'S CONSOLE) プロンプトで、第 2 レベルのプロセスへのアクセスを可能にする、メイン・ユーザー・インターフェースです。

OPCON で行われる装置の動作パラメーターの変更の一部のものは、装置を再初期化しなくても、即時に有効になります。変更が有効にならない場合は、* プロンプトで **reload** コマンドを使用します。

* プロンプトでは、広範なコマンド・セットにより、各種の内部ソフトウェアの状況を検査したり、装置のインターフェースおよびパケット転送の性能を監視したり、さまざまな動作パラメーターを構成したりすることができます。

OPCON コマンド

この節では OPCON コマンドについて説明します。頻繁に必要とされるコマンドは、『- - - -』の区切り記号の前に表示されます。各コマンドについて、説明、構文の要件、および例を示します。OPCON コマンドの要約を表3に示します。これらのコマンドを使用するには、OPCON プロセスにアクセスし、OPCON プロンプト (*) で該当のコマンドを入力します。

表3. OPCON コマンド

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Configuration*	装置の構成プロセスにアクセスします。(talk 6)
Console*	装置のコンソール・プロセスにアクセスします。(talk 5)
Event Logging	装置のイベント・ログ・システムにアクセスします。(talk 2)
System*	
ELS Console*	装置の2次 ELS コンソール・プロセスにアクセスします。(talk 7)
Logout	リモート・コンソールをログオフします。
Ping	指定された IP アドレスを Ping します。
Reload	装置を再ロードします。
Telnet	別の装置に接続します。

Diags	装置状況およびハードウェア・テスト・ログとハードウェア・エラー・ログの目次を表示します。
Divert	プロセスからの出力をコンソールまたは他の端末に送ります。
Flush	プロセスからの出力を廃棄します。
Halt	プロセスからの出力を中断します。
Intercept	デフォルトの OPCON インターセプト文字を設定します。
Memory	装置のメモリー使用量を報告します。
Status	すべての装置プロセスに関する情報を示します。
Talk	別の装置プロセスに接続し、そのコマンドの使用を可能にします。

* このコマンドを初めて使用する時、**Ctrl-P** を使用して、MOS オペレーター・コンソール・プロンプト (*) に戻れることを忘れないよう注意されます。

Configuration

configuration コマンドは、装置の構成プロセス (talk 6) にアクセスするのに使用します。詳細については、47ページの『第4章 CONFIG プロセス (CONFIG - Talk 6) およびコマンド』を参照してください。

構文:

configuration

例:

* **configuration**

(To return to the MOS Operator Console prompt (*), press Control-P)

```
Gateway user configuration
Config>
```

Console

console コマンドは、装置のコンソールおよび監視プロセス (talk 5) にアクセスするのに使用します。詳細については、149ページの『第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』を参照してください。

構文:

console

例:

```
* console
CGW Operator Console
+
```

Diags

diags コマンドは、診断メイン・メニューを表示するのに使用します。診断メニューでは、ハードウェア・アダプターまたはポートを使用可能にしたり、使用不可にしたり、テストすることができます。診断メニューには、さまざまなオプションや使用可能な状況情報についてのスクリーン内のヘルプがあります。

“b” (back) キーを使用すれば、直前のメニューに戻ることができます。診断を終了して、OPCON コマンド・プロンプトに戻るには、“e” (exit) キーを使用します。

診断サポートについて詳しくは 2210 用の *Service and Maintenance Manual* を参照してください。

構文:

diags

Divert

divert コマンドは、指定のプロセスからの出力を指定の端末に送信するのに使用します。このコマンドを使用すると、複数のプロセスの出力を同じ端末に着信転送し、出力を同時に見ることができます。**divert** が通常使用されるのは、MONITR 出力メッセージを特定の端末に転送する場合です。装置で着信転送が許されるのは、特定のプロセスだけです。

divert コマンドは PID と tty# (出力端末の番号) を必要とします。これらの値は、OPCON **status** コマンドを使用して入手することができます。端末番号は、ローカル・コンソール (tty0) またはリモート・コンソール (tty1, tty2) の 1 つのいずれかです。次の例は、MONITR プロセス (2) で生成されたイベント・ログ・システム・メッセージをリモート・コンソール tty1 (1) に送信する場合を示しています。

イベント・メッセージは、コマンドを入力している最中であっても、即時に表示されます。コマンドが混同されるのを防止するために、ディスプレイとキーボードにはそれぞれ別々のバッファが用意されています。次の例は、**divert 2 0** コマンドの

実行後、MONITR プロセスが TTY0 に接続されたことを示しています。出力を停止したい場合は、**halt 2** と入力します。**halt** コマンドについては、37ページの『Halt』で説明しています。

構文:

divert *pid tty#*

例:

Copyright Notices:
Copyright IBM Corp. 1994, 1997
MOS Operator Console

For help using the Command Line Interface, press ESCAPE, then '?'

* **divert 2 0**

* **status**

Pid	Name	Status	TTY	Comments
1	COpCN1	IOW	TTY0	gzs
2	Monitr	IDL	TTY0	
3	Tasker	RDY	--	
4	MOSDBG	DET	--	
5	CGWCon	DET	--	
6	Config	DET	--	
7	ELSCon	DET	--	
8	ROpCN1	IDL	TTY1	
9	ROpCN2	RDY	TTY2	jlg@128.185.40.40

Els

els コマンドは、装置の 2 次 ELS コンソール・プロセス (talk 7) にアクセスするのに使用します。詳細については、18ページの『2 次 ELS コンソール・プロセスへのアクセス、ELSCon (Talk 7)』を参照してください。

構文:

els

Event

event コマンドは、装置のイベント・ログ・プロセス (talk 2) にアクセスするのに使用します。詳細については、169ページの『第10章 イベント・ログ・システム (ELS) の使用』を参照してください。

構文:

event

Flush

flush コマンドは、プロセスの出力バッファを消去するのに使用します。一般的に、このコマンドは MONITR の FIFO バッファの内容を表示する前に使用され、メッセージがスクロールして画面から消えるのを防止します。累積されたメッセージは廃棄されます。

装置でフラッシュが許されるのは、特定のプロセスだけです。PID と tty# を入手するには、OPCON **status** コマンドを使用します。次の例では、**flush 2** コマンドを実行すると、MONITR プロセスの出力は Sink (フラッシュ済み) に送信されます。

構文:

```
flush pid
```

例:

```
* flush 2
* status
Pid Name      Status TTY  Comments
1   COpCN1    IOW   TTY0
2   Monitr    IDL   SNK
3   Tasker    RDY   --
4   MOSDBG    DET   --
5   CGWCon    DET   --
6   Config    DET   --
7   ELSCon    DET   --
8   ROpCN1    IDL   TTY1
9   ROpCN2    RDY   TTY2 jlg@128.185.40.40
```

Halt

halt コマンドは、指定のプロセスからのすべての後続の出力を、そのプロセスに対して **divert**、**flush**、または **talk** OPCON コマンドが出されるまで中断するのに使用します。装置は、すべてのプロセスを転送できるわけではありません。**Halt** は、プロセスからの出力のデフォルトの状態です。このコマンドで使用する PID を入手するには、OPCON **status** コマンドを使用します。次の例では、**halt 2** コマンドの実行後は、MONITR プロセスは TTY0 に接続されなくなります。イベント・メッセージも表示されなくなります。

構文:

```
halt pid
```

例:

```
* halt 2
* status
Pid Name      Status TTY  Comments
1   COpCN1    IOW   TTY0 gzs
2   Monitr    IDL   --
3   Tasker    RDY   --
4   MOSDBG    DET   --
5   CGWCon    DET   --
6   Config    DET   --
7   ELSCon    DET   --
8   ROpCN1    IDL   TTY1
9   ROpCN2    RDY   TTY2 jlg@128.185.40.40
```

Intercept

intercept コマンドは、OPCON インターセプト文字を変更するのに使用します。インターセプト文字とは、OPCON プロセスに戻るために、他のプロセスから入力する文字です。デフォルトのインターセプト・キーの組み合わせは **Ctrl-P** です。

インターセプト文字は、制御文字になることができます。^ (シフト 6) 文字に続けて、インターセプト文字に使用したいレター文字や !@#\$% などの非英数字文字を入力します。

注: この変更は、現行のログイン・セッションにのみ適用されます。

構文:

intercept [^] *character*

例 1:

* **intercept** ^a

この例から、インターセプト文字は **Ctrl-A** になっています。

例 2:

* **intercept** !

この例から、インターセプト文字は **!** になっています。

Logout

logout コマンドを使用すると、logout コマンドを入力したユーザーの現行セッションが終了します。コンソール・ログインが使用可能になっている場合、このコマンドにより、次のユーザーは許可ユーザー ID/パスワードの組み合わせを使用してログインする必要があります。コンソール・ログインが使用可能になっていない場合は、OPCON プロンプトが再び表示されます。

構文:

logout

Memory

memory コマンドは、装置のグローバル・ヒープ・メモリーの使用に関する情報を入手したり、表示したりするのに使用します。この表示を見れば、装置が効率的に使用されているかどうかを判断することができます。メモリー使用状況の例は、39ページの図3 を参照してください。

talk 5 によるメモリー使用量については、159ページの『Memory』を参照してください。

構文:

memory

例:

* **memory**
Number of bytes: Busy = 319544, Idle = 1936, Free = 1592

Busy 現在割り振られているバイト数を示します。

Idle 以前に割り振られていたが解放され、再利用できるバイト数を示します。

Free 初期の空き記憶域から一度も割り振られたことのないバイト数を示します。

注: Idle と Free メモリーの和が、使用可能な合計ヒープ・メモリーに等しくなります。



図3. メモリーの使用状況

Ping

ping コマンドは、装置が一定のあて先に ICMP エコー・メッセージを送信して (つまり、『ping』)、応答を監視するようにさせるのに使用します。このコマンドは、インターネットワークでトラブルを分離するのに使用することができます。

構文:

ping *dest-addr [src-addr data-size ttl rate tos data-value]*

ping プロセスは継続的に行なわれ、パケットが追加されるたびに ICMP 順序番号が増分されます。突き合わせる受信された各 ICMP エコー応答は、その順序番号と往復時間を使って報告されます。往復時間計算の細分度 (時間解像度) は、プラットフォームによって異なりますが、通常は約 20 ms (ミリ秒) です。

ping プロセスを停止するには、コンソールで任意の文字を入力します。その時点で、パケット紛失、往復時間、および到達不能 ICMP あて先の数が表示されます。

同報通信またはマルチキャスト・アドレスがあて先として与えられるとき、送信された各パケット (各グループ・メンバーに 1 つずつ) について複数の応答が印刷される場合があります。戻される各応答は、応答側の発信元アドレスと一緒に表示されます。

ping のサイズ (ICMP メッセージ内のデータ・バイトの数 (ICMP ヘッダーを除く))、データの値、活動時間 (TTL) 値、**ping** の速度、および設定する TOS ビットを指定することができます。発信元 IP アドレスも指定することができます。発信元 IP アドレスを指定しない場合、装置は、指定されたあて先への発信インターフェース上のローカル・アドレスを使用します。装置の他方のインターフェースのどれかから宛先への接続性を妥当性検査する場合、そのインターフェースの IP アドレスを発信元アドレスとして入力します。

あて先パラメーターだけが必須です。他のすべてのパラメーターは任意選択です。デフォルトでは、サイズは 56 バイト、TTL は 64、速度は 1 ping / 秒で、TOS 設定値は 0 です。最初の 4 バイトの ICMP データは、タイム・スタンプに使用されます。デフォルトでは、残りのデータは、X'04' から始まり、X'FF' から X'00' へと循環する、1 ずつ増分する値をもつ一連のバイトです (たとえば、X'04 05 06 07 . . . FC FD FE FF 00 01 02 03 . . .)。これらの値が増分されるのは、デフォルトが使用される場合だけです。データ・バイト値が指定される場合、ICMP データはすべて (最

初の 4 バイトを除く) その値に設定され、その値は増分されません。たとえば、データ・バイト値を 'X'FF' に設定する場合、ICMP データは 'X'FF FF FF ...' の値をもつ一連のバイトです。

例:

```
* ping
Destination IP address [0.0.0.0]? 192.9.200.1
Source IP address [192.9.200.77]?
Ping data size in bytes [56]?
Ping TTL [64]?
Ping rate in seconds [1]?
Ping TOS (00-FF) [0]? e0
Ping data byte value (00-FF) [ ]?
PING 192.9.200.77-> 192.9.200.1:56 data bytes,ttl=64,every 1 sec.
56 data bytes from 192.9.200.1:icmp_seq=0.ttl=255.time=0.ms
56 data bytes from 192.9.200.1:icmp_seq=1.ttl=255.time=0.ms
56 data bytes from 192.9.200.1:icmp_seq=2.ttl=255.time=0.ms

----192.9.200.1 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max=0/0/0 ms
```

Reload

reload コマンドは、装置ソフトウェアの新規コピーをロードすることによって、装置をリブートするのに使用します。 リモート・コンソールからこのコマンドを使用すると、装置のところに行かなくても、新規ソフトウェア・ロードを導入することができます。このコマンドは、装置がダンプを取らないこと (そのように構成されている場合) を除けば、リセット・ボタンが押されたときと同じ機能を実行します。再ロードが有効になる前に、再ロードの確認を求めるプロンプトが出ます。 構成変更を保管しなかった場合も、プロンプトが出ます。

構文:

reload

例:

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

Status

status コマンドは、すべての装置プロセスに関する情報を表示するのに使用します。
status コマンドの後に **PID** を入力することにより、必要なプロセスだけの状態を見ることができます。次の例は、すべての状態を表示しています。

構文:

status *pid*

例:

```
* status
Pid Name Status TTY Comments
1 COpCN1 IOW TTY0
2 Monitr IDL --
3 Tasker RDY --
4 MOSDBG DET --
5 CGWCon IOW --
```

```

6  Config  IOW  TTY1
7  ELSCon  DET  --
8  ROpCN1  IOW  TTY1 128.185.46.101
9  ROpCN2  RDY  TTY2 128.185.46.104

```

Pid PID を指定します。これは OPCODE との間でトークするためのプロセスであり、特定プロセスの状態に関する情報を要求する STATUS コマンドの引き数として使用することができます。

Name プロセス名を指定します。通常は、プロセスで実行中のプログラムの名前に対応しています。

Status

次のいずれか 1 つを指定します。

IDL プロセスがアイドルで、何らかの外部事象 (非同期入出力など) が完了するのを待っています。

RDY プロセスがレディー状態で、CPU の使用を待っていることを示します。

IOW プロセスが同期入出力 (通常は、予期する標準入力) が完了するのを待っています。

DET プロセスの出力が表示可能な状態にあり、プロセスはディスプレイ・コンソールに接続されるのを待っているか、その出力が指定コンソールに着信転送されるのを待っていることを示しています。

FZN プロセスがエラーのために凍結されていることを示します。これは通常、プロセスが、障害のある装置または間違っ構成されている装置を使おうとしていることを意味しています。

TTY_n プロセスが現在接続されている出力端末 (もしあれば) を指定します。

TTY0 ローカル・コンソール

TTY1 または TTY2
Telnet コンソール

Sink プロセスはフラッシュされた。

Two dashes (--)
プロセスは停止された。

Comments

ユーザーが Telnet を使用してログインするときに提供した、ユーザーのログイン IP アドレスを指定します (ROpCon)。

Suspend

suspend コマンドは、現行セッションについてのみコマンド完成 (Command Completion) を一時的に使用不可にするのに使用します。自動スクリプトを使用している場合、コマンド完成を一時的に使用不可にしたいときは、最初のコマンドとして **suspend yes** を発行することができます。

コマンド完成については、26ページの『コマンド完成』を参照してください。

構文:

suspend

Talk

configuration、**console**、または **event** コマンドを使用して、**CONFIG**、**GWCON**、または **MONITR** などの他のプロセスに接続するか、**talk** コマンドを使用することができます。新しいプロセスに接続した後は、そのプロセスに特定のコマンドを送信し、そのプロセスから出力を受信することができます。ただし、**TASKER** または **OPCON** プロセスとは接続できません。

PID を入手するには、**OPCON status** コマンドを使用します。第 2 レベルのプロセス (**CONFIG** など) に接続した後で * プロンプトに戻るには、インターセプト文字 **Ctrl-P** を使用します。

構文:

```
talk pid
```

例:

```
* talk 5  
  
CGW Operator Console  
+
```

第 3 レベルのプロセス (**SNMP Config>** または **SNMP>** など) を使用しているときに、第 2 レベルに戻るには **exit** コマンドを使用します。

Telnet

telnet コマンドは、別の装置またはリモート・ホストにリモート接続するのに使用します。唯一のオプション・パラメーターは、エミュレートしたい端末タイプです。

telnet コマンドは、IPv4 または IPv6 アドレスとともに使用することができます。

装置は最大 5 つの Telnet セッションを持つことができます。2 つのサーバー (装置への着信) と 3 つのクライアント (装置からの発信) です。

注: 純粋なブリッジング環境で Telnet を使用する場合は、ホスト・サービスを使用可能にする必要があります。

構文:

```
telnet ip-address terminal-type
```

例 1: **telnet 128.185.10.30** または **telnet 128.185.10.30 23** または **telnet 128.185.10.30 vt100**

```
Trying 128.185.10.30 ...  
Connected to 128.185.10.30  
Escape character is '^']'
```

例 2: **telnet 1:9::10**

```
Trying 1:9::10 ...  
Connected to 1:9::10  
Escape character is '^']'
```

存在しない IP アドレスに Telnet でログインすると、装置は次のように表示します。

Trying 128.185.10.30 ...

Telnet コマンド・モードに入るには、エスケープ文字列 (どのプロンプトでも **Ctrl-J**) を入力します。

```
telnet>
```

装置に Telnet でログインするときは、次のようにします。

- コマンド行に入力した最後の文字を削除するには **← 後退** キーを押す。

注: VT100 端末を使用している場合、**← 後退** キーを押すと、目に見えない文字が挿入されるので、このキーは押さないようにしてください。最後の文字を削除するときは **Delete** キーを押してください。

- コマンド行の入力全体を削除してコマンドを再入力できるようにするには、telnet> プロンプトで **Ctrl-U** を押す。

Telnet コマンド・モードは、以下のサブコマンドから構成されます。

close 現行接続をクローズします。

display

動作パラメーターを表示します。

mode 逐次行モードまたは逐次文字モードに入るを試みます。

open サイトに接続します。

quit Telnet を終了します。

send 特殊文字を送信します (続く場合は send ?)。

set オペレーティング・パラメーターを設定します (続く場合は set ?)。

status 状態情報を印刷します。

toggle オペレーティング・パラメーターを切り替えます (続く場合は toggle ?)。

z Telnet を中断します。

? ヘルプ情報を印刷します。

status および **send** サブコマンドでは、ユーザーが別のホストに接続されているかどうかに応じて、2 つのレスポンスのうち 1 つになります。たとえば、次のように入力します。

ホストに接続されている場合:

```
telnet> status
Connected to 128.185.10.30   Operating in character-at-a-time mode.
Escape character is ^].
```

```
telnet> send ayt
```

注: send コマンドが現在サポートするのは ayt だけです。

ホストに接続されていない場合:

```
telnet> status
Need to be connected first.
```

```
telnet> send ayt
Need to be connected first.
```

リモート・ホストへの接続をクローズし、Telnet セッションを終了するには、**close** サブコマンドを使用します。 **telnet** コマンド・モードを終了し、接続をクローズして Telnet セッションを終了するには、**quit** サブコマンドを使用します。

```
telnet>  close
```

または

```
telnet>  quit
```

```
logout
```

```
*
```

第2部 基本サービスの概要、構成、および使用

第4章 CONFIG プロセス (CONFIG - Talk 6) およびコマンド

この章では、CONFIG プロセスの構成コマンドおよびオペレーショナル・コマンドについて説明します。本章には、以下の節が含まれています。

- 『CONFIG とは』
- 57ページの『CONFIG への出入り』
- 58ページの『CONFIG コマンド』

CONFIG とは

構成プロセス (CONFIG) は、装置ユーザー・インターフェースの第 2 レベルのプロセスです。CONFIG コマンドを使用して、次のことが行えます。

- 構成パラメーターを設定または変更する
- ハードウェア構成にインターフェースを追加または削除する
- Boot CONFIG コマンド・モードに入る
- クイック構成モードに入る
- 構成情報を消去、リスト、または更新する
- コンソール・ログインを使用可能または使用不可にする
- プロトコル環境を含めて、第 3 レベルのプロセスと通信する

注: 新しいコード・レベルへの移行については、*IBM 2210 Nways Multiprotocol Router Service and Maintenance Manual* の『Migrating to a New Code Level』という章を参照してください。

CONFIG では、装置の不揮発性構成メモリーに記憶されている構成情報を表示したり、変更したりすることができます。システム・パラメーターおよびプロトコル・パラメーターに加えた変更は、装置ソフトウェアを再ロードするまでは有効になりません。(詳細については、33ページの『OPCON プロセスとは』の **OPCON reload** を参照してください。)

注: 装置のフラッシュ・メモリーでの変更を保管するには、**write** コマンドを入力する必要があります。

CONFIG コマンド・インターフェースは、いくつかのレベル (モードと呼ばれる) で構成されています。各モードには、それぞれ独自のプロンプトがあります。たとえば、SNMP プロトコルのプロンプトは `SNMP config>` です。

自分が通信しているプロセスおよびモードを知りたい場合は、**Enter** キーを押すと、プロンプトが表示されます。この章で説明する一部のコマンド (**network** や **protocol** など) では、CONFIG の種々のレベルにアクセスし、それを終了することができます。CONFIG プロセスから出すことができるコマンドのリストについては、58ページの表 5 を参照してください。

Config-Only モード

Config-Only モードに入るのは、使用している構成ファイルが空であるか、プロトコルが何も構成されていない場合です。Config-Only モードには、ルーターの起動時の障害の原因になる無効な構成から回復するために、手動で入ることもできます。

Config-Only モードに自動的に入る

Config-Only モードに入るのは、ルーターが空の構成ファイルを使ってブートしているか、構成ファイルに不完全な構成データが含まれている場合です。

以下の状態で、ルーターは Config-Only モードに入ります。

- 装置は構成されているが、プロトコルが構成されていません。
- すべてのルーター・インターフェース情報の削除
- 構成ファイルが空です。

Config-Only モードに手動で入る

Config-Only モードに入るには、次のいずれかを行います。

- 構成せずにルーターを再ロードする。
- インターフェースを構成せずにルーターを再ロードする。
- プロトコルを構成せずにルーターを再ロードする。

詳しくは、133ページの『第7章 ブート・オプション』を参照してください。

クイック構成

クイック構成 (Quick Config) は、ルーター・ロードに存在する bridging protocols and routing protocols を構成するのに必要な最小限の 1 組のコマンドを提供します。また、WRITE_READ_TRAP アクセスをもつ SNMP コミュニティを構成することもできます。これにより、初期設定時に、構成プログラムが SNMP SET コマンドを使用して構成を転送することができるようになるので便利です。

重要: クイック構成を使用する前に少なくとも 1 つのネットワーク装置を構成する必要があります。装置を追加するには、`config(only)> or config>` プロンプトで **add device** コマンドを使用します。詳細については、19ページの『ネットワーク・インターフェース構成プロセスへのアクセス』を参照してください。

次の表は、Quick Config によってサポートされるプロトコルをリストしています。

表 4. Quick Config 機能

ATM プロトコル	ブリッジング・プロトコル	ルーティング・プロトコル
LAN エミュレーション	STB、SRT、SRB	IP、IPX、DNA IV

Quick Config は、ショートカットを提供して、既存の構成プロセスを補足します。このショートカットにより、構成プロセスを終了して別の構成プロセスに入らずに、これらの bridging protocols and routing protocols に必要な最小数のパラメーターを構成することが可能になります。その他のパラメーターは、選択されたデフォルトに設定されます。

ルーターのクイック構成が必要になる状態としては、次のものがあります。

- 構成メモリーがブランクであるか、破壊されている (次のいずれかの状態が生じた場合など)
 - ルーターを初めて構成する場合
 - 電圧変動によってが破壊された場合 the hard file.
- デモンストレーションで、ルーターの機能を実証するためにルーターをクイック構成する必要がある場合
- ベンチマーク・テストで、各種のテストを進める (ルーターのオペレーティング・システム・コマンドについて学習する必要はない) 場合

Quick Config は、以下のように動作します。

- デフォルト値を示しながら一連の質問をする。
- 通常モード・コマンド・セットの詳細構成へのショートカットを提供する。

Quick Config は、構成質問に対するユーザーの応答に基づいて、多数のデフォルト・パラメーターを設定します。 Quick Config で構成できないものは、これを終了した後で、Config を使用して構成することができます。

Quick Config の内部から Quick Config 情報を削除することはできません。ただし、いったん終了して Quick Config に戻るか、一部の Quick Config 質問への応答として **reload** コマンドを入力するかのいずれかにより、情報を訂正することができます。

Quick Config ソフトウェアの使用についての詳しい説明は、755ページの『付録A. クイック構成リファレンス』を参照してください。

Quick Config モードに手動で入る

ルーターの機能を実証するため、またはルーターのオペレーティング・システム・コマンドを学習する必要なしにベンチマーク・テストを行うよう動的に再構成するために、Quick Config を手動で実行したい場合があります。

Quick Config に入るには、Config> プロンプトで **qconfig** と入力します。

Quick Config モードの終了

Quick Config を終了するには、任意のプロンプトから **r** を入力し、リスタートします。 **no** を入力するまでは照会に従って進み、その後で **q** と入力して終了します。ルーターは Config (only)> または Config> プロンプトに戻ります。

ユーザー・アクセスの構成

装置構成プロセスでは、最大 50 名のユーザー名、パスワード、および許可レベルを使用することができます。各ユーザーにパスワードと許可レベルを割り当てる必要があります。許可には管理、操作、および監視の 3 つのレベルがあります。

詳細については、65 ページを参照してください。

技術サポートへのアクセス

システム管理者が最初に新規ユーザーを追加するとき、技術サポート・アクセスを追加したいかどうかを尋ねられます。yes と応答すると、ユーザーがシステム管理者として持っているのと同じアクセス特権が、技術サポートに対しても認められます。

このためのパスワードはソフトウェアによって自動的に選択され、サービス技術員に知らされます。このパスワードは **change user** コマンドを使用して変更できますが、パスワードを変更すると、カスタマー・サービスはリモート・サポートを提供できなくなります。 **change user** コマンドの使用についての詳しい説明は、66ページの『Change』を参照してください。

予備インターフェースの構成

ときには、装置をリスタートせずに、新規インターフェースをそのブリッジングおよびルーティング・プロトコルと共に構成することが必要になる場合があります。装置上に多数の予備インターフェースを構成しておくことによって、これを実現できます。予備インターフェースは、次のような場合に便利です。

- 新規アダプターを装置に『ホット・プラグ』する場合。
アダプターを導入し、構成した後、装置のプラグを抜いたり、リスタートしたりせずに、アダプターを起動することができます。
- ダイヤル回線を装置に追加する場合
予備インターフェースを使用して、新規の V.25bis または ISDN ダイヤル回線を既存の V.25bis または ISDN インターフェースに追加します。

注: 予備インターフェースは、チャンネル化された ISDN T1/E1 インターフェースに追加することはできません。
- ATM LAN エミュレーション・クライアントを追加する場合
予備インターフェースを使用して、トークンリングまたはイーサネット ATM LAN エミュレーション・クライアントを既存の ATM インターフェースに追加します。
- バーチャル・ネットワークを既存の ESCON チャンネル・アダプターまたは並列チャンネル・アダプターに追加しています。

予備インターフェースを構成するには、以下のようになります。

1. **configuration** と入力して、CONFIG プロセスにアクセスする。
2. **set spare-interfaces** コマンドを使用して、予備インターフェースの数を構成する。
3. **Ctrl-P** を押して、CONFIG プロセスを終了する。
4. 装置をReload する。

例:

```
* configuration
Config> set spare 2
Config>
*reload
Are you sure you want to reload the gateway? (Yes or [No]) yes
```

装置をreloadsすると、予備インターフェースは空き装置として導入されます。

予備インターフェースの 1 つを使用するには、次のようにします。

1. 新しいアダプターをアダプター・スロットに挿入する。

注: ESCON または並列チャンネル・アダプターを使用している場合は、追加のアダプターを使用せずに、接続された各ネットワークごとに予備インターフェースを定義することができます。この場合では、このステップを無視することができます。

2. **configuration** と入力して、CONFIG プロセスにアクセスする。
3. **add device** コマンドを使用して、an interface or a dial circuit を追加する。
4. **net** コマンドを使用して予備インターフェースを構成し、インターフェースを構成するか、ATM LAN エミュレーション・クライアントを追加します。
5. **protocol** および **feature** コマンドを使用して、種々のプロトコルおよび機能を構成する。
6. **Ctrl-P** を押して、CONFIG プロセスを終了する。
7. **console** と入力して、GWCON プロセスにアクセスする。
8. **activate** コマンドを使用して、新規インターフェースをネットワークにオンラインにする。

次の例は、IP プロトコルが使用可能にされた新規ダイヤル回線を構成し、起動する方法を示しています。ダイヤル回線と IP プロトコルの構成は示されていません。

例:

```
*configuration
Config> add device dial-circuit
Config> net 6
Circuit configuration
Circuit config>
:
Here you would configure the dial circuit
:
Circuit config> exit
Config> protocol ip
IP>
:
Here you would configure the IP protocol on the dial circuit.
:
IP>exit
Config>
*console
+ activate 6
```

次の例では、IP プロトコルが構成されている新しい ATM LAN エミュレーション・クライアントを構成して、起動する方法を示します。ATM LAN エミュレーション・クライアントおよび IP 構成は示されていません。

```
* configuration
Config> net 0
ATM User Configuration
ATM Config> le-client
ATM LAN Emulation Clients Configuration
LE Client config> add token-ring
Added Emulated LAN as interface 6
LE Client config> config 6
```

CONFIG プロセスの使用

```
ATM LAN Emulation Client configuration
⋮

(Here you would configure the ATM LAN Emulation Client)
⋮

Token Ring Forum Compliant LEC Config> exit
LE Client config> exit
ATM Config> exit
Config> protocol ip
IP Config>
⋮

(Here you would configure IP on the ATM LAN Emulation Client)
⋮

IP Config> exit
Config> write
ctrl-p
* console
+ activate 6
Interface 6 activated successfully
```

予備インターフェースの制約事項

以下の条件下では、**activate** コマンドを使用して、ネットワーク上で新規インターフェースを起動することはできません。

- すでに **delete interface** コマンドを入力した場合。**いずれかの** インターフェースを削除した場合は、装置をリスタートする必要があります。予備インターフェース (リストに **null** と表示) は削除できません。
- 予備インターフェースが、プロトコルまたはフィーチャーを使用可能にする唯一のインターフェースである場合。プロトコルまたはフィーチャーは、既存のインターフェース上ですでに使用可能にされていないと、予備インターフェースで使用することはできません。
- 新規の予備インターフェースのヘッダー・サイズまたはトレーラー・サイズが、他のインターフェースのサイズより大きい場合
- 新規インターフェース用の受信バッファを割り当てるためのメモリーが不十分である場合

このような場合には、装置をリスタートしないと、新規インターフェースをオンラインにすることはできません。

以下のインターフェースは、予備インターフェースとして構成することは可能ですが、**activate** コマンドを使用してネットワーク上で起動することはできません。

- ATM
- SDLC
- SDLC リレー
- V.25bis
- PPP マルチリンク・マスターおよび専用リング・ネット

装置をリスタートしないと、これらのインターフェースをオンラインにすることはできません。

以下のプロトコルは、予備インターフェース上で構成することは可能ですが、**activate** コマンドを使用してネットワーク上で起動することはできません。

- LNM
- OSI/DECnet V
- XTP

注: 構成プログラムを使用している場合は、以下の手順を実行して、予備インターフェースを使用できるようにします。

1. 装置の予備インターフェースの構成変更を行う。
2. 装置上で **activate** コマンドを入力して、予備インターフェース、プロトコル、またはフィーチャーをオンラインにする。
3. 構成プログラムを使用して、構成を検索する。
4. 検索した構成を、構成プログラム・データベースに保管する。

機能によっては、制約があります。制約は次のとおりです。

APPN	予備インターフェースでこのプロトコルをアクティブにするためには、最初にインターフェースを起動し、次に起動されたインターフェース上でプロトコルを構成することが必要です。
帯域幅予約 (BRS)	予備インターフェースに BRS を構成するには、各ネットワーク・インターフェースの BRS を使用可能にして、フレーム・リレー回線をアクティブにしてから、予備インターフェースを起動することが必要です。予備インターフェースを起動した後、 BRS 構成コマンドを使用して、トラフィック・クラスを追加したり、トラフィック・クラスにプロトコルを割り当てるなどの変更を加えることができます。
DECnet IV	予備インターフェースでこのプロトコルをアクティブにするためには、最初にインターフェースを起動し、次に起動されたインターフェース上でプロトコルを構成することが必要です。構成変更を起動するには、 DECnet IV set コマンドを使用します。
フレーム・リレー	<ul style="list-style-type: none"> • ダイアル回線の基本ネットがすでにアクティブになっていないと、FR ダイアル回線インターフェースを起動することはできません。 • 予備インターフェースに必要なフレーム・サイズ、MAC ヘッダー、またはトレーラーが、すでに基本ネットに割り当てられている他のダイアル回線よりも大きい場合、FR ダイアル回線の起動は失敗します。 • 装置のデータ圧縮がすでにアクティブになっていないと、データ圧縮用に定義された予備インターフェースのデータ圧縮は機能しません。
BGP	新しい近隣を起動するには、 BGP reset neighbor コマンドを使用します。
IPX	予備インターフェースの静的ルート、静的サービス、およびフィルター・リストをアクティブにするには、 reset コマンドを使用します。
PPP	<ul style="list-style-type: none"> • 装置のデータ圧縮がすでにアクティブになっていないと、データ圧縮用に定義された予備インターフェースのデータ圧縮は機能しません。 • 装置のブロック・バッファが小さすぎて 1500 バイト PPP MRU をサポートできない場合、予備 PPP インターフェースを起動することはできません。 • ダイアル回線の基本ネットがすでに起動されていないと、PPP ダイアル回線インターフェースを起動することはできません。 • 予備インターフェースに必要なフレーム・サイズ、MAC ヘッダー、またはトレーラーが、すでに基本ネットに割り当てられている他のダイアル回線よりも大きい場合、PPP ダイアル回線の起動は失敗します。

CONFIG プロセスの使用

ブリッジング	<ul style="list-style-type: none">ブリッジングがすでにアクティブになっていない場合予備インターフェースに NetBIOS フィルターが定義されている場合予備インターフェースにより、ブリッジ個別設定または動作が変更される場合 (たとえば、純粋な TB ブリッジに SR ポートを追加するなど)
IP	アクセス制御およびパケット・フィルターの構成変更をオンラインにするには、reset IP コマンドを使用します。
チャンネル・ バーチャル・ ネット (MPC、LCS、 LSA)	予備インターフェースは、その構成済みのサブチャンネルが別のインターフェースによりすでに使用中であるか、共用されている場合は、起動できません。
WAN 復元/ WAN 再ルート	以下の条件が存在する場合、予備インターフェースは起動できません。 <ul style="list-style-type: none">予備インターフェースが WRS 1 次として構成されており、構成済みの WRS 2 次が、すでに WRS 1 次、WRR 1 次、または WRR 代替である場合予備インターフェースが WRS 1 次として構成され、構成済みの WRS 2 次が、すでに他の WRS 1 次を復元するために起動されている場合予備インターフェースが WRS 2 次として構成されており、構成済みの WRS 1 次が、すでに WRS 2 次、WRR 1 次、または WRR 代替である場合予備インターフェースが WRS 2 次として構成されており、構成済みの WRS 1 次が、すでに他の WRS 2 次を復元するために起動されている場合予備インターフェースが WRR 1 次として構成されており、構成済みの WRR 代替が、すでに WRS 1 次、WRS 2 次、WRR 1 次、または WRR 代替である場合予備インターフェースが WRR 代替として構成されており、構成済みの WRR 1 次が、すでに WRS 1 次、WRS 2 次、または WRR 代替である場合予備インターフェースが WRR 代替として構成されており、構成済みの WRR 1 次が、すでに他の WRR 代替による復元が起動されている場合

インターフェースのリセット

ときには、装置をリスタートせずに、ネットワーク・インターフェースを、そのブリッジングおよびルーティング・プロトコルとともに、構成変更することが必要になる場合があります。reset コマンドを使用すると、ネットワーク・インターフェースを使用不可にした後、新しいインターフェース、ブリッジングおよびルーティング構成パラメーターを使用して使用可能にすることができます。

インターフェース、プロトコル、およびフィーチャーの構成パラメーターの変更は、CONFIG プロセス (talk 6) コマンドを使用して行います。talk 6 コマンドは、構成メモリーの内容に影響を与えます。構成変更をアクティブにするには、GWCON プロセス (talk 5) reset コマンドを出します。

インターフェースのリセットは、以下の手順で行います。

1. CONFIG プロセス (talk 6) にアクセスする。

2. **net** コマンドおよび他のコマンドを使用して、構成パラメーターを変更する。
3. **protocol** および **feature** コマンドを使用して、インターフェースに基づく構成パラメーターを変更する。
4. **Ctrl-P** を押して、CONFIG プロセスを終了する。
5. GWCON プロセス (talk 5) にアクセスする。
6. **reset** コマンドを使用して、インターフェースおよびインターフェース上のプロトコルとフィーチャーをリセットする。

例:

```
* configuration
Config>net 1
PPP Config>

... change PPP parameters ...

PPP Config>exit
Config>protocol ipx
IPX Config>

... change IPX parameters on the PPP interface ...

IPX Config>exit
Config>
*talk 5
+reset 1
Resetting net 1 PPP/0...successful
```

注: 構成プログラムを使用している場合は、既存のインターフェースへの構成変更を行うには次のようにします。

1. 装置上のインターフェースの構成変更を行う。
2. **reset** コマンドを入力して、インターフェース、プロトコル、およびフィーチャーパラメーターをリセットする。
3. 構成プログラムを使用して、構成を検索する。
4. 検索した構成を、構成プログラム・データベースに保管する。

インターフェースのリセットに関する制約事項

以下の場合、**reset** コマンドを使用してネットワーク・インターフェースをリセットすることはできません。

- すでに **delete interface** コマンドを入力した場合。いずれかのインターフェースを削除した場合は、装置を再ロードする必要があります。
- ハードウェアまたはデータ・リンク・タイプを変更した場合。たとえば、データ・リンク・タイプを PPP からフレーム・リレーに変更した場合などです。
- より大きい MTU を構成した場合
- インターフェース上にルーティング・プロトコルまたはブリッジングを構成したが、そのルーティング・プロトコルまたはブリッジングが現在、装置上でアクティブになっていない場合

このような状態では、装置を再ロードしないと、構成変更を起動することができません。

以下のタイプのインターフェースは、構成パラメーターを変更することはできませんが、**reset** コマンドを使用してその変更を起動することはできません。

CONFIG プロセスの使用

- ATM
- PPP マルチリンク・マスターおよび専用リング・ネット
- ISDN
- SDLC
- SDLC リレー
- V.25bis

装置を再ロードしないと、構成変更を起動することはできません。

以下のプロトコルおよびフィーチャーは、構成パラメーターを変更することはできませんが、**reset** コマンドを使用してその変更を起動することはできません。

- AppleTalk
- Vines
- OSI/DECnet V
- LNM
- XTP
- WAN 復元
- WAN 再ルート

装置を再ロードしないと、構成変更を起動することはできません。

また、機能によっては、制約もあります。制約は次のとおりです。

PPP ダイアル回線 PPP ダイアル回線は、ダイヤル回線パラメーターを変更した場合は、リセットできません。

フレーム・リレー・ダイヤル回線 フレーム・リレー・ダイヤル回線は、ダイヤル回線パラメーターを変更した場合は、リセットできません。

圧縮 圧縮は、大きいサイズのヘッダーおよびトレーラーを必要とします。すでに他のインターフェース上で圧縮が使用可能になっていない場合、ヘッダーおよびトレーラーのサイズが小さくなり過ぎる可能性があります。この場合、インターフェース上の圧縮は自動的に使用不可にされ、ELS メッセージがログに記録されます (インターフェースのリセット全体が失敗するのではなく)。

ESCON 基本ネット ESCON 基本ネットをリセットすると、すべての関連するバーチャル・ネットは自動的にリセットされます。

PCA 基本ネット PCA 基本ネットをリセットすると、すべての関連するバーチャル・ネットは自動的にリセットされます。

チャンネル・バーチャル・ネット (MPC、LCS、LSA) 次のバーチャル・ネット・パラメーターをリセットするには、ESCON または PCA 基本ネットをリセットする必要があります。Subchannels (adding/deleting/changing/moving)、LAN type、LAN number、Block timer、Acknowledgement length。

ブリッジング	<ul style="list-style-type: none"> ブリッジングがすでにアクティブになっていない場合 リセットするインターフェースに NetBIOS フィルターが定義されている場合 リセット・インターフェースにより、ブリッジ個別設定または動作が変更される場合 (たとえば、純粋な TB ブリッジに SR ポートを追加するなど)
BGP	近隣の構成変更を起動するには、BGP reset neighbor コマンドを使用します。
APPN	構成変更を起動するには、 activate_new_config コマンドを使用します。
IPX	静的ルート、静的サービス、およびフィルター・リストの構成変更を起動するには、IPX reset コマンドを使用します。
DNA IV	構成変更を起動するには、DNA IV set コマンドを使用します。
SNMP	構成変更を起動するには、SNMP revert コマンドを使用します。

システム・ダンプの使用

2210 を使って問題をデバッグするための便利なツールは、システム・ダンプです。ダンプとは、システムがハード・ディスク (ある場合)、またはネットワーク上のリモート・ホスト に保管する圧縮されたスナップショットです。

ダンプを構成するには、次のようにします。

- どの 3 つのダンプ・ファイルを保管するか指定する。詳細については、92 ページを参照してください。
- ダンプの発生後、ダンプを再び使用可能にしたいかどうかを指定する。詳細については、91 ページを参照してください。
- 2210 でダンプを使用可能にする。詳細については、78 ページを参照してください。

システム・ダンプの状況を表示するか、システムからダンプを検索できます。それぞれ、96ページの『System View』および 95ページの『System Retrieve』を参照してください。

CONFIG への出入り

OPCON から CONFIG に入るか、CONFIG プロンプトを入手するには、**configuration** コマンドを入力します。あるいは、OPCON **talk** コマンドと PID を入力して、CONFIG を表示させることもできます。CONFIG の PID は 6 です。

* **configuration**

または

* **talk 6**

コンソールに CONFIG プロンプト (Config>) が表示されます。このプロンプトが表示されない場合は、再度 **Enter** キーを押してください。

CONFIG プロセスの使用

CONFIG を終了して OPCON プロンプト (*) に戻るには、インターセプト文字を入力します。(デフォルトは **Ctrl-P** です。)

CONFIG コマンド

この節では、個々の CONFIG コマンドについて説明します。各コマンドについて、説明、構文の要件、および例を示します。CONFIG コマンドの要約を表5 に示します。

CONFIG 環境にアクセスした後、Config> プロンプトで構成コマンドを入力します。

表 5. CONFIG コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Add	装置構成にインターフェースを追加するか、装置にユーザーを追加します。
Boot	Boot CONFIG コマンド・モードに入ります。
Change	ユーザーのパスワード、またはこのインターフェースに関連するユーザーのパラメーター値を変更します。インターフェースのロット/ポートも変更します。
Clear	構成情報を消去します。
Delete	ルーター構成からインターフェースを削除するか、構成済みのユーザーを削除します。システム・ダンプ・ファイルも削除します。
Disable	コマンド完成を使用不可にし、リモート・コンソールからのログインを使用不可にし、モデムの使用を使用不可にします。
Enable	コマンド完成を使用可能にし、リモート・コンソールからのログインを使用可能にし、モデムの使用を使用可能にします。
Event	イベント・ログ・システム構成環境に入ります。
Feature	通常の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、独立した装置フィーチャーの構成コマンドへのアクセスを提供します。
List	システム・パラメーター、ハードウェア構成、ユーザーの全リスト
Load	オプションのソフトウェア・パッケージをリスト、追加、または削除する。
Network	指定されたネットワークの構成環境に入ります。
Patch	装置のグローバル構成を変更します。
Performance	基本プロセッサの使用状況の統計のスナップショットを提供します。
Protocol	指定されたプロトコルのコマンド環境に入ります。
Qconfig	Quick Config プロセスを開始します。
Set	バッファ、ホスト名、非活動タイマー、パケット・サイズ、プロンプト・レベル、予備インターフェースの数、ダンプ・パラメーター、ロケーション、および連絡担当者など、システム全体のパラメーターを設定します。
System Retrieve	ダンプを検索します。
System View	ダンプ設定値および現行のダンプ状況を表示します。ダンプの要約も表示します。
Time	システム時刻を維持し、コンソールに表示します。
Unpatch	変更した変数をデフォルト値に復元します。
Write	不揮発性メモリーに現行の構成情報を書き込みます。

Add

add コマンドは、インターフェースを構成に追加したり、ユーザー・アクセスのために使用します。このコマンドは、不注意で構成を消失した場合、装置レコードを再作成するのにも使用されます。

構文:

```
add                callback . . .
                   device
                   isdn-address . . .
                   ppp-user
                   tunnel-profile
                   user . . .
                   v25-bis-address
```

callback

ISDN 上のコールバックに関する情報を追加、削除、またはリストするには、**add callback** コマンドを使用します。

Add 認証リストにコールバック番号を追加します。

Delete 認証リストからコールバック番号を削除します。

Lists 認証リストおよびその他の関連する情報を表示します。

device *device_type additional-config-info*

add device コマンドでは、インターフェース装置タイプ (*device_type*) を入力する必要があります。追加の構成パラメーターを入力するよう促されます。この追加情報は、装置およびプラットフォームによって異なります。装置タイプと構成パラメーターについての追加情報は、18ページの『装置の追加』を参照してください。

注: 複数のインターフェースを追加している場合は、それらを追加する順番が重要です。装置は、インターフェースが追加されるときにインターフェース番号を順次割り当てるからです。このインターフェース番号は、装置リスト内のインデックス番号です。これは、装置を他のプロトコル構成情報 (たとえば、装置に関連する IP アドレスなど) とリンクします。(詳細については、81ページの『List』の **list devices** コマンドを参照してください。)

ネットワーク・インターフェースに関連する装置およびプロトコル構成情報はすべて、インターフェース番号別に保管されます。インターフェース番号を変更すると、プロトコル内の装置構成情報の大部分が無効になります。

例:

```
add device atm
Device Slot #(1-8) [1]? 2
Adding CHARM ATM Adapter device in slot 2 port 1 as interface x
(where x is the interface number assigned)
```

CONFIG コマンド

どの装置を追加できるか判別するには、**add devices ?** コマンドを使用します。

isdn-address *address-name network-dial-address network-subdial-address*

ルーターと通信する ISDN エンドポイントのローカル番号とリモート番号を追加します。

address-name

何でもかまいません (ポートの記述など)。

network-dial-address

ローカル・ポートまたはあて先ポートの電話番号です。

network-subdial-address

インターフェースを PBX に接続したときに解釈される、電話番号の追加部分 (内線番号など)。このパラメーターはオプションです。

注: 句読点 (括弧やダッシュなど) も使用できますが、句読点は有効文字とはみなされません (ルーターは数字だけを使用します)。

```
Example: add isdn-address line 1 local
Assign network dial address [0 - 32 digits]? 1 2345 67
Assign network subdial address [0 - 19 digits]? 98765
```

ppp-user

リモート・ユーザーのユーザー・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 DIAL クライアントの PPP ユーザーを追加します。次の条件のいずれかが存在する場合には、PPP ユーザーを構成する必要があります。

- PPP 認証プロトコル、PPP 暗号化、ユーザーにダイヤルアウト・フィーチャーの使用を許可している場合。暗号化制御プロトコル (ECP) または Microsoft ポイント・ポイント暗号化 (MPPE) のいずれかのタイプの暗号化のために PPP ユーザーを構成する必要があります。ただし、MPPE では暗号化キーが必要です。
- PPP ユーザー・データベースを装置でローカルに保管または管理したい場合。PPP ユーザー情報を RADIUS、TACACS、または TACACS+ サーバーから入手するようにしたい場合は、ローカル PPP ユーザーを構成する代わりに、認証フィーチャーを構成する必要があります。

注: MPPE は RADIUS、TACACS、または TACACS+ サーバーを使用することができません。MPPE の場合、PPP ユーザー・データベースはローカル側にある必要があります。

ユーザーに対し ECP が使用可能にされた場合、PPP ユーザー名、パスワード、IP アドレス、および暗号化キーを入力するよう求められます。

DIAL 機能がソフトウェア・ロードに含まれている場合、これは DIAL ユーザーであるかどうかを尋ねられます。

DIALs クライアントにユーザーを追加している場合は、ホスト名、ルートのタイプ、ネットワーク・マスク、接続時間、およびコールバック情報の入力を求めるプロンプトが出ます。

詳しくは、フィーチャーの使用と構成の『LAN へのダイヤルイン・アクセス (DIAL) サーバーの使用』を参照してください。

装置上にローカルに保管されるユーザー・プロファイルは、以下から構成されます。

Name 認証時に使用される、PPP ユーザーのユーザー ID。 526ページの『PPP 認証プロトコル』を参照してください。

Password

認証時に使用される、ユーザーと装置に認知されるパスワード。これは、最大 31 文字までの長さで、英数字から構成され、大文字小文字を区別します。詳しくは、526ページの『PPP 認証プロトコル』を参照してください。

Enter again to verify

確認のためにパスワードをもう一度入力します。

Allow inbound access

このユーザー・プロファイルへのインバウンド・アクセスを許可します。

有効値: yes、no

デフォルト値: no

Will user be tunneled?

このダイヤルイン・ユーザーを LNS へて先にトンネル伝送する必要があるかどうかを指定します。『yes』と入力する場合は、LNS に関する情報の入力を求めるプロンプトが出ます。

有効値: yes、no

デフォルト値: no

Number of days before account expiry

アカウントが失効する前の日数

有効値: 0 ~ 360

デフォルト値: 180

Number of grace logins allowed

パスワードが失効した後に許可されるログイン試行の数

有効値: 0 ~ 100

デフォルト値: 0

Hostname to use when connecting to this peer:

トンネルの設定時に ID として LNS に渡される、この LAC のローカル・ホスト名を指定します。

Tunnel Server endpoint:

このユーザーのトンネル伝送先の LNS の IP アドレスを指定します。

Type of Route

『Host Route』または『Net Route』です。

ホスト・ルートは通常、単一ユーザー・アクセスの場合に使用します。ネット・ルートは通常、ネットワーク・アクセスの場合に使用します。ネット・ルートの場合は、ネットマスクも入力できます。

IP Address

ユーザーに割り当てられる IP アドレス

要求された場合にダイヤルイン・クライアントに提供される、ユーザー・プロファイルに基づく IP アドレスです。2210 には、ダイヤルイン・クライアントの IP アドレスを入手するさまざまな方法があります。詳細については、533ページの『IP 制御プロトコル』を参照してください。

有効値: 任意の有効な IP アドレス

デフォルト値: なし

Net-Route Mask

ネットワーク・ユーザーのマスク

ダイヤルイン・ユーザーが、DIAL 使用可能の PPP インターフェースに接続している場合、ルーターは PPP セッションの間、自動的にそのクライアントに一時的な静的ルートを追加します。通常、この静的ルートは 255.255.255.255 (デフォルト値) のネットマスクを持っています。これは、その PPP リンクの反対側は単一の IP ホストであることを意味しています。ただし、このネットマスクは指定変更することが可能です。マスクを構成した場合、そのマスクは一時ルートを追加するときに使用されます。これの例は、小規模なルーターが、ホスト間の単一ルートを使用して、DIAL 使用可能のルーターにダイヤルインする場合です。この小規模オフィス・ルーターへの単一ルートは、ユーザー・プロファイルに基づいて自動的に導入されるので、2つのホスト間のルーティング・プロトコルを構成する必要はなくなり、低速リンク上でのルーティングによる通信量のオーバーヘッド軽減することができます。

Hostname

動的 DNS を使用するためにプロキシ DHCP サーバーに送信されるホスト名。詳しくは、フィーチャーの使用と構成の『LAN へのダイヤルイン・アクセス (DIAL) サーバーの使用』を参照してください。

Time-Allotted

DIAL ユーザーに接続できる時間の長さ。これは、このセッションの合計時間を指しており、非活動タイマーと混同しないようにしてください。

有効値: 0 ~ 71 827 788 分 (0=無制限)

デフォルト値: 0

Callback type

コールバック方式。『Roaming』または『Required』のいずれかです。コールバック・パラメーターは、ルーターがユーザーをコールバックするかどうか、およびコールバックするときの番号を指定するのに使用します。詳細については、530ページの『PPP コールバックの構成』を参照してください。

Set encryption key

このユーザー/ポートの ECP 暗号化を使用可能にするかどうかを指定します。

有効値: yes、no

デフォルト値: no

ECP encryption key

16 文字の ECP 暗号化キーを入力します。

このパラメーターが表示されるのは、talk 6 PPP Config> **enable ecp** コマンドを使用して PPP 暗号化制御プロトコル (ECP) が使用可能にされている場合のみです。MPPE は暗号化キーを必要としません。この暗号化キーは、PPP 暗号化制御プロトコル (ECP) によって使用されます。フィーチャーの使用と構成の『暗号化プロトコルの使用と構成』を参照してください。

Disable user

ユーザー・プロファイルを使用不可にします。

有効値: yes、no

デフォルト値: no

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
```

ECP 暗号化を使った例:

CONFIG コマンド

```
Config> add ppp-user
Enter name: [ ]? ppp_user2
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALS' user? (Yes, No): [Yes]
Type of route? (hostroute, netroute): [hostroute]
Number of days before account expiry[0-1000] [0]?
Number of grace logins allowed after an expiry[0-100] [0]?
IP address: [11.0.0.185]?
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No] 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):
ECP encryption key is set.
Disable user ? (Yes, No): [No]
```

```
PPP user name: ppp_user2
User IP address: 11.0.0.185
Netroute Mask: 255.255.255.255
  Hostname:          Virtual Conn: disabled
  Time allotted: Box Default
  Callback type: disabled
  Dial-out: disabled
  Encryption: enabled
  Status: enabled
  Login Attempts: 0
  Login Failures: 0
  Logout Attempts: 0
  Account Expiry:    Password Expiry:
Is information correct? (Yes, No, Quit): [Yes]

User 'ppp_user1' has been added
```

tunnel *tunnel-name*

IP ネットワーク通したルーターへのトンネル同位間アクセスを指定します。これにより、同位 (相手) はルーターへのトンネル伝送 PPP セッションを開始できるようになります。トンネルを構成するには、以下のものを指定する必要があります。

Name トンネル伝送のピアのホスト名

Hostname to use when connecting to this peer

このピアに接続するとき使用するローカル・ホスト名。この名前は、ピア上のホストの名前を識別するのに使用します。

Set shared secret

共用される機密を使用するかどうかと指定します。

Shared Secret

LAC と LNS 間で共有される機密。トンネルの両側で正確に一致していることが必要です。

Enter again to verify

確認のために共用された機密を入力します。

Tunnel-Server endpoint address

トンネル伝送のピア (LAC または LNS) の IP アドレス

例:

```
Config> add tunnel
Enter name: [ ]? tunne102
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

user *user_name*

装置へのユーザー・アクセスを許可します。最高 50 のユーザーに、装置へのアクセスを許可することができます。各 *user_name* は 8 文字で、大文字小文字を区別します。

最初のユーザーが追加されると、コンソール・ログインが自動的に使用可能にされます。追加された各ユーザーに、表6 に定義されている許可レベルの 1 つを割り当てる必要があります。

ユーザーを追加した場合は、ログイン認証をローカルに設定します。そうでない場合は、リモート・サーバーを使用しなければなりません。

表 6. アクセス許可

許可レベル	説明
システム管理者 (A)	構成およびユーザー情報を表示し、構成およびユーザー情報を追加/変更/削除します。システム管理者は、どのルーター機能にもアクセスできます。
オペレーター (O)	ルーター構成の表示、統計の表示、システム中断の有無を調べるテストの実行、ルーターの動作の動的変更、およびルーターのリスタートを行います。オペレーターは、固定されたルーター構成を変更することはできません。処置はすべて、システム・リスタートによってやり直すことができます。
モニター (M)	ルーターの構成および統計を表示しますが、ルーターの動作を変更したり、中断したりすることはできません。
技術サポート	パスワードを忘れたときに、サービス技術員がルーターにアクセスできるようにします。ユーザーに割り当てることはできません。

注: ユーザーを追加するには、管理許可が必要です。ユーザーを追加した後でルーターを再初期化する必要はありません。

例:

```
add user John
Enter password:
Enter password again:
Enter permission (A)dmin, (O)perations, (M)onitor [A]?
Do you want to add Technical Support access? (Yes or [No]):
```

Enter password

ユーザーのアクセス・パスワードを指定します。80 字の英数字に限定され、大文字小文字を区別します。

Enter password again

ユーザーのアクセス・パスワードを確認します。

Enter permission

ユーザーの許可レベル (A、O、または M を指定します (表6 を参照してください))。

v25-bis-address

ルーターと通信する V.25bis エンドポイントのローカルおよびリモートの番号を追加します。ネットワーク・アドレス名は、ポートの記述など、任意のもので構いません。最大 23 字までの印刷可能 ASCII 文字列を使用できま

CONFIG コマンド

す。 *network-dial-address* は、ローカル・ポートまたは先ポートの電話番号です。詳細については、673ページの『第39章 V.25bis ネットワーク・インターフェースの使用』を参照してください。

注: 句読点 (括弧やダッシュなど) も使用できますが、句読点は有効文字とはみなされません (ルーターは数字だけを使用します)。

Example: add v25-bis-address
remote-site baltimore 1-909-555-0983

Boot

boot コマンドは、Boot CONFIG コマンド環境に入るのに使用します。 Boot CONFIG 情報については、101ページの『第5章 ブート CONFIG プロセス』を参照してください。

構文:

boot

Change

change コマンドは、構成内のインターフェースの変更、ユーザー自身のパスワードの変更、またはユーザー情報の変更を行うのに使用します。

構文:

```
change                               device . . .  
                                       password  
                                       ppp_user . . .  
                                       tunnel-profile
```

device *device_type*

change device コマンドでは、以下のことができます。

- 既存のインターフェースのスロットを変更する。(インターフェース・レコード *n* 内のスロット *x* を *y* に変更する。ここで、スロット *y* は空になっています。)
- 既存のインターフェースのポートを変更する。(インターフェース・レコード *n* 内のポート *x* を *y* に変更する。ここで、ポート *y* は空になっています。)
- 2つの既存インターフェースのスロットをスワップする。(インターフェース・レコード内のスロット *x* とスロット *y* を *x* または *y* でスワップする。)
- 2つの既存のインターフェースのポートをスワップする。(1つのインターフェース・レコード内のポート *u* およびスロット *x* を、同じハードウェア・タイプの別のインターフェース・レコード内のポート *v* およびスロット *y* とスワップする。)

CONFIG コマンド

- 既存のインターフェース内のスロットを、別のインターフェース内のスロットで置き換える。(スロット x 用のインターフェース構成は、スロット y 用のインターフェース構成になります。スロット y 用のインターフェース・レコードは削除されます。)
- 1 つの既存のインターフェースのポートを、別のインターフェースのポートで置き換える。(スロット x ポート u 用のインターフェース構成は、スロット y ポート v 用のインターフェース構成になります。スロット y ポート v 用のインターフェース・レコードは削除されます。)

ターゲット・スロットが空でない場合、次のようになります。

1. 『swap』(スワップ) オプションを選択する場合、ソースとターゲットのスロットは、それらが表示されるすべてのインターフェース・レコードでスワップされます。
2. 『replace』(置き換え) オプションを選択する場合、スロット x 用のインターフェース構成はスロット y 用のインターフェース構成になります。スロット y 用のインターフェース・レコードが削除されます。

ターゲット・ポートが空でない場合、次のようになります。

1. 『swap』 オプションを選択する場合、ソースとターゲットのポートは、それぞれのインターフェース・レコード内でスワップされます (これらのインターフェース・レコード内のハードウェア・タイプが同一である場合)。たとえば、1 ポート ISDN T1/J1。
2. 『replace』 オプションを選択する場合、スロット x ポート u 用のインターフェース構成は、スロット y ポート v 用のインターフェース構成になります。スロット y ポート v 用のインターフェース・レコードは削除されます。

注: イーサネットまたはトークンリング・アダプター・カードは、スロット 3、4、7、または 8 に取り付けられる場合は、2 つの空のスロットを必要とします。したがって、トークンリングまたはイーサネット・アダプター・カードは、スロット 3 と 4 (または 7 と 8) の両方が空である場合のみ、スロット 3 か 4 (またはスロット 7 か 8) に取り付けることができます。

スロット 3 と 4 (または 7 と 8) の両方が空でないときに、トークンリングまたはイーサネット・アダプターのスロットをスロット 3 か 4 (または 7 か 8) に変更しようとする、変更は受け入れられず、68 ページの例『インターフェース 1 上のスロット 6 を空のスロット 8 に変更』に示されるような警告メッセージが出されます。

例 - インターフェース 1 上のスロット 1 を空のスロット 2 に変更 (置き換え):

```
Config>list dev
Ifc 0 CHARM ATM                Slot: 2 Port: 1
Ifc 1 CHARM ATM                Slot: 1 Port: 1

Config>change device
Which configured slot would you like to change? (1, 2) [2]? 1
Which slot would you like to change to? (1-2) [1]? 2

Configuration for slot 2 already exists. You can:
a - abort this operation
r - replace configuration
(Interface configuration for slot 1 will become interface
```

CONFIG コマンド

```
configuration for slot 2. Interface records for slot 2
will be deleted!)
s - swap configuration (slot 1 will be swapped with slot 2.)
r

Moved slot 2 to slot 1 in 1 intf (port) record...
```

```
Config>list dev
Ifc 0 CHARM ATM Slot: 2 Port: 1
```

例 - インターフェース 0 上のスロット 5 を空のスロット 7 に変更:

```
Config>list dev
Ifc 0 Token Ring Slot: 5 Port: 1
Ifc 1 Token Ring Slot: 6 Port: 1
Ifc 2 Token Ring Slot: 1 Port: 1
Ifc 3 8 port EIA-232E/V.24 PPP Slot: 2 Port: 0
Ifc 4 8 port EIA-232E/V.24 PPP Slot: 2 Port: 1
Ifc 5 8 port EIA-232E/V.24 PPP Slot: 2 Port: 2
Ifc 6 6 port V.35/V.36 PPP Slot: 3 Port: 0
Ifc 7 6 port V.35/V.36 PPP Slot: 3 Port: 5
Ifc 8 8 port EIA-232E/V.24 PPP Slot: 4 Port: 0
```

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 5, 6)[1]? 5
Change all ports on slot # 5 (Yes or No)? [Yes]: y
Which slot would you like to change to? (1-8) [1]? 7
```

```
Changed slot 5 to slot 7 in 1 intf (port) record...
```

```
Config>list dev
Ifc 0 Token Ring Slot: 7 Port: 1
Ifc 1 Token Ring Slot: 6 Port: 1
Ifc 2 Token Ring Slot: 1 Port: 1
Ifc 3 8 port EIA-232E/V.24 PPP Slot: 2 Port: 0
Ifc 4 8 port EIA-232E/V.24 PPP Slot: 2 Port: 1
Ifc 5 8 port EIA-232E/V.24 PPP Slot: 2 Port: 2
Ifc 6 6 port V.35/V.36 PPP Slot: 3 Port: 0
Ifc 7 6 port V.35/V.36 PPP Slot: 3 Port: 5
Ifc 8 8 port EIA-232E/V.24 PPP Slot: 4 Port: 0
```

これでインターフェース 0 はスロット 7 に変更されました。

例 - インターフェース 1 上のスロット 6 を空のスロット 8 に変更:

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 6, 7)[1]? 6
Change all ports on slot # 6 (Yes or No)? [Yes]: y
Which slot would you like to change to? (1-8) [1]? 8
```

```
Cannot add Token Ring to slot 8.
Slot 7 is occupied so Token Ring cannot be added in slot 8.
```

注: トークンリングまたはイーサネットでスロット3、4、7、および8に変更するための要件については、67ページの2の注を参照してください。

例 - インターフェース 1 上のスロット 6 を空でないスロット 1 にスワップ:

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 6, 7) [1] 6
Change all ports on slot # 6 (Yes or No)? [Yes]: y
Which slot would you like to change to? (1-8) [1]? 1
```

```
Configuration for slot 1 already exists. You can:
a - abort this operation
r - replace configuration
(Interface configuration for slot 6 will become interface
configuration for slot 1. Interface records for slot 1
will be deleted!)
s - swap configuration (slot 1 will be swapped with slot 6.)
s
```

```
Swapped slot 6 with slot 1 in 1 port record...
```

```
Config>list dev
Ifc 0 Token Ring Slot: 7 Port: 1
Ifc 1 Token Ring Slot: 1 Port: 1
Ifc 2 Token Ring Slot: 6 Port: 1
Ifc 3 8 port EIA-232E/V.24 PPP Slot: 2 Port: 0
Ifc 4 8 port EIA-232E/V.24 PPP Slot: 2 Port: 1
Ifc 5 8 port EIA-232E/V.24 PPP Slot: 2 Port: 2
```

```
Ifc 6 6 port V.35/V.36 PPP          Slot: 3 Port: 0
Ifc 7 6 port V.35/V.36 PPP          Slot: 3 Port: 5
Ifc 8 8 port EIA-232E/V.24 PPP      Slot: 4 Port: 0
```

インターフェース 2 とインターフェース 1 の構成がスワップされます。

例 - インターフェース 1 上のスロット 1 がスロット 6 に置き換えられ、インターフェース 1 が削除される:

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 6, 7) [1] 6
Change all ports on slot # 6 (Yes or No)? [Yes]: y
Which slot would you like to change to? (1-8) [1]? 1

Configuration for slot 1 already exists. You can:
a - abort this operation
r - replace configuration
   (Interface configuration for slot 6 will become interface
   configuration for slot 1. Interface records for slot 1
   will be deleted!)
s - swap configuration (slot 1 will be swapped with slot 6.)
r

Moved slot 6 to slot 1 in 1 intf (port) record...

Config>list dev
Ifc 0 Token Ring          Slot: 7 Port: 1
Ifc 1 Token Ring          Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP Slot: 2 Port: 0
Ifc 3 8 port EIA-232E/V.24 PPP Slot: 2 Port: 1
Ifc 4 8 port EIA-232E/V.24 PPP Slot: 2 Port: 2
Ifc 5 6 port V.35/V.36 PPP Slot: 3 Port: 0
Ifc 6 6 port V.35/V.36 PPP Slot: 3 Port: 5
Ifc 7 8 port EIA-232E/V.24 PPP Slot: 4 Port: 0
```

スロット 6 のレコードが元のスロット 1 のレコードに置き換えられ、他のインターフェースの番号が付け替えられます。

例 - スロット 2 を空のスロット 5 に変更:

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 7) [1]? 2
Change all ports on slot # 2 (Yes or No)? [Yes]: y
Which slot would you like to change to? (1-8) [1]? 5

Changed slot 2 to slot 5 in 3 intf (port) records...

Config>list dev
Ifc 0 Token Ring          Slot: 7 Port: 1
Ifc 1 Token Ring          Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP Slot: 5 Port: 0
Ifc 3 8 port EIA-232E/V.24 PPP Slot: 5 Port: 1
Ifc 4 8 port EIA-232E/V.24 PPP Slot: 5 Port: 2
Ifc 5 6 port V.35/V.36 PPP Slot: 3 Port: 0
Ifc 6 6 port V.35/V.36 PPP Slot: 3 Port: 5
Ifc 7 8 port EIA-232E/V.24 PPP Slot: 4 Port: 0
```

前にスロット 2 で構成されたインターフェース 2、3、および 4 がスロット 5 で構成されるようになります。

例 - ポート 1 スロット 5 を空のスロット 2 のポート 0 に変更:

```
Config>change device
Which configured slot would you like to change? (1, 3, 4, 5, 7) [1]? 5
Change all ports on slot # 5 (Yes or No)? [Yes]: n
Which port would you like to change in slot 5? (0, 1, 2) [0]? 1
Which slot would you like to change to? (1-8) [1]? 2
Which port would you like port 1 in slot 5 to move to in slot2?#(0-7)[0]? 0

Changed slot 5 port 1 to slot 2 port 0...

Config>list dev
Ifc 0 Token Ring          Slot: 7 Port: 1
Ifc 1 Token Ring          Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP Slot: 5 Port: 0
Ifc 3 8 port EIA-232E/V.24 PPP Slot: 2 Port: 0
Ifc 4 8 port EIA-232E/V.24 PPP Slot: 5 Port: 2
```

CONFIG コマンド

```
Ifc 5 6 port V.35/V.36 PPP          Slot: 3 Port: 0
Ifc 6 6 port V.35/V.36 PPP          Slot: 3 Port: 5
Ifc 7 8 port EIA-232E/V.24 PPP      Slot: 4 Port: 0
```

スロット 5 - ポート 1 にあったインターフェース 3 がスロット 2 ポート 0 に変更されます。

例 - ポート 0 スロット 2 をスロット 3 のポート 5 に変更 (異なるハードウェア・タイプ):

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 5, 7) [1]? 2
Change all ports on slot # 2 (Yes or No)? [Yes]: n
Which port would you like to change in slot 2? (0) [0]? 0
Which slot would you like to change to? (1-8) [1]? 3
Which port would you like port 0 in slot 2 to move to in slot 3? #(0-7) [0] 5

Aborting - source and target slots of different type.
```

例 - ポート 0 スロット 2 をスロット 4 のポート 5 に変更 (同じハードウェア・タイプ):

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 5, 7) [1]? 2
Change all ports on slot # 2 (Yes or No)? [Yes]: n
Which port would you like to change in slot 2? (0) [0]? 0
Which slot would you like to change to? (1-8) [1]? 4
Which port would you like port 0 in slot 2 to move to in slot 4? #(0-7)[0] 5

Changed slot 2 port 0 to slot 4 port 5...
```

```
Config>list dev
Ifc 0 Token Ring          Slot: 7 Port: 1
Ifc 1 Token Ring          Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP Slot: 5 Port: 0
Ifc 3 8 port EIA-232E/V.24 PPP Slot: 4 Port: 5
Ifc 4 8 port EIA-232E/V.24 PPP Slot: 5 Port: 2
Ifc 5 6 port V.35/V.36 PPP Slot: 3 Port: 0
Ifc 6 6 port V.35/V.36 PPP Slot: 3 Port: 5
Ifc 7 8 port EIA-232E/V.24 PPP Slot: 4 Port: 0
```

ポート 0、スロット 2 にあったインターフェース 3 がポート 5、スロット 4 に変更されます。

例 - ポート 5 スロット 4 をスロット 4 内のポート 1 に変更 (同じスロット):

```
Config>change device
Which configured slot would you like to change? (1, 3, 4, 5, 7) [1]? 4
Change all ports on slot # 4 (Yes or No)? [Yes]: n
Which port would you like to change in slot 4? (0, 5) [0]? 5
Which slot would you like to change to? (1-8) [1]? 4
Which port would you like port 5 in slot 4 to move to in slot 4? #(0-7) [0] 1

Changed slot 4 port 5 to slot 4 port 1...
```

```
Config>list dev
Ifc 0 Token Ring          Slot: 7 Port: 1
Ifc 1 Token Ring          Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP Slot: 5 Port: 0
Ifc 3 8 port EIA-232E/V.24 PPP Slot: 4 Port: 1
Ifc 4 8 port EIA-232E/V.24 PPP Slot: 5 Port: 2
Ifc 5 6 port V.35/V.36 PPP Slot: 3 Port: 0
Ifc 6 6 port V.35/V.36 PPP Slot: 3 Port: 5
Ifc 7 8 port EIA-232E/V.24 PPP Slot: 4 Port: 0
```

インターフェース 3 は、ポート 1、スロット 4 になりました。

例 - ポート 1 スロット 4 をスロット 5 の空でないポート 0 に変更 (スワップ):

```
Config>change device
Which configured slot would you like to change? (1, 3, 4, 5, 7) [1]? 4
Change all ports on slot # 4 (Yes or No)? [Yes]: n
Which port would you like to change in slot 4? (0, 1) [0]? 1
```



```
Which slot would you like to change to? (1-8) [1]? 5
Which port would you like port 1 in slot 4 to move to in slot 5? #(0-7) [0] 0

Configuration for slot 5 (port 0) already exists. You can:
a - abort this operation
r - replace configuration
   (Interface record for slot 4 port 1 will become interface
   configuration for slot 5 port 0. The interface record for
   slot 5 port 0 will be deleted!)
s - swap configuration (slot 5 port 0 will be swapped with slot 4
   port 1.)
s

Swapped slot 4 port 1 with slot 5 port 0...
```

```
Config>list dev
Ifc 0 Token Ring                Slot: 7 Port: 1
Ifc 1 Token Ring                Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 1
Ifc 3 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 0
Ifc 4 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 2
Ifc 5 6 port V.35/V.36 PPP      Slot: 3 Port: 0
Ifc 6 6 port V.35/V.36 PPP      Slot: 3 Port: 5
Ifc 7 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 0
```

インターフェース 2 とインターフェース 3 は、それらのポートとスロットの構成をスワップしました。

例 - ポート 1 スロット 4 をスロット 5 の空でないポート 0 に変更 (置き換え):

```
Config>change device
Which configured slot would you like to change? (1, 3, 4, 5, 7) [1]? 4
Change all ports on slot # 4 (Yes or No)? [Yes]: n
Which port would you like to change in slot 4? (0, 1) [0]? 1
Which slot would you like to change to? (1-8) [1]? 5
Which port would you like port 1 in slot 4 to move to in slot 5? #(0-7) [0] 0

Configuration for slot 5 (port 0) already exists. You can:
a - abort this operation
r - replace configuration
   (Interface configuration for slot 4 port 1 will become interface
   configuration for slot 5 port 0. The interface record for
   slot 5 port 0 will be deleted!)
s - swap configuration (slot 5 port 0 will be swapped with slot 4
   port 1.)
r

Moved slot 4 port 1 to slot 5 port 0...
```

```
Config>list dev
Ifc 0 Token Ring                Slot: 7 Port: 1
Ifc 1 Token Ring                Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 0
Ifc 3 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 2
Ifc 4 6 port V.35/V.36 PPP      Slot: 3 Port: 0
Ifc 5 6 port V.35/V.36 PPP      Slot: 3 Port: 5
Ifc 6 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 0
```

インターフェース 2 はスロット 5 - ポート 0 に構成されます。元のインターフェース 3 は削除され、他のインターフェースの番号が付け替えられます。

password

現在ログインしているユーザーのパスワードを変更します。

注: ユーザー・パスワードを変更するには、管理許可が必要です。

例:

```
change password
Enter current password:
Enter new password:
Enter new password again:
```

Enter current password

現行パスワードを指定します。

Enter new password

新規パスワードを指定します。

Enter new password again

確認のために、新規パスワードを再び指定します。確認のために指定したパスワードが直前に指定した新規パスワードに一致しない場合、旧パスワードが有効のままになります。

ppp_user

特定の PPP ユーザーに関する情報を変更します。

構文:

```
change ppp_user           encryption-key
                             parameters
                             password
```

encryption-key

PPP ユーザーの暗号化キーを変更します。次の例は、暗号化キーを変更するためのダイアログを示しています。

例 - 暗号化キーの変更

```
Config>change ppp_user encryption-key
Enter user name: []? leslie
Enable encryption for this user/port (y/n) [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):
User 'leslie' has been updated
Config>
```

parameters

ユーザーのすべての ppp-user オプションを変更します。このパラメータは **add ppp_user** と同様に動作します。ただし、[] 内に示されている値は現行値であり、change コマンドは変更の確認を行ったり、変更時にリストを再表示したりしません。 **add ppp_user** コマンドの詳細については、59ページの『Add』を参照してください。

password

PPP ユーザーのパスワードを変更します。

例 - パスワードの変更

```
Config>change ppp_user password
Enter user name: []? sam
Password:
Enter password again:
User 'sam' has been updated
Config>
```

user 以前に **add user** コマンドを使用して構成したユーザー情報を変更します。

注: ユーザーを変更するには、管理許可が必要です。

Example:

```
change user
User name: []
Change password? (Yes or No)
Change permission? (Yes or [No])
```

tunnel-profile

トンネル伝送のピア (相手) の構成を変更します。

```

Config>change tunnel-profile
Enter name: []? lac.org
Enter hostname to use when connecting to this peer: [lns.org]?
set shared secret? (Yes, No): [No]
Tunnel-Server endpoint address: [11.0.0.1]? 11.0.0.2

profile 'lac.org' has been updated
Config>

```

Clear

clear コマンドは、不揮発性構成メモリーから装置の構成情報を削除するのに使用します。

考慮事項: このコマンドは、サービス技術員に連絡してから使用してください。

構文:

```

clear
  all
  ap2 (AppleTalk 2)
  arp (ARP)
  asrt (Adaptive Source Route Protocol)
  appn (Advanced Peer-to-Peer Networking)
  atm (Asynchronous Transfer Mode)
  auth (Authentication)
  bgp (Border Gateway Protocol)
  boot
  brs (Bandwidth Reservation)
  callback
  cmprs (Data Compression)
  dls (Data Link Switching)
  device
  dialer-circuit
  dn (DECnet)
  els (Event Logging System Information)
  fr (Frame Relay)
  gsmp (OSI)
  hdlc
  hod (Host On-Demand Client Cache) *
  hostname
  ip (IP)
  ip-security
  ipv6
  ipx (Novell IPX)

```

CONFIG コマンド

isdn
l2tp
lnm
mcf
named-profiles
nat
ndp6
ndr
osi (OSI)
ospf (OSPF routing protocol)
ppp (Point-to-Point)
prompt
rip6
rsvp
sdlc
snmp
srly (SDLC Relay)
tcp/ip-host
time (Time of day information)
tsf (Thin Server)
user
v25bis
vines (Banyan VINES)
webc (Web Server Cache) *
wrs (WAN Restoral feature)
x25
xtp

*注: HOD と WEBC は、同じソフトウェア・イメージ内で共存することはありません。

プロセスを不揮発性構成メモリーから消去するときは、**clear** コマンドとプロセス名を入力します。装置情報を除いて、すべての情報を構成メモリーから消去するときは、**clear all** コマンドを使用します。装置情報を含めて、すべての情報を消去するときは、**clear all** コマンドを使用し、次に **clear device** コマンドを使用します。

clear user コマンドは、装置コンソール・ログイン情報を除いて、すべてのユーザー情報を消去します。これは、デフォルト値が『disabled』であっても、使用可能のままにされます (使用可能として構成した場合)。

注:

1. ユーザー情報を消去するには、管理許可が必要です。
2. ソフトウェア・ロードに組み込まれているものに応じて、リストに他の項目が含まれている場合があります。

例: clear els

```
You are about to clear all Event Logging configuration information
Are you sure you want to do this (Yes or No):
```

注: 上記のメッセージは、どのパラメーター構成を消去している場合も表示されません。

Delete

delete コマンドは、構成に保管されている装置のリストからインターフェースまたは一定範囲のインターフェースを除去するため、あるいはユーザーを除去するために使用します。 **delete** コマンドを使用するには、管理許可が必要です。

構文:

```
delete                coprocessor . . .
                        interface . . .
                        dump-files
                        isdn-address
                        ppp_user . . .
                        tunnel
                        user . . .
                        v25-bis-address
```

interface [intfc# or intfc#range]

インターフェースを削除するには、インターフェースまたはネットワークの番号をコマンドの一部として入力します。(削除できるのは、**add device** コマンドを使用して追加した装置だけです。) 装置が割り当てるインターフェース番号を入手するには **list device** コマンドを使用します。

delete interface コマンドは、そのインターフェースの装置構成とプロトコル情報を削除します。ただし、装置は再ロードされるまで、前の構成の実行を続けます。

基本 ISDN インターフェースまたは基本 ATM インターフェースを削除しているときは、その基本ネット上で実行されているすべてのバーチャル・インターフェースも削除されます。したがって、ISDN インターフェースが削除されるときは、基本 ISDN インターフェース上にダイヤル回線があれば削除されます。また、ATM 基本ネットを削除しているときは、基本 ATM インターフェース上で稼働している LAN エミュレーション・クライアントはすべて削除されます。

一定範囲のインターフェースを削除する場合は、下の例に示すように、範囲の最初と最後のインターフェースをハイフンで区切って指定します。

CONFIG コマンド

`delete interface 13-21`

プロンプトで指示されたときに、インターフェース番号またはインターフェース番号の範囲を指定することもできます。

interface [*intfc#* or *intfc#range*]

インターフェースを削除するには、インターフェースまたはネットワークの番号をコマンドの一部として入力します。(削除できるのは、**add device** コマンドを使用して追加した装置だけです。) 装置が割り当てるインターフェース番号を入手するには **list device** コマンドを使用します。

`delete interface` コマンドは、そのインターフェースの装置構成とプロトコル情報を削除します。ただし、装置は再ロードされるまで、前の構成の実行を続けます。

基本 ISDN インターフェースまたは基本 ATM インターフェースを削除しているときは、その基本ネット上で実行されているすべてのバーチャル・インターフェースも削除されます。したがって、ISDN インターフェースが削除されるときは、基本 ISDN インターフェース上にダイヤル回線があれば削除されます。また、ATM 基本ネットを削除しているときは、基本 ATM インターフェース上で稼働している LAN エミュレーション・クライアントはすべて削除されます。

一定範囲のインターフェースを削除する場合は、下の例に示すように、範囲の最初と最後のインターフェースをハイフンで区切って指定します。

`delete interface 13-21`

プロンプトで指示されたときに、インターフェース番号またはインターフェース番号の範囲を指定することもできます。

isdn-address *address-name*

前に追加された ISDN アドレスを削除します。

注: *address-name* にスペースが含まれている場合 (たとえば、**remote site XYZ**)、コマンドを 1 行に入力することはできません。

`delete isdn-address` と入力して **Return** を押します。次に、プロンプトで指示されたら、名前を入力します。

ppp_user *user_name*

PPP ユーザー・データベースからユーザーを削除します。

tunnel-profile

トンネル・プロファイル・データベースからトンネルを削除します。

user *user_name*

指定されたユーザーの、装置へのユーザー・アクセスを削除します。

v25-bis-address *address-name*

前に追加された V25bis アドレスを削除します。

注: *address-name* にスペースが含まれている場合 (たとえば、**remote site Baltimore**)、コマンドを 1 行に入力することはできません。

`delete v25-bis-address` と入力して **Return** を押します。次に、プロンプトで指示されたら、名前を入力します。

Disable

disable コマンドは、コマンド完成を使用不可にし、リモート・コンソールからのログインを使用不可にし、モデムの使用を使用不可にするのに使用します。

構文:

```
disable
        command-completion
        console-login
        dump-memory . . .
        interface . . .
        reboot-system . . .
```

command-completion

disable command-completion コマンドは、自動コマンド完成機能を使用不可にするのに使用します。自動コマンド完成機能の説明については、26ページの『コマンド完成』を参照してください。

注: コマンド完成は、既存の構成の場合はデフォルトが *disabled* となり、新しい構成の場合はデフォルトが *enabled* になります。既存の構成を使用しており、コマンド完成を使用したい場合は、

enable command-completion コマンドを使用してこの機能を使用可能にする必要があります。

console-login

物理コンソール上でユーザー ID とパスワードの入力をユーザーに求めることを使用不可にします。デフォルトは使用不可です。

interface *interface*#

reload command. デフォルトは *enabled* (使用可能) です。

dump-memory

重大なエラーが発生すると、取り付けられたハード・ディスクへのシステム・メモリーのダンプを使用不可にします。

reboot-system

重大なエラーが発生したときに、システムのリブートを使用不可にします。ネットワーク・サービス要員がエラーをオンラインでトラブルシューティングしたい場合は、これが必要になる場合があります。システム・リブートは、メモリー・ダンプも使用不可にされない限り、使用不可にすることができません。メモリー・ダンプが使用可能にされているときにシステム・リブートを使用不可にしようとする、システム・リブートは打ち切られ、次のメッセージが表示されます。

```
System reboot not disabled: memory dumping must be disabled first
```

Enable

enable コマンドは、コマンド完成を使用可能にし、リモート・コンソールからのログインを使用可能にし、モデムの使用を使用可能にするのに使用します。

構文:

CONFIG コマンド

```
enable  
command-completion  
console-login  
dump-memory . . .  
interface . . .  
reboot-system . . .
```

command-completion

enable command-completion コマンドは、コマンド構文を補助する自動コマンド完成機能を使用可能にするのに使用します。自動コマンド完成機能の説明については、26ページの『コマンド完成』を参照してください。

console-login

物理コンソール上でユーザー ID とパスワードの入力をユーザーに求めることを使用可能にします。これはセキュリティーに役立ちます。管理ユーザーを構成せずにこの機能を使用可能にすると、次のようなメッセージが表示されます。

```
Warning: Console login is disabled until an  
administrative user is added.
```

注: 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 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、装置が認証サーバーに到達できない場合には、装置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しておくことにより、ロック状態を防止できます。

dump-memory

重大なエラーが発生した場合に、取り付けられたハード・ディスクへのシステム・メモリーのダンプを使用可能にします。これは、エラーの時点での装置の状態を保存して後でトラブルシューティングで使うことができるようにするのに必要な場合があります。ダンプ・メモリー機能は、システム・リブートが使用可能にされていない限り、使用可能にすることができません。システム・リブートが使用不可にされているときにダンプ・メモリー機能を使用可能にしようとする、ダンプ・メモリー機能は使用可能にされず、次のメッセージが表示されます。

```
System memory dump function not enabled: rebooting must be enabled first
```

最初の 3 つのダンプ・ファイルを保管するようにシステム・ダンプを構成し、ハード・ディスク上に 3 つのダンプ・ファイルがすでに存在する場合、ダンプ・メモリーを使用可能にすると、システムは次のメッセージを表示します。

```
*** System dump cannot be enabled until the   ***  
*** existing dump files are deleted.          ***
```

set dump enable-mode および **set dump save-mode** コマンドを参照してください。

例:

```
Config> enable dump  
Current System Dump Status:
```



```
System dump is currently disabled.
Number of existing dump files: 0
```

```
Enable system memory dumping? [No]: Yes
```

```
Current System Dump Status:
System dump is currently enabled.
Number of existing dump files: 0
```

注: このコマンドを入力するが、ハード・ディスクが使用可能でない場合、ドライブが使用不可能であることを示すメッセージが表示されます。

interface *interface#*

reload コマンドが出された後、インターフェースは使用可能になります。

modem-control [**carrier-wait or ring-wait**] [**service1 or service2**]

物理コンソールがモデムを介して装置に接続されている場合、物理コンソールでログインするために装置をセットアップします。このコマンドを使用する前に、必ず次のことを行ってください。

モデムを自動応答に設定する。

コンソールのボー・レートがモデムのボー・レートと等しいことを確認する。

モデムを装置に接続しているケーブルが正しく構成されていることを確認する。

ATE0 コマンドを使用して、エコーをオフにする。

ATQ1 コマンドを使用して、クワイエット・モードで稼働する。

必要なジャンパーがすべてセットされていることを確認する。詳細については、装置の *使用者の手引き* を参照してください。ログアウトすると、装置は自動的にモデムを停止します。また、モデムを使用中に、モデムが装置から切り離されると、装置はユーザーをログアウトします。

enable modem-control carrier-wait および

enable modem-control ring-wait コマンドの両方について、サービス・ポートを指定します。サービス・ポートを 2 つ持つ装置の場合は、どちらのサービス・ポートにモデムを接続したかも示すために、**service1** または **service2** を指定します。両方の サービス・ポートを使用可能にする場合は、それらを別々に使用可能にします。

注: すべての構成をクリアし、装置をリスタートしないと、モデム制御を使用可能にした後で装置とコンソールを接続することができません。

Request to Send を送信する前に、モデムからの carrier-detect 信号を待つように装置に指示することができます。これはモデム制御の標準的な方法です。

Request to Send または Data Terminal Ready を実行する前に、ring-indication 信号を待つように装置に指示することができます。これは初期のハンドシェイクを必要とする国のために提供されています。

例:

```
Config> enable modem-control carrier-wait service1
```

reboot-system

重大なエラーが発生した場合、システムのリブートが使用可能となります。

Event

event コマンドは、イベント・ログ・システム (ELS) 環境に入り、コンソールに表示されるメッセージを定義できるようにします。ELS についての説明は、169ページの『第10章 イベント・ログ・システム (ELS) の使用』を参照してください。

構文:

event

Feature

feature コマンドは、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装置フィーチャーの構成コマンドにアクセスするのに使用します。

構文:

feature [feature# or feature-short-name]

すべての 2210 フィーチャーには、次の方法で実行されるコマンドがあります。

- フィーチャーを初期構成して使用可能にしたり、後で構成変更を行うために、構成プロセスにアクセスする。
- 各フィーチャーに関する情報を表示したり、一時的な構成変更を行うために、コンソール・プロセスにアクセスする。

これらのプロセスにアクセスする手順は、すべてのフィーチャーで同じです。この手順を以下で説明します。

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には、**feature** コマンドの後に疑問符を入力します。

フィーチャーの構成プロンプトにアクセスするには、**feature** コマンドを入力し、その後続けてフィーチャー番号または短縮名を入力します。表7 は、指定できるフィーチャー番号と名前をリストしています。

表7. IBM 2210 フィーチャー番号と名前

フィーチャー番号	フィーチャー短縮名	アクセスするフィーチャー構成プロセス
0	WRS	WAN 復元/再ルート
1	BRS	帯域幅予約
2	MCF	MAC フィルター
4	VCRM	バーチャル・サーキットと資源管理
7	ES	符号化サブシステム
8	NDR	ネットワーク・ディスプレイ
9	DIALs	LANへのダイヤルイン・アクセス
10	AUTH	認証
11	IPSec	IP セキュリティー・フィーチャー・ユーザー構成
12	LAYER	レイヤー 2 トンネル・プロトコル、レイヤー 2 フィルター、ポイント・ポイント・トンネル・プロトコル

表 7. IBM 2210 フィーチャー番号と名前 (続き)

フィーチャー番号	フィーチャー短縮名	アクセスするフィーチャー構成プロセス
13	NAT	ネットワーク・アドレス変換機構ユーザー構成
14	TSF	シン・サーバー機能
15	WEBC	Web サーバー・キャッシュ ¹
15	HOD	ホスト・オンデマンド・クライアント・キャッシュ ¹
16	DHCP	DHCP サービス
20	POLICY	ポリシー・フィーチャー
21	DS	差別化サービス

¹HOD および WEBC は、同じソフトウェア・イメージ内で共存することはありません。そのため、これらは同じ機能番号を持っています。

フィーチャーの構成プロンプトにアクセスしたら、そのフィーチャー特有の構成コマンドの入力を開始することができます。CONFIG プロンプトに戻るには、フィーチャーの構成プロンプトから **exit** コマンドを入力します。

List

list コマンドは、すべてのネットワーク・インターフェースについての構成情報、または装置についての構成情報を表示するのに使用します。

構文:

```
list
configuration
devices
named-profile
isdn-address
patches . . .
ppp_users . . .
tunnel-profile
users . . .
v25-bis-address
vpd
```

configuration

装置に関する構成情報を表示します。

例: list configuration

```
Hostname: [none]
Maximum packet size: [autoconfigured]
Maximum number of global buffers: [autoconfigured]
Number of spare interfaces: 0
Console inactivity timer (minutes): 0
Physical console login: disabled
System rebooting on error: disabled
System memory dumping: disabled
Contact person for this node: [none]
Location of this node: [none]
```

Configurable Protocols:

CONFIG コマンド

```
Num Name Protocol
0 IP DOD-IP
3 ARP Address Resolution
4 DN DNA Phase IV
6 VIN Banyan Vines
7 IPX NetWare IPX
8 OSI ISO CLNP/ISIS/ISIS
9 DVM Distance Vector Multicast Routing Protocol
10 BGP Border Gateway Protocol
11 SNMP Simple Network Management Protocol
12 OSPF Open SPF-Based Routing Protocol
20 SDLC SDLC/HDLC-Relay
22 AP2 AppleTalk Phase 2
23 ASRT Adaptive Source Routing Transparent Enhanced Bridge
24 HST TCP/IP Host Services
25 LNM LAN Network Manager
26 DLS Data Link Switching
27 XTP X.25 Transport Protocol
28 APPN Advanced Peer-to-Peer Networking [HPR]
29 NHRP Next Hop Routing Protocol
30 APPN Advanced Peer-to-Peer Networking [ISR]
```

Configurable Features:

```
Num Name Feature
0 WRS WAN Restoral
1 BRS Bandwidth Reservation
2 MCF MAC Filtering
6 QOS Quality of Service
7 CMPRS Data Compression Subsystem
8 NDR Network Dispatching Router
10 AUTH Authentication
14 TSF Thin Server Function
```

26176 bytes of configuration memory free

devices [*device or devicerange*]

インターフェース番号とハードウェア・インターフェースの関係を表示します。このコマンドは、**add** コマンドを出して装置が正しく追加されているかどうかを検査するのにも使用できます。

また、次の例に示すように、一定範囲の装置をリストするように指定することもできます。

```
list dev 2-5
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
```

注: インターフェース番号またはインターフェースの範囲を指定しないと、すべてのインターフェースが表示されます。

例: list devices

```
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
Ifc 6 Ethernet Slot: 5 Port: 1
Ifc 7 Ethernet Slot: 5 Port: 2
Ifc 8 Ethernet Slot: 6 Port: 1
Ifc 9 Ethernet Slot: 6 Port: 2
Ifc 10 V.35/V.36 Frame Relay Slot: 8 Port: 0
Ifc 11 V.35/V.36 X.25 Slot: 8 Port: 1
Ifc 12 V.35/V.36 PPP Slot: 8 Port: 2
Ifc 13 V.35/V.36 PPP Slot: 8 Port: 3
Ifc 14 V.35/V.36 PPP Slot: 8 Port: 4
Ifc 15 V.35/V.36 PPP Slot: 8 Port: 5
```

注: 注記されている受信バッファ数は、受信バッファのデフォルト値からの例外報告です。**set receive buffers** コマンドについては、90ページの『Set』で説明しています。

isdn-address

現行 ISDN アドレス構成を表示します。

```
Example: list isdn-address
Address assigned name   Network Address   Network Subdial Address
-----
remote site XYZ        1 2345 67        98765
```

patches

patch コマンドを使用して入力されたパッチ変数の値を表示します。

例:

```
list patches
Patched variable      Value
-----
ping-size              60
ping-ttl               59
ethernet-security     3
```

ppp_users

特定の PPP ユーザー・プロファイル・パラメーターをリストします。

例: List of PPP users when DIALs is not in the software load

```
Config> list ppp_users
List (Name, Verb, User, Addr, Encr):

    PPP User Name: joe
    User IP Address: Interface Default
    Encryption: Not Enabled
```

例: List of PPP users when DIALs is in the software load

```
Config> list ppp_users
List (Name, Verb, User, Addr, Call, Time, Dial, Encr):

    PPP User Name: joe
    User IP Address: Interface Default
    Net-Route Mask: 255.255.255.255
    Hostname: <undefined>
    Time-Allotted: Box Default
    Call-Back Type: Not Enabled
    Dial-Out: Not Enabled
    Encryption: Not Enabled
```

list ppp_users を入力すると、ソフトウェアは以下の 1 つを入力するように求めるプロンプトを出します。

Name データベース内のすべての名前をリストします。

Verb 各ユーザーの詳細情報をリストします。各ユーザー・プロファイルに関するすべての情報をリストします。

User 単一ユーザーに関する詳細情報をリストします。

Addr (address)

各ユーザーのアドレス情報 (IP アドレス、ネットマスク、およびホスト名を含む) をリストします。

Call (callback)

各ユーザーのコールバック情報 (コールバックのタイプと番号を含む) をリストします。

Time 各ユーザーに構成された許容時間をリストします。

Encr (encryption)

各ユーザーについて、暗号化が使用可能かどうかをリストします。

tunnel-profile

トンネル・プロファイル・パラメーターを表示します。

例:

CONFIG コマンド

```
Config>list tunnel-profile
Endpoint      Tunnel name  Hostname
11.0.0.192    lac         1ns
1 TUNNEL record displayed.
Config>
```

Tunnel Name

構成されたピア (相手) の名前を指定します。

Server Endpoint

ピアの IP アドレス

Type ピア間接続のタイプを指定します。

Medium

トンネル伝送に使用されるプロトコルを指定します。

Local Host Name

ピアに接続するとき使用する、構成済みの名前を指定します。

users システムにアクセスするように構成されたユーザーを表示します。

例:

```
list users
USER      PERMISSION
joe       operations
mary      administrative
peter     monitor
```

v25-bis-address

現行の V25bis アドレス構成を表示します。V25bis アドレス構成は、ローカル・ポート (シリアル・ライン・インターフェース) またはあて先ポートのネットワーク・アドレスとネットワーク・アドレス名から構成されます。ネットワーク・アドレスは、ローカル・ポートまたはあて先ポートの電話番号です。ネットワーク・アドレス名は、ポートの記述など、任意のもので構いません。詳細については、673ページの『第39章 V.25bis ネットワーク・インターフェースの使用』を参照してください。

```
Example:
list v25-bis-address
Address assigned name      Network Address
-----
v25-1                      8982800
v25-2                      8980001
delaware                   1-666-555-4444
```

vpd ハードウェアとソフトウェアの重要プロダクト・データを表示します。

Load

load コマンドは、使用可能だが構成されていないソフトウェア・ロード内のパッケージ、またはソフトウェア・ロード内で構成されているパッケージをリストするのに、使用します。**load** コマンドは、ソフトウェア・パッケージを追加または削除するのにも使用します。

構文:

```
load                add package packagename
                     delete package packagename
                     list . . .
```

CONFIG コマンド

ソフトウェアは、複数のロード・モジュールに分割されます。これらのロード・モジュールはソフトウェア・パッケージにグループ化されます。これらのソフトウェア・パッケージの一部はオプションです。それらは製品と一緒に出荷されますが、自動的にロードされるわけではないからです。

暗号化を含むソフトウェア・パッケージは、インターネットを使用してアクセス可能な 2210 Web サーバーから入手できます。

任意選択のソフトウェア・パッケージをロードして実行するには、次のようにします。

1. **load add** コマンドを使用してパッケージを追加する。
2. リポートする。このアクションにより、オプションのソフトウェアが装置のメモリにロードされます。
3. オプションのソフトウェアを構成する。
4. 構成を保管する。
5. 装置をリポートする。このアクションは、ソフトウェアを新しい構成で使用可能にします。

add package *packagename*

ソフトウェア・パッケージをソフトウェアに追加します。*packagename* は、ソフトウェアに組み込みたいロード・モジュールのパッケージの名前です。

例: load add package appn

delete package *packagename*

ソフトウェアからソフトウェア・パッケージを除去します。*packagename* とは、ソフトウェアから除去したいロード・モジュールのパッケージの名前です。

例: load delete package appn

list 使用可能だが構成されていないソフトウェア・ロード内のパッケージ、またはソフトウェア・ロード内で構成されているパッケージのいずれかをリストします。次のいずれかを指定することができます。

available

構成されていない現行のソフトウェア・ロード内のソフトウェア・パッケージをリストします。

configured

構成されている現行のソフトウェア・ロード内のソフトウェア・パッケージをリストします。

Network

network コマンドは、サポートされるネットワークのネットワーク・インターフェース構成環境に入るのに使用します。インターフェース番号またはネットワーク番号をコマンドの一部として入力します。(インターフェース番号を入手するには、**CONFIG list device** コマンドを使用します。) 該当する構成プロンプト (たとえば、TKR Config>) が表示されます。必要なネットワーク・インターフェース・タイプの構成についての詳しい説明は、本書のネットワーク・インターフェース構成の章を参照してください。

CONFIG コマンド

構文:

network *interface#*

注:

1. ユーザーが構成可能なパラメーターを変更する場合、GWCON **reset interface** コマンドを使用するか、装置を **再ロード** して変更を有効にすることもできます。これを行うには、OPCON プロンプト (*) で **reload** コマンドを入力します。
2. ネットワーク・インターフェースは、すべてがユーザーによる構成が可能とは限りません。ユーザーが構成できないインターフェースの場合は、メッセージ `That network is not configurable.` を受け取ります。

Patch

patch コマンドは、装置のグローバル構成を変更するのに使用します。パッチ変数は不揮発性メモリーに記録され、即時に有効になります。装置を次回にリスタートするまで待つ必要はありません。このコマンドを使用するのは、一般的でない構成を扱う場合だけに限ります。普通に構成するものは、やはり特定の構成コマンドを使用して処理すべきです。以下に示すのは、このリリースで文書化され、サポートされている現行のパッチ変数のリストです。

構文:

patch *bgp-subnets*
dls-ignore-lfs
ethernet-security
filter-nr
ip-default-ttl
ip-mtu
lnm-link-via-tbport
more-lines
mosheap-lowmark
ospf-import-rate
ping-size
ping-ttl
ppp-echo
relax-jate
rip-static-suppress
tftp-max-rxto-time
tftp-min-rexmtime

bgp-subnets *new value*

BGP スピーカーが近隣にサブネット・ルートを公示するようにしたい場合は、*new value* を 1 に設定します。デフォルトは 0 です。

dls-ignore-lfs *new value*

1 に設定すると、回線の設定時に、DLSw は発信元ルーティング・フレーム内の『最大フレーム』サイズ・ビットを無視します。これにより、これらのビットを正しく設定しない一部の旧 LAN プロダクトに伴う回線設定の問題を回避することができます。デフォルトは 0 です。

ethernet-security *new value*

非ゼロ値に設定すると、データ部分が物理最小値の 60 バイト未満のイーサネット・パケットに適用される埋め込みをゼロにします。セキュリティ上の理由から、これが必要になる場合があります。デフォルト値: 0。

filter-nr

NetBIOS 『Name Recognized』を、ブリッジ・コードによってフィルターされる NetBIOS フレームの現行のリストと一緒にフィルターに掛けることができます。NetBIOS Name フィルターは、次のタイプのいずれでもない NetBIOS パケットをすべて通過させます。ADD_GROUP_NAME_QUERY、ADD_NAME_QUERY、DATAGRAM、NAME_QUERY。このパラメーターは、タイプのリストに NAME_RECOGNIZED を追加します。

ip-default-ttl *#_of_packets*

装置によって発信されるパケットで使用される TTL。デフォルト値は 64 です。

注: **set ttl** IP 構成コマンドを使用して、このパラメーターを設定することをお勧めします。(Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 1 巻の『IP の使用および構成』の章の『Set』の節を参照してください。) このパッチ変数は、旧リリースの構成との互換性のために残されています。

ip-mtu *bytes*

このパラメーターは、IP MTU サイズを指定された値に制限します。このパラメーターが設定されている場合、ネットワーク・インターフェースの IP MTU サイズは、ip-mtu の値とそのネットワーク・インターフェースに構成されているフレーム・サイズに収まる最大値のうちの小さい方の値に設定されます。

lnm-link-via-tbport *new value*

LNM がイーサネット透過型ブリッジ (TB) ポートを介してトークンリングにリンクできるようにします。

1 に設定されている場合、LNM リンクは許可されます。

0 (デフォルト) に設定されている場合、LNM リンクは許可されません。

more-lines *#_of_lines*

長い出力をリストするとき、コンソール上で表示される行数

mosheap-lowmark *new value*

このパラメーターは、空き MOS ヒープ・メモリーのパーセント値を指定します。この値に達すると、装置は out-of-memory (メモリー不足) エラーが近づいていることをオペレーターに知らせます。この通知により、装置がエラーを受け取って停止する前に、オペレーターは MOS ヒープ・メモリーを解放する処置を取ることができます。

CONFIG コマンド

オペレーターは通知を受け取ると、装置を再構成してリポートすることによって、ネットワークの故障率を最小化することができます。このパラメーターを 0 に指定すると、この警告は抑止されます。

有効値: 0 ~ 100

デフォルト値: 10

ospf-import-rate *rate*

1 秒当たりのインポートされるルートの数

ping-size *bytes*

IP> **ping** コマンドによって送信される ICMP PING パケットのデータ部分 (つまり、IP ヘッダーと ICMP ヘッダーを除いた部分) のサイズ。デフォルト: 56 バイト。(PING データのサイズは、*Nways* マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 1 巻の『IP の監視』の章の『Ping』の節で説明されている **ping** コマンドのパラメーターとして入力することもできます。)

ping-ttl *seconds*

IP>**ping** コマンドによって PING で送信される TTL (活動時間)。デフォルト: 64。(TTL は、*Nways* マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 1 巻の『IP の監視』の章の『Ping』の節で説明されている **ping** コマンドのパラメーターとして入力することもできます。)

ppp-echo *new value*

1 に設定すると、装置はどの PPP インターフェースでも PPP エコー要求を送信しません。リモート装置を動作可能に維持するために、PPP エコー要求は PPP 保守の一部としてリモート装置に送信されます。PPP を低速ラインで実行しており、そのラインを大きなデータ・パケットの転送に使用しているので、PPP インターフェースをアップに保つのに十分な頻度で PPP 保守パケットが交換されない場合に、この変数を使用可能にすることを考慮してください。

relax-jate

JATE ISDN 制限を緩和します。

rip-static-suppress *new value*

非ゼロ値に設定すると、インターフェースに IP config> **enable send static** コマンドが与えられない限り、静的ルートはそのインターフェースを介して RIP によって公示されなくなります。これは **enable send static** コマンドの意味を変更します。rip-static-suppress が 0 (デフォルト) のときは、RIP を介して公示されるルートのリストは、そのインターフェースの RIP フラグによって指定されたルートの集合になります。

tftp-max-rxto-time

tftp-max-rxto-time では、転送が失敗する前にパートナーからの応答を待つ最大時間を指定することができます。デフォルト値: 5 分

このパッチ変数の単位は秒です。

tftp-min-remtime

ftp-min-rexmtime では、送信された最後のパケットを再送する前にパートナーからの応答を待つ時間の最小間隔を指定することができます。デフォルト値: 1

このパッチ変数の単位は秒です。

注: 変更したいパッチ変数は、完全な名前を指定する必要があります。パッチ名に省略構文を使用することはできません。

Performance

performance コマンドは、Config> プロンプトで性能のための構成環境を入力するのに使用します。詳細については、247ページの『第12章 性能の構成および監視』を参照してください。

performance

Protocol

protocol コマンドは、Config> プロンプトで、装置に導入されたプロトコル・ソフトウェアの構成環境を入力するのに使用します。

構文:

protocol [prot# or prot_name]

protocol コマンドに続けて、必要なプロトコル番号または短縮名を入力すると、プロトコルのコマンド環境に入ることができます。このコマンドを入力すると、指定したプロトコルのプロンプトが表示されます。このプロンプトから、そのプロトコル特定のコマンドを入力できます。Config> に戻るには、**exit** コマンドを入力します。

注:

1. ソフトウェア・ロード内のプロトコルの名前と番号を見たい場合は、Config> プロンプトで **list configuration** と入力します。
2. ユーザーが構成可能なパラメーターを変更するとき、プロトコルの GWCON **reset** コマンドを使用することもでき、変更を有効にするために装置をリスタートする必要がある場合もあります。これを行うには、OPCON プロンプト (*) で **reload** コマンドを入力します。

CONFIG を通して加えた変更は、不揮発性メモリー内の構成データベースに保管され、装置をリスタートすると再び呼び出されます。

Qconfig

qconfig コマンドは、Quick Config を開始するのに使用します。Quick Config では、ブリッジングおよびルーティング・プロトコルのパラメーターを、それぞれ別々の構成環境に入らずに構成することができます。

構文:

qconfig

CONFIG コマンド

注: 装置に用意されている Quick Config ソフトウェアの使用についての詳しい説明は、755ページの『付録A. クイック構成リファレンス』を参照してください。

Set

set コマンドは、システム全体の種々のパラメーターを構成するのに使用します。

構文:

```
set contact-person . . .  
data-link . . .  
down-notify . . .  
dump enable-mode  
dump save-mode  
global-buffers  
hostname  
inactivity-timer  
input-low-water  
location . . .  
logging level  
packet-size  
prompt  
receive-buffers  
spare-interfaces
```

contact-person *sysContact*

この管理 SNMPノードの連絡担当者の名前または識別番号を設定します。*sysContact* 名の長さは、最大 80 字に制限されます。

この変数は、情報のためだけのものであり、装置の動作には影響しません。システムの SNMP 管理 ID として有用です。

data-link *type interface#*

シリアル・インターフェースまたはダイヤル回線インターフェースのデータ・リンク・タイプを選択します。 *type* は次のいずれかです。

- FRAME-RELAY
- PPP
- SDLC
- SRLY
- V25BIS
- X25

注:

1. PPP、SDLC、およびフレーム・リレーのみが、ダイヤル回線インターフェースでサポートされるデータ・リンクです。X.25 は、ISDN BRI D チャネルでのみサポートされます。

2. すべてのデータ・リンク・タイプは、8 ポート EIA 232E アダプター、6 ポート V.35/V.36 アダプター、および 8 ポート X.21 アダプターで使用することができます。ただし V.25bis は例外で、EIA 232E アダプターでだけ使用することができます。

*Interface #*は、構成するインターフェースの番号です。

down-notify interface# # of seconds

ユーザーは、インターフェースをダウンとして宣言するまでの秒数を指定することができます。通常の保守パケット間隔は 3 秒で、保守障害が 4 回検出されると、インターフェースはダウンとして宣言されます。

set down-notify コマンドを主に使用するのは、OSPF を使用して IP ネットワークを介して LLC トラフィックをトンネル伝送するときです。インターフェースがダウンした場合、インターフェースをダウンとして宣言するまでに時間がかかるために、OSPF はただちにそれを検出することはできません。そのため、LLC セッションはタイムアウトを開始します。down-notify タイマーを低い値に設定すれば、OSPF はより早くインターフェースのダウンを検知できるようになります。これにより、代替ルートを迅速に選択して、LLC セッションのタイムアウトを防止することが可能になります。

注: シリアル・リンクの一方の端で **set down-notify** コマンドを実行する場合、リンクの他方の端でも同じコマンドを実行する必要があります。そうしないと、リンクがアップにならず、アップに保てないことがあります。

Interface#

構成するインターフェースの番号です。

of seconds

ダウンしたインターフェースがダウンとしてマーク付けされるまでに経過する最大時間を指定するダウン通知タイム値です。値を大きくすると、装置は一時的な接続問題を無視することになり、値を小さくすると、装置はより迅速に反応するようになります。値の範囲は 1 ~ 300 秒で、デフォルトは 0 (3 秒間に設定) です。ダウン通知タイムを 0 に設定すると、そのインターフェースのデフォルト時間に復元されます。

list devices コマンドは、デフォルト値がオーバーライドされているインターフェースのダウン通知タイムを表示します。

dump enable-mode

次のシステム・ダンプに従ってダンプが使用可能にされるかどうかを指定します。保管モード (**set dump save-mode** コマンドを参照) を構成して、最初の 3 つのダンプを保管し、システムがすでに 3 つのダンプ・ファイルを作成してある場合、ユーザーの指定にかかわらずダンプが使用不可にされます。3 番目のダンプ・ファイルを作成する場合、次のメッセージが表示されます。

```
Active Dump Detected.
Dump Compression in Progress, please be patient ...
```

```
*** System dumping is being DISABLED because dumping is ***
*** configured to save the 3 initial dumps, but 3          ***
*** dump files already exist.                               ***
```

CONFIG コマンド

例:

```
Config> set dump enable-mode
```

```
Current System Dump Settings:  
  Disable System Dump following the next system dump.  
  Save the last 3 (most recent) dump files.
```

```
Do you want to change system dump enable-mode to  
re-enable System Dump following the next system dump ? (Yes, No): [No] Yes
```

```
Current System Dump Settings:  
  Re-enable System Dump following the next system dump.  
  Save the last 3 (most recent) dump files.
```

```
Current System Dump Status:  
  System dump is currently enabled.  
  Number of existing dump files: 2
```

デフォルト値: disable

注: Dumping is enabled with the **enable dump-memory** command.

dump save-mode

最初の 3 つの (initial) システム・ダンプ・ファイルまたは最後の 3 つ (最も recent) のどちらを保管するか指定します。initail モードに対立するものとしての recent モードの使用を検討している場合は、**dump enable-mode** を参照してください。

例:

```
Config> set dump save-mode
```

```
Current System Dump Settings:  
  Re-enable System Dump following the next system dump.  
  Save the last 3 (most recent) dump files.
```

```
Do you want to change system dump save-mode to  
save the first (initial) dump files ? (Yes, No): [No] Yes
```

```
Current System Dump Settings:  
  Re-enable System Dump following the next system dump.  
  Save the first 3 (initial) dump files, then disable system dump.
```

```
Current System Dump Status:  
  System dump is currently enabled.  
  Number of existing dump files: 2
```

デフォルト値: recent

global-buffers *max#*

グローバル・パケット・バッファ (ローカル発信パケットに使用されるパケット・バッファ) の最大数を設定します。デフォルトでは、バッファの最大数 (最高 10000) を自動構成します。デフォルトに復元するには、この値を 0 に設定します。global-buffers の設定値を表示したい場合は、**list configuration** コマンドを使用します。

hostname *name*

装置名を追加または変更します。装置名は識別のためだけのものであり、装置アドレスには影響を与えません。*name* は、78 文字未満で大文字・小文字を区別します。

inactivity-timer *#_of_min*

非活動タイマーの設定値を変更します。このコマンドで指定された時間の間、リモート(または、物理) コンソールが非活動状態の場合、非活動タイマーはユーザーをログアウトします。このコマンドは、ログインを必要とする

コンソールにのみ適用されます。デフォルト設定値の 0 は非活動タイマーをオフにし、どんなに長時間コンソールが非活動状態のままでも、ログオフは行われないことを示します。

input-low-water *interface# low_#_of_receive_buffers*

受信バッファ用のインターフェースの低いしきい値を構成することができます。インターフェース用の受信バッファの現行の番号がインターフェースの低いしきい値より小さいとき、パケットが、高いしきい値 (かなりの) 値に達した出力待ち行列で待ち行列に入れられる場合、そのパケットはフロー制御 (除去) に適格です。フロー制御の詳細については、GWCON **queue** コマンドを参照してください。

低いしきい値を下げると、このインターフェースからのパケットが、輻輳 (ふくそう) したネットワーク上に送信された場合に、除去される確率が低くなります。ただし、値を下げたために、受信バッファ待ち行列が空になるためだけにアンダーランが発生する場合は、性能に悪影響が生じることがあります。値を上げると、これとは逆の影響があります。アンダーランが発生しているかどうか判別するには、GWCON **interface** コマンドを使用して、インターフェース番号を指定します。低いしきい値に達したためにこのインターフェースからのパケットが除去されているか判別するには、GWCON (Talk 5) **error** コマンドを使用して、インターフェースについての Input Flow Drop カウンター値を調べます。

値の範囲は 1 ~ 255 です。デフォルトは、製品固有と装置固有の両方です。低いしきい値は、受信バッファの要求される数未満である必要があります。0 の値を指定すると、自動構成されたデフォルトが復元されます。

低いしきい値の設定を表示するには、GWCON (Talk 5) **buffer** および **queue** コマンドを使用します。

*Interface #*は、構成するインターフェースの番号です。 *Low_#_of_receive_buffers* は、低いしきい値です。

location *sysLocation*

SNMP ノードの物理ロケーションを設定します。 *sysLocation* 名の長さは 80 文字に制限されます。この変数は、通知のためだけのものであり、装置の動作には影響しません。システムの SNMP 管理 ID として有用です。

logging level *#*

まだ ELS に変換されていないメッセージの出力を制御します。(ELS について詳しくは、を参照してください。) ログ・レベルは構成に記録されます。装置の電源をオンにするか、リスタートすると、ログ・レベルが有効になり、メッセージ出力を判別します。デフォルトのログ・レベルは 76 です。ログ・レベル 0 は、ログ・レベルがないことに等しくなります。

Example: set logging level 76

packet-size *max_packet_size_in_bytes*

グローバル・バッファおよび受信バッファの最大サイズを設定または変更します。値 0 を最大パケット・サイズとして指定した場合、インターフェースの受信バッファ・サイズは、そのインターフェースに構成されているパケット・サイズになり、グローバル・バッファのサイズは自動構成されます。非ゼロ値を指定した場合、構成された値がグローバル・バッファ・パケット・サイズとして使用され、この最大パケット・サイズよ

CONFIG コマンド

り大きいパケット・サイズが構成されているインターフェースは、それぞれの受信バッファの最大パケット・サイズを使用します。値 0 (自動構成) がデフォルトです。

注: このコマンドは、サービス技術員の直接の指示のもとでのみ使用してください。パケット・サイズを小さくする目的では**絶対に** 使用しないでください。大きくする場合に**のみ** 使用してください。

prompt *user-defined-name*

ユーザー定義の名前をすべてのオペレーター・プロンプトへのプレフィックスとして追加し、ホスト名と置き換えます。

user-defined-name は、文字、数字、およびスペースを任意に組み合わせて、最大 80 字まで使用できます。また、特殊文字も、表8 に説明されている追加機能を要求するのに使用できます。

例:

```
set prompt
What is the new MOS prompt [y]? AnyHost 99
AnyHost 99 Config>
```

表 8. *Set Prompt Level* コマンドによって提供される追加機能

特殊文字	Set Prompt Level コマンドによって提供される追加機能
\$n	ホスト名を表示します。これは、ホスト名をプロンプトに含めたい場合に便利です。たとえば、次のように入力します。 Config> set prompt What is the new MOS prompt [y]? \$n hostname:: Config>
\$t	時刻を表示します。たとえば、次のように入力します。 Config> set prompt. What is the new MOS prompt [y]? \$t 02:51:08[GMT-300] Config>
\$d	現在の年月日を表示します。たとえば、次のように入力します。 Config> set prompt. What is the new MOS prompt [y]? \$d 26-Feb-1997 Config>
\$v	ソフトウェア VPD 情報を、次のような形式で表示します。 program-product-name Feature xxxx Vx Rx.x PTFx RPQx
\$e	ユーザー定義プロンプト内のこの組み合わせの後の 1 文字を消去します。
\$h	ユーザー定義プロンプト内のこの組み合わせの前の 1 文字を消去します。
\$_	ユーザー定義プロンプトに復帰を追加します。
\$\$	\$ を表示します。
<p>注: これらのコマンドを組み合わせて使用することができます。たとえば、次のように入力します。</p> <pre>Config> set prompt What is the new MOS prompt [y]? \$n::\$d hostname::26-Feb-1997 Config></pre>	

receive-buffers *interface# max#*

ほとんどのインターフェースについて私設受信バッファの数を調整して、

インターフェースの受信性能を改善し、ルーターが高速インターフェースから低速インターフェースに多数のパケットを転送しているときに、フロー制御による廃棄数を減らします。値の範囲は 5 ~ 1000 です。デフォルトを復元するには、0 の値を指定します。すべての装置タイプで、受信バッファの最大数を許可するか、最大 1000 までの受信バッファをサポートするわけではありません。各装置タイプについてデフォルトと最大値を判別するには、表9 を使用してください。このコマンドは、表9 で示されている最大値を強制するわけではありません。これは、装置によってサポートされない最大値を構成することを可能にします。このコマンドの効果は、GWCON **buffer** コマンドによって示されています。有効な最大値を構成する場合、この値は、GWCON コマンド出力の Input Req 欄に表示されます。装置によってサポートされていない最大値を構成する場合、GWCON **buffer** コマンドは、受信バッファのデフォルト数が Input Req 欄に表示し、GW サブシステム ELS メッセージがログに記録されます。

注: このコマンドは、ISDN 1 次インターフェースには適用できません。ISDN PRI の場合、受信バッファの数は、B チャネル当り 5 つに固定されており、T1 の場合は 115、E1 の場合は 150 です。チャンネル化されたモードの場合、PRI は構成されたタイム・スロットごとに 5 つの受信バッファを入手します。

表9. インターフェースのデフォルトおよび最大設定値

インターフェース	デフォルト値	最大値
ATM	80*	1000
10 Mbps イーサネット	40*	1000
10/100 Mbps イーサネット	64*	1000
シリアル	24	250
TKR	40*	1000
FDDI	80	80
HSSI	60*	1000
ESCON	1000	1000
PCA	1000	1000

* これは、2216-400 についてのデフォルト値です。ネットワーク・ユーティリティーの場合、デフォルト値は 1000 です。

spare-interfaces *n*

この装置の予備インターフェースの数 *n* を定義します。詳細については、50ページの『予備インターフェースの構成』を参照してください。

System Retrieve

system retrieve コマンドは、重大なエラーが発生した後、ハード・ディスクから 1 つまたは複数のメモリー・イメージ・ファイルを検索するのに使用します。

構文:

```
system                retrieve
```

TFTP を使用して、リモート・ホストに選択されたメモリー・イメージ・ファイルを送信します。システムは、リモート・ホストの IP アドレスとファイル名を入力するよう求めるプロンプトを出します。

CONFIG コマンド

ダンプ・ファイルがない場合、次のメッセージが表示されます。

```
No dump files exist to retrieve
```

例:

```
Config> system retrieve
```

```
Current System Dump Settings:
```

```
Re-enable System Dump following the next system dump.
```

```
Save the first 3 (initial) dump files, then disable system dump.
```

```
3 dump files currently exist.
```

```
Do you want to see a summary of the dump files ? (Yes, No): [No] No
```

```
Destination IP address [0.0.0.0]? 9.9.9.1
```

```
Filename: core0.cmp
```

```
Dump Date: Tue May 05 14:38:59 1998
```

```
Do you want to retrieve this file ? (Yes, No): [No] Yes
```

```
Fully qualified destination path/file name [/tmp/dump0.cmp]?
```

```
The memory image file is 19.3 Mb long.
```

```
Proceed? [No]: Yes
```

```
Sending memory image file by tftp
```

```
TFTP transfer of /hd0/core0.cmp complete, size=20331888 status: OK
```

```
tftp transfer completed successfully.
```

```
Filename: core1.cmp
```

```
Dump Date: Wed May 06 07:53:51 1998
```

```
Do you want to retrieve this file ? (Yes, No): [No]
```

```
Filename: core2.cmp
```

```
Dump Date: Wed May 06 09:14:55 1998
```

```
Do you want to retrieve this file ? (Yes, No): [No]
```

System View

system view コマンドは、現行のシステム・ダンプ設定値およびシステム・ダンプの状況 (ダンプ・ファイルがいくつあるかを含めて) を表示するのに使用します。ダンプ・ファイルの要約も表示できます。

構文:

```
system view
```

例:

```
Config> system view
```

```
Current System Dump Settings:
```

```
Re-enable System Dump following the next system dump.
```

```
Save the first 3 (initial) dump files, then disable system dump.
```

```
Current System Dump Status:
```

```
System dump is currently enabled.
```

```
Number of existing dump files: 2
```

```
Do you want to see a summary of the dump files ? (Yes, No): [No] Yes
```

```
-----  
Filename: core0.cmp
```

```
Dump Date: Tue May 05 14:38:59 1998
```

Fatal messages:
Data St. Excp Reading 0x6c6966b1 at 0x3090fca4 in thread MOSDBG (0x304d54)

CMVC Build: cc_144b
Builder: build
Build Name: LML.ltd
Retain Name: MAS.DF1
Product Number: 2216-MAS
Build Date: Wed May 6 11:47:03 1998

Filename: core1.cmp

Dump Date: Wed May 06 07:53:51 1998

Fatal messages:
Data St. Excp Reading 0x6c6966b1 at 0x3090fca4 in thread MOSDBG (0x304d54)

CMVC Build: cc_144b
Builder: build
Build Name: LML.ltd
Retain Name: MAS.DF1
Product Number: 2216-MAS
Build Date: Wed May 6 11:47:03 1998

Time

time コマンドは、2210 システム・クロックと日付を設定し、それらの値をユーザー・コンソールに表示するのに使用します。これらの値を使用して、ELS メッセージにタイム・スタンプを表示することができます。

注: 2210 には、装置の再初期化後に日付と時刻を維持するハードウェア・クロックが内蔵されています。

構文:

```
time                host . . .
                       list
                       offset
                       set . . .
                       sync . . .
```

host *IP_address*

時刻ソースとして使用される RFC 868 準拠のホストの IP アドレスを設定します。これは、現在の時刻が入っているデータグラムを使用して、UDP ポート 37 の空のデータグラムに応答するホストのアドレスです。

list 構成された時刻関連のすべてのパラメーターを表示します。これには、現在の時刻 (設定されている場合) および時刻ソース (最後に受信した時刻の発信元のオペレーターまたは IP アドレス) が含まれます。

```
Example: time list
05:20:27 Wednesday December 7, 1994
Set by: operator
Time Host: 131.210.4.1
Sync Interval: 10 seconds GMT
Offset: -300 minutes
```

offset *minutes*

GMT (グリニッジ標準時) からの時間帯のオフセットを分単位で定義します。

CONFIG コマンド

GMT の西側の値は負になることに注意してください。たとえば、EST (米東部標準時) は GMT より 5 時間早いので、コマンドは **time offset -300** となります。

有効値: -720 ~ 720

デフォルト値: 0

set <year month date hour minute second>

現在の時刻を入力するように求めます。このコマンドで時刻全体を指定しなかった場合は、残りの値の入力を求めるプロンプトが出ます。次の例に示すように、日付を変更することができます。

```
Example: time set
year [1996] 1997
month [12]?
date [6]? 7
hour [11]? 12
minute [3]?
second [2]?
```

sync seconds

装置が現在の時刻を時刻ホストにポーリングする期間を秒数で設定します。

Unpatch

unpatch コマンドは、**patch** コマンドで入力したパッチ変数の値をデフォルト値に復元するのに使用します。詳細については、86ページの『Patch』の **patch** コマンドを参照してください。

構文:

unpatch *variable_name*

注: 必ず、復元するパッチ変数の完全な名前を指定することが**必要**です。

Update

update コマンドは、新しいソフトウェア・ロードを受け取ったときに、構成メモリーを更新するのに使用します。

構文:

update *version-of-SRAM*

ソフトウェアに添付されているリリース通知の指示に従ってください。**update** コマンドは、新規ソフトウェアをロードするときに最後に入力するコマンドです。このコマンドを入力すると、構成メモリーを更新中であることを示すメッセージがコンソールに表示されます。

Write

write コマンドは、再ロードする前に構成を装置に保管するのに使用します。

構文:

write

CONFIG コマンド

`write` コマンドを出さずに、装置を再ロードしようとする場合、構成を保管したいかどうか尋ねられます。構成は、現在使用しているバンク内のハード・ディスク上で次の CONFIG に保管されます。

CONFIG コマンド

第5章 ブート CONFIG プロセス

この章ではブート CONFIG プロセスについて説明します。本章には、以下の節が含まれています。

- 『ブート CONFIG とは』
- 102ページの『BOOTP 転送プロセスの働き』
- 104ページの『トリビアル・ファイル転送プロトコル (TFTP) の使用』
- 108ページの『構成ロードの妥当性検査』
- 108ページの『特定時刻にイメージをロード』
- 109ページの『ダンプの構成』

ブート CONFIG とは

ルーターの不揮発性構成データベース・メモリーには、ルーターのブートおよびダンプ機能を制御するデータが入っています。ブート CONFIG コマンドを使用して、このデータを変更することができます。

ブート CONFIG コマンドを使用すると、次のことができます。

- ブートおよびダンプ構成データベースの項目を追加、変更、または除去する。
- ネットワーク・メモリー・ダンプを使用可能または使用不可にし、ダンプ・ファイルに固有の名前を割り当てる。
- TFTP プロトコルを使用して、ルーター・メモリーとリモート・ホストの間で構成情報を転送する (TFTP コマンドまたは **copy** コマンドを使用)。
- 現行のブートおよびダンプ構成データベースを表示する。
- ファイル・イメージを統合ブート装置 (IBD) に保管する。
- 現行イメージを IBD に保管する。
- ブート CONFIG コマンド環境から抜けて CONFIG プロセスに戻る。
- IBD の内容をリストする。
- IBD からファイルを削除する。
- ローカル・ルーター・メモリーと別のローカル・ルーター・メモリーまたはホスト・ファイル・システムの間でファイルをコピーする。
- システム・パラメーターおよびプロトコル・パラメーターに加えた変更をすべて保管する。

ブート CONFIG を用いてシステム・パラメーターおよびプロトコル・パラメーターに加えた変更が有効になるのは、ルーターをリスタートしたとき、またはルーター・ソフトウェアを再ロードしたときです。

ブートの構成

ブート・ファイルはロード・イメージ・ファイルと同じものです。ブート・ファイルにはソフトウェア・ロードが入っており、ホスト・サーバーまたは IBD に常駐し

ブート CONFIG プロセスの使用

ています。ホスト・サーバーは、たとえば、IP プロトコルおよび TFTP を実行している任意の PC、ルーター、またはワークステーションです。ブート構成データベースには、**add** コマンドを用いて構成して、各ブート・ファイルごとに 1 つの項目を入れることができます。各項目には、ホスト・サーバーのアドレス、次のホップ・ルーター、およびブート・ファイルのタイムアウト、パス、およびファイル名が含まれます。

各ブート・ファイルのパスと名前を指定することにより、ブート構成データベースに複数のブート・ファイルを構成することができます (114ページの『Add』で説明する **add** コマンドを使用して)。複数のホスト・サーバーがある場合、1 つのホスト・サーバーがネットワーク経由で接続できないときには、別のホスト・サーバーを使用してルーターをブートすることができます。

ブートを構成するには、以下の手順で行います。

1. Boot config> プロンプトから **add address** コマンドを使用して、ブートを実行したいインターフェースを指定するアドレス・レコードを追加する。
2. Boot config> プロンプトから **add boot-entry** コマンドを使用してブート・レコードを追加し、ホスト・アドレス、次のホップ・ルーター (必要な場合)、およびホストのパスとファイル名を指定する。

ブート・サーバーとしての装置の使用

装置はブート・サーバーとして機能することもできます。IBD がない装置では、IBD のあるルーターからロード・ファイルまたはブート・ファイルを入手することができます。この場合は、**add boot-entry** コマンドを使用して、ブート・ファイルにルーターの場所を指定します。このコマンドにはロード・ファイルの全パス名を必ず組み込んでください。ロードが IBD 内にあるルーターの場合、これは *IBD/filename* になります。

BOOTP 転送プロセスの働き

BOOTP (RFC 951 に文書化されています) は、ルーターまたはディスクのないワークステーションが、その IP アドレス、ブート・ファイルの場所、およびブート・サーバー名を知るために使用するブートストラップ・プロトコルです。装置は、*BOOTP* クライアントとして、あるいは別の装置の *BOOTP* リレー・エージェントとして機能することができます。以下の項では、これらの 2 つのプロセスについて説明します。

BOOTP クライアントとしての装置

装置が *BOOTP* クライアントとして機能するのは、ブート・ファイルおよびブート・サーバーの場所を見つける必要があるときです。ユーザーが装置のブート PROM 構成レコードを特別に構成して、ルーターが *BOOTP* クライアントとして機能できるようにすることもできますし、ブート時に有効なファイル名およびブート・ファイルとブート・サーバーの場所への有効なパスがない場合は、ルーターが *BOOTP* クライアントになることもできます。この 2 つの条件のいずれかが存在するとき、ルーターは LAN インターフェースの 1 つを介して、ブート・ファイルおよびブート・サーバーのパス名をもつ *BOOTP* サーバー に UDP パケットを同報通信します。

以下に、BOOTP クライアントの転送プロセスを説明します。

1. BOOTP クライアントは、その MAC アドレス (イーサネットまたはトークンリング) を BOOTP パケット (UDP パケット) にコピーし、それをローカル LAN 上でブロードキャストします。BOOTP は UDP の最上位で稼働します。
2. BOOTPサーバーは要求を受信し、そのデータベースにあるクライアントのイーサネット・アドレスを調べます。見つかった場合、クライアントの IP アドレス、そのブート・ファイルの場所、およびブート・サーバー名を含む BOOTP 応答にフォーマットします。次に、この応答は LAN を介して BOOTP クライアントに送り返されます。

注: BOOTP サーバーに到達するまでにいくつかのホップが必要な場合は、BOOTP リレー・エージェントがそのパケットを受け取ります。BOOTP リレー・エージェントについては、次の項で説明します。

3. ルーターが BOOTP 応答パケットを受け取ると、そこに含まれている情報を使用して、ブート・サーバーに TFTP 要求を開始します。

BOOTP リレー・エージェントとしての装置

BOOTP 要求が BOOTP サーバーに到達するまでにいくつかのホップを必要とする場合、BOOTP リレー・エージェントが知っている BOOTP サーバーすべてに IP 経由でパケットを送ります。IP を介してパケットが送信されている間に、他のルーターがこれを受信すると、そのパケットを検査してそれが BOOTP パケットかどうかを判別し、知っている BOOTP サーバーの方へパケットを回送します。以下に、BOOTP リレー・エージェントの転送プロセスを説明します。

1. ローカル BOOTP リレー・エージェントとして機能する装置は、BOOTP クライアントから BOOTP 要求を受信し、チェックサムを変更し、リレー・エージェントの IP アドレスを BOOTP 要求の本体にコピーして、パケットに IP ヘッダーを付け、そのパケットをすべての BOOTP サーバーに送ります。
2. BOOTP サーバーがその要求を受け取ると、クライアントの MAC アドレスをデータベースの中で探します。サーバーがクライアントのアドレスを見つけると、クライアントの IP アドレス、そのブート・ファイルの位置、およびブート・サーバー名を含めた BOOTP 応答にフォーマットします。次に、その応答が BOOTP リレー・エージェントに送られます。
3. BOOTPリレー・エージェントは応答を受け取り、クライアントのために ARP テーブル内に登録してから、応答を BOOTP クライアントへ転送します。
4. クライアントは、BOOTP 応答パケットに含まれているブート・サーバーへの TFTP 要求を開始するための情報を使用して、ブートを続けます。

BOOTP 転送の使用可能/使用不可

ルーターでの BOOTP 転送を使用可能または使用不可にするには、IP 構成プロンプトで、次の該当するコマンドを入力します。

```
IP Config> enable bootp
```

```
IP Config> disable bootp
```

BOOTP を使用可能にする場合、次の値を入力するようにプロンプトで指示されます。

- BOOTP 要求が経由するアプリケーション・ホップの最大数

ブート CONFIG プロセスの使用

これは、パケットを転送できる BOOTP リレー・エージェントの最大数です。BOOTP サーバーへの IP ホップの最大数では**ありません**。このパラメーターの標準値は 4 です。

- BOOTP 要求を転送する前にクライアントが再試行する秒数。このパラメーターは通常は使用されません。このパラメーターの標準値は 0 です。

BOOTP 要求を受け付けると、ルーターはその BOOTP 要求を各 BOOTP サーバーに転送します。BOOTP に複数サーバーが構成されている場合、転送するサーバーはパケットを複写します。

BOOTP サーバーの構成

BOOTP サーバーは、*bootpd* daemon をもつ AIX または UNIX ホスト、あるいは DOS ホスト (FTP ソフトウェアから利用可能なソフトウェアを実行) です。BOOTP サーバーには、このサーバーが担当するすべての BOOTP クライアントと、それぞれの関連の IP アドレス、ブート・ファイルの場所、およびブート・サーバー名をリストした 1 つのファイルが収められています (ネットワーク管理者が管理します)。

BOOTP サーバーは、BOOTP 要求を受け取ると、クライアントの MAC アドレスと、サーバーの BOOTP ファイルにある MAC アドレスとを突き合わせます。一致した場合、サーバーは BOOTP 応答を構成し、クライアントの IP アドレスと、ブート・サーバーおよびブート・ファイル名の場所を追加します。一致しない場合、パケットは廃棄されます。

ルーターの構成に BOOTP サーバーを追加するには、IP 構成プロンプトで次のコマンドを入力します。

```
IP Config> add BOOTP-SERVER [IP address of server]
```

複数のサーバーを構成することができます。さらに、サーバーのネットワーク番号のみを知っている場合、あるいは複数のサーバーが同じネットワーク・セグメント上に存在する場合は、IP config>> プロンプトで **enable directed-broadcast** コマンドを入力して、サーバー用の同報通信アドレスを構成することができます。

トリビアル・ファイル転送プロトコル (TFTP) の使用

TFTP は、インターネット UDP プロトコル上で実行されるファイル転送プロトコルです。この実現では、ルーターの不揮発性構成メモリー、統合ブート装置 (IBD)、およびリモート・ホストの間で、複数の TFTP ファイル転送を同時に行うことができます。

TFTP では、以下のことが可能です。

- ルーターからサーバーへの構成ファイルの保管
- サーバーからルーターへの構成ファイルのコピー
- IBD への構成のコピーまたはファイルのロード

TFTP 転送には、クライアント・ノードとサーバー・ノードが関与します。クライアント・ノードは、ネットワーク上に TFTP 要求を生成します。ルーターはクライアント・ノードとして機能し、Boot Config> プロセスの **copy** コマンドを使用して、ルーター・コンソールから TFTP 要求を生成します。

注: **tftp** コマンドと **copy** コマンドは、同じ機能を持っていますが、構文は異なります。

このクライアントは、構成メモリーに保管されている構成ファイルのコピーまたは IBD に保管されているファイルを転送することができます。

サーバーは、TFTP 要求を受け取ってサービスを提供する任意の装置 (たとえば、パーソナル・コンピュータ (PC)、ルーター、またはワークステーション) を使用できます。ルーターがサーバーとして動作する場合、転送はユーザーに透過的に行われます。ELS サブシステム tftp メッセージ・ログを使用すると、進行中の転送を見ることができます。

注: ファイル・サーバーまたはルーターは、ファイルを他のルーターの不揮発性構成メモリーまたは IBD にコピー することはできません。ルーターに書き込みを行うには、あて先のローカル `Boot config>>` プロンプトから **copy** コマンドを使用します。

copy コマンドを使用するときは、次の点に注意してください。

- 装置構成に IP プロトコルが組み込まれており、構成済みの IP アドレスが少なくとも 1 つは必要です。また、ルーターが CONFIG-Only モードで動作してはなりません。
- 装置の構成メモリーが空の場合 (つまり、装置の初期導入時、SRAM が破壊されている場合など) は、次のパラメーターを設定して、装置の構成を復元する必要があります。
 1. 装置のホスト名を設定する。
 2. 保存されている構成を用いて、装置が各ホストに到達できるように IP を構成する。IP 構成コマンドについては、*プロトコルの構成と監視解説書* で説明しています。
- TFTP 転送の発信元 IP アドレスは、装置 ID です。デフォルトでは、この ID は装置のネットワーク・インターフェースの 1 つの構成済み IP アドレスになります。ルーター ID を変更するには、`IP Config>` プロンプトで **set router ID** コマンドを入力します。
- すべての TFTP データ転送は、512 バイトの長さです。512 バイト未満のデータ転送は、転送の終わりを示します。プロトコル、クライアント、またはリモート・ホストにエラーがあると、転送を終了させるエラー・パケットが生成されません。
- 構成ファイルをダウンロードする場合は、ファイルをアップロードしたときと同じタイプのルーターにダウンロードしてください。

注: この TFTP は、他のルーターに *copy* することはできません。

各 TFTP 転送には、クライアントとサーバーの UDP ポート番号が付いています。クライアント・ノードがサーバーへの最初の要求を生成するときに、クライアント・ノードの未使用の UDP ポート番号が、クライアント・ノードとしてランダムに選択されます。サーバー・ポートは UDP ポート番号 69 (10 進数) になります。サーバー上で TFTP サーバーが稼働している場合、UDP ポート 69 を監視します。サーバー

ブート CONFIG プロセスの使用

ーがネットワークから要求を受信すると、サーバー上の現在未使用の UDP ポート番号が、ホスト・ポートとしてランダムに選択されます。この 2 つの UDP ポート間で、ファイル転送が行われます。

リモート・ホストまたはルーターからの構成ファイルへのアクセス

リモート・ホストまたはルーターから構成ファイルへアクセスするには、以下の手順で行います。

1. Boot config>>プロンプトで、**copy**と入力し、**Enter** を押す。
2. source filename [CONFIG]? プロンプトで、リモート IP アドレスとパス名を指定する。
これは TFTP ホスト、または IBD 内にファイルが入っている別のルーターです。
3. destination filename [Config]? プロンプトで、**Enter** を押す。
Enter を押すことによって、デフォルトのファイル名 CONFIG を受け入れます。たとえば、次のように入力します。

```
Boot config>copy
source filename[CONFIG]?128.185.210.125:loads/configs/v1-28.cfg
destination filename [CONFIG]?
COPYing from "128.185.210.125:loads/configs/v1-28.cfg" to
"CONFIG"
COPY succeeded
```

IBD のファイル名の定義

IBD に保管されている各ファイルまたはイメージ には、それに関連した固有の *loadname* が必要です。 IBD のファイル名には、ファイル名の他に、完全パス名を含めることができます。

例 1: test.cfg

例 2: /usr/loads/test.ldc

次の例は、Boot config> プロンプトでファイルを IBD に保管する方法を示しています。

例: copy 128.185.210.125:/usr/config/test.cfg ibd/test.cfg

ルーターは、ファイル名定義の一部として任意の印刷可能 ASCII 文字を受け入れますが、次の 2 つの例外があります。

- ファイル名は、数字で始めることはできません。
- ファイル名に RETURN または LF (改行) 文字を含めることはできません。

文字列にはスペースを含めることができますが、この文字は目に見えないので、使用しないことをお勧めします。別のユーザーが必須のスペースを抜かしてファイル名を入力しようとする、エラー・メッセージを受け取ることになります。

注: IBM 2210 を他のルーターのサーバーとして使用する場合には、ブート・ルーター上の **add boot-entry** コマンドを使用して、ロード・ファイルに完全パス名を必ず組み込んでください。

下の表に、ファイル名拡張子に関する規則を示します。

表 10. ファイル名の拡張子に関する規則

ファイルのタイプ	ファイル名の拡張子
構成	.cfg
Load	.ldc

ファイル転送時の IBD に関する考慮事項

IBD にファイルを転送する場合、次の事項を考慮してください。

- 全ロードは、IBD の 1 つのバンクには収容できません。
- ロードを保管するために複数のバンクが必要な場合、連続する番号の空のバンクにのみ書き込みます。たとえば、ロードが大きすぎてバンク 2 に収容しきれない場合、バンク 3 が空の場合にのみ、ロードはバンク 3 に保管されます。
- 大きなロードを保管するために隣接バンクを利用できない場合、コンソールに TFTP Disk Full メッセージが表示され、そのロードは保管されず、IBD は変更されないうまになります。バンクに部分的に保管されたロードは除去されます。

複数のファイルへの大量のデータの転送

この機能は、受信側の TFTP サーバーが、ブロック・カウンットの処理にバグがあり、循環してゼロに戻るか X'8000' の値をもつような状態で重要です。TFTP プロトコルは、ブロック・カウンットが各データ・ブロックとともに送信されることを要求します。そのデータ・ブロックに対する確認応答には、確認されたデータ・ブロック内にあったブロック番号が入っています。データの送信側は、送信された最後のデータ・ブロックに対する確認応答を受信するまで、それ以上データを送信しようとしません。データの受信側が確認応答を送信すると、それが前に受信したブロック・カウンットより 1 だけ大きいブロック・カウンットをもつデータ・ブロックを受信することを予期します。このブロック・カウンットは 2 バイトの長さです。

一部の TFTP サーバーは、これを符号付きの短いワード (2 バイトの変数、ここで高位ビットが 1 である場合はマイナスの値を意味します) として、その他を符号なしの長いワード (4 バイトの変数) として設定しましたが、これは不適切です。

転送されるデータの量が多いためブロック・カウンットが折り返される場合は、受信側がブロック・カウンットをどのように検査するかに応じて、データを確認する場合も、しない場合もあります。受信側が符号付きの短いワードを使用する場合、ブロック・カウンットが X'7FFFF' から X'8000' に進むときに問題が発生します。受信側が符号なしの長いワードまたは短いワードを使用する場合、ブロック・カウンットが X'FFFF' から X'0000' に進むときに問題が発生します。両方の場合で、データ・ブロック内のブロック・カウンットは、前に受信したブロック・カウンットより小さく見えるので、受信側は混乱します。

ルーター上で TFTP を送信すると、エラー・パケットを受信するか、受信側が応答するのを待ちながらタイムアウトになるかのいずれかです。これが発生するとき、ルーター上の TFTP は、ブロック・カウンットが折り返されたことを理解するか、新しいファイルについて受信側への書き込み要求を行うことにより自動的に回復します。新しいファイル名は、元のファイル名から派生します。新しいファイル名は、元のファイル名の最後の 2 文字を 2 つの 10 進数字で上書きすることで派生します。ブ

ブート CONFIG プロセスの使用

ロック・カウントが折り返されるたびに、すべてのデータが転送されるまで、新しいファイルが作成されます。受信側で **cat** などのツールを使用して、ファイルを連結することができます。

受信側でファイルを転送するためにブロックの最大数を指定

受信側でファイルを転送するためのブロックの最大数を指定することができるように、パッチ変数が追加されました。これにより、指定されたブロックの数が送信されると、新しいファイル用の書き込み要求を自動的に行うよう装置に指示することができます。これを行うと、上記の自動回復がう回され、5 分のタイムアウト期間を避けることにより転送をスピードアップします。

このパッチ変数に指定できる値は、X'FFFF' (65535) および X'7FFF' (32767) だけです。

このパッチ変数が役に立つのは、受信側のサーバーにブロック・カウントの折り返しの処理に問題があることが分かっている場合です。

構成ロードの妥当性検査

イメージが装置の構成メモリーに書き込まれる前にイメージを検査するには、次の 2 通りの方法があります。

- 最初の方法は、保存されているイメージおよび復元されるイメージのそれぞれのプラットフォーム・タイプに、装置がマジック・ナンバーと呼ばれる識別コードを割り当てます。この番号が一致しない場合は、転送は打ち切られ、コンソールに **Bad Magic Number** というメッセージが表示されます。
- 2 番目の方法は、最初にイメージを保存した装置のホスト名と、イメージを復元する装置のホスト名が比較されます。このホスト名が一致しないと、転送は打ち切られ、コンソールに以下のメッセージが表示されます。

```
COPY error -  
Got hostname "<hostname>" - is this okay (Yes or [NO])? no
```

したがって、ホスト名が一致しなくても、別の装置から構成を導入することができます。構成は、使用している装置のモデルに適合する正しいものであることが必要です。

RAM スペースの不足が原因で転送が正常に行われなときは、コンソールにエラー・メッセージが表示されます。

特定時刻にイメージをロード

ユーザーに不都合な特定の日時に装置にロードしたい場合があります。 **timeload activate** コマンドを使用すると、指定した時刻に装置がロードを実行するように構成することが可能です。装置にスケジュールされているロード情報を表示したり、スケジュールされたロードを取り消したりするコマンドも用意されています。これらのコマンドについては、113ページの『ブート CONFIG コマンド』を参照してください。

ダンプの構成

2210 の重要なフィーチャーは、ソフトウェア・クラッシュやハードウェア障害が原因でシステム・リセットが行われるとき、あるいはリセット・ボタンを押したときに、システム・メモリーおよびプロセッサ・レジスターの内容を他のホストへダンプできることです。

ダンプを構成するには、`Boot config>` プロンプトから以下のことを実行します。

1. アドレスを追加する。

これはブートの構成で使用したブート・アドレスと同じで構いません。

2. ダンプ項目を追加する。

これは、ダンプ・ファイルを受信するホストまたはサーバーの場所です。

add dump-entry コマンドを使用して、ダンプ項目を追加することができます。ダンプ・ファイルの平均サイズは 8 MB です。

3. ダンプを使用可能にする。

ダンプを使用可能にするには、**enable dumping** コマンドを使用します。ダンプを使用不可にするには、**disable dumping** コマンドを使用します。

ダンプ・ファイル

ダンプ・ファイルには、システム・メモリーとプロセッサ・レジスターの内容が入っています。

装置がクラッシュし、ダンプが使用可能になっているときは、TFTP を使用して、メモリーの内容がリモート・ホストに書き込まれます。各ダンプ項目には、ホスト・サーバーおよびパスの場所、タイムアウト、およびダンプ・ファイルのファイル名が含まれています。

ダンプ・ファイル名に固有の文字列を自動的に追加するように、装置を構成することも可能です。こうすると、既存のダンプ・ファイルが後続のダンプによって上書きされるのを防ぐことができます。ただし、ダンプ・ファイルに固有の名前を付けると、連続的にダンプが行われた場合、サーバーのディスクがいっぱいになる可能性があります。TFTP サーバーによっては、固有の命名はセキュリティー要件に反することもあります。また、一部のサーバーでは、サーバー上にすでに存在しているファイルにしか、ダンプを書き込むことができません。

ダンプ・ファイルは診断のためにだけ使用します。装置のダンプ機能および固有の命名機能を使用可能にするのは、カスタマー・サービス技術員の助言があった場合だけにしてください。

TFTP サーバー、ブートおよびダンプ・ディレクトリー

ブート・ファイルおよびダンプ・ファイルを入れるために、あて先サーバー上にディレクトリーを作成する必要があります。これらのディレクトリーはホスト・サーバーに常駐し、ブート・ディレクトリーはグローバルに読み取り可能で、ダンプ・ディレクトリーはグローバルに書き込み可能でなければなりません。ブートおよびダンプ機能は、TFTP プロトコルを使用します。ユーザーの TFTP サーバーには、その他の制約事項がある場合があります。

ソフトウェア / コードの導入

サーバーから IBD へ新規のロード・モジュールをダウンロードするには、次のステップで行います。

1. 装置が到達可能なサーバーにロード・ファイルをインストールする。サーバー上で TFTP デーモンが稼働していることを確認してください。装置のルーター・コンソールで、以下のコマンドを入力します。

2. OPCON プロンプト (*) で:

- a. **status** と入力し、Config プロセス ID (PID) を表示する。

```
* status
```

- b. **talk** と Config PID を入力して、Config> コマンド環境にアクセスする。

```
* talk 6
```

3. Config> プロンプトで、**boot** と入力する。これにより、Boot config> コマンド環境にアクセスします。

```
Config> boot  
Boot config>
```

4. Boot config> プロンプトで **add address** と入力して、装置がブートできる IP アドレスを指定する。これは、使用できるようにしたい各インターフェースに対して、1 回だけ行う必要があります。新規のロード・モジュールを取得するたびにを行う必要はありません。

続いて、次の情報を求められます。

- Interface number ルーターがファイルを転送するのに使用するインターフェースの番号です。
- New address このインターフェースの IP アドレスです。
- Net mask このインターフェースのネットワーク・マスクです。

```
Boot config> add address  
Which interface is this address for [0]?  
New address [0.0.0.0] ?  
Net mask for this interface [255.255.255.0]?
```

以下のステップは、ブート・アドレスを追加した場合にだけ必要です。ブート・アドレスを構成済みの場合は、以下のステップを省略して、9 へ進んでください。

5. **Ctrl-P** を押して、OPCON プロンプト (*) に戻る。
6. OPCON プロンプトで、**restart** と入力する。
7. **talk** と Config PID を入力する。
8. Config> プロンプトで **boot** と入力して、Boot config> コマンド環境に戻る。
9. Boot config> プロンプトで、**tftp get** と入力する。これで、ロード・モジュールのファイル転送を開始します。

次の情報を求められます。

- Local filename ローカル・ファイル名として、IBD 内の新規ロードのファイル名を入力します。
- Remote host リモート・ホストとして、サーバーの IP アドレスを入力します。
- Host filename ホスト・ファイル名として、ホスト・マシン上の完全なパスとファイル名を指定します。


```

Boot config> tftp get
Local filename []? ibd/newloadfile
Remote host []?
Host filename []?

```

10. Boot config> プロンプトで、**list boot-entries** と入力する。こうすると、IBD 内のロード・モジュールがリストされます。

```
Boot config> list boot-entries
```

このロード・モジュールを受け取る前に使用していた IBD 内のロード・モジュールの項目番号をメモしておいてください。

ブート・データベースで、ルーターはロード・モジュールを入手する場所を調べます。データベースには、複数の項目を入れることができます。通常は、最初の項目は IBD 内のロード・モジュールで、2 番目の項目はリモート・ホストまたはルーターのロード・モジュールです。

11. Boot config> プロンプトで **change boot** と入力して、ブート・データベースのポインターをロードしたばかりのモジュールに変更する。これにより、次回にルーターをリブートしたときに使用されるロード・モジュールが決まります。

```
Boot config> change boot
```

次に、IBD 内で使用していた以前のモジュールの項目番号を求められます。これは、ステップ 10 でメモした項目番号です。ブート項目番号は、通常は "1" になります。

```
Change which entry?: 1
```

12. 新規ロードのファイル名を入力する。これは、IBD に保管するためにステップ 110ページの9 で指定した名前です。ファイル名は大文字・小文字を区別します。

```
remote host or IBD load name:
```

13. **exit** と入力する。

```
Boot config> exit
```

14. **Ctrl-P** を押して、OPCON プロンプト (*) に戻る。

15. **restart** と入力して、"change boot" コマンドによる構成変更が有効になっていることを確認する。

16. **reload** と入力して、装置に新規ロード・モジュールをロードする。

17. 新規ロードを確認した後、直前のロードを消去して、IBD 内に将来のロードのためのスペースを作成することができます。

a. **talk 6** と入力する。

b. **boot** と入力する。

```
Config> boot
```

- c. **list ibd** と入力して、バンクの内容をリストする。前のロードが保管されていたバンクの番号をメモしておいてください。

```
Boot config>list ibd
```

- d. **erase** と前のロード名またはバンク番号を入力する。たとえば、バンク 36 ~ 50 を消去するには、次のように入力します。

```
Boot config> erase 36-50
```

ブート CONFIG プロセスの使用

第6章 ブート CONFIG の構成

この章では、ブート CONFIG 構成コマンドおよびオペレーショナル・コマンドについて説明します。本章には、以下の節が含まれています。

- 『ブート CONFIG の開始と終了』
- 『ブート CONFIG コマンド』

ブート CONFIG の開始と終了

ブート CONFIG コマンド環境へ入るには、CONFIG の **boot** コマンドを使用します。ルーターのソフトウェアは、初期ロード時には OPCON プロセスで動作し、* プロンプトが表示されます。* プロンプトから、次のようにします。

1. **talk 6** と入力する。
2. Config> プロンプトで、**boot** と入力する。
3. Boot config> プロンプトで、**?** を入力する。コマンドのリストについては、114ページの『Add』を参照してください。
CONFIG プロセスに戻るには、**exit** と入力します。

ブート CONFIG コマンド

この節では、ブート CONFIG コマンドについて説明します。各コマンドごとに、説明、構文の要件、および例を示します。表11 は、ブート CONFIG コマンドの要約を示しています。

ブート CONFIG 環境にアクセスした後、Boot config> プロンプトでブート構成コマンドを入力します。

表11. ブート CONFIG コマンド

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Add	指定されたインターフェース、ホスト・ブート項目、またはホスト・ダンプ項目に、ブート・インターフェースの IP アドレスを追加します。
Change	ブート・インターフェース IP アドレス、ネットワーク・ブート項目データ、またはネットワーク・ダンプ項目データを変更します。
Copy	リモート構成ファイルとホスト間で、あるいはルーター内の各資源の間で、ブート・ファイルおよび構成ファイルをコピーします。
Describe	IBD 内に保管されているロード・ファイル・イメージに関する情報を表示します。
Delete	ネットワーク・ブート・インターフェース・アドレス、ホスト・ブート項目、またはホスト・ダンプ項目を削除します。

表 11. ブート CONFIG コマンド (続き)

コマンド	機能
Disable	ダンプ・ファイルのメモリー・ダンプまたは固有の命名を使用不可にします。
Enable	ダンプ・ファイルのメモリー・ダンプまたは固有の命名を使用可能にします。
Erase List	IBD バンクに保管されているイメージを消去します。 すべてのネットワーク・ブート・アドレス、すべてのブートおよびダンプ構成データ、IBD の内容、BOOTP 名の設定値、およびスケジュールされたイメージ・ロード情報を表示します。
Load	IBD または RAM からブート・ファイルをコピーするか、またはリモート・ホストから RAM にブート・ファイルをコピーします。
Store Timedload	RAM から IBD にブート・ファイルをコピーします。 特定の日に装置にイメージをロードすることをスケジュールしたり、スケジュールされたロードを取り消したり、あるいはスケジュールされたロード情報を表示したりします。
TFTP	装置メモリーまたは IBD とリモート・ホストとの間で TFTP ファイル転送を開始します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Add

add コマンドは、装置の構成データベースにブート/ダンプ・パラメーターを入れるのに使用します。

構文:

```
add                address
                    boot-entry
                    bp-device
                    dump-entry
```

address

装置がブートまたはダンプできるインターフェースまたは装置の IP アドレスを指定します。 **add address** コマンドを使用する場合、次の情報を提供するかまたはそのデフォルト値を受け入れる必要があります。

- ネットワーク・インターフェースのインターフェース番号
- IP アドレス
- ネットワーク・マスク

インターフェース番号 (Ifc#) を入手するには、CONFIG **list devices** コマンドを使用します。このコマンドについては、47ページの『CONFIG とは』で説明しています。

注: アドレスを追加しないと、装置はネットワーク上でブートまたはダンプを行えなくなります。

以下の点に注意してください。

- 入力する最初のアドレスは、入力した最初のブート項目に対応し、2 番目のアドレスは 2 の項目に対応するというようになります。

- 複数のブート項目で同じ IP アドレス (インターフェース) を使用することができます。
- **add boot-entry**、**add dump-entry**、および **load remote** コマンドを使用する場合は、このコマンドを入力する必要があります。

```
Example: add address
Which interface is this address for [0]?
New address [0.0.0.0] ? 128.185.1.2
Net mask for this interface [255.255.255.0]?
```

boot-entry

装置が TFTP ホスト・サーバーを見つけて、ブート・イメージ・ファイルを検索するために必要な情報を指定します。装置をブートするには、いくつかの方法があります。

- ルーターが自身の IBD に保管されているソフトウェアを使用してブートする場合、IBD ロード名を構成の最初のブート項目として指定することが必要です。複数のブート装置を構成することもできます。ロード名は **list ibd** コマンドを使用して入手してください。ロード名は、大文字・小文字を区別します。

```
Example: add boot-entry
remote host or IBD loadname [0.0.0.0]? 128.185.30.0
via gateway (0.0.0.0 if none) [0.0.0.0]? 0.0.0.0
timeout in seconds [3]? 10
file name [ ]? loads/Y21.1dc
```

- 装置が TFTP サーバーに保管されているソフトウェアを使用してブートする場合は、リモート TFTP ホスト・サーバーの IP アドレスを指定することが必要です。TFTP ホスト・サーバーは、IBD をもつ別の装置でも構いません。
- TFTP ホスト・サーバーがリモート・ネットワーク (ブートを行うルーターとは直接接続されていない) にある場合には、ホスト・サーバーに向けての次のホップ (ルーター) の IP アドレスを指定する必要があります。

表 12. Add Boot Entry パラメーター

remote host or IBD loadname?	リモート・ホストの IP アドレスまたは IBD ロード名。 注: IBD ロード名は、英字で始まっていなければなりません。そうしないと、システムはその文字列を IP アドレスと解釈します。
via gateway?	最初のホップ・ルーターの IP アドレス (存在する場合)。TFTP ホスト・サーバーが、直接接続されたネットワーク上にある場合には、0.0.0.0 と応答します。
timeout in seconds?	再伝送が行われる前に、装置が待つ時間の長さを指定します。デフォルト値は 3 秒です。極度に遅いブート・パスの場合は、もっと長い時間を設定することが必要になる場合があります。

表 12. Add Boot Entry パラメーター (続き)

file name?	<p>TFTP ホスト・サーバー上のブート・イメージ・ファイルの完全なディレクトリー・パスと名前。(完全ディレクトリー・パスを必要としない機械もあります。デフォルトでは、パスは <code>tftpboot/</code> であるものと想定しますが、これはユーザーからは見えないので、パスが <code>/tftpboot/loads/name</code> のときは loads/name と入力します。)</p> <ul style="list-style-type: none"> - UNIX ベースのオペレーティング・システムに保管されているファイルを参照するときは、前向きスラッシュ <code>/</code> を使用し、ファイル名は大文字・小文字の区別が必要です。パスの先頭に前向きスラッシュ <code>(/)</code> が必要な場合には、二重の前向きスラッシュ <code>(//)</code> を使用します。 <code>128.185.15.1//tftpboot/loads/name.</code> - DOS ディスク上に保管されているファイルを参照するときは、前向きバック・スラッシュ <code>\</code> を使用し、ファイル名は大文字・小文字の区別をしません。
------------	---

注: 現行のブート構成のリストを表示するには、ブート CONFIG **list boot** コマンドを入力します。

```
Example: list boot-entry
remote host or IBD loadname [0.0.0.0]? 10.0.0.5
via gateway (0.0.0.0 if none) [0.0.0.0]? 12.0.0.7
timeout in seconds [3] 10
file name [ ] loads/v1.1dc
```

bp-device

BOOTP (ブート・プロトコル) 装置から装置のソフトウェアを取り出すために、以下のような BOOTP ブート機能を提供します。

- 装置が構成されていないか、装置の自動ブート構成情報が欠けており、しかも自動ブート・スイッチが使用可能に設定されている場合、装置は自動的にすべての LAN インターフェース上の BOOTP を使用してブート情報を取り出そうと試みます。
- 自動ブート時には、最初に装置はブート項目に提供されている情報を使用して、ロード・イメージ・ファイルを取り出そうと試みます。ブート項目の情報からロード・イメージ・ファイルを取り出せなかった場合、次に装置は BOOTP を使用してブートを試みます。
- **add bp-device** コマンドで選択されるインターフェースは、ネットワーク内の BOOTP サーバーの位置によって異なります。
- BOOTP を使用して、直接接続されたシリアル・インターフェースを介してブートすることはできません。

```
Example: add bp-device
Which interface number [0]? 1
```

dump-entry

ダンプ・ファイルを受け取るリモート・ホストの IP アドレスを指定します。

add dump-entry コマンドを入力するときに、次の情報を提供する必要があります。

remote host?	ダンプ・ファイルが保管されるリモート・ホストの IP アドレス。通常はブート・サーバーと同じです。
via gateway?	ホストがリモート・ネットワーク上にある (ブート装置に直接接続されていない) 場合は、ホストに向けての次のホップ (ルーター) の IP アドレスを指定することが必要です。ホストが直接接続ネットワーク上にある場合は、0.0.0.0 と答えます。

timeout in seconds?	再伝送が行われる前に、装置が待つ時間の長さを指定します。デフォルト値は 3 秒です。極度に遅いブート・パスの場合は、もっと長い時間を設定することが必要になる場合があります。
file name?	基本ダンプ・パスとファイル名 (固有の接尾部を付けることができます)。

ダンプ構成リストを表示するには、**list dump-entries** コマンドを入力します。

例:

```
add dump-entry
remote host [0.0.0.0]? 128.185.162.30
via gateway (0.0.0.0 if none) [0.0.0.0]? 128.185.160.3
timeout in seconds [3]?
file name []? c:\dump\gertrude.dmp
```

Change

change コマンドは、情報を削除して再追加するのではなく、既存のアドレス、ブート項目、およびダンプ項目情報内の項目を変更します。**change** コマンドを使用する代わりに、情報を削除して再入力することもできます。

構文:

```
change                address
                        boot-entry
                        bp-device
                        dump-entry
```

address

以前に追加したブート・インターフェースまたは装置の既存アドレスを変更します。**change address** を入力するときは、次の情報を提供する必要があります。

- アドレス項目番号
- ネットワーク・インターフェースのインターフェース番号
- IP アドレス
- ネットワーク・マスク

注: ブート CONFIG の **list** コマンドを入力すると、この情報の一部のもの (アドレス項目番号など) がコンソールに表示されます。インターフェース番号 (Ifc#) を入手したい場合は、CONFIG **list devices** コマンドを使用します。(このコマンドについては、47ページの『CONFIG とは』で説明しています。)

例:

```
change address
Change which entry [1]? 1
Which interface is this address for [0]? 1
New address [192.9.1.1]? 128.185.162.1
Net mask for this interface [255.255.255.0]?
```

boot-entry

以前に追加したネットワーク・ブート・ファイルに関する構成を変更します。**change boot-entry** コマンドを入力するときは、次の情報を提供する必要があります。

- ブート項目番号
- リモート・ホストの IP アドレス
- 最初のホップ・ルーターの IP アドレス (存在する場合)
- TFTP 再送タイマー値
- ブート・ファイル名 (現行ファイル名と異なる場合)

注: ブート CONFIG の **list boot-entries** コマンドを入力すると、この情報の一部のもの (ブート項目番号など) コンソールに表示されます。

例:

```
change boot-entry
change which entry [1]?
remote host [18.123.0.16]?
via gateway (0.0.0.0 if none) [0.0.0.0]?
timeout in seconds [3]?
file name [user/lib/gw/gwimage.ldb]?
```

bp-device

BOOTP 装置であるインターフェースを変更します。インターフェースの項目番号を入手するには、**list boot-entries** コマンドを使用します。

例:

```
change bp-device
Change which entry [1]?
Which interface is this entry for [1]?
```

注: BOOTP プロトコルと関連のプロセスについての詳細は *プロトコルの構成と監視 解説書* の中の IP プロトコルの構成と監視に関する章を参照してください。

dump-entry

以前に追加したネットワーク・ダンプ・ファイルに関する構成を変更します。**change dump-entry** コマンドを入力するときは、次の情報を提供する必要があります。

- ダンプ項目番号
- リモート・ホストの IP アドレス
- 最初のホップ・ルーターの IP アドレス (存在する場合)
- TFTP 再送タイマー値
- 基本ブート・ファイル名 (現行ファイル名と異なる場合)

注: この情報を表示するには、ブート CONFIG の **list dump-entries** コマンドを使用します。

例:

```
change dump-entry
change which entry [1]? 1
remote host [18.123.0.16]?
via gateway (0.0.0.0 if none) [0.0.0.0]?
timeout in seconds [3]?
file name [user/lib/gw/gwimage.ldb]? c:\dump\debug1.dmp
```


Copy

copy コマンドは、リモート・ルーターとホストの間でブート・ファイルおよび構成ファイルをコピーするのに使用します。 **copy** コマンドを使用するためには、装置に IP が構成されており、少なくとも 1 つのインターフェース上で稼働していることが必要です。装置は Config-only モードであってはなりません。

構文:

```
copy                config
                    [ibd or filename]
                    [host-ip-address or filename]
```

例 1 - リモート・ルーターからのコピー

```
Boot config> copy
source filename [CONFIG] 128.185.110.30/ibd/Y17.1dc
destination filename IBD/Y17.1dc
```

Source filename および *destination filename* は、次のいずれかでなければなりません。

config 構成メモリー

ibd/filename

IBD にあるファイル名。完全なパス名を指定してください。

IP address/remote

TFTP ホストにあるリモート・ファイル

path and filename

完全なパス名を指定してください。

注: IBD にファイルをコピーするときには、ファイルは連続した空きバンクの最も大きい集合に入れられます。バンクが利用不能の場合は、コンソールに COPY error - TFTP Disk Full or IBD full というメッセージが表示されます。

上の例では、128.185.110.30 の IP アドレスをもつリモート・ルーターからソース・ファイル入手します。IBD のファイル名は Y17.1dc です。ここではコロン (:) は区切り文字として使用されています。 *destination* のファイル名は Y17.cfg です。

例 2 - リモート・ホストからのコピー

```
Boot config> copy
source filename [CONFIG] 128.185.110.30/router/loads/2210.02.cfg
destination filename ibd/2210.02.cfg
```

上の例では、ソースはパスとファイル名が指定されています。あて先は IBD です。

例 3 - 装置内でのコピー

```
Boot config> copy
source filename [CONFIG] config
destination filename [CONFIG]? ibd/2210.02.cfg
```

上の例では、ソースは構成メモリーです。あて先は IBD です。

config copy と入力して **Enter** キーを押したと同じ結果が得られます。ただし、ソース・ファイル名を求めるプロンプトは表示されません。

[*ibid* or *filename*]

IBD からブート・ファイルまたは構成ファイルをコピーします。ファイル名を含める必要があります。

[*host-ip-address* or *filename*]

リモート・ホストからブート・ファイルまたは構成ファイルをコピーします。ファイル名を含める必要があります。

Delete

delete コマンドは、ブートおよびダンプの構成データベースから項目を除去するのに使用します。

構文:

```
delete address  
boot-entry  
bp-device  
dump-entry
```

address

ブートおよびダンプの構成データベースからインターフェース・アドレス項目を除去します。

delete address コマンドを入力すると、削除したい項目を尋ねるプロンプトが表示されます。アドレス・エン트리番号は、`Boot config>>` プロンプトで

list address コマンドを入力したときに各行に表示される最初の番号です。

削除されたことを確認するには、**list** コマンドを使用します。

例:

```
delete address  
Delete which entry [1]?
```

boot-entry

ブートおよびダンプの構成データベースからブート項目を除去します。

delete boot-entry コマンドを入力すると、削除したいブート項目を尋ねるプロンプトが表示されます。ブート項目番号は、`Boot config>>` プロンプトで

list boot-entries コマンドを入力したときに各行に表示される最初の番号です。

削除されたことを確認するには、**list** コマンドを使用します。

例:

```
delete boot-entry  
Delete which entry [1]? 2
```

bp-device

BOOTP 装置として指定されたインターフェースを除去します。

例:

```
delete bp-device  
Delete which entry [1]?
```

注: BootP プロトコルと関連のプロセスについての詳細は *プロトコルの構成と監視 解説書* 中の IP プロトコルの構成と監視に関する章を参照してください。

dump-entry

ブートおよびダンプの構成データベースからダンプ項目を除去します。**delete dump-entry** コマンドを入力すると、削除したい項目を尋ねるプロンプトが表示されます。ダンプ項目番号は、Boot config>> プロンプトで **list dump-entries** コマンドを入力したときに各行に表示される最初の番号です。削除されたことを確認するには、**list** コマンドを使用します。

例:

```
delete dump-entry
Delete which entry [1]?
```

Describe

describe コマンドは、IBD に保管されているイメージに関する情報を表示するのに使用します。

構文:

describe *loadname*

loadname

指定されたロード名に関する以下の情報を表示します。

- 著作権情報
- サポートされるプロトコル、フィーチャー、およびデータ・リンク・タイプ
- サポートされるネットワーク・インターフェース

例:

```
describe ibd/test.ldb
Copyright Notice .....

IBM 2210 Bridging Router V1 R2.0[Y69] Wed Mar 8 10:24:20 1995
Software configuration: Expanded Multi-Protocol DLsw
Includes:
Internet Protocol - IP & OSPF
Novell - IPX
AppleTalk Phase 2 - AP2
Banyan VINES - VIN
Adaptive Source Routing Transparent Bridge - ASRT
with NETBIOS Name Caching & Filtering
Data Link Switching - DLsw
SDLC Relay - SRLY
Frame Relay
PPP
X.25
V.25bis
WAN Restoral/Reroute - WRS
Bandwidth Reservation - BRS
MAC Filtering - MCF
```

Disable

disable コマンドは、メモリー・ダンプおよびダンプ・ファイルの固有の命名を使用不可にするのに使用します。

構文:

disable dumping
 unique-naming

dumping

システム障害の発生時に装置がネットワークへのメモリー・ダンプを実行するのを抑止します。このコマンドを入力した後、ブート CONFIG の **list all** コマンドを使用してダンプ設定値を確認してください。 **enable dumping** コマンドを入力するまで、ダンプは抑制されます。 **Disable dumping** がデフォルト設定です。

unique-naming

ダンプ・ファイルの自動固有命名を抑制します。このコマンドを入力した後、ブート CONFIG の **list all** コマンドを使用して、固有命名の設定値を確認してください。 **enable unique-naming** コマンドを入力するまで、固有命名は抑制されます。 **Disable unique-naming** がデフォルト設定です。

Enable

enable コマンドは、メモリー・ダンプおよびダンプ・ファイルの固有命名を使用可能にします。 **add dump-entry** コマンドで供給されたデータを使用したダンプ操作をオンにするには、このコマンドを使用する必要があります。ダンプを使用可能にするのは、装置に原因不明の問題が生じた場合だけにすることが必要です。ダンプ・ファイルは非常に大きくなり、ディスク・スペースを大量に消費する可能性があります。インターネットを介して大きなダンプ・ファイルをダンプ・ホストに転送するのは、かなりの時間がかかります。

構文:

enable dumping
 unique-naming

dumping

システム障害の発生時に装置がネットワークへのメモリー・ダンプを実行するのを可能にします。このコマンドを入力した後、ブート CONFIG の **list all** コマンドを使用してダンプ設定値を確認してください。 **disable dumping** コマンドを入力するまで、ダンプは使用可能です。

unique-naming

ダンプ・ファイルの固有命名を使用可能にします。ダンプ時に、構成済みダンプ・ファイル名に 1 ～ 5 文字のランダムな接尾部 (16 進数) が追加されます。

このコマンドを入力した後、ブート CONFIG の **list all** コマンドを使用して、固有命名の設定値を確認してください。 **disable unique-naming** コマンドを入力するまで、ダンプ・ファイルには固有の名前が組み込まれます。

Erase

erase コマンドは、保管されているイメージまたは IBD バンクを消去するのに使用します。

構文:

erase [loadname または bank-number]

loadname または **bank-number**

保管されているイメージまたは IBD バンクを消去します。**erase** コマンドの後に、ロード名またはロードが入っているバンク番号 (1 ~ 64) を入力します。消去されたことを確認するには、**list ibd** コマンドを使用します。

10 回の試行しても消去が正常に行われない場合、装置はそのバンクに障害のマークを付けます。

IBD パラメーター:

IBD サイズ: 4 MB

バンク・サイズ: 64 KB

開始バンク番号: 1

終了バンク番号: 64

ロード・イメージ・ファイルが大きくて 2 つ以上のバンクにまたがっている場合は、バンク番号を指定すると、ロード・イメージ・ファイルが部分的に消去されることになる場合があります。

例 1:

```
erase test
Erasing bank 5 ...
Banks 1-4 contain ...
Banks 5-7 have been erased
```

例 2:

```
erase 2
Are you sure you want to erase bank 2? (Yes or [No]): yes
Erasing bank 2 ...
Banks 5-7 has been erased
```

例 3:

```
erase
Loadname or Bank Number: 4
Are you sure you want to erase bank 4? (Yes or [No]): yes
Erasing bank 4...
Bank 1 contains load "v1-29.cfg" which use 131094 bytes
  Loaded using TFTP over IP
  Filename config
  Host 0.0.0.0
Banks 2-3 contain load "v1-22.cfg" which uses 1832848 bytes
  Manual Booted using TKR-4/16 at (80001000, 72) as 10.1.155.29
  Filename loads/latest-gen.c5-multisna.ldc
  Host 128.185.210.125, Gateway 10.1.155.43
Bank 4 has been erased
```

消去が正常に行われなかった場合は、障害を示すメッセージが、障害を生じたバンクとともにコンソールに表示されます。ルーターがリスタートされていない場合は、**list** コマンドを使用して、障害情報を表示することができます。ルーターは、障害のあるバンク内のイメージを参照するブート・レコードを自動的に削除することはありません。

ブート時に、ブート PROM がイメージを見つけれない場合は、メッセージを表示して、次のブート・レコードを試行します。

List

list コマンドは、現行のブートおよびダンプ構成データベース、IBD の内容、およびスケジュールされたイメージ・ロード情報を表示するのに使用します。

構文:

list addresses
all
boot-entries
bp-device
dump-entries
ibd
view

addresses

add address コマンドを使用して入力されたすべてのネットワーク・ブート・インターフェースの IP アドレスとサブネット・マスクを表示します。

例:

```
list addresses
Interface addresses:
1: 192.9.1.1 on interface 0, mask 255.255.255.252
2: 192.9.223.39 on interface 2, mask 255.255.255.0
```

all すべてのブートおよびダンプ構成データ、ならびにダンプ、固有命名機能、およびスケジュールされたイメージ・ロード情報の現行設定値を表示します。

例:

```
Interface Addresses:

Boot files:
  1: "/u/steve/v1/load/v1060694/v1.X11.1dc" on 216.1.2.100 via 0.0.0.

BOOTP over interface(s): 0
Dumping disabled
Unique-naming disabled
Dump to:

Banks 1-19 contain load "v1.X11.1dc" which uses 1199272 bytes
  Loaded using TFTP over IP
  Filename /u/steve/v1/load/v1060694/v1.X11.1dc
  Host 216.1.2.100
Banks 20-48 have been erased
Bank 49 in unknown(AA) state
Banks 50-57 contain load "v1051894.1dc" which uses 508492 bytes
  Loaded using TFTP over IP
  Filename /u/steve/v1/load/v1051894/v1051894.1dc
  Host 216.1.2.100
Banks 58-64 have been erased

Time Activated Load Schedule Information...

The router is scheduled to reload as follows.

Date: April 1, 1997
Time: 13:00
Remote host IP address: 1.1.1.2
Via gateway: 0.0.0.0
Timeout in seconds: 10
Filename: /tftpboot/v13.img
Interface address: 0
New address: 1.1.1.1
New mask: 255.255.255.0
```

boot-entries

ブート・ファイル構成を表示します。

例:

```
list boot-entries
1: /usr/lib/gw/this-dn.ldb on 192.9.1.2 via 0.0.0.0 for 3 secs
2: /usr/lib/gw/this.ldb on 192.9.2.2 via 192.9.1.4 for 3 secs
3: IBD load "test"
```

bp-device

以前に **add bp-device** コマンドを使用して追加されたインターフェースをリストします。

例:

```
list bp-device
BOOTP over interface(s): 0 1
```

dump-entries

ダンプ・ファイル構成を表示します。

ibd IBD の内容を表示します。GWCON **boot information** コマンドと同様の情報を提供し、ファイルのロード名とファイルのロード元のホスト・サーバーを表示します。さらに、必要な場合には、IBD の消去済みおよび障害のあるバンクおよび障害のあるチップも表示されます。

例:

```
list ibd
Bank 1 contains load "2210-29.cfg" which uses 131094 bytes
  Loaded using TFTP over IP
  Filename config
  Host 0.0.0.0
Banks 2-3 contain load "v1/load-ver2.ldc" which uses
  1652961 bytes
  Loaded using TFTP over IP
  Filename loads/v1/load-ver2.ldc
  Host 128.185.210.125
Bank 4 contains load "v1/load-ver4.cfg" which uses 131084 bytes
  Loaded using TFTP over IP
  Filename CONFIG
  Host 0.0.0.0
```

『Loaded using TFTP over IP』は、このローカル・コマンドから IBD への **copy** コマンドが使用されたことを暗黙的に示しています。

view スケジュールされたイメージ・ロードの時刻、日付、およびその他の情報を表示します。

例:

```
list view
Time Activated Load Schedule Information...

The router is scheduled to reload as follows.

Date: April 1, 1997
Time: 13:00
Remote host IP address: 1.1.1.2
Via gateway: 0.0.0.0
Timeout in seconds: 10
Filename: /tftpboot/v13.img
Interface address: 0
New address: 1.1.1.1
Network mask for this interface: 255.255.255.0
```

Load

load コマンドは、ローカルまたはリモート・ソースから装置のメイン・メモリーにブート・ファイルをコピーするのに使用します。**load** コマンドの結果は、* プロンプトから **reload** コマンドを実行した場合と同じです。

構文:

load

_local . . .

_remote . . .

local *loadname*

以前に保管したロード・イメージ・ファイルを装置の IBD から取り出して、ルーターのメモリーに入れます。ロード名は、IBD 内に保管されているロード名の 1つと一致していなければなりません。ロード名は、大文字・小文字を区別します。

IBD をセットアップするには **add boot-entry** コマンドを使用します。これには最高で 5 分ほどかかります。

IBD 内にロード・ファイルがないと、**load local** コマンドは正常に行われません。

例:

```
load local  
Loadname: ibd/softrel.ldc
```

注: ソフトウェアは、ロード・ファイルが見つからない場合はブート・モニターに行き、ブート・スイッチの設定に応じて、自動ブートまたは手動ブートを実行します。

remote

リモート・ホストから RAM ヘブート・ファイルをロードします。リモート・ロードを実行するには、次のようにします。

1. Boot config> が表示された後、**load remote** コマンドを入力し、プロンプトで指示されたら、リモート・ホスト・アドレス、リモート・パス名、最初のホップ・アドレス、および TFTP タイムアウトを入力します。
2. 次にロードの確認を求めるプロンプトが出ます。 **no** を入力すると、コマンドは取り消されます。 **yes** を入力すると、リモート・ホストから RAM にブート・ファイルがロードされます。

例:

```
load remote  
Remote Host Address [0.0.0.0]? 128.185.210.125  
Remote Pathname[]? /loads/v1.ldc  
First Hop Address[0.0.0.0]? 128.185.208.38  
TFTP Timeout Value [3]?  
Are you sure you want to reload the gateway(Yes or No): yes
```

Remote Host Address

ブート・ファイルが入っているホストの IP アドレス

Remote Pathname

ロードしたいブート・ファイルのパス名とファイル名

First Hop Address

他のネットワークに転送する最初のホップ・ルーターのアドレス。リモート・ホスト・アドレスが直接接続されたネットワーク上には、これを指定する必要があります。そうでない場合は、デフォルト値の 0.0.0.0 を使用します。

TFTP Timeout Value

TFTP パケットの再転送の時間間隔。低速のネットワークやシリアル回線を介してブートする場合、長い時間値 (デフォルト値の 3 より長い時間値) を指定することが必要になる場合があります。

Store

store local コマンドは、IBD の消去済みバンクに圧縮イメージを保管するのに使用します。保管されたバイト数がコンソールに表示されます。イメージが保管されたことを確認するには、**list ibd** コマンドを使用します。

注: ルーターは、バンク 1 ~ 4 に順番にイメージを保管します。4 つのバンクすべてがいっぱいの場合、エラー・メッセージを受け取ります。バンク内にスペースを作成するには、**erase loadname** または **erase bank-number** コマンドを使用します。

装置のロード・イメージ・ファイルは、IBD に保管されるときに圧縮されます。ロード・イメージ・ファイルは、消去されていない IBD には上書きせず、また IBD の終わりを超えると書き込みを試みません。圧縮が失敗した場合は、オペレーターに通知され、影響を受けた IBD は消去されます。

ロード名の長さは最大 80 文字の任意の名前が可能で、英字で始まり、大文字・小文字を区別します。

構文:

store *local loadname*

loadname

指定されたイメージを IBD の消去済みバンクに保管します。

例:

```
store local
Loadname: test
Will start storing at bank #2
.
.
Number (dec) bytes used
Boot config>
```

Timedload

timedload コマンドは、装置へのイメージ・ロードをスケジュールする、スケジュールされたロードを取り消す、またはスケジュールされたロード情報を表示するのに使用します。

このコマンドにより、サポート技術員が不在のときでも、ネットワーク通信量のピーク期間を外して装置へのロードを実行することが可能になります。

構文:

timedload *activate*
deactivate
view

activate

装置へのイメージ・ロードをスケジュールします。 **add boot-entry** および

add address コマンドと同様に、イメージのソースを説明する情報の入力を求められます。パラメーターについての詳細は、114ページの『Add』を参照してください。

Time of day to load image

装置が新しいイメージをロードする日付と時刻を指定します。この値は *YYYYMMDDHHMM* 形式で指定します。ただし、

YYYY は 4 桁の年号です。

注: 装置の現在の月が 12 月のときは、年号データは現行年または翌年でなければなりません。また、装置の現在の月が 1 月～11 月のときは、年号データは現行年でなければなりません。

MM は 2 桁の月です。

MM の有効値: 01 ~ 12 (01 は 1 月を表します)

DD は 2 桁の日です。

DD の有効値: 01 ~ 31 (*MM* の値によって異なります)

HH は 2 桁の時間 (24 時間計) です。

HH の有効値: 00 ~ 23

MM は 2 桁の分です。

MM の有効値: 00 ~ 59

以下に、種々のソースからのロードをスケジュールする例を示します。

例 1: リモート・ホストからのロード

```
Boot config> timedload activate
Time Activated Load Processing...

Remote host IP address or IBD load name [0.0.0.0] 1.1.1.2
Via gateway (0.0.0.0 if none) [0.0.0.0]? 0.0.0.0
Timeout in seconds [10]? 10
File name []? /tftpboot/v13.cce
Do you want to configure an interface address? (Yes, No, Quit): [No] yes
Which interface do you want to configure an address to boot over [0]? 0
New address [0.0.0.0]? 1.1.1.1
Network mask for this interface [255.255.255.0]? 255.255.255.0
Config filename [CONFIG] ? ibd/v13.cfg
Time of day to load image (YYYYMMDDHHMM) []? 199703191630
The load timer has been activated.
```

例 2: IBD からのロード

```
Boot config> timedload activate
Time Activated Load Processing...

Remote host IP address or IBD load name [0.0.0.0] ibd:v13.cce
Time of day to load image (YYYYMMDDHHMM) []? 199703191630
The load timer has been activated.
```

deactivate

スケジュールされたロードを取り消します。

例 1: 時刻によって起動されたロードの非活動化

```
Boot Config> timedload deactivate
Deactivate Load Timer Processing...

Do you want to deactivate the load timer? (Yes, No, Quit) [No]? yes
The load timer has been deactivated
```

view スケジュールされたロード情報を表示します。

例 1: ロード・イメージ・ソースがリモート・ホストの場合

```
Boot Config> timedload view
Time Activated Load Schedule Information...

The router is scheduled to reload as follows.

Date: March 19, 1997
Time: 16:30
Remote host IP address: 1.1.1.2
Via gateway: 0.0.0.0
Timeout in seconds: 10
Filename: /tftpboot/v13.cce
Interface address: 0
New address: 1.1.1.1
Network mask for this interface: 255.255.255.0
Config filename: ibd/v13.cfg
```

例 2: ロード・イメージ・ソースが IBD の場合

```
Boot Config> timedload view
Time Activated Load Schedule Information...

The router is scheduled to reload as follows.

Date: March 19, 1997
Time: 16:30
Filename: v13.cce
Config filename: ibd/v13.cfg
```

TFTP

TFTP コマンドは、リモート・ホストと装置の不揮発性構成メモリーまたは IBD の間で TFTP ファイル転送を開始するのに使用します。このコマンドにより、TFTP サーバーまたは IBD をもつルーターとの間でロード・イメージを保管/検索する機能が提供されます。

ルーターは TFTP クライアントとして動作します。リモート・ホストは、TFTP サーバー・ノードとして動作する、IP を実行している任意の装置 (たとえば、ルーター、ワークステーション、PC) です。ルーターは Config-only モードであってはなりません。

TFTP get および **put** コマンドを入力すると、この操作の間、CONFIG プロセスはロックされます。TFTP 操作時には、次の 2 つのキーボード文字の組み合わせが認識されます。

Ctrl-P OPCON プロンプト (*) を表示します。

Ctrl-C TFTP 操作を取り消します。

注: ルーターが **TFTP get** 操作を実行中は、リセット・ボタンを押さないでください。リセット・ボタンを押すとルーターの電源が切れます。この場合、あて先の構成メモリーは矛盾した (無効な) 状態になります。すなわち、構成またはロードの一部分しか持っていないこととなりますが、これが有効であるように見えます。

構文:

```
tftp                                get
                                       put
```

get CONFIG address-remote-server path/filename

サーバーから 装置へ ファイルを転送するために、TFTP サーバーへの要求を開始します。サーバーはデータ・パケットを送信し、クライアントはデータの受信を確認します。このサイクルは、転送が完了し、次のようなメッセージがコンソールに表示されるまで続きます。

TFTP transfer complete, Status: OK

TFTP 転送が失敗すると、詳細なエラー・メッセージが画面に表示されます。ファイルを CONFIG に転送している間、次のようなメッセージがコンソールに表示されます。

Updating Config: Do Not Interrupt

IBD にファイルを転送しようとしたときに、IBD 内に十分なメモリがない場合には、次のようなメッセージがコンソールに表示されます。

No Free IBD Bank

重要: 構成メモリの更新が進行中に、ルーターをリセットしたり、電源を切ったりしてはなりません。そうすると、構成メモリ内のデータが破壊され、ルーターを再構成しなければならなくなります。

例:

```
tftp get
local filename [CONFIG]?
remote host [0.0.0.0]? 128.185.163.1
host filename [0A019947.cfg]? configs/v1-28.cfg
TFTP transfer complete, status: OK
```

Local filename

ローカル装置に転送された後のファイル名を指定します。ファイルを IBD に転送する場合は、ファイル名を入力するときに、必ず**完全**なパス名を指定してください。デフォルトは CONFIG です。

Remote Host

転送したいファイルが入っているホストのアドレスを指定します。ファイルに保管されているマジック・ナンバーが、静的 RAM 内の番号と比較されます。こうすることによって、ルーターのタイプ間で、不揮発性メモリーを取り違えてロードするのを防止することができます。

Host filename

ホスト上の転送したいファイルの名前を指定します。必ず、**完全**なパス名を指定してください。デフォルト値は、ホストの IP アドレス (16 進数) の 1 つを ASCII 表示したものです。これによって、ファイルは固有の名前を持ちます。

ホスト名は、保存ファイル内のホスト名と一致していなければなりません。ホスト名は大文字・小文字を区別します。

put CONFIG address-remote-server path/filename

ルーターから サーバーへ ファイルを転送するために、TFTP サーバーへの要求を開始します。サーバーは要求に対して確認応答し、クライアントはファイルを転送します。このサイクルは、転送が完了し、次のようなメッセージがコンソールに表示されるまで続きます。

TFTP transfer complete, Status: OK

注: TFTP put コマンドを用いて、別の装置の構成メモリーまたは IBD にファイルを入れることはできません。そのようにしたい場合は、該当の装置にログインし、TFTP get コマンドを使用する必要があります。

コンソールの表示は TFTP get コマンドの場合と同じです。

例:

```
tftp put
Local filename [CONFIG]?
Remote host [0.0.0.0]? 128.185.163.1
Host filename [0A019947.cfg]?
TFTP transfer complete, status: Timeout
```

local filename?

CONFIG が、装置の不揮発性メモリーを参照するファイル名です。

remote Host?

CONFIG をリモート・ホストに保管するために使用する、リモート・ホストの IP アドレスとファイル名を指定する必要があります。

host filename?

ホスト上の転送したいファイルの名前を指定します。必ず、完全なパス名を指定してください。デフォルト値は、ホストの IP アドレス (16 進数) の 1 つを ASCII 表示したものです。これによって、ファイルは固有の名前を持ちます。ホスト名は、保存ファイル内のホスト名と一致していなければなりません。ホスト名は大文字・小文字を区別します。

例:

```
tftp put IBD/r151.ldc
Remote host [0.0.0.0]? 140.187.2.100
Host filename [80B9D626.cfg]? v1605.ldc
TFTP transfer complete, status: OK
```

TFTP トランザクションを中断する場合は、**Ctrl-C** を押します。Are you sure (yes or no): に対して **yes** と応答します。

TFTP コマンドは、以下のエラー・メッセージを生成します。

エラー・メッセージ	意味
Unknown Error	プロトコル障害
File Not Found	指定したホスト・ファイルが存在しない。
Access Violation	ファイル保護エラー
Disk Full	書き込み中にファイル・システムがいっぱいになった。
Illegal Operation	未定義の TFTP 操作が要求された。
Unknown TID	予期しない TFTP パケットを受信した。
File Already Exists	ファイルはすでに存在している。
No Such User	TFTP がホストでサポートされていない。

第7章 ブート・オプション

この章では、使用可能なブート・オプションについて説明します。通常、装置は統合ブート装置 (IBD) からブートします。本章が必要となるのは、保守または診断操作のため、あるいはソフトウェア・アップグレードの場合のみです。

ブート・オプションにより、以下の方式によって 2210 をブートすることができます。

表 13. ブート方式の説明

ブート方式	説明
IBD	照会を使用して IBD からブートする。2210 は異なるブート方式に構成されているが、それに代えて IBD から 2210 をブートしたい場合に、この方式を使用します。
TFTP ホスト・サーバー	TFTP ホスト・サーバー上のロード・イメージ・ファイルからブートする。別のルーターが TFTP ホスト・サーバーとして動作することができます。
BOOTP	ブートストラップ・プロトコルを用いて LAN ポートを介してブートする。

ブート・モニター・プロンプトから使用可能なその他のオプションを使用して、診断の実行、構成情報の表示、ネットワーク上のホストからまたはサービス・ポートを介した構成メモリのロード、SRAM 内の構成の消去、およびサービス・ポートを介したルーター・コードのダウンロードとアップロードを実行することができます。

この章には、以下の節が含まれています。

- 『始める前に』
- 135ページの『使用可能なブート・オプション』
- 137ページの『ブート・オプション・プロンプト』
- 148ページの『2210 の構成』

始める前に

2210 をブートする前に、以下のことに注意してください。

- この章の手順を使用するためには、2210 に直接接続された端末が必要です (端末の接続方法については、2210 *Nways* マルチプロトコル・ルーター 設置と初期構成の手引き を参照してください。)
- 2210 は、ブート・ファイル (IBD に保管されている) を添えて出荷されます。
- 2210 を ISDN インターフェースを介してブートすることはできません。
- トークンリング・インターフェースを介してブートしている場合、アクティブのトークンリング・リンクがない場合には、次のメッセージを受け取ります。

```
lobe media test failed: function failure.
```

注: 2210 のブートを停止する場合は、端末のキーボードで **Ctrl-C** を押します。

コンソール端末を使用した統合ブート装置からのブート

コンソール端末を使用した IBD ブートの例は、この手順の最後に示します。このブート方式は、IBD にロード・イメージが保管されている場合に使用します。

1. 次のような著作権情報がコンソールの画面に表示されていなければなりません。必要な場合は、**Reset** ボタンを押してから **Ctrl-C** を押して、この情報を表示させてください。

```
Bootstrap Monitor V1.0  
(c) Copyright IBM Corp. 1994, 1997
```

2. **bm** と入力すると、次の情報と最初のブート・プロンプトがコンソールに表示されます。

```
PROM Load/Dump Program * Revision: 1.0 *  
Copyright IBM Corp. 1994, 1997
```

```
IBD has load(s) load image names
```

```
Device Slot Number or IBD Load Name:
```

3. ロード・イメージ名を入力します。IBD ロード名は、大文字・小文字を区別します。**Return** を押してください。次のメッセージが表示されれば、ソフトウェアのロードが進行しています。

```
Loading using IBD Load Image "ibmMRNS.1dc"
```

コンソール端末を使用した BOOTP

BOOTPは、最初に自己テストが正常に行われたカードから始めて、すべての可能なハードウェア構成を使用して、すべての導入済みインターフェースを介してブートを試みます。通常は、イーサネット、次にトークンリングの順で行われます。BOOTP に関する詳しい情報は、第5章 ブート CONFIG プロセス を参照してください。

コンソールに次の情報が表示されれば、BOOTP ブートが成功したことを示します。

```
PROM Load/Dump Program * Revision: 1.0 *  
Copyright IBM Corp. 1994, 1997
```

```
BOOTP Using interface name at (CSR address, vector address)
```

```
Trying connector
```

```
Doing BOOTP
```

```
Trying host IP address
```

```
file name
```

```
loading
```

```
Copyright IBM Corp. 1994, 1997
```

```
Config Only Mode - Switch Selected
```

```
*
```

* は、ロード・イメージのロードが終了したことを示します。

BOOTP の失敗

BOOTP ブートは、次の条件下では正常に行われません。

- サーバーが 2210 について知らない場合。コンソールには次の情報が表示されます。

```
PROM Load/Dump Program * Revision: 1.0 *  
Copyright IBM Corp. 1994, 1997
```

```
BOOTP Using interface at (CSR address, vector address)
```



```
Trying connector
Doing BOOTP          BOOTP timeout
Auto BOOTP failed
```

コンソールには、手動ブートを行うように指示するプロンプトが出ます。これらのプロンプトについての説明は、137ページの表15 に示してあります。

- サーバーは 2210 について知っていても、ロード・ファイルが存在しない場合、コンソールには次のような情報が表示されます。

```
PROM Load/Dump Program * Revision: 1.0 *
Copyright IBM Corp. 1994, 1997
```

```
BOOTP Using interface at (CSR address, vector address)
```

```
Trying connector
Doing BOOTP
BOOTP got reply but server sent no filename
Manual BOOTP failed - Enter @ at prompt BOOTP again
```

@ を入力して、BOOTP を再度試行してください。再試行も失敗した場合は、別の方法を使用して 2210 をブートします。

コンソール端末を使用した TFTP ホスト・サーバーからのブート

TFTP ホスト・サーバー上のロード・イメージ・ファイルを使用して、2210 をブートすることができます。別のルーターが TFTP ホスト・サーバーとして動作することができます。TFTP ブートの例を、以下に示します。

1. ブート・モニター・プロンプト (>) で **bm** と入力して、次のような情報と最初のブート・プロンプトを表示します。

```
PROM Load/Dump Program * Revision: 1.0 *
Copyright IBM Corp. 1994, 1997
```

```
Device Types available:
```

```
   IBD
   Token Ring
   WAN
```

2. 表示されるプロンプトは、ブートに使用するインターフェースのタイプによって異なります。イーサネット、トークンリング、または WAN ポートのブートについての詳細は、139ページの『BM (コンソール照会を使用したブート)』を参照してください。これらのプロンプトについての説明は、137ページの表15 に示してあります。

使用可能なブート・オプション

136ページの表14 に、使用可能なブート・オプションのリストを示してあります。表の後に、ブート・プロセスおよびシステム・プロンプトの詳しい説明があります。

ブート・オプションへのアクセス

1. ロード手順を開始するために、装置の電源を入れるか、または OPCON (*) プロンプトで **reload** と入力し、**Enter** キーを押します。
2. ブート・モニター・プロンプト (>) を表示するために、ロード手順中に **Ctrl-C** を押します。

3. ブート・プロンプト (>) で ? と入力すると、ブート・オプションが表示されま
す。表14 は、これらのオプションについて説明しています。

表14. ブート・オプション

オプション	名前	説明
B	保管済み構成を使用したブート	TFTP または IBD 内に保管されている構成を使用して自動的にブートします。
BC	コンソール照会を使用した Config-only モードへのブート	2210 を手動でブートするためのプロンプトを表示し、Config-only モードに入ります。2210 の構成を開始することができます。
BM	コンソール照会を使用したブート	2210 を手動でブートするためのプロンプトを表示します。これらのプロンプトについての説明は、137ページの表15 に示してあります。
BN	コンソール照会を使用したブート (実行禁止)	デバッグのためにサービス技術員が使用します。ブートしてブートストラップ・モニターへ戻りません。ただし、ロードは開始しません。
BP	BOOTP を使用したブート	ブートストラップ・プロトコルを使用してブートするためのプロンプトを表示します。
D	保管済み構成を使用したダンプ	このフィーチャーは現在 2210 上では利用できません。
DIAG	IBM 拡張診断の開始	内部テストを開始します。内部テストが完了したら、システム拡張チェックアウト (内部テストと外部テスト)、WAN/LAN 折り返しテスト・メニュー、または診断ユーティリティを使用して、テストを継続するかどうかの選択ができます。いつでも終了して再ブートすることができます。
DM	コンソール照会を使用したダンプ	このフィーチャーは現在 2210 上では利用できません。
UB	ブート構成の表示	静的 RAM の TFTP ブートストラップ構成を表示します。
UC	ハードウェア構成の表示	ハードウェア構成に関する情報を表示します。これには装置タイプ、ボー・レート、記憶域サイズ、基本 MAC アドレス、部品番号、製造番号、および改訂レベルが含まれます。
UG	RAM 内のアドレスへの移動と実行	このオプションはサービス技術員が使用します。
LC	構成メモリのロード	ネットワークに接続するホストから構成メモリーをロードします。
CC	構成メモリの消去	SRAM 内の構成を消去します。
ZB	ZModem ブート	サービス・ポートを通してルーター・コードをダウンロードおよびアップロードします。
ZC	ZModem 構成メモリーのロード	サービス・ポートを通して構成メモリーをロードします。

ブート・オプション・プロンプト

以下では、各ブート・オプションについて詳しく説明します。

表15 では、2210 がブートされたときに表示されるプロンプトについて説明しています。これらのプロンプトは、ハードウェア構成および 2210 にロードされているソフトウェアによって異なります。

表 15. ブート・オプション・プロンプト

プロンプト	説明
Device Type	2210 のブートを行う装置タイプ。IBD、トークンリング、あるいはイーサネット・インターフェース
IBD Loadname	IBD ロード名。最大 79 の文字、数字、記号を含めることができ、大文字・小文字を区別します。初期導入時に、リリース情報 (バックアップ・ソフトウェア・ディスク上ファイル README.NTS) にファイル名を入力します。
Interface IP Address	ブートに使用する 2210 インターフェースの IP アドレス
IP Mask	IP ネットワーク・アドレスを他の IP アドレス・フィールドから分離する 16 進値。ネットワークとサブネットの部分のビットはすべて 1 でなければなりません。
Boot From Host	ブート元のホストの IP アドレス
Via gateway	ブート元のホストが別の (サブ) ネットワークにある場合、中間ルーターが存在します。その中間ルーターの IP アドレスを入力します。
Load Image Name	初期導入の場合、リリース情報 (バックアップ・ソフトウェア・ディスク上ファイル README.NTS) に記載されているロード・イメージ名を入力します。
Boot File Name	ホスト・サーバーに常駐するロード・イメージ・ファイルのフル・パス名。たとえば、/usr/local/ibm2210.ldc (UNIX の例)。
イーサネット・プロンプト	
Connector Type (AUI/RJ45)	以下のいずれかを入力して、このポートに接続されるケーブル・タイプを指定します。 AUI Thick/AUI (10BASE5) RJ45 シールドなし対より線 (10BASE-T) AUTOCONFIG ケーブル・タイプを自動的に検知します。
トークンリング・プロンプト	
Speed (4/16) Mb	4 または 16 を入力して、トークンリング媒体の転送速度を Mbps 単位で指定します。 注: 入力する値は、リングの速度と一致していなければなりません。
Media (UTP/STP)	以下のいずれかを入力して、このインターフェースに接続されるケーブル・タイプを指定します。 UTP シールドなし対より線 STP シールド付き対より線
WAN プロンプト	

表 15. ブート・オプション・プロンプト (続き)

プロンプト	説明
WAN port	2210 をブートするのに使用する WAN ポート。1 または 2。
Timeout (secs)	インターフェースがネットワークを介してブートを試みる時間の長さ (秒)。タイムアウトは 5 秒より大きくなければなりません。
Clock Source (INT/EXT)	接続によって、次のようになります。 <ul style="list-style-type: none"> • モデムまたは DSU に接続している場合、外部刻時を指定する EXT を入力します。 • DTE 装置に接続し、DCE ケーブルを使用している場合は、内部刻時を指定する INT を入力します。
Internal Clock Speed	このプロンプトは、Clock Source として INT を入力した場合のみ表示されます。範囲は 1 ~ 10 000 000 です。
Cable Type (X21/Other)	X.21 ケーブルをこのポートに入力する場合は、 X21 を入力します。他のケーブル・タイプをこのポートに接続する場合は、 other を入力します。

B (ブート)

構成メモリーに保管されている構成を使用して、ルーターを自動的にブートします。構成が TFTP ホストに保管されていない限り、このオプションはルーターに IBD からブートさせます。

BC (Config-only モードでのブート)

2210 をブートし、ただちに Config-only モードに入ります。以下の例は、IBD、トークンリング、イーサネット、および WAN インターフェースを介して 2210 をブートする方法を示しています。ユーザーの入力は太字体で示されています。大括弧内に示されているデフォルト値を受け入れる場合は、**Enter** を押します。

注: 以下のインターフェース・ダイアログの例では、装置のインターフェース・タイプは、Device Types リストおよび Device Type プロンプトには、トークンリングまたはイーサネットのいずれかとして示されています。

ブート・プロンプト (>) で **bc** と入力します。ソフトウェアは、次のルーター情報の入力を求めます。

Device Types available:

```

IBD
Token Ring/Ethernet
WAN
Device Type [WAN]: IBD

```

• **IBD** を入力すると、以下が表示されます。

```

IBD has load(s) loadname
IBD Load Name: loadname

```

現行構成を再ロードする場合は、**Enter** を押します。

```

Loading using IBD Load Image "load name"

```

正しくないか、あるいは存在しないロード名を指定すると、システムはメッセージ No such load を出して、IBD Load Name のプロンプトに戻ります。

- **Token Ring** と入力すると、以下が表示されます。

```
Media (UTP/STP) [UTP]:  
Speed (4/16)Mb [16Mb]:  
Interface IP address: 123.175.23.119  
IP Mask (FFFFFF00):  
Boot from host: 123.175.68.190  
Via gateway: 123.175.23.213  
Boot file name: ibmMRNS.ldc
```

```
Using Token Ring at (6000000, 0).  
Trying host 123.175.68.190 via 123.175.23.213  
file ibmMRNS.ldc
```

```
.loading  
.....
```

```
Starting at 1040010
```

```
The Standalone Configuration Process. You are here because  
the watchdog timer timed out and/or Autoboot not selected.
```

```
Config (only)>
```

トークンリング・リンクがアクティブでない場合、次のメッセージを受け取りま
す。

```
lobe media test failed: function failure
```

- **Ethernet** を入力すると、以下が表示されます。

```
Connector Type (AUI/RJ45) [AUTO_CONFIG]:  
Interface IP Address: 123.175.56.119  
IP Mask (FFFFFF00):  
Boot from host: 123.175.68.213  
Via Gateway: 123.175.56.190  
Boot File Name: ibmMRNS.ldc
```

```
Using Ethernet at (6000000, 0)  
Trying host 123.175.68.213 via 123.175.56.190  
file ibmMRNS.ldc
```

```
.loading  
.....
```

```
Starting at 1040010
```

```
The Standalone Configuration Process. You are here because  
the watchdog timer timed out and/or Autoboot not selected.
```

```
Config (only)>
```

- **WAN** を介したブート

指定された WAN ポート上でアクティブとなっている CTS 信号が存在しない場合
には、CTS not active on WAN port # というメッセージを受け取ります。

注: PPP プロトコルは、WAN インターフェースを介してブートするときに使用可
能な、現在では唯一のデータ・リンク・レイヤー・プロトコルです。

BM (コンソール照会を使用したブート)

コンソール照会を使用してブートを実行します。以下の例は、IBD を介して、また
トークンリング、イーサネット、および WAN インターフェースを介して 2210 をブ

ートする方法を示しています。ユーザーの入力は太字体で示されています。大括弧内に示されているデフォルト値を受け入れる場合は、**Enter** を押します。

このオプションを使用して TFTP ホスト・サーバー上のロード・イメージ・ファイルからブートすることもできます。

注: 以下に示すインターフェース・ダイアログの例では、2210 特定のインターフェース・タイプは、Device Types のリストおよび Device Type のプロンプトに、トークンリングまたはイーサネットのいずれかとして示されています。

ブート・プロンプト (>) で **bm** と入力します。ソフトウェアは、次のルーター情報の入力を求めます。

Device Types available:

IBD
Token Ring/Ethernet
WAN

Device Type [Token Ring/Ethernet]: **IBD**

- **IBD** を入力すると、以下が表示されます。

```
IBD has load(s) load image name  
IBD Load Name: load image name
```

現行構成を再ロードする場合は、**Enter** を押します。別の構成をロードする場合は、プロンプトにロード名を入力します。

```
Loading using IBD Load Image "load name"
```

正しくないか、あるいは存在しないロード名を入力すると、システムは **No such load** というメッセージを出して、IBD Load Name のプロンプトに戻ります。

- **Token Ring** を入力すると、コンソールに次のような構成ダイアログが表示されません。

注: 指定されたホストにルーターが直接アクセスできない場合、ゲートウェイの IP アドレスを入力するよう指示されます。このプロンプトは、下の例では括弧で囲んで示されています。

```
Media (UTP/STP) [UTP]:  
Speed (4/16)Mb [16Mb]:  
Interface IP address: 123.175.56.119  
IP Mask (FFFFFF00):  
Boot from host: 123.175.68.213  
Via Gateway: 123.175.56.190  
Boot File Name: ibmMRNS.1dc
```

```
Using Token Ring at (6000000, 0).  
Interface configured for 16Mbps & UTP  
Trying host 123.175.68.213 via 123.175.56.190  
file ibmMRNS.1dc  
loading  
.....
```

```
Starting at 1040000
```

```
Copyright Notices:  
Copyright IBM Corp. 1994, 1997
```

MOS Operator Console

For help using the Command Line Interface, press ESCAPE, then '?'
*

- **Ethernet** を入力すると、以下が表示されます。

```
Connector Type (AUI/RJ45) [AUTO_CONFIG]:  
Interface IP Address: 123.175.56.119  
IP Mask (FFFFFF00):  
Boot from host: 123.175.68.213  
Via Gateway: 123.175.56.190  
Boot File Name: ibmMRNS.1dc
```

```
Using Ethernet at (6000000, 0)  
Trying host 123.175.68.213 via 123.175.56.190  
file ibmMRNS.1dc
```

```
.loading  
.....
```

```
Starting at 1040000
```

```
Copyright Notices:  
Copyright IBM Corp. 1994, 1997
```

MOS Operator Console

For help using the Command Line Interface, press ESCAPE, then '?'
*

- **WAN** を介したブート

指定された WAN ポート上にアクティブの CTS 信号が存在しない場合には、CTS not active on WAN port # というメッセージを受け取ります。

注: PPP プロトコルは、WAN インターフェースを介してブートするときに使用可能な、現在では唯一のデータ・リンク・レイヤー・プロトコルです。

BN (コンソール照会を使用したブート、実行禁止)

このブート・オプションは使用しないでください。このオプションはサービス技術員だけが使用します。

BP (BootP を使用したブート)

ブートストラップ・プロトコルを使用してブートします。以下の例は、2210 のブート方法を示しています。ユーザーの入力は太字体で示されています。大括弧内に示されているデフォルト値を受け入れる場合は、**Enter** を押します。

注: 以下のインターフェース・ダイアログの例では、装置のインターフェース・タイプは、Device Types リストおよび Device Type プロンプトには、トークンリングまたはイーサネットのいずれかとして示されています。

ブート・プロンプト (>) で **bp** と入力します。ソフトウェアは、次のルーター情報の入力を求めます。

Device Types available:

```
Token Ring/Ethernet  
Device type (for BOOTP) [Token Ring]:
```

- **Token Ring** と入力すると、以下が表示されます。

```
Media (UTP/STP) [UTP]:  
Speed (4/16)Mb [16Mb]:
```

```
BOOTP Using Token Ring at (6000000, 0).  
Doing BOOTP o  
Interface configured for 16Mbps & UTP  
Trying host 123.175.68.213 via 123.175.56.190  
file load image name  
.loading  
.....
```

```
Copyright Notices:  
Copyright IBM Corp. 1994, 1997
```

```
MOS Operator Control  
*
```

- **Ethernet** を入力すると、以下が表示されます。

```
Connector Type (AUI/RJ45)[AUTO_CONFIG]:
```

```
BootP Using Ethernet at (6000000, 0)  
Doing BootP o o o o  
Trying host 123.175.68.213 via 123.175.56.190  
file load image name  
.loading  
.....
```

```
Copyright Notices:  
Copyright IBM Corp. 1994, 1997
```

```
MOS Operator Control  
*
```

端末に OPCON (*) プロンプトが表示されれば、BOOTP ブートは成功したことになります。

BOOTP の失敗

BOOTP ブートが失敗するのは、サーバーがダウン状態の場合、サーバーが指定されたファイルを見つけられない場合、あるいは TFTP が失敗した場合です。BOOTP が失敗しすると、端末に次のメッセージが表示されます。

```
Manual BOOTP failed - enter "@" at prompt to BOOTP again.
```

@ を入力して、BOOTP を再試行してください。再試行も失敗した場合は、別の方法を使用して 2210 をブートします。

D (保管済み構成を使用したダンプ)

システム障害が発生すると、システム・メモリーの内容をファイルに書き込みます。固有命名が使用可能にされている場合、ルーターは自動的にダンプ・ファイル名に文字列を付加します。このコマンドを使用すると、既存のダンプ・ファイルが後続のダンプによって上書きされるのを防止することができます。固有命名を使用可能にする方法については、122 ページを参照してください。

ブート・プロンプト (>) で **d** と入力します。画面に次のような情報が表示されます。

PROM Load/Dump Program * Revision 1.0
Copyright IBM Corp. 1994, 1997
Host 325.321.62.763 loading

Using Token Ring/Ethernet (00000, 0)
Trying host 235.211.62.243 via 123.192.23.243
file load image name

Loading

Starting at 1040000

ダンプが失敗した場合、**Dump failed** (ダンプ失敗) というメッセージが、障害の原因の簡単な説明とともに表示されます。

DIAG (IBM 拡張診断プログラムの実行)

内部自己テストを開始します。内部自己テストが完了すると、提供された拡張診断ユーティリティを選択することができます。拡張診断テストを実行するためには、拡張診断サービス・キット (フィーチャー・コード 2532) が必要です。このキットには、LAN、シリアル、およびサービスの各ポートに必要なすべての折り返しプラグが入っています。

1. ブート・プロンプト (>) に **diag** と入力して、内部自己テストを実行します。画面に次のようなメッセージが表示されます。

Starting at 1FF00

Starting Hardware Diagnostics
Version: XXXXXX XXXXXX

Testing System Internal

System Checkout: All Systems Pass

Press space to continue.....

2. スペース・バーを押して、診断テストの次のレベルに入ります。これらのテストを実行するには、ネットワークからケーブルを取り外して、該当する折り返しプラグを接続することが必要です。折り返しプラグの取り付けは、拡張診断サービス・キットに入っている説明書に従ってください。

折り返しプラグを取り付けずに、これらのテストのいずれかを実行しようとする
と、次のメッセージが出ます。

You have selected a test that requires external wrap
plugs to be present. Remove the cable(s) from the
network, and attach the appropriate wrap plug(s).

3. スペース・バーを押して使用可能な診断オプションの 1 つを選択し、拡張診断サービス・キットに入っている説明書に下がってください。

Diagnostic Main Menu (c) 1994

- 1) System Checkout (Internal Tests)
- 2) System Extended Checkout (Internal and External Tests)
- 3) WAN/LAN Wrap Menu
- 4) Diagnostic Utilities

x) Exit (and Reboot)

DM (コンソール照会を使用したダンプ)

手動でネットワーク・ダンプ情報を構成するためのプロンプトを表示します。

ブート・プロンプト (>) で **dm** と入力します。

画面に次のような情報が表示されます。

```
PROM Load/Dump Program * Revision 1.0
Copyright IBM Corp. 1994, 1997
Host ??? loading
```

```
Using Token Ring/Ethernet (00000, 0)
Trying host 0.0.0.0 via 0.0.0.0
  file load image name
```

```
loading
```

```
Starting at 1040000
```

ダンプが失敗した場合、**Dump failed** (ダンプ失敗) というメッセージが、障害の原因の簡単な説明とともに表示されます。

UB (TFTP ブート構成の表示)

以下の情報を含む、静的 RAM の TFTP ブートストラップ構成を表示します。

- ホスト名
- ダンプが使用可能か使用不可か
- 固有命名が使用可能か使用不可か
- インターフェース IP アドレス、インターフェースのタイプ、およびマスク
- ブート・ファイル名
- ホストの IP アドレス
- ゲートウェイの IP アドレス

ダンプ・ファイルが作成されている場合、UB はダンプ・ファイル名とダンプ・ファイルが存在するホストの IP アドレス、および中間ゲートウェイの IP アドレス (該当する場合) も表示します。

この情報を表示するには、ブート・プロンプト (>) の後に **ub** と入力します。画面に次の例と同様の情報が表示されます。

```
TFTP bootstrap configuration:
  Host ibmMRNSV1 - .191, Dumping disabled, Unique dump naming off
Interface Addresses:
  1: 128.196.145.191 on port 0 (Token Ring/Ethernet), mask FFFFF00
Boot Files
  1: ibmMRNS.ldc on 123.175.68.213 via 123.175.56.190 for 20 secs
  2: r15.1.ldc on 123.175.68.213 via 123.175.56.190 for 20 secs
  3: ibmMRNS-univ.ldc on 123.175.68.213 via 123.175.56.190 for 20 secs
Dump Files:
  1: "gw/ibmMRNS.dmp" on 123.175.68.213 via 123.175.56.190 for 20 secs
>
```

UC (ハードウェア構成の表示)

次の情報を表示します。

- 使用可能な装置タイプ

- コンソールのボー・レート
- 主メモリーと IBD のサイズ (MB 単位)
- 基本 MAC アドレス
- ルーターの製造番号
- システム・カードの製造番号
- モデム番号
- システム・カードの部品番号
- システム・カードの改訂 (ECO) レベル
- プラットフォームの改訂

注: 各 2210 は、イーサネットの配列の基本 MAC アドレスを使用して、工場プログラムされています。トークンリング装置を使用している場合、2210 はアドレスをトークンリングの配列に変換しますが、**uc** コマンドは、アドレスをイーサネット配列で表示します。

ブート・プロンプト (>) で **uc** と入力します。画面に以下のような情報が表示されます。

```

Boot device types available:
    IBD
    Token Ring
    WAN

Console Baud Rate:      9600 (Autobaud)
Main Memory size:      8 MB
IBD (flash Memory) size: 4 MB
Base MAC Address:      000093808068
System Part Number     04H7063
System Serial Number   55554000008
System EC Level        D50514
System Card Part Number 13H7771
System Card Serial Number 110653
System EC Level        C99200B

```

UG (RAM 内アドレスでの実行)

このオプションはサービス技術員だけが使用します。

LC (構成メモリーのロード)

ネットワークに接続するホストから構成メモリーをロードします。このオプションを使用する場合は、以下を実行します。

ブート・プロンプト (>) で **lc** と入力します。画面に以下のような情報が表示されません。

```

Device Types available:

    IBD
    Token Ring/Ethernet
    WAN

Device type [Token Ring]:

```

- **Token Ring** を入力すると、次のように表示されます。

```

Media (UTP/STP) [UTP]:
Speed (4/16)Mb [16Mb]:
Interface IP address: 123.175.56.119

```

```
IP Mask (FFFFFF00):
Load Cfg from host: 123.175.68.213
Via gateway: 123.175.56.190
Config File Name: ibmMRNS.cfg
```

```
Using Token Ring at (6000000, 0).
Trying host 123.175.68.213 via 123.175.56.190
file ibmMRNS.cfg
```

```
.loading
Receiving config memory image
.....
```

```
Starting at 1040000
```

```
Copyright Notices:
Copyright IBM Corp. 1994, 1997
```

```
MOS Operator Control
*
```

- **Ethernet** を入力すると、次のように表示されます。

```
Connector Type (AUI/RJ45)[AUTO_CONFIG]:
Interface IP address: 123.175.56.119
IP mask (FFFFFF00):
Load Cfg from host: 123.175.68.219
Via gateway: 123.175.56.190
Config file name: ibmMRNS.cfg
```

```
Using Ethernet at (6000000, 0).
Trying host 123.175.68.219 via 123.175.56.190
file ibmMRNS.cfg
```

```
.loading
Receiving config memory image
.....
```

```
Starting at 1040000
```

```
Copyright Notices:
Copyright IBM Corp. 1994, 1997
```

```
MOS Operator Control
*
```

- **WAN** を入力すると、次のように表示されます。

```
WAN port [2]:
Timeout (secs) [20] ?
Clock Source (INT/EXT) [INT]:
Internal Clock Speed 1
Interface IP address: 123.175.56.119
IP mask [FFFFFF00]:
Load Cfg from host: 123.175.68.219
Via gateway: 123.175.56.190
Config file name: ibmMRNS.cfg
```

```
Using Serial Line at ( 0, 0).
Trying host 123.175.68.219 via 123.175.56.190
file ibmMRNS.cfg
```

```
.loading
Receiving config memory image
.....
```

```
Starting at 1040000
```

```
Copyright Notices:
```

CC (構成メモリーの消去)

重要: このコマンドを出すと、すべての構成情報が失われます。

このコマンドはメモリー内の構成を消去します。ブート・プロンプト (>) で **cc** と入力します。ソフトウェアは、次のような消去の確認を求めるプロンプトを出します。

Are you sure you want to clear config memory?

ZB (ZModem ブート)

コンソール・ポートを介して、ルーター・コードをダウンロードおよびアップロードします。

1. ブート・プロンプト (>) で **ZB** と入力すると、コンソールに次のような表示が出ます。

Are you sure you want to load via the console?

2. **y** を入力すると、コンソールに次のメッセージが表示されます。

Okay, GO!!

3. **Return** を押すと、操作が開始されます。システム・プロンプト (>) が画面に表示されれば、操作は完了です。

注: コンソール端末で使用する ZModem コマンドについては、ZModem ソフトウェアに付属の資料を参照してください。

ZC (ZModem 構成メモリーのロード)

コンソール・ポートを通して構成メモリーをロードします。

注: このオプションを使用するためには、リモート・ブート・サーバーが ZModem ソフトウェアをサポートしていることが必要です。

1. ブート・プロンプト (>) で **ZC** と入力します。コンソールに次のようなプロンプトが表示されます。

Are you sure you want to load config memory via the console?

2. **y** を押します。コンソールに次のようなメッセージが表示されます。

Okay, GO!!

3. **Return** を押すと、操作が開始されます。ブート・プロンプトが画面に表示されれば、この操作は完了です。

4. **n** を入力して、OPCON プロンプトに戻ります。

注: コンソール端末で使用する ZModem コマンドについては、ZModem ソフトウェアに付属の資料を参照してください。

2210 の構成

2210 のブート後、これを構成することができます。以下では、**ASCII 端末**を使用している場合に利用できる構成プロセスを簡単に説明します。

注: IBM Nways マルチプロトコル・ルーティング・サービス構成プログラム (構成プログラム) を使用して 2210 を構成することもできます。構成プログラムは、**スタンドアロン・ワークステーション**で実行し、**グラフィカル・ユーザー・インターフェイス**を備えています。事前構成またはクイック構成を行っておけば、構成プログラムを使用して 2210 を完全に構成することができます。

構成プロセスを開始するには、以下の手順で行います。

1. * プロンプトで **status** と入力すると、構成 (Config) の PID (プロセス ID) が表示されます。

Pid	Name	Status	TTY	Comments
1	COpCN1	RDY	TTY0	
2	Monitr	DET	--	
3	Tasker	RDY	--	
4	MOSDDT	DET	--	
5	CGWCon	DET	--	
6	Config	DET	--	
7	ROpCN1	IDL	TTY1	128.185.133.2
8	ROpCN2	RDY	TTY2	128.185.134.50

2. **talk** と PID を入力します。ステップ 1 の出力から、次のように入力します。

```
* talk 6
```

Return を押すと、次のような情報が表示されます。

```
Gateway user configuration
Config>
```

3. これで、以下のプロセスの 1 つを使用して、インターフェイス、ブート・レコード、ブリッジング、およびルーティング・プロトコルを構成することができます。

- **クイック構成プロセス**を使用すると、クイック構成プロンプトに応答しながら、選択された装置、ブリッジング・プロトコル、およびルーティング・プロトコルを構成することができます。最小構成を作成した後、TFTP を使用して完全な構成を 2210 に転送する必要があります。

Config> プロンプトで **qc** と入力して、クイック構成プロセスを開始します。

- **CONFIG プロセス**を使用すると、Config> プロンプトでコマンドを入力することにより、すべてのブリッジングおよびルーティング・プロトコル、インターフェイス、およびブート・レコードを構成することができます。

CONFIG プロセスを使用してプロトコルを構成する場合は、**プロトコルの構成と監視 解説書**の該当するプロトコルの章を参照してください。また、インターフェイスやブート・レコードを含めたその他のパラメーターの構成については、この資料の該当する構成の章を参照してください。

第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド

この章では GWCON プロセスについて説明し、以下の節が含まれています。

- 『GWCON とは』
- 『GWCON の出入り』
- 150ページの『GWCON コマンド』

GWCON とは

ゲートウェイ・コンソール (監視) プロセス GWCON (CGWCON とも言います) は、装置ユーザー・インターフェースの第 2 レベルのプロセスです。

GWCON コマンドを使用して、次のことが行えます。

- 装置に現在構成されているプロトコルおよびインターフェースをリストする。
- メモリーおよびネットワークの統計を表示する。
- 現行のイベント・ログ・システム (ELS) パラメーターを設定する。
- 指定されたネットワーク・インターフェースをテストする。
- 第 3 レベルのプロセス (プロトコル環境を含む) と通信する。
- インターフェースを使用可能および使用不可にする。

GWCON コマンド・インターフェースは、いくつかのレベル (モードと呼ばれる) で構成されています。各モードには、それぞれ独自のプロンプトがあります。たとえば、SNMP プロトコルのプロンプトは `SNMP>` です。

自分が通信しているプロセスおよびモードを知りたい場合は、**enter** キーを押すと、プロンプトが表示されます。この章で説明する一部のコマンド (**network** や **protocol** など) では、GWCON の種々のレベルにアクセスすることができます。

GWCON の出入り

OPCON (*) から GWCON に入るには、以下の方法のいずれかを選択します。

1. OPCON **console** コマンドを次のように入力する。
* **console**
2. OPCON プロンプトで **status** コマンドを入力して、GWCON の PID を見つける。
(**status** コマンドの出力例は、11 ページを参照してください。)

* **status**

次に、**talk** コマンドに続けて GWCON の PID 番号を次のように入力する。

* **talk 5**

コンソールに GWCON プロンプト (+) が表示されます。このプロンプトが表示されない場合は、**enter** を押します。ここで GWCON コマンドを入力することができます。

OPCON に戻るには、OPCON インターセプト文字を入力します。
(デフォルトは **Ctrl-P** です。)

GWCON コマンド

この節には GWCON コマンドを記載します。各コマンドごとに、説明、構文の要件、および例を示します。GWCON コマンドの要約を表16 に示します。

GWCON コマンドを使用するには、**talk 5** と入力して GWCON プロセスにアクセスし、(+) プロンプトで GWCON コマンドを入力します。

表 16. GWCON コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Activate	新たに構成された予備インターフェースを使用可能にします。
Buffer	各インターフェースに割り当てられたパケット・バッファに関する情報を表示します。
Clear	ネットワーク統計を消去します。
Configuration	現行のプロトコルおよびインターフェースの状態をリストします。
Disable	指定されたインターフェースまたはスロットをオフラインにします。
Enable	すべてのインターフェースを使用可能にします。
Error	誤りの件数を表示します。
Event	イベント・ログ・システム環境に入ります。
Feature	通常のプロトコルおよびネットワーク・インターフェースのコンソール・プロセスの外部の、独立した装置フィーチャーのコンソール・コマンドへのアクセスを提供します。
Interface	ネットワークのハードウェア統計または指定されたインターフェースの統計を表示します。
Memory	メモリー、バッファ、およびパケット・データを表示します。
Network	指定されたネットワークのコンソール環境に入ります。
Performance	基本プロセッサの使用状況の統計のスナップショットを提供します。
Protocol	指定されたプロトコルのコマンド環境に入ります。
Queue	指定されたインターフェースのバッファ統計を表示します。
Reset	指定されたインターフェースを使用不可にした後で、新しいインターフェース、プロトコル、およびフィーチャー構成パラメーターを使用して、再びインターフェースを使用可能にします。
Statistics	指定されたインターフェースの統計を表示します。
Test	使用不可にされているインターフェースを使用可能にするか、または指定されたインターフェースをテストします。
Uptime	装置の時間に関する統計を表示します。

Activate

activate コマンドは、この装置上の予備インターフェースを使用可能にするのに使用します。詳細については、50ページの『予備インターフェースの構成』を参照してください。

構文:

activate *interface#*

Buffer

buffer コマンドは、各インターフェースまたは一定範囲のインターフェースに割り当てられたパケット・バッファに関する情報を表示するのに使用します。

注: 1 つの装置上の各バッファは同じサイズで、動的に作成されます。バッファのサイズは装置によって異なります。

1 つのインターフェースだけの情報を表示する場合は、そのインターフェースまたはネットワークの番号を、コマンドの一部として入力します。インターフェース番号を入手するには、GWCON **configuration** コマンドを使用します。

構文:

buffer *[network# or range_of_network#]*

複数のインターフェースに関する情報を表示するには、*range_of_network#* (または、*network#* と *range_of_network#* の組み合わせ) を指定します。たとえば、**buffer 0 3 25-50** と指定すると、ネット 0、3、および 25 ~ 50 の情報が表示されます。

例:

buffer

Nt	Interface	Input Buffers:				Buffer sizes:					
		Req	Alloc	Low	Curr	Hdr	Wrap	Data	Trail	Total	Bytes Alloc
0	TKR/0	20	20	7	0	109	92	2052	7	2260	45200
1	PPP/0	20	20	7	20	109	92	2052	7	2260	45200
2	PPP/1	10	10	4	0	108	92	2048	0	2248	22480

Nt ソフトウェアに対応するネットワーク・インターフェース番号

Interface

インターフェースのタイプ

Input Buffers:

Req 要求された受信バッファの数。これは、装置の受信バッファのデフォルト数または CONFIG (Talk 6) **set receive-buffers** コマンドを使って設定された有効な値のいずれかです。

注:

1. インターフェースについてこの欄が 0 の場合は、これは受信バッファが割り振られていないバーチャル・インターフェースです。この場合、バーチャル・インターフェースはそれがマップされている装置の受信バッファを使用します。たとえば、ダイヤル回線インターフェースは、その基本ネットまたはインターフェースの受信バッファを使用します。
2. CONFIG **set receive-buffers** コマンドで装置によってサポートされていない値を指定する場合は、要求されたバッファの数は装置の受信バッファのデフォルト数に等しくなります。

Alloc 割り振られた受信バッファの数

注: 要求された数のバッファを割り振るのに十分なメモリがない場合、割り振られた受信バッファの数は、要求された受信バッファの数より小さくなります。

Low 受信バッファについての装置の低いしきい値。インターフェース用の受信

GWCON コマンド

(入力) バッファの現行の値が、インターフェースの低いしきい値より小さい場合、パケットはフロー制御 (除去) に適格です。フロー制御の詳細については、GWCON (Talk 5) **queue** コマンドの説明を参照してください。低いしきい値は、CONFIG (Talk 6) **set input-low-water** コマンドを使用して構成可能です。

Curr この装置の現行のバッファ数。装置が使用不可にされている場合は、この値は 0 になります。パケットを受信したときに、*Curr* の値が *Low* より下である場合、そのパケットはフロー制御可能です。(条件については、**queue** を参照してください。)

Buffer Sizes:

Hdr 最大ハードウェア、MAC、およびデータ・リンク・ヘッダー数の合計

Wrap プロトコル折り返しのために MAC、LLC、またはネットワーク・レイヤー・ヘッダーに与えられる許容範囲

Data 最大データ・リンク・レイヤー・パケット・サイズ

Trail 最大 MAC およびハードウェア・トレーラー数の合計

Total 各パケット・バッファの合計サイズ

Bytes Alloc

この装置のバッファ・メモリーの量。この値は、 $Alloc \times Total$ の乗算値によって決まります。

Clear

clear コマンドは、装置のネットワーク・インターフェースの 1 つまたはすべてに関する統計情報を削除するのに使用します。このコマンドは、大容量カウンター内の変更を追跡するのに便利です。このコマンドを使用しても、スペースの節約や装置の高速化にはつながりません。

インターフェース (または、ネットワーク) 番号を、コマンドの一部として入力します。インターフェース番号を入手するには、GWCON **configuration** コマンドを使用します。

構文:

clear *interface#* or *range_of_interface#*

複数のインターフェースに関する情報を消去するには、*range_of_network#* (または *interface#* と *range_of_interface#* の組み合わせ) を指定します。たとえば、**clear 0 3 25-50** と指定すると、ネット 0、3、および 25 ~ 50 の情報が消去されます。

Configuration

configuration コマンドは、プロトコルまたはネットワーク・インターフェースに関する情報を表示するのに使用します。出力は 3 つのセクションに分けて表示されます。最初のセクションには、装置の識別、ソフトウェア・バージョン、ブート ROM

バージョン、および自動ブート・スイッチの状態がリストされます。2番目と3番目のセクションには、プロトコルおよびインターフェースの情報がリストされません。

構文:

configuration

複数のインターフェースに関する情報を表示するには、`range_of_network#` (または、`network#` と `range_of_network#` の組み合わせ) を指定します。たとえば、**configuration 0 3 25-50** と指定すると、ネット 0、3、および 25 ~ 50 の情報が表示されます。

例:

configuration

Multiprotocol Access Services

2216-MAS Feature 2822 V3.2 Mod 0 PTF 0 RPQ 0 MAS.EF9 cc4_2a

```

Num Name Protocol
0 IP DOD-IP
3 ARP Address Resolution
4 DN DNA Phase IV
6 VIN Banyan Vines
7 IPX NetWare IPX
10 BGP Border Gateway Protocol
11 SNMP Simple Network Management Protocol
12 OSPF Open SPF-Based Routing Protocol
22 AP2 AppleTalk Phase 2
23 ASRT Adaptive Source Routing Transparent Enhanced Bridge
26 DLS Data Link Switching
27 XTP X.25 Transport Protocol
28 APPN Advanced Peer-to-Peer Networking [HPR]
30 APPN Advanced Peer-to-Peer Networking [ISR]

```

```

Num Name Feature
2 MCF MAC Filtering

```

```

16 Networks:
Net Interface MAC/Data-Link Hardware State
0 TKR/0 Token-Ring/802.5 Token-Ring Up
1 TKR/1 Token-Ring/802.5 Token-Ring Up
2 TKR/2 Token-Ring/802.5 Token-Ring Up
3 TKR/3 Token-Ring/802.5 Token-Ring Up
4 Eth/0 Ethernet/IEEE 802.3 Ethernet Up
5 Eth/1 Ethernet/IEEE 802.3 Ethernet Up
6 Eth/2 Ethernet/IEEE 802.3 Ethernet Up
7 Eth/3 Ethernet/IEEE 802.3 Ethernet Up
8 Eth/4 Ethernet/IEEE 802.3 Ethernet Up
9 Eth/5 Ethernet/IEEE 802.3 Ethernet Up
10 FR/0 Frame Relay V.35/V.36 Up
11 X25/0 X.25 V.35/V.36 Up
12 PPP/0 Point to Point V.35/V.36 Up
13 PPP/1 Point to Point V.35/V.36 Up
14 PPP/2 Point to Point V.35/V.36 Up
15 PPP/3 Point to Point V.35/V.36 Up

```

- 最初の行は、プロダクト名を示しています。
- 2行目には、プログラム/プロダクト番号、フィーチャー番号、バージョン、リリース、PTF、および RPQ 情報がリストされます。
- 残りの行は、構成済みのプロトコルをリストし、その後に構成済みのフィーチャーをリストしています。

プロトコルに関する以下の情報が表示されます。

Num プロトコルに対応する番号

GWCON コマンド

Name プロトコルの簡略名

Protocol

プロトコルのフルネーム

フィーチャーに関する以下の情報が表示されます。

Num フィーチャーに対応する番号

Name フィーチャーの簡略名

Feature

フィーチャーのフルネーム

ネットワークに関する以下の情報が表示されます。

Net ソフトウェアがインターフェースに割り当てるネットワーク番号。ネットワークには 0 から始まる番号が付けられます。これらの番号は、CONFIG プロセスの項で説明したインターフェース番号に対応しています。

Interface

インターフェースの名前とこのタイプのインターフェースのインスタンス

MAC/Data Link

インターフェースに構成された MAC/データ・リンクのタイプ

Hardware

ハードウェア・タイプで表された特定の種類のインターフェース

State ネットワーク・インターフェースの現在の状態

Testing

インターフェースが自己テスト中であることを示します。自己テストが行われるのは、装置が最初にスタートしたとき、インターフェースで問題が検出されたとき、または **test command** が使用されたときです。(enable slot コマンドは、アダプター上のすべてのインターフェースの自己テストを開始するために使用することもできます。)

インターフェースが動作可能のときは、インターフェースは定期的に保守パケットを送り出すか、ポートまたは伝送路の物理的状态をチェックする(あるいは、その両方を行う)ことによって、インターフェースがまだ正常に機能していることを確認します。この保守で障害が生じた場合、インターフェースはダウンとして宣言され、5 秒後に自己テストを実行するようにスケジュールされています。自己テストに失敗した場合、インターフェースはダウン状態に変換され、次の自己テストまでの期間が、最大 2 分まで増やされます。自己テストが正常に行われた場合は、ネットワークはアップとして宣言されます。

Up インターフェースが動作可能であることを示します。

Down インターフェースが動作不能であり、自己テストに失敗したことを示します。ネットワークは定期的に **testing** 状態になり、インターフェースが再び動作可能になったかどうかを調べます。

Disabled

インターフェースが使用不可にされていることを示します。インターフェースは、次の方法で使用不可にすることができます。

- **CONFIG disable** コマンドを使用して、インターフェースを使用不可として構成する。装置を再初期化するたびに、インターフェースの初期状態は使用不可になります。使用可能にする処置を取るまでは、使用不可の状態のままです。
- **GWCON disable** コマンドを使用して、インターフェースを使用不可にする。この方法は一時的なもので、装置を再初期化すると、インターフェースは構成された状態 (使用可能または使用不可) に戻ります。
- ネットワーク・マネージャーが **SNMP** を使用してインターフェースを使用不可にする。この方法は一時的なもので、装置を再初期化すると、インターフェースは構成された状態 (使用可能または使用不可) に戻ります。

インターフェースが使用不可にされている場合、次の方法の 1 つを使用して使用可能にするまでは、使用不可のままです。

- **GWCON test** コマンドを使用して、インターフェースの自己テストを開始する。
- **GWCON enable slot** コマンドを使用して、アダプター上のすべてのインターフェースで自己テストを開始する。
- ネットワーク・マネージャーが **SNMP** を使用して自己テストを開始する。

WAN 再ルートを使用して、使用不可にされたインターフェースの状態を変更することもできます。インターフェースが WAN 再ルートの代替インターフェースとして構成されており、構成された状態が使用不可である場合、WAN 再ルートは、1 次インターフェースがダウンするとインターフェースの自己テストを開始します。1 次インターフェースが再び動作可能になり安定すると、WAN 再ルートは代替インターフェースを構成された状態に戻します。詳細については、**フィーチャーの使用と構成** の **WAN 再ルート・フィーチャー** を参照してください。

Available

インターフェースは 2 次 WAN 復元インターフェースとして構成されており、1 次インターフェースのバックアップとして利用可能であることを示します。

Not Present

インターフェースのアダプターのプラグが差し込まれていないことを示します。

Not Present は、空の装置の状態を示すのにも使用されます。予備インターフェースは、起動されるまでは空の装置として表示されます。

HW Mismatch

構成されたアダプター・タイプが、実際にスロット内に存在するアダプターのタイプと一致していないことを示します。

GWCON コマンド

HW Failure

インターフェースのハードウェアについて回復不能なハードウェア・エラーがあることを示します。

Diagnostics

ハードウェア診断が実行中であることを示します。

Disable

disable コマンドは、ネットワーク・インターフェースまたはスロットをオフラインにし、そのインターフェースまたはスロットを利用不能にするのに使用します。このコマンドは、インターフェースまたはスロットを即時に使用不可にします。確認を求めるプロンプトは出ず、検証メッセージも表示されません。このコマンドを使ってインターフェースまたはスロットを使用不可にした場合、**GWCON test** コマンドまたは **OPCON reload** コマンドを使用してそれを使用可能にするまで、使用不可のままです。

インターフェースまたはネット番号またはスロットを、コマンドの一部として入力します。インターフェース番号またはスロット番号を入手するには、**GWCON configuration** コマンドを使用します。

注: 使用不可にしようとしているインターフェースが代替 WAN 再ルートとして構成されている場合、この代替インターフェースを含む WAN 再ルート 1 次/代替の組みを使用不可にするかどうかを尋ねられます。 *yes* と応答すると、インターフェースは使用不可にされ、1 次インターフェースのバックアップとして利用できなくなります。 *no* と応答すると、代替インターフェースは使用不可にされますが、対応する 1 次インターフェースがダウンした場合には、WAN 再ルートはこれの起動を試みます。代替インターフェースを使用不可にするときに、そのインターフェース上の WAN 再ルートを使用不可にして、アダプターを取り外せるようにしたい場合があります。追加情報については、 **フィーチャーの使用と構成の WAN 再ルート・フィーチャー**、WAN 復元の使用、および WAN 復元の構成と監視を参照してください。

構文:

```
disable                interface interface#  
                        slot slot#
```

Enable

Enable コマンドは、アダプターのすべてのインターフェースを使用可能にするのに使用します。これは **test** コマンド (165ページの『Test』を参照) と同じ動作をしますが、指定されたスロット内のアダプターを使用して、各インターフェースごとに処置を実行します。

構文:

```
enable                slot slot#
```

Error

error コマンドは、ネットワークの誤りの統計を表示するのに使用します。このコマンドは、誤りカウンターのグループを表示します。

構文:

error [network# or range_of_network#]

複数のインターフェースに関する情報を表示するには、range_of_network# (または、network# と range_of_network# の組み合わせ) を指定します。たとえば、**error 0 3 25-50** と指定すると、ネット 0、3、および 25 ~ 50 の情報が表示されます。

例:

error

Nt	Interface	Input Discards	Input Errors	Input Unk Proto	Input Flow Drop	Output Discards	Output Errors
0	TKR/0	0	0	0	0	0	0
1	PPP/0	0	0	0	0	0	0
2	PPP/1	0	0	0	0	0	0

Nt ソフトウェアに対応するネットワーク・インターフェース番号

Interface

インターフェースのタイプ

Input Discards

誤りは検出されなかったが、高位レイヤー・プロトコルに送達される可能性を防止するために廃棄された着信パケットの数。これらのパケットは、バッファ・スペースを空けるために廃棄された可能性もあります。

Input Errors

データ・リンクで欠陥が見つかったパケットの数

Input Unk Proto

確認不能のプロトコルの受信パケットの数

Input Flow Drop

出力時にフロー制御された受信パケットの数

Output Discards

装置がフロー制御のために転送せずに廃棄することを選択したパケットの数

Output Errors

ダウンしているネットワークや、転送中にダウンしたネットワーク上で送信を試みるといった出力誤りの数

注: 廃棄された出力パケットの合計は、すべてのネットワーク上の入力フロー除去数と同じではありません。廃棄された出力には、ローカルで発信されたパケットが含まれていることもあります。

Event

event コマンドは、イベント・ログ・システム (ELS) コンソール環境にアクセスするのに使用します。この環境は、トラブルシューティングのために一時的にメッセージ・フィルターを設定するのに使用されます。 ELS コンソール環境で行われたすべての変更は即時に有効になりますが、装置が再初期化されると無効になります。イ

GWCON コマンド

イベント・ログ・システムとそのコマンドについては、169ページの『第10章 イベント・ログ・システム (ELS) の使用』を参照してください。GWCON プロセスに戻るには **exit** コマンドを使用します。

構文:

event

Feature

feature コマンドは、プロトコルおよびネットワーク・インターフェースのコンソール・プロセスの外部の、特定 2210 フィーチャーのコンソール・コマンドにアクセスするのに使用します。

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には、**feature** コマンドの後に疑問符を入力します。

そのフィーチャーのコンソール・プロンプトにアクセスするには、GWCON プロンプトで **feature** コマンドを入力し、その後続けてフィーチャー番号または短縮名を入力します。80ページの表7 に、利用可能なフィーチャー番号と名前をリストしてあります。

フィーチャーのプロンプトにアクセスしたら、そのフィーチャーを監視するための特定のコマンドの入力を開始することができます。GWCON プロンプトに戻るには、フィーチャーのコンソール・プロンプトで **exit** コマンドを入力します。

構文:

feature *feature# or feature-short-name*

Interface

interface コマンドは、ネットワーク・インターフェース (たとえば、イーサネット) についての統計情報を表示するのに使用します。このコマンドは、修飾子を付けずに使用して、すべてのインターフェースの要約 (下記の出力に表示) を示したり、修飾子を付けて、1 つの特定インターフェースの詳しい情報を表示したりすることができます。

各タイプのインターフェースの詳細な出力についての説明は、本書の中の特定インターフェースの監視 の項に記載されています。インターフェース番号を入手するには、GWCON **configuration** コマンドを使用します。

構文:

interface *[interface# or range_of_interface#]*

複数のインターフェースに関する情報を表示するには、*range_of_network#* (または *interface#* と *range_of_interface#* の組み合わせ) を指定します。たとえば、**interface 0 3 25-50** と指定すると、ネット 0、3、および 25 ~ 50 の情報が表示されます。

例: **interface**

Nt	Nt'	Interface	Slot-Port	Self-Test Passed	Self-Test Failed	Maintenance Failed
0	0	TKR/0	Slot: 1 Port: 1	1	0	0
1	1	TKR/1	Slot: 1 Port: 2	2	1	0
2	2	TKR/2	Slot: 2 Port: 1	2	1	0
3	3	TKR/3	Slot: 2 Port: 2	2	1	0
4	4	Eth/0	Slot: 4 Port: 1	1	0	0
5	5	Eth/1	Slot: 4 Port: 2	1	0	0
6	6	Eth/2	Slot: 5 Port: 1	1	0	0
7	7	Eth/3	Slot: 5 Port: 2	3	2	2
8	8	Eth/4	Slot: 6 Port: 1	1	0	0
9	9	Eth/5	Slot: 6 Port: 2	5	4	1
10	10	FR/0	Slot: 8 Port: 0	2	1	0
11	11	X25/0	Slot: 8 Port: 1	1	0	0
12	12	PPP/0	Slot: 8 Port: 2	2	1	0
13	13	PPP/1	Slot: 8 Port: 3	1	0	0
14	14	PPP/2	Slot: 8 Port: 4	1	0	0
15	15	PPP/3	Slot: 8 Port: 5	1	0	0

注: 表示は装置に応じて異なります。

Nt グローバル・インターフェース番号

Nt' ダイヤル回線用に予約済み。ダイヤル回線が使用する物理ネットワーク・インターフェースのインターフェース番号

Interface

インターフェース名

Slot-Port

インターフェースのスロット番号とポート番号

Self-Test Passed

自己テストが正常に行われた回数 (インターフェースがダウンからアップに変わった状態)

Self-Test Failed

自己テストが正常に行われなかった回数 (インターフェースがアップからダウンに変わった状態)

Maintenance Failed

保守障害の数

Memory

memory コマンドは、現行の CPU メモリー使用量 (バイト)、バッファの数、およびバケット・サイズを表示するのに使用します。

このコマンドを使用するためには、空きメモリーが利用可能であることが必要です。空きバケット・バッファ数がゼロまで低下し、一部の着信バケットが失われる結果を招くことがあります。それによって装置の動作に悪影響を与えることはありません。装置のアイドル時には、空きバッファ数は一定に保たれていなければなりません。一定に保たれていない場合は、サービス技術員に連絡してください。

構文:

memory

例:

```
memory
Physical installed memory:      16 MB
Total routing (heap) memory:    12 MB
```

GWCON コマンド

Routing memory in use: 13 %

	Total	Reserve	Never Alloc	Perm Alloc	Temp Alloc	Prev Alloc
Heap memory	12231155	26488	10687312	1438487	104924	432

Number of global buffers: Total = 300, Free = 300, Fair = 77, Low = 60
Global buff size: Data = 2048, Hdr = 17, Wrap = 72, Trail = 65, Total = 2208

Physical installed memory

装置内に取り付けられた物理 RAM の合計量

Total routing memory

ルーティング機能に使用できるメモリーの量 (基本オペレーティング・システム、システム拡張、または APPN などのオプションに割り振られたメモリーの量を除く)。これは、“ヒープ” メモリーとも呼ばれ、その直後にバイト数で示される “合計の” ヒープ・メモリー・サイズに一致します。

Routing memory in use

ルーティング機能によって現在使用されている合計ルーティング・メモリーのパーセント。現在使用中のヒープ・メモリーは、次のヘッダーのもとでカウントされます。**Perm Alloc** および **Temp Alloc**。

Heap memory:

データ構造を動的に割り振るのに使用されたメモリーの量

Total メモリーの割り振りに使用できるスペースの合計量

Reserve

現在構成済みのプロトコルおよびフィーチャーが必要とするメモリーの最少量

Never Alloc

割り振られたことがないメモリー

Perm Alloc

装置タスクによって永続的に要求されているメモリー

Temp Alloc

装置タスクに一時的に割り振られるメモリー

Prev Alloc

一時的に割り振られ、返却されるメモリー

グローバル・バッファの数:

Total システム内のグローバル・バッファの合計数

Free 使用可能なグローバル・バッファの数

Fair 各インターフェースの妥当なバッファ数 (『Low』の項を参照)

Low バッファを保存するように割り振り方式が変更される基準となる空きバッファ数。Free の値が Low を下回った場合、Fair 値を上回るバッファ数が入っている待ち行列には、バッファは割り振られなくなります。

Global buff size:

グローバル・バッファ・サイズ

Data インターフェースの最大データ・リンク・パケット・サイズ

Header

最大ハードウェア、MAC、およびデータ・リンク・ヘッダー数の合計

Wrap プロトコル折り返しのために MAC、LLC、またはネットワーク・レイヤー・ヘッダーに認められる許容範囲

Trailer

最大 MAC およびハードウェア・トレーラー数の合計

Total 各パケット・バッファの全体サイズ

Network

network コマンドは、サポートされるネットワーク (X.25 ネットワークなど) のコンソール環境に入るのに使用します。このコマンドでは、指定されたインターフェースのコンソール・プロンプトが得られます。このプロンプトから、統計情報 (トークンリング・ネットワークのルーティング情報フィールドなど) を表示することができます。

構文:

network *interface#*

GWCON プロンプト (+) で **configuration** コマンドを入力すると、装置に構成されているプロトコルとネットワークを見ることができます。構成コマンドについての詳細は、152ページの『Configuration』を参照してください。

装置が構成されているネットワークを表示するには、+ プロンプトで **interface** と入力します。

GWCON **network** コマンドと監視または変更するインターフェースの番号を入力します。たとえば、次のように入力します。

```
+network 3
X.25>
```

この例では X.25> プロンプトが表示されます。X.25 動作コマンドを入力することにより X.25 インターフェースに関する情報を表示することができます。

監視するインターフェースのインターフェース番号を識別した後、インターフェース特有の情報が必要な場合は、本書の中の指定のネットワークまたはリンク・レイヤー・インターフェースの対応する監視の項を参照してください。以下のネットワークおよびリンク・レイヤー・インターフェースには、コンソール・サポートが提供されています。

- イーサネット
- フレーム・リレー
- PPP
- SDLC
- SDLC リレー (SRLY)
- トークンリング
- V.25bis
- X.25
- ATM
- ISDN
- ダイヤルイン
- マルチリンク PPP (MP)

GWCON コマンド

- レイヤー 2 トンネル伝送

Performance

性能に関する監視環境に入るには、GWCON プロンプトで **performance** コマンドを使用します。詳細については、247ページの『第12章 性能の構成および監視』を参照してください。

Protocol

protocol コマンドは、装置に導入されているネットワーク・プロトコルを実現している装置ソフトウェアと通信するのに使用します。プロトコルのコマンド環境にアクセスするには **protocol** コマンドを使用します。このコマンドを入力すると、指定したプロトコルのプロンプトが表示されます。このプロトコルから、そのプロトコルに特有のコマンドを入力することができます。

構文:

protocol *prot#*

プロトコルの番号または短縮名を、コマンドの一部として入力します。プロトコルの番号または短縮名を入力するには、**CONFIG** コマンド環境 (Config>) に入り、**list configuration** コマンドを入力します。Config> にアクセスする方法については、16ページの『構成プロセスへのアクセス、CONFIG (Talk 6)』を参照してください。GWCON に戻るには、**exit** と入力します。

特定のプロトコルのコンソール・コマンドについては、本書または **プロトコルの構成と監視 解説書** の該当する監視の項を参照してください。

Queue

queue コマンドは、指定したインターフェース上の入出力待ち行列の長さに関する統計を表示するのに使用します。queue コマンドによって提供される入出力待ち行列に関する情報には、以下のものが含まれます。

- 割り振られたバッファの合計数
- 最低水準バッファ値
- インターフェース上の現在アクティブのバッファの数

構文:

queue *interface#or range_of_interface#*

複数のインターフェースに関する情報を表示するには、*range_of_network#* (または *interface#* と *range_of_interface#* の組み合わせ) を指定します。たとえば、**queue 0 3 25-50** と指定すると、ネット 0、3、および 25 ~ 50 の情報が表示されます。

1つのインターフェースだけの情報を表示する場合は、そのインターフェースまたはネットワークの番号を、コマンドの一部として入力します。インターフェース番号を入力するには、GWCON **configuration** コマンドを使用します。

例:

queue		Input Queue			Output Queue	
Nt	Interface	Alloc	Low	Curr	Fair	Curr
0	Eth/0	30	10	30	30	1
1	PPP/0	24	4	24	4	0
2	FR/0	24	4	24	5	0

Nt ソフトウェアに対応するネットワーク・インターフェース番号

Interface

インターフェースのタイプ

Input Queue:

Alloc この装置に割り振られたバッファの数

Low 受信 (入力) バッファの低いしきい値は、この装置のフロー制御を活動化するのに使用します。低いしきい値は、CONFIG (Talk 6) **set input-low-water** コマンドを使用して構成可能です。

Curr この装置の現行のバッファ数。装置が使用不可にされている場合は、この値は 0 になります。

Output Queue:

Fair 入力装置についてフロー制御が活動化されときのインターフェースの出力待ち行列の高いしきい値。

注: PPP とフレーム・リレー・インターフェース用に帯域幅予約 (BRS) が構成されている場合、出力の fair 値は無視され、フロー制御によりパケットを廃棄する必要があるかどうか判断するのに、BRS を使って構成可能な待ち行列の長さが使用されます。

Curr この装置上で現在送信されるのを待っているパケットの数。適格性廃棄は **memory** コマンドで説明されているグローバル最低水準点によって異なります。

パケットが受信され、入力待ち行列の現行値が入力待ち行列の低いしきい値より小さい場合は、パケットがフロー制御の対象になります。ローカルで発信されるパケットについて、パケットがフロー制御の対象になるのは、空のグローバル・バッファの数がグローバル・バッファの低いしきい値より少ない場合です。フロー制御の対象となるパケットが、出力待ち行列の高いしきい値 (fair) より大きい出力待ち行列現行値をもつ装置に伝送される場合は、パケットが待ち行列に入れられずに、除去されます。パケットがフロー制御のため除去されると、出力廃棄カウンターが増分され、ELS イベント GW.036 または GW.057 がログに記録されます。パケットがローカルに発信されなかった場合、入力インターフェースについて入力フロー除去カウンターが増分されます。出力廃棄数と入力フロー除去カウンターが、GWCON **error** コマンドによって表示されます。

装置のスケジューリング・アルゴリズムが原因で、Curr (特に、Input Queue Curr) の動的な数が、パケット転送中の標準的な値を十分に表していないことがあります。コンソール・コードは、入力待ち行列が空になったときのみ実行されます。したがって、Input Queue Curr が非ゼロになるのは、通常、パケットが低速の送信待ち行列上で待っているときだけということになります。

Reset

reset コマンドは、指定したインターフェースを使用不可にした後で、新しいインターフェース、プロトコル、およびフィーチャー構成パラメーターを使用して、再びインターフェースを使用可能にするのに使用します。詳細については、54ページの『インターフェースのリセット』を参照してください。

構文:

```
reset                interface#
```

Statistics

statistics コマンドは、ネットワーク・ソフトウェアに関する統計情報 (装置内のネットワークの構成など) を表示するのに使用します。

構文:

```
statistics          interface#or range_of_interface#
```

複数のインターフェースに関する情報を表示するには、*range_of_network#* (または *interface#* と *range_of_interface#* の組み合わせ) を指定します。たとえば、**statistics 0 3 25-50** と指定すると、ネット 0、3、および 25 ~ 50 の情報が表示されます。

1 つのインターフェースだけの情報を表示する場合は、そのインターフェースまたはネットワークの番号を、コマンドの一部として入力します。インターフェース番号を入手するには、GWCON **configuration** コマンドを使用します。

例:

```
statistics
  Nt Interface  Unicast  Multicast  Bytes  Packets  Bytes
  0 Eth/0       Pkts Rcv   Pkts Rcv   Received  Trans   Trans
  0 Eth/0       137      1         8832    1068    65297
  1 PPP/0       0         0         0        0        0
  2 PPP/1       0         0         0        0        0
```

Nt ソフトウェアに対応するネットワーク・インターフェース番号

Interface

インターフェースのタイプ

Unicast Pkts Rcv

MAC レイヤーの非マルチキャスト、非ブロードキャストの、特別にアドレス指定されたパケットの数

Multicast Pkts Rcv

受信されたマルチキャストまたはブロードキャスト・パケットの数

Bytes Received

MAC レイヤーのこのインターフェースで受信されたバイト数

Packets Trans

送信されたユニキャスト、マルチキャスト、またはブロードキャスト・タイプのパケットの数

Bytes Trans

MAC レイヤーで送信されたバイト数

Test

test コマンドは、インターフェースの状態を検証するため、または以前に **disable** コマンドによって使用不可にされたインターフェースを使用可能にするために使用します。インターフェースが使用可能で、通信が行われている場合、**test** コマンドを使用すると、インターフェースはネットワークから除去され、インターフェース上で自己診断テストが実行されることとなります。

構文:

```
test interface#
```

注: このコマンドが機能するためには、コマンドの**完全な** 名前に続けて、インターフェース番号を入力する必要があります。

インターフェース番号またはネットワーク番号をコマンドの一部として入力します。インターフェース番号を入力するには、**GWCON configuration** コマンドを使用します。たとえば、テストが開始されると、コンソールに次のようなメッセージが表示されます。

```
Testing net 0 TKR/0...
```

テストが完了するか、失敗するか、あるいは **GWCON** がタイムアウトになると (30 秒後)、次のようなメッセージが表示される可能性があります。

```
Testing net 0 Eth/0 ...successful
Testing net 0 Eth/0 ...failed
Testing net 0 Eth/0 ...still testing
```

インターフェースによっては、テストが完了するまでに 30 秒以上かかる場合があります。

注: テストしているインターフェースが代替 WAN 再ルート・インターフェースとして構成されている場合、次のことを尋ねるプロンプトが出ます。

- 現在 WAN 再ルートの代替インターフェースが使用不可にされている場合、インターフェースの 1 次/代替の組みを使用可能にするかどうか。

yes と応答した場合は、フィーチャーの使用と構成 の WAN 復元の構成と監視で説明されている **t 5 enable alternate-circuit** WAN 再ルート・コマンドを入力した場合と同じ処置が取られます。

- インターフェースをテストしたいかどうか。

通常、WAN 再ルート・インターフェースは、対応する 1 次インターフェースをバックアップする必要が生じるまで、使用不可にされています。 *yes* と応答すると、インターフェースの自己テストが開始します。 *no* と応答すると、自己テストは行われません。

追加情報については、フィーチャーの使用と構成 の WAN 再ルート・フィーチャー、WAN 再ルート・フィーチャー、および WAN 復元の構成と監視を参照してください。

GWCON コマンド

Uptime

uptime コマンドは、装置の時間に関する統計を表示するのに使用します。以下のものが表示されます。

- リスタートの回数
- 認知されたクラッシュの数
- 前回は装置は再ロードされたのか、リスタートされたのか
- 前回の再ロードからの経過時間
- 前回のリスタートからの経過時間

構文:

uptime

第9章 メッセージ処理 (MONITR - Talk 2) プロセス

この章では、メッセージを収集および表示する方法について説明します。(ELS およびメッセージのフォーマットについての詳細は、169ページの『第10章 イベント・ログ・システム (ELS) の使用』を参照してください。) 各メッセージの説明は、*IBM Nways* イベント・ログ・システム・メッセージの手引きを参照してください。本章には、以下の節が含まれています。

- 『メッセージ処理 (MONITR) とは』
- 『メッセージ処理に影響を与えるコマンド』
- 『メッセージ処理 (MONITR) プロセスへの出入り』
- 168ページの『メッセージの受信』

メッセージ処理 (MONITR) とは

MONITR プロセスでは、装置およびネットワークの内部の活動を表示して見ることができます。MONITR は、ソフトウェアからのログに記録されたメッセージも表示します。

メッセージ処理に影響を与えるコマンド

以下のコマンドは、メッセージ処理プロセスに影響します。

- OPCON コマンド:
 - **divert** は、一時的に出力を別の装置に転送します。
 - **flush** は、ソフトウェアが収集したメッセージを廃棄させます。
 - **halt** は、divert コマンドの処置を取り消します。
 - **talk** は、メッセージ出力を表示します。
- **CONFIG set logging disposition** コマンドは、ソフトウェアがその出力を送信する最初の装置を設定します。

メッセージ処理 (MONITR) プロセスへの出入り

OPCON からメッセージ処理プロセスに入るには、**event** コマンドまたは **talk 2** コマンドを入力します。

ソフトウェアが収集したメッセージがコンソールに表示されます。

メッセージ処理を終了して OPCON に戻るには、OPCON インターセプト文字 (デフォルトは **Ctrl-P**) を入力します。

メッセージの受信

コンソールでメッセージを受信するには、前の節で説明したようにして、メッセージ処理プロセスに入ります。ソフトウェアは、前回に呼び出された以降に記録したすべてのメッセージを表示します。メッセージ処理プロセスに接続されている間、到着するすべてのメッセージが表示されます。

OPCON **divert** および **halt** コマンドを使用すれば、装置で何か別のことを行いながら、software メッセージを見ることができます。許可された装置は、出力を TTY0 (ローカル・コンソール)、TTY1、または TTY2 (リモート・コンソール) に着信転送します。

第10章 イベント・ログ・システム (ELS) の使用

この章では、イベント・ログ・システム (ELS) とその構成について説明します。ELS は、すべてのイベントを継続的にログに記録し、それらをユーザーが選択したパラメーターに従ってフィルター処理します。動作カウンターと ELS の組み合わせにより、システムの正常な動作と活動を監視するのに必要な情報が提供されます。この章は、以下の節に分けて説明します。

- 『ELS とは』
- 170ページの『ELS 構成環境への出入り』
- 170ページの『イベント・ログの概念』
- 174ページの『ELS の使用』
- 176ページの『ELS を使用してのトラブルシューティング』
- 177ページの『ELS リモート・ログ記録の使用および構成』
- 187ページの『ELS メッセージ・バッファの使用』

ELS とは

ELS は監視システムで、ルーター・オペレーティング・システムの一部です。ELS では、装置活動の結果としてログに記録されたメッセージを管理します。ELS コマンドを使用すれば、ユーザーにとって重要なメッセージだけをえり分けるように構成を設定できます。そのメッセージは、コンソール端末画面に表示したり、リモート・ワークステーションのログに記録したり、あるいはシンプル・ネットワーク管理プロトコル (SNMP) トラップを使用してネットワーク管理ステーションに送信したりすることができます。

ELS システムと動作カウンターは、装置に生じた問題を分離するための最良のトラブルシューティング・ツールです。イベント・メッセージにざっと目を通せば、装置に問題が生じているかどうかを知り、問題の解明をどこから始めればよいか分かります。

ELS 構成環境では、コマンドを使用してデフォルト構成を設定します。このデフォルト構成は、装置が初期化されるまでは有効になりません。

ときには、ELS 構成環境で設定したものの以外のパラメーターを使用してメッセージを一時的に表示して見ることが役に立ちますが、その場合は装置を再初期化する必要はありません。ELS 動作および監視環境は、以下の目的で使用します。

- デフォルトの ELS 表示設定値を一時的に変更する。
 - ELS コンソール環境で行った変更は、即時に有効になります。
 - コンソール・コマンドを使用して行った変更は、不揮発性構成記憶域には保管されません。
- ELS による動的 RAM の使用に関する統計情報を表示する。

注: 特定の ELS メッセージについては、*IBM Nways イベント・ログ・システム・メッセージの手引き* で説明しています。

ELS は、OPCON プロセスからアクセスするサブプロセスです。

ELS 構成環境への出入り

ELS 構成環境 (CONFIG プロセスからアクセス可能) は、ELS Config> プロンプトによって示されます。このプロンプトで入力されたコマンドは、ELS のデフォルト状態を作成します。これは装置のリスタート後に有効になります。これらのコマンドについては、この章の後半で詳しく説明します。

サブシステム、グループ、またはイベントをパラメーターとする構成コマンドは、次の順序で実行されます。

- サブシステム
- グループ
- イベント

基本 ELS 構成を設定するには、ELS Config> プロンプトで **display subsystem all standard** コマンドを入力します。このコマンドは、STANDARD ログ・レベル (つまり、すべての誤りと異常通知コメント) を持つすべてのサブシステムからのメッセージを表示するように、ELS を構成します。

注: 装置には、デフォルトの ELS 構成はありません。ユーザーが ELS 構成環境に入り、デフォルト状態を設定する必要があります。

OPCON から ELS 構成環境に入るには、次のようにします。

1. **configuration** コマンドを入力する。コンソールに CONFIG プロンプト (Config>) が表示されます。最初に CONFIG に入ったときにプロンプトが表示されない場合は、**enter** を押してください。
2. CONFIG プロンプトで、次のコマンドを入力して ELS にアクセスする。

```
Config> eve
```

コンソールに ELS 構成プロンプト (ELS config>) が表示されます。これで、ELS 構成コマンドを入力できます。

ELS 構成環境を終了するには、**exit** コマンドを入力します。

イベント・ログの概念

この節では、イベントをログに記録する方法およびメッセージの解釈方法について説明します。また、サブシステムの概念、イベント番号、およびログ・レベルについても説明します。大部分の ELS 機能は、サブシステム、イベント番号、およびログ・レベルをパラメーターとして受け入れるコマンドが基本になっています。

イベントの原因

イベントは、装置が動作している間、連続的に発生します。以下の理由のいずれも、その原因になります。

- システム活動
- 状態の変更

- サービス要求
- データの送受信
- データ誤りおよび内部誤り

イベントが発生すると、ELS はその発生源とイベントの性質を識別するデータを、システムから受け取ります。ELS は、受信したデータをその一部として使用してメッセージを生成します。

メッセージの解釈

この節では、ELS によって生成されるメッセージの解釈方法について説明します。図4 に、メッセージの内容を示します。

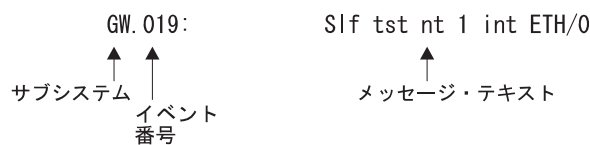


図4. イベントによって生成されるメッセージ

図4 に示されている情報、および **list subsystem** コマンドによって表示される ELS ログ・レベル情報について、以下で説明します。

サブシステム

サブシステム とは、装置のコンポーネント (プロトコルやインターフェースなど) を表す、事前定義された短縮名です。図4 では、**GW** がこのイベントを発生したサブシステムを識別しています。

その他のサブシステムの例としては、**IP**、**TKR**、および **X25** があります。特定の装置上に実際に存在するサブシステムは、その装置に構成されているハードウェアおよびソフトウェアによって異なります。この章で後述する **list subsystem** コマンドを使用すれば、装置上のサブシステムのリストを表示して見ることができます。

ELS コマンドの影響がサブシステム全体に及ぶようにしたい場合は、そのサブシステムをコマンドのパラメーターとして入力します。たとえば、ELS コマンド **display subsystem GW** は、GW サブシステム全体で発生するすべてのイベント ('debug' ログ・レベルのイベントを除く) を表示します。

イベント番号

イベント番号 は、サブシステム内の各メッセージに割り当てられる、事前定義された固有の任意の番号です。図4 では、**019** が GW サブシステム内のイベント番号です。**list subsystem** コマンドを使用すれば、サブシステム内のすべてのイベントのリストを表示することができます (ただし、*subsystem* はそのサブシステムの短縮名)。

イベント番号は、常にサブシステム識別子と共に表示され、サブシステム識別子との間をピリオドで区切られています。たとえば、**GW.019** のように表示されます。サブシステムとイベント番号の組み合わせで、個々の イベントを識別します。これら

は、ELS コマンドのパラメーターとして入力されます。コマンドの影響が指定のイベントだけに及ぶようにしたい場合は、サブシステムとイベント番号をその ELS コマンドのパラメーターとして入力します。

ログ・レベル

ログ・レベル は、各メッセージをその生成の原因となったイベントのタイプによって分類する、事前定義された設定値です。この設定値は、**list subsystem** ELS コンソール・コマンドを使用すると表示されます。表17 は、ログ・レベルとタイプをリストしています。ERROR、INFO、TRACE、STANDARD、および ALL は、他のログ・レベル・タイプを集合したものです。STANDARD が推奨されるデフォルト値です。

表 17. ログ・レベル

ログ・レベル	タイプ
UI ERROR	異常な内部エラー
CI ERROR	共通の内部エラー
UE ERROR	異常な外部エラー
CE ERROR	共通の外部エラー
ERROR	上記のすべてのエラー・レベルが含まれる
UINFO	異常な通知コメント
CINFO	共通の通知コメント
INFO	上記のすべてのコメント・レベルが含まれる
STANDARD	すべてのエラー・レベルとすべての通知コメント・レベルが含まれる (デフォルト)
PTRACE	パケット単位のトレース
UTRACE	異常な動作トレース・メッセージ
CTRACE	共通の動作トレース・メッセージ
TRACE	上記のすべてのトレース・レベルが含まれる
DEBUG	デバッグ用のメッセージ
ALL	すべてのログ・レベルが含まれる

ログ・レベルの設定値は、以下のコマンドの動作に影響を与えます。

- **Display subsystem**
- **Nodisplay subsystem**
- **Trap subsystem**
- **Notrap subsystem**
- **Remote subsystem**
- **Noremote subsystem**

ログ・レベルは、上記のコマンドの 1 つのパラメーターとして指定すると、その特定コマンドに対して設定されます。たとえば、次のように入力します。

display subsystem IP ERROR

このログ・レベルをコマンド行に含めると、**display** コマンドが変更されて、UI-ERROR または CI-ERROR のログ・レベルをもつイベントがサブシステム TKR で発生するたびに、その結果のメッセージがコンソールに表示されるようになります。

グループまたはイベントに影響を与える動作に対してログ・レベルを指定することはできません。

メッセージ・テキスト

メッセージ・テキスト は短縮形で表示されます。171ページの図4 で、`Slf tst nt 1 int Eth/0` は、このイベントによって生成されたメッセージです。変数 (`source_address` や `network` など) は、メッセージがコンソールに表示されるときに実際のデータで置き換えられます。

一部のイベント・ログ・システム・メッセージ記述では、変数 `error_code` が参照されます (通常は、その前に `rsn` (reason 理由) が付いています)。これらは、検出されたパケット誤りのタイプを示しています。表18 は、誤り符号、つまりパケット完了符号を記述しています。パケット完了コードは、装置によって受信されたパケットの後処理を示します。

表 18. パケット完了コード (エラー・コード)

コード	意味
0	パケットは出力のために正常に待ち行列に入れられました。
1	ランダム不特定エラー
2	パケットは、フロー制御が理由で、出力のために待ち行列に入れられませんでした。
3	パケットは、ネットワークのダウンにより、待ち行列に入れられませんでした。
4	パケットは、ループまたは不正なブロードキャストを避けるため、待ち行列に入れられませんでした。
5	パケットは、あて先ホストのダウンのため (これを検出できるネットワーク上のみ)、待ち行列に入れられませんでした。

ELS はネットワーク情報を、次のように表示します。

`nt 1 int Eth/0` (または) `network 1, interface Eth/0,`

ただし、

- 1 はネットワーク番号 (装置上の各ネットワークには、ゼロから順に番号が付けられています)
- 0 は、装置番号 (各ハードウェア・タイプのインターフェースには、ゼロから順に番号が付けられています)

イーサネットおよび 802.5 ハードウェア・アドレスは、長い 16 進数として表示されます。

IP (インターネット・プロトコル) アドレスは、ピリオドで区切られた 4 つの 10 進バイト (たとえば、18.123.0.16) として表示されます。

グループ

グループ は、名前が付けられた (グループ名) ユーザー定義のイベントの集合です。サブシステム、サブシステムとイベント番号、およびログ・レベルと同様に、グループ名も ELS コマンドのパラメーターとして使用することができます。ただし、事前定義されたグループ名はありません。グループを作成してからでないと、その名前をコマンド行で指定することができません。

ELS の使用

グループを作成するには、**add** 構成コマンドを使用し、グループの呼び名を指定し、次にそのグループに含めるイベントを指定します。グループに追加するイベントは、サブシステムおよびログ・レベルが異なっていても構いません。

グループを作成した後は、そのグループ名を使用して、グループ内のイベント全体をまとめて操作することができます。たとえば、`grouptwo` という名前のグループに追加されたイベントからのすべてのメッセージの表示をオフにするには、次のように、コマンド行にグループ名を含めます。

```
nodisplay group grouptwo
```

グループを削除するときは、**delete** コマンドを使用します。

ELS の使用

ELS を効果的に使用するには、以下を行います。

- ELS システムを使用する前に、何を必要とするか知っておく。MONITR プロセスを使用する前に、表示して見たい問題またはイベントを明確に定義しておきます。
- コマンド **nodisplay subsystem all all** を実行して、すべての ELS メッセージをオフにする。
- 直面している問題に関連したメッセージだけをオンにする。
- *IBM Nways* イベント・ログ・システム・メッセージの手引きを使用して、どのメッセージが正常でないか判別する。

MONITR プロセスから初めて ELS を表示したときは、かなりの量の情報が表示されます。中度から重度の負荷時には、装置はすべてのパケットをバッファリングして表示することはできないので、バッファリングはフラッシュされます。この状態が起これると、次のようなメッセージが表示されます。

```
xx messages flushed
```

装置は、これらのメッセージを保管しません。このメッセージが表示されたときは、監視している現行タスクにとって重要な情報だけを表示するように、ELS 出力を調整するか、拡張 ELS コマンドを使用して、メッセージ・バッファリングを設定します。187ページの『ELS メッセージ・バッファリングの使用』を参照してください。

ELS メッセージの回転の管理

ELS メッセージは装置のバッファリングを連続して回転していることに注意することも大切です。ELS メッセージの表示の停止およびリスタートには、以下のキーの組み合わせを使用します。

Ctrl-S スクロールを一時停止する場合

Ctrl-Q スクロールを再開する場合

Ctrl-P 直前のプロセスに戻る場合

ELS 出力をファイルに取り込むこともできます。これは、装置に Telnet 接続しているときに、自分の場所からスクリプト・ファイルまたはログ・ファイルを開始して行うことができます。あるいは、PC を装置のコンソール・ポートに接続し、端末エミ

ュレーション・パッケージ内からログ・ファイルを開始して行うこともできます。この情報は、カスタマー・サービスによる問題の診断に役立てるために必要です。

UNIX ホスト上の Telnet 接続を使用した ELS 出力の取り込み

AIX または UNIX ホスト上の Telnet 接続を使用して、画面上の ELS メッセージをホスト上のファイルに取り込むことができます。始める前に、189ページの『第11章 イベント・ログ・システム (ELS) の構成および監視』の ELS コンソール・コマンドを使用して、取り込みたいメッセージ用に ELS を設定します。

AIX または UNIX ホスト上のファイルに ELS 出力を取り込む場合は、以下のステップに従います。

1. ホストから、**telnet device_ip_addr | tee local_file_name** と入力する。
 - *device_ip_addr* は装置の IP アドレスです。
 - *local_file_name* は、ELS メッセージを保管したいホスト上のファイルの名前です。
 - **tee** コマンドは、ELS メッセージを画面に表示し、同時に、それをローカル・ファイルにコピーします。
2. OPCON プロンプト (*) から **t 2** と入力する。これにより MONITR プロセスにアクセスしますが、これが ELS メッセージを画面に表示するプロセスです。構成した ELS メッセージに応じて、画面に ELS メッセージが表示されるはずですが、MONITR プロセスにある限り、すべての ELS メッセージがローカル・ファイルに書き込まれます。MONITR プロセスを終了する (**Ctrl-P** を入力して) か、Telnet セッションを終了すると、ローカル・ファイルへのメッセージのログは停止します。

UNIX ホスト上で ELS 出力を取り込む代わりに、リモート・ログ記録を使用することもできます。リモート・ログ記録についての詳細は、177ページの『ELS リモート・ログ記録の使用および構成』を参照してください。

イベント・メッセージを SNMP トラップで送信できるように ELS を構成

イベント・メッセージが SNMP エンタープライズ特定トラップでネットワーク管理ワークステーションに送信できるように、ELS を構成することができます。これらのトラップは、状態や診断結果を報告するのに便利で、2210 のリモート監視にしばしば使用されます。ELS が適正に構成されていると、選択されたイベントが発生するたびに、SNMP トラップが生成されます。SNMP の詳細については、*プロトコルの構成と監視 解説書* を参照してください。

特定のイベントを SNMP トラップとして送信するために起動する必要があることを ELS に通知するには、ELS config> プロンプトまたは ELS> プロンプトで、たとえば IP を使用して、次のように入力します。

```
trap event ip.007
```

注: ELS config> プロンプトを使用する場合は、リポートする必要があります。

ELS エンタープライズ特定トラップを使用可能にするには、以下のステップに従います。

ELS の使用

1. SNMP config> プロンプトで、たとえば **public** を使用して、次のように入力する。

```
SNMP config> add address public <network manager IP address>
SNMP config> enable trap enterprise public
SNMP config> set community access read_trap public
```

注: これらの変更をアクティブするためには、リブートする必要があります。

2. ネットワーク管理ステーションがエンタープライズ特定トラップを受信し、正しく表示できるようにする。

これらのステップに従って、グループ、サブシステム、およびイベントをトラップします。

ELS を使用してのトラブルシューティング

特定の問題のトラブルシューティングを行う場合は、その問題に関連するメッセージを表示します。たとえば、ブリッジングの問題が起きている場合は、ブリッジング・メッセージをオンにします。

```
display subsystem srt all
```

```
display subsystem br all
```

画面上のメッセージのスクロールする速度が速いので、当初は、表示された番号をメモしておき、後でそれをイベント・ログ・システム・メッセージの手引きで調べても構いません。特定プロトコルについて表示される種々のタイプのメッセージに慣れてきたら、トラブルシューティングに必要な情報が含まれているメッセージだけをオン、オフにすることができるようになります。以下に、特定の ELS の例を示します。問題の種類によって必要なステップが異なることに注意してください。

ELS 例 1

トークンリング・インターフェース上のポーリングの頻度を調べ、ポーリングが正常に行われているかどうかを知りたい場合

```
ELS> nodisplay subsystem all all
ELS> display subsystem tkr all
Ctrl-P
* t 2
```

メッセージがスクロールし始めたら、ELS メッセージ tkr.031 を探します。

ELS 例 2

SRB ブリッジングが動作していない場合

1. 構成をチェックする。
2. GWCON ブリッジング・コンソールを使用して、ブリッジング・インターフェースが使用可能になっているかどうかを検査する。
3. 次のように入力する。

```
* t 6
config> event
ELS config> nodisplay subsystem all all
ELS config> display subsystem srb all
ELS config> exit
config> Ctrl-P
```

- ルーティング・サブシステムをリスタートする。サブシステムがリスタートしたら、次のように入力する。

```
* t 2
```

ELS 例 3

ルーターがイーサネット上の IPX と通信できない場合

- talk** コマンドと GWCON の PID を入力する。

```
* talk 5
```

コンソールに GWCON プロンプト (+) が表示されます。最初に GWCON に入ったときにこのプロンプトが表示されない場合は、**Return** を押してください。

- GWCON プロンプト (+) で **IPX** と入力し、IPX コンソール・プロンプト (IPX>) にアクセスする。
- IPX コンソール・プロンプトで **slist** コマンドを入力して、そのサーバーがリストされているかどうかを検査する。(slist コマンドについては、プロトコルの構成と監視 解説書 の IPX の監視に関する項を参照してください。)
- IPX 構成をチェックする。
- 次のように入力する。

```
* t 5
+ event
ELS> nodisplay subsystem all all
ELS> display subsystem IPX all
ELS> display subsystem eth all
ELS> Ctrl-P
* t 2
```

メッセージがスクロールし始めたら、ELS メッセージ eth.001 を探します。これは、サーバーのイーサネット・タイプ・フィールドが正しくないことを示します。

ELS リモート・ログ記録の使用および構成

リモート・ログに記録された ELS メッセージには、talk 2 の下で表示されるような、監視待ち行列にある ELS メッセージに含まれるすべての含まれ、図5 に示されるような追加情報も含まれます。

Date/Time	IP address assigned by the user	Sequence Number used for detecting missing messages	Local Name assigned by the user	ELS Subsystem Name, & Formatted message
Nov 20 12:13:47	5.1.1.1	Msg [0444] from	** IBM/2210 **	:els: MPC.011 Del ent ...

図5. Syslog メッセージ記述

リモート・ログ表示には、以下のような相違点があります。

- 時刻として、時間に加えて月と日が常に表示されます。
- IP アドレスは、ユーザー指定の発信元 IP アドレスです。DNS サーバーが発信元 IP アドレスをホスト名に変換した場合、そのホスト名が IP アドレスの代わりに表示されます。

ELS の使用

- 発信元の装置によってシーケンス番号がメッセージに付加されるので、廃棄されたメッセージを検出するのに役立ちます。廃棄メッセージについての説明は、182ページの『リモート・ログ記録の出力』を参照してください。メッセージのシーケンス番号が 9999 に達すると、その次のシーケンス番号は 0001 になります。
- 発信元装置の『ローカル名』は、複数のソースからのメッセージを区別するのに役立ちます。ローカル名を構成しなかった場合、このフィールドはブランクになります。

Syslog ファシリティとレベル

リモート・ログ ELS メッセージは、UDP パケットに入れてネットワーク上で転送されます。UDP ヘッダー内のあて先ポート番号は、常に 514 (syslog ポート) です。UDP パケットを受信して処理するためには、ELS メッセージを受信してログに記録するリモート・ワークステーションで *syslog* デーモン (syslogd) が実行されていることが必要です。詳細については、『リモート・ワークステーションの構成』を参照してください。

リモート・ログ ELS メッセージには表示されませんが、UDP パケットに入れてネットワーク上で送信される各 ELS メッセージには、*syslog_facility* と *syslog_level* を割り当てる必要があります。syslog デーモンは、ファシリティとレベルの組み合わせを使用して、メッセージの送信先を判別します。通常は、ELS メッセージはリモート・ホストの 1 つまたは複数のファイルに書き込まれます。その他のオプションとしては、メッセージをコンソールに表示する、メッセージを 1 人または複数のユーザーに送信する、あるいはメッセージを別のワークステーションに送信するといったことが可能です。

syslog_facility と *syslog_level* の値を指定するのに使用するコマンド、およびその他のリモート・ログ関連のコンソール・コマンドについては、213ページの『ELS 監視コマンド』および 189ページの『ELS 構成コマンド』で説明しています。次の節に進む前に、これらのコマンドについて理解しておいてください。

リモート・ワークステーションの構成

以下に示す構成では、単一の 2210 が単一のリモート・ワークステーションにリモート・ログ記録するものと想定しています。複数の 2210 が同一のリモート・ワークステーションにリモート・ログ記録するように構成することも可能です。ただし、ある特定の 2210 は 1 つだけのリモート・ワークステーションのログにしか記録できません。この例で使用しているオペレーティング・システムは AIX 4.2 です。ユーザーの環境とは、いくぶん異なっている可能性があります。syslog についての詳細は、ご使用のオペレーティング・システムの資料を参照してください。

AIX ワークステーションで構成を実行するためには、**ルート** としてログインする必要があります。ワークステーションの構成は、以下の手順で行います。

1. *syslog.conf* ファイルを作成または編集して、特定の *syslog_facility* 値と *syslog_level* 値をもつ ELS メッセージを書き込む場所を指定する。メッセージのあて先を指定する方法の例は、180ページの図6 の最下部を見てください。ログ・ファイルは、完全なパス名を指定する必要があることに注意してください。syslog 構成ファイルのデフォルトの場所は、*/etc/syslog.conf* です。

2. syslog.conf ファイルに指定した syslog メッセージをログ記録するためのファイルを作成する。
3. **syslogd** と入力して、syslog デーモンを開始する。SRC (システム・リソース・コントローラー) から syslog デーモンを開始するときは、**startsrc -s syslogd** と入力します。構成ファイルのパス名が /etc/syslog.conf ではないときは、**syslogd -f pathname** を入力します。デバッグ・モードで syslog デーモンを開始するときは、**syslogd -d** と入力します。

注: syslog デーモンの複数インスタンスを実行することは、サポートされません。

4. syslog.conf ファイルを作成または変更したときに、すでに syslog デーモンが実行されていた場合は、デーモンをリスタートして、syslog.conf からデーモンを再初期化する必要があります。
5. 次のように **logger** コマンドを使用して、設定を確認する。

```
logger -p user.alert THIS IS A TEST MESSAGE (user.alert)
logger -p news.info THIS IS A TEST MESSAGE (news.info)
```

設定が正しければ、syslog.conf で指定したファイルに THIS IS A TEST MESSAGE... が書き込まれます。

```
# @(#)34      1.9 src/bos/etc/syslog/syslog.conf, cmdnet, bos411, 9428A410j 6/13/93 14:52:39
#
# COMPONENT_NAME: (CMDNET) Network commands.
#
# FUNCTIONS:
#
# ORIGINS: 27
#
# (C) COPYRIGHT International Business Machines Corp. 1988, 1989
# All Rights Reserved
# Licensed Materials - Property of IBM
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
# /etc/syslog.conf - control output of syslogd
#
# Each line must consist of two parts:-
#
# 1) A selector to determine the message priorities to which the
#    line applies
# 2) An action.
#
# The two fields must be separated by one or more tabs or spaces.
#
# format:
#
# <msg_src_list>          <destination>
#
# where <msg_src_list> is a semicolon separated list of <facility>.<priority>
# where:
#
# <facility> is:
# * - all (except mark)
# kern,user,mail,daemon, auth, syslog, lpr, news, uucp, cron, authpriv, local0 - local7
#
# <priority or level> is one of (from high to low):
# emerg,alert,crit,err(or),warn(ing),notice,info,debug
# (meaning all messages of this priority or higher)
#
# <destination> is:
# /filename - log to this file
# username[,username2...] - write to user(s)
# @hostname - send to syslogd on this machine
# * - send to all logged in users
#
# example:
# "mail messages, at debug or higher, go to Log file. File must exist."
# "all facilities, at debug and higher, go to console"
# "all facilities, at crit or higher, go to all users"
# mail.debug          /usr/spool/mqueue/syslog
# *.debug             /dev/console
# *.crit              *
#
#   syslog messages with facility / priority values of LOG_USER,  LOG_ALERT
user.alert           /tmp/syslog_user_alert
#
#   syslog messages with facility / priority values of LOG_NEWS, LOG_INFO
news.info            /tmp/syslog_news_info
```

図6. *syslog.conf* 構成ファイル

リモート・ログ記録用の 2210 の構成

2210 を構成するには、次のように行います。

1. talk 6 で、181ページの図7 に示すように、リモート・ログ・ファシリティを構成する。 *source-ip-addr* として指定する IP アドレスは、リモート・ログ ELS メッセージに表示された IP アドレスまたはホスト名を識別しやすくするために、2210 に構成された IP アドレスを使用することが必要です。また、この IP アドレスは、ネーム・サーバーが速やかにホスト名に変換できること、あるいは少な

ELS の使用

くともネーム・サーバーが速やかに『address not found』を応答できるものであることを確認する必要があります。これを調べるには、ワークステーション上で次のような **host** コマンドを出します。

```
workstation> host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

応答に 1 秒以上かかる場合は、もっと迅速に解決できる IP アドレスを選択してください。

2. talk 6 で、182ページの図8 に示すように、リモート・ログ記録用のイベントおよびサブシステムを構成する。
3. 構成を書き込み、2210 を再ロードする。

```
ELS config>set remote source-ip-addr 5.1.1.1
Source IP Addr = 5.1.1.1

ELS config>set remote remote-ip-addr 192.9.200.1
Remote Log IP Addr = 192.9.200.1

ELS config>set remote local-id ** IBM/2210 **
Remote Log Local ID = ** IBM/2210 **

ELS config>set remote no-msgs-in-buffer 100
Number of messages in Remote Log Buffer must be 100-512
Number of Messages in Remote Buffer = 100

ELS config><B>set remote facility log_news
Default Syslog Facility = LOG_NEWS

ELS config>set remote level log_info
Default Syslog Level = LOG_INFO

ELS config>set remote on
Remote Logging is ON

ELS config>list remote

----- Remote Log Status -----

Remote Logging is ON
Source IP Address = 5.1.1.1
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_NEWS
Default Syslog Priority Level = LOG_INFO
Number of Messages in Remote Log = 100
Remote Logging Local ID = ** IBM / 2210 **
ELS config>
```

図7. リモート・ログ記録用の 2210 の構成

ELS の使用

```
ELS config>display sub snmp all
ELS config>remote sub snmp all log_news log_info

ELS config>display event srt.017
ELS config>remote event srt.017 log_news log_info

ELS config>display event stp.016
ELS config>remote event stp.016 log_user log_info

ELS config>display event stp.026
ELS config>remote event stp.026 log_news log_info

ELS config>display event stp.024
ELS config>remote event stp.024 log_news log_info

ELS config>display event ip.068
ELS config>remote event ip.068 log_news log_info

ELS config>display event ip.058
ELS config>remote event ip.058 log_news log_info

ELS config>display event ip.022
ELS config>remote event ip.022 log_news log_info

ELS config>display event gw.022
ELS config>remote event gw.22 log_news log_info

ELS config>display event arp.011
ELS config>remote event arp.011 log_user log_alert

ELS config>display event arp.002
ELS config>remote event arp.022 log_user log_alert

ELS config>list status
Subsystem:      SNMP
Disp levels:    ERROR INFO TRACE
Trap levels:    none
Trace levels:   none
Remote levels:  ERROR INFO TRACE
                Syslog Facility/Level: LOG_NEWS LOG_INFO

Event   Display Trap   Trace   Remote
SRT.017 On      Unset   Unset   On
                Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.016 On      Unset   Unset   On
                Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.026 On      Unset   Unset   On
                Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.024 On      Unset   Unset   On
                Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.068  On      Unset   Unset   On
                Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.058  On      Unset   Unset   On
                Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.022  On      Unset   Unset   On
                Syslog Facility/Level: LOG_NEWS LOG_INFO
GW.022  On      Unset   Unset   On
                Syslog Facility/Level: LOG_NEWS LOG_INFO
ARP.011 On      Unset   Unset   On
                Syslog Facility/Level: LOG_USER LOG_ALERT
ARP.002 On      Unset   Unset   On
                Syslog Facility/Level: LOG_USER LOG_ALERT
```

図8. リモート・ログ記録用のサブシステムおよびイベントの構成

リモート・ログ記録の出力

183ページの図9 は、/tmp/syslog_news_info ファイルからの出力の例を示しています。最初のメッセージはシーケンス番号 310 であることに注意してください。これは、最初の 309 ELS メッセージは、発信元の 2210 から送られなかったことを意味しています。これには、いくつかの理由があります。

- メッセージが最初に ELS に渡されたときに、リモート・ログ・ファシリティの初期化が完了していなかった。
- 発信元 2210 からリモート・ワークステーションへのルートが、ルーティング・テーブルになかった。
- ELS メッセージが入っている発信 UDP パケット用のインターフェースが『Up』状態でなかった。

1 では、メッセージ 311-313 がリモート・ログに記録されなかったことに注意してください。これは、ARP 要求がアウトスタンディングであったためであり、ARP レスポンスを受信するまでは、最初のパケットを除く発信元 2210 内のすべてのパケットが廃棄されます。また、ARP キャッシュは、ユーザーが構成したリフレッシュ速度で消去され、新規の ARP 要求が出されます。この状態が起きているかどうかを調べるために、対象となる ELS イベントに加えて、イベント ARP.002 と ARP.011 もリモート・ログに記録して見ることができます。184ページの図11 は、`syslog_user_alert` ファイルに記録された ARP イベントを示しています。ここにはイベント 445 と 446 が記録されており、これらは図9 には脱落として示されています。

```
Nov 20 12:03:16 worksta01 root: THIS IS A TEST MESSAGE (news.info)
Nov 20 12:08:48 5.1.1.1 Msg [0310] from ** IBM / 2210 **: els: IP.022: add nt 192.9.200.0 int 192.9.200.20
nt 0 int Eth/0
```

1 (messages 311, 312, and 313 did not get remote-logged due to ARP request outstanding - see explanation in the text)

2 (messages 314 and 315 were logged to a separate file - see explanation in the text)

```
Nov 20 12:08:48 5.1.1.1 Msg [0316] from ** IBM / 2210 **: els: IP.068: routing cache cleared
Nov 20 12:08:48 5.1.1.1 Msg [0317] from ** IBM / 2210 **: els: IP.022: add nt 5.0.0.0 int 5.1.1.1 nt 5 int Eth/4
Nov 20 12:08:48 5.1.1.1 Msg [0318] from ** IBM / 2210 **: els: SRT.017: Enabling SRT on port 5 nt 5 int Eth/4
```

(message 319 was logged to a separate file)

```
Nov 20 12:08:48 5.1.1.1 Msg [0320] from ** IBM / 2210 **: els: IP.068: routing cache cleared
```

(120 messages not shown)

```
Nov 20 12:13:33 5.1.1.1 Msg [0441] from ** IBM / 2210 **: els: GW.022: Nt fld slf tst nt 3 int Eth/3
Nov 20 12:13:33 5.1.1.1 Msg [0442] from ** IBM / 2210 **: els: GW.022: Nt fld slf tst nt 6 int Eth/5
Nov 20 12:13:38 5.1.1.1 Msg [0443] from ** IBM / 2210 **: els: GW.022: Nt fld slf tst nt 11 int ISDN/0
```

(messages 444 and 447 were logged to a separate file)

(messages 445 and 446 did not get remote-logged due to ARP request outstanding)

```
Nov 20 12:13:50 5.1.1.1 Msg [0448] from ** IBM / 2210 **: els: GW.022: Nt fld slf tst nt 4 int PPP/0
Nov 20 12:13:50 5.1.1.1 Msg [0449] from ** IBM / 2210 **: els: IP.068: routing cache cleared
Nov 20 12:13:50 5.1.1.1 Msg [0450] from ** IBM / 2210 **: els: IP.058: del nt 4.0.0.0 rt via 0.0.0.4 nt 4 int PPP/0
```

図9. Syslog News Info ファイルの内容の例

ブート中およびブート直後に生成される初期 ELS メッセージに特に関心がある場合は、これらのメッセージもモニター待ち行列に表示することをお勧めします。これは talk 2 で表示されます。184ページの図10 は、リモート・ログに記録されなかった初期メッセージが含まれている talk 2 出力を示しています。talk 2 出力には、リモート・ログ・ファシリティが使用可能であることを示すメッセージがあることに注意してください。これは、リモート・ワークステーションへのルートが存在することを示しているのでもなく、関連のインターフェースが『Up』状態にあることを示しているのでもありません。これは単に、それ以前はメッセージを正常にリモート・ログに記録できないことを示す参照点として示されています。

ELS の使用

また、talk 2 出力には、脱落していたメッセージ (183ページの図9 に **2** で示されている) も記録されていることに注意してください。

```
12:08:17 SNMP.024: generic trc (P2) at snmp_mg.c(766): Now 0 trap destinations
12:08:17 SNMP.012: comm public added
12:08:17 SNMP.012: comm public added
12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_device_if_info(): sr
rdrec failed

12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_device_if_info(): sr
rdrec failed

12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:28 GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:28 IP.022: add nt 4.0.0.0 int 4.1.1.1 nt 4 int PPP/0

    ( 297 messages not shown )

12:08:43 GW.022: Nt fld slf tst nt 12 int PPP/2
12:08:43 GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:48 IP.022: add nt 192.9.200.0 int 192.9.200.20 nt 0 int Eth/0
12:08:48 SRT.017: Enabling SRT on port 1 nt 0 int Eth/0
12:08:48 STP.016: Select as root TB-1, det topol chg
12:08:48 STP.026: Root TB-1, strt hello tmr
12:08:48 ARP.002: Pkt in 1 1 800 nt 0 int Eth/0
12:08:48 ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
12:08:48 IP.068: routing cache cleared

    ( 126 messages not shown )

12:13:38 GW.022: Nt fld slf tst nt 11 int ISDN/0
12:13:47 ARP.011: Del ent 1 3 nt 0 int Eth/0
12:13:47 ARP.011: Del ent 1 3 nt 0 int Eth/0
12:13:47 ARP.002: Pkt in 1 1 800 nt 5 int Eth/4
12:13:47 ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
12:13:50 GW.022: Nt fld slf tst nt 4 int PPP/0
```

*Corresponding Sequence
Numbers in
Remote-Logging Files :*

```
[0310] first message logged
-- not logged (ARP request) --
-- not logged (ARP request)--
-- not logged (ARP request)--
[0314]
[0315]
[0316]

[0443]
[0444]
-- not logged (ARP request) --
-- not logged (ARP request)--
[0447]
[0448]
```

図 10. Talk 2 からの出力

タイム・スタンプを使用して (これは、リモート・ログ出力ファイルと talk 2 出力の両方に表示されます)、最初の ELS メッセージが正常にリモート・ログに記録された時刻を調べることができます。この目的のためにタイム・スタンプを使用するには、ELS を構成して、モニター待ち行列内のタイム・スタンプが時刻を表示するようにします。

183ページの図9 では、メッセージ 311-313 がリモート・ログに記録されなかったことにも注意してください。これは ARP 要求がアウトスタンディングであったためであり、ARP レスポンスを受信するまでは、最初のパケットを除く発信元 IBM 2210 内のすべてのパケットが廃棄されます。ARP キャッシュは、ユーザーが構成したリフレッシュ速度で消去され、装置は新規の ARP 要求を出します。ARP 要求が出されているかどうかを調べるために、対象となる ELS イベントに加えて、イベント ARP.002 と ARP.011 もリモート・ログに記録して見ることができます。図11 は、`syslog_user_alert` ファイルに記録された ARP イベントを示しています。ここにはイベント 445 と 446 が記録されており、これらは 183ページの図9 には脱落として示されています。

```
Nov 20 12:02:53 worksta01 root: THIS IS A TEST MESSAGE (user.alert)
Nov 20 12:08:48 5.1.1.1 Msg [0314] from ** IBM / 2210 **: els: ARP.002: Pkt in 1 1 800 nt 0 int Eth/0
Nov 20 12:08:48 5.1.1.1 Msg [0315] from ** IBM / 2210 **: els: ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
Nov 20 12:08:48 5.1.1.1 Msg [0319] from ** IBM / 2210 **: els: ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
Nov 20 12:13:47 5.1.1.1 Msg [0444] from ** IBM / 2210 **: els: ARP.011: Del ent 1 3 nt 0 int Eth/0
Nov 20 12:13:47 5.1.1.1 Msg [0447] from ** IBM / 2210 **: els: ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
```

図 11. `syslog_user_alert` ファイルの内容の例

IP アドレスと MAC アドレスの間に静的な関係を設定しておくことによって、この ARP シーケンスが原因で生じる ELS メッセージの損失を防止することができます。基本的なステップを以下に示し、その例を 図12 に示します。

1. talk 5 で、リモート・ワークステーションの IP アドレスを『ping』する。
2. talk 5 で、メッセージをリモート・ワークステーションの IP アドレスに送信するのに使用するインターフェース (ネット) 番号を調べる。
3. 前のステップからのネット番号を使用して、対応する MAC アドレスを調べる。
4. talk 6 で、ARP 項目を追加して、IP アドレスと MAC アドレスの静的な関係を設定する。

```
*t 5
+p ip

IP>ping 192.9.200.1
PING 192.9.200.20 -> 192.9.200.1: 56 data bytes, ttl=64, every 1 sec.
56 data bytes from 192.9.200.1: icmp_seq=0. ttl=64. time=0. ms
----192.9.200.1 PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms

IP>dump

  Type  Dest net          Mask          Cost  Age      Next hop(s)
  .
  Dir*  192.9.200.0      FFFFFFF0     1      102305   Eth/0
  .
IP>exit
+int

Net  Net'  Interface  Slot-Port          Self-Test  Self-Test  Maintenance
0    0      Eth/0      Slot: 1  Port: 1          Passed     Failed     Failed
                                1          0              0
  .
+p arp
ARP>dump
Network number to dump [0]? 0
Hardware Address      IP Address      Refresh
02-60-8C-2D-69-5D   192.9.200.1    2

Ctrl-P
*t 6
config>p arp
ARP config>add entry
Interface Number [0]? 0
Protocol [IP]? IP
IP Address [0.0.0.0]? 192.9.200.1
Mac Address []? 02608C2D695D
ARP config> list entry

Mac address translation configuration

IF #      Prot #  Protocol -> Mac address
0         0      192.9.200.1 -> 02608C2D695D
ARP config>exit
Config>write

Ctrl-P

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

(after reload, static ARP entry is active)
```

図 12. 静的 ARP 項目の設定例

その他の考慮事項

IP アドレスを含む ELS メッセージ

リモート・ワークステーションの IP アドレスに一致する IP アドレスを含んでいる ELS メッセージは、たとえリモート・ログ記録用に構成されていても、リモート・ログには記録されず、talk 2 のもとで表示されます。このようなメッセージは、過度の UDP パケットがネットワーク上で送信されるのを防止するために、リモート・ログに記録されずに、廃棄されます。

重複ログ

`syslog.conf` 内でファシリティ値が繰り返されている場合、たとえば、

```
user.debug      /tmp/syslog_user_debug
user.alert      /tmp/syslog_user_alert
```

syslog デーモンは、`user.debug` メッセージは `/tmp/syslog_user_debug` ファイルにのみ記録し、一方の `user.alert` メッセージは `/tmp/syslog_user_debug` ファイルと `/tmp/syslog_user_alert` ファイルの両方に記録します。これは、重大な状態は複数の場所に記録するという syslog 設計に従うものです。

この重複ログ記録を防止するために、`syslog.conf` ファイルには、異なるファシリティ値を指定することをお勧めします。合計 19 のファシリティ値を使用できます。

Syslog 出力ファイル内の反復シーケンス番号

ネットワークの構成によっては、ELS メッセージが入った重複する UDP パケットが、リモート・ホストに到着する可能性があります。また、パケットが送信された順序とは異なる順序で到着する可能性もあります。この現象の例を 図13 に示します。シーケンス番号が 628 ~ 633 のメッセージが 2 度記録されていることに注意してください。また、最初のシーケンス番号 0630 の後に、シーケンス番号 0629 が再び記録され、その後に 2 度目の 0630 があることにも注目してください。

```
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
```

図 13. Syslog 出力内の反復シーケンス番号の例

Syslog と UDP はどちらも重複シーケンスまたはシーケンス誤りパケットを処理する能力を備えていないので、重複シーケンス番号が発生する可能性があることを認識しておくことが重要です。

ELS メッセージ・バッファの使用

メッセージ・バッファは、問題判別に役立つ ELS の拡張機能です。ELS がメッセージ・バッファに使用するデフォルトを設定したり、装置の稼働時にメッセージがどのようにバッファされるかを変更することができます。メッセージ・バッファは、メッセージがデフォルト・メッセージ・バッファで折り返されたために情報が失われるのを最小限に抑えることができます。メッセージ・バッファは、**advanced** 構成コマンドまたは監視コマンドを通じてアクセス可能です。これを使って、以下のことを行うことができます。

- バッファがアクティブであるかどうか指定する。
- メッセージ・バッファにどのイベントが書き込まれるか指定する。
- バッファを停止し、バッファに割り振られたメモリーを解放する。
- メッセージ・バッファの状態を表示する。
- メッセージ・バッファを停止するイベントを指定し、イベントが発生したときにシステムがどのような処置を取るかを指定する。
- バッファのフォーマットされたバージョンをリモート・サーバーにあるファイルに送信する。
- バッファ内の特定の数またはすべての ELS メッセージを表示する。
- ハード・ディスク がある場合は、バッファをハード・ディスク に書き込む。
- ハード・ディスク がある場合は、形式化された ELS メッセージ・バッファを含むファイルをハード・ディスク から読み取る。
- ハード・ディスク がある場合は、形式化された ELS メッセージ・バッファを含むファイルをハード・ディスク から送信する。

コマンドについて詳しくは、209ページの『ELS メッセージ・バッファ構成コマンド』および 241ページの『ELS メッセージ・バッファ監視コマンド』を参照してください。

次の例は、ELS メッセージ・バッファを構成する方法を示しています。

注: 拡張 ELS バッファ・サイズの設定は、talk 6 のもとで実行する必要があります。残りのセットアップ・ステップは、talk 5 または talk 6 のどちらのもとでも実行できます。

```
*t 6
Gateway user configuration
Config>event
Event Logging System user configuration
ELS config>advanced
Advanced ELS Config Console
ELS Config Advanced>set buffer
Enter buffer size of 0 or in range 5073 to 20294 KB [5073]?
Buffer size set to 5073 KB
NOTE: Any more config changes made before rebooting
could affect the availability of sufficient memory after
reboot!
ELS Config Advanced>exit
ELS config>exit
Config>write
Config>
*reload
Are you sure you want to reload the gateway? (Yes or [No]): Yes
```

(after reloading...)

```

*t 5

CGW Operator Console

+event
Event Logging System user console
ELS>advanced
Advanced ELS Console
ELS Advanced>list status
-----Advanced ELS Configuration-----
Logging Status: OFF Wrap Mode: ON Logging Buffer Size: 5073 KB
Stop-Event: NONE Stop-String: NONE
Additional Stop-Action: NONE
-----Run-Time Status-----
Has Stop Condition Occurred? NO Messages currently in buffer: 0

ELS Advanced>set stop event gw.26
Stop Event "GW.026" has been set
ELS Advanced>exit
ELS>list event gw.26
Level: C-TRACE
Message: Mnt nt %n int %s/%d
Active: Count: 742

ELS>advanced
Advanced ELS Console
ELS Advanced>set stop string Mnt nt 5
Stop String set to "Mnt nt 5"
ELS Advanced>set stop action SYSTEM-DUMP
Stop Action has been set to SYSTEM-DUMP
ELS Advanced>set wrap off
Advanced Wrap Mode set to OFF.

ELS Advanced>log subsys gw all
ELS Advanced>set logging on
Advanced Logging set to ON.
ELS Advanced>list status
-----Advanced ELS Configuration-----
Logging Status: OFF Wrap Mode: OFF Logging Buffer Size: 5073 KB
Stop-Event: GW.026 Stop-String: Mnt nt 5
Additional Stop-Action: SYSTEM-DUMP
-----Run-Time Status-----
Has Stop Condition Occurred? YES Messages currently in buffer: 7

ELS Advanced>view all noscroll

[1] 10:52:10 GW.026: Mnt nt 0 int Eth/0
[2] 10:52:10 GW.026: Mnt nt 5 int Eth/1 1
[3] 10:52:14 GW.026: Mnt nt 0 int Eth/0
[4] 10:52:14 GW.026: Mnt nt 5 int Eth/1
[5] 10:52:18 GW.026: Mnt nt 0 int Eth/0
[6] 10:52:18 GW.026: Mnt nt 5 int Eth/1
[7] 10:52:22 GW.026: Mnt nt 0 int Eth/0

Dump initiated by ELS Stop Action.

```

1 これは停止アクションを起動します。ログ記録が停止し、停止アクションが発生する前に、さらに 5 つのイベントがログ記録されることに注意してください。

注: 実際には、停止アクションが SYSTEM-DUMP である場合、ルーターは再ロードを試みているので、上記のように最終状況をリストすることはできず、バッファを表示することもできません。

第11章 イベント・ログ・システム (ELS) の構成および監視

この章では、ELS によってログに記録されるイベントの構成方法および ELS コマンドの使用法について説明します。この章には、以下の節が含まれています。

- 『ELS 構成環境へのアクセス』
- 『ELS 構成コマンド』
- 213ページの『ELS 動作環境への出入り』
- 213ページの『ELS 監視コマンド』

イベント・ログ・システムについての詳細、および ELS イベント・メッセージの解釈の仕方については、169ページの『第10章 イベント・ログ・システム (ELS) の使用』を参照してください。

ELS 構成環境へのアクセス

ELS 構成環境は、ELS config> プロンプトによって示されます。このプロンプトで入力できるコマンドについては、『第11章 イベント・ログ・システム (ELS) の構成および監視』で説明しています。

ELS 構成環境に入るには、次のようにします。

1. **configuration** と入力する。

ディスプレイに Config> プロンプトが表示されます。このプロンプトが表示されない場合は、**enter** を押します。

2. Config> プロンプトで、次のコマンドを入力して ELS にアクセスする。

event

ディスプレイに ELS 構成プロンプト (ELS config>) が表示されます。これで、ELS 構成コマンドを入力できます。

ELS 構成環境を終了するには、**exit** コマンドを入力します。

ELS 構成コマンド

表19 は、ELS 構成コマンドを要約しています。この節の残りの部分で、各コマンドについて詳しく説明します。ELS 構成環境にアクセスした後、ELS Config> プロンプトから ELS 構成コマンドを入力することができます。

表 19. ELS 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Add	イベントを既存のグループに追加するか、または新しいグループを作成します。

ELS 構成コマンド (Talk 6)

表 19. ELS 構成コマンドの要約 (続き)

コマンド	機能
Advanced	メッセージ・バッファを構成することができる拡張構成環境に入ります。
Clear	すべての ELS 構成情報を消去します。
Default	イベント、グループ、またはサブシステムの表示またはトラップ設定値をリセットします。
Delete	イベント番号を既存のグループから削除するか、またはグループ全体を削除します。
Display	コンソール・モニター上のメッセージの表示を使用可能にします。
Filter	ネット番号に基づいて ELS メッセージをフィルターに掛けます。
List	ELS 設定値およびメッセージに関する情報をリストします。
Nodisplay	コンソール上のメッセージの表示を使用不可にします。
Noremote	リモート・ワークステーションへのリモート・ログ記録を使用不可にします。
Notrace	パケット・トレース・イベントの使用不可化を制御します。
Notrap	メッセージが SNMP トラップで送信されないようにします。
Remote	メッセージがリモート・ワークステーションのログに記録されるようにします。
Set	ピン・パラメーターおよびタイム・スタンプ機能オプションを設定します。
Trace	パケット・トレース・イベントの使用可能化を制御します。
Trap	メッセージが SNMP トラップでネットワーク管理ステーションに送信されるようにします。
View	トレースされたパケットを表示できるようにします。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Add

add コマンドは、個々のイベントを既存のグループに追加したり、新しいグループを作成したりするのに使用します。グループ名は英字で始める必要があり、大文字小文字を区別します。サブシステム全体をグループに追加することはできません。

構文:

add *group_name subsystem.event_number*

注: 指定されたグループが存在しない場合は、次のようなプロンプトが出され、新しいグループの作成を確認するように求められます。

```
Group not found. Create new group? (yes or no)
```

Advanced

advanced コマンドは、拡張構成環境に入るのに使用します。この環境では、メッセージ・バッファを構成します。

構文:

advanced

Clear

clear コマンドは、すべての ELS 構成情報を消去するのに使用します。

構文:

clear

例:

```
clear
```

```
You are about to clear all ELS configuration information
Are you sure you want to do this (Yes or No):
```

Default

イベント、グループ、またはサブシステムの表示またはトラップ設定値をリセットして、使用不可の状態に戻します。

構文:

```
default                display
                        trap
                        remote
```

display *event or group or subsystem*

モニターへのメッセージの表示の出力を制御します。

trap *event or group or subsystem*

ネットワーク管理ステーションへのトラップの生成を制御します。

remote *event or group or subsystem*

リモート端末へのトラップの生成を制御します。

Delete

delete コマンドは、既存のグループからイベント番号を削除したり、グループ全体を削除したりするのに使用します。指定したイベントがグループ内で削除される最後のイベントのときは、ユーザーに通知されます。 *subsystem.event_number* ではなく *all* を指定した場合は、グループ全体の削除を確認するように求めるプロンプトが出ます。

構文:

```
delete                group_name subsystem.event_number
```

Display

display コマンドは、特定のイベント、サブシステムの一定範囲のイベント、グループ、またはサブシステムについて、モニター上のメッセージの表示を使用可能にするのに使用します。

構文:

```
display                event . . .
```

ELS 構成コマンド (Talk 6)

```
group . . .  
range . . .  
subsystem . . .
```

event *subsystem.event#*

指定されたイベント (*subsystem.event#*) のメッセージを表示します。

group *groupname*

指定されたグループ (*groupname*) のメッセージを表示します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージを表示します。

例:

```
display range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 を表示します。

subsystem *subsystemname*

指定されたサブシステムに関連するメッセージを表示します。装置上にあるサブシステムを調べたい場合は、**list subsystems** を入力します。

注: ELS は装置上のすべてのサブシステムをサポートしますが、すべての装置がすべてのサブシステムをサポートしているとは限りません。現在サポートされているサブシステムのリストについては、**イベント・ログ・システム・メッセージの手引き** を参照してください。

Filter

filter コマンドは、フィルター構成コマンド環境にアクセスするのに使用します。このコマンドについての詳細は、206ページの『ELS ネット・フィルター構成コマンド』を参照してください。

構文:

```
filter net
```

List

list コマンドは、ELS 設定値の更新情報および選択されたメッセージのリストを入手するのに使用します。

構文:

```
list all  
filter-status  
groups  
pin
```

```

remote-log status
status
subsystem . . .
subsystems all
trace-status

```

all すべての **list** カテゴリの情報をリストします。

filter-status

ELS ネット番号フィルターをリストします。

groups

ユーザー定義のグループ名と内容をリストします。

pin SNMP トラップで送信される ELS イベント・メッセージの現在数 (1 秒当り) をリストします。

remote-log status

リモート・ログ記録オプションの現行値をリストします。

例:

```

list r
Remote Logging is ON
Source IP Address = 192.67.38.2
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_DAEMON
Default Syslog Priority Level = LOG_CRIT
Number of Messages in Remote Log = 256
Remote Logging Local ID = MYHOSTNAME

```

status display, nodisplay, trap, notrap, trace, notrace, remote, および noremote コマンドによって変更されたサブシステム、グループ、およびイベントをリストします。

例:

```

list status
Subsystem:          TKR
Disp Levels:        STANDARD
Trap levels:         none
Trace levels:        none
Remote levels:       ERROR INFO TRACE
Syslog Facility/Level: LOG_USER LOG_INFO

Group   Disp   Trap   Trace   Remote
Mygroup Unset  Unset  Unset   On
Syslog Facility/Level: LOG_DAEMON LOG_CRIT

Event   Disp   Trap   Trace   Remote
IP.007  Unset  Unset  Unset   On
Syslog Facility/Level: LOG_CRON LOG_NOTICE

```

注: ディスプレイには、リモート・ログ記録が使用可能であることだけでなく、各サブシステム、グループ、およびイベントの Syslog Facility/Level 値も表示されます。イベントの範囲は、個々のイベントとしてリストされます。

subsystem

すべてのサブシステムの名前、イベント、および記述をリストします。

(**list subsystem** コマンドの出力例は、218 ページに記載してあります。)

ELS 構成コマンド (Talk 6)

subsystem *subsystem*

指定されたサブシステム内のすべてのイベントをリストします。

例:

```
list subsystem gw
```

Event	Level	Message
GW.001	ALWAYS	Copyright 1984 Mass Institute of Technology
GW.002	ALWAYS	Portable CGW %s Rel %s strtd
GW.003	ALWAYS	Unus pkt len %d nt %d int %s/%d
GW.004	ALWAYS	Sys %s q adv alloc %d excd %d
GW.005	ALWAYS	Bffrs: %d avail %d idle fair %d low %d
GW.006	C-INFO	Pkt frm nt %d int %s/%d for uninit prt, disc
GW.007	C-INFO	Ip err %x nt %d int %s/%d
GW.008	U-INFO	Ip ovfl nt %d int %s/%d, disc
GW.009	UI-ERROR	Nt dwn ip rstrt nt %d int %s/%d
GW.010	UI-ERROR	Ip q len %d no ip buf nt %d int %s/%d
GW.011	U-INFO	Op err %x hst %wo nt %d int %s/%d
GW.012	U-INFO	Op err cnt excd hst %wo nt %d int %s/%d
GW.013	U-INFO	Rtrns cnt excd hst %wo nt %d int %s/%d
GW.014	UI-ERROR	Nt dwn op rstrt nt %d int %s/%d
GW.015	UI-ERROR	Nt dwn to hst %wo nt %d int %s/%d
GW.016	U-INFO	Op ovfl to hst %wo nt %d int %s/%d
GW.017	UE-ERROR	Intfc hdw mssng nt %d int %s/%d
GW.018	U-TRACE	Strt nt slf tst nt %d int %s/%d
GW.019	C-INFO	Slf tst nt %d int %s/%d
GW.020	U-TRACE	Nt pss slf tst nt %d int %s/%d
GW.021	UE-ERROR	Nt up nt %d int %s/%d
GW.022	U-TRACE	Nt fld slf tst nt %d int %s/%d

subsystems all

すべてのサブシステム内のすべてのイベントをリストします。

trace-status

構成および実行時情報を含めて、パケット・トレースの状況に関する情報を表示します。

例:

```
list trace-status
```

```
----- Configuration -----  
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON  
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000  
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100  
Trace File Record Size:2048  Stop Trace Event: TCP.013  
Maximum Hours to HD Shadow: 1
```

Nodisplay

nodisplay コマンドは、コンソール上のメッセージ表示を選択して、オフにするのに使用します。

構文:

```
nodisplay          event . . .  
                   group . . .  
                   range . . .  
                   subsystem . . .
```

event *subsystem.event#*

指定されたイベント (*subsystem.event#*) の表示を抑制します。

group *groupname*

指定されたグループ (*groupname*) に以前に追加されたメッセージの表示を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージを表示を抑制します。

例:

```
nodisplay range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 の表示を抑制します。

subsystem *subsystemname*

指定されたサブシステムに関連するメッセージの表示を抑制します。

Noremute

noremute コマンドは、イベント番号、グループ、イベントの範囲、またはサブシステムに基づくりモート・ワークステーションへのイベント・ログ記録を抑制するのに使用します。

注: 通常、**noremute** コマンドでは、**remote** コマンドの場合のように、*syslog_facility* と *syslog_level* を指定する必要はありません。ただし、**noremute subsystem** コマンドには、すべてをオフにする代わりに、特定のメッセージ・レベルを選択して (たとえば、『error』のみ、あるいは『trace』のみ) それだけを抑制するオプションがあります。(特定のメッセージ・レベルを指定しなかった場合は、『all』が想定されます。) さらに、**noremute subsystem** コマンドは、オフにしなかった残りのメッセージ・レベルに対して *syslog_facility* と *syslog_level* を設定することも可能です。

構文:

```
noremute          event . . .
                   group . . .
                   range . . .
                   subsystem . . .
```

event *subsystem.event#*

指定されたイベントのメッセージのリモート・ログ記録を抑制します。

group *group.name*

以前に指定されたグループ (*group.name*) に追加されたメッセージのリモート・ログ記録を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージのリモート・ログ記録を抑制します。

例:

ELS 構成コマンド (Talk 6)

```
noremove range gw 19 22
```

gw.019, gw.020, gw.021, および gw.022 のリモート・ログ記録を抑制します。

subsystem *subsystem.name* [*syslog_facility* *syslog_level*]

指定されたサブシステム (*subsystem.name*) に関連するメッセージのリモート・ログ記録を抑制します。

例 1:

```
noremove subsystem tkr
```

すべての 『tkr』 メッセージのリモート・ログ記録を抑制します。

例 2:

```
ELS config> noremove subsystem tkr info
ELS config> SYSLOG FACILITY[LOG_USER]?
ELS config> SYSLOG LEVEL[LOG_INFO]?
```

この例で、『LOG_USER』と『LOG_INFO』は、サブシステム TKR に対して最後に指定された値です。指定されたコマンドは、『info』用に生成されたメッセージについてのみ、サブシステム TKR のリモート・ログ記録を抑制します。 *syslog_facility* と *syslog_level* が指定されていないので、ソフトウェアは *syslog_facility* と *syslog_level* を求めるプロンプトを出します。プロンプトに対して別8の値を入力すると、*syslog_facility* と *syslog_level* はその値で置き換えられ、TKR サブシステムの残りのリモート・ログ・メッセージに適用されます。

list all または **list status** コマンドを使用すれば、**noremove** および **remove** コマンドで行った設定を表示することができます。

syslog_facility および *syslog_level* についての詳細は、198ページの『Remote』を参照してください。

Notrace

指定されたイベント/範囲/サブシステム/グループのトレースを使用不可にします。

構文:

```
notrace                event . . .
                        group . . .
                        range . . .
                        subsystem . . .
```

event *subsystem.event#*

指定された *event#* のパケット・トレース・データの送信を抑制します。

group *groupname*

指定されたグループ (*groupname*) に以前に追加されたパケット・トレース・データの送信を抑制します。

range *subsystemname first_event_number last_event_number*

ELS 構成コマンド (Talk 6)

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージの packets・traces・データの送信を使用不可にします。

例:

```
trace range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 の packets・traces・データの送信を抑制します。

subsystem *subsystemname*

指定されたサブシステム (*subsystemname*) の packets・traces・データの送信を抑制します。

Notrap

notrap コマンドは、メッセージを選択してオフにし、SNMP トラップでネットワーク管理ステーションに送信されないようにするのに使用します。

構文:

```
notrap                event . . .  
                        group . . .  
                        range . . .  
                        subsystem . . .
```

event *subsystem.event#*

指定されたメッセージの SNMP トラップでの送信 (*subsystem.event#*) を抑制します。

group *groupname*

指定されたグループ (*groupname*) に以前に追加されたメッセージの SNMP トラップでの送信を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のイベントのメッセージの SNMP トラップでの送信を抑制します。

例:

```
notrap range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 のメッセージの SNMP トラップでの送信を抑制します。

subsystem *subsystemname*

指定されたサブシステムに関連するメッセージの SNMP トラップでの送信を抑制します。

ELS 構成コマンド (Talk 6)

Remote

remote コマンドは、イベント番号、イベントの範囲、グループ、またはサブシステムに基づいて、リモート・ワークステーションにログ記録するイベントを選択するのに使用します。

構文:

```
remote                event . . .  
                        range . . .  
                        group . . .  
                        subsystem . . .
```

event *subsystem.event# syslog_facility syslog_level*

指定されたイベントをリモート・ログに記録します。

リモート・ワークステーションの `syslog` デーモンは、`Syslog` ファシリティー値とレベル値を使用して、メッセージを記録する場所を判別します。この値は、**set facility** および **set level** コマンドを使用して設定したデフォルト値をオーバーライドします。

syslog_facility

- log_auth
- log_authpriv
- log_cron
- log_daemon
- log_kern
- log_lpr
- log_mail
- log_news
- log_syslog
- log_user
- log_uucp
- log_local0-7

syslog_level

- log_emerg
- log_alert
- log_crit
- log_err
- log_warning
- log_notice
- log_info
- log_debug

これらの値は、IBM 2210 上のデーモンと特別な関連はありません。リモート・ワークステーション上の syslog デーモンによって使用される識別子にすぎません。

range *subsystemname first_event_number last_event_number syslog_facility syslog_level*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のイベントが、*syslog_facility* 値と *syslog_level* 値に基づいて、リモート・ログに記録されます。

198ページの『remote event コマンド』を参照してください。

例:

```
remote range gw 19 22 log_user log_info
```

イベント gw.19、gw.20、gw.21、および gw.22 が、log_user の *syslog_facility* 値と log_info の *syslog_level* 値に基づいて、リモート・ログに記録されます。

group *group.name syslog_facility syslog_level*

指定されたグループに属するイベントを、*syslog_facility* 値と *syslog_level* 値に基づいて、リモート・ログに記録することができます。

198ページの『remote event コマンド』を参照してください。

subsystem *subsystem.name message_level syslog_facility syslog_level*

ここで、*subsystem.name* はサブシステムの名前、*message_level* は、サブシステム内の選択されたメッセージのレベルです。

指定された *subsystem.name* の中の、*message_level* が指定の *message_level* に一致するイベントが、*syslog_facility* 値と *syslog_level* 値に基づいて、リモート・ログ・ファイルに記録されます。198ページの『remote event コマンド』を参照してください。

Message_level の値は、『ALL』、『ERROR』、『INFO』、または『TRACE』です。172ページの『ログ・レベル』を参照してください。

remote コマンドで指定された値は、サブシステム内の特定のイベントにコーディングされた値と一致していなければなりません。そうでない場合、サブシステム内のそのイベントはリモート・ログに記録されません。

例:

```
remote subsystem TKR all log_user log_info
```

上の例では、サブシステム TKR 内のすべてのメッセージ (『all』には、『error』、『info』、または『trace』として符号化されているメッセージがすべて含まれます) が、log_user 値と log_info の値に基づいて、リモート・ホストのログに記録されます。

list all または **list status** コマンドを使用すれば、**noremote** および **remote** コマンドで行った設定を表示することができます。

Set

set コマンドは、1 秒当たりの最大タグ数の設定、タイム・スタンプ・フィーチャーの設定、またはトレース・オプションの設定に使用します。

ELS 構成コマンド (Talk 6)

構文:

```
set                pin . . .  
                    remote-logging . . .  
                    timestamp . . .  
                    trace . . .
```

pin *max_traps*

ピン・パラメーターを秒単位で送信できるトラップの最大数に設定するには、**set pin** コマンドを使用します。内部で、ピンは 10 分の 1 秒ごとにリセットされます。(10 分の 1 の数 (*max_traps*) が、10 分の 1 秒ごとに送信されます。)

remote-logging

set remote-logging コマンドは、リモート・ログ記録オプションを構成するのに使用します。これらのオプションを監視環境から構成した場合、変更は即時に有効になり、装置がリブートされると以前に構成された設定値に戻ります。

構文:

```
set remote-logging  on  
                     off  
                     facility . . .  
                     level . . .  
                     no-msgs  
                     remote_ip_addr . . .  
                     source_ip_addr ...  
                     local_id
```

on リモート・ログ記録をオンにします。これでリモート・ログ記録が使用可能になり、**remote** コマンドで選択したメッセージを記録することができます。

off リモート・ログ記録をオフにします。'remote' コマンドによって選択されたすべてのメッセージがログに記録されなくなります。

facility

リモート・ワークステーションの syslog デーモンが、メッセージを記録する場所を判別するために、*level* 値と組み合わせて使用する値を指定します。**remote** コマンドを使用して、特定の ELS イベント、範囲、グループ、またはサブシステムに対して異なる値を指定しない限り、この値がすべてのリモート・ログ記録 ELS メッセージに適用されます。

すべての可能な syslog ファシリティ値は、次のとおりです。

```
log_auth  
log_authpriv  
log_cron  
log_daemon  
log_kern  
log_lpr
```

```
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7
```

level リモート・ワークステーションの `syslog` デーモンが、メッセージを記録する場所を判別するために、*facility* 値と合わせて使用する値を指定します。 **remote** コマンドを使用して、特定の ELS イベント、範囲、グループ、またはサブシステムに対して異なる値を指定しない限り、この値がすべてのリモート・ログ記録 ELS メッセージに適用されます。

すべての可能な `syslog` レベル値は、次のとおりです。

```
log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug
```

no-msgs

ログが循環する前の、リモート・ログ用のバッファ内のメッセージの数を指定します。

remote_ip_addr

これは xxx.xxx.xxx.xxx 形式の IP アドレスです。ただし、xxx は 0 ~ 255 の任意の整数です。これは、ログ・ファイルが存在するリモート・ホストの IP アドレスです。

source_ip_addr

これは xxx.xxx.xxx.xxx 形式の IP アドレスです。ただし、xxx は 0 ~ 255 の任意の整数です。

リモート・ログ ELS メッセージに示された IP アドレスまたはホスト名を識別しやすくするために、2210 に構成された IP アドレスを使用することが必要です。また、この IP アドレスは、ネーム・サーバーが速やかにホスト名に変換できること、あるいは少なくともネーム・サーバーが速やかに『address not found』を応答できるものであることを確認する必要があります。

IP アドレスの解決が適切に行われるかどうかを調べるには、ユーザーのワークステーションで、次のような **host** コマンドを入力してみます。

```
workstation>host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

ELS 構成コマンド (Talk 6)

応答に 1 秒以上かかる場合は、もっと迅速に解決できる IP アドレスを選択してください。

local_id

これは、リモート・ログ・ファイルに記録されたメッセージに含まれ、そのメッセージを記録したマシンを識別するのに役立つ、最高 32 文字までの任意の文字列です。

timestamp [timeofday or uptime or off]

メッセージ・タイム・スタンプをオンにして、時刻またはアップタイム (日付はなく、装置の最後の初期化以降の時間、分、および秒数) が、各メッセージの横に表示されます。Set timestamp をオフにすることもできます。

set timestamp コマンドを使用して、以下のタイム・スタンプ・オプションの 1 つを使用可能にします。

timeofday

1 日 24 時間での発生時刻を示す HH:MM:SS プレフィックスを、各メッセージに追加します。

uptime

100 時間周期における発生時刻を示す HH:MM:SS プレフィックスを、各メッセージに追加します。アップタイム 100 時間後に、アップタイム・カウンターはゼロに戻り、別の 100 時間周期を開始します

off ELS タイム・スタンプ・プレフィックスをオフにします。

trace トレース・オプションを構成するには、**set trace** コマンドを使用します。トレース・オプションを監視環境から構成した場合、変更は即時に有効になります。装置をリブートすると、トレース・オプションは、前に構成された設定値に戻ります。

注: トレースは、熟練したサポート技術員の指示の下でのみ使用してください。トレースは、特にシャドー・ディスクを使用可能にして使用する場合、装置の資源を使用するので、全体的な性能およびスループットに影響を与える可能性があります。

構文:

```
set trace decode  
default-bytes-per-pkt  
disk-shadowing  
max-bytes-per-pkt  
memory-trace-buffer-size  
off  
on  
reset  
stop-event  
wrap-mode
```

decode *off/on*

パケットの復号をオンまたはオフにします。パケット復号は、すべてのコンポーネントによってサポートされているとは限りません。

default-bytes-per-pkt *bytes*

デフォルトのトレースされるバイト数を設定します。トレースを行うコンポーネントによって値が指定されない場合、この値が使用されます。

disk-shadowing **[[off or on] or record-size or time-limit or delete-file or max-file-size]**

ディスクのシャドーイングをオンまたはオフにするか、最大トレース・ファイル・サイズを設定するか、ディスク・シャドーイング・トレースの最大時間を設定します。

[off or on]

ディスク・シャドーイングをオンまたはオフにします。ディスク・シャドーイングが使用可能にされている場合、トレース・レコードがハード・ディスクにコピーされます。トレースされたレコードがハード・ディスクにコピーされると、それを監視から見ることはできなくなります。

注: WRITE、TFTP software、RETRIEVE system dump、または COPY software コマンドが出されるたびに、ディスク・シャドーイングを OFF に設定する必要があります。

disk-shadowing delete-file

トレース・ファイルを削除します。

disk-shadowing max-file-size *Mbytes*

トレース・ファイルの最大ファイル・サイズを設定します。

有効値: 1 MB ~ 16 MB

デフォルト値: 10

disk-shadowing record-size *bytes*

トレース・ファイル・レコードのレコード・サイズを設定します。

有効値 1024、2048、または 4096 バイト

デフォルト 2048 バイト

注:

1. トレース・ファイルがすでに存在する場合は、『Cannot change Record Size without first deleting the existing Trace File』が表示され、レコード・サイズは変更されません。
2. レコード・サイズを構成し、トレース・ファイルがすでに存在する場合、トレースは既存のファイルのレコード・サイズを使用します。

disk-shadowing time-limit *hours*

トレースのディスク・シャドーイングの最大時間を設定します。

有効値 1 ~ 72 時間

デフォルト 24 時間

ELS 構成コマンド (Talk 6)

注: この時間が経過した後、ディスク・シャドーイングが停止します (トレースは継続します)。ディスク・シャドーイングが再度オンにされると、実際の時間は 0 にリセットされます。

max-bytes-per-pkt *bytes*

各パケットごとに、トレースされる最大バイト数を設定します。

memory-trace-buffer-size *bytes*

RAM トレース・バッファのサイズをバイト単位で設定します。

有効値: 0, ≥10,000

デフォルト値: 0

off パケット・トレースを使用不可にします。

on パケット・トレースを使用可能にします。

reset トレース・バッファをクリアし、すべての関連のカウンターをリセットします。

stop-event *event id*

イベント (*event id*) が発生したときに、トレースを停止します。 ELS イベント *id* (たとえば、TCP.013) または『None』のいずれかを入力します。デフォルトは『None』です。トレースが停止するのは、特定の ELS イベントの表示が使用可能にされている場合だけです。

stop-event が発生すると、トレース・バッファにエントリーが書き込まれます。このトレース・エントリーの **view** コマンドは、『Tracing stopped due to ELS Event Id: TCP.013』を表示します。

stop-event のためトレースが停止した後は、**set trace on** コマンドを使ってトレースを再度使用可能にする必要があります。(ELS Config> プロンプトから使用可能にしてある場合は、リスタートでも、トレースが再度使用可能になります。)

wrap-mode [**off** or **on**]

トレース・バッファ折り返しモードをオフにします。折り返しモードがオンで、トレース・バッファが満杯の場合は、トレースを継続する必要に応じて、前のトレース・レコードに新しいトレース・レコードが上書きされます。

Trace

指定されたイベント/範囲/サブシステム/グループのトレースを使用可能にします。**trace** コマンドを ELS Config> プロンプトから使用した場合、変更は構成の一部になり、その変更をアクティブにするためにはリブートが必要です。

構文:

```
trace event . . .  
group . . .  
range . . .  
subsystem . . .
```

event *subsystem.event#*

指定されたトレース・イベント (*subsystem.event#*) をシステム・モニターに表示します。

group *groupname*

指定されたグループに以前に追加されたトレース・イベントを、装置モニターに表示できるようにします。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のトレース・イベントを、システム・モニターに表示します。

例:

```
trace range gw 19 22
```

トレース・イベント gw.19、gw.20、gw.21、および gw.22 を、システム・モニターに表示します。

subsystem *subsystemname*

指定されたサブシステムに関連するトレース・イベントを装置モニターに表示できるようにします。

Trap

trap コマンドは、リモート SNMP ネットワーク管理ワークステーションに送信するメッセージを選択するのに使用します。リモート SNMP ネットワーク管理ワークステーションは、SNMP マネージャーとして働くネットワーク内の IP ホストです。

構文:

```
trap                event . . .
                    group . . .
                    range . . .
                    subsystem . . .
```

event *subsystem.event#*

指定されたメッセージ (*subsystem.event#*) が SNMP でネットワーク管理ワークステーションに送信されるようにします。

group *groupname*

指定されたグループに以前に追加されたメッセージが、SNMP トラップでネットワーク管理ワークステーションに送信されるようにします。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

ELS 構成コマンド (Talk 6)

指定されたサブシステムの指定された範囲のメッセージが、SNMP トラップでネットワーク管理ワークステーションに送信されるようにします。

例:

```
trap range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 内のメッセージが、SNMP トラップでネットワーク管理ワークステーションに送信されるようにします。

subsystem *subsystemname*

指定されたサブシステムに関連するメッセージが、SNMP トラップで管理ワークステーションに送信されるようにします。

注: IP、ICMP、ARP、および UDP サブシステムのメッセージは、SNMP トラップで送信することはできません。これらの区域は SNMP トラップを送信する過程で使用されているか、使用される可能性があるからです。これはトラフィックの無限のループを招いて、装置に不当な負担をかけることとなります。

ELS ネット・フィルター構成コマンド

ELS ネット・フィルターは、特定のネット番号をもつ ELS メッセージのみを見つけ、その他の ELS メッセージは廃棄する機能を提供します。

フィルターを作成するときには、そのフィルターを適用するサブシステム、イベント、またはイベントの範囲を指定します。待ち行列も指定します (たとえば、『DISPLAY』、『TRAP』、『TRACE』、または『REMOTE-LOGGING』)。最後に、フィルターに掛けるネット番号 (または、ネット番号の範囲) を指定します。

フィルターを使用可能にすると、ELS コマンドによってオンにされたメッセージがフィルターに掛けられます。フィルターは、指定されたネット番号をもつメッセージのみを通過させます。指定されたネット番号を含まないメッセージは、装置に廃棄させます。

送信される ELS メッセージの数を減らすことによって、対象のインターフェースに関するメッセージを見つけやすくなります。

この節では、ELS ネット・フィルターを構成するためのコマンドについて説明します。これらのフィルターを構成するには、ELS> プロンプトで **filter net** コマンドを入力します。次に、ELS Filter net> プロンプトで構成コマンドを入力します。

表 20. ELS ネット・フィルター構成コマンド

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Create	フィルターを作成し、それに番号を割り当てます。最大 64 のフィルターを作成できます。
Delete	指定されたフィルター番号またはすべてのフィルターを削除します。
Disable	指定されたフィルター番号またはすべてのフィルターを使用不可にします。

表 20. ELS ネット・フィルタ構成コマンド (続き)

コマンド	機能
Enable	指定されたフィルタ番号またはすべてのフィルタを使用可能にします。
List	指定されたフィルタ番号またはすべてのフィルタをリストにします。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Create

create コマンドは、ELS ネット・フィルタを作成するのに使用します。

構文:

```
create queue                event event_name net#_start net#_end
                               _range event_range net#_start net#_end
                               _subsystem subsystem_name net#_start net#_end
```

queue フィルタを設定する待ち行列。有効な待ち行列は、次のとおりです。

Display

Trace

Trap

Remote

event *event_name net#_start net#_end*

フィルタに掛けるイベントとネット番号を指定します。

net#_start と *net#_end* を同じ番号として指定した場合、1つのネット番号をフィルタに掛けることになります。

コマンド **create trap event GW.009 2 10** は、ネット番号 2 ~ 10 のメッセージ GW.009 のトラップをフィルタに掛けます。

range *event_range net#_start net#_end*

フィルタに掛ける ELS メッセージの範囲とネット番号を指定します。

net#_start と *net#_end* を同じ番号として指定した場合、1つのネット番号をフィルタに掛けることになります。

コマンド **create remote range ipx 19 22 3 6** は、リモート・ログ記録用の、ネット番号 3 ~ 6 の IPX.019 で始まり IPX.022 で終わるすべての IPX メッセージをフィルタに掛けます。

subsystem *subsystem_name net#_start net#_end*

フィルタに掛けるサブシステムとネット番号を指定します。

net#_start と *net#_end* を同じ番号として指定した場合、1つのネット番号をフィルタに掛けることになります。

コマンド **create display subsys ip 1 1** は、ディスプレイへの、ネット番号 1 を含む IP サブシステムのすべての ELS メッセージをフィルタに掛けます。その他の IP サブシステム・メッセージはすべて廃棄します。

ELS 構成コマンド (Talk 6)

Delete

delete コマンドは、特定の ELS フィルターまたはすべての ELS フィルターを削除するのに使用します。

構文:

```
delete                all  
                        filter filter#
```

all 現在構成されているすべてのフィルターを削除します。

filter *filter#*

filter# によって指定されたフィルターを削除します。削除したいフィルターの番号を入手するには、**list** コマンドを使用します。

Disable

disable コマンドは、特定の ELS フィルターまたはすべての ELS 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#
```

all 現在構成されているすべてのフィルターを使用不可にします。

filter *filter#*

filter# によって指定されたフィルターを使用不可にします。使用不可にしたいフィルターの番号を入手するには、**list** コマンドを使用します。

Enable

enable コマンドは、特定の ELS フィルターまたはすべての ELS 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#
```

all 現在構成されているすべてのフィルターを使用可能にします。

filter *filter#*

filter# によって指定されたフィルターを使用可能にします。使用可能にしたいフィルターの番号を入手するには、**list** コマンドを使用します。

List

list コマンドは、特定の ELS フィルターまたはすべての ELS フィルターをリストするのに使用します。

構文:

```
list                  all
```

filter *filter#*

all 現在構成されているすべてのフィルターをリストします。

filter *filter#* によって指定されたフィルターをリストします。

ELS メッセージ・バッファ構成コマンド

表21 は、ELS Config Advanced> プロンプトで利用可能なコマンドをリストしています。

表21. ELS メッセージ・バッファ構成コマンド

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
List	メッセージ・バッファの構成設定値を表示します。
Log	メッセージ・バッファへの選択されたメッセージのログ記録を行うことができます。
Nolog	メッセージ・バッファへの選択されたメッセージのログ記録をオフにします。
Set	メッセージ・バッファのサイズ、折り返しモード、ログ記録が行なわれるかどうか、どのイベントがメッセージ・バッファを終了させるか、およびイベントによりメッセージ・バッファが停止したときにシステムが何を行うかを設定します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、ELS メッセージ・バッファの構成をリストするのに使用します。

構文:

list status

例:

```
ELS Config Advanced> list status
```

```
-----Configuration-----
Logging Status:  OFF   Wrap Mode:  ON   Logging Buffer Size:  8500   Kbytes
Stop-Event:     APPN.2   Stop-String:  netdn for intf 6
Additional Stop-Action:  NONE
```

画面の値を変更するコマンドの説明については、211ページの『Set』を参照してください。

Log

log コマンドは、どのメッセージをメッセージ・バッファに記録するか選択するのに使用します。

構文:

log event

ELS 構成コマンド (Talk 6)

group

range

subsystem

event *subsystem.event#*

指定されたメッセージ (*subsystem.event#*) がメッセージ・バッファに記録されるようにします。

group *groupname*

指定されたグループに以前に追加されたメッセージを、メッセージ・バッファに記録できるようにします。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のメッセージを、メッセージ・バッファに記録します。

例:

```
log range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 のメッセージを、メッセージ・バッファに記録します。

subsystem *subsystemname*

指定されたサブシステムに関連するメッセージを、メッセージ・バッファに記録できるようにします。

Nolog

nolog コマンドは、メッセージ・バッファに記録されたメッセージの定義済みリストからメッセージを除去するのに使用します。

構文:

nolog

event

group

range

subsystem

event *subsystem.event#*

指定されたメッセージ (*subsystem.event#*) がメッセージ・バッファに記録されないようにします。

group *groupname*

指定されたグループに以前に追加されたメッセージを、メッセージ・バッファに記録されないようにすることができます。

range *subsystemname first_event_number last_event_number*

ELS 構成コマンド (Talk 6)

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のメッセージを、メッセージ・バッファに記録されないようにします。

例:

```
log range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 のメッセージを、メッセージ・バッファに記録されないようにします。

subsystem *subsystemname*

指定されたサブシステムに関連するメッセージを、メッセージ・バッファに記録できないようにします。

Set

set コマンドは、さまざまな ELS メッセージ・バッファ・オプションを構成するのに使用します。

構文:

```
set                buffer-size Kbytes  
                   logging [on or off]  
                   stop action . . .  
                   stop event subsystem.event#  
                   stop string text  
                   wrap on or off]
```

buffer-size *Kbytes*

システムが割り振る必要があるメッセージ・バッファのサイズを、K バイト単位で指定します。**mem** コマンドは、このメモリーを Never Alloc として表示します。この値を高く設定し過ぎると、リブートの後、プロトコルとフィーチャー用のメモリーの不足のために、装置が正しく動作できなくなる可能性があります。

有効値: 0 KB ~ 装置上で使用可能なメモリーの 80%

デフォルト値: 0 (メッセージ・バッファなし)

注: このコマンドを使ってバッファを割り振らないと、ログ記録をオンに設定できません。

logging [*on* or *off*]

メッセージ・バッファが行なわれるかどうかを指定します。このコマンドは、**set buffer-size** コマンドを使用してバッファを割り振るまで有効になりません。デフォルトは *off* です。

ELS 構成コマンド (Talk 6)

stop action [**appn-dump** or **disk-offload** or **none** or **system-dump**]

『stop event』(および指定されている場合は、『stop string』)が発生するときにシステムが取る追加のアクションを指定します。アクションは、次のとおりです。

appn-dump

APPN プロトコルがアクティブである場合は、それをダンプします。APPN ダンプは、停止アクションのためダンプが取られたことを示します。

disk-offload

バッファの形式化されたバージョンをハード・ディスク上のファイルに書き込みます。ファイルがすでに存在する場合、新しいファイルがそれにとって代わります。次に、**tftp file** 監視コマンドを使用して、ファイルをリモート・ホストに送信できます。

none ログ記録が停止した後、他のアクションが取られません。

system-dump

システム全体をダンプします。システム・ダンプは、停止アクションのためダンプが取られたことを示します。

デフォルト値: なし

stop event [*subsystem.event#* or **none**]

ログ記録を停止するイベント (*subsystem.event#*) を指定します。停止文字列を指定してある場合は、停止文字列内のテキストも一致する必要があります。停止イベントが発生すると、次のようになります。

1. 次の 5 つの ELS メッセージがログに記録されます。
2. ログ記録が停止します。
3. システムが、指定された『停止アクション』を実行します。

次回に **set logging on** コマンドを出すか、装置をリポートするまで、ログ記録は停止されたままになります。

このコマンドを入力するときに停止イベントを指定しない場合、システムは停止イベントを入力するよう求めます。**none** を指定すると、停止イベント機能が使用不可にされます。

デフォルト値: なし

stop string *text* or **none**

ログ記録を停止するために、『stop event』とともに使用される文字列を指定します。stop event を指定しなかった場合、システムは『stop string』を無視します。

テキストは、最大 32 文字の長さの任意の ASCII 文字列にすることができます。このコマンドを入力するときにテキストを指定しない場合、システムは文字列を入力するよう求めます。**none** を入力すると、『stop string』はクリアされます。

デフォルト値: なし

wrap [on or off]

バッファがいっぱい有的时候きにログを停止するかどうか (off)、あるいはバッファの始めに新しいメッセージを記録するかどうか (on) を指定します。

デフォルト値: off

ELS 動作環境への出入り

ELS 監視環境 (GWCON プロセスからアクセス可能) は、ELS> プロンプトによって示されます。このプロンプトで入力されるコマンドは、現行の ELS パラメーターの設定値を変更します。これらのコマンドについては、189ページの『第11章 イベント・ログ・システム (ELS) の構成および監視』で説明します。

OPCON から ELS 監視環境に入るには、次のようにします。

1. **console** コマンドを入力します。

* console

モニターに GWCON プロンプト (+) が表示されます。最初に GWCON に入ったときにプロンプトが表示されない場合は、**enter** を押してください。

2. GWCON プロンプトで、次のコマンドを入力して ELS にアクセスする。

+ event

モニターに ELS 監視プロンプト (ELS>) が表示されます。これで、ELS 監視コマンドを入力できます。

ELS 監視環境を終了するには、**exit** コマンドを入力します。

ELS 監視コマンド

この節では、すべての ELS 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。ELS 監視環境にアクセスした後、ELS> プロンプトから ELS 監視コマンドを入力することができます。

表 22. ELS 監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Advanced	メッセージ・バッファを構成することができる拡張構成環境に入ります。
Clear	指定されたイベント、グループ、またはサブシステムに関連したメッセージのカウントをゼロにリセットします。
Display	コンソール上のメッセージの表示を使用可能にします。
Exit	ELS コンソール・プロセスを終了し、ユーザーを GWCON に戻します。
Filter	ネット番号に基づいて ELS メッセージをフィルターに掛けます。
List	ELS 設定値およびメッセージに関する情報をリストします。
Nodisplay	コンソール上のメッセージの表示を使用不可にします。
Noremote	リモート・ワークステーションのファイルへのリモート・ログ記録を使用不可にします。

ELS 監視コマンド (Talk 5)

表 22. ELS 監視コマンドの要約 (続き)

コマンド	機能
Notrace	コンソール上のトレース・イベントの表示を使用不可にします。
Notrap	メッセージが SNMP トラップでネットワーク管理ワークステーションに送信されないようにします。
Packet-trace	アクティブ・パケット・トレース・パラメーターを設定およびリストするための拡張集中環境を提供します。
Remote	メッセージがリモート・ワークステーション上のファイルに記録されるようにします。
Remove	保管されている情報を消去して、メモリーを解放します。
Restore	現行の設定値をクリアして、初期 ELS 構成を再ロードします。
Retrieve	保管されている ELS 構成を再ロードします。
Save	現行構成を保管します。
Set	ピン・パラメーターおよびタイム・スタンプ・フィーチャーを設定します。
Statistics	使用可能なサブシステムと関連の統計を表示します。
Trace	コンソール上のトレース・イベントの表示を使用可能にします。
Trap	メッセージが SNMP トラップでネットワーク管理ステーションに送信されるようにします。
View	トレースされたパケットを表示できるようにします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Advanced

advanced コマンドは、拡張監視環境に入るのに使用します。この環境では、メッセージ・バッファ動作を変更します。

構文:

advanced

Clear

clear コマンドは、特定のイベント、グループ、またはサブシステムに関連した display、trace、trap、または remote コマンドのカウントをゼロにリセットするのに使用します。

構文:

clear event . . .
group . . .
subsystem . . .

event *subsystem. event#*

指定されたイベント (*subsystem.event#*) の表示、トラップ、トレース、またはリモート・ログ記録用のイベントのカウントをゼロにリセットします。

group *group.name*

指定されたグループ (*group.name*) の表示、トラップ、トレース、またはリモート・ログ記録用のイベントのカウントをゼロにリセットします。

subsystem *subsystem.name*

指定されたサブシステム (*subsystem.name*) の表示、トラップ、トレース、またはリモート・ログ記録用のイベントのカウントをゼロにリセットします。

Display

`display` コマンドは、特定のイベントについて、監視モニター上のメッセージの表示を使用可能にするのに使用します。

構文:

```
display          event . . .
                  group . . .
                  range . . .
                  subsystem . . .
```

event *subsystem.event#*

指定されたイベント (*subsystem.event#*) に関するメッセージを表示します。

group *groupname*

指定されたグループ (*groupname*) のメッセージを表示します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージを表示します。

例:

```
display range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 を表示します。

subsystem *subsystem.name*

指定されたサブシステム (*logging level*) に関連するメッセージを表示します。ログ・レベルを指定しないと、そのサブシステムのすべてのメッセージがオンになります。

Files Trace TFTP

`files trace tftp` コマンドは、次のものに関連するサブディレクトリーからトレース・ファイルを検索するのに使用します。

- 現在アクティブなバンク (ハード・ディスク上のバンク A またはバンク B)
- ハード・ディスク上のバンク A
- ハード・ディスク上のバンク B
- ネットワーク・サブディレクトリーに保管されているトレース・ファイル (アクティブなバンクがない場合)

構文:

```
files trace tftp          active-bank ...
```

ELS 監視コマンド (Talk 5)

bank-a ...
bank-b ...
net-subdir ...

remote server IP address および *remote path/file name* を入力するよう求められます。

active-bank

現在アクティブなバンクからトレース・ファイルを検索します。

bank-a

バンク A からトレース・ファイルを検索します。

bank-b

バンク B からトレース・ファイルを検索します。

net-subdir

ネットワーク・サブディレクトリーに保管されているトレース・ファイルを検索します (アクティブなバンクがない場合)

Filter

filter コマンドは、フィルター構成コマンド環境にアクセスするのに使用します。このコマンドについての詳細は、238ページの『ELS ネット・フィルター監視コマンド』を参照してください。

構文:

filter net

List

list コマンドは、ELS 設定値の更新情報や、選択されたメッセージのリストを入手するのに使用します。

構文:

list all
active . . .
event . . .
filter-status
groups . . .
pin
remote-log status
subsystem . . .
trace-status

all すべてのサブシステム、定義されたグループ、使用可能にされたサブシステム、使用可能にされたイベント、およびピンをリストします。

active *subsystem.name*

特定のサブシステムについてアクティブであるか、非ゼロ・メッセージ・カウントをもつイベントを表示します。

例:

```
list active ip
Event      Active  Count  Message
IP.007                2874  %I -> %I
IP.022                13    add nt %I int %I nt %n int %s/%d
IP.036                2874  rcv pkt prt %d frm %I
IP.058                23    del nt %I rt via %I nt %n int %s/%d
IP.068      D          37    routing cache cleared
D=Display on  T=Trap on  P=Packet Trace on  F=Filter on  R=Remote Logging on
A=Advanced on
```

リモート・ログ記録がオンになっている場合、サブシステムについてアクティブとして表示されているイベントは、その名前の横に『R』が表示されます。

event *subsystem.event#*

指定されたイベントのログ・レベル、メッセージ、およびカウントを表示します。

例:

```
list event ip.007
Level: p-TRACE
Message: source_ip_address -> destination_ip_address
Active: Count: 84182
```

このイベントに対してリモート・ログ記録がアクティブにされており、*syslog_facility* と *syslog_level* の値が、それぞれ *log_daemon* と *log_crit* である場合、最後の行は次のようになります。

```
Active: R count:84182
Syslog Facility: log_daemon Syslog Level: log_crit
```

filter-status

ELS ネット番号フィルターをリストします。

groups *group.name*

ユーザー定義のグループ名を表示します。

pin SNMP トラップで送信される ELS イベント・メッセージの現在数 (1 秒当り) をリストします。これは、SNMP トラップ・トラフィックの量を減らすために使用できる限界値です。

例:

```
list pin
Pin: 100 events/second
```

remote-log status

set remote-logging コマンドで設定されたりリモート・ログ記録オプションの現行値をリストします。

例:

```
list r
Remote Logging is On
Source Ip Address = 192.9.200.8
Remote Log IP Address = 192.9.200.1
```

ELS 監視コマンド (Talk 5)

```
Default Syslog Facility = LOG_USER
Default Syslog Priority Level = LOG_INFO
Number of Messages in Remote Log = 256
Remote Logging Local ID = SPHINX
```

subsystem *subsystem.name*

イベント名、発生したイベントの合計数、およびその記述をリストします。

注: ELS は装置上のすべてのサブシステムをサポートしますが、すべての装置がすべてのサブシステムをサポートしているとは限りません。現在サポートされているサブシステムのリストについては、ELS メッセージを参照してください。

subsystem *subsystem.name*

指定されたサブシステムに関するすべてのイベント、ログ・レベル、およびメッセージをリストします。

例:

```
list subsystem eth
```

```
Event      Level      Message
ETH.001    P-TRACE    brd rcv unkwn type packet_type source_Ethernet_address ->
            destination_Ethernet_address nt network
ETH.002    UE-ERROR    rcv unkwn typ packet_type source_Ethernet_address ->
            destination_Ethernet_address nt network
ETH.010    C-INFO      LLC unk SAP_DSAP source_Ethernet_address ->
            destination_Ethernet_address nt network
```

subsystem all

すべてのイベント、ログ・レベル、および装置上で発生した各イベントのすべてのメッセージをリストします。

trace-status

構成および実行時情報を含めて、パケット・トレースの状況に関する情報を表示します。

例:

```
list trace-status
```

```
----- Configuration -----
Trace Status:ON Wrap Mode:ON Decode Packets:ON HD Shadowing:ON
RAM Trace Buffer Size:100000 Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256 Default Packet Bytes Traced:100
Trace File Record Size:2048 Stop Trace Event: TCP.013
Maximum Hours to HD Shadow: 1
----- Run-time Status -----
Packets in RAM Trace Buffer:1 Free Trace Buffer Memory:99958
Trace Errors:0 First Packet:1 Last Packet:1
Trace Records Stored on HD:8 Trace Buffer File Size:16560
HD-Shadowing Time Exceeded? NO Elapsed Time: 0 hr, 0 min, 10 sec
Has Stop Trace Event Occurred? NO
```

- STOP-ON-EVENT アクションが発生すると、LIST TRACE-STATUS 画面の『Trace Status』は OFF を示します。
- STOP-ON-EVENT アクションが発生するか、タイム・リミットを超過すると、LIST TRACE-STATUS 画面の『HD Shadowing』は OFF を示します。
- トレース・ファイルで折り返しが行われると、『Trace Buffer File Size』は <wrapped> を表示します。
- シャドー・ディスクのタイム・リミットを超過したが、時間が満了した以降はトレース・レコードが書き込まれていない場合には、『HD-Shadowing Time Exceeded? NO <Next trace will turn it OFF>』が表示されます。次のトレース・レコードが書き込まれると、『HD-Shadowing Time Exceeded? YES』が表示されます。

talk 6 の下の ELS Config>LIST TRACE コマンドは、次のような情報を表示します。

```
----- Configuration -----
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
Maximum Hours to HD Shadow: 1
```

Nodisplay

nodisplay コマンドは、コンソール上のメッセージ表示を選択して、オフにするのに使用します。

構文:

```
nodisplay          event . . .
                   group . . .
                   range . . .
                   subsystem . . .
```

event *subsystem.event#*

指定されたイベントに関するメッセージの表示を抑制します。

group *group.name*

指定されたグループ (*group.name*) に以前に追加されたメッセージの表示を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージを表示を抑制します。

例:

```
nodisplay range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 の表示を抑制します。

subsystem *subsystem.name*

指定されたサブシステム (*logging level*) に関連するメッセージの表示を抑制します。

Noremote

noremote コマンドは、リモート・ワークステーションへのログを選択し、それをオフにするのに使用します。

構文:

```
noremote          event . . .
                   group . . .
                   range . . .
```

ELS 監視コマンド (Talk 5)

subsystem . . .

event *subsystem.event#*

指定されたイベントのメッセージのリモート・ログ記録を抑制します。

group *group.name*

以前に指定されたグループ (*group.name*) に追加されたメッセージのリモート・ログ記録を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージのリモート・ログ記録を抑制します。

例:

```
noremove range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 のリモート・ログ記録を抑制します。

subsystem *subsystem.name*

指定されたサブシステム (*logging level*) に関連するメッセージのリモート・ログ記録を抑制します。

例:

```
noremove subsystem tkr
```

注: noremove では、Remote の場合のように、Syslog ファシリティ値とレベル値を指定する必要はありません。

remote および **noremove** コマンドを使用して設定した内容を確認する場合は、**list event** および **list active** コマンドを使用します。

Notrace

notrace コマンドは、選択されたトレース・イベントのモニターの表示を停止するのに使用します。

構文:

notrace

event . . .

group . . .

range . . .

subsystem . . .

event *subsystem.event#*

指定されたトレース・イベントの表示を抑制します。

group *groupname*

指定されたグループ (*groupname*) に関連するトレース・イベントの表示を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージのパケット・トレース・データの送信を使用不可にします。

例:

```
notrace range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 のパケット・トレース・データの送信を抑制します。

subsystem *subsystemname [logging-level]*

指定されたサブシステムとログ・レベルに関連したトレース・イベントの表示を抑制します。 *logging-level* を指定しないと、そのサブシステムのすべてのログ・レベルのトレースが抑制されます。

例:

```
notrace subsystem fr1 error
```

```
notrace subsystem fr1
```

Notrap

notrap コマンドは、メッセージを選択してオフにし、SNMP トラップでネットワーク管理ステーションに送信されないようにするのに使用します。

構文:

```
notrap                event . . .
                        group . . .
                        range . . .
                        subsystem . . .
```

event *subsystem.event#*

指定されたメッセージの SNMP トラップでの送信 (*subsystem.event#*) を抑制します。

group *groupname*

指定されたグループ (*groupname*) に以前に追加されたメッセージの SNMP トラップでの送信を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のイベントのメッセージの SNMP トラップでの送信を抑制します。

例:

```
notrap range gw 19 22
```

ELS 監視コマンド (Talk 5)

イベント gw.19、gw.20、gw.21、および gw.22 のメッセージの SNMP トラップでの送信を抑制します。

subsystem *subsystemname* [*logging-level*]

指定されたサブシステムとログ・レベルに関連したメッセージの SNMP トラップでの送信を抑制します。 *logging-level* を指定しないと、そのサブシステムのすべてのログ・レベルのトラップが抑制されます。

例:

```
notrap subsystem eth error
```

Packet Trace

packet-trace コマンドは、種々のサブシステムに関するパケット・トレース情報を表示/使用可能/使用不可にするのに使用します。

構文:

packet-trace

Packet Trace の使用を終了するときは、**Exit** コマンドを使用します。

コマンドについての詳しい説明は、235ページの『パケット・トレース監視コマンド』を参照してください。

Remote

remote コマンドは、イベント番号、イベントの範囲、グループ、またはサブシステムに基づいて、リモート・ログ・ファイルに記録するイベントを選択するのに使用します。

構文:

```
remote event . . .  
 group . . .  
 range . . .  
 subsystem . . .
```

event *subsystem.event# syslog_facility syslog_level*

指定されたイベントをリモート・ログに記録します。

リモート・ワークステーションの syslog デーモンは、Syslog ファシリティー値とレベル値を使用して、メッセージを記録する場所を判別します。この値は、**set facility** および **set level** コマンドを使用して設定したデフォルト値をオーバーライドします。

syslog_facility

log_auth

log_authpriv

log_cron

log_daemon


```
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7
```

syslog_level

```
log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug
```

これらの値は、IBM 2210 上のデーモンと特別な関連はありません。リモート・ワークステーション上の syslog デーモンによって使用される識別子にすぎません。

例:

```
remote event gw.019 log_user log_info
```

group *group.name syslog_facility syslog_level*

指定されたグループに属するイベントを、*syslog_facility* 値と *syslog_level* 値に基づいて、リモート・ログに記録することができます。

222ページの『remote event コマンド』を参照してください。

range *subsystemname first_event_number last_event_number syslog_facility syslog_level*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のイベントを、*syslog_facility* と *syslog_level* に基づいて、リモート・ログに記録します。222ページの『remote event コマンド』を参照してください。

例:

```
remote range gw 19 22 log_user log_info
```

イベント gw.19、gw.20、gw.21、および gw.22 が、log_user の *syslog_facility* 値と log_info の *syslog_level* 値によって指定されたリモート・ログ・ファイルに記録されます。

ELS 監視コマンド (Talk 5)

subsystem *subsystem.name message_level syslog_facility syslog_level*

ここで、*subsystem.name* はサブシステムの名前、*message_level* は、サブシステム内の選択されたメッセージのレベルです。

指定された *subsystem.name* の中の、*message_level* が指定の *message_level* に一致するイベントが、*syslog_facility* 値と *syslog_level* 値に基づいて、リモート・ログ記録されます。222ページの『remote event コマンド』を参照してください。

Message_level は、ALL、ERROR、INFO、または TRACE などの値です。172ページの『ログ・レベル』を参照してください。**remote** コマンドで指定された値は、サブシステム内の特定のイベントにコーディングされた値と一致していなければなりません。そうでない場合、サブシステム内のそのイベントはリモート・ログに記録されません。

例:

```
remote subsystem eth all log_user log_info
```

上の例では、サブシステム TKR 内のすべてのメッセージ (『all』には、『error』、『info』、または『trace』として符号化されているメッセージがすべて含まれます) が、*log_user* 値と *log_info* の値に基づいて、リモート・ホストのログに記録されます。

remote および **noremove** コマンドを使用して設定した内容を確認する場合は、**list event** および **list active** コマンドを使用します。

Remove

remove コマンドは、保管されている情報を消去して、メモリーを解放するのに使用します。以前に **save** コマンドを使用して現行構成を保管した場合、**remove** を使用すると、保管した構成を消去することができます。

構文:

remove

Restore

restore コマンドは、すべての現行設定値 (カウンターを除く) をクリアし、初期 ELS 構成を再ロードするのに使用します。現行設定値を保存する場合は、初期構成に復元する前に **save** コマンドを使用します。

構文:

restore

Retrieve

retrieve コマンドは、保管された ELS 構成を再ロードするのに使用します。以前に **save** コマンドを使用して現行構成を保管した場合、**retrieve** を使用してそれを再ロードします。**Retrieve** を実行しても、保管された構成は消去されません。保管された構成を消去するには、**remove** コマンドを使用します。

構文:

retrieve

Save

save コマンドは、現行構成 (カウンターを除く) を保管するのに使用します。 **Save** は、デフォルト構成 (構成コマンドを用いて設定した構成) には影響を与えません。監視コマンドを用いて構成を変更した後に **save** を使用するのには、リスタート後もこの構成を保存したい場合です。保管された構成は、一度に 1 つしか存在できません。保管された構成を再ロードするには、**retrieve** コマンドを使用します。

構文:

save

Set

set コマンドは、1 秒当りの最大トラップ数の設定、タイム・スタンプ機能の設定、またはトレース・オプションの設定に使用します。

構文:

```
set                pin . . .
                   _remote-logging . . .
                   _timestamp . . .
                   trace . . .
```

pin ピン・パラメーターを秒単位で送信できるトラップの最大数に設定するには、**set pin** コマンドを使用します。内部で、ピンは 10 分の 1 秒ごとによりセットされます。(10 分の 1 の数 (*max_traps*) が、10 分の 1 秒ごとに送信されます。)

remote-logging

set remote-logging コマンドは、リモート・ログ記録オプションを構成するのに使用します。これらのオプションを監視環境から構成した場合、変更は即時に有効になり、装置がリブートされると以前に構成された設定値に戻ります。

構文:

```
set remote-logging  on
                     off
                     facility . . .
                     level . . .
                     local_id
                     remote_ip_addr . . .
                     source_ip_addr ...
```

ELS 監視コマンド (Talk 5)

on リモート・ログ記録をオンにします。これでリモート・ログ記録が使用可能になり、**remote** コマンドで選択したメッセージを記録することができます。

off リモート・ログ記録をオフにします。**remote** コマンドによって選択されたすべてのメッセージがログに記録されなくなります。

facility

リモート・ワークステーションの `syslog` デーモンが、メッセージを記録する場所を判別するために、*level* 値と組み合わせて使用する値を指定します。**remote** コマンドを使用して、特定の ELS イベント、範囲、グループ、またはサブシステムに対して異なる値を指定しない限り、この値がすべてのリモート・ログ記録 ELS メッセージに適用されます。

すべての可能な `syslog` ファシリティ値は、次のとおりです。

- `log_auth`
- `log_authpriv`
- `log_cron`
- `log_daemon`
- `log_kern`
- `log_lpr`
- `log_mail`
- `log_news`
- `log_syslog`
- `log_user`
- `log_uucp`
- `log_local0-7`

level リモート・ワークステーションの `syslog` デーモンが、メッセージを記録する場所を判別するために、*facility* 値と合わせて使用する値を指定します。**remote** コマンドを使用して、特定の ELS イベント、範囲、グループ、またはサブシステムに対して異なる値を指定しない限り、この値がすべてのリモート・ログ記録 ELS メッセージに適用されます。

すべての可能な `syslog` レベル値は、次のとおりです。

- `log_emerg`
- `log_alert`
- `log_crit`
- `log_err`
- `log_warning`
- `log_notice`
- `log_info`
- `log_debug`

local_id

リモート・ログ・メッセージに表示され、特定のメッセージを記録したマシンを識別するのに役立つ、1 ~ 32 文字の識別子を指定します。

remote_ip_addr

これは、ログ・ファイルが存在するリモート・ホストの IP アドレスです。

source_ip_addr

リモート・ログ記録するメッセージを発信したマシンの IP アドレスを指定します。

リモート・ログ ELS メッセージに示された IP アドレスまたはホスト名を識別しやすくするために、2210 に構成された IP アドレスを使用することが必要です。また、この IP アドレスは、ネーム・サーバーが速やかにホスト名に変換できること、あるいは少なくともネーム・サーバーが速やかに『address not found』を応答できるものであることを確認する必要があります。

IP アドレスの解決が適切に行われるかどうかを調べるには、ユーザーのワークステーションで、次のような **host** コマンドを入力してみます。

```
workstation>host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

応答に 1 秒以上かかる場合は、もっと迅速に解決できる IP アドレスを選択してください。

timestamp

メッセージ・タイム・スタンプをオンにして、時刻またはアップタイム (日付はなく、装置の最後の初期化以降の時間、分、および秒数) が、各メッセージの横に表示したり、あるいはメッセージ・タイム・スタンプをオフにしたりすることができます。

注: タイム・スタンプをオンにする場合は、CONFIG プロセスに戻り、time コマンドを使用してルーターの日付と時刻を設定することを忘れないようにしてください。そうしないと、すべてのメッセージに 00:00:00 が表示されるか、時間、分、または秒数 (あるいは、その全部) に負数が表示される (たとえば、00:-4:-5) ことになります。

set timestamp コマンドを使用して、以下のタイム・スタンプ・オプションの 1 つを使用可能にします。

timeofday

1 日 24 時間での発生時刻を示す HH:MM:SS プレフィックスを、各 ELS メッセージに追加します。

uptime

装置のアップタイムの 100 時間周期における発生時刻を示す HH:MM:SS プレフィックスを、各 ELS メッセージに追加します。アップタイム 100 時間後に、アップタイム・カウンターはゼロに戻り、別の 100 時間周期を開始します

ELS 監視コマンド (Talk 5)

off ELS タイム・スタンプ・プレフィックスをオフにします。

構文:

set timestamp [timeofday or uptime or off]

trace トレース・オプションを構成するには、**set trace** コマンドを使用します。トレース・オプションを監視環境から構成した場合、変更は即時に有効になり、装置がリブートされると以前に構成された設定値に戻ります。

構文:

set trace decode . . .
default-bytes-per-pkt . . .
disk-shadowing . . .
max-bytes-per-pkt . . .
memory-trace-buffer-size . . .
off
on
reset
stop-event . . .
wrap-mode . . .

decode . . .

パケット復号オプションを設定します。パケット復号は、すべてのコンポーネントによってサポートされているとは限りません。

exclude

指定されたフレーム・タイプを復号から除外します。除外が可能なフレーム・タイプは次のとおりです。

lecontrol

LE Control

ip IP

arp ARP

ipx IPX

netbios

NetBIOS

bpdu BPDU

appletalk

AppleTalk

aarp AppleTalk ARP

hex 16 進数フレーム・データの印刷をオフにします。

summary

1 行の要約復号の印刷をオフにします。完全な復号が印刷されます。

ELS 監視コマンド (Talk 5)

all すべてのパケット・タイプをトレースから除外します。フレーム・タイプは復号されません。

none トレースからパケット・タイプを除外しません。これは *exclude all* と正反対です。

include

指定されたフレーム・タイプを復号に組み込みます。組み込みが可能なフレーム・タイプは次のとおりです。

lecontrol

LE Control

ip IP

arp ARP

ipx IPX

netbios

NetBIOS

bpdu BPDU

appletalk

AppleTalk

aarp AppleTalk ARP

hex 16 進数フレーム・データの印刷をオンにします。

summary

1 行の要約復号の印刷をオンにします。完全な復号は印刷されません。

all トレース内にすべてのパケット・タイプを組み込みます。

none トレース内にパケット・タイプを組み込みません。これは、*include all* の正反対です。

off 復号をオフに設定します。

on 復号をオンに設定します。

注: デフォルトの設定は、すべてのフレーム・タイプについて完全な復号出力を印刷することです。 **list trace-status** コマンドを使用して、現行の復号設定を調べてください。218 ページを参照してください。

default-bytes-per-pkt *bytes*

デフォルトのトレースされるバイト数を設定します。トレースを行うコンポーネントによって値が指定されない場合、この値が使用されます。

disk-shadowing **[[off or on] or [delete-file or record-size or time-limit]]**

ディスク・シャドーイングをオンまたはオフにするか、最大トレース・ファイル・サイズを設定するか、ディスク・シャドーイング・トレースの最大時間を設定します。

[off or on]

ディスク・シャドーイングをオンまたはオフにします。ディスク・シャドーイングが使用可能にされている場合、トレース・レコードがハード・ディスクにコピーされます。トレースされたレコードがハード・ディスクにコピーされると、それを監視から見ることはできなくなります。

注: WRITE、TFTP software、RETRIEVE system dump、または COPY software コマンドが出されるたびに、ディスク・シャドーイングを OFF に設定する必要があります。ディスク・シャドーイングをオンまたはオフにし、最大トレース・ファイル・サイズを設定します。ディスク・シャドーイングが使用可能にされている場合、トレース・レコードがハード・ディスクにコピーされます。トレースされたレコードがハード・ディスクにコピーされると、監視を通じてそれを見ることができなくなります。

record-size *bytes*

トレース・ファイル・レコードのレコード・サイズを設定します。

有効値: 1024、2048、または 4096 バイト

デフォルト: 2048 バイト

注:

1. トレース・ファイルがすでに存在する場合は、『Cannot change Record Size without first deleting the existing Trace File』が表示され、レコード・サイズは変更されません。
2. レコード・サイズを構成し、トレース・ファイルがすでに存在する場合、トレースは既存のファイルのレコード・サイズを使用します。

delete-file

トレース・ファイルを削除します (アクティブなバンクとだけ関連付けられたサブディレクトリーで)。

注: コマンドが出されたときにディスク・シャドーイングがオンである場合、『Disk-shadowing must be set to OFF before trace file can be deleted』が表示され、ファイルは削除されません。

time-limit *hours*

トレースのディスク・シャドーイングの最大時間を設定します。

有効値:
1 ~ 72 時間

デフォルト
24

ELS 監視コマンド (Talk 5)

注: この時間が経過した後、ディスク・シャドーイングが停止します (トレースは継続します)。ディスク・シャドーイングが再度オンにされると、実際の時間は 0 にリセットされます。

max-bytes-per-pkt *bytes*

各パケットごとに、トレースされる最大バイト数を設定します。

memory-trace-buffer-size *bytes*

RAM トレース・バッファのサイズをバイト単位で設定します。

有効値: 0、 $\geq 10,000$

デフォルト値: 0

off パケット・トレースを使用不可にします。

on パケット・トレースを使用可能にします。

reset トレース・バッファをクリアし、すべての関連のカウンターをリセットします。

stop-event *event id*

イベント (event id) が発生したときに、トレースを停止します。 ELS イベント id (たとえば、TCP.013) または『None』のいずれかを入力します。デフォルトは『None』です。トレースが停止するのは、特定の ELS イベントの表示が使用可能にされている場合だけです。

stop-event が発生すると、トレース・バッファにエントリーが書き込まれます。このトレース・エントリーの **view** コマンドは、『Tracing stopped due to ELS Event Id: TCP.013』を表示します。

stop-event のためトレースが停止した後は、**set trace on** コマンドを使ってトレースを再度使用可能にする必要があります。(ELS Config> プロンプトから使用可能にしてある場合は、リスタートでも、トレースが再度使用可能になります。)

例:

```
set trace stop-event TCP.013
```

wrap-mode *off/on*

トレース・バッファ折り返しモードをオフにします。折り返しモードが使用可能のときにトレース・バッファが満杯の場合、トレースを継続するのに必要なため、前のトレース・レコードが新しいトレース・レコードによって上書きされます。

Statistics

statistics コマンドは、すべての利用可能なサブシステムとその統計のリストを表示するのに使用します。

注: 以下の例は、ご使用のディスプレイとは正確に一致しない場合があります。コマンドの出力は、導入されているソフトウェアのバージョンおよびリリースによって異なります。

構文:

ELS 監視コマンド (Talk 5)

statistics

例:

statistics

Subsys	Vector	Exist	String	Active	Heap
GW	105	101	3411	0	0
FLT	20	7	184	0	0
BRS	50	5	201	0	0
ARP	150	142	7030	0	0
IP	100	100	2463	2	20
ICMP	30	21	529	0	0
TCP	60	57	2420	0	0
UDP	10	6	179	0	0
BTP	40	13	695	0	0
RIP	30	22	474	0	0
OSPF	80	73	2859	0	0
MSPF	40	17	593	0	0
TFTP	35	29	819	0	0
SNMP	30	28	821	0	0
DVM	30	21	589	0	0
DN	140	115	5842	0	0
XN	35	21	780	0	0
IPX	110	110	4705	0	0
CLNP	80	58	1763	0	0
ESIS	40	24	716	0	0
ISIS	80	58	2422	0	0
DNAV	50	26	1314	0	0
AP2	80	70	1755	0	0
ZIP2	60	51	1859	0	0
R2MP	50	38	1185	0	0
VIN	90	79	3159	0	0
SRT	120	94	5040	0	0
STP	60	32	1590	0	0
BR	50	30	1616	0	0
SRLY	30	28	1409	0	0
ETH	60	47	1098	0	0
SL	50	35	584	0	0
TKR	60	45	2031	0	0
X25	70	53	1909	0	0
FDDI	30	27	1155	0	0
SDLC	100	95	4263	0	0
FRL	130	97	6068	0	0
PPP	190	186	6394	0	0
X251	50	16	546	0	0
X252	50	34	996	0	0
X253	50	42	1649	0	0
ISDN	50	43	1994	0	0
IPPN	20	4	132	0	0
WRS	40	33	1938	0	0
LNМ	70	60	3137	0	0
LLC	170	168	9840	0	0
BGP	80	74	2477	0	0
MCF	15	9	244	0	0
DLS	500	497	24340	0	0
V25B	30	28	1058	0	0
BAN	30	29	1223	0	0
COMP	80	26	1050	0	0
NBS	100	50	3029	0	0
ATM	300	216	10808	0	0
LEC	200	174	7258	0	0
APPN	100	28	467	0	0
ILMI	150	23	487	0	0
SAAL	30	26	621	0	0
SVC	30	26	465	0	0
LES	400	361	22333	0	0
LECS	150	145	5666	0	0
EVLOG	1	1	105	0	0
NOT	25	15	508	0	0
NHRP	250	211	8193	0	0
XTP	64	58	2271	0	0
ESC	150	67	3122	0	0
LCS	40	22	858	0	0
LSA	70	61	3506	0	0
MPC	130	30	1677	3	44

SCSP	40	34	1234	0	0
ALLC	50	36	1842	0	0
NDR	50	38	1150	0	0
MLP	100	93	4006	0	0
SEC	50	30	688	0	0
ENCR	100	4	194	0	0
PM	25	6	120	0	0
DGW	20	9	238	0	0
QLLC	55	54	2411	0	0
Total	6490	4942	215805	5	64

Maximum:7976 vector, 155 subsystem
 Memory:71784/620 vector+ 81256/217714 data+ 64 heap=371438Subsys

Subsys

サブシステムの名前

Vector

サブシステムの最大サイズ

Exist このサブシステム内で定義されているイベントの数

String このサブシステム内でメッセージの記憶域に使用されるバイト数

Active サブシステム内の活動 (表示されるか、トラップされるか、またはカウントされた) イベントの数

Heap サブシステムにより使用中の動的メモリー

Trace

trace コマンドは、システム・モニターに表示するトレース・イベントを選択するのに使用します。このコマンドは、235ページの『パケット・トレース監視コマンド』に説明されている **packet trace** コマンドに似た機能を提供します。

構文:

```
trace                event . . .
                        group . . .
                        range . . .
                        subsystem . . .
```

event *subsystem.event#*

指定されたトレース・イベント (*subsystem.event#*) をシステム・モニターに表示します。

group *groupname*

指定されたグループに以前に追加されたトレース・イベントを、装置モニターに表示できるようにします。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のトレース・イベントを、システム・モニターに表示します。

ELS 監視コマンド (Talk 5)

例:

```
trace range gw 19 22
```

トレース・イベント gw.19、gw.20、gw.21、および gw.22 を、システム・モニターに表示します。

subsystem *subsystemname*

指定されたサブシステムに関連するトレース・イベントを装置モニターに表示できるようにします。

Trap

trap コマンドは、リモート SNMP ネットワーク管理ワークステーションに送信するメッセージを選択するのに使用します。リモート SNMP ネットワーク管理ワークステーションは、SNMP マネージャーとして働くネットワーク内の IP ホストです。

構文:

```
trap                               event . . .  
                                       group . . .  
                                       range . . .  
                                       subsystem . . .
```

event *subsystem.event#*

指定されたメッセージ (*subsystem.event#*) が SNMP でネットワーク管理ワークステーションに送信されるようにします。

group *groupname*

指定されたグループに以前に追加されたメッセージが、SNMP トラップでネットワーク管理ワークステーションに送信されるようにします。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のメッセージが、SNMP トラップでネットワーク管理ワークステーションに送信されるようにします。

例:

```
trap range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 内のメッセージが、SNMP トラップでネットワーク管理ワークステーションに送信されるようにします。

subsystem *subsystemname*

指定されたサブシステムに関連するメッセージが、SNMP トラップで管理ワークステーションに送信されるようにします。

注: IP、ICMP、ARP、および UDP サブシステムのメッセージは、SNMP トラップで送信することはできません。これらの区域は SNMP トラップを

送信する過程で使用されているか、使用される可能性があるからです。これはトラフィックの無限のループを招いて、装置に不当な負担をかけることとなります。

View

view コマンドは、トレース・パケットを表示するのに使用します。

構文:

```
view                current
                    first
                    jump
                    last
                    next
                    prev
                    search ...
```

current

現在のトレース・パケットを表示します。現在パケットが無効の場合は、トレース・バッファ内の最初のパケットが表示されます。

first トレース・バッファ内の最初のトレース・パケットを表示します。

jump *n*

現在パケットから *n* パケット前または後のトレース・パケットを表示します。

last トレース・バッファ内の最後のトレース・パケットを表示します。

next 次のトレース・パケットを表示します。

prev 直前のトレース・パケットを表示します。

search

指定された情報が入っている、次のトレース・パケットを表示します。検索情報を次のものによって指定することができます。

- 16 進数ストリング
- IP アドレス
- ASCII テキスト

パケット・トレース監視コマンド

この節では、Packet-trace 監視コマンドについて説明します。Packet-trace 監視環境にアクセスした後、ELS Packet Trace> プロンプトから Packet-trace 監視コマンドを入力することができます。

ELS 監視コマンド (Talk 5)

表 23. パケット・トレース監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Off	パケット・トレースを使用不可にします。
On	パケット・トレースを使用可能にします。メモリー・トレース・バッファ・サイズの入力を求めるプロンプトが出ます (前に設定されていない場合)。
Reset	トレース・バッファをクリアし、すべての関連カウンターをリセットします。
Set	トレース・オプションを構成します。
Subsystems	パケット・トレースをサポートするサブシステムのトレースを起動するか、または要約を表示します。
Trace-status	構成および実行時情報を含めて、パケット・トレースの状態に関する情報を表示します。
View	取り込まれたパケット・トレース・バッファをコンソールに表示する機能を提供します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Off

off コマンドは、パケット・トレースを使用不可にするのに使用します。

構文:

off

On

on コマンドは、パケット・トレースを使用可能にするのに使用します。

構文:

on

Reset

reset コマンドは、トレース・バッファをクリアし、すべての関連カウンターをリセットするのに使用します。

構文:

reset

Set

set コマンドは、トレース・オプションを構成するのに使用します。

構文:

set

decode

default-bytes-per-pkt

disk-shadowing
max-bytes-per-pkt
memory-trace-buffer-size
stop-event
wrap-mode
exit

set コマンドの説明については、228 ページを参照してください。

Subsystems

subsystems コマンドは、パケット・トレースをサポートするサブシステムのトレースを起動するか、または要約を表示するのに使用します。

構文:

```

subsystems          atm
                       fddi
                       lec
                       summary

```

例:

```

subsystems atm
Network number? 0
ATM Interface is selected
on | off | list [list]? on
Note that SVC uses VPI = 0, VCI = 5
and ILMI uses VPI = 0, VCI = 16
Beginning of VPI range [0]?
End of VPI range [0]?
Beginning of VCI range [0]? 16
End of VCI range [0]? 16
Tracing event ATM.88: ATM frames

```

例:

```

subsystems lec
Network number? 1
ATM Emulated LAN is selected
on | off | list [list]? on
Trace which types of frames (data, control, both) [both]?
Tracing event LEC.11: data frames over ATM Forum LEC: interface 1
Tracing event LEC.12: control frames over ATM Forum LEC: interface 1
Note that if the user DISABLEs and TESTs this LEC interface,
the LEC trace settings from Talk 6 Config will take effect.

```

MAC Address packet filtering can be enabled under the LEC net using the 'trace mac-address' command.

例:

```

subsystems summary
Subsystems Being Traced

ATM      net number = 0, VPI Range:    0 -    0
          VCI Range:    16 -   16
LEC      net number = 1

```

ELS 監視コマンド (Talk 5)

Trace-Status

trace-status コマンドは、パケット・トレースに関する更新情報を入手するのに使用します。

構文:

trace-status

例:

```
trace-status
----- Configuration -----
Trace Status:OFF  Wrap Mode:OFF  Decode Packets:OFF  HD Shadowing:OFF
RAM Trace Buffer Size:0  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: None
Maximum Hours to HD Shadow: 24
----- Run-time Status -----
Packets in RAM Trace Buffer:0  Free Trace Buffer Memory:0
Trace Errors:0  First Packet:0  Last Packet:0
Trace Records Stored on HD:0  Trace Buffer File Size:0
HD-Shadowing Time Exceeded? NO
Has Stop Trace Event Occurred? NO
```

View

view コマンドは、取り込まれたパケット・トレース・バッファをモニターに表示する環境に入るのに使用します。

view コマンドの説明は、235ページの『View』を参照してください。

構文:

```
view          _current
              _first
              _jump
              _last
              _next
              _prev
              _search
              _exit
```

ELS ネット・フィルター監視コマンド

この節では、ELS ネット・フィルターを操作するためのコマンドについて説明します。フィルター環境に入るには、ELS> プロンプトで **filter net** コマンドを入力します。次に、ELS Filter net> プロンプトで監視コマンドを入力します。

表 24. ELS ネット・フィルター監視コマンド

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。

表 24. ELS ネット・フィルター監視コマンド (続き)

コマンド	機能
Create	フィルターを作成し、それに番号を割り当てます。最大 64 のフィルターを作成できます。
Delete	指定されたフィルター番号またはすべてのフィルターを削除します。
Disable	指定されたフィルター番号またはすべてのフィルターを使用不可にします。
Enable	指定されたフィルター番号またはすべてのフィルターを使用可能にします。
List	指定されたフィルター番号またはすべてのフィルターをリストにします。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Create

create コマンドは、ELS ネット・フィルターを作成するのに使用します。

構文:

```
create queue event event_name net#_start net#_end
           _range event_range net#_start net#_end
           _subsystem subsystem_name net#_start net#_end
```

queue フィルターを設定する待ち行列。有効な待ち行列は、次のとおりです。

Display
Trace
Trap
Remote

event *event_name* *net#_start* *net#_end*

フィルターに掛けるイベントとネット番号を指定します。

net#_start と *net#_end* を同じ番号として指定した場合、1つのネット番号をフィルターに掛けることになります。

コマンド **create trap event GW.009 2 10** は、ネット番号 2 ~ 10 のメッセージ GW.009 のトラップをフィルターに掛けます。

range *event_range* *net#_start* *net#_end*

フィルターに掛ける ELS メッセージの範囲とネット番号を指定します。

net#_start と *net#_end* を同じ番号として指定した場合、1つのネット番号をフィルターに掛けることになります。

コマンド **create remote range ipx 19 22 3 6** は、リモート・ログ記録用の、ネット番号 3 ~ 6 の IPX.019 で始まり IPX.022 で終わるすべての IPX メッセージをフィルターに掛けます。

subsystem *subsystem_name* *net#_start* *net#_end*

フィルターに掛けるサブシステムとネット番号を指定します。

net#_start と *net#_end* を同じ番号として指定した場合、1つのネット番号をフィルターに掛けることになります。

ELS 監視コマンド (Talk 5)

コマンド **create display subsys ip 1 1** は、ディスプレイへの、ネット番号 1 を含む IP サブシステムのすべての ELS メッセージをフィルターに掛けます。その他の IP サブシステム・メッセージはすべて廃棄します。

Delete

delete コマンドは、特定の ELS フィルターまたはすべての ELS フィルターを削除するのに使用します。

構文:

```
delete                all  
                        filter filter#
```

all 現在構成されているすべてのフィルターを削除します。

filter *filter#*

filter# によって指定されたフィルターを削除します。削除したいフィルターの番号を入手するには、**list** コマンドを使用します。

Disable

disable コマンドは、特定の ELS フィルターまたはすべての ELS 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#
```

all 現在構成されているすべてのフィルターを使用不可にします。

filter *filter#*

filter# によって指定されたフィルターを使用不可にします。使用不可にしたいフィルターの番号を入手するには、**list** コマンドを使用します。

Enable

enable コマンドは、特定の ELS フィルターまたはすべての ELS 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#
```

all 現在構成されているすべてのフィルターを使用可能にします。

filter *filter#*

filter# によって指定されたフィルターを使用可能にします。使用可能にしたいフィルターの番号を入手するには、**list** コマンドを使用します。

List

list コマンドは、特定の ELS フィルターまたはすべての ELS フィルターをリストするのに使用します。

構文:

```
list                all
                   filter filter#
```

all 現在構成されているすべてのフィルターをリストします。

filter filter#
filter# によって指定されたフィルターをリストします。

ELS メッセージ・バッファ監視コマンド

表25 は、ELS Config Advanced> プロンプトで利用可能なコマンドをリストしていません。

表 25. ELS メッセージ・バッファ監視コマンド

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Flush	メッセージ・バッファをクリアし、メッセージ・バッファへのログ記録をオフにします。
List	メッセージ・バッファの動作設定値を表示します。
Log	メッセージ・バッファへの選択されたメッセージのログ記録を行うことができます。
Nolog	メッセージ・バッファへの選択されたメッセージのログ記録をオフにします。
Read-file	形式化メッセージ・バッファをファイルから読み取り、それをコンソール上に表示します。
Set	メッセージ・バッファのサイズ、折り返しモード、ログ記録が行なわれるかどうか、どのイベントがメッセージ・バッファを終了させるか、およびイベントによりメッセージ・バッファが停止したときにシステムが何を行うかを設定します。
Tftp	リモート・ホストにあるファイルに ELS メッセージ・バッファを送信します。
View	メッセージ・バッファ内のすべてまたは特定の数のメッセージを表示します。メッセージがスクロールして画面から消える方法も制御することができます。
Write-buffer	ELS メッセージ・バッファをハード・ディスクに書き込みます。バッファは形式化されてから、書き込まれます。ハード・ディスク上のファイル名は、常に ELSADV.LOG です。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

ELS 監視コマンド (Talk 5)

Flush

flush コマンドは、ログ記録をオフに設定し、バッファからメッセージをクリアし、システムによる他の使用のためにバッファ・メモリーを解放するために使用します。

構文:

```
flush                buffer
```

List

list コマンドは、ELS メッセージ・バッファの構成をリストするのに使用します。

構文:

```
list                  status
```

例:

```
ELS Advanced> list status
-----Configuration-----
Logging Status:  OFF      Wrap Mode:  ON   Logging Buffer Size:  8500 Kytes
Stop-Event:     APPN.2    Stop-String:  netdn for intf 6
Additional Stop-Action:  APPN DUMP
-----Run-Time Status-----
Has Stop Condition Occurred ?   YES      Messages currently in buffer:  1222
```

画面の値を変更するコマンドの説明については、244ページの『Set』を参照してください。

Log

log コマンドは、どのメッセージをメッセージ・バッファに記録するか選択するのに使用します。

構文:

```
log                   event
                        group
                        range
                        subsystem
```

event *subsystem.event#*

指定されたメッセージ (*subsystem.event#*) がメッセージ・バッファに記録されるようにします。

group *groupname*

指定されたグループに以前に追加されたメッセージを、メッセージ・バッファに記録できるようにします。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のメッセージを、メッセージ・バッファに記録します。

例:

```
log range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 のメッセージを、メッセージ・バッファに記録します。

subsystem *subsystemname*

指定されたサブシステムに関連するメッセージを、メッセージ・バッファに記録できるようにします。

Nolog

nolog コマンドは、メッセージ・バッファに記録されたメッセージの定義済みリストからメッセージを除去するのに使用します。

構文:

```
nolog                event
                        group
                        range
                        subsystem
```

event *subsystem.event#*

指定されたメッセージ (*subsystem.event#*) がメッセージ・バッファに記録されないようにします。

group *groupname*

指定されたグループに以前に追加されたメッセージを、メッセージ・バッファに記録されないようにすることができます。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のメッセージを、メッセージ・バッファに記録されないようにします。

例:

```
log range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 のメッセージを、メッセージ・バッファに記録されないようにします。

subsystem *subsystemname*

指定されたサブシステムに関連するメッセージを、メッセージ・バッファに記録できないようにします。

ELS 監視コマンド (Talk 5)

Read-file

read-file コマンドは、**write-buffer** コマンドによって作成された、ハード・ディスク上のファイル `ELSADV.LOG` から、形式化された ELS メッセージを読み取るのに使用します。

注: このコマンドを入力したが、ハード・ディスク が使用可能でない場合、ドライブが使用できないことを示すメッセージが表示されます。

構文:

read-file

Set

set コマンドは、構成済みの ELS メッセージ・バッファ・オプションを変更するのに使用します。

構文:

```
set                logging [on or off]  
                   stop action . . .  
                   stop event subsystem.event#  
                   stop string text  
                   wrap [on or off]
```

logging [on or off]

メッセージ・バッファが行なわれるかどうかを指定します。このコマンドは、**set buffer-size** コマンドを使用してバッファを割り振るまで有効になりません。デフォルトは `off` です。

stop action [**appn-dump** or **disk-offload** or **none** or **system-dump**]

『stop event』(および指定されている場合は、『stop string』)が発生するときにシステムが取る追加のアクションを指定します。アクションは、次のとおりです。

appn-dump

APPN プロトコルがアクティブである場合は、それをダンプします。APPN ダンプは、停止アクションのためダンプが取られたことを示します。

disk-offload

バッファの形式化されたバージョンをハード・ディスク上のファイルに書き込みます。ファイルがすでに存在する場合、新しいファイルがそれにとって代わります。次に、**tftp file** 監視コマンドを使用して、ファイルをリモート・ホストに送信できます。

none ログ記録が停止した後、他のアクションが取られません。

system-dump

システム全体をダンプします。システム・ダンプは、停止アクションのためダンプが取られたことを示します。

デフォルト値: なし

stop event [*subsystem.event#* or **none**]

ログ記録を停止するイベント (*subsystem.event#*) を指定します。停止文字列を指定してある場合は、停止文字列内のテキストも一致する必要があります。停止イベントが発生すると、次のようになります。

1. 次の 5 つの ELS メッセージがログに記録されます。
2. ログ記録が停止します。
3. システムが、指定された『停止アクション』を実行します。

次回に **set logging on** コマンドを出すか、装置がリブートするまで、ログ記録は停止されたままになります。

このコマンドを入力するときに停止イベントを指定しない場合、システムは停止イベントを入力するよう求めます。 **none** を指定すると、停止イベント機能が使用不可にされます。

デフォルト値: なし

stop string *text* or **none**

ログ記録を停止するために、『stop event』とともに使用される文字列を指定します。stop event を指定しなかった場合、システムは『stop string』を無視します。

テキスト は、最大 32 文字の長さの任意の ASCII 文字列にすることができます。このコマンドを入力するときに テキスト を指定しない場合、システムは文字列を入力するよう求めます。 **none** を入力すると、『stop string』はクリアされます。

デフォルト値: なし

wrap [**on** or **off**]

バッファがいっぱいのときにログを停止するかどうか (off)、あるいはバッファの始めに新しいメッセージを記録するかどうか (on) を指定します。

デフォルト値: off

Tftp

tftp コマンドは、ELS メッセージ・バッファを定様式ファイルとしてリモート・ホストに送信するのに使用します。

構文:

```
tftp buffer [formatted ] dest_ip_address dest_filename
      file dest_ip_address dest_filename
```

buffer [formatted] *dest_ip_address dest_filename*

ELS メッセージ・バッファが *dest_ip_address* によって示されるリモート・ホストにファイル *dest_filename* として送信されるよう指定します。バッファは、様式化されていても構いません。

ELS 監視コマンド (Talk 5)

View

view コマンドは、メッセージ・バッファ内のすべてのメッセージまたは特定の数のメッセージを表示するのに使用します。

構文:

```
view                all [scroll/noscroll]  
                    last [scroll/noscroll number]
```

all *scroll/noscroll*

メッセージ・バッファ内のすべてのメッセージを表示します。

[scroll]

スペース・バーを押す前に画面が一時停止するよう指定します。

注: 多数のメッセージを表示している場合は、重要なメッセージを見逃すことがないようにスクロールを指定してください。

noscroll

メッセージの数が画面の長さを超えたら、メッセージがスクロールして画面から消えるよう指定します。

last *scroll/noscroll number*

メッセージ・バッファ内の最後の 数 のメッセージを表示します。

[scroll]

全画面のメッセージが表示した後、画面が一時停止し、ユーザーが次の画面を見るためにスペース・バーを押すのを待つよう指定します。

注: 多数のメッセージを表示している場合は、重要なメッセージを見逃すことがないようにスクロールを指定してください。

noscroll

バッファ内のすべてのメッセージ (または要求される最後のメッセージ数) が表示されるまで、スクロール制御なしにメッセージが連続的にスクロールして画面から消えるよう指定します。

number

1 からメッセージ・バッファ内のメッセージの合計数までの数を指定します。バッファ内のメッセージの合計数を表示するには、**list status** 監視コマンドを使用します。

Write-buffer

write-buffer コマンドは、形式化された ELS メッセージをハード・ディスク に書き込むのに使用します。

注: このコマンドを入力したが、ハード・ディスク が使用可能でない場合、ドライブが使用できないことを示すメッセージが表示されます。

構文:

```
write-buffer
```

第12章 性能の構成および監視

この章では、性能の構成コマンドと監視動作コマンドの使用方法について説明します。本章には、以下の節が含まれています。

- 『性能の概要』
- 『性能報告の正確度』
- 『性能構成環境へのアクセス』
- 248ページの『性能構成コマンド』
- 249ページの『性能監視環境へのアクセス』
- 249ページの『性能監視コマンド』

性能の概要

性能を構成すると、CPU 負荷を監視することができます。アイドル (非作業ロード) 状態では、性能は、装置が外部インターフェースの管理の一部として連続的に実行される運用を反映しています。アイドル状態で登録される CPU ロードは、以下に応じて異なります。

- 実行中のプロトコルの数
- 取り付けられたインターフェース/カードの数
- 取り付けられたインターフェースのタイプ

性能機能は、傾向分析、ボトルネック評価、およびキャパシティー・プランニングのツールとして使用することができます。装置上の CPU 使用率情報を収集することにより、ネットワーク管理プログラムは、以下のことを監視することができます。

- CPU 負荷 対 時刻
- CPU 負荷 対 ネットワーク内の装置の位置
- CPU 負荷 対 トラフィック・スループット
- CPU 負荷 対 ユーザー負荷 (たとえば、TN3270 セッション、ISDN ダイヤルイン・クライアント)

性能報告の正確度

2210 が最初にオンラインになるときに、性能分析を要求する場合、ネットワーク・トラフィックがほとんどまたはまったくない初期設定状態を反映する値が表示されます。したがって、ネットワーク負荷の平衡を取るのを助けようとしても無駄です。

約 2 分間動作した後、通常の負荷のもとで生成される性能報告を使用するのが最善です。

性能構成環境へのアクセス

性能監視構成プロセスにアクセスするには、以下の手順で行います。

1. OPCON プロンプトで、**talk 6** と入力する。(このコマンドの詳細については、47ページの『CONFIG とは』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 configuration と入力したときにこのプロンプトが表示されない場合は、**enter** をもう一度押してください。

2. CONFIG プロンプトで **perf** コマンドを入力して、PERF Config> プロンプトを表示する。

性能構成コマンド

性能を構成するには、PERF Config> プロンプトでコマンドを入力します。

表 26. PERF 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Disable	CPU 使用率統計の収集または Talk 2 ELS モニター出力を使用不可にします。
Enable	CPU 使用率統計の収集または Talk 2 ELS モニター出力を使用可能にします。
List	構成をリストします。
Set	報告期間を設定します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Disable

disable コマンドは、CPU 使用率統計の収集および talk 2 ELS モニター出力を使用不可にするのに使用します。

構文:

```
disable                cpu statistics
                        t2 output
```

Enable

enable コマンドは、CPU 使用率統計の収集および talk 2 ELS モニター出力を使用可能にするのに使用します。

構文:

```
enable                cpu statistics
                        t2 output
```

List

list コマンドは、性能監視構成を表示するのに使用します。

構文:

```
list
```

Set

set コマンドは、報告期間を設定するのに使用します。

構文:

```
set time
```

time ショート・ウィンドウ・タイムを指定します。

有効値: 2 ~ 30 秒

デフォルト値: 2

性能監視環境へのアクセス

性能監視コマンドにアクセスするには、以下の手順で行います。このプロセスにより、性能監視 プロセスにアクセスできます。

1. OPCON プロンプトで、**talk 5** と入力する。(このコマンドの詳細については、149ページの『第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』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、GWCON プロンプト (+) が端末に表示されます。最初に **configuration** と入力したときにこのプロンプトが表示されない場合は、**enter** をもう一度押してください。

2. + プロンプトで **perf** コマンドを入力して、PERF Console> プロンプトを表示する。

例:

```
+ perf
PERF Console>
```

性能監視コマンド

この節では、性能監視コマンドについて説明します。

表 27. PERF 監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Clear	CPU 使用率高水準統計をクリアし、報告期間をリセットして新しいサイクルにします。
Disable	CPU 使用率統計の収集または Talk 2 ELS モニター出力を使用不可にします。

性能監視コマンド (Talk 5)

表 27. *PERF* 監視コマンドの要約 (続き)

コマンド	機能
Enable	CPU 使用率統計の収集または Talk 2 ELS モニター出力を使用可能にします。
List	構成をリストします。
Report	性能統計の報告を表示します。
Set	報告期間を設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Disable

disable コマンドは、CPU 使用率統計の収集および talk 2 ELS モニター出力を使用不可にするのに使用します。

構文:

```
disable                cpu statistics
                        t2 output
```

Enable

enable コマンドは、CPU 使用率統計の収集および talk 2 ELS モニター出力を使用可能にするのに使用します。

構文:

```
enable                 cpu statistics
                        t2 output
```

List

list コマンドは、性能監視構成を表示するのに使用します。

構文:

```
list
```

Report

report コマンドは、性能監視統計を表示するのに使用します。

構文:

```
report
```

例:

```
PERF Console>report
-----
KEY: SW = Short Window = 9 seconds
KEY: LW = Long Window = 9.0 minutes (60 x SW)

CPU UTIL :  Most recent SW           = 38%
            Most recent LW           = 33%
            Highest for all SW's     = 92%
            Highest for all LW's     = 52%
            % of time cpu util (SW) was > 60% = 16%
            % of time cpu util (SW) was > 70% = 15%
            % of time cpu util (SW) was > 80% = 1%
```

```
% of time cpu util (SW) was > 90% = 0%  
% of time cpu util (SW) was > 95% = 0%
```

Set

set コマンドは、報告期間を設定するのに使用します。

構文:

set *time*

time ショート・ウィンドウ・タイムを指定します。

有効値: 2 ~ 30 秒

デフォルト値: 2

性能監視コマンド (Talk 5)

第3部 インターフェースの概要、構成、および動作

第13章 ネットワーク・インターフェースの開始

この章では、ルーターによってサポート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・プロトコルの構成と監視の方法について説明します。この章の目的は、いくつかの基本的な構成と監視に関するガイドラインを示すことです。また、GWCON **interface** コマンドを用いてインターフェースを監視するのに必要な基本的な手順および情報も提供します。本章には、以下の節が含まれています。

- 『先に進む前に』
- 『ネットワーク・インターフェースと GWCON インターフェース・コマンド』
- 『ネットワーク・インターフェースの構成プロセスおよびコンソール・プロセスへのアクセス』
- 256ページの『リンク・レイヤー・プロトコルの構成プロセスおよびコンソール・プロセスへのアクセス』
- 256ページの『予備インターフェースの定義』

先に進む前に

先に進む前に、ネットワーク・インターフェース構成プロセスにアクセスするのに必要な手順を十分に理解しておいてください。

これらの手順についての詳しい情報は、本章の以下の節を参照してください。

ネットワーク・インターフェースと GWCON インターフェース・コマンド

ネットワーク・インターフェースの構成時に、特定のインターフェースについての特定の情報を表示することが必要になる場合があります。一部のインターフェースは、それぞれ独自の監視用コンソール・プロセスを備えています。GWCON 環境から **interface** コマンドを使用すると、ルーターはすべての 導入済みのネットワーク・インターフェースの統計を表示します。(158ページの『Interface』を参照してください。)

ネットワーク・インターフェースの構成プロセスおよびコンソール・プロセスへのアクセス

以下に示す参照箇所には、背景情報と、インターフェースの構成プロンプトおよびコンソール・プロンプトにアクセスする方法の例が示されています。

インターフェースの構成プロセスおよびコンソール・プロセスへのアクセスに関する詳しい情報は、18ページの『装置の追加』、19ページの『ネットワーク・インターフェース構成プロセスへのアクセス』、および 23ページの『ネットワーク・インターフェース・コンソール・プロセスへのアクセス』を参照してください。これらの

ネットワーク・インターフェースの開始

プロセスにアクセスすると、ルーターで使用されているネットワーク・インターフェースのソフトウェア構成可能パラメーターの変更や監視を行うことができます。

リンク・レイヤー・プロトコルの構成プロセスおよびコンソール・プロセスへのアクセス

プロトコルの構成プロセスおよびコンソール・プロセスへのアクセスについての詳しい情報は、3ページの『第1章 開始』を参照してください。これらのプロセスにアクセスすると、ルーターによってサポートされているリンク・レイヤー・プロトコルの構成可能パラメーターの変更や監視を行うことができます。

予備インターフェースの定義

装置上に現在は存在していないインターフェースを定義することが必要になる場合があります。装置のこの**動的再構成**は、装置を構成する際に予備インターフェースを定義しておき、装置が存在するようになったときに、コンソール・プロセスを使用して起動する方法で行います。詳しくは、50ページの『予備インターフェースの構成』および150ページの『Activate』を参照してください。

第14章 IEEE 802.5 トークンリング・ネットワーク・インターフェースの構成

この章では、トークンリング・インターフェースの構成コマンドとオペレーショナル・コマンドについて説明します。本章には、以下の節が含まれています。

- 『トークンリング・インターフェース構成プロセスへのアクセス』
- 『トークンリング構成コマンド』
- 261ページの『インターフェース監視プロセスへのアクセス』
- 261ページの『トークンリング・インターフェース監視コマンド』
- 263ページの『トークンリング・インターフェースと GWCON インターフェース・コマンド』

トークンリング・インターフェース構成プロセスへのアクセス

TKR config> プロンプトを表示するには、network コマンドに続けて、トークンリング・インターフェースのインターフェース番号を入力します。たとえば、次のように入力します。

```
Config>network 0
Token-Ring interface configuration
TKR Config>
```

Config> プロンプトで **list devices** コマンドを使用すると、ルーター上に構成されているインターフェース番号のリストを表示することができます。

注: パラメーターを変更した場合は、必ずルーターをリスタートして、その変更を有効にする必要があります。

トークンリング構成コマンド

この節では、トークンリング構成コマンドについて説明します。コマンドは TKR config> プロンプトで入力します。表28 は、トークンリング構成コマンドをリストしています。

表 28. トークンリング構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13 ページの『ヘルプの入手』を参照してください。
List	選択されたトークンリング・インターフェース構成を表示します。
LLC	LLC 構成環境およびサブコマンドにアクセスします。
Media	媒体タイプを shielded (シールド付き) または unshielded (シールドなし) として設定します。
Packet-size	すべてのトークンリング・ネットワークのパケット・サイズのデフォルト値を変更します。
Set	RIF キャッシュの経時タイマーおよび物理 (MAC) アドレスを設定します。全二重または半二重の動作モードも設定します。

トークンリング・ネットワーク・インターフェースの構成

表 28. トークンリング構成コマンドの要約 (続き)

コマンド	機能
Source-routing	インターフェース上のソース・ルーティングを使用可能または使用不可にします。
Speed	インターフェースの速度を Mbps 単位で設定します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、トークンリングの現行構成を表示するのに使用します。

注: MAC アドレスが 0 のときは、デフォルトの端末アドレスが使用されます。

構文:

list

例:

```
list
Token-Ring configuration:

    Packet size (INFO field): 2052
Speed:                        16 Mb/sec
Media:                        Shielded

RIF Aging Timer:             120
Source Routing:               Enabled
MAC Address:                  000000000000
```

Packet size

トークンリング・パケットのサイズ

Speed ネットワークの速度

Media ネットワークが使用する媒体のタイプ (シールド付きまたはシールドなし)

RIF Aging Timer

ルーティング情報フィールド (RIF) に入っている情報をルーターが保持する時間の長さ

Source Routing

ソース・ルーティング・フィーチャーの状態 (使用可能または使用不可)。

MAC Address

set physical-address コマンドを用いて設定した、構成済みの MAC アドレス。オール 0 が表示された場合、その MAC アドレスはデフォルト・アドレスです。

LLC

LLC コマンドは、LLC 構成環境にアクセスするのに使用します。各コマンドについての説明は、267ページの『LLC 構成コマンド』を参照してください。

構文:

llc

トークンリング・ネットワーク・インターフェースの構成

注: ルーター・ソフトウェア・ロードに APPN が含まれていない場合、このコマンドを使用しようとすると、次のようなメッセージを受け取ります。

```
LLC configuration is not available for this network.
```

LLC 構成環境は、ソフトウェア・ロードに APPN が含まれている場合にのみ利用可能です。

Media

media コマンドは、ネットワーク媒体タイプを変更するのに使用します。デフォルトの媒体タイプは STP ケーブルです。有効な媒体タイプ値は shielded (シールド付き) および unshielded (シールドなし) です。 **media** コマンドに続けて、*media-type* を入力します。

構文:

```
media                               media-type
```

例:

```
media unshielded
```

Packet-Size

packet-size コマンドは、すべてのトークンリング・ネットワークの最大パケット・サイズを変更するのに使用します。 **packet-size** コマンドの後に、必要なバイト数を入力します。

構文:

```
packet-size                          bytes
```

表 29. トークンリング 4/16 の有効なパケット・サイズ

ネットワーク・データ速度	値 (バイト数)
4 Mbps	516 ~ 4498 注: 4 Mb TR に対して 4498 より大きい値が定義されている場合、ソフトウェアはそれを 4498 に設定します。ユーザーが値を指定しない場合は、デフォルト値の 2052 になります。
16 Mbps	516 ~ 18144 注: 値を指定しない場合は、デフォルト値の 2052 になります。

注: パケット・サイズが大きくなると、バッファのメモリ所要量が増えます。

Set

set コマンドは、ルーティング情報フィールド (RIF) タイマーおよび物理 (MAC) アドレスを設定するのに使用します。

構文:

```
set                               physical-address  
                                   rif-timer
```

トークンリング・ネットワーク・インターフェースの構成

physical-address

トークンリング・インターフェースの MAC サブレイヤー・アドレスにローカル管理アドレスを定義するか、あるいは工場出荷時のデフォルトの端末アドレス (オール 0 で示される) を使用するかを指示します。MAC サブレイヤー・アドレスは、トークンリング・インターフェースがフレームの送受信に使用するアドレスです。

注: **Return** を押すと、値はそのままです。 **0** を入力して **Return** を押すと、ルーターは工場出荷時の端末アドレスを使用します。デフォルトでは、工場出荷時の端末アドレスを使用します。

有効値: 任意の 12 桁の 16 進アドレス

デフォルト値: 刻印されたアドレス (オール 0 で示されます)

例:

```
set physical-address
MAC address in 00:00:00:00:00:00 form []?
```

rif-timer

RIF 内の情報が更新される前に維持されている最大時間 (秒数) を設定します。デフォルト値は 120 です。

例:

```
set rif-timer
RIF aging timer value [120]? 120
```

Source-routing

source-routing コマンドは、端末ステーションのソース・ルーティングを使用可能または使用不可にするのに使用します。ソース・ルーティングというのは、エンド・ステーションがソース・ルーティング・ブリッジを経由するのに使用するソース・ルートを決めるプロセスです。ソース・ルーティングにより、IP、IPX、および AppleTalk フェーズ 2 プロトコルは、ソース・ルーティング・ブリッジの反対側のノードに到達することが可能になります。

このスイッチは完全に独立しており、このインターフェースが SRT 転送機能を介してソース・ルーティングを提供しているかどうかとは無関係です。デフォルトの設定値は「使用可能」です。

一部のステーションでは、ソース・ルーティング RIF をもつフレームを正常に受信できません。これは特に NetWare ドライバーに共通に見られる特徴です。この状態のときは、ソース・ルーティングを使用不可にすれば、これらのステーションと通信できるようになります。

IP、IPX、および AppleTalk フェーズ 2 パケットを通過させたいソース・ルーティング・ブリッジがこのリング上に存在する場合だけ、ソース・ルーティングを使用可能にします。また、LLC テスト応答メッセージを戻すようにしたい場合にも、ソース・ルーティングを使用可能にする必要があります。

構文:

```
source-routing enable
```

disable

speed

speed コマンドは、データ速度を変更するのに使用します。デフォルトの速度は、4 Mbps です。**speed** コマンドの後に速度値 (Mbps 単位) を入力します。

構文:

speed *speed-value*

speed-value

トークンリング・インターフェースを設定している速度

有効値: 4 または 16 Mbps

デフォルト値: 4 Mbps

インターフェース監視プロセスへのアクセス

トークンリング監視プロンプト (TKR>) を表示するには、**network** コマンドに続けて、トークンリング・インターフェースのインターフェース番号を入力します。たとえば、次のように入力します。

```
+network 0
TKR>
```

Config> プロンプトで **list devices** コマンドを使用すると、ルーター上に構成されているインターフェース番号のリストを表示することができます。

19ページの『ネットワーク・インターフェース構成プロセスへのアクセス』で説明されている手順に従って、本章で説明するインターフェースのインターフェース監視プロセスにアクセスします。必要なインターフェース監視プロセスにアクセスしたら、監視コマンドの入力を開始することができます。

トークンリング・インターフェース監視コマンド

この節では、トークンリング監視コマンドの要約を示します。コマンドは TKR> 監視プロンプトで入力します。表30 は、監視コマンドをリストしています。

表 30. トークンリング監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Dump	RIF キャッシュのダンプを表示します。
LLC	LLC 監視プロンプトを表示します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

トークンリング・ネットワーク・インターフェースの構成

Dump

tkr config> プロセスでソース・ルーティングが使用可能にされている場合、**dump** コマンドを使用して、RIF キャッシュの内容のダンプを要求することができます。

構文:

dump

例:

```
dump
MAC address      State      Usage      RIF
0000C90B1A57    ON_RING    Yes        0220
```

MAC address

トークンリングの MAC アドレスを表示します。

State インターフェースの状態の 1 つを表示します。

On_ring - そのリング上のノードの RIF が見つかったことを示します。

Have_route - リモート・リング上のノードの RIF が見つかったことを示しています。

No_route - 探索フレームが送信され、ルーターが戻りを待っている間、短時間表示されます。

Discovering - RIF を再発見するためにルーターが探索フレームを送信したことを示しています。

St_route - スパニング・ツリー探索からルートが得られたことを示しません。

Usage パケット内で RIF が使用されたことを示します。番号は任意で、機能上の意味はありません。

RIF RIF を示すコードを 16 進数で表示します。

注: RIF は、トークンリング・インターフェース上でソース・ルート・ブリッジングが使用可能にされている場合にのみ表示されます。

- NetBIOS RIF データは、次のコマンド・シーケンスを使用して表示することができます: **talk 5, protocol ASRT, name-caching, list cache rifs**。
- データ・リンク交換 RIF データは、次のコマンド・シーケンスを使用して表示することができます: **talk 5, protocol dlsw, list llc2 session all**。

LLC

LLC コマンドは、LLC 監視プロンプトにアクセスするのに使用します。LLC コマンドは、この新たに表示されたプロンプトで入力します。各コマンドについての説明は、271ページの『LLC 監視コマンド』を参照してください。

構文:

llc

トークンリング・インターフェースと GWCON インターフェース・コマンド

トークンリング・インターフェースには独自の監視用コンソール・プロセスがありますが、GWCON 環境から **interface** コマンドを使用すると、ルーターも導入済みのネットワーク・インターフェースの統計を表示します。

802.5 トークンリング・インターフェースについて表示される統計

GWCON 環境からトークンリング・インターフェースに対して **interface <net#>** コマンドを入力すると、以下の統計が表示されます。

```

Nt Nt' Interface Slot-Port Self-Test Self-Test Maintenance
0 0 TKR/0 Slot: 1 Port: 1 Passed Failed Failed
                                1 0 0

```

Token-Ring/802.5 MAC/data-link on Token-Ring interface

```

Physical address      08005AFE0106
Microcode Level      ww19cg
Network speed        16 Mbps
Max packet size (INFO) 2052
Handler state        Ring open
Last Reported Ring status SERR | CO
# times Signal lost  0 # times Beaconsing      0
Hard errors          0 Lobe wire faults      0
Auto-removal errors  0 Removes received     0
Ring recovery actions 0
Line errors          0 Burst errors          0
ARI/FCI errors      0 Inputs dropped       0
Frame copy errors    0 Token errors         0
Lost frames          0
Input overflows      0 Driver output errors 0

```

以下では、一般的なインターフェース統計について説明します。

Nt グローバル・インターフェース番号

Nt' ダイヤル回線にのみ適用されます。

Interface

タイプ『intrfc』のインターフェース内のこのインターフェースのインターフェース名と番号

Port ポート番号

Slot スロット番号

Self-Test: Pass

成功した自己テストの回数

Self-Test: Fail

失敗した自己テストの回数

Maint: Fail

保守障害の数

以下では、トークンリング・インターフェースに特有の統計を説明します。

Physical address

トークンリング・インターフェースの物理アドレスを指定します。

GWCON インターフェース・コマンドの使用

Network speed

インターフェースに接続しているトークンリング・ネットワークの速度を指定します。ネットワーク速度カウンターは、インターフェースが毎秒通過させることができるパケット数を表示します。

Max packet size (info)

そのインターフェースに構成された最大パケット・サイズを表示します。最大パケット・サイズ・カウンターは、インターフェースが送信または受信できるパケットの最大長さ (バイト数) を表示します。このカウンターは、ユーザーが定義します。

Handler state

トークンリング・ハンドラーの現行状態を表示します。ハンドラー状態カウンターは、自己テストの実行後のハンドラーの状態を示します。

Last Reported Ring status

トークンリング・インターフェースの最後のリング状態

SIGL SIGNAL_LOSS インターフェースはリング上で信号の損失を検出しました。

HERR HARD_ERROR インターフェースは現在リング上でビーコン・フレームを送信または受信中です。

SERR SOFT_ERROR インターフェースは報告エラー MAC フレームを転送しました。

BEAC TRANSMIT_BEACON インターフェースはリングへ (または、リングからの) ビーコン・フレームを転送中です。

LWF LOBE_WIRE_FAULT インターフェースは、インターフェースと集線装置の間のケーブルで回線の開きまたは短絡を検出しました。インターフェースはクローズされ、初期化後の状態になっています。

ARMV AUTO_REMOVAL_ERROR インターフェースは、ローブ折り返しテストに失敗し (ビーコン自動除去プロセスの結果として)、自動的にリングから除去されました。インターフェースはクローズされ、初期化後の状態になっています。

RMVD REMOVED_RECEIVED インターフェースはリング・ステーション除去 MAC フレーム要求を受信し、自動的にリングから除去されました。インターフェースはクローズされ、初期化後の状態になっています。

CO COUNTER_OVERFLOW 次のエラー・カウンターの 1 つが 254 から 255 に増分されました。Line, ARI/FCI, Frame Copy, Lost Frames, Burst, Lobe wire faults, Removes received。このディスプレイは、これらのエラー・カウンターを表示します。

SSTA SINGLE_STATION インターフェースは、それがリング上の唯一のステーションであることを検出しました。

RR RING_RECOVERY インターフェースは、リング上でトークン請求 MAC フレームを監視します。インターフェースはトークン請求フレームを送信している可能性があります。この状態は、インターフェースがリング除去フレームを送信するまで残ります。

of times signal lost

信号の損失のためにルーターがパケットを転送できなかった合計回数を指定します。

Hard errors

インターフェースがネットワークからビーコン・フレームを送受した回数を表示します。

Auto-removal errors

ビーコン自動除去プロセスが原因で、インターフェースがローブ折り返しテストに失敗し、自動的にネットワークから除去された回数を表示します。

Ring recovery actions

インターフェースがネットワークでトークン請求媒体アクセス制御 (MAC) フレームを検出した回数を表示します。

Line errors

フレームが反復またはコピーされ、着信フレームのエラー検出標識 (EDI) がゼロのときに増分されます。

さらに、以下の条件の 1 つも存在している必要があります。

- コード違反のトークンが存在する。
- フレームの開始区切り文字と終了区切り文字の間にコード違反がある。
- フレーム検査シーケンス (FCS) エラーが発生している。

ARI/FCI errors

ARI/FCI (アドレス認知標識/フレーム複写標識) エラー・カウンターは、インターフェースが次のいずれかを受信すると増分します。

ARI/FCI ビットがゼロに等しいアクティブ・モニター・プレゼント (AMP) MAC フレームと、ARI/FCI ビットがゼロに等しい待機モニター・プレゼント (SMP) MAC フレーム。

AMP MAC フレームが介在しない、ARI/FCI ビットがゼロに等しい複数の SMP MAC フレーム。

このエラーは、アップストリーム近隣がフレームをコピーしたが、ARI/FCI ビットをセットできないことを示しています。

Frame copy errors

受信/反復モードのインターフェースが特定のアドレスにアドレス指定されたフレームを認識したが、そのアドレス認識標識 (ARI) ビットがゼロでないことを発見した回数を表示します。このエラーは、回線ヒットまたは重複アドレスの可能性を示します。

Lost frames

インターフェースが送信モード (除去) にあり、送信フレームの終了を受信できなかった回数を表示します。

Input overflows

受信され、入力バッファ・サイズより大きかったフレーム数を指定します。単一の入力バッファに入れるには大き過ぎるフレームは廃棄されません。

times beaconing

インターフェースがビーコン・フレームをネットワークに送信した回数を表示します。

GWCON インターフェース・コマンドの使用

Lobe wire faults

インターフェースが、インターフェースと集線装置の間のケーブルに回線の開きまたは短絡を検出した回数を表示します。

Removes received

インターフェースがリング・ステーション除去 MAC フレーム要求を受信し、自動的にネットワークから除去された回数を表示します。

Burst errors

インターフェースが、開始区切り文字 (SDEL) と終了区切り文字 (EDEL) の間、あるいは EDEL と SDEL の間で、5 回の半ビット期間に変換がなかったことを検出した回数を表示します。

Inputs dropped

反復モードにあるインターフェースが、自身のアドレス宛てのフレームを認知したが、利用可能なバッファ・スペースがないためにフレームをコピーできなかった回数を表示します。

Token errors

トークン・エラー・カウンターは、アクティブ・モニターが以下のいずれかのエラーをもつトークン・プロトコルを検出すると増分されます。

非ゼロの優先順位をもつトークンの MONITOR_COUNT ビットが 1 に等しい。

フレームの MONITOR_COUNT ビットが 1 に等しい。10-ms ウィンドウ以内にトークンまたはフレームを受信していません。

開始区切り文字/トークンのシーケンスの、コード違反が存在してはならない区域にコード違反がある。

第15章 LLC インターフェースの構成および監視

この章では、インターフェース・コマンドまたは GWCON インターフェース・コマンドを使用して、ルーター内の特定の LLC インターフェースを構成する方法について説明します。

論理リンク・レベルは『サブプロトコル』と考えることができます。Talk 6 (構成) または Talk 5 (監視) 環境から直接アクセスすることはできません。代わりに、**LLC** コマンドを入力して、トークンリング、ポイント・ポイント (PPP)、またはフレーム・リレー・プロトコルからアクセスします。

本章には、以下の節が含まれています。

- 『インターフェース構成プロセスへのアクセス』
- 271ページの『インターフェース監視プロセスへのアクセス』
- 271ページの『LLC 監視コマンド』
- 『LLC 構成コマンド』

インターフェース構成プロセスへのアクセス

LLC を介して構成するプロトコルの構成コマンドにアクセスするには、次のようになります。

- トークンリングの場合は、257ページの『第14章 IEEE 802.5 トークンリング・ネットワーク・インターフェースの構成』の説明に従います。
- ポイント・ポイントの場合は、519ページの『第30章 ポイント・ポイント・プロトコル・インターフェースの使用』の説明に従います。
- フレーム・リレーの場合は、443ページの『第28章 フレーム・リレー・インターフェースの使用』の説明に従います。
- FDDI の場合は、の説明に従います。

これらのプロンプト・レベルのそれぞれに LLC コマンドがあります。 **LLC** と入力して LLC 構成コマンドにアクセスし、LLC を構成します。終了したら、**Exit** と入力して、構成しているプロトコルのプロンプト・レベルに戻ります。

LLC 構成コマンド

SNA ネットワークを介してパケットを渡す必要がある場合、LLC の構成が必要です。これらのコマンドを入力するには、最初に LLC 構成環境に入る必要があります (257ページの『トークンリング・インターフェース構成プロセスへのアクセス』を参照してください。)

この節では、すべての LLC 構成コマンドの要約を示し、その後で個々のコマンドについて説明します。268ページの表31 に示されているこれらのコマンドを使用すると、SNA ネットワークを介してパケットを渡す必要がある場合に、LLC を構成することができます。

LLC の構成

表 31. LLC 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
List	選択された LLC 構成を表示します。
Set	LLC に関連したタイマーと、送信および受信ウィンドウのサイズを設定します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、LLC の現行構成を表示するのに使用します。

構文:

list

例:

```
list
Reply Timer (T1):          1 seconds
Receive ACK Timer (T2):    100 milliseconds
Inactivity Timer (Ti):     30 seconds
Max Retry value (N2):      8
Rcvd I-frames before ACK (N3): 1
Transmit Window (Tw):     2
Receive Window (Rw):      2
Acks needed to increment Ww (Nw): 1
```

Reply Timer (T1)

このタイマーは、LLC が相手側の LLC ステーションから必要な確認またはレスポンスを受信できないと満了します。

Receive ACK Timer (T2)

このタイマーは、受信 I フォーマット・フレームの確認の送信を遅らせるのに使用します。

Inactivity Timer (Ti)

このタイマーは、指定された期間に LLC がフレームを受信しないと満了します。このタイマーが満了すると、相手側の LLC が応答するか、N2 再試行カウントを超えるまで、LLC は RR を送信します。デフォルト値は 30 秒。

Max Retry value (N2)

LLC プロトコルによる最大再試行数。デフォルト値は 8。

Rcvd I-frames before ACK (N3)

この値は、T2 タイマーと合わせて、受信 I フレームの確認応答トラフィックを削減するのに使用されます。このカウンターは、指定された値にセットされ、I フレームを受信するたびに減分されます。このカウンターが 0 に達するか、T2 タイマーが満了すると、確認応答が送信されます。デフォルト値は 1。

Receive Window (Rw)

LLC がリモート・ホストから受信できる、未確認のシーケンス番号付き I フレームの最大数を示します。

Transmit Window (Tw)

RR を受信する前に送信できる I フレームの最大数を示します。

Acks needed to increment Ww (Nw)

このフィールドは、デフォルト値の 1 に設定します。

Set

set コマンドは、LLC を構成するのに使用します。

重要: LLC パラメーターをデフォルト値から変更すると、LLC プロトコルの動作方法に影響を与える可能性があります。

構文:

```
set                n2-max-retry count
                   n3-frames-rcvd-before-ack count
                   nw-acks-to-inc-window count
                   rw-receive-window count
                   t1-reply-timer seconds
                   t2-receive-ack-timer seconds
                   ti-inactivity-timer seconds
                   tw-transmit-window count
```

n2-max-retry

LLC プロトコルによる再試行の最大数。たとえば、N2 は、非活動タイマーが満了したときに、LLC が確認応答を受信せずに RR を送信する最大回数です。デフォルト値は 8。最小値は 1。最大値は 127。

例:

```
set n2-max-retry
Max Retry value (N2) [8]?
```

n3-frames_rcvd-before-ack

この値は、T2 タイマーと合わせて、受信 I フレームの確認応答トラフィックを削減するのに使用されます。このカウンターは、指定された値に設定します。I フレームを受信するたびに、この値が減分します。このカウンターが 0 に達するか、T2 タイマーが満了すると、確認応答が送信されます。デフォルト値は 1。最小値は 1。最大値は 255。

例:

```
set n3-frames_rcvd-before-ack
Number I-frames received before sending ACK(N3) [1]?
```

rw-receive-window

LLC がリモート LLC ピアから受信できる未確認のシーケンス番号付き I フレームの最大数を示します。この値は 127 以下でなければなりません。

例:

```
set rw-receive-window
Receive Window (Rw), 127 Max. [2]?
```

nw-acks-to-inc-ww

このフィールドは、デフォルト値の 1 に設定します。

t1-reply-timer

このタイマーは、LLC が相手側の LLC ステーションから必要な確認またはレスポンスを受信できないと満了します。このタイマーが満了すると、ポーリング・ビットをセットして RR が送信され、T1 が再びスタートします。LLC が構成された再試行最大数 (N2) の後もレスポンスを受信しない場合、基礎リンクは動作不能として宣言されます。デフォルト値は 1。最小値は 1。最大値は 256。

例:

```
set t1-reply-timer
Reply Timer (T1) in sec. [1]?
```

t2-receive-ack-timer

このタイマーは、受信 I フォーマット・フレームの確認の送信を遅らせるのに使用します。このタイマーは、I フレームを受信するスタートします。確認が送信されると、タイマーはリセットされます。このタイマーが満了すると、LLC2 はできるだけ速やかに確認を送信します。この値は、T1 の値より小さくなるように設定します。これにより、T1 タイマーが満了する前に、リモート LLC2 ピアが遅らせた確認を確実に受信できるようになります。デフォルト値は 1 (100 ミリ秒)。最小値は 1。最大値は 2560。

例:

```
set t2-receive-ack-timer
Receive Ack timer (T2) in 100 millisec. [1]?
```

注: このタイマーが 1 (デフォルト値) に設定されている場合、タイマーは動作しません (たとえば、**n3-frames_rcvd-before-ack=1**)。

ti-inactivity-timer

このタイマーは、指定された期間に LLC がフレームを受信しないと満了します。このタイマーが満了すると、相手側の LLC が応答するか、N2 再試行カウントを超えるまで、LLC は RR を送信します。デフォルト値は 30 秒。最小値は 1 秒。最大値は 256 秒。

例:

```
set ti-inactivity-timer
Inactivity Timer (Ti) in sec. [30]?
```

tw-transmit-window

RR を受信する前に送信できる I フレームの最大数を示します。相手側の LLC セッションが実際にこの数の連続 I フレームを受信することが可能であり、しかもルーターに確認を受信するまでこれらのフレームのコピーを保持できる十分なヒープ・メモリーがあると仮定した場合、この値を大きくすると、スループットが向上します。デフォルト値は 2。最小値は 1。最大値は 127。

例:

```
set tw-transmit-window
Transmit Window (Tw), 127 Max. [2]?
```


インターフェース監視プロセスへのアクセス

LLC を介して監視するプロトコルの監視コマンドにアクセスするには、次のようにします。

- トークンリングの場合は、257ページの『第14章 IEEE 802.5 トークンリング・ネットワーク・インターフェースの構成』の説明に従います。
- ポイント・ポイント場合は、539ページの『第31章 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』の説明に従います。
- フレーム・リレー場合は、465ページの『第29章 フレーム・リレー・インターフェースの構成および監視』の説明に従います。
- FDDI の場合は、の説明に従います。

これらのプロンプト・レベルのそれぞれに LLC コマンドがあります。 **LLC** と入力して、LLC を監視するための LLC 監視コマンドにアクセスします。終了したら、**Exit** と入力して、監視しているプロトコルのプロンプト・レベルに戻ります。

LLC 監視コマンド

この節では、すべての LLC 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32 に示されるこれらのコマンドを使用すると、SNA ネットワークを介してパケットを渡している間 LLC を監視することができます。

表 32. LLC 監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Clear-counters	すべての統計カウンターを消去します。
List	インターフェース、SAP、およびセッション情報を表示します。
Set	セッションの存続期間中だけ有効な LLC パラメーターを動的に構成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。13ページの『下位レベル環境の終了』を参照してください。

Clear-Counters

clear-counters コマンドは、すべての LLC 統計カウンターをクリアするのに使用します。

構文:

clear-counters

List

list コマンドは、インターフェース、サービス・アクセス・ポイント (SAP)、およびセッション情報を表示するのに使用します。

構文:

```
list interface
sap . . .
session
```

interface

このインターフェース上のすべてのオープンしている SAP を表示します。

例:

```
list interface
SAP      Number of Sessions
F4       1
```

sap sap_number

そのインターフェース上の指定された SAP の情報を表示します。

例:

```
list sap
SAP value in hex (0FE) [1]? F4

Interface          0, TKR/0
Reply Timer(T1)    1 sec
Receive ACK Timer (T2) 100 millisec
Inactivity Timer (Ti) 30 sec
MAX Retry Value (N2) 8
MAX I-field Size (N1) 2052
Rcvd I-frames before ACK (N3) 1
Transmit Window Size (Tw) 2
Acks Needed to Inc Ww (Nw) 1

Frame              Xmt   Rcvd
UI-frames          4     5
TEST-frames        0     1
XID-frames         0     0
I-frames           291   26
RR-frames          81    291
RNR-frames         0     0
REJ-frames         0     0
SABME-frames       1     0
UA-frames          0     1
DISC-frames        0     0
DM-frames          0     0
FRMR-frames        0     0
I-frames discarded by LLC 0
I-frames Refused by LLC user 0

Cumulative number of sessions 1
Number of active sessions     1

Session ID          Remote
(int-sap-id) Local MAC Remote MAC SAP State
00F40000 00:00:C9:08:41:DB 10:00:5A:F1:02:37 F4 OPENED
```

SAP value in hex (0FE)

そのセッションの SAP 値

Interface

セッションが使用するインターフェースの番号とタイプ

Reply Timer (T1)

LLC が他の LLC ステーションから確認応答またはレスポンスを受信しなかった場合、このタイマーが満了するまでにかかる時間を示します。

Receive ACK Timer (T2)

LLC が受信した I フレームに対する確認応答を送信する前に使用する時間遅延を示します。

Inactivity Timer (Ti)

RR を出す前の非アクティブ時に LLC が待機する時間を示します。

MAX Retry Value (N2)

LLC プロトコルによる最大再試行数

MAX I-field Size (N1)

LLC2 フレームの I フィールドに入れられるデータの最大量 (バイト数)

Rcvd I-frame before ACK (N3)

受信した I フレームに対する確認応答トラフィックを減らすために、T2 タイマーとともに使用される値を示します。

Transmit Window Size (Tw)

RR を受信する前に送信できる I フレームの最大数を示します。

Acks Needed to Inc Ww (Nw)

このフィールドは、デフォルト値の 1 に設定します。

Frames Xmt and Rcvd

転送された (Xmt) および (Rcvd) フレーム・タイプの合計数を表示するカウンター

I-frames discarded by LLC

LLC によって廃棄された (通常は、シーケンス番号が順序通りでないという理由で) I フレームの合計数を表示するカウンター

I-frames refused by LLC user

LLC の上位ソフトウェアによって廃棄された I フレーム数を示すカウンター。たとえば、DLSw (データ・リンク交換)

Cumulative number of sessions

この SAP を介してオープンされたセッションの合計数

Number of active sessions

インターフェース上で実行されている現在アクティブのセッションの合計数

Session ID (int-sap-id)

監視しているインターフェースのセッション ID

Local MAC

ルーターの LLC MAC アドレス

Remote MAC

リモート LLC の MAC アドレス

Remote SAP

LLC 接続のリモート SAP

Remote State

LLC ピア間のインタラクションの結果としての有限状態。以下に説明する 21 の状態があります。

Link_Closed

リモート LLC ピアがローカル LLC ピアに認知されず、存在しないものと見なされます。

Disconnected

ローカル LLC ピアは、相手側に認知されています。この LLC ピアは、

LLC の監視

XID、TEST、SABME、および DISC コマンド、XID TEST、UA、および DM レスポンスを送受信することができます。

Link_Opening

受信した SABME に応答して SABME または UA を送信した後のローカル LLC ピアの状態

Disconnecting

DISC コマンドをリモート LLC ピアに送信した後のローカル LLC の状態

FRMR_Sent

ローカル LLC ピアは、フレーム・リジェクト例外状態に入り、リンクを介して FRMR レスポンスを送信しました。

Link_Opened

ローカル LLC ピアは、データ転送フェーズにあります。

Local_Busy

ローカル LLC ピアは、追加の I フレームを受信できません。

Rejection

ローカル LLC ピアが、1 つまたは複数のシーケンス誤り I フレームを受信しました。

Checkpointing

ローカル LLC ピアは、リモート LLC ピアにポーリングを送信し、適切なレスポンスを待っています。

CKPT_LB

checkpointing 状態と local busy 状態の組み合わせ

CKPT_REJ

checkpointing 状態と rejection 状態の組み合わせ

Resetting

ローカル LLC ピアは SABME を受信し、リンクを再確立中です。

Remote_Busy

リモート LLC ピアから RNR を受信したときに生じる状態

LB_RB

local_busy 状態と remote_busy 状態の組み合わせ

REJ_LB

rejection 状態と local_busy 状態の組み合わせ

REJ_RB

rejection 状態と remote_busy 状態の組み合わせ

CKPT_REJ_LB

checkpointing、rejection、および local_busy 状態の組み合わせ

CKPT_CLR

LLC ピアが CKPT_LB の間に local_busy 状態が終了した結果生じた組み合わせ状態

CKPT_REJ_CLR

リンク・ステーションが CKPT_REJ_LB 状態にあるときに未確認ローカル・ビジー・クリアが転送された結果生じた組み合わせ状態

REJ_LB_RB

rejection、local_busy、および remote_busy 状態の組み合わせ

FRMR_Received

ローカル LLC ピアは、リモート LLC ピアから FRMR レスポンスを受信しました。

Session

インターフェース上でオープンしている指定の LLC セッションに関する情報を表示します。

例:

```
list session
Session Id: [0]? 00-F4-0000

Interface0,           TKR/0
Remote MAC addr      10:00:5A:F1:02:37
Source MAC addr      00:00:C9:08:35:47
Remote SAP           F4
Local SAP            F4
RIF                  (089E 0101 0022 0010)
Access Priority       0
State                LINK_OPENED
Replay Timer         1 sec
Receive ACK Timer (T2) 100 millisec
Inactivity Timer (Ti) 30 sec
MAX I-field Size (N1) 2052
MAX Retry Value (N2) 8
Rcvd I-frames before ACK (N3) 1
Transmit Window Size (Tw) 2
Working Transmit Size (Ww) 2
Acks Needed to Inc Ww (Nw) 1
Current Send Seq (Vs) 9
Current Rcv Seq (Vr) 7
Last ACK'd sent frame (Va) 9
No. of frames in ACK pend q 0
No. of frames in Tx pend q 0
Local Busy           NO
Remote Busy          NO
Poll Retry count     8
Appl output flow stopped NO
Send process running YES

Frame                Xmt   Rcvd
I-frames             1456  2678
RR-frames            502   403
RNR-frames           0     0
REJ-frames           0     0
I-frames discarded by LLC 0
I-frames Refused by LLC user 0
```

Session Id

セッション ID 番号を示します。

Interface

このセッションを実行しているインターフェースの番号を示します。

Remote MAC addr

リモート LLC ピアの MAC アドレスを示します。

Source MAC addr

ローカル LLC の MAC アドレスを示します。

Remote SAP

LLC 接続のリモート側 SAP

Local SAP

LLC 接続のローカル側 SAP

RIF フレームの実際の RIF

Access Priority

パケットの優先順位。高位レイヤー制御の場合は 07

State LLC ピア間のインターアクションの結果としての有限状態。詳細については、272 ページの **list sap** コマンドの項を参照してください。

Receive ACK timer (T2)

LLC が受信した I フレームに対する確認応答を送信する前に使用する時間遅延を示します。

Inactivity timer (Ti)

RR を出す前の非アクティブ時に LLC が待機する時間を示します。

MAX I-field size (N1)

フレームのデータ・フィールドの最大サイズ (バイト数)。デフォルト値は、インターフェースのサイズです。

MAX Retry Value (N2)

LLC が確認応答を受信せずに RR を送信する最大回数

Rcvd I-frames before ACK (N3)

受信した I フレームに対する確認応答トラフィックを減らすために、T2 タイマーとともに使用される値を示します。

Transmit window size (Tw)

RR を受信する前に送信できる I フレームの最大数を示します。

Working transmit size (Ww)

RR を受信する前に送信できる I フレームの最大数

Acks Needed to Inc Ww (Nw)

このフィールドは、デフォルト値の 1 に設定します。

Current send seq (Vs)

送信状態変数 (転送される次の I フレームの Ns 値)

Current Rcv seq (Vr)

受信状態変数 (受け付ける次の in-sequence Ns)

Last ACK'd sent frame (Va)

確認応答された状態変数 (受信した最後の有効な Nr)

No. of frames in ACK pend q

確認応答を待機中の送信済み I フレーム数

No. of frames in transmit pend q

送信されるのを待っているフレーム数

Local Busy

LLC 接続のローカル側が RNR を送信中

Remote Busy

LLC 接続のリモート側が RNR を受信済

Poll Retry count

LLC プロトコル内のカウンターの再試行の現行値 (カウントダウン) を示します。

Appl output flow stopped

LLC がアプリケーションに対して発信データ・フレームの供給停止を指示しました。

Send process running

このプロセスは、その他のフレーム・アクションと並行して実行され、I フレームを送信待ち行列に入れて送信します。

Frames Xmt and Rcvd

転送されたフレーム・タイプ (Xmt) および (Rcvd) の総数を表示します。

I-frames discarded by LLC

LLC によって廃棄された (通常は、シーケンス番号が順序通りでないという理由で) I フレームの合計数を表示するカウンター

I-frames refused by LLC user

LLC の上位ソフトウェアによって廃棄された I フレーム数を示すカウンター。たとえば、DLSw (データ・リンク交換)

Set

set コマンドは現行 LLC セッションに関する LLC パラメーターを動的に構成するのに使用します。パラメーターに加えた変更は、セッションの存続期間中だけ有効です。これらのパラメーターは、269ページの『Set』にリストされているものと同一です。

重要: LLC パラメーターをデフォルト値から変更すると、LLC プロトコルの動作方法に影響を与える可能性があります。

構文:

```

set                                n2-max_retry count
                                       n3-frames-rcvd-before-ack count
                                       nw-acks-to-inc-ww count
                                       t1-reply-timer seconds
                                       t2-receive-ack-timer seconds
                                       ti-inactivity-timer seconds
                                       tw-transmit-window seconds
    
```

n2-max_retry

LLC プロトコルによる再試行の最大数。たとえば、N2 は、非活動タイマーが満了したときに、LLC が確認応答を受信せずに RR を送信する最大回数です。デフォルト値は 8。最小値は 1。最大値は 127。

n3-frames-rcvd-before-ack

この値は、T2 タイマーと合わせて、受信 I フレームの確認応答トラフィックを削減するのに使用されます。このカウンターは、指定された値に設定します。I フレームを受信するたびに、この値が減分します。このカウンターが 0 に達するか、T2 タイマーが満了すると、確認応答が送信されます。デフォルト値は 1。デフォルト値は 1。最小値は 255。

nw-acks-to-inc-ww

このフィールドは、デフォルト値の 1 に設定します。

t1-reply-timer

このタイマーは、LLC が相手側の LLC ステーションから必要な確認またはレスポンスを受信できないと満了します。このタイマーが満了すると、ポーリング・ビットをセットして RR が送信され、T1 が再びスタートします。LLC が構成された再試行最大数 (N2) の後もレスポンスを受信しない場合、基礎リンクは動作不能として宣言されます。デフォルト値は 1。デフォルト値は 1。最小値は 256。

t2-receive-ack-timer

このタイマーは、受信 I フォーマット・フレームの確認の送信を遅らせるのに使用します。このタイマーは、I フレームを受信するとスタートし、確認を送信するとリセットされます。このタイマーが満了すると、LLC2 はできるだけ速やかに確認を送信します。この値は、T1 の値より小さくなるように設定します。これにより、T1 タイマーが満了する前に、リモート LLC2 ピアが遅らせた確認を確実に受信できるようになります。デフォルト値は 1 (100 ミリ秒)。最小値は 1。最大値は 2560。

注: このタイマーが 1 (デフォルト値) に設定されている場合、タイマーは動作しません (たとえば、**n3-frames_rcvd-before-ack=1**)。

ti-inactivity-timer

このタイマーは、指定された期間に LLC がフレームを受信しないと満了します。このタイマーが満了すると、相手側の LLC が応答するか、N2 タイマーが満了するまで、LLC は RR を送信します。デフォルト値は 30 秒。最小値は 1 秒。最大値は 256 秒。

tw-transmit-window

RR を受信する前に送信できる I フレームの最大数を示します。相手側の LLC セッションが実際にこの数の連続 I フレームを受信することが可能であり、しかもルーターに確認を受信するまでこれらのフレームのコピーを保持できる十分なヒープ・メモリーがあると仮定した場合、この値を大きくすると、スループットが向上します。デフォルト値は 2。最小値は 1。最大値は 127。

第16章 イーサネット・ネットワーク・インターフェースの使用

この章では、イーサネット・インターフェースの使用法について説明します。本章には、『インターフェース・コマンドによるイーサネット統計の表示』が含まれています。

インターフェース・コマンドによるイーサネット統計の表示

GWCON 環境から **interface** コマンドを使用して、以下の統計を表示することもできます。

```
+ interface 4
                Self-Test Self-Test Maintenance
Nt Nt' Interface Slot-Port          Passed  Failed   Failed
4 4  Eth/0  Slot: 4 Port: 1             3      1       0
    Ethernet/IEEE 802.3 MAC/data-link on Ethernet interface
    Physical address      AA0004000318
    PROM address          10005AFF0016
    Microcode Level       Uu17c

Input statistics:
failed, packet too long      0 failed, CRC error           1
failed, alignment error     0 failed, FIFO over-run      0
buffer full warnings        0 packets missed             1
internal mac rx errors      0

Output statistics:
initially deferred          12 single collision            1
multiple collisions         1 total collisions           4
failed, excess collisions   0 failed, FIFO under-run     0
failed, carrier check       0 CD heartbeat error        0
```

これらの統計は、次のような意味を持っています。

Nt グローバル・ネットワーク番号

Nt' このフィールドは、シリアル・インターフェース・カード用です。出力とは無関係です。

Interface

インターフェース名とそのインスタンス番号

Port ポート番号

Slot スロット番号

Self-Test: Passed

成功した自己テストの回数

Self-Test: Failed

失敗した自己テストの回数

Maintenance: Failed

保守障害の数

Physical address

現在使用している装置のイーサネット・アドレス。これは PROM アドレス、あるいは他のプロトコルによって上書きされたアドレスです。

PROM address

このイーサネット・インターフェースの PROM 内の永続的な固有のイーサネット・アドレス。

イーサネット・ネットワーク・インターフェースの使用

Input statistics:

failed, packet too long or failed, frame too long

「障害、パケットが長過ぎる」カウンターは、インターフェースが、イーサネット・フレームの最大サイズである 1518 バイトより大きいパケットを受信すると増分します。このデータは SNMP を介して dot3StatsFrameTooLongs カウンターとしてエクスポートされます。

failed, CRC error or failed, FCS (Frame Check Sequence) error

「障害、CRC (巡回冗長検査) エラー」カウンターは、インターフェースが CRC エラーを含むパケットを受信すると増分します。このデータは SNMP を介して dd3StatsFCSErrors カウンターとしてエクスポートされます。

failed, framing error or failed, alignment error

「障害、フレーム・エラー」カウンターは、インターフェースが、長さ (ビット数) が 8 の倍数でないパケットを受信すると増分します。

failed, FIFO over-run or failed, FIFO overrun

「障害、FIFO (先入れ先出し) オーバーラン」カウンターは、イーサネット・チップ・セットが、線路から送り出される速度に見合う速度で、ローカル・パケット・バッファにバイトを保管できない場合に増分します。

buffer full warnings

「バッファ満ぱい警告」カウンターは、ローカル・パケット・バッファがいっぱいになるたびに増分します。

packets missed

「パケット紛失」カウンターは、インターフェースがパケットを受信しようとしたが、ローカル・パケット・バッファが満ぱいであるときに増分します。このエラーは、インターフェースの処理能力を超えるトラフィックがネットワーク上に存在することを示しています。

internal mac rcv errors

遅延、過剰、またはキャリア・チェック衝突以外の受信エラー。このデータは SNMP を介して dot3StatsInternalMacReceiveErrors カウンターとしてエクスポートされます。この統計は FIFO オーバーランの合計値です。

Output statistics:

initially deferred or deferred transmission

「初期遅延」カウンターは、キャリア・センス機構がインターフェースの転送を遅らせるようなライン・アクティビティを検出すると増分します。このデータは SNMP を介して dot3StatsDeferredTransmissions カウンターとしてエクスポートされます。

single collision

「単一衝突」カウンターは、初回の転送試行でパケットが衝突した後、2 回目の転送試行でパケットを正常に送信できた場合に増分します。このデータは SNMP を介して dot3StatsSingleCollisionFrames カウンターとしてエクスポートされます。

multiple collisions

「複数衝突」カウンターは、パケットが正常に転送されるまでに複数回の衝突が生じた場合に増分します。このデータは SNMP を介して dot3MultipleCollisionFrames カウンターとしてエクスポートされます。

total collisions

「合計衝突数」カウンターは、パケットに発生した衝突の数だけ増分されません。

failed, excess collisions

「障害、超過衝突」カウンターは、16回の連続衝突によりパケット転送が失敗すると増分します。このエラーは、ネットワーク通信量が多いか、ネットワークにハードウェア問題があることを示しています。このデータは SNMP を介して dot3StatsExcessiveCollisions カウンターとしてエクスポートされます。

failed, FIFO underrun

「障害、FIFO アンダーラン」カウンターは、インターフェースがネットワーク上の転送に対応できる速度でローカル・パケット・バッファからパケットを取り出せないためにパケットの転送に失敗すると増分します。

failed, carrier check or failed, carrier sense error

「障害、キャリア・チェック」カウンターは、キャリア・センスが使用不可にされているためにパケットが衝突すると増分します。このエラーは、インターフェースとそのイーサネット・トランシーバー間に問題があることを示しています。このデータは SNMP を介して dot3StatsCarrierSenseErrors カウンターとしてエクスポートされます。

CD heartbeat error or SQE test error

「CD (衝突検出) ハートビート・エラー」または「SQE (信号品質エラー)」カウンターは、インターフェースがパケットを送信したが、トランシーバーがハートビートを生成しないことを検出すると増分します。トランシーバーによってはハートビートを生成しないものがあるので、このパケットは正常に転送されたものとして扱われます。このデータは SNMP を介して dot3StatsSQETestErrors カウンターとしてエクスポートされます。

イーサネット・ネットワーク・インターフェースの使用

第17章 イーサネット・ネットワーク・インターフェースの構成および監視

この章では、イーサネット・インターフェースの構成コマンドおよびオペレーショナル・コマンドについて説明します。本章には、以下の節が含まれています。

- 285ページの『イーサネット・インターフェース動作プロセスへのアクセス』
- 285ページの『イーサネット・インターフェース監視コマンド』

イーサネット・インターフェース構成プロセスへのアクセス

構成プロセスにアクセスするには、以下の手順を使用します。このプロセスにより、イーサネット・インターフェースの構成 プロセスにアクセスできます。

1. OPCON プロンプトで **talk 6** と入力する。(このコマンドの詳細については、33ページの『OPCON プロセスとは』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>
```

コンソールに CONFIG プロンプト (Config>) が表示されます。最初に構成に入ったときにプロンプトが表示されない場合は **Return** をもう一度押してください。

2. CONFIG プロンプトで **list devices** コマンドを入力して、ルーターが現在構成されているネットワーク・インターフェース番号を表示する。
3. インターフェース番号を記録する。
4. **network** コマンドと、構成するイーサネット・インターフェースの番号を入力する。たとえば、次のように入力します。

```
Config> network 0
ETH Config>
```

イーサネット構成プロンプト (ETH Config>) が表示されます。

イーサネット構成コマンド

この節では、イーサネット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。コマンドは ETH config> プロンプトで入力します。

表 33. イーサネット構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Connector-Type	コネクタ・タイプを設定します。
IP-Encapsulation	IP カプセル化を、イーサネット (タイプ X'0800') または IEEE (SNAP 付き 802.3) として設定します。
List	現行のコネクタ・タイプ、NetWare IPX カプセル化、および IP カプセル化を表示します。

イーサネット構成コマンド (Talk 6)

表 33. イーサネット構成コマンドの要約 (続き)

コマンド	機能
Physical-Address Exit	物理 MAC アドレスを設定します。 直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Connector-Type

connector-type コマンドは、コネクタ・タイプを設定するのに使用します。2210 は、AUI (10BASE5) および RJ-45 (10BASE-T) コネクタと、自動構成 (auto-config) オプションをサポートします。

構文:

```
connector-type          name
```

IP-Encapsulation

ip-encapsulation コマンドは、イーサネット (イーサネット・タイプ X'0800') または IEEE 802.3 (SNAP を備えたイーサネット 802.3) を選択するのに使用します。 **e** または **i** を入力します。

構文:

```
ip-encapsulation      type
```

List

list コマンドは、コネクタ・タイプ、IPX カプセル化タイプ、および IP カプセル化タイプを含めて、イーサネット・インターフェースの現行構成を表示するのに使用します。

構文:

```
list                  all
```

例: **list all**

```
Connector type:      AUI (10BASE5)  
MAC Address:        12:15:00:FA:00:FE
```

Physical-Address

physical-address コマンドは、物理 (MAC) アドレスを設定するのに使用します。

構文: **physical-address** *address*

physical-address

このコマンドでは、イーサネット・インターフェースの MAC サブレイヤー・アドレスにローカル管理アドレスを定義するのか、あるいはデフォルトの刻印されたアドレス (オール 0 で示される) を使用するのかを指示することができます。MAC サブレイヤー・アドレスは、イーサネット・インターフェースがフレームの送受信に使用するアドレスです。

イーサネット構成コマンド (Talk 6)

注: **Enter** を押すと、値はそのままになります。**0** を入力すると、ルーターは刻印されたアドレスを使用します。デフォルトでは、刻印されたアドレスを使用します。

有効値: 任意の 12 桁の 16 進アドレス

デフォルト値: 刻印されたアドレス (オール 0 で示されます)

例: `physical-address`

MAC address in 00:00:00:00:00:00 form []? **12:15:00:FA:00:FE**

イーサネット・インターフェース動作プロセスへのアクセス

イーサネット・ネットワーク・インターフェースに関連する情報を監視するには、以下の手順を使用して、インターフェース監視プロセスにアクセスします。

1. OPCODE プロンプトで **talk 5** と入力する。たとえば、次のように入力します。

```
* talk 5
```

GWCON プロンプト (+) がコンソールに表示されます。最初に GWCON に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. GWCON プロンプトで **configuration** コマンドを入力して、ルーターに構成されているプロトコルとネットワークを表示する。たとえば、次のように入力します。

```
+configuration
```

(**configuration** コマンドの出力例については、152ページの『Configuration』を参照してください。)

3. **network** コマンドとイーサネット・インターフェースの番号を入力する。この例では、次のように入力します。

```
+ network 0  
ETH>
```

イーサネット監視プロンプトが表示されます。これで、監視コマンドを入力すれば、イーサネット・インターフェースに関する情報を見ることができます。

イーサネット・インターフェース監視コマンド

この節では、イーサネット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 ETH> プロンプトで入力します。表34 は、監視コマンドをリストしています。

表34. イーサネット構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Collisions	指定されたイーサネット・インターフェースの衝突統計を表示します。

イーサネット・インターフェース監視コマンド (Talk 5)

表 34. イーサネット構成コマンドの要約 (続き)

コマンド	機能
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Collisions

このコマンドは、正常に転送される前に衝突を起こしたパケットの転送数を示します。カウンターは、15回の衝突の後に送信された、衝突 **XXXXx** パケットの後に送信されたパケット数を示します。衝突を伴って転送されたパケット数が増えること、およびパケット当たりの衝突回数が増えることは、ビジー状態のイーサネットに転送されていることを示しています。

これらのカウンターは、OPCON **clear** コマンドによってクリアされます。このデータは SNMP を介して dot3CollTable カウンターとしてエクスポートされます。

構文:

collisions

例:

```
Eth> coll
Transmitted with 1 collisions:0
Transmitted with 2 collisions:0
Transmitted with 3 collisions:0
Transmitted with 4 collisions:0
Transmitted with 5 collisions:0
Transmitted with 6 collisions:0
Transmitted with 7 collisions:0
Transmitted with 8 collisions:0
Transmitted with 9 collisions:0
Transmitted with 10 collisions:0
Transmitted with 11 collisions:0
Transmitted with 12 collisions:0
Transmitted with 13 collisions:0
Transmitted with 14 collisions:0
Transmitted with 15 collisions:0
```

第18章 LAN エミュレーションの概説

注: 本章で使用されている頭字語および用語の定義については、用語集を参照してください。

IBM 2210 は、複数のベンダーの複数のプロトコルのインターオペラビリティのための業界標準として広く受け入れられている *LAN Emulation Over ATM: Version 1.0 Specification* を実現しています。この章では、MSS インプリメンテーションのコンテキストの中で LAN エミュレーション (LE) の基本概念を紹介します。最初に、エミュレートされた LAN (ELAN) を導入する動機について検討します。

LAN エミュレーションの利点

LAN エミュレーション・プロトコルは、ATM ネットワークをイーサネット LAN またはトークンリング LAN のように見せることができます。LAN エミュレーションは、ATM の利点のすべてを活用できるわけではありませんが、ATM 技術への移行やネットワーク管理コストの削減に役立ちます。高速 ATM リンクを利用できる上に、ソフトウェアとハードウェアの投資の保護を図れます。

ソフトウェア投資を保護できるのは、アプリケーション・インターフェースが変更されないからです (LAN エミュレーションは、エンド・ステーションのデバイス・ドライバ・インターフェースの下にあるデータ・リンク制御レイヤー内で実現されます)。ハードウェア投資を保護できるのは、転送装置本体が LAN ネットワークや ATM ネットワークをブリッジするので、既存のアダプターや配線を引き続き使用できるからです。

LAN エミュレーションを使用すれば、高帯域幅をもつステーション (たとえば、サーバー、技術ワークステーション、マルチメディア・ワークステーション) に ATM アダプターを徐々に増設していくことができます。単純な LAN エミュレーションの例の物理図と論理図を 図14 に示します。

LAN エミュレーションの概説

単純な LAN エミュレーション・ネットワーク

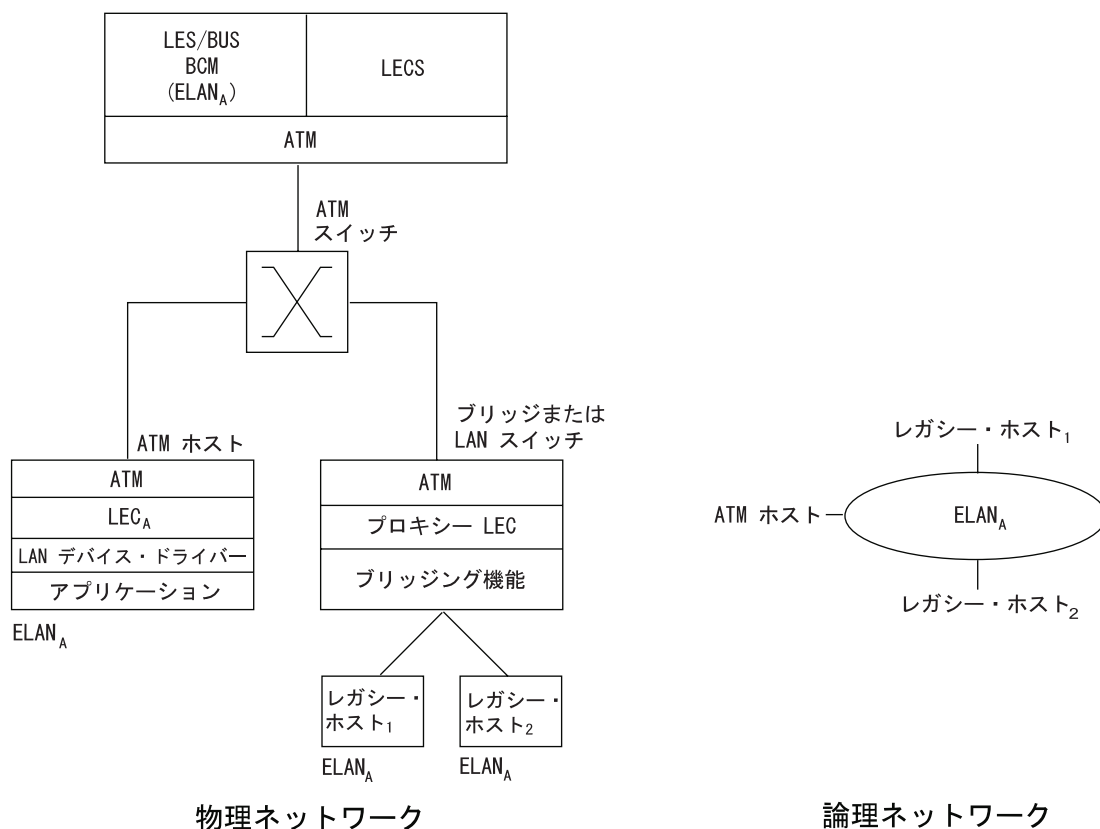


図 14. 単純な LAN エミュレーション・ネットワークの物理図と論理図

エミュレートされた LAN (ELAN) のネットワーク管理上の利点は、移動、追加、および変更が柔軟になることから得られます。ELAN のメンバーシップは物理的な場所に基づくのではなく、論理的に関連したステーションがグループ化されて、1 つの ELAN を形成します (ステーションは複数の ELAN のメンバーになることも可能です)。

ELAN メンバーシップが保持されている限り、ステーションが物理的に別の場所へ移動しても、再構成の必要はありません。同様に、ステーションをある ELAN から別の ELAN へ移動しても、配線を変える必要はありません。

LAN エミュレーションのコンポーネント

以下のコンポーネントによって ELAN が実現します。

LAN エミュレーション (LE) クライアント (LEC)

エミュレートされた LAN のユーザーを表す LAN エミュレーションのコンポーネント

LE 構成サーバー (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

LE サーバー (LES)

LAN あて先を ATM アドレスに変換する LAN エミュレーション・サービス・コンポーネント

ブロードキャストおよび不明サーバー (BUS)

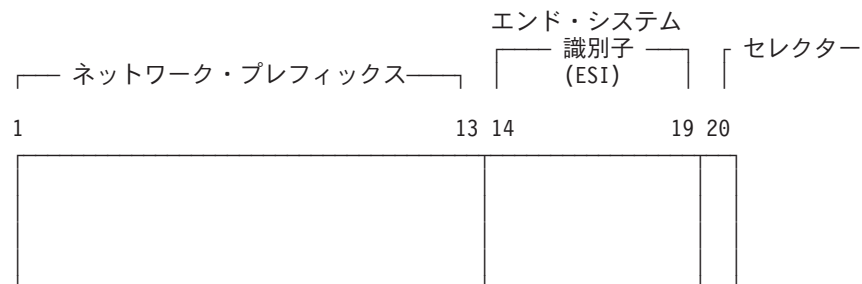
マルチキャスト・フレームおよび不明ユニキャスト・フレームの送達を担当する LAN エミュレーション・サービス・コンポーネント

LES、BUS、および LECS をまとめて LE サービス・コンポーネントと呼んでいます。各 ELAN には専用の LES および BUS があります。LE クライアントは、エンド・システム内 (ATM 接続ホスト内、あるいはブリッジまたは LAN スイッチ内のいずれか) に存在します。ブリッジまたは LAN スイッチは、イーサネット LAN またはトークンリング LAN に接続されているホストを表します。LE クライアントは、MAC レベルのサービスを高位レベル・ソフトウェアに提供します。イーサネット IEEE 802.3 または IEEE 802.5 トークンリング LAN をエミュレートすることができますが、ELAN 上のすべてのステーションが同じタイプであることが必要です。

トークンリングまたはイーサネット LAN セグメントと ELAN 間をブリッジする機能は、プロキシ LEC と呼ばれます。LAN をエミュレートする場合は、LE クライアントは LECS、LES、および BUS からのサービスを要求します。以下の節では、ATM アドレッシングおよび関連の中間ローカル管理インターフェース (ILMI) 機能について簡単に説明します。これらの概念を理解しておかないと、ネットワーク内の LE コンポーネントの機能は理解できません。

ATM でのアドレッシング

ATM では 20 バイトの階層型アドレッシングを使用します。



ATM アドレスの最初の 13 オクテットはネットワーク・プレフィックスです。ATM ネットワーク内の各スイッチは、固有のネットワーク・プレフィックスをもっていることが必要です。ATM スイッチは、ネットワーク・プレフィックスを使用して、VCC 設定要求をあて先 ATM スイッチにルーティングします。エンド・システム (このルーターのような) は、起動したときに、ATM スイッチからネットワーク・プレフィックスを取り出します。

ATM アドレスのオクテット 14-19 は、エンド・システム識別子 (ESI) です。同じスイッチに接続されている各エンド・システムは、別々の ESI セットを使用しなければなりません。エンド・システムが起動すると、インターリム・ローカル管理インターフェース (ILMI) を使用して、その ESI を ATM スイッチに登録しようと試みます。

LAN エミュレーションの概説

ILMI は、エンド・システムと ATM スイッチ間のインターフェースを管理するのに使用される 1 組の SNMP ベースの手順を定義します。エンド・システムは ILMI を使用して、以下のことを行います。

- スイッチからネットワーク・プレフィックスを入手する。
- ESI をスイッチに登録する。
- ATM スイッチの UNI バージョンを動的に判別する。
- LEC はスイッチから LECS アドレスのリスト入手できるようになる。

スイッチは、すべての登録済み ESI が固有になるようにします。

ATM アドレスのオクテット 20 はセレクターです。

エンド・ステーションは、スイッチからネットワーク・プレフィックスを入手し、ESI とセレクターを追加して、独自のアドレスを形成します。こうして作成されたアドレスがスイッチに登録されますが、ATM アドレスが固有でない場合、スイッチは登録を拒否します。

ESI

ルーター上の各 ATM インターフェースは、汎用管理または出荷時設定 MAC アドレスをもっています。この MAC アドレスを、ルーターの ATM アドレスの一部または全部の ESI として使用することができます。あるいは、各インターフェースに最大 64 個のローカル管理アドレスを定義することもできます。すべてのエンド・システムが汎用管理 MAC アドレスを ESI として使用すれば、ATM アドレスが固有であることが保証されます。こうすれば、構成の負担が軽くなります。ただし、ローカル管理 ESI を使用すると、問題判別が容易になる場合もあります。ユーザーは、汎用管理 ESI とローカル管理 ESI を任意に組み合わせて使用することができます。

固有の ATM アドレスを得る 1 つの方法として、出荷時設定 IEEE MAC アドレスを ESI として使用し、固有のセレクターをローカルで選択するという方法もあります。デフォルトでは、ルーターは ATM インターフェースの MAC アドレスを、その ATM アドレス内の ESI として使用します。各 ATM インターフェースに追加 ESI を構成できます。

各 ESI は最大 255 個の対応するセレクター (0x00 ~ 0xff) をもつことができます。セレクターの範囲は、構成されるセレクター範囲と自動的に割り当てられるセレクター範囲の 2 つに区分されています。構成されるセレクター範囲の上限は、ATM インターフェース・パラメーター max-configured-selector で定めます。

ルーター上の ATM コンポーネントは、さまざまな方法でセレクターを選択します。あるコンポーネントの場合は、構成されたセレクター範囲から、ユーザーが明示的にセレクターを構成する必要があります。このようなコンポーネントの例としては、LES/BUS があります。別のコンポーネント (クラシカル IP クライアントなど) は、実行時に自動的にセレクターを割り当てることができます。ユーザーはセレクターを選択する必要はなく、ルーターが起動時にこれを選択します。このセレクターは、ルーターのリスタートのたびに一貫しているとは保証されません。自動的なセレクターの割り当ては、ネットワーク上の他の装置があらかじめその ATM アドレスを知っていなくても構わない ATM コンポーネントの場合にのみ便利です。

ATM の構成は、エミュレートされた LAN、ブリッジング、またはルーティングを構成する前に行う必要があります。

LAN エミュレーション・コンポーネントの ATM アドレス

一般的には、ATM アドレスは LAN エミュレーション・コンポーネント間で固有であることが必要です。唯一の例外として、同じ ELAN にサービスする LES と BUS は ATM アドレスを共用できます (ルーターはこれに相当します)。

LAN エミュレーション・コンポーネントは、特定の ATM インターフェースに対して構成されます。コンポーネントの ATM アドレスの ESI 部分として出荷時設定 MAC アドレスの使用することに決めても構いませんし、その ATM インターフェースに対して定義されたローカル管理 ESI の 1 つを選択することもできます。セクターが固有であれば、複数の LE コンポーネントが同じ ESI を共用することも可能です。デフォルトでは、構成インターフェースが各 ESI コンポーネントごとに、構成済み ESI に対して固有のセクター値を割り当てます。ただし、この割り当てをオーバーライドして、明示的に特定のセクター値を構成することも可能です。

ATM インターフェース・パラメーターを用いて、明示的な割り当て用として予約される ESI 当たりのセクター数を定めます。残りは、実行時に ATM インターフェースが動的に割り当てられるのに利用できます。LE コンポーネントは、明示的な割り当て用に予約されたセクターのみを使用します。デフォルトでは、ESI 当たり可能な 256 個のセクターのうち 200 個が、明示的割り当て用として予約されます。実行時のセクター割り当てが有利なのは、割り当てられたセクターを制御する必要がない場合です。たとえば、ARP サーバーと対をなしていないクラシカル IP 内のクライアントを構成する場合などです。

LE コンポーネント間では ATM アドレスは固有でなければなりません、LE コンポーネントは、クラシカル IP サーバー機能のような非 LE コンポーネントとは同じ ATM アドレスを使用しても構いません。

関連 ILMI 機能の概説

ILMI は、エンド・システムと ATM スイッチの間の ユーザー・ネットワーク・インターフェース (UNI) を管理するのに使用される 1 組の SNMP ベースの手順を定義します。特に LAN エミュレーションに関係のある ILMI 機能には、次の 3 つがあります。

1. ATM アドレス登録 (289ページの『ATM でのアドレッシング』で説明)
2. スイッチで実行中の信号バージョンの動的な判別
3. LECS ATM アドレスの獲得

289ページの『ATM でのアドレッシング』で説明しているように、ATM アドレス登録は、ATM エンド・システムとスイッチの間で共同で行われる作業です。あらかじめスイッチに ATM アドレスを登録しておかないと、コールを送信または受信することはできません。

デフォルトでは、ルーターの ATM インターフェースは ILMI 手順を使用してスイッチ MIB を照会し、スイッチで実行されている信号バージョンの判別 (UNI 3.0 または 3.1) を試みます。照会が正常に行われた場合、ATM インターフェースはスイッチ

LAN エミュレーションの概説

と同じ UNI バージョンを実行します。照会が正常に行われなかった場合は、ATM インターフェースは UNI 3.0 を実行します。あるいは、デフォルトをオーバーライドして、ATM インターフェースで実行される UNI バージョンを明示的に構成することもできます。

信号バージョンの手動による構成

ATM スイッチが UNI 3.1 を実行しており、UNI バージョン MIB 変数がない場合は、信号バージョンを手動で構成する必要があります。この場合、ATM インターフェースは UNI バージョンを動的に判別することはできません。ルーターの ATM インターフェースは、デフォルトでは UNI 3.0 を使用するの、ユーザーは ATM インターフェースが UNI 3.1 を使用するよう手動で構成する必要があります。

ILMI の使用による LECS の探索

ILMI は、LECS を見つける方法として特に優れています。ATM スイッチの ILMI MIB には、LE クライアントが検索できる LECS ATM アドレスのリストが入っています。この方式が便利な理由は、LECS ATM アドレスを構成する必要があるのは ATM スイッチだけで、LE クライアントはその必要がなく、しかもスイッチの数は LE クライアントの数より少ないことにあります。クライアントは、このリストの最初の LECS への接続を試みます。接続に失敗すると、クライアントは接続が確立されるまで、順番に次の LECS アドレスへの接続を試みます。

LECS 機能の概説

LE クライアントは、LECS の使用が推奨されますが、必ず使用しなければならないわけではありません。LECS を使用しない場合は、各 LE クライアントで、ELAN にサービスする LES の ATM アドレスを構成することが必要です。LECS は、構成データの中央リポジトリとして機能することによりネットワーク管理の負担を減らし、LE クライアントの構成を最小限に抑えます。

注: 各ルーターに構成できる LECS は最高で 1 つです。

クライアントは、事前定義された手順を使用して LECS に接続します。LECS へのバーチャル・チャンネル・コネクション (VCC) が確立されるまで、クライアントは以下の手順を試みます。

1. 構成された LECS アドレス情報があれば (LE クライアントでの LECS ATM アドレスの構成はオプションであり、推奨されていません)、それを使用して LECS に接続する。
2. ILMI を使用して LECS のリストを入手し、VCC が確立されるまで、リストの各 LECS への接続を順番に試みる。
3. ATM フォーラムで定義されている事前割り当て LECS ATM アドレスへの VCC を確立する。

前述のとおり、LE クライアントが LECS を見つける方法としては、ILMI が優先されます。一部のスイッチは ILMI 方式をサポートしないので、事前割り当て LECS アドレスが必要になります。LE クライアントで LECS アドレスを構成するのは、スイ

ッチが ILMI 方式をサポートせず、LE サービスが事前割り当て LECS アドレスをサポートしない場合に**限る** が必要です。

ルーターと IBM ATM スイッチは、3 つの方式、つまり、事前割り当て LECS アドレス、ILMI 接続、および事前割り当て LECS ATM アドレスをすべてサポートします。

LECS は、初期構成データを LE クライアントに提供する必要があります。最も重要なデータは、LES の ATM アドレスです。この情報を LE クライアントに提供するためには、LECS が LE クライアントを識別し、その LE クライアントの正しい LES を判別できることが必要です。LECS は、LE クライアントによって送信される LE_CONFIGURATION_REQUEST フレーム内の情報を使用して、LE クライアントを識別します。この構成要求には、LE クライアントが加入を求めている ELAN を識別するための情報も含まれています。構成要求には、以下の情報を含めることができます。

1. LE クライアントの 1 次 ATM アドレス

このフィールドは必須であり、LE クライアントを固有に識別します。

2. LAN クライアントに対応する LAN あて先

このフィールドには、LE クライアントを固有に識別する MAC アドレスまたはルート記述子を入れてもよいし、指定しないでおくこともできます。

3. ELAN ネーム

このフィールドには、要求される ELAN または要求する LE クライアントを識別する名前を入れることができます。ルーターの実現では、ELAN ネームは標準 ASCII スtring です。ELAN ネームは、要求の中で指定しなくても構いません。

4. ELAN タイプ

このフィールドでは、LE クライアントがイーサネットまたはトークンリングに属することを指定できますが、指定しなくても構いません。LE クライアントが ELAN のタイプを指定している場合、LECS はそのクライアントに異なるタイプの ELAN を割り当てることはできません。

5. LE クライアントによってサポートされる最大フレーム・サイズ

このフィールドでは、LE クライアントが処理できるデータ・フレームのサイズの上限を指定できますが、指定しなくても構いません。LECS はクライアントを、そのクライアントが指定したより**大きい** 最大フレーム・サイズをもつ ELAN に割り当てることはできません。ELAN が使用するフレームが大きすぎてクライアントが処理できない場合、クライアントはその ELAN 上では機能できません。

この情報に基づいて、LECS は LE クライアントを LES に割り当てます。これは、ポリシーとポリシー値を使用して行います。ポリシーとは、LECS が LE クライアントの LES への割り当てを決めるときに使用する基準のことです。ポリシー値とは、指定の値を指定の LES に割り当てることを指示する値の組み合わせ (値、LES) です。たとえば、ポリシーは LE クライアントの MAC アドレスとし、ポリシー値は (MAC ADDR_A, LES_1) というように指定します。MAC ADDR_A の LE クライアントが、LES_1 に割り当てられることとなります (その LE クライアントが、ポリシーの優先順位が上位のために、すでに別の LES に割り当てられていない場合)。1 組のポリシーとポリシー値が、すべての ELAN に適用されます。

2 番目のタイプの ATM アドレス・ポリシー値は、ATM アドレスの ESI とセレクターです。たとえば、ポリシー値 (10002345003281, LES_A) は、ESI が 100023450032 で、セレクターが 81 の LE クライアントを、LES A に割り当ててることを意味しています。

LE クライアントの ATM アドレスが与えられると、LECS は最初に ESI とセレクターが一致するものを探します。一致が戻されなかった場合、LECS は、一致するプレフィックスが最も長い ATM アドレス・プレフィックス・ポリシー値を探します。したがって、上記の例のポリシーは、ポリシー値 (39999999999990000, LES_B) より優先されます。

ATM アドレス ESI とセレクター・ポリシー値を使用すると、LE クライアントの物理的な場所から独立した形で、クライアントを LES に割り当てることができます (ESI とセレクターは、ローカルでクライアントに定義されます)。ATM アドレス・プレフィックスが、地理情報を示す唯一のポリシー値です。

LAN あて先ポリシー

MAC アドレスまたはルート記述子に基づいて、LE クライアントを LES に割り当てることができます。LAN あて先は、地理的な場所から独立した形で LE を固有に識別するので、このポリシーは、LE クライアントを物理的な場所とは関係なく (たとえば、ワークステーションをあるスイッチから別のスイッチに移動するとき、そのメンバーシップを保持したままで) 正しい ELAN に確実に割り当てることができるので便利です。

ELAN ネーム・ポリシー

ELAN ネームは、おそらく最も柔軟な割り当て基準です。以下に、ELAN ネーム・ポリシー値を使用できる方法をいくつか挙げます。

- ELAN の実名の使用

LES_A が Elan 1 にサービスする場合は、ポリシー値 (Elan 1, LES_A) を作成します。この場合、構成要求で Elan 1 を指定している LE が、LES_A に割り当てられます。

- ELAN の別名の使用

たとえば、経理部に属するすべての LE クライアントは ELAN ネーム *Accounting* を使用し、技術部に属するすべての LE クライアントは ELAN ネーム *Engineering* を使用するように構成することができます。ELAN 上の LE クライアントの数に応じて、これらの名前を同じ ELAN に割り当てる場合は、ポリシー値を次のように構成します。

```
(Accounting, LES_A)  
(Engineering, LES_A)
```

あるいは、異なる ELAN に割り当てる場合は、ポリシー値を次のように構成します。

```
(Accounting, LES_A)  
(Engineering, LES_B)
```

この設定の場合は、LE クライアントに正しい ELAN ネームを構成することが必要です。

LAN エミュレーションの概説

- LE クライアントの名前の使用

各 LE クライアントに独自の名前を与えることができます。たとえば、ポリシー値 (Joe, LES_A) と (Mary, LES_A) を作成できます。この場合、これらの名前を構成された LE クライアントは、同じ LES に割り当てられることとなります。この方法では、個々の LE クライアントと LECS で、ELAN ネームを構成する必要があります。ただし、Joe と Mary はクライアントを新しい場所に移動することができます。移動によって、クライアントは新しい ATM アドレスまたは MAC アドレスを持つこととなりますが、新しい LE クライアントを同じ ELAN ネームで構成する限り、元の ELAN のメンバーシップが保持されます。各 LE クライアントの名前をパスワードとみなせば、この方式は適度のセキュリティーも提供することとなります。

ELAN タイプ・ポリシー

ELAN タイプ・ポリシー値は、デフォルト ELAN を提供する場合に非常に便利です。たとえば、次のポリシー値は、個々の LE クライアントが確実に LES の 1 つに割り当てられます。

```
(Token-ring ELAN Type,  LES_A)
(Ethernet ELAN Type,    LES_B)
(Unspecified ELAN Type, LES_C)
```

一般的には、デフォルト ELAN 割り当てを提供するポリシーには低い優先順位を与え、特定のポリシーが先に考慮されるようにすべきです。

最大フレーム・サイズ・ポリシー

最大フレーム・サイズ・ポリシーも、デフォルト ELAN 割り当てを提供するのに使用できます。

重複ポリシー値

特定のポリシーの複数の LES に対して同じポリシー値が対応している場合に、重複が起きます。ELAN タイプ・ポリシーと最大フレーム・サイズ・ポリシーでは、重複ポリシー値は許容されますが、その他のポリシーでは認められません。重複値が便利なのは、同じ優先順位の異なるポリシーと組み合わせる場合だけです。

たとえば、次のような 3 つの ELAN があるとします。最大フレーム・サイズが 4544 バイトのイーサネット ELAN、最大フレーム・サイズが 4544 バイトのトークンリング ELAN、および最大フレーム・サイズが 18190 バイトの別のトークンリング ELAN です。ELAN タイプ・ポリシーと最大フレーム・サイズ・ポリシーを同じ優先順位に設定し、次のポリシー値を定義することにより、LE クライアントを該当する ELAN に割り当てることができます。

```
(Ethernet ELAN Type,  LES_1)  (Max Frame Size = 4544,  LES_1)
(Token-Ring ELAN Type, LES_2)  (Max Frame Size = 4544,  LES_2)
(Token-Ring ELAN Type, LES_2)  (Max Frame Size = 18190, LES_2)
```

TLV に関するその他の情報

TLV は、ELAN ベースで定義されます。したがって、特定の ELAN に割り当てられるすべての LE クライアントに、同じ TLV セットが戻されます。構成応答に TLV が含まれている場合、LE クライアントは TLV に指定されている値を動作パラメー

ターとして使用することが必要です (LE クライアントがその ELAN タイプを認識できる場合)。TLV が有益と考えられる状況の例を、以下にいくつか挙げます。

- ELAN が地理的に大きな場所に広がっている場合は、LE クライアントのデフォルトのタイムアウト値では不十分な場合があります。すべての LE クライアントのタイムアウト値は、LECS で TLV にそれぞれの値を指定することによって制御できます。
- デフォルトでは、ELAN はベストエフォート・コネクションを使用して BUS に接続します。BUS トラフィックが多い ELAN の場合、BUS への予約帯域幅接続を使用することにより、性能の向上を図ることができます。LE クライアントと BUS 間のマルチキャスト・センド VCC の特性は、TLV を用いて制御することができます。
- TLV を使用して、ELAN セグメント番号をソース・ルート・ブリッジにダウンロードすることができます。

TLV は、構成の微調整に加えて、ELAN 上のすべてのクライアントが矛盾のないパラメーターで動作することを要求します。IBM 2210 は、すべての ATM フォーラム定義の TLV、ならびに任意のユーザー定義の TLV をサポートします。

LES への接続

LES への ATM アドレスを入手した後、LE クライアントは LES へのコントロール・ダイレクト VCC を開始します。この VCC が確立されると、LE クライアントは LE_JOIN_REQUEST を LES に送信します。LES は、LE クライアントを該当するポイント・マルチポイント間コントロール・ディストリビュート VCC に追加し、LE_JOIN_RESPONSE を戻して応答します。デフォルトでは、298ページの図15に示すように、LES はプロキシ・クライアントと非プロキシ・クライアントを区分して、別々のコントロール・ディストリビュート VCC に割り当てますが、必要なポイント・マルチポイント VCC の数を減らすために、すべての LE クライアントに対して単一のコントロール・ディストリビュート VCC を使用するように構成することも可能です。VCC を区分すると、非プロキシ・クライアントに送信される妨害トラフィックが減るので、一般的には有用です。298ページの『アドレス解決』で説明するように、LE_ARP_REQUEST が非プロキシ LE クライアントに送信されることはありません。

LAN エミュレーションの概説

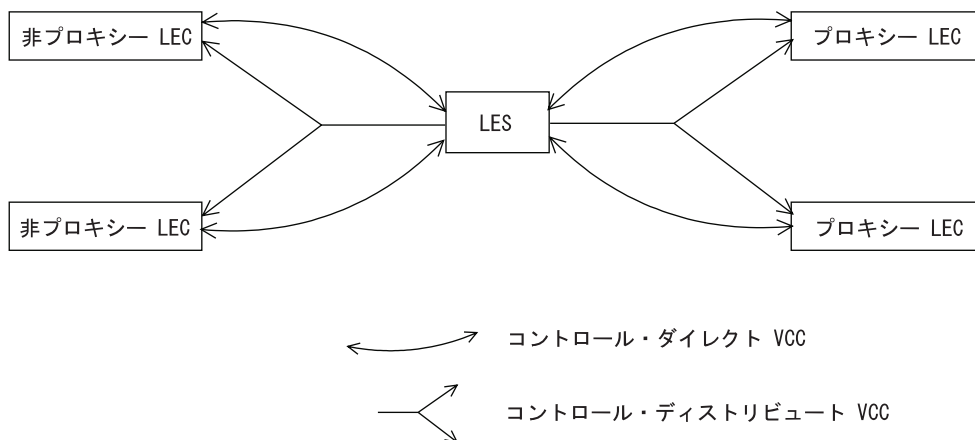


図 15. LE クライアントと LES 間のデフォルト接続

LE クライアントと LES 間に、以下の ATM 接続が確立されます。

コントロール・ダイレクト VCC (双方向、ポイント・ポイント)

LE クライアントから LES へ

コントロール・ディストリビュート VCC (ポイント・マルチポイント)

LES から LE クライアントへ

アドレス登録

LE クライアントは、LAN あて先を LES に登録して固有性を確保し、LES が LE_ARP_REQUEST (LE クライアントが、特定の LAN あて先に対応する ATM アドレスを確認するために出す) に応答できるようにします。登録するのは、LAN あて先と、LE クライアントがその LAN あて先に対応付ける ATM アドレスです。LAN あて先は、MAC アドレスまたはルート記述子のいずれでも構いません。

プロキシー LE クライアントは、それが ELAN にブリッジしている LAN セグメント上のステーションの MAC アドレスを登録しません。これに対して、非プロキシー LE クライアントは、それが表す LAN あて先をすべて登録する必要があります。ルート記述子は、対応する LE クライアントがプロキシーであるか、非プロキシーであるかに関係なく、すべて登録する必要があります。ルート記述子を適用できるのは、ソース・ルート・ブリッジングを実行しているプロキシー LEC だけです。ルート記述子には、プロキシー LE クライアントのブリッジ番号と、LE クライアントがブリッジしている先のリンクのセグメント番号 (1 ホップの隔たりに相当する) が入っています。

アドレス解決

LAN 通信は、発信元とあて先の MAC アドレスが基礎になります。このような通信を ATM ネットワーク上で可能にするためには、MAC アドレスを ATM アドレス変換 (解決) することが必要です。LE クライアントは、LE_ARP_REQUEST を LES に送信して、特定の LAN あて先の ATM アドレスを確認します。LAN あて先が登録されている場合、LES はその LAN あて先に対応する ATM アドレスで応答します。そうでない場合は、要求はコントロール・ディストリビュート VCC 上のすべてのプ

ロキシー LE クライアントに転送されます。非プロキシー LEC は、それぞれの LAN あて先がすべて登録されているので、要求を転送する必要はありません。ただし、LES が単一のコントロール・ディストリビュート VCC を使用するように構成されている場合には、プロキシーおよび非プロキシーの両方の LE クライアントが要求を受け取ることになります。コントロール・ディストリビュート VCC は、LES が複数の LE クライアントに制御フレームを配布するための効率的な手段を提供します。

プロキシー LE クライアントは、それが表す未登録 MAC アドレスに対する LE_ARP_REQUEST に応答します。LE_ARP_RESPONSE は、コントロール・ダイレクト VCC で LES に送信され、LES は要求を出した LE クライアントに応答を転送します。

BUS への接続

LES に接続した後、LE クライアントはオール 1 の同報通信 MAC アドレスに対して LE_ARP_REQUEST を出します。LES は、BUS の ATM アドレスで応答します。次に LE クライアントは、BUS へのマルチキャスト・センド VCC の確立を開始します。BUS は、LE クライアントを該当するポイント・マルチポイント間マルチキャスト・フォワード VCC に追加することによって応答します。デフォルトでは、プロキシー・クライアントと非プロキシー・クライアントを区分して、別々のマルチキャスト・フォワード VCC に割り当てますが、コントロール・ディストリビュート VCC の場合と同様に、すべての LE クライアントに対して単一のマルチキャスト・フォワード VCC を使用するように BUS を構成することも可能です。図16 は、分割されたマルチキャスト・フォワード VCC を示します。

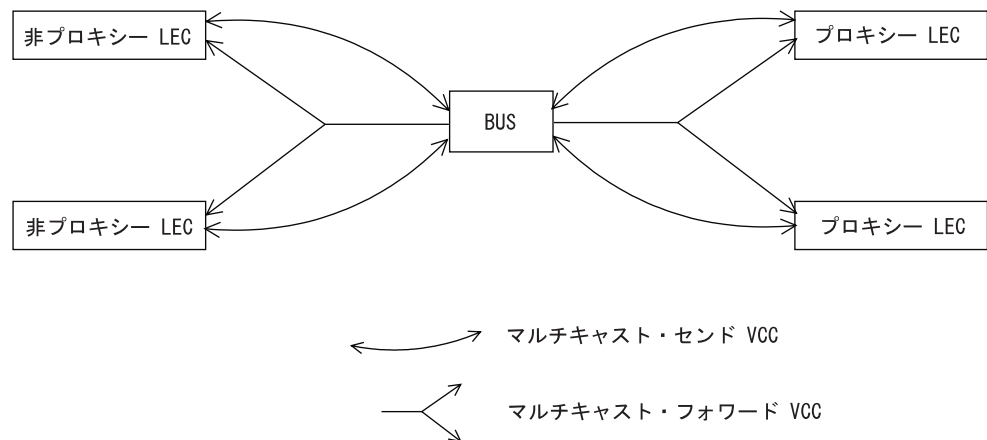


図16. LE クライアント (LEC) と BUS 間のデフォルト接続

LE クライアントと BUS 間に確立される ATM 接続を明確にするために、次のリストを示します。

マルチキャスト・センド VCC (双方向、ポイント・ポイント)

LE クライアントから BUS へ

マルチキャスト・フォワード VCC (ポイント・マルチポイント)

BUS から LE クライアントへ

BUS 機能

BUS には 2 つの基本機能があります。

1. マルチキャスト・フレームを ELAN 内のすべての LE クライアントに配布する。
2. ユニキャスト・フレームを該当するあて先に転送する。

LE クライアントがユニキャスト・フレームを BUS に送信するのは、あて先を表す LE クライアントへの直接接続がない場合です。BUS にネックが生じるのを避けるために、LE クライアントが BUS にユニキャスト・フレームを送信できる速度には制限があります。

このルーターの実現では、BUS には 2 つの動作モードがあります。つまり、ユニキャスト・フレーム・ドメインの区分化と、ユニキャスト・フレーム・ドメインの非区分化です。ユニキャスト・フレーム・ドメインを区分化した場合、BUS は 2 つのマルチキャスト・フォワード VCC を使用します。そうでない場合、BUS は単一のマルチキャスト・フォワード VCC を使用します。

単一のマルチキャスト・フォワード VCC が使用される場合、BUS の動作は非常に単純です。受信したすべてのフレームがすべての LE クライアントに転送されるだけです。2 つのマルチキャスト・フォワード VCC が使用される場合、BUS はユニキャスト・フレームをすべての LE クライアントに同報通信する必要はありません。代わりに、非プロキシ・クライアントあてのユニキャスト・フレームが、マルチキャスト・センド VCC であて先 LE クライアントに直接転送され、それ以外のすべてのユニキャスト・フレームは、プロキシ・マルチキャスト・フォワード VCC を使用して、プロキシ LE クライアントにだけ転送されます。2 つのマルチキャスト VCC が使用される場合、ルーターはインテリジェント BUS (IBUS) モードにあるものと見なされます。

IBUS では、妨害ユニキャスト・フレーム (クライアントあてでないユニキャスト・フレーム) が減ります。プロキシ・クライアントは非プロキシ・クライアント宛てのユニキャスト・フレームは受信せず、非プロキシ・クライアントが妨害ユニキャスト・フレームを受信することは決してありません。妨害フレーム専用のネットワーク帯域幅も減ります。一方、BUS の処理の所要量は増え、マルチキャスト・フレームは 2 回 (各マルチキャスト・フォワード VCC ごとに 1 回) 転送する必要があります。一般的には IBUS 動作が推奨されますが、非プロキシとして ELAN に加入するソース・ルート・ブリッジをもつ構成では、このオプションを使用不可にする必要があります。

データ・ダイレクト VCC の確立

データ・ダイレクト VCC は、2 つの LE クライアントを接続し、BUS が介在せずにユニキャスト・フレームを交換するのに使用されます。LE クライアントは、アドレス解決手順を使用して、必要な LAN あて先に対応する ATM アドレスを判別します。LE クライアントがすでにその ATM アドレスへのデータ・ダイレクト VCC を持っている場合 (おそらく、そのターゲット LE クライアントによって表される別の LAN あて先への)、以降のユニキャスト・フレームは既存の VCC 上で伝送されます。そうでない場合は、LE クライアントは信号プロトコルを起動して、新しい VCC を確立します。

LE クライアントは、LAN あて先と ATM アドレスのマッピングが入っている LE_ARP キャッシュを維持します。このキャッシュのエントリーはエージング (経時処理) されるので、定期的に更新する必要があります。LAN あて先からデータ・フレームを受信すると、エントリーは更新されます。データ・トラフィックがないときでも、LE クライアントはエントリーの更新を試みます。

また、データ・ダイレクト VCC の使用状況が監視され、VCC タイムアウト期間 (これは構成可能) にトラフィックがないと、VCC は解放されます。利用可能な資源が不十分なために新規データ・ダイレクト VCC を正常に確立できない場合も、LRU 方式で (最も古くに使用されたものから順に) データ・ダイレクト VCC が解放されます。

LAN エミュレーションの拡張機能の概説

IBM では、ルーター上で利用可能な ATM フォーラム LAN エミュレーションを機能強化して付加価値を付けました。これらの機能強化により、性能、信頼性、セキュリティ、および管理性の向上が図られています。

同報通信管理プログラム (BCM)

この機能は、ELAN の同報通信を減らすことにより、ネットワーク全体の性能を向上させます。

冗長度 冗長機構は、1 次サーバーに障害が生じたときにバックアップ・サーバーに引き継ぐことを可能にし、信頼性を高めます。

セキュリティ

LECS に ELAN メンバーシップを制御させることにより、セキュリティが向上します。

BUS モニター

この機能は、BUS の上位ユーザーを識別することにより、管理を強化します。

以下の各節では、これらの拡張機能のそれぞれについて説明します。

ブロードキャスト・マネージャー

ブロードキャスト・マネージャー (BCM) は、IBM による LAN エミュレーション BUS 拡張機能からなる LAN エミュレーションの拡張です。BCM がないと、以下の事象が起こります。

- BUS に送信されたマルチキャスト・フレームが、ELAN 上のすべての LE クライアントに転送される。
- ブリッジング・サポートを提供するためにプロキシ機能が組み込まれている LE クライアントは、同報通信フレームを他の LAN セグメントに転送する。
- すべてのエンド・ステーションが、すべての同報通信フレームを受信して処理する。

BCM は、個々の ELAN 上で次のプロトコルに対して使用可能にすることができます。

IP
IPX

LAN エミュレーションの概説

NetBIOS

BCM が使用可能の場合、BUS に送信される特定タイプの同報通信フレームの最少量のレイヤー 2 およびレイヤー 3 情報が復号されます。可能な場合はいつでも、BCM は同報通信フレームをユニキャスト・フレームに変換し、それを関係のある LE クライアントとエンド・ステーションにのみ送信します。BCM は、妨害同報通信フレームをフィルターすることにより、ネットワーク上の通信量および関連のエンド・ステーションの両方のオーバーヘッドを減らします。これらの機能により、システム全体の性能を高め、より大規模な ELAN の実用化を可能にします。

IP の BCM サポート

IP に対して使用可能にすると、BCM はすべての IP ARP 要求と応答をスキャンし、この ELAN を含む IP サブネット内の IP アドレスのロケーションを確認します。その目的は、BCM が各同報 ARP 要求フレームを受け取り、それをユニキャスト・フレームとして直接、ターゲット IP ステーションを表す LE クライアントに転送することです。要求は、マルチキャスト・フォワード VCC を通してすべての LE クライアントに同報通信されるのではなく、マルチキャスト・センド VCC で該当する LE クライアントに直接転送されるので、ネットワークの通信量とエンド・ステーションの処理の両方が削減されます。着信先ステーションがブリッジ機能の背後にある場合は、そのあて先ステーションが属する LAN も、同報通信通信量の削減の恩恵を受けることになります。

IPX の BCM サポート

IPX の場合、BCM は公示やその他の同報通信要求の範囲を制限します。IPX ルーターとサーバーは、それぞれが知っているネットワーク情報およびサービス情報を定期的に同報通信します。IPX クライアントは、同報通信要求を送信して、特定のサービスまたはルーターを見つけます。一般的には、これらの同報通信 (ルーティング情報プロトコル (RIP) およびサービス公示プロトコル (SAP) パケットと呼ばれます) は、他の IPX ルーターおよびサーバーのみが受信する必要があるものです。

IPX に対して使用可能にされている場合、BCM は伝送された公示に基づいて IPX ルーターとサーバーの集合を動的に識別し、RIP および SAP 公示およびその他の同報通信要求を、他の IPX ルーターおよびサーバーにのみ転送します。BCM IPX によって管理される同報通信フレームは、一連のユニキャスト・フレームとして、動的に確認された IPX ルーターとサーバーの組み合わせに送られます。

「BCM IPX サーバー・ファーム検出」が使用可能のとき、BCM IPX は指定の LEC の背後で見つかった IPX ルーターとサーバーの数が、構成可能な限界値 (BCM IPX サーバー・ファーム限界値) を超えると、IPX サーバー・ファームを検出します。サーバー・ファームが検出されると、BCM IPX はサーバー・ファーム内の各ダウンストリーム IPX ルーターとサーバーに個別に複数のユニキャスト・フレームを転送するのではなく、そのサーバー・ファームを代表する各 LEC に対して管理フレームを同報通信します。このように BCM IPX は、ネットワークの望まれる分野で、うまく同報通信メカニズムを活用できるようになりました。

BCM IPX BCM を使用可能にした場合は、IPX 公示を受信する必要があるクライアント装置 (つまり、IPX 公示を転送しない装置) を BCM 静的ターゲットとして構成

する必要があります。このような装置の例としては、IPX 公示を監視することにより IPX ネットワーク・トポロジーを検出するソフトウェアを実行するステーションがあります。

BCM IPX サーバー・ファーム検出が使用可能のときに、特定の LEC が BCM IPX によってサーバー・ファームとして扱われるのを防止したい場合には、その LEC の ATM アドレスと MAC アドレスを 00.00.00.00.00.00. と指定して BCM 静的ターゲットを構成します。これにより、たとえ検出されたルーターとサーバーの数が *BCM IPX* サーバー・ファーム限界値 を超えても、強制的に BCM IPX はこの LEC の背後で検出された各ダウンストリーム IPX ルーターとサーバーに対して、BCM が管理するフレームを複数のユニキャスト・フレームとして送信するようにされます。

NetBIOS の BCM サポート

NetBIOS は同報通信を多用するプロトコルと見なされているので、BCM には最適な用途です。NetBIOS 通信は名前に基づいて行われます。送信側ステーションは、照会を同報通信するか、フレームを NetBIOS 機能アドレスにマルチキャストすることによって、特定の着信名に対応する MAC アドレスを確認することができます。後者の場合、ネットワーク上のすべての NetBIOS 装置がフレームを受信し、フレームのあて先名が自身に該当するかどうかを判別する必要があります。さらに悪いことに、NetBIOS 装置は特定タイプのフレームの転送を 10 回も繰り返す傾向があります。従来、これはネットワークの輻輳（ふくそう）がひどい場合に、すべての装置が確実にフレームを受信できるようにするために取られた処置です。

BCM ストラテジーは、BUS に送信された NetBIOS フレームから名前を確認して、固有の NetBIOS 名を MAC アドレスと LE クライアントに対応付けます。固有の NetBIOS 名が確認された後は、その名前あての後続の NetBIOS 同報通信フレームは、単一の LE クライアントにユニキャスト・フレームとして転送されます。また、BCM は、繰り返し同報通信される特定の NetBIOS フレームをフィルターに掛けます。

BCM は、NetBIOS ネーム・シェアリングに対するサポートを提供します。すなわち、BCM NetBIOS は、同じ NETBIOS 名を共用する複数の LAN アダプターを持つ OS/2 LANServer ステーションを扱うことができます。

ソース・ルート・ブリッジの BCM サポート

ソース・ルート・マネージメント (SRM) は、802.5 ELAN 用に構成できる追加 BCM フィーチャーです。使用可能な場合、このフィーチャーは BCM IP または BCM NetBIOS によって管理されたフレームをさらに処理し、可能な場合はいつでも、全ルート探索 (ARE) またはスパンニング・ツリー探索 (STE) フレームを特別ルート・フレーム (SRF) に変換します。フレームを SRF に変換すれば、そのフレームはブリッジ・ネットワークの各リングに転送する必要がなくなります。

各 LE クライアントの背後のトークンリング・トポロジーは、BUS が受信したフレームのルーティング情報フィールド (RIF) を記録することによって確認されます。SRM はトークンリング・トポロジー情報を動的に確認するので、エージング (経年処理) 機構を使用して、最近更新されていない情報を除去します。

LAN エミュレーションの概説

BCM または SRM (あるいは、その両方) を使用可能にするかどうかを決める際は、ネットワーク・システム全体の利益と、BCM または SRM を使用可能にした場合に避けられないパケット転送速度の低下とを比較検討する必要があります。

注: ブロードキャスト・マネージャーおよびソース・ルート・マネージメント機能は、**bus-mode** が *adapter* または *vcc-splice* に設定されている場合は利用できず、使用可能にすることはできません。

LAN エミュレーションの信頼性

確実性の欠如が、これまでの LAN エミュレーションに対する最も大きな批判の 1 つでした。ATM フォーラムでは、LE サービス配布の仕様を用いてこの問題の解決に取り組んでいますが、ルーターはその中間解答の 1 つを提供するものです。図17は、MSS 冗長問題の解決の枠組みを示しています。

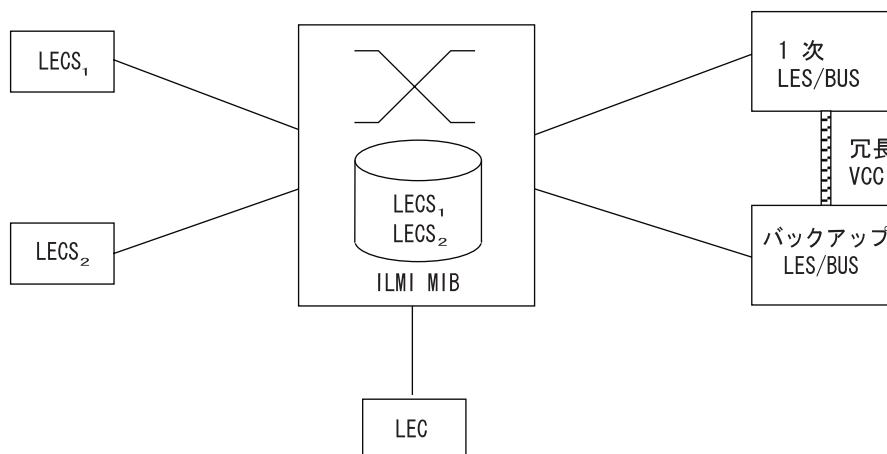


図17. LAN エミュレーションの冗長度

各 LES/BUS を独立して構成することにより、冗長度をもたせることができます (デフォルトでは冗長度なし)。冗長度が使用可能な場合、LES/BUS は 1 次またはバックアップの役割を担うように構成されます。冗長 LES/BUS として構成されていない場合は、LES/BUS は 1 次です。通常は、LE クライアントから見える LES/BUS は、1 次 LES/BUS だけです。これがバックアップ LES への冗長 VCC の設定と維持の責任を持ちます。この VCC が存在し、折よく状況メッセージが出ると、1 次 LES/BUS が運用可であることを示しています。

拡張冗長 VCC が存在 **しない** 場合、バックアップ LES/BUS は通常通りに ELAN 要求にサービスします。拡張冗長 VCC が 1 次によって確立されるときに、バックアップ LES/BUS が ELAN にサービスしている場合、振る舞いは LES/BUS ピア冗長サポートの設定によって決定されます。

ピア冗長サポートを確立すると、1 次とバックアップの LES/BUS の間で拡張冗長 VCC が確立された後も、クライアントがバックアップ LES/BUS でアクティブでいられます。冗長サポートが使用可能にされているが、ピア冗長が使用不可にされるとき、拡張冗長 VCC が確立されるときに、バックアップはそのすべてのクライアントを終わらせ、常に 1 次 LES/BUS に譲ります。冗長とピア冗長サポートが両方とも

使用可能にされ、拡張冗長 VCC がアップであるとき、1 次とバックアップの LES/BUS は、アクティブ・クライアントの数を含む状況メッセージを相互に伝送します。拡張冗長 VCC が確立された時点で、1 次およびバックアップの LES/BUS がそれぞれアクティブ・クライアントをもっている場合、アクティブ・クライアントの数が少ない方の LES/BUS がそのクライアントを終わらせ、アクティブ・クライアントの数が多き方の LES/BUS に譲ります。アクティブ・クライアントの数が等しい場合、バックアップ LES/BUS が 1 次に譲ります。1 次とバックアップがほぼ同時に動作可能になるような競合状態で 1 次 LES/BUS を優先するために、バックアップがそれ自身を ATM スイッチに登録して 1 分以内に拡張冗長 VCC が確立された場合には、バックアップが 1 次に譲ります。

単純にするために、1 次 LES/BUS だけがピア冗長オプションをもちます。直前のリリースの ルーター ソフトウェアの冗長動作を維持するため、デフォルトではピア冗長が使用不可にされます。

冗長プロトコルが有効であるためには、LE クライアントは 1 次 LES/BUS を検出し、バックアップに接続しなければなりません。LE クライアントは VCC の解放によってサーバーの障害を検出します。バックアップ LES/BUS への接続は、LECS を介して行われます。

LE_CONFIGURE_REQUEST を受信すると、LECS は LE クライアントを該当する LES および ELAN に割り当てます。この LES にバックアップが構成されていない場合、LECS は LES の ATM アドレスを戻します。LES にバックアップ LES が構成されている場合には、LECS は 1 次またはバックアップ LES アドレスを戻します。

LECS がバックアップ LES アドレスを戻すのは、バックアップ LES が LECS と同じ MSS サーバー上に存在し、現在 ELAN として機能している場合、1 次 LES が LECS と同じ MSS サーバー上に存在し、現在 ELAN として機能していない場合、あるいはどちらの LES も LECS と同じ MSS サーバー上に存在せず、クライアントが 1 次 LES に割り当てられた最後のクライアントである場合 (過去 5 分以内) です。それ以外の場合は、1 次 LES アドレスが LE クライアントに戻されます。

LECS は、すべてのクライアント割り当ての短期メモリーを保存し、LE クライアントの割り当てを 1 次とバックアップ LES の間で交代できるようにしています。この単純な手法は、実質的に無障害で正しい割り当てを行い、自動修正します。最悪の場合でも、この手法は、LE クライアントを ELAN に加入させる構成フェーズを繰り返すだけです。

LECS 確実性は、複数のプラットフォームに重複 LECS を設定し、それらの ATM アドレスを ILMI データベースに含めることによって達成できます。これで、1 次 LECS が利用不能の場合に、LE クライアントはバックアップ LECS に接続できるようになります。

LAN エミュレーションのセキュリティー

従来型の LAN では、物理接続により、2 つのステーションが同じ LAN 上にあることが暗黙に示されるので、その意味ではセキュリティーが提供されています。複数のエミュレートされた LAN が単一の ATM ネットワーク上に存在できるので、ELAN 上に存在しないステーションが ELAN 上のステーションに物理的に接続することが可

LAN エミュレーションの概説

能です。このような状態では、不許可ステーションが LES に接続し、そのサービスの使用を試みることができるので、セキュリティー上の危険が生じます。

ELAN メンバーシップを制御するために、LECS で LE_JOIN_REQUEST を検証するように MSS LES を構成することができます。このモードでは、LES は LE_JOIN_REQUEST からの情報を使用して、LE クライアントに代わって、LE_CONFIGURE_REQUEST を作成します。これらの LE_CONFIGURE_REQUEST には、IBM セキュリティー TLV とともに、発信元 LAN あて先、発信元 ATM アドレス、ELAN タイプ、最大フレーム・サイズ、LE_JOIN_REQUEST からの ELAN ネームが入っています。セキュリティー要求は、LECS インターフェースと呼ばれる多重化コンポーネントによって LECS に転送され、LECS はその要求を ELAN 割り当てデータベースを用いて検証してからでないと、LE クライアントは ELAN への加入を認められません。

LECS インターフェースは ATM インターフェースに対応しており、ATM インターフェース上に構成されたすべての LES が同じ LECS インターフェースを使用します。LECS インターフェースは、複数の LES からのセキュリティー要求を多重化して単一の VCC で LECS に送ることにより、VCC 資源を節約します。LECS インターフェースは、ILMI および事前割り当て LECS アドレス機構を使用して、LECS を動的に見つけます。LECS への VCC を確立した後、LECS インターフェースはローカル照会を出して、LECS が同じルーター上にあるかどうかを調べます。LECS が同じルーター上にある場合は、ATM ネットワーク上に要求を転送しないで、ローカル・インターフェースを使用して、加入の要求を確認します。

LECS インターフェースを使用すると、ルーターは、LECS が結合を承認した場合にのみ LE クライアントは ELAN に結合されることを保証することができます。これにより、セキュリティーの責任が LES から LECS に移ります。しかし残念ながら、LECS も安全ではありません。LECS は、任意のステーションからの接続や照会を、検証せずに受け入れます。侵入したステーションが LECS に接続して、繰り返し各種の構成を照会する可能性があります。また、侵入したステーションが他のステーションを装って、別のステーションの構成をダウンロードする可能性もあります。

LECS アクセス制御は、ユーザーが LECS 構成データベースへのアクセスを許可しない ATM アドレス・プレフィックスのリストを構成できるようにします。リストに一致する ATM アドレスからのすべての LECS 接続の試みと LE_CONFIGURE_REQUEST が自動的に拒否されます。LECS インターフェースと合わせて使用すれば、安全な LANE 環境を提供することができます。

ELAN のセキュリティーを最大化するために、以下のステップを実行することをお勧めします。

1. LECS で、ATM アドレスを使用して、クライアントを LES に割り当てる。詳細については、292ページの『LECS 機能の概説』を参照してください。
2. ルーター上の LECS インターフェースを起動する。
3. LES のセキュリティー・オプションを起動する。
4. LECS へのアクセスを認めない ATM アドレス・プレフィックスに対して、LECS アクセス制御をアクティブにする。

5. ATM スイッチで アドレス・スクリーニング を使用する。このオプションにより、スイッチはコーリング・ステーションがコール設定で実際の ATM アドレスを使用しているかどうかを検証します。これにより、ステーションは他のステーションを偽装することはできません。

これらのステップにより、ステーションが正しく識別され、許可されたステーションのみが ELAN に加入することが保証されます。

LAN エミュレーションの主要な構成パラメーター

この節では、ルーターの LAN エミュレーション・コンポーネントの必須構成パラメーターについて、簡単に説明します。LAN エミュレーション・コンポーネントの ATM インターフェースを定義してからでないと、コンポーネントを作成することはできません。

1. LEC:

LE クライアントを作成するには、ELAN タイプを指定するだけです。1 つの ATM インターフェース上に 2 つの LE クライアントを定義し、それらを一緒にブリッジする場合には、LE クライアントの 1 つはデフォルト以外の MAC アドレスを使用することが必要です。デフォルトでは、LE クライアントは ATM インターフェースの出荷時設定 MAC アドレスを使用します。デフォルトの最大フレーム・サイズは、イーサネット LE クライアントの場合は 1516 バイトで、トークンリング LE クライアントの場合は 4544 バイトです。

LAN エミュレーションの概説

第19章 ATM の使用

この章では、ATM インターフェースの使用法について説明します。本章には、以下の節が含まれています。

- 『ATM および LAN エミュレーション』
- 『アドレスを入力する方法』
- 310ページの『ATM-LLC 多重化』
- 310ページの『ATM バーチャル・インターフェースの概念』

ATM および LAN エミュレーション

LAN エミュレーションは、ATM ネットワークを介するバーチャル・トークンリングおよびイーサネット LAN に対するサポートを提供します。ATM アドレッシングについては、『アドレスを入力する方法』を参照してください。

アドレスを入力する方法

アドレスを入力する方法は、アドレスが (1) IP アドレスであるか、あるいは (2) ATM アドレス、MAC アドレス、またはルート記述子であるかによって、2 通りの方法があります。

1. IP アドレス

IP アドレスは、小数点付き 10 進数で入力し、4 バイト・フィールドに 4 つの 10 進数 (0 ~ 255) をピリオド (.) で区切って指定します。

IP アドレスの例

01.255.01.00

2. ATM アドレス、MAC アドレス、またはルート記述子

ATM アドレス、MAC アドレス、およびルート記述子は、16 進文字列として入力し、バイト間の区切り文字を使用するかしないかは任意選択です、有効な区切り文字は、ダッシュ (-)、ピリオド (.), またはコロン (:) です。

ATM アドレス、MAC アドレス、またはルート記述子の例

A1FF01020304

or

A1-FF-01-02-03-04

or

A1.FF.01.02.03.04

or

39.84.0F.00.00.00.00.00.00.00.00.00.03.10.00.5A.00.DE.AD.08

or

A1:FF:01:02:03:04

or even

A1-FF.01:0203:04

各タイプのアドレスに必要な 16 進文字数は、それぞれ異なります。

ATM 40

MAC 12

ESI 12

ATM と LAN エミュレーションの構成

ルート記述子

4

この情報は、ATM、LAN エミュレーション、クラシカル IP と ATM を介する ARP、ATM を介する IPX、および ATM を介する ARP に対して入力するアドレスに適用されます。

ATM-LLC 多重化

ATM インターフェースを介して固有に実行されるプロトコルは、ATM-LLC 多重化を使用して、ATM アドレスと SVC および PVC の両方のチャンネルを、ユーザー間で共用することができます。ATM-LLC は、プロトコルを構成するときに暗黙に構成され、**t 5** から ATM Config+ コマンド・プロンプトを使用して監視することができます。ATM-LLC 多重化機能の明示的な構成オプションはありません。たとえば、ATM-LLC 多重化を使用する 2 つのプロトコルが同じローカル ATM アドレス (ローカル・エンドポイント) を使用するように構成されている場合、これは暗黙に、両方のプロトコルが同じ共用 ATM アドレスを使用するように構成していることとなります。

詳細については、327ページの『ATM-LLC 監視コマンド』を参照してください。

ATM-LLC 多重化機能を使用するプロトコルと ATM-LLC 多重化機能を使用しないプロトコル (クラシカル IP など) の間で、ATM アドレスまたは SVC/PVC チャンネルを共用することはできません。現在、ATM-LLC 多重化機能を使用できるプロトコルは、サーバー・キャッシュ同期プロトコル (SCSP) と APPN の 2 つだけです。

ATM バーチャル・インターフェースの概念

ATM バーチャル・インターフェース (AVI) は、実際には 1 つの物理インターフェースしか存在しないのに、複数の ATM インターフェースがあるような様相を呈します。装置上の各物理 ATM インターフェースごとに 1 つまたは複数の AVI を構成することができます。AVI には、次のような特性があります。

- 各 AVI は、1 つの (そして、1 つだけの) 物理 ATM インターフェースに定義する必要があります。以下では、物理 ATM インターフェースを意味するものとして、ATM 実インターフェース (ARI) を使用します。
- 装置上の各 ARI で 1 つまたは複数の AVI を構成することができます。
- 高位レイヤーのプロトコルは、ARI と AVI を同等に扱います。プロトコルは、ATM インターフェースの合計数を、装置上に構成された ARI と AVI の数の合計とみなします。
- プロトコルは、他のインターフェースからは独立して、各 ATM インターフェース (実または仮想) ごとに構成することができます。

たとえば、インターフェース 0 (これは、実 ATM インターフェース) では IP アドレス 9.1.1.1 を用いて IP を構成し、インターフェース 1 (これは AVI) ではアドレス 9.2.1.1 を用いて IP を構成することができます。インターフェースが実 ATM インターフェースであるか、実インターフェースに構成されたバーチャル・インターフェースであるかは、プロトコル (たとえば、IP) にとっては違いはありません。

せん。また、バーチャル・インターフェース 1 が、実 ATM インターフェース 0 上に構成されているのか、他の物理 ATM インターフェース上に構成されているのかも、プロトコルにとっては無関係です。

ATM バーチャル・インターフェースの使用による利点

ATM バーチャル・インターフェースを使用することによる主な利点は、次のとおりです。

- ATM バーチャル・インターフェース・フィーチャーを使用すると、物理 ATM インターフェースでサポートできるプロトコル・インスタンスが増えます。

ARI 上に構成できる AVI の実際数は、装置上で利用可能な物理資源 (メモリーなど) によって制限されます。作成できるインターフェースの合計数は、インターフェースのデータ・パケット・サイズによって異なりますが、最大数は装置当たり 253 に限定されています。

AVI を使用すると、ATM インターフェース当たり 1 インスタンス (または、アドレス) に制限されているプロトコル (IPX など) の構成オプションが、大きく改善されます。適切な数の AVI を構成することによって、各物理 ATM インターフェースが複数の IPX アドレスをサポートできるようになります。

- ATM バーチャル・インターフェース・フィーチャーは、ATM ネットワーク上のマルチキャスト・ルーティング・プロトコル (MOSPF など) をサポートするために欠かせないものです。

マルチキャストが正しく動作するためには、各論理サブネットを異なるインターフェース上に構成する**必要**があります。マルチキャスト・ルーティング・プロトコルは、通常、装置インターフェースから来たパケットは、決して同じインターフェースを介して送信しないという方法で動作するからです。つまり、あるインターフェースに 2 つ以上のサブネットが構成されており、あるサブネット内の発信元が、同じインターフェース上に定義された別のサブネット内のメンバーにマルチキャスト・パケットを送信する場合、このメンバーは決してそのパケットを受信することはありません。

各サブネットに対して個別のバーチャル・インターフェースを作成することによって、パケットのマルチキャストを正常に実行することができます。通常は、装置上の ATM インターフェースの数が制限され、そのために、マルチキャスト動作に正しく構成できるサブネットの数が制限されることとなります。しかし、AVI を (装置上に構成する必要があるサブネットの数に応じて) 必要な数だけ作成すれば、物理 ATM インターフェースの数によって、装置に構成できるサブネットの数が制限されることはなくなり、正しいマルチキャスト動作を行えるようになります。

たとえば、『one-armed』ルーターは、AVI フィーチャーがなければ、ELAN 以外のインターフェースを介したマルチキャスト・トラフィックをサポートできません。着信パケットは決して同じインターフェースから送信されることはなく、廃棄されてしまうからです。

- ARI 上に複数の AVI を作成し、同じ ARI 上の異なる AVI に異なるプロトコル・インスタンス (たとえば、各 IP サブネット) を構成することによって、性能の向上を図ることができます。

たとえば、1 つの物理 ATM インターフェース上に複数のサブネットが構成されている場合は、インターフェースは、最大伝送単位または MTU (そのインターフェー

ATM バーチャル・インターフェースの概念

スを介して送信または受信できる最大パケット・サイズ) を、同じインターフェースを共用するすべてのサブネットのうちの最小の MTU に減らすことが必要になります。しかし、その ARI に複数の AVI が作成されており、各 IP サブネットが異なる AVI 上に構成されている場合には、各サブネットは、同じ物理 ATM インターフェース上に構成された他のサブネットを考慮せずに、既存の MTU サイズを使用続けることができます。これにより、MTU サイズの縮小によるパケットの分割と再組み立てが原因でのスループットの低下や遅延を回避することができます。

さらに、物理インターフェースに構成されたプロトコル・アドレスの数を、同じ物理インターフェースに構成された異なるバーチャル・インターフェースに分散させることによっても、性能の向上を図ることができます。インターフェース当たりのプロトコル・リストが短縮されるので、探索が速くなり、処理時間を削減できるからです。

ATM バーチャル・インターフェースの使用による不利益

ATM バーチャル・インターフェースを使用した場合の不利益としては、以下のものがあります。

- AVI は独自の物理資源をもっていないので、各バーチャル・インターフェースで確立できるバーチャル・コネクション (VC) の数は、1 つの物理インターフェースで確立できる数より少なくなります。利用可能な資源 (この場合は、VC) は、1 つの ARI 上に構成された異なるバーチャル・インターフェースと ARI 自体の間で区分されます。

現行のインプリメンテーションでは、資源の割り当てはオンデマンド方式になっています。各物理 ATM インターフェースが資源をプールしており、これをすべての AVI と 1 つの ARI 自体が利用できるようになっています。

注: すべての資源が ARI とそのすべての AVI 間で共用されるので、ARI に追加された ESI は、自動的に ARI 上に構成されたすべての AVI で利用可能になります。同じ ARI を使用する 2 つの異なるプロトコル・クライアントに対しては、それらが異なる AVI 上に構成されていても、同じ ESI とセレクターの組み合わせを割り当てるべきではありません。

ARI と ARI 上に構成された AVI との間では、限定された PVC 共用が許されています。PVC の共用は、異なるプロトコル・インスタンスとの間での共用のみに限定されています。同じプロトコルの複数のインスタンスが同じ PVC を共用することはできません。

第20章 ATM の構成および監視

この章では、ATM インターフェースの構成コマンドおよびオペレーショナル・コマンドについて説明します。本章には、以下の節が含まれています。

- 『ATM インターフェース構成プロセスへのアクセス』
- 314ページの『ATM 構成コマンド』
- 314ページの『ATM インターフェース構成コマンド』
- 321ページの『ATM バーチャル・インターフェース構成コマンド』
- 327ページの『ATM バーチャル・インターフェース監視コマンド』
- 323ページの『ATM 監視プロセスへのアクセス』
- 323ページの『ATM 監視コマンド』
- 324ページの『ATM インターフェース監視コマンド (ATM INTERFACE+ プロンプト)』
- 327ページの『ATM-LLC 監視コマンド』

ATM インターフェース構成プロセスへのアクセス

構成プロセスにアクセスするには、以下の手順を使用します。

1. OPCON プロンプトで **talk 6** と入力する。(このコマンドの詳細については、33ページの『OPCON プロセスとは』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>
```

コンソールに CONFIG プロンプト (Config>) が表示されます。最初に構成に入ったときにプロンプトが表示されない場合は **Return** をもう一度押してください。

2. CONFIG プロンプトで **list devices** コマンドを入力して、装置が現在構成されているネットワーク・インターフェース番号を表示する。
3. インターフェース番号を記録する。ATM がインターフェースとして指定されていない場合は、Config> プロンプトで **add device** コマンドを使用して ATM インターフェースを作成する。
4. **network** コマンドと構成する ATM の番号を入力する。たとえば、次のように入力します。

ATM 構成プロンプト (ATM Config>) が表示されます。

ATM 構成コマンド

この節では、ATM 構成コマンドの要約を示します。コマンドは ATM config> プロンプトで入力します。

表 35. ATM 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Interface	<p>ATM Interface Config> プロンプトを表示するので、ここから ATM インターフェースをリスト、変更、または構成することができます。</p> <ul style="list-style-type: none"> • ESI を追加する • 現行構成をリストする、または ESI をリストする • ESI を除去する • ATM ネットワークのパラメーターを設定する • ESI を使用可能または使用不可にする • 終了する
Le-client	<p>LE Client Config> プロンプトを表示するので、329ページの『第21章 LAN エミュレーション・クライアントの使用』で説明しているように、LAN エミュレーション・クライアント・インターフェースをリスト、変更、または構成することができます。</p> <ul style="list-style-type: none"> • トークンリングまたはイーサネットのエミュレートされた LAN に対して、LAN エミュレーション・クライアント (LEC) を追加する。 • ネットワーク # により LEC を構成する。このコマンドは LE Config> プロンプトを表示するので、ここから特定の LAN エミュレーション・クライアント (LEC) を構成することができます。 • LAN エミュレーション・クライアント (LEC) をリストする。 • LAN エミュレーション・クライアント (LEC) を除去する。
Virtual ATM	<p>ATM Virtual Interface Config> プロンプトを表示するので、321ページの『ATM バーチャル・インターフェース構成コマンド』で説明しているように、ATM バーチャル・インターフェースをリスト、追加、または除去することができます。</p>
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

ATM インターフェース構成コマンド

この節では、特定の ATM インターフェースを構成するためのコマンドの要約を示し、個々のコマンドについて説明します。

ATM インターフェース構成コマンド (Talk 6)

コマンドは ATM INTERFACE> プロンプトで入力します。

表 36. ATM INTERFACE 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Add	ESI を追加します。
List	現行構成をリストするか、または ESI をリストします。
Qos	ATM I/F 0 QoS Config> プロンプトを表示するので、316ページの『QoS 構成』で説明しているように、サービス品質 (QoS) を構成することができます。
Remove	ESI を除去します。
Set	ATM ネットワークのパラメーターを設定します。
Disable	ESI を使用不可にします。
Enable	ESI を使用可能にします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Add

add コマンドは、ESI を ATM 構成に追加するのに使用します。

ATM アドレスのオクテット 14-19 は、エンド・システム識別子 (ESI) です。同じスイッチに接続されている各エンド・システムは、別々の ESI セットを使用しなければなりません。エンド・システムが起動すると、ILMI を使用して、その ESI を ATM スイッチに登録しようと試みます。スイッチは、すべての登録済み ESI が固有になるようにします。

構文:

add esi *esi-address*

esi *esi-address*

エンド・システム識別子のアドレス

有効値: 任意の 12 桁の 16 進数

デフォルト値: なし

List

list コマンドは、この ATM 装置の構成をリストしたり、あるいは構成された ESI の集合をリストするのに使用します。

構文:

list configuration

esi

configuration

ATM 装置構成をリストします。リストされたフィールドの説明は、316ページの『Set』を参照してください。

例: **list con**

ATM インターフェース構成コマンド (Talk 6)

ATM Configuration

```
Interface (net) number = 0
Maximum VCC data rate Mbps = 155
Maximum frame size = 9234
Maximum number of callers = 209
Maximum number of calls = 1024
Maximum number of parties to a multipoint call = 512
Maximum number of Selectors that can be configured = 200
UNI Version = UNI 3.0
Packet trace = OFF
```

esi ATM 構成内の ESI をリストします。

例: **list esi**

```
ATM INTERFACE> list esi
```

ESI	Enabled
0000000000009	YES
0000000000100	YES

QoS 構成

qos-configuration コマンドを使用すると ATM I/F 0 QoS Config> プロンプトが表示されるので、『QoS 構成』で説明しているように、サービス品質 (QoS) を構成することができます。

構文:

qos-configuration

Remove

remove コマンドは、ESI を ATM 構成から除去するのに使用します。この ESI を使用しているすべての ATM コンポーネントは、別の ESI を使用するように再構成する必要があります。除去された ESI を使おうとする ATM コンポーネントは、次の装置のリスタート時には起動されない可能性があります。

構文:

```
remove esi esi-address
```

esi *esi-address*

エンド・システム識別子のアドレス

有効値: 任意の 12 桁の 16 進数

デフォルト値: なし

Set

set コマンドは、ATM ネットワーク・パラメーターを指定するのに使用します。

構文:

```
set max-callers
max-calls
max-config-selectors
```

ATM インターフェース構成コマンド (Talk 6)

max-data-rate

max-frame

max-mp-parties

network-id

trace

uni-version

max-callers

ATM インターフェースを使用する、装置上のエンティティの最大数を設定します。各 LEC、クラシカル IP クライアント、および 1483 ブリッジ・インターフェースは、ATM インターフェースのユーザーとしての資格があります。このパラメーターを増やすと、インターフェースのユーザーの数を増やすことができますが、システム・メモリーの使用量も増えます。

有効値:

64 ~ 1024 の範囲の整数

デフォルト値:

209

例:

```
ATM INTERFACE> set max-callers 25
```

max-calls

この ATM 装置上に存在できるスイッチド・バーチャル・サーキット (SVC) の最大数を設定します。すべてのポイント・ポイントおよびポイント・マルチポイント SVC は、システム資源を使用します。このパラメーターは、信号接続および交換接続用に予約されるシステム資源を制限するのに役立ちます。このパラメーターを増やすと、同時伝送する SVC の数を増やすことができますが、これらの接続を管理するために必要なシステム・メモリーも増えることになります。

有効値:

64 ~ 10500 の範囲の整数

デフォルト値:

1024

例:

```
ATM INTERFACE> set max-calls 500
```

max-config-selectors

ユーザーの特定の制御下にあるセレクターの最大数を設定します。

セレクターは、同じエンド・システム上の異なるユーザーを区別するのに使用されます。VCC 設定要求は、次のような階層方式でルート指定されます。つまり、ATM スイッチがネットワーク・プレフィックスを使用してあて先 ATM スイッチに転送します。あて先 ATM スイッチは、ESI を使用してあて先エンド・システムに転送します。そして、エンド・システムがセレクターに基づいてあて先ユーザーに通知します。

各 ESI は最大 255 個の対応するセレクター (0x00 ~ 0xff) をもつことができます。セレクターの範囲は、構成されるセレクター範囲と自動的に割り当

ATM インターフェース構成コマンド (Talk 6)

てられるセレクター範囲の 2 つに区分されています。構成されるセレクター範囲の上限は、ATM インターフェース・パラメーター `max-configured-selector` で定めます。

装置上の ATM コンポーネントは、さまざまな方法でセレクターを選択します。あるコンポーネントの場合は、構成されたセレクター範囲から、ユーザーが明示的にセレクターを構成する必要があります。別のコンポーネント (クラシカル IP クライアントなど) は、実行時に自動的にセレクターを割り当てることができます。ユーザーはセレクターを選択する必要はなく、装置が起動時にこれを選択します。このセレクターは、装置のリスタートのたびに一貫しているとは保証されません。自動的なセレクターの割り当ては、ネットワーク上の他の装置があらかじめその ATM アドレスを知っていなくても構わない ATM コンポーネントの場合にのみ便利です。

セレクターの範囲の相対サイズは、装置上の ATM ユーザーのタイプと数に適合するように変更することができます。

有効値:

0 ~ 255 (0x00 ~ 0xFF)

デフォルト値:

200

注: セレクターは、20 バイトの ATM アドレスのバイト 20 です。

例:

```
ATM INTERFACE> set max-config-selectors 225
```

max-data-rate *speed*

ほとんどの LANE および CIP 接続の VCC トラフィック・パラメーターのデフォルト値および上限を設定します。たとえば、これは LE クライアントが開始するベストエフォート VCC のデフォルト PCR です。シグナルされた SCR 数および PCR 数は、この限界を超えることはできません。たいいていの状況では、デフォルト値で十分です。この値を変更した方が有利な状況の一例として、大多数のステーションが 25-Mbps のアダプターを使用している場合があります。この場合は、VCC 上のデータ速度を 25 Mbps に制限して、低速のステーションが装置からのフレームに圧倒されないようにします。このパラメーターの単位は Mbps です。

有効値:

25

100

155

デフォルト値:

155

例:

```
ATM INTERFACE> set speed 155
```

max-frame

ATM インターフェース上で送信または受信されるデータに許されるオクテットの最大数を設定します。このパラメーターに基づいて、システム・メモリーが割り当てられます。max-frame を増やすと、システム・メモリーの所要量がふえますが、より大きなフレームを処理できるようになります。

ATM インターフェース構成コマンド (Talk 6)

ATM インターフェースを使用するすべての装置エンティティは、ATM インターフェースの `max-frame-size` 以下の最大フレーム・サイズを使用する必要があります。これには、すべての LEC および 1483 ブリッジ・インターフェースが含まれます。

有効値:

512 ~ 31000 の範囲の整数

デフォルト値:

9234

例:

```
ATM INTERFACE> set max-frame 1000
```

max-mp-parties

装置が開始するポイント・マルチポイント接続上のリーフの最大数を設定します。このパラメータは、システム・メモリの割り当てに影響を与えます。装置が多数のあて先へのポイント・マルチポイント接続を設定する必要がある場合は、この値を増やすことが必要です。

有効値:

1 ~ 5000 の範囲の整数

デフォルト値:

512

例:

```
ATM INTERFACE> set max-mp-parties 300
```

network-id

ATM インターフェースのネットワーク ID を設定します。インターフェース間が ATM で接続されている場合は、複数の ATM インターフェースは同じネットワーク ID をもっていることが必要です。

有効値:

0 ~ 255

デフォルト値:

0

trace

インターフェース上のパケット・トレース・パラメータを設定します。パケット・トレースは、VPI/VCI 値の範囲で、使用可能または使用不可にすることができます。トレースの一般的な VPI/VCI 値は、次のとおりです。

- 信号パケットの場合は、0/5
- ILMI パケットの場合は、0/16

有効値:

on、off

デフォルト値:

off

トレースする VPI/VCI 範囲を入力するようにプロンプトで指示されます。

開始 VPI の有効値:

0 ~ 255

デフォルト値:

0

終了 VPI の有効値:

0 ~ 255

ATM インターフェース構成コマンド (Talk 6)

デフォルト値:

255

開始 VCI の有効値:

0 ~ 65535

デフォルト値:

0

終了 VCI の有効値:

0 ~ 65535

デフォルト値:

65535

例:

```
ATM INTERFACE> set trace on
beginning of VPI range [0]? 0
end of VPI range [255]? 0
beginning of VCI range [0]? 5
end of VCI range [65535]? 5
```

uni-version

ATM インターフェースが、接続された ATM スイッチと通信するのに使用する、ユーザー・ネットワーク・インターフェース (UNI) バージョンを設定します。ATM スイッチおよび ATM 装置インターフェース上で、UNI バージョンが特定のバージョン (AUTO-DETECT ではなく) に構成されている場合は、その UNI バージョンと一致していることが必要です。

UNI バージョンが AUTO として構成されている場合、ATM 装置は使用する UNI バージョンをスイッチから確認しようと試みます。

UNI AUTO-DETECT モードでは、スイッチが UNI バージョンの照会に 응답しない場合、デフォルトは UNI 3.0 になります。スイッチが UNI 3.0 または UNI 3.1 以外の値を応答した場合、デフォルトは UNI 3.1 になります。

有効値:

[UNI 3.0|UNI 3.1|AUTO-DETECT|None]

デフォルト値:

UNI 3.0

注: ATM スイッチと一致していることが必要です。

例:

```
ATM INTERFACE> set uni-version 3.0
```

Enable

enable コマンドは、ATM 装置の構成内の ESI を使用可能にするのに使用します。ATM インターフェースは、起動されると、使用可能な ESI のみを登録しようと試みます。

構文:

enable esi *esi-address*

esi *esi-address*

エンド・システム識別子のアドレス

ATM インターフェース構成コマンド (Talk 6)

有効値:

任意の 12 桁の 16 進数

デフォルト値:

なし

例: **enable esi**

```
ATM INTERFACE> enable esi 00:00:00:00:00:09
```

Disable

disable コマンドは、構成内の ESI を使用不可にするのに使用します。使用不可にされた ESI を使用している ATM コンポーネントは、次回に装置がリスタートされるときには、アクティブになりません。

構文: **disable** esi *esi-address*

esi *esi-address*

エンド・システム識別子のアドレス

有効値:

任意の 12 桁の 16 進数

デフォルト値:

なし

例: **disable esi**

```
ATM INTERFACE> disable esi 00:00:00:00:00:09
```

バーチャル ATM インターフェース構成プロセスへのアクセス

選択された実 ATM インターフェースの ATM Config> プロンプトから、**Virtual ATM** コマンドを使用して、バーチャル ATM 構成コマンド・モードに入ります。

ATM バーチャル・インターフェース構成コマンド

この節では、ATM バーチャル・インターフェース構成コマンドの要約を示します。コマンドは ATM virtual interface config> プロンプトで入力します。

表 37. ATM バーチャル・インターフェース構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Add	バーチャル ATM インターフェースを追加します。
List	現在構成されているバーチャル ATM インターフェースをリストします。
Remove	バーチャル ATM インターフェースを現行構成から除去します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

ATM バーチャル・インターフェース構成コマンド (Talk 6)

Add

add コマンドは、ATM バーチャル・インターフェースを追加するのに使用します。新規の ATM バーチャル・インターフェースが、対応する ATM 実インターフェース (この ATM バーチャル・インターフェースにアクセスするのに使用した構成メニュー) に追加されます。新たに作成された ATM バーチャル・インターフェースに割り当てられたネット/インターフェース番号が表示されます。

構文:

add

例:

```
ATM Virtual Interface config> add
Added ATM Virtual Interface Net as interface 5 on physical ATM interface 0
ATM Virtual Interface config>
```

List

list コマンドは、現行の実 ATM インターフェースに定義された構成済み ATM バーチャル・インターフェースをリストするのに使用します。

構文:

list

例:

```
ATM Virtual Interface config> list

                        ATM Virtual Interface Nets
-----
  ATM interface number = 0
  ATM Virtual Interface Net interface number = 5

ATM Virtual Interface config>
```

Remove

remove コマンドは、ATM バーチャル・インターフェースを除去するのに使用します。実 ATM インターフェース上の、指定されたインターフェース番号をもつバーチャル ATM インターフェースが、SRAM 構成レコードから除去されます。インターフェース番号を指定しなかった場合は、この実 ATM インターフェース上の最後の ATM バーチャル・インターフェースが削除されます。疑問符 (?) を入力すると、現行の実 ATM インターフェース上のすべての ATM バーチャル・インターフェースがリストされ、そのリストから削除したいインターフェースを選択することができます。

構文:

remove *n*

例: **remove 5**

```
Virtual ATM 5 deleted successfully.
ATM Virtual Interface config>
```

ATM 監視プロセスへのアクセス

構成プロセスにアクセスするには、以下の手順を使用します。このプロセスにより ATM の監視 プロセスにアクセスできます。

1. OPCON プロンプトで **talk 5** と入力する。(このコマンドの詳細については、33ページの『OPCON プロセスとは』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
+
```

GWCON プロンプト (+) がコンソールに表示されます。最初にコンソール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 **interface** と入力して、構成されたインターフェースのリストを表示する。
3. インターフェース番号を記録する。
4. **network** と入力し、続けて ATM インターフェースの番号を入力する。

```
+ network 1
ATM+
```

ATM 監視プロンプト (ATM+) が表示されます。

ATM 監視コマンド

この節では、ATM インターフェースを監視するための ATM コンソール・コマンドの要約を示します。コマンドは、ATM+ プロンプトで入力します。

表 38. ATM 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Interface	ATM Interface+ プロンプトを表示するので、324ページの『ATM インターフェース監視コマンド (ATM INTERFACE+ プロンプト)』で説明しているように、ATM インターフェースを監視することができます。
Atm-llc	ATM LLC+ プロンプトを表示するので、エンドポイント、一連のユーザー・クライアントおよび一連の ATM チャンネルを監視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。 13ページの『下位レベル環境の終了』を参照してください。

Interface

324ページの『ATM インターフェース監視コマンド (ATM INTERFACE+ プロンプト)』で説明している ATM Interface+ プロンプトを表示します。

構文:

```
interface
```


ATM インターフェース監視コマンド (Talk 5)

- VCCs
- 予約帯域幅

circuit 特定の VCI-VPI 組みを指定することにより、特定の VCC の統計をリストします。コマンド行で回線を指定することもできます (たとえば、list circuit 33)。

例:

```
ATM INTERFACE+ list circuit
VPI [0]?
VCI [32]?33
```

```
Frames transmitted = 2 Bytes transmitted = 216
Frames received = 2 Bytes received = 216
```

vccs 装置によって確立されたすべての VCC をリストします。VCC は、パーマネント (PVC) またはスイッチド (SVC)、ポイント・ポイントまたはポイント・マルチポイントで、それぞれ固有の VPI/VCI によって識別されます。trace コマンドは、VCC の VPI/VCI 値を使用して、特定の VCC 上でパケット・トレースを実行します。

例:

```
P-P ポイント・ポイント VCC
P-MP ポイント・マルチポイント VCC
ILMI インターリム・ローカル管理インターフェース VCC
SAAL 信号 VCC
Bx-y VPI x、VCI y への内部結合 VCC
Sx-y VPI x、VCI y への内部スプライス VCC
```

reserved-bandwidth

ATM インターフェース上の予約帯域幅をリストします。

例:

```
ATM INTERFACE+ list reserved-bandwidth
Line Rate : 155000 Kbps
Peak Reserved Bandwidth : None
Sustained Reserved Bandwidth : None
```

Trace

trace コマンドは、指定された範囲の VPI/VCI 値に対するパケット・トレースを起動するのに使用します。235ページの『View』で説明しているように、ELS を使用してトレース・データを表示することができます。

構文:

```
trace list
           on
           off
```

list ATM インターフェース上の現行のパケット・トレース・オプションを表示します。

例:

ATM インターフェース監視コマンド (Talk 5)

```
ATM Interface+ trace
on | off | list []? list
Packet trace is ON
Range of VPIs to be traced:      0 -      0
Range of VCIs to be traced:     32 -     39
```

on 指定された VPI/VCI 範囲内のすべてのアクティブ VCC 上のパケット・トレースを開始します。

例:

```
ATM Interface+ trace on
beginning of VPI range [0]?
end of VPI range [0]?
beginning of VCI range [32]?
end of VCI range [65535]? 39
```

off すべての VCC 上のパケット・トレースを停止します。

例:

```
ATM Interface+ trace off
ATM Interface+ trace list
Packet trace is OFF
```

Wrap

wrap コマンドは、アダプターの ATM インターフェース上でループバック・データ・テストを実行するのに使用します。Wrap は、VPI-VCI の組を指定することにより、VC 単位で出すことができます。データは内部でループバックされます。

ラップの開始、ラップの停止、または現行ラップ設定値の表示を、選択的にスタートさせることができます。

ラップを停止または表示すると、以下の統計が表示されます。

- ラップ送信数
- ラップ受信数
- ラップ送信エラーの数
- ラップ受信エラーの数
- ラップ受信タイムアウト数

表示の場合は、現行ラップ統計が表示されます。

停止の場合は、最終ラップ統計が表示されます。

構文:

```
wrap                display
                    start
                    stop
```

display

現行ラップ設定値を表示します。

start ラップ手順を開始し、パターンの VPI-VCI 長さパターン自体を指定します。

例:

ATM インターフェース監視コマンド (Talk 5)

```
ATM Interface+ wrap start
VPI [0]?
VCI [32]?
wrap pattern length [32]?
Enter 32-byte wrap pattern: [ABCDEFGHIJKLMNOPQRSTUVWXYZ123456]?
```

stop ラップ手順を停止し、最終ラップ統計を表示します。

ATM-LLC 監視コマンド

この節では、ATM LLC 多重化のためのコマンドについて説明します。

コマンドは ATM-LLC+ プロンプトで入力します。

表 40. ATM LLC 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
List	各種のオプションをリストします。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、さまざまなカテゴリーの ATM LLC 監視データをリストするのに使用します。

構文:

```
list                               endpoints
list                                 channels
```

endpoints

装置上の ATM-LLC 多重化機能を使用するプロトコルによって使用される ATM アドレスをリストします。エンドポイントは、エンド・システム識別子とセレクターとして表示されます。

例: **list endpoints**

```
ATM-LLC+ list endpoints
```

channels

装置上の ATM-LLC 多重化機能を使用するプロトコルによって使用されるチャンネルをリストします。

例: **list channels**

```
ATM-LLC+ list channels
```

ATM バーチャル・インターフェース監視コマンド

ATM バーチャル・インターフェースの監視は、ATM LLC 監視コマンドを使用して行います。詳細については、『ATM-LLC 監視コマンド』を参照してください。

ATM バーチャル・インターフェース監視コマンド (Talk 5)

第21章 LAN エミュレーション・クライアントの使用

この章では LAN エミュレーション・クライアント (LEC) について説明します。本章には、以下の節が含まれています。

- 『LAN エミュレーション・クライアントの概要』

LAN エミュレーション・クライアントの概要

ルーター上の LEC は、従来のルーターおよびブリッジ上の『プロンプト』または『インターフェース』の役目を果たします。ルーターは、LEC を介してトラフィックを送受信することによって、ポート間のトラフィックをブリッジおよびルートします。

LEC には、次の 2 つのプロンプト・レベルがあります。

1. LE Client Config> では、すべての LEC の環境を制御するコマンドを入力できます。このプロンプト・レベルのコマンドについては、331ページの『LAN エミュレーション・クライアントの構成』で説明します。
2. コマンドの 1 つの **config** を使用すると、もう 1 つのプロンプト・レベルである LEC Config> にアクセスします。ここでは、特定の LEC を構成するためのコマンドを入力できます。

LAN エミュレーション・クライアントに関するコマンドについては、以下で説明します。

第22章 LAN エミュレーション・クライアントの構成および監視

この章では、LAN エミュレーション・クライアント (LEC) の構成方法について説明します。本章には、以下の節が含まれています。

- 『LAN エミュレーション・クライアントの構成』
- 333ページの『ATM フォーラム準拠 LE クライアントの構成』
- 351ページの『LEC 監視環境へのアクセス』
- 352ページの『LEC 監視コマンド』

LAN エミュレーション・クライアントの構成

この節では、特定の ATM インターフェース上の LE クライアントの集合を表示、変更、および使用するためのコマンドについて説明します。

LE Client Config> プロンプトにアクセスするには、314ページの『ATM 構成コマンド』で説明しているように、ATM Config> プロンプトで **le-c** と入力します。

コマンドは、314ページの『ATM 構成コマンド』で説明しているように、ATM Config> プロンプトのものと LE Client Config> プロンプトで入力します。

表 41. LAN EMULATION クライアント構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Add	以下のタイプの ATM フォーラム準拠のエミュレートされた LAN アーキテクチャーの LEC を追加します。 <ul style="list-style-type: none">• イーサネット• トークンリング
Config	LEC Config> プロンプトを表示するので、ここから特定の LAN エミュレーション・クライアントを構成することができます。
List	LEC をリストします。
Remove	LEC を削除します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Add

add コマンドは、トークンリングまたはイーサネット・エミュレート LAN の LEC を追加するのに使用します。

構文:

```
add Ethernet  
                  Token Ring
```

token-ring

トークンリング・エミュレート LAN

LE Client Config>

例: add token ring

```
LE Client Config> add token-ring
Added Emulated LAN as interface 3
```

ethernet

イーサネット・エミュレート LAN

例: add ethernet

```
LE Client Config> add ethernet
Added Emulated LAN as interface 2
```

Config

config コマンドを使用すると、LEC Config> プロンプトが表示されるので、ここから特定の LAN エミュレーション・クライアントの詳細を構成することができます。

構文:

config interface#

interface#

LEC が構成に追加されたとき、ルーターによって割り当てられた整数の番号。LEC に割り当てられているインターフェース番号を調べるときは、**list** コマンドを使用します。

例: **config**

```
LE Client Config> config 3
ATM LAN Emulation Client configuration
```

List

list コマンドは、LAN エミュレーション・クライアントをリストするのに使用します。

構文:

list

例:

```
LE Client Config> list
ATM Forum Compliant Emulated LANs
-----
Physical ATM interface number = 0
LEC interface number = 1
Emulated LAN type = Token Ring Forum Compliant
Emulated LAN name =
```

Remove

remove コマンドは、LEC を除去するのに使用します。LEC が構成に追加されたときにルーターによって割り当てられたインターフェース番号を指定する必要があります。LEC に割り当てられているインターフェース番号を調べるときは、**list** コマンドを使用します。

構文:

remove interface#

interface#

ルーターによって割り当てられた整数の番号

ATM フォーラム準拠 LE クライアントの構成

このプロセスを使用して、該当する LEC Config> プロンプトにアクセスすることができます。

1. LE Client Config> プロンプトで **config** コマンドを使用して、該当する LEC インターフェイス番号にアクセスするか、**network** 構成コマンドを該当する LEC インターフェイス番号と一緒に使用する。
2. Ethernet Forum Compliant LEC Config> プロンプトまたは Token Ring Forum Compliant LEC Config> プロンプトで該当するコマンドを入力する。下表のコマンドは、指摘されているものを除いて、トークンリング LEC およびイーサネット LEC の両方に適用されます。

この節では、ATM フォーラム準拠 LAN エミュレーション・クライアントを構成するためのコマンドについて説明します。

表 42. LAN エミュレーション・クライアントの構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
ARP-Configuration	ATM フォーラム準拠クライアントの LE-ARP 構成を構成することができます。
Frame	NetWare IPX カプセル化タイプを設定します。
IP-Encapsulation	IP カプセル化を、イーサネット (タイプ X'0800') または IEEE (SNAP 付き 802.3) として設定します。イーサネット LEC にのみ適用されます。
List	LAN エミュレーション・クライアント構成をリストします。
LLC	トークンリング LEC の LLC Config> 構成プロンプトにアクセスします。
QoS-Configuration	elan-x LEC QoS Config> プロンプトを表示するので、ここから フィーチャーの使用と構成 の LE クライアント QoS 構成コマンドで説明されているサービス品質を構成することができます。
RIF-Timer	RIF 内の情報が更新される前に維持されている最大時間数を設定します。トークンリング LEC にのみ適用されます。
Set	LAN エミュレーション・クライアントのパラメーターを設定します。
Source-routing	ソース・ルート・ブリッジングを使用可能または使用不可にするのに使用します。トークンリング LEC にのみ適用されます。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

ARP Configuration

arp-configuration コマンドは、ATM フォーラム準拠 LAN エミュレーション・クライアントの静的 LE-ARP エントリを構成するのに使用します。

フォーラム LE クライアントの構成

構文:

arp-configuration

例:

```
Token Ring Forum Compliant LEC Config> arp-configuration  
ATM LAN Emulation Clients ARP configuration
```

表 43. ATM LAN エミュレーション・クライアント ARP 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Add	MAC またはルート記述子 ARP を使用して、LE-ARP キャッシュ・エントリーを追加します。
Config List	キャッシュ・エントリー QoS パラメーター値を設定します。構成された ARP キャッシュ・エントリーをリストします。
Remove	ARP キャッシュ・エントリーを除去します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Add

add コマンドは、MAC アドレスまたはルート記述子を使用して ARP キャッシュ・エントリーを追加するのに使用します。

MAC アドレスおよびルート記述子は、16 進文字列として入力し、バイト間の区切り文字を使用するかしないかは任意選択です。有効な区切り文字は、ダッシュ (-)、ピリオド (.), またはコロン (:)

構文:

```
add mac  
route-descriptor
```

例 1:

```
ARP config for LEC>add mac  
MAC address of LE ARP Entry []? 123456789098  
ATM address in 00.00.00.00.00.00:... form []? 390f0000000000000000000000000000123456789098  
Destination Type - REMOTE or LOCAL [Remote]?
```

例 2:

```
ARP config for LEC>add route 12.34  
ATM address in 00.00.00.00.00.00:... form []? 390f00000000000000000000000000001234567890988888  
ARP config for LEC>
```

Config

Config コマンドは、ATM フォーラム準拠 LAN エミュレーション・クライアントの固定 ARP キャッシュ・エントリー QoS パラメーターを構成するのに使用します。

構文:

```
config arp-entry-number
```


例:

```
ARP config for LEC> config
ARP entry number [1]
Configure LEC ARP entry
```

表 44. ATM LAN エミュレーション・クライアント ARP 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Set	QoS パラメーター値を設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Set:

Set コマンドは、ATM フォーラム準拠 LAN エミュレーション・クライアントの固定 ARP キャッシュ・エントリー QoS パラメーターを設定するのに使用します。

構文:

```
set
    max-reserved-bandwidth
    traffic-type
    peak-cell-rate
    sustained-cell-rate
    qos-class
    max-burst-size
```

例:

```
ARP entry 'identifier' config> set ?
MAX-RESERVED-BANDWIDTH
TRAFFIC-TYPE
PEAK-CELL-RATE
SUSTAINED-CELL-RATE
QOS-CLASS
MAX-BURST-SIZE
```

QoS パラメーターについての詳しい情報は、 [フィーチャーの使用と構成](#) の中のサービス品質 (QoS) の構成と監視を参照してください。

List

list コマンドは、ARP 構成に関する情報を表示するのに使用します。

Remove

remove コマンドは、構成された MAC アドレスまたはルート記述子 LE-ARP エントリーを除去するのに使用します。

提供されたリストから、除去する ARP エントリー番号を選択します。

構文:

```
remove
    arp-entry-number
```

Frame

frame コマンドは、NetWare IPX カプセル化タイプを設定するのに使用します。コマンド・オプションは、LEC のタイプ (トークンリングまたはイーサネット) に応じて異なります。トークンリング LEC の場合は、次のいずれかを入力します。

オプション	説明	構文
MSB を使用する トークンリング	標準 802.2 IPX ヘッダーを非標準 トークンリング・アドレス・ビット 配列 (MSB) と一緒に使用します。	frame token-ring msb
LSB を使用する トークンリング	802.2 IPX ヘッダーを非標準アドレ ス・ビット配列 (LSB) と一緒に使 用します。	frame token-ring lsb
MSB を使用する 802.2 SNAP を使 うトークンリング	802.2 形式を SNAP ヘッダーおよ び非標準アドレス・ビット配列と一 緒に使用します。このカプセル化 は、主にブリッジング環境で使用さ れます。	frame token-ring_snap msb
LSB を使用する 802.2 SNAP を使 うトークンリング	802.2 形式を SNAP ヘッダーおよ び標準アドレス・ビット配列と一緒 に使用します。	frame token-ring_snap lsb
イーサネット 2.0	イーサネットのバージョン 2.0 の プロトコル 81-37 を使用します。	frame ethernet_II
イーサネット 802.2	イーサネット 802.3 を 802.2 SA E0 と一緒に使用します。	frame ethernet_8022
イーサネット 802.3	イーサネット 802.3 を 802.2 ヘッ ダーを付けずに使用します。	frame ethernet_802.3
イーサネット SNAP	802.3、802.2 を SNAP PID 00-00-00-81-37 と一緒に使用しま す。	frame ethernet_SNAP

構文:

frame *ipx-encapsulation type*

注: frame コマンドは、インターフェースが IPX を使用して構成されていない限り、ネットワーク構成プロセスで IPX カプセル化を設定するのに使用することはできません。

IPX カプセル化は、IPX 構成環境で設定することもできます。詳細については、プロトコル構成と監視の解説書で IPX の構成に関する章を参照してください。

例:

```
frame token_ring msb
```

IP-Encapsulation (イーサネット ATM フォーラム準拠 LEC の場合のみ)

IP-encapsulation コマンドは、イーサネット (イーサネット・タイプ X'0800') または IEEE 802.3 (SNAP を備えたイーサネット 802.3) を選択するのに使用します。タイプ **E** (イーサネット) または **I** (IEEE-802.3) のいずれかを指定します。

構文:

IP-encapsulation Ethernet
IEEE-802.3

List

list コマンドは、LE クライアントの構成をリストするのに使用します。

構文:

list

LLC

論理リンク制御は『サブプロトコル』と考えることができます。Talk 6 (構成) または Talk 5 (コンソール) 環境から直接アクセスすることはできません。代わりに、**LLC** コマンドを入力して、トークンリング LEC 構成メニューからアクセスします。

llc コマンドは、LLC Config> プロンプトにアクセスするのに使用します。詳細については、350ページの『LLC 構成コマンド』を参照してください。

構文:

llc

QoS

qos-configuration コマンドは、LEC QoS Config> プロンプトを表示させて、そこから、**フィーチャーの使用と構成** の LE クライアント QoS 構成コマンドで説明されているようにサービス品質を構成するのに使用します。

構文:

qos-configuration

RIF-Timer (トークンリング・フォーラム準拠 LEC の場合のみ)

RIF-Timer コマンドは、RIF 内の情報が更新される前に維持されている最大時間数を設定するのに使用します。範囲は 0 ~ 4096 です。デフォルト値は 120 秒です。

構文:

rif-timer *value*

例:

rif-timer 100

Set

set コマンドは、LE クライアントのパラメーターを設定するのに使用します。

構文:

フォーラム LE クライアントの構成

set

arp-aging-time
arp-cache-size
arp-queue-depth
arp-response-time
auto-config
best-effort-peakrate
bus-connect-retries
conn-completion-time
control-timeout
data-direct-timeout
data-direct-vcc-mode
elan-name
esi-address
flush-timeout
forward-delay
forward-disconnect-timeout
frame-size
initial-control-timeout
lecs-atm-address
les-atm-address
mac-address
multicast-send-avg
multicast-send-peak
multicast-send-type
multiplier-control-timeout
path-switch-delay
reconfig-delay-min
reconfig-delay-max
retry-count
selector
trace
unknown-count
unknown-time
vcc-timeout

arp-aging-time

ARP エージング・タイムを設定します。これは、その関係の検証がない場合

に、LEC が LE_ARP キャッシュに項目を維持する最大時間です。エージング・タイムを大きくすると、セッションの設定時間が速くなりますが、メモリーの使用量が増え、ネットワーク構成の変更への対応が遅くなる可能性があります。

有効値:

10 ～ 300 秒の範囲の整数

デフォルト値:

300

例:

```
LEC Config> set arp-aging-time 200
```

arp-cache-size

ARP キャッシュ内のエン트리数を設定します。ARP キャッシュのサイズは、同時伝送できるデータ・ダイレクト VCC の数を制限します。ARP キャッシュを大きくすると、メモリーの所要量が増えますが、クライアントはより多くのあて先と同時に通話できるようになります。

有効値:

10 ～ 65535 の範囲の整数

デフォルト値:

5000

例:

```
LEC Config> set arp-cache-size 10
```

arp-queue-depth

ARP キャッシュ・エン트리当たりの待ち行列化フレームの最大数を設定します。LEC は、データ・パスを、マルチキャスト・センド VCC からデータ・ダイレクト VCC に切り替えるときに、フレームを待ち行列に入れます。待ち行列が満ぱいときは、転送するために LEC に渡されたフレームは廃棄されます。待ち行列を大きくすると、メモリーの所要量は増えますが、データ・パスを切り替えるときに廃棄されるフレームの数が減ります。

有効値:

0 ～ 10 の範囲の整数

デフォルト値:

5

例:

```
LEC Config> set arp-queue-depth 10
```

arp-response-time

予期される ARP 応答時間を設定します。この値は、未応答 LE ARP 要求を再試行する頻度を制御します。値を大きくすると、LE ARP の数が少なくなり、その結果、トラフィックが減って、データ・ダイレクト VCC が確立される前の時間が長くなる可能性があります。

有効値:

1 ～ 30 秒の範囲の整数

フォーラム LE クライアントの構成

デフォルト値:

1 秒

例:

```
LEC Config> set arp-response-time 20
```

auto-config

この LEC が LECS auto-config モードを使用するかどうかを指定します。YES または NO を指定します。LEC は LECS に連絡して、その LES のアドレスおよびその他の種々の構成パラメーターを入手することができます。

有効値:

YES のときは、LES の ATM アドレスを構成する必要はありません。

NO のときは、343 で説明しているように、**set les-atm-address** コマンドを使用して、LES の ATM アドレスを構成する必要があります。

デフォルト値:

NO

例:

```
LEC Config> set auto-config yes
```

best-effort-peakrate

ベストエフォート・ピーク速度を設定します。ベストエフォート・マルチキャスト送信接続を確立するときに使用されます。

最大ピーク速度は、ATM 装置の最大データ速度によって決まります。

以下のように、1 から最大ピーク速度 (定義は最大データ速度) までの範囲内の整数 (Kbps) を指定します。

- ATM 最大データ速度が 25 Mbps の場合、最大ピーク速度は 25,000 Kbps
- ATM 最大データ速度が 155 Mbps の場合、最大ピーク速度は 155,000 Kbps

有効値:

1 ~ 装置の最大データ速度の範囲の整数

デフォルト値:

155000

例:

```
LEC Config> set best-effort-peakrate 24000
```

bus-connect-retries

このパラメーターは、LEC が初期状態に戻る前に、BUS への再接続を試みる最大試行回数を設定します。

有効値:

0 ~ 2

デフォルト値:

1

connection-completion-time

接続完了時間を設定します。これは、コーリング側からのデータまたは READY_IND メッセージが予期される時間間隔です。

クライアントへのデータ・ダイレクト VCC が確立されると、LEC は、この時間枠内にデータまたは READY_IND メッセージを受信することを予期します。LEC は、データまたは READY_IND を受信するまでは、確立されたデータ・ダイレクト VCC を介してフレームを送信しません。このパラメーターは、LEC が READY QUERY (READY_IND を受信するホップ数) を出す前に経過する時間を制御します。値を小さくすると、応答時間が速くなりますが、不要な伝送も増えます。

有効値:

1 ~ 10 秒の範囲の整数

デフォルト値:

4

例:

```
LEC Config> set connection-completion-time 5
```

control-timeout

このパラメーターは、要求の最大累算制御タイムアウトを設定します。

現行タイムアウト値は、**initial-control-timeout** の値に初期設定されます。要求に対するレスポンスを現行タイムアウト値以内に受け取らなかった場合、現行タイムアウト値に **multiplier-control-timeout** の値が乗算され、その後で再度その要求が出されます。現行タイムアウト値が満了するたびに、このプロセスが繰り返され、現行タイムアウト値が **control-timeout** の値を超えるまで続けられます。

有効値:

10 ~ 300 秒の範囲の整数

デフォルト値:

30

例:

```
LEC Config> set control-timeout 100
```

data-direct-timeout

データ・ダイレクト VCC のタイムアウト値を指定します。このパラメーターは、LEC が LES/BUS への接続をもたずに、データ・ダイレクト VCC がアップのままている時間を制限します。タイマーが満了する前に LEC が LES/BUS に再結合する場合、時間は停止されます。

有効値:

10 ~ 300 秒

デフォルト値:

30

data-direct-vcc-mode

持続的なデータ・ダイレクト VCC モードを使用可能または使用不可のどちらにするか指定します。データ・ダイレクト VCC モードが使用可能にされると、LEC が LES/BUS への接続を失う場合、データ・ダイレクト VCC が除

フォーラム LE クライアントの構成

去され、再接続タイムアウト・タイマーが始動します。LEC は、引き続き LES/BUS へ再接続しようとしています。 **data-direct-timeout** が満了する前に、LEC が LES/BUS に再接続できない場合、すべてのデータ・ダイレクト VCC が切断されます。

有効値:

yes または no

デフォルト値:

no

elan-name

LEC が加入を望む ELAN の名前を指定します。これは、構成要求で LECS に送信される (LEC が自動構成される場合)、または加入要求で LES に送信される ELAN ネームです。LECS または LES は、レスポンスで異なる ELAN ネームを戻すことがあります。

有効値:

0 ~ 32 バイトの長さの文字列

デフォルト値:

Blank

注: ブランク名 (長さが 0 のストリング) は有効です。

例:

```
LEC Config> set elan-name FUZZY
```

esi-address

LEC の ATM アドレスの ESI 部分を設定します。

LEC の ATM アドレスの ESI 部分 (オクテット 13 ~ 19) を指定します。LEC の ESI とセレクターの組み合わせは、装置上のすべての LAN エミュレーション・コンポーネント間で固有であることが必要です。

有効値:

任意の 12 桁の 16 進数字

デフォルト値:

Burned-in ESI

例:

```
set esi
Select ESI
(1) Use burned in ESI
(2) 11.22.33.44.55.66

Enter selection [1]?
```

flush-timeout

フラッシュ・タイムアウトを設定します。LE_FLUSH_REQUEST の送信後、回復処置を取る前に LE_FLUSH_RESPONSE の受信を待つ制限時間です。回復時に、待ち行列化されていたフレームは廃棄され、新たなフラッシュ要求が送信されます。

データ・バスを、マルチキャスト送信からデータ・ダイレクトに切り替えるときに、クライアントはマルチキャスト送信 VCC を介してフラッシュ要求を

送信します。フラッシュ応答を受信するまで、またはパス・スイッチ遅延が満了するまで、フレームはあて先用の待ち行列に入れられます。

有効値:

1 ~ 4 秒の範囲の整数

デフォルト値:

4

例:

```
LEC Config> set flush-timeout 3
```

forward-delay

転送遅延を設定します。LE ARP キャッシュ内のエントリは、定期的に再検証する必要があります。転送遅延時間は、ネットワーク・トポロジーの変更時に、リモート・エントリがキャッシュ内にとどまっていた最大時間です。エイジング・タイムを長くすると、古い(無効な)エントリが増えますが、再検証のための通信量は減ります。

有効値:

4 ~ 30 秒の範囲の整数

デフォルト値:

15

例:

```
LEC Config> set forward-delay 10
```

forward-disconnect-timeout

このパラメーターは、LEC が BUS からの最後のマルチキャスト・フォワード VCC を失った後、初期状態に戻る前に待つ時間を設定します。この遅延により、BUS は初期状態に戻る前にクライアントへの再接続を試みる可能性があります。

有効値:

10 ~ 300 秒

デフォルト値:

60

frame-size

フレーム・サイズを設定します。

frame-size に指定される値は、318 ページで説明されているように、ATM INTERFACE> **set max-frame** コマンドを使用して ATM max-frame に対して指定される値以下であることが必要です。

有効値:

1516

4544

9234

18190

フォーラム LE クライアントの構成

デフォルト値:

ELAN タイプがトークンリングの場合、デフォルト値は 4544 です。
ELAN タイプがイーサネットの場合、デフォルト値は 1516 です。

例:

```
LEC Config> set frame-size 4544
```

initial-control-timeout

このパラメーターは、341 ページで説明されている制御タイムアウト・アルゴリズムで使用される初期制御タイムアウトの値を設定します。

有効値:

1 ~ 10

デフォルト値:

5

例:

```
LEC Config> set initial-control-timeout 10
```

lecs-atm-address

LECS の ATM アドレスを指定します。

自動構成に設定されている場合、クライアントは LECS への接続を試みます。ある LECS に接続できない場合には、別の LECS ATM アドレスを試行することができます。LECS ATM アドレスを試行する順序は、次のとおりです。

1. この構成された LECS アドレス
2. ILMI を通して入手した任意の LECS アドレス
3. ATM フォーラムによって定義された事前割り当て LECS アドレス

デフォルト値は、提供されていません。

注: このコマンドは、1 行のコマンド行に入力しなければなりません。本書では、スペースの関係で 2 行に示してあります。

Example:

```
LEC Config> set lecs-atm-address  
39.84.0F.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.01
```

les-atm-address

LES ATM アドレスを設定します。340 ページの **set auto-config** コマンドの項に説明されている **lecs-auto-config** の設定値に応じて、このコマンドは任意選択または必須になります。

- auto-config が YES のときは、les-atm-address は構成できません。
- auto-config が NO のときは、les-atm-address は必須です。

LES の ATM アドレスを指定します。デフォルト値は、提供されていません。

注: このコマンドは、1 行のコマンド行に入力しなければなりません。本書では、スペースの関係で 2 行に示してあります。

例:

```
LEC Config> set les-atm-address
39.84.0F.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.02
```

mac-address

この LE クライアントの MAC アドレスを設定します。クライアントが ATM インターフェースの出荷時設定 MAC アドレスを使用すると指定しても、あるいは別の MAC アドレスを指定しても構いません。2 つのクライアントがブリッジされている場合は、それぞれ異なる MAC アドレスを使用する必要があります。

この MAC アドレスは、クライアントが ELAN に加入するときに LES に登録されます。

有効値:

任意の有効な MAC アドレス

デフォルト値:

なし

例:

```
LEC Config> set mac-address
Use adapter address for MAC? [No]
MAC address []: 10.00.5a.00.00.01
```

multicast-send-avg

マルチキャスト・センド VCC の平均速度 (Kbps) を設定します。VCC 上の帯域幅を BUS に予約するために LEC によって使用されます。これは、予約帯域幅マルチキャスト・センド VCC を設定するときに使用され、順方向と逆方向の持続セル速度を指定します。

このパラメーターは、multicast-send-type が予約帯域幅である場合にのみ適用されます。multicast-send-avg と multicast-send-peak が等しいときには、固定ビット速度 (CBR) マルチキャスト送信がシグナルされます。そうでない場合は、可変ビット速度 (VBR) マルチキャスト送信がシグナルされます。Multicast-send-avg は multicast-send peak 以下でなければなりません。

予約帯域幅マルチキャスト・センド VCC は、輻輳 (ふくそう) したネットワークではデータ転送速度が速くなる可能性があります。帯域幅を予約しておきながら、それを使用しないことは、ネットワーク・リソースの浪費になります。

multicast-send-type が予約されている場合は、multicast-send-avg および multicast-send-peak を指定する必要があります。

例:

```
LEC Config> set multicast-send-avg 4000
```

multicast-send-peak

マルチキャスト送信ピーク速度 (Kbps) を設定します。VCC 上の帯域幅を BUS に予約するために LEC によって使用されます。これは、予約帯域幅マルチキャスト・センド VCC を設定するときに使用され、順方向と逆方向のピーク・セル速度を指定します。

このパラメーターは、multicast-send-type が予約帯域幅である場合にのみ適用されます。multicast-send-avg と multicast-send-peak が等しいときには、固定ビット速度 (CBR) マルチキャスト・センドがシグナルされます。そうでない

フォーラム LE クライアントの構成

場合は、可変ビット速度 (VBR) マルチキャスト・センドがシグナルされません。Multicast-send-avg は multicast-send peak 以下でなければなりません。

予約帯域幅マルチキャスト・センド VCC は、輻輳 (ふくそう) したネットワークではデータ転送速度が速くなる可能性があります。帯域幅を予約しておきながら、それを使用しないことは、ネットワーク・リソースの浪費になります。

multicast-send-type が予約されている場合は、multicast-send-avg および multicast-send-peak を指定する必要があります。

Example:

```
LEC Config> set multicast-send-peak 155
```

multicast-send-type

マルチキャスト送信タイプを設定します。マルチキャスト・センド VCC を確立するときに LEC が使用する方式を指定します。

multicast-send-avg と multicast-send-peak が等しいときには、固定ビット速度 (CBR) マルチキャスト・センドがシグナルされます。そうでない場合は、可変ビット速度 (VBR) マルチキャスト・センドがシグナルされます。

Multicast-send-avg は、少なくとも multicast-send peak に等しくなければなりません。

予約帯域幅マルチキャスト・センド VCC は、輻輳 (ふくそう) したネットワークではデータ転送速度が速くなる可能性があります。帯域幅を予約しておきながら、それを使用しないことは、ネットワーク・リソースの浪費になります。

multicast-send-type が予約されている場合は、multicast-send-no および multicast-send-peak を指定する必要があります。

有効値:

ベストエフォートまたは予約 (Reserved)

デフォルト値:

ベストエフォート

例:

```
LEC Config> set multicast-send-type best-effort
```

multiplier-control-timeout

このパラメーターは、341 ページで説明されている制御タイムアウト・アルゴリズムで使用される制御タイムアウト乗数値を設定します。

有効値:

2 ~ 5

デフォルト値:

2

例:

```
LEC Config> set multiplier-control-timeout 5
```

path-switch-delay

パス・スイッチ遅延を設定します。

フォーラム LE クライアントの構成

LEC は、データ・ダイレクト VCC の使用を開始する前に、BUS を通してあて先に送信されたすべてのフレームがあて先に到達したことを確認する必要があります。この確認は、フラッシュ・プロトコルを使用して行うか、あるいは BUS に最後のパケットを送信した後で `path-switch-delay` 秒数だけ待つことによって行います。値を小さくすると性能が改善しますが、非常に輻輳(ふくそう)したネットワーク上では、順序誤り (out-of-order) パケットが発生する可能性があります。

有効値:

1 ~ 8 秒の範囲の整数

デフォルト値:

6

例:

```
LEC Config> set path-switch-delay 5
```

reconfig-delay-min

このパラメーターは、LEC が初期状態に戻るときの最小遅延時間を設定します。この値は \leq **reconfig-delay-max** でなければなりません。

有効値:

1 ~ **reconfig-delay-max** の値

デフォルト値:

1

例:

```
LEC Config> set reconfig-delay-min 5
```

reconfig-delay-max

このパラメーターは、LEC が初期状態に戻るときの最大遅延時間を設定します。この値は \geq **reconfig-delay-min** でなければなりません。

有効値:

1 ~ 10

デフォルト値:

5

例:

```
LEC Config> set reconfig-delay-max 9
```

retry-count

再試行カウントを設定します。これは、LEC が特定のフレームの LAN あて先に対して `LE_ARP_REQUEST` を再試行する回数です。指定された回数後も ARP レスポンスを受信しなかった場合、そのエントリーは LE ARP キャッシュから除去されます。

有効値:

0、1、または 2

デフォルト値:

1

例:

フォーラム LE クライアントの構成

```
LEC Config> set retry-count 2
```

selector

クライアントの ATM アドレスのセレクター部分を指定します。ESI とセレクターの組み合わせは、装置上のすべての LANE コンポーネント間で固有であることが必要です。デフォルトでは、構成された ESI に対して固有のセレクターが選択されます。

有効値:

同じ ESI を使用する別の LANE コンポーネントによって使用されていない、16 進数の任意のオクテット

例:

```
LEC Config> set selector 01
```

trace LEC のトレースを使用可能にします。パケット・トレースを実行するには、3 つのステップが必要です。

1. パケット・トレース・システムを使用可能にする (ELS 下で)
2. LEC サブシステム上のトレースを使用可能にする (ELS 下で)
3. 必要な LEC 上のパケット・トレースを使用可能にする (このコマンドを使用して)

有効値:

Yes または No

デフォルト値:

No

例:

```
Token Ring LEC config>set trace  
Trace packets on the LEC? [No]?yes
```

unknown-count

不明フレーム・カウントを設定します。これは、unknown-time パラメーターで指定された時間内に BUS に送信できる、特定のユニキャスト MAC アドレスまたはルート記述子のフレームの最大数です。値を大きくすると、廃棄されるフレーム数は減りますが、BUS の負荷が増えます。

有効値:

1 ~ 255 の範囲の整数

デフォルト値:

10

unknown-time

不明フレーム時間を設定します。これは、特定のユニキャスト MAC アドレスまたはルート記述子のフレームの最大数 (unknown-count パラメーターで示された) を BUS に送信できる時間間隔です。値を大きくすると、廃棄されるフレーム数が増えますが、BUS の負荷は減ります。

有効値:

1 ~ 60 秒の範囲の整数

デフォルト値:

1

例:

```
LEC Config> set unknown-time 5
```

vcc-timeout

VCC タイムアウトを設定します。この期間トラフィックの送信がなかった場合、データ・ダイレクト VCC を解放する必要があります。

有効値: 0 ~ 31536000 秒 (1 年)

デフォルト値: 1200

注: このパラメーターに意味があるのは、SVC 接続の場合だけです。

例:

```
LEC Config> set vcc-timeout 1000
```

Source-Routing (トークンリング・フォーラム準拠 LEC の場合のみ)

source-routing コマンドは、エンド・ステーションのソース・ルーティングを使用可能または使用不可にするのに使用します。ソース・ルーティングというのは、エンド・ステーションがソース・ルーティング・ブリッジを経由するのに使用するソース・ルートを決めるプロセスです。ソース・ルーティングにより、IP、IPX、および AppleTalk フェーズ 2 プロトコルは、ソース・ルート・ブリッジの反対側のノードに到達することが可能になります。

ソース・ルーティングが使用可能でも使用不可でも、装置のこの機能は変更されません。デフォルトの設定値は「使用可能」です。

一部のステーションは、ソース・ルーティング RIF をもつフレームを正常に受信できません。これは特に NetWare ドライバーに共通に見られる特徴です。この状態のときは、ソース・ルーティングを使用不可にすれば、これらのステーションと通信できるようになります。

ソース・ルーティングを使用可能にするのは、IP、IPX、および AppleTalk フェーズ 2 パケットを通過させたいソース・ルーティング・ブリッジがこのリング上に存在する場合だけに限るべきです。また、LLC テスト応答メッセージを戻すようにしたい場合は、ソース・ルーティングを使用可能にする必要があります。

構文:

```
source-routing          enable
                           disable
```

例:

```
source-routing disable
```

LLC 構成コマンド

この節では、すべての LLC 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45 に示されるこれらのコマンドを使用すると、SNA ネットワークを介してパケットを渡している間 LLC を監視することができます。

表 45. LLC コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
List	構成情報を表示します。
Set	セッションの存続期間中だけ有効な LLC パラメーターを動的に構成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。13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、構成情報を表示するのに使用します。

構文:

list

Set

set コマンドは現行 LLC セッションに関する LLC パラメーターを動的に構成するのに使用します。パラメーターに加えた変更は、セッションの存続期間中だけ有効です。

重要: LLC パラメーターをデフォルト値から変更すると、LLC プロトコルの動作方法に影響を与える可能性があります。

構文:

set *n2-max_retry count*
n3-frames-rcvd-before-ack count
nw-acks-to-inc-ww count
rw-receive-window seconds
t1-reply-timer seconds
t2-receive-ack-timer seconds
ti-inactivity-timer seconds
tw-transmit-window seconds

n2-max_retry

LLC プロトコルによる再試行の最大数。たとえば、N2 は、非活動タイマーが満了したときに、LLC が確認応答を受信せずに RR を送信する最大回数です。デフォルト値は 8。最小値は 1。最大値は 127。

n3-frames-rcvd-before-ack

この値は、T2 タイマーと合わせて、受信 I フレームの確認応答トラフィックを削減するのに使用されます。このカウンターは、指定された値に設定します。I フレームを受信するたびに、この値が減分します。このカウンターが 0 に達するか、T2 タイマーが満了すると、確認応答が送信されます。デフォルト値は 1。最小値は 1。最大値は 255。

nw-acks-to-inc-ww

このフィールドは、デフォルト値の 1 に設定します。

rw-receive-window

RR が送信される前に受信できる I フレームの最大数を設定します。デフォルト値は 2。最小値は 1。最大値は 127。

t1-reply-timer

このタイマーは、LLC が相手側の LLC ステーションから必要な確認またはレスポンスを受信できないと満了します。このタイマーが満了すると、ポーリング・ビットをセットして RR が送信され、T1 が再びスタートします。LLC が構成された再試行最大数 (N2) の後もレスポンスを受信しない場合、基礎リンクは動作不能として宣言されます。デフォルト値は 1。デフォルト値は 1。最小値は 256。

t2-receive-ack-timer

このタイマーは、受信 I フォーマット・フレームの確認の送信を遅らせるのに使用します。このタイマーは、I フレームを受信するとスタートし、確認を送信するとリセットされます。このタイマーが満了すると、LLC2 はできるだけ速やかに確認を送信します。この値は、T1 の値より小さくなるように設定します。これにより、T1 タイマーが満了する前に、リモート LLC2 同位が遅らせた確認を確実に受信できるようになります。デフォルト値は 1 (100 ミリ秒)。最小値は 1。最大値は 2560。

注: このタイマーが 1 (デフォルト値) に設定されている場合、タイマーは動作しません (たとえば、**n3-frames_rcvd-before-ack=1**)。

ti-inactivity-timer

このタイマーは、指定された期間に LLC がフレームを受信しないと満了します。このタイマーが満了すると、相手側の LLC が応答するか、N2 タイマーが満了するまで、LLC は RR を送信します。デフォルト値は 30 秒。最小値は 1 秒。最大値は 256 秒。

tw-transmit-window

RR を受信する前に送信できる I フレームの最大数を示します。相手側の LLC セッションが実際にこの数の連続 I フレームを受信することが可能であり、しかも装置に確認を受信するまでこれらのフレームのコピーを保持できる十分なヒープ・メモリーがあると仮定した場合、この値を大きくすると、スループットが向上します。デフォルト値は 2。最小値は 1。最大値は 127。

LEC 監視環境へのアクセス

LEC 監視コマンドにアクセスするには、以下の手順を使用します。このプロセスによって、LEC 監視 プロセスにアクセスすることができます。

LLC の構成

1. OPCON プロンプトで **talk 5** と入力する。(このコマンドの詳細については、33ページの『OPCON プロセスとは』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、GWCON プロンプト (+) がコンソールに表示されます。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. + プロンプトで **network ?** コマンドを入力して、装置が現在構成されているネットワーク・インターフェース番号を表示し、監視したい LEC の インターフェース番号 を入力する。たとえば、次のように入力します。

```
+ network ?

1 : ATM Ethernet LAN Emulation: ETH
2 : IP Protocol Network
3 : Bridge Application
5 : CHARM ATM Adapter
Network number [0]? 1
LEC+
```

LEC 監視プロンプト (LEC+) が表示されます。

監視したい LEC のインターフェース番号が分かっている場合は、**network** コマンドに続けて、その LEC のインターフェース番号 を入力します。

```
+ network 1
LEC+
```

LEC 監視コマンド

この節では、LEC 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。LEC 監視コマンドには LEC+ プロンプトからアクセスできます。表46 は、コマンドを示しています。

表 46. LE クライアント監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
List	以下のものをリストします。 <ul style="list-style-type: none">• LEC アドレス解決テーブル (ARP)• LEC 構成• データ直送 VCC 情報• グループ・アドレス• RIF 情報• LEC 統計• VCC テーブル
LLC	トークンリング LEC の LLC> 監視プロンプトを表示します。

表 46. LE クライアント監視コマンドの要約 (続き)

コマンド	機能
MIB	以下を含む LEC MIB オブジェクトを表示します。 <ul style="list-style-type: none"> • LEC MIB 構成テーブル • LEC MAC ARP テーブル • LEC ルート記述子テーブル • LEC MIB サーバー VCC テーブル • LEC MIB 統計テーブル • LEC MIB 状態テーブル
QoS	LEC x QoS+ プロンプトを表示するので、フィーチャーの使用と構成のサービス品質監視コマンドで説明されているように、そこからサービス品質を監視することができます。
Trace	パケット・トレースをオンまたはオフに設定するか、トレース・アドレスまたはトレース・マスクを設定します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、LEC アドレス解決テーブル (ART)、LEC 構成、データ・ダイレクト VCC 情報、または LEC 統計をリストするのに使用します。

構文:

```
list
    arp-table
    configuration
    data-direct-vccs
    group
    rif
    statistics
    vcc-table
```

arp LEC アドレス解決テーブル (ARP キャッシュ内のエントリ) をリストします。

例:

```
LEC+ list arp
```

```
LEC Address Resolution (LE ARP Cache) Table
Max Table Size          = 10
Free Table Entries      = 10
Current Mac Entries     = 0
Current RD Entries      = 0
Arp Aging Time          = 300
Verify Sweep Interval   = 60

MAC Address      Remote Handle  Conn  Xmit  BUS  Arp
                Depth  Queue  Frame  Retry  Aging
                Handle  Depth  Count  Count  Timer  Destination ATM Ad
                0      0      0      0      60    39.99.99.99.99.99.
                99.00.00.99.99.30.02.40.00.00.00.00.09.81
```

注: スイープ間隔は常に ARP エージング・タイマー値の 1/5 です。

LE クライアントの監視

Max Table Size

利用可能なエントリーの合計数

Free Table Entries

空きエントリーの数

Current MAC Entries

Current RD Entries

ルート記述子 ATM エントリー

ARP Aging Time

エントリーをエージングにより除去するまでの時間

Verify Sweep Interval

MAC Address

Remote

Connection Handle

Queue Depth

Xmit Frame Count

BUS Retry Count

ARP Aging Timer

Destination ATM Address

configuration

LEC 構成がリストされます。

イーサネットの場合:

例:

```
IBM LEC+list config      ATM IBM LEC Configuration = 0
Physical ATM interface number = 7
LEC interface number     = 7
Primary ATM address      = Use burned in addr
      ESI address         = 0x3
      Selector byte       = Ethernet IBM
Emulated LAN type        = 1523
Maximum frame size       = Use burned in addr
LE Client MAC address    = 00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00
LE Server ATM address    = 155000
Forward Peak Rate        = 155000
Backward Peak Rate       = 32
MAC cache size           = 60
MAC cache aging period   = 32
Route Descriptor cache size = 60
Route Descriptor aging period = 60
LES Registration interval = 60
```

```

LES Registration retry count    = 3
LES keep alive count           = 10
Packet trace                   = No
IP Encapsulation               = ETHER

```

トークンリング IBM の場合:

Example:

IBM LEC+list config

```

                        ATM IBM LEC Configuration
Physical ATM interface number = 0
LEC interface number         = 10
Primary ATM address
  ESI address                 = Use burned in addr
  Selector byte               = 0x6
Emulated LAN type            = Token Ring IBM
Maximum frame size           = 4551
LE Client MAC address        = Use burned in addr
LE Server ATM address        = 39.84.07.00.00.00.00.00.00.00.00.01.10.00.5A.DD.DA.02
Forward Peak Rate            = 155000
Backward Peak Rate           = 155000
MAC cache size                = 32
MAC cache aging period       = 60
Route Descriptor cache size   = 32
Route Descriptor aging period = 60
LES Registration interval     = 60
LES Registration retry count  = 3
LES keep alive count         = 10
Packet trace                  = No
RIF Aging Timer               = 120
Source Routing                = Enabled

```

トークンリング・フォーラム準拠の場合:

例:

LEC+ list config

```

Physical ATM interface number = 0
LEC interface number         = 9
LEC ATM address              = 39.99.99.99.99.99.00.00.99.99.31.01.09.FC.DD.D0.32.70.0A
LEC MAC address              = 40.00.82.10.17.09
lecConfigMode                 = Manual
lecConfigLanType              = 802.5 - Token Ring
lecConfigMaxDataFrameSize     = 4544
lecConfigLanName              =
lecConfigLesAtmAddress        = 39.99.99.99.99.99.00.00.99.99.31.01.40.00.82.10.17.00.09
lecControlTimeout             = 30
lecMaxUnknownFrameCount       = 10
lecMaxUnknownFrameTime       = 1
lecVccTimeoutPeriod           = 1200
lecMaxRetryCount              = 1
lecAgingTime                   = 300
lecForwardDelayTime           = 15
lecExpectedArpResponseTime    = 1
lecFlushTimeout               = 4
lecPathSwitchingDelay         = 6
lecLocalSegmentId             = 0x0
lecMulticastSendType          = 1
lecMulticastSendAvgRate       = 365566
lecMulticastSendPeakRate      = 365566
lecConnectionCompleteTimer    = 4
lecInitialControlTimeout      = 5
lecControlTimeoutMultiplier   = 2
V2 Capable                    = TRUE
lecForwardDisconnectTimeout   = 60
lecMinReconfigDelay           = 1
lecMaxReconfigDelay           = 5
lecMaxBusConnectRetries       = 0
lecElanId                     = 0
ExplorerExclude                = TRUE
Data direct VCC mode          = TRUE
Data direct timeout           = 20
LE ARP queue depth            = 5
LE ARP cache size             = 5000
Forward peakrate              = 365566
Backward peakrate             = 365566
Packet trace                   = Off
RIF aging timer               = 120
Source Routing                 = enabled

```

LE クライアントの監視

上記の例に示されているパラメーターの定義は、337ページの『Set』を参照してください。

data LEC データ・ダイレクト VCC 情報をリストします。

例:

LEC+ list data

```
LEC Data Direct VCC Table
Max Table Size      = 1019      Max no of SVC connections
Current Size        = 0          Currently used
Inactivity Timeout  = 1200      No Data Xfer Timeout before connection is
                                   closed (seconds)
Sweep Interval      = 60
Conn Handle         VPI  VCI      Inactive Timer  User Count  Destination ATM Address
-----
652      0  7241    300      1      39.99.99.99.99.99.00.00.99.99.30.02.
                                   40.00.00.00.00.09.81
-----
```

group LEC によって使用されているグループ・アドレスをリストします。

rif LEC によって使用される MAC アドレスとルーティング情報フィールド (RIF) のマッピングをリストします。

statistics

LEC 統計をリストします。

例:

LEC+ list stat

```
LEC Statistics
In Octets.high      = 0          No of Bytes received
In Octets.low       = 346
In Discards         = 2          Packets discarded
In Errors           = 0          Rx.Errors
In Unknown Protos  = 0          Unknown protocols received
Out Octets.high     = 0          No of Bytes xmitted.
Out Octets.low      = 0
Out Discards        = 0
Out Errors          = 0          Tx.Errors
In Frames           = 0
Out Frames          = 0
In Bytes            = 0
Out Bytes           = 0
```

VCC table

VCC テーブルをリストします。

例:

LEC+ list vcc

LLC

論理リンク制御は『サブプロトコル』と考えることができます。Talk 6 (構成) または Talk 5 (コンソール) 環境から直接アクセスすることはできません。代わりに、**LLC** コマンドを入力して、トークンリング LEC 監視メニューからアクセスします。

llc コマンドは、LLC> プロンプトにアクセスするのに使用します。詳細については、362ページの『LLC 監視コマンド』を参照してください。

構文:

llc

| MIB

mib コマンドは、MIB オブジェクトを表示するのに使用します。

注: この情報の中には、**list** コマンドを使用して、別のフォーマットで表示できるものもあります。

構文:

```
mib                                config-table
                                       mac-arp-table
                                       rd-arp-table
                                       server-vcc-table
                                       statistics-table
                                       status-table
```

config LEC MIB 構成テーブルを表示します。

例:

LEC+ **mib config**

```
lecConfigTable:
lecConfigMode                = Manual
lecConfigLanType             = 802.3 - Ethernet
lecConfigMaxDataFrameSize   = 1516
lecConfigLanName             =
lecConfigLesAtmAddress       = 39.84.0F.00.00.00.00.00.11.23.24.24.24.24.55.66.77.88.99.00
lecControlTimeout           = 120
lecMaxUnknownFrameCount     = 1
lecMaxUnknownFrameTime      = 0
lecVccTimeoutPeriod         = 1200
lecMaxRetryCount            = 1
lecAgingTime                 = 300
lecForwardDelayTime         = 15
lecExpectedArpResponseTime  = 1
lecFlushTimeout             = 4
lecPathSwitchingDelay       = 6
lecLocalSegmentId           = 0
lecMulticastSendType        = 1
lecMulticastSendAvgRate     = 25000000
lecMulticastSendPeakRate    = 25000000

lecConnectionCompleteTimer  = 4
lecInitialControlTimeout    = 5
lecControlTimeoutMultiplier= 2
lecConfigV2Capable          = TRUE
lecForwardDisconnectTimeout = 60
lecMinReconfigDelay         = 1
lecMaxReconfigDelay         = 5
lecMaxBusConnectRetries    = 1
ExplorerExclude              = FALSE
Data direct VCC mode        = TRUE
Data direct timeout         = 20
```

lecConfigMode

LEC config モード: AUTO または MANUAL。AUTO の場合、LEC は LECS を使用して LES ATM アドレスを入手します。

lecConfigLanType

LAN タイプ。イーサネットまたはトークンリングのいずれかです。

lecConfigMaxDataFrameSize

最大フレーム・サイズ

LE クライアントの監視

lecConfigLanName

ELAN ネーム

lecConfigLesAtmAddress

LE サーバー ATM アドレス

lecControlTimeout

要求/応答制御フレームのタイムアウト

lecMaxUnknownFrameCount

不明フレームの最大数

lecMaxUnknownFrameTime

この期間に、LEC は特定のユニキャスト LAN あて先の最大数の MaxUnknownFrameCount フレームを BUS に送信し、さらにアドレス解決プロトコルを開始して、その LAN あて先を変換する必要もあります。

lecVccTimeoutPeriod

SVC データ・ダイレクト VCC の非活動タイムアウト

lecMaxRetryCount

LE ARP 再試行カウント

lecAgingTime

ARP テーブル内の未検証エントリーの存続期間

lecForwardDelayTime

lecExpectedArpResponseTime

ARP 要求/応答サイクル・タイム

lecFlushTimeout

LE フラッシュ要求/フラッシュ応答タイムアウト期間

lecPathSwitchingDelay

lecLocalSegmentId

エミュレートされた LAN のセグメント ID。 802.5 クライアントの場合のみ

lecMulticastSendType

LEC がマルチキャスト・センド VCC で使用するシグナル・パラメーター

lecMulticastSendAvgRate

LEC がマルチキャスト・センド VCC で使用するシグナル・パラメーター

lecMulticastSendPeakRate

LEC がマルチキャスト・センド VCC で使用するシグナル・パラメーター

lecConnectionCompleteTimer

READY_QUERY を送信する前に待つ時間

lecInitialControlTimeout

最大累積制御タイムアウトを指定します。

lecControlTimeoutMultiplier

制御タイムアウト乗数を指定します。

lecConfigV2Capable

LEC で LANE バージョン 2 が使えるかどうかを指定します。

lecForwardDisconnectTimeout

最後のマルチキャスト・フォワード VCC を失った後に待つ時間枠を指定します。

lecMinReconfigDelay

初期状態で LEC が待つ最小遅延時間を指定します。

lecMaxReconfigDelay

初期状態で LEC が待つ最大遅延時間を指定します。

lecMaxBusConnectRetries

初期状態に戻る前の最大 BUS 接続再試行回数を指定します。

ExplorerExclude

RIF 探索フレームを除去するかどうかを指定します。

Data Direct VCC Mode

持続的なデータ・ダイレクト・モードを指定します。

Data Direct Timeout

持続的なデータ・ダイレクト VCC タイムアウトを指定します。

mac LEC MAC ARP テーブルを表示します。

rd LEC ルート記述子テーブルを表示します。

server LEC MIB サーバー VCC テーブルを表示します。

例:

LEC+ mib server

```
lecServerVccTable:
  lecConfigDirectInterface    = 0
  lecConfigDirectVpi          = 0
  lecConfigDirectVci          = 0
  lecControlDirectInterface   = 1
  lecControlDirectVpi         = 0
  lecControlDirectVci         = 38
  lecControlDistributeInterface = 1
  lecControlDistributeVpi     = 0
  lecControlDistributeVci     = 37
  lecMulticastSendInterface   = 1
  lecMulticastSendVpi         = 0
  lecMulticastSendVci         = 34
  lecMulticastForwardInterface = 1
  lecMulticastForwardVpi      = 0
  lecMulticastForwardVci      = 33
```

lecConfigDirectInterface

コンフィグレーション・ダイレクト VCC に対応するインターフェース

lecConfigDirectVpi

上記の VCC (存在する場合) を識別する VPI

lecConfigDirectVci

上記の VCC (存在する場合) を識別する VCI

lecControlDirectInterface

コントロール・ダイレクト VCC に対応するインターフェース

LE クライアントの監視

lecControlDirectVpi

上記の VCC (存在する場合) を識別する VPI

lecControlDirectVci

上記の VCC (存在する場合) を識別する VCI

lecControlDistributeInterface

コントロール・ディストリビュート VCC に対応するインターフェース

lecControlDistributeVpi

上記の VCC (存在する場合) を識別する VPI

lecControlDistributeVci

上記の VCC (存在する場合) を識別する VCI

lecMulticastSendInterface

マルチキャスト・SEND VCC に対応するインターフェース

lecMulticastSendVpi

上記の VCC (存在する場合) を識別する VPI

lecMulticastSendVci

上記の VCC (存在する場合) を識別する VCI

lecMulticastForwardInterface

マルチキャスト・フォワード VCC に対応するインターフェース

lecMulticastForwardVpi

上記の VCC (存在する場合) を識別する VPI

lecMulticastForwardVci

上記の VCC (存在する場合) を識別する VCI

statistics

LEC MIB 統計テーブルを表示します。

例:

```
LEC+ mib statistics
```

```
lecStatisticsTable:
  lecArpRequestsOut      = 1
  lecArpRequestsIn       = 0
  lecArpRepliesOut       = 0
  lecArpRepliesIn        = 1
  lecControlFramesOut    = 2
  lecControlFramesIn     = 2
  lecSvcFailures         = 1
```

lecArpRequestsOut

この LEC によって送信された LE ARP 要求の数

lecArpRequestsIn

この LEC によって受信された LE ARP 要求の数

lecArpRepliesOut

この LEC によって送信された LE ARP 応答の数

lecArpRepliesIn

この LEC によって受信された LE ARP 応答の数

lecControlFramesOut

この LEC によって送信された制御パケットの数

lecControlFramesIn

この LEC によって受信された制御パケットの数

lecSvcFailures

以下の合計数

- このクライアントがオープンを試行したが失敗した発信 LAN エミュレーション SVC の数
- このクライアントが確立を試行したが失敗した着信 LAN エミュレーション SVC の数
- このクライアントがプロトコルまたはセキュリティーを理由に拒否した着信 LAN エミュレーション SVC の数

status MIB 状態をリストします。

例:

LEC+ mib status

```
lecStatusTable:
  lecPrimaryAtmAddress      = 39.84.0F.00.00.00
  Client ATM address=     = 00.00.00.00.01.10.00.5A.00.DE.AD.03
  lecId                     = 1                               Assigned by LES
  lecInterfaceState        = Operational                    State of the LEC
  lecLastFailureRespCode   = None                               Error code from last
  lecLastFailureState      = Initial State                  State of LEC when
  lecProtocol              = 1                               Protocol specified by
  LecVersion               = 1                               LEC in Join requests.
  lecTopologyChange        = False                          LEC Protocol Version
  lecConfigServerAtmAddress = 00.00.00.00.00.00.              of above
  lecConfigSource          = Did not use LECS
  lecActualLanType         = 802.3 - Ethernet               Frame format currently
  lecActualMaxDataFrameSize = 1516                          used by LEC
  lecActualLanName         = ETH                             Name of emulated LAN
  lecActualLesAtmAddress   = 39.84.0F.00.00.00.              that LEC joined.
  lecProxyClient           = False                           Is LES acting like a
  lecProxyClient           = False                           proxy ?
```

QoS Information

qos-information コマンドは、LEC x QoS+ プロンプトを表示させて、そこから、**フィーチャーの使用と構成** のサービス品質監視コマンドに説明されているように、サービス品質を監視するのに使用します。

構文:

qos-information

Trace

trace コマンドは、LEC 上でパケット・トレースをオンまたはオフにするのに使用します。詳細については、235ページの『パケット・トレース監視コマンド』を参照してください。

trace mac-address コマンドは、トレースされるデータを制限するために使用します。パケットがトレースされるのは、トレース MAC マスクと論理的に AND される着信先または送信元 MAC アドレスが、トレース MAC マスクと論理的に AND されるトレース MAC アドレスと等しい場合です。

構文:

trace

LLC 監視コマンド

この節では、すべての LLC 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47 に示されるこれらのコマンドを使用すると、SNA ネットワークを介してパケットを渡している間 LLC を監視することができます。

表47. LLC 監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
List	構成情報を表示します。
Set	セッションの存続期間中だけ有効な LLC パラメーターを動的に構成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。13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、構成情報を表示するのに使用します。

構文:

list

Set

set コマンドは現行 LLC セッションに関する LLC パラメーターを動的に構成するのに使用します。パラメーターに加えた変更は、セッションの存続期間中だけ有効です。

重要: LLC パラメーターをデフォルト値から変更すると、LLC プロトコルの動作方法に影響を与える可能性があります。

構文:

set n2-max_retry *count*
n3-frames-rcvd-before-ack *count*
nw-acks-to-inc-ww *count*
t1-reply-timer *seconds*
t2-receive-ack-timer *seconds*
ti-inactivity-timer *seconds*
tw-transmit-window *seconds*

n2-max_retry

LLC プロトコルによる再試行の最大数。たとえば、N2 は、非活動タイマー

が満了したときに、LLC が確認応答を受信せずに RR を送信する最大回数です。デフォルト値は 8。最小値は 1。最大値は 127。

n3-frames-rcvd-before-ack

この値は、T2 タイマーと合わせて、受信 I フレームの確認応答トラフィックを削減するのに使用されます。このカウンターは、指定された値に設定します。I フレームを受信するたびに、この値が減分します。このカウンターが 0 に達するか、T2 タイマーが満了すると、確認応答が送信されます。デフォルト値は 1。最小値は 1。最大値は 255。

nw-acks-to-inc-ww

このフィールドは、デフォルト値の 1 に設定します。

t1-reply-timer

このタイマーは、LLC が相手側の LLC ステーションから必要な確認またはレスポンスを受信できないと満了します。このタイマーが満了すると、ポーリング・ビットをセットして RR が送信され、T1 が再びスタートします。LLC が構成された再試行最大数 (N2) の後もレスポンスを受信しない場合、基礎リンクは動作不能として宣言されます。デフォルト値は 1。最小値は 1。最大値は 256。

t2-receive-ack-timer

このタイマーは、受信 I フォーマット・フレームの確認の送信を遅らせるのに使用します。このタイマーは、I フレームを受信するとスタートし、確認を送信するとリセットされます。このタイマーが満了すると、LLC2 はできるだけ速やかに確認を送信します。この値は、T1 の値より小さくなるように設定します。これにより、T1 タイマーが満了する前に、リモート LLC2 同位が遅らせた確認を確実に受信できるようになります。デフォルト値は 1 (100 ミリ秒)。最小値は 1。最大値は 2560。

注: このタイマーが 1 (デフォルト値) に設定されている場合、タイマーは動作しません (たとえば、**n3-frames_rcvd-before-ack=1**)。

ti-inactivity-timer

このタイマーは、指定された期間に LLC がフレームを受信しないと満了します。このタイマーが満了すると、相手側の LLC が応答するか、N2 タイマーが満了するまで、LLC は RR を送信します。デフォルト値は 30 秒。最小値は 1 秒。最大値は 256 秒。

tw-transmit-window

RR を受信する前に送信できる I フレームの最大数を示します。相手側の LLC セッションが実際にこの数の連続 I フレームを受信することが可能であり、しかも装置に確認を受信するまでこれらのフレームのコピーを保持できる十分なヒープ・メモリーがあると仮定した場合、この値を大きくすると、スループットが向上します。デフォルト値は 2。最小値は 1。最大値は 127。

LLC の監視

第23章 シリアル・ライン・インターフェースの構成

この章では、シリアル・インターフェースのインターフェース構成プロセスについて説明し、以下の節が含まれています。

- 『インターフェース構成プロセスへのアクセス』
- 366ページの『ネットワーク・インターフェースおよび GWCON インターフェース・コマンド』

重要: シリアル・インターフェース上のフレーム・リレー、PPP、X.25、V.25bis、SDLC リレー、および SDLC プロトコルを構成する場合は、本章のコマンドを使用した上で、特定プロトコルについて説明している章のコマンドを参照してください。

プロトコルのリストおよびこれらのプロトコルをサポートするインターフェースの一覧表は、21ページの『ネットワーク・インターフェースの構成』を参照してください。

インターフェース構成プロセスへのアクセス

シリアル・インターフェースを追加する方法についての説明は、18ページの『装置の追加』を参照してください。それが完了している場合は、以下で、インターフェースのデータ・リンクを正しく設定する方法、およびそのデータ・リンクの構成コマンドにアクセスする方法について説明します。

シリアル・インターフェースのインターフェース構成プロセスにアクセスするには、最初に `Config>` プロンプトにアクセスし、コマンド **set data-link** を出します。次に、`Config>` プロンプトで、インターフェースのタイプと番号を入力して、そのインターフェースの構成環境にアクセスします。

たとえば、X.25 のシリアル・インターフェースを構成する場合は、次のようなコマンドを出して、`X.25 config>` 環境にアクセスする必要があります。

```
Config> set data-link X25 2
Config>network 2
```

`X.25 config>` 環境から、シリアル・インターフェース上の X.25 の構成を完了させることができます。367ページの『第24章 X.25 ネットワーク・インターフェースの使用』を参照してください。

シリアル・インターフェースの構成が完了したら、`OPCON` プロンプト(*) の後に **restart** コマンドを入力し、新規構成を使用可能にするかどうかを尋ねるプロンプトに対して **yes** と応答します。

クロックおよびケーブルのタイプ

この節は、FR、PPP、X.25、SDLC リレー、および SDLC のシリアル・ポートの使用に適用されます。

シリアル・ライン・インターフェースの構成

モデムまたは CSU/DSU がシリアル・ポートに接続されている場合、ルーターはそのラインのクロックに関しては DTE の役割を果たすので、DTE ケーブル・タイプおよび外部クロックを構成します。

モデム、CSU/DSU、またはモデム・エリミネーターを使用せずに 2 つのルーターを直接接続したい場合は、一方のルーターが、そのラインのクロックに関して DCE の役割を果たします。DCE として働くルーターに直接接続ケーブルを接続し、そのシリアル・インターフェースに対して以下のパラメーターを構成します。

1. DCE ケーブル・タイプ
2. 内部クロック
3. クロック/ライン速度

他方のルーターは、クロックに関して DTE の役割を果たすので、モデムまたは CSU/DSU に接続されている場合と同様に構成することが必要です。

注: DTE ケーブルの構成は、DCE ケーブルの場合とは異なり、WAN ネット・ハンドラーがピア装置上で使用されるか否かに影響を与えません。たとえば、たとえフレーム・リレー・インターフェースが DCE ケーブルを使用するように構成されていても、ルーターは常にフレーム・リレー DTE 装置として働き、FR UNI インターフェースを使用します。

ネットワーク・インターフェースおよび GWCON インターフェース・コマンド

シリアル・ライン・インターフェースには、監視のための独自のコンソール・プロセスはありませんが、GWCON 環境から **interface** コマンドを使用すれば、ルーターはすべての導入済みネットワーク・インターフェースの完全な統計を表示することができます。**interface** コマンドと統計の表示について詳しくは、第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド を参照してください。

第24章 X.25 ネットワーク・インターフェースの使用

X.25 ネットワーク・インターフェースは、ルーターを X.25 バーチャル・サーキット・スイッチド・ネットワークに接続します。X.25 ネットワーク・インターフェースのソフトウェアとハードウェアにより、ルーターは公衆 X.25 ネットワークを介して通信することができます。X.25 ネットワーク・インターフェースは、X.25 インターフェースの CCITT 1980、CCITT 1984、CCITT 1988、および ISO 8208 1990 仕様に準拠しており、多重化チャネルおよび広域ネットワークを経由する高信頼性エンド・エンド間データ転送を提供します。

本章には、以下の節が含まれています。

- 『基本構成手順』
- 370ページの『ヌル・カプセル化』
- 372ページの『閉域ユーザー・グループの概要』

TCP/IP を介して X.25 トラフィックを伝送するための X.25 トランスポート・プロトコル (XTP) の構成については、415ページの『第26章 XTP の使用』を参照してください。

基本構成手順

この節では、X.25 インターフェースを立ち上げて実行するのに必要な最小構成ステップについて概説します。X.25 パラメーターは、ルーター上のインターフェースが接続する X.25 ネットワークと一致していなければなりません。詳細については、本章で説明する構成コマンドを参照してください。

注: 構成変更を有効にするためには、ルーターをリスタートする必要があります。

1. **OPCON** プロンプト (*) で **talk 6** と入力する。
Config> プロンプトが表示されます。
2. **list devices** を入力して、インターフェースのリストを表示すると、そこから選択することができます。以下のステップでは、該当するインターフェース番号を使用してください。
3. **set data-link x25** と入力する。
Interface Number [0]? プロンプトが表示されます。
4. 該当するインターフェース番号を入力する。
5. Config> プロンプトで **net #** と入力して、ネットワークに接続する。
X.25 Config[#]> プロンプトが表示されます。
6. このプロンプトで、**set address x.25-node-address** と入力する。

X.25 アドレスは、コール設定時に使用される固有の X.121 アドレスです。DDN ネットワークの場合は、**add htf-addr** および **set htf-addr** コマンドを使用して、このインターフェースに対応するプロトコル・アドレスを DDN アドレス変換に必要な X.121 アドレス・フォーマットに変換します。ネットワーク・アドレスを設定しないと、X.25 インターフェースを接続ネットワークに結合することができません。

X.25 ネットワーク・インターフェースの使用

7. **set equipment-type** と入力し、フレームおよびパケット・レベルが DCE または DTE のいずれで動作するのかを指定する。このコマンドのデフォルト値は DTE です。
8. **set svc** と入力して、使用する SVC 数の最低値と最高値を定義する。デフォルトは 1 SVC です。
9. **add protocol** *protocol_name* と入力して、X.25 インターフェースを介して実行されるプロトコルを追加する。ウィンドウ・サイズ、デフォルト・パケット・サイズ、最大パケット・サイズ、回線アイドル・タイム、および最大 VC 数を尋ねるプロンプトが出ます。

注: ルーター上のすべてのX.25 ネットワークに対して 1 回だけプロトコルを追加すれば済みます。

10. **add address** *protocol_name* と入力して、このインターフェースを介して到達可能な各プロトコルのあて先アドレスのアドレス変換を追加する。
11. **exit** と入力して、Config> プロンプトに戻る。
12. **Ctrl-P** を押して、OPCON プロンプト (*) に戻る。
13. **restart** と入力し、プロンプトに対して **yes** と応答する。

ナショナル・パーソナリティーの設定

各公衆データ通信網 (GTE の Telenet や DDN の Defense Data Network など) は、それぞれ独自の標準構成を持っています。ナショナル・パーソナリティー という用語は、公衆データ通信網の特性を定義するのに使用される変数グループを指定します。ナショナル・パーソナリティー内の構成情報は、リンクを介して転送されるパケットの制御情報をルーターに提供します。ナショナル・パーソナリティー・オプションは、各公衆データ通信網の 27 のデフォルト・パラメーターを定義します。

X.25 ナショナル・パーソナリティーの構成値を表示するには、X.25 構成 **list detailed** コマンドを実行します。ルーターに接続されている各公衆データ通信網を構成するには、X.25 構成 **national-personality set** コマンドを実行します。

ナショナル・パーソナリティーは、網構成の汎用テンプレートです。必要な場合は、各フレームおよびパケット・レイヤー・パラメーターを個別に構成することができます。

X.25 のデフォルト値について

下表は、X.25 *set*、*national set*、および *national enable* コマンドの各種パラメーターのデフォルト値をリストしています。

表 48. Set コマンド

パラメーター	デフォルト値
<u>address</u> ...	なし
<u>cable</u>	なし
<u>calls-out</u> ...	4
<u>clocking</u> ...	外部
<u>default-window-size</u> ...	2

X.25 ネットワーク・インターフェースの使用

表 48. Set コマンド (続き)

パラメーター	デフォルト値
<u>encoding</u>	NRZ
<u>equipment-type</u> ...	DTE
<u>htf addr</u> ...	なし
<u>inter-frame-delay</u> ...	0
<u>mtu</u>	1500
<u>national-personality</u> ...	GTE Telenet
<u>pvc</u> ...	低=0 高=0
<u>speed</u>	9600
<u>svc</u>	低 着信=0、高 着信=0 低 両方向=1、 高 両方向=64 低 発信=0、高 発信=0
<u>throughput-class</u> ...	着信=発信=2400
<u>vc-idle</u> ...	30

表 49. National Enable パラメーター

パラメーター	DDN デフォルト値	GTE デフォルト値
<u>accept-reverse-charges</u>	off	on
<u>bi-cug</u>	off	off
<u>bi-cug-with-outgoing-access</u>	off	off
<u>cug</u>	off	off
<u>cug-deletion</u>	off	off
<u>cug-insertion</u>	off	off
<u>cug-with-incoming-access</u>	off	off
<u>cug-with-outgoing-access</u>	off	off
<u>cug-zero-override</u>	off	off
<u>flow-control-negotiation</u>	on	on
<u>frame-ext-seq-mode</u>	off	off
<u>packet-ext-seq-mode</u>	off	off
<u>request-reverse-charges</u>	off	on
<u>suppress-calling-addresses</u>	off	off
<u>throughput-class-negotiation</u>	on	on
<u>truncate-called-addresses</u>	off	off

表 50. National Set パラメーター

パラメーター	DDN デフォルト値	GTE デフォルト値
<u>call-req</u>	20 デカ秒	20 デカ秒
<u>clear-req</u> ...	再試行=1	再試行=1
	18 デカ秒	18 デカ秒
<u>disconnect-procedure</u> ...	受動	受動
<u>dly-recall-timer</u> ...	0	0
<u>dp-timer</u>	500 ミリ秒	500 ミリ秒
<u>frame-window-size</u>	7	7

X.25 ネットワーク・インターフェースの使用

表 50. *National Set* パラメーター (続き)

パラメーター	DDN デフォルト値	GTE デフォルト値
n2-timeouts	20	20
packet-size ...	128、最大=256	128、最大=256
reset ...	再試行=1	再試行=1
	18 デカ秒	18 デカ秒
restart ...	再試行=1	再試行=1
	18 デカ秒	18 デカ秒
max-recall-retires ...	3	3
min-recall	10 秒	10 秒
min-connect	90 秒	90 秒
collision-timer	10 秒	10 秒
standard-version	1984	1984
t1-timer	4 秒	4 秒
t2-timer	0	0
truncate-called-addr-size	2	2

ヌル・カプセル化

ヌル・カプセル化は、ユーザーが 1 つの X.25 回線上で複数のネットワーク・レイヤー・プロトコルを多重化することを可能にします。この機能は、過度のバーチャル・サーキットが使用されるのを回避するために使用することができます。

制限

ヌル・カプセル化は、QLLC に対してはサポートされません。この機能は、スイッチド・バーチャル・サーキット (SVC) に対してはサポートされていますが、パーマネント・バーチャル・サーキット (PVC) に対してはサポートされていません。

構成変更

カプセル化オプションの NULL が、以下の T6 コマンドに追加されました。

X25 config の下: add address IP (enc type = NULL と入力)

X25 config の下: add address IPX (enc type = NULL と入力)

X25 config の下: add address DNA (enc type = NULL と入力)

X25 config の下: add address VINES (enc type = NULL と入力)

X25 config の下: list addr は、priority 1 type が NULL の場合、active enc type = NULL を表示します。

T5 コマンド:

X25 int の下: リスト SVCS には enc type = NULL が含まれるようになります。

ヌル・カプセル化および閉域ユーザー・グループ (CUG) の構成

ヌル・カプセル化を使用しているときには、1つのバーチャル・サーキットを介して複数のプロトコルを実行できるので、そのサーキット上の各プロトコルに定義された CUG は同一でなければなりません。ユーザーは、以下の方法を使用して、複数のプロトコルに対して同一のあて先を構成することを強くお勧めします。

`add address` を使用して CUG を構成する。定義された CUG は、同じアドレスに定義された各プロトコルで同一でなければなりません。

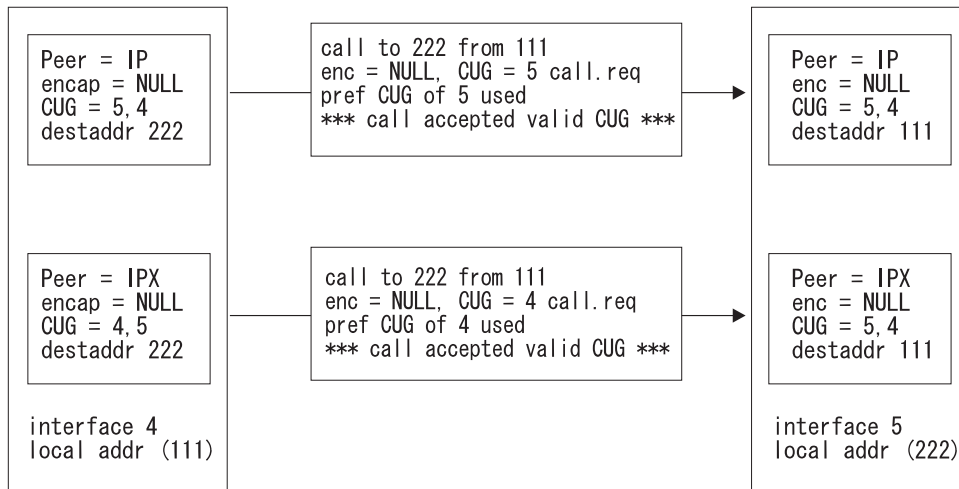
CUG が `add protocol` レベルで定義されている場合は、CUG はすべてのピアで同一でなければなりません (この方法は、より限定的です)。

インターフェース・レベルで CUG を構成する。これにより、すべてのピアが同じ CUG 値を持つことが保証されます (この方法が最も限定的です)。

着信コール CUG 定義がその回線を共用するすべてのプロトコルに有効である限り、上述のどの方法を使用しても構いません。「有効」とは、CUG が特定のアドレスに定義されているか、もしくはデフォルトでプロトコルまたはインターフェースの回線定義が使用されるようになっていることを意味しています。

X.25 ネットワーク・インターフェースの使用

例 1: 両方のピアに有効な着信閉域
ユーザー・グループ (CUG)



例 2: 両方のピアに有効ではない着信閉域
ユーザー・グループ (CUG)

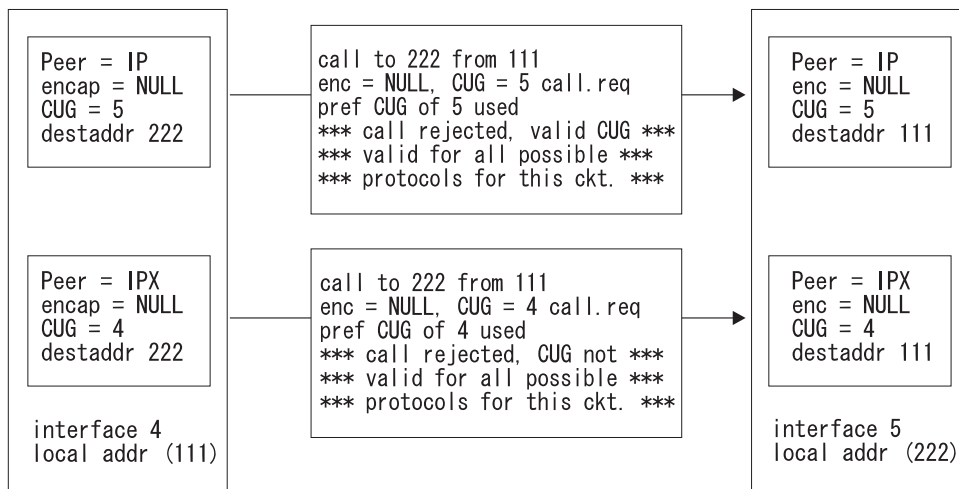


図 18. 閉域ユーザー・グループのヌル・カプセル化

閉域ユーザー・グループの概要

閉域ユーザー・グループ (CUG) とは、他の特定の DTE と接続を確立することが許可されている X.25 DTE のグループをいいます。CUG 番号はネットワーク提供者によって定義され、ユーザーはネットワーク提供者が割り当てた CUG しか使用することができません。ユーザーは、アドレス特定 CUG、プロトコル特定 CUG、またはインターフェース特定 CUG を構成することができます。ある DTE に対してこの 3 つのタイプの CUG メンバーのすべてが構成されている場合、閉域ユーザー・グループ・ファシリティーは、別の DTE に接続するときのコール・リクエストで、アドレス特定のあて先 CUG を使用します。ある DTE に対してプロトコル特定およびイン

X.25 ネットワーク・インターフェースの使用

ターフェース特定 CUG のみが構成されている場合、閉域ユーザー・グループ・ファシリティは、別の DTE に接続するときのコール・リクエストで、プロトコル特定 CUG を使用します。

1 つの DTE が複数の CUG に属することも可能です。ユーザーは、その DTE の優先 CUG を指定する必要があります。ルーターは他の DTE にコールするときに、優先 CUG を使用します。1 つの DTE は、合計 5 つを超える優先または通常の閉域ユーザー・グループを持つことはできません。

相互形閉域ユーザー・グループ

相互形閉域ユーザー・グループ (BCUG) とは、2 つだけの DTE で構成される閉域ユーザー・グループです。BCUG 内の DTE は、BCUG のメンバー、およびどの CUG または BCUG にも属さない任意の DTE にコールすることができます。1 つの DTE は、合計 5 つを超える優先または通常の相互形 CUG を持つことはできません。

DTE が BCUG を使用して回線を確認する方法は、DTE が CUG を使用して回線を確認する方法 (374ページの表51を参照) と同じですが、インターフェース、プロトコル、またはアドレスに対して BCUG と CUG の両方が定義されている場合には、BCUG を使用して回線が確立されます。

拡張閉域ユーザー・グループのタイプ

閉域ユーザー・グループに対する以下の拡張がサポートされています。

出アクセスをもつ CUG

DTE は 1 つまたは複数の CUG に属することができます。DTE は、CUG のメンバー、および入アクセスをもつ他の CUG に属する任意の DTE に発呼することができます。

入アクセスをもつ CUG

DTE は 1 つまたは複数の CUG に属することができます。DTE は、どの CUG にも属さない DTE、または出アクセスをもつ他の CUG に属する DTE からのコールを受信することができます。

出アクセスをもつ BCUG

DTE は 1 つまたは複数の BCUG に属することができます。DTE は、BCUG のメンバー、およびどの BCUG にも属さない任意の DTE にコールすることができます。

装置上に閉域ユーザー・グループをもつ X.25 回線の確立

閉域ユーザー・グループ・ファシリティが使用可能の場合、DTE はコール・リクエストを受け取ると、そのコール・リクエストの中の CUG を使用して、DTE からのコールを受諾するか、リジェクトするかを判別します。コール・リクエストの中の CUG が、インターフェース、プロトコル、またはコーリング DTE に対応するあて先に構成されている CUG に一致しない場合、要求はリジェクトされます。374ページの表51 は、インターフェース、プロトコル、およびアドレス CUG メンバーが異なっており、入アクセスが使用可能でない場合に、CUG に基づいて X.25 回線を確認する方法を要約しています。

X.25 ネットワーク・インターフェースの使用

表 51. 閉域ユーザー・グループの着信 X.25 回線の確立

着信コール・リクエストの内容	受信 DTE CUG 定義							
	インターフェース CUG のみ	プロトコル CUG のみ	アドレス特定 CUG	インターフェースおよびプロトコル CUG	インターフェースおよびアドレス CUG	プロトコルおよびアドレス CUG	すべての CUG	CUG なし
CUG なし	リジェクト	リジェクト	リジェクト	リジェクト	リジェクト	リジェクト	リジェクト	受諾
インターフェース CUG	受諾	リジェクト	リジェクト	リジェクト	リジェクト	リジェクト	リジェクト	リジェクト
プロトコル CUG	リジェクト	受諾	リジェクト	受諾	リジェクト	リジェクト	リジェクト	リジェクト
アドレス特定 CUG	リジェクト	リジェクト	受諾	リジェクト	受諾	受諾	受諾	リジェクト

インターフェース上の発信コールの場合、CUG または BCUG ファシリティーが使用可能のときには、あて先に構成された優先 CUG (もしあれば) が、各コール・リクエストに入れられます。アドレス特定 CUG が構成されていない場合、使用される CUG はプロトコルに定義された CUG になり、プロトコル特定 CUG が構成されていない場合は、使用される CUG はインターフェースに定義された CUG になります。CUG メンバーが構成されていない場合には、CUG ファシリティーはコール・リクエストに組み込まれません。

CUG 0 の閉域ユーザー・グループ処理のオーバーライド

コール・リクエストの中に 0 の CUG が入っている着信コールは妥当性検査をしないように DTE を構成することができます。この機能により、入アクセスが使用可能でなくても、特定のコールを完了させることが可能になります。 **national enable cug 0 override** コマンドを使用すると、CUG 番号が 0 のときには CUG ファシリティーを無視することを装置に強制できます。そのコール・リクエストは、構成された CUG 番号との比較は行われません。

X.25 閉域ユーザー・グループの構成

X.25 インターフェース上で閉域ユーザー・グループを使用するには、次のようにします。

1. ネットワーク提供者から CUG 番号を入手する。これらの番号は、X.25 を構成するときに必要になります。
2. **national enable cug** コマンドと関連のコマンドを使用して、閉域ユーザー・グループ・ファシリティーを使用可能にする。
3. **national enable bi-cug** コマンドと関連のコマンドを使用して、相互形閉域接続ユーザー・グループを使用可能にする (必要な場合)。
4. DTE に対して該当の CUG 番号を構成する。必要に応じて、優先 CUG、CUG、優先相互形 CUG、および相互形 CUG を指定する。これは **add address** コマンドを使用して行います。
5. プロトコルに対して該当する CUG および相互形 CUG を構成する (必要な場合)。これは **add protocol** コマンドを使用して行います。

X.25 ネットワーク・インターフェースの使用

注: アドレス特定 CUG でオーバーライドしない限り、このプロトコルの X.25 インターフェースを介して確立されるすべての X.25 回線を、この固有 CUG または BCUG に属する DTE のみに限定したい場合は、これらの CUG のみを構成する必要があります。

6. インターフェースに対して該当する CUG および相互形 CUG を構成する (必要な場合)。これは **add cug** コマンドを使用して行います。

注: アドレス特定またはプロトコル特定 CUG でオーバーライドしない限り、X.25 インターフェースを介して確立されるすべての X.25 回線を、この固有 CUG または BCUG に属する DTE のみに限定したい場合には、これらの CUG のみを構成する必要があります。

X.25 ネットワーク・インターフェースの使用

第25章 X.25 ネットワーク・インターフェースの構成および監視

この章では X.25 構成および動作コマンドについて説明し、以下の節が含まれています。

- 『X.25 構成コマンド』
- 407ページの『インターフェース監視プロセスへのアクセス』
- 407ページの『X.25 監視コマンド』
- 411ページの『X.25 ネットワーク・インターフェースおよび GWCON インターフェース・コマンド』

X.25 構成コマンド

この節では、すべての X.25 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。

X.25 構成コマンドでは、X.25 パケットを転送するルーター・インターフェースのネットワーク・パラメーターを指定することができます。構成コマンドで指定した情報は、ルーターをリスタートすると有効になります。

X.25 構成コマンドは X.25 config> プロンプトで入力します。表52 は、コマンドをリストしています。

表 52. X.25 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Set	ローカルおよび DDN X.25 ノード・アドレス、パケット・レベルのウィンドウ・サイズを設定し、ナショナル・パーソナリティーの識別、MTU、およびコールの最大数を識別します。PVC および SVC チャネル範囲、交換回線が切断される前にアイドル状態でいられる秒数を定義し、1つのルーターが DCE として動作する必要があるかどうか (X.25 ネットワークが介在せずに2つのルーターが直接接続されている場合) あるいは X.25 ネットワークに接続されている DTE で一般的な方式で動作するかを指定します。また、速度、符号化、クロック、スループット・クラス、およびケーブル・タイプも設定します。
Enable/Disable	着信コール禁止フィーチャー、発信コール禁止フィーチャー、動的 DDN アドレス変換、および lower-dtr フィーチャーを使用可能/使用不可にします。
National Enable or National Disable	ナショナル・パーソナリティー構成で定義されたパラメーターを使用可能/使用不可にします。
National Set	ナショナル・パーソナリティー構成で定義されたパラメーターを設定します。
National Restore	ナショナル・パーソナリティー構成をそのデフォルト値に復元します。

X.25 ネットワーク・インターフェースの構成

表 52. X.25 構成コマンドの要約 (続き)

コマンド	機能
Add/Change/Delete	アドレス変換、プロトコル・カプセル化、または PVC 定義を追加/変更/削除します。
List	定義済みのアドレス変換、ナショナル・パーソナリティー・パラメーター、プロトコル・カプセル化、または PVC 定義をリストします。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Set

set コマンドは、ローカル X.25 ノード・アドレス、コールの最大数、フレームおよびバケット・レベルのウィンドウ・サイズ、PVC および SVC チャネル数の最低値と最高値、交換回線のアイドル・タイムを構成するのに使用します。

構文:

```
set address . . .  
cable  
calls-out . . .  
clocking . . .  
default-window-size . . .  
encoding  
equipment-type . . .  
htf addr . . .  
inter-frame-delay . . .  
mtu  
national-personality . . .  
pvc . . .  
speed . . .  
svc  
throughput-class . . .  
vc-idle . . .
```

address *x.25-node-addr*

ローカル X.25 インターフェース・アドレス (*x.25-node-addr*) を設定します。ローカル X.25 アドレスを削除する場合は、ローカル X.25 ノード・アドレスを 0 に (00 ではなく) 設定します。

例: **set address 8982800**

cable *type*

ケーブル・タイプを次のように設定します。

- RS-232 DTE
- RS-232 DCE

X.25 ネットワーク・インターフェースの構成

- V35 DTE
- V35 DCE
- V36 DTE
- V36 DCE
- X21 DTE
- X21 DCE

DTE ケーブルは、ルーターをあるタイプの DCE 装置 (たとえば、モデムまたは DSU/CSU) に接続するときを使用します。

DCE ケーブルは、ルーターが DCE として動作し、直接接続のためのクロックを提供するときを使用します。

注:

1. インターフェースを 8 ポート EIA 232 アダプター上で構成している場合は、構成できるケーブル・タイプは RS-232 DTE および RS-232 DCE だけです。
2. インターフェースを 6 ポート V.35/V.36 アダプター上で構成している場合は、構成できるケーブル・タイプは V.35 DTE、V.35 DCE、V.36 DTE、V.36 DCE だけです。
3. インターフェースを 8 ポート X.21 アダプター上で構成している場合は、構成できるケーブル・タイプは X.21 DTE および X.21 DCE だけです。

calls-out *value*

ローカルで開始し、同時にアクティブにできる SVC の最大数を設定します。

有効値: 1 ~ 239

デフォルト値: 4

clocking *external or internal*

モデムまたは DSU に接続するには、外部クロックを構成し、**set cable** コマンドを使って該当する DTE ケーブルを選択します。回線速度を構成するには、**set speed** コマンドを使用します。

別の DTE 装置に直接接続するには、内部クロックを構成し、**set cable** コマンドを使って該当する DCE ケーブルを選択し、**set speed** コマンドを使ってクロック/回線速度を構成します。

デフォルト値: external

default-window-size *value*

コール・リクエスト・パケット内にウィンドウ・サイズ・ファシリティが存在しない場合、ルーターによって割り当てられるパケット・レベルのウィンドウ・サイズを設定します。範囲は、ナショナル・パーソナリティのパケット・モジュラス (PACKET-EXT-SEQ-MODE) によって決まります。

デフォルト値: 2

例: **set default-window-size 3**

encoding *NRZ or NRZI*

インターフェースの HDLC 伝送符号化規則を設定します。符号化規則は、NRZ (非ゼロ復帰記録) または NRZI (非ゼロ復帰反転) に設定できます。NRZ は、広く一般的に使用されている符号化規則であり、一方の NRZI は一部の IBM 構成で使用されます。

X.25 ネットワーク・インターフェースの構成

デフォルト値: NRZ

equipment-type *DCE or DTE*

フレームおよびパケット・レベルが DCE として動作するのか、DTE として動作するのかを指定します。このコマンドは、使用しているケーブル・タイプには無関係です。

デフォルト: DTE (X.31 の場合は DTE が必須)

htf addr *x.25-node-addr*

DDN が使用されている場合、ローカル DTE アドレスを設定します。これは、CCITT が使用されているときにローカル DTE アドレスを設定するのに使用される **set address** コマンドとは反対に、IP アドレスを X.121 アドレスに変換します。

inter-frame-delay *value*

このパラメーターは、送信フレーム間の最小遅延を定義します。このパラメーターを設定しておくで、旧式装置に直接インターフェースする場合に役立ちます。このパラメーターは、フレーム間の時間の長さ (秒単位) です。

注: 8 ポート EIA-232E アダプター、6 ポート V.35/V.36 アダプター、または 8 ポート X.21 アダプター上の X.25 インターフェースについて非ゼロのフレーム間遅延を構成する場合、**set speed** コマンドを使用して速度を構成します。

デフォルト値: 0

mtu *value*

最大送信単位 (MTU) をバイト数で設定します。これは、パッケージに入れてシリアル・ライン経由で転送するために X.25 インターフェースに送達される最大メッセージ・サイズです。範囲は 576 ~ 16384 です。

デフォルト値: 1500

X.25 インターフェースを介してデータを転送するときにパケット再組み立てタイムアウトが発生する場合、エンドポイントに達するまでのすべての LAN またはシリアル・インターフェースの最小パケット・サイズを調べて、より適切な X.25 MTU を計算する必要があります。X.25 は実際より小さいパケット・サイズを使用する傾向があるので、この計算では、実際の X.25 パケット・サイズを直接考慮しないでください。X.25 は通常、最大 7 つのパケットを一度に送信して、確認応答を待ちます。

たとえば、以下のものが含まれているネットワーク・トポロジを考えてみてください。

- パケット・サイズが 4000 のトークンリング LAN
- パケット・サイズが 128、ウィンドウ・サイズが 7、およびビット・レートが 9600 bps の X.25 シリアル・ライン
- パケット・サイズが 1500 のイーサネット LAN

この場合は、おそらく X.25 MTU を 1500 に設定する必要があります。これは、約 12 のパケットが X.25 インターフェースを介して送信されることを意味しています (MTU / X.25 パケット・サイズ = 送信される X.25 パケット数)。

X.25 ネットワーク・インターフェースの構成

MTU が 4096 のときは、X.25 インターフェースを介して 32 のパケットを送信する必要があります (4000 / 128 = 31.25)。この場合、X.25 モデムの速度が 9600 bps のときは、おそらくパケット再組み立てタイムアウトが発生することが予想されます。X.25 モデムの速度を 56 Kbps であれば、この問題を解決できるものと思われます。

注:

1. MTU パラメーターは、装置のメモリー所要量とメモリー使用率に大きな影響を与えます。メモリーが 8M より小さい装置では、8192 以下の MTU 値を使用してください。
2. 装置の稼働中に使用可能なメモリーの量によって、SVC を確立し、しかも最適な性能に維持できる数が制限されます。推奨される SVC の最大数については、WWW 上の製品のホーム・ページを参照してください。

national-personality *GTE-Telenet* または *DDN*

GTE-Telenet または DDN ナショナル・パーソナリティーの 28 のデフォルト・パラメーターを設定します。

デフォルト値: GTE-Telenet

pvc low/high *value*

パーマネント・バーチャル・サーキットの最低と最高のチャンネル番号を定義します。ゼロは、PVC がないことを示します。デフォルトでは「PVC なし」になります。

pvc low

0

pvc high

0

範囲は 1 ~ 4095 です。これらの値は、指定の VC 範囲の限界値を設定します。最大 2500 の PVC があります。

例: **set pvc low 40**

注: 値は、SVC 用に設定した値とオーバーラップしてはなりません。

speed *speed-setting*

内部クロックの場合は、このコマンドを使用して送信および受信クロック回線の速度を指定します。

外部クロックの場合は、このコマンドは WAN/シリアル回線の動作には影響を与えませんが、一部のプロトコル (IPX など) がルーティング・コスト・パラメーターを判別するのに使用する速度を設定します。速度は、実際の回線速度に一致するように設定する必要があります。

有効値:

内部クロック: 382ページの表53 を参照してください。

外部クロック: 382ページの表54を参照してください。

注: X.25 ソフトウェアがサポートされるのは、速度が 256 000 bps 以下の場合だけです。

X.25 ネットワーク・インターフェースの構成

表 53. 内部クロックが 2210 インターフェースに使用される時の回線速度

アダプター・タイプ	速度範囲
8 ポート EIA 232	9600 ~ 64 000 bps
6 ポート V.35/V.36	9600 ~ 460 800 bps、1 544 000 bps、または 2 048 000 bps
8 ポート X.21	9600 ~ 460 800 bps、1 544 000 bps、または 2 048 000 bps

表 54. 外部クロックが 2210 インターフェースに使用される時の回線速度

アダプター・タイプ	速度範囲
8 ポート EIA 232	2400 ~ 64 000 bps
6 ポート V.35/V.36	2400 ~ 2 048 000 bps
8 ポート X.21	2400 ~ 2 048 000 bps

デフォルト値: 9600

svc low/high inbound or two-way or outbound value

スイッチド・バーチャル・サーキットの最低および最高チャネル番号を定義します。low=high=0 のときは、このカテゴリーの VC は定義されていません。

例: **set SVC low-two-way 1**

Inbound

インバウンド SVC に割り当てられる論理チャネル番号の範囲を指定します。デフォルトでは、インバウンド専用の SVC はないことになります。

有効値: 0 ~ 4095

デフォルト値: 0

Two-way

両方向 SVC に割り当てられる論理チャネル番号の範囲を指定します。デフォルトでは、64 の両方向 SVC があります。

有効値: 0 ~ 4095

デフォルト値:

svc low

1

svc high

64

Outbound

アウトバウンド SVC に割り当てられる論理チャネル番号の範囲を指定します。デフォルトでは、アウトバウンド専用の SVC はないことになります。

有効値: 0 ~ 4095

デフォルト値: 0

注: 各範囲の値は、他の SVC 範囲とも、PVC 範囲ともオーバーラップしてはなりません。383ページの表55 は、可能な VC 構成を示しています。

表 55. VC 定義の例

	低	高
PVC	1	40
インバウンド	0	0
両方向	41	59
アウトバウンド	60	500

throughput-class inbound または outbound bit-rate

スループットのネゴシエーションが使用可能な場合、コール・リクエストを
 するとき要求されるスループット・クラスを定義します。

デフォルト値: 2400 bps

着信コール・リクエストの処理時には、この設定値は無視されます。

vc-idle value

ルーターによって切断される前に、交換回線がアイドル状態になれる秒数を
 定義します。ゼロは、ルーターがアイドル回線を切断しないことを示しま
 す。

有効値: 1 ~ 255

デフォルト値: 30 秒

Enable

enable コマンドは、DDN アドレス変換、インターフェース・リセット、または着信
 コール禁止、発信コール禁止、および lower-dtr フィーチャーを使用可能にするのに
 使用します。

構文:**enable**ddn--address-translations

注: ddn-address-translations は、使用可能にすることが
 できなくなりました。このフィーチャーは、選
 択されたナショナル・パーソナリティが DDN
 の場合は、デフォルトで使用可能になり、その
 他の場合は、デフォルトで使用不可になりま
 す。

incoming-calls-barredlower-dtroutgoing-calls-barred**incoming-calls-barred**

ルーターは着信コールを受け入れないことを指定します。このパラメーター
 のデフォルト設定値は、使用不可またはオフ で、これは着信コールを受け入
 れます。

lower-dtr

このパラメーターは、使用不可にされている専用シリアル・ライン・インタ
 ーフェースにおけるデータ端末レディー (DTR) 信号の処理方法を決めます。

X.25 ネットワーク・インターフェースの構成

このパラメーターが "使用不可" (デフォルト値) に設定されている場合、インターフェースが使用不可のときは、DTR 信号は上がります。

`lower-dtr` が "使用可能" に設定されている場合、インターフェースが使用不可のときは、DTR は下がります。この動作が適している状況は、インターフェースが WAN 再ルートの代替リンクとして構成されており、インターフェースが、DTR 信号の状態に基づいてダイヤル接続を維持するダイヤルアウト・モデムに接続されているような場合です。

`lower-dtr` が使用可能で、インターフェースが使用不可のとき、DTR 信号は下がり、モデムはダイヤル接続をダウンに保持します。インターフェースが使用可能になると (WAN 再ルートのバックアップ・シナリオにより)、DTR は上がり、モデムは保管しているバックアップ・サイトへの番号をダイヤルします。1 次インターフェースが復元すると、代替インターフェースは使用不可にされ、DTR は下がって、モデムはダイヤル接続を切断します。

以下のケーブル・タイプがサポートされます。

RS-232

V.35

V.36

デフォルト設定値は使用不可です。

outgoing-calls-barred

ルーターは発信コールを許可しないことを指定します。このパラメーターのデフォルト設定値は、使用不可またはオフで、これは発信コールを許可します。

Disable

disable コマンドは、DDN アドレス変換、ネットワーク認証の一部としてのインターフェース・リセット、あるいは着信コール禁止または発信コール禁止フィーチャーを使用不可にするのに使用します。

注: DDN をナショナル・パーソナリティーとして設定した場合、DDN アドレス変換が自動的に使用可能になり、このパラメーターは無効になります。

構文:

disable

ddn-address-translations

注: `ddn-address-translations` は、使用不可にすることができなくなりました。このフィーチャーは、選択されたナショナル・パーソナリティーが DDN の場合は、デフォルトで使用可能になり、その他の場合は、デフォルトで使用不可になります。

incoming-calls-barred

lower-dtr

outgoing-calls-barred

National Enable

national enable コマンドは、ナショナル・パーソナリティー構成で定義されたフィーチャーを使用可能にするのに使用します。

構文:

national enable accept-reverse-charges
 bi-cug
 bi-cug-outgoing-access
 cug
 cug-deletion
 cug-incoming-access
 cug-insertion
 cug-outgoing-access
 cug-zero-override
 flow-control-negotiation
 frame-ext-seq-mode (required for X.31)
 packet-ext-seq-mode
 request-reverse-charges
 suppress-calling-addresses
 throughput-class-negotiation
 truncate-called-addresses

accept-reverse-charges

コール設定時の着信課金を受け入れます。このオプションは、DDN では利用不能です。

DDN デフォルト値

off

GTE デフォルト値

on

bi-cug この装置上の相互形閉域接続ユーザー・グループ・ファシリティを使用可能にします。デフォルトでは、このファシリティは使用不可です。

注: このパラメーターが使用可能でない場合は、相互形 CUG を追加することはできません。

bi-cug-outgoing-access

この装置上の出アクセスをもつ相互形 CUG を使用可能にします。デフォルトでは、このファシリティは使用不可です。

cug この装置上の閉域接続ユーザー・グループ・ファシリティを使用可能にします。デフォルトでは、このファシリティは使用不可です。

X.25 ネットワーク・インターフェースの構成

注: このパラメーターが使用可能でない場合は、CUG を追加することはできません。

cug-deletion

X.25 を介して転送する前に、XTP から受信したコール・パケットから CUG ファシリティを除去します。デフォルトでは、この機能は使用不可です。

cug-incoming-access

この装置上の入アクセスをもつ CUG を使用可能にします。デフォルトでは、このファシリティは使用不可です。

cug-insertion

IP を介して要求を転送する前に、X.25 インターフェースから XTP が受信したコール・リクエストに、該当する (アドレス特定、プロトコル特定、またはインターフェース特定) 優先 CUG 番号を挿入します。コール・パケット内にすでに CUG ファシリティが存在する場合は、それを置き換えません。デフォルトでは、この機能は使用不可です。

cug-outgoing-access

この装置上の出アクセスをもつ CUG を使用可能にします。デフォルトでは、このファシリティは使用不可です。

cug-zero-override

閉域ユーザー・グループ・ファシリティに対して、CUG 番号 0 をもつコール・リクエスト・パケット内の CUG ファシリティを無視させます。デフォルトでは、この機能は使用不可です。

flow-control-negotiation

SVC のコール設定時にパケットおよびウィンドウ・サイズのネゴシエーションを使用可能にします。

DDN デフォルト値

on

GTE デフォルト値

on

frame-ext-seq-mode

フレーム・レイヤーのシーケンス番号をモジュロ 128 (つまり、0 ~ 127) に設定します。

DDN デフォルト値

off (X.31 の場合は on が必須)

GTE デフォルト値

off

packet-ext-seq-mode

パケット・レイヤーが拡張シーケンス番号 (0 ~ 127) を使用できるようにします。

DDN デフォルト値

off

GTE デフォルト値

off

request-reverse-charges

すべての発信コールに対して着信課金を要求します。

DDN デフォルト値

off

GTE デフォルト値

on

suppress-calling-address

コール・パケット内の発信元アドレスを抑制します。

DDN デフォルト値

off

GTE デフォルト値

off

throughput-class-negotiation

スループット・クラスの登録を使用可能にします。

DDN デフォルト値

off

GTE デフォルト値

on

truncate-called-addresses

DTE へのコールの転送時のコールされる DTE アドレスの切り捨てを使用可能にします。このオプションは XTP 回線にのみ適用されます。

DDN デフォルト値

off

GTE デフォルト値

off

National Disable

national disable コマンドは、ナショナル・パーソナリティ構成で定義されたフィーチャーを使用不可にするのに使用します。

構文:

```
national disable          accept-reverse-charges
                           bi-cug
                           bi-cug-outgoing-access
                           cug
                           cug-deletion
                           cug-incoming-access
                           cug-insertion
                           cug-outgoing-access
                           cug-zero-override
```

X.25 ネットワーク・インターフェースの構成

flow-control-negotiation
frame-ext-seq-mode
packet-ext-seq-mode
request-reverse-charges
suppress-calling-addresses
throughput-class-negotiation
truncate-called-addresses

National Set

national set コマンドは、ナショナル・パーソナリティー構成のデフォルト値の 1 つまたはすべてを設定するのに使用します。

構文:

national set call-req
clear-req . . .
disconnect-procedure . . .
dly-recall-timer . . .
dp-timer
frame-window-size
n2-timeouts
packet-size . . .
reset . . .
restart . . .
max-call-retries . . .
min-recall
min-connect
collision-timer
standard-version
t1-timer
t2-timer
truncate-called-addr-size

call-req

コール・リクエストをあきらめて切断する前に許される 10 秒間隔の回数を指定します。ゼロは、無期限に待つことを示します。list コマンドの出力では、これは t21 タイマーとして表示されます。

DDN デフォルト値

20 デカ秒

GTE デフォルト値

20 デカ秒

clear-req *retries or timer*

復旧要求の再送の回数を指定します。

Retriesアクションを取る前に許される復旧要求の伝送の回数。 `list` コマンドの出力では、これは `r23` 再試行カウントとして表示されます。**DDN デフォルト値**

再試行=1

GTE デフォルト値

再試行=1

Timer 復旧要求パケットを再送する前に待つ 10 秒間隔の回数。タイマー値のゼロは、無期限に待つことを示します。 `list` コマンドの出力では、これは `t23` タイマーとして表示されます。**DDN デフォルト値**

18 デカ秒

GTE デフォルト値

18 デカ秒

disconnect-procedure *passive or active*

接続時に使用する接続手順のタイプを指定します。

DDN デフォルト値

passive

GTE デフォルト値

passive

Passive

接続時に SABM フレームがルーターによって開始されないことを指定します。

Active 接続時に SABM フレームがルーターによって開始されることを指定します。**dly-recall-timer**このコマンドは **XTP** または **QLLC** には適用されません。連続して `max-call-retries` の試行に失敗した後に遅らせる時間を指定します。`max-call-retries` を超えるまで、コール試行の間で遅らせるのに `min-recall` タイマーが引き続き使用されます。`min-recall` または `dly-recall` タイマーの実行中はコールの試行は行なわれません。範囲は 0 ~ 1080 分です。 `dly` タイマーが使用されない場合は、0 を指定します。**DDN デフォルト値**

0

GTE デフォルト値

0

例: `national set dly-recall 30`

X.25 ネットワーク・インターフェースの構成

dp-timer

フレーム・レベルが切断状態のままのミリ秒数を指定します。ゼロは、即時に切断フェーズからリンク設定状態に移行することを示します。

DDN デフォルト値

500 ミリ秒

GTE デフォルト値

500 ミリ秒

frame-window-size

確認の前にアウトスタンディング状態に置くことができるフレーム数を指定します。

DDN デフォルト値

7

GTE デフォルト値

7

n2-timeouts

インターフェースがリサイクルされる前に再送タイマー (T1) を満了させることができる回数を指定します。

DDN デフォルト値

20

GTE デフォルト値

20

packet-size *default or maximum or window*

パケットのサイズを指定します。

default

パケットのデータ部分のバイト数。可能なオプションは、128、256、512、1024、2048、および4096です。この値は、パケット・サイズのネゴシエーションが行われない場合に使用されます。*Default* は *maximum* より大きい値であってはなりません。

DDN デフォルト値

128

GTE デフォルト値

128

maximum

パケットのデータ部分の最大バイト数。可能なオプションは、128、256、512、1024、2048、および4096です。

DDN デフォルト値

256

GTE デフォルト値

256

window

確認応答が必要になる前に許されるアウトスタンディング I フレームの数。範囲は、ナショナル・パーソナリティーの packets・モジュラスによって決まります。

関連の構成パラメーターは、次のとおりです。

- Protocol max default window
- Set default window size

reset *retries or timer*

リセット要求の再送回数を指定します。

例: **national set reset retries 2**

retries

コールが切断される前に許されるリセット要求の伝送回数。範囲は 0 ~ 255 です。list コマンドの出力では、これは r22 再試行カウントとして表示されます。

DDN デフォルト値

1

GTE デフォルト値

1

timer リセット要求パケットを再送する前に待つ 10 秒間隔の回数。範囲は 0 ~ 255 です。タイマー値のゼロは、無期限に待つことを示します。list コマンドの出力では、これは t22 タイマーとして表示されます。

DDN デフォルト値

18 デカ秒

GTE デフォルト値

18 デカ秒

restart *retries or timer*

リスタート要求の伝送回数を指定します。

retries

インターフェースがリサイクルされる前に許されるリスタート要求の伝送回数。範囲は 0 ~ 255 です。list コマンドの出力では、これは r20 再試行カウントとして表示されます。

DDN デフォルト値

1

GTE デフォルト値

1

timer リスタート要求パケットを再送する前に待つ 10 秒間隔の回数。範囲は 0 ~ 255 です。タイマー値のゼロは、無期限に待つことを示します。list コマンドの出力では、これは t20 タイマーとして表示されます。

DDN デフォルト値

18 デカ秒

X.25 ネットワーク・インターフェースの構成

GTE デフォルト値

18 デカ秒

max-recall-retries

このコマンドは **XTP** または **QLLC** には適用されません。データを消去して、遅延リコール・タイマーが始動する前に、(あて先ごとに) リコールの試行が何回行なわれるかを指定します。max-call-retries は、インターフェースを通じて定義されます。リコールの試行が行なわれない場合は、0 を指定します。

DDN デフォルト値

3

GTE デフォルト値

3

例: **national set max-call-retries 5**

min-recall

SVC をオープンするためにコールを再初期化する前に待つ最小秒数を指定します。範囲は 0 ~ 255 秒です。

DDN デフォルト値

10 秒

GTE デフォルト値

10 秒

min-connect

すべての誤り状態を禁止するコネクションが確立された後、SVC が確立状態に保たれる最小時間を秒数で指定します。範囲は 0 ~ 255 秒です。

DDN デフォルト値

90 秒

GTE デフォルト値

90 秒

collision-timer

元の試行結果がコール衝突であった場合、SVC をオープンするためにコールを再初期化する前に使用する時間遅延を秒数で指定します。範囲は 0 ~ 255 秒です。

DDN デフォルト値

10 秒

GTE デフォルト値

10 秒

standard-version

オプションは、none、v1980、v1984、および v1988 です。

DDN デフォルト値

1984

GTE デフォルト値

1984

t1-timer

フレーム再送時間を秒数で指定します。範囲は 1 ～ 255 です。

DDN デフォルト値

4 秒

GTE デフォルト値

4 秒

t2-timer

I フレームを確認応答する前の遅延時間を秒数で指定します。これは最適化パラメーターです。タイマーを 0 に設定すると、これは使用不可になります。範囲は 0 ～ 255 です。

DDN デフォルト値

0

GTE デフォルト値

0

truncate-called-addr-size

コールされるアドレスの末端から切り捨てられる文字数を指定します。このオプションは XTP 回線にのみ関係します。範囲は 0 ～ 10 です。

DDN デフォルト値

2

GTE デフォルト値

2

National Restore

national restore コマンドは、**national set**、**national enable**、または **national disable** コマンドを使用してナショナル・パーソナリティー構成で設定したデフォルト値の 1 つまたはすべてを復元するのに使用します。

構文:

```
national restore           all
                             accept-reverse-charges
                             bi-cug
                             bi-cug-outgoing-access
                             call-req
                             clear-req . . .
                             cug
                             cug-deletion
                             cug-incoming-access
                             cug-insertion
                             cug-outgoing-access
                             cug-zero-override
```

X.25 ネットワーク・インターフェースの構成

disconnect-procedure . . .
dp-timer
flow-control-negotiation
frame-ext-seq-mode
frame-window-size
min-collision-timer
min-connect-timer
min-recall-timer
network-type . . .
n2-timeouts
packet-size . . .
packet-ext-seq-mode
request-reverse-charges
reset . . .
restart . . .
standard-version
suppress-calling-addresses
throughput-class-negotiation
t1-timer
t2-timer
truncate-called-addresses
truncate-called-addr-size

Add

add コマンドは、X.121 アドレス、DDN X.25 アドレス、プロトコル構成、または PVC 定義を追加するのに使用します。

構文:

```
add                address  
                   bi-cugs  
                   cugs  
                   htf-address  
                   protocol  
                   pvc
```

address

ルーターの構成でサポートされているプロトコルの X.121 アドレス変換を追加します。表示されるプロンプトは、追加するプロトコル・アドレスによっ

X.25 ネットワーク・インターフェースの構成

て異なります。(以下の例を参照してください。) 入力するプロトコル・アドレスおよび X.121 アドレスは、そのプロトコルと、ルーター X.25 インターフェースに接続するリモート DTE の X.121 DTE アドレスを表します。プロトコルが APPN または DLSw でない限り、プロトコル・アドレスと X.121 アドレスのマッピングは固有でなければなりません。プロトコル・アドレスは、複数の X.121 アドレスにマップすることはできません。また、特定の X.121 アドレスを複数のプロトコル・アドレスにマップすることもできません。ローカル X.25 アドレスを設定するには **set address** コマンドを使用します。ローカル X.25 アドレスを設定した後は、ダイヤルアウト用の X.25 リモート・アドレスおよびオプションのコール ID 用の着信リモート・アドレスを使用できるようになります。リモートのコールされるアドレスのみを入力した場合、このアドレスが、発信コールと着信コールの検証に使用されます。

例: add address

IP の例:

```
Protocol [IP]? IP
IP Address [0.0.0.0]? 128.185.1.2
Enc Priority 1 []? CC
Enc Priority 2 []? SNAP
Enc Priority 3 []? Null
X.25 Address []? 1234590
Remote address []?
Pref CUG []? 11
CUG (2) []? 12
CUG (3) []? 13
CUG (4) []? 14
CUG (5) []? 15
Pref BI-CUG []? 21
BI-CUG (2) []? 22
BI-CUG (3) []?
```

IPX の例:

```
Protocol [IP]? IPX
CUD Field Usage (Standard or Proprietary)
IPX Host Number (in hex) []?
Enc Priority 1 []? SNAP
Enc Priority 2 []? Null
X.25 Address []?
Pref CUG []?
Pref Bi-CUG []? 1
BI-CUG (2) []? 3
BI-CUG (3) []?
```

Protocol

追加するアドレス・マッピングのプロトコル・タイプを指定します。有効値は、APPN、DECnet、DLSw、IP、IPX、および VINES です。デフォルト値は IP です。

Enc Priority

CUD に書き込まれるカプセル化タイプ (RFC 1356 で定義) を決めます。IP の場合、有効な選択は CC、SNAP または Null です。IPX の場合、有効な選択は SNAP または Null です。

IP Address

あて先の IP アドレスを指定します。

CUD Field Usage

このフィールドは、IPX から X.25 へのアドレス・マッピング専用です。これは、IPX のコール・リクエスト・パケットを受信したときの

X.25 ネットワーク・インターフェースの構成

コール・ユーザー・データ (CUD) フィールドの記入方法を決めます。CUD フィールドは Standard または Proprietary のいずれかです。Standard (標準) は、その使用法が RFC 1356 で使用されているプロトコル多重化であることを示します。Proprietary (専有) は、2210 またはこれと整合性のあるルーターのみが使用できる専有の CUD フィールドであることを示します。デフォルト値は Standard です。

IPX Host Number

あて先の IPX ホスト番号を指定します。

X.25 Address

ルーター X.25 インターフェースに接続するリモート DTE の X.121 DTE アドレスを指定します。最大アドレス長は 15 桁です。

pref cug

この DTE の優先閉域ユーザー・グループ番号を指定します。DTE は発信コールでこの CUG を使用します。

有効値: 0 ~ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、閉域ユーザー・グループ・ファシリティを使用可能にした場合は、この値を求めるプロンプトが出ます。

CUG この DTE の閉域ユーザー・グループ番号を指定します。優先 CUG を含めて、最大 5 つの CUG を定義することができます。

有効値: 0 ~ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、閉域ユーザー・グループ・ファシリティを使用可能にした場合は、この値を求めるプロンプトが出ます。

pref bi-cug

この DTE の優先相互形閉域ユーザー・グループ番号を指定します。DTE は発信コールでこの CUG を使用します。

有効値: 0 ~ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、相互形閉域ユーザー・グループ・ファシリティを使用可能にならなかった場合は、この値を求めるプロンプトは出ません。

bi-cug この DTE の相互形閉域ユーザー・グループ番号を指定します。最大 5 つの CUG を定義することができます。

有効値: 0 ~ 9999

デフォルト値: なし

X.25 ネットワーク・インターフェースの構成

注: **national enable** コマンドを使用して、相互形閉域ユーザー・グループ・ファシリティを使用可能になかった場合は、この値を求めるプロンプトは出ません。

cugs この X.25 インターフェースの閉域ユーザー・グループ番号を指定します。

有効値: 0 ~ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、閉域ユーザー・グループ・ファシリティを使用可能にした場合は、この値を求めるプロンプトが出ます。

例:

```
add cugs
Pref CUG [ ]? 23
CUG (2) [ ]? 24
CUG (3) [ ]? 25
CUG (4) [ ]? 26
CUG (5) [ ]? 27
```

pref cug

この DTE の優先閉域ユーザー・グループ番号を指定します。この DTE は発信コールでこの CUG を使用します。

有効値: 0 ~ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、閉域ユーザー・グループ・ファシリティを使用可能にした場合は、この値を求めるプロンプトが出ます。

cug この DTE の閉域ユーザー・グループ番号を指定します。最大 5 つの CUG を定義することができます。

有効値: 0 ~ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、閉域ユーザー・グループ・ファシリティを使用可能にした場合は、この値を求めるプロンプトが出ます。

bi-cugs

この DTE の閉域ユーザー・グループ番号を指定します。

有効値: 0 ~ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、閉域ユーザー・グループ・ファシリティを使用可能にした場合は、この値を求めるプロンプトが出ます。

例:

X.25 ネットワーク・インターフェースの構成

```
add bi-cugs
Pref BI-CUG [ ]? 23
BI-CUG (2) [ ]? 24
BI-CUG (3) [ ]? 25
BI-CUG (4) [ ]? 26
BI-CUG (5) [ ]? 27
```

pref bi-cug

この DTE の優先閉域ユーザー・グループ番号を指定します。この DTE は発信コールでこの BI-CUG を使用します。

有効値: 0 ~ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、相互形閉域ユーザー・グループ・ファシリティを使用可能にならなかった場合は、この値を求めるプロンプトは出ません。

bi-cug この DTE の閉域ユーザー・グループ番号を指定します。最大 5 つの CUG を定義することができます。

有効値: 0 ~ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、相互形閉域ユーザー・グループ・ファシリティを使用可能にならなかった場合は、この値を求めるプロンプトは出ません。

htf-address

Defense Data Network (DDN) の X.25 アドレス変換を追加します。

例:

```
add htf-address
Protocol [IP]
Convert HTF address
```

Protocol

X.25 インターフェースを介して実行するプロトコルを指定します。DDN は IP のみをサポートします。

Convert HTF address

プロトコル・アドレスをホスト・テーブル・フォーマット (HTF) 形式のあて先 X.121 アドレスに変換します。Enable/Disable コマンドの `ddn-address-translations` の項も参照してください。

protocol

プロトコル・カプセル化を使用可能にし、関連のパラメーターを定義します。

例:

```
add protocol
Protocol [IP]?
Window Size [2]?
Default Packet Size [128]?
Maximum Packet Size [256]?
Circuit Idle Time [30]?
Max VCs [4]?
Pref CUG [ ]? 1
CUG (2) [ ]? 2
CUG (3) [ ]? 3
```


X.25 ネットワーク・インターフェースの構成

```
CUG (4) [ ]? 4
CUG (5) [ ]? 5
Pref BI-CUG [ ]? 11
BI-CUG (2) [ ]? 12
BI-CUG (3) [ ]? 13
BI-CUG (4) [ ]? 14
BI-CUG (5) [ ]? 15
```

QLLC の例:

```
X.25 Config> add prot
Protocol [IP]? d1s
Idle timer [30]?
QLLC response timer (in decaseconds) [2]?
QLLC response count [3]?
Accept Reverse Charges [N]?
Request Reverse Charges [N]?
Station Type (1) PRI (2) SEC (3) (PEER) [3]?
Max Packet Size [128]?
Packet window size [7]?
Max Message Size [1500]?
Call User Data (in hex, 0 for null) [ ]?
Pref CUG [ ]? 20
CUG (2) [ ]? 21
CUG (3) [ ]?
Pref BI-CUG [ ]?
```

Protocol

カプセル化パラメーターを追加したいプロトコル (APPN、 XTP、 IP、 DECnet、 IPX、 DLSw、または Banyan VINES) を指定します。デフォルト値は IP です。

Window Size

パケットの確認が必要になる前にアウトスタンディング状態に置けるパケット数を表す、最大交渉可能パケット・ウィンドウ・サイズを指定します。デフォルト値は 2 です。ウィンドウ・サイズはコールされる側の DTE によって最低 1 まで交渉できます。

関連の構成パラメーターは、次のとおりです。

- Set Default Window

Default Packet Size

SVC のデフォルトの要求パケット・サイズを指定します。この値は、最低交渉可能パケット・サイズとして使われ、

national set packet-size コマンドで指定された最大パケット・サイズ以下でなければなりません。最小 *default packet size* は 4096 バイトです。このパラメーターのデフォルト値は 128 バイトです。

関連の構成パラメーターは、次のとおりです。

- National Set Packet Size Default
- National Set Packet Size Maximum

Maximum Packet Size

SVC の最大交渉可能パケット・サイズを指定します。この値は、**national set packet-size** コマンドで指定された最大パケット・サイズ以下でなければなりません。このパラメーターのデフォルト値は 256 バイトです。このパラメーターに構成できる最大値は 4096 バイトです。この値は、この X.25 インターフェースの最大フレーム・サイズを計算するのに使用されます。

関連の構成パラメーターは、次のとおりです。

- National Set Packet Size Default

X.25 ネットワーク・インターフェースの構成

- National Set Packet Size Maximum

Circuit Idle Time

ルーターによって切断される前に、SVC がアイドル状態でいられる秒数を指定します。範囲は 0 ～ 65365 です。デフォルト値は 30 秒です。0 (ゼロ) は、その回線はルーターによって切断されることがないことを示します。

Maximum VCs

あるプロトコルの同じ DTE アドレスに対してオープンできる回線の最大数を指定します。このパラメーターの用法については、RFC 1356 を参照してください。有効範囲は 1 ～ 10 です。デフォルト値は 4 です。

pref CUG, CUG, pref bi-cug, bi-cug

add address コマンドを参照してください。

以下は、QLLC 固有のパラメーターです。

QLLC response timer

再送する前に Q レスポンス・パケットを待つ秒数

QLLC response count

QLLC を再送するする最大回数。この再試行回数が尽きると、回線がルーターによって切断またはリセットされる可能性があることを高位レイヤーに通知します。

Accept Reverse Charges

このプロトコルを使用して、このナショナル・パーソナリティー・パラメーターの設定値を指定変更することができます。これは、ナショナル・パーソナリティー・パラメーターには影響を与えません。

Request Reverse Charges

このプロトコルを使用して、このナショナル・パーソナリティー・パラメーターの設定値を指定変更することができます。これは、そのナショナル・パーソナリティー・パラメーターには影響を与えません。

Station Type

このプロトコルのデフォルトのステーション・タイプを指定します。

Pri 1 次ステーション

Sec 2 次ステーション

Peer ピア・ステーション

Max message size

このプロトコルの最大メッセージ・サイズ。インターフェースの最大 MTU サイズ以下の値を指定します。

Call User Data

このプロトコルのコール・パケットで使用されるデフォルトの CUD フィールドを指定します。1 ～ 16 文字を指定します。文字を指定しない場合は、デフォルトの 0xC3 が使用されます。

X.25 ネットワーク・インターフェースの構成

pvc PVC、ウィンドウ・サイズ、およびパケット・サイズの定義を追加します。

例: **add pvc**

IP の例:

```
Protocol [IP]? IP
Packet Channel Range Start [1]?
Destination X.25 Address [ ]?
Packet Channel Range End [1]?
Window Size [2]?
Packet Size [128]?
```

Protocol

カプセル化を変更したいプロトコル (APPN、XTP、DECnet、Banyan Vines、DLSw、IP、または IPX) を指定します。デフォルト値は IP です。

Packet Channel Range Start

この範囲の PVC の始めの回線番号を指定します。

Packet Channel Range End

この範囲の PVC の最後の回線番号を指定します。デフォルトでは、Packet Channel Range Start の値となります。

Destination X.25 Address

PVC のあて先の X.25 アドレスを指定します。

Remote Address

受信したコールのコラー ID のリモート・アドレスを指定します。

Window Size

パケットの確認が必要になる前にアウトスタンディング状態に置けるパケット数を指定します。デフォルト値は 2 です。

関連の構成パラメーターは、次のとおりです。

- Set Default Window

Packet Size

PVC の最大交渉可能パケット・サイズを指定します。この値は、**national set packet-size** コマンドで指定された最大パケット・サイズ以下でなければなりません。このパラメーターのデフォルト値は 128 バイトです。このパラメーターに構成できる最大値は 4096 バイトです。X.31 の最大値は 256 バイトです。この値は、この X.25 インターフェースの最大フレーム・サイズを計算するのに使用されます。

関連の構成パラメーターは、次のとおりです。

- Nat Set Packet Size Default
- Nat Set Packet Size Maximum

Change

change コマンドは、X.121 アドレス、DDN X.25 アドレス、プロトコル構成、または PVC 定義を変更するのに使用します。

X.25 ネットワーク・インターフェースの構成

注: X.121 アドレスに関連付けられている IP アドレスを変更する場合は、アドレス
相関が入っているレコードを削除した後で、アドレス・マッピングを再定義す
る必要があります。

構文:

```
change                address
                        htf-address
                        protocol
                        pvc
```

address

X.121 アドレス変換を変更します。表示されるプロンプトは、変更するプロト
コル・アドレスによって異なります。

例: **change address**

IP の例:

```
Protocol [IP] IP
IP Address [0.0.0.0]?
Enc Priority []?
X.25 Address [00000124040000]?
```

IPX の例:

```
Protocol [IP] IPX
CUD Field Usage (Standard or Proprietary) [Standard]?
IPX Host number (in hex) []?
Enc Priority []?
X.25 Address [00000124040000]?
```

htf address

Defense Data Network (DDN) X.25 アドレス変換を変更します。

例:

```
change htf-address
Protocol [IP]
Change HTF address [0.0.0.0]?
New HTF address [10.4.0.124]?
```

protocol

プロトコル構成定義を変更します。

例:

```
change protocol
Protocol [IP]
Window Size [2]
Default Packet Size [128]
Maximum Packet Size [256]
Circuit Idle Time [30]
Maximum VCs [6]
```

QLLC の例:

```
X.25 Config> change prot
Protocol [IP]? dls
Idle Timer [30]?
QLLC response timer (in decaseconds) [15]?
QLLC response count [255]?
Accept Reverse Charges [N]?
Request Reverse Charges [N]?
Station Type (1) PRI (2) SEC (3) PEER [3]?
Max Packet Size [256]?
```

X.25 ネットワーク・インターフェースの構成

Packet Window size [7]?
Max message size [2048]?
Call User Data (in HEX, 0 for Null) []? **C3010000525450**

pvc PVC、ウィンドウ・サイズ、およびパケット・サイズの定義を変更します。

注: プロトコル、パケット・チャネル、またはあて先 X.25 アドレスを変更する場合は、その定義が入っているレコードをいったん削除した後、変更されたパラメーターを使用して再び追加する必要があります。変更は、Packet Channel Range Start によって定義された範囲の回線にあるすべての PVC に適用されます。

例:

```
change pvc
Protocol [IP]? IP
Packet Channel Range Start [1]?
Destination X.25 Address [ ]?
Packet Channel Range End [1]
Window Size [2]?
Packet Size [128]?
```

Delete

delete コマンドは、X.121 アドレス、プロトコル構成定義、または PVC 定義を削除するのに使用します。

構文:

```
delete                address
                        bi-cugs
                        cugs
                        protocol . . .
                        pvc
```

address

X.121 アドレス変換を削除します。

例: delete address

IP の例:

```
Protocol [IP]?
IP Address [0.0.0.0]?
```

IPX の例:

```
Protocol [IP]? IPX
IPX Host Number (in hex) [2]?
```

bi-cugs

このインターフェースによって使用される相互形閉域ユーザー・グループ番号を削除します。

有効値:

Y 現行の CUG を削除します。

N 現行の CUG を削除しません。

ALL 残りの CUG をすべて削除します。

X.25 ネットワーク・インターフェースの構成

Q 残りの CUG の削除を中止します。

例:

```
delete bi-cugs
Delete Pref BI-CUG [Y]?
Delete BI-CUG (2) [Y]? N
Delete BI-CUG (3) [Y]? q
```

cugs このインターフェースによって使用される閉域ユーザー・グループ番号を削除します。このコマンドの機能は **delete bi-cug** コマンドに似ています。

例:

```
del cug
Delete Pref CUG [Y]?
Delete CUG (2) [Y]?
Delete CUG (3) [Y]? q
```

protocol *prot-type*

プロトコル・カプセル化構成定義を削除します。 *Prot-type* は、ルーターの構成に現在定義されているプロトコル・カプセル化の名前または番号です。

pvc PVC 定義を削除します。Packet Channel Range Start パラメーターによって定義された範囲の回線のすべての PVC が削除されます。

例:

```
delete pvc
Protocol [IP]?
Destination X.25 Address [ ]?
Packet Channel Range Start [ ]?
```

List

list コマンドは、指定されたパラメーターの現行構成を表示するのに使用します。

構文:

```
list address
all
cugs
detailed
protocols
pvc
summary
```

address

すべての X.121 アドレス変換をリストします。

例:

```
list address
IF#      Prot #      Active Enc      Protocol ->      X.25 address
1        0(IP)        CC              10.1.2.3 ->      1238765742
1        7(IPX)       SNAP           10              ->      12389
                CUGS: 11 12 13 14 15          BI-CUGS: 21 22
```

X.25 ネットワーク・インターフェースの構成

all すべての X.25 アドレス、ナショナル・パーソナリティ・パラメーター、すべての定義済みプロトコルとそれらの値、およびすべての定義済み PVC をリストします。

例:

list all

X.25 Configuration Summary

```
Node Address:      313131
Max Calls Out:     4
Inter-Frame Delay: 0      Encoding: NRZ
Speed:             64000   Clocking: Internal
MTU:               2048    Cable:      V.35 DCE
Lower DTR:         Disabled
Default Window:    2      SVC idle:   30 seconds
National Personality: GTE Telenet (DTE)
PVC                low: 1  high: 1
Inbound            low: 0  high: 0
Two-Way            low: 2  high: 64
Outbound           low: 0  high: 0
Throughput Class in bps Inbound: 2400
Throughput Class in bps Outbound: 2400
```

X.25 National Personality Configuration

```
Request Reverse Charges: on  Accept Reverse Charges: on
Frame Extended seq mode: off Packet Extended seq mode: off
Incoming Calls Barred: off  Outgoing Calls Barred: off
Throughput Negotiation: on  Flow Control Negotiation: on
Suppress Calling Addresses: off DDN Address Translation: off
Truncate Called Addresses: off
Number of digits to truncate called addresses to: 2
CUG Support: off          BI-CUG Support: off
CUG Outgoing Access: off  CUG Incoming Access : off
BI-CUG Outgoing Access: off CUG 0 Override: off
CUG Insertion: off       CUG deletion: off
Call Request Timer:      20 decaseconds
Clear Request Timer:     18 decaseconds (1 retries)
Reset Request Timer:     18 decaseconds (1 retries)
Restart Request Timer:   18 decaseconds (1 retries)
Min Recall Timer         10 seconds
Min Connect Timer        90 seconds
Collision Timer          5 seconds
T1 Timer: 4.00 seconds   N2 timeouts: 20
T2 Timer: 2.00 seconds   DP Timer: 500 milliseconds
Standard Version: 1984   Network Type: CCITT
Disconnect Procedure: passive
Window Size Frame: 7     Packet: 2
Packet Size Default: 128 Maximum: 256
```

X.25 protocol configuration

No protocols defined

X.25 PVC configuration

No PVCs defined

X.25 address translation configuration

No address translations defined

cugs この装置内の各 X.25 インターフェースの CUG および BI-CUG 番号をリストします。

例:

li cugs

CUGS: 23 24 25 26 27

X.25 ネットワーク・インターフェースの構成

detailed

national set コマンドで変更したすべてのデフォルト・パラメーターの値をリストします。画面表示の説明は、本章の後方で説明する **national set** コマンドの項に示してあります。

例:

list detail

X.25 National Personality Configuration

```
Follow CCITT: on      OSI 1984:   on      OSI 1988:   off
Request Reverse Charges: off  Accept Reverse Charges:  off
Frame Extended seq mode: off  Packet Extended seq mode: off
Incoming Calls Barred:  off   Outgoing Calls Barred:  off
Throughput Negotiation: on   Flow Control Negotiation: off
Suppress Calling Addresses: off DDN Address Translation: off
Truncate Called Addresses: off
Number of digits to truncate called address to: 2
CUG Support: off          BI-CUG Support: off
CUG Outgoing Access: off  CUG Incoming Access : off
BI-CUG Outgoing Access: off CUG 0 Override: off
CUG Isertion: off        CUG deletion: off
T21 (Call Request Timer): 20 decaseconds
T23 (Clear Request Timer): 18 decaseconds (1 retries)
T22 (Reset Request Timer): 18 decaseconds (1 retries)
T20 (Restart Request Timer): 18 decaseconds (1 retries)
Min Recall Timer: 10 seconds
Min Connect Timer: 90 seconds
Collision Timer: 8 seconds
T1 Timer: 4.00 seconds    N2 timeouts: 20
T2 Timer: 0.00 seconds    DP Timer: 500 milliseconds
Standard Version: 1984    Network Type: CCITT
Disconnect Procedure: active
Window Size   Frame: 7    Packet: 2
Packet Size   Default: 256    Maximum: 256
```

protocols

すべての定義済みプロトコル構成をリストします。パラメーターの説明は、394ページの『Add』を参照してください。

例:

list protocols

X.25 protocol configuration

Protocol Number	Window Size	Packet-Size Default	Packet-Size Maximum	Idle Time	Max VCs
0(IP)	2	128	256	30	4
CUGS: 11 12 13 14 15		BI-CUGS: 21 22			

QLLC Protocols

Protocol Number	Packet Window	Packet MaxSize	Idle Time	Response Timer	Response Count	Reverse Charges Accept	Reverse Charges Request	Max Message	Station Type
26(DLSW)	7	256	30	15	255	N	N	2048	PEER
CUD : [C3 01 00 00 52 54 50]									
CUGS: 11 12 13 14 15		BI-CUGS: 21 22							

pvc すべての定義済み PVC をリストします。

例:

list pvc

X.25 PVC configuration

Prtcl	X.25 Address	Active Enc	Window	Pkt_len	Pkt_chan
0	8383838383	CC	4	1024	3 - 3

summary

set および **enable** コマンドで設定されたすべての値をリストします。これらの値は X.25 構成を変更します。

例:

list summary

X.25 Configuration Summary

```

Node Address:      313131
Max Calls Out:    4
Inter-Frame Delay: 0      Encoding: NRZ
Speed:            64000    Clocking: Internal
MTU:              2048     Cable:      V.35 DCE
Lower DTR:        Disabled
Default Window:   2        SVC idle:   30 seconds
National Personality: GTE Telenet (DTE)
PVC               low: 1    high: 1
Inbound           low: 0    high: 0
Two-Way           low: 2    high: 64
Outbound          low: 0    high: 0
Throughput Class in bps Inbound: 2400
Throughput Class in bps Outbound: 2400

```

インターフェース監視プロセスへのアクセス

X.25 ネットワーク・インターフェースに関連する情報を監視するには、以下の手順を使用して、インターフェース監視プロセスにアクセスします。

1. OPCON プロンプトで **talk 5** と入力する。たとえば、次のように入力します。

```
* talk 5
+
```

GWCON プロンプト (+) がコンソールに表示される。最初に GWCON に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. GWCON プロンプトで **configuration** コマンドを入力して、ルーターに構成されているプロトコルとネットワークを表示する。たとえば、次のように入力します。

```
+ configuration
```

(**configuration** コマンドの出力例については、152ページの『Configuration』を参照してください。)

3. **network** コマンドと X.25 インターフェース番号を入力する。

```
+ network 2
X.25>
```

X.25 監視プロンプトが、コンソールに表示されます。次に、X.25 監視コマンドを入力すると、X.25 インターフェースに関する情報を表示することができます。

X.25 監視コマンド

この節では、X.25 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。X.25 監視コマンドを使用して、X.25 パケットを転送するインターフェースおよびネットワークのパラメーターと統計を表示することができます。監視コマンドは、物理レベル、フレーム・レベル、およびパケット・レベルの構成値を表示します。この3つのプロトコル・レベルのすべての値を同時に表示するオプションもあります。

X.25 監視コマンドは X.25> プロンプトで入力します。408ページの表56は、コマンドを示しています。

X.25 ネットワーク・インターフェースの構成

表 56. X.25 監視コマンドの要約

監視コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
List	個々の PVC または SVC 統計および一般情報をリストします。
Parameters	X.25 構成の任意のレベルの現行パラメーターを表示します。
Reset	このインターフェース上のすべてのピアについて dly-recall および min-recall タイマーをリセットするか、特定のあて先のタイマーを、X.25 あて先アドレスを入力することによりリセットします。これにより、コーリング・シーケンスを開始することができます。
Statistics	X.25 構成の任意のレベルの現行統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、現在アクティブの PVC および SVC を表示するのに使用します。

構文:

list pvc
svc

pvc 構成されたパーマネント・バーチャル・サーキットを表示します。

svc アクティブのスイッチド・バーチャル・サーキットを表示します。

例:

list svc

LCN/ State	Destination Address	Originate Call	Transmits Queued	Protocol Encapsulated	Totals Xmts Rcvts	Resets
13 D	898280077113	YES	0	IP	8943 261	1
20 D	898280077114	NO	0	IP	943 43	0
42 P	898280077116	YES	6	IP	0 0	0
23 C	898280077117	YES	0	IP	3054 110	0

D - Data Transfer P - Call Progressing
C - Call Clearing

Parameters

parameters コマンドは、X.25 構成の任意のレベルの現行パラメーターを表示するのに使用します。

構文:

parameters all
frame
packet
physical

all パケット、フレーム、および物理レベルのパラメーターを表示します。

frame フレーム・レベルのパラメーターを表示します。

例:

```
parameters frame
Frame Layer Parameters:
Maximum Frame Size = 262 Maximum Window Size = 7
Protocol Enabled = YES Equipment Type = DTE
T1 Retransmit Timer = 4 T2 Acknowledge Timer = 2
N2 Retry Counter = 20 Disconnect Procedure = PASSIVE
Disconnect Timer = 500 Network Type = GTE
Protocol Options: Inhibit Idle RRs No MOD 128 NO Enable SARM NO
```

packet

パケット・レベルのパラメータを表示します。

例:

```
parameters packet
Packet Layer Parameters:
Default Packet Size = 128 Maximum Packet Size = 256
Log 2 Packet size = 2 Acknowledge Delay = 0
Layer Enabled = YES Default Window Size = 2
Lowest SVC = 1 Highest SVC = 64
Lowest PVC = 0 Highest PVC = 0
T20 (Restart) = 18 R20 (Retry) = 1
T21 (Call) = 20
T22 (Reset) = 18 R22 (Retry) = 1
T23 (Clear) = 18 R23 (Retry) = 1
Network Type = GTE Equipment Type = DTE
```

physical

物理レベルのパラメータを表示します。

例:

```
parameters physical
Physical Layer Parameters:
Interface Type = V.35

Maximum Frame Size = 264 InterFrame Delay = 2
Configured Speed = 0 Clocking = External
Encoding = NRZ
Protocol Enabled = Yes
```

Reset

reset コマンドは、dly-recall または min-recall タイマーをリセットして、すべての X.25 あて先または特定の X.25 あて先についてコーリング試行をリスタートします。

構文:

```
reset                all-peer-recall-tmrs
                        peer-recall-tmr
```

all-peer-recall-tmrs

このインターフェース上のすべての X.25 あて先 (ピア) についてコーリング・シーケンスをリセットします。したがって、あて先が dly-recall の最中である場合は、これを使用して、タイマーをリセットし、シーケンスを開始することができます。

例: **reset all-peer**

このコマンドは、次のメッセージのいずれかを戻します。

- Reset delay recall timers completed.
- No recall timers running for this net.
- No peers located for this net.

X.25 ネットワーク・インターフェースの構成

peer-recall-tmr

このインターフェース上の特定の X.25 あて先 (ピア) についてコーディング・シーケンスをリセットします。リセットする X.25 あて先を入力します。

例 1: reset peer-recall-tmr

```
reset peer-recall-tmr
Enter X.25 address: 89828007713
```

このコマンドは、次のメッセージのいずれかを戻します。

- Reset delay recall timers completed.
- No recall timers running for this net.

例 2: reset peer-recall-tmr 89828007713

```
reset peer-recall-tmr 89828007713
```

このコマンドは、次のメッセージのいずれかを戻します。

- Reset delay recall timers completed.
- No recall timers running for this net.

Statistics

statistics コマンドは、X.25 構成の任意のレベルの現行統計を表示するのに使用します。

構文:

statistics

all

frame

packet

physical

all パケット、フレーム、および物理レベルの統計を表示します。

frame フレーム・レベルの統計を表示します。

例:

```
statistics frame
Frame Layer Counters:      Received      Transmitted
Information Frames         0              0
RR Command                 0              0
RR Response                0              0
RNR Command                0              0
RNR Response               0              0
REJ Command                0              0
REJ Response               0              0
SABM                       0              71
SABME                      0              0
UA                         0              0
DISC                       0              0
DM                         0              0
FRMR                       0              0
Total Bytes                0              0
Frame Layer Miscellaneous:
Queued Output Frames = 0 Protocol Layer State = Link Setup
Send Sequence N(S)    = 0 Receive Sequence N(R) = 0
```

packet

パケット・レベルの統計を表示します。

例:

X.25 ネットワーク・インターフェースの構成

```
statistics packet
Packet Counters:          Received          Transmitted
Call Request              0              0
Call Accepted             0              0
Clear Request             0              0
Clear Confirm             0              0
Interrupt Request         0              0
Interrupt Confirm         0              0
RR Packet                 0              0
RNR Packet                0              0

Reset Request             0              0
Reset Confirm             0              0
Restart Request           0              0
Restart Confirm           0              0
Diagnostic                0              0
Data Packet               0              0
Data Bytes                0              0
Buffers Queued            0              0
Invalid Packets Received = 0
Switched Circuits Opened = 0
```

physical

物理レベルの統計を表示します。

例:

```
statistics physical
X.25 Physical Layer Counters:
Rx Bytes          0  Tx Bytes          0

Adapter cable:    V.35 DTE

Nicknames:      RTS CTS DSR DTR DCD
PUB 41450:     CA CB CC CD CF
State:         ON ON ON ON ON

Line speed:      unknown
Last port reset: 12 minutes, 21 seconds ago

Input frame errors:
CRC error        0  alignment (byte length)  0
missed frame     0  too long (> 0 bytes)    0
aborted frame    0  DMA/FIFO overrun        0
Output frame counters:
DMA/FIFO underrun errors  0  Output aborts sent      0
```

X.25 ネットワーク・インターフェースおよび GWCON インターフェース・コマンド

X.25 インターフェースには独自の監視用コンソール・プロセスがありますが、GWCON 環境から **interface** コマンドを使用すれば、ルーターも導入済みネットワーク・インターフェースの統計を表示します。(interface コマンドについて詳しくは、第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド を参照してください。)

X.25 インターフェースに関して表示される統計

GWCON 環境から X.25 インターフェースに対して **interface** コマンドを入力すると、以下の統計が表示されます。

```
+interface 11
Nt Nt' Interface Slot-Port          Passed Self-Test Self-Test Maintenance
11 11 X25/0 Slot: 8 Port: 1          1      Failed   Failed         0

X.25 MAC/data-link on V.35/V.36 interface
Interface State: DCD CTS Packet Layer Frame Layer
                  ON ON   UP          UP
Packet Counters: Received Transmitted
Data Packet       0          353
Data Bytes        0          18888
Buffers Queued    0           0
Invalid Packets Received = 0
```

X.25 ネットワーク・インターフェースの構成

```
Switched Circuits Opened =      0

Frame Layer Counters:      Received      Transmitted
Information Frames        354              354

X.25 Physical Layer Counters:
Rx Bytes                  3316   Tx Bytes              22204

Adapter cable:            V.35 DTE

V.24 circuit: 105 106 107 108 109
Nicknames:   RTS CTS DSR DTR DCD
PUB 41450:   CA  CB  CC  CD  CF
State:       ON  ON  ON  ON  ON

Line speed:             64.000 Kbps
Last port reset:       1 hour, 20 minutes, 25 seconds ago

Input frame errors:
CRC error                0 alignment (byte length)      0
missed frame             0 too long (> 2057 bytes)      0
aborted frame           0 DMA/FIFO overrun            0
Output frame counters:
DMA/FIFO underrun errors 0 Output aborts sent          0
Interface buffer pool: Total = 57, Free = 56
```

下のリストは、インターフェース統計を説明しています。

Nt グローバル・インターフェース番号

Nt' 将来のダイヤル回線使用に予約

Interface

インターフェース名と番号 (同一タイプのインターフェース内の)

Slot インターフェースのスロット番号

Port インターフェースのポート番号

Self-Test Passed

成功した自己テストの回数

Self-Test Failed

失敗した自己テストの回数

Maintenance Failed

保守障害の数

Interface state

入力モデム制御信号、パケット・レイヤー (X.25 レイヤー 3)、およびフレーム・リレー (X.25 レイヤー 2) の現在の状態を表示します。

Packet Counters

送受信パケットに関する統計を表示します。

Data Packets

インターフェースがネットワーク上で送受信したデータ・パケット数を表示します。

Data Bytes

インターフェースがネットワーク上で送受信したデータ・バイト数を表示します。

Buffers Queued

ネットワーク上に転送するため現在待ち行列化されているバッファの数を

X.25 ネットワーク・インターフェースの構成

表示します。これらは、フレームまたはパケット・レイヤーの監視メッセージや転送パケットである場合もあります。

Invalid Packets Received

ネットワークから受信した無効な X.25 パケットの数を表示します。

Switched Circuits Open

現在オープンしている交換回線の数を表示します。

Frame Layer Counters

フレーム・レイヤー・カウンターから生成された統計を提供します。

Information Frames

インターフェースが送受信した X.25 情報フレームの数を表示します。

X.25 Physical Layer Counters

物理レイヤー・カウンターから生成された統計を提供します。

RX Bytes

物理レイヤーによって受信されたバイト数を表示します。

TX Bytes

物理レイヤーによって送信されたバイト数を表示します。

Line speed

送信クロック・レート

Last port reset

前回のポート・リセット以降の時間の長さ

Input frame errors:

CRC error

チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment

長さが 8 ビットの偶数倍でなかったために廃棄された受信パケットの数

Too short

長さが 2 バイト未満であったために廃棄された受信パケットの数

Too long

構成されたサイズより大きかったために廃棄されたパケットの数

Aborted frame

送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

DMA/FIFO overrun

シリアル・インターフェース・カードがシステム・パケット・バッファ・メモリーにデータを送信する速度が遅かったために、データをネットワークから受信できなかった回数

Missed frame

フレームが装置に到着したときに利用可能なバッファがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

X.25 ネットワーク・インターフェースの構成

L & F bits not set

シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファが完全なフレームを受け入れたことを示します。いずれかのビットがセットされていない場合、パケットは廃棄され、L & F bits not set カウンターが増分され、バッファは消去されて再利用できるようになります。

注: L & F bits not set カウンターはトラフィックによる影響は受けません。

Output frame counters:

DMA/FIFO underrun errors

シリアル・インターフェース・カードがシステム・パケット・バッファ・メモリーからデータを取り出す速度が遅かったために、データをネットワーク上に送信できなかった回数。

Output aborts sent

高位レベルのソフトウェアの要求によって打ち切られた伝送の数

第26章 XTP の使用

この章では、TCP/IP を介して X.25 トラフィックを伝送するための X.25 トランスポート・プロトコル (XTP) について説明します。本章には、以下の節が含まれています。

- 『X.25 トランスポート・プロトコル』
- 418ページの『DTE アドレス・ワイルドカード』
- 418ページの『XTP バックアップ・ピア機能』
- 419ページの『ローカル XTP』
- 420ページの『XTP と閉域ユーザー・グループ』
- 420ページの『XTP の構成』
- 420ページの『構成手順』

X.25 トランスポート・プロトコル

X.25 トランスポート・プロトコル (XTP) は、『プロトコル転送機能』のサービスを提供します。プロトコル転送機能は、インバウンドおよびアウトバウンド・プロトコル・パケット処理の中心拠点です。転送機能は、あるネットワーク・インターフェース上でパケットを受信し、それを別のインターフェースに送信します。

XTP は 複数のリモート・サイトに設置された X.25 装置に対応できるように設計されています。このような環境で、XTP は X.25 パケット交換ネットワークを使用せずに、1 つまたは複数の中央サーバーと通信できるようにします。

これを使用可能にするには、サーバー位置とリモート位置のルーターを使用してデータをカプセル化し、TCP/IP を介してクライアントとサーバー間で X.25 パケットを送達します。

416ページの図19 は、XTP の使用前と使用後のネットワーク構成を示しています。

XTP の使用

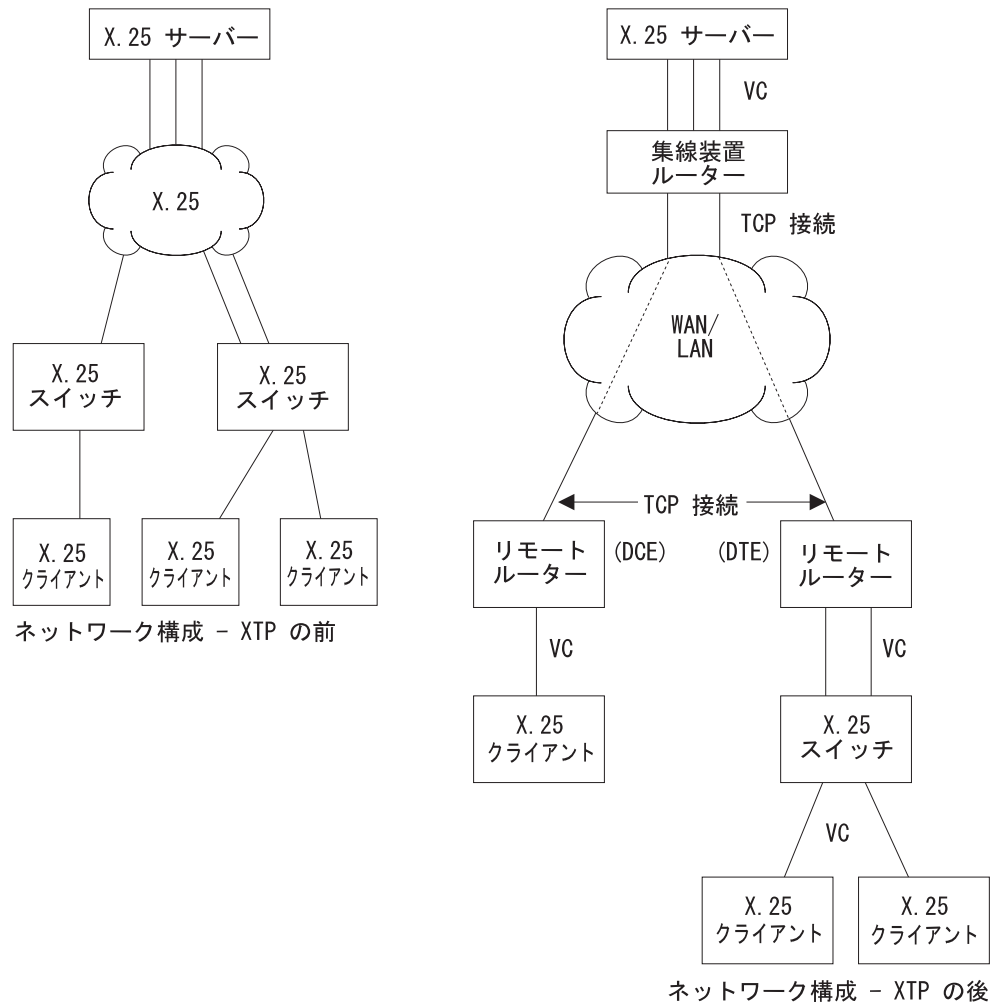


図 19. XTP の使用前と使用後の構成

構成情報

X.25 は、XTP 用に構成されたノード・アドレスに基づいて、XTP の着信コールを認知します。したがって、X.25 ノード間で X.25 トラフィックを伝達するためには、データ端末装置 (DTE) アドレスおよびノードが接続されているルーターの IP アドレスにマップするように X.25 を構成する必要があります。

たとえば、図19 では、リモート・ルーターと集線装置ルーター上に X.25 クライアントを構成しています。この例では、リモート・ルーター は、X.25 サーバーにアクセスするための TCP/IP ネットワークに X.25 クライアントを接続します。集線装置ルーター は、リモート・ルーターにアクセスするための TCP/IP ネットワークに X.25 サーバーを接続します。

注: XTP を構成する場合、ルーターは、X.25 スイッチに接続されている場合は DTE と見なされます。スイッチに接続されていない場合は DCE (データ回線終端装置) と見なされます。

ルーターを XTP 用に構成するには、XTP config> プロンプトから以下の情報を定義した後で、ルーターをリスタートします。

- ローカル DTE
- ピア・ルーター
- リモート DTE
- PVC
- CUG

ローカル DTE

ルーターの X.25 インターフェースに接続されている X.25 ノード。

ローカル DTE を構成するには、ローカル DTE に割り当てられている X.121 アドレスを使用します。1 つのインターフェースに複数のローカル DTE を構成することもできます。

ピア・ルーター

TCP/IP を介して通信する相手のルーター

ピア・ルーターは『観点』によって異なります。たとえば、416ページの図 19 では、集線装置側から見ると、2 つのリモート・ルーターがピア・ルーターになります。2 つのリモート・ルーター側から見ると、集線装置ルーターがピア・ルーターになります。

ピア・ルーターは、内部 IP アドレスによって指定します。

リモート DTE

ローカル X.25 ノードがコネクションをオープンし、データを交換するリモート X.25 ノード。リモート DTE に割り当てられている X.121 アドレスを使用します。

それぞれのピア・ルーターに固有の IP アドレスを構成します。たとえば、416ページの図19 では、集線装置ルーターは各リモート・ルーターの固有の IP アドレスを知っている必要があり、各リモート・ルーターは集線装置ルーターの固有の IP アドレスを知っていることが必要です。

PVC X.25 のリスタート後も接続されたままになるパーマネント・チャンネル。

PVC は固定されたチャンネルなので、専用電話回線に似ています。PVC は、XTP のコンテキストでは、ローカル X.25 DTE ノードからリモート X.25 DTE への PVC です。

ルーターを PVC 用に構成する場合は、ピア・ルーターの IP アドレスと、リモートおよびローカル DTE の PVC 番号をマップします。PVC は、次の 4 つの情報によって識別されます。

- ローカル PVC の論理チャンネル番号
- ローカル DTE の X.121 アドレス
- リモート (ピア) ルーターの PVC の論理チャンネル番号
- リモート DTE の X.121 アドレス

CUGS XTP プロトコルの閉域ユーザー・グループ。372ページの『閉域ユーザー・グループの概要』を参照してください。

追加の構成情報は、420ページの『XTP の構成』、および 429ページの『XTP 構成コマンド』に記載されています。

DTE アドレス・ワイルドカード

DTE アドレス構成には、『*』ワイルドカードを使用することができます。この他に『?』文字も使用できます。これを DTE アドレスの中で指定すると、アドレスのその位置は任意の 1 桁の数字であることを表します。たとえば、『1?2?3』という指定は、アドレス 18243 (2 番目、3 番目、および 5 番目の数字がそれぞれ 1、2、および 3) に一致します。

『*』ワイルドカード文字は、ゼロ桁またはそれ以上の桁数の任意の文字列を表すことができます。これを使用できる位置は、DTE アドレスの指定の末尾だけに限定されます。たとえば、『123*』、『5555*』、『9*』、または『*』というように使用します。DTE アドレスの特殊な例である『*』は、任意の DTE アドレス (ヌル・アドレスも含む) を表します。ヌル・アドレスは、X.25 コール・リクエスト・パケットに発信元アドレスが入っていない着信コールを処理するのに便利です。

『*』ワイルドカードを使用すると、既存のアドレスと競合するローカルまたはリモート DTE アドレスが加わる確率が高くなります。 **add local-dte** および **add remote-dte** コマンドは、ユーザーが既存のアドレスと競合する DTE アドレスを追加しようとする、競合アドレスを表示するように機能強化されています。

例: xtp config> **add local-dte**

```
Interface number [0]? 1
DTE address [ ] 123456
DTE address [ ]?
```

```
XTP config>add local-dte
Interface number [0]?1
DTE address [ ]?1*
DTE address conflicts with existing DTE address 123456
```

XTP バックアップ・ピア機能

バックアップ・ピア機能は、複数のピア・ルーターとリモート DTE とのアソシエーションを可能にします。ユーザーは、リモート DTE に対応するピア・ルーターのリストを指定します。

例:

```
XTP config>add rem
DTE address [ ]?123456
Peer router's internal IP Address [0.0.0.0]?10.0.0.2
Peer router's internal IP Address [0.0.0.0]?10.0.0.4
Peer router's internal IP Address [0.0.0.0]?11.0.0.1
Peer router's internal IP Address [0.0.0.0]?
```

リモート DTE への着信コールを受信すると、リスト内の各ルーターを経由するリモート DTE への接続が、リストに表示されている順序で試行されます。

リモート DTE の検索

DTE がリモート DTE へのコールを開始すると、両方の DTE アドレスを検査して、X.25 トランスポートのために受け入れ可能かどうかを調べます。受け入れ可能の場合、X.25 トランスポート・プロトコル転送機能は、どのピア・ルーターを介してコールを接続するかを決めます。リモート DTE のピア・ルーター・リストの最初のルー

ターから検索を開始します。満たしている必要がある第 1 条件は、ピア・ルーターへのアクティブの TCP 接続が存在することです。ピア・ルーターへのアクティブ TCP 接続がない場合は、リストの中の次のルーターを検査します。アクティブの TCP 接続が見つかり、コールされます。コール接続プロセスの時間を計るために、接続要求タイマーがスタートします。

リモート DTE の検索は、次のイベントの 1 つによって終了します。

- コールがピア・ルーターを介して正常に接続された。
この場合は、コール設定処理は完了し、リモート DTE の検索は終了します。
- コールがピア・ルーターによってリジェクトされた。
この場合は、リモート DTE の検索がピア・ルーター・リスト内の次のルーターに進みます。
- 接続要求タイマーが満了した。
この場合は、リモート DTE の検索がピア・ルーター・リスト内の次のルーターに進みます。

どのピア・ルーターを介した接続も成功しないうちにピア・ルーター・リストの終わりに達してしまった場合、ローカル DTE へのコールは解除されます。

接続要求タイマー

接続要求タイマーは、コール設定手順が不特定時間ハングしていることがないようにするために使用されます。各ピア・ルーターごとにタイマーを構成します。

例:

```
XTP config>add peer-router
Router's internal IP Address [0.0.0.0]?10.0.0.2
Connection setup timeout [230]?60
```

接続要求タイマーは 10 ~ 480 秒に構成できます。デフォルト値は 230 秒です。このデフォルト値は、X.25 コール・リクエスト・タイマーのデフォルト設定値が 200 秒であることに基づいています。

タイマーは、ピア・ルーターを介してコールした時点でスタートします。コールの試みがピア・ルーターによって受け入れられるか、リジェクトされた時点でストップします。

ローカル XTP

ローカル XTP は、着信 X.25 トラフィックを現行ルーター上の同一の、または異なるインターフェースに転送することができます。ローカル XTP を構成するには、**add peer** コマンドで、ルーターの内部 IP アドレスをピア・アドレスとして指定します。

XTP と閉域ユーザー・グループ

XTPは、**add local** または **add cug** コマンドによって定義されたローカル DTE アドレスを使用する閉域ユーザー・グループをサポートします。XTP が閉域ユーザー・グループを使用できるようにするには、以下のことが必要です。

- 該当する X.25 インターフェース上の CUG または BI-CUG を使用可能にする。
- **add cug** および **add bi-cug** コマンドを使用して、XTP プロトコル特定 CUG を提供する (必要な場合)。
- **add local** コマンドで、該当する閉域ユーザー・グループ番号を提供する。これには、以下のものが含まれます。
 - 閉域ユーザー・グループ番号
 - 優先閉域ユーザー・グループ番号
 - 相互形閉域ユーザー・グループ番号
 - 優先相互形閉域ユーザー・グループ番号
- **national enable cug_insertion** または **national enable cug_deletion** コマンドで、インターフェースの CUG の挿入または削除を使用可能にする (必要な場合)。
- **national enable cug 0 override** コマンドで、CUG 0 オーバーライド・オプションを使用可能にする (必要な場合)。

XTP の構成

XTP は、TCP/IP を介して X.25 トラフィックをトランスポートするのに使用されるプロトコル転送機能です。XTP を使用すると、既存の X.25 装置が TCP/IP バックボーンを介して通信し、X.25 ネットワークからユーザーが選択したネットワークに移行することが可能になります。

構成手順

この節では、421ページの図20 に表示されているネットワークを構成するための詳細を定義します。

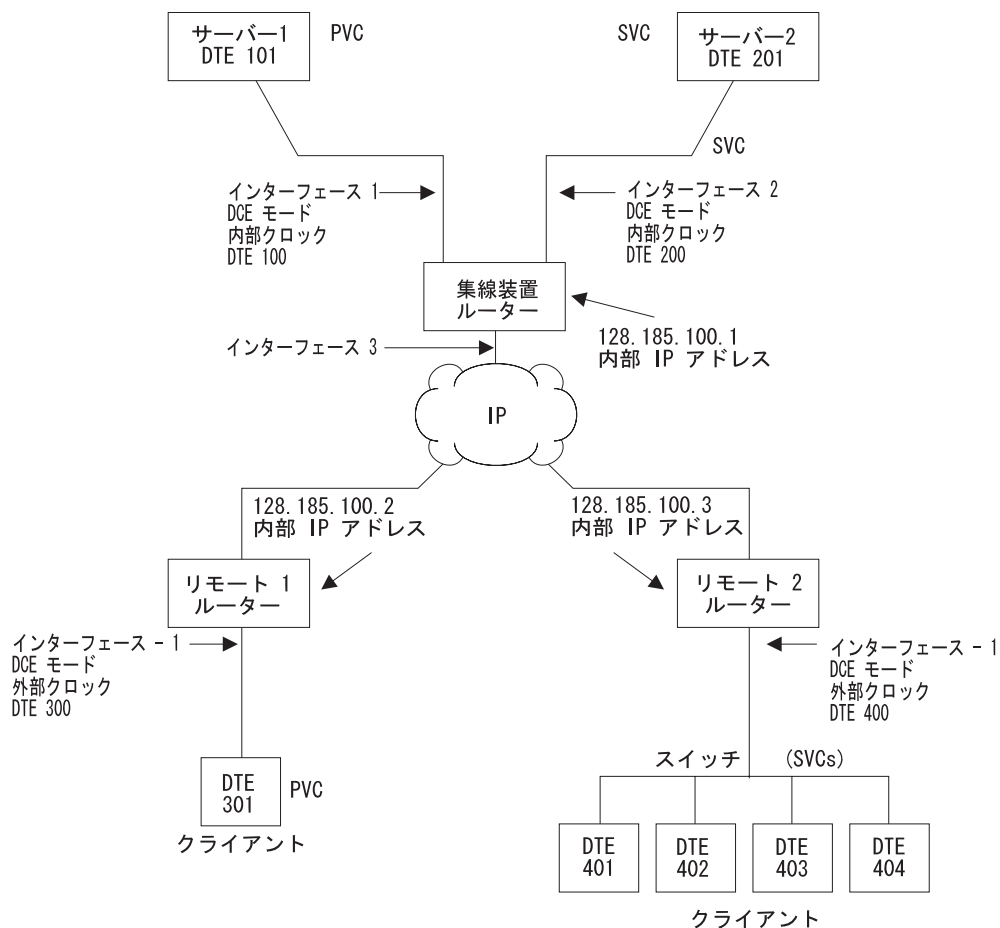


図 20. サンプル XTP 構成

この構成は、3 つのルーター（集線装置ルーター、リモート 1 ルーター、およびリモート 2 ルーター）を示しています。このネットワーク上で XTP を運用できるようにするためには、それぞれのルーターに対して以下のステップを実行します。

- データ・リンクを設定する
- IP インターフェースを構成する
- X.25 を構成する
- ナショナル・パーソナリティ値を設定する
- IP アドレスを定義する
- 内部 IP アドレスを設定する
- XTP を構成する

注: 新規の構成は、ルーターをリスタートするまでは有効になりません。

データ・リンクの設定

データ・リンクは、ネットワーク上でデータ・パケットを送信するのに使用するプロトコルを定義します。構成するルーターと各シリアル・インターフェースの間のデータ・リンクを定義します。図 20 の例は、3 つのシリアル・インターフェース (X.25 用に 2 つと、PPP 用に 1 つ) を持つ集線装置ルーターを構成します。

XTP の使用

シリアル・インターフェースのデータ・リンク・プロトコルを設定します。

```
Config>set data-link X25 1
Config>set data-link x25 2
Config>set data-link ppp 3
```

IP インターフェースの構成

421ページの図20 では、IP インターフェースは PPP です。この PPP インターフェースを構成するには Config> プロンプトで **network 3** と入力します。

```
Config>network 3
PPP interface configuration
```

注: この手順では PPP の構成については詳しく説明しません。詳細については、ソフトウェア使用者の手引き を参照してください。

X.25 の構成

XTP を構成する前に、各インターフェースの X.25 パラメーターを構成します。次の例は、X.25 の基本パラメーターを構成しており、421ページの図20 のトポロジーに基づいています。

構成する必要があるパラメーターは、ネットワーク・トポロジーによって異なります。すべての X.25 パラメーターの詳細については、ソフトウェア使用者の手引き を参照してください。

インターフェース 1

421ページの図20 に定義されている集線装置ルーター上の インターフェース 1 は、以下の手順で構成します。

1. Config> プロンプトで **network** と入力し、続いて X.25 インターフェースの番号を入力する。この例では、インターフェース 1 になります。

```
Config>network 1
X.25 User Configuration
X.25 Config>
```

2. XTP プロトコルを X.25 インターフェースに追加し、汎用のインターフェース値を定義する。X.25 Config> プロンプトで **add protocol xtp** と入力します。このコマンドは 1 回だけ 入力します。

```
X.25 Config>add protocol xtp
Window Size [2]?
Default Packet Size [128]?
Maximum Packet Size [256]?
```

3. **set address** X.25 node address と入力して、ネットワーク・アドレスを指定する。421ページの図20 では、ノード・アドレス (DTE アドレス) は 100 です。

```
X.25 Config>set address 100
```

4. **set clocking** と入力し、その後、ルーター・タイプに応じて **internal** または **external** と入力する。

```
X.25 Config>set clocking internal
```

5. **set speed** と入力し、続いてアクセス速度 (ライン速度) を入力する。

```
X.25 Config>set speed
Access rate in bps [9600]?19200
```


6. **set equipment-type** と入力し、フレームおよびパケット・レベルが DCE または DTE のいずれとして動作するのかを指定する。

```
X.25 Config>set equipment-type dce
```

7. **set pvc** と入力し、使用する最低および最高の PVC を定義する。

```
X.25 Config>set pvc low 1
X.25 Config>set pvc high 1
```

8. **add pvc** と入力し、個々の PVC を定義する。

```
X.25 Config>add pvc
Protocol [IP]?xtp
Packet Channel [1]?
Destination X.25 Address [ ]?101
Window Size [2]?
Packet Size [128]
```

9. (オプション) **national enable truncate-called-addresses** と入力する。被呼アドレス・サイズを切り捨てたい場合は、**national set truncate-called-addr-size** と入力し、続けてコールされる DTE アドレスの切り捨て後の桁数を入力します。
10. (オプション) 必要に応じて、CUG サポート、CUG 挿入、および CUG 削除を使用可能にする。

インターフェース 2

インターフェース 2 は、以下の手順で構成します。

1. Config> プロンプトで **network** と入力し、続いて X.25 インターフェースの番号を入力する。421ページの図20 では、これは 2 になります。

```
Config>network 2
X.25 User Configuration
X.25 Config>
```

2. 422ページの『インターフェース 1』で定義したのと同じ手順を使用して、インターフェース 2 に対して以下のパラメーターを設定する。

- アドレス = 200
- クロック = 内部
- 速度 = 19200
- 装置 = dce

3. **set svc** と入力し、使用する最低および最高の SVC を定義する。

SVC には、両方向、インバウンド、およびアウトバウンドの 3 つのタイプがあります。デフォルト値は『svc low-two-way = 1』および『svc high-two-way = 64』です。その他の SVC タイプはすべて、デフォルト値は 0 になります。SVC および PVC についての詳細は、ソフトウェア使用者の手引き を参照してください。

```
X.25 Config>set svc ?
X.25 Config>set svc low-inbound 0
X.25 Config>set svc high-inbound 0
X.25 Config>set svc low-outbound 0
X.25 Config>set svc high-outbound 0
X.25 Config>set svc low-two-way 2
X.25 Config>set svc high-two-way 2
```

4. X.25 Config> プロンプトを終了する。

```
X.25 Config>exit
Config>
```

XTP の使用

ナショナル・パーソナリティーの設定

各 X.25 公衆ネットワークには、それぞれ独自の標準構成があります。ナショナル・パーソナリティーというのは、公衆データ通信網の特性を定義する 28 の変数のグループです。これらの変数は、リンクを介して転送されるパケットの制御情報をルーターに提供し、XTP ルーターとそのローカル DTE 間で使用される X.25 ファシリティーに影響を及ぼします。

着信コール・リクエストに入っているファシリティーは、ローカル・ルーターがそのファシリティーをサポートするように構成されているかどうかに関係なく、すべてピア・ルーターに渡されます。たとえば、パケット・サイズ・ネゴシエーションが着信コールで要求されており、フロー制御ネゴシエーションがルーターに構成されていないといった場合です。

ルーターは、交渉されたパケット・サイズおよびウィンドウ・サイズが、必ず X.25 インターフェースの定義時に指定された範囲内になるようにします。たとえば、`packet-ext-seq-mode` が X.25 インターフェースに定義されていない場合、7 より大きいパケット・ウィンドウは、交渉によって 7 まで下げられます。

構成値を見たい場合は X.25 Config> プロンプトで **list detailed** と入力します。ナショナル・パーソナリティーのデフォルト値を設定するには、X.25 Config> プロンプトで **set national-personality** と入力します。詳細については、ソフトウェア使用者の手引きを参照してください。

IP アドレスの定義

集線装置ルーター (421ページの図20 に表示) を XTP 用に構成する前に、このルーターの IP アドレスを定義します。Config> プロンプトで **protocol ip** と入力し、IP config> プロンプトで **add address** と入力します。

```
Config>protocol ip
IP config>add address
Which net is this address for [0]?3
New address [0.0.0.0]?128.185.100.7
Address mask [255.255.0.0]?255.255.255.0
```

内部 IP アドレスの設定

ルーターはそのピア・ルーターを、ピア・ルーターの内部 IP アドレスによって識別します。

ピア・ルーターの内部 IP アドレスを設定するには、IP Config> プロンプトで **set internal IP address** と入力します。

```
IP config>set internal-ip-address
Internal IP address [0.0.0.0]?128.185.100.1
```

XTP の構成

X.25 を構成し、IP アドレスを定義したら、ルーターの XTP を構成する準備が整ったこととなります。

XTP を構成する際に、詳しい構成情報が必要になった場合は、429ページの『XTP 構成コマンド』を参照してください。

注: ユーザーのネットワークを XTP 用に構成する場合、ピア・ルーターは常にユーザーが TCP/IP を介して通信する相手のルーターであることを念頭においてください。すなわち、ピア・ルーターは観点によって異なります。421ページの図20でリモート 1 ルーターおよびリモート 2 ルーターとして定義されたルーターを構成する場合、これらにとってのピア・ルーターは、集線装置ルーターになります。

ルーターの XTP を構成するには、以下のステップを実行します。

1. XTP config> プロンプトにアクセスするために、Config> で **protocol xtp** と入力する。
2. インターフェース 1 を XTP 構成に追加する。XTP Config> プロンプトで **add local-dte** と入力します。

```
XTP config>add local-dte
Interface number [0]?1
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?101
Pref CUG [ ]? 18
CUG (2) [ ]? 2
CUG (3) [ ]?
Pref BI-CUG [0]?
DTE address [ ]?
```

ヌル DTE アドレスを入力すると、コマンドの入力を終了します。

3. インターフェース 2 を XTP 構成に追加する。XTP Config> プロンプトで **add local-dte** と入力します。

```
XTP config>add local-dte
Interface number [0]?2
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?201
DTE address [ ]?
```

ヌル DTE アドレスを入力すると、コマンドの入力を終了します。

4. (オプション) XTP プロトコル特定 CUG を追加する。

```
add cug
Pref CUG [ ]? 11
CUG (2) [ ]? 12
CUG (3) [ ]? 13
CUG (4) [ ]? 14
CUG (5) [ ]? 15
add bi-cug
Pref BI-CUG [ ]? 21
BI-CUG (2) [ ]? 22
BI-CUG (3) [ ]?
```

5. リモート 1 ルーターをピア・ルーターとして追加する。**add peer-router** と入力し、このルーターの IP アドレスを入力します。

```
XTP config>add peer-router
Router's internal IP Address [0.0.0.0]?128.185.100.2
Connection setup timeout [230]?
```

6. リモート 1 ルーターのリモート DTE を入力する。**add remote-dte** と入力し、この DTE の IP アドレスおよび DTE アドレスを入力します。

```
XTP config>add remote-dte
DTE address [ ]?301
Peer router's internal IP Address [0.0.0.0]?128.185.100.2
Peer router's internal IP Address [0.0.0.0]?
```

注: リモート DTE が必須なのは、以下のいずれかに該当する場合だけです。

- 集線装置ルーターが、そのローカル DTE からの着信コールのために、リモート DTE への XTP 接続を開始する場合

XTP の使用

- DTE が XTP PVC 定義に含まれている場合
7. リモート 2 ルーターを (ピア・ルーターとして) 追加する。 **add peer-router** と入力し、このルーターの IP アドレスを入力します。

```
XTP config>add peer-router
Router's internal IP Address [0.0.0.0]?128.185.100.3
Connection setup timeout [230]?
```

8. リモート 2 ルーターのリモート DTE を追加する。 **add remote-dte** と入力し、この DTE の IP アドレスと DTE アドレスを入力します。

```
XTP config>add remote-dte
DTE address [ ]?401
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?
```

```
XTP config>add remote-dte
DTE address [ ]?402
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?
```

```
XTP config>add remote-dte
DTE address [ ]?403
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?
```

```
XTP config>add remote-dte
DTE address [ ]?404
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?
```

9. XTP PVC を追加して、サーバー 1 へのローカル PVC とリモート DTE 301 とを論理的に関連付ける。

```
XTP config>add pvc
Local PVC Range Start [1]?
Local PVC Range End [1]?
Local X.25 DTE address [ ]? 101
Remote PVC Range Start [1]?
Remote PVC Range End [1]?
Remote X.25 DTE address [ ]?301
```

DTE アドレスを入力するときには、次のいずれかを指定できます。

'?' を任意の数字の代わりに指定します。 '?' は、この桁位置は任意の 1 つの数字であることを意味します。

'*' をアドレスの最後の桁として指定し、ゼロ桁またはそれ以上の桁数の任意の組み合わせを表します。

リモート・ルーターのサンプル構成

以下に示すのは、リモート 1 ルーターおよびリモート 2 ルーターのサンプル構成です (421ページの図20 を参照)。このプロセスは、420ページの『構成手順』の節で定義されているものと同じです。

リモート 1 ルーター

*talk 6

```
Config>set data-link x25 1
Config>set data-link ppp 2
Config>network 1
```

```
X.25 Config>set address 300
X.25 Config>set clocking internal
X.25 Config>set speed 19200
X.25 Config>set equipment-type dce
X.25 Config>set pvc low 1
X.25 Config>set pvc high 1
X.25 Config>add pvc
Protocol [IP]?xtp
```

```

Packet Channel [1]?1
Destination X.25 Address [ ]?301

Window Size [2]?
Packet Size [128]?
X.25 Config>exit
Config>

Config>protocol ip
IP config>add address
Which net is this address for [0]?2
New address [0.0.0.0]?128.185.100.8
Address mask [255.255.0.0]?255.255.255.0

IP config>set internal-ip-address
Internal IP address [0.0.0.0]?128.185.100.2
IP Config>exit
Config>

Config>protocol xtp
XTP config>add local-dte
Interface number [0]?1
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?301
DTE address [ ]?

XTP config>add peer-router
Router's IP address?128.185.100.1

XTP config>add remote-dte
DTE address [ ]?101
Peer router's internal IP Address [0.0.0.0]?128.185.100.1
Peer router's internal IP Address [0.0.0.0]?

XTP config>add pvc
Local PVC Range Start [1]?
Local PVC Range End [1]?
Local X.25 DTE address [ ]? 101
Remote PVC Range Start [1]?
Remote PVC Range End [1]?
Remote X.25 DTE address [ ]? 301

```

リモート 2 ルーター

```

*talk 6

Config>set data-link x25 1
Config>set data-link ppp 2
Config>network 1

X.25 Config>set address 400
X.25 Config>set clocking external
X.25 Config>set speed 19200
X.25 Config>set equipment-type dte
X.25 Config>set svc low-inbound 0
X.25 Config>set svc high-inbound 0
X.25 Config>set svc low-outbound 0
X.25 Config>set svc high-outbound 0
X.25 Config>set svc low-two-way 1
X.25 Config>set svc high-two-way 64
X.25 Config>add protocol
Protocol [IP]?xtp
Window Size [2]?
Default Packet Size [128]?
Maximum Packet Size [256]?
X.25 Config>exit

Config>protocol ip
IP config>add address
Which net is this address for [0]?2
New address [0.0.0.0]?128.185.100.9
Address mask [255.255.0.0]?255.255.255.0

IP config>set internal-ip-address
Internal IP address [0.0.0.0]?128.185.100.3
IP Config>exit
Config>

Config>protocol xtp

```

XTP の使用

```
XTP config>add local-dte
Interface number [0]?1
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?401
Pref CUG [ ]? 23
CUG (2) [ ]? 24
CUG (3) [ ]? 25
CUG (4) [ ]? 26
CUG (5) [ ]? 27

DTE address [ ]?402
Pref CUG [ ]?
DTE address [ ]?403
Pref CUG [ ]?
DTE address [ ]?404
Pref CUG [ ]?
DTE address [ ]?

XTP Config>add peer-router
Router's IP address?128.185.100.1

XTP config>add remote-dte
DTE address [ ]?201
Peer router's internal IP Address [0.0.0.0]?128.185.100.1
Peer router's internal IP Address [0.0.0.0]?
XTP config>exit

Config>
```

第27章 XTP の構成および監視

この章では、XTP 構成コマンドおよび監視コマンドについて説明します。本章には、以下の節が含まれています。

- 『XTP 構成コマンド』
- 436ページの『XTP 監視コマンド』

XTP 構成コマンド

この節では、XTP 構成コマンドについて説明します。

XTP 構成環境にアクセスするには、Config> プロンプトで **protocol xtp** コマンドを入力します。

```
Config> p xtp
XTP config>
```

XTP 構成コマンドは XTP config> プロンプトで入力します。

表 57. XTP 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Add	インターフェース、ピア・ルーター、閉域ユーザー・グループ、リモート DTE、または PVC 定義を追加します。
Change	ピア・ルーター、リモート DTE または PVC 定義を変更します。
Delete	ローカル DTE、ピア・ルーター、閉域ユーザー・グループ、リモート DTE、または PVC 定義を削除します。
Enable-XTP	XTP 転送機能を起動します。
Disable-XTP	XTP 転送機能を停止します。
Set	XTP キープアライブ・タイマーの値を設定します。
List	インターフェース、ピア・ルーター、リモート DTE および PVC 定義をリストします。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Add

ローカル X.25 ノード、ピア・ルーター、リモート X.25 ノード (対応するルーターと共に)、またはローカル X.25 ノードからリモート X.25 ノードへの PVC を追加します。

XTP 転送機能には、ワイルドカード・アドレス指定が組み込まれています。ローカルまたはリモート DTE アドレスを入力するときには、ワイルドカード文字 (? または *) を含めることができます。ワイルドカードの使用についての詳細は、418ページの『DTE アドレス・ワイルドカード』を参照してください。

構文:

```
add                               bi-cug
```

XTP 構成コマンド (Talk 6)

cug
_local-dte
peer-router
_remote-dte
pvc

cug XTP プロトコルの閉域ユーザー・グループ番号を指定します。入力を求められる最初の CUG は、優先 cug です。

有効値: 0 ~ 9999

デフォルト値: なし

例:

```
add cug
Pref CUG [ ]? 114
CUG (2) [ ]? 314
CUG (3) [ ]? 478
CUG (4) [ ]?
```

bi-cug XTP プロトコルの相互形閉域ユーザー・グループ番号を指定します。入力を求められる最初の bi-cug は、優先 bi-cug です。

有効値: 0 ~ 9999

デフォルト値: なし

例:

```
add bi-cug
Pref BI-CUG [ ]? 50
BI-CUG (2) [ ]? 51
BI-CUG (3) [ ]? 52
BI-CUG (4) [ ]? 53
BI-CUG (5) [ ]? 54
```

local-dte

指定されたインターフェース上のルーターと通信する X.25 DTE アドレス、または X.25 ノードを追加します。XTP とともに使用する有効なインターフェース番号は 0 ~ 255 です。

複数のローカル・ノードを構成することも可能です。ただし、コーリング DTE アドレスがない着信コールを認めるオプションを選択しており、そのようなコールを受信した場合、追加された最後の ローカル DTE アドレスが、そのコールのコーリング DTE アドレスになります。

例:

```
add local-dte

Interface number [0]?4
Allow inbound calls without calling DTE address? (Y or N) [N]? y
DTE address [ ]?101
Pref CUG [ ]? 23
CUG (2) [ ]? 24
CUG (3) [ ]? 25
CUG (4) [ ]? 26
CUG (5) [ ]? 27
Pref BI-CUG [ ]? 6
BI-CUG (2) [ ]? 7
BI-CUG (3) [ ]? 8
BI-CUG (4) [ ]? 9
BI-CUG (5) [ ]? 10
DTE address [ ]?
```


peer-router

ピア・ルーターを追加します。リモート X.25 ノードが接続するルーターの内部 IP アドレスを入力します。これらの IP アドレスを使用して TCP 接続をオープンし、接続要求と X.25 データが入っている X.25 パケットを伝達することができます。

ピア・ルーターに構成されている内部 IP アドレスが、このルーターの内部 IP アドレスである場合、ソフトウェアはローカル XTP 接続を確立します。

例:

```
add peer-router
```

```
Router's internal IP Address [0.0.0.0]?128.185.100.2
Connection setup timeout [230]?
```

remote-dte

リモート X.25 ノードと、対応するルーターを追加します。リモート・ノードとローカル X.25 ノードを接続し、データを交換できるようにします。構成する各リモート X.25 ノードごとに IP アドレスを構成する必要があります。このリモート・ノードに送信された要求またはデータは、すべてルーターに送られます。ルーターはそのローカル X.25 インターフェースの 1 つを使用して、データを X.25 ノードに転送します。

リモート DTE を定義するのは、このルーターがローカル DTE からの着信コールのためにリモートへの XTP 接続を開始する必要がある場合、またはリモート DTE が XTP PVC 定義に含まれている場合です。

ローカル XTP を使用するためには、ピア・ルーター・アドレスがローカル・ルーターの内部アドレスであること、および DTE アドレスが以前に **add local** コマンドを使用して定義されていることが必要です。

例:

```
add remote-dte
```

```
DTE address [ ]?301
Peer router's internal IP Address [0.0.0.0]?128.185.100.2
Peer router's internal IP Address [0.0.0.0]?
```

pvc

ローカル X.25 ノードからリモート X.25 ノードへの PVC を追加します。

PVC 構成を起動するためには、次の 3 つが存在している必要があります。

- ルーターからローカル X.25 ノードへの X.25 PVC
- ピア・ルーターからリモート X.25 ノードへの X.25 PVC
- リモート・ノードが常駐しているピア・ルーターへの TCP 接続

例:

```
XTP config>add pvc
Local PVC Range Start [1]?
Local PVC Range End [1]?
Local X.25 DTE address [ ]? 101
Remote PVC Range Start [1]?
Remote PVC Range End [1]?
Remote X.25 DTE address [ ]? 301
```

注:

1. ルーター構成に PVC を追加する場合は、X.25 にも PVC を構成する必要があります。X.25 インターフェースの構成についての詳細は、ソフトウェア使用者の手引き を参照してください。

XTP 構成コマンド (Talk 6)

- ローカル XTP の場合、両方向に PVC を定義する必要があります。ルーターはローカル機能とリモート機能の両方を実行するので、この定義が必要です。たとえば、ローカル XTP を使用している場合、ローカル PVC 8 とリモート PVC 10 を定義するには、次のように指定します。

```
XTP config>add pvc
Local PVC Range Start [1]? 8
Local PVC Range End [1]? 8
Local X.25 DTE address [ ]? 108
Remote PVC Range Start [1]? 10
Remote PVC Range End [1]? 10
Remote X.25 DTE address [ ]? 301

XTP config>add pvc
Local PVC Range Start [1]? 10
Local PVC Range End [1]? 10
Local X.25 DTE address [ ]? 310
Remote PVC Range Start [1]? 8
Remote PVC Range End [1]? 8
Remote X.25 DTE address [ ]? 108
```

- PVC 範囲は、PVC 範囲開始パラメーターと PVC 範囲終了パラメーターによって定義することができます。ローカル PVC 範囲では、リモート PVC 範囲と同じ数の回線を定義する必要があります。たとえば、ローカル PVC 範囲で 1 つの回線を定義したら、リモート PVC 範囲でも回線を 1 つ定義する必要があります。
- 定義される PVC は、1 ~ 255 の範囲になる必要があります。

注: ルーター構成に PVC を追加する場合は、X.25 にも PVC を構成する必要があります。X.25 インターフェースの構成についての詳細は、ソフトウェア使用者の手引きを参照してください。

Change

XTP 構成からピア・ルーター、リモート DTE、または PVC を変更します。

構文:

```
change peer-router
remote-dte
pvc
```

peer-router

XTP 構成から特定のピア・ルーターを変更します。

例:

```
change peer-router
Router IP Address [0.0.0.0]?128.185.100.2
```

remote-dte

XTP 構成から特定のリモート DTE を変更します。

例:

```
change remote-dte
DTE address [ ]?401
Peer router's internal IP Address [0.0.0.0]?128.185.100.2
Peer router's internal IP Address [0.0.0.0]?
```

pvc Local PVC Range Start パラメーターによって定義される範囲内のすべての PVC について PVC の定義を変更します。

例:

```
change pvc
Local PVC Range Start [1]?1
Local DTE address [ ]?301
```

Delete

XTP 構成からローカル DTE、ピア・ルーター、リモート DTE、または PVC を削除します。

構文:

```
delete                bi-cug
                        cug
                        local-dte
                        peer-router
                        remote-dte
                        pvc
```

bi-cug このインターフェースによって使用される相互形閉域ユーザー・グループ番号を削除します。

有効値:

Y 現在の CUG を削除します。
N 現在の CUG を削除しません。
ALL 残りの CUG をすべて削除します。
Q 残りの CUG の削除を中止します。

例:

```
delete bi-cug
Delete Pref BI-CUG [Y]?
Delete BI-CUG (2) [Y]? N
Delete BI-CUG (3) [Y]? q
```

cug このインターフェースによって使用される閉域ユーザー・グループ番号を削除します。このコマンドの機能は **delete bi-cug** コマンドと同様です。

例:

```
del cug

Delete Pref CUG [Y]?
Delete CUG (2) [Y]?
Delete CUG (3) [Y]? q
```

local-dte

XTP 構成から特定のピア・インターフェースを削除します。

例:

```
delete local-dte

Interface number [0]?1
DTE address [ ]?101
Record deleted
```

peer-router

XTP 構成から特定のピア・ルーターを削除します。

例:

XTP 構成コマンド (Talk 6)

delete peer-router

Router IP Address [0.0.0.0]?**128.185.100.2**
Record deleted

remote-dte

XTP 構成から特定のリモート DTE を削除します。

例: **delete remote-dte**

DTE address []?**401**

pvc Local PVC Range Start パラメーターによって定義される範囲内のすべての PVC について PVC の定義を削除します。

例:

delete pvc

Local PVC Range Start [1]?**1**
Local DTE address []?**301**
Record deleted

Enable

XTP 転送機能を起動します。

構文: enable-xtp

例: **enable-xtp**

Disable

XTP 転送機能を停止します。

構文: disable-xtp

例: **disable-xtp**

Set

XTP キープアライブ・タイマーを設定します。

構文: keep-alive-timer

例:

set keep-alive-timer

Keepalive timer in seconds [10]?**60**

List

インターフェース、ピア・ルーター、リモート DTE、または PVC をリストします。

構文:

list all
cugs

keep-alive-timerlocal-dtespeer-routersremote-dtespvcsxtp-status

all XTP 用に構成されたすべてのインターフェース、ピア・ルーター、リモート DTE、および PVC を表示します。

例:**list all**

STATUS: XTP-DISABLED

Local DTEs:

Interface	DTE Address		Calling DTE address is optional
1	44444		
	Pref CUG : 7777	Others : 9999 0	
	Pref BI-CUG : 0	Others :	
4	33333		Calling DTE address is optional
	Pref CUG : 1	Others : 2 3 4 5	
	Pref BI-CUG : 6	Others : 7 8 9 10	

Peer Routers Connection Timeout

Remote DTEs:

DTE Address Peer Router(s)

PVCs:

Local PVC LCN Range	Local DTE Address	Remote PVC LCN Range	Remote DTE Address
Pref CUG : 114	Others : 314 478		
Pref BI-CUG : 1	Others : 1 1 1 1111		

KEEP-ALIVE-TIMER: 10 seconds

cugs XTP プロトコル用に定義された CUG および BI-CUG 番号をリストします。

keep-alive-timer

XTP 用に構成されたすべてのキープアライブ・タイムを表示します。

local-dtes

XTP 用に構成されたすべてのローカル DTE を表示します。

例:**list local-dtes**

Local DTEs:

Interface	DTE Addr	
1	101	Calling DTE address is required
2	201	Calling DTE address is required

peer-routers

XTP 用に構成されたすべてのピア・ルーターを表示します。

例:**list peer-routers**

```
Peer Routers:
128.185.100.2
128.185.100.3
```

pvcs XTP 用に構成されたすべての PVC を表示します。

XTP 構成コマンド (Talk 6)

例

```
list pvcs
```

PVCs:

Local PVC LCN Range	Local DTE Address	Remote PVC LCN Range	Remote DTE Address
1 - 1	100	1 - 1	301

remote-dtes

XTP 用に構成されたすべてのリモート DTE を表示します。

例:

```
list remote-dtes
```

Remote DTEs: DTE Address	Peer Router
301	128.185.100.2
401	128.185.100.3
402	128.185.100.3
403	128.185.100.3
404	128.185.100.3

xtp-status

XTP の状態 (使用可能か使用不可か) を表示します。

例:

```
list xtp-status
```

STATUS: XTP-ENABLED

XTP 監視コマンド

この節では、XTP 監視コマンドについて説明します。これらのコマンドでは、現在アクティブのインターフェース、ピア・ルーター、リモート DTE、PVC、および SVC を表示することができます。また、インターフェース、DTE、またはピア・ルーターを動的に追加または削除することもできます。

XTP> プロンプトを表示するには、監視 (+) プロンプトで **protocol xtp** と入力します。

```
+protocol xtp
X.25 Transport Console
XTP>
```

XTP 監視コマンドは、XTP> プロンプトで入力します。

表 58. XTP 監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Add	ローカル DTE、リモート DTE、またはピア・ルーターを動的に追加します。
Delete	ローカル DTE、リモート DTE、またはピア・ルーターの構成を動的に削除します。
List	個々の PVC または SVC の統計および一般情報を表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Add

インターフェース、ピア・ルーター、またはリモート DTE を XTP 構成に追加します。

構文:

```
add                                local-dtes
                                       peer-router
                                       remote-dtes
```

local-dtes

ローカル・インターフェースを XTP 構成に追加します。

例:

```
add local-dtes
Interface number [0]?1
DTE address [ ]?101
```

peer-router

ピア・ルーターを XTP 構成に追加します。

例:

```
add peer-router
Router's IP Address [0.0.0.0]?128.185.100.2
```

remote-dtes

リモート DTE を XTP 構成に追加します。

例:

```
add remote-dtes
Peer router's IP Address [0.0.0.0]?128.185.100.2
DTE address [ ]?301
DTE address [ ]?
```

Delete

ローカル DTE、ピア・ルーター、またはリモート DTE をルーター構成から削除します。

構文:

```
delete                               local-dtes
                                       peer-router
                                       remote-dtes
```

local-dtes

ローカル・インターフェースを XTP 構成から削除します。

例:

```
delete local-dtes
Interface Number [0]?1
DTE address [ ]?101
DTE address [ ]?
```

XTP 監視コマンド (Talk 5)

peer-router

ピア・ルーターを XTP 構成から削除します。

例: delete peer-router

```
Router's IP Address [0.0.0.0]?123.185.100.2
```

remote-dtes

リモート DTE を XTP 構成から削除します。

例:

```
delete remote-dtes
```

```
DTE address [ ]?401  
DTE address [ ]?
```

List

現在アクティブのインターフェース、ピア・ルーター、リモート DTE、PVC、および SVC を表示します。

構文:

```
list                                all  
list                                xtp-status  
list                                local-dtes  
list                                peer-routers  
list                                remote-dtes  
list                                pvc  
list                                pvc-detailed  
list                                pvc-all-detailed  
list                                svcs  
list                                svc-detailed  
list                                svc-all-detailed
```

all すべての list コマンド・オプションの出力を表示します。

例:

```
list all
```

```
STATUS: XTP-ENABLED  
KEEP-ALIVE TIMER = 20 seconds
```

LIST OF LOCAL DTES

```
-----  
Interface      Local  
No             DTE  
1              101    Calling DTE address is required  
2              201    Calling DTE address is required
```

LIST OF PEER ROUTERS

```
-----  
Router          CNN      Number  Received      Sent  
                State   of Ckts  Pkts  Bytes  Pkts  Bytes  
128.185.100.3  Active  15      60    1533   12    142  
128.185.100.2  Active  12      63    1620   10    130
```


LIST OF REMOTE DTES

```

-----
Remote Router
DTE IP
404 128.185.100.3
403 128.185.100.3
402 128.185.100.3
401 128.185.100.3
301 128.185.100.2
    
```

LIST OF PVCs

```

-----
Index Int PVC Local Local Remote Remote
No No State LCN DTE LCN DTE
1 1 Active 100 301
    
```

LIST OF SVCS (list svcs)

```

-----
Index Int Logical SVC Local Remote Peer
No No Channel State DTE DTE Router
1 2 5 ACT 333333333333 4444444444444 3.3.3.3
    
```

SVC 1 IN DETAIL (list svc-detailed)

```

-----
Int Log SVC Received Sent Dropped
No Chn State Pkts Bytes Pkts Bytes Pkts Bytes
2 5 ACT 2 116 2 106 0 0
    
```

LIST OF SVCS (svcs-all-detailed)

```

-----
Int Log SVC Received Sent Dropped
No Chn State Pkts Bytes Pkts Bytes Pkts Bytes
2 5 ACT 1 7 1 2 0 0
    
```

xtp-status

XTP が使用可能/使用不可のいずれか、およびキープアライブ・タイマーに指定された時間を表示します。

例:

list xtp-status

```

STATUS: XTP-ENABLED
KEEP-ALIVE-TIMER = 20 seconds
    
```

local-dtes

XTP 用に構成されたすべてのインターフェースを表示します。

例:

list local-dtes

LIST OF LOCAL DTES

```

-----
Interface Local
No DTE
1 101 Calling DTE address is required
2 201 Calling DTE address is required
    
```

peer-routers

XTP 用に構成されたすべてのピア・ルーターを表示します。

例:

list peer-routers

LIST OF PEER ROUTERS

```

-----
Router CNN Number Received Sent
State of Ckts Pkts Bytes Pkts Bytes
128.185.100.3 Active 15 60 1533 12 142
128.185.100.2 Active 12 63 1620 10 130
    
```

remote-dtes

XTP 用に構成されたすべてのリモート・インターフェースを表示します。

XTP 監視コマンド (Talk 5)

例:

```
list remote-dtes
LIST OF REMOTE DTES
-----
Remote Router
DTE IP
404 128.185.100.3
403 128.185.100.3
402 128.185.100.3
401 128.185.100.3
301 128.185.100.2
```

pvcs XTP 用に構成されたすべての PVC を表示します。

例:

```
list pvcs
LIST OF PVCS
-----
Index Int PVC Local Local Remote Remote
No No State LCN DET LCN DTE
1 1 Active 100 301
```

pvc-detailed

特定の PVC 定義の詳細情報を表示します。インデックス番号をリストしたい場合は、xtp> プロンプトで **list all** と入力します。

例:

```
list pvc-detailed
PVC Index Number [1]?1
PVC 1 IN DETAIL
-----
Int PVC Received Sent Dropped
No State Pkts Bytes Pkts Bytes Pkts Bytes
1 ACTIVE 55 3220 35 2350 15 1870
```

pvcs-all-detailed

すべての PVC 定義の詳細情報を表示します。

例:

```
list pvcs-all-detailed
LIST OF PVCS
-----
INT Local PVC Received Sent Dropped
No LCN State Pkts Bytes Pkts Bytes Pkts Bytes
1 1 ACTIVE 55 3220 35 2350 15 1870
```

svcs すべての SVC 定義を表示します。

例:

```
list svcs
LIST OF SVCS
-----
Index Int LOG SVC Local Remote Peer
No No Chan State DTE DTE Router
1 1 Active 200 401 3.3.3.3
2 1 Active 200 402 3.3.3.3
3 2 Active 200 403 3.3.3.3
4 2 Active 200 404 3.3.3.3
```

svc-detailed

特定の SVC 定義の情報を表示します。

例:

```
list svc-detailed
SVC Index Number [1]?1
SVC 1 IN DETAIL
-----
```

XTP 監視コマンド (Talk 5)

Int No	LOG Chan	SVC State	Received		Sent		Dropped	
			Pkts	Bytes	Pkts	Bytes	Pkts	Bytes
1		ACTIVE	75	4220	55	3350	20	870

svcs-all-detailed

すべての SVC 定義の情報を表示します。

例:

```
list svcs-all-detailed
```

```
LIST OF SVCS
```

Index No	Int No	Log Chn	SVC State	Received		Sent		Dropped	
				Pkts	Bytes	Pkts	Bytes	Pkts	Bytes
1	1		ACTIVE	4220	55	550	20	870	
2	1		ACTIVE	3220	40	2350	15	970	
3	2		ACTIVE	4003	50	3892	20	870	
4	2		ACTIVE	3967	58	4167	12	800	

XTP 監視コマンド (Talk 5)

第28章 フレーム・リレー・インターフェースの使用

この章では、フレーム・リレー・インターフェースの使用法について説明します。本章には、以下の節が含まれています。

- 『フレーム・リレーの概説』
- 452ページの『フレーム・リレー・ネットワーク管理』
- 454ページの『フレーム・リレー・データ速度』
- 457ページの『回線輻輳』
- 460ページの『フレーム・リレーを介する帯域幅予約』
- 462ページの『フレーム・リレー構成プロンプトの表示』
- 462ページの『フレーム・リレー基本構成手順』
- 463ページの『フレーム・リレー PVC マネージメントの使用可能化』
- 464ページの『フレーム・リレー SVC マネージメントの使用可能化』

フレーム・リレーの概説

フレーム・リレー (FR) プロトコルとは、X.25 のパケット交換とポート共用を、高速で遅延の少ない時分割多重 (TDM) 回線交換と組み合わせて、相互接続パケットを転送する方式です。FR を使用すると、複数の LAN を、複数のポイント・ポイント・バーチャル・サーキット (VC) をもつ単一の高速 (1.54 Mbps) WAN リンクに接続することができます。FR は、以下のフィーチャーを提供します。

- 高いスループットと少ない遅延。D チャンネル (LAPD) データ・リンク・プロトコルであるリンク・アクセス・プロトコルの中心機能 (誤り検出、アドレッシング、および同期) を利用することにより、FR ではすべてのネットワーク・レイヤー (レイヤー 3) の処理を不要にします。FR は、中心機能のみを使用することにより、各フレームの処理の遅延を減らします。
- 輻輳 (ふくそう) 検出。逆方向明示的輻輳 (ふくそう) 通知 (BECN) または順方向明示的輻輳 (ふくそう) 通知 (FECN) を受信すると、ルーターは制御下でトラフィックを減速し、FR ネットワークが完全に遮断されるのを回避します。
ルーターは、統合リンク・レイヤー・マネージメント (CLLM) 輻輳 (ふくそう) メッセージを受信した場合も、トークンリングの減速を開始することができます。CLLM は、フレーム・リレー・ネットワークの動作に関する追加管理情報を、接続された DTE に提供する、フレーム・リレー標準のオプション部分です。
- 回線アクセスと制御。ルーターは非構成回線 (オーファン回線) の利用可能性を動的に確認するので、これらの新規回線へのアクセスを制御することができます。
- ネットワーク管理オプション。ネットワークの要件に応じて、FR プロトコルは、ローカル・ネットワーク管理インターフェースを使用して動作することも、使用せずに動作することもできます。
- 多重化プロトコル。1 つの VC を使用して複数のプロトコルを渡します。
- データ圧縮。FRF.9 標準をサポートします。詳細については、フィーチャーの使用と構成のデータ圧縮の使用を参照してください。

フレーム・リレーの使用

- データ暗号化。専用の暗号化方式を使用します。詳細については、[フィーチャーの使用と構成](#) のデータ暗号化の使用と構成を参照してください。

FR は、誤り訂正または再送の機能は提供しません。FR は、ホスト装置の機能に依存して、誤りのないエンド・エンド間のデータ転送を行います。

フレーム・リレー・ネットワーク

FR ネットワークは、FR サービスを提供する FR バックボーン (FR キャリアによって提供される FR スイッチから成る) から構成されます。ルーターは、FR 接続装置として機能します。ルーターは FR フレームをカプセル化し、それらをデータ・リンク接続識別子 (DLCI) に基づいてネットワーク上でルーティングします。DLCI は、ルーターと FR あて先装置間の PVC または SVC を識別する媒体アクセス制御 (MAC) アドレスです。たとえば、図21 では、ルーター B からルーター D に送られるパケットは、ルーター D に到達するために DLCI は 19 になりますが、ルーター D からルーター B に送られるパケットの DLCI は 16 になります。

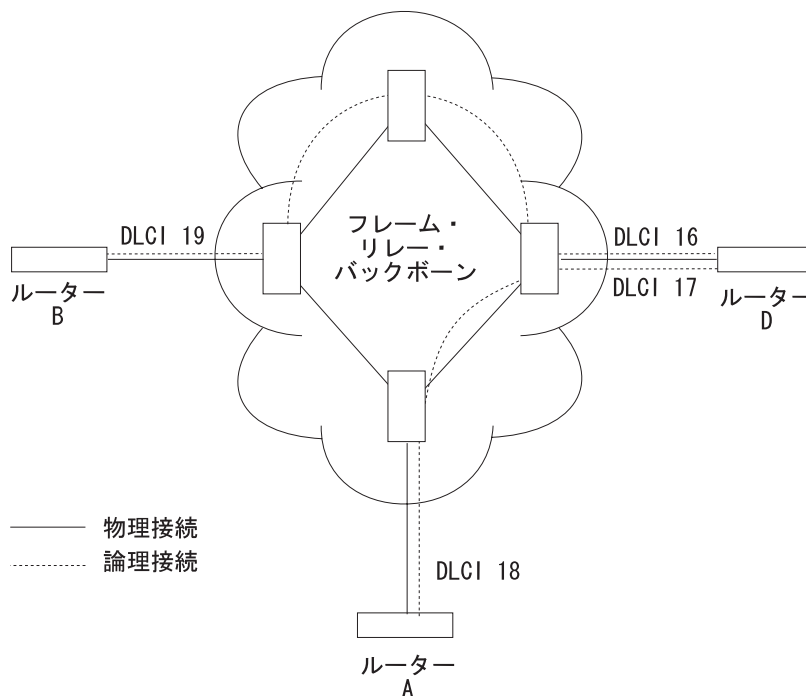


図21. フレーム・リレー・ネットワーク内の DLCI

DLCI は、ローカルまたはグローバルの意味を持つことができます。ローカル DLCI は、ネットワークへの入り口点で有効であり、グローバル DLCI はネットワーク全体で有効です。ただし、ユーザーから見ると、ルーターがパケットをルーティングするのに使用する DLCI は、ユーザーがフレームのグローバルまたはローカルあて先に対応付ける DLCI ということになります。DLCI は、FR 構成プロセスで構成するか、あるいは FR マネージメントを通して確認されます。

FR PVC は、FR ネットワークを通じてデータを発送するために使用される事前定義接続です。ネットワーク内で PVC に割り振られる帯域幅は、加入オプションであり、PVC がそれを使用するかどうかにかかわらず PVC に割り振られる必要があります。

フレーム・リレーネットワークには、次のような特性があります。

- フレームを透過的に伝達します。ネットワークが変更できるのは、DLCI、輻輳 (ふくそう) ビット、およびフレーム・チェック・シーケンスだけです。ハイレベル・データ・リンク制御 (HDLC) フラグおよびゼロ・ビット挿入により、フレームの区切り、配列、および透過性を実現します。
- 伝送誤り、フォーマット誤り、および運用誤り (不明 DLCI を持つフレーム) を検出します。
- 個々の VC 上のフレーム転送順序を保存します。
- フレームの確認または再送は行いません。

フレーム・リレー・スイッチド・バーチャル・サーキット

フレーム・リレー・スイッチド・バーチャル・サーキット (SVC) は、フレーム・リレー・ネットワーク内で "カットスルー" ルーティングを実現することができ、DTE 間の中間ルーター・ホップを最小化するか、除去します。ネットワークの複雑さを単純化することができ、DTE の性能が改善されます。

SVC は PVC に取って代わり、ネットワーク帯域幅を保持したまま、帯域幅コストを削減することができます。

FR SVC 標準は、ISDN 標準のサブセットであり、ISDN ほど複雑でなく、ISDN と同じ利点の多くを提供します。

FR SVC を介して、以下のプロトコルがサポートされます。

- AppleTalk 2
- ARP
- ブリッジング
- DECnet IV
- DLSw
- IP/OSPF/RIP/BGP4
- IPX

SVC は要求されることがなく、要求されるグループに属することはありません。

フレーム・リレー・インターフェースの初期化

ローカル管理インターフェース (LMI) は、フレーム・リレー・インターフェース上の PVC の状態を判別するのに使用されます。LMI が使用可能な場合、ルーターと FR スイッチ間の LMI フレームの交換が正常に行われると、FR インターフェースはアクティブになります。しかし、その DLCI の相手側ルーターへの PVC 状態がアクティブであることが LMI 状態メッセージで示されるまでは、別のルーターとの間でのデータの受信または送信を行うことはできません。また、FR インターフェースの状態が PVC の状態と結合されているために、LMI または Q.922 交換が正常に行われてもインターフェースが起動しないといった事態が生じることもあります (詳細については、448ページの『フレーム・リレー・インターフェースの状態に影響を与える PVC 状態の構成』を参照してください)。

フレーム・リレーの使用

LMI が使用可能にされておらず、SVC が使用可能にされている場合、ルーターと隣接装置間で Q.922 フレームの交換が正常に行なわれると、フレーム・リレー・インターフェースはアクティブになります。この時点では、すべての PVC がアクティブと見なされます。ただし、SVC がアクティブになるのは、Q.933 の起動交換が正常に行なわれた後だけです。

PVC 状態は、すべての PVC について、アクティブまたは非アクティブとして示されます。アクティブ PVC は、エンド・システムへの完全なコネクションが確立されています。非アクティブ PVC は、エンド・システムまたは FR スイッチのいずれかがオフラインであるために、エンド・システムへの完全なコネクションが確立されていません。

たとえば、図22 では、ルーター B はルーター D への PVC が構成されています。ルーター B は、FR スイッチ B を介して FR マネージメントと正常に相互作用しています。別の FR スイッチがダウンしているか、エンド・システムがダウンしているために、エンド・エンド PVC コネクションは確立されていません。ルーター B は、その PVC について非アクティブ状態を受け取ります。

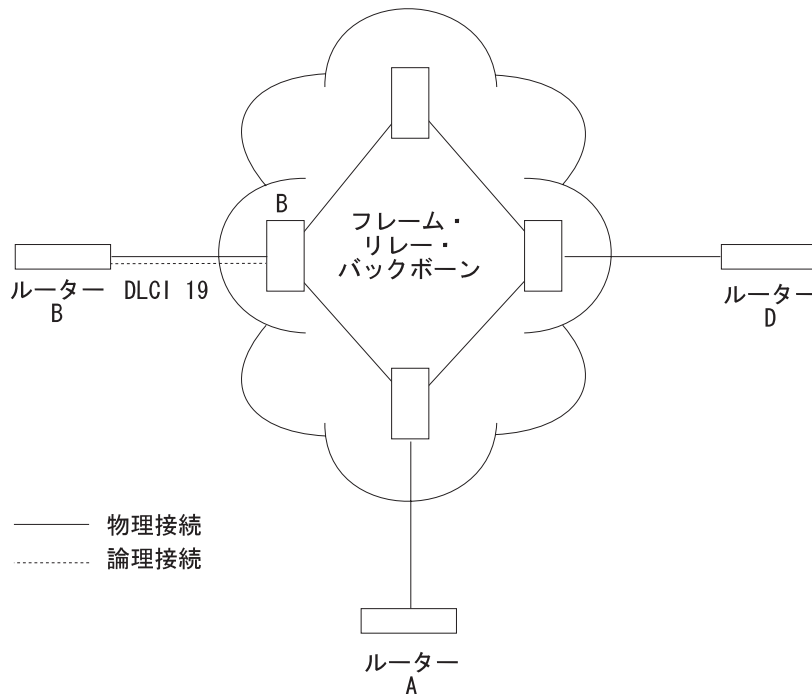


図22. フレーム・リレー・ネットワーク内の DLCI

LMI および SVC が使用不可にされ、FR インターフェースがシリアル・ライン上で稼働し、DTE ケーブルが使用されている場合、FR 制御機能が DTR および RTS モデム制御信号を代入します。(X.21 の場合は、Control 信号が代入されます。) DSR、CTS、および DCD モデム制御信号がオンになると、FR インターフェースはアップになります。(X.21 が使用されている場合、Indication モデム制御信号がオンになると、FR インターフェースはアップになります。) DSR、CTS、または DCD がオフであるか、あるいは X.21 が使用されている場合は、Indication 信号がオフのときは、FR インターフェースはダウンしているか、テスト状態にあります。したがって、FR スイッチまたは他の FR DTE (FR DTE と DTE の接続性のために構成されてい

る場合) が失われた場合、使用されているモデム、モデム・エリミネーター、または DSU が、これらの信号の 1 つまたは複数を廃棄していないか確認する必要があります。

オーファン回線

オーファン・パーマネント・バーチャル・サーキットとは、ルーターには構成されていないが、ネットワーク管理エンティティのアクションを通して間接的に確認された PVC のことです。たとえば、図23 では、ルーター B には、ルーター D への構成された PVC がありますが、ルーター A への構成された PVC はないものと想定しています。ルーター A がルーター B への PVC を構成すると、ルーター B は、LMI メッセージからルーター A への PVC を確認し、それをオーファンとして分類します。

オーファン PVC は、**enable orphan-circuit** および **disable orphan-circuit** コマンドを使用してそれらを使用可能または使用不可にすることを除いて、構成された回線と同じに扱われます。

オーファン回線を使用不可にすると、構成されていない回線からネットワークに無許可で入るのを防止できるので、ネットワークのセキュリティー手段を追加できます。オーファン回線を使用可能にすると、ルーターは、構成されていなかった回線を介してパケットを転送することができます。通常ならば廃棄されていたパケットが転送できるようになります。

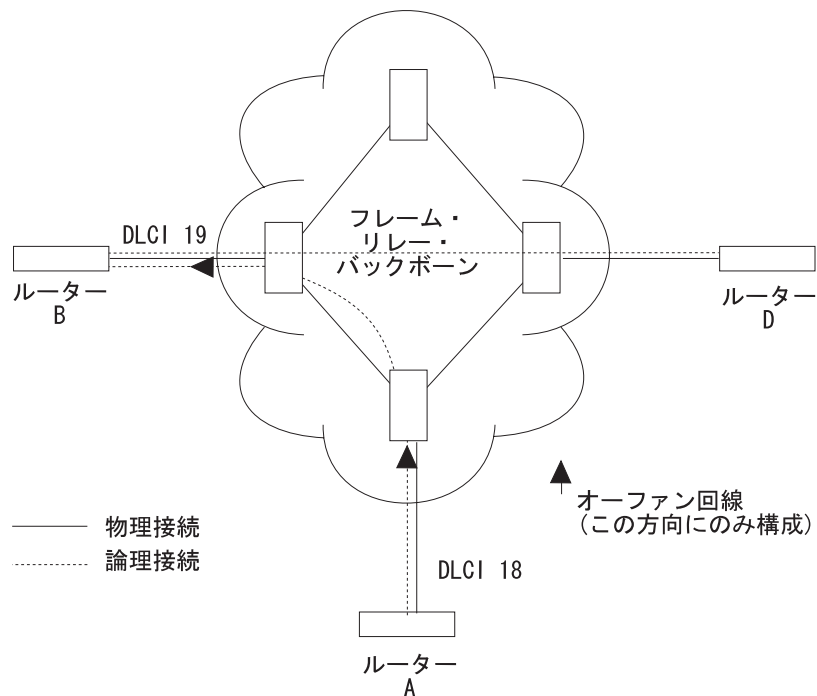


図 23. オーファン回線

オーファン・スイッチド・バーチャル・サーキットは、ルーターには構成されていないが、それへのコール・インが受信されると作成されます。これは、図23 に似ています。ただし、回線を生成し、該当するパラメーターをそれに対応付けるには、LMI

フレーム・リレーの使用

の代わりに Q.933 メッセージが使用されます。オーファン SVC は、**enable switched-virtual-circuit** コマンドのコール・イン・オプションを使用してそれらを使用可能または使用不可にできることを除いて、構成された SVC と同じに扱われます。

フレーム・リレー・インターフェースの状態に影響を与える PVC 状態の構成

以下により、フレーム・リレー・インターフェースの動作を制御することができます。

1. 『No-PVC』フィーチャーを使用可能にする
2. 『必須 PVC』を構成する
3. 『必須 PVC グループ』を構成する

フレーム・リレー『No-PVC』フィーチャーを使用可能にした場合、インターフェース上にアクティブの PVC が存在しないと、フレーム・リレー・インターフェースは非アクティブになります。少なくとも 1 つの PVC がアクティブの場合、ルーターと FR スイッチ間で LMI 交換が正常に行われると、フレーム・リレー・インターフェースはアクティブになります。

PVC を『必須 PVC』として構成することができます。ある PVC が必須であるが、グループに含まれていない場合、その PVC が非アクティブになると、フレーム・リレー・インターフェースは非アクティブになります。その PVC がアクティブになった場合、ルーターとフレーム・リレー・スイッチ間での LMI フレーム交換が正常に行われると、インターフェースはアクティブになります。

複数の PVC が必須であり、PVC グループに含まれていない場合、すべての必須 PVC がアクティブになるまで、インターフェースはアクティブになりません。

必須 PVC が PVC グループに属している場合、PVC グループ内のすべての PVC が非アクティブになると、フレーム・リレー・インターフェースは非アクティブになります。グループ内の少なくとも 1 つの PVC がアクティブになった場合、ルーターと FR スイッチ間での LMI フレーム交換が正常に行われると、インターフェースはアクティブになります。複数の PVC グループが存在する場合、各グループ内の少なくとも 1 つの PVC がアクティブになるまでは、インターフェースはアクティブになりません。

『必須 PVC グループ』は、名前によって対応付けられている回線の集りです。ここにおける『名前』は、必須 PVC グループの名前を指します。

これらのフィーチャーを WAN 再ルートで使用すると、1 次 FR リンク上のすべての PVC、必須 PVC、または PVC グループが非アクティブになった場合に、代替リンクを起動させることができます。

フレーム・リレーのフレーム

FR フレームは、固定サイズのアドレス・フィールドと可変サイズのカプセル化されたユーザ・データから構成されます。449ページの図24 は、フレーム・リレーのフレーム・フォーマットを示しています。

フレーム・リレーの使用

APPN 高性能ルーティング (HPR) は、このビットがセットされているのを検出し、高速トランスポート・プロトコルの適応速度フロー/輻輳制御アルゴリズムにより、データ送信速度を調整できるようにします。このアルゴリズムは、トラフィックのバーストと輻輳を防止し、スループットを高レベルに維持します。

逆方向明示的輻輳通知 (BECN)

FR バックボーン・ネットワークはこのビットを 1 にセットすることにより、この PVC 上でこのルーターによって送信されたフレームが輻輳 (ふくそう) に遭遇したことをユーザーに通知します。次にルーターは、CIR または輻輳監視が使用可能にされている場合、ユーザー定義の CIR 以下の速度まで減速し始めます。PVC の CIR は、FR サービス提供者によって提供され、**add permanent-virtual-circuit** コマンドを使用して構成されます。

廃棄可能性 (DE)

フレーム・リレー・ネットワークは、PVC 上の CIR を超過し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。廃棄可能なトラフィックを識別するには、次のようにします。

1. フレーム・リレー・インターフェースおよび廃棄可能にするトラフィックが通るすべての FR 回線上に BRS を構成する。
2. **assign** コマンドを使用して、BRS トラフィック・クラスにプロトコルまたはフィルターを割り当てる。このプロトコルまたはフィルター・トラフィックについて、DE ビットをオンにセットするかどうかを指定します。

ユーザー・データ

このフィールドには、転送されるプロトコル・パケットが入っています。このフィールドには最大 8188 オクテットを含めることが可能ですが、フレーム・チェック・シーケンス (FCS) が効率的に誤りを検出できるのは、最大 4096 オクテットまでのデータです。プロトコル・データの前に、RFC 1490 および RFC 2427 で定義されているフレーム・リレー・カプセル化ヘッダーが置かれています。

フレーム・チェック・シーケンス

このフィールドは、HDLC および LAPD フレームが使用する標準 16 ビット巡回冗長検査 (CRC) です。このフィールドは、フレームの開始フラグと FCS の間のビットに発生したビット誤りを検出します。

注: HSSI アダプター上のフレーム・リレー・インターフェース用に 32 ビットの CRC を構成することができます。

フレーム・リレー・ネットワークを介したフレーム転送

FR プロトコルは、カプセル化のためにパケットを受信すると、パケットのネットワーク・アドレスをアドレス解決プロトコル (ARP) キャッシュ内のエントリーと比較しま

す。ARP キャッシュにネットワーク・アドレスに一致する DLCI 番号が含まれている場合、FR プロトコルは、そのパケットをフレームにカプセル化し、指定されたローカル DLCI を介してフレームを転送します。ARP キャッシュに一致するものが含まれていない場合、FR プロトコルは、インターフェース上のすべての構成済み PVC 上に ARP 要求を送信します。該当するエンドポイントが ARP レスポンスで応答した場合、FR プロトコルは、その ARP レスポンスを受信したローカル DLCI を ARP キャッシュに追加します。同じネットワーク・アドレスあての後続のデータ・パケットは、フレームにカプセル化され、そのローカル DLCI を介して転送されます。

プロトコル・アドレス

プロトコル・アドレスは、ローカルに構成された名前を使用して静的に FR ネットワーク PVC アドレスにマップすることも、逆 ARP または ARP を介して動的に見つけることもできます。(ARP および逆 ARP についての詳細は、プロトコル構成と監視 解説書 を参照してください。) いずれの方法も、表59 に示すように、プロトコルに依存します。

注: 静的プロトコル・アドレスは、静的 ARP エントリーとも呼ばれます。静的 ARP エントリーは、**add protocol-address** コマンドを使用して構成に追加します。

表59. プロトコル・アドレス・マッピング

プロトコル・タイプ	ARP および逆 ARP の使用	静的マッピング	プロトコル構成で構成された VC
AP2	可	可	不可
IP	可	可	不可
IPX	可	可	不可
Banyan VINES**	不可	不可	不可
DNA IV	可	可	不可
OSI*, **	不可	不可	可

* プロトコル・アドレスを FR PVC にマップするためには、プロトコル・レベルで OSI を構成する必要があります。

** SVC を使用してはサポートされません。

マルチキャスト・エミュレーションとプロトコル・ブロードキャスト

マルチキャスト・エミュレーションは、ARP のようなマルチキャストを必要とするプロトコルが FR インターフェース上で正常に機能できるようにする任意選択フィーチャーです。マルチキャスト・エミュレーションを使用すると、マルチキャスト・フレームが各アクティブ PVC 上に転送されます。**enable** および **disable multicast** コマンドを使用して、このフィーチャーをオンまたはオフにすることができます。マルチキャストを使用するプロトコルは、AP2、ARP、Banyan VINES、DNA4、IP、および IPX です。

プロトコル・ブロードキャストは、FR インターフェース上で IP RIP プロトコルが正常に機能できるようにする、もう 1 つの任意選択フィーチャーです。**enable protocol-broadcast** および **disable protocol-broadcast** コマンドを使用して、このフィーチャーをオンまたはオフにすることができます。

フレーム・リレーの使用

フレーム・リレーを介する ARP/InARP をサポートするプロトコルの場合、プロトコル・アドレスが回線で確認されたか、回線に構成されている場合にのみ、フレーム・リレーはその回線を介してプロトコル・パケットをマルチキャストします。

マルチキャストは、個別の SVC について使用可能または使用不可にすることもできます。マルチキャスト・オプションは、**add switched-virtual-circuit** で使用します。

フレーム・リレー・ネットワーク管理

FR ネットワークのバックボーンを提供者が FR ネットワーク管理機能を提供します。インターフェースで利用可能な PVC の状態情報および構成情報を FR エンド・ステーション (ルーター) に提供するのはネットワーク管理の責任です。

PVC の場合、FR プロトコルは、ANSI T1.617 付録 D、ITU-T Q.933 付録 A (CCITT Q.933 付録 A と呼ばれる)、およびインターリム・ローカル管理インターフェース (LMI) マネージメント・エンティティをサポートします。これらのエンティティは、**enable** および **disable** LMI 構成コマンドを使用して、オンまたはオフにすることができます。特に、FR LMI は、以下の情報を提供します。

- 追加 PVC (オフアン) およびそれらがアクティブか非アクティブかの通知、または PVC の削除の通知
- 構成された PVC の利用可能性の通知。PVC の利用可能性は、PVC エンドポイントがハートビート・ポーリング プロセスに正常に参加できるかどうかに関係します。これについては、453ページの『リンク整合性検証報告書』で詳しく説明します。
- キープアライブ シーケンス番号交換の使用による、エンド・ステーションとネットワーク間の物理リンクの整合性の検証

FR インターフェースは PVC ネットワーク管理をサポートしますが、インターフェースが FR バックボーンを介して動作するためには、マネージメントを FR バックボーン上で実行する必要はありません。たとえば、バックツーバック構成のマネージメントを使用不可にすることができます。

SVC の場合、FR プロトコルは、FRF 4 (フレーム・リレー・インプリメンテーション合意 4) をサポートします。これには、ANSI Q.922 のインプリメンテーションおよび ANSI Q.933 のサブセットが記載されています。Q.922 は、ルーターとネットワーク間の物理リンクの整合性の検証を提供します。Q.933 は、ネットワークを通じて SVC を設定または切断する手段を提供します。SVC が使用される場合、Q.922 および Q.933 は常に、使用可能にされます。

管理状態報告書

要求に応じて、FR LMI は 2 種類の状態報告書、つまり、全状態報告書とリンク整合性検証報告書を提供します。全状態報告書は、インターフェースが知っているすべての PVC に関する情報を提供します。リンク整合性検証報告書は、特定のエンド・ステーションとネットワーク・スイッチの間のコネクションを検証します。すべての状態照会および応答は、ANSI T1.617 付録 D および ITU-T Q.933 付録 A の場合は DLCI 0 を介して、また中間 LMI マネージメントの場合は DLCI 1023 を介して送信されます。

全状態報告書

FR インターフェースが全状態報告書を必要とする場合、ルーターの FR プロトコルは、全状態報告書を要求する状態照会メッセージを FR ネットワーク・バックボーンに送信します。状態照会メッセージは、インターフェース上のすべての PVC の状態に対する要求です。この要求を受信すると、FR マネージメントは、リンク整合性検証要素と各 PVC の PVC 状態情報要素から成る全状態報告書で応答する必要があります。(『リンク整合性検証報告書』を参照してください。)

PVC 状態情報要素には、以下の情報が入っています。すなわち、特定 PVC のローカル DLCI 番号、PVC の状態 (アクティブまたは非アクティブ)、および PVC が新しいものか、あるいはマネージメントがすでに知っている既存の PVC であるかです。

注: FR インターフェースで提供される PVC の数は、ネットワークのフレーム・サイズ、および全状態報告書に入れることができる個々の PVC 情報要素の量によって制限されます。たとえば、フレーム・サイズが 1K のネットワークの PVC の最大数は 202 です。

リンク整合性検証報告書

リンク整合性検証報告書 (ハートビート・ポーリングとも呼ばれる) には、リンク整合性検証要素が入っています。この要素は、送信シーケンス番号と受信シーケンス番号の交換が行われる場所です。シーケンス番号を交換することによって、マネージメントとエンド・ステーションは、同期リンクの整合性を評価することができます。送信シーケンス番号は、メッセージ発信元の現在の送信シーケンス番号です。受信側はこの番号を見つけ、それを前回の送信シーケンス番号と比較して、この番号が正しく増分されているかどうかを検証します。受信シーケンス番号は、発信元がインターフェースを介して送信した前回の送信シーケンス番号です。送信シーケンス番号のコピーを受信シーケンス番号フィールドに入れるのは、受信側の責任です。この方法で、発信元は受信側がフレームの受信と解釈を正しく行ったことを確認できます。

あるエンド・ステーションがこのポーリング・プロセスに参加できなかった場合、マネージメントの全状態報告書機構を介して、論理接続された PVC をもつすべてのリモート・エンド・ステーションに、その PVC は非アクティブであることが通知されます。

統合リンク・レイヤー・マネージメント (CLLM)

CLLM は、業界で広くサポートされてはいませんが、一部のフレーム・リレー・スイッチの製造元で採用されているオプションの FR 管理機能です。CLLM は、LMI によって提供されるのと同じ管理情報のいくつか(特に、故障通知)を提供します。CLLM の主な用途は、接続装置に PVC の非同期輻輳 (ふくそう) 通知を提供することです。1 つの CLLM メッセージで、複数の PVC の故障または輻輳 (ふくそう) を示すことができます。フレーム・リレー・プロトコルは、CLLM について以下の標準をサポートしています。すなわち、ANSI T1.618, ITU-T (CCITT) Q.922 付録 A および ITU-T (CCITT) X.36 付録 C です。

フレーム・リレー・データ速度

この節では、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) のデータ速度について説明します。

認定情報速度 (CIR)

CIR は、通常の輻輳 (ふくそう) のない条件下の VC に対して、ネットワークがサポートすることを認定しているデータ速度です。構成または確認されたすべての VC に対して、CIR が提供されます (FR サービス提供者によって)。CIR は、物理リンクの総帯域幅の一部分で、0 または VC 用に予約された 300 bps ~ 2 Mbps* のいずれかです。単一 DS0 チャンネルでは 64 Kbps の値が、最も一般的です。

*注: HSSI アダプター上の FR インターフェースの最大 CIR 値は 52 Mbps です。

add permanent-virtual-circuit、**change permanent-virtual-circuit**、**add switched-virtual-circuit**、または **change switched-virtual-circuit** 構成コマンドを使用して、CIR を定義します。 **set circuit** コンソール・コマンドを使用すれば、CIR を動的に変更できます。また、**set CIR-defaults** コマンドを使用して、このインターフェース上のすべてのフレーム・リレー回線のデフォルト CIR を設定することもできます。

一部のフレーム・リレー・スイッチでは、CIR を値 0 に構成することが可能です。CIR が 0 のときは、フレーム・リレー・ネットワーク・バックボーンには VC 用に予約されている帯域幅はほとんど、あるいはまったくなく、VC のトラフィックは予約されていない帯域幅を使用します。

オーファン・パーマネント・バーチャル・サーキットの CIR

ルーターは、インターフェース・レベルで構成された CIR デフォルトに基づいて、オーファン回線に CIR を割り当てます。重要なデータのルーティングをオーファン回線に依存しており、CIR、Bc、および Be 値がインターフェース・レベルで構成された値と異なっている場合は、オーファン回線の代わりに PVC を定義することをお勧めします。これにより、ネットワークがサポートすることを認定している CIR を割り当てることができます。

認定バースト (Bc) サイズ

認定バースト (Bc) サイズとは、算定時間 (Tc) 間隔に送達することをネットワークが認定しているデータの最大量 (ビット数) です。Tc は、Bc を CIR で割った値に等しくなります ($Tc = Bc / CIR$)。CIR を 0 に構成すると、フレーム・リレーは Tc に 1 秒の値を使用します。

たとえば、VC の CIR を 9600 bps に設定し、認定バースト・サイズを 14 400 ビットに設定した場合、時間間隔は 1.5 秒になります。(14 400 ビット/9600 bps = 1.5 sec)。これは、VC が 1.5 秒間に最大 14 400 ビットを転送できることを意味しています。

注: FR によってサポートされる最小 Tc は .03 秒です。

認定バースト・サイズと最大フレーム・サイズの関係から、このパラメーターは重要です。最大フレーム・サイズ (ビット数) が認定バースト・サイズより大きい場合、ネットワークはサイズが認定バースト・サイズを超過しているフレームを廃棄する可能性があります。したがって、認定バースト・サイズは最大フレーム・サイズ以上にすることが必要です。また、ネットワークの提供者と共に設定したバースト・サイズに等しくすることも必要です。

add permanent-virtual-circuit、**change permanent-virtual-circuit**、**add switched-virtual-circuit** または **change switched-virtual-circuit** 構成コマンドを使用して、認定バースト・サイズを設定します。**set circuit** コンソール・コマンドを使用すると、認定バースト・サイズを動的に変更することができます。また、**set CIR-defaults** コマンドを使用して、このインターフェース上のすべてのフレーム・リレー回線のデフォルトの認定バースト・サイズを設定することもできます。

装置は、**set CIR-defaults** コマンドによって設定されたデフォルトに基づいて、オフファン回線に認定バースト・サイズを割り当てます。CIR を 0 に構成すると、認定バースト (Bc) サイズも 0 になります。

超過バースト (Be) サイズ

超過バースト (*Be*) サイズ は、CIR および Bc が非ゼロの場合、Tc ($Tc = Bc/CIR$) 期間中にルーターが PVC 上で Bc を超過して転送できる非認定データの最大量です。CIR = 0 のとき、フレーム・リレーは Tc に 1 秒の値を使用します。

ネットワーク上では、この超過データは、認定バースト・サイズよりも成功の確率が低い状態で送達されます。Be をゼロより大きい値に設定するのは、データが廃棄されるリスクと高位レイヤーのプロトコルの性能に与える影響を容認できる場合に限りしてください。Be は、ネットワークの提供者と共に設定した値に等しくする必要があります。

フレーム・リレーの構成時に **add permanent-virtual-circuit**、**change permanent-virtual-circuit**、**add switched-virtual-circuit** または **change switched-virtual-circuit** コマンドを使用して、超過バースト・サイズを設定します。**set circuit** コンソール・コマンドを使用すると、超過バースト・サイズを動的に変更することができます。オフファン回線は、**set CIR-defaults** コマンドで設定された値に等しい超過バースト・サイズを受け取ります。CIR を 0 に構成する場合は、超過バースト (Be) サイズを非ゼロ値に構成する必要があります。また、**set CIR-defaults** コマンドを使用して、このインターフェース上のすべてのフレーム・リレー回線に対するデフォルト超過バースト・サイズを設定することもできます。

回線速度

回線速度 とは、インターフェースの回線速度のことです。

FR インターフェースの回線速度は、**set line-speed** 構成コマンドを使用して構成します。内部クロックを使用する場合は、回線速度の構成は必須です。ただし、外部クロックの場合も回線速度を構成することをお勧めします。輻輳 (ふくそう) 監視が使用可能になっている場合、ルーターは最大情報速度として回線速度を使用するから

フレーム・リレーの使用

です。また、一部のプロトコルは、ルートのコストを計算するときに、インターフェースに構成されている回線速度を使用します。

フレーム・リレー・ダイヤル回線インターフェース上では、回線速度は構成不能です。ダイヤル回線が ISDN 基本インターフェースにマップされる場合は、64 Kbps が回線速度として使用されます。

チャンネル化 T1/E1 を基本ネットとして使用するダイヤル回線の場合、回線速度は、割り当てられたタイム・スロット数に 64 Kbps を掛けた値、もしくは 56 Kbps (チャンネル化回線の帯域幅を 56 Kbps に設定した場合) です。たとえば、チャンネル化回線のタイム・スロットの数を 3 に設定した場合、回線速度は 192 Kbps (3 * 64 Kbps) になります。

ダイヤル回線が V.25bis 基本インターフェースにマップされる場合は、V.25bis インターフェースの回線速度が FR ダイヤル回線として使用されます。

最小情報速度

最小情報速度 (IR) は、輻輳 (ふくそう) が通知されたときにルーターがそこまで減速する VC の最小データ速度です。set ir-adjustment 構成コマンドを使用して、最小 IR を CIR の比率として設定します。set ir-adjustment コンソール・コマンドを使用すれば、動的に変更することができます。CIR を 0 に構成した場合、最小 IR は 1500 bps になります。

最大情報速度

最大データ速度 は、ルーターが VC 上で転送する最大データ速度です。CIR 監視機能が使用可能であり、CIR および Bc が非ゼロの場合、最大情報速度は、CIR、Bc、および Be を使用して、次のように計算します。

$$(Bc + Be) \text{ per } Tc \text{ interval}$$

CIR 監視機能が使用可能であり、CIR および Bc が 0 に構成されている場合、最大情報速度は秒当たりの超過バースト・サイズ (Be) に等しくなります。

CIR 監視機能が使用可能でない場合、最大情報速度は回線速度に等しくなります。

可変情報速度

CIR 監視または輻輳 (ふくそう) 監視機能が使用可能である場合、可変情報速度 (VIR) は、構成された最小 IR から計算された最大 IR までの範囲です。ルーターが回線の輻輳 (ふくそう) を通知されると、VIR は徐々に最小情報速度まで減速され、ルーターが輻輳 (ふくそう) 通知を受信しなくなると、徐々に最大情報速度まで加速されます。set ir-adjustment 構成コマンドを使用して、ルーターが輻輳 (ふくそう) を通知されたときに VIR を減速する情報速度の比率を構成します。輻輳 (ふくそう) が終わったときに VIR を徐々に加速する情報速度の比率も、このコマンドを使用して構成します。

ネットワークのインパルス・ロードを避けるために、ルーターは VC がアクティブになったときに、VIR を CIR に初期設定します。CIR を 0 に構成した場合、VIR は

超過バースト (Be) に MIR 調整比率を掛けた値に初期設定されます。たとえば、Be が 64 000 に設定され、MIR 調整比率が 25% に設定されている場合、初期 VIR は 16 000 bps になります。

場合によっては、VIR が実際には最大値を超えても構わないことがあります。フレームの長さ (ビット数) が最大 IR より大きくても、フレーム・リレーはともかくフレームを転送します。

回線輻輳

回線の輻輳 (ふくそう) は、次の理由の 1 つによって発生します。

- 送信側が許容されるスループットより高速で転送している。
- 受信側のフレームの処理が遅過ぎる。
- 中間バックボーン・リンクが輻輳 (ふくそう) しており、結果的に、送信側が利用可能なスループット許容値より高速で転送することになる。

回線の輻輳 (ふくそう) が発生すると、ネットワークはパケットを廃棄するか、遮断する (もしくは、その両方を行う) が必要になります。

回線輻輳 (ふくそう) に応じて、ルーターは減速を実施します。これは、構成された最小 IR まで、パケット転送の速度を段階的に減らして行くこと言います。減速は、以下の条件を満たすときに行われます。

- 回線が輻輳 (ふくそう) している。
- ルーターがフレームの送信側である。
- CIR 監視または輻輳 (ふくそう) 監視が使用可能になっている。

この節では、フレーム・リレーのデータ速度および回線輻輳 (ふくそう) の監視について説明します。

CIR の監視

CIR 監視は、ルーターが FR ネットワーク上に輻輳 (ふくそう) 状態が生じるのを防止するために各インターフェースに設定することができる、オプションのフレーム・リレー・フィーチャーです。CIR 監視により、VC の VIR を、構成された最小 IR と最大 IR の間の範囲に設定することができます。

CIR 監視は、**enable cir-monitor** 構成コマンドを使用して構成し、デフォルトでは使用不可になります。CIR 監視が使用可能にされている場合、輻輳 (ふくそう) 監視をオーバーライドします。また、**enable cir-monitor** および **disable cir-monitor** コンソール・コマンドを使用して、動的に CIR 監視を使用可能にしたり、使用不可にしたりすることもできます。

輻輳監視

輻輳 (ふくそう) 監視は、インターフェースごとに設定される任意選択フィーチャーで、VC の VIR をネットワークの輻輳 (ふくそう) に応じて変えることができます。VIR は、回線速度の最小 IR と最大 IR の間の値を取ります。デフォルトでは、輻輳 (ふくそう) 監視は使用可能になります。使用不可にするときは **disable congestion-monitor** 構成コマンドを使用し、再び使用可能にするときは **enable congestion-monitor** コマンドを使用します。また、**enable congestion-monitor** お

フレーム・リレーの使用

よび **disable congestion-monitor** コンソール・コマンドを使用して、動的に輻輳 (ふくそう) 監視を使用可能および使用不可にすることもできます。

CIR 監視が使用可能の場合、輻輳 (ふくそう) 監視をオーバーライドします。CIR 監視と輻輳 (ふくそう) 監視の両方とも使用不可にされている場合には、インターフェース上の各 VC の VIR は回線速度に設定され、ネットワーク輻輳 (ふくそう) に応じて減速されません。

注: 圧縮が使用可能の場合であっても、装置は非圧縮サイズのフレームを使用して、VIR が超過しているかどうかを判別します。

輻輳通知と回避

輻輳 (ふくそう) が発生すると、FR バックボーン・ネットワークは、FECN または BECN 信号を送って、送信側と受信側に通知する責任があります。FECN および BECN は、輻輳 (ふくそう) が発生していることを VC の各端の DTE に通知するために、フレーム内に設定されるビットです。FECN は、フレームを受信したのと同じ方向で輻輳 (ふくそう) が発生していることを示します。送信側が輻輳 (ふくそう) の原因になっています。BECN は、この DTE によって送信されたフレームがネットワーク輻輳 (ふくそう) の原因になっていることを示します。

オプションで、ネットワークは CLLM メッセージを使用して、PVC の輻輳 (ふくそう) 情報を伝えることができます。CLLM メッセージは、輻輳 (ふくそう) の発生源にのみ送信され、DTE は BECN メッセージと同様に処理する必要があります。

459ページの図25 の例は、フレームがルーター X からルーター Y に送信される場合の、スイッチ B における輻輳 (ふくそう) 状態を示しています。FR バックボーン・ネットワークは、ルーター X に送信するフレームに BECN ビットをセットして、送信するフレームが輻輳 (ふくそう) に遭遇していることをルーター X に通知します。また、FR バックボーン・ネットワークはルーター Y に対しても、FECN ビットをセットして、それが受信するフレームが輻輳 (ふくそう) に遭遇していることを通知します。

ルーターが BECN の入っているフレームを受信した場合、CIR 監視または輻輳 (ふくそう) 監視のいずれかが使用可能のときは、ルーターは VC の VIR (可変情報速度) を減速する責任があります。ルーターは、最小 IR に達するか、BECN のないフレームが到着するまで、BECN が入っている連続フレームを受信している間、徐々に減速します。FR スイッチは、輻輳 (ふくそう) 限界値に達すると複数のフレームに BECN をセットすることがしばしばあります。ネットワークが複数のフレームに BECN をセットしている場合、FR がネットワーク輻輳 (ふくそう) に対して過剰に反応するのを回避するために、FR は VC の VIR を多くても毎秒 1 回に減らします。これによって、VIR は徐々に減少します。BECN のない連続フレームを受信するようになったら、VIR を最大 IR まで徐々に加速します。

FR ネットワークの運用によっては、装置が FECN を受信した場合、装置は VC の VIR を減速して、ネットワークに送られるトラフィックの全体量をできるだけ速やかに最小化することが必要になる場合があります。ネットワーク上の全体的な負荷を削減すると、輻輳 (ふくそう) を緩和するためにすべての VC で廃棄されるパケットの数を減らすことができます。CIR または輻輳 (ふくそう) 監視オプションと合わせて、**throttle-transmit-on-fecn** パラメーターを使用可能にすると、装置は FECN を

BECN と同様に扱うので、輻輳 (ふくそう) 通知を受け取ったときに、全体的な FR ネットワーク輻輳 (ふくそう) を軽減することができます。 `throttle-transmit-on-fecn` パラメーターは、入力と出力の両方について、専用のバッファを提供しない待ち行列化方式を採用している FR ネットワークでのみ使用してください。

`throttle-transmit-on-fecn` が使用可能の場合、FR は各 BECN または FECN を受信するたびに、VC の VIR を多くても毎秒 1 回に減らします。

一部の FR ネットワーク・スイッチは、輻輳 (ふくそう) を通知するために FECN をセットしますが、BECN はセットしません。輻輳 (ふくそう) の発生元に輻輳 (ふくそう) 通知を提供したい場合、`notify-fecn-source` パラメーターを使用可能にすると、装置は FECN を受信した VC を介して送信するフレームに BECN をセットします。このアクションは、ネットワーク輻輳 (ふくそう) の原因になっている装置に、その VC の VIR を減速するように知らせる信号を提供します。

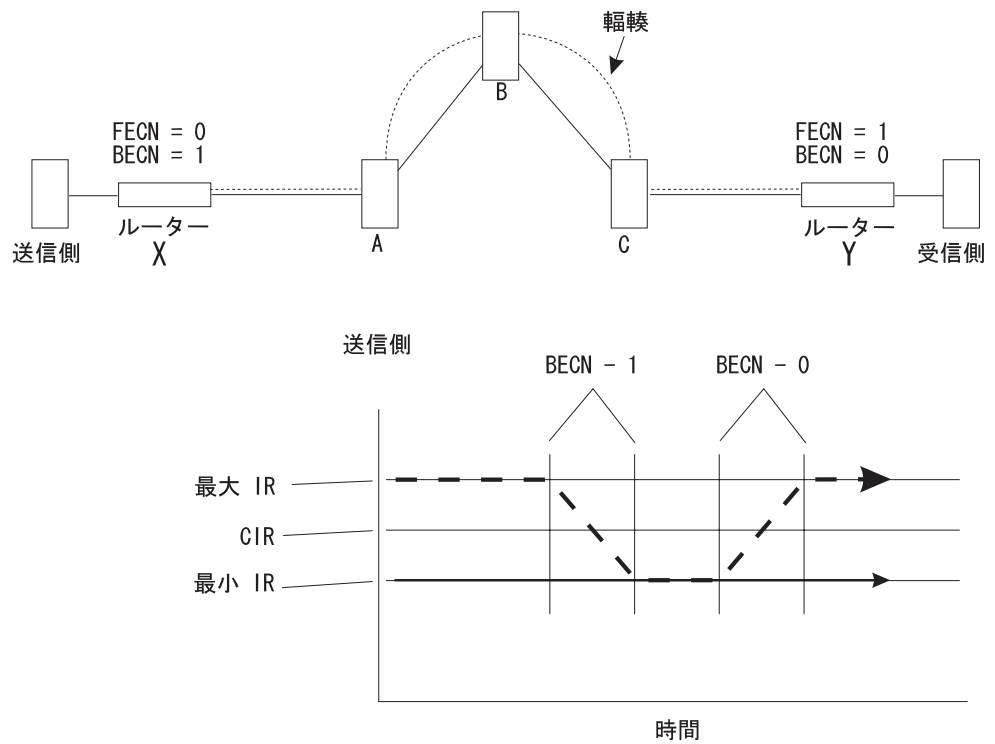


図 25. 輻輳通知と減速

注: 輻輳 (ふくそう) が発生したときに 2 つのエンド・ステーション間に複数の DLCI が構成されている場合、最初の DLCI 上の輻輳 (ふくそう) 状態が解決されるまで、第 2 の DLCI を使用すれば、より高いスループットでデータを転送できる可能性があります。

同様に、ネットワークの提供者が CLLM をサポートしている場合、CLLM メッセージに入っている PVC の伝送速度を減速するようにフレーム・リレーを構成することができます。CLLM メッセージには、報告されている問題のタイプと重大度を示す原因符号が入っています。装置の反応は、原因符号および CLLM メッセージ内の各 PVC に構成されている CIR によって異なります。装置が受け取る CLLM メッセージの内容とそれに対する反応は、次のとおりです。

フレーム・リレーの使用

- 短期的状態を受け取り、PVC に構成されている CIR が非ゼロの場合、フレーム・リレー・プロトコルは、該当する PVC の伝送速度を、構成された IR 減分率で減速します。
- 長期的状態を受け取った場合、フレーム・リレー・プロトコルは、該当する PVC の伝送速度を、計算された最小情報速度に設定します。
- ファシリティーまたは装置の障害あるいは保守作業を受信した場合、または CIR がゼロに構成されていた場合、FR プロトコルは、該当する PVC への待ち行列データの転送は続けますが、輻輳 (ふくそう) 状態が解消されるまでは、高位レイヤー・プロトコルからの発信パケットは受け付けません。

ある PVC の CLLM メッセージを受信した後、装置が T_y タイマーの期間内に CLLM メッセージまたは BECN を受信しない場合、あるいは BECN を含まないフレームを受信した場合、装置は輻輳 (ふくそう) 状態が解消されたものと見なし、徐々に PVC を構成された伝送速度に戻します。輻輳 (ふくそう) 制御のために CLLM を使用している場合は、他の用途のために DLCI 1007 を構成してはなりません。

フレーム・リレーを介する帯域幅予約

フレーム・リレーを介する帯域幅予約については、フィーチャーの使用と構成の『帯域幅予約および優先待ち行列の使用』および『帯域幅予約の構成と監視』を参照してください。

インターフェース上で断片化が使用可能にされている場合は、帯域幅予約システム (BRS) は、データ・フレーム断片を優先順位付けするように構成する必要があります。『フレーム・リレー・インターフェースを介する断片化』を参照してください。

フレーム・リレー・インターフェースを介する断片化

フレーム・リレーを介する音声 (VoFR) は、フレーム・リレー回線を通じて音声パケットを送信する方式です。フレーム・リレー回線を使用してリアルタイム (音声) とデータ・トラフィックの両方を搬送することを計画している場合、リンクが比較的低速 (たとえば、64Kbps) の場合は特に、その回線がデータ・トラフィックを断片化するように構成する必要があります。音声をサポートしていないインターフェースが音声をサポートするインターフェースと交換する場合は、前者のインターフェース上の回線でも断片化が必要になります。

エンド・エンドおよびインターフェース (または UNI/NNI) の 2 つのタイプの断片化があります。インターフェース・レベルの断片化は、主要なフレーム・リレー・スイッチのベンダーでは実装されていないので、フレーム・リレー・サービス提供者から用意されていません。フレーム・リレー実装合意 FRF.12 に従い、エンド・エンド断片化は、PVC でのみサポートされています。したがって、音声サポートをもつインターフェースは、SVC ではなく、フレーム・リレー PVC をサポートするのに使用できます。

断片サイズを構成することができます。断片サイズは、インターフェース間で交渉または通信されることがないので、2 つの相互接続された PVC について異なる場合があります。断片サイズは、リンクのアクセス速度、PVC の CIR、およびこのインタ

一フェースが実際にリアルタイム・データを搬送しているのか、リアルタイム・データを搬送するインターフェースをもつ別のルーターと通信しているかに応じて、リンクまたは PVC によって異なることがあります。フレーム・リレーを介する音声の断片化を構成するときに考慮するその他の要因には、認定バースト・サイズ、BRS トラフィック・クラスと待ち行列の深さ (BRS が構成されている場合)、作成されたグローバル・バッファの数、および各インターフェースに割り振られた受信バッファの数が含まれます。

断片化に関連するオーバーヘッドのため、断片サイズはできるだけ大きく保持し、しかも高品質のリアルタイム・データ通信を維持するのが最善です。

回線がリアルタイム・データを伝送する場合、そのインターフェースおよび回線上でフレーム・リレー断片化に加えて帯域幅予約システム (BRS) を構成する必要があります。BRS を使用可能にすると、リアルタイム・データに他のデータより高い優先順位を与えることができます。その結果、リアルタイム・データを、断片化された他のデータの間インターリーブすることができるので、リアルタイム・データの待ち行列遅延を最小化することができます。

BRS が必要とされるのは、実際にリアルタイム・データおよびその他のデータを送信中の回線のみです。インターフェース上の他の回線、またはリアルタイム・データをサポートするインターフェースと通信している回線は、インターリービングを許可するのに特に BRS サポートは必要としません。

BRS の構成について詳しくは、フィーチャーの使用と構成 中の『帯域幅予約の構成と監視』という章の **assign** コマンドを参照してください。

注: 断片化は、インターフェースまたは回線 (PVC とも呼ばれます) のどちらかのために構成することができます。PVC 用の断片化を構成する場合、

add permanent-virtual-circuit または **change permanent-virtual-circuit** コマンドを使用する必要があります。次の例は、**add permanent-virtual-circuit** コマンドを示しています。

```
FR 1 Config>add perm 18
Committed Information Rate (CIR) in bps [64000]?
Committed Burst Size (Bc) in bits [64000]? 4800
Excess Burst Size (Be) in bits [0]?
Assign circuit name : :? VoFRcircuit1
Is circuit required for interface operation [N]?
Enable circuit for voice forwarding [N]?
Do you want to have end-to-end fragmentation performed [N]? y
Fragment size (50 to 1000) [256]?
Fragmented packet reassembly timer (3 to 10 seconds) [256]?
```

フレーム・リレーを介しての音声転送

フレーム・リレーを介しての音声転送は、音声機能をもつルーターまたは音声機能をもたないルーターが、固有の音声アダプターを使用せずに、フレーム・リレー PVC 間で FRF.11 カプセル化パケット (つまり、音声パケット) を転送することを可能にします。これにより、音声機能をもつルーターは、フレーム・リレー・ネットワークを通じて同じバーチャル・サーキットを介して音声およびデータを多重化することができます。次に、音声転送ルーターは、受信されたデータを、受信されたトラフィックに関連するプロトコル・スタックを使用して発送し、音声トラフィックを

フレーム・リレーの使用

同じまたは別のフレーム・リレー・インターフェースを通じて別の PVC に転送します。典型的な構成では、音声トラフィックはローカルに接続された音声機能をもつ装置に転送されます。

DCE に似た機能ですが、音声パケット転送は、DTE として定義されたバーチャル・サーキットを通じて行なわれます。PVC で音声転送が許可されるのは、フレーム・リレーを介する音声は PVC 専用をサポートされている場合だけです。

音声パケット転送に使用される PVC は、構成を通じてそのようにできるようにする必要があります。実際、異なっていると想定されるフレーム・リレー・インターフェース上のペアの PVC は、相互に音声パケットを転送するよう定義する必要があります。PVC を音声転送用に使用可能にするには、PVC が音声パケットを転送する必要がある PVC のネット番号と DLCI を提供する必要があります。フレーム・リレーは、音声転送を行うよう定義されたペアの PVC 間ですべての音声パケットを転送します。

フレーム・リレー構成プロンプトの表示

フレーム・リレ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. 構成プロンプト (Config>) で **list devices** コマンドを入力して、ルーターに構成されているインターフェースのリストを表示する。
3. **network** コマンドを入力して、フレーム・リレー構成プロンプトを表示する。ネットワーク番号は、フレーム・リレー・インターフェースの番号です。

```
Config>network
What is the network number [0] 2
Frame Relay user configuration
FR 2 Config>
```

4. フレーム・リレー・インターフェース構成プロンプト (FR Config>) で、本章で説明するコマンドを使用して、フレーム・リレー・パラメーターを構成する。

フレーム・リレー基本構成手順

この節では、フレーム・リレー・プロトコルを立ち上げて実行するのに必要な最小構成ステップについて概説します。詳しい構成情報および説明が必要な場合は、本章の構成コマンドの説明箇所を参照してください。

注: 新しい構成変更を有効にするためには、ルーターをリスタートする必要があります。

- **FR マネージメントを選択する。** FR ローカル管理インターフェース (LMI) プロトコルは、デフォルトでは ANSI になります。中間 LMI (REV1)、ANSI T1.617 付録 D マネージメント、または ITU-T/CCITT Q.933 付録 A マネージメントを使用するネットワークに接続するオプションが提供されています。 **enable** および **set** コマンドを使用して、必要なマネージメントを使用可能にしたり、設定したりしてください。
- **PVC を追加する。** FR マネージメントが使用不可のとき、またはオーファン回線が使用不可のときに必要な必須 PVC を追加します。 FR PVC を介してブリッジ

したい場合、または FR PVC を介して APPN を実行したい場合には、その PVC も構成する必要があります。 **add permanent-virtual-circuit** コマンドを使用してください。

- **FR あて先アドレスを構成する。** FR インターフェースを介して IP または IPX のようなプロトコルを実行しており、FR 上のアドレス解決プロトコル (ARP) または逆 ARP をサポートしない装置と接続している場合、**add protocol-address** コマンドを使用して、静的プロトコルとアドレス・マッピングを追加します。
- **フレーム・リレー上の帯域幅予約を構成する。** 必須の基本フレーム・リレー構成に加えて、フレーム・リレー上の帯域幅予約 (オプション機能) も構成することができます。帯域幅予約の構成については、**フィーチャーの使用と構成** の帯域幅予約および優先待ち行列の使用を参照してください。
- **廃棄可能性を構成する。** 帯域幅予約を使用する際の廃棄可能性 (DE) 輻輳 (ふくそう) 制御を構成することができます。廃棄可能性の構成については、**フィーチャーの使用と構成** の帯域幅予約および優先待ち行列の使用を参照してください。
- **データ圧縮を構成する。** フレーム・リレーに対するデータ圧縮を構成することができます。データ圧縮の構成については、**フィーチャーの使用と構成** のデータ圧縮の構成と監視を参照してください。
- **データ暗号化を構成する。** フレーム・リレーに対するデータ暗号化を構成することができます。データ暗号化の構成については、**フィーチャーの使用と構成** のデータ暗号化の使用と構成を参照してください。

フレーム・リレー PVC マネージメントの使用可能化

フレーム・リレーのもとには 3 つのマネージメント・オプションがあります。

- インターリム・ローカル管理インターフェース 改訂 1
- ANSI T1.617 付録 D マネージメント
- ITU-T/CCITT Q.933 付録 A マネージメント

フレーム・リレーのデフォルトでは、ANSI が使用可能になります。マネージメント・タイプを変更したい場合、あるいは ANSI マネージメントを再び使用可能にしたい場合は、以下の手順で行います。フレーム・リレー上のマネージメントを使用可能にするには、2 つのステップで行います。

1. FR Config> プロンプトで **enable lmi** コマンドを入力して、マネージメント・アクティビティを使用可能にする。
2. **set lmi-type** コマンドを入力して、そのインターフェースのマネージメントのタイプを選択する。

set コマンドで利用可能なマネージメント・タイプについての詳細は、表60 を参照してください。

これらのマネージメント・タイプの設定方法の例を、表の後に示してあります。詳細については、この章の **enable** および **set** コマンドの節も参照してください。

表 60. フレーム・リレー・マネージメント・オプション

コマンド	オプション	説明
set	lmi-type rev1	LMI 改訂 1 (Stratacom のフレーム・リレー・インターフェース仕様) に準拠します。

フレーム・リレーの使用

表 60. フレーム・リレー・マネージメント・オプション (続き)

コマンド	オプション	説明
set	lmi-type ansi	ANSI T1.617 ISDN-DSS1-Signalling Specification for Frame Relay Bearer Service (付録 D と呼ばれます) に準拠します。
set	lmi-type ccitt	ITU-T/CCITT 勧告 Q.933 の付録 A - DSS1 Signalling Specification for Frame Mode Basic Call Control に準拠します。

例: **enable lmi**
 set lmi-type ansi

フレーム・リレー SVC マネージメントの使用可能化

SVC が使用可能にされていると、フレーム・リレー SVC マネージメントは自動的に使用可能にされます。

第29章 フレーム・リレー・インターフェースの構成および監視

この章では、フレーム・リレ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。本章には、以下の節が含まれています。

- 『フレーム・リレー構成コマンド』
- 500ページの『フレーム・リレー監視プロンプトへのアクセス』
- 500ページの『フレーム・リレー監視コマンド』
- 515ページの『フレーム・リレー・インターフェースおよび GWCON インターフェース・コマンド』

注: フレーム・リレー上の帯域幅予約の監視については、フィーチャーの使用と構成の帯域幅予約の構成と監視を参照してください。

フレーム・リレー構成コマンド

この節では、フレーム・リレー構成コマンドについて説明します。コマンドはすべて `Frame Relay n>` プロンプトで入力します。ここで、*n* はインターフェース番号を表します。`Frame Relay n>` プロンプトにアクセスするには、次のステップを実行します。

1. `OPCON` プロンプト (*) で **talk 5** と入力する。
2. `GWCON` プロンプト (+) で、**interface** コマンドを入力して、ルーター上に構成されているインターフェースのリストを表示する。
3. 構成するフレーム・リレー・インターフェースを選択する。
4. **exit** と入力する。
5. `OPCON` プロンプト (*) で **talk 6** と入力する。
6. `Config>` プロンプトで、**network** コマンドに続けて、フレーム・リレー・インターフェースのネットワーク番号を入力します。たとえば、次のように入力します。

```
Config> net 2
Frame Relay user configuration
FR 2 Config>
```

新しい構成変更を有効にするためには、ルーターをリスタートする必要があります。表61 は、コマンドを示しています。

表61. フレーム・リレー構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Add	PVC、必須 PVC グループ、SVC、およびあて先プロトコル・アドレスを、フレーム・リレー・インターフェースに追加します。
Change	以前に add コマンドによって定義された PVC、SVC、または必須 PVC グループを変更します。
Disable	使用可能にされたフレーム・リレー・フィーチャーを使用不可にします。

フレーム・リレー・インターフェースの構成

表 61. フレーム・リレー構成コマンドの要約 (続き)

コマンド	機能
Enable	回線監視、マネージメント・オプション、マルチキャスト、プロトコル・ブロードキャスト、断片化、およびオーファンなどのフレーム・リレー・フィーチャーを使用可能にします。
List	LMI、PVC、必須 PVC グループ、SVCs、HDLC 情報、およびプロトコル・アドレスの現行構成を表示します。
LLC	フレーム・リレー・インターフェース上の LLC パラメーターを構成します。これらの LLC パラメーターは、フレーム・リレーを介して APPN を実行するときが必要です。
Remove	以前に追加された PVC、SVC、または必須 PVC グループ (空のとき)、またはプロトコル・アドレスを削除します。
Set	フレーム・リレー・マネージメント・オプションおよびパラメーター (N1-parameter、N2-parameter、N3-parameter、P1 parameter、および T1-parameter) を構成します。FR シリアル・インターフェースの物理レイヤー・パラメーターを構成します。最大フレーム・サイズを設定します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

注: この節では、回線番号 および PVC という用語は、DLCI (データ・リンク回線識別子) という用語と同義です。

Add

add コマンドは、フレーム・リレー・インターフェースによってサポートされる PVC、必須 PVC グループ、またはあて先プロトコル・アドレスを追加するのに使用します。

構文:

```
add                permanent-virtual-circuit . . .  
                    protocol-address . . .  
                    pvc-group . . .  
                    switched-virtual-circuit . . .
```

permanent-virtual-circuit

フレーム・リレー・インターフェースの予約された範囲 0 ~ 15 を超えて PVC を追加します。追加が可能な PVC の最大数は約 992 ですが、インターフェースが実際にサポートできる PVC の数は、各 PVC に必要なスループット、回線速度、インターフェース上で実行されているプロトコルのタイプ、および最大フレーム・サイズに収めることができるローカル管理インターフェース PVC 情報要素の数によって決まります。

例:

```
add permanent-virtual-circuit  
Circuit Number [16]?  
Committed Information Rate (CIR) in bps [64000]?  
Committed Burst Size (Bc) in bits [64000]?  
Excess Burst Size (Be) in bits [0]?  
Assign Circuit name []?  
Is circuit required for interface operation [N]?y  
Does the circuit belong to a required PVC group [N]? y  
What is the group name []? group1  
Do you want to have data compression performed [Y]?
```

フレーム・リレー・インターフェースの構成

```
Do you want to have end-to-end fragmentation performed [Y]?
Fragment size (50 to 8190) [256]?
Fragmented packet reassembly timer (3 to 10 seconds) [3]?
Enable circuit for voice forwarding [N]? y
Network number of voice forwarding PVC [0]?
Circuit number of voice forwarding PVC [16]?
Do you want to have data encryption performed [N]? y
Should the encryption algorithm be CDMF (CDMF) or triple-DES (3DES) [CDMF]?
Data encryption requires a key that is 16 hexadecimal characters long for CDMF,
48 hexadecimal characters long for 3DES.
```

You will be asked to enter the key twice for security reasons

Please enter the key for the first time now

A valid encryption key has been entered

Please confirm the key by entering it again

The encryption keys match - the key has been accepted

Circuit Number

この PVC の回線番号を示します。

有効値: 16 ~ 1007

Committed Information Rate

認定情報速度 (CIR) を示します。CIR は、0、または 300 bps ~ 2 048 000 bps の範囲の値のいずれかにすることができます。詳しくは、454ページの『認定情報速度 (CIR)』を参照してください。最大値は、インターフェースに構成されているデフォルト CIR の値です。

注: デフォルト値は、インターフェース・レベルで設定される CIR デフォルトに従って決定されます。

Committed Burst Size

ネットワークで合意されている、認定バースト (Bc) サイズ/CIR 秒数に相当する測定期間に送達できる最大データ量 (ビット)。範囲は 300 ~ 2 048 000 ビットです。最大値は、インターフェースに構成されているデフォルトの認定バースト値です。

注:

1. デフォルト値は、インターフェース・レベルで設定された Bc デフォルトに従って決定されます。
2. CIR が 0 として構成されている場合、認定バースト・サイズも 0 に設定され、値の入力を求めるプロンプトは出ません。詳しくは、454ページの『認定バースト (Bc) サイズ』を参照してください。

Excess Burst Size

(認定バースト・サイズ/CIR) 秒数に相当する測定期間にネットワークが送達を試みることができる、認定バースト・サイズを超過する未認定データの最大量 (ビット数)。範囲は 0 ~ 2 048 000 ビットです。最大値は、インターフェースに構成されている超過バースト・サイズの値です。詳しくは、455ページの『超過バースト (Be) サイズ』を参照してください。

注: デフォルト値は、インターフェース・レベルで設定される Be デフォルトに従って決定されます。

フレーム・リレー・インターフェースの構成

Assign Circuit Name

PVC を記述するために割り当てられる ASCII スtringを示します。デフォルト値は unassigned (未割り当て) です。

Is the circuit required for operation

その回線がインターフェースの運用に必要であるかどうかを示すために、Y または N を指定します。

Does the circuit belong to a required PVC group

このプロンプトは、必須の回線に対してのみ表示されます。回線が必須 PVC グループに属するかどうかを示すために、Y または N を指定します。

What is the group name

PVC を必須グループに所属するとして定義した場合、必須 PVC グループの名前を指定することができます。疑問符 (?) を入力すると、現在定義されているグループのリストが表示されます。

Do you want to have compression performed

回線がデータ・パケットを圧縮するかどうかを指定することができます。この質問は、インターフェースで圧縮が使用可能にされている場合にのみ出されます。

注: PVC 上の圧縮を使用可能にし、インターフェースの圧縮回線限界を超過した場合、メッセージが出ます。回線上の圧縮は、可能な場合 (つまり、回線がアクティブになったときにアクティブ圧縮限界を超えていなかった場合) に実行されます。圧縮限界には、SVC ならびに PVC に割り振られた圧縮コンテキストの数が含まれます。

Enable circuit for voice forwarding

回線が音声パケットを転送するかどうかを指定することができます。Y (yes) を指定する場合、この PVC が音声フレームを転送する PVC のネットワークおよび回線番号を指定することができます。

Do you want to have end-to-end fragmentation performed

回線が全回線を通じて断片化を実行するかどうかを指定することができます。この質問は、インターフェースでエンド・エンド断片化が使用可能にされている場合にのみ出されます。UNI/NNI 断片化が使用可能にされている場合、このインターフェース上のすべての回線は断片化が自動的に使用可能にされ、この質問は出されません。

断片サイズおよび再組み立てタイマー値を指定するとき、このインターフェース用に構成されたエンド・エンド断片サイズおよび再組み立てタイマー値のデフォルトを上書きすることができます。

Do you want to have data encryption performed

回線がデータ・パケットを暗号化するかどうかを指定することができます。この質問は、インターフェースで暗号化が使用可能にされている場合にのみ出されます。この質問に対して『yes』(または『y』) と応答した場合にのみ、暗号化キーおよびアルゴリズムの入力を求めるプロンプトが出ます。

フレーム・リレー・インターフェースの構成

暗号化キーの指定: 暗号化キー値は、16 進文字で指定する必要があります。

有効値: CDMF では 16、3DES では 48

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

protocol-address

このコマンドは、静的に構成されたあて先プロトコル (プロトコル名) アドレスを、フレーム・リレー・インターフェースに追加します。静的に構成されたあて先プロトコル・アドレスは、逆 ARP も ARP も選択できない場合やセキュリティーの上で役立ちます。プロトコル名とアドレス・マッピング (静的 ARP) を追加するのは、逆 ARP または ARP より非効率的です。

- 逆 ARP は、ブロードキャストせずに動的にアドレス・マッピングを行うので、推奨される効率的な方法です。
- ARP は、逆 ARP を選択できない場合に使用することをお勧めします。これは、アドレスをブロードキャストし、一定の間隔でマッピングを再確認するので、逆 ARP より非効率的です。

このパラメーターでは、追加するプロトコルのタイプによって、異なる情報を求めるプロンプトが出ます。

例:

```
add protocol-address  
Protocol name or number [0]?
```

IP プロトコル:

```
IP Address [0.0.0.0]?  
Circuit Number or name[16]?
```

IPX プロトコル:

```
Host Number (in hex)[]?  
Circuit Number or name[16]?
```

AppleTalk フェーズ 2 プロトコル:

```
Network Number (1-65279) []?  
Node Number (1-253) []?  
Circuit Number or name[16]?
```

DN プロトコル:

```
Node address [0.0]?  
Circuit Number or name[16]?
```

Protocol name or number

追加するプロトコルの名前または番号を定義します。サポートされないプロトコルを指定すると、システムはエラー・メッセージを出して知らせます。

Unknown protocol name, try again

たとえば、次のいずれかを誤って指定している可能性があります。

```
Prot# Name  
0 IP  
4 DN  
7 IPX  
22 AP2
```

フレーム・リレー・インターフェースの構成

サポートされるプロトコル・タイプのリストを見たい場合は、Protocol name or number [IP]? プロンプトで ? を入力します。

IP Address

リモート IP ホストの 32 ビットの IP アドレスを小数点表記法で定義します。

Host Number

リモート IPX ホストの 48 ビット IPX ノード・アドレスを定義します。

Network Number

リモート AppleTalk ホストの AppleTalk フェーズ 2 ネットワーク番号を定義します。

Node Number

リモート AppleTalk ホストに接続されているインターフェースのノード番号を定義します。

Node address

リモート DECnet ホストの DECnet ノード・アドレスを定義します。ノード・アドレスは *x.y* フォーマットで構成します。ただし、*x* は 6 ビットのエリア・アドレスで、*y* は 10 ビットのノード番号です。

Circuit Number or name

PVC を DLCI または名前によって定義するか、SVC を、このリモート・プロトコル・アドレスが対応付けられている名前によって定義します。

pvc-group *groupname*

必須 PVC グループ名を追加します。

注: SVC は、必須 PVC グループに属していない場合があります。

switched-virtual-circuit

スイッチド・バーチャル・サーキット (SVC) を追加します。SVC の動作は PVC と似ていますが、SVC の帯域幅は、SVC がアクティブな場合のみ、FR ネットワークによって動的に割り振られる点が異なります。追加できる SVC の数は、数が各回線に要求されるスループット、回線速度などによって決まるという点で、追加できる PVC の数に似ています。ただし、SVC の帯域幅が予約されるのは、SVC がアクティブである場合に限られるので、インターフェースを経由して、PVC より多くの SVC をサポートすることが可能です。

```
FR 4 Config>add switched-virtual-circuit
Circuit name []? svc01
Remote party number []? 12345
Remote party number numbering plan (E.164 or X.121) [E.164]?
Remote party number type (Unknown or International) [International]?
Remote party subaddress in hexadecimal []? 01
Remote party subaddress format (private or NSAP) [private]1?
Requested outgoing Committed Information Rate (CIR) in bps [64000]?
Minimum acceptable outgoing Committed Information Rate (CIR) in bps [64000]?
Requested incoming Committed Information Rate (CIR) in bps [64000]?
Minimum acceptable incoming Committed Information Rate (CIR) in bps [64000]?
Requested outgoing Committed Burst size (Bc) in bits [64000]?
Requested incoming Committed Burst size (Bc) in bits [64000]?
Requested outgoing Excess Burst size (Be) in bits [0]?
Requested incoming Excess Burst size (Be) in bits [0]?
Idle timer in seconds [60]?
```


フレーム・リレー・インターフェースの構成

Establish circuit to learn remote protocol addresses [Y]?
Is multicast required for this circuit [Y]?
Are call-ins allowed for this circuit [Y]?

Circuit name

SVC の回線名を指定します。この名前は、コールをプロトコルと BRS 定義の両方に対応付けるのに使用し、回線番号の代わりに接続を識別するのに使用します。

有効値: 1 ~ 32 文字の ASCII 文字列

デフォルト値: 名前が必須であり、このインターフェースについて固有である必要があります。

Remote party number

リモートあて先のフレーム・リレー・アドレスを指定します。

有効値: 10 進数の 1 ~ 20 文字の文字列

デフォルト値: なし

Remote party numbering plan

リモート側の番号の形式を指定します。番号計画は、FR ネットワークによって使用されるものに一致している必要があります。

有効値: E.164 (ISDN) または X.121 (Data)

デフォルト値: E.164

Remote party number type

あて先のフレーム・リレー・パーティー番号タイプを指定します。番号タイプは、FR ネットワークによって使用されるものに一致している必要があります。

有効値: International または Unknown

デフォルト値: International

Remote party subaddress

あて先ノード内のパーティー・エンティティ (たとえば、プロトコル) を指定します。サブアドレスが使用される場合は、これはリモート装置のサブアドレスに照合されます。接続の両端のサブアドレスは、同じである必要があります。

リモート・パーティーのサブアドレスは、以下のようになります。

- NSAP

入力される数字の数は、偶数で、X'0' ~ X'F' の範囲にある必要があります。

- 私設

符号化が BCD である場合には、0 ~ 9 の範囲の奇数の数字を入力することができます。

符号化が BCD でない場合には、X'0' ~ X'F' の範囲の偶数の数字を入力することができます。

remote party number と **remote party subaddress** の組み合わせは、このインターフェース上で固有である必要があります。2 つのルーター・インターフェース間の平行接続が必要である場合、

フレーム・リレー・インターフェースの構成

各スイッチド・バーチャル・コネクションの定義を固有に識別するには、サブアドレスを使用する必要があります。

有効値: 1 ~ 40 文字の16 進数文字列

デフォルト値: なし

Requested outgoing throughput (CIR)

要求される発信 CIR を指定します。ネットワークはこの帯域幅 (使用可能な場合) を提供します。

有効値: CIR は、0、または 300 bps ~ 2 048 000 bps の範囲の値のいずれかにすることができます。

注: HSSI アダプター上の FR インターフェースの有効値は 0 または 300 ~ 52 000 000 です。

デフォルト値: デフォルト値は、インターフェース・レベルでの CIR デフォルトによって決まります。

Minimum acceptable outgoing Committed Information Rate (CIR)

ネットワークが要求された CIR を提供できない場合に受け入れられる、最小 CIR を指定します。

有効値: CIR は、0、または 300 bps ~ 2 048 000 bps の範囲の値 (最大値は **requested outgoing throughput (CIR)**) のいずれかです。

注: HSSI アダプター上の FR インターフェースの有効値は 0 または 300 ~ 52 000 000 です。

デフォルト値: デフォルト値は、インターフェース・レベルでの CIR デフォルトによって決まります。

Requested incoming CIR

要求された着信 CIR を指定します。

有効値: CIR は 0 または 300 bps ~ 2 048 000 bps の範囲の値のいずれかにすることができます。

注: HSSI アダプター上の FR インターフェースの有効値は、0 または 300 ~ 52 000 000 です。

デフォルト値: **requested outgoing CIR** の値

Minimum acceptable incoming Committed Information Rate (CIR)

ネットワークが要求された CIR を提供できない場合に受け入れられる、最小 CIR を指定します。

有効値: CIR は、0 または 300 bps ~ 2 048 000 bps の範囲の値 (最大値は **requested incoming CIR**) のいずれかにすることができます。

注: HSSI アダプター上の FR インターフェースの有効値は、0 または 300 ~ 52 000 000 です。

デフォルト値: **minimum acceptable outgoing CIR** と同じ

フレーム・リレー・インターフェースの構成

Requested outgoing committed burst size (Bc)

要求される発信認定バースト・サイズを指定します。

有効値: CIR は 0 または 300 bps ~ 2 048 000 bps の範囲の値のいずれかにすることができます。

注: HSSI アダプター上の FR インターフェースの有効値は、0 または 300 ~ 52 000 000 です。

デフォルト値: インターフェース・レベルでの CIR デフォルトによって決まる値

Requested incoming committed burst size (Bc)

要求される着信認定バースト・サイズを指定します。

有効値: CIR は、0、または 300 bps ~ 2 048 000 bps の範囲の値のいずれかにすることができます。

注: HSSI アダプター上の FR インターフェースの有効値は、0 または 300 ~ 52 000 000 です。

デフォルト値: requested outgoing Bc に等しい値

Outgoing excess burst size (Be)

要求される発信バースト・サイズを指定します。

有効値: CIR は、0、または 300 bps ~ 2 048 000 bps の範囲の値のいずれかにすることができます。

注: HSSI アダプター上の FR インターフェースの有効値は、0 または 300 ~ 52 000 000 です。

デフォルト値: インターフェース・レベルでの CIR デフォルトによって決まる値

Requested incoming excess burst size (Be)

要求される着信超過バースト・サイズを指定します。

有効値: CIR は、0、または 300 bps ~ 2 048 000 bps の範囲の値のいずれかにすることができます。

注: HSSI アダプター上の FR インターフェースの有効値は、0 または 300 ~ 52 000 000 です。

デフォルト値: requested outgoing excess burst size (Be) と同じ

Idle timer

トラフィックがないときに、SVC がアクティブのままの時間枠を指定します。0 に指定すると、この SVC を、それにデータが最初に到着するときに設定され、それを介してトラフィックが流れない場合でも切断されない固定回線として指定することになります。

有効値: 0 ~ 65535 秒

デフォルト値: 60

フレーム・リレー・インターフェースの構成

Establish circuit to learn remote protocol addresses

隣接ノードのプロトコル・アドレスを確認するためにインターフェースが起動するとき、この SVC を設定する必要があるかどうかを指定します。このオプションは、静的に構成されたあて先プロトコルの名前の代わりに使用することができ、IP、IPX、Appletalk2、および DECnet IV など動的アドレス・ディスカバリーをサポートして、ルーターに、指示された InARP を介してリモート装置に関連付けられたプロトコル・アドレスを確認させるプロトコルにあてられます。このオプションを使用すると、ARP ブロードキャストを削減するのに役立ちます。プロトコル・アドレスが確認されると、SVC を切断するのにアイドル・タイマーが使用されます。

有効値: yes または no

デフォルト値: yes

Is multicast required for this circuit

このインターフェース上でマルチキャスト・パケットを送信するためにこの SVC を使用する必要があるかどうか (そのようにするために SVC を設定することを意味する場合であっても) を指定します。SVC を介してマルチキャストを要求しないようにするために静的ルートを使用して、ルーティング情報を交換するためだけに SVC が設定されることがないようにすることができます。

有効値: yes または no

デフォルト値: インターフェース・レベルでのマルチキャスト・エミュレーション設定に応じたデフォルト

Are call-ins allowed

このリモート DTE からのコール・インを受け入れる必要があるかどうかを指定します。no を指定すると、特定のユーザーからのコール・インを妨害して、コール・イン/コール・アウトの競争状態を解消することができます。

有効値: yes または no

デフォルト値: yes

Compression capable

フレーム・リレー圧縮がサポートさ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: 圧縮がインターフェースに使用可能にされている場合は、yes。それ以外の場合は、no。

Encryption capable

回線がデータ・パケットを暗号化するかどうかを指定することができます。この質問は、インターフェースで暗号化が使用可能にされている場合にのみ出されます。暗号化キーおよびアルゴリズムの入力を求めるプロンプトが出るのは、SVC 上で暗号化をアクティブにしている場合のみです。

暗号化キーの指定: 暗号化キー値は、16 進文字で指定する必要があります。

有効値: CDMF では 16、3DES では 48

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

Change

change permanent-virtual-circuit コマンドは、以前に **add permanent-virtual-circuit** コマンドを使用して追加された PVC を変更するのに使用します。エンド・エンド・タイプの断片化を使用する場合は、**change permanent-virtual-circuit** コマンドを使用して、エンド・エンド断片化が行なわれる PVC を指定します。

構文:

```
change                permanent-virtual-circuit . . .
                        switched-virtual-circuit . . .
```

例:

```
change permanent-virtual-circuit
Circuit Number [16]?
Committed Information Rate in bps [64000]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign Circuit Name: []?
Is the circuit required for interface operation [N]?
Does the circuit belong to a required PVC group [N]?
Do you want to have data compression performed [Y]?
Do you want end-to-end fragmentation performed on this circuit [Y]?
Fragment size (50 to 8190) [256]?
Fragmented packet reassembly timer (3 to 10 seconds) [3]?
Do you want to have data encryption performed [N]?
Enable circuit for voice forwarding [N]?
```

permanent virtual circuit

断片化パラメーターを除くパラメーターの説明については、466 ページの **add permanent-virtual-circuit** コマンドを参照してください。これらは、**enable fragmentation** コマンドで説明されています。

switched-virtual-circuit

```
FR 4 Config>change switched-virtual-circuit
Circuit name []? svc01
Remote party number []? 12345
Remote party number numbering plan (E.164 or X.121) [E.164]?
Remote party number type (Unknown or International) [International]?
Remote party subaddress in hexadecimal []? 01
Remote party subaddress format (private or NSAP) [private]?
Requested outgoing Committed Information Rate (CIR) in bps [64000]?
Minimum acceptable outgoing Committed Information Rate (CIR) in bps [64000]?
Requested incoming Committed Information Rate (CIR) in bps [64000]?
Minimum acceptable incoming Committed Information Rate (CIR) in bps [64000]?
Requested outgoing Committed Burst size (Bc) in bits [64000]?
Requested incoming Committed Burst size (Bc) in bits [64000]?
Requested outgoing Excess Burst size (Be) in bits [0]?
Requested incoming Excess Burst size (Be) in bits [0]?
Idle timer in seconds [60]?
Establish circuit to learn remote protocol addresses [Y]?
Is multicast required for this circuit [Y]?
Are call-ins allowed for this circuit [Y]?
```

パラメーターの説明については、470 ページを参照してください。

Disable

disable コマンドは、以前に **enable** コマンドを使用して使用可能にしたフィーチャーを使用不可にするのに使用します。

構文:

```
disable
    cir-monitor
    cllm
    compression
    congestion-monitor
    dn-length-field
    encryption
    fragmentation
    lmi
    lower-dtr
    multicast-emulation
    no-pvc
    notify-fecn-source
    orphan-circuits
    protocol-broadcast
    switched-virtual-circuits
    throttle-transmit-on-fecn
```

cir-monitor

IS (情報分離)このフィーチャーを使用不可にすると、回線の情報速度は、**add permanent-virtual-circuit** または **add switched-virtual-circuit** コマンドを用いて構成されたパラメーターを使用して計算された最大情報速度を超えることが許されます。このフィーチャーのデフォルト設定は、使用不可です。詳細については、457ページの『回線輻輳』を参照してください。

cllm 装置が CLLM メッセージに応答して減速 するのを使用不可にします。デフォルトは使用不可です。詳細については、457ページの『回線輻輳』を参照してください。

compression

インターフェース上の圧縮を使用不可にします。どの VC でも圧縮は行われなくなります。

congestion-monitor

輻輳 (ふくそう) 監視機能を使用不可にします。この機能を使用不可にすると、回線の情報速度が、輻輳 (ふくそう) に応じて最小情報速度から回線速度までの間で変えられなくなります。詳細については、457ページの『回線輻輳』を参照してください。このフィーチャーのデフォルト設定は、使用可能です。

dn-length-field

フレーム・リレーのフレーム内の DECnet パケットの前に長さフィールドを必要とする DECnet フェーズ IV の実現を、フレーム・リレーを介して相互運用できなくしますが、DECnet パケットの前に長さフィールドを使用しない DECnet フェーズ IV フレーム・リレー・ソフトウェアとの相互運用は許されず、dn-length-field を使用不可にすると、フレーム・リレーは DECnet パケットが入っている転送フレームに長さフィールドを挿入せず、また DECnet パケットが入っている受信フレームからの長さフィールドの除去も試みません。

注: このオプションは、構成オプションとしてのみ提供されています。

encryption

インターフェース上の暗号化を使用不可にします。このインターフェース上の PVC が暗号化が可能であっても、暗号化は行われません。

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

fragmentation

このインターフェースについて断片化をグローバルに使用不可にします。

lmi

このパラメーターを使用不可にすると、実際のネットワークまたは管理インターフェースを使用せずに、通常の運用またはエンド・エンド間のフレーム・リレー・テストを行うことができます。エンド・エンド間のフレーム・リレー・テストの場合は、リンクの両端に同様の PVC (同じ PVC 番号、たとえば、16 と 16 のように) を追加することが必要です。

lower-dtr

このパラメーターは、ルーター上の専用シリアル・ライン・インターフェースのデータ端末レディー (DTR) 信号の扱い方を決めます。フレーム・リレー・ダイヤル回線インターフェースではサポートされません。lower-dtr パラメーターについての詳しい説明は、**enable lower-dtr** コマンドの項を参照してください。

以下のケーブル・タイプがサポートされます。

EIA 232 (RS-232)

V.35

V.36

デフォルト設定値は **disable lower-dtr** です。

multicast-emulation

各アクティブ VC 上のマルチキャスト・エミュレーションを使用不可にします。このフィーチャーのデフォルト設定は、使用可能です。このフィーチャーを使用不可にする場合は、プロトコル静的アドレス・マップを追加する必要があります。

マルチキャスト・エミュレーションが使用不可にされている場合、一部のプロトコル (IPX RIP など) はフレーム・リレー・インターフェース上で機能しません。また、プロトコル・ブロードキャスト (protocol-broadcast) フィーチャーも、正しく機能するためにはマルチキャスト・エミュレーションを必要

フレーム・リレー・インターフェースの構成

とします。詳細については、451ページの『マルチキャスト・エミュレーションとプロトコル・ブロードキャスト』を参照してください。

no-pvc

インターフェースをアクティブと見なすか、非アクティブと見なすかを制御します。no-pvc が使用不可にされている場合、インターフェース上のアクティブ PVC の存在は、フレーム・リレー・インターフェースをアクティブまたは非アクティブのいずれに見なすかには影響を与えません。

notify-fecn-source

ルーターが、FECN ビットがセットされた受信パケットの発信元の装置に最初に送るパケットに BECN ビットをセットするのを使用不可にします。詳細については、457ページの『回線輻輳』を参照してください。

orphan-circuits

インターフェースでのすべての未構成 PVC オーフアン回線の使用を禁止します。オーファン回線のデフォルト設定は、使用可能です。オーファン回線を使用不可にすると、未構成回線からの不許可侵入が防止されるので、ネットワークのセキュリティー手段が追加されます。ただし、オーファン回線を使用不可にする場合は、インターフェースで使用する PVC を追加することが必要になります。

protocol-broadcast

IP RIP のようなプロトコルがフレーム・リレー・インターフェースを介して機能するのを禁止します。詳細については、451ページの『マルチキャスト・エミュレーションとプロトコル・ブロードキャスト』を参照してください。このフィーチャーのデフォルト設定は、使用可能です。

switched-virtual-circuits

SVC の使用を禁止します。

throttle-transmit-on-fecn

FECN ビットがオンにセットされているパケットに応答して、装置がパケットの転送を減速 するのを禁止します。デフォルトは使用不可です。詳細については、457ページの『回線輻輳』を参照してください。

Enable

enable コマンドは、フレーム・リレー・フィーチャーを使用可能にするのに使用します。

構文:

```
enable                cir-monitor
                        cllm
                        compression
                        congestion-monitor
                        dn-length-field
                        encryption
                        fragmentation
```


フレーム・リレー・インターフェースの構成

lmi

lower-dtr

multicast-emulation

notify-fecsn-source

no-pvc

orphan-circuits

protocol-broadcast

switched-virtual-circuits

throttle-transmit-on-fecsn

cir-monitor

回線監視フィーチャーを使用可能にします。回線監視フィーチャーは、**add permanent-virtual-circuit** コマンドまたは **change permanent-virtual-circuit** コマンドで構成されたパラメーターを用いて計算された最小情報速度と最大情報速度の間で、回線の情報速度を変化させます。

注: 輻輳 (ふくそう) が存在するときは、回線監視フィーチャーは輻輳 (ふくそう) 監視フィーチャーをオーバーライドします (両方のフィーチャーが使用可能にされている場合)。このフィーチャーのデフォルト設定は、使用不可です。

CIR 監視について詳しくは、457ページの『CIR の監視』を参照してください。

注: データ圧縮を実行している回線のスループットを最大化するために、圧縮を使用可能にしたのと同じインターフェースでは、CIR 監視を使用可能にすべきではありません。装置は PVC の VIR を超過しているかどうかを調べる際には未圧縮サイズのフレームを使用しますが、圧縮されたフレームはそれより少ない帯域幅しか必要としないので、装置が監視を厳重に実施して構成済み CIR を超過しないようにすると、PVC の CIR が十分に活用されないこととなります。代わりに、輻輳 (ふくそう) 監視を使用して、装置が FR ネットワークから送られた輻輳 (ふくそう) 表示に反応できるようにすれば、フレームの損失を回避できます。

cllm 装置が CLLM メッセージに応答して減速 するのを使用可能にします。このサポートが利用可能かどうかについては、FR ネットワークの提供者に尋ねてください。詳細については、457ページの『回線輻輳』を参照してください。

compression

インターフェース上の圧縮を使用可能にします。コンテキストが利用可能であり、アクティブ圧縮回線限界を超えていない場合、インターフェース上のすべての圧縮可能 VC がデータ・パケットを圧縮できます。(詳細については、フィーチャーの使用と構成 のデータ圧縮の構成と監視を参照してください。)

注: データ圧縮を実行している回線のスループットを最大化するために、圧縮を使用可能にしたのと同じインターフェースでは、CIR 監視を使用可能

フレーム・リレー・インターフェースの構成

にすべきではありません。装置は VC の VIR を超過しているかどうかを調べる際には未圧縮サイズのフレームを使用しますが、圧縮されたフレームはそれより少ない帯域幅しか必要としないので、装置が監視を厳重に実施して構成済み CIR を超過しないようにすると、VC の CIR が十分に活用されないこととなります。代わりに、輻輳 (ふくそう) 監視を使用して、装置が FR ネットワークから送られた輻輳 (ふくそう) 表示に反応できるようにすれば、フレームの損失を回避できます。

congestion-monitor

輻輳 (ふくそう) 監視フィーチャーを使用可能にします。このフィーチャーは、回線の情報速度を輻輳 (ふくそう) に応じて最小情報速度から回線速度までの間で変化させることができます。

注: 輻輳 (ふくそう) が存在するときは、回線監視フィーチャーは輻輳 (ふくそう) 監視フィーチャーをオーバーライドします (両方のフィーチャーが使用可能にされている場合)。このフィーチャーのデフォルト設定は、使用可能です。

輻輳 (ふくそう) 監視についての詳細は、457ページの『輻輳監視』を参照してください。

dn-length-field

フレーム・リレーのフレーム内の DECnet パケットの前に長さフィールドを必要とする DECnet フェーズ IV の実現を、フレーム・リレーを介して相互運用することをサポートします。dn-length-field を使用可能にすると、フレーム・リレーは DECnet パケットが入っている転送フレームに長さフィールドを挿入し、また DECnet パケットが入っている受信フレームからの長さフレームを除去します。このオプションは、デフォルトでは使用不可になります。デフォルトでは、フレーム・リレーは長さフィールドの挿入も除去も行いません。

注: このオプションは、ルーター・ソフトウェアに DECnet フェーズ IV プロトコルが含まれている場合に、構成オプションとしてのみ提示されません。

encryption

インターフェース上の暗号化を使用可能にします。暗号化が使用可能として構成されているすべての VC が、すべての転送データを暗号化します。

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

fragmentation *fragmentation-type fragment-size fragmented packet-reassembly-timer*

インターフェース上で断片化を使用可能にします。回線上の断片化は、断片化サイズより大きいフレームを小さい断片に分割し、個別のフレームとして伝送させます。エンド・エンド断片化が使用可能にされる場合、断片サイズより小さいフレームは断片化ヘッダーを付けて送信されず、他のフレームの断片の間にインターリーブすることができます。音声フレームを転送しているか、音声フレームを転送している別のインターフェースと通信している回線に対して、断片化を使用可能にする必要があります。ただし、断片化およ

フレーム・リレー・インターフェースの構成

びインターリーピングは、任意の優先順位データに対して行うことができません。つまり、インターリーピングは、フレーム・リレーを介しての音声以外のプロトコルでサポートされます。

音声などのリアルタイム・トラフィックに優先順位を与えるために断片化を使用可能にするときは、帯域幅予約システム (BRS) を構成する必要があることに留意してください。フレーム・リレーを介しての帯域幅予約については、**フィーチャーの使用と構成** の『帯域幅予約および優先待ち行列の使用』および『帯域幅予約の構成と監視』を参照してください。

fragmentation-type

このパラメーターの値は、次のとおりです。

- ユーザー・ネットワーク・インターフェース (UNI)/ ネットワーク・ネットワーク・インターフェース (NNI)
- エンド・エンド

ユーザー・ネットワーク・インターフェース (UNI)/ネットワーク・ネットワーク・インターフェース (NNI) がデフォルト・タイプです。UNI は DTE から DCE への断片化です。NNI は DCE から DCE への断片化であり、エンド・エンドは、インターフェース内の特定の指定された PVC を通じての DCE から DCE への断片化です。

UNI/NNI 断片化が使用可能にされる場合、インターフェース上のすべての回線 (マネージメント PVC (つまり、DLCI 0) を含む) について断片化が発生します。PVC を通じての断片化を構成する場合、その回線についての断片化タイプは常にエンド・エンドです。断片化しているときは、PVC の両端でエンド・エンド断片化を使用可能にする必要があります。ただし、断片化サイズは、両方向で同じである必要はありません。

次のルーターへのパスがフレーム・リレー・スイッチを通過する場合、エンド・エンドの断片化タイプを使用する必要があります。2210 から次のルーターへ UNI/NNI 接続を使用する場合は、フレーム・リレー・ネットワーク・プロバイダーが UNI/NNI 断片化をサポートしていることを確認してください。

有効値: UNI/NNI、またはエンド・エンド

デフォルト値: UNI/NNI

fragment-size

各断片の断片サイズをバイト数で表示します。UNI/NNI の断片化の場合、このパラメーターは、インターフェース上のすべての回線について使用される断片サイズを指定します。エンド・エンド断片化の場合、このパラメーターは、このインターフェース上の PVC についてのデフォルトの断片サイズを指定します。

断片サイズは交渉されず、PVC の両側で同じである必要はありません。ただし、送信されるフレームは、断片サイズにかかわらず、PVC の受信側の端の MTU より大きくすることはできません。フレームが受信側の端の MTU を超える場合、受信側を過剰負荷させる断片が到着すると、受信側は次のアクションを実行します。

1. 断片をバッファリングできないことを示すエラー・メッセージを送信する。

フレーム・リレー・インターフェースの構成

2. その断片を廃棄する。
3. メッセージ *Out of sequence fragments* を表示する。
4. 最終的にはそのフレームのすべての断片を廃棄する。

断片サイズを選択するためのヒント:

- 断片サイズを指定するとき、断片サイズがリンクの容量に適切であるか確認してください。選択された断片サイズは、アクセス速度およびリンクを共用するリアルタイム・データについて許容可能な遅延の量に基づく必要があります。
- それに加えて、ルーター上のバッファが各断片に割り振られます。フレーム・サイズが大きく、断片サイズが非常に小さい場合、ルーターはそのバッファの多くを断片に割り振ることができるので、ルーター自体の性能は低下します。

有効値: 50 ~ 8190 バイト

デフォルト値: 256 バイト

fragmented-packet-reassembly-timer

断片の受信側が、シーケンス内の次の断片が到着するのを待つ時間の長さを秒数で表示します。次の断片が到着する前にタイマーが満了する場合、そのフレームについて受信されるすべての断片が廃棄されます。

有効値: 3 ~ 10 秒

デフォルト値: 3 秒

lmi マネージメント・アクティビティーを使用可能にします。

enable lmi コマンドを出した後、**set lmi-type** コマンドを使用して、フレーム・リレー・インターフェースの管理モードを選択します。463ページの『フレーム・リレー PVC マネージメントの使用可能化』を参照してください。システムのデフォルトでは ANSI T1.617 付録 D マネージメントになります。

以前にフレーム・リレー・マネージメントを使用不可にした場合は、**enable lmi** コマンドを使用して、LMI マネージメントを再開してください。

LMI は、インターフェース上の PVC に関する情報を提供するだけなので、ネットワークによって要求されない限り、SVC だけが使用される場合は、使用可能にする必要がありません。Q.922 は、インターフェース上のすべての SVC の使用可能度を決定し、インターフェース自体の状態のインディケータとなります。PVC と SVC の両方がインターフェース上にあるときは、LMI と Q.922 が同時にアクティブである場合があります。

lower-dtr

このパラメーターは、使用不可にされている専用シリアル・ライン・インターフェースのデータ端末レディー (DTR) 信号の扱い方を決めます。フレーム・リレー・ダイヤル回線インターフェースではサポートされません。このパラメーターが『使用不可』(デフォルト値) に設定されている場合、インターフェースが使用不可のときは DTR 信号は上がったままになります。

lower-dtr が使用可能の場合は、インターフェースが使用不可にされると、DTR は下がります。この動作が適している状況は、インターフェースが WAN 再

フレーム・リレー・インターフェースの構成

ルートの代替リンクとして構成されており、インターフェースが、DTR 信号の状態に基づいてダイヤル接続を維持するダイヤルアウト・モデムに接続されているような場合です。

このフィーチャーが使用可能で、インターフェースが使用不可のとき、DTR 信号は下がり、モデムはダイヤル接続をダウンに維持します。インターフェースが使用可能になると (WAN 再ルートのバックアップ・シナリオにより)、DTR は上がり、モデムは保管しているバックアップ・サイトへの番号をダイヤルします。1 次インターフェースが復元すると、代替インターフェースは使用不可にされ、DTR は下がって、モデムはダイヤル接続を切断します。

以下のケーブル・タイプがサポートされます。

EIA 232 (RS-232)

V.35

V.36

デフォルト設定値は **disable lower-dtr** です。

multicast-emulation

マルチキャスト・エミュレーションを使用可能にします。これにより、各アクティブ VC 上でマルチキャスト/ブロードキャスト・フレームを転送できるようになります。ARP、IPX RIP、および IP RIP などのプロトコルは、フレーム・リレー・インターフェースを介して正しく機能するためには、マルチキャスト・エミュレーションを使用可能にしておく必要があります。詳細については、451ページの『マルチキャスト・エミュレーションとプロトコル・ブロードキャスト』を参照してください。このパラメーターのデフォルト値は、使用可能です。

no-pvc

インターフェースをアクティブと見なすか、非アクティブと見なすかを制御します。このフィーチャーが使用可能のとき、インターフェース上にアクティブの PVC が存在しないと、フレーム・リレー・インターフェースは非アクティブになります。少なくとも 1 つの PVC がアクティブの場合、ルーターと FR スイッチ間で LMI 交換が正常に行われると、フレーム・リレー・インターフェースはアクティブになります。

notify-fecn-source

ルーターが、FECN ビットがセットされた受信パケットの発信元の装置に最初に送るパケットに BECN ビットをセットするのを使用可能にします。このパラメーターは、FR スイッチ自体は BECN をセットしないが、FECN はセットするネットワークで、装置の輻輳 (ふくそう) 制御機構を拡張するのに使用します。詳細については、457ページの『回線輻輳』を参照してください。

orphan-circuits

すべての未構成オーファン回線の使用を使用可能にします。このフィーチャーのデフォルトは、使用可能です。デフォルト CIR 値についての詳細は、454ページの『オーファン・パーマネント・バーチャル・サーキットの CIR』を参照してください。

protocol-broadcast

IP RIP のようなプロトコルがフレーム・リレー・インターフェースを介して正しく機能するようにします。プロトコル・ブロードキャスト・フィーチャ

フレーム・リレー・インターフェースの構成

ーが正しく機能するには、マルチキャスト・エミュレーション・フィーチャーを使用可能にする必要があります。このフィーチャーのデフォルト設定は、使用可能です。

switched-virtual-circuits

SVC の使用を可能にし、ローカル SVC ネットワーク番号、番号計画、オフファン SVC からのコール・インが許可されるかどうか、インターフェース上のすべての SVC について実行されるダイヤルアウト再試行の数、およびバックツーバック (たとえば、ダイヤル・サーキット) ルーター構成で使用されるネットワーク・エミュレーション・モード が必要であるかどうかを入力するよう求めます。

SVC がすでに使用可能にされている場合は、

enable switched-virtual-circuits コマンドを使用して、構成済みの SVC インターフェース・パラメーターを変更することもできます。

例:

```
FR 1 Config> enable switched
Local party number []? 4141990
Local party number numbering plan (E.164 or X.121) [E.164]?
Local party number type (Unknown or International) [International]?
Are call-ins allowed on this interface [Y]?
Call-out redial attempts [2]?
Network emulation mode [N]?
```

Local party number

あて先のフレーム・リレー・アドレスを指定します。

有効値: 10 進数の 1 ~ 20 文字の文字列

デフォルト値: なし

Local party numbering plan

パーティー番号の形式を指定します。番号計画は、FR ネットワークによって使用されるものに一致する必要があります。

有効値: E.164 (ISDN) または X.121 (Data)

デフォルト値: E.164

Local party number type

あて先のフレーム・リレー・パーティー番号タイプを指定します。番号タイプは、FR ネットワークによって使用されるものに一致している必要があります。

有効値: International または Unknown

デフォルト値: International

Call-ins allowed

このインターフェースで未構成 (オフファン) SVC からのコールが許可されるかどうか指定します。

Call-out redial attempts

このインターフェース上でコール・アウト・タイムアウトが発生した場合に、各 SVC で実行されるコール・アウト・リダイヤル試行の数を指定します。

デフォルト値: 2

フレーム・リレー・インターフェースの構成

Encoding

シリアル・インターフェースの伝送符号化法。符号化法は NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) です。

Idle データ・リンク・アイドル状態: フラグまたはマーク

Clocking

クロックのタイプ: 内部または外部

Cable type

シリアル・アダプター・ケーブル・タイプ: RS-232、V.35、V.36、または X.21

Line Speed (bps)

フレーム・リレー・インターフェースの物理データ速度を示します。

Maximum frame size

任意の時間にネットワークを介して送信または受信できる最大フレーム・サイズを示します。

Transmit delay

フレーム間に送信される追加のフラグ・バイト数を示します。

Lower DTR

WAN 再ルート代替リンクが不要になったときに、ルーターが DTR 信号を下げるかどうかを示します。DTR 信号が降下すると、モデムは代替リンクの専用回線接続を終了します。ケーブル・タイプが X.21 のときは、Lower DTR は表示されません。

注:

FR ダイヤル回線インターフェースの場合は、最大フレーム・サイズのみが表示されます。

HSSI アダプター上の FR インターフェースの場合、**list hdlc** コマンドは、上記の HDLC パラメーターのサブセットを表示するだけです。

lmi フレーム・リレー・インターフェースの論理マネージメントおよび関連構成情報を表示します。

例:

```
Frame Relay Configuration

LMI enabled           = No   LMI DLCI           = 0
LMI type             = ANSI LMI Orphans OK       = Yes
CLLM enabled         = No   Timer Ty seconds   = 11
SVCs enabled         = No

Protocol broadcast    = Yes  Congestion monitoring = Yes
Emulate multicast    = Yes  CIR monitoring       = No
Notify FECN source   = No   Throttle transmit on FECN = No

Data compression     = No

3
Fragmentation Type = END-TQ-END
Fragmentation Size = 440 Fragment reassembly timer = 3

Number VCs 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
```


フレーム・リレー・インターフェースの構成

MIR % of CIR	=	25	IR % Increment	=	12
IR % Decrement	=	25	DECnet length field	=	No
Default CIR	=	64000	Default Burst Size	=	64000
Default Excess Burst	=	0			

3 このマーカーに続く 2 行は、断片化がオン (yes) のときだけ表示されます。

LMI enabled

フレーム・リレー・インターフェース上でマネージメント・フィーチャーが使用可能になっているかどうか (yes または no) を示します。

LMI DLCI

マネージメント回線番号を示します。この番号は LMI タイプを反映します。ANSI および ITU-T/CCITT の場合は 0 で、REV1 の場合は 1023 です。

LMI Type

LMI タイプ (REV1、ANSI、または CCITT) を示します。

LMI Orphans OK

未構成回線を使用できるかどうか (yes または no) を示します。

CLLM Enabled

フレーム・リレー・インターフェース上で CLLM が使用可能かどうかを示します。

Timer Ty seconds

装置が輻轉 (ふくそう) 状態は解消されたものと見なして徐々に PVC を構成された伝送速度に戻す前に、装置が CLLM メッセージまたは BECN を受信せずに経過する必要がある時間の長さを指定します。

SVC network number

このインターフェース上の SVC のネットワーク番号を指定します。

SVC number type

SVC 番号タイプが unknown または international のいずれかを指定します。

SVC numbering plan

番号計画が E.164 または X.121 のいずれかを指定します。

SVC call-out redial attempts

このインターフェース上でのコール・アウト・リダイヤル試行の数を指定します。

SVC network emulation mode

このインターフェースが SVC のネットワーク・エミュレーション・モードで動作するかどうか指定します。

SVC call-ins allowed

このインターフェース上でコール・インが許可されるかどうかを指定します。

Protocol Broadcast

IP RIP のようなプロトコルがフレーム・リレー・インターフェースを介して機能できるかどうか (yes または no) を示します。

フレーム・リレー・インターフェースの構成

Emulate multicast

各アクティブ PVC 上のマルチキャスト・エミュレーション・フィーチャーが使用可能かどうか (yes または no) を示します。

Congestion Monitoring

ネットワーク輻輳 (ふくそう) に対応する輻輳 (ふくそう) 監視フィーチャーが使用可能かどうか (yes または no) を示します。

CIR monitoring

伝送速度を強制する回線監視フィーチャーが使用可能かどうか (yes または no) を示します。

Notify FECN Source

この装置が、FECN ビットがセットされた受信パケットの発信元の装置に最初に送るパケットに BECN ビットをセットするかどうかを示します。

Throttle Transmit on FECN

この装置が、FECN ビットがオンにセットされているパケットにตอบสนองして、パケットの転送を減速 するかどうかを示します。

Data compression

このインターフェースではデータ圧縮が使用可能にされているかどうかを示します。

Data encryption

このインターフェースではデータ暗号化が使用可能にされているかどうかを示します。

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

Fragmentation

このインターフェース上で断片化が使用可能かどうかを示します。

Fragmentation type

断片化タイプを表示します: ユーザー・ネットワーク (UNI) インターフェース、ネットワーク・ネットワーク (NNI) インターフェース、またはエンド・エンド (指定された PVC を通じてのピア DTE による断片化)。

Fragment size

各断片の断片サイズをバイト数で表示します。

Fragmentation timer value

断片の受信側が、次の断片が到着するのを待つ時間の長さを秒数で表示します。次の断片が到着する前にタイマーが満了する場合、そのフレームについて受信されるすべての断片が廃棄されます。

Orphan compression

このインターフェース上のオーファン回線で、データ圧縮が使用可能かどうかを示します。

注: オーファン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 が利用可能な圧縮コンテキストの数が減ります。

フレーム・リレー・インターフェースの構成

オーファン圧縮は、PVC と SVC の両方に適用されます。

Compression circuit limit

データ圧縮に参加できるサーキットの最大数を示します。

Number of compression VCs

データ圧縮をサポートしている現行の VC 数を示します。

P1 allowed

このインターフェースで使用できる PVC および SVC の数を示します。

Timer T1 seconds

フレーム・リレー・インターフェースがフレーム・リレー・スイッチ LMI エンティティとシーケンス番号交換を行う頻度を示します。

Counter N1 increments

完全な LMI 状態照会を実行する前に満了する必要がある T1 タイマー間隔の回数を示します。

LMI N2 error threshold

N3 ウィンドウ内で発生した、フレーム・リレー・インターフェースのリセットの原因になる管理イベント誤りの数を示します。

LMI N3 error threshold window

N2 誤り限界値を測定するのに使用される、監視された管理イベントの数を示します。

MIR % of CIR

CIR の比率として表される最小 IR

IR % Increment

最大 IR に達するまで、ルーターが BECN のないフレームを受信するたびに IR を増分する比率

IR % Decrement

最小 IR に達するまで、ルーターが BECN を含むフレームを受信するたびに IR を減分する比率

Default CIR

このインターフェース上の VC のデフォルト値として使用される認定情報速度 (ビット/秒)

Default Burst Size

このインターフェース上の VC のデフォルト値として使用される認定バースト・サイズ (ビット数)

Default Excess Burst Size

このインターフェース上の VC のデフォルト値として使用される超過バースト・サイズ (ビット数)

permanent-virtual-circuits

フレーム・リレー・インターフェース上のすべての構成済み PVC を表示します。

例:

フレーム・リレー・インターフェースの構成

```
FR 0 Config>LIST PERMANENT-VIRTUAL-CIRCUITS
```

```
Maximum circuits allowable = 64
Total circuits configured = 3
Total PVCs configured = 3
```

Circuit Name	Circuit Number	Options	CIR in bps	Burst Size	Excess Burst
Unassigned	16	R	64000	64000	0
Bigcir	17	F V	64000	64000	0
Unassigned	18		64000	64000	0

```
R = circuit is required
G = circuit is required and belongs to a required PVC group
F = circuit is fragmentation capable
c = circuit is data compression capable
V = circuit is voice forwarding enabled
```

Maximum circuits allowable

このインターフェースに存在できる PVC および SVC の数を示します。この数には、**add permanent-virtual-circuit** コマンドを使って追加した PVC および **add switched-virtual-circuit** コマンドを使って追加した SVC で、管理インターフェースを通じて動的に確認されたものが含まれます。

Total circuits configured

このインターフェース用に存在することができる現在構成されている PVC および SVC の合計数を示します。

Circuit Name

構成された PVC の ASCII 名を示します。

Circuit Number

現在構成されている PVC の DLCI を示します。

Circuit Type

現在構成されているバーチャル・サーキットのタイプを示します。フレーム・リレーのこのリリースでは、パーマネント・バーチャル・サーキットのみがサポートされます。

Committed Information Rate

ネットワークで合意されている、通常の条件下でのデータ転送の情報速度を示します。

Committed Burst Size

ネットワークで合意されている、(認定バースト・サイズ/CIR) 秒数に等しい測定期間中に送達できる最大データ量 (ビット数)。

Excess Burst Size

(認定バースト・サイズ/CIR) 秒数に等しい測定期間中にネットワークが送達を試みることができる、認定バースト・サイズを超過した未認定データの最大量 (ビット数)。

pvc-groups

フレーム・リレー・インターフェース上のすべての必須 PVC グループを表示します。

例:

```
list pvc-groups
Required PVC group = group1
Circuit # 16
```

protocol-addresses

フレーム・リレー・インターフェースのすべての静的に構成された回線マッピングのプロトコル・アドレスを表示します。

例:

list protocol-addresses

Frame Relay Protocol Address Translations

Protocol Type	Protocol Address	Circuit Number or Name
IP	125.2.29.4	21
IPX	000000004503	16

Protocol Type

インターフェースを介して実行されているプロトコルの名前を表示します。

Protocol Address

回線の相手側の装置のプロトコル・アドレスを表示します。

Circuit Number or Name

PVC の DLCI またはプロトコルを処理している SVC の名前を表示します。

switched-virtual-circuits

FR 0 Config>LIST SWITCHED-VIRTUAL-CIRCUITS

Maximum circuits allowable = 64
Total circuits configured = 5

Circuit Name	Options	Idle Timer		Outgoing Value	Incoming Value
SVC1	ILM c	60	CIR:	64000	64000
Remote party number: IE3445667			Min CIR:	64000	64000
Remote subaddress: Pc4456d			Burst:	64000	64000
			Excess:	0	0
svc1	ILM c	60	CIR:	64000	64000
Remote party number: IE3445666			Min CIR:	64000	64000
Remote subaddress: P344566			Burst:	64000	64000
			Excess:	0	0

Options: I - call-ins allowed, L - learn protocols, M - Multicast required
c - compression capable, F - UNI/NNI fragmentation enabled
Address type: I - International, U - Unknown
Numbering plan: E - E.164, X - X.121
Subaddress format: N - NSAP, P - private

Maximum circuits allowable

このインターフェースに存在できる回線の数を示します。

Total circuits configured

このインターフェースに現在構成されている回線の合計数を示します。

Circuit Name

構成された回線の ASCII 名を示します。

Committed Information Rate

ネットワークで合意されている、通常の条件下でのデータ転送の情報速度を示します。

Committed Burst Size

ネットワークで合意されている、(認定バースト・サイズ/CIR) 秒数に等しい測定期間中に送達できる最大データ量 (ビット数)。

フレーム・リレー・インターフェースの構成

Excess Burst Size

(認定バースト・サイズ/CIR) 秒数に等しい測定期間中にネットワークが送達を試みることができる、認定バースト・サイズを超過した未認定データの最大量 (ビット数)

Idle Timer

トラフィックがないときに、SVC がアクティブのままの時間枠

Options

回線に構成されるオプションを示します。

Remote party number

リモートあて先 FR アドレス。このアドレスの接頭部に、使用されるアドレス・タイプおよび番号計画が付きます。

Remote subaddress

この接続に割り当てられたリモート側のサブアドレス。サブアドレスの接頭部にサブアドレス形式が付きます。

voice-forwarding-circuits

```
FR 2 Config>list voice
```

Circuit Name	Circuit Number	Forwarding Network	Forwarding Circuit
-----	-----	-----	-----
circ11	17	0	16

Circuit Name

構成された回線の ASCII 名を示します。

Circuit Number

この PVC の回線を示します。

Forwarding Network

この回線が音声フレームを転送する先のネット番号を示します。

Forwarding Circuit

この回線が音声フレームを転送する先の回線番号を示します。

LLC

LLC コマンドは、LLC 構成環境にアクセスするのに使用します。これらの各コマンドの説明は、267ページの『LLC 構成コマンド』を参照してください。

注: **LLC** コマンドは、ソフトウェア・ロードに APPN が含まれている場合にのみサポートされます。

構文:

llc

Remove

remove コマンドは、PVC、必須 PVC グループ、または以前に **add** コマンドを使用して追加されたプロトコル・アドレスを削除するのに使用します。

構文:

remove

`permanent-virtual-circuit . . .`
`protocol-address`
`pvc-group`
`switched-virtual-circuit circuit-name`

permanent-virtual-circuit pvc#

16 ~ 1007 の範囲の構成された PVC を削除します。

注:

1. 圧縮を実行している PVC を削除すると、インターフェースはアクティブ圧縮 PVC のカウントを減らします。このアクションによって圧縮 PVC のカウントが限界以下になる場合、それを知らせるメッセージを受け取ります。
2. 暗号化を実行している PVC を削除すると、インターフェースはアクティブの暗号化 PVC のカウントを減らします。

注: 暗号化サポートはオプションであり、**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。ソフトウェア使用者の手引きの CONFIG プロセス **load** コマンドを参照してください。

ルーター内での複数の暗号化の使用 (暗号化を IP セキュリティー・レイヤーおよびフレーム・リレーまたは PPP データ・リンク・レイヤーの両方で使用する) は、米国政府輸出規制によって制限されています。これは、厳密な輸出規制のもとにあるソフトウェア・ロード (128 ビット・キーとトリプル DES をもつ 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。

protocol-address

構成されたプロトコル・アドレス (静的 ARP エントリー) を削除します。このパラメーターでは、追加するプロトコルのタイプによって、異なる情報を求めるプロンプトが出ます。

例:

remove protocol-address
 Protocol name or number [IP]?

IP プロトコル:

IP Address [0.0.0.0]?
 Circuit Name or Number [16]?

IPX プロトコル:

Host Number (in hex) []?
 Circuit Name or Number [16]?

AppleTalk フェーズ 2 プロトコル:

Network Number (1-65279) []?
 Node Number (1-253) []?
 Circuit Name or Number [16]?

DN プロトコル:

Node address [0.0]?
 Circuit Name or Number [16]?

フレーム・リレー・インターフェースの構成

Protocol name or number

削除するプロトコルの名前または番号を定義します。サポートされないプロトコルを削除しようとする、システムは誤りメッセージを出します。

Unknown protocol name, try again

サポートされるプロトコルのリストを見たい場合は、Protocol name or number [IP]? プロンプトで ? を入力します。

IP Address

リモート IP ホストの 32 ビット・インターネット・アドレスを小数点表記法で定義します。

Host Number

リモート IPX ホストの 48 ビット・ノード・アドレスを定義します。

Network Number

AppleTalk フェーズ 2 ネットワーク番号を定義します。

Node Number

リモート AppleTalk ホストに接続されているインターフェースのノード番号を定義します。

Node address

リモート DECnet ホストの DECnet ノード・アドレスを定義します。ノード・アドレスは x,y フォーマットで構成します。ただし、x は 6 ビットのエリア・アドレスで、y は 10 ビットのノード番号です。

Circuit Number

プロトコルが実行される PVC または SVC の名前を定義します。

pvc-group *groupname*

構成された PVC グループを名前によって削除します。グループは、メンバー回線をもっていない場合にのみ削除されます。

例: **remove pvc-group PVC group name [IP]?**

switched-virtual-circuit

構成済みの SVC を回線名で削除します。

Set

set コマンドは、フレーム・リレー・プロトコルを実行するインターフェースを構成するのに使用します。

Set コマンドの考慮事項

構成を始める前に、2 つのパラメーター (n2-parameter と n3-parameter) について説明しておきます。n2-parameter は、管理イベントの誤り限界値を設定し、n3-parameter は、イベント・ウィンドウで監視されるイベントの数を設定します。イベント・ウィンドウ内の管理誤りの数が n2 に等しくなると、フレーム・リレー・インターフェースはリセットされます。たとえば、次のように入力します。

set n3-parameter 4

set n2-parameter 3

フレーム・リレー・インターフェースの構成

ここでは、ウィンドウ・サイズは 4 ($n3 = 4$)、誤り限界値は 3 ($n2 = 3$) に設定されました。これは、システムは 4 つの管理イベントを監視して、いずれかに誤りがないかチェックします。誤りのあるイベントの数が 3 ($n2$ parameter) に等しくなると、フレーム・リレー・インターフェースはリセットされ、ネットワークの状態はネットワークがダウン と見なされます。

ネットワークの状態がネットワークがアップ と見なされるためには、状態が変更される前の、ウィンドウ内の誤りのあるイベント数が $n2$ より少なくなければなりません。

構文:

```
set                                cable*
                                     cir-defaults
                                     clocking*
                                     crc-type*
                                     encoding*
                                     frame-size
                                     idle . . .*
                                     ir-adjustment . . .
                                     line-speed*
                                     lmi-type n1-parameter
                                     n2-parameter
                                     n3-parameter
                                     p1-parameter
                                     t1-parameter
                                     transmit-delay . . .*
                                     ty-parameter
```

* **Note:** 後ろに * が付いているコマンドは、FR ダイヤル回線インターフェースでは利用不能です。

cable *physical-interface-link-type data-connection-type*

ネットワークの物理リンクのケーブル・タイプを設定します。

DTE ケーブルは、ルーターをあるタイプの DCE 装置 (たとえば、モデムまたは DSU/CSU) に接続するときを使用します。DCE ケーブルは、ルーターが DCE として動作し、直接接続のためのクロックを提供するときを使用します。

利用可能なオプションを以下に示します。

物理インターフェース・リンク・タイプ	データ接続タイプ
EIA 232 (RS-232)	DTE, DCE
V35	DTE, DCE
V36	DTE, DCE
X21	DTE, DCE
HSSI	DTE, DCE (see note)

フレーム・リレー・インターフェースの構成

注: HSSI DCE ケーブルが使用される場合、HSSI DCE ケーブルを使用するためにその他の装置も構成する必要があります。

cir-defaults

回線輻輳 (ふくそう) パラメーターのデフォルト値を設定します。パラメーターを以下に示します。

cir *cir* のデフォルト値を、フレーム・リレー・ネットワークの提供者によって提供された値に設定します。

有効値: 0 または 300 ~ 204 800 bps

デフォルト値: 64 000

HSSI の場合、構成できる最大値は 52 000 000 bps です。

bc *bc* のデフォルト値を、フレーム・リレー・ネットワークの提供者によって提供された値に設定します。

有効値: 454ページの『認定バースト (Bc) サイズ』を参照してください。

デフォルト値: 64 000

HSSI の場合、構成できる最大値は 52 000 000 bps です。

be *be* のデフォルト値を、フレーム・リレー・ネットワークの提供者によって提供された値に設定します。

有効値: 455ページの『超過バースト (Be) サイズ』を参照してください。

デフォルト値: 0

HSSI の場合、構成できる最大値は 52 000 000 bps です。

例:

```
FR 6 config> set cir-default
Default Committed Information Rate (CIR) in bps [64000]? 48000
Default Committed Burst Size (Bc) in bits [64000]? 40000
Default Excess Burst Size (Be) in bits [0]? 52000
```

clocking [external or internal]

モデムまたは DSU に接続するには、外部クロックを構成し、**set cable** コマンドを使って該当する DTE ケーブルを選択します。回線速度を構成するには、**set line-speed** コマンドを使用します。

別の DTE 装置に直接接続するには、内部クロックを構成し、**set cable** コマンドを使って該当する DCE ケーブルを選択し、**set line-speed** コマンドを使ってクロック/回線速度を構成します。

デフォルト値: external

注: クロック・タイプは、フレーム・リレーが HSSI アダプター上で構成されているときは、構成可能ではありません。クロック・タイプは、ケーブル・タイプによって決定されます。HSSI DCE ケーブル・タイプが構成される場合は内部クロックが使用され、HSSI DTE ケーブル・タイプが構成される場合は外部クロックが使用されます。

crc-type [crc-ccitt-16 or crc-ccitt-32]

CRC タイプは、16 ビット CRC または 32 ビット CRC として構成できます。デフォルトは、**crc-ccitt-16** です。

フレーム・リレー・インターフェースの構成

注: CRC タイプは、HSSI アダプター上の FR インターフェースにだけ構成することができます。

encoding [NRZ or NRZI]

HDLC 伝送符号化法を NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) に設定します。ほとんどの構成では NRZ が使用され、これがデフォルト値です。

注: HSSI アダプター上の FR インターフェースでは符号化は NRZ に設定され、構成可能ではありません。

frame-size

インターフェース上で送受信されるフレームのネットワーク・レイヤー部分の最大サイズを設定します。この最大サイズには、図 39-4 に示されている 2 バイトの DLCI アドレスとユーザー・データが含まれています。構成するサイズは、フレーム・リレー・スイッチおよびフレーム・リレー・ネットワークの他の FR DTE によってサポートされる最大フレーム・サイズに矛盾しない値でなければなりません。値は 262 ~ 8190 です。デフォルト値は 2048 です。構成されたフレーム・サイズには、DLCI アドレスと FR RFC 1490 および RFC 2427 マルチプロトコル・カプセル化ヘッダーが含まれているので、転送できる最大プロトコル・パケット・サイズは、構成されたフレーム・サイズより小さくなり、その大きさはプロトコルによって異なります。下の表は、インターフェース上で送受信できる最大プロトコル・パケット・サイズを算定するために、構成されたフレーム・サイズから差し引く必要があるバイト数を示しています。

IP	4 バイト
IPX	10 バイト
Appletalk フェーズ 2	10 バイト
DECnet フェーズ IV (DNA IV)	12 バイト
Banyan Vines	10 バイト
OSI	10 バイト
ブリッジング	10 バイト
APPN	58 バイト (注を参照)

注: FR ヘッダーのバイト数の他に T/R MAC アドレス・ヘッダーと LLC ヘッダーも追加された、APPN BAN の最悪のケースを想定しています。FR データ暗号化が使用可能の場合には、さらに最大 12 バイトを差し引く必要があります。

フレーム・リレー SVC を使用しているときは、最大の情報フィールド・サイズは、バーチャル・サーキットの両端で同じである必要があります。最大の情報フィールド・サイズを判別するには、SVC で暗号化が使用可能にされている場合は、フレーム・サイズから 16 バイトを減算し、SVC で暗号化が使用可能にされていない場合は、4 バイトを減算します。

idle [flag or mark]

HDLC フレームの伝送アイドル状態を設定します。デフォルト値は **flag** で、これはフレーム間に連続フラグ (7E 16 進数) を提供します。マーク・オプションは、フレーム間の伝送路をマーキング状態 (OFF, 1) にします。

注: HSSI アダプター上の FR インターフェースでは Idle は **flag** に設定され、構成可能ではありません。

フレーム・リレー・インターフェースの構成

ir-adjustment *increment-% decrement-% minimum-IR*

最小情報速度 (IR) と、ネットワークの輻輳 (ふくそう) に応じて IR を増分および減分する比率を設定します。

最小 IR (CIR の比率で表す) は、情報速度の下限です。最小比率は 1 で、最大比率は 100 です。デフォルト値は 25 です。

ネットワークの輻輳 (ふくそう) が解消されると、情報速度は、最大情報速度に達するまで、IR 調整増分比率ずつ徐々に増分されます。最小比率は 1 で、最大比率は 100 です。デフォルト値は 12 です。

ネットワークの輻輳 (ふくそう) が発生すると、情報速度は、最小情報速度に達するまで、BECN が入ったフレームを受信するたびに IR 調整減分比率ずつ減分されます。最小比率は 1 で、最大比率は 100 です。デフォルト値は 25 です。

例:

```
set ir-adjustment
  IR adjustment % increment [12]?
  IR adjustment % decrement [25]?
  Minimum IR as % of CIR [25]?
```

line-speed *rate*

内部クロックの場合は、このコマンドを使用して送信および受信クロック回線の速度を指定します。

外部クロックの場合は、このコマンドは WAN/シリアル回線の動作には影響を与えませんが、一部のプロトコル (IPX など) がルーティング・コスト・パラメーターを判別するのに使用する速度を設定します。速度は、実際の回線速度に一致するように設定する必要があります。速度が構成されていない場合、プロトコルは 1 000 000 bps の速度を想定します。

有効値:

内部クロック: 表62 を参照してください。

外部クロック: 表63 を参照してください。

表 62. 2210 インターフェースに内部クロックが使用される時の回線速度

アダプター・タイプ	速度範囲
8 ポート EIA 232	9600 ~ 64 000 bps
6 ポート V.35/V.36	9600 ~ 460 800 bps、1 544 000 bps、または 2 048 000 bps
8 ポート X.21	9600 ~ 460 800 bps、1 544 000 bps、または 2 048 000 bps
1 ポート HSSI	22 368 000 bps または 44 736 000 bps

表 63. 2210 インターフェースに外部クロックが使用された時の回線速度

アダプター・タイプ	速度範囲
8 ポート EIA 232	2400 ~ 64 000 bps
6 ポート V.35/V.36	2400 ~ 2 048 000 bps
8 ポート X.21	2400 ~ 2 048 000 bps
1 ポート HSSI	1 544 000 bps ~ 52 000 000 bps

lmi-type [*rev1 or ansi or ccitt*]

インターフェースのマネージメント・タイプを設定します。フレーム・リレ

フレーム・リレー・インターフェースの構成

ー・マネージメントの設定についての詳細は、463ページの『フレーム・リレー PVC マネージメントの使用可能化』を参照してください。デフォルトでは、タイプ **ansi** が使用可能になります。

表 64. フレーム・リレー・マネージメント・オプション

コマンド	マネージメント・タイプ	説明
set	lmi-type rev1	LMI 改訂 1 (Stratacom のフレーム・リレー・インターフェース仕様) に準拠します。
set	lmi-type ansi	ANSI T1.617 ISDN-DSS1-Signalling Specification for Frame Relay Bearer Service (付録 D と呼ばれます) に準拠します。
set	lmi-type ccitt	ITU-T/CCITT 勧告 Q.933 の付録 A - DSS1 Signalling Specification for Frame Mode Basic Call Control に準拠します。

n1-parameter *count*

完全な PVC 状態照会を実行する前に満了する必要がある T1 タイマー間隔の回数を構成します。*Count* は、1 ~ 255 の範囲の間隔です。デフォルト値は 6 です。

n2-parameter *max#*

フレーム・リレー・インターフェースがリセットされる前に、n3-parameter によって監視される管理イベント・ウィンドウで発生しても構わない誤りの数を構成します。*Max#* は、1 ~ 10 の範囲の数です。デフォルト値は 3 です。このパラメーターは、n3-parameter の値以下でなければなりません。そうでない場合は、誤りメッセージを受け取ります。

n3-parameter *max#*

n2-parameter を測定するのに使用される、監視された管理イベントの数を構成します。*Max#* は、1 ~ 10 の範囲の数です。デフォルト値は 4 です。

p1-parameter *max#*

フレーム・リレー・インターフェースによってサポートされる PVC の最大数を構成します。これには、アクティブ、非アクティブ、除去済み、および構成済み PVC が含まれます。*Max#* は、0 ~ 992 の範囲の数です。デフォルト値は 64 です。0 (ゼロ) は、インターフェースが PVC をサポートしないことを意味します。

t1-parameter *time*

フレーム・リレー・マネージメントとのシーケンス番号交換の間隔 (秒数) を構成します。マネージメントの T2 タイマーは、エンド・ステーションがマネージャーとのシーケンス番号交換を要求するのに許される間隔です。T1 間隔は、ネットワークの T2 間隔より小さくなければなりません。*Time* は、5 ~ 30 の範囲の値です。デフォルト値は 10 です。

transmit-delay *#*

転送されるパケット間に遅延を挿入することができます。このコマンドの目的は、シリアル・ラインを減速して、相手側の旧型で低速のシリアル装置に整合させることです。伝送路間でシリアル・ライン・ハロー・パケットが失われるのも防止できます。*#* は、0 ~ 15 個の余剰フラグです。デフォルト値はゼロ (0) です。このパラメーターを設定すると、送信フレーム相互間に

フレーム・リレー・インターフェースの構成

0 ～ 15 個の余剰フラグが挿入されます。表65 は、シリアル・インターフェースの単位と範囲を示しています。

注: 8 ポート EIA-232E アダプター、6 ポート V.35/V.36 アダプター、または 8 ポート X.21 アダプター上の FR インターフェースに非ゼロの伝送遅延を構成した場合、**set line-speed** コマンドを使用して回線速度を構成する必要があります。

表 65. 2210 シリアル・インターフェースの転送遅延の単位と範囲

単位	最小	最大
余剰フラグ	0	15

ty-parameter time

装置が CLLM メッセージの受信によって示された既存の輻輳 (ふくそう) 状態が解消されたと見なす前に経過する必要があるインターバルを構成します。このタイマーが満了する前に、装置が CLLM メッセージを受信した場合、装置はこのタイマーをリセットします。

有効値: 5 ～ 30 秒

デフォルト値: 11 秒

フレーム・リレー監視プロンプトへのアクセス

フレーム・リレー動作コマンドにアクセスし、ルーター上でフレーム・リレーを監視するには、次のステップを実行します。

1. OPCON プロンプト (*) で **talk 5** と入力する。
2. GWCON プロンプト (+) で、**interface** コマンドを入力して、ルーター上に構成されているインターフェースのリストを表示する。
3. **network** コマンドに続けて、フレーム・リレー・インターフェースのネットワーク番号を入力する。たとえば、次のように入力します。

```
+ net 2
Frame Relay Monitoring
FR 2 >
```

フレーム・リレー監視コマンド

この節では、フレーム・リレー監視コマンドの要約を示し、個々のコマンドについて説明します。これらのコマンドは、データベースから情報を収集するのに使用します。表66 は、コマンドを示しています。

表 66. フレーム・リレー監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Clear	フレーム・リレー・インターフェースに関する統計情報を消去します。
Disable	フレーム・リレー・インターフェース上の CIR 監視および輻輳 (ふくそう) 監視を使用不可にします。

フレーム・リレー・インターフェースの監視

enable コマンドは、ルーター構成を動的に変更します。これらの変更は、ルーターをリスタートすると失われます。

構文:

```
enable                cir-monitor
                        cllm
                        congestion-monitor
                        notify-fecn-source
                        throttle-transmit-on-fecn
```

List

list コマンドは、データ・リンク・レイヤーおよびフレーム・リレー・インターフェースに特有の統計を表示するのに使用します。

構文:

```
list                  all
                        circuit . . .
                        lmi
                        permanent-virtual-circuits
                        pvc-groups
                        svcs
                        switched-virtual-circuit
                        virtual-circuits
                        voice-forwarding-circuits
```

all フレーム・リレー・インターフェースの回線、マネージメント、および VC 統計を表示します。このコマンドで表示される出力は、**list lmi** コマンドと **list permanent-virtual-circuit** コマンドの組み合わせです。

circuit *name or number*

入力回線名または DLCI を使用して、指定された VC に関する詳しいパッチャル・サーキット構成および統計情報を表示します。

例:

```
list circuit 347
```

```
Circuit name = Valencia
```

```
Circuit state      = Active  Circuit is orphan = No
Frames transmitted = 0      Bytes transmitted = 0
Frames received   = 0      Bytes received    = 0
Total FECNs      = 0      Total BECNs      = 0
Times congested  = 0      Times Inactive    = 0
CIR in bits/second = 64000 Potential Info Rate = 56000
Committed Burst (BC) = 1200 Excess Burst (Be) = 54800
Minimum Info Rate = 16000 Maximum Info Rate = 64000
Required         = Yes    PVC group name   = group1

Compression capable = Yes  Operational      = Yes
R-Rs received      = 0    R-Rs transmitted = 0
R-As received      = 0    R-As transmitted = 0
R-R mode discards  = 0    Enlarged frames  = 0
Decompress discards = 0    Compression errors = 0
```


フレーム・リレー・インターフェースの監視

```
Compression ratio = 1.72 to 1 Decompression ratio = 1.10 to 1
Fragmentation type = END-TO-END
Fragmentation Size = 0 Reassembly timer = 0
Fragments xmitted = 0 Fragments received = 0
Voice Frames xmitted = 0 Voice Frames rcv'd = 0

Encryption capable = Yes Operational = Yes
Encryption errors = 0 Decryption errors = 0
Rcv error discards = 0

Current number of xmit frames queued = 0
Xmit frames dropped due to queue overflow = 0
```

Circuit state

回線の状態 (非アクティブ、アクティブ、または輻輳 (ふくそう)) を示します。非アクティブ (Inactive) は、フレーム・リレー・インターフェースがダウンしているか、もしくはフレーム・リレー・マネージメント・エンティティが回線がアクティブであることをフレーム・リレー・プロトコルに通知しなかったために、トラフィックのために回線を利用できないことを示しています。アクティブ (Active) は、データを転送中であることを示しています。輻輳 (ふくそう) (Congested) は、データ・フローが制御されていることを示しています。

Circuit is orphan

その回線が LMI マネージメントを通して確認された未構成の PVC であるか、非構成 SVC のコール・インかどうかを示します。

Frames/Bytes transmitted

この VC が送信したフレーム数およびバイト数を示します。

Frames/Bytes received

この VC が受信したフレーム数およびバイト数を示します。

Total FECNS

この VC がインバウンドまたはダウンストリームの輻輳 (ふくそう) を通知された回数を示します。

Total BECNs

この VC がアウトバウンドまたはアップストリームの輻輳 (ふくそう) を通知された回数を示します。

Times congested

この VC が輻輳 (ふくそう) 状態になった回数を示します。

Times inactive

この VC が運用不可になった回数を示します。

CIR in bits/sec

300 bps ~ 2 048 000 bps の範囲内の VC の情報速度を示します。値 0 もサポートされます。

Potential Info Rate

回線上のデータ転送の現行の最大速度 (ビット/秒) を示します。実際のデータ速度は、待ち行列の長さおよび回線に対応付けられている優先順位によって決まります。

このフィールドの値が『Line Speed』の場合は、このインターフェースに対して回線速度が構成されていなかったり、間違って構成されていても、最大データ速度は実際の回線速度になります。

フレーム・リレー・インターフェースの監視

Committed Burst (BC)

時間間隔 (Tc) の間に、ルーターが送信することができるデータの最大量 (ビット数)。 ($Tc=Bc/CIR$ 。)

Excess Burst (Be)

この時間間隔 (Tc) の間に、ルーターが VC 上で Bc を超過して転送できる未認定データの最大量 (ビット数)

Minimum Info Rate

最小情報速度。輻輳 (ふくそう) を通知されたときにルーターがそこまで減速する VC の最小データ速度

Maximum Info Rate

最大情報速度。ルーターが VC に送信する最大データ速度

Required

Yes または No。yes の場合、PVC は必須 PVC です。

PVC group name

PVC が必須 PVC グループのメンバーの場合、その名前がここに表示されます。そうでない場合は『Unassigned』が表示されます。

Compression capable

回線がデータ・パケットを圧縮できるかどうかを示します。

Operational

回線上で圧縮がアクティブかどうかを示します。これが yes の場合、このリンク上でデータが圧縮中です。

R-Rs received

ピア解凍機能によって送信されたりセット要求パケットの数を示します。ピア解凍機能は、ピア圧縮機能との同期が外れたことを検出するたびに、リセット要求を送信します。この数が急激に増える場合は、この回線上のパケットは失われているか、破壊されています。

R-Rs transmitted

回線上で圧縮が開始された以降に送信されたりセット要求パケットの数を示します。この数が急激に増える場合は、この回線上のパケットは失われているか、破壊されています。

R-As received

リセット要求への応答として受信されたりセット確認の数を示します。圧縮機能は、圧縮ヒストリーをリセットしたことを知らせるときも、このパケットを送信します。

R-As transmitted

これは、ピアに送信されたりセット確認の数です。

R-R mode discards

R-R を送信した後 R-A を待っている間に廃棄された圧縮データ・フレームの数を示します。

Enlarged frames

これは圧縮できなかったフレームの数です。通常は、圧縮不能なフ

フレーム・リレー・インターフェースの監視

フレームは、圧縮しない形で特殊な圧縮フレーム・タイプに入れて送信され、圧縮機能と解凍機能の同期が保たれます。

Decompress discards

解凍誤りのために廃棄された圧縮フレームの数を示します。

Compression errors

圧縮されない形で転送された圧縮誤りのあるフレームの数を示します。

Compression ratio

圧縮機能の概略の効率を示します。

Decompression ratio

解凍機能の概略の効率を示します。

Fragmentation type

断片化タイプを示します。値は UNI/NNI およびエンド・エンドです。詳しくは、talk 6 **enable fragmentation** コマンドを参照してください。

Fragmentation size

断片のサイズを示します。詳しくは、talk 6 **enable fragmentation** コマンドを参照してください。

注: エンド・エンド断片化が構成される場合、断片化サイズは、各 PVC のサイズではなく、インターフェースの構成済みサイズを示します。

Reassembly timer

断片化されたパケット再組み立てタイマーで設定された時間を示します。このタイマーが満了する前に、断片化されたパケット内の次の順番の断片が到着しない場合、断片は到着すると廃棄され、そのフレームのすべての断片が除去されます。

Encryption capable

この回線で暗号化が使用可能かどうかを示します。

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

Operational

回線上で暗号化がアクティブかどうかを示します。これが yes の場合、このリンク上でデータが暗号化中です。

Encryption errors

暗号化誤りが生じたフレームの数を示します。

Decryption errors

復号誤りが生じたフレームの数を示します。

Rcv error discards

受信に問題があったために廃棄された圧縮フレームの数を示します。

フレーム・リレー・インターフェースの監視

Current number of xmit frames queued

FR によってこの回線のために現在待ち行列化されているフレームの数を示します。これらのフレームは、このインターフェースのシリアル装置ハンドラー送信待ち行列上のスペースが利用可能になるのを待っています。

Xmit frames dropped due to queue overflow

出力待ち行列オーバーフローのためにこの VC に送信できなかったフレームの数を示します。

lmi フレーム・リレー・インターフェース上の論理マネージメントに関する統計を表示します。

例:

```
list lmi
Management Status:
-----
LMI enabled           = Yes  LMI DLCI           = 0
LMI type              = ANSI LMI Orphans OK = YES
CLLM enabled         = No

SVC local net number = 12345678
SVC Number type      = International
SVC Numbering plan   = E.164  SVC Call-out retries = 2
SVC Call-ins allowed = Yes  SVC Network emulation mode = No

Protocol broadcast    = Yes  Congestion monitoring = Yes
Emulate multicast    = Yes  CIR monitoring         = No
Notify FECN source   = No   Throttle transmit on FECN = No
Number VCs P1 allowed = 64  Interface down if no PVCs = No
Line speed (bps)     = 1000000 Maximum frame size (bytes) = 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          = 64000 Default Burst Size      = 64000
  Default Excess Burst = 0
Current receive sequence = 0
Current transmit sequence = 1
Total status enquiries = 9  Total status responses = 0
Total sequence requests = 0  Total responses        = 0

Data compression enabled = No
Data encryption enabled  = No
Fragmentation enabled    = No

Virtual Circuit Status:
-----
Total allowed = 64  Total configured = 2
Total active  = 0  Total congested  = 0
Total PVCs left net = 0  Total PVCs join net = 0
```

Management Status:

LMI enabled

フレーム・リレー・マネージメントがアクティブかどうか (yes または no) を示します。

LMI DLCI

マネージメント回線番号を示します。この番号は 0 (ANSI デフォルトまたは ITU-T/CCITT) または 1023 (中間 LMI REV1) です。

LMI type

使用されているフレーム・リレー・マネージメントのタイプ (ANSI、ITU-T/CCITT、または LMI 改訂 1) を示します。

LMI orphans OK

フレーム・リレー LMI マネージメントから確認されたすべての未構成回線を使用できるかどうか (yes または no) を示します。

CLLM enabled

CLLM フレームを受信したときに、この回線が減速するかどうかを指定します。

Timer Ty seconds

CLLM Ty タイマーの値を示します。このフィールドは、CLLM が使用可能のときにのみ表示されます。

Last CLLM cause code

受信した最後の CLLM メッセージに示されていた輻輳 (ふくそう) の原因符号を示すか、あるいは CLLM メッセージを受信しなかった場合は **None** が示されます。このフィールドは、CLLM が使用可能のときにのみ表示されます。

SVC local net number

このインターフェース上の SVC のネットワーク番号を指定します。

SVC number type

SVC 番号タイプが unknown または international のいずれかを指定します。

SVC numbering plan

番号計画が E.164 または X.121 のいずれかを指定します。

SVC call-out retries

このインターフェース上でのコール・アウト・リダイヤル試行の数を指定します。

SVC network emulation mode

このインターフェースが SVC のネットワーク・エミュレーション・モードで動作するかどうか指定します。

SVC call-ins allowed

このインターフェース上でコール・インが許可されるかどうかを指定します。

Protocol broadcast

IP RIP のようなプロトコルがフレーム・リレー・インターフェースを介して動作できるかどうかを示します。

Congestion monitoring

ネットワーク輻輳 (ふくそう) に対応する輻輳 (ふくそう) 監視フィーチャーが使用可能かどうか (yes または no) を示します。

Emulate multicast

各アクティブ PVC 上のマルチキャスト・エミュレーション・フィーチャーが使用可能かどうか (yes または no) を示します。

CIR monitoring

伝送速度を強制する回線監視フィーチャーが使用可能かどうか (yes または no) を示します。

フレーム・リレー・インターフェースの監視

PVCs P1 allowed

このインターフェースで使用できる VC の数を示します。この数は、インターフェース上でサポートできるアクティブ、輻輳 (ふくそう)、非アクティブ、および除去された VC の最大数です。

Interface down if no PVCs

アクティブ PVC が存在しないときに、ルーターがインターフェースを利用不能と見なすかどうかを示します。

Line speed (bps)

フレーム・リレー・インターフェースの構成されたデータ速度を示します。

Timer T1 seconds

フレーム・リレー・インターフェースがフレーム・リレー・スイッチ LMI エンティティとシーケンス番号交換を行う頻度を示します。

Counter N1 increments

完全な LMI 状態照会を実行する前に満了する必要がある T1 タイマー間隔の回数を示します。

LMI N2 error threshold

N3 ウィンドウ内で発生した、フレーム・リレー・インターフェースのリセットの原因になる管理イベント誤りの数を示します。

LMI N3 error threshold window

N2 誤り限界値を測定するのに使用される、監視された管理イベントの数を示します。

MIR % of CIR

CIR の比率として表される最小 IR

IR % Increment

最大 IR に達するまで、ルーターが BECN のないフレームを受信するたびに IR を増分する比率

IR % Decrement

最小 IR に達するまで、ルーターが BECN を含むフレームを受信するたびに IR を減分する比率

DECnet length field

DECnet 長さフィールド・フィーチャーが使用可能かどうかを示します。一部のフレーム・リレー DECnet フェーズ IV 実現では、フレーム・リレー・マルチプロトコル・カプセル化ヘッダーと DECnet パケットの間に長さフィールドが必要です。DECnet 長さフィールド・フィーチャーが使用可能な場合は、長さフィールドが挿入されます。

Default CIR

このインターフェースのデフォルト CIR を指定します。

Default Burst Size

このインターフェースのデフォルト・バースト・サイズを指定します。

Default Excess CIR

このインターフェースのデフォルト超過バースト・サイズを指定します。

Current receive sequence

フレーム・リレー・インターフェースがフレーム・リレー管理エンティティから受信した現行の受信シーケンス番号を示します。

Current transmit sequence

フレーム・リレー・インターフェースがフレーム・リレー管理エンティティに送信した現行の送信シーケンス番号を示します。

Total status enquiries

フレーム・リレー・インターフェースがフレーム・リレー管理エンティティに行った状態照会の合計数を示します。

Total status responses

フレーム・リレー・インターフェースが、状態照会への応答としてフレーム・リレー管理エンティティから受け取ったレスポンスの合計数を示します。

Total sequence requests

フレーム・リレー・インターフェースがフレーム・リレー管理エンティティに送信したシーケンス番号要求の合計数を示します。

Total responses

フレーム・リレー・インターフェースがフレーム・リレー管理エンティティから受信したシーケンス番号レスポンスの合計数を示します。

Data compression enabled

このインターフェース上でデータ圧縮が使用可能かどうかを示します。

Data encryption enabled

このインターフェース上のデータ暗号化が使用可能かどうかを示します。

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

Fragmentation enabled

このインターフェース上でフレーム・リレー・パケット断片化が使用可能かどうかを示します。

Orphan compression

このインターフェース上のオーファン回線で、データ圧縮が使用可能かどうかを示します。

注: オーファン回線上の圧縮を使用可能にすると、装置上のネイティブ VC が利用可能な圧縮コンテキストの数が減ります。

オーファン圧縮は、PVC と SVC の両方に適用されます。

フレーム・リレー・インターフェースの監視

Compression circuit limit

このインターフェース上でデータを圧縮できる VC の最大数を指定します。

Active compression circuits

このインターフェース上で現在データを圧縮中の VC 数を指定します。

Data encryption enabled

このインターフェース上のデータ暗号化が使用可能かどうかを示します。

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

Active encryption circuits

現在データを暗号化している VC の数を示します。

Virtual Circuit Status:

- *Total allowed*--このインターフェースでの使用状態がアクティブ、輻輳 (ふくそう)、除去、または非アクティブであることが許容される VC の数 (オーファンを含む) を示します。
- *Total configured*--このインターフェースに現在構成されている VC の合計数を示します。
- *Total active*--このインターフェース上のアクティブな VC の数を示します。
- *Total congested*--ネットワーク内の輻輳 (ふくそう) のために減速されている VC の数を示します。
- *Total PVCs left net*--ネットワークから除去された PVC の数を示します。
- *Total PVCs joined net*--ネットワークに追加された PVC の合計数を示します。

permanent-virtual-circuit

フレーム・リレー・インターフェース上に構成されているすべての PVC の一般リンク・レイヤー統計および構成情報を表示します。

例:

```
FR 0>LIST PERMANENT-VIRTUAL-CIRCUITS
```

Circuit Number	Circuit Name	Options	Type/ State	Frames Transmitted	Frames Received
16	Unassigned	R	P/I	0	0
17	Bigcir	F V	P/I	0	0
18	Unassigned		P/I	0	0

```
Circuit type: 0 - Orphan P - PVC S - SVC
Circuit state: A - Active I - Inactive R - Removed C - Congested
R - Required G - Required and belongs to a PVC group
F - circuit is fragmentation capable
c - Data compression capable but not operational
C - Data compression capable and operational
V - circuit is voice forwarding enabled
```


Circuit#

PVC の DLCI を示します。

Circuit Name

回線の名前の ASCII ストリングです。

Orphan Circuit

PVC が未構成回線かどうか (yes または no) を示します。

Type/State

回線の状態、A (アクティブ)、I (非アクティブ)、P (固定)、C (輻輳 (ふくそう))、または R (除去) を示します。

Frames Transmitted

この PVC が送信したフレームの数を示します。

Frames Received

この PVC が受信したフレームの数を示します。

pvc-groups

すべての必須 PVC グループの必須 PVC グループ情報を表示します。各グループは、グループ名、グループ内の回線、および各回線の状態 (アクティブ、非アクティブ、または除去) からなっています。

例:

```
list pvc-groups
Group name          Circuits in group  Circuit status
-----
group1              16                active
                   44                inactive
                   240               removed
```

svcs

状態とは無関係に、インターフェース上のすべての SVC (構成済みまたはオーファンのいずれか) を表示します。

例:

```
FR 1>list svcs
Circuit Name          Remote party number  Circuit State  Call State  DLCI
-----
flotsam               911                  R            N            0
jetsam                666                  R            N            0
Circuit states: A - Active  I - Inactive  R - Removed  C - Congested
Call states: N - Null      I - Call Initiated  O - Outgoing call proceeding
A - Active  D - Disconnect request  R - Release request
```

switched-virtual-circuit

次の例は、単一の SVC について名前別に構成および運用情報を表示します。

例:

```
FR 1>list switched-virtual-circuit flotsam
Circuit Name          Opt- Idle   Outgoing   Incoming
Name                  ions  Timer      Value      Value
-----
flotsam               ILM    60    CIR:       0          0
Call state: Null      Burst:  0          0
Call initiated by: None  DLCI: 0    Excess:    0          0
Remote party number: IE911
Remote subaddress: None
Options: I - call-ins allowed, L - learn protocols, M - multicast required
```

フレーム・リレー・インターフェースの監視

C - compression capable and operational, c - compression capable
E - encryption capable and operational, e - encryption capable

Address type: I - International, U - Unknown
Numbering plan: E - E.164, X - X.121
Subaddress format: N - NSAP, P - private

virtual-circuits

すべての PVC およびアクティブ SVC を、**list permanent-virtual-circuit** コマンドと同一の関連情報とともに表示します。

FR 1>list virtual-circuits

Circuit Number	Circuit Name	Orphan Circuit	Type/State	Frames Transmitted	Frames Received
16	circ16	No	P/A	4	8
17	Unassigned	Yes	c P/I	0	0
18	flotsam	No	S/A	12	10
19	Unassigned	Yes	c P/A	7	2
24	circ24	No	P/R	0	0

P - PVC S - SVC A - Active I - Inactive R - Removed C - Congested

R - Required G - Required and belongs to a PVC group
c - Data compression capable but not operational
C - Data compression capable and operational

voice-forwarding-circuits

音声パケットを転送できるとして定義されたすべての PVC を表示します。

FR 2>list voice-forwarding-circuits

Circuit Name	Circuit Number	Forwarding Network	Forwarding Circuit
circ16	16	2	17
circ17	17	2	16

LLC

LLC コマンドは、LLC 監視プロンプトにアクセスするのに使用します。LLC コマンドは、この新たに表示されたプロンプトで入力します。これらの各コマンドの説明は、271ページの『LLC 監視コマンド』を参照してください。

構文:

llc

注: LLC コマンドは、ソフトウェア・ロードに APPN が含まれている場合にのみサポートされます。

Notrace

notrace コマンドは、個々の回線またはインターフェース全体についてパケット・トレースを使用不可にするのに使用します。特定の回線またはインターフェースのトレースが必要とされるときに、このコマンドをフィルターとして使用することができます。デフォルト設定は、すべての回線をトレースすることです。

構文:

notrace circuit#

circuitname

all

例:

```
notrace 16
    Disables packet tracing on circuit (PVC or SVC) with DLCI 16.
notrace circuit phoenix
    Disables packet tracing on circuit (PVC or SVC) named phoenix.
notrace circuit all
    Disables packet tracing on all circuits on this interface.
```

Set

set コマンドは、指定された VC の認定情報速度 (CIR)、認定バースト速度、および超過バースト速度の値を設定するのに使用します。IR 調整比率の値も設定できます。

このコマンドで行った変更は、構成データには影響を与えず、ルーターがリスタートされるまでしか有効ではありません。

構文:

```
set                circuit . . .
                    ir-adjustment . . .
```

circuit *circuit# or name cirvol bcval beval*

指定された VC の認定情報速度 (CIR)、認定バースト速度、超過バースト速度を設定し、PVC またはアクティブ SVC の運用可能な発信 CIR、Bc、および Be を変更するのに使用することができます。

例:

```
set circuit
Circuit number [16]?
Committed Information Rate (CIR) in bps [1200]?
Committed Burst Size (Bc) in bits [1200]?
Excess Burst Size (Be) in bits [56000]?
```

Circuit Number

16 ~ 1007 の範囲で回線番号を示します。

Committed Information Rate

認定情報速度 (CIR) を示します。CIR は、0、または 300 bps ~ 2 048 000 bps の範囲の値のいずれかにすることができます。デフォルトは 64 Kbps です。詳しくは、454ページの『認定情報速度 (CIR)』を参照してください。

Committed Burst Size

認定バースト (Bc) サイズ/CIR 秒数に相当する測定期間にルーターが送達できる最大データ量 (ビット)。範囲は、300 ~ 2 048 000 ビットです。デフォルト値は 64 Kb です。

注: CIR が 0 として構成されている場合、認定バースト・サイズも 0 に設定され、値の入力を求めるプロンプトは出ません。詳しくは、454ページの『認定バースト (Bc) サイズ』を参照してください。

フレーム・リレー・インターフェースの監視

Excess Burst Size

(認定バースト・サイズ/CIR) 秒数に相当する測定期間にルーターが送達を試みることができる、認定バースト・サイズを超過する未認定データの最大量 (ビット数)。範囲は 0 ~ 2 048 000 ビットです。デフォルト値は 0 です。詳しくは、455ページの『超過バースト (Be) サイズ』を参照してください。

ir-adjustment increment-% decrement-% minimum-IR

最小情報速度 (IR) と、ネットワークの輻輳 (ふくそう) に応じて IR を増分および減分する比率を設定します。

最小 IR (CIR の比率で表す) は、情報速度の下限です。最小比率は 1 で、最大比率は 100 です。デフォルト値は 25 です。

ネットワークの輻輳 (ふくそう) が解消されると、情報速度は、最大情報速度に達するまで、IR 調整増分比率ずつ徐々に増分されます。最小比率は 1 で、最大比率は 100 です。デフォルト値は 12 です。

ネットワークの輻輳 (ふくそう) が発生すると、情報速度は、最小情報速度に達するまで、BECN が入ったフレームを受信するたびに IR 調整減分比率ずつ減分されます。最小比率は 1 で、最大比率は 100 です。デフォルト値は 25 です。

例:

```
set ir-adjustment
IR adjustment % increment [12]?
IR adjustment % decrement [25]?
Minimum IR as % of CIR [25]?
```

Trace

Trace コマンドは、個々の回線またはインターフェース全体のパケット・トレースを使用可能にするか、このインターフェース上のすべての回線のトレース機能をリストするのに使用します。特定の回線またはインターフェースのトレースが必要とされるときに、このコマンドをフィルターとして使用することができます。デフォルト設定は、すべての回線をトレースすることです。

構文:

```
trace all
      circuitname
      circuit#
      list
```

例:

```
trace 16
  Enables packet tracing on circuit (PVC or SVC) with DLCI 16.
trace circuit phoenix
  Enables packet tracing on circuit (PVC or SVC) named phoenix.
trace circuit all
  Enables packet tracing on all circuits on this interface.
```

```
trace list
The following circuits are available for packet trace
Circuit Name          Circuit Number
-----
Unassigned            16
```

```
phoenix                25
jetsam                 0
```

Lists the packet tracing capability of all circuits on this interface.

フレーム・リレー・インターフェースおよび GWCON インターフェース・コマンド

フレーム・リレー・インターフェースには監視用の監視プロセスがありますが、GWCON 環境から **interface** コマンドを使用すれば、ルーターも導入済みインターフェースの完全な統計を表示します。(interface コマンドについての詳細は、149ページの『第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』を参照してください。)

フレーム・リレー・インターフェースについて表示される統計

フレーム・リレー・インターフェースに対して GWCON 環境から **interface** コマンドを実行すると、次のような統計が表示されます。

```
+interface 10
                Self-Test Self-Test Maintenance
Nt Nt' Interface Slot-Port      Passed   Failed   Failed
10 10  FR/0      Slot: 8 Port: 0           2       1       0

Frame Relay MAC/data-link on V.35/V.36 interface

Adapter cable:          V.35 DTE

V.24 circuit: 105 106 107 108 109
Nicknames:   RTS CTS DSR DTR DCD
PUB 41450:   CA  CB  CC  CD  CF
State:       ON  ON  ON  ON  ON

Line speed:          ^ 64.000 Kbps
Last port reset:    1 hour, 20 minutes, 42 seconds ago

Input frame errors:
CRC error                0 alignment (byte length)      0
missed frame            182 too long (> 2062 bytes)     0
aborted frame           0 DMA/FIFO overrun            0
Output frame counters:
DMA/FIFO underrun errors 0 Output aborts sent          0
```

Nt 初期構成時にソフトウェアによって割り当てられたインターフェース番号を示します。

Nt' 初期構成時にソフトウェアによって割り当てられたインターフェース番号を示します。

注: FR ダイヤル回線インターフェースの場合、Nt' は Nt と異なります。Nt' は、ダイヤル回線が実行されている基本インターフェース (ISDN) を示します。

Interface

インターフェースのタイプとそのインスタンス番号を示します。フレーム・リレーは FR 名を持っています。

Slot フレーム・リレーを実行しているインターフェースのスロットを示します。

Port フレーム・リレーを実行しているインターフェースのポートを示します。

フレーム・リレー・インターフェースの監視

Self-test Passed

フレーム・リレー・インターフェースが自己テストに合格した回数を示します。

Self-test Failed

フレーム・リレー・インターフェースが自己テストに失敗した回数を示します。

Maintenance Failed

インターフェースがフレーム・リレー・マネージメントと通信できなかった合計回数を示します。

V.24 circuit, Nicknames, and State

回線、制御信号、ピン割り当てとそれらの状態 (ON または OFF)。

注: 監視出力の記号 - - - は、値または状態が不明であることを示します。

Line speed

送信クロック・レート

Last port reset

前回のポート・リセット以降の時間の長さ

Input frame errors:

CRC error

チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment

長さが 8 の偶数倍でないために廃棄された受信パケットの数

Too short

長さが 2 バイト未満であったために廃棄された受信パケットの数

Too long

構成されたサイズより大きかったために廃棄されたパケットの数

Aborted frame

送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

DMA/FIFO overrun

シリアル・インターフェースがシステム・パケット・バッファ・メモリーにデータを送信する速度が遅かったために、データをネットワークから受信できなかった回数

Missed frame

フレームが装置に到着したときに利用可能なバッファがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

L & F bits not set

シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファが完全なフレームを受け入れたこと

フレーム・リレー・インターフェースの監視

を示します。いずれかのビットがセットされていない場合、パケットは廃棄され、L & F bits not set カウンターが増分され、バッファは消去されて再利用できるようになります。

注: L & F bits not set カウンターはトラフィックによる影響は受けません。

Output frame counters:

DMA/FIFO underrun errors

シリアル・インターフェースがシステム・パケット・バッファ・メモリーからデータを取り出す速度が遅かったために、データをネットワーク上に送信できなかった回数。

Output aborts sent

高位レベルのソフトウェアの要求によって打ち切られた伝送の数

GWCON 環境から interface コマンドを実行すると、フレーム・リレー・ダイヤル回線について次のような統計が表示されます。

+interface 3

Nt	Nt'	Interface	Passed	Self-Test Failed	Self-Test Failed	Maintenance
3	2	FR/1		1	0	0

Frame Relay MAC/data-link on ISDN Primary Rate interface

フレーム・リレー・インターフェースの監視

第30章 ポイント・ポイント・プロトコル・インターフェースの使用

この章では、装置上のインターフェースのポイント・ポイント・プロトコルの使用方法について説明します。本章には、以下の節が含まれています。

- 『PPP の概説』
- 522ページの『PPP リンク制御プロトコル (LCP)』
- 526ページの『PPP 認証プロトコル』
- 531ページの『PPP を用いた AAA の使用』
- 532ページの『PPP ネットワーク制御プロトコル』
- 535ページの『バーチャル・コネクションの使用および構成』

マルチリンク PPP プロトコルの使用については、589ページの『第32章 マルチリンク PPP プロトコルの使用』および 595ページの『第33章 マルチプロトコル PPP プロトコル (MP) の構成および監視』を参照してください。

PPP の概説

PPP は、シリアル・ポイント・ポイント・リンクを介して、データ・リンク・レイヤーでプロトコル・データグラムを転送する方法を提供します。PPP は、以下のサービスを提供します。

- リンク接続を確立、構成、およびテストするためのリンク制御プロトコル (LCP)
- シリアル・ポイント・ポイント・リンク上でプロトコル・データグラムをカプセル化するためのカプセル化プロトコル
- ピア (リモート) 装置の識別子の妥当性を検査し、またユーザー自身の識別子をピアに転送して妥当性検査を依頼するための認証プロトコル (AP)
- 各種のネットワーク・レイヤー・プロトコルの設定および構成を行うためのネットワーク制御プロトコル (NCP)。 PPP では、複数のネットワーク・レイヤー・プロトコルを使用できます。

520ページの図26 は、ポイント・ポイント・シリアル・リンクの例を示しています。

PPP の使用

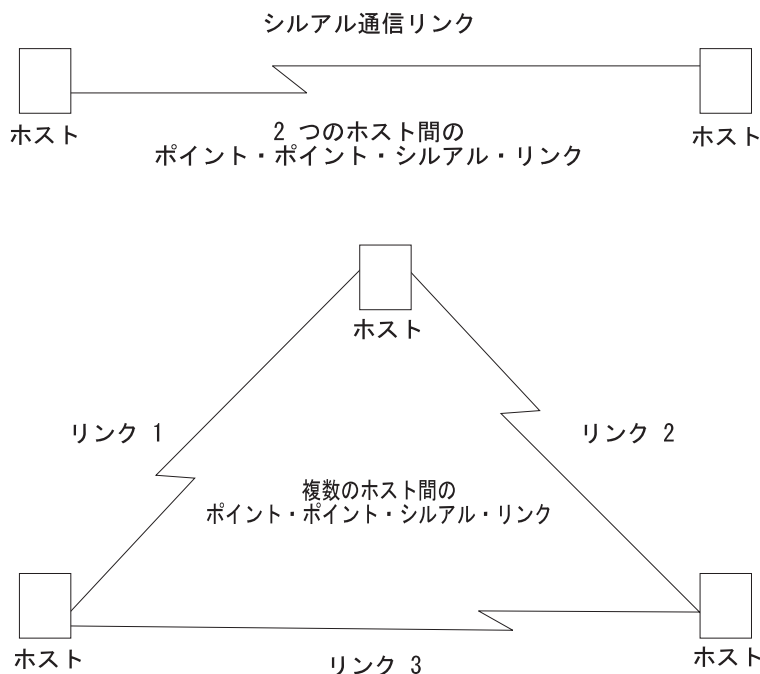


図 26. ポイント・ポイント・リンクの例

PPP は現在、以下の制御プロトコルをサポートしています。

- AppleTalk 制御プロトコル (ATCP)
- DECnet プロトコル制御プロトコル (DNCP)
- Banyan VINES 制御プロトコル (BVCP)
- ブリッジング・プロトコル (BCP、NBCP、および NBFCP)
- インターネット・プロトコル制御プロトコル (IPCP)
- インターネット・プロトコルバージョン 6 制御プロトコル (IPv6CP)
- IPX 制御プロトコル (IPXCP)
- APPN HPR 制御プロトコル (APPN HPRCP)
- APPN ISR 制御プロトコル (APPN ISRCP)
- OSI 制御プロトコル (OSICP)

各端は、始めに LCP パケットを送信して、データ・リンクを構成し、テストします。リンクが確立された後、PPP は NCP パケットを送信して、1 つまたは複数のネットワーク・レイヤー・プロトコルを選択し、構成します。ネットワーク・レイヤー・プロトコルを構成すると、各ネットワーク・レイヤーからのデータグラムをリンクを介して送信できるようになります。以下の節では、これらの概念についてさらに詳しく説明します。

PPP データ・リンク・レイヤー・フレーム構造

PPP は、ハイレベル・データ・リンク制御 (HDLC) フレームと同じ構造のデータ・フレームを転送します。PPP は、単一のフレーム・フォーマットを用いてすべてのデータ交換および制御交換を行うバイト指向の伝送方式を使用します。521ページの図27 は PPP フレーム構造を示しており、その後に各フィールドの詳しい説明があります。

フラグ	アドレス	制御	プロトコル	情報	FCS	Flag
8ビット	8ビット	8ビット	16ビット	可変	16ビット	8ビット

図27. PPP フレーム構造

フラグ・フィールド

フラグ・フィールドは、各フレームを開始および終了し、固有のパターン 01111110 をもっています。通常は、1 つのフラグが、あるフレームを終了し、次のフレームを開始します。リンクに接続されている受信側は、このフラグ・シーケンスを継続的に探索して、次のフレームの開始と同期します。

アドレス・フィールド

アドレス・フィールドは 1 オクテット (8 ビット) で、2 進シーケンス 11111111 (16 進 0xff) が入っています。これは、全ステーション・アドレスと呼ばれます。PPP は個別ステーション・アドレスは割り当てません。

制御フィールド

制御フィールドは 1 オクテットで、2 進シーケンス 00000011 (16 進 0x03) が入っています。このシーケンスは、P/F ビットがゼロにセットされた非番号制情報 (UI) コマンドを識別します。

プロトコル・フィールド

プロトコル・フィールドは PPP によって定義されます。このフィールドは 2 オクテット (16 ビット) で、その値はフレームの情報フィールドにカプセル化されたプロトコル・データグラムを識別します。

'0xC000' ~ '0xFFFF' の範囲のプロトコル・フィールドは、LCP、PAP、CHAP、SPAP、および CCP のようなレイヤー 3 データ (プロトコル・データグラム) を示します。'8000' ~ 'BFFF' の範囲の値は、データグラムがネットワーク制御プロトコル (NCP) に属することを示します。'0' ~ '3FFF' の範囲の値は、特定のデータグラムのネットワーク・プロトコルを識別します。

情報フィールド

情報フィールドには、プロトコル・フィールドに指定されているプロトコルのデータグラムが入っています。これは、ゼロまたはそれ以上のオクテットです。

プロトコル・タイプが LCP の場合、PPP データ・リンク・レイヤー・フレームの情報フィールドには、正確に 1 つの LCP パケットがカプセル化されています。

フレーム・チェック・シーケンス (FCS) フィールド

フレーム・チェック・シーケンス・フィールドは、16 ビット巡回冗長検査 (CRC) です。

PPP リンクは、各種のオプションの使用をネゴシエート (交渉) することにより、基本フレーム・フォーマットを変更することができます。以下の説明は、このような変更を行う前のフレーム・フォーマットに適用されます。PPP LCP パケットは、交渉で決められたオプションに関係なく、常にこのフォーマットでも送信され、伝送路上の同期が失われた場合でも、LCP パケットを認識できるようにされています。

ルーターは、このようなオプションのうちの 2 つをサポートしています。すなわち、アドレスおよび制御フィールド圧縮 (ACFC) とプロトコル・フィールド圧縮 (PFC) です。これらについては、後で詳しく説明します。

PPP リンク制御プロトコル (LCP)

PPP のリンク制御プロトコル (LCP) は、ポイント・ポイント・リンクを確立、構成、保守、および終了します。このプロセスは 4 つのフェーズで行われます。

1. PPP は、ネットワーク・レイヤー・データグラムを交換する前に、最初に LCP 構成パケットを交換して、コネクションをオープンします。このネゴシエーション・プロセスの一部として、PPP は、転送できる最大パケット・サイズや、リンクの各端がネットワーク・トラフィックを伝送する前に認証機構を使用してそれぞれのピアに自分自身を識別する必要があるかどうかなど、さまざまな基本的リンク・レベル・パラメーターについて、リンクの各端で合意が得られるように処理します。

このネゴシエーションが不成功の場合、リンクは『ダウン』と見なされ、ネットワーク・トラフィックを伝送することはできません。ネゴシエーションに成功した場合、LCP が『オープン』状態になり、PPP は次のフェーズに進みます。

2. LCP が正常にオープン状態になったら、リンク確立の次のステップは、認証を実行することです。つまり、リンクの各端は、LCP ネゴシエーションで相手側が指定した『認証プロトコル』を使用して、相手側に自分自身を識別します。

認証が不成功の場合、リンクは『ダウン』としてマークされ、ネットワーク・トラフィックを伝送することはできません。認証に成功した場合、または認証が不要の場合、PPP リンクは次のフェーズに移ります。

3. 認証を交渉した後で、ピア間でリンクの暗号化を交渉します。認証フェーズが完了した後、ルーターは暗号化制御プロトコル (ECP) パケットを使用して、暗号化の使用を交渉します。つまり、リンクの各端は、この PPP リンク上のデータを暗号化するのに使用する暗号化アルゴリズムを交渉します。ECP が『オープン』状態に達することができなかった場合、リンクは『ダウン』としてマークされ、ネットワーク・トラフィックを伝送することはできません。ECP が正常に『オープン』状態に達した場合、または暗号化は不要の場合、PPP リンクは次のフェーズである NCP ネゴシエーション (ECP を除く、これも技術的には NCP です) に移ります。リンクは『オープン』またはこの場合は『アップ』(ただし、まだレイヤー 3 プロトコル・データグラムは転送できません) と見なされます。
4. リンクがオープンしたら、ルーターはネットワーク制御プロトコル (NCP) パケットを使用して、各種のレイヤー 3 プロトコル (たとえば、IP、IPX、DECnet、Banyan Vines) の使用を交渉します。各レイヤー 3 プロトコルには、それぞれ独自の関連ネットワーク制御プロトコルがあります。たとえば、IP には IPCP があり、IPX には IPXCP があります。これらの NCP パケットの基本フォーマットとメカニズムは、すべてのプロトコルで同一であり、基本的には、この節で後述する LCP 機構のスーパーセットです。

各レイヤー 3 プロトコルは、それぞれ個別に交渉されます。特定の NCP の交渉に成功した場合、リンクはそのプロトコルのトラフィックに対して『アップ』になります。LCP の場合と同様に、この交渉の中で構成情報を交換することができます。たとえば IPCP は、IP アドレスを交換したり、“Van Jacobson IP ヘッダー圧縮”の使用を交渉したりすることができます。

LCP と同様に、NCP もそのピアとの交渉が不成功に終わる可能性があります。ピアが特定のプロトコルをサポートしなかったり、一部の構成オプションが受け入れられなかった場合にそうなります。NCP が『オープン』状態に達しなかった場合、他のレイヤー 3 プロトコルが PPP リンクを介して正常にトラフィックの受け渡しを行っていても、そのプロトコルのレイヤー 3 プロトコル・パケットは交換することができません。

- 最後に、LCP はいつでもリンクを終了させることができます。通常はユーザーからの要求によって終了しますが、他の理由で終了することもあります。たとえば、管理上の理由でのリンクのクローズ、アイドル・タイマーの満了、あるいは CHAP 再チャレンジ時に再認証に失敗した場合などです。

PPP LCP、認証、および汎用 NCP 交渉機構の詳細については、RFC 1331、1334、1570、および 1661 を参照してください。

LCP パケット

LCP パケットは、PPP リンクを確立し、管理するのに使用され、おおまかに 3 つのカテゴリに分けることができます。

- リンク確立パケット は、構成情報を交換し、リンクを確立します。
- リンク終了パケット は、リンクを切断するか、あるいは特定の時点にリンクが接続を受け入れていないことを知らせます。また、特定のプロトコルが認知されない (たとえば、NCP ネゴシエーション時に) ことを知らせるのにも使用できます。
- リンク保守パケット は、リンクを監視し、デバッグします。

PPP データ・リンク・レイヤー・フレームの情報フィールドには、正確に 1 つの LCP パケットがカプセル化されます。LCP パケットの場合、プロトコル・フィールドには“リンク制御プロトコル”(16 進 C021) が入ります。図28 は LCP パケットの構造を示しており、その後に各フィールドの詳しい説明があります。

符号	識別子	長さ	データ(オプション)
----	-----	----	------------

図28. LCP フレーム構造 (PPP 情報フィールド内の)

符号 符号フィールドは 1 オクテットの長さで、LCP パケットのタイプを識別します。524ページの表67 の符号は、パケット・タイプの区別を示します。これらについては、後で詳しく説明します。

表 67. LCP パケット符号

符号	パケット・タイプ
1	Configure-Request (リンク確立)
2	Configure-Ack (リンク確立)
3	Configure-Nak (リンク確立)
4	Configure-Reject (リンク確立)
5	Terminate-Request (リンク終了)
6	Terminate-Ack (リンク終了)
7	Code-Reject (リンク確立)
8	Protocol-Reject (リンク確立)
9	Echo-Request (リンク保守)
10	Echo-Reply (リンク保守)
11	Discard-Request (リンク保守)

識別子 識別子フィールドは 1 オクテットの長さで、パケット要求と応答を一致させるのに使用されます。

長さ 長さフィールドは 2 オクテットの長さで、LCP パケットの全長 (すなわち、すべてのフィールドを含めた) を示します。

データ (オプション)

データ・フィールドは、長さフィールドに示されているゼロまたはそれ以上のオクテット数です。このフィールドのフォーマットは、符号によって決まります。

NCP パケットは、構造は LCP パケットと同一ですが、異なる PPP『プロトコル』値を持っているので識別できます。各 LCP パケット・タイプ (符号フィールドによって識別) は、各 NCP に対しても同じ意味を持ちます。ただし、個々の NCP にすべての可能な LCP パケット・タイプが実現されているわけではありません。NCP は通常、LCP で定義されているリンク確立タイプ・パケットはすべて実現されています。また、いくつかの追加 LCP パケット・タイプが実現されている場合もあり、LCP で使用されている以外の追加パケット・タイプを定義することもできます。LCP パケットの場合とは異なり、リンク確立フェーズで LCP によって交渉されたオプションに従って NCP フレームの構造を変更することが可能です。

リンク確立パケット

リンク確立パケットは、ポイント・ポイント・リンクを確立し、構成するもので、以下のパケット・タイプが含まれます。

Configure-Request

LCP パケット符号フィールドは 1 にセットされます。LCP はポイント・ポイント・リンクをオープンしたいときに、このパケット・タイプを送信します。Configure-Request を受信すると、ピア・ステーションの LCP エンティティは、パケットを処理する準備ができていのかどうかに応じて、該当する応答を送信します。

Configure-Ack

LCP パケット符号フィールドは 2 にセットされます。Configure-Request パケット内の各構成オプションが受け入れ可能な場合、相手側はこのパケット・タイプを送信します。Configure-Ack (ack = 確認) を受信すると、発信元ステ

ーションは識別子フィールドを検査します。このフィールドは、最後に送信された `Configure-Request` からの値に一致していなければなりません。そうでない場合、そのパケットは無効です。

両側が `Configure-Request` を送信し、両側が `Configure-Ack` を受信しなければ、リンクはオープンしません。ある方向について交渉されたオプションが、他の方向について交渉されたオプションと異なっても構いません。『マスター・スレーブ』の関係はなく、それぞれの端が対称的に動作します。

Configure-Nak

LCP パケット符号フィールドは 3 にセットされます。`Configure-Request` パケット内の構成オプションのある部分が受け入れ不能である場合、ピアはこのパケット・タイプを送信します。識別子フィールドは受信した

`Configure-Request` からコピーされ、データ (オプション) フィールドには、受信した受け入れ不能の構成オプションが記入されます。識別子フィールドは最後に送信された `Configure-Request` からの値に一致していなければなりません。そうでない場合、そのパケットは無効であり、廃棄されます。

発信元は、`Configure-Nak` パケットを受信すると、修正された、受け入れ可能な構成オプションを入れた新たな `Configure-Request` パケットを送信します。

Configure-Reject

LCP パケット符号フィールドは 4 にセットされます。`Configure-Request` パケット内の構成オプションのある部分が受け入れられない場合、ピアはこのパケット・タイプを送信します。識別子フィールドは受信した `Configure-Request` からコピーされ、データ (オプション) フィールドには、受信した受け入れ不能の構成オプションが記入されます。識別子フィールドは最後に送信された `Configure-Request` からの値に一致していなければなりません。そうでない場合、そのパケットは無効であり、廃棄されます。

発信元は、`Configure-Reject` パケットを受信すると、`Configure-Reject` パケットで受信した構成オプションのいずれも含まない新たな `Configure-Request` パケットを送信します。

Code-Reject

LCP パケット符号フィールドは 7 にセットされます。このパケット・タイプの送信は、受信したパケットの LCP 『符号』フィールドが有効な値と見なされないことを示します。これは誤りを示している可能性があります。ユーザーが使おうとしている機能がピアで実現されていないことを示している場合もあります。

Protocol-Reject

LCP パケット符号フィールドは 8 にセットされます。このパケット・タイプの送信は、サポートされない、または不明のプロトコルが含まれている PPP フレームが受信された (パケットの PPP 『プロトコル』フィールドが認知されなかった) ことを示しています。これは通常、相手側がサポートしないプロトコルの NCP を交渉しようとした場合に起こります。たとえば、DECnet CP (DNCP) が `Config-Request` を送信し、相手側が DECnet について知らない場合、相手側は DNCP に対して LCP `Protocol-Reject` で応答します。

`Protocol-Reject` パケットを受信すると、リンクは不正なプロトコルの送信を停止します。

PPP の使用

注: NCP パケット・タイプと構造は LCP と同じですが、一部の NCP に関連したいくつかの追加『符号』フィールドがあります。

リンク終了パケット

リンク終了パケットはリンクを終了させるもので、以下のパケット・タイプが含まれます。

Terminate-Request

LCP パケット符号フィールドは 5 にセットされます。ポイント・ポイント・リンクをクローズする必要があるときに、LCP はこのパケット・タイプを送信します。これらのパケットは、Terminate-Ack パケットが返送されるまで、または Ack を待っている間に再試行カウンターが超過するまで送信されません。

Terminate-Ack

LCP パケット符号フィールドは 6 にセットされます。Terminate-Request パケットを受信した場合、符号フィールドを 6 にセットして、このパケット・タイプを送信しなければなりません。予期していなかった Terminate-Ack パケットの受信は、リンクがクローズされたことを示します。

リンク保守パケット

リンク保守パケットは、リンクを管理し、デバッグするもので、以下のパケット・タイプが含まれます。

Echo-Request および Echo-Reply

LCP パケット符号フィールドは、それぞれ 9 および 10 にセットされます。LCP は、リンクの両方向のデータ・リンク・レイヤー・ループバック機構を提供するために、これらのパケット・タイプを送信します。これらの機能は、たとえば、障害のあるリンクをデバッグした後でリンクの品質を調べる場合などに便利です。これらのパケットは、リンクがオープン状態にあるときにのみ送信されます。

Discard-Request

LCP パケット符号フィールドは 11 にセットされます。LCP は、データ・リンク・レイヤーのテストのために、このパケット・タイプをデータ受信側に提供します。Discard-Request を受け取ったピアは、そのパケットを廃棄する必要があります。これは、リンクをデバッグする場合に便利です。これらのパケットは、リンクがオープン状態にあるときにのみ送信されます。

PPP 認証プロトコル

PPP 認証プロトコルは、PPP リンクを介して接続されている 2 つのノード間に一種のセキュリティーを提供します。あるボックスで認証が必要な場合、2 つのボックスは LCP レイヤーのリンクの使用に関するネゴシエーションに成功した直後に (LCP が『オープン』状態になるまで LCP パケットが交換されます) 『認証』フェーズに入り、認証パケットを交換します。認証のネゴシエーションが正常に完了するまでは、ボックスはネットワーク・データ・パケットを伝送することも、ネットワーク・プロトコル (NCP トラフィック) の使用を交渉することもできません。

異なるタイプの認証プロトコルを使用できます。つまり、パスワード認証プロトコル (PAP) とチャレンジ/ハンドシェイク認証プロトコル (CHAP) です。Windows ワークステーションおよびピア・ルーターを認証するには、Microsoft PPP CHAP (MS-CHAP) も使用可能です。PAP および CHAP については RFC 1334 に詳細に記述されていますが、この節の後方でも簡単に説明しておきます。MS-CHAP については RFC 1994 で説明されています。

リモート・ダイヤルイン・アクセス・ポートでは、第 3 の認証プロトコルが使用可能です。これは、Shiva が所有権をもつプロトコルである Shiva パスワード認証プロトコル (SPAP) です。詳細については、528ページの『Shiva パスワード認証プロトコル (SPAP)』を参照してください。

あるボックスが相手側に対してそれ自身の認証を要求しているかどうか (要求している場合は、どのプロトコルを使用するか) については、LCP ネゴシエーション・フェーズで判別されます。一方の側が相手側に必要な認証プロトコルの使用法を知らなかったり、その使用を拒否する場合、リンク確立フェーズ (LCP ネゴシエーション) の段階でも、認証は『不成功』と見なすことができます。

リンクの各端は、相手側が自身を認証する方法について、独自の要件を設定します。たとえば、2 つのルーター『A』と『B』が PPP リンクを介して接続されている場合、A 側は B が PAP を使用して自身を A に認証することを要求し、同様に B 側は A が CHAP を使用して自身を識別することを要求するといったことが可能です。また、一方の側が認証を必要とし、他方の側は認証を必要としないというのも有効です。

リンク確立時の初期認証に加えて、一部のプロトコルの認証機能は、ピアが定期的な再証明することを要求することもできます。たとえば、CHAP では、認証機能はいつでも再チャレンジを出すことができ、ピアは正常に応答できなければなりません。そうでないと、リンクは失われます。

リンク上に複数の認証プロトコルが使用可能にされている場合、初期時にルーターは、次の優先順位でそれらの使用を試みます。

1. MS-CHAP
2. CHAP
3. PAP
4. SPAP

注: SPAP は、ダイヤルイン回線が構成された IBM DIAL を備えたインターフェース上でのみ利用可能です。

リモート側が認証要求に対して NAK で応答し、代替を提案した場合、ルーターは、その代替がリンク上で使用可能になっていれば代替を使用します。リモート側がルーターの提案に対して NAK で応答し続け、ルーターで使用可能にされている代替を提案しない場合、リンクは終了されます。

パスワード認証プロトコル (PAP)

パスワード認証プロトコル (PAP) は、ピアが両方向ハンドシェイクを使用して自身のアイデンティティを設定する簡単な方法を提供します。これは初期リンク確立時のみ行われます。リンク確立の後、認証が確認されるかコネクションが終了され

PPP の使用

るまで、ピアは認証機能に ID/パスワードの組みを送信します。パスワードは『解放された』回線を介して送信され、再生や反復的試行および誤ったアタックに対する保護はありません。ピアが試行の頻度とタイミングを制御します。

チャレンジ/ハンドシェーク認証プロトコル (CHAP)

チャレンジ/ハンドシェーク認証プロトコル (CHAP) は、両方向ハンドシェークを使用して、ピアのアイデンティティを定期的に確認するのに使用します。これは初期リンク確立時に行われ、リンク確立後の任意の時点で反復しても構いません。初期リンク確立後に、認証機能はピアに『チャレンジ』メッセージを送ります。ピアは、『単方向ハッシュ』機能を使用して計算された値で応答します。認証機能は、その応答を、自身が計算した予想ハッシュ値と突き合わせて検査します。値が一致している場合、認証は確認されます。そうでない場合、コネクションは終了します。

Microsoft PPP CHAP 認証 (MS-CHAP)

MS-CHAP は、リモート Windows ワークステーションおよびピア・ルーターを認証するのに使用される PPP CHAP の拡張です。MS-CHAP と CHAP は両方とも、PPP のリンク制御プロトコル (LCP) を使用して、必要な認証プロトコルを片方向または両方向でネゴシエーションします。両方とも CHAP プロトコル識別子を PPP プロトコルとして使用します。各プロトコルは、レスポンスの一部として暗号化されたランダム・チャレンジを使用します。

MS-CHAP は、内部 PPP ユーザー・ローカル・リスト・データベースとともに使用することができますが、**フィーチャーの使用と構成** の『ローカルまたはリモート認証の使用』の章で説明されている外部 AAA 認証サーバーとともに使用することはできません。PPP インターフェース上で Microsoft PPP 暗号化 (MPPE) を使用する予定の場合は、MPPE を構成する前に、そのインターフェースで MS-CHAP を使用可能にする必要があります。talk 6 コマンド **enable mschap** は、MS-CHAP を使用可能にするのに使用します。

Shiva パスワード認証プロトコル (SPAP)

注: SPAP は、IBM DIAL ダイヤルイン回線が構成されたインターフェース上でのみ利用可能です。

Shiva パスワード認証プロトコル (SPAP) は、PAP と同様に、ピアが両方向ハンドシェークを使用して自身のアイデンティティを設定する簡単な方法を提供します。リンク確立フェーズが完了した後、認証が確認されるか、接続が終了するか、あるいは再試行カウンターが満了するまで、ピアは認証機能に ID/パスワードを繰り返し送信します。

SPAP は、専有のパスワード暗号化アルゴリズムを使用する、中程度の強さの認証プロトコルです。SPAP は、認証の他に次の機能を提供します。

- パスワードを変更することができる。
- パスワード認証の後、ルーターは、クライアントからの確認応答を要求する構成可能なバナーを送信することができる。

- 追加のセキュリティー・フィーチャーとしてコールバックを使用することができる。
- バーチャル・コネクション

PPP 認証の構成

以下では、2 つの状況での PPP 認証の構成について説明します。

- リモート装置を認証するよう 2210 を構成する。
- リモート装置によって認証されるよう 2210 を構成する。

この 2 つの状況は、それぞれ独立しています。一方または他方を構成することができます。

リモート装置を認証する PPP インターフェースの構成

リモート装置またはダイヤルイン・クライアントを認証するには、次のようにします。

1. PPP インターフェース上の認証を使用可能にする。

- Config> プロンプトで **network** コマンドを入力して、構成する PPP インターフェースを選択する。
- PPP Config> プロンプトで、使用する認証プロトコルを使用可能にする。

次のプロトコルを使用できます。

- PAP
- MS-CHAP

注: MS-CHAP は、PPP ローカル・データベースを使用して認証することはできませんが、認証サーバーを使用することはできません。

- CHAP
- SPAP

注: SPAP は、IBM DIAL ダイヤルイン回線が構成されたインターフェース上でのみ利用可能です。

2. 認証をローカルで行うか、認証サーバーを通して行うかを定める。

- ローカルで認証する場合は、名前とパスワードを PPP ユーザー・データベースに入力します。

Config> プロンプトで **add ppp_user** コマンドを使用します。詳細については、59ページの『Add』を参照してください。

2210 は単一の PPP ユーザー・データベースを維持しています。認証フェーズで、リモート・ルーターまたは装置がその名前とパスワードを装置に送ると、装置はその名前とパスワードが PPP ユーザー・データベース内に存在するかどうか検査します。

- TACACS、TACACS+、または RADIUS を使用して、認証サーバーを通して認証する場合は、認証サーバーに到達するように装置を構成する必要があり、その名前とパスワードがサーバーのデータベースに存在していなければなりません。フィーチャーの使用と構成の『ローカルまたはリモート認証の使用』を参照してください。

リモート装置によって認証される PPP インターフェースの構成

リモート装置またはダイヤルイン・クライアントによって認証されるように装置を構成するには、装置の名前とパスワードを構成します。

1. Config> プロンプトで **network** コマンドを使用して、構成するインターフェースを選択する。
2. PPP Config> プロンプトで **set name** コマンドを使用して、認証フェーズで装置が自身をリモート・ルーターまたは装置に識別する名前とパスワードを提供する。

注: 装置に、フィーチャーの使用と構成 の『ローカルまたはリモート認証の使用』で説明されているように認証を行わせたいのでない限り、次のコマンドは使用しないでください。

- **enable pap**
- **enable chap**
- **enable spap**

注: SPAP は、IBM DIAL ダイヤルイン回線が構成されたインターフェース上でのみ利用可能です。

- **enable mschap**

PPP コールバックの構成

コールバックは、シングル・ユーザー・ダイヤルイン・ソリューションに関連した PPP フィーチャーです。これは 2 つの目標の達成を試みます。目標は、次のとおりです。

- コールバックは、セキュリティの 1 種として使用することができます。この方法で使用されるコールバックは通常、必須コールバックと呼ばれます。必須コールバックがネゴシエーションされる場合、ユーザーの事前設定された番号にダイヤルしてコールバックされます。その場合にのみ、PPP リンクはアップになることが許可されます。
- コールバックは、通話料節約フィーチャーとして実現することもできます。この方法で使用されるコールバックは通常、ローミング・コールバックと呼ばれます。必須コールバックとは異なり、ローミング・コールバックはクライアントによって要求されます。ローミング・コールバックの主な機能は、通話料金をユーザーではなく、DIAL サーバーを維持している会社に請求することです。

コールバックは、ISDN ネットワークを介したダイヤルイン・ダイヤル回線上でのみサポートされます。

例 1: 必須コールバックが使用可能

```
Config>add PPP
Enter user name: [ ]? nocalldback
Password:
Enter password again:
Is this a Single-User or a Network? (Single-User, Network): [Single-User]

IP address for user nocalldback [0.0.0.0]?
Enter HostName: [ ]?
Give 'nocalldback' default time allotted ? (Yes, No): [Yes]
Enable Callback for 'nocalldback' ? (Yes, No): [No] yes
Type of Callback (Roaming Callback, Required Callback): [Roaming Callback] Requ
Dialback number for this user [ ]? 555-1234
Will 'nocalldback' be able to dial-out ? (Yes, No): [No]
```

```

PPP User Name: nocallback
Type: Single User
User IP Address: Interface Default
SubNetMask: 255.255.255.255
Hostname: <undefined>
Time-Allotted: Box Default
Call-Back Type: Required Callback
Phone Number: 543-3186
Dial-Out: Not Enabled
Encryption: Not Enabled

Is information correct? (Yes, No, Quit): [No] yes

```

例 2: コールバックが使用不可

```

Config>add PPP
Enter user name: [ ]? sallydoe
Password:
Enter password again:
Is this a Single-User or a Network? (Single-User, Network): [Single-User]

IP address for user nocallback [0.0.0.0]?
Enter HostName: [ ]?
Give 'no callback' default time allotted ? (Yes, No): [Yes]
Enable Callback for 'no callback' ? (Yes, No): [No]
Will 'no callback' be able to dial-out ? (Yes, No): [No]

PPP User Name: no callback
Type: Single User
User IP Address: Interface Default
SubNetMask: 255.255.255.255
Hostname: <undefined>
Time-Allotted: Box Default
Call-Back Type: Not Enabled
Dial-Out: Not Enabled
Encryption: Not Enabled

Is information correct? (Yes, No, Quit): [No] yes

```

例 3: ローミング・コールバックが使用可能

```

Config>add PPP roaming_callback
Password:
Enter password again:
Is this a Single-User or a Network? (Single-User, Network): [Single-User]

IP address for user roaming_callback [0.0.0.0]?
Enter HostName: []?
Give 'roaming_callback' default time allotted ? (Yes, No): [Yes]
Enable Callback for 'roaming_callback' ? (Yes, No): [No] yes
Type of Callback (Roaming Callback, Required Callback): [Roaming Callback]

Will 'roaming_callback' be able to dial-out ? (Yes, No): [No]n

PPP User Name: roaming_callback
Type: Single User
User IP Address: Interface Default
SubNetMask: 255.255.255.255
Hostname: <undefined>
Time-Allotted: Box Default
Call-Back Type: Roaming Callback
Dial-Out: Not Enabled
Encryption: Not Enabled

Is information correct? (Yes, No, Quit): [No] yes

```

PPP を用いた AAA の使用

この情報については、フィーチャの使用と構成の『ローカルまたはリモート認証の使用』および『認証の構成』を参照してください。

PPP ネットワーク制御プロトコル

PPP には、各種のネットワーク・レイヤー・プロトコルを設定および構成するためのネットワーク制御プロトコル (NCP) ファミリーがあります。NCP は、ポイント・ポイント・リンクの両端で、ネットワーク・レイヤー・プロトコルの構成、使用可能化、および使用不可化を行います。LCP がコネクションをオープンし、リンクがオープン状態に達するまでは、NCP パケットを交換することはできません。

PPP は、以下のネットワーク制御プロトコルをサポートします。

- AppleTalk 制御プロトコル (ATCP)
- Banyan VINES 制御プロトコル (BVCP)
- ブリッジング・プロトコル (BCP、NBCP、および NBFCP)
- コールバック制御プロトコル
- DECnet 制御プロトコル (DNCP)
- IP 制御プロトコル (IPCP)
- IPv6 制御プロトコル (IPv6CP)
- IPX 制御プロトコル (IPXCP)
- OSI 制御プロトコル (OSICP)
- APPN 高性能ルーティング制御プロトコル (APPN HPRCP)
- APPN 中間セッション・ルーティング制御プロトコル (APPN ISRCP)

AppleTalk 制御プロトコル

ATCP は Request for Comments (RFC) 1378 に指定されています。IBM の ATCP の実現は、AppleTalk アドレス・オプションをサポートします。この実現は、全ルーター・モードおよび半ルーター・モードをサポートします。詳細については、*Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 2 巻*の『PPP を介する AppleTalk』を参照してください。

Banyan VINES 制御プロトコル

RFC 1763 に BVCP の記述があります。IBM の BVCP の実現は、どのオプションもサポートしません。

Bridging Control Protocol

BCP は RFC 1638 に指定されています。IBM の BCP の実現は、IEEE 802.5 回線識別オプションおよび Tinygram 圧縮オプションをサポートします。

NetBIOS 制御プロトコル (NBCP) は、Shiva Corporation によって開発された専有の NCP で、IBM Dial In Access to LAN Client for OS/2、DOS、および Windows for single-user dial-in によって使用されます。NBCP は、2210 DIAL サーバーにダイヤルされた、これらのクライアントからの NetBIOS および LLC/802.2 ブリッジ・トラフィックを、接続された LAN にトランスポートします。IBM で実現された NBCP は、MAC-Address および NetBIOS Name Projection オプションをサポートします。

NetBIOS Frame Control Protocol (NBFCP) の仕様は、RFC 2097 に規定されています。NBFCP は、Microsoft Windows 95 および Windows NT Dial-Up Networking clients for single-user dial-in によって使用されます。NBFCP は、2210 DIAL サーバーにダイヤ

ルインされた、これらのクライアントからの NetBIOS ブリッジ・トラフィックを、接続された LAN にトランスポートします。IBM で実現された NBFCP は、Name-Projection、Peer-Information、および IEEE-MAC-Address-Required オプションをサポートします。

コールバック制御プロトコル

注: CBCP は、IBM DIAL ダイヤルイン回線が構成されたインターフェース上でのみ利用可能です。

コールバック制御プロトコル (CBCP) は、Microsoft ダイヤルアップ・ネットワーキング・クライアントによりコールバックをネゴシエーションするのに使用されます。2210 は、単一ユーザーによって指定された番号へのコールバック (ローミング・コールバック) および管理者によって指定された番号へのコールバック (必須コールバック) をサポートしています。番号のリストを呼び出す CBCP オプションは、サポートされていません。

CBCP コールバックを使用したい PPP ユーザーには、何らかの形式の認証 (PAP、CHAP、SPAP または MS-CHAP など) が使用可能にされている必要があります。CBCP 用の構成パラメーターはありません。(それをいつ使用するかは、クライアントが決めます。) コールバック用の PPP ユーザーの構成については、530ページの『PPP コールバックの構成』を参照してください。

DECnet IV 制御プロトコル

DNCP は RFC 1762 に指定されています。IBM の実現は、どの DNCP オプションもサポートしません。

IP 制御プロトコル

IPCP は RFC 1332 に指定されています。IBM の実現は、次のオプションをサポートします。

- RFC 1144 に記述されている Van Jacobsen IP ヘッダー圧縮
- IP アドレスの要求

このインターフェースには、IP アドレスを要求することができます。このインターフェースについて IP 構成で動的アドレスが使用可能にされる場合、接続が確立されるたびに、ピアがアドレスを提供します。

- IP アドレス

ルーターは、その IP アドレスを送信したり、ピアからの IP アドレスを受け入れたり、あるいは要求された場合は、ピアに IP アドレスを提供したりすることができます。特定のインターフェース上のルーターが『Send Our Address』用に構成されており、そのインターフェースに有効な番号制 IP アドレスがある場合、IPCP は初期 Configure-Request でオプション 3 (IP アドレス) としてそのアドレスを送信します。また、その PPP インターフェースに有効な番号制アドレスが構成されている場合、ピアがオプション 3 (IP アドレス) を 0.0.0.0 にセットした Configure NAK を送信した場合にも、IPCP はそのアドレスを送信します。IPCP は、非番号制アドレスはピアに送信しません。

PPP の使用

ピアはこのアドレスを指定することも (『クライアント指定』と呼ばれます)、初期構成要求のオプション 3 で 0.0.0.0 を送信してルーターからアドレスを要求することもできます。ルーターはこのアドレスを、認証されたユーザー・プロファイルまたはインターフェース自体から入手できます。ユーザー・プロファイル・アドレスがインターフェース・アドレスより優先されます。ユーザー・プロファイルからのアドレスを提供したくない場合は、プロファイル内のそのユーザーのアドレスを 0.0.0.0 のままにしておけば、ルーターがそのインターフェースに構成されているリモート・アドレスを提供します。インターフェースまたはユーザー・プロファイルにリモート・アドレスが構成されておらず、ピアがアドレスの要求を続けた場合は、IPCP は失敗します。

ルーターは、ネゴシエーションに成功したアドレスの PPP インターフェースへの静的ルートを自動的に追加して、データがそのダイヤルイン・クライアントに正しく送達されるようにします。IPCP コネクションが何らかの理由で終了した場合、この静的ルートは除去されます。デフォルトでは、このルートのネットマスクは 255.255.255.255 (ホスト・ルート) になります。ただし、認証されたユーザーのプロファイルにネットマスクを指定すれば (529ページの『PPP 認証の構成』を参照)、これ以外のネットマスクを使用して、PPP リンクを介して複数のホストにルーティングすることも可能です (必要な場合は、ルートを発見するために RIP またはその他のルーティング・プロトコルも使用できます)。

IPv6 制御プロトコル

IPv6 制御プロトコルは、RFC 2023 に指定されています。IBM の IPv6CP の実現では、ルーターは、その IP アドレスを送信したり、ピアからの IP アドレスを受け入れたり、あるいは要求された場合は、ピアに IP アドレスを提供したりすることができます。特定のインターフェース上のルーターが『Send Our Address』用に構成されており、そのインターフェースに有効な番号制 IP アドレスがある場合、IPv6CP は初期 Configure-Request でオプション 3 (IP アドレス) としてそのアドレスを送信します。また、その PPP インターフェースに有効な番号制アドレスが構成されている場合、ピアがオプション 3 (IP アドレス) を ::/0 にセットした Configure NAK を送信した場合にも、IPv6CP はそのアドレスを送信します。IPv6CP は、非番号制アドレスはピアに送信しません。

同位はこのアドレスを指定することも (『クライアント指定』と呼ばれます)、初期構成要求のオプション 3 で ::/0 を送信してルーターからアドレスを要求することもできます。ルーターはインターフェースからこのアドレスを入手します。このインターフェースに構成されたリモート・アドレスがなく、ピアがアドレスを要求し続ける場合、IPv6CP は失敗します。

ルーターは、ネゴシエーションに成功したアドレスの PPP インターフェースへの静的ルートを自動的に追加して、データがそのダイヤルイン・クライアントに正しく送達されるようにします。IPv6CP コネクションが何らかの理由で終了した場合、この静的ルートは除去されます。デフォルトでは、このルートの接頭部の長さは 128 (ホスト・ルート) です。

IPX 制御プロトコル

IPXCP は RFC 1552 に指定されています。IBM の実現は、どの IPXCP オプションもサポートしません。

OSI 制御プロトコル

OSICP は RFC 1377 に指定されています。IBM の OSICP の実現は、どのオプションもサポートしません。

APPN HPR 制御プロトコル

拡張ピアツーピア・ネットワーク機能 (APPN) 高性能ルーティング (HPR) 制御プロトコルは、RFC 2043 に指定されています。この制御プロトコルでは、どのオプションも交渉されません。

APPN ISR 制御プロトコル

拡張ピアツーピア・ネットワーク機能 (APPN) 中間セッション・ルーティング (ISR) 制御プロトコルは、RFC 2043 に指定されています。この制御プロトコルでは、どのオプションも交渉されません。

PPP インターフェースの暗号化の構成については、フィーチャーの使用と構成 の『データ暗号化の使用と構成』を参照してください。

バーチャル・コネクションの使用および構成

バーチャル・コネクション (VC) とは、事前に決められた時間だけ非アクティブになるときに、中断することができる DIAL ダイアルイン回線です。接続を中断できるので、アクティブでない DIAL ダイアルイン・クライアントの回線料金を節約することでネットワーク・コストを制御するのに役立ちます。接続をアクティブに保持する代わりに、システムはセッションに関する情報を保管してから、コールをクローズします。同じ DIAL ダイアルイン・クライアントがサーバーに再接続すると、セッション情報が復元され、接続は中断がなかったかのように再開されます。詳細については、536ページの『VC の構成』を参照してください。

指定された時間だけ中断されていた VC を終了するよう DIAL サーバーを構成することができます。VC は手動でいつでも終了することもできます。関連するコマンドについては、フィーチャーの使用と構成 の **set DIAL** コマンドおよび『DIAL グローバル監視コマンド』を参照してください。

VC の考慮事項

VC を構成するときは、以下のことに留意してください。

- AAA ローカル・リストまたは RADIUS 認証を使用できるのは、VC の使用中だけです。
- VC は IPX をサポートしません。VC を使用するようにユーザーを構成すると、そのユーザー用の IPX サポートは使用不可にされます。

PPP の使用

- クライアント構成は、VC の中断および再開を制御します。DIAL サーバーは、接続のその局面を制御することはできません。
- VC は、MP バンドルを通じて設定することができます。
- VC は L2TP を介して稼働することはできません。
- 中断された VC は、現行のネットワーク管理ツールを使って表示することはできません。
- インターフェースによってリモート・ユーザーに IP アドレスを割り当てないでください。あるクライアントがそれと VC を設定するインターフェースを別のクライアントが使用することがありうるので、VC がサーバーと再接続しようとするとき、IP アドレスが使用中であるため、接続が失敗することがあります。
- ダイヤルイン・クライアントは、認証に SPAP を使用する必要があります。

VC の構成

Config> プロンプトで DIAL クライアントを追加するときに、VC を構成します。ユーザーを構成するときに、最大中断時間および非活動タイムアウトに DIAL ダイヤルイン・デフォルト（フィーチャーの使用と構成 の **set DIAL** コマンド）を使用したり、特定のクライアントに特定の値を構成したりすることができます。次の例は、DIAL ダイヤルイン・クライアント『jose』の VC についての最小構成を示しています。

```
Config>
Config> add ppp
Enter user name: []? jose
Password:
Enter password again:
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route? (hostroute, netroute): [hostroute]
IP address: [0.0.0.0]?
Enter hostname for dynamic DNS: []?
Allow Virtual Connections ? (Yes, No): [No] Yes
  Use Box Default inactivity timeout value and maximum suspended time? (Yes, No): [Yes] No
  User-based Max Suspend Time (hours)
  0-48 0=unlimited: [12] ? 10
  User-based Inactivity Timeout (seconds)
  10-1024: [30] ? 60
Give 'jose' default time allotted ? (Yes, No): [Yes]
Enable callback for 'jose' ? (Yes, No): [No]
Will 'jose' be able to dial-out ? (Yes, No): [No]
```

```
PPP user name: jose
User IP address: Interface Default
Netroute Mask: 255.255.255.255
  Hostname:
  Time allotted: Box Default
  Callback type: Not Enabled
  Dial-out: Not Enabled
```

```
Is information correct? (Yes, No, Quit): [Yes]
```

```
User 'jose' has been added
Config>
```

最大バーチャル・コネクション、アイドル・タイムアウト期間、およびグローバル・デフォルト最大中断時間についてボックス・レベルのデフォルト値を表示するには、DIAL 機能で DIALs config>**list vc-parameters** コマンドを使用してください。

PPP の使用

すべての接続について、これらのパラメーターを最大中断時間および非活動タイムアウトとともに表示するには、DIAL 機能で **list all** コマンドを使用します。フィーチャーの使用と構成 の『DIAL グローバル監視コマンド』を参照してください。

第31章 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

この章では、装置内のポイント・ポイント・プロトコル・インターフェースの構成コマンドおよびオペレーショナル・コマンドについて説明します。本章には、以下の節が含まれています。

- 『インターフェース構成プロセスへのアクセス』
- 540ページの『ポイント・ポイント構成コマンド』
- 560ページの『インターフェース監視プロセスへのアクセス』
- 560ページの『ポイント・ポイント監視コマンド』
- 585ページの『ポイント・ポイント・プロトコル・インターフェースと GWCON インターフェース・コマンド』

インターフェース構成プロセスへのアクセス

ルーターの構成プロセスにアクセスするには、以下の手順を使用します。このプロセスにより、特定のインターフェースの構成 プロセスにアクセスすることができます。

1. OPCON プロンプト (*) で **status** コマンドを入力して、CONFIG の PID を見つける。(status コマンドの出力例については、11 ページを参照してください。)
2. OPCON プロンプトで、OPCON **talk** コマンドと CONFIG の PID を入力する。(このコマンドの詳細については、33ページの『OPCON プロセスとは』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

talk 6 コマンドを入力すると、CONFIG プロンプト (Config>) がコンソールに表示されます。最初に **CONFIG** に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

3. CONFIG プロンプトで **list devices** コマンドを入力して、ルーターが現在構成されているネットワーク・インターフェース番号を表示する。
4. インターフェース番号を記録する。
5. CONFIG **network** コマンドと、構成するインターフェースの番号を入力する。たとえば、次のように入力します。

```
Config> network 1
```

これで、該当する構成プロンプト (たとえば、トークンリングの場合は TKR Config>) がコンソールに表示されます。

注: ネットワーク・インターフェースは、すべてがユーザーによる構成が可能とは限りません。構成できないインターフェースの場合は、次のようなメッセージが出ます。

```
That network is not configurable
```

PPP インターフェースの構成 (Talk 6)

PPP インターフェース構成プロンプトへのアクセス

PPP config> プロンプトを表示するには、次のようにします。

1. Config> プロンプトで **list devices** コマンドを入力して、インターフェースのリストを表示する。
2. まだ行っていない場合は、Config> プロンプトで **set data-link ppp** と入力して、シリアル・インターフェースの 1 つのデータ・リンク・プロトコルを PPP に設定する。たとえば、次のように入力します。

```
Config> set data-link ppp
Interface Number [0]? 2
```

3. **network** と入力し、続けて PPP インターフェースの番号を入力する。たとえば、次のように入力します。

```
Config> network 2
PPP config>
```

ポイント・ポイント構成コマンド

表68 は、PPP 構成コマンドの要約を示しており、本節の残りの部分で、これらのコマンドについて説明します。コマンドは PPP config> プロンプトで入力します。

表 68. ポイント・ポイント構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Disable	データ圧縮 (CCP)、DTR 回線処理、CHAP、PAP、ECP を使用不可にします。リモート LAN アクセス・フィーチャー・イメージの SPAP 認証も使用不可にします。
Enable	データ圧縮 (CCP)、DTR 回線処理、CHAP、PAP、ECP を使用可能にします。リモート LAN アクセス・フィーチャー・イメージの SPAP 認証も使用可能にします。
List	ポイント・ポイント・インターフェース・プロトコル、パラメーター、およびオプションに関連するすべての情報をリストします。
Set	物理回線 (HDLC) パラメーター、LCP パラメーター、一般 NCP パラメーター、および各種の NCP 特有の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。13ページの『下位レベル環境の終了』を参照してください。

Disable

データ圧縮、認証プロトコル、multilink PPP, and the Lower DTR feature.

構文:

```
disable                ccp
                        chap
                        enp
                        lower-dtr
                        mp
```

mppemschappap

- ccp** インターフェース上のデータ圧縮の使用を使用不可にします。詳細については、フィーチャーの使用と構成の『データ圧縮の構成と監視』を参照してください。
- chap** チャレンジ/ハンドシェイク認証プロトコルの使用を使用不可にします。詳細については、528ページの『チャレンジ/ハンドシェイク認証プロトコル (CHAP)』を参照してください。
- ecp** これは、ルーターがこのインターフェースでの ECP 暗号化の使用を強制しないようにすることができます。ピアが ECP を使用している場合には、インターフェースは暗号化制御プロトコル (ECP) を受け入れ、これを実行します。

注: 暗号化サポートはオプションであり、**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。ソフトウェア使用者の手引きの CONFIG プロセス **load** コマンドを参照してください。

ルーター内での複数の暗号化の使用 (暗号化を IP セキュリティー・レイヤーおよびフレーム・リレーまたは PPP データ・リンク・レイヤーの両方で使用する) は、米国政府輸出規制によって制限されています。これは、厳密な輸出規制のもとにあるソフトウェア・ロード (128 ビット・キーとトリプル DES をもつ 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。

lower-dtr

使用不可にされている専用シリアル・ライン・インターフェースのデータ端末レディー (DTR) 信号の扱い方を決めます。このパラメーターが『使用不可』(デフォルト) に設定され、インターフェースが使用不可の場合、DTR 信号は降下しません。

- mp** このインターフェース上のマルチリンク・プロトコル (MP) を使用不可にします。詳細については、589ページの『第32章 マルチリンク PPP プロトコルの使用』を参照してください。

例:

```
disable mp
Disabled as a MP link
```

- mppe** このインターフェース上で Microsoft ポイント・ポイント暗号化 (MPPE) を使用不可にします。

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

mschap

このインターフェース上で MS-CHAP 認証を使用不可にします。MS-CHAP を使用不可にすると、MPPE が mandatory (必須) または optional (任意選択) のどちらとして構成されているかに応じて、MPPE に 2 つの影響があります。MPPE が mandatory の場合は、MS-CHAP を使用不可にすると、リンクがダウンします。MPPE が optional の場合は、MS-CHAP を使用不可にするとり

PPP インターフェースの構成 (Talk 6)

リンクを介しての MPPE は使用不可になります。詳細については、528ページの『Microsoft PPP CHAP 認証 (MS-CHAP)』を参照してください。

pap パスワード認証プロトコルの使用を使用不可にします。詳細については、527ページの『パスワード認証プロトコル (PAP)』を参照してください。

spap Shiva パスワード認証プロトコル (SPAP) の使用を使用不可にします。

注: SPAP は、IBM DIAL ダイヤルイン回線が構成されたインターフェース上でのみ利用可能です。

Enable

この PPP インターフェース上のデータ圧縮、暗号化、認証プロトコル、Lower-DTR、およびマルチリンク PPP プロトコルを使用可能にします。複数の認証プロトコルが使用可能にされている場合、装置は次の優先順位でそれらの使用を試みます。

1. MS-CHAP
2. CHAP
3. PAP

構文:

```
enable                ccp  
                        chap  
                        ecp  
                        lower-dtr  
                        mp  
                        mppe  
                        mschap  
                        pap
```

ccp インターフェース上のデータ圧縮の使用を使用可能にします。

注: HSSI アダプター上の PPP インターフェースについてデータ圧縮を使用可能にすることはお勧めしません。

chap チャレンジ/ハンドシェイク認証プロトコルの使用を使用可能にします。再チャレンジ間隔を指定するように求めるプロンプトがでます。初期認証フェーズが完了した後に定期的に再チャレンジしない場合は、0 を指定します。詳細については、528ページの『チャレンジ/ハンドシェイク認証プロトコル (CHAP)』を参照してください。

例:

```
enable chap  
Rechallenge Interval in seconds (0=NONE) [0] 10  
CHAP enabled
```

ecp 暗号化制御プロトコル (ECP) と交渉して、このインターフェース上でデータ暗号化を使用することを使用可能にします。これが行われると、MS-CHAP がリンクのアクティブな認証プロトコルでない限り、暗号化が使用可能にされ、有効な暗号化キーを持っているすべての PPP ユーザーは、このポートに接続するために ECP を使用しなければなりません。認証プロトコルが

PPP インターフェースの構成 (Talk 6)

MS-CHAP である場合は、ECP は使用できません。暗号化は、MPPE を使用して行う必要があります。暗号化が使用可能にされていない PPP ユーザーはまだこのインターフェースに接続することができます。

ECP を使用可能にすると、ローカル・ルーターの ECP 暗号化キーを入力するよう求められます。リモート・ユーザーを構成するために Config> プロンプトで **talk 6 add ppp-user** コマンドを使用するときは、リモート・ユーザーの暗号化キーも提供する必要があります。MPPE では、ローカルまたはリモート・ユーザーのどちらでも暗号化キーを構成する必要はありません。

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

lower-dtr

使用不可にされている専用シリアル・ライン・インターフェースのデータ端末レディー (DTR) 信号の扱い方を決めます。このパラメーターが『使用不可』(デフォルト) に設定され、インターフェースが使用不可の場合、DTR 信号は降下しません。

Lower DTR が『使用可能』に設定されている場合は、インターフェースが使用不可のときには、DTR 信号は降下します。この動作が適している状況は、インターフェースが WAN 再ルートの代替リンクとして構成されており、インターフェースが、DTR 信号の状態に基づいてダイヤル接続を維持するダイヤルアウト・モデムに接続されているような場合です。

インターフェースが使用不可のときは、DTR 信号は下がり、モデムは接続をダウンに保ちます。インターフェースが使用可能になると (WAN 再ルートのバックアップ・シナリオにより)、DTR は上がり、モデムは保管しているバックアップ・サイトへの番号をダイヤルします。1 次インターフェースが復元すると、代替インターフェースは使用不可にされ、DTR は下がって、モデムはダイヤル接続を切断します。

以下のケーブル・タイプがサポートされます。

RS-232
V.35
V.36

注: **enable lower-dtr** コマンドは、PPP ダイヤル回線インターフェースではサポートされません。

mp

このインターフェース上のマルチリンク・プロトコル (MP) を使用可能にします。詳細については、589ページの『第32章 マルチリンク PPP プロトコルの使用』を参照してください。

例:

```
enable mp
Enabled as a MP link
Is this link a dedicated MP link? [no] yes
MP interface for this MP link? [0] 3
```

mppe [mandatory/optional] [stateless/stateful]

Microsoft ポイント・ポイント暗号化 (MPPE) を使用可能にします。MS-CHAP がインターフェース上で使用可能にされていない場合、そのインターフェース上で MPPE を使用可能にすることはできません。詳細については、フィー

PPP インターフェースの構成 (Talk 6)

チャーの使用と構成 の“暗号化プロトコルの使用と構成”という章の Microsoft ポイント・ポイント暗号化 (MPPE) を参照してください。

mandatory

クライアントとサーバーは MPPE を交渉する必要があります。さもないと、リンクは除去されます。

optional

クライアントは MPPE を交渉しようとしませんが、交渉が失敗する場合は、PPP リンクはアクティブなままになります。

stateless

各パケットを送信した後、セッション・キーが再生成されます。この機能は現在、Microsoft ダイアルアップ・ネットワーキング (DUN) クライアントによってサポートされていません。

stateful

256 のパケットを送信するごとに、セッション・キーが再生成されます。

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

mschap

MS-CHAP 認証を使用可能にします。MS-CHAP を使用可能にすると、認証機能再チャレンジ間隔を提供するよう求められます。秒数で表したこの値は、認証を再確認するために、認証機能が認証要求の受信側に別のチャレンジを送信する前に経過する時間の長さを定義します。値 0 は、初期認証の後にそれ以上チャレンジが送信されないことを示します。

2210 のローカル名を認証するためにピア・ルーターが構成されている場合に、2210 の名前を構成するには、**set name** コマンドを使用します。

フィーチャーの使用と構成 の『ローカルまたはリモート認証の使用』の章で説明されているように、外部認証サーバーが構成されている場合は、MS-CHAP を使用可能にすることができないことに注意してください。詳細については、528ページの『Microsoft PPP CHAP 認証 (MS-CHAP)』を参照してください。

pap パスワード認証プロトコルの使用を使用可能にします。詳細については、527ページの『パスワード認証プロトコル (PAP)』を参照してください。

List

list コマンドは、PPP インターフェースとそのプロトコル・パラメーターおよびオプションに関連する情報を表示するのに使用します。

構文:

```
list                all  
                    bcp  
                    ccp
```

ecp
hdlc
ipcp
ipv6cp
lcp
ncp

all PPP インターフェースに関連するすべてのオプションおよびパラメーターをリストします。

list all コマンドは、以下で説明する個々の **list...** パラメーターのすべての出力を表示します。

bcp ブリッジング・ネットワーク制御プロトコル・オプションをリストします。

例:

```
list bcp
BCP Options
-----
Tinygram Compression:DISABLED
```

Tinygram Compression:

Tinygram 圧縮の使用可能/使用不可を表示します。

ccp データ圧縮が使用可能にされている場合は、現在選択されているデータ圧縮オプションを表示します。詳細については、**フィーチャーの使用と構成**の『データ圧縮の構成と監視』を参照してください。

Microsoft ポイント・ポイント暗号化 (MPPE) とデータ圧縮が両方とも使用可能にされている場合、データ圧縮のタイプは MPPC です。

ecp 暗号化制御プロトコルの現在の状態を表示します。

例:

```
list ecp
ECP Options
-----
Data Encryption enabled
Algorithm list: DESE-CBC
DESE (Data Encryption Standard Encryption Protocol)
```

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

Data Encryption Enabled/Disabled

インターフェース上のデータ暗号化が使用可能か使用不可かを示します。

Algorithm List

サポートされる暗号化アルゴリズムを表示します。DES (RFC 1969 に記述) が、現在サポートされている唯一の暗号化アルゴリズムです。

hdlc ハイレベル・データ・リンク制御 (HDLC) プロトコルに関連するパラメーターを表示します。PPP ダイアル回線インターフェースでは、『list hdlc』オプションは利用不能です。ダイアル回線の場合、ハードウェア・データ・リン

PPP インターフェースの構成 (Talk 6)

ク・パラメーターは、PPP ダイアル回線ではなく、基本ネットワークの機能です。詳細については、743ページの『第45章 ダイアル回線の構成および監視』を参照してください。

例:

```
list hdlc
Encoding: NRZ
Idle State: Flag
Clocking: Internal
Cable type: V.35 DCE
Speed (bps): 6400

Transmit Delay Counter: 0
Lower DTR: Disabled
```

Encoding:

HDLC 伝送符号化法、NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転)。

Idle State:

インターフェースがデータを転送していないときにポイント・ポイント・リンク上で転送されるビット・パターン、フラグまたはマーク

Clocking:

インターフェースのクロック、外部または内部

Cable type:

使用するケーブルのタイプ (RS-232、V.35、または V.36) を指定します。

Speed (bps):

インターフェースの物理データ速度。クロックが内部の場合、これは内部クロックによって生成されるデータ速度です。

Transmit Delay Counter:

フレーム相互間に送信されるフラグの数

Lower DTR:

使用可能または使用不可。Lower DTR が使用可能のとき、WAN 再ルートの代替リンクが不要になると、ルーターは DTR 信号を下げます。DTR 信号が降下すると、モデムは代替リンクの専用回線接続を終了します。

注:

1. **list hdlc** コマンドは、PPP ダイアル回線インターフェースではサポートされません。
2. このコマンドは、構成されたケーブル・タイプの Lower DTR がサポートされている場合にのみ、Lower DTR 状態を表示します。
3. HSSI アダプター上の PPP インターフェースに対するこのコマンドは、上記の HDLC パラメーター・リストのサブセットを表示します。

ipcp インターネット・プロトコル制御プロトコル・オプションをリストします。

例:

```
list ipcp
IPCP Options
-----
IPCP Compression:          None
```

PPP インターフェースの構成 (Talk 6)

```
Request an IP Address          No
Send Our IP Address:          Yes
Remote IP Address to Offer if Requested: 10.0.0.3
```

IPCP compression

PPP ハンドラーが圧縮された IP ヘッダーを受け入れるかどうかを示します。PPP は Van Jacobson TCP/IP ヘッダー圧縮 (RFC 1144) をサポートします。ポイント・ポイント・リンクが低いボー・レートで動作しているときは、このオプションを使用可能にしてください。

値『Van Jacobson』は、ヘッダー圧縮がサポートされることを示します。値『NONE』は、ヘッダー圧縮が受け入れられていないことを示します。

Request an IP Address

IPCP が初期『構成要求』でこの PPP インターフェースのローカル IP アドレスをリンクのリモート側から検索するように構成されているかどうかを示します。

Send Our IP Address

IPCP が初期『構成要求』でこの PPP インターフェースのローカル IP アドレスをリンクのリモート側に送信するように構成されているかどうかを示します。一部の PPP 実現では、この情報を必要とします。

ipv6cp

インターネット・プロトコル バージョン 6 制御プロトコル・オプションをリストします。

例:

```
list ipv6cp
IPv6CP Options
-----
Send Our IP Address:          Yes
```

Send Our IP Address

IPv6CP が初期『構成要求』でこの PPP インターフェースのローカル IP アドレスをリンクのリモート側に送信するように構成されているかどうかを示します。一部の PPP 実現では、この情報を必要とします。

lcp

リンク制御プロトコルのパラメーターおよびオプションをリストします。

例:

PPP 7 Config>list lcp

```
LCP Parameters
-----
Config Request Tries:          20   Config Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:              1522   Magic Number:             Yes
Peer to Local (RX) ACCM:      A0000
Protocol Field Comp(PFC):      No   Addr/Cntl Field Comp(ACFC): No

Authentication Options
-----
Authenticate remote using:     none
Identify self as:              ibm
```

PPP インターフェースの構成 (Talk 6)

リンク制御プロトコルには、リモート・ピアを認証するために使用される認証プロトコルが含まれます。認証プロトコルが CHAP または Microsoft PPP CHAP (MS-CHAP) のいずれかである場合、再チャレンジ間隔が表示されません。

例:

PPP 7 Config>list lcp

```
LCP Parameters
-----
Config Request Tries:          20   Config Nak Tries:          10
Terminate Tries:              10   Retry Timer:              3000

LCP Options
-----
Max Receive Unit:             1522  Magic Number:             Yes
Peer to Local (RX) ACCM:      A0000
Protocol Field Comp(PFC):     No    Addr/Cntl Field Comp(ACFC): No

Authentication Options
-----
Authenticate remote using:    MSCHAP or SPAP or CHAP or PAP [Listed in priority order]
CHAP Rechallenge Interval:    0
MSCHAP Rechallenge Interval:  0
Identify self as:             ibm
```

Config Request Tries:

PPP リンクのオープンを試みているときに、LCP がピア・ステーションに configure-request パケットを送信した回数

Config Nak Tries:

PPP リンクのオープンを試みているときに、LCP がピア・ステーションに configure-nak (『not acknowledged』) パケットを送信した回数

Terminate Tries:

PPP リンクをクローズするときに、LCP がピア・ステーションに terminate-request パケットを送信した回数

Retry Timer:

『Config tries』パラメーターによって設定された回数に従ってパケット転送を続行する前に経過するミリ秒数

Max Receive Unit:

リンクによって処理される最大情報フィールド (パケット) サイズを表示します。

Peer to Local (Rx) ACCM

非同期伝送路上のルーターにパケットを転送するときに、ピアが『エスケープ』する必要がある文字を表示します。

Magic Number:

マジック番号ループバック検出オプションが使用可能かどうかを示します。

Protocol Field Comp (PFC):

PFC オプションが使用可能かどうかを示します。

Addr/Cntl Field Comp(ACFC):

ACFC が使用可能かどうかを示します。

Authenticate remote using:

使用可能にされている認証プロトコルのリスト。

Identify Self As:

set name コマンドで設定された名前。

ncp すべてのネットワーク制御プロトコルのパラメーターをリストします。

例:

```
list ncp
NCP Parameters
-----
Config Request Tries:          20  Config Nak Tries:          10
Terminate Tries:              10  Retry Timer:                3000
```

Config Request Tries:

PPP リンクのオープンを試みているときに、NCP がピア・ステーションに `configure-request` パケットを送信した回数

Terminate Tries:

Terminate-Ack を待っている間に、NCP が PPP リンクをクローズする前に `Terminate-Request` を送信した回数

Config Nak Tries:

PPP リンクのオープンを試みているときに、NCP がピア・ステーションに `configure-nak` (not acknowledged) パケットを送信した回数

Retry Timer:

NCP の `configure-request` パケット (リンクをオープンするため) および `terminate-request` パケット (リンクをクローズするため) の転送がタイムアウトになる前に経過するミリ秒数

LLC

LLC コマンドは、LLC 構成環境にアクセスするのに使用します (ソフトウェア・ロードに APPN が含まれている場合にのみ利用可能です)。各コマンドについての説明は、267ページの『LLC 構成コマンド』を参照してください。

構文:

llc

Set

set コマンドは、HDLC パラメーター、LCP オプションとパラメーター、IPCP オプション、BCP オプション、および NCP パラメーターを設定するのに使用します。

『パラメーター』は、再試行カウントのように内部動作に関連するものです。『オプション』は、相手側と交渉されるものです。

注:

1. コマンド・オプション・プロンプトの直後の値は、そのオプションの現行設定値です。それらは必ずしも、この章に示されているデフォルト値とは限りません。
2. **set hdlc** コマンドは、PPP ダイアル回線インターフェースではサポートされません。

構文:

```
set                                bcp
                                     ccp options
```

PPP インターフェースの構成 (Talk 6)

ccp algorithms
hdlc...
ipcp
ipv6cp
lcp...
name...
ncp...

bcp ブリッジング制御プロトコル (BCP) パラメーターを設定します。

例:

```
set bcp  
TINYGRAM COMPRESSION [no]:
```

Tinygram Compression

Tinygram 圧縮が使用されるかどうかを示します。このオプションは、低速 (64 Kbps 以下) 伝送路を介してブリッジするときの問題が起こりやすいプロトコルには便利です。これらのプロトコルは、データとフレーム・チェックサムの間でゼロを追加して、プロトコル・データ単位 (PDU) を最小サイズまで埋め込みます。Tinygram 圧縮は、ゼロを除去し、フレーム・チェックサムを送信側で保存します。受信側でパケットを最小長さに復元します。

ccp options

圧縮アルゴリズムの構成可能オプションに関するプロンプトを出します。一部のオプションは、WAN リンク上のピア・ルーターとの PPP ネゴシエーションによって、後で変更することができます。詳細については、『フィーチャーの使用と構成』の『データ圧縮の構成と監視』を参照してください。

例:

```
set ccp options  
STAC: check mode (0=none, 1=LCB, 2=CRC, 3=Seq, 4=Ext) [3]?  
STAC: # histories [1]?
```

STAC: check mode (0=none, 1=LCB, 2=CRC, 3=Seq, 4=Ext)

STAC 圧縮データグラムには通常、リンクの両端が圧縮パケットの紛失または破壊を認知するのに使用する検査値が含まれており、送信側と受信側のヒストリーを再同期するための何らかのアクションが必要です。

注: 不良パケットを検出できないと、後続のすべてのデータが正しく圧縮されない可能性があります。

このオプションは、使用する正確な形の検査値を設定します。以下の 1 つを選択してください。

- 0** None: 検査値は使用されません。検査値がないと、パケットの紛失、シーケンス誤り、または破壊を調べる方法がありません。基礎のデータ・リンクが高信頼性の順序保存パケット送達を行わない限り、このモードは使用しないでください。
- 1** LCB: 『縦方向制御バイト』が使用されます。これは単純な 8 ビット排他 OR チェックサムです。受信側はパケットの紛失

PPP インターフェースの構成 (Talk 6)

またはシーケンス誤りを検出できず、PPP フレーム・チェックサムの方が高い信頼性でパケットの整合性をテストできるので、これを使用することは、まったくお勧めできません。

- 2 CRC: 16 ビットの巡回冗長検査文字が使用されます。これは、パケットの整合性のテストとして LCB よりは良いと言えますが、受信側はやはりパケットの紛失やシーケンス誤りを検出できず、またフレーム・チェックサムと大きく重複することになるので、この使用もあまりお勧めできません。
- 3 SEQ: 8 ビットのシーケンス番号が使用されます (デフォルト)。これは運用上優れた方式です。ヒストリーの数が 0 でない場合は、これ以外のモードを使用しないように強くお勧めします。ただし、ある種の RFC 非準拠のルーターとのインターオペラビリティのために別のモードを使用することが必要になる場合があります。
- 4 EXT: シーケンス番号モードに似ている拡張モード。各パケットにシーケンス番号が組み込まれますが、圧縮されたフレーム・フォーマットが、より大きく変更されます。拡張モードは、ピアとの再同期の方法が、他のモードとは異なっています。つまり、2 つのノード間のシグナルは、別個の CCP 制御パケットではなく、圧縮されたデータグラムヘッダーで渡されるフラグに基づいて行われます。

拡張モードは、ある種の非 RFC 準拠のインプリメンテーションとの整合性のために提供されています。モード 3 をサポートしないクライアントの場合にのみ使用してください。

STAC: # histories

これは、STAC 圧縮エンジンによって使用される圧縮『コンテキスト』または『ヒストリー』の数を設定します。

非ゼロ値は、圧縮エンジンが指定された数のヒストリーを維持し、そこに以前にパケットで送信されたデータに関する情報を保持することを意味します。このヒストリー・データは、圧縮の効率を改善するのに使用されます。

受信側も同様のヒストリーを維持しており、送信側と受信側のヒストリーの同期が保たれている限り、受信側は受信したパケットを正しく解凍することができます。ヒストリーの同期が外れると、パケットは使用不能データとして廃棄されます。リンクの品質が非常に悪くない限り、通常はヒストリーの数は 1 に設定します。

ゼロの値は、送信される各パケットは、過去に送信されたパケットに関係なく圧縮されることを意味しており、常に受信側によって高信頼性で解凍される可能性があります。しかし、圧縮機能は残っている過去のパケットから何も情報を取り出せないため、圧縮の効率はあまりよくないのが一般的です。

一部のインプリメンテーションは、複数のヒストリーをサポートし、データ・ストリームを別々のストリームに分けて、独立して圧縮します。ルーターは、PPP リンクでの複数のヒストリーの使用をサポートしません。

PPP インターフェースの構成 (Talk 6)

ccp algorithms list-of-algorithms

使用する圧縮アルゴリズムの正確なリストを指定します。優先順位は、リスト内のエントリーの順序によって決まります。リンクで MPPE が起動すると、CCP アルゴリズムの順序は無視され、Microsoft ポイント・ポイント圧縮 (MPPC) だけが使用されます。

リンクは、別のノードと圧縮を交渉するときに、プロトコルの全リストを優先順にピア・ノードに提供します。ピア・ノードは、優先順位リストから使用できる最初のプロトコルを選択する必要があります。複数のプロトコルを使用可能にすると、ピアはリンク上で使用する圧縮アルゴリズムを指示できるようになります。あるアルゴリズムを避けたい場合は、そのアルゴリズムをリストに指定しないようにします。

none を指定すると、圧縮を使用不可にするのに有効なプロトコルが使用できなくなります。有効な圧縮アルゴリズムは、次のとおりです。

STAC-LZS

RFC 1974 に記述されている STAC-LZS

MPPC RFC 2118 に記述されている Microsoft ポイント・ポイント圧縮アルゴリズム

例:

```
set ccp algorithms
PPP 6 Config>set ccp alg
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
```

hdlc cable cable type

HDLC ケーブル・タイプ (インターフェースに接続されている) を、以下のタイプの 1 つに設定します。

RS-232 DTE
RS-232 DCE
V35 DTE
V35 DCE
V36 DTE
V36 DCE
X21 DTE
X21 DCE
HSSI DTE
HSSI DCE

表69 はいろいろなアダプターで構成できるケーブル・タイプをリストしています。

表69. 2210 インターフェースのケーブル・タイプ

アダプター・タイプ	ケーブル・タイプ
8 ポート EIA 232	RS-232 DTE および RS-232 DCE
6 ポート V.35/V36	V.35 DCE、V.35 DTE、V.36 DCE、または V.36 DTE
8 ポート X.21	X.21 DCE および X.21 DTE
1 ポート HSSI	HSSI DCE および HSSI DTE*

PPP インターフェースの構成 (Talk 6)

*注: HSSI DCE ケーブルが使用される場合、他方の装置も HSSI DCE ケーブルを使用するよう構成する必要があります。

例: **set hdlc cable rs-232 dce**

DTE ケーブルは、ルーターをあるタイプの DCE 装置 (たとえば、モデムまたは DSU/CSU) に接続するときに使用します。

DCE ケーブルは、ルーターが DCE として動作し、直接接続のためのクロックを提供するときに使用します。

hdlc clocking *external* または *internal*

モデムまたは DSU に接続するには、外部クロックを構成し、**set hdlc cable** コマンドを使って該当する DTE ケーブルを選択します。回線速度を構成するには、**set hdlc speed** コマンドを使用します。

別の DTE 装置に直接接続するには、内部クロックを構成し、**set hdlc cable** コマンドを使って該当する DCE ケーブルを選択し、**set hdlc speed** コマンドを使ってクロック/回線速度を構成します。

デフォルト値: external

例: **set hdlc clocking internal**

注: クロック・タイプは、PPP が HSSI アダプター上で構成されているときは、構成可能ではありません。クロック・タイプは、ケーブル・タイプによって決定されます。HSSI DCE ケーブル・タイプが構成されるときは内部クロックが使用され、HSSI DTE ケーブル・タイプが構成されるときは外部クロックが使用されます。

hdlc encoding *NRZ* または *NRZI*

インターフェースの HDLC 伝送符号化法を設定します。符号化規則は、NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) に設定できます。NRZ は、広く一般的に使用されている符号化規則であり、一方の NRZI は一部の IBM 構成で使用されます。デフォルト値は NRZ です。

注: 符号化は、HSSI アダプター上の PPP インターフェースで NRZ に設定され、構成可能ではありません。

例: **set hdlc encoding nrz**

hdlc idle flag or mark

データ・リンク・アイドル状態をフラグまたはマークに設定します。

フラグ・オプションは、フレーム間に連続フラグ (7E 16 進数) を提供します。

マーク・オプションは、フレーム間の伝送路をマーキング状態 (OFF, 1) にします。

注: アイドルは、HSSI アダプター上の PPP インターフェースで flag に設定され、構成可能ではありません。

例: **set hdlc idle flag**

hdlc speed *value*

PPP インターフェースの構成 (Talk 6)

内部クロックの場合は、このコマンドを使用して送信および受信クロック回線の速度を指定します。

外部クロックの場合は、このコマンドは WAN/シリアル回線の動作には影響を与えませんが、一部のプロトコル (IPX など) がルーティング・コスト・パラメーターを判別するのに使用する速度を設定します。速度は、実際の回線速度に一致するように設定する必要があります。速度が構成されていない場合、プロトコルは 1 000 000 bps の速度を想定します。

有効値:

内部クロック: 表70 を参照してください。

外部クロック: 表71 を参照してください。

表 70. 2210 インターフェースに内部クロックが使用されるときの回線速度

アダプター・タイプ	速度範囲
8 ポート EIA 232	9600 ~ 64 000 bps
6 ポート V.35/V.36	9600 ~ 460 800 bps、1 544 000 bps、または 2 048 000 bps
8 ポート X.21	9600 ~ 460 800 bps、1 544 000 bps、または 2 048 000 bps
1 ポート HSSI	22 368 000 bps または 44 736 000 bps

表 71. 2210 インターフェースに外部クロックが使用されるときの回線速度

アダプター・タイプ	速度範囲
8 ポート EIA 232	2400 ~ 64 000 bps
6 ポート V.35/V.36	2400 ~ 2 048 000 bps
8 ポート X.21	2400 ~ 2 048 000 bps
1 ポート HSSI	1 544 000 bps ~ 52 000 000 bps

例: `set hdlc speed 56000`

`hdlc transmit-delay value`

フレーム相互間に送信されるフラグの数を設定します。このコマンドの目的は、シリアル・ラインを減速して、相手側の旧型で低速のシリアル装置に整合させることです。

範囲は 0 ~ 15 です。デフォルトは 0 です。

注: 8 ポート EIA- 232E アダプター、6 ポート V.35/V.36 アダプター、または 8 ポート X.21 アダプター上の PPP インターフェースに非ゼロの伝送遅延を構成する場合、`set hdlc speed` コマンドを使用して回線速度を構成する必要があります。

例: `set hdlc transmit-delay 15`

ipcp そのリンクのインターネット・プロトコル制御プロトコル・オプションを設定します。

例:

```
set ipcp
IP COMPRESSION [yes]:
Number of Slots: [16]?
Request an IP address [no]:
Send our IP address [yes]:
Note: unnumbered interface addresses will not be sent.
Interface remote IP address to offer if requested (0 for none) [0.0.0.0]? 10.0.0.3
```

IPCP compression

PPP ハンドラーが圧縮 IP データを受け入れるかどうかを選択します。PPP は、RFC 1144 に記述されている Van Jacobson (VJ) TCP/IP ヘッダー圧縮をサポートします。ポイント・ポイント・リンクが低いポー・レートで動作しているときは、このオプションを使用可能にする必要があります。

この値を **yes** に設定すると、圧縮オプションが使用可能になります。この値を **no** に設定すると、オプションは使用不可能になります。デフォルト設定値は **no** です。

Slots 使用可能にされている圧縮のタイプを調べるときに参照するために保存される IP ヘッダーの数を設定します。範囲は 1 ~ 16 です。デフォルト値は 16 です。

Request an IP address

このインターフェースのローカル IP アドレスをリンクのリモート側から検索する必要があるかどうかを指定します。このリンクの相手側が IP アドレスを提供する場合は、このオプションを **yes** に設定する必要があります。これは、ISPs (インターネット・サービス提供者) によって提供される典型的なフィーチャーです。

この要求されたアドレスが利用可能になるには、このインターフェースが適切な IP 構成をもつ必要があります。特に、このインターフェースで Dynamic-Address を使用可能にする必要があります。

注: **Request an IP address** が **yes** に設定される場合は、次の質問である **Send Our IP address** は、表示されません。

Send Our IP address

ローカル IP アドレスをリンクのリモート側に送信するかどうかを指定します。リンクの相手側が IP アドレスを必要とする場合は、このオプションを **yes** に設定する必要があります。

この値を **yes** に設定すると、インターフェースに番号制 IP アドレスが構成されている場合 (つまり、アドレスが 0 で始まっていない場合)、IPCP は PPP インターフェースの IP アドレスを送信します。このオプションが **no** に設定され、ピアが IP アドレス・オプションを 0.0.0.0 にセットした Configure NAK を送信した場合、2210 は、番号制アドレスが構成されている場合には、PPP インターフェースのアドレスで応答します。

ipv6cp

リンクの IPv6 制御プロトコル・オプションを設定します。

例:

```
set ipv6cp
Send Our IP address [no]:
```

Send Our IP address

ローカル IPv6 アドレスをリンクのリモート側に送信するかどうかを指定します。リンクの相手側が IPv6 アドレスを必要とする場合は、このオプションを **yes** に設定します。

PPP インターフェースの構成 (Talk 6)

このパラメーターを **yes** に設定すると、インターフェースに番号制 IPv6 アドレスが構成されている場合 (つまり、アドレスが 0 で始まっていない場合)、IPv6CP は PPP インターフェースの IPv6 アドレスを送信します。このオプションが **no** に設定され、ピアが IPv6 アドレス・オプションを `::/0` にセットした **Configure NAK** を送信した場合、2210 は、番号制アドレスが構成されている場合には、PPP インターフェースのアドレスで応答します。

lcp options or parameters

PPP リンクのリンク制御プロトコル・オプションおよびパラメーターを設定します。

例:

```
set lcp options
Maximum Receive Unit (bytes) [2048]?
Magic Number [yes]:
Peer-to-Local Async Control Character Map (RX ACCM) [A0000] ?
Protocol Field Compression (PFC) [no]?
Addr/Cntl Field Compression (ACFC) [no]?
```

Maximum receive unit

1 つのデータグラムで転送される情報フィールドの最大サイズを設定します。範囲は 576 ~ 4089 バイトです。デフォルト値は 2048 です。

Magic number

マジック番号オプションが使用可能かどうかを指定します。マジック番号は、シリアル・ライン構成内のループバック・リンクを検出する方法を提供します。このオプションが使用可能の場合、リンクはシステム・クロックを乱数発生ルーチンとして使用します。生成された乱数は、マジック番号と呼ばれます。

LCP は、マジック番号が存在する (つまり、マジック番号オプションが使用可能にされている) 構成要求を受信すると、受信したマジック番号をピアに送信した最後の構成要求内のマジック番号と比較します。2 つのマジック番号が異なっている場合、リンクはループバックと見なされません。2 つの番号が同一の場合、PPP ハンドラーはリンクをダウンにし、マジック番号を再交渉するために再度アップにすることを試みます。

この値を **Yes** に設定すると、マジック番号オプションが使用可能になります。この値を **no** に設定すると、オプションは使用不可になります。デフォルト設定値は **Yes** です。

Async Control Character Map

非同期伝送路上のルーターにパケットを転送するときに、ピアが『エスケープ』する必要がある文字を示します。これにより、特定の重要な ASCII 制御文字 (XON や XOFF など) をリンク上で透過的に転送することができます。

32 ビットのビット・マスクを 16 進数で指定します。マスクの位置 'N' のビットがセットされている場合、対応する ASCII 文字 'N' をエスケープする必要があります (LSB はビット番号 0 で、ASCII NUL 文字に対応します)。

PPP インターフェースの構成 (Talk 6)

このオプションのデフォルト値は '0A0000' で、XON および XOFF (control-Q および control-S) をエスケープする必要があることを示します。これは、XON/XOFF を使用してソフトウェアのハンドシェイクを行うモデムのために取られている処置です。これが問題でない場合には、ACCM をゼロ (どの文字もエスケープしない) に変更することをお勧めします。

LCP は常に ACCM の交渉を望み (同期伝送路でさえも)、PPP 監視プロセスの **list lcp** コマンドによって、交渉された値が表示されます。しかし、同期伝送路では『エスケープ』機構ではなく『ビット・スタッフィング』機構が採用されているので、ACCM は同期伝送路上では意味をもたないのが通常です。ただし、ルーターが同期から非同期への変換を行うモデムに接続されている場合は、意味を持つことがあります。その場合、その値は非同期側に接続されているモデムの要件を反映させることが必要です。

Addr/Cntl Field Compression (ACFC)

ピアがアドレスおよび制御フィールドの圧縮を採用できるかどうかを指定します。

ACFC オプションが LCP によって正常に交渉されている場合には、リンク上でやり取りされるデータグラムでは、各パケットを開始するアドレスおよび制御フィールド・バイトを省略しても構わないことを意味します。これらのバイトは常に 0xFF 03 で、実際の情報は提供しません。ACFC を使用可能にすることは、転送されるデータグラムが 2 バイト短くなることを意味します。

正確に言うと、ユーザーが ACFC を使用可能に設定することは、受信側の能力を示していることとなります。ACFC を使用可能にし、LCP がその交渉に成功した場合、相手側はローカル側に転送するパケットに ACFC を採用できるようになります (ほとんどの PPP オプションはこのように動作します)。ローカル側は、相手側もそのようなパケットを処理する能力があることを示した場合にのみ、アドレスおよび制御フィールドを含まないパケットを転送します。

ACFC を使用可能にすることは、たとえば、相手側がそのオプションを受け入れたとしても、相手側にアドレスおよび制御フィールドなしでパケットを送信することを義務付けるものではありません。ACFC を使用可能にすることは、オプションで ACFC を使用しても構わないこと、およびルーターはその着信パケットを処理できることを、ピアに通知するに過ぎません。ピアが ACFC を処理できることを示した場合、ACFC がローカルで使用可能にされているかどうかに関係なく、ルーターは常に転送するパケットで ACFC を実行します。

LCP パケットは、常にアドレスおよび制御フィールドを付けて送信されます。これにより、リンクの同期が失われても、LCP パケットが認知されることが保証されます。

Protocol Field Compression (PFC)

ピアがプロトコル・フィールドの圧縮を採用するかどうかを指定します。

PPP インターフェースの構成 (Talk 6)

『yes』を指定し、PFC オプションが LCP によって正常に交渉された場合、転送するパケットで 1 バイト節約するために、'0x0000'～'0x00FF' の範囲のこれらのプロトコル値の『プロトコル』フィールドから先行ゼロ・バイトを省略しても構いません。この範囲には、大多数のレイヤー 3 プロトコル・データグラムが含まれます。

PPP プロトコル値はすべて、プロトコルの上位バイトには偶数値、下位バイトには奇数値が割り当てられています (ISO 3309 アドレス・フィールドの拡張機構に記述されている汎用機構の使用の一部)。そのため、受信側はプロトコル値の先行バイトが省略されていることを容易に検出できるので (プロトコル・フィールドの最初のバイトは偶数ではなく奇数)、PFC を使用してもフレームの解釈があいまいになることはありません。

PFC は、ACFC と同様に、受信側の能力であり、前述の ACFC の説明が PFC にも当てはまります。

例:

```
set lcp parameters
Config tries [20]?
NAK tries [10]?
Terminate tries [10]?
Retry timer (mSec) [3000]?
```

注: コマンド・オプション・プロンプトの直後の値は、そのオプションの現行設定値です。これは必ずしも、この章に示されているデフォルト値とは限りません。

Retry timer

LCP の configure-request パケット (リンクをオープンするため) および terminate-request パケット (リンクをクローズするため) の転送がタイムアウトになる前に経過する時間 (ミリ秒) を設定します。このタイマーが満了するとタイムアウトになり、configure-request および terminate-request パケットの転送が停止します。範囲は 200 ～ 3000 ミリ秒です。デフォルト設定値は 3000 ミリ秒です。

Config tries

PPP リンクをオープンするために LCP が configure-request パケットをピア・ステーションに送信する回数を設定します。デフォルト値は 20 です。範囲は 1 ～ 100 です。

最初の configure-request パケットが送信された後、再試行タイマーがスタートします。これはパケット紛失を防止するために行われます。

NAK tries

PPP リンクのオープンを試みているときに、LCP がピア・ステーションに configure-nak (nak = not acknowledged) パケットを送信する回数を設定します。デフォルト値は 10 です。範囲は 1 ～ 100 です。

LCP は、受け入れ不能の構成オプションを含んでいる configure-request パケットを受信すると、configure-nak パケットを送信します。これらのパケットは、提供された構成オプションを拒否し、変更された受け入れ可能な値を提案するために送信されます。

Terminate tries

PPP リンクをクローズするために LCP がピア・ステーションに terminate-request パケットを送信する回数を設定します。デフォルト値は 10 です。範囲は 1 ~ 100 です。

最初の terminate-request パケットが送信された後、再試行タイマーがスタートします。これはパケット紛失を防止するために行われます。

name ルーターが別のルーターからの認証要求に応答するときに使用する名前を設定します。

注:

1. この製品では、リンク上のピアに送信する名前およびパスワードに使用する『大文字小文字』はそのまま保たれますが、すべての名前およびパスワードを小文字で入力した方が、他のベンダーの製品とのインターオペラビリティが容易です。
2. 他の実現では、この製品でサポートされているのと同じ最大長の名前を扱えない場合があります。そのような場合、認証機能から無効な名前があることを知らせるメッセージが出るだけです。このタイプのメッセージを受け取った場合は、ルーター ID を短くしてみてください。
3. このコマンドは、ローカル・ルーターの名前を設定します。ローカル・データベースを使用してリモート・ユーザーを追跡したい場合は、Config> プロンプトで talk 6 add ppp-user コマンドを使用して、各リモート・ユーザーをローカル・データベースに追加します。代替方法は、フィーチャーの使用と構成の『ローカルまたはリモート認証の使用』の章で説明されている外部 AAA 認証サーバーを構成することです。

注: 外部 AAA 認証サーバーは、MS-CHAP では使用できません。

例:

```
set name
PPP 7 Config>set name
Enter Local Name: [ ]? newyork
Password:
Enter password again:
PPP Local Name = newyork
```

ncp parameters

ほとんどの NCP の基本動作パラメーターを設定します。

注: このコマンドには特定のインターフェースを通してアクセスしますが、このコマンドはすべての PPP インターフェースのパラメーターをリセットします。

例:

```
set ncp parameters
Config tries [20]
NAK tries [10]?
Terminate tries [10]?
Retry timer (mSec) [3000]?
```

Config tries

PPP リンクをオープンするために NCP が configure-request パケットをピア・ステーションに送信する回数を設定します。範囲は 1 ~ 100 です。デフォルト値は 20 です。

PPP インターフェースの構成 (Talk 6)

このアクションは、指定された 1 組の構成オプションを使用して NCP コネクションをオープンしたいことを示します。configure-request パケットが送信された後、再試行タイマーがスタートします。これはパケット紛失を防止するために行われます。

NAK tries

PPP リンクのオープンを試みているときに、NCP がピア・ステーションに送信する configure-nak (nak = not acknowledged) パケットの数を設定します。範囲は 1 ~ 100 です。デフォルト値は 10 です。

受け入れ不能の構成オプションを含んでいる configure-request パケットを受信すると、NCP は configure-nak パケットを送信します。これらのパケットは、提供された構成オプションを拒否し、変更された受け入れ可能な値を提案するために送信されます。

Terminate tries

PPP リンクをクローズするために NCP がピア・ステーションに送信する terminate-request パケットの数を設定します。範囲は 1 ~ 100 です。デフォルト値は 10 です。

このアクションは、NCP コネクションをクローズしたいことを示します。terminate-request パケットが送信された後、再試行タイマーがスタートします。これはパケット紛失を防止するために行われます。

Retry timer

NCP の configure-request パケット (リンクをオープンするため) および terminate-request パケット (リンクをクローズするため) の転送がタイムアウトになる前に経過する時間 (ミリ秒) を設定します。このタイマーが満了するとタイムアウトになり、configure-request および terminate-request パケットの転送が停止します。範囲は 200 ~ 30000 ミリ秒です。デフォルト設定値は 3000 ミリ秒です。

インターフェース監視プロセスへのアクセス

PPP インターフェース監視プロセスにアクセスするには、次のようにします。

1. + プロンプトで **interface** と入力して、構成されたインターフェースのリストを表示する。
2. **network** と入力し、続けて PPP インターフェースの番号を入力する。

```
+ network 2
PPP>
```

ポイント・ポイント監視コマンド

この節では、ポイント・ポイント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 PPP> プロンプトで入力します。561ページの表72 は、コマンドを示しています。

注: このコマンドで利用可能なオプションは、ルーター・ソフトウェアで利用可能なプロトコルによって決まります。たとえば、ルーター・ソフトウェア (イメージ) に APPN サポートが含まれていない場合、**list isrcp**、**list isr**、**list hprcp**、**list hpr**、および **llc** コマンドは利用不能です。

PPP インターフェースの監視 (Talk 5)

bcp - Bridging (ASRT) CP
brg - Bridging (ASRT)
stp - Spanning Tree Protocol
nbc - NetBios
nbfc - NetBios Frame
ipcp - Internet Protocol CP
ip - Internet Protocol
ip6cp - Internet Protocol version 6 CP
ip6 - Internet Protocol version 6
ipxcp - Novell IPX CP
ipx - Novell IPX
atcp - AppleTalk (Phase 2) CP
ap2 - AppleTalk (Phase 2)
dncp - DECnet IV CP
dn - DECnet IV
osicp - ISO's OSI CP
osi - ISO's OSI
bvc - Banyan VINES CP
vines - Banyan VINES
isrcp - APPN ISR CP
isr - APPN ISR
hprcp - APPN HPR CP
hpr - APPN HPR

all ポイント・ポイント・インターフェースと PPP パラメーターおよびオプションに関連したすべての情報およびカウンターをリストします。このコマンドで表示される出力は、すべての個別の **list item** コマンドからの表示の組み合わせです。

注: あるネットワーク制御プロトコルがインターフェース上で利用不能の場合、そのネットワーク制御プロトコルの **list** コマンドに対して、プロトコルまたは統計情報が得られないことを知らせるメッセージが表示されます。

cbcp コールバック制御プロトコルの統計をリストします。

例: list cbcp

CBCP Statistics	In	Out
-----	----	-----
Packets:	0	0
Octets:	0	0
Callback attempts:	0	
Successful callbacks:	0	

Packets

現行のポイント・ポイント・インターフェースを介して送信 (out) および受信 (in) された CBCP パケットの合計数を示します。

Octets

CBCP フレームの場合、現行のポイント・ポイント・インターフェースを介して送受信されるオクテットの合計バイト数を示します。

Callback attempts

進行中のものを含めて、試行された CBCP コールバックの数

Successful callbacks

正常に完了したコールバックの数

control

制御プロトコルの交渉されたオプションまたはその他の状態情報をリストします。

```
ccp
ecp
lcp
bcp
nbcP
nbfcP
ipcp
ipxcp
atcp
dncp
osicp
bvcp
isrcp
hprcp
```

リスト制御 CCP コマンドの例**STAC-LZC の例:**

```
list control ccp
CCP State:          Open
Previous State:     Ack Sent
Time Since Change:  264 hours, 56 minutes and 58 seconds

Compressor:  STAC-LZS histories 1, check_mode SEQ
Decompressor: STAC-LZS histories 1, check_mode SEQ

MPPE : Negotiated 40 bit stateful
```

MPPC の例:

```
list control ccp
CCP State:          Open
Previous State :    Listen
Time Since Change:  167 minutes

Compressor : none
Decompressor : none

MPPE : Negotiated 40 bit stateful
```

リスト制御 CCP の例の中の用語の定義**CCP state**

ポイント・ポイント・リンクの現行状態。『Open』の場合、このリ

PPP インターフェースの監視 (Talk 5)

リンクでは圧縮の交渉に成功しています。Open でない場合は、リンク上では圧縮は実行されていません。MPPE の交渉に成功した場合は、『Open』としても表示されます。

Previous State

現行状態フィールドに表示されている状態の前のポイント・ポイント・リンクの状態

Compressor

交渉された圧縮機能と使用されているオプションを示します。

Decompressor

交渉された解凍機能と使用されているオプションを示します。

MPPE 交渉された MPPE オプション。これらのパラメーターの説明については、talk 6 **enable mppe** コマンドを、詳細については、*フィーチャーの使用と構成* の“暗号化プロトコルの使用と構成”の章の Microsoft ポイント・ポイント暗号化 (MPPE) を参照してください。

リスト制御 ECP コマンドの例

例:

```
PPP x>list control ecp
```

```
ECP State:          Open
Previous State:     Ack Sent
Time Since Change:  16 minutes and 40 seconds
```

```
Local (transmit) encrypter: DES
Remote (receive) encrypter: DES
```

リスト制御 ECP の例の中の用語の定義

ECP State:

ポイント・ポイント・リンクの現行状態。『Open』の場合、このリンクでは暗号化の交渉に成功しています。『Open』でない場合は、リンク上では暗号化は実行されていません。

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

Previous State:

現行状態フィールドに表示されている状態の前のポイント・ポイント・リンクの状態

Time Since Change:

上記の 2 つの状態変更の間の経過時間

Local (transmit) encrypter:

この暗号化アルゴリズムが、この PPP インターフェース上で送信されるデータの暗号化に使用されます。

Remote (receive) encrypter:

この暗号化アルゴリズムが、このインターフェースで受信されたデータの暗号化解除に使用されます。

リスト制御 LCP コマンドの例

例:

`list control lcp`

```

Version:                1
Link phase:             Establishing connection (LCP)
LCP State:              Listen
Previous State:         Req Sent
Time Since Change:      1 minute and 57 seconds
Remote Username:        - No Authentication -
Last Identification Rx'd
Time Connected:         - No Connection -

LCP Option              Local              Remote
-----
Max Receive Unit:       2048              1500
Async Char Mask:        FFFFFFFF          FFFFFFFF
Authentication:         None              None
Magic Number:           7A8CBFD7          None
Protocol Field Comp:    No                  No
Addr/Cntl Field Comp:   No                  No
32-Bit Checksum:        No                  No

```

リスト制御 LCP の例の中の用語の定義

Version

ポイント・ポイント・プロトコルの現行バージョンを表示します。

Link phase

リンク上の現行アクティビティを表示します。これは次の値のいずれかです。

Dead リンク上にはアクティビティが存在しません。インターフェースはダウンしています。

LCP リンクは LCP ネゴシエーションの最中です。インターフェースを最初に立ち上げるときに、この状態になります。このとき、インターフェースは自己テストを実行している可能性があります。

Authenticate

リンクは初期認証を実行中です。

ECP リンクは ECP 暗号化アルゴリズムを交渉中です。

注: 暗号化サポートはオプションであり、**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。ソフトウェア使用者の手引きの CONFIG プロセス **load** コマンドを参照してください。

ルーター内での複数の暗号化の使用 (暗号化を IP セキュリティ・レイヤーおよびフレーム・リレーまたは PPP データ・リンク・レイヤーの両方で使用する) は、米国政府輸出規制によって制限されています。これは、厳密な輸出規制のもとにあるソフトウェア・ロード (128 ビット・キーとトリプル DES をもつ 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。

Ready リンクは通常どおり運用可です。NCP はネゴシエーションを

PPP インターフェースの監視 (Talk 5)

実行し、NCP ネゴシエーションが成功した後、関連のデータ・トラフィックを伝送することができます。

Terminate

リンクは遮断中です。

LCP State

ポイント・ポイント・リンクの現行状態を表示します。これらの状態には、以下のものが含まれます。

OPEN - コネクションが確立され、データを送信できることを示します。この状態では、再試行タイマーは動作しません。

CLOSED - リンクはダウンしており、それをオープンする試みは行われていないことを示します。この状態では、ピアからのすべての接続要求はリジェクトされます。

LISTEN - リンクはダウンしており、それをオープンする試みは行われていないことを示します。ただし、CLOSED 状態とは異なり、ピアからのすべての接続要求は受け入れられます。

REQUEST-SENT - リンクをオープンする試みが実行されていることを示します。Configure-request パケットが送信されましたが、Configure-Ack はまだ受信も送信もされていません。このときは、再試行タイマーが動作しています。

ACK-RECEIVED - Configure-request パケットが送信され、Configure-Ack パケットを受信したことを示します。Configure-Ack パケットが送信されていないので、再試行タイマーはまだ動作しています。

ACK-SENT - Configure-Ack パケットと Configure-request パケットが送信されたが、Configure-Ack パケットを受信していないことを示します。この状態では、常に再試行タイマーが動作しています。

CLOSING - リンクをクローズする試みが実行されていることを示します。Terminate-request パケットが送信されましたが、Terminate-Ack パケットを受信していません。この状態では、再試行タイマーが動作しています。

Previous State

現行状態フィールドに表示されている状態の前のポイント・ポイント・リンクの状態を表示します。これらの状態は、Current state フィールドで説明したものと同じです。

Time since change

前回のリンク状態変更からの経過時間を表示します。

Remote Username

リンク上で認証が必要とされている場合、このフィールドはピアが提供した名前を示します。

Last Identification Rx'd

LCP に対して定義されているオプションのパケット・タイプは『Identification』パケットです。このパケットの内容は未定義ですが、通常は、名前、製造業者、モデル番号、あるいは製造業者が提

PPP インターフェースの監視 (Talk 5)

供するその他の情報など、何らかの識別情報を与えるためにピアによって提供される人間可読ストリングが想定されます。ルーターがこの種の packets を受信した場合、最後に受信した packet の内容がここに表示されます。

Time Connected

ピアがこのリンクに接続されていた時間の長さを示します。

LCP Option

これらのフィールドは、LCP がオープン状態のときは、ピアと交渉されたオプションの値を示します。LCP がオープンしていないときは、これらの値は、以降の LCP ネゴシエーションで使用される初期デフォルト値または構成値を表します。

Max Receive Unit

ローカル側とリモート側が送信できる packet ・サイズの最大長を示します。これは PPP packet のペイロード部分の最大長であり、PPP ヘッダーとトレーラーのバイト数は含まれません。

LCP がオープン状態のときは、この値はピアと交渉された長さを示します。ルーターは、相手側とローカル側で MRU 長さが異なることはサポートしないので、これらの値は同一になります。

Async Character Mask

これは、交渉された非同期制御文字マスクを示します。ルーターは同期伝送路でも ACCM ネゴシエーションを受け入れます。ただし、これは実際の packet ・データ送信には影響を与えません。ACCM の詳細については、556 ページの **set lcp options** コマンドの項を参照してください。

Authentication

リンクの各側に必要な認証プロトコル (もしあれば) を示します。各側で複数のプロトコルを使用することも可能です。この値は、装置が使用することに合意したプロトコルを示します。

Magic number

リンクのローカル側とリモート側の両方でループバック検出に使用されている現行のマジック番号を表示します。

Protocol compression

PFC が交渉されたかどうかを示します。

Address/Control compression

ACFC が交渉されたかどうかを示します。

32-bit checksum

現在はサポートされていません。PPP は、受信した場合、このオプションをリジェクトします。

リスト制御 BCP コマンドの例

例:

```
list control bcp
BCP State:          Closed
Previous State:     Closed
Time Since Change:  5 hours, 25 minutes and 3 seconds
```

PPP インターフェースの監視 (Talk 5)

```
BCP Option          Local          Remote
Tinygram Compression  DISABLED      DISABLED
Source-route Info:
Remote side does not support source-route bridging
```

リスト制御 **BCP** の例の中の用語の定義

BCP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

Tinygram Compression

リンクのローカル側およびリモート側の Tinygram 圧縮が使用可能か使用不可かを表示します。

Source-route Info

このインターフェースに対応するローカル・ポートおよびリモート・ポートのソース・ルート・ブリッジングが使用可能かどうかを表示します。

リスト制御 **NBCP** コマンドの例 リスト制御 **NBCP** の例の中の用語の定義 リスト制御 **NBFCP** コマンドの例

例:

```
list control nbfcf
NBFCP State:          Closed
Previous State:       Closed
Time Since Change:    4 hours, 5 minutes and 58 seconds

NetBIOS Frame Control Protocol Info:
Local MAC Address = 0x000000000000
Remote MAC Address = 0x444553540000
Remote NetBIOS Names: (0)

Remote Peer Class:    0
Remote Peer Version Major: 0
Remote Peer Version Minor: 0
```

リスト制御 **NBFCP** の例の中の用語の定義

NBFCP State フィールドは、**list control lcp** コマンドの項で説明したものと同じです。

Local MAC Address

ローカル MAC アドレスは、Win 95/NT ダイアルアップ・ネットワーク・クライアントによって使用される MAC アドレスです。これは、疑似乱数またはローカル管理アドレス (LAA) (クライアントに LAA を構成した場合) です。

Remote MAC Address

リモート MAC アドレスは、LAN 上で使用するために 2210 DIAL サーバーがこのクライアントに割り当てた MAC アドレスです。

Remote NetBIOS Name

クライアントがアクセスを要求した LAN リソースの NetBIOS ネームのリスト

Remote Peer

Remote Peer Class、Version Major、および Version Minor は、NBFCP ピア情報オプションによって 2210 に戻される情報です。

リスト制御 IPCP コマンドの例

例:

```
list control ipcp
IPCP State: Listen
Previous State: Closed
Time Since Change: 1 hour, 57 minutes and 52 seconds

IPCP Option Local Remote
-----
IP Address 0.0.0.0 10.0.0.152
Compression Slots None None

DNS servers obtained from remote:
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0

DHCP State: BOUND
Lease Server: 10.0.0.111
Leased IP Address: 10.0.0.152
Lease Time: 4 minutes and 0 seconds
Renewal Time: 2 minutes and 0 seconds
Rebind Time: 3 minutes and 30 seconds
Lease Time Elapsed: 1 second
Lease Time Remaining: 3 minutes and 59 seconds

DHCP Client ID: 0100120B0000
```

リスト制御 IPCP の例の中の用語の定義

IPCP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

IP Address:

このインターフェースの構成または交渉された IP アドレス (Local) およびリモートの交渉されたアドレス (Remote) (もしあれば) を示します。

Compression Slots

使用可能にされている圧縮のタイプを調べるときに参照するために保存された IP ヘッダーの数を示します。

DNS servers obtained from remote

相手側によって提供されたドメイン・ネーム・サーバー (DNS) の IP アドレスを示します。

DHCP State

これは RFC 1541 に記述されている プロキシ DHCP です。

Lease Server

このサーバーからリースを獲得しました。

Leased IP address

クライアントにリースされたアドレス。このアドレスは、上記の『Remote IP Address』と同等でなければなりません。

Lease Time

このアドレスを DHCP サーバーからリースしている時間の長さ。

『Lease Time Elapsed』がこの時間に等しくなると、リースは満了し、IPCP コネクションはクローズされます。

Renewal Time

この時間の後で、プロキシ DHCP はサーバーからのこのリースの延長を試みます。『Lease Elapsed Time』がこの時間に等しくなると、

PPP インターフェースの監視 (Talk 5)

プロキシー DHCP はリースの更新を試み、成功した場合は、『Lease Time』、『Lease Elapsed Time』、および『Lease Time Remaining』をリセットします。

Rebind Time

プロキシー DHCP が、構成された任意の DHCP サーバーから新規リースを取得することを試みる前の時間。『Lease Elapsed Time』がこの時間に等しくなると、プロキシー DHCP は新規リースの取得を試み、成功した場合は、『Lease Time』、『Lease Elapsed Time』、および『Lease Time Remaining』をリセットします。

Leased Time Elapsed

このリースの経過時間。リースは更新されている可能性があるため、これは必ずしもこの特定のダイヤルイン・セッションの時間を示すものではありません。リースが更新されると、このタイマーは 0 に戻されます。

Leased Time Remaining

このリースの残り時間。このパラメーターは、『Lease Time』から『Lease Time Elapsed』を差し引いた値に等しくなります。

DHCP client ID

このクライアント (ダイヤルイン・ユーザー) の固有の ID。DHCP サーバーとの間でやり取りされるすべての DHCP メッセージは、このクライアント ID によって識別されます。

リスト制御 IPXCP コマンドの例

例:

```
list control ipxcp
IPXCP State:      Closed
Previous State:   Closed
Time Since Change: 2 hours, 9 minutes and 9 seconds
```

IPXCP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。リスト制御 **ATCP** コマンドの例

例:

```
list control atcp
ATCP State:      Closed
Previous State:   Closed
Time Since Change: 6 hours, 27 minutes and 7 seconds

AppleTalk Address Info:
Common network number = 12
Local node ID = 49
Remote node ID = 76
```

リスト制御 ATCP の例の中の用語の定義

ATCP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

Common Network Number

ポイント・ポイント・リンクの 2 つの端のネットワーク番号。(リンクの両端は、同じネットワーク番号を持つように静的に構成する必要があります。)

Local Node ID

リンクのローカル側の固有のノード番号

Remote Node ID

リンクのリモート側の固有のノード番号

例:

```
list control dnpc
DNCN State:          Closed
Previous State:      Closed
Time Since Change:   2 hours, 2 minutes and 58 seconds
```

DNCN 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

例:

```
list control osicp
OSICP State:         Closed
Previous State:      Closed
Time Since Change:   6 hours, 28 minutes and 32 seconds
```

OSICP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。リスト制御 **BVCP** コマンドの例

例:

```
list control bvcp
BVCP State:          Open
Previous State:      Ack Sent
Time Since Change:   403 hours, 49 minutes and 2 seconds
```

BVCP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

注: コマンド・ワード **bvcp** および頭字語 BVCP は、Banyan VINES 制御プロトコル (BVCP) を表します。

リスト制御 **ISRCP** コマンドの例

例:

```
list control isrcp
APPN ISRCP State:    Open
Previous State:      Ack Rcvd
Time Since Change:   1 hour, 48 minutes and 5 seconds
```

APPN ISR 制御プロトコル (ISRCP) 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。リスト制御 **HPRCP** コマンドの例

例:

```
list control hprcp
APPN HPRCP State:    Open
Previous State:      Ack Rcvd
Time Since Change:   1 hour, 48 minutes and 10 seconds
```

APPN HPR 制御プロトコル (HPRCP) 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

error PPP ソフトウェアによって検出されたすべての誤り状態に関連する情報をリストします。

例:

PPP インターフェースの監視 (Talk 5)

```
list error
Error Type          Count      Last One
-----
Bad Address:        0           0
Bad Control:        0           0
Unknown Protocol:   0           0
Invalid Protocol:   0           0
Config Timeouts:    0           0
Terminate Timeouts: 0           0
```

Bad address

ポイント・ポイント・リンク上で検出された不正なアドレスの合計数を示します。『Bad addresses』は、パケットの先頭の HDLC フレーム・バイトを表します。

Bad control

ポイント・ポイント・リンク上で検出された不正な制御パケットの合計数を示します。『Bad control』は、HDLC カプセル化 PPP パケットの 0x03 プレフィックス (0xFF の後に続く『UI』値) を表します。

Unknown protocol

現行のリンクで検出された不明なプロトコル・パケットの合計数を示します。

Invalid protocol

現行のリンクで検出された無効なプロトコル・パケットの合計数を示します。

Config timeouts

リンクで発生した構成タイムアウトの合計数を示します。

Terminate timeouts

リンクで発生したリンク終了タイムアウトの合計数を示します。

interface

PPP インターフェースの統計をリストします。

例:

```
list interface
Interface Statistic  In      Out
-----
Packets:             0       0
Octets:              0       0
```

Packets

このインターフェースで送受信されたパケットの数を示します。

Octets

このインターフェースで送受信されたオクテット数を示します。

lcp

リンク制御プロトコルの統計をリストします。

例:

```
list lcp
LCP STATISTIC      IN      OUT
-----
PACKETS:           42      42
OCTETS:            1260    1260
CFG REQ:           0        0
CFG ACK:           0        0
CFG NAK:           0        0
CFG REJ:           0        0
TERM REQ          0        0
TERM ACK          0        0
```

PPP インターフェースの監視 (Talk 5)

ECHO REQ:	21	21
ECHO RESP:	21	21
DISC REQ:	0	0
CODE REJ:	0	0

Packets

現行のポイント・ポイント・インターフェースを介して送信 (out) および受信 (in) された LCP パケットの合計数を示します。

Octets

LCP フレームの場合、現行のポイント・ポイント・インターフェースを介して送受信されたバイトの合計数をオクテットで示します。

CFG REQ

現行のポイント・ポイント・インターフェースを介して送受信された構成要求 (configure-request) LCP パケットの合計数を示します。

CFG ACK

現行のポイント・ポイント・インターフェースを介して送受信された構成確認 (configure-ack (acknowledged)) LCP パケットの合計数を示します。

CFG NAK

現行のポイント・ポイント・インターフェースを介して送受信された構成非確認 (configure-nak (not acknowledged)) LCP パケットの合計数を示します。

CFG REJ

現行のポイント・ポイント・インターフェースを介して送受信された構成リジェクト (configure-reject) LCP パケットの合計数を示します。

TERM REQ

現行のポイント・ポイント・インターフェースを介して送受信された終了要求 (terminal-request) LCP パケットの合計数

TERM ACK

現行のポイント・ポイント・インターフェースを介して送受信された終了確認 (terminal-ack) LCP パケットの合計数

ECHO REQ

現行のポイント・ポイント・インターフェースを介して送受信されたエコー要求 (echo-request) LCP パケットの合計数を示します。

ECHO RESP

現行のポイント・ポイント・インターフェースを介して送受信されたエコー応答 (echo-response) LCP パケットの合計数を示します。

DISC REQ

現行のポイント・ポイント・インターフェースを介して送受信された廃棄要求 (discard-request) LCP パケットの合計数を示します。

CODE REJ

現行のポイント・ポイント・インターフェースを介して送受信された符号リジェクト (code-reject) LCP パケットの合計数を示します。

pap

パスワード認証プロトコルの統計をリストします。

例:

PPP インターフェースの監視 (Talk 5)

```
list pap
PAP Statistics          In          Out
-----
Packets:                0            0
Octets:                 0            0
Requests:               0            0
Acks:                   0            0
Naks:                   0            0
```

Packets

送信または受信された PAP パケットの合計数

Octets

このパケットで送信または受信されたデータのバイト数

Requests

送信または受信された PAP 『要求』パケットの数。これらは PAP 名前/パスワードの組みが入っているパケットです

Acks PAP 要求に対して送信または受信された Ack (肯定応答) の数 (たとえば、ピアが有効な要求パケットを送信した場合、ルーターは Ack で応答します)。

Naks PAP 要求に対して送信または受信された Nak の数 (たとえば、ピアが無効な要求パケットを送信した場合、ルーターは Nak で応答します)。

chap チャレンジ/ハンドシェイク認証プロトコルの統計をリストします。

例:

```
list chap
CHAP Statistics          In          Out
-----
Packets:                0            0
Octets:                 0            0
Challenges:            0            0
Responses:              0            0
Successes:              0            0
Failures:               0            0
```

Packets

送信または受信された CHAP パケットの合計数

Octets

パケットで送信または受信されたデータのバイト数

Challenges

送信または受信された CHAP 『チャレンジ』パケットの数。CHAP チャレンジ・パケットには、ランダムに生成された暗号化キーが入っており、そのキーおよび保管されているパスワード情報に基づいて適切なレスポンスを生成することをピアに要求します。

Responses

送信または受信された CHAP 『レスポンス』パケットの数。レスポンス・パケットには、『チャレンジ』要求に対するピアの応答が入っています。

Successes/Failures

送信または受信された成功 (Success) または不成功 (Failure) パケットの数。装置はチャレンジ・パケットを送信し、ピアのレスポンス・

PPP インターフェースの監視 (Talk 5)

パケットを待ちます。次に、レスポンス・パケットを調べて、そのレスポンスが有効であったかどうかを示すために成功または不成功パケットを送信します。

これらのカウンターは、送信された成功または不成功パケットを反映します。認証が失敗と見なされる前に、ピアは正常に応答するために数回試行します。

mschap

各方向の MS-CHAP 統計をリストします。

Packets

MS-CHAP パケットの合計数

Octets

MS-CHAP パケットに含まれるバイトの合計数

Challenges

MS-CHAP チャレンジ・パケットの数

Responses

MS-CHAP 応答パケットの数

Successes

MS-CHAP 成功パケットの数

Failures

MS-CHAP 失敗パケットの数

Failure: Restricted Hours

PPP ユーザーがそのユーザーに許可された時間外に 2210 にアクセスしようと試みたために送信に失敗したパケットの数。このカウンターはサポートされておらず、常に 0 となります。

Failure: Account Disabled

PPP ユーザーの ID が 2210 で使用不可だったために送信に失敗したパケットの数

Failure: Password Expired

PPP ユーザーのパスワードの有効期限が切れたために送信に失敗したパケットの数

Failure: No Dialin Permission

PPP ユーザーがこの 2210 に許可ダイヤルインすることが許可されていなかったために送信に失敗したパケットの数

Failure: Authentication

PPP ユーザーの信用証明 (ID またはパスワード) が 2210 に不明であったために送信に失敗したパケットの数

Failure: Change Password

パスワード変更パケットの処理中にエラーが検出されたために送信に失敗したパケットの数

Change Password

パスワード変更パケットの数。ルーターはパスワード変更パケットを決して送信しないので、アウトバウンド・カウンターは常に 0 となります。

PPP インターフェースの監視 (Talk 5)

ecp インターフェース上で送信または受信された ECP (暗号化制御プロトコル) パケットの統計をリストします。

例:

```
PPP x>list ecp
```

```
ECP Statistic          In          Out
-----
Packets:                2            2
Octets:                 26          26
Reset Reqs:             0            0
Reset Acks:             0            0
Prot Rejects:          0            -
Local (transmit) encrypter: DES
Remote (receive) encrypter: DES
```

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

Packets

現行のポイント・ポイント・インターフェースを介して送信 (out) および受信 (in) された ECP パケットの合計数を示します。

Octets

ECP パケットで送受信された合計バイト数を示します。

Reset Reqs

このインターフェースで送受信されたりセット要求の数を示します。リセット要求は、ECP が EDP パケットを廃棄するたびに送信されます。

注: DES (サポートされる唯一の暗号化アルゴリズム) はリセット要求を送信しないので、この数はゼロになります。

Reset Acks

このインターフェースで送受信されたりセット確認の数を示します。リセット確認 (Reset Ack) パケットは、リセット要求パケットを受信するたびに送信されます。

注: DES (サポートされる唯一の暗号化アルゴリズム) はリセット要求を送信しないので、この数はゼロになります。

Prot Rejects

現行のポイント・ポイント・インターフェースを介して送受信されたプロトコル・リジェクト・パケットの合計数を示します。

Local (transmit) encrypter

このポイント・ポイント・インターフェースで送信されるデータの暗号化には、この暗号化アルゴリズムが使用されます。

Remote (receive) encrypter

このポイント・ポイント・インターフェースで受信したデータの暗号解除には、この暗号化アルゴリズムが使用されます。

edp インターフェース上で送信または受信された EDP 暗号化パケットに関連した統計をリストします。

例:

PPP インターフェースの監視 (Talk 5)

PPP x>list edp

Encryption Statistic	In	Out
-----	--	---
Packets:	20	30
Octets:	29164	44790
Encrypted Octets:	29280	44880
Discarded Packets:	0	0
Prot Rejects:	0	-

注: 暗号化サポートはオプションであり、**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。84ページの『Load』を参照してください。

Packets

現行のポイント・ポイント・インターフェースを介して送信 (out) および受信 (in) された IP パケットの合計数を示します。

Octets

現行 IP コネクションを介して送受信されたデータ・バイトの合計オクテット数を示します。

Encrypted Octets

このインターフェースで送受信された、暗号化されたオクテット数を示します。

Discarded Packets

正常に暗号化解除できないために廃棄されたパケットの数を示します。

Prot Rejects

現行のポイント・ポイント・インターフェースを介して送受信されたプロトコル・リジェクト・パケットの合計数を示します。

mppe Microsoft PPP 暗号化 (MPPE) 構成の暗号化データ統計を表示します。

例:

```
list mppe
MPPE Statistic      In      Out
-----
Encrypted Octets :   0        0
Encrypted Packets :   0        0
Discarded Packets :   0        0
```

spap Shiva パスワード認証プロトコルの統計をリストします。

例:

```
list spap
SPAP Statistic      In      Out
-----
Packets:            0        0
Octets:             0        0
Requests:           0        0
Acks:               0        0
Naks:               0        0
Dialbacks:          0        0
PleaseAuthenticates: 0        0
Change Passwords:   0        0
Alerts:             0        0
MCCP Call Reqs     0        0
MCCP Callbacks     0        0
MCCP ACKs          0        0
MCCP NAKs          0        0
```

Packets

送信または受信された SPAP パケットの合計数

PPP インターフェースの監視 (Talk 5)

Octets

このパケットで送信または受信されたデータのバイト数

Requests

送信または受信された SPAP 『Request』 パケットの数。これらは SPAP 名前/パスワードの組みが入っているパケットです

Acks SPAP 要求に対して送信または受信された Ack (肯定応答) の数 (たとえば、ピアが有効な要求パケットを送信した場合、ルーターは Ack で応答します)。

Naks SPAP 要求に対して送信または受信された Nak の数 (たとえば、ピアが無効な要求パケットを送信した場合、ルーターは Nak で応答します)。

Dialbacks

ユーザーが以下のことを行った回数

- コールバック (ローミング・コールバック) を要求して、それが認められた回数
- ダイヤルインし、それらが必須コールバックに構成されていたために、ユーザー・プロファイルに保管されている事前定義された番号にダイヤルしてコールバックされた回数

PleaseAuthenticates

このインターフェース上で送信または受信された SPAP please authenticate パケットの数。SPAP please authenticate パケットは、相手側が SPAP 認証要求を送ってくるのを待っているときにタイムアウトになった場合に送信されます。

Change Passwords

このインターフェース上で送信または受信されたパスワード変更要求の数

Alerts 送信または受信された SPAP バナーの数

MCCP Call Reqs

2 番目の MP リンクにダイヤルするために送信側が別の電話番号を要求したことを示します。

MCCP Callbacks

2 番目の MP リンクを設定するためにコールバックされなければならない電話番号を送信側が提供したことを示します。

MCCP ACKs

MCCP によって送信または受信される確認応答の数

MCCP NAKs

MCCP によって送信または受信される否定応答の数

ccp 圧縮制御プロトコルの統計をリストします。

例:

```
list ccp
CCP  Statistic      In      Out
-----
Packets:           24      25
Octets:            174     177
```

PPP インターフェースの監視 (Talk 5)

Reset Reqs	0	0
Reset Acks:	0	0
Prot Rejects:	0	0

Packets

このインターフェースで送受信されたパケットの数を示します。

Octets

このインターフェースで送受信されたオクテット数を示します。

Reset Reqs

送信または受信された CCP ディクショナリー『リセット要求』の数

Reset Acks

送信または受信された CCP ディクショナリー『リセット確認』の数
リセット要求およびリセット確認パケットは、リンクの各端でデータ・ディレクトリーの同期を維持するために、各端の CCP エンティティー間で渡される制御パケットです。

Prot Rejects

ピアによって送信された CCP パケットのプロトコル・リジェクトの数を示します (プロトコル・リジェクトの受信は、ピアが CCP をサポートしないことを意味しています)。

cdp

このインターフェースで送信または受信された圧縮データ・パケットに関連する統計を表示します。

例:

```
list cdp
Compression Statistic      In              Out
-----
Packets:                   31035          46550
Octets:                    1614885       2421137
Compressed Octets:         931416        1521039
Incompressible Packets:    0              0
Discarded Packets:         0              0
Prot Rejects:              0              -
Compression Ratios         1.70           1.70
```

Packets

これらのカウンターは、送受信された圧縮データグラムを示します。出力側では、カウントには実際に PPP 圧縮データグラムとして送信されたパケットのみが含まれます。圧縮不能であることが検出され、元の未圧縮の形で送信されたパケットは含まれません。

これらのカウンターは、送信または受信された PPP プロトコル・タイプ X'00FD' (CDP) のパケットをカウントします。STAC 拡張モードまたは MPPC が交渉された場合、圧縮不能パケットを CDP データグラムにカプセル化することができます。このカプセル化の場合は、圧縮不能パケットもこれらのカウントに含まれます。

Octets

これらのカウンターは、圧縮された形で有効に送信または受信されたバイト数を示します。これらのカウントは、圧縮前または解凍後の元のデータグラムの長さを反映します。

Compressed octets

これらのカウンターは、送受信されたすべての圧縮データグラムのバイト数を示します。これらのカウントは、圧縮後または解凍前の実際の CDP パケットの長さです。

PPP インターフェースの監視 (Talk 5)

Incompressible packets

これらのカウンターは、圧縮不能であったために元の未圧縮の形で送信されたパケットの数を示します。

Discarded packets

これらのカウンターは、正常に解凍できなかつたために廃棄されたパケットの数を示します。通常、これらのパケットは、ルーターがリセット要求を送信した直後、ただしピアがそのリセット要求を受信して処理する前に、ピアが送信したパケットです。また、ルーターがパケット内のデータに誤りを検出した場合も、パケットは廃棄されます。データの誤りの一例は、不正なシーケンス番号が入っているパケットです。

廃棄されたパケット数が急増する場合は、おそらく伝送路のノイズまたはリンク性能の低下が原因で、パケットが失われているか、破壊されています。

Protocol rejects

このカウンターは、ピアから受信した CDP パケットのプロトコル・リジェクトの数を示します。このカウントはゼロでなければなりません。圧縮の使用が交渉済みでなければ、リンクは CDP パケットを送信しないからです。

Compression ratios

比率は、圧縮機能または解凍機能の効率の概略値を表示します。これらの比率は、テキスト・バイト数を対応する圧縮バイト数で割った値に基づいているので、入力側と出力側の両方とも、1 より大きい値が望まれます。数値が高いほど、圧縮効果が高くなります。

出力比率は、元のテキスト・バイト数を圧縮を試みた結果として送信された (パケットが実際に圧縮されたか、あるいは CDP パケットとして送信された) バイト数で割った比率として計算されます。データ・ストリームが十分に圧縮されず、ほとんどのパケットが元の形あるいは拡大 CDP パケットで送信される場合には、圧縮出力比率は低下します。比率が 1.0 以下に低下する場合は、圧縮機能は実際には伝送路の有効帯域幅を増やすどころか、減らしていることになるので、この状態が長く続く場合は、そのインターフェース上の圧縮を使用不可にすべきです。

入力比率は、CDP フレームで受信したバイト数を解凍されたバイト数で割って計算されます。出力比率とは異なり、このカウントには圧縮不能のためテキスト形式で送信されたパケットは含まれません。これはルーターが、受信した非 CDP パケットは、ピアがテキスト形式で送信した圧縮不能パケットであるのか、単にピアが圧縮を試みなかったパケットであるのかを判別できないからです。

この計算方法のため、リンクの一端の出力比率は、必ずしも他端の入力比率と一致していません。

compression

このコマンドは `list cdp` と同じ情報を表示します。

bcp ブリッジング制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list bcp
BCP Statistic          In          Out
-----
Packets:                0            0
Octets:                  0            0
Prot Rejects:           0            -
```

brg PPP インターフェースを介して送受信されたブリッジ・パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list brg
BRG Statistic          In          Out
-----
Packets:                0            0
Octets:                  0            0
Prot Rejects:           0            -
```

stp スパニング・ツリー・プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list stp
Spanning Tree Statistic In          Out
-----
Packets:                0            0
Octets:                  0            0
```

nbcip ポイント・ポイント・インターフェースの NetBIOS 制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list nbcip
NBCIP Statistic        In          Out
-----
Packets:                0            0
Octets:                  0            0
Prot Rejects:           0            -
```

nbfcip ポイント・ポイント・インターフェースの NetBIOS フレーム制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list nbfcip
NBFCIP Statistic       In          Out
-----
Packets:                0            0
Octets:                  0            0
Prot Rejects:           0            -
```

ipcp ポイント・ポイント・インターフェースのインターネット・プロトコル制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

PPP インターフェースの監視 (Talk 5)

```
list ipcp
IPCP STATISTIC      IN      OUT
-----
PACKETS:            0        0
OCTETS:             0        0
PROT REJECTS:      0
```

ip ポイント・ポイント・リンクを経由する IP パケットに関するすべての情報をリストします。

例:

```
list ip
IP Statistic      In      Out
-----
Packets:         349     351
Octets:         128488 129412
Prot Rejects:    0
```

Packets

現行のポイント・ポイント・インターフェースを介して送信 (out) および受信 (in) された IP パケットの合計数を示します。

Octets

現行 IP コネクションを介して送受信されたオクテットの合計数を示します。

Prot Rejects

現行のポイント・ポイント・インターフェースを介して送受信されたプロトコル・リジェクト・パケットの合計数を示します。

ipv6cp

ポイント・ポイント・インターフェースのインターネット・プロトコルバージョン 6 制御プロトコル統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(『ip』を参照してください。)

例:

```
list ipv6cp
IPv6CP STATISTIC  IN      OUT
-----
PACKETS:          0        0
OCTETS:           0        0
PROT REJECTS:    0
```

ipv6 ポイント・ポイント・リンクを経由する IPv6 パケットに関するすべての情報をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(『ip』を参照してください。)

例:

```
list ipv6
IPv6 Statistic    In      Out
-----
Packets:         0        0
Octets:          0        0
Prot Rejects:    0
```

ipxcp IPX 制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(『ip』を参照してください。)

例:

```
list ipxcp
IPXCP Statistic   In      Out
-----
```


PPP インターフェースの監視 (Talk 5)

```
Packets:          0          0
Octets:           0          0
Prot Rejects:    0          -
```

ipx ポイント・ポイント・インターフェースの IPX 統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list ipx
IPX Statistic      In      Out
-----
Packets:           0        0
Octets:            0        0
Prot Rejects:     0        -
```

atcp AppleTalk 制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list atcp
ATCP Statistic     In      Out
-----
Packets:           0        0
Octets:            0        0
Prot Rejects:     0        -
```

ap2 ポイント・ポイント・インターフェースの AppleTalk フェーズ 2 の統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list ap2
AP2 Statistic      In      Out
-----
Packets:           349     351
Octets:           128488 129412
Prot Rejects:     0
```

dncp DECnet 制御プロトコル・パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list dncp
DNCP Statistic     In      Out
-----
Packets:           0        0
Octets:            0        0
Prot Rejects:     0        -
```

dn PPP インターフェースを介して送受信された DECnet パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list dn
DN Statistic       In      Out
-----
Packets:           0        0
Octets:            0        0
Prot Rejects:     0        -
```

osicp OSI 制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

PPP インターフェースの監視 (Talk 5)

例:

```
list osicp
OSICP Statistic      In      Out
-----
Packets:             0        0
Octets:              0        0
Prot Rejects:       0        -
```

osi PPP インターフェースを介して送受信された OSI パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list osi
OSI Statistic      In      Out
-----
Packets:           0        0
Octets:            0        0
Prot Rejects:     0        -
```

bvcp Banyan VINES 制御プロトコルに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list bvcp
BVCP Statistic      In      Out
-----
Packets:            0        0
Octets:            0        0
Prot Rejects:     0        -
```

vines PPP インターフェースを介して送受信された Banyan VINES パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list vines
Vines Statistic      In      Out
-----
Packets:           10       13
Octets:           320     340
Prot Rejects:     0        -
```

isrcp APPN ISR 制御プロトコル・パケットの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list isrcp
APPN ISRCP Statistic In      Out
-----
Packets:            3        3
Octets:           12       12
Prot Rejects:     0        -
```

isr PPP インターフェースを介して送受信された APPN ISR パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list isr
APPN ISR Statistic  In      Out
-----
Packets:           220     219
Octets:          1266    1157
Prot Rejects:     0        -
```

PPP インターフェースの監視 (Talk 5)

hprcp APPN HPR 制御プロトコル・パケットの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list hprcp
APPN HPRCP Statistic      In              Out
-----
Packets:                   3                3
Octets:                     12              12
Prot Rejects:              0                -
```

hpr PPP インターフェースを介して送受信された APPN HPR パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(582ページの『ip』を参照してください。)

例:

```
list hpr
APPN HPR Statistic        In              Out
-----
Packets:                   780             715
Octets:                    131907          69685
Prot Rejects:              0                -
```

LLC

LLC コマンドは、LLC 監視プロンプトにアクセスするのに使用します。LLC コマンドは、この新たに表示されたプロンプトで入力します。各コマンドについての説明は、271ページの『LLC 監視コマンド』を参照してください。

注: このコマンドは、ソフトウェア・ロードに APPN が含まれている場合にのみ表示されます。

構文:

llc

ポイント・ポイント・プロトコル・インターフェースと GWCON インターフェース・コマンド

PPP インターフェース・トラフィックは、基礎のデータ・リンク・レベルの装置ドライバーによって伝送されます。PPP リンクの監視に役立つ追加統計を、装置ドライバーの統計から入手できる場合があります。この統計は GWCON 環境から **interface** コマンドを使用して表示します。(interface コマンドの詳細については、149ページの『第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』を参照してください。)

この節に示す統計は、ポイント・ポイント構成で使用される以下のインターフェースについて、GWCON 環境 (talk 5) から **interface** コマンドを実行すると表示されます。

例:

+ interface 12

Net	Net'	Interface	Slot-Port	Self-Test Passed	Self-Test Failed	Maintenance Failed
12	12	PPP/0	Slot: 8 Port: 2	2	1	0

PPP インターフェースの監視 (Talk 5)

Point to Point MAC/data-link on V.35/V.36 interface

Adapter cable: V.35 DTE

V.24 circuit: 105 106 107 108 109
Nicknames: RTS CTS DSR DTR DCD
PUB 41450: CA CB CC CD CF
State: ON ON ON ON ON

Line speed: 64.000 Kbps
Last port reset: 1 hour, 20 minutes, 42 seconds ago

Input frame errors:
CRC error 0 alignment (byte length) 0
missed frame 182 too long (> 2062 bytes) 0
aborted frame 0 DMA/FIFO overrun 0
Output frame counters:
DMA/FIFO underrun errors 0 Output aborts sent 0

Net 初期構成時にソフトウェアによって割り当てられたインターフェース番号

Net' 初期構成時にソフトウェアによって割り当てられたインターフェース番号

注: ダイヤル回線インターフェース回線の場合、Net' は Net と異なっています。ダイヤル回線インターフェースの場合は、Net' はダイヤル回線で使われる基本インターフェース (ISDN または V.25bis) を示します。

Interface No

インターフェースのタイプとそのインスタンス番号。ポイント・ポイント・インターフェース・タイプは PPP です。

Slot PPP が実行されているインターフェースのスロット番号

Port PPP が実行されているインターフェースのポート番号

Self-Test: Passed

ポイント・ポイント・インターフェースが自己テストに成功した合計回数

Self-Test: Failed

ポイント・ポイント・インターフェースが自己テストに失敗した合計回数

Maintenance: Failed

保守障害の合計数

Adapter cable

構成されたアダプター・ケーブルのタイプ (たとえば、V.35 DTE)

V.24 circuit

V.24 で使用される回線。注: 監視出力の記号 - - - は、値または状態が不明であることを示します。

Nicknames

制御信号の注: 監視出力の記号 - - - は、値または状態が不明であることを示します。

PUB 41450

ピン割り当ての注: 監視出力の記号 - - - は、値または状態が不明であることを示します。

State V.24 回線の状態 (オンまたはオフ)。注: 監視出力の記号 - - - は、値または状態が不明であることを示します。

Line speed

構成された回線速度、または想定されるデフォルト値 (回線速度が 0 として構成されている場合)

Last port reset

ポートがリセットされた後の経過時間

CRC error

チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment (byte length)

長さが 8 ビットの偶数倍でなかったために廃棄された受信パケットの数

Too long (> 2048 bytes)

構成されたフレーム・サイズより大きかったために廃棄されたパケットの数

Aborted frame

送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

DMA/FIFO overrun

シリアル・インターフェースがシステム・パケット・バッファ・メモリーにデータを送信する速度が遅かったために、データをネットワークから受信できなかった回数

Missed frame

フレームが装置に到着したときに利用可能なバッファがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

L & F bits not set

シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファが完全なフレームを受け入れたことを示します。いずれかのビットがセットされていない場合、パケットは廃棄され、L & F bits not set カウンターが増分され、バッファは消去されて再利用できるようになります。

注: L & F bits not set カウンターはトラフィックによる影響は受けません。

Output Frame Counters:

DMA/FIFO underrun errors

シリアル・インターフェースがデータをシステム・パケット・バッファ・メモリーから速く検索できなかったため、ネットワークヘッダを送信できなかった回数

Output aborts sent

高位レベルのソフトウェアの要求によって打ち切られた伝送の数

GWCON 環境から **interface** コマンドを実行すると、PPP ダイアル回線について次のものに似た統計が表示されます。

PPP インターフェースの監視 (Talk 5)

```
+interface 29
Net Net' Interface          Self-Test Self-Test Maintenance
29 10  PPP/20              Passed     Failed     Failed
Point to Point MAC/data-link on V.25bis Dial Circuit interface
```

第32章 マルチリンク PPP プロトコルの使用

この章では、マルチリンク PPP プロトコル (MP) の使用法について説明します。本章には、以下の節が含まれています。

- 590ページの『MP の考慮事項』
- 591ページの『マルチシャシー MP』
- 591ページの『マルチリンク PPP インターフェースの構成』

マルチリンク PPP プロトコルにより、次のものの帯域幅を増やすことができます。

- PPP 専用線 (チャンネル化された回線および I43x ISDN 回線を含む)
- PPP ISDN ダイアル回線
- PPP V.25bis ダイアル回線
- PPP レイヤー 2 トンネル伝送回線

帯域幅を増やすには、複数のリンクから構成される**バーチャル・リンク**を定義します。得られる MP バンドルの帯域幅は、個々のリンクの帯域幅の合計にほぼ等しくなります。この方式の利点は、単一リンクを介して転送される大きなデータ・パケットを分割し、複数のリンクを介して転送し、受信側ステーションで再び組み立てることができることです。MP は、帯域幅割り当てプロトコルと帯域幅割り当て制御プロトコルの両方を使用して、PPP dial 回線をバーチャル・リンクに追加したり、除去したりします。MP は、帯域幅オンデマンド (BOD) も使用して、既存のバンドルに『専用』MP ダイアル・リンクを追加します。

MP リンクには 2 つのタイプがあります。すなわち、専用のリンクと使用可能にされるリンクです。専用 MP リンクは、特定の MP インターフェースへのリンクとして構成された MP 使用可能インターフェースです。リンクが別の MP バンドルに結合しようとした場合、あるいは MP がまったく交渉されない場合、ソフトウェアはリンクを終了します。レイヤー 2 トンネル伝送インターフェースを除くすべての PPP リンクは、専用の MP リンクとして構成することができます。PPP 専用リンクは、専用の MP リンクとして構成する必要があります。

PPP ダイアル回線およびレイヤー 2 トンネル伝送は、MP 使用可能として構成することができます。非専用の MP 使用可能リンクは、任意の MP バンドルにリンクすることができます。MP が交渉されない場合、リンクはそのリンクの構成済みプロトコルを使用して、独立したインターフェースとして稼働します。

複数の PPP ダイアル回線からなるマルチリンク PPP インターフェースを、MP バンドルの一部として構成することができます。

MP インターフェースにも 2 つのタイプがあります。すなわち、専用のリンクを持っているものと、持っていないものです。以下の状態のいずれの場合も、MP インターフェースは専用リンクが必要です。

- リンクが MP インターフェース専用である。
- MP インターフェースがアウトバウンド・コール用に構成されている。この場合、専用リンクにあて先電話番号とコーラー ID を構成する必要があります。

MP の使用

- MP インターフェースが、特定のインバウンド・コールを受信するように構成されている。この場合、専用リンクにはインバウンドあて先電話番号とコーラー ID を構成する必要があります。
- MP インターフェースがアウトバウンド認証を行う必要がある。この場合、すべてのリンクが同じ認証名を使用します。

専用リンクを持たない MP インターフェースは、インバウンド専用インターフェースでなければなりません。これらのインターフェースは、インバウンド・ダイヤル回線に似ています。

MP インターフェースは、帯域幅割り当てプロトコル (BAP) と帯域幅割り当て制御プロトコル (BACP) を用いて、ダイヤル回線を追加したり除去したりして、帯域幅を増やしたり減らしたりすることができます。帯域幅使用率アルゴリズムにより、バンドルにリンクを追加する必要があると判定された場合、利用可能な PPP ダイヤル回線およびピアの合意があれば、追加のコールが行われます。

BAP は、最初に MP インターフェースにアイドル状態の専用 PPP ダイヤル回線を探し、次に MP が使用可能な PPP ダイヤル回線を探します。しかし、別の MP 回線の専用 PPP ダイヤル回線は使用しません。また、MP インターフェースに構成されているリンクの最大数を超えることはありません。

BOD は、既存のバンドルに専用 MP ダイヤル・リンクを追加するのに必要な場合は、構成済みのダイヤル回線電話番号を使用してコールを行います。リンクは、ポーリング期間中に必要な場合、一度に 1 つずつバンドルに追加されます。BOD は、最初に任意の PPP シリアル・リンクをバンドルにリンクし、バンドルの存続期間を通じてそのシリアル・リンクを保存します。BOD は、ダイヤル・リンクを除去するだけです。

MP は、以下のフィーチャーをサポートしています。

- BRS
- WRR
- WRS
- ダイヤル・オンデマンド
- DIALs

ただし、WRS、ダイヤル・オンデマンド、および DIALs は、ダイヤル回線だけを含む MP バンドルでだけサポートされます。

MP の考慮事項

MP バンドルを構成するときは、次のことを念頭に入れてください。

- ダイヤル回線を『専用』線と混合すると、ソフトウェアはバンドル上の BAP を使用不可にし、代わりに BOD を使用します。ダイヤル回線を『専用』回線と混ぜて使うのは、バンドルを管理するのに BOD を使用したい場合だけにしてください。
- PPP 『専用』線またはレイヤー 2 トンネル伝送回線のいずれかを含む MP バンドルにはダイヤル・オンデマンドまたは WRS を使用することはできません。
- PPP 『専用』線を含むバンドルでは DIALs を使用することはできません。
- MP バンドルを結合するすべての装置では、リンク速度を構成しておく必要があります。

重要:

1. 極端に異なる特性をもつ媒体とともにバンドルを構成しないでください。たとえば、HSSI リンクと V.25bis リンクを含むバンドルを構成することは、バンドルの効果的な使用ではありません。最大のリンクは、最小のリンクの容量の 4 倍を超えてはなりません。MP バンドル内のリンクの速度が大きく異なる場合、速い方のリンクに受信バッファを追加する必要があります。
2. ISDN B チャネルを低速の媒体タイプと束ねる場合は、ISDN バッファの数を増やす必要があります。ISDN 一次群の場合は、ISDN B チャネルを低速リンクと一緒に束ねることはお勧めできません。

マルチシャシー MP

複数の物理ネットワーク・アクセス・サーバーにまたがる電話ハント・グループを含むレイヤー 2 トンネルをもつ MP バンドルは、マルチシャシー MP と呼ばれます。マルチシャシー MP は、`rhelm` またはユーザーに基づくトンネル伝送 (フィーチャーの使用と構成 の『ローカルまたはリモート認証の使用』を参照) を使用して、MP エンドポイントあて先を設定します。L2TP の詳細については、フィーチャーの使用と構成 の『レイヤー 2 トンネル・プロトコル (L2TP) の使用』を参照してください。

マルチリンク PPP インターフェースの構成

MP インターフェースの構成は、MP バンドルで使用されるインターフェースのタイプによって異なります。以下の節には、さまざまな構成の例が記載されています。

MP インターフェースを構成した後、帯域幅オンデマンド (BOD) を構成することができます。次の例では、既存の MP インターフェース 17 の上で BOD を構成します。

```
Config> net 17
MP config: 17> enable bod
Enable BAP? [N]

MP config: 17> set bandwidth-on-demand parameters
Add bandwidth % [90]:
Drop bandwidth % [70]:
Bandwidth test interval (sec) [15]

MP config: 17>
```

PPP ダイアル回線での MP の構成

この節では、2 つの ISDN ダイアル回線をもつマルチリンク PPP インターフェースの例を使用して、マルチリンク PPP インターフェースを構成する方法を示します。

1. 2 つのダイアル回線およびマルチリンク PPP インターフェースを追加する。

```
*t 6

Config>add dev dial-circuit
Adding device as interface 7
Defaulting Data-link protocol to PPP
Use "net 7" command to configure circuit parameters
Config>add dev dial-circuit
Adding device as interface 8
Defaulting Data-link protocol to PPP
```

MP の使用

```
Use "net 8" command to configure circuit parameters
Config>add dev multilink-ppp
Enter the number of multilink PPP interfaces [1]?
Adding device as interface 9
Defaulting Data-link protocol to PPP
Use "net intf" command to configure circuit parameters
Config>
```

2. 各 PPP ダイアル回線を構成する。(743ページの『第45章 ダイアル回線の構成および監視』を参照してください。) この例では、あて先側、コールの方向、および LID は、ダイアル回線の 1 つに設定されています。

```
Config>net 7
Circuit configuration
Circuit config: 7>set dest out
Circuit config: 7>set calls outbound
Circuit config: 7>set net 6
Circuit config: 7>
```

3. 次のように入力して、MP に使用する各ダイアル回線上の MP を使用可能にする。

```
Circuit config: 7>encapsulator
Point-to-Point user configuration
PPP 7 Config>enable mp

Enabled as a Multilink PPP Link,
Use as a dedicated Multilink PPP link? [No]: yes
Multilink PPP net for this Multilink PPP link [1]? 9
NOTE: PPP configuration will be obtained from the Multilink PPP
net. It is NOT necessary to configure PPP for this net!
```

注: このプロンプトからは、専用リンクの PPP パラメーターを構成することはできません。専用リンクは、既存の MP インターフェースの PPP 構成を使用します。

質問『Use as a dedicated Multilink PPP link?』に対して『Yes』と応答すると、そのリンクは指定されたマルチリンク PPP インターフェース (この例では 9) の専用になります。この場合、このリンクは MP バンドル専用を使用する**必要**があり、指定された MP インターフェースに結合する**必要**があります。このリンクは、通常の PPP ダイアル回線として使用することはできません。

『Use as a dedicated Multilink PPP link?』に対して『No』と応答すると、この PPP ダイアル回線は任意の MP インターフェースに結合することができます。少なくとも 1 つの PPP ダイアル回線が、発信 MP インターフェースへの専用リンクであることが**必要**です。

専用 PPP ダイアル回線は、すべての PPP パラメーター (LCP オプション、認証、その他) を MP インターフェースから入手します。同じ MP バンドルに結合されている MP 使用可能 PPP ダイアル回線は、ネゴシエーションにより同じ LCP パラメーターおよび認証名に設定する**必要**があります。

4. MP インターフェースを構成する。プロトコル BAP、BRS、WAN 復元、WAN 再ルート、およびダイアル・オンデマンドはすべて、PPP ダイアル回線上ではなく、MP インターフェース上で実行されます。

PPP シリアル・リンクでの MP の構成

PPP シリアル・リンク上で MP を構成するには、**net** コマンドを使用してインターフェース上で MP を使用可能にします。リンクは、その PPP 構成を MP ネットから入手します。

例:

```

Config> net 1
PPP 1 Config> enable MP

Multilink PPP net for this Multilink PPP link [1]? 8
NOTE: PPP configuration will be obtained from the Multilink PPP
      net. It is NOT necessary to configure PPP for this net!
PPP 1 Config>

```

レイヤー 2 トンネル伝送ネット上での MP の構成

L2TP ネット上で MP を構成するには、L2TP カプセル化機能を通じて MP を使用可能にします。次に、同じ PPP 交渉パラメーターを構成する必要があります (単一のバンドルに結合されるすべてのネットについては、フィーチャーの使用と構成の『L2TP の構成』を参照してください)。

例:

```

Config> feature layer-2-tunneling
Layer-2-Tunneling Config> encapsulator
PPP-L2TP Config> enable mp

```

NOTE: It IS necessary to configure PPP for this net! PPP negotiation parameters must be configured the same for all nets wishing to join the same Multilink PPP bundle.
PPP-L2TP Config>

マルチシャシー MP の構成

マルチシャシー MP 用の MP を構成するには、DIAL フィーチャーをマルチシャシー MP 用に構成します。ソフトウェアは、使用するエンドポイント識別子を入力するよう求めます。

例:

```

Config> feature DIALs
DIALs Config> set multi-chassis-mp
Enter Endpoint Discriminator to use from stacked group (0 for box S/N): 2345
DIALs Config>

```

次の例は、ポート RTR-2 および RTR-3 がハント・グループに含まれる場合のマルチシャシー MP を示しています。

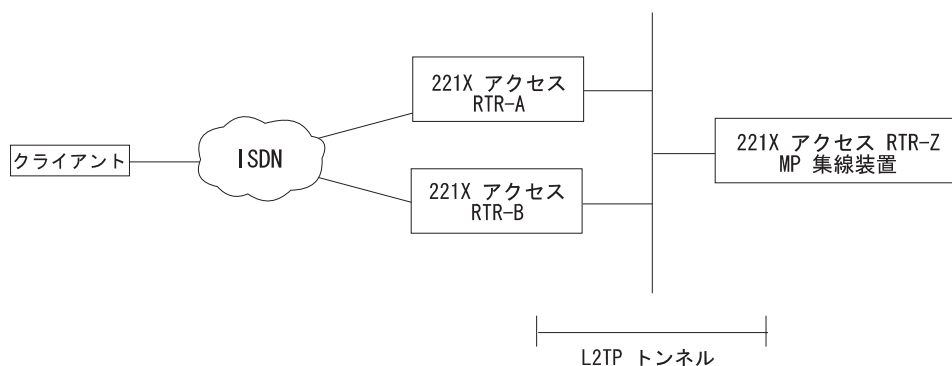


図 29. マルチシャシー MP

MP の使用

アクセス・ルーターと MP 集線装置の間には多数対多数の関係があるので、すべてのアクセス・ルーター (RTR-A、RTR-B) は、『MP 集線装置』ルーター (RTR-Z) とは別の管理ドメインに保持する必要があります。リモート認証 (つまり、RADIUS) を使用したい場合はこれが当てはまります。アクセス・ルーター用に 1 つと MP 集線装置用に 1 つ、あわせて 2 つの RADIUS サーバーが必要になります。ローカル・リストを使用している場合は、すでに別個の管理ドメインを使用しています。

このシナリオでは、PPP ユーザー名または "rhelm" 名に基づいてトンネル伝送することができます。rhelm に基づくトンネル伝送を使用した方が楽です。アイデアとしては、RTR-A と RTR-B の両方で RTR-Z 用のトンネル・プロファイルを構成することになります。これらのルーターでは、追加の PPP ユーザーは必要ありません。RTR-Z は 2 つのトンネル・プロファイル (RTR-A 用に 1 つと RTR-B 用に 1 つ) と PPP ユーザー名 (<username>@RTRZ の形式のもの) を必要とします。すべてのダイヤルイン回線は、『アクセス』ルーター上で構成されます。『MP 集線装置』は、レイヤー 2 トンネル伝送装置およびマルチリンク PPP 装置をもつことになります。

これまでに、マルチシャシー MP を『静的に構成』しました。つまり、特定の PPP ユーザー名は、必ず事前に構成済みのルーター上の MP に終端します。MP バンドルのヘッドを動的に検索し、必要に応じてトンネル伝送する、その他のプロトコルをサポートするようなことはしません。このネットワークの実現は、バンドル内の各リンクごとに異なる媒体タイプを使用するときに、クライアントの PPP 交渉の特異性 (たとえば、あるリンクはトンネル伝送するが、その他はしない) を回避するのに役立ちます。たとえば、DIALs クライアントは、いつでも LCP を交渉できるわけではありません。また、Microsoft DUN クライアントは、LCP 再交渉を完全にサポートしているわけではありません。

第33章 マルチプロトコル PPP プロトコル (MP) の構成および監視

この章では、装置内の特定のマルチリンク PPP インターフェースを構成する方法について説明します。本章には、以下の節が含まれています。

- 『MP 構成プロンプトへのアクセス』
- 『マルチリンク PPP インターフェースの MP 構成コマンド』
- 599ページの『MP インターフェース状態の監視』
- 599ページの『MP 監視コマンドへのアクセス』
- 600ページの『マルチリンク PPP プロトコル監視コマンド』

MP 構成プロンプトへのアクセス

MP 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. **net n** と入力する。ただし、n は、MP が使用可能にされているダイヤル回線または MP インターフェースの番号です。

注: ここで構成するのは、マルチリンク PPP インターフェースであって、MP バンドルの一部である PPP ダイヤル回線ではありません。

マルチリンク PPP インターフェースの MP 構成コマンド

表73 は、MP config > プロンプトで利用可能なコマンドをリストしています。

表 73. MP 構成コマンド

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Disable	帯域幅オンデマンドのネゴシエーションを使用不可にします。
Enable	帯域幅オンデマンドのネゴシエーションを使用可能にします。
Encapsulator	PPP config > プロンプトに入り、データ・リンク・プロトコル構成を変更できるようにします。
List	MP インターフェース構成パラメーターを表示します。
Set	MP インターフェースをインバウンドまたはアウトバウンド・トラフィック用に構成します。アイドル・タイムアウトやその他の MP および BAP パラメーターを設定することもできます。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

MP の構成

Disable

disable コマンドは、帯域幅オンデマンド (BOD) のネゴシエーションを使用不可にするのに使用します。BOD を使用不可にすると、リンクは必要なときに追加帯域幅を割り振りません。

構文:

```
disable                bod
```

Enable

enable コマンドは、BOD のネゴシエーションを使用可能にするのに使用します。BOD を使用可能にすると、リンクは必要なときに追加帯域幅を割り振ることができま

構文:

```
enable                bod
```

Encapsulator

encapsulator コマンドは、マルチリンク PPP インターフェースの PPP リンク・レイヤー構成にアクセスするのに使用します。

構文:

```
encapsulator
```

例:

```
encapsulator  
Point-to-Point user configuration  
PPP config>
```

List

list コマンドは、現行の MP 構成を表示するのに使用します。

構文:

```
list
```

例:

```
list  
Idle timer = 0 (fixed circuit)  
Outbound calls = allowed  
Dialout MP Link net = 7  
Max fragment size = 750  
Min fragment size = 375  
Maximum number of active links = 2  
Links associated with this MP bundle:  
net number 7  
net number 8  
BAP enabled  
Add bandwidth percentage = 90  
Drop bandwidth percentage = 70  
Bandwidth test interval (sec) = 15
```

Idle timer

この回線のアイドル・タイマーの設定値 (秒)

設定値 0 は、固定回線を示します。非ゼロの設定値は、回線が指定された秒数の間アイドル状態であるとダウンにされるダイヤル・オンデマンド MP 回線を構成します。ネットワーク通信が再開されると、回線は再起動されません。

Outbound calls

インターフェースをアウトバウンド・コール用に構成するかどうかを指定します。インターフェースがアウトバウンド・コールを開始できない場合には、この行は表示されません。

Inbound calls

インターフェースをインバウンド・コール用に構成するかどうかを指定します。インターフェースがインバウンド・コールを受け入れることができない場合には、この行は表示されません。

Max fragment size

MP リンクを介して送信するためにパケットを分割する前に、パケットに含めることができるデータの最大バイト数を指定します。

Min fragment size

これは、パケットが **Max fragment size** を超過する場合にソフトウェアが分割する最小サイズ (バイト) です。

Maximum number of active links

MP バーチャル・リンク (**バンドル** と呼ばれます) に構成できるリンクの最大数を指定します。

Links associated with this MP bundle

この MP インターフェースに専用のリンクを表示します。

BAP enabled

このインターフェース上で BAP が使用可能かどうかを指定します。

Add bandwidth percentage

BAP が使用可能の場合、ソフトウェアが新規リンクの追加を試みる際の帯域幅使用率

Drop bandwidth percentage

BAP が使用可能の場合、ソフトウェアが MP バンドルからリンクを除去するときの帯域幅使用率

Bandwidth test interval

バンドルにリンクを追加したり、除去したりする必要があるかどうかを調べるために、ソフトウェアが帯域幅使用率をチェックする時間間隔 (秒)

Set

set コマンドは、以下を構成するのに使用します。

- インバウンド・コール用またはアウトバウンド・コール用の MP インターフェース
- アイドル・タイムアウト
- MP パラメーター
- BAP パラメーター

MP の構成

構文:

```
set bod parameters
      calls
      idle
      mp parameters
```

bod parameters

BOD 追加および除去の帯域幅使用率と BOD テスト間隔を指定するようにプロンプトで指示されます。

例:

```
set bod parameters
Add bandwidth % [90]? 80
Drop bandwidth % [70]? 50
Bandwidth test interval (sec) [15]? 25
```

Add bandwidth %

ソフトウェアが新規リンクの追加を試みる際の帯域幅使用率

有効値: 1 ~ 99

デフォルト値: 90

Drop bandwidth %

ソフトウェアが MP バンドルからリンクを除去するときの帯域幅使用率

有効値: 1 ~ 99

デフォルト値: 70

Bandwidth test interval (sec)

バンドルにリンクを追加したり、除去したりする必要があるかどうかを調べるために、ソフトウェアが帯域幅使用率をチェックする時間間隔 (秒)

有効値: 10 ~ 200 秒

デフォルト値: 15

calls このインターフェースが発信専用、着信専用、あるいは両方のタイプの呼のいずれに使用されるのかを指定します。

有効値: インバウンド、アウトバウンド、または両方

デフォルト値: インバウンド

注: アウトバウンドまたは両方を指定した場合、ソフトウェアは最初にコールする専用 MP リンクの番号を要求します。

例:

```
set calls outbound
Dialout MP link net for this MP net []? 4
```

idle MP インターフェースがすべてのリンクのコールを終了する前に、インターフェース上にプロトコル・トラフィックがない状態でいられる期間 (秒数) を指定します。

有効値: 0 ~ 65535

デフォルト値: 0

mp parameters

最大と最小の分割サイズとアクティブ・リンクの最大数を入力するように求めます。

例:

```
set mp parameters
Max frag size [750]? 675
Min frag size [375]? 300
Max number of active links [2]? 4
```

Max frag size

MP リンクを介して送信するためにパケットを分割する前に、パケットに含めることができるデータの最大バイト数を指定します。

有効値: 100 ~ 3 000

デフォルト値: 750

Min frag size

これは、パケットが **Max fragment size** を超過する場合にソフトウェアが分割する最小サイズ (バイト) です。

有効値: 100 ~ 3 000

デフォルト値: 375

Max number of active links

MP バーチャル・リンク (バンドル と呼ばれます) に構成できるリンクの最大数を指定します。

有効値: 1 ~ 64

デフォルト値: 2

MP インターフェース状態の監視

装置内のすべての MP インターフェースの状態を調べるには、**talk 5** で **configuration** コマンドを使用します (152ページの『Configuration』を参照してください)。

MP 監視コマンドへのアクセス

MP 監視コマンド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 5** と入力する。
2. **net n** と入力する。ただし、**n** は、**talk 6** で **add device multilink-ppp** コマンドを使用して作成された MP インターフェースの番号です。

マルチリンク PPP プロトコル監視コマンド

表74は、MP インターフェースで利用可能なコマンドを示しています。

表 74. MP 監視コマンド

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
List	BAP、BACP、BOD、および MP 統計、誤り、およびその他の情報を表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、帯域幅割り当て統計を含めて、MP インターフェースに関する情報を表示するのに使用します。

構文:

```
list [bap | bacp | bod | mp]
```

注: 以下の例では、この装置上の MP インターフェースは、ネットワーク番号 6 と想定しています。

bacp list bacp コマンドは、この MP 回線上で送信または受信された帯域幅割り当て制御パケットの統計をリストします。

例:

```
PPP 6> list bacp

BACP Statistic      In      Out
-----
Packets:            6        8
Octets:             60       80
Rejects:            0         -
```

bap list bap コマンドは、この MP 回線上で送信または受信された帯域幅割り当てプロトコル・パケットの統計をリストします。

例:

```
PPP 6> list bap

BAP Statistic      In      Out
-----
Packets:            3        3
Octets:            22       37
Call Requests:      1        0
Call Response(ACK): 0         1
Call Resp(NK & FLLNK): 0         0
Call Response(Rej): 0         0
```

```

Callback Requests:          0          0
Callback Response(ACK):    0          0
Cllbck Resp(NK & FLLNK):  0          0
Callback Response(Rej):    0          0
Drop Requests:             0          1
Drop Response(ACK):        1          0
Drop Resp(NK & FLLNK):     0          0
Drop Response(Rej):        0          0
Call Status(Success):      1          0
Call Status(Fail):         0          0

```

ピアの要求に対するレスポンスは、ACK、NAK、FULL-NAK、および REJECT の 4 種類です。

ACK ピアの要求が受け入れられたことを示します。

NAK (NK)

ピアの要求はサポートされますが、この時点では受け入れられないことを示します。後で再試行します。

FULL-NAK (FLLNK)

ピアの要求はサポートされますが、資源の状態により、この時点では受け入れられないことを示します。MP バンドル全体の合計帯域幅が変更されるまでは、この要求を再び送信してはなりません。

REJECT (REJ)

要求はサポートされないことを示します。

control bacp

list control bacp コマンドは、PPP 内部の BACP 状態遷移の現行状態をリストします。この状態情報は、すべての PPP 制御プロトコルで生成されるものと同一です。優先ピアに関する情報もリストされます。優先ピアは、BAP パケット衝突 (両側が同時に要求を開始した場合) を回避するために使用されます。BACP ネゴシエーションの際に、それぞれの側がマジック番号を送信し、小さい方のマジック番号をもつ側が優先ピアとなり、衝突したときには優先されます。通常は、コール開始側はマジック番号 X'1' を選択し、コールの受信側はマジック番号 X'FFFFFFF' を選択するので、コール開始側が優先ピアになります。

```
PPP 6> list control bacp
```

```

BACP State:                Open

BACP Option                Local          Remote
-----
Magic Number:              FFFFFFFF          1
Favorite Peer:             NO                YES

```

control bod

list control bod コマンドは、帯域幅オンデマンド (BOD) の現行状態をリストします。この情報には、BAP 状態、帯域幅の追加および削除のために構成された帯域幅オンデマンド・パラメーター、現行の帯域幅、および前回の帯域幅ポーリングからの情報が含まれます。

有効な BAP 状態は、以下のとおりです。

Closed

BACP はオープンされていません - BAP が使用可能にされていないか、ピアによってサポートされないかのいずれかです。

Ready BACP がオープンされ、処理中のアウトスタンディング要求はありません。

Call Req Sent

ローカル・マシンから送信されたアウトスタンディング・コール・リクエストがあります。

Callback Req Sent

ローカルで送信されたアウトスタンディングのコールバック要求があります。

Call Placed

帯域幅を追加するための BAP 要求の結果、コールされました。

Retry Status Sent

発信コールが MP バンドルに結合するのに失敗し、再試行状態が送信されました。

No Retry Status Sent

発信コールが成功したか、またはすべての再試行回数を使い尽くして、再試行不能状態が送信されました。

Drop Req Sent

ローカルで送信されたアウトスタンディングの除去要求があります。

構成された bandwidth-on-demand パラメーターには、追加比率、除去比率、MP バンドル内のアクティブ・リンクの最大数、および帯域幅ポーリング間隔が含まれます。

バンドルにリンクを追加するための BAP 要求は、次の条件が両方とも満たされている場合に開始されます。

- 現在のアクティブ・リンク数が、構成されたリンクの最大数より少ない。
- MP バンドル内のすべてのリンクの帯域幅使用率が、その MP バンドルで利用可能な合計帯域幅の追加比率より大きい。

MP からリンクを除去するための BAP 要求は、次の条件が両方とも満たされている場合に開始されます。

- アクティブ・リンクの数が 1 より多い。
- MP バンドル内のすべてのリンクの帯域幅使用率が、その MP バンドルのリンク数マイナス 1 の利用可能な合計帯域幅の除去比率より小さい。

帯域幅のポーリングは、BAP がレディー状態のときのみ行うことができます。前回のポーリングからリストされた情報は、MP バンドル全体の帯域幅使用率の様子を伝えます。

除去を開始できるときには、次の 2 組の情報が表示されます。

- バンドル全体の帯域幅使用率
- リンク数マイナス 1 の帯域幅使用率

スラッシングを防止するために、リンクを除去するかどうかを判別するときには、2 番目の組の情報が使用されます。

例:

```
PPP 11>list control bod
```

```
BOD : Disabled
BAP : Disabled
```

```

Bandwidth test interval (sec):          15
Add bandwidth percentage:              90
Drop percentage (links-1):            70
Max # active links in MP bundle:       2
Time since last Bandwidth check (sec): 19
Currently:
  # active links in MP bundle:          0
  Total MP bandwidth (Bytes/sec):       0
Last Bandwidth Check:
  # active links in MP bundle:          0
  Avg Inbound bandwidth util (%):      0
  Avg Outbound bandwidth util (%):     0

```

control mp

list control mp コマンドは、アクティブ・リンク数と帯域幅、構成されたリンクの最大数、および廃棄されたパケット数の統計を含めて、この MP 回線の現行状態をリストします。廃棄された MP パケットは、4 つのカテゴリに分類されます。

M シーケンス番号が受信されておらず、すべてのリンクの前回受信したシーケンス番号のうちの最小シーケンス番号より小さいためにパケットが廃棄されました。

Timeout

タイムアウト期間中にシーケンス番号を受信しなかったため、パケットが廃棄されました。

Q depth

最大待ち行列の長さを超えたために、パケットが廃棄されました。

Seq order

予期しなかったシーケンス番号を受信したために、パケットが廃棄されました。これは MP がすでに紛失したと宣言された遅延パケットを受信した場合に起こります。

パケットがネットワーク・レイヤーで廃棄された場合は、M、Timeout、または Q depth パケットのいずれかです。これらのカウンターは、パケットが廃棄されると、それに応じて増分されます。

```

PPP 11> list control mp
Current # active links in MP bundle:    0
Max # active links in MP bundle:       2
Total MP bandwidth (Bytes/sec):         0
Dropped Frags (lost packets):           0
Dropped Frags (timeout or receive overflow): 0
Dropped Frags (sequence not expected):  0

```

PPP 11>

mp list mp コマンドは、この MP 回線で送信または受信されたパケットの統計をリストします。表示されるバイト数は、マルチリンク PPP バンドルの解凍がネゴシエーションされた場合は、解凍前のパケットのバイト数です。

```

PPP 6> list mp

```

```

MP Statistic          In          Out
-----
Bytes (Compressed):   61230     60259

```

MP の監視

第34章 SDLC リレーの構成および監視

この章では同期データ・リンク制御 (SDLC) リレー機能の概要を記載し、その構成コマンドおよびオペレーショナル・コマンドについて説明します。

DLSw SDLC と SDLC リレーの使い分け方については、*Nways* マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第1巻 中の『DLSw の使用』の章の『SDLC リレー機能の関係』を参照してください。

本章には、以下の節が含まれています。

- 『SDLC リレーの概要』
- 607ページの『基本構成手順』
- 607ページの『動的再構成』
- 616ページの『SDLC リレー監視環境へのアクセス』
- 617ページの『SDLC リレー監視コマンド』
- 620ページの『SDLC リレー・インターフェースおよび GWCON インターフェース・コマンド』

SDLC リレーの概要

SDLC リレーは、IP 接続を経由して IP 内にカプセル化された SDLC パケットをトランスポートする機能です。SDLC 接続は、1 次 (ポーリング側) エンドポイントおよび 2 次 (ポーリングされる側) エンドポイントから構成されます。これらは、ポイント・ポイント (1 つの 1 次装置および 1 つの 2 次装置) またはマルチポイント (1 つの 1 次装置および複数の 2 次装置) のいずれかです。SDLC リレーはこの設計を保持していますが、ルーターが、1 次と 2 次の SDLC 装置間でフレームを転送する点が異なります。

606ページの図30 は、1 次 SDLC 装置が 2 つの 2 次 SDLC 制御装置に接続されている SDLC リレー構成の例を示しています。

SDLC リレーの構成および監視

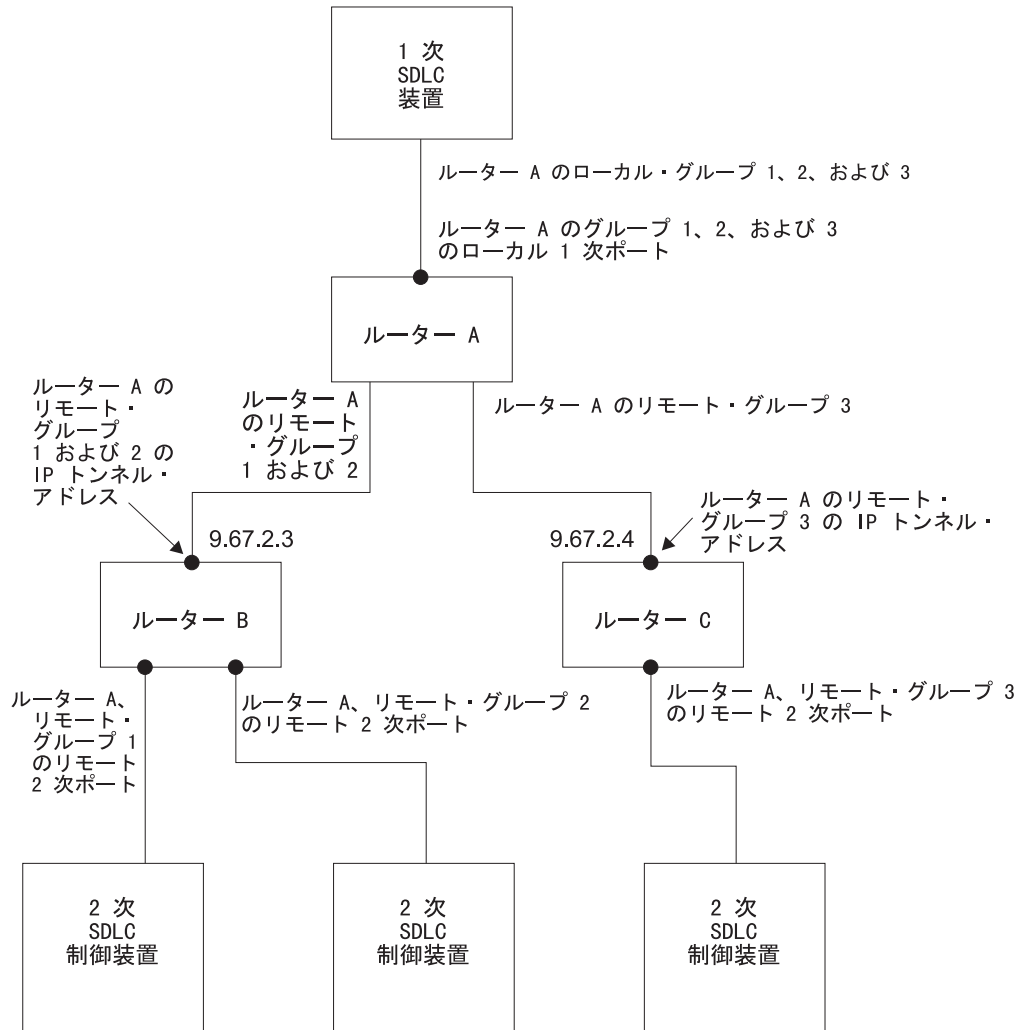


図 30. SDLC リレー構成の例

示されているように、1 次および 2 次 SDLC 装置はそれぞれローカルにルーターに接続されています。ルーターは、IP 接続またはトンネルを通じて通信し、SDLC エンドポイント間のパイプとして働きます。構成時に、ルーターへの接続をバーチャル・グループとして定義します。これらのグループには任意の番号も割り当て、ルーターに対してそれらを識別します。ローカル・グループには、ルーターのローカル・インターフェースであるローカル・ポートが含まれます。各ローカル・グループには、1 つの対応するリモート・グループがあり、後者は、リモート・ルーターのインターフェースであるリモート・ポート、およびローカル・ルーターをリモート・ルーターに接続する IP トンネルのアドレスから構成されます。リモート・ルーターは、ローカル・ルーターのピアです。たとえば、ルーター B およびルーター C はルーター A のリモート・ルーターです。トンネルの IP アドレスは、リモート・ルーターの内部 IP アドレスです。詳細については、*Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 2 巻* の `set internal-ip-address` コマンドを参照してください。

各ポートは、接続の最終エンドポイントに応じて、1 次または 2 次としても識別されます。各グループ内で、1 つのポートは 1 次で、1 つは 2 次です。例にあるグループでは、ローカル・グループおよび対応するリモート・グループに同じ番号が付い

ていますが、このマッチングは必須ではありません。たとえば、ルーター A の場合、ローカル・グループ 2 には、ローカル・グループ 2 用のローカル 1 次ポートが含まれています。対応するリモート・グループにも 2 の番号が付いていますが、別の番号によって識別することもできます。

この例でルーター B に接続されていた 2 次 SDLC 制御装置は、同じ回線に接続されていません。これは、バーチャル・マルチポイント・コネクションの例です。SDLC 制御装置が同じ回線に直接接続されている場合、これは物理接続と見なされます。1 つのネットワーク内で、物理接続とバーチャル・コネクションの両方をもつことができます。

マルチポイント・ネットワーク内で、2 次装置は 1 バイトまたは 2 バイトのステーション・アドレスによって識別されます。1 つの SDLC ネットワーク内のすべての SDLC リレー・ルーターは、同じ数のアドレス・バイト (すべて 1 バイトまたはすべて 2 バイトのいずれか) を使用する必要があります。ルーターは、2 次 SDLC 制御装置を動的に識別します。その知識に基づき、ルーターは、特定の装置へのフレームをその装置に送信することができます。同報通信フレームは、送信側の装置からネットワーク内の他のすべての装置に引き続き同報通信されます。

半二重伝送モードだけがサポートされます。これは、各伝送の前に送信要求 (RTS) を出す必要があることを意味します。送信可 (CTS) は、永続的にアップのままになるわけではありません。

基本構成手順

この節では、SDLC リレー・プロトコルを立ち上げて実行するのに必要な最小構成ステップについて概説します。パラメーターの詳しい説明については、605 ページの『SDLC リレーの概要』および構成コマンドの説明を参照してください。

- ローカル・グループを追加する。 **add group** コマンドを使用してローカル・グループを構成する必要があります。
- ローカル・ポートを追加する。これは、ローカル・ポートで使用するインターフェースを識別します。またこれにより、選択したインターフェースに対して IP アドレスが構成されないことも保証されます。 **add local-port** コマンドを使用します。
- リモート・ポートを追加する。これは、シリアル・ラインのリモート側に直接接続されたポートを識別します。 **add remote-port** コマンドを使用します。

動的再構成

Talk 5 **reset interface#** および **activate interface#** コマンドは、Talk 6 を使ってインターフェース上に構成したすべての SDLC リレー・パラメーターをアクティブにするのに使用することができます。あるいは、ルーターをリスタートまたは再ロードして、新しい構成変更を有効にすることができます。

SDLC リレー構成環境へのアクセス

SDLC リレー (SRLY) 構成環境にアクセスするには、次のようにします。

1. Config> プロンプトで **set data-link srlly** と入力する。
2. インターフェース番号を入力する。
3. SRLY インターフェースを構成するために、**network interface#** コマンドを入力する。**network interface#** を入力すると、SRLY *interface#* Config> プロンプトが表示されます。

```
Config>network 2
SDLC Relay interface user configuration
SRLY 1 Config>
```

4. SRLY プロトコル・パラメーターを構成するために、**protocol sdlc** コマンドを入力する。**protocol sdlc** を入力すると、SDLC Relay config> プロンプトが表示されます。

```
Config>protocol sdlc
SDLC Relay protocol user configuration
SDLC Relay config>
```

SDLC リレー構成コマンド

この節では、SDLC リレー構成コマンドの要約を示します。この章には、SDLC リレーの **network** パラメーターと **protocol** パラメーターの両方が記載されています。

SDLC リレー構成コマンドでは、SDLC リレー・フレームを転送するインターフェースのルーター・パラメーターを指定することができます。表75 は、**network sdlc** および **protocol sdlc** の両方のコマンドを示しています。

表 75. SDLC リレー構成コマンドの要約

コマンド	ネットワーク		機能
	ネットワーク SRLY	プロトコル SDLC	
? (Help)	可	可	すべての SDLC リレー構成コマンドをリストするか、または特定のコマンドに関連するオプションをリストします。
Add		可	グループ、ローカル・ポート、およびリモート・ポートを追加します。
Delete		可	グループおよびポートを削除します。
Disable		可	グループおよびポートを使用不可にします。
Enable		可	グループおよびポートを使用可能にします。
List	可	可	SDLC リレー全体の構成およびグループ特有の構成を表示します。
Set	可		リンク・パラメーターおよびリモート端末パラメーターを設定します。
Exit	可	可	SDLC リレー構成環境を終了して、CONFIG 環境に戻ります。

Add

add コマンドは、ローカル・グループ、ローカル・ポート、およびリモート・ポートを追加するのに使用します。

構文:

```
add group local-group# group-type local-group-name
      local-port
      remote-port
```

group ローカル・グループを定義します。ローカル・グループは、番号および名前によって識別されます。

例: add group

```
Local group number: [1]?
Local group name [1]? CHICAGO-TO-MIAMI
(P)oint-to-Point or (M)ultipoint: [P]?
```

Local-group-number

ローカル・グループを識別するのに指定するグループ番号

Local-group-name

これは、このローカル・グループの名前です。ローカル・グループに名前を付けるのに最大 32 文字の ASCII 文字を使用することができます。名前を提供しない場合、デフォルト名の LOCAL-GROUP-*n* が使用されます。ここで、*n* はローカル・グループ番号です。

Group-type

グループ・タイプは、ポイント・ポイントまたはマルチポイントです。

local-port

ローカル・ポートに使用するインターフェースを識別します。

例: add local-port

```
Local group number: [1]?
Interface number: [0]? 3
(P)rimary or (S)econdary: [S]? p
```

Local group number

ポートのローカル・グループ番号

Network or interface number

ローカル・ポートを示すルーターのネットワークまたはインターフェース番号

Primary or Secondary

ポート・タイプ (1 次 (P) または 2 次 (S)) を指定します。デフォルトは 2 次です。

remote-port

リモート・ルーターのシリアル・ラインに直接接続されたポートを識別します。

例: add remote-port

```
Local group number: [1]?
IP address of remote router: [0.0.0.0]? 9.67.2.3
Is the remote's upper group number limit 255 (current) or 15 (migration): [255]?
Remote router group number: [1]?
Does the connection use 2-byte station addressing: [Y]?
(P)rimary or (S)econdary: [S]? s
```

Group number

ポートのローカル・グループ番号

SDLC リレーの構成および監視

IP address of remote router

リモート・ルーターの内部 IP アドレス。ルーターをリモート・ルーターに接続する IP トンネルを識別します。

Upper group number limit

使用することができるグループ番号の上限によって定義されたリモート・ルーターのサポート・レベル。デフォルトはカレントで、これは 255 の限度および 1 ~ 255 の範囲です。

Remote router group number

このリモート・ポートが属するリモート・グループのグループ番号。ローカルおよびリモートのグループ番号は同じ番号である必要はありません。

Two-byte or one-byte station addressing

ステーション・アドレス内のバイトの数。ステーション・アドレスは、2 次 SDLC 装置の SDLC アドレスです。デフォルトは 2 バイトです。

Primary or Secondary

ポート・タイプ (1 次 (P) または 2 次 (S)) を指定します。デフォルトは 2 次です。

Delete

delete コマンドは、グループ番号、ローカル・ポート、およびリモート・ポートを削除するのに使用します。

構文:

```
delete                group . . .  
                        local-port . . .  
                        remote-port
```

group *group#*

ローカル・グループ (*group#*) を除去します。

local-port *group#*

指定されたグループのローカル・ポートを除去します。

remote-port

指定されたグループのリモート・ポートを除去します。

例: **delete remote-port**

```
Group number: [1]? 1
```

Group number

リモート・ポートのリモート・グループ番号

Disable

disable コマンドは、リレー・グループ全体または特定のリレー・ポートのリレーを抑制します。

構文:

SDLC リレーの構成および監視

例:

```
list
Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable Type: RS-232 DTE
Speed (bps): 0
Transmit Delay Counter: 0
```

Maximum frame size in bytes

リンクを介して送信できる最大フレーム・サイズ。最大フレーム・サイズは、最大フレームと 6 バイトの SRLY ヘッダーが収まる大きさでなければなりません。

Encoding

シリアル・インターフェースの伝送符号化法。符号化法は、NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) です。

Idle State

データ・リンク・アイドル状態: フラグまたはマーク

Clocking

クロックのタイプ: 内部または外部

Cable Type

シリアル・インターフェースのケーブル・タイプ

Speed (bps)

送信クロックと受信クロックの速度をリストします。

Transmit Delay Counter

連続するフレーム相互間に送信されるフラグの数

List (プロトコル SDLC リレーの場合)

list コマンドは、特定のグループまたはすべてのグループの構成を表示するのに使用します。

構文:

```
list                                all
                                   group . . .
```

all すべてのローカル・グループの構成を表示します。

例: **list all**

SDLC/HDLC Relay Configuration

```
Local group      = 1
Group Name       = CHICAGO-TO-MIAMI
Group Type       = MULTI                               Enabled    = YES
Local port      = PRIMARY                             Enabled    = YES
Interface       = 2
Remote port     = SECONDARY                            Enabled    = YES
Remote group    = 1                                  Addressing = 2-BYTE
IP Address      = 9.67.2.3                             Code level = CURRENT

Local group      = 2
Group Name       = CHICAGO-TO-RALEIGH
Group Type       = MULTI                               Enabled    = YES
```

Local port	= PRIMARY	Enabled	= YES
Interface	= 3		
Remote port	= SECONDARY	Enabled	= YES
Remote group	= 2	Addressing	= 2-BYTE
IP Address	= 9.67.2.3	Code level	= CURRENT
Local group	= 3		
Group Name	= CHICAGO-T0-PITTSBURGH		
Group Type	= PT-PT	Enabled	= YES
Local port	= PRIMARY	Enabled	= YES
Interface	= 4		
Remote port	= SECONDARY	Enabled	= YES
Remote group	= 3	Addressing	= 2-BYTE
IP Address	= 9.67.2.4	Code level	= CURRENT

Local group

ローカル・グループ番号を示します。

Group Name

ローカル・グループ名を示します。

Group Type

ローカル・グループ・タイプ (ポイント・ポイントまたはマルチポイント) を示します。

Local port

ポートが 1 次または 2 次のどちらであるか、その状況が **enabled** (使用可能) または **disabled** (使用不可) のどちらであるかを示します。

Interface

ローカル・ポートのネットワークまたはインターフェース番号を示します。この番号は、**Config list devices** コマンドを使用して表示された番号に一致します。

Remote port

リモート・ポートが 1 次または 2 次のどちらであるか、その状況が **enabled** (使用可能) または **disabled** (使用不可) のどちらであるかを示します。

Remote group

リモート・グループのグループ番号を示します。

Addressing

1 バイトまたは 2 バイトのどちらのアドレッシングが使用されるかを示します。

IP address

このグループのリモート・ルーターの内部 IP アドレスを示します。ルーターをリモート・ルーターに接続する IP トンネルを識別します。

Code level

コード・レベルが現行または移行のどちらであるかを示します。コード・レベルは、グループを識別するために使用することができる番号の範囲を決定します。現行コード・レベルは 1 ~ 255 の範囲をもち、移行コード・レベルは 0 ~ 15 の範囲をもちます。

group *group#*

指定されたグループの構成を表示します。

Set

set コマンドは、SRLY インターフェース・パラメーターを構成するのに使用します。

構文:

```
set cable
      clocking
      encoding
      frame-size
      idle
      speed
      transmit-delay
```

cable シリアル・インターフェースで使用されるケーブルを設定します。オプションは、次のとおりです。

- RS-232 DTE
- RS-232 DCE
- V35 DTE
- V35 DCE
- V36 DTE
- V36 DCE
- X21 DTE
- X21 DCE

表76 では、各種のアダプターで構成することができるケーブル・タイプをリストします。

表 76. 2210 インターフェースのケーブル・タイプ

アダプター・タイプ	ケーブル・タイプ
8 ポート EIA 232	RS-232 DTE および RS-232 DCE
6 ポート V.35/V36	V.35 DCE、V.35 DTE、V.36 DCE、または V.36 DTE
8 ポート X.21	X.21 DCE および X.21 DTE

例: **set cable V35 dte**

DTE ケーブルは、ルーターをあるタイプの DCE 装置 (たとえば、モデムまたは DSU/CSU) に接続するときを使用します。

DCE ケーブルは、ルーターが DCE として動作し、直接接続のためのクロックを提供するときを使用します。

clocking *internal or external*

モデムまたは DSU に接続するには、外部クロックを構成し、**set cable** コマンドを使って該当する DTE ケーブルを選択します。

別の DTE 装置に直接接続するには、内部クロックを構成し、**set cable** コマンドを使って該当する DCE ケーブルを選択し、**set speed** コマンドを使ってクロック/回線速度を構成します。

デフォルト値: external

Example:

```
set clocking internal
```

encoding nrz or nrzi

SRLY インターフェースの伝送符号化法を NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) として構成します。NRZ がデフォルトです。

例: `set encoding nrz`

frame-size

データ・リンク上で送受信できるフレームの最大サイズを構成します。この値を `add remote-secondary` コマンドで指定した値より大きく設定した場合、この値はその最大値を反映するように変更されます。IBM 2210 は、この値が変更されることをユーザーに警告するメッセージを生成します。ユーザーは、これが SRAM 構成内で変更されるまで、この ELS メッセージを継続的に受け取ります。有効な入力値を表77 に示します。

注: 最大フレーム・サイズは、最大フレームと 15 バイトの SRLY ヘッダーが収まる大きさでなければなりません。

表 77. *Set Frame-Size* コマンドのフレーム・サイズの有効値

最小	最大	デフォルト
128	8187	2048

idle flag

SRLY インターフェース上のフレーム転送の送信アイドル状態を構成します。デフォルト設定はフラグ・オプションで、これはフレーム相互間に連続フラグ (16 進 7E) を提供します。

リンクはフラグ・アイドルを透過的に受け取ります。

idle mark

SRLY インターフェース上のフレーム転送の送信アイドル状態を構成します。マーク・オプションは、フレーム間の伝送路をマーキング状態 (OFF, 1) にします。

リンクはマーク・アイドルを透過的に受け取ります。

speed

内部クロックの場合は、このコマンドを使用して送信および受信クロック回線の速度を指定します。

外部クロックの場合は、このコマンドは WAN/シリアル・ラインの動作に影響を与えません。

有効値:

内部クロック: 表78 を参照してください。

外部クロック: 616ページの表79 を参照してください。

表 78. 2210 インターフェースに内部クロックが使用されるときの内線速度

アダプター・タイプ	速度範囲
8 ポート EIA 232	9600 ~ 64 000 bps
6 ポート V.35/V.36	9600 ~ 460 800 bps、1 544 000 bps、または 2 048 000 bps

SDLC リレーの構成および監視

表 78. 2210 インターフェースに内部クロックが使用されるときの回線速度 (続き)

アダプター・タイプ	速度範囲
8 ポート X.21	9600 ~ 460 800 bps、1 544 000 bps、または 2 048 000 bps

表 79. 2210 インターフェースに外部クロックが使用されるときの回線速度

アダプター・タイプ	速度範囲
8 ポート EIA 232	2400 ~ 64 000 bps
6 ポート V.35/V.36	2400 ~ 2 048 000 bps
8 ポート X.21	2400 ~ 2 048 000 bps

transmit-delay value

転送されるパケット間に遅延を挿入することができます。このコマンドは、フレーム相互間の最小遅延を保証することにより、相手側の旧型で低速のシリアル装置に整合させます。この値は、連続するフレーム間に送信するフラグ・バイト数として指定します。範囲は 0 ~ 15 です。デフォルトは 0 です。

注: 8 ポート EIA- 232E アダプター、6 ポート V.35/V.36 アダプター、または 8 ポート X.21 アダプター上の SDLC リレー・インターフェースに非ゼロの伝送遅延を構成する場合は、**set speed** コマンドを使用して回線速度を構成する必要があります。

SDLC リレー監視環境へのアクセス

SDLC リレー・インターフェースに関連する情報を監視するには、以下を行って、インターフェース監視プロセスにアクセスします。

1. **status** コマンドを入力して、GWCON の PID を見つける。(status コマンドの出力例については、11 ページを参照してください。)
2. OPCON プロンプトで、**talk** コマンドと GWCON の PID を入力する。たとえば、次のように入力します。

```
* talk 5  
+
```

GWCON プロンプト (+) がコンソールに表示される。最初に GWCON に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

3. GWCON プロンプトで **configuration** コマンドを入力して、ルーターに構成されているプロトコルとネットワークを表示する。たとえば、次のように入力します。

```
+ configuration
```

(configuration コマンドの出力例については、152 ページを参照してください。)

4. **protocol sdlc** コマンドを入力する。たとえば、次のように入力します。

```
+ prot sdlc  
SDLC Relay>
```

SDLC リレー・プロンプトがコンソールに表示されます。これで、SDLC リレー監視コマンドを入力して、SDLC リレー・グループに関する情報を表示することができます。

SDLC リレー監視コマンド

この節では、SDLC リレー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。SDLC リレー監視コマンドでは、SDLC リレー・フレームを転送するインターフェースのパラメーターを表示することができます。これらのコマンドの一部 (**enable** および **disable** など) も、操作上は有効になりますが、構成には影響を与えません。すべての SDLC リレー監視コマンド用の SDLC Relay> プロンプトが表示されます。表80 は、コマンドを示しています。

表 80. SDLC リレー監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Clear-Port-Statistics	指定されたポートの SDLC リレー統計を消去します。
Disable	グループおよびポートを一時的に抑制します。
Enable	グループおよびポートを一時的にオンにします。
List	SDLC リレー全体の構成およびグループ特有の構成を表示します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Clear-Port-Statistics

clear-port-statistics コマンドは、すべてのポートの SDLC リレー統計を廃棄するのに使用します。統計には、転送されたパケットおよび廃棄されたパケットのカウンターが含まれます。

構文:

clear-port-statistics

clear-port-statistics

前回のルーターのリスタートまたは統計の消去以降に収集されたポート統計を消去します。

例:

```
clear-port-statistics
Clear all port statistics? (Yes or No): Y
```

Disable

disable コマンドは、グループ全体または特定のリレー・ポートのデータ転送を抑制します。SRAM (静的読み取りアクセス・メモリー) は、**disable** 監視コマンドの影響を永続的に保存しません。そのため、ルーターをリスタートすると、このコマンドの影響は消去されます。

構文:

```
disable group . . .
port
```

SDLC リレーの構成および監視

group *group#*

指定されたローカル・グループ (group#) との間の SDLC リレー・フレームの転送を抑制にします。

port 指定されたローカルまたはリモート・ポートとの間の SDLC リレー・フレームの転送を抑制にします。

Enable

enable コマンドは、グループ全体または特定のローカル・インターフェース・ポートのデータ転送をオンにするのに使用します。SRAM は、**enable** 監視コマンドの影響を永続的に保存しません。そのため、ルーターをリスタートすると、このコマンドの影響は消去されます。

構文:

```
enable                group . . .  
                        port
```

group *group#*

指定されたローカル・グループ (group#) との間の SDLC リレー・フレームの転送を可能にします。

port 指定されたローカルまたはリモート・ポートとの間の SDLC リレー・フレームの転送を可能にします。

List

list コマンドは、特定のグループまたはすべてのグループの構成を表示するのに使用します。

構文:

```
list                  all  
                        group . . .
```

all すべてのローカル・ポートの構成を表示します。

例:

```
list all  
SDLC/HDLC Relay Configuration  
  
Local group      = 1  
Group Name       = CHICAGO-TO-MIAMI  
Group Type       = MULTI           Enabled    = YES  
Local port       = PRIMARY         Enabled    = YES  
Interface        = 2  
Remote port      = SECONDARY       Enabled    = YES  
Remote group     = 1               Addressing = 2-BYTE  
IP Address       = 9.67.2.3        Code level = CURRENT  
  
Local group      = 2  
Group Name       = CHICAGO-TO-RALEIGH  
Group Type       = MULTI           Enabled    = YES  
Local port       = PRIMARY         Enabled    = YES  
Interface        = 3  
Remote port      = SECONDARY       Enabled    = YES  
Remote group     = 2               Addressing = 2-BYTE  
IP Address       = 9.67.2.3        Code level = CURRENT  
  
Local group      = 3
```

Group Name	= CHICAGO-TO-PITTSBURGH	Enabled	= YES
Group Type	= PT-PT	Enabled	= YES
Local port	= PRIMARY		
Interface	= 4		
Remote port	= SECONDARY	Enabled	= YES
Remote group	= 3	Addressing	= 2-BYTE
IP Address	= 9.67.2.4	Code level	= CURRENT

Local group

ローカル・グループ番号を示します。

Group Name

ローカル・グループ名を示します。

Group Type

ローカル・グループ・タイプ (ポイント・ポイントまたはマルチポイント) を示します。

Local port

ポートが 1 次または 2 次のどちらであるか、その状況が enabled (使用可能) または disabled (使用不可) のどちらであるかを示します。

Interface

ローカル・ポートのネットワークまたはインターフェース番号を示します。この番号は、Talk 6 **list devices** コマンドまたは Talk 5 **config** コマンドを使用して表示された番号に一致します。

Remote port

リモート・ポートが 1 次または 2 次のどちらであるか、その状況が enabled (使用可能) または disabled (使用不可) のどちらであるかを示します。

Remote group

リモート・グループのグループ番号を示します。

Addressing

1 バイトまたは 2 バイトのどちらのアドレッシングが使用されるかを示します。

IP address

このグループのリモート・ルーターの内部 IP アドレスを示します。ルーターをリモート・ルーターに接続する IP トンネルを識別します。

Code level

コード・レベルが現行または移行のどちらであるかを示します。コード・レベルは、グループを識別するために使用することができる番号の範囲の上限を決定します。

group *group#*

指定されたグループの構成を表示します。

SDLC リレー・インターフェースおよび GWCON インターフェース・コマンド

SDLC リレー・インターフェースには独自の監視目的の監視プロセスがありますが、GWCON 環境から **interface** コマンドを使用すれば、ルーターも導入済みネットワーク・インターフェースの完全な統計を表示します。(**interface** コマンドの詳細については、第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド を参照してください。)

第35章 SDLC インターフェースの使用

この章では、SDLC インターフェースの使用法について説明します。本章には、以下の節が含まれています。

- 『基本構成手順』
- 『交換 SDLC コールイン・インターフェースの構成』
- 623ページの『SDLC 構成要件』

SDLC 構成コマンドは `SDLC # Config>` プロンプトで入力します。ただし、`#` は `network` コマンドで指定するインターフェースを識別します。ルーターの構成に加えた変更は、即時には有効にはならず、ルーターがリスタートされたときに、ルーターの静的構成メモリーの一部になります。

基本構成手順

この節では、DLSw または APPN で SDLC を使用できるようにするのに必要な最小構成について概説します。

構成手順を開始する前に、`config` プロセスから `list device` コマンドを使用して、各種の装置のインターフェース番号のリストを表示します。`Config` プロンプトで、`network interface number` または `n interface number` のいずれかを入力して、構成するインターフェースを選択します。構成コマンドについて詳しい説明が必要な場合は、本章の構成コマンドの説明箇所を参照してください。

交換 SDLC コールイン・インターフェースの構成

交換 SDLC コールイン・インターフェースを使用すると、PU タイプ 2.0 装置が交換 SDLC 回線を使用して 2210 にダイヤルインすることが可能になり、ネットワークの接続オプションが追加されます。インターフェースは PU タイプ 2.0 装置に限られ、DLSw しか実行することができません。

注: 交換 SDLC コールイン・インターフェースを介する APPN は構成できません。

交換 SDLC コールイン・インターフェースを構成するには、次のようにします。

1. V.25bis 基本ネットワークを構成する。

```
Config> set data-link v25bis 2
Config> net 2
V25bis Config>
(configuration the V25bis net)
```

V.25bis の構成についての詳細は、673ページの『第39章 V.25bis ネットワーク・インターフェースの使用』を参照してください。

注: `encoding type` および `full` 対 `half duplex` といった物理レイヤーのパラメーターはすべて、交換 SDLC ダイヤル回線インターフェース上ではなく、V.25bis インターフェース上で構成します。

2. ダイヤル回線装置を追加する。

```
Config> add device dial
```

SDLC インターフェースの使用

- ダイヤル回線インターフェースのデータ・リンクを SDLC に設定する。この例では、ダイヤル回線はインターフェース 3 です。

```
Config> set data-link sdlc 3
```

- ダイヤル回線を構成する。

```
Config> net 3
Dial circuit config> set net 2 1
Dial circuit config> encapsulator
sdlc config>
  (configure SDLC)
sdlc config> exit
Dial circuit config> exit
Config>
```

- DLSw を構成する。

```
Config> prot dls
DLSw protocol user configuration
DLSw config> add sdlc
Interface # [0]? 3
SDLC Address or 'sw' (switched dial-in) [sw]? sw 2
Source MAC address [4000112402C1]? 4000003174d2
Source SAP in hex [4]?
Destination MAC address [000000000000]? 400000000004 3
Destination SAP in hex [0]? 4 4

XID0 block num in hex (0-0xfff) [0]? 017
XID0 id num in hex (0-0xffff) [0]? 00001
For a switched dial-in link station ....
- PU type is forced to be 2
- Configured XID block/id num is used to override
  fields in the XID0 from the SDLC station
  - if block/id set to zeroes, XID0 is not modified
  - otherwise configured fields are put into XID0
- Poll type is not configured (not used)
DLSw config> li sdlc all
Net Addr Status Source SAP/MAC Dest SAP/MAC PU Blk/IdNum PollFrame
3 FF(sw) Enabled 04 4000003174D2 04 400000000004 2 017/00001 TEST

DLSw config> exit
Config>
```

1 その他のパラメータ値はすべて、ソフトウェアがデフォルト値を取るの
で、これ以外のダイヤル回線パラメータは設定できません。デフォルト値について
の詳細は、744ページの『Encapsulator』を参照してください。

2 『sw』という指定は、これが交換 SDLC コールイン・インターフェースである
ことを示します。

3 あて先 MAC アドレスは、オール 0 であってはなりません。0 を指定した
り、デフォルト値の 0 を受け入れた場合、ソフトウェアは有効なアドレスを入力
するように求めるプロンプトを出します。

4 あて先 SAP は 0 であってはなりません。0 を指定したり、デフォルト値の
0 を受け入れた場合、ソフトウェアは有効なアドレスを入力するように求めるプロ
ンプトを出します。

DLSw の構成についての追加情報は、*Nways* マルチプロトコル・ルーティング・サー
ビス プロトコルの構成と監視 解説書 第 1 巻の『DLSw の監視』の章の『DLSw の
使用および構成』の項を参照してください。

SDLC 構成要件

この章で説明した SDLC 特有の構成手順およびコマンドに加えて、DLSw または APPN プロトコルでも SDLC を構成する必要があります。特定の SDLC インターフェース上では、一度に 1 つのプロトコル (DLSw または APPN) しか実行できません。言い換えると、特定の SDLC インターフェース上のリンク・ステーションは、APPN と DLSw 間で分割することはできません。同じ SDLC インターフェースに対する DLSw 構成と APPN 構成が存在する場合は、最初にアクティブになったプロトコルが、その SDLC インターフェースを所有することになります。

第36章 SDLC インターフェースの構成および監視

この章では、SDLC の構成コマンドおよびオペレーショナル・コマンドについて説明します。

本章には、以下の節が含まれています。

- 『SDLC 構成環境へのアクセス』
- 626ページの『SDLC 構成コマンド』
- 639ページの『SDLC 監視環境へのアクセス』
- 640ページの『SDLC 監視コマンド』
- 650ページの『SDLC インターフェースおよび GWCON インターフェース・コマンド』
- 650ページの『SDLC インターフェースで表示される統計』

構成コマンド・コンソール (SDLC CONFIG>) で行った変更は、ルーターをリスタートすると SRAM 構成の一部になります。

逆に、SDLC 監視プロセス内で入力した SDLC 監視コマンドは、即時に有効になります。ただし、監視コマンドを用いて行った変更は、ルーターの静的構成の一部にはなりません。ルーターをリスタートすると、監視コマンドの影響は、ルーターの静的構成によって上書きされます。監視は、以下のアクションから構成されます。

- 現在ルーターによって使用されているプロトコルおよびネットワーク・インターフェースを監視する。
- SDLC 構成に永続的な影響を与えずに、SRAM 構成をリアルタイムで変更する。
- ルーターのアクティビティおよび性能に関連する ELS (イベント・ログ・システム) メッセージを表示する。

SDLC 構成環境へのアクセス

ルーターの構成を変更するには、CONFIG プロセスを使用します。新規の構成は、ルーターをリスタートすると有効になります。

構成プロセスに入るには、次のようにします。

1. OPCODE (*) プロンプトで **talk 6** (または **t 6**) を入力する。これにより、次の例のような CONFIG> プロンプトが表示されます。

```
MOS Operator Console
For help using the Command Line Interface, press ESCAPE, then '?'
* talk 6
CONFIG>
```

CONFIG> プロンプトがすぐに表示されない場合は、**Enter** キーをもう一度押してください。

SDLC インターフェースの構成

SDLC 構成コマンドは SDLC config> プロンプトで入力します。GWCON t 5 (149ページの『第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』を参照) 環境を使用して、動的な構成変更を行います。ただし、装置がリスタートされると、これらの変更は消えます。

2. Config> プロンプトで **set data-link sdlc** コマンドを入力する。プロンプトが出たら、SDLC 装置に関連付けるインターフェースの名前を入力します。

```
Config>set data-link sdlc
Interface number [0]? 2
Config>
```

3. 次に、**network** コマンドと、前に入力した SDLC インターフェースの番号を入力する。

```
Config>network 2
SDLC 2 Config>
```

構成環境に関する情報は、3ページの『第1章 開始』を参照してください。

SDLC 構成コマンド

SDLC 構成コマンドを用いて、SDLC インターフェース構成を作成または変更することができます。この節では、ネットワーク構成コンソール内の SDLC Config> プロンプトから出すことができる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。コマンドとそのパラメーターのデフォルト値は、プロンプトの直後に大括弧で囲んで表示されています。

注: 本章に説明されているコマンドを使用して SDLC を構成するのに加えて、DLSw または APPN プロトコルでも SDLC を構成する必要があります。

2210 は、RS-232、X.21、および V.35 シリアル・インターフェースを介する SDLC 接続をサポートします。表81 は、SDLC 構成コマンドとその機能をリストしています。

表 81. SDLC 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Add	SDLC エンド・ステーションを追加します。ステーションが特に追加されない場合、DLSw または APPN が装置をアクティブにするときに、デフォルト値を使って動的に作成されます。
Delete	SDLC エンド・ステーションを除去します。
Disable	SDLC リンク・ステーションの 1 つへの接続を防止します。
Enable	SDLC リンク・ステーションの 1 つへの接続を可能にします。
List	SDLC リンク・ステーションまたは回線について構成済みの情報を表示します。
Set	特定のインターフェースおよびリンク・ステーション情報を構成します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Add

add コマンドは、エンド・ステーションを追加するのに使用します。ルーターは、デフォルトでは、1 次エンド・ステーションです。このコマンドを使用しないで、DLSw または APPN で SDLC ステーションを構成した場合、そのエンド・ステーションが追加されます。ソフトウェアは、以下のようなデフォルト値をステーションに割り当てます。

- Maximum BTU は、インターフェースによって許容される最大値
- Tx および Rx ウィンドウは、MOD 8 の場合は 7、MOD 128 の場合は 127

デフォルト値で十分な場合は、SDLC ステーションを追加する必要はありません。

構文:

```
add station
```

例:

```
add station
Enter station address (in hex) [C4]?
Enter station name [SDLC_C4]?
Include station in router as secondary group poll list (Yes or [No]):
Enter router as primary group poll address (0 means disable) [00]?
Enter max packet size [2048]?
Enter "A" for 2-WAY-ALTERNATING or "S" for 2-WAY-SIMULTANEOUS [S]?
Enter router as secondary link station poll pause [0]?
Enter receive window [7]?
Enter transmit window [7]?
```

Enter station address

01 ~ FE の範囲のステーションの SDLC アドレス

Enter station name

SDLC ステーションの名前指定 (最大 8 文字)

Include station in router as secondary group poll list

このインターフェースに関する 2 次グループ・ポーリング・リストに、このステーションを含めるかどうかを選択します。SDLC ソフトウェアは、SDLC 2 次ステーションの IBM 3174 グループ・ポーリング機能をサポートします。このパラメーターを有効にするためには、**set link group-poll** コマンドを使用して、グループ・ポーリング・アドレスを追加する必要があります。

Enter router as primary group poll address (0 は disable を意味します)

ポーリングされるグループ・アドレスを指定します。ステーションごとに 1 次グループ・ポーリング・アドレスが入力されます。

有効値: X'00' to X'FE'、ここで 0 はグループ・ポーリングを使用しないことを示します。

デフォルト値: X'00'

Enter max packet size

リモート・リンク・ステーションとの間で送受信できる最大パケット・サイズ。この値は、リンクに指定された最大値より大きくすることはできません。この値は **set link frame-size** コマンドを使用して構成します。

SDLC インターフェースの構成

Enter "A" for 2-WAY-ALTERNATING or "S" for 2-WAY-SIMULTANEOUS

リンク・ステーションが両方向同時モードまたは両方向交替モードのどちらで動作しているかを指定します。デフォルトは、インターフェース構成から継承されます。

Enter router as secondary link station poll pause

2 次ステーションが、ポーリングされた後ポーリング・ファイナルの送信を遅らせる時間の量を指定します。

注:

1. この値は、1 次ステーションのポーリング・タイムアウトより少ない必要があります。
2. マルチポイント・リンクで 0 以外の値を使用すると、応答時間が遅くなる場合があります。

有効値: 0.1 秒の増分で 0 ~ 25.5 秒

デフォルト値: 0

Enter receive window

ルーターが、確認応答を送信せずに受信することができるパケットの最大数

注: ウィンドウ・サイズを超えるとルーターはステーションを切断するので、受信ウィンドウ・サイズが十分に大きいことを確認してください。

receive window を構成されたモジュールの最大値に設定します。**receive window** サイズを綿密に監視する理由があるので、これは、使用されているモジュールの最大値に設定する必要があります。

Enter transmit window

ルーターが確認応答を受信せずに送信することができるパケットの最大数

Delete

delete コマンドは、指定されたエンド・ステーション (ステーション名またはアドレス) を SDLC 構成から除去するのに使用します。ルーターは 1 次エンド・ステーション (デフォルト) と見なされます。

構文:

delete *station name or address*

Disable

disable コマンドは、SDLC リンク・ステーションとの接続が作成されるのを防止します。

構文:

disable *link*
station . . .

link インターフェース上のすべての構成済み SDLC リンクへのデータの送受信を防止します。

station name or address

指定されたエンド・ステーション (ステーション名またはアドレス) へのデータの送受信を防止します。

Enable

enable コマンドは、リモート SDLC リンク・ステーションへの接続を可能にします。

構文:

```
enable                link
                        station
```

link ルーター内のサブシステム (たとえば、DLSw) が SDLC のファシリティを使用できるようにします。

station name or address

指定された 2 次リモート・エンド・ステーション (リンク・ステーション名) に接続できます。

List

list コマンドは、1 つまたはすべての SDLC リンク・ステーションの構成情報を表示するのに使用します。

構文:

```
list                  link
                        station name or all
```

link SDLC インターフェースの構成を表示します。

例:

```
list link
Link configuration for: LNK00001 (ENABLED)

Role:          PRIMARY          Type:          POINT-TO-POINT
Modulo:        8                 Frame Size:    2048
Sc Gp Poll:    00                Dflt protcl:  ALTERNATE

Timers:        XID/TEST response: 2.0 sec
                SNRM response:    2.0 sec
                Poll response:     2.0 sec
                Inter-poll delay:  0.0
                Primary poll pause: 0.5 sec
                Dflt sec poll pause: DISABLED
                RTS hold delay:     DISABLED
                Inactivity timeout: 30.0 sec

Counters:      XID/TEST retry:    8
                SNRM retry:        6
                Poll retry:        10
SDLC 1 Config>
```

Link configuration

ルーターの構成に存在する SDLC リンクの名前と状態

Role **set link role** コマンドを使用して構成するリンク・ステーションの役割 (1 次、2 次、または交渉可能)

SDLC インターフェースの構成

Type リンクのタイプ (マルチポイントまたはポイント・ポイント)。 **role (役割)** が 2 次 の場合、このパラメーターに マルチポイント の値を指定すると、伝送していないときに、RTS が下げられます。

Duplex

回線のハードウェア機能を指定します。両方向同時リンク・マネージメントの場合、全二重 ハードウェア機能が必要とされます。

Modulo

リンクで使用するシーケンス番号の範囲。MOD 8 (0 ~ 7) または MOD 128 (0 ~ 127)。

Idle state

インターフェースがデータを送信していないとき、回線上を送信されるビット・パターン (FLAG または MARK)

Speed インターフェースの物理データ速度。クロックが内部の場合、これは内部クロックによって生成されるデータ速度です。外部クロック回線の場合、このパラメーターは影響を与えません。

Group Poll

グループ・ポーリング・フィーチャーに使用されるアドレス。グループ組み込みが *yes* として構成されている 2 次ステーションは、このアドレスから受信した非番号制ポーリングに応答します。このリンクの 2 次ステーションに対してグループ・ポーリング・フィーチャーを有効にするためには、このアドレスを非ゼロにする必要があります。各 2 次ステーションは、グループ・アドレスに加えて、特定のステーション・アドレスも持ちます。

Cable 使用するケーブルのタイプを指定します (RS-232、V.35、V.36、または X.21)。

Encoding

SDLC 伝送符号化法を NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) として構成します。

Clocking

インターフェースのクロック (外部または内部)

Frame Size

インターフェースを介して送信できる最大フレーム・サイズ

Timers:

以下にリストするタイマーはすべて 100ms の分解能です。

XID/TEST resp.

XID または TEST フレームを再送する前に、XID または TEST 応答メッセージを待つ最大時間。0 の値は、ルーターがその次のポーリング・リストの番を過ぎて再試行を遅らせないことを意味します。

SNRM response

ステーションが SNRM(E) を再送する前に、UA 応答メッセージを待つ最大時間

Poll response

再試行の前に、ポーリング・ステーションからのレスポンスを待つ最大時間

Inter-poll delay

ルーター (1 次の役割をもつ) がレスポンスを受信した後、次のステーションをポーリングする前に待つ時間

注: Primary Poll Pause は優先されるポーリング・タイマーです。Inter-Poll Delay により、エンド・ユーザー応答時間の問題が生じます。1 次ポーリング休止の詳細については、636 ページを参照してください。

Interframe delay

フレーム間でフラグを差しはさむ時間の量を指定します。9600 ボーの回線について、最大値 120 はフレーム間で約 15 のフラグを差しはさみます。

Leading Flags

インターフェースの遅延が、このリンクの反対側の装置に回答するのに十分な場合に送信されるフラグの数。これは、最大値 100 をもつ時間単位です。

Inactivity timeout

アイドル NRM/E 2 次ステーションの場合、インターフェースがステーションを回復状態に変更する前に経過する時間を設定します。0 (ゼロ) に設定すると、ステーションは無期限にアイドル状態のままになります。

Counters:**XID/TEST retry**

タイムアウト前に、応答の受信なしにルーターが XID または TEST フレームを送信する最大回数。値 0 は、ルーターが無期限に再試行することを示します。

SNRM タイムアウトの前に、ルーターがレスポンスを受信せずに SNRM(E) フレームを送信する最大回数。値 0 は、ルーターが無期限に再試行することを示します。

Poll retry

タイムアウトの前に、ルーターがレスポンスを受信せずにステーションをポーリングする最大回数。値 0 は、ルーターは無期限に再試行を継続することを示します。

注: **duplex type**、**speed**、**cable type**、**encoding**、**clocking**、**leading flags**、および **inter-frame delay** といった物理レイヤー・パラメーターは SDLC ダイアル回線インターフェースには適用されず、**list link** コマンドによって表示されません。

station all or address or link station name

指定された SDLC リンク・ステーションまたはすべてのリンク・ステーションの情報を表示します。

例:

```
list station c1
Addr-A/S      Name      Status    Max BTU  Rx  Tx  Secondary  Primary
(Sec Gp)                               Window Window Poll Pause GP Addr
-----
C1      A SDLC_C1  ENABLED   2048     7   7     0.0 sec   00
```

例:

SDLC インターフェースの構成

```
list station all
Addr-A/S      Name      Status      Max BTU      Rx      Tx      Secondary      Primary
(Sec Gp)                               Window      Window      Poll Pause     GP Addr
-----
C1  A SDLC_C1  ENABLED      2048         7        7        0.0 sec       00
C2  A SDLC_C2  ENABLED      2048         1        7        0.0 sec       00
```

Address

SDLC リンク・ステーションのアドレス。括弧内のアドレスは、インターフェースの "2 次としてのルーター" のグループ・アドレスで、ステーションがグループ包含を設定してあり、リンクが 2 次で、2 次グループ・アドレスが非ゼロである場合にステーションによって使用されます。

Name SDLC リンク・ステーションの文字列での名前指定

Status

SDLC リンク・ステーションの状況 (ENABLED または DISABLED)

Max BTU

ステーションのフレーム・サイズ限界。このフレーム・サイズは、**set link frame-size** コマンドで構成された最大基本伝送単位 (BTU) パケット・サイズより大きくてはなりません。

Rx Window

受信ウィンドウのサイズ

Tx Window

送信ウィンドウのサイズ

Set

set コマンドは、1 つまたはすべての SDLC リンク・ステーションの特定情報を構成するのに使用します。

構文:

```
set link
      cable*
      clocking*
      duplex* . . .
      encoding* . . .
      frame-size
      group poll* ...
      idle* . . .
      inactivity ...
      inter-frame delay*
      leading flags*
      modulo . . .
      name
      poll . . .
```

```

role* . . .
snrm
speed*
type* . . .
xid/test
station
address. . .
group-inclusion
gp-address-prim
max-packet
name
protocol
receive-window
secondary-phase
transmit-window

```

*注: これらのコマンドは SDLC ダイヤル回線インターフェースでは利用不能です。

link cable *type*

このインターフェースに接続されるケーブルを設定します。 オプションとしては、次の DCE および DTE タイプがあります。 V.36、RS-232、V.35、および X.21。

表82 は、各種アダプター上で構成できるケーブル・タイプをリストしています。

表 82. 2210 インターフェースのケーブル・タイプ

アダプター・タイプ	ケーブル・タイプ
8 ポート EIA 232	RS-232 DTE および RS-232 DCE
6 ポート V.35/V36	V.35 DCE、V.35 DTE、V.36 DCE、または V.36 DTE
8 ポート X.21	X.21 DCE および X.21 DTE

DTE ケーブルは、ルーターをあるタイプの DCE 装置 (たとえば、モデムまたは DSU/CSU) に接続するときに使用します。

DCE ケーブルは、ルーターが DCE として動作し、直接接続のためのクロックを提供するときに使用します。

link clocking *internal or external*

モデムまたは DSU に接続するには、外部クロックを構成し、**set link cable** コマンドを使って該当する DTE ケーブルを選択します。

別の DTE 装置に直接接続するには、内部クロックを構成し、**set link cable** コマンドを使って該当する DCE ケーブルを選択し、**set link speed** コマンドを使ってクロック/回線速度を構成します。

デフォルト値: external

SDLC インターフェースの構成

link duplex full or half

SDLC 回線を全二重 (*full-duplex*) または半二重 (*half-duplex*) 信号用に構成します。半二重は、2210 がデータを転送する前に、RTS を上げて CTS を待つことを意味します。全二重は、2210 がデータを転送する前に CTS が上がるのを待たないことを意味します。

注: 二重タイプは、SDLC が SDLC プロトコル・レベルでどのように動作するか (両方向同時または両方向交替) は制御しません。

link encoding nrz または nrzi

SDLC 伝送符号化法を NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) として構成します。NRZ がデフォルトです。

link frame-size

データ・リンク上で送受信できるフレームの最大サイズを構成します。有効な入力値を表83 に示します。

表 83. Link Frame-Size コマンドのフレーム・サイズの有効値

最小	最大	デフォルト
128	8187	2048

リンク・フレーム・サイズは、**set station xxx max packet** コマンドを使用して構成した最大パケット・サイズ以上に設定してください。そうでないと、ルーターは自動的に最大パケット・サイズをリンク・フレーム・サイズとして設定し直し、次のような ELS メッセージを出します。

```
SDLC.054: nt 3 SDLC/0 Stn xx-MaxBTU too large for Link adjusted (4096->2048)
```

例: **set link frame-size**

```
Frame size in bytes (128 - 8187)[2048]?
```

link group-poll

リンク上の 2 次ステーションとしてのグループ・ポーリング・アドレスを設定します。SDLC ソフトウェアは、IBM 3174 グループ・ポーリング機能をサポートします。ステーションをグループ・ポーリング・リストに含めるには、**add station** または **set station group inclusion** コマンドを使用します。

例:

```
set link group-poll
Enter group poll address router as secondary (in hex) [00:]?f3
Group poll support enabled
```

link idle flag

SDLC フレーム転送の送信アイドル状態を構成します。デフォルト設定はフラグ・オプションで、これはフレーム相互間に連続フラグ (7E) を提供します。

例: **set link idle flag**

リンクはフラグ・アイドルを透過的に受け取ります。

link idle mark

SDLC フレーム転送の送信アイドル状態を構成します。マーク・オプションは、フレーム間の伝送路をマーキング状態 (OFF, 1) にします。

link inactivity #-of-seconds

アイドル NRM/E 2 次ステーションの場合、インターフェースがステーショ

SDLC インターフェースの構成

ンを回復状態に変更する前に経過する時間を設定します。範囲は 0 ~ 7200 秒です。デフォルト値は 30 です。0 (ゼロ) に設定すると、ステーションは無期限にアイドル状態のままになります。

例:

```
set link inactivity
Enter secondary link station inactivity timeout :[30.0]?
```

link inter-frame delay

転送されるパケット間に遅延を挿入することができます。このコマンドは、フレーム相互間の最小遅延を保証することにより、相手側の旧型で低速のシリアル装置に整合させます。このパラメーターは、フレーム間の時間の長さです。

有効値: 0 ~ 120

デフォルト値: 0

例:

```
set link inter-frame
Transmit Delay Counter [0]?
```

link leading flags

先行フラグの数を設定します。このコマンドを使用するのは、フレーム間の遅延が十分でないために 2210 から別の装置に応答を送ることができない場合です。モデムが CTS モデム信号を出してもすぐにパケットを受信することができない半二重モデムを使用している場合にも、このコマンドを使用して先行フラグ遅延を設定する必要があります。

有効値: 0 ~ 100

デフォルト値: 0

例:

```
set link leading flags
Leading flags delay [0]?
```

link modulo 8 or 128

リンクで使用するシーケンス番号範囲 (MOD 8 (0-7) または MOD 128 (0 - 127)) を指定します。デフォルトは MOD 8 です。

注: この値を変更すると、ウィンドウ・サイズが無効になります。**set station** コマンドを使用して、受信ウィンドウおよび送信ウィンドウのサイズを変更してください。有効なウィンドウ・サイズは 0 ~ 7 です。

また、**link modulo** が 128 の場合、接続の起動時に SNRM ではなく SNRME が使用され、監視フレーム・ヘッダーは追加バイト分だけ拡張されます。

link name

構成するリンクの文字ストリングを設定します。このパラメーターは情報としてのみ使用されます。

例:

```
set link name
Enter link name: [LINK_0]?
```

link poll delay

インターフェースを介して送信される各ポーリング間の時間遅延を設定しま

SDLC インターフェースの構成

す。**link poll delay** より **link poll ppause** が優先されます。**link poll delay** は各ポーリングの間に遅延を入れるので、リンクがあまり使用されていない場合でも、応答時間の問題が生じます。**link poll ppause** が > 0 に設定されている場合には、**link poll delay** を 0 に設定する必要があります。

例:

```
set link poll delay
Enter delay between polls [0]?
```

t 5 コマンド **set link poll ppause** を使用しても **primary poll pause** を設定することができます。

link poll ppause

1 次ポーリング休止を設定します。

このパラメーターは、ポーリング・サイクルをリスタートするための最小時間を決定します。たとえば、分岐リンク上に 5 つのステーションがあり、5 つのステーションがすべて 0.2 秒内にポーリングされ、PPAUSE が 0.5 秒に設定されている場合、最初のステーションのポーリングは、さらに 0.3 秒待ちます。いくつかのステーションからデータが受信されたとしたら、5 つのステーションすべてのポーリングを完了する時間は 0.5 秒より長くかかるかもしれませんが、最初のステーションのポーリングが遅れることはないかもしれません。

例:

```
set link poll ppause
Enter delay between polls [0.5]?
```

link poll retry

コネクションをクローズする前に、インターフェースが 2 次 SDLC リンク・ステーションのポーリングを再試行する回数を設定します。

例:

```
set link poll retry
Enter poll retry count (0 = forever) [10]?
```

link poll timeout

タイムアウトになる前に、インターフェースがポーリング・レスポンスを待つ時間を設定します。

例:

```
set link poll timeout
Enter poll timeout [2.0]?
```

link role *primary or secondary or negotiable*

インターフェースを SDLC 1 次、2 次、または交渉可能リンク・ステーションとして構成します (デフォルトは 1 次)。

注:

1. DLSw の場合、**negotiable** は初期ポーリングに X'FF' (同報通信アドレス) を使用します。

役割を交渉するのに同報通信アドレスを使用する場合、リンクは初期にデフォルト SDLC 構成を使用して、特定のアドレスが一致する場合、構成済みのステーションになります。

primary がリンクの役割のときは、リンクは特定アドレスに対して初期ポーリングを行います。

SDLC インターフェースの構成

2. APPN ポイント・ポイントまたは交渉可能の場合、初期ポーリングには同報通信アドレスが使用されます。1 次多地点の場合は、特定のアドレスが使用されます。
3. 交換 SDLC の場合は、装置は 1 次でなければならないので、**link role type** は SDLC ダイアル回線インターフェースに対しては構成できません。

link snrm timeout or retry

1 次ステーションに関する以下の SNRM(E) 情報を構成します。

timeout

SNRM(E) を再送する前に、非番号制確認 (UA) レスポンスを待つ時間

retry あきらめる前に、レスポンスを受信せずに SNRM (E) 再送する回数

例:

```
set link snrm timeout
Enter SNRM response timeout [2.0]?
```

例:

```
set link snrm retry
Enter SNRM retry count (0=forever) [6]?
```

link speed

内部クロックの場合は、このコマンドを使用して送信および受信クロック回線の速度を指定します。

外部クロックの場合は、このコマンドは WAN/シリアル・ラインの動作に影響を与えません。

有効値:

内部クロック: 表84 を参照してください。

外部クロック: 表85 を参照してください。

表 84. 2210 インターフェースに内部クロックが使用されるときの回線速度

アダプター・タイプ	速度範囲
8 ポート EIA 232	9600 ~ 64 000 bps
6 ポート V.35/V.36	9600 ~ 460 800 bps、1 544 000 bps、または 2 048 000 bps
8 ポート X.21	9600 ~ 460 800 bps、1 544 000 bps、または 2 048 000 bps

表 85. 2210 インターフェースに外部クロックを使用するときの回線速度

アダプター・タイプ	速度範囲
8 ポート EIA 232	2400 ~ 64 000 bps
6 ポート V.35/V.36	2400 ~ 2 048 000 bps
8 ポート X.21	2400 ~ 2 048 000 bps

例:

```
set link speed
Line Speed [64000]?
```

SDLC インターフェースの構成

link type *multipoint or point-to-point*

SDLC リンクをマルチポイント・リンクまたはポイント・ポイント・リンクとして構成します。ルーターが 2 次である場合、このパラメーターは RTS が制御されるかどうかを決定します。

注: 交換 SDLC の場合、リンクは常にポイント・ポイントなので、**link type** は SDLC ダイアル回線インターフェースに対しては構成できません。

link xid/test *timeout or retry*

1 次ステーションの以下の XID/test 情報を構成します。

timeout

XID または TEST フレームの再送する前に、XID または TEST フレーム応答を待つ最大時間

retry あきらめる前に、XID または TEST フレームを再送する最大回数。0 (ゼロ) に設定すると、ルーターは無期限に再試行します。

remote-secondary *address or link_station_name address <argument>*

リモート・ステーションの SDLC アドレス (02 ~ FE の範囲) を変更します。

例: **set remote-secondary SDLC_C1 address ce**

station *address or name address*

ステーションの SDLC アドレス (01 ~ FE の範囲) を変更します。

例:

```
set station c1 address
Enter station address (in hex) [C1]?
```

station *address or link_station_name group-inclusion no or yes*

SDLC 2 次ステーションの場合、このステーションをこのリンクのグループ・ポーリング・リストに含めるかどうかを設定します。これを有効にするには、**set link group-poll** コマンドを使用して、2 次グループ・ポーリング・アドレスを追加します。

例: **set station c1 group-inclusion yes**

station *gr-address-prim*

ルーターをポーリングされる 1 次グループ・アドレスとして指定します。特定のアドレスをグループ・アドレスとして使用することもできません。

有効値: X'00' ~ X'FE'、ここで X'00' はグループ・ポーリングを使用しないことを意味します。

デフォルト値: X'00'

station *address or name max-packet*

ステーションが受信できるパケットの最大サイズ (デフォルトは 2048)。最大パケット・サイズは、**set link frame-size** コマンドで構成したリンク・フレーム・サイズより大きく設定しないでください。そのように設定すると、ルーターは自動的に最大パケット・サイズをリンク・フレーム・サイズとして設定し直し、次のような ELS メッセージを出します。

```
SDLC.054: nt 3 SDLC/0 Stn xx-MaxBTU too large for Link adjusted (4096->2048)
```

例:


```
set station c1 max-packet
Enter max packet size [2048]?
```

station address or name name

SDLC ステーションの名前

例:

```
set station c1 name
Enter station name [SDLC_C1]?
```

station protocol

ステーションが両方向交替 (TWA) または両方向同時 (TWS) のどちらとして動作するか定義します。

注: TWS は全二重ハードウェアを必要とします。

station address or name receive window

ルーターがレスポンスを送信する前に受信できるフレームの最大数。範囲は 1 ~ 7 で、デフォルトは 7 です。

例:

```
set station c1 receive-window
Enter receive window [7]?
```

注: ウィンドウ・サイズを超えるとルーターはステーションを切断するので、受信ウィンドウ・サイズが十分に大きいことを確認してください。

receive window を構成されたモジュールの最大値に設定します。

station secondary-pause

2 次ステーションが、ポーリングされた後ポーリング・ファイナルの送信を遅らせる時間の長さを指定します。

注:

1. この値は、1 次ステーションのポーリング・タイムアウトより少ない必要があります。
2. マルチポイント・リンクで 0 より大きい値を使用すると、応答時間が遅くなる場合があります。

有効値: 0.1 秒の増分で 0 ~ 25.5 秒。0 より大きい値は、同時に両方向に送信できるので、TWS ポイント・ポイント・リンクで最も有用です。

デフォルト値: 0

station address or name transmit-window

ルーターがレスポンス・フレームを受信する前に送信できるフレームの最大数。MOD 8 の範囲は 1 ~ 7 です。MOD 128 の範囲は 8 ~ 127 です。

例:

```
set station c1 transmit-window
Enter transmit window [7]?
```

SDLC 監視環境へのアクセス

監視環境は GWCON プロセスです。GWCON プロセスに入るには、次のようにします。

SDLC インターフェースの監視

1. OPCON (*) プロンプトで **talk 5** (または **t 5**) を入力する。これにより、次の例のような GWCON (+) プロンプトが表示されます。

```
MOS Operator Console
For help using the Command Line Interface, press ESCAPE, then '?'
* talk 5
+
```

2. 次に、**network #** コマンドを入力して、以前に SDLC 装置に構成したインターフェースを識別する番号を指定する。

```
+ network 2
SDLC Console
SDLC-2>
```

GWCON (監視) コマンドはすべて + プロンプトで入力します。

監視環境に関する情報は、3ページの『第1章 開始』を参照してください。

SDLC 監視コマンド

この節では、SDLC コンソールおよび関連のコマンドの要約を示し、個々のコマンドについて説明します。これらのコマンドは、データベースから情報を収集するのに使用します。表86 は、SDLC 監視コマンドとその機能をリストしています。

表 86. SDLC 監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Add	SDLC リンク・ステーションを追加します。
Clear	SDLC インターフェースに関するカウンターをクリアします。
Delete	SDLC リンク・ステーションを動的に除去します。
Disable	1 つの SDLC リンク・ステーションへの接続を使用不可にします。
Enable	1 つの SDLC リンク・ステーションへの接続を使用可能にします。
List	SDLC リンク・ステーションの構成およびリンク・ステーション情報を表示します。
Msgsz	他の方法では見ることができないデータ内のバイトを監視することができます。SDLC ELS メッセージ 50 ~ 53 について 12 ~ 50 バイトが表示されます。
Set	特定のインターフェースおよびリンク・ステーション情報を構成します。
Test	ルーターと SDLC リンク・ステーション間のリンクをテストします。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Add

add コマンドは、エンド・ステーションを追加するのに使用します。ルーターは、デフォルトでは、1 次エンド・ステーションです。このコマンドを使用しないで、DLSw または APPN で SDLC ステーションを構成した場合、そのエンド・ステーションが追加されます。

構文:

add station

add コマンドの例および詳しい情報は、627ページの『Add』を参照してください。

Clear

clear コマンドは、インターフェース、1つのステーション、またはすべてのステーションのカウンターをクリアするのに使用します。ステーションをリストしたい場合は、**list all stations** コマンドを使用します。

構文: **clear** link
station ...

link *name or address*

SDLC インターフェースのカウンターをクリアします。

station *name or address or all*

特定のステーションまたはすべてのステーションのカウンターをクリアします。

Delete

delete コマンドは、SRAM 内の SDLC 構成に影響を与えずに、既存の SDLC コネクションを終了するのに使用します。このコマンドは、リンク・ステーションで進行中のすべての SDLC セッションを終了させます。ルーターは、デフォルトでは、1 次エンド・ステーションと見なされます。

構文:

delete station name or address

Disable

disable コマンドは、SRAM 内の SDLC 構成に影響を与えずに、1つまたはすべての SDLC リンク・ステーション上のコネクション確立を使用不可にするのに使用します。**disable** コマンドは、そのステーションへの既存のすべてのコネクションも終了します。

構文: **disable** link
station . . .

link すべてのコネクションを終了して、インターフェースに構成されているすべての SDLC リンク・ステーションの接続を防止します。

station *name or address*

既存のコネクションを終了して、指定されたエンド・ステーション (リンク・ステーション名) への接続を防止します。

Enable

enable コマンドは、SDLC 構成 SRAM に影響を与えずに、リモート SDLC リンク・ステーションと接続を確立できるようにするのに使用します。

SDLC インターフェースの監視

構文:

```
enable                link  
                        station . . .
```

link サブシステム (たとえば、DLSw) が SDLC のファシリティを使用できるようにします。

```
station name or address  
指定されたエンド・ステーションへの接続を可能にします。
```

List

list コマンドは、データ・リンク・レイヤーおよびインターフェースに特有の統計を表示するのに使用します。

構文:

```
list                  link configuration  
                      link counters  
                      station . . .
```

link configuration

インターフェース上のすべての構成済み SDLC リンク・ステーションの情報を表示します。

list コマンドの例および詳しい情報は、629ページの『List』を参照してください。

link counters 前回のルーターのリスタートまたは前回の clear counters 以降の SDLC カウンターの情報を表示します。

I-Frames

送受信された情報フレームの合計数

I-Bytes

送受信された情報バイトの合計数

Re-Xmit

再送されたフレームの合計数

UI-Frames

送受信された非番号制情報フレームの合計数

UI-Bytes

送受信された非番号制情報バイトの合計数

RR 送受信された受信可 (RR) の合計数

RNR 送受信された受信不可 (RNR) の合計数

REJ 送受信されたリジェクトの合計数

UP 送受信された非番号制ポーリング数 (グループ・ポーリング)

```
station all or address or link station name
```

指定された SDLC リンク・ステーションまたはすべてのステーションの状態を表示します。ソフトウェアは、**add station** コマンドを使

SDLC インターフェースの監視

用して明示的に構成されていないが、プロトコル・レイヤー (DLSw または APPN) で定義されて起動されたために構成に追加されたステーションの横に * を表示します。

インターフェース上の指定された SDLC リンク・ステーション (リンク・ステーション名) の情報を表示します。

Address

SDLC リンク・ステーションのアドレス。括弧内のアドレスは、そのステーションのグループ・アドレスです。(00) は、グループ・アドレスが定義されていないことを示します。

Name SDLC リンク・ステーションの文字列での名前指定

Status

SDLC リンク・ステーションの状態

Enabled

使用可能であるが、割り当てられていない。

Idle

割り当てられているが、使用されていない。

Connected

接続状態

Disconnected

切断状態

Connecting

接続確立中

Discnectng

切断中

Recovering

一時データ・リンク誤りからの回復を試行中

Max BTU

リモート・ステーションのフレーム・サイズ限界。このフレーム・サイズは、**set link frame-size** コマンドで構成された最大基本伝送単位 (BTU) パケット・サイズより大きくてはなりません。デフォルト値は 2048 バイトです。

Rx Window

受信ウィンドウのサイズ

Tx Window

送信ウィンドウのサイズ

station name or address counters

指定されたリンク・ステーションのフレーム送信および受信カウンタを表示します。

I-Frames

送受信された情報フレームの数

I-Bytes

送受信された情報バイトの数

SDLC インターフェースの監視

Re-Xmit

再送されたフレームの数

UI-Frames

送受信された非番号制情報フレームの数

UI-Bytes

送受信された非番号制情報バイトの数

XID-Frames

送受信された識別交換フレームの数

RR 送受信された受信可フレームの数

RNR 送受信された受信不可フレームの数

REJ 送受信されたリジェクトの数

TEST 送受信されたテスト・フレームの数

SNRM 送受信された通常応答モード設定フレームの数

DISC 送受信された切断フレームの数

UA 送受信された非番号制確認フレームの数

DM 送受信された切断モード・フレームの数

FRMR 送受信されたフレーム・リジェクト・フレームの数

UP 送受信された非番号制ポーリング数 (グループ・ポーリング)

例:

```
SDLC-2> list link counters
      I-Frames  I-Bytes  Re-Xmit  UI-Frames  UI-Bytes
-----
Send   0          0         0         0          0
Recv   0          0         0         0          0

      RR      RNR      REJ      UP
-----
Send   0          0         0         0
Recv   0          0         0         0
```

```
SDLC-2> list station c1
Addr-A/S  Name  Status  Max BTU  Rx Window  Tx Window  Secondary Poll Pause  Primary GP Addr
-----
C1  A SDLC_C1  ENABLED  2048    7          7          0.0 sec  00
```

例:

```
SDLC-2> list station all
Addr-A/S  Name  Status  Max BTU  Rx Window  Tx Window  Secondary Poll Pause  Primary GP Addr
-----
C1  A SDLC_C1  ENABLED  2048    7          7          0.0 sec  00
C2  A SDLC_C2  ENABLED  2048    1          7          0.0 sec  00
```

例:

```
SDLC-2> list station c1 counters
      I-Frames  I-Bytes  Re-Xmit  UI-Frames  UI-Bytes  XID-Frames
-----
Send   9          384         0         0          0          6
Recv  29         42792        0         0          0          3

      RR      RNR      REJ      TEST      SNRM      DISC
-----
Send   598         0         0         0          1          0
```

Recv	587	0	0	0	0	0
	UA	DM	FRMR	UP		
Send	0	0	0	0	0	
Recv	1	0	0	0	0	

Msgsz

msgsz コマンドは、SDLC ELS メッセージ 50 ~ 53 の 12 ~ 50 バイトを表示するのに使用します。

構文:

msgsz

Enter between 12 and 50 bytes

表示するバイトの数を指定します。デフォルトは 12 バイトです。

Set

set コマンドは、SRAM 内の SDLC 構成に影響を与えずに、1 つまたはすべての SRAM リンク・ステーションの特定情報を動的に構成するのに使用します。SDLC 監視環境では、**set** コマンドは、使用不可にされたリンクまたはステーション上でしか実行できません。タイム値はすべて 0.1 秒の分解能で、秒数で入力します。

構文:

```

set link
    group poll* ...
    inactivity ...
    modulo . . .
    name
    poll . . .
    protocol . . .
    role* . . .
    secondary-pause . . .
    snrm
    type* . . .
    xid/test
station
    address. . .
    group-inclusion
    gp-address-prim
    max-packet
    name

```

SDLC インターフェースの監視

protocol

receive-window

secondary-pause

transmit-window

*注: これらのコマンドは SDLC ダイアル回線インターフェースではサポートされません。

link group-poll address

リンク上の 2 次ステーションのグループ・ポーリング・アドレスを設定します。SDLC ソフトウェアは、IBM 3174 グループ・ポーリング機能をサポートします。ステーションをグループ・ポーリング・リストに含めるには、**add station** または **set station group inclusion** コマンドを使用します。

例:

```
set link group-poll
Enter group poll address (in hex) [00:]?f3
Group poll support enabled
```

link inactivity

アイドル NRM/E 2 次ステーションの場合、インターフェースがステーションを回復状態に変更する前に経過する時間を設定します。範囲は 0 ~ 7200 秒です。デフォルト値は 30 です。0 (ゼロ) に設定すると、ステーションは無期限にアイドル状態のままになります。

例:

```
set link inactivity
Enter secondary link station inactivity timeout :[30.0]?
```

link modulo

SRAM 構成に影響を与えずに、データ・リンクで使用されるシーケンス番号の範囲を動的に変更します。モジュロ 8 はシーケンス番号範囲 0 ~ 7 を指定し、モジュロ 128 は 0 ~ 127 を指定します。デフォルトは 8 です。

注: この値を変更すると、送信および受信ウィンドウ・サイズが無効になります。**set station** コマンドを使用して、受信ウィンドウおよび送信ウィンドウのサイズを変更してください。

link name

SRAM 構成に影響を与えずに、リンクの名前を動的に変更します。最大 8 文字を入力できます。このパラメーターは情報としてのみ使用されます。

例:

```
set link name
Enter link name: [LINK_0]?
```

link poll delay or timeout or retry

SRAM 構成に影響を与えずに、以下のポーリング情報を動的に変更します。

delay インターフェースを介して送信される各ポーリング間の遅延を構成します。

timeout

タイムアウトになる前に、インターフェースがポーリング・レスポンスを待つ時間を構成します。

retry コネクションをクローズする前に、インターフェースがリモート SDLC リンク・ステーションのポーリングを再試行する回数を構成します。

例:

```
set link poll delay
Enter delay between polls [0.2]?
```

link protocol

ステーションが TWA または TWS のどちらとして動作するか定義します。

注: TWS は全二重ハードウェアを必要とします。

link role *primary, secondary, or negotiable*

インターフェースを SDLC 1 次、2 次、または交渉可能リンク・ステーションとして構成します。デフォルトは 1 次です。このコマンドの使用は SRAM 構成には影響を与えません。

注:

1. DLSw の場合、**negotiable** は初期ポーリングに X'FF' (同報通信アドレス) を使用します。
役割を交渉するのに同報通信アドレスを使用する場合、リンクはデフォルトの SDLC 構成を使用します。
primary がリンクの役割のときは、リンクは特定アドレスに対して初期ポーリングを行います。
2. APPN ポイント・ポイントまたは交渉可能の場合、初期ポーリングには同報通信アドレスが使用されます。1 次マルチポイントの場合は、特定のアドレスが使用されます。
3. 交換 SDLC の場合は、装置は 1 次でなければならないので、**link role type** は SDLC ダイアル回線インターフェースに対しては構成できません。

link secondary-pause

2 次ステーションが、ポーリングされた後ポーリング・ファイナルの送信を遅らせる時間の長さを指定します。

注:

1. この値は、1 次ステーションのポーリング・タイムアウトより少ない必要があります。
2. マルチポイント・リンクで 0 より大きい値を使用すると、応答時間が遅くなる場合があります。

有効値: 0.1 秒の増分で 0 ~ 25.5 秒。値 > 0 は、同時に両方向に送信できるので、TWS ポイント・ポイント・リンクで最も有用です。

デフォルト値: 0

link snrm *timeout or retry*

1 次ステーションの場合、SRAM 構成に影響を与えずに、以下の SNRM(E) 情報を動的に変更します。

SDLC インターフェースの監視

timeout

SNRM(E) を再送する前に、非番号制確認 (UA) レスポンスを待つ時間

retry あきらめる前に、レスポンスを受信せずに SNRM (E) 再送する回数

例:

```
set link snrm timeout
Enter SNRM response timeout [2.0]?
```

link type multipoint or point-to-point

SRAM 構成に影響を与えずに、SDLC リンクをマルチポイント・リンクまたはポイント・ポイント・リンクに動的に変更します。

注: 交換 SDLC の場合、リンクは常にポイント・ポイントなので、**link type** は SDLC ダイアル回線インターフェースに対しては構成できません。

link xid/test timeout or retry

1 次ステーションの場合、SRAM 構成に影響を与えずに、以下の XID/テスト情報を動的に変更します。

timeout

テスト・フレームを再送する前に、XID または TEST フレーム・レスポンスを待つ最大時間

retry あきらめる前に、XID または TEST フレームを再送する最大回数。0 (ゼロ) に設定すると、ルーターは無期限に再試行します。

注: 以下のパラメーターの例および説明は、632ページの『Set』の SDLC 構成の章にあります。

station address or name address

ステーションの SDLC アドレスを変更します。

station group-inclusion

SDLC 2 次ステーションの場合、このステーションをこのリンクのグループ・ポーリング・リストに含めるかどうかを設定します。これを有効にするには、**set link group-poll** コマンドを使用して、2 次グループ・ポーリング・アドレスを追加します。

例: **set station c1 group-inclusion yes**

station gp-address-prim

ポーリングされるグループ・アドレスを指定します。特定のアドレスをグループ・アドレスとして使用することもできません。

有効値: X'00' ~ X'FE'、ここで X'00' はグループ・ポーリングを使用しないことを示します。

デフォルト値: X'00'

station address or name max-packet

このステーションが受信できるパケットの最大サイズ

station address or name name

SDLC ステーションの名前

station protocol

ステーションが TWA または TWS のどちらとして動作するか定義します。

注: TWS は全二重ハードウェアを必要とします。

station address or name receive-window

確認応答が要求される前にルーターが受信するフレームの最大数

station secondary poll pause

2 次ステーションが、ポーリングされた後ポーリング・ファイナルの送信を遅らせる時間の長さを指定します。

注:

1. この値は、1 次ステーションのポーリング・タイムアウトより少ない必要があります。
2. マルチポイント・リンクで 0 より大きい値を使用すると、応答時間が遅くなる場合があります。

有効値: 0.1 秒の増分で 0 ~ 25.5 秒。0 より大きい値は、同時に両方向に送信できるので、TWS ポイント・ポイント・リンクで最も有用です。

デフォルト値: 0

station address or name transmit-window

ルーターが、レスポンス・フレームを受信する前に送信するフレームの最大数

Test

指定された数の TEST フレームを指定されたステーションに送信し、レスポンスを待ちます。このコマンドは、接続の整合性をテストするのに使用します。テストを取り消すときは、任意のキーを押します。

注: このコマンドを使用する前に、指定されたリンク・ステーションを使用不可にしてください。

構文:

test *station name or address #frames-to-send frame-size*

例:

```
test station c1
Number of frames to send [1]? 5
Frame length [265]?
Starting echo test -- press any key to abort
5 frames sent, 5 frames received, 0 compare errors, 0 timeouts
```

Number of test frames to send

送信するフレームの合計数

Frame length

送信するフレームの長さ。フレームの長さは、指定されたステーションの最大フレーム長より大きくすることはできません。

任意のキーを押せば、テストを打ち切ることができます。

SDLC インターフェースおよび GWCON インターフェース・コマンド

SDLC インターフェースには動作用のコンソール・プロセスがありますが、GWCON 環境から **interface** コマンドを使用すれば、2210 も導入済みインターフェースの完全な統計を表示します。(**interface** コマンドの詳細については、149ページの『第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』を参照してください。)

SDLC インターフェースで表示される統計

interface コマンドを使用すると、SDLC 監視プロセスに入らずに、SDLC 装置の統計を表示することができます。これを行うには、+ プロンプトで **interface** コマンドとインターフェース番号を入力します。

+ **interface 12**

このコマンドは、次の形式で統計をリストします。

```

                                Self-Test  Self-Test  Maintenance
                                Passed      Failed      Failed
12 12  SDLC/0  Slot: 8  Port: 2      2          1          0
SDLC MAC/data-link on V.35/V.36 interface

Adapter cable:                V.35 DTE

V.24 circuit: 105 106 107 108 109
Nicknames:    RTS CTS DSR DTR DCD
PUB 41450:    CA  CB  CC  CD  CF
State:        ON  ON  ON  ON  ON

Line speed:          64.000 Kbps
Last port reset:    1 hour, 20 minutes, 42 seconds ago

Input frame errors:
CRC error                0  alignment (byte length)          0
missed frame            182  too long (> 2062 bytes)          0
aborted frame           0  DMA/FIFO overrun                0
Output frame counters:
DMA/FIFO underrun errors 0  Output aborts sent              0

```

Nt 初期構成時にソフトウェアによって割り当てられたインターフェース番号を示します。

Nt' 初期構成時にソフトウェアによって割り当てられたインターフェース番号を示します。

注: SDLC インターフェースの場合、Nt' インターフェース番号は、常に Nt インターフェース番号と同じです。

Slot SDLC を実行しているインターフェースのスロット番号を示します。

Port SDLC を実行しているインターフェースのポート番号を示します。

Self-test passed

SDLC インターフェースが自己テストに合格した合計数を示します。

Self-test failed

SDLC インターフェースが自己テストに合格できなかった合計数を示します。

Maintenance failed

保守障害の数の示します。

以下のパラメーターは、ケーブルが接続されている場合にのみ表示されます。表示される情報は、接続されているケーブルによって決まります。他のケーブルでは、異なるパラメーターが表示されます。

Adapter cable

レベル変換器が使用されているアダプター・ケーブルのタイプを示します。

V.24 circuit

V.24 で使用されている回線を示します。

Nicknames

V.24 回線で使用されている信号を示します。

RS-232

EIA 232 (RS 232) 回線名

State V.24 回線、信号、およびピン割り当て (ON または OFF)

Line speed (configured)

SDLC インターフェースに現在構成されている回線速度を示します。

Last port reset

前回にポートがリセットされた時期を示します。

Input frame errors

入力フレーム誤りタイプ (CRC 誤り、短すぎる、強制終了、配列、長すぎる、DMA/FIFO オーバーラン) および発生した誤りの合計数を示します。

Output frame counters

出力フレームの DMA/FIFO オーバーランおよび送信された出力強制終了の合計数を示します。

Missed frame

フレームが装置に到着したときに利用可能なバッファーがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

L & F bits not set

シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファーが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファーが完全なフレームを受け入れたことを示します。いずれかのビットがセットされていない場合、パケットは廃棄され、L & F bits not set カウンターが増分され、バッファーは消去されて再利用できるようになります。

注: L & F bits not set カウンターはトラフィックによる影響は受けません。

SDLC インターフェースの監視

第37章 バイナリー同期リレー (BRLY) の使用

この章では、バイナリー同期リレー (BRLY) プロトコルの使用法について説明します。本章には、以下の節が含まれています。

- 『BRLY の概要』
- 657ページの『BRLY の考慮事項』

バイナリー同期リレー (BRLY) は、バイナリー同期通信 (BSC) トラフィックをカプセル化し、IP 接続を通じてトラフィックを送信するプロトコルです。この機能により、BSC 接続がピア間に存在するかのように、BSC トラフィックが BSC ピア間を流れることが可能になります。以下の節では、BRLY、いくつかの一般的な構成、および BRLY シナリオを構成する方法について説明します。

BRLY の概要

BSC 接続は、1 次エンド・ポイント (ポーリング側) と 2 次エンド・ポイント (ポーリングされる側) から構成される点では SDLC 接続と似ています。接続は次のいずれかです。すなわち、1 次が単一の 2 次と通信する場合は、ポイント・ポイントであり、1 次が複数の 2 次と通信する場合は、マルチポイントです。BRLY は、物理マルチポイント・コネクションとバーチャル・マルチポイント・コネクションの両方をサポートします。

このインプリメンテーションでは、1 次および 2 次の BSC 装置はルーターに接続され、ルーター自体は IP を通じて相互間に接続されます。図31 は、ポイント・ポイントおよび物理マルチポイント BRLY 構成のダイアグラムです。物理マルチポイント・コネクションは、すべての 2 次装置が同じ物理接続上にある接続です。

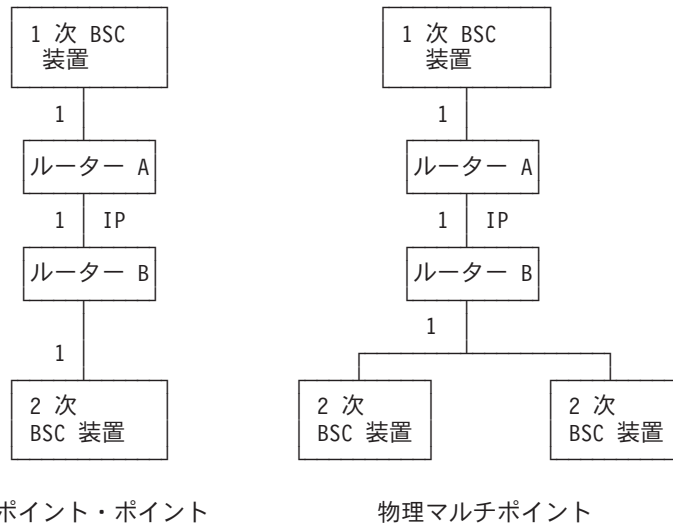


図 31. 物理 BSC リレー構成. 図の中の数字は、BSC リレーのグループ番号を表しています。

バーチャル・マルチポイント・コネクションは、異なる BRLY グループ (異なる物理接続) を使用して、単一の BSC 1 次と複数の BSC 2 次を接続します。図32 はバーチャル・マルチポイント構成のダイアグラムです。

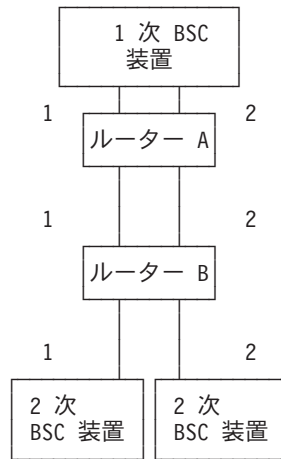


図32. バーチャル BSC リレー・マルチポイント構成. 図の中の数字は、BSC リレーのグループ番号を表しています。

BSC リレーは、バーチャルおよび物理マルチポイント・コネクションの組み合わせもサポートします。図33 は、バーチャルおよび物理マルチポイント・コネクションの組み合わせのダイアグラムです。

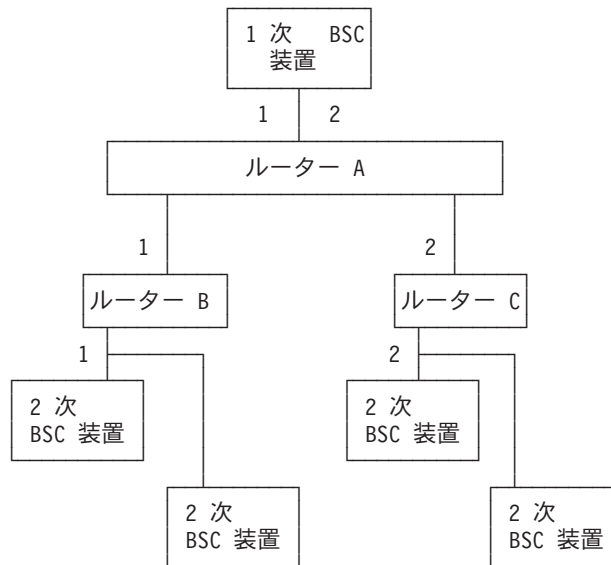


図33. バーチャルおよび物理 BRLY マルチポイント構成の組み合わせ. 図の中の数字は、BSC リレーのグループ番号を表しています。

BRLY 構成のサンプル

以下の例は、図33 のネットワークに似た BRLY ネットワークの構成を示しています。これらの例は、次の前提事項を使用しています。

- ルーター A、B、および C 上のインターフェース 1 は、BSC インターフェースとして構成済みです。
- 1 次 BSC 装置のローカル・ポートの IP アドレスは 6.6.6.4 です。
- ルーター B の 2 次 BSC 装置ローカル・ポートの IP アドレスは 6.6.6.1 です。
- ルーター C の 2 次 BSC 装置ローカル・ポートの IP アドレスは 6.6.6.2 です。

```

Config>protocol brly
BSC Relay protocol user configuration
BRLY config>add group 1
Local group number: [1]?
Point to Point connection?(Yes or [No]):
BRLY config>add local
Local group number: [1]?
Interface number: [0]? 1
(P)primary or (S)econdary: [S]? p
Does this interface communicate with multiple remote groups [N]? y
BRLY config>add remote
Local group number: [1]?
IP address of remote router: [0.0.0.0]? 6.6.6.1
Remote router group number: [1]?
(P)primary or (S)econdary: [S]? s
Station address in hexadecimal (1 - FF): [1]? c1
BRLY config>li all

```

BSC Relay Configuration

Local Group	Group Type	Port Status	Net Number	Remote Group	Station Address	IP Address
1 (E)	MULTI	Local PRMRY (E) Remote SCNDRY (E)	1	1	C1	6.6.6.1

E = enabled, D = disabled

```

BRLY config>add group 2
Local group number: [1]? 2
Point to Point connection?(Yes or [No]):
BRLY config>add local
Local group number: [1]? 2
Interface number: [0]? 1
(P)primary or (S)econdary: [S]? p
Does this interface communicate with multiple remote groups [N]? y
BRLY config>add remote
Local group number: [1]? 2
IP address of remote router: [0.0.0.0]? 6.6.6.2
Remote router group number: [1]? 2
(P)primary or (S)econdary: [S]? s
Station address in hexadecimal (1 - FF): [1]? c5
BRLY config>li all

```

BSC Relay Configuration

Local Group	Group Type	Port Status	Net Number	Remote Group	Station Address	IP Address
1 (E)	MULTI	Local PRMRY (E) Remote SCNDRY (E)	1	1	C1	6.6.6.1
2 (E)	MULTI	Local PRMRY (E) Remote SCNDRY (E)	1	2	C5	6.6.6.2

E = enabled, D = disabled

図 34. ルーター A の BRLY 構成 (ルーター A で入力されたコマンド)

注:

1. グループ 1 の構成は 1 から始まります。
2. グループ 2 の構成は 2 から始まります。

```

BRLY config>add group
Local group number: [1]?
Point to Point connection?(Yes or [No]):
BRLY config>add local
Local group number: [1]?
Interface number: [0]? 1
(P)primary or (S)econdary: [S]? s
Station address in hexadecimal (1 - FF): [1]? c1
BRLY config>add remote
Local group number: [1]?
IP address of remote router: [0.0.0.0]? 6.6.6.4
Remote router group number: [1]?
(P)primary or (S)econdary: [S]? p
BRLY config>li all

```

BSC Relay Configuration

Local Group	Group Type	Port Status	Net Number	Remote Group	Station Address	IP Address
1 (E)	MULTI	Local SCNDRY (E) Remote PRMRY (E)	1	1	C1	6.6.6.4

E = enabled, D = disabled

図 35. ルーター B の BRLY 構成 (ルーター B で入力されたコマンド)

```

BRLY config>add group
Local group number: [1]? 2
Point to Point connection?(Yes or [No]):
BRLY config>add local
Local group number: [1]? 2
Interface number: [0]? 1
(P)primary or (S)econdary: [S]? s
Station address in hexadecimal (1 - FF): [1]? c5
BRLY config>add remote
Local group number: [1]? 2
IP address of remote router: [0.0.0.0]? 6.6.6.4
Remote router group number: [1]? 2
(P)primary or (S)econdary: [S]? p
BRLY config>li all

```

BSC Relay Configuration

Local Group	Group Type	Port Status	Net Number	Remote Group	Station Address	IP Address
2 (E)	MULTI	Local SCNDRY (E) Remote PRMRY (E)	1	2	C5	6.6.6.4

E = enabled, D = disabled

図 36. ルーター C の BRLY 構成 (ルーター C で入力されたコマンド)

BRLY の考慮事項

BRLY を構成するときは、次のことを念頭に入れてください。

- BRLY を使用可能にすると、ネットワーク内のポーリングが増え、合計のネットワーク・スループットは低下することになります。

- BSC 装置は、非活動タイマーが満了すると自動的に切断されます。デフォルトでは、これは 3 秒後に起こります。使用中の場合が極度に多いネットワークでは、BSC 装置が頻繁に切断されることとなります。

第38章 BSC リレーの構成および監視

この章では、2 進データ同期通信 (BSC) リレ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。本章には、BSC インターフェースを構成するための手順も記載されています。

本章には、以下の節が含まれています。

- 『基本構成手順』
- 660ページの『BSC リレー構成コマンド』
- 669ページの『BSC リレー監視コマンド』
- 672ページの『BSC リレー・インターフェースおよび GWCON インターフェース・コマンド』

基本構成手順

この節では、BSC インターフェースおよび BSC リレー・プロトコルを構成する手順を概説します。詳しい構成情報および説明については、本章で説明されている構成コマンドを参照してください。

BSC リレー・インターフェースを構成し、そのインターフェースを介して BRLY を稼働するには、次のようにします。

1. インターフェースを BSC インターフェースとして構成する。

- a. Config> プロンプトで **set data-link bsc** を入力する。
- b. プロンプトで指示されたら、インターフェース番号を入力する。
- c. BSC インターフェース構成プロンプトにアクセスする。

```
Config>network 2
BSC interface user configuration
BSC 2 Config>
```

- d. **list** コマンドを使用し、必要な場合は **set** コマンドを使用して、現行のインターフェース設定を表示する。
- e. 必要な BSC インターフェースをすべて構成し終わるまで繰り返す。

2. BRLY プロトコルを構成する。

- a. BRLY プロトコルにアクセスする。

```
Config>protocol brly
BSC Relay protocol user configuration
BSC Relay config>
```

- b. **add group** コマンドを使用してグループを追加する。
- c. **add local-port** コマンドを使用してローカル・ポートを追加する。
- d. **add remote-port** コマンドを使用してリモート・ポートを追加する。これは、シリアル・ラインのリモート側に直接接続されたポートを識別し、その接続の IP アドレスを指定します。
- e. 必要なグループ、ローカル・ポート、およびリモート・ポートをすべて構成し終わるまでステップ 2b ~ 2d を繰り返す。

BSC リレー構成コマンド

この節では、BSC リレー構成コマンドについて説明します。本章では、BSC リレー用のネットワーク・パラメーターとプロトコル・パラメーターの両方について説明します。

BSC リレー構成コマンドでは、BSC リレー・フレームを送信するインターフェースのルーター・パラメーターを指定することができます。構成コマンドをアクティブにするには、ルーターをリスタートする必要があります。表87は、ネットワーク BSC とプロトコル BRLY の両方のコマンドを示しています。

表 87. BSC リレー構成コマンドの要約

コマンド	ネットワーク		機能
	BSC	BRLY	
? (Help)	可	可	すべての構成コマンドをリストするか、または特定の構成コマンドに関連するオプションをリストします。
Add		可	グループ、ローカル・ポート、およびリモート・ポートを追加します。
Delete		可	グループ、ローカル・ポート、およびリモート・ポートを削除します。
Disable		可	グループおよびポートを使用不可にします。
Enable		可	グループおよびポートを使用可能にします。
List	可	可	BSC リレー全体、グループ固有、およびインターフェースの構成を表示します。
Set	可		リンク・パラメーターおよびリモート端末パラメーターを設定します。
Exit	可	可	BSC リレー構成環境を終了して、CONFIG 環境に戻ります。

Add

add コマンドは、グループ、ローカル・ポート、およびリモート・ポートを追加するのに使用します。

構文:

```
add                group group#
                    _local-port
                    _remote-port
```

group group#

1 次から 2 次への接続を定義します。異なる接続ごとに、異なるグループ番号が必要です。

例: add group

```
Group number: [1]? 1
Group type: [multipoint]
```

Group number

そのグループに指定するグループ番号

有効値: 1 ~ 16

デフォルト値: 1

Group type

このグループがサポートする BSC 接続のタイプを指定します。

有効値: point-to-point または multipoint

デフォルト値: multipoint

local-port

特定のグループのローカル・ポートとして使用するインターフェースを識別します。ローカル・ポートは、構成している 2210 に直接接続されている BSC 装置への接続です。次の例は、1 次ローカル・ポートを追加します。

例: add local-port

```
Group number: [1]? 1
Interface number: [0]? 2
(P)rimary or (S)econdary:[S]? p
```

Group number

そのポートのグループ番号。この番号は、**add group** コマンドを使用して事前に構成する必要があります。

Interface number

ローカル・ポートを示すルーターのインターフェース番号

Primary or Secondary

ポート・タイプ (1 次 (P) または 2 次 (S)) を指定します。

デフォルト値: S

Station address character

システムが 2 次ポートについて表示する文字を指定します。これを入力するよう求められるのは、ローカル・ポートを 2 次として構成する場合のみです。

有効値: X'01' ~ X'FF'

デフォルト値: なし

注: この値は、表示のためにだけ使用され、2 次のグループを識別します。

remote-port

リモート (同位) ルーターでシリアル・ラインに直接接続されたポートの IP アドレスを識別します。次の例は、2 次としてのリモート・ポートの構成をしています。

例: add remote-port

```
Group number: [1]? 1
IP address of remote router:[0.0.0.0]? 128.185.121.97
(P)rimary or (S)econdary:[S]? s
Remote group number: [1]? 2
Station address character? cd
```

Group number

そのポートのグループ番号。この番号は、**add group** コマンドを使用して事前に構成する必要があります。

BSC リレーの構成 (Talk 6)

IP address of remote router

リモート・ユーザーと通信するインターフェースの IP アドレスを指定します。

Primary or Secondary

ポート・タイプ (1 次 (P) または 2 次 (S)) を指定します。

Remote group number

リモート・ポートのグループ番号はリモート・ルーターで定義されているので、このグループ番号を指定します。

Station Address Character

システムが 2 次ポートについて表示する文字を指定します。これを入力するよう求められるのは、ローカル・ポートを 2 次として構成する場合のみです。

有効値: X'01' ~ X'FF'

デフォルト値: なし

注: この値は、表示のためにだけ使用され、2 次のグループを識別します。

Delete

delete コマンドは、グループ、ローカル・グループ、およびリモート・ポートを除去するのに使用します。

構文:

```
delete                group group#
                        local-port
                        remote-port
```

group *group#*

グループ (group#) を除去します。

例: **delete group 1**

local-port *group#*

指定されたグループのローカル・ポートを除去します。

例: **delete local-port**

Group number: [1]? 2

Group number

ローカル・ポートのグループ番号

remote-port

指定されたグループのリモート・ポートを除去します。

例: **delete remote-port**

Group number: [1]? 1

Group number

リモート・ポートのグループ番号

Disable

disable コマンドは、リレー・グループ全体または特定のリレー・ポートのリレーを抑制します。

構文:

```
使用不可 (disable)      group group#
                          port
```

group *group#*

特定のローカル・グループとの間の BSC リレー・フレームの転送を抑制します。

例: **disable group 1**

port 特定のローカルまたはリモート・リレー・ポートとの間の BSC リレー・フレームの転送を抑制します。

例: **disable port**

```
Group number: [1]? 2
Local or Remote:[local]? remote
```

Group number

使用不可にするポートのグループ番号

Local or Remote

ローカルまたはリモート・ポートを使用不可にするかどうか指定します。

デフォルト値: local

Enable

enable コマンドは、リレー・グループ全体または特定のリレー・ポートのデータ転送をオンにするのに使用します。

構文:

```
enable                  group group#
                          port
```

group *group#*

指定されたグループとの間の BSC リレー・フレームの転送を可能にします。

例: **enable group 1**

port 指定されたローカル・ポートとの間の BSC リレー・フレームの転送を可能にします。

例: **enable port**

```
Group number: [1]? 2
Local or Remote:[local]? remote
```

Group number

使用可能にするポートのグループ番号

BSC リレーの構成 (Talk 6)

Local or Remote

ローカルまたはリモート・ポートを使用可能にするかどうか指定します。

デフォルト値: local

List (ネットワーク BSC の場合)

list コマンドは、特定の BSC インターフェースの構成を表示するのに使用します。これらのコマンドは、`BSC n Config>` プロンプトから入力します。ここで、*n* はインターフェースの番号です。

構文:

list

例:

```
list
Maximum frame size in bytes: 2048
Encoding: NRZI
Idle State: Sync
Clocking: Internal
Cable type: V.35 DCE
Speed (bps): 2048000
Code: ASCII
Checking algorithm: LRC
Link EOT: No
Number of pairs of SYNs: 1
```

Maximum frame size in bytes

リンクを介して送信できる最大フレーム・サイズ。最大フレーム・サイズは、最大フレームと 15 バイトの BRLY ヘッダーが大ききでなければなりません。

Encoding

シリアル・インターフェースの伝送符号化法。符号化法は、NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) です。

Idle state

データ・リンク・アイドル状態: 同期またはマーク

Clocking

クロックのタイプ: 内部または外部

Cable type

シリアル・インターフェースのケーブル・タイプ

Speed (bps)

送信クロックと受信クロックの速度をリストします。

Code この装置によって使用されるコード・タイプ

Checking algorithm

データの検査文字スキーム

Link EOT

EOT 伝送がポーリングと結合されており、伝送がバックツーバックに発生するときは、伝送を選択するかどうかを指定します。

Number of pairs of SYNs

システムがデータの前に送信する同期文字の組みの数

List (プロトコル BRLY の場合)

list コマンドは、特定のグループまたはすべてのグループの構成を表示するのに使用します。これらのコマンドは、BSC Relay config> プロンプトから入力されます。

構文:

```
list                               all
                                   group group#
```

all すべてのグループの構成を表示します。

例: **list all**

BSC Relay Configuration							
Local Group	Group Type	Port Status		Net Number	Remote Group	Station Address	IP Address
1 (E)	MULTI	Local	PRMRY (E)	1	1	C1	6.6.6.1
		Remote	SCNDRY (E)				
2 (E)	MULTI	Local	PRMRY (E)	1	2	C5	6.6.6.2
		Remote	SCNDRY (E)				

E = enabled, D = disabled

注: リモート・ポートのネット番号は、ローカル・グループの構成の一部ではないので、システムはそれをローカル・ポートでは表示しません。

Group Number

グループ番号とグループの状態 (使用可能 (E) または使用不可 (D)) を示します。

Port Status

ポートのタイプ (ローカル/リモート 1次/2次) とその状態 (使用可能 (E) または使用不可 (D)) を示します。

Net Number

ローカル・ポートのインターフェース番号を示します。

Remote Group

リモート・ルーターにあるグループの番号

Address Character

1 つの 2 次局に割り当てられたアドレス文字

IP Address

リモート・ポートの IP アドレスを示します。

```
group group#
指定されたグループの構成を表示します。
```

Set

set コマンドは、BSC インターフェース・パラメーターを構成するのに使用します。

構文:

BSC リレーの構成 (Talk 6)

set

- cable
- clocking [internal or external]
- code [ebcdic or ascii]
- check [CRC16, LRC or none]
- encoding [nrz or nrzi]
- eotlink [yes or no]
- frame-size
- idle [sync or mark]
- speed *bps*
- syns *number*

cable シリアル・インターフェースで使用されるケーブルを設定します。オプションは、次のとおりです。

- RS-232 DTE
- RS-232 DCE
- V35 DTE
- V35 DCE
- V36 DTE
- X21 DTE
- X21 DCE

表88 は、各種のアダプターで構成することができるケーブル・タイプをリストしています。

表 88. 2210 インターフェースのケーブル・タイプ

アダプター・タイプ	ケーブル・タイプ
8 ポート EIA 232	RS-232 DTE および RS-232 DCE
6 ポート V.35/V36	V.35 DCE、V.35 DTE、または V.36 DTE
8 ポート X.21	X.21 DCE および X.21 DTE

例: **set cable V35 dte**

DTE ケーブルは、ルーターをあるタイプの DCE 装置 (たとえば、モデムまたは DSU/CSU) に接続するときに使用します。

DCE ケーブルは、ルーターが DCE として動作し、直接接続のためのクロックを提供するときに使用します。

clocking [internal or external]

モデムまたは DSU に接続するには、外部クロックを構成し、**set cable** コマンドを使って該当する DTE ケーブルを選択します。

別の DTE 装置に直接接続するには、内部クロックを構成し、**set cable** コマンドを使って該当する DCE ケーブルを選択し、**set speed** コマンドを使ってクロック/回線速度を構成します。

デフォルト値: external

code [ebcdic or ascii]

この BSC 装置によって使用されるコード・タイプを指定します。

デフォルト値: ebcddic

check [CRC16, LRC, or none]

この BSC 装置によって使用される検査アルゴリズムを指定します。*none* が指定される場合は、検査アルゴリズムは使用されません。データが移動され、検査が行なわれる場合、これはアプリケーションによって行なわれます。

デフォルト値:

- コードが EBCDIC の場合、デフォルトは巡回冗長検査 (CRC16) です。
- コードが ASCII である場合、デフォルトは水平冗長検査 (LRC) です。

encoding [nrz or nrzi]

BSC インターフェースの伝送符号化法を NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) として構成します。NRZ がデフォルトです。

例: `set encoding nrz`

eotlink [yes or no]

EOT 伝送をポーリングと結合するかどうか、また伝送がバックツーバックで発生するときは伝送を選択するかどうかを指定します。

デフォルト値: yes

frame-size

システムがデータ・リンク上で送受信することができるフレームの最大サイズを構成します。この値を **add remote-secondary** コマンドで指定した値より大きく設定した場合、システムはこの値を、その最大値を反映するように変更します。IBM 2210 は、ユーザーに警告する ELS メッセージを生成します。ユーザーは、これが SRAM 構成内で変更されるまで、この ELS メッセージを継続的に受け取ります。有効な入力値を表 89 に示します。

注: フレーム・サイズは、受信された最大フレームに 15 バイトの BRLY ヘッダーを加えたものが収まる大きさでなければなりません。

表 89. Set Frame-Size コマンドのフレーム・サイズの有効値

最小	最大	デフォルト
128	8190	2048

idle [sync or mark]

システムが BSC データ伝送の間にどの文字を送信するか指定します。

sync BSC 同期文字が送信されることを指定します。(syms パラメーターを参照してください。)

mark すべて 1 ビットの文字 (X'FF') が送信されることを指定します。

デフォルト値: mark

speed bps

内部クロックの場合は、このコマンドを使用して送信および受信クロック回線の速度を指定します。

外部クロックの場合は、このコマンドは WAN/シリアル・ラインの動作に影響を与えません。

有効値:

BSC リレーの構成 (Talk 6)

内部クロック: 表90 を参照してください。

外部クロック: 表91 を参照してください。

表 90. 2210 インターフェースに内部クロックが使用されるときの回線速度

アダプター・タイプ	速度範囲
8 ポート EIA 232	9600 ~ 64 000 bps
6 ポート V.35/V.36	9600 ~ 460 800 bps、1 544 000 bps、または 2 048 000 bps
8 ポート X.21	9600 ~ 460 800 bps、1 544 000 bps、または 2 048 000 bps

外部クロックの場合、このコマンドはハードウェアに影響を与えません。

表 91. 2210 インターフェースに外部クロックが使用されるときの回線速度

アダプター・タイプ	速度範囲
8 ポート EIA 232	2400 ~ 64 000 bps
6 ポート V.35/V.36	2400 ~ 2 048 000 bps
8 ポート X.21	2400 ~ 2 048 000 bps

syms システムがデータの前に送信する SYN 文字の組の数を指定します。SYN は BSC 同期文字です。(idle パラメーターを参照してください。)

BSC リレー監視環境へのアクセス

BSC リレー・プロトコルに関連する情報を監視するには、次のようにして、インターフェース監視プロセスにアクセスします。

1. OPCON プロンプトで、**talk** コマンドと GWCON の PID を入力する。たとえば、次のように入力します。

```
* talk 5  
+
```

システムは、コンソールに GWCON プロンプト (+) を表示します。最初に GWCON に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. GWCON プロンプトで **configuration** コマンドを入力して、ルーターに構成されているプロトコルとネットワークを表示する。たとえば、次のように入力します。

```
+ configuration
```

(**configuration** コマンドの出力例については、152 ページを参照してください。)

3. **protocol BRLY** コマンドを入力する。たとえば、次のように入力します。

```
+ prot brly  
BSC Relay>
```

システムは、コンソール上に BSC リレー・プロンプトを表示します。ここで、BSC リレー監視コマンドを入力して、BSC リレー・ポートに関する情報を表示させることができます。

BSC リレー監視コマンド

この節では、BSC リレー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。BSC リレー監視コマンドでは、BSC リレー・フレームを送信するインターフェースのパラメーターを表示することができます。システムは、すべての BSC リレー監視コマンドについて BSC Relay> プロンプトを表示します。表92 は、コマンドを示しています。

表 92. BSC リレー監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Clear	BSC リレー統計を消去します。
Disable	グループおよびポートを抑制します。
Enable	グループおよびポートをオンにします。
List	BSC リレー全体の構成およびグループ特有の構成を表示します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Clear

clear コマンドは、すべてのポートの BSC リレー統計を廃棄するのに使用します。統計には、転送されたパケットおよび廃棄されたパケットのカウンターが含まれます。このコマンドは、前回のルーターのリスタートまたは統計の消去以降に収集されたローカルおよびリモートのポート統計を消去します。

構文:

clear

例:

```
clear
Clear all port statistics? (Yes or No): Y
```

Disable

disable コマンドは、グループ全体または特定のリレー・ポートのデータ転送を抑制します。SRAM (静的読み取りアクセス・メモリー) は、**disable** 監視コマンドの影響を永続的に保存しません。そのため、ルーターをリスタートすると、このコマンドの影響は消去されます。

構文:

```
disable                group group#
                        port
```

group group#

特定のグループとの間の BSC リレー・フレームの転送を抑制します。

port 特定のローカルまたはリモート・ポートとの間の BSC リレー・フレームの転送を抑制します。

BSC リレーの監視 (Talk 5)

例:

```
disable port
Group number: [1]? 2
Local or Remote: [local]? remote
```

Group number

使用不可にするポートのグループ番号を示します。

Local or Remote

ローカルまたはリモート・ポートを使用不可にするかどうか指定します。

デフォルト値: local

Enable

enable コマンドは、グループ全体または特定のローカル・インターフェース・ポートのデータ転送をオンにするのに使用します。SRAM は、**enable** 監視コマンドの影響を永続的に保存しません。そのため、ルーターをリスタートすると、このコマンドの影響は消去されます。

構文:

```
enable                group group#
                        port
```

group *group#*

指定されたグループとの間の BSC リレー・フレームの転送を可能にします。

port 指定されたローカル・ポートとの間の BSC リレー・フレームの転送を可能にします。

例:

```
enable port
Group number: [0]? 2
Local or Remote: [local]? remote
```

group number

使用可能にするポートのグループ番号を示します。

Local or Remote

ローカルまたはリモート・ポートを使用可能にするかどうか指定します。

デフォルト値: local

List

list コマンドは、特定のグループまたはすべてのグループの構成を表示するのに使用します。

構文:

```
list                all
                        group group#
```


all すべてのローカル・グループの統計を表示します。出力例については、**list group** コマンドを参照してください。

group *group#*

指定されたグループの統計を表示します。

例:

list group 1

```

                                BSC Relay Configuration
  Local  Group      Port      Net  Remote  Station  IP
  Group  Type      Status    Number Group  Address  Address
  -----
  1 (E)  MULTI  Local  PRMRY (E)  1      1      C1      6.6.6.1
                Remote SCNDRY (E)

Local port statistics:
Packets forwarded =      0
Packets discarded =      0

Remote port statistics:
Packets forwarded =      0
Packets discarded =      0

```

Local Group

グループ番号とグループの状態 (使用可能 (E) または使用不可 (D)) を示します。

Group Type

このグループがサポートする BSC 接続のタイプが point-to-point または multipoint のどちらかを指定します。

Port Status

ポートのタイプ (ローカル/リモート 1次/2次) とその状態 (使用可能 (E) または使用不可 (D)) を示します。

Net Number

ローカル・ポートの装置番号を示します。

Station Address

システムが 2 次ポートについて表示する文字

IP Address

リモート・ポートの IP アドレスを示します。

Remote Group

リモート・ルーターにあるグループの番号

Packets Forwarded

システムがポートについて転送したパケットの数を示します。

Packets Discarded

システムがポートについて廃棄したパケットの数を示します。

次の例は、654ページの『BRLY 構成のサンプル』の図のルーター A について作成された構成を示しています。

BSC リレーの監視 (Talk 5)

```
Ctrl-P
* talk 5
+p brly
BSC Console
BSC>1i all
```

BSC Relay Configuration

Local Group	Group Type	Port Status	Net Number	Remote Group	Station Address	IP Address
1 (E)	MULTI	Local PRMRY (E) Remote SCNDRY (E)	1	1	C1	6.6.6.1

Local port statistics:

```
Packets forwarded = 0
Packets discarded = 0
```

Remote port statistics:

```
Packets forwarded = 0
Packets discarded = 0
```

Local Group	Group Type	Port Status	Net Number	Remote Group	Station Address	IP Address
2 (E)	MULTI	Local PRMRY (E) Remote SCNDRY (E)	1	2	C5	6.6.6.2

Local port statistics:

```
Packets forwarded = 0
Packets discarded = 0
```

Remote port statistics:

```
Packets forwarded = 0
Packets discarded = 0
```

E = enabled, D = disabled

```
BSC>exit
```

BSC リレー・インターフェースおよび GWCON インターフェース・コマンド

BSC インターフェースには独自の監視プロセスがありますが、GWCON 環境から **interface** コマンドを使用すると、ルーターも導入済みのネットワーク・インターフェースの完全な統計を表示します。(**interface** コマンドの詳細については、第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド を参照してください。)

第39章 V.25bis ネットワーク・インターフェースの使用

V.25bis インターフェースは、ルーターが V.25bis モデムを使用して、交換電話回線を介してシリアル・コネクションを確立できるようにします。この章では、V.25bis インターフェースの使用法について説明します。本章には、以下の節が含まれています。

- 『始める前に』
- 『構成手順』

注:

1. あて先名をコネクション・リストに割り当て、あて先番号をリスト内の各回線に割り当てることができます。そのあて先名がコールされると、接続されるまで、またはリストが尽きるまで、リスト内の番号が 1 つずつ試されます。
2. V.25bis は、8 ポート EIA 232 アダプターでだけサポートされます。

始める前に

ルーター上の V.25bis を構成する前に、以下が用意されていることを確認してください。

- 同期 V.25bis コマンドおよび 1988 ITU/CCITT V.25bis 仕様をサポートする V.25bis モデム
- モデムが自動的に応答の発信元を検出しない場合は、以下を行う必要があります。
 - リンクの一端のモデムを発呼用に構成する。
 - リンク他端のモデムを応答用に構成する。
 - 応答側のモデムを自動応答用に設定する。

構成手順

この節では、ルーターを V.25bis 用に構成する方法について説明します。実行する必要があるタスクは、次のとおりです。

1. V.25bis アドレスを追加する。
2. V.25bis パラメーターを構成する。
3. ダイヤル回線を追加する。
4. ダイヤル回線を構成する。

注: V.25bis 構成の変更を有効にするためには、ルーターをリスタートする必要があります。

V.25bis アドレスの追加

各ローカル V.25bis インターフェースおよび各あて先の V.25bis アドレスを追加することが必要です。V.25bis アドレスには、次のものが含まれます。

V.25bis の使用

- アドレス名。アドレス名は、アドレスの記述です。最大 23 字までの印刷可能 ASCII 文字列を使用できます。
- ネットワーク・ダイヤル・アドレス。ローカル・ポートまたは先ポートの電話番号です。接続された V.25bis モデムに有効なフォーマットで、最大 30 文字まで入力できます。詳細については、モデムのマニュアルを参照してください。

注: CCITT によって定義され、IBM 2210 によってサポートされている電話番号の有効な文字セットには、以下が含まれます。

- 10 進数の 0 ~ 9
- コロン (:) -- "待機トーン"
- 左かぎ括弧 (<) -- "ポーズ"、数字シーケンス間に一定の遅延 (モデムによって異なる) を挿入するのに使用されます。たとえば、PBX または PTN を通ずる場合などに使用します。
- 等号 (=) -- "区切り記号 3"、これは "国内用" です。(モデムのマニュアルを参照してください。)
- 文字 P -- "パルス方式でダイヤルを継続" (一部のモデムではサポートされません。)
- 文字 T -- "DTMF 方式でダイヤルを継続" (一部のモデムではサポートされません。)

V.25bis アドレスを追加するには、Config> プロンプトで **add v25-bis-address** コマンドを入力します。たとえば、次のように入力します。

```
Config>add v25-bis-address
Assign address name [1-23] chars []? remote-site-baltimore
Assign network dial address [1-30 digits][]? 19095551234
```

V.25bis インターフェースの構成

この節では、V.25bis インターフェースを構成する方法について説明します。構成するには、以下を行います。

1. V.25bis 用のシリアル・ライン・インターフェースを設定するために、シリアル・ライン・インターフェースのデータ・リンク・プロトコルを設定する。Config> プロンプトから **set data-link v25bis** コマンドを使用します。たとえば、次のように入力します。

```
Config>set data-link v25bis
Interface Number [0]? 2
```

2. **network** コマンドに続けてインターフェースの番号を入力して、V.25bis 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>network 2
V.25bis Data Link Configuration
V25bis Config>
```

Config> プロンプトで **list devices** コマンドを使用すると、ルーター上に構成されているインターフェース番号のリストを表示することができます。

3. **set local-address** コマンドを使用して、ローカル・ポートのネットワーク・アドレス名を指定する。**add v25bis-address** コマンドを使用して定義したアドレス名の 1 つを入力する必要があります。たとえば、次のように入力します。

```
V25bis Config>set local-address
Local network address name []? remote-site-baltimore
```

注: 構成変更を有効にするためには、ルーターをリスタートする必要があります。

オプション V.25bis パラメーター

以下は、ユーザーが設定できるオプション V.25bis パラメーターです。これらのコマンドの詳しい説明は、679ページの『V.25bis 構成コマンド』を参照してください。

- アクセス不能なアドレスまたはその種のコールを拒否するアドレスへの連続コール回数を制限することができます。これを行うには、**set retries-no-answer** および **set timeout-no-answer** コマンドを使用します。
- **set disconnect-timeout** コマンドは、ルーターが前回のコールからの信号を除去した後、コールを開始するまでに待つ時間を制御します。
- **set command-delay-timeout** コマンドは、ルーターが DTR をオンにした後、コールを発信するかコールに応答するまでに待つ時間を制御します。
- **set connect-timeout** は、コールを設定するのに許容される秒数を指定します。
- **set duplex** コマンドは、コールの二重方式を設定します。
- **set encoding** コマンドは、コールの符号化を設定します。
- インターフェースの構成を終了したら、**list** コマンドを使用して、構成を表示してみることができます。

ダイヤル回線の追加

ダイヤル回線は、V.25bis シリアル・ライン・インターフェースにマップされます。複数のダイヤル回線を 1 つのシリアル・ライン・インターフェースにマップすることも可能です。

ダイヤル回線を追加するには、Config> プロンプトから **add device dial-circuit** コマンドを使用します。ソフトウェアが、各回線にインターフェース番号を割り当てます。この番号を使用して、ダイヤル回線を構成します。

例:

```
Config>add device dial-circuit
Adding device as interface 6
```

注: ダイヤル回線は、デフォルトではポイント・ポイント・プロトコル (PPP) になります。フレーム・リレー (FR) または SDLC を使用するようにダイヤル回線を構成することも可能です。

ダイヤル回線の構成

この節では、ダイヤル回線の構成方法について説明します。ダイヤル回線コマンドの詳しい説明は、743ページの『第45章 ダイヤル回線の構成および監視』を参照してください。

注: カプセル化タイプが SDLC の場合、ユーザーが設定できる唯一のダイヤル回線パラメーターは、基本ネット番号です。

ダイヤル回線を構成するには、以下を行います。

1. **network** コマンドに続けてダイヤル回線のインターフェース番号を入力して、Circuit Config> プロンプトを表示する。Config> プロンプトで **list devices** コ

V.25bis の使用

マンドを使用すると、追加したダイヤル回線のリストを表示することができます。たとえば、次のように入力します。

```
Config>network 6
Circuit configuration
Circuit Config>
```

2. ダイヤル回線を V.25bis インターフェースにマップする。基本ネットは V.25bis インターフェース番号です。たとえば、次のように入力します。

```
Circuit Config>set net
Base net for this circuit [0]? 0
```

3. ダイヤル回線を接続するリモート・ルーターのアドレス名を指定する。
add v25-bis-address コマンドを使用して定義した名前の 1 つを入力する必要があります。たとえば、次のように入力します。

```
Circuit Config>set destination
Assign destination address name []? newyork
```

4. ダイヤル回線をアウトバウンド・コール発信専用、インバウンド・コールの受信専用、またはコールの発信と受信の両方として構成する。

set calls コマンドを使用します。リンクの両側が同時にコール設定を試みた場合に競合を避けるために、リンクの一方の端のダイヤル回線はインバウンド・コールの受信専用構成し、リンクの他方の端のダイヤル回線はアウトバウンド・コール発信専用構成します。たとえば、次のように入力します。

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

注: WAN 復元動作または別のダイヤル・オンデマンド・アプリケーションの場合、回線をインバウンド用またはアウトバウンド用のいずれかに設定することが必要です。

5. 回線のタイムアウト期間を指定する。

set idle コマンドを使用します。この指定された期間、回線上にトラフィックがないと、ダイヤル回線はハングアップします。回線を専用回線として構成する場合は、アイドル・タイマーをゼロに設定します。回線をダイヤル・オンデマンドに構成する場合は、アイドル・タイマーをゼロ以外の値に設定します。範囲は 0 ~ 65535 で、デフォルトは 60 秒です。たとえば、次のように入力します。

```
Circuit Config>set idle
Idle timer (seconds, 0 means always active) [60]? 0
```

注: WAN 復元動作の場合、アイドル・タイムを 0 に設定する必要があります。

6. オプションで、コール設定と初期パケット送信の間の時間を遅らせることができます。

set selftest-delay コマンドを使用します。自己テスト遅延を設定すると、初期パケットが廃棄されるのを防止できます。モデムが同期のために余分な時間が必要な場合は、この遅延を調整します。たとえば、次のように入力します。

```
Circuit Config>set selftest-delay
Selftest delay(milli-seconds,0 means no delay)[150]?200
```

7. インバウンド・アドレス名を設定する。

set inbound コマンドを使用します。このコマンドを使用する必要があるのは、回線がインバウンド・コールとアウトバウンド・コールの両方に設定されており、ルーターのあて先アドレスが、リモート・ルーターがダイヤルするあて先アドレスと異なっている場合だけです。たとえば、ルーターの 1 つが PBX、国

際、または LATA 間交換局を通す必要がある場合は、番号が異なることとなります。たとえば、次のように入力します。

```
Circuit Config>set inbound  
Assign destination inbound address name []? newyork
```

add v25-bis-address コマンドを使用して定義した名前の 1 つに一致していることが必要です。

8. **set duplex** コマンドを使用して、回線の二重方式を設定する。
9. **set encoding** コマンドを使用して、回線の符号化方式を設定する。
10. オプションで、ダイヤル回線上で実行されているデータ・リンク・レイヤー・プロトコル (PPP またはフレーム・リレー) の構成プロセスに入ることができます。**encapsulator** コマンドを使用します。たとえば、次のように入力します。

```
Circuit Config> encapsulator
```

V.25bis の使用

第40章 V.25bis ネットワーク・インターフェースの構成および監視

この章では、V.25bis 構成コマンドとオペレーショナル・コマンド、および GWCON コマンドについて説明します。本章には、以下の節が含まれています。

- 『インターフェース構成プロセスへのアクセス』
- 『V.25bis 構成コマンド』
- 684ページの『インターフェース監視プロセスへのアクセス』
- 684ページの『V.25bis 監視コマンド』
- 689ページの『V.25bis と GWCON コマンド』

インターフェース構成プロセスへのアクセス

V.25bis 構成プロセスにアクセスするには、以下の手順を使用します。

1. OPCON プロンプトで、**talk** コマンドと CONFIG の PID を入力する。(このコマンドの詳細については、OPCON プロセスとは 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>) がコンソールに表示されます。最初に **CONFIG** に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. CONFIG プロンプトで **list devices** コマンドを入力して、ルーターが現在構成されているネットワーク・インターフェース番号を表示する。
3. インターフェース番号を記録する。
4. CONFIG **network** コマンドと、構成するインターフェースの番号を入力する。たとえば、次のように入力します。

```
Config> network 1  
V.25bis Config>
```

これで、V.25bis 構成プロンプトがコンソールに表示されます。

V.25bis 構成コマンド

680ページの表93 は、V.25bis 構成コマンドの要約を示しており、本節の残りの部分で、個々のコマンドについて説明します。これらのコマンドを用いて、V.25bis 構成を表示、作成、または変更することができます。V.25bis 構成コマンドは、V.25bis Config> プロンプトで入力します。

V.25bis 構成コマンド

表 93. V.25bis 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
List	V.25bis 構成を表示します。
Set	ローカル・アドレス、接続、切断、および無応答タイムアウト、無応答後の再試行回数、コマンド遅延タイムアウト、および符号化を設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、現行の V.25bis 構成を表示するのに使用します。

構文:

list

例:

```
list
      V.25bis Configuration

Duplex                = Full
Encoding              = NRZ
Local Network Address Name = v403
Local Network Address  = 15088982403

Non-Responding addresses:
Retries               = 1
Timeout               = 0 seconds

Call timeouts:
Command Delay         = 0 ms
Connect               = 60 seconds
Disconnect            = 2 seconds

Cable type            = V.35 DTE
Speed                  = 9600
```

Duplex

ダイヤル接続が確立された場合、インターフェースの二重方式を表示します。

Encoding

ダイヤル接続が確立された場合、インターフェースの伝送符号化法を表示します。符号化法は、NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) です。

Local Network Address Name:

ローカル・ポートのネットワーク・アドレス名を表示します。

Local Network Address:

ローカル・ポートのネットワーク・ダイヤル・アドレスを表示します。

Non-responding addresses:

Retries

ルーターがタイムアウト期間中に無応答アドレスに対して試行する呼の最大数

Timeout

ルーターは、無応答アドレスへの試行の最大数に達した場合、この時間が満了するまでコール設定を試行しません。このタイムアウト期間は、ルーターが最初のコールを試みた時点で開始します。

Call timeouts:

コールのタイムアウトの回数

Command Delay

ルーターが DTR (データ端末レディー) をオンにした後、コールするかコールに応答するまでに待つ時間 (ミリ秒)。このパラメーターを 0 に設定した場合、モデムが CTS (送信可) 信号で DTR に応答するのを待ってから、ルーターはコマンドを出します。

Connect

コールを設定するのに許容される秒数。このパラメーターが 0 に設定されている場合、モデムがコール設定タイムアウトを制御します。

Disconnect

ルーターは DTR を除去した後、この時間だけ待ってから、次のコールを開始します。このパラメーターを 0 に設定すると、モデムが CTS および DSR を除去することによって DTR 除去に応答するのを待ってから、ルーターは次のコールを開始します。

Set

set コマンドは、ローカル・アドレス、コールのタイムアウトと遅延、無応答アドレスの再試行とタイムアウト、および HDLC ケーブル・タイプを構成するのに使用します。

構文:

```
set                command-delay timeout . . .
                   connect-timeout . . .
                   disconnect-timeout . . .
                   duplex
                   hdlc cable . . .
                   hdlc encoding . . .
                   hdlc speed . . .
                   local-address . . .
                   retries-no-answer . . .
                   timeout-no-answer . . .
```

command-delay-timeout # of milliseconds

ルーターは DTR (データ端末レディー) をオンにした後、この時間数だけ待ってから、コールを開始したり、コールに応答したりします。このパラメー

V.25bis 構成コマンド

ターを 0 に設定した場合、モデムが CTS (送信可) 信号で DTR に応答するのを待ってから、ルーターはコマンドを出します。範囲は 0 ~ 65535 ミリ秒で、デフォルトは 0 です。

connect-timeout # of seconds

コールを設定するのに許容される秒数を設定します。範囲は 0 ~ 65535 秒で、デフォルトは 60 です。このパラメーターを 0 に設定すると、モデムがコネクション・タイムアウトを制御します。最初にこのパラメーターを 0 に設定し、次に ELS イベント V25B.027 を使用して、種々のあて先に接続を確立するための所要時間を調べる必要があります。その後で、このパラメーターを、最長接続時間よりわずかに高い値に設定します。

注: 通常は政府規制により、モデム製造業者はコール設定を最大長にするように制限されています。この値は単に最適化のためのものであり、一部の DSU との相互運用では、このパラメーターを変更することが必要になる場合もあります。

disconnect-timeout # of seconds

ルーターが DTR を除去後、次のコールを開始する前に待機する時間 (秒) を指定します。範囲は 0 ~ 65535 秒で、デフォルト値は 2 です。このパラメーターを 0 に設定した場合、モデムが CTS および DSR を除去して DTR 除去に応答するのを待ってから、ルーターはコマンドを出します。

duplex

回線の二重タイプを指定します。

全二重が構成されている場合、ダイヤル接続が確立された後は、RTS モデム信号は代入されたままになります。

半二重が構成されている場合、ルーターは転送時になると RTS を上げて、モデムが CTS を代入するのを待ちます。CTS が代入されると、ルーターはデータ・パケットを転送し、転送している間は RTS を除去して、ピア装置が応答できるようにします。

交換 SDLC を扱うために V.25bis インターフェースを使用している場合、およびモデムが半二重方式の動作を必要とする場合には、半二重のみを構成してください。

注:

1. PPP またはフレーム・リレー回線の場合は、全二重でなければなりません。
2. 8 ポート EIA-232E アダプター上の V.25bis インターフェースに半二重を構成する場合、**set hdlc speed** コマンドを使用して回線速度を構成する必要があります。

有効値: full または half

デフォルト値: full

hdlc cable rs232 dtc

このインターフェースに接続されるケーブルのタイプを指定します。このパラメーターを設定した場合、GWCON (+) プロンプトで **interface** コマンド

を入力するか、V.25bis> 監視プロンプトで **statistics** コマンドを入力すれば、ケーブル・タイプを見ることができます。このパラメーターは、ルーターの動作には影響を与えません。

hdlc encoding

HDLC 伝送符号化法を NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) に設定します。ほとんどの構成は NRZ を使用します。構成された符号化法は、エンド・エンド間の接続で使用されます。

注: NRZI を構成することも可能ですが、DTE とモデム間の交換では (CCITT 勧告の V.25bis に記述) NRZ が符号化法として使用されます。

有効値: NRZ または NRZI

デフォルト値: NRZ

hdlc speed

このインターフェースの回線速度を指定します。このパラメーターを設定した場合、GWCON (+) プロンプトで interface コマンドを入力したとき、および V.25bis> 監視プロンプトで statistics コマンドを入力したときに、回線速度が表示されます。範囲は 2400 to 64 000 bps. デフォルトは 9600 bps です。

注: このコマンドは実際の回線速度には影響を与えませんが、一部のプロトコル (IPX など) が、V.25bis インターフェースにマップされるダイヤル回線のルーティング・コストを計算するのに使用する速度を設定します。

local-address *address name*

ローカル・ポートのネットワーク・ダイヤル・アドレスを表示します。このアドレス名は、Config> で **add v25-bis-address** コマンドを使用して定義した名前の 1 つに一致していることが必要です。

例: **set local-address line-1-local**

retries-no-answer *value*

一部の電話サービス提供者は、自動リコール装置に対して、アクセス不能アドレスまたは自動リコールを拒否するアドレスへの連続コール回数を制限しています。このパラメーターは、ルーターがタイムアウト期間中に無応答アドレスに対して試行するコールの最大数を指定します。範囲は 0 ~ 10 で、デフォルトは 1 です。

注: 政府規制により、モデム製造業者がこのパラメーターを変更するのを制限している場合もあります。

timeout-no-answer *# of seconds*

ルーターは、無応答アドレスへの **retries-no-answer** の最大数に達した場合、この時間が満了するまで、次のコールを開始しません。このタイムアウト期間は、あるアドレスにルーターが最初のコールを試みた時点で開始します。範囲は 0 ~ 65535 秒で、デフォルトは 0 です。このパラメーターを 0 に設定すると、モデムがタイムアウト期間を制御します。

インターフェース監視プロセスへのアクセス

V.25bis の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。

```
+ network #
```

ただし、# は、V.25bis シリアル・ラインの番号です。ダイヤル回線の V.25bis 監視プロセスには直接アクセスできませんが、シリアル・ライン・インターフェースにマップされたダイヤル回線を監視することができます。

注: V.25bis インターフェースには、V.25bis 関連のアクティビティを監視するのに使用できる ELS トラブルシューティング・メッセージもあります。詳細については、*IBM Nways* イベント・ログ・システム・メッセージの手引き を参照してください。

V.25bis 監視コマンド

この節では、V.25bis 動作コマンドの要約を示し、個々のコマンドについて説明します。これらのコマンドを用いて、V.25bis インターフェースのコール、回線、パラメーター、および統計を見ることができます。

V.25bis 監視コマンドは、V.25bis> プロンプトで入力します。表94 は、コマンドを示しています。

表 94. V.25bis 監視コマンドの要約

監視コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Calls	前回にルーター上の統計がリセットされた以降に、このインターフェースにマップされた各ダイヤル回線で行われた、完了した接続および試行された接続の数をリストします。
Circuits	V.25bis インターフェースに構成されたすべてのデータ回線の状態を示します。
Parameters	V.25bis インターフェースの現行パラメーターを表示します。(このコマンドは、V.25bis Config> list コマンドに似ています。)
Statistics	V.25bis インターフェースの現行統計を表示します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Calls

calls コマンドは、前回にルーター上の統計がリセットされた以降に、このインターフェースにマップされた各ダイヤル回線で行われた、完了した接続および試行された接続の数をリストするのに使用します。

構文:

```
calls
```

例:

```
calls
Net Interface Site Name      In   Out  Rfsd  Blckd
1   PPP/0     v403          2    0    0     0
```

Unmapped connection indications: 0

Net このインターフェースにマップされたダイヤル回線の数

Interface

インターフェースのタイプとそのインスタンス番号

Site Name

ダイヤル回線のネットワーク・アドレス名

In このダイヤル回線で受け入れられたインバウンド接続の数

Out このダイヤル回線によって開始され、完了した接続の数

Rfsd このダイヤル回線によって開始されたが、ネットワークまたはリモートあて先ポートによって拒否された接続の数

Blckd ルーターがブロックした接続試行の数。ルーターが接続試行をブロックするのは、ローカル・ポートがすでに使用されている場合、無応答アドレスへの再試行の最大数に達している場合、またはモデムが応答していない場合です。

Unmapped connection indications:

着信コールを受け入れるように構成されている使用可能なダイヤル回線がないために、ルーターによって拒否された接続試行の数

Circuits

circuits コマンドは、V.25bis ポートに構成されているすべてのダイヤル回線の状態を示します。

構文:

circuits

例:

```
circuit
Net Interface MAC/Data-Link State Reason Duration
2   PPP/0     Point to Point Avail Rmt Disc 1:02:25
```

Net このインターフェースにマップされたダイヤル回線の数

Interface

インターフェースのタイプとそのインスタンス番号

MAC/DataLink

このダイヤル回線に構成されたデータ・リンク・プロトコルのタイプ

State ダイヤル回線の現行状態

Up - 現在接続されています。

Available - 現在は接続されていませんが、利用可能です。

Disabled - ダイヤル回線は使用不可にされました。

Down - ダイヤル回線がビジーであるか、リンク・レイヤー・プロトコルがダウンしているために、接続に失敗しました。

V.25bis 動作コマンド

Reason

現行状態の理由:

nnn_Data - (nnn はプロトコルの名前) プロトコルに送信するデータがあったので、回線は Up です。

Remote Disconnect - リモート着側がコールを切断したので、回線は Down または Available のいずれかです。

Operator Request - 前回のコールが監視コマンドによって切断されたので、回線は Available です。

Inbound - 回線がインバウンド・コールに応答したので、回線は Up です。

Restoral - WAN 復元動作のため、回線は Up です。

Self Test - 回線は静的として構成されており (アイドル・タイム = 0)、使用可能にされたときに正常に接続されました。

Duration

回線が現行状態にある時間の長さ

Parameters

parameters コマンドは、現行の V.25bis シリアル・ライン構成を表示するのに使用します。これは、V.25bis Config> list コマンドで表示される情報と同じです。

構文:

parameters

例:

```
parameters
V.25bis port Parameters

Local Network Address Name   = v402
Local Network Address       = 15088982402

Non-Responding addresses:
Retries                     = 1
Timeout                     = 0 seconds

Call timeouts:
Command Delay               = 0 ms
Connect                     = 0 seconds
Disconnect                  = 0 seconds
```

Local Network Address Name:

ローカル・ポートのネットワーク・アドレス名

Local Network Address:

ローカル・ポートのネットワーク・ダイヤル・アドレス

Non-responding addresses:

Retries

ルーターがタイムアウト期間中に無応答アドレスに対して試行するコールの最大数

Timeout

ルーターは、無応答アドレスへの試行の最大数に達した場合、この時間が満了するまでコール設定を試行しません。このタイムアウト期間は、あるアドレスにルーターが最初のコールを試みた時点で開始します。

Call timeouts:**Command Delay**

ルーターが DTR (データ端末レディー) をオンにした後、コールするかコールに応答するまでに待つ時間 (ミリ秒)。このパラメーターを 0 に設定した場合、モデムが CTS (送信可) 信号で DTR に応答するのを待ってから、ルーターはコマンドを出します。

Connect

コールを設定するのに許容される秒数。このパラメーターが 0 に設定されている場合、モデムがコール設定タイムアウトを制御します。

Disconnect

ルーターは DTR を除去した後、この時間だけ待ってから、次のコールを開始します。このパラメーターを 0 に設定すると、モデムが CTS および DSR を除去することによって DTR 除去に応答するのを待ってから、ルーターは次のコールを開始します。

Statistics

statistics コマンドは、この V.25bis インターフェースの現行統計を表示するのに使用します。

構文:**statistics****例:**

```
statistics
V.25bis port Statistics

Adapter cable:          RS-232 DTE

Nicknames:  RTS CTS DSR DTR DCD RI
RS-232      CA CB  CC CD  CF CE
State:      OFF OFF OFF OFF OFF OFF

Line speed:          4800
Last port reset:    24 seconds ago

Input frame errors:
CRC error           0 alignment (byte length)  0
missed frame        0 too long (> 2182 bytes)  0
aborted frame       0 DMA/FIFO overrun          0
L & F bits not set  0

Output frame counters:
DMA/FIFO underrun errors  0 Output aborts sent      0
```

Adapter cable:

使用されているアダプター・ケーブルのタイプ

Nicknames:

回線の通称名

RS-232

回線の EIA 232 (RS-232 と呼ばれる) 名

V.25bis 動作コマンド

State: 回線の現在の状態: ON、OFF、または "---" (これは、このタイプのインターフェースの状態は未定義であることを意味します。)

Line speed:

送信クロック速度 (概略値)

Last port reset:

ポートがリセットされた後の経過時間

Input frame errors:

CRC error

チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment (byte length)

長さが 8 の偶数倍でないために廃棄された受信パケットの数

Missed Frame

フレームが装置に到着したときに利用可能なバッファがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

too long (> nnnn bytes)

構成されたフレーム・サイズ (nnnn) より大きかったために廃棄された受信パケットの数

aborted frame

送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

DMA/FIFO overrun

シリアル・インターフェース・カードがシステム・パケット・バッファ・メモリーにデータを送信する速度が遅かったために、ネットワークからデータを受信できなかった回数

L & F bits not set

シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファが完全なフレームを受け入れたことを示します。いずれかのビットがセットされていない場合、パケットは廃棄され、L & F bits not set カウンターが増分され、バッファは消去されて再利用できるようになります。

注: L & F bits not set カウンターはトラフィックによる影響は受けません。

Output frame counters:

DMA/FIFO underrun errors

シリアル・インターフェース・カードがシステム・パケット・バッファ・メモリーからデータを取り出す速度が遅かったために、パケットをネットワーク上に送信できなかった回数

Output aborts sent

高位レベルのソフトウェアの要求によって打ち切られた伝送の数

V.25bis と GWCON コマンド

V.25bis には独自の監視のための監視プロセスがありますが、GWCON 環境から interface、statistics、および error コマンドを使用すれば、ルーターも構成情報と、装置および回線の完全な統計を表示します。また、GWCON **test** コマンドを使用して、DCE および回線をテストすることもできます。

注: V.25bis シリアル・インターフェースに対して **test** コマンドを出すと、現行のコールは除去され、再ダイヤルされます。

GWCON コマンドについての詳細は、149ページの『第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』を参照してください。

V.25bis インターフェースおよびダイヤル回線の統計

V.25bis シリアル・ライン・インターフェースおよびダイヤル回線の統計を表示するには、GWCON (+) プロンプトから **interface** コマンドを使用します。

V.25bis シリアル・ライン・インターフェースの以下の統計を表示するには、**interface** コマンドに続けて V.25bis シリアル・ライン・インターフェースのインターフェース番号を入力します。

例: interface 10

```

Nt Nt' Interface Slot-Port Self-Test Self-Test Maintenance
10 10 V.25/0 Slot: 4 Port: 0 Passed Failed Failed
V.25bis Base Net MAC/data-link on EIA 232E/V.24 interface

Adapter cable: RS-232 DTE

V.24 circuit: 105 106 107 108 109 125
Nicknames: RTS CTS DSR DTR DCD RI
RS-232: CA CB CC CD CF CE
State: OFF OFF OFF ON OFF OFF

Line speed: 19.200 Kbps
Last port reset: 55 minutes, 1 second ago

Input frame errors:
CRC error 6 alignment (byte length) 0
missed frame 1 too long (> 2054 bytes) 0
aborted frame 34 DMA/FIFO overrun 0
Output frame counters:
DMA/FIFO underrun errors 0 Output aborts sent 0

```

ダイヤル回線の以下の統計を表示するには、**interface** コマンドに続けてダイヤル回線のインターフェース番号を入力します。

例:

```

interface 29
Nt Nt' Interface Self-Test Self-Test Maintenance
29 10 PPP/20 Passed Failed Failed
Point to Point MAC/data-link on V.25bis Dial Circuit interface

```

V.25bis 動作コマンド

以下のリストは、シリアル・ライン・インターフェースとダイヤル回線の両方の出力を説明しています。

Nt シリアル・ライン・インターフェース番号またはダイヤル回線インターフェース番号

Nt' “Nt” がダイヤル回線の場合、これはダイヤル回線がマップされる V.25bis シリアル・ライン・インターフェースの番号です。

Interface

インターフェース・タイプとそのインスタンス番号

Slot V.25bis を稼働しているインターフェースのスロット番号

Port V.25bis を実行しているインターフェースのポート番号

Self-Test Passed

成功した自己テストの回数

Self-Test Failed

失敗した自己テストの回数

Maintenance: Failed

保守障害の数

Adapter cable:

使用されているアダプター・ケーブルのタイプ

V.24 circuit:

V.24 仕様で識別された回線番号

RS-232

回線の EIA 232 (RS-232 と呼ばれる) 名

State 回線の現在の状態 (ON または OFF)

Line speed

送信クロック速度 (概略値)

Last port reset

ポートがリセットされた後の経過時間

Input frame errors:

CRC error

チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment (byte length)

長さが 8 の偶数倍でないために廃棄された受信パケットの数

Missed Frame

フレームが装置に到着したときに利用可能なバッファがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

too long (> nnnn bytes)

構成されたフレーム・サイズより大きかったために廃棄された受信パケットの数

DMA/FIFO overrun

シリアル・インターフェース・カードがシステム・パケット・バッファ・メモリーにデータを送信する速度が遅かったために、ネットワークからデータを受信できなかった回数

L & F bits not set

シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファが完全なフレームを受け入れたことを示します。いずれかのビットがセットされていない場合、パケットは廃棄され、L & F bits not set カウンターが増分され、バッファは消去されて再利用できるようになります。

注: L & F bits not set カウンターはトラフィックによる影響は受けません。

aborted frame

送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

Output frame counters:**DMA/FIFO underrun errors**

シリアル・インターフェース・カードがシステム・パケット・バッファ・メモリーからデータを取り出す速度が遅かったために、パケットをネットワーク上に送信できなかった回数

Output aborts sent

高位レベルのソフトウェアの要求によって打ち切られた伝送の数

V.25bis 動作コマンド

第41章 V.34 ネットワーク・インターフェースの使用

V.34 インターフェースでは、ルーターが、標準 AT コマンド・セットをサポートする外付けのモデムを使用して、専用回線または交換電話回線を介してシリアル・コネクションを確立できるようにします。この章では、V.34 インターフェースの使用法について説明します。本章には、以下の節が含まれています。

- 『始める前に』
- 『構成手順』

注:

1. あて先名を**コネクション・リスト**に割り当て、あて先番号をリスト内の各回線に割り当てることができます。あて先名がコールされると、接続されるまで、またはリストが尽きるまで、リスト内の番号が 1 つずつ試されます。
2. V.34 は、統合 WAN ポート、4 ポート・アナログ・モデム・アダプター、および 4 ポート WAN アダプター上でサポートされます。

始める前に

IBM 2210 は専用回線モードまたは交換回線モードで動作します。交換回線モードを使用している場合は、Hayes AT コマンド・セットをサポートする非同期モデムがあるか確認してください。また、各モデムの最大 DTE 速度も知っている必要があります。

構成手順

この節では、ルーターを V.34 用に構成する方法について説明します。必要な作業には、次のものが含まれます。

1. V.34 アドレスを追加する。
2. V.34 パラメーターを構成する。
3. ダイヤル回線を追加する。
4. ダイヤル回線を構成する。

注: V.34 構成の変更を有効にするためには、ルーターをリスタートする必要があります。

V.34 アドレスの追加

V.34 インターフェースを初めて構成すると、デフォルトの V.34 アドレスが生成されます (『default_address』と呼ばれます)。V.34 インターフェース上に構成されたダイヤル回線は、デフォルトでは同じアドレスになるので、V.34 アドレスを変更せずに、いくつかのダイヤルイン・アプリケーションを実行することができます。

ダイヤルアウト・アプリケーションを使用する予定の場合は、V.34 アドレスを追加する (または、default_address を変更する) 必要があります。V.34 アドレスには、以下のものが含まれています。

V.34 の使用

- アドレス名。アドレス名は、アドレスの記述です。最大 23 字までの印刷可能 ASCII 文字列を使用できます。
- ネットワーク・ダイヤル・アドレス。ローカル・ポートまたは先ポートの電話番号です。最大 31 文字までの、接続されたモデムの有効なダイヤル文字を入力できます。

注: CCITT によって定義され、IBM 2210 によってサポートされている電話番号の有効な文字セットには、以下が含まれます。

- 10 進数の 0 ~ 9
- コロン (:) - "待機トーン"
- 左かぎ括弧 (<) - "ポーズ"、数字シーケンス間に一定の遅延 (モデムによって異なる) を挿入するのに使用されます。たとえば、PBX または PTN を通ずる場合などに使用します。
- 等号 (=) - "区切り記号 3"、これは "国内用" です。(モデムのマニュアルを参照してください。)
- 文字 P - "パルス方式でダイヤルを継続" (一部のモデムではサポートされません。)
- 文字 T - "パルス方式でダイヤルを継続" (一部のモデムではサポートされません。)

V.34 アドレスはインターフェース特有ではないので、Config> プロンプトから追加します。たとえば、次のように入力します。

```
Config>add v34-address
Assign address name [1-23] chars []? remote-site-baltimore
Assign network dial address [1-20 digits][]? 1-909-555-1234
```

V.34 インターフェースの構成

この節では、V.34 インターフェースの構成方法について説明します。構成は、次のように行います。

1. V.34 用のシリアル・ライン・インターフェースを設定するために、シリアル・ライン・インターフェースのデータ・リンク・プロトコルを設定する。Config> プロンプトから **set data-link v34** コマンドを使用します。たとえば、次のように入力します。

```
Config> set data-link v34
Interface Number [0]? 2
```

2. **network** コマンドに続けてインターフェースの番号を入力して、V.34 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>network 2
V.34 Data Link Configuration
V34 System Net Config 2>
```

Config プロンプトで **list devices** コマンドを使用すると、ルーター上に構成されているインターフェース番号のリストを表示することができます。

3. **set local-address** コマンドを使用して、ローカル・ポートのネットワーク・アドレス名を指定する。**add v34-address** コマンドを使用して定義したアドレス名の 1 つを入力する必要があります。たとえば、次のように入力します。

```
V34 System Net Config 2>set local-address
Local network address name []? remote-site-baltimore
```


注: 構成変更を有効にするためには、ルーターをリスタートする必要があります。

オプションの V.34 パラメーター

以下のものは、ユーザーが設定することができるオプションの V.34 パラメーターです。これらのコマンドについては、699ページの『V.34 構成コマンド』で詳しく説明しています。

- V.34 インターフェースでは、ルーターが専用回線または交換電話回線を介してシリアル・コネクションを確立できるようにします。専用回線モードは、1 つのあて先に専用の通信回線を使用します。交換回線モードでは、他の装置をコールすることができ、1 つのあて先に専用ではありません。
- アクセス不能なアドレスまたはコールを拒否するアドレスへの連続コール回数を制限することができます。これを行うには、**set retries-no-answer** および **set timeout-no-answer** コマンドを使用します。
- **set disconnect-timeout** コマンドは、ルーターが前回のコールからの信号を除去した後、コールを開始するまでに待つ時間を制御します。
- **set command-delay-timeout** コマンドは、ルーターが DTR をオンにした後、コールするかコールに応答するまでに待つ時間を制御します。
- **set connect-timeout** は、コールを設定するのに許容される秒数を指定します。
- **speed** コマンドは、モデムの最大 DTE 速度を設定します。
- **modem-init-string** コマンドは、ユーザーの要件または外部機器の要件を組み込むことによって、モデムの構成に柔軟性をもたせることができます。
- インターフェースの構成を終了したら、**list** コマンドを使用して、構成を表示してみることができます。

ダイヤル回線の追加

ダイヤル回線は、V.34 シリアル・ライン・インターフェースにマップされます。複数のダイヤル回線を 1 つのシリアル・ライン・インターフェースにマップすることも可能です。

V.34 インターフェースは、複数のタイプのダイヤル回線をサポートします。ダイヤル回線を追加するには、Config> プロンプトから以下のコマンドを使用します。

- **add device dial-circuit**

ソフトウェアが、各回線にインターフェース番号を割り当てます。この番号を使用して、ダイヤル回線を構成します。

例:

```
Config> add device dial-circuit
Adding device as interface 6
```

注: ダイヤル回線は、デフォルトではポイント・ポイント・プロトコル (PPP) になります。**set data-link** コマンドを使用すれば、ダイヤル回線のデータ・リンクをフレーム・リレーに設定することも可能ですが、V.34 上では PPP ダイヤル回線しかサポートされません。

ダイヤル回線の構成

この節では、ダイヤル回線の構成方法について説明します。ダイヤル回線コマンドの詳しい説明は、743ページの『第45章 ダイヤル回線の構成および監視』を参照してください。ダイヤル回線を構成するには、次のようにします。

1. **network** コマンドに続けてダイヤル回線のインターフェース番号を入力して、Circuit Config プロンプトを表示する。Config プロンプトで **list devices** コマンドを使用すると、追加したダイヤル回線のリストを表示することができます。たとえば、次のように入力します。

```
Config>network 6
Circuit configuration
Circuit Config>
```

2. ダイヤル回線を V.34 インターフェースにマップする。基本ネット (base net) は V.34 インターフェース番号です。たとえば、次のように入力します。

```
Circuit Config>set net
Base net for this circuit [0]? 0
```

3. ダイヤル回線を接続するリモート・ルーターのアドレス名を指定する。
add v34-address コマンドを使用して定義した名前の 1 つを入力する必要があります。たとえば、次のように入力します。

```
Circuit Config>set destination
Assign destination address name []? newyork
```

4. ダイヤル回線をアウトバウンド・コール発信専用、インバウンド・コール受信専用、またはコールの発信と受信の両方として構成する。

set calls コマンドを使用します。リンクの両側が同時にコール設定を試みた場合に競合を避けるために、リンクの一方の端のダイヤル回線はインバウンド・コール受信専用構成し、リンクの他方の端のダイヤル回線はアウトバウンド・コール発信専用構成します。たとえば、次のように入力します。

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

注: WAN 復元動作または別のダイヤル・オンデマンド・アプリケーションの場合、回線をインバウンド・コール用またはアウトバウンド・コール用のいずれかに設定することが必要です。

5. 回線のタイムアウト期間を指定する。

set idle コマンドを使用します。この指定された期間、回線上にトラフィックがないと、ダイヤル回線はハングアップします。回線を専用回線として構成する場合は、アイドル・タイマーをゼロに設定します。回線をダイヤル・オンデマンドに構成する場合は、アイドル・タイマーをゼロ以外の値に設定します。範囲は 0 ~ 65535 で、デフォルトは 60 秒です。たとえば、次のように入力します。

```
Circuit Config>set idle
Idle timer (seconds, 0 means always active) [60]? 0
```

注: WAN 復元動作の場合、アイドル・タイムを 0 に設定する必要があります。

6. オプションで、コール設定と初期パケット送信の間の時間を遅らせることができます。

set selftest-delay コマンドを使用します。自己テスト遅延を設定すると、初期パケットが廃棄されるのを防止できます。モデムが同期のために余分な時間が必要な場合は、この遅延を調整します。たとえば、次のように入力します。

```
Circuit Config>set selftest-delay  
Selftest delay(milli-seconds,0 means no delay)[150]?200
```

7. インバウンド・アドレス名を設定する。

set inbound コマンドを使用します。このコマンドを使用する必要があるのは、回線がインバウンド・コールとアウトバウンド・コールの両方に設定されており、ルーターのあて先アドレスが、リモート・ルーターがダイヤルするあて先アドレスと異なっている場合だけです。たとえば、ルーターの 1 つが PBX、国際、または LATA 間交換局を通す必要がある場合は、番号が異なることになります。たとえば、次のように入力します。

```
Circuit Config>set inbound  
Assign destination inbound address name []? newyork
```

インバウンド・アドレス名は、**add v34-address** コマンドを使用して定義した名前の 1 つに一致していることが必要です。

8. オプションとして、ダイヤル回線上で実行されているデータ・リンク・レイヤー・プロトコル (PPP またはフレーム・リレー) の構成プロセスに入ることができます。**encapsulator** コマンドを使用します。たとえば、次のように入力します。

```
Circuit Config>encapsulator
```

V.34 の使用

第42章 V.34 ネットワーク・インターフェースの構成および監視

この章では、V.34 構成コマンドとオペレーショナル・コマンド、および GWCON コマンドについて説明します。本章には、以下の節が含まれています。

- 『インターフェース構成プロセスへのアクセス』
- 『V.34 構成コマンド』
- 703ページの『インターフェース監視プロセスへのアクセス』
- 704ページの『V.34 監視コマンド』
- 709ページの『V.34 と GWCON コマンド』

インターフェース構成プロセスへのアクセス

V.34 構成プロセスにアクセスするには、以下の手順を使用します。

1. OPCON プロンプトで、**talk** コマンドと CONFIG の PID を入力する。(このコマンドの詳細については、OPCON プロセスとは 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、コンソールに CONFIG プロンプト (Config) が表示されます。最初に **CONFIG** に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. CONFIG プロンプトで **list devices** コマンドを入力して、ルーターが現在構成されているネットワーク・インターフェース番号を表示する。
3. V.34 インターフェースは、『V.34 Base Net』としてリストされます。構成するインターフェースのインターフェース番号を記録してください。
4. CONFIG **network** コマンドと、構成するインターフェースの番号を入力する。たとえば、次のように入力します。

```
Config> network 1  
V.34 System Net Config >
```

これで、V.34 構成プロンプトがコンソールに表示されます。

V.34 構成コマンド

700ページの表95 にコマンドの要約を示し、この節の残りの部分で、個々の V.34 構成コマンドについて説明します。これらのコマンドを用いて、V.34 構成を表示、作成、または変更することができます。V.34 構成コマンドは V.34 Config> プロンプトで入力します。

V.34 の構成

表 95. V.34 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
List	V.34 構成を表示します。
Set	ローカル・アドレス、接続、切断、および無応答タイムアウト、無応答後の再試行回数、およびコマンド遅延タイムアウトを設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、現行の V.34 構成を表示するのに使用します。

構文:

list

交換回線モードの例:

```
list
      V.34 System Net Configuration:

Operating Mode           = Switched

Local Network Address Name = v403
Local Network Address    = 1-508-898-2403

Non-Responding addresses:
Retries                  = 1
Timeout                  = 0 seconds

Call timeouts:
Command Delay            = 0 ms
Connect                  = 60 seconds
Disconnect                = 2 seconds

Modem strings:
Initialization string    = AT&S1L1&D2&C1X3

Speed (bps)              = 115200
```

専用回線モードの例:

```
list
      V.34 System Net Configuration:

Operating Mode           = Leased

Call timeouts:
Connect                  = 60 seconds
Disconnect                = 2 seconds

Speed (bps)              = 115200
```

Operating Mode

インターフェースが交換回線モードまたは専用回線モードのどちらかを指定します。

Local Network Address Name:

ローカル・ポートのネットワーク・アドレス名を表示します。

Local Network Address:

ローカル・ポートのネットワーク・ダイヤル・アドレスを表示します。

Non-responding addresses:**Retries**

タイムアウト期間中に無応答アドレスに対してルーターが試みるコールの最大数

Timeout

ルーターは、無応答アドレスへの試行の最大数に達した場合、この時間が満了するまでコール設定を試行しません。このタイムアウト期間は、ルーターが最初のコールを試みた時点で開始します。

Call timeouts:

呼のタイムアウトの回数

Command Delay

ルーターが DTR (データ端末レディー) をオンにした後、コールするかコールに応答するまでに待つ時間 (ミリ秒)。このパラメーターを 0 に設定した場合、モデムが CTS (送信可) 信号で DTR に応答するのを待ってから、ルーターはコマンドを出します。

Connect

コールを設定するのに許容される秒数。このパラメーターが 0 に設定されている場合、モデムがコール設定タイムアウトを制御します。

Disconnect

ルーターは DTR を除去した後、この時間だけ待ってから、次のコールを開始します。このパラメーターを 0 に設定すると、モデムが CTS および DSR を除去することによって DTR 除去に応答するのを待ってから、ルーターは次のコールを開始します。

Modem strings:

接続されたモデムに送信されるコマンド文字列

Initialization string

これは初期化時 (コールが受け入れまたは試行される前) にモデムに送信される最後の AT コマンド文字列です。ほとんどのモデムに適用されるデフォルト文字列が提供されています。

注: 3Com/U.S. Robotics によって製造されたモデムの場合、初期化文字列を AT&S1L1&D2&C1X3&B1&H1&R2 に変更する必要があります。

Speed (bps)

これは DTE 速度です。ほとんどのモデムではデフォルト値を適用できますが、場合によっては、正しく動作させるために速度を低く設定したり、モデムがサポートする最大データ速度を達成するために高く設定したりすることが必要になることがあります。

Set

set コマンドは、ローカル・アドレス、コールのタイムアウトと遅延、無応答アドレスの再試行とタイムアウト、および HDLC ケーブル・タイプを構成するのに使用します。

V.34 の構成

構文:

```
set command-delay timeout . . . (交換回線モードのみ)
      connect-timeout . . .
      disconnect-timeout . . .
      speed . . .
      local-address . . . (交換回線モードのみ)
      mode . . .
      modem-init-string . . . (交換回線モードのみ)
      retries-no-answer . . . (交換回線モードのみ)
      timeout-no-answer . . .
```

注: V.34 インターフェースを専用回線モードで構成している場合は、以下のパラメータは構成できません。

- **command-delay-timeout**
- **local-address** *address*
- **local-address** *name*
- **modem-init-string**
- **retries-no-answer**

command-delay-timeout # of milliseconds

ルーターは DTR (データ端末レディー) をオンにした後、この時間だけ待ってから、コールを開始したり、コールに回答したりします。このパラメーターを 0 に設定した場合、モデムが CTS (送信可) 信号で DTR に回答するのを待ってから、ルーターはコマンドを出します。範囲は 0 ~ 65535 ミリ秒で、デフォルトは 0 です。

connect-timeout # of seconds

コールを設定するのに許容される秒数を設定します。範囲は 0 ~ 65535 秒で、デフォルトは 60 です。このパラメーターを 0 に設定すると、モデムがコネクション・タイムアウトを制御します。最初にこのパラメーターを 0 に設定し、次に ELS イベント V34B.027 を使用して、種々のあて先に接続を確立するための所要時間を調べる必要があります。その後で、このパラメーターを、最長接続時間よりわずかに高い値に設定します。

注: 通常は政府規制により、モデム製造業者はコール設定を最大長にするように制限されています。この値は単に最適化のためのものであり、一部の DSU との相互運用では、このパラメーターを変更することが必要になる場合があります。

disconnect-timeout # of seconds

ルーターが DTR を除去後、次のコールを開始する前に待機する時間 (秒) を指定します。範囲は 0 ~ 65535 秒で、デフォルト値は 2 です。このパラメーターを 0 に設定した場合、モデムが CTS および DSR を除去して DTR 除去に回答するのを待ってから、ルーターはコマンドを出します。

speed # bits per second

モデムの DTE 速度をビット / 秒で指定します。モデムがサポートする最大

速度を使用することが必要です。ただし、モデムによってはサポートされる速度が正しく自動選択されない場合もあります。問題が生じる懸念がある場合は、速度を下げてください。

local-address *address name*

ローカル・ポートのネットワーク・ダイヤル・アドレスを表示します。このアドレス名は、Config> で **add v34-address** コマンドを使用して定義した名前の 1 つに一致している必要があります。

mode インターフェイスが交換回線インターフェイスまたは専用回線インターフェイスのどちらとして構成されているか指定します。

注: **set mode** コマンドを使用して、*switched* の値と *leased* の値の間で切り替えることができます。

モードを *switched* の値に設定した場合、このパラメーターは **mode-leased** として表示され、モードを *leased* に変更するのに使用することができます。

モードを *leased* の値に設定した場合、このパラメーターは **mode-switched** として表示され、モードを *switched* に変更するのに使用することができます。

デフォルト値: Switched

modem-init-string *value*

これは、正常に行われたインターフェイスの初期化の最後にモデムに送信される AT コマンド文字列です。これを使用して、ユーザーのアプリケーションに適合するようにモデムのパラメーターを調整することができます。

retries-no-answer *value*

一部の電話サービス提供者は、自動リコール装置に対して、アクセス不能アドレスまたは自動リコールを拒否するアドレスへの連続コール回数を制限しています。このパラメーターは、ルーターがタイムアウト期間中に無応答アドレスに対して試行するコールの最大数を指定します。範囲は 0 ~ 10 で、デフォルトは 1 です。

注: 政府規制により、モデム製造業者がこのパラメーターを変更するのを制限している場合もあります。

timeout-no-answer *# of seconds*

ルーターは、無応答アドレスへの **retries-no-answer** の最大数に達した場合、この時間が満了するまで、次のコールを開始しません。このタイムアウト期間は、あるアドレスにルーターが最初のコールを試みた時点で開始します。範囲は 0 ~ 65535 秒で、デフォルトは 0 です。このパラメーターを 0 に設定すると、モデムがタイムアウト期間を制御します。

インターフェイス監視プロセスへのアクセス

V.34 のインターフェイ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。

+ network #

V.34 の構成

ただし、# は、V.34 インターフェースの番号です。ダイヤル回線の V.34 監視プロセスには直接アクセスできませんが、シリアル・ライン・インターフェースにマップされたダイヤル回線を監視することができます。

注: V.34 インターフェースには、V.34 関連のアクティビティを監視するのに使用できる ELS トラブルシューティング・メッセージもあります。詳細については、*IBM Nways イベント・ログ・システム・メッセージの手引き* を参照してください。

V.34 監視コマンド

この節では、V.34 監視コマンドの要約を示し、個々のコマンドについて説明します。これらのコマンドを用いて、V.34 インターフェースのコール、回線、パラメーター、および統計を見ることができます。

V.34 監視コマンドは V.34> プロンプトで入力します。表96 は、コマンドを示しています。

表 96. V.34 監視コマンドの要約

監視コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Calls	前回にルーター上の統計がリセットされた以降に、このインターフェースにマップされた各ダイヤル回線に行われた、完了した接続および試行された接続の数をリストします。
Circuits	V.34 インターフェース上に構成されたすべてのデータ回線の状態を示します。
Reset	接続を切断し、インターフェースをリセットします。
Parameters	V.34 インターフェースの現行パラメーターを表示します。(このコマンドは、インターフェース構成 "list" コマンドと同じ情報を表示します。)
Statistics	V.34 インターフェースの現行統計を表示します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Calls

calls コマンドは、前回にルーター上の統計がリセットされた以降に、このインターフェースにマップされた各ダイヤル回線で行われた、完了した接続および試行された接続の数をリストするのに使用します。

構文:

calls

例:

```
calls
Net Interface Site Name           In   Out  Rfsd  Blckd
1   PPP/0     v403                2    0    0     0
```

Unmapped connection indications: 0

Net このインターフェースにマップされたダイヤル回線の数

Interface

インターフェースのタイプとそのインスタンス番号

Site Name

ダイヤル回線のネットワーク・アドレス名

In このダイヤル回線で受け入れられたインバウンド接続の数

Out このダイヤル回線によって開始され、完了した接続の数

Rfsd このダイヤル回線によって開始されたが、ネットワークまたはリモート着信ポートによって拒否された接続の数

Blckd ルーターがブロックした接続試行の数。ルーターが接続試行をブロックするのは、ローカル・ポートがすでに使用されている場合、無応答アドレスへの再試行の最大数に達している場合、またはモデムが応答していない場合です。

Unmapped connection indications:

着信コールを受け入れるように構成されている使用可能なダイヤル回線がないために、ルーターによって拒否された接続試行の数

Circuits

circuits コマンドは、V.34 ポートに構成されているすべてのダイヤル回線の状態を示します。

構文:

circuits

例:

```

circuit
Net Interface  MAC/Data-Link  State  Reason  Duration
2  PPP/0      Point to Point  Avail  Rmt Disc  1:02:25

```

Net このインターフェースにマップされたダイヤル回線の数

Interface

インターフェースのタイプとそのインスタンス番号

MAC/DataLink

このダイヤル回線に構成されたデータ・リンク・プロトコルのタイプ

State ダイヤル回線の現行状態

Up - 現在接続されています。

Available - 現在は接続されていませんが、利用可能です。

Disabled - ダイヤル回線は使用不可にされました。

Down - ダイヤル回線がビジーであるか、リンク・レイヤー・プロトコルがダウンしているために、接続に失敗しました。

Reason

現行状態の理由:

nnn_Data - (nnn はプロトコルの名前) プロトコルに送信するデータがあったので、回線は Up です。

V.34 の構成

Remote Disconnect - リモートあて先がコールを切断したので、回線は Down または Available のいずれかです。

Operator Request - 前回のコールが監視コマンドによって切断されたので、回線は Available です。

Inbound - 回線がインバウンド・コールに応答したので、回線は Up です。

Restoral - WAN 復元動作のため、回線は Up です。

Self Test - 回線は静的として構成されており (アイドル・タイム = 0)、使用可能にされたときに正常に接続されました。

Duration

回線が現行状態にある時間の長さ

Parameters

parameters コマンドは、現行の V.34 シリアル・ライン構成を表示するのに使用します。これは、V.34 Config> list コマンドで表示される情報と同じです。

構文:

parameters

例:

```
parameters
  V.34 port Parameters

Local Network Address Name   = v402
Local Network Address       = 1-508-898-2402

Non-Responding addresses:
Retries                      = 1
Timeout                      = 0 seconds

Call timeouts:
Command Delay                = 0 ms
Connect                     = 0 seconds
Disconnect                   = 0 seconds

Modem strings:
Initialization string       = AT&S1L1&D2&C1X3
```

Local Network Address Name:

ローカル・ポートのネットワーク・アドレス名

Local Network Address:

ローカル・ポートのネットワーク・ダイヤル・アドレス

Non-responding addresses:

Retries

タイムアウト期間中に無応答アドレスに対してルーターが試みるコールの最大数

Timeout

ルーターは、無応答アドレスへの試行の最大数に達した場合、この時間が満了するまでコール設定を試行しません。このタイムアウト期間は、あるアドレスにルーターが最初のコールを試みた時点で開始します。

Call timeouts:

Command Delay

ルーターが DTR (データ端末レディー) をオンにした後、コールするかコールに応答するまでに待つ時間 (ミリ秒)。このパラメーターを 0 に設定した場合、モデムが CTS (送信可) 信号で DTR に応答するのを待ってから、ルーターはコマンドを出します。

Connect

コールを設定するのに許容される秒数。このパラメーターが 0 に設定されている場合、モデムがコール設定タイムアウトを制御します。

Disconnect

ルーターは DTR を除去した後、この時間だけ待ってから、次のコールを開始します。このパラメーターを 0 に設定すると、モデムが CTS および DSR を除去することによって DTR 除去に応答するのを待ってから、ルーターは次のコールを開始します。

Statistics

statistics コマンドは、この V.34 インターフェースの現行統計を表示するのに使用します。

構文:**statistics****例:**

```
statistics
  V.34 port Statistics
  Adapter cable:          RS-232 DTE

  V.24 circuit: 105 106 107 108 109 125 141

  Nicknames:   RTS CTS DSR DTR DCD RI
  RS-232       CA CB CC CD CF CE
  State:       OFF OFF OFF OFF OFF OFF
  Line speed:   115.200 Kbps
  Last port reset: 24 seconds ago

  Input frame errors:
  CRC error           0  alignment (byte length)  0
  missed frame        0  too long (> 2182 bytes)  0
  aborted frame       0  DMA/FIFO overrun      0
  L & F bits not set  0

  Output frame counters:
  DMA/FIFO underrun errors  0  Output aborts sent  0
```

Adapter cable:

使用されているアダプター・ケーブルのタイプ

Nicknames:

回線の通称名

RS-232

回線の EIA 232 (RS-232 と呼ばれる) 名

State: 回線の現在の状態: ON、OFF、または "---" (これは、このタイプのインターフェースの状態は未定義であることを意味します。)

V.34 の構成

Line speed:

送信クロック速度 (概略値)

Last port reset:

ポートがリセットされた後の経過時間

Input frame errors:

CRC error

チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment (byte length)

長さが 8 の偶数倍でないために廃棄された受信パケットの数

Missed Frame

フレームが装置に到着したときに利用可能なバッファがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンタを増分します。

too long (> nnnn bytes)

構成されたフレーム・サイズ (nnnn) より大きかったために廃棄された受信パケットの数

aborted frame

送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

DMA/FIFO overrun

シリアル・インターフェース・カードがシステム・パケット・バッファ・メモリーにデータを送信する速度が遅かったために、ネットワークからデータを受信できなかった回数

L & F bits not set

シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファが完全なフレームを受け入れたことを示します。いずれかのビットがセットされていない場合、パケットは廃棄され、L & F bits not set カウンタが増分され、バッファは消去されて再利用できるようになります。

注: L & F bits not set カウンタはトラフィックによる影響は受けません。

Output frame counters:

DMA/FIFO underrun errors

シリアル・インターフェース・カードがシステム・パケット・バッファ・メモリーからデータを取り出す速度が遅かったために、パケットをネットワーク上に送信できなかった回数

Output aborts sent

高位レベルのソフトウェアの要求によって打ち切られた伝送の数

V.34 と GWCON コマンド

V.34 には独自の監視用の監視プロセスがありますが、GWCON 環境から `interface`、`statistics`、および `error` コマンドを使用すれば、ルーターも構成情報と、装置および回線の完全な統計を表示します。また、GWCON `test` コマンドを使用して、DCE および回線をテストすることもできます。

注: V.34 シリアル・インターフェースに対して `test` コマンドを出すと、現行の呼は除去され、再ダイヤルされます。

GWCON コマンドについての詳細は、149ページの『第8章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』を参照してください。

V.34 インターフェースおよびダイヤル回線の統計

V.34 シリアル・ライン・インターフェースおよびダイヤル回線の統計を表示するには、GWCON (+) プロンプトから `interface` コマンドを使用します。

V.34 シリアル・ライン・インターフェースの以下の統計を表示するには、`interface` コマンドに続けて V.34 シリアル・ライン・インターフェースのインターフェース番号を入力します。

例:

```
interface 10
```

Nt	Nt'	Interface	Slot-Port	Self-Test Passed	Self-Test Failed	Maintenance Failed
10	10	V.34/0	Slot: 4 Port: 0	1	0	0

```
V.34 Base Net MAC/data-link on EIA 232E/V.24 interface
Adapter cable:          RS-232 DTE
V.24 circuit: 105 106 107 108 109 125
Nicknames:   RTS CTS DSR DTR DCD RI
RS-232:      CA CB CC CD CF CE
State:       OFF OFF OFF ON  OFF OFF
Line speed:  115.200 Kbps
Last port reset: 55 minutes, 1 second ago
Input frame errors:
CRC error          6 alignment (byte length)          0
missed frame       1 too long (> 2054 bytes)          0
aborted frame     34 DMA/FIFO overrun              0
Output frame counters:
DMA/FIFO underrun errors  0 Output aborts sent          0
```

ダイヤル回線の以下の統計を表示するには、`interface` コマンドに続けてダイヤル回線のインターフェース番号を入力します。

例:

```
interface 29
```

Nt	Nt'	Interface	Self-Test Passed	Self-Test Failed	Maintenance Failed
29	10	PPP/20	2	1	0

```
Point to Point MAC/data-link on V.34 Dial Circuit interface
```

V.34 の構成

以下のリストは、シリアル・ライン・インターフェースとダイヤル回線の両方の出力を説明しています。

Nt シリアル・ライン・インターフェース番号またはダイヤル回線インターフェース番号

Nt' “Nt” がダイヤル回線の場合、これはダイヤル回線がマップされる V.34 シリアル・ライン・インターフェースの番号です。

Interface

インターフェース・タイプとそのインスタンス番号

Slot V.34 を稼働しているインターフェースのスロット番号

Port V.34 を実行しているインターフェースのポート番号

Self-Test Passed

成功した自己テストの回数

Self-Test Failed

失敗した自己テストの回数

Maintenance: Failed

保守障害の数

Adapter cable:

使用されているアダプター・ケーブルのタイプ

V.24 circuit:

V.24 仕様で識別された回線番号

RS-232

回線の EIA 232 (RS-232 と呼ばれる) 名

State 回線の現在の状態 (ON または OFF)

Line speed

送信クロック速度 (概略値)

Last port reset

ポートがリセットされた後の経過時間

Input frame errors:

CRC error

チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment (byte length)

長さが 8 の偶数倍でないために廃棄された受信パケットの数

Missed Frame

フレームが装置に到着したときに利用可能なバッファがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

too long (> nnnn bytes)

構成されたフレーム・サイズより大きかったために廃棄された受信パケットの数

DMA/FIFO overrun

シリアル・インターフェース・カードがシステム・パケット・バッファ・メモリーにデータを送信する速度が遅かったために、ネットワークからデータを受信できなかった回数

L & F bits not set

シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファが完全なフレームを受け入れたことを示します。いずれかのビットがセットされていない場合、パケットは廃棄され、L & F bits not set カウンターが増分され、バッファは消去されて再利用できるようになります。

注: L & F bits not set カウンターはトラフィックによる影響は受けません。

aborted frame

送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

Output frame counters:**DMA/FIFO underrun errors**

シリアル・インターフェース・カードがシステム・パケット・バッファ・メモリーからデータを取り出す速度が遅かったために、パケットをネットワーク上に送信できなかった回数

Output aborts sent

高位レベルのソフトウェアの要求によって打ち切られた伝送の数

V.34 の構成

第43章 ISDN インターフェースの使用

重要

元の0 2210 ISDN T1 および E1 単一ポート LIC (それぞれ、IBM PN 11J7466 または 78H6147 および 11J7465 または 78H6148) は、DIAL クライアント用に MAC アドレス割り当てをサポートしていません。この割り当てが必要なのは、固有に DIAL リモート LAN アクセス環境で NetBIOS または SNA プロトコルあるいはその両方を使用したいお客様だけです。他のすべての ISDN 機能および DIAL 機能 (たとえば、ダイヤルイン IP および IPX) は、アップグレードなしでも正しく働きます。新式の ISDN T1 および E1 単一ポート LIC は、DIAL クライアントおよびすべての DIAL 機能用に MAC アドレス割り当てをサポートしています。元の ISDN LIC を備えるお客様で、NetBIOS または SNA DIAL 機能あるいはその両方を使用したい方は、IBM サービス技術員に問い合わせる新式の LIC にアップグレードする必要があります。

この章では、IBM 2210 上のサービス総合デジタル網 (ISDN) インターフェースについて説明します。本章には、以下の節が含まれています。

- 『ISDN の概説』
- 717ページの『ISDN 原因符号』
- 719ページの『サンプル ISDN 構成』
- 720ページの『チャンネル化 T1/E1』
- 721ページの『ISDN インターフェースの要件と制約』
- 721ページの『始める前に』
- 722ページの『構成手順』
- 727ページの『I.431 スイッチの機種』

ISDN の概説

ISDN インターフェース・ソフトウェアにより、ルーター間、またはダイヤルイン・ユーザーからルーターへの ISDN 接続を確立することができます。インターフェースを設定して、専用リンクとして機能するようにすることができ、あるいは交換回線接続の開始および受信を行うようにすることもできます。これはオンデマンドで、リスタートから自動的に、あるいはオペレーターがコマンドを出して行うことができます。

I.430、I.431、およびチャンネル化 T1/E1 は、交換回線ではありません。これらは固定的な専用線タイプの接続です。

ISDN の使用

ISDN アダプターとインターフェース

IBM 2210 は、以下の ISDN-PRI アダプターをサポートします。

- 1 ポート・チャンネル化 E1 ISDN-PRI
- 1 ポート・チャンネル化 T1/J1 ISDN-PRI
- 4 ポート・チャンネル化 E1 ISDN-PRI
- 4 ポート・チャンネル化 T1/J1 ISDN-PRI

PRI/チャンネル化アダプターには CSU/DSU が内蔵されているので、外付けの CSU/DSU は必要ありません。

注: talk 6 を使用して BRI から PRI にアップグレードする場合は、最初に ISDN とダイヤル構成を消去し、その後で PRI を起動して、PRI を構成することが必要です。

- PRI アダプターは、マルチポイントをサポートしません。
- PRI アダプターは、T1/J1 および E1 サポートを提供します。
 - T1/J1 は、23 の 64-Kbps B チャンネルおよび 1 つの 64-Kbps D チャンネルをサポートします。
 - E1 は、30 の 64-Kbps B チャンネルおよび 1 つの 64-Kbps D チャンネルをサポートします。
- PRI アダプターは拡張回線 ID (LID) サポートを提供します。

ダイヤル回線

ダイヤル回線には 4 つのタイプがあります。

- 静的回線 (または、リンク)

注:

1. I.430、I.431、およびチャンネル化 T1/E1 は専用回線接続なので、ダイヤル回線ではありません。
 2. ISDN は、D チャンネルを介した X.25 トラフィックを静的回線と見なします。ただし、ダイヤル回線構成のもとで **encapsulator** コマンドを使用して、X.25 回線を PVC または SVC として構成することもできます。
- オンデマンドでダイヤルし、指定されたアイドル時間の後で切れる交換回線
 - 割り当てられた 1 次専用回線に障害が生じたときにのみ使用される WAN 復元回線
 - ダイヤルイン回線は、リモート・クライアントにネットワーク上の資源へのアクセスを提供するために使用されます。

ダイヤル・オンデマンド・インターフェースを介してブリッジングするときは、スパンニング・ツリーを使用不可にし、MAC フィルターを作成して、すべての不要なトラフィックを除去することをお勧めします。(MAC フィルターは、特定の MAC アドレスをあて先に指定していないすべてのフレームを廃棄します。) これにより、不要なトラフィックのためにダイヤル回線が接続されたままになるのを防止することができます。

注: FR ダイアル・オンデマンド・インターフェース上で BAN トラフィックを行う場合は、MAC フィルターを追加する必要はありません。BAN ソフトウェアは常にフィルターを適用することにより、ダイアル・オンデマンド回線をハングアップさせないブリッジング・トラフィックは、あて先 MAC アドレスが BAN DLCI MAC アドレスに一致するトラフィックだけになるようにします。

可能な各あて先ごとにダイアル回線を追加します。複数のダイアル回線を 1 つの ISDN インターフェースにマップすることも可能です。各ダイアル回線は、ポイント・ポイント・プロトコル (PPP)、フレーム・リレー、または X.25 (D チャネルのみ) を実行する、通常のシリアル・ライン・ネットワークです。これらのプロトコルは、ダイアル回線を介して動作するように構成されています。

注: あて先の名前を **コネクション・リスト** に割り当て (add ISDN address)、あて先の番号をリスト内の各回線に割り当てることができます。あて先名がコールされると、接続されるまで、またはリストが尽きるまで、リスト内の番号が 1 つずつ試されます。

ルート可能プロトコルおよびブリッジング・フィーチャーとルーティング・フィーチャーは、ISDN インターフェースと直接通信することはできません。これらのプロトコルはダイアル回線上で実行するように構成する必要があります。この実現では、以下の ISDN ダイアル回線のプロトコルおよびフィーチャーをサポートします。

- APPN
- Banyan VINES
- DECnet
- DLSw
- IP
- IPX
- IPv6
- AppleTalk 2
- ブリッジング (SRB、STP、SR-TB、および SRT)
- 帯域幅予約
- WAN 復元
- DIALS

アドレッシング

ISDN でコールを発信するには、あて先の電話番号を指定します。ユーザー自身をスイッチに識別するためには、ユーザー自身の電話番号を指定する必要があります。ISDN の場合、電話番号はコールされる側ネットワーク・ダイアル・アドレスであり、便宜上、ネットワーク・アドレス名と呼ばれる名前 (電話番号を表す) が付けられています。

ISDN インターフェースの設定時に、可能な各あて先のアドレスとユーザー自身の電話番号 (ローカル・ネットワーク・アドレスと呼ばれる) を追加します。ダイアル回線を構成するときには、ローカル・ネットワーク・アドレスを物理インターフェース構成から入手して、その回線のあて先アドレスを設定します。

過剰加入および回線の競合

ISDN PRI T1/J1 インターフェースは最大 23 のアクティブ・コールをサポートし、ISDN PRI E1 インターフェースは最大 30 のアクティブ・コールをサポートします。ISDN インターフェース上には、サポートされているアクティブ・コール数よりも多くのダイヤル回線を構成することができます。これは過剰加入 (oversubscribing) と呼ばれます。ISDN インターフェースのすべてのコールがアクティブのときに、あるダイヤル回線がコールを試みた場合は、2 通りの可能性があります。1) そのダイヤル回線の優先順位が、アクティブ・コールをもつ回線より高い場合、低い優先順位のダイヤル回線のアクティブ・コールは打ち切られ、高い優先順位をもつダイヤル回線のコールが試みられます。2) そのダイヤル回線の優先順位が、アクティブ・コールをもついずれのダイヤル回線の優先順位よりも高くない場合、コールは行われません。ルーターは、ISDN あて先に接続できないダイヤル回線上のプロトコルによって送信されたパケットを廃棄します。

注: D チャンネルを介して X.25 通信を行っている場合、D チャンネルは常に X.25 接続に利用可能なので、回線の競合は起こりません。

優先順位についての詳細は、747ページの『Set』を参照してください。

デマンド回線を介したコスト制御

プロトコルから見ると、ダイヤル・オンデマンド回線は常にアップ状態に見えます。ほとんどのプロトコルは定期的にルーティング情報を送信し、ルーターはルーティング情報が送信されるたびに、ダイヤル・オンデマンド回線を介してダイヤルすることになります。定期的なルーティング更新を制限するには、IP と OSI が静的ルートのみを使用するように構成し、ダイヤル回線を介するルーティング・プロトコル (RIP、OSPF) を使用不可にします。IPX を使用している場合は、静的ルートとサービスを構成して、ダイヤル回線を介するルーティング・プロトコル (RIP、SAP) を使用不可にします。もう 1 つの選択肢は、RIP と SAP の更新間隔を低い頻度に構成することです。ただし、この場合、ルーティング情報が変更されたときに、RIP と SAP がその変更を同報通信するのを防止することはできません。また、IPX キープアライブ・フィルターも使用可能にしておく必要があります。これにより、KEEPALIVE パケットやシリアル化パケットが連続的にダイヤル・オンデマンド・リンクを起動するのを防止することができます。

コーラー ID および LID

ISDN サービスが、ISDN コール設定メッセージの中で発信側番号 (CPN) を提供することで ANI または CallerID (CLID) を提供する場合、それを使用して、ダイヤル回線を該当する発信者に突き合わせるすることができます。そうでない場合は、所有回線識別プロトコル (LID) を使用するか、“ANY INBOUND”である回線を提供する必要があります。

LID プロトコルは、ダイヤル回線構成のインバウンドあて先、およびコーリング・ダイヤル回線を受信ダイヤル回線に突き合わせるために受信された LID を使用します。LID プロトコルは、コーラーが開始し、受信者が応答する、短い識別プロトコルで

す。any_inbound ダイヤル回線が構成されないときは、コーラーが LID メッセージを提供しない場合、受信者はコールをリジェクトすることができます。LID 交換は、B チャンネル上で行なわれます。

論理 ID (LID) をサポートしないルートに接続する場合は、個々のダイヤル回線構成で構成オプションを使用して、LID 交換を抑制することができます。

```
config> set lid_used no
```

着信側で lid_used=no の場合、コールは完了し、IBM 2210 は、LID が B チャンネルに到着するのを待ちません。その代わりに、IBM 2210 は受信した callerID を使用することを試みます。callerID に一致するものがない場合、IBM 2210 は any_inbound ダイヤル回線が使用可能かどうかを検査します。any_inbound 回線が使用できない場合、コールはリジェクトされます。

発信側では、PPP/FR 自己テストは、B チャンネルが割り振られた後、即時に開始されます。

ISDN 原因符号

この ISDN インプリメンテーションでは、ルーターが ISDN インターフェースを介して接続の確立を試みるのを停止させる原因符号を指定しています。アプリケーションが再試行されると、ルーターは再びこのインターフェースを介して接続の確立を試み、元の問題が解決されていれば、その試みは成功します。再試行中にルーターが同じ原因符号を検出した場合、アプリケーションはそれ以上、このインターフェースを介して接続処理を試みません。

原因符号は、次のように解釈します。

1. cause0 が "0x5" でないときは、原因符号を無視する。
2. cause0 が "0x5" のときは、cause1 を見る。cause1 の高位 (最上位) ビットが ON のときは、それを OFF にセットする。
3. 結果を 10 進数に変換し、下表 (ITU-T 勧告 Q.850 から抜粋) で意味を調べる。

表 97. ISDN Q.931 原因符号

符号	原因
1	未割り当て (割り当てられていない番号)
2	指定された中継ネットワークへのルートなし
3	あて先へのルートなし
6	チャンネル受付不可
7	コール受付、確立チャンネルで呼出通知中
16	通常のコール切断
17	ユーザー・ビジー
18	ユーザー応答なし
19	相手ユーザー応答なし (ユーザー呼出中)
21	コール・リジェクト
22	相手端末番号変更
26	非選択ユーザー切断
27	相手端末故障

表 97. ISDN Q.931 原因符号 (続き)

符号	原因
28	無効番号フォーマット (アドレス不完了)
29	ファシリティ拒否
30	状態照会 (STATUS ENQUIRY) への応答
31	正常、未指定
34	回線/チャンネル利用不可
38	ネットワーク障害
41	一時障害
42	スイッチ輻輳 (ふくそう)
43	アクセス情報廃棄
44	要求回線/チャンネル利用不可
47	リソース利用不可、未指定
49	サービス品質利用不可
50	要求ファシリティ未登録
57	伝達能力不許可
58	現在伝達能力不許可
63	サービスまたはオプション利用不可、未指定
65	伝達能力未定義
66	未提供チャンネル・タイプ指定
69	要求ファシリティ未定義
70	限定デジタル情報伝達能力のみ利用可
79	サービスまたはオプション未定義、未指定
81	無効コール番号値
82	識別チャンネル未定義
83	コール中断あり、ただしこのコール識別ではない
84	コール識別使用中
85	コール中断なし
86	要求されたコール識別のコールが切断された
88	端末属性不一致
91	無効中継ネットワーク選択
95	無効メッセージ、未指定
96	必須情報要素不足
97	メッセージ種別未定義
98	コール状態とメッセージ不一致、またはメッセージ種別未定義
99	情報要素未定義
100	無効通知要素
101	コール状態とメッセージ不一致
102	タイマー満了による回復
111	プロトコル誤り、未指定
127	相互接続、未指定

サンプル ISDN 構成

以下に、いくつかの標準的な ISDN 構成を示します。

ISDN を介するフレーム・リレー構成

図37 は、ISDN ネットワークを介してフレーム・リレー・ネットワークを接続する方法を示しています。この構成では、ダイヤル回線上のデータ・リンクをフレーム・リレーとして設定します。

注: ダイヤル回線は、デフォルトではポイント・ポイント (PPP) プロトコルになります。プロトコルをフレーム・リレーに変更するには、`Config>` プロンプトで **set data-link fr** と入力します。コネクションを使用できるのは、両側のデータ・リンクが一致している場合 (たとえば、FR と FR、あるいは PPP と PPP) だけです。

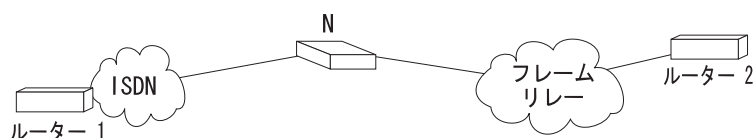


図 37. ISDN を介するフレーム・リレー構成

注: N は、FR スイッチに接続された ISDN TA、または FR スイッチ内の ISDN カードのいずれかです。

WAN 復元の構成

720ページの図38 は、障害が起きた専用 WAN リンクをバックアップするために (WAN 復元) ISDN 接続を使用する方法を示しています。この例では、ルーター A は通常は WAN リンクを使用してルーター B と通信します。その接続に障害が起きた場合、ISDN ダイヤルアップ・リンクが 2 つのルーターを再接続します。WAN リンクが回復すると、2 次リンクは自動的に切断します。WAN 復元用にルーターを構成する方法についての詳細は、[フィーチャーの使用と構成](#) の WAN 復元の使用を参照してください。

ISDN の使用

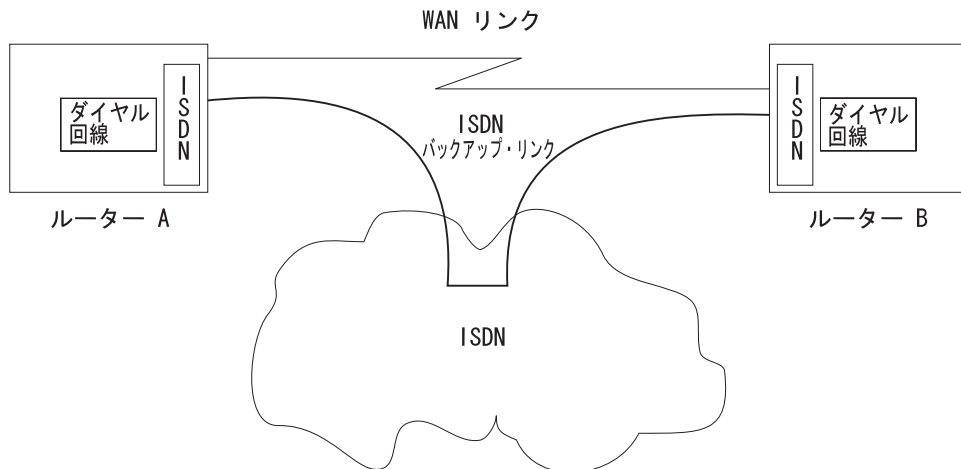


図38. WAN 復元のための ISDN の使用

WAN 復元の場合、2 次リンクとして使用できるのは、PPP 用に構成されたダイヤル回線だけです。WAN 再ルートの場合は、PPP ダイヤル回線または FR ダイヤル回線を代替リンクとして使用できます。

チャンネル化 T1/E1

チャンネル化として構成されている場合、チャンネル化/PRI アダプターは分割/チャンネル化 T1/J1/E1 サポートを提供します。56-Kbps または $N*64\text{-Kbps}$ のチャンネルを使用することができます。これにより、複数の専用回線接続 (たとえば、56-Kbps の V.35 を使用する) を多重化して、1 つの物理接続にまとめることが可能になります。

T1 または E1 の 1 次アダプターをチャンネル化として構成するには、次のようにします。

1. ISDN インターフェイス用のスイッチとして『Channelized』を選択する。
2. ダイヤル回線を構成するときに、この ISDN インターフェイス用に使用するタイム・スロットを構成する。詳細については、747ページの『Set』を参照してください。

チャンネル化 T1 インターフェイスの構成例

```
Config>n 6
ISDN Config>set switch chan
ISDN Config>list
```

ISDN Configuration

```
Maximum frame size in bytes      = 2048
Switch Variant/Service Type      = Channelized
Available Timeslots: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
```

```
Config>n 7
Circuit config: 7>set net 6
Circuit config: 7>set timeslot 2 3 4 24
Circuit config: 7>list
```

Base net	= 6
Idle character	= 7E
Bandwidth	= 64 Kbps
Timeslot	= 2 3 4 24

注: これが E1 回線の場合には、利用可能なタイム・スロットは 1 ~ 31 になります。

ISDN インターフェースの要件と制約

サポートされるスイッチ/サービス

ISDN 1 次群インターフェース (PRI) は、以下のスイッチ/サービスをサポートします。

スイッチ名	有効なコマンド
AT&T 5ESS (北米)	5ESS
AT&T 4ESS (北米)	4ESS
Australia (AUSTEL)	AUSPRI
INS-Net 1500 (日本、NTT)	INSPRI
National ISDN 2 (北米)	USNI2
NET 5 (欧州 ISDN、ETSI)	NET5
Northern Telecom DMS (DMSPRI)	DMSPRI
Native I.431	I431 (727ページの『I.431 スwitchの機種』を参照)
Channelized T1/E1	CHANNELIZED

ISDN インターフェースの制約事項

- ISDN インターフェースを介して、ルーターのブートまたはダンプを行うことはできません。
- X.25 パケット・データ用に D チャネルを使用することを可能にする BRI の場合を除き、データ・トラフィックに D チャネルを使用することはできません。通常、D チャネルは、B チャネル接続の設定と切断にのみ使用します。

ダイヤル回線の構成要件

ISDN を使用する PPP またはフレーム・リレーを構成するときは、以下の要件を考慮する必要があります。

- ISDN インターフェースは、PPP 構成で設定した転送遅延カウンターを強制しません。
- ダイヤル回線では pseudo-serial-ethernet を使用可能にしてはなりません。

始める前に

ISDN の構成を開始する前に、以下の情報が必要です。

- ローカル ISDN ポートの電話番号
- あて先の電話番号 (内線番号を含む)
- ISDN インターフェースを接続するスイッチのタイプ。スイッチのリストは、『サポートされるスイッチ/サービス』を参照してください。

ISDN の使用

注: スイッチのタイプおよびサービス提供者によっては、その他のパラメーター (TEI や SPID など) も必要になることがあります。

構成手順

この節では、ISDN インターフェースと関連のダイヤル回線を構成する方法について説明します。特に実行する必要がある作業は、次のとおりです。

1. ISDN アドレスを追加する
2. ISDN パラメーターを構成する
3. ISDN インターフェースを構成する
4. ダイヤル回線を追加する
5. ダイヤル回線を構成する

注: 構成変更を有効にするためには、ルーターをリスタートする必要があります。

ISDN アドレスの追加

各 ISDN インターフェースおよび各あて先の ISDN アドレスを追加することが必要です。ISDN アドレスには、次のものが含まれます。

- アドレス名。アドレス名は、アドレスの記述です。最大 23 字までの印刷可能 ASCII 文字列を使用できます。
- ネットワーク・ダイヤル・アドレス。ローカル・ポートまたはあて先ポートの電話番号です。句読点を含めて最大 25 桁の数字と 6 文字を入力できます。ルーターは数字のみを使用します。
- ネットワーク・サブダイヤル・アドレス。これは任意選択です。これは、インターフェースが PBX に接続した後で解釈される、電話番号の追加部分 (たとえば、内線番号) です。最大 20 桁の数字の他に、11 個のスペースと句読点を含めることができますが、ルーターは数字のみを使用します。

ISDN アドレスを追加するには、Config> プロンプトで **add isdn-address** コマンドを入力します。たとえば、次のように入力します。

```
Config>add isdn-address
Assign address name [23] chars []? baltimore
Assign network dial address [1-15 digits] []? 1-555-0983
Assign network subdial address [1-20 digits] []? 23
```

ISDN アドレスのリストを見たい場合は、Config> プロンプトで **list isdn-address** を入力します。

リストから ISDN アドレスを削除する場合は、Config> プロンプトで **delete isdn-address** コマンドを入力します。

ISDN パラメーターの構成

ISDN Config> プロンプトにアクセスします。ISDN Config> プロンプトにアクセスするには、Config> プロンプトで、**network** コマンドに続けて ISDN インターフェースのインターフェース番号を入力します。たとえば、次のように入力します。

```
Config>network 3
ISDN user configuration
ISDN Config>
```

Config> プロンプトで **list devices** コマンドを使用すると、ルーター上に構成されているインターフェース番号のリストを表示することができます。構成コマンドについての詳細は、729ページの『ISDN 構成コマンド』を参照してください。

1. この ISDN インターフェースが接続されているスイッチ/サービスのタイプを指定する。

set switch-variant コマンドを使用して、この ISDN インターフェースが接続されているスイッチのタイプを指定します。スイッチ/サービスのリストは、721ページの『サポートされるスイッチ/サービス』を参照してください。たとえば、次のように入力します。

```
ISDN Config>set switch net5
```

これは、スイッチで実行されているソフトウェアのタイプです (たとえば、DMS100 は DMS100 Custom ソフトウェアが実行されていることを意味します)。

2. ローカル・ポートのネットワーク・アドレス名を指定する。

set local-address-name コマンドを使用して、ローカル・ポートのネットワーク・アドレス名を指定します。**add isdn-address** コマンドを使用して定義したアドレス名の 1 つを使用する必要があります。たとえば、次のように入力します。

```
ISDN Config>: set local-address-name
Assign local address name []? baltimore
```

注: これは、ISDN 設定メッセージの発番号 (Calling Party Number) フィールドに入れて送られたものです。

3. ローカル・ポートのディレクトリー番号を設定する。
4. **set framesize** コマンドを使用して、フレーム・サイズを設定する。たとえば、次のように入力します。

```
ISDN Config>set framesize
Framesize in bytes (1024/2048/4096/8192) [1024]? 2048
```

注: 1024 のフレーム・サイズを選択した場合、PPP は ISDN ダイヤル回線では動作しません。PPP の最小サイズは 1500 であるからです。

ISDN フレーム・サイズの設定については、730ページの『Set』を参照してください。

任意選択の ISDN パラメーター

この節では、ユーザーが設定できる任意選択の ISDN パラメーターについて説明します。コマンドについての詳しい説明は、729ページの『ISDN 構成コマンド』を参照してください。

- INSPRI を除くすべての ISDN スイッチでは、あるアドレスへのコール数の限界を構成することができます。**set retries-call-address** コマンドを使用して、応答しないあて先へのコール回数を設定します。また、**set timeout-call-address** コマンドを使用して、コールを再試行する前に待つ時間を設定します。

ISDN インターフェースの構成が終了したら、**list** コマンドを使用して、構成を表示してみることができます。

ISDN インターフェースの構成

ISDN PRI の場合、アダプターに応じて、各アダプターに T1/J1 または E1 を構成する必要があります。

T1/J1 PRI インターフェース

以下の T1/J1 パラメーターを指定します。

1. T1/J1 PRI インターフェースの場合、伝送路再構成 (line build out) は、ルーターの T1 ポートによって送信される信号の減衰を指定します。サービス提供者によって提供された情報に基づいて、lbo (line build out) を指定します。

```
a= -00.0 dB
b= -07.5 dB
c= -15.0 dB
d= -22.5 dB
```

たとえば、次のように入力します。

```
set int lbo a
```

2. code を B8ZS または AMI に指定する。B8ZS がデフォルトです。この情報はサービス提供者が提供します。

たとえば、次のように入力します。

```
set int code AMI
```

3. ZBTSI (Zero Byte Time Slot Inversion) を ENABLED または DISABLED に指定する。デフォルトは DISABLED です。この情報はサービス提供者が提供します。

たとえば、次のように入力します。

```
set int ZBTSI enabled
```

4. esf-data-link を指定する。サービス契約に基づいて、次の 1 つを選択します。

ANSI-T1.403 ANSI-IDLE AT&T-IDLE

デフォルトは ANSI-T1.403 です。

たとえば、次のように入力します。

```
set int esf-data-link ansi-idle
```

E1 PRI インターフェース

E1 PRI インターフェースの場合、以下のパラメーターを指定します。

1. code を HDB3 または AMI に指定する。HDB3 がデフォルトです。この情報はサービス提供者が提供します。

たとえば、次のように入力します。

```
set int code HDB3
```

2. crc4 を ENABLED または DISABLED に指定する。デフォルトは ENABLED です。この情報はサービス提供者が提供します。

たとえば、次のように入力します。

```
set int crc4 enabled
```

ダイヤル回線の追加

ダイヤル回線は ISDN インターフェースにマップされます。複数のダイヤル回線を 1 つの ISDN インターフェースにマップすることができます。

ダイヤル回線を追加するには、Config> プロンプトで **add device dial-circuit** コマンドを入力します。ソフトウェアが、各回線にインターフェース番号を割り当てます。この番号を使用して、ダイヤル回線を構成します。たとえば、次のように入力します。

```
Config>add device dial-circuit
Enter the number of PPP Dial Circuit interfaces [1]?
Adding device as interface 6
Base net for the circuits(s) [0]?
```

構成できるダイヤル回線の数は、構成されるパラメーターの合計数、およびその結果の構成ファイルのサイズによって決まります。

注: ダイヤル回線は、デフォルトではポイント・ポイント (PPP) プロトコルになります。ダイヤル回線プロトコルをフレーム・リレーに変更する場合は、Config> プロンプトで **set data-link fr** コマンドを入力します。他のデータ・リンク・タイプ (X.25、SDLC、および SRLY) は、ISDN ではサポートされません。

ダイヤル回線の構成

この節では、ダイヤル回線の構成方法について説明します。

1. **network** コマンドに続けてダイヤル回線のインターフェース番号を入力して、Circuit Config> プロンプトを表示する。Config> プロンプトで **list devices** コマンドを入力すると、ルーター上に構成されているインターフェース番号のリストを表示することができます。たとえば、次のように入力します。

```
Config>network 6
Circuit configuration
Circuit Config>
```

2. ダイヤル回線を ISDN インターフェースにマップする。**set net** コマンドを使用します。基本ネットは ISDN インターフェース番号です。(これが必要とされるのは、基本ネットを変更している場合のみです。) たとえば、次のように入力します。

```
Circuit Config> set net
Base net for this circuit [0]? 3
```

注: ダイヤル回線データ・リンク・タイプが X.25 の場合、または基本ネット・スイッチの機種が I.43x またはチャンネル化の場合には、以下のステップ (3~727ページの11) は適用されません。

3. ダイヤル回線を接続するリモート・ルーターのアドレス名を指定する。**add isdn-address** コマンドを使用して定義した名前の 1 つを使用する必要があります。たとえば、次のように入力します。

```
Circuit Config> set destination
Assign destination address name []? baltimore
```

4. ダイヤル回線をアウトバウンド・コール発信専用、インバウンド・コール受信専用、またはコールの発信と着信の両方として構成する。

set calls コマンドを使用します。たとえば、次のように入力します。

```
Circuit Config>set calls outbound
Circuit Config>set calls inbound
Circuit Config> set calls both
```

注: WAN 復元動作またはダイヤル・オンデマンド・アプリケーションの場合、回線をインバウンド・コール用またはアウトバウンド・コール用のいずれかに設定することが必要です。

5. 回線のタイムアウト期間を指定する。

set idle コマンドを使用します。この指定された期間、回線上にトラフィックがないと、ダイヤル回線はハングアップします。回線を専用回線として構成する場合は、アイドル・タイマーをゼロに設定します。回線をダイヤル・オンデマンドに構成する場合は、アイドル・タイマーをゼロ以外の値に設定します。範囲は 0 ~ 65535 で、デフォルトは 60 秒です。たとえば、次のように入力します。

```
Circuit Config> set idle
Idle timer (seconds, 0 means always active) [0]? 0
```

注: WAN 復元/再ルートは、修正する必要があります。

6. 任意選択で、**lid_out_addr** を指定することにより、送信する LID 名を (あて先名であるデフォルト LID の代わりに) 提供することができます。

2 つのルーター間に複数の回線が構成されている場合 (並列回線)、どちらのダイヤル回線が接続するのかを両方のルーターが知るための手段が必要です。この目的のために、一方の端のルーター (コーラー側) から **lid_out_addr** が送信されます。ダイヤル回線を接続するためには、受信側ルーターが、送信側ルーター上の **lid_out_address** に一致するインバウンドあて先アドレスを持っていることが必要です。**lid_out_addr** は、以前に **config>** プロンプトで『ADD ISDN-ADDRESS』を使用して追加したアドレス名でなければなりません。

```
Circuit Config> set lid_out_addr router2
```

7. 任意選択で、ダイヤル回線の相対的な優先順位を設定することができます。

優先順位フィールドは、利用可能なチャンネルがないときに、ある回線を別の回線より優先させることを可能にします。アウトバウンド・コールがあり、すべてのチャンネルが使用中の場合、要求しているダイヤル回線の優先順位を、通信中のすべてのダイヤル回線と照合します。それより低い優先順位の回線があった場合、その回線は切断され、高い優先順位のダイヤル回線のためのコール設定が行われます。

注: ダウンにされるのは、アウトバウンド・ダイヤル・オンデマンド回線だけです。

優先順位についての詳細は、747ページの『Set』を参照してください。

```
Circuit Config> set priority 1
```

8. 任意選択で、コール設定と初期パケット送信の間の時間を遅らせることができます。**set selftest-delay** コマンドを使用します。一部の ISDN スイッチは、あて先の回線の確立が完了したことを示す信号を受信する前にデータの送信を開始します。自己テスト遅延を設定すると、初期パケットが廃棄されるのを防止できます。たとえば、次のように入力します。

```
Circuit Config> set selftest-delay
Selftest delay(milli-seconds,0 means no delay)[150]?200
```

9. インバウンド・アドレス名を設定する。

set inbound コマンドを使用します。このコマンドはインバウンド回線専用です。たとえば、次のように入力します。

```
Circuit Config>set inbound
Assign destination inbound address name []? newyork
```

着信 LID または CallerID をダイヤル回線と突き合わせるためにインバウンドあて先番号が使用されます。一致がある場合は、ダイヤル回線はコールを受け取ります。

10. 任意選択で、ダイヤル回線上で実行されているデータ・リンク・レイヤー・プロトコル (PPP またはフレーム・リレー) の構成プロセスに入ることができます。

encapsulator コマンドを使用します。たとえば、次のように入力します。

```
Circuit Config> encapsulator
```

11. 任意選択で、**set bandwidth** コマンドを使用して、コールを行う回線速度 (56-Kbps または 64-Kbps のいずれか) を設定することができます。これにより、ISDN インターフェースにコールごとの制御を提供します。たとえば、次のように入力します。

```
Circuit Config> set bandwidth 56Kbps
```

I.431 スイッチの機種

ISDN PRI (T1/J1 のみ) を介して専用線を稼働している場合は、スイッチの機種を I.431 として符号化してください。

ネイティブ I.431 サポート

ネイティブ I.431 サポートを構成する場合は、ダイヤル回線は 1 つしか使用できません。これを基本ネットに接続する必要があります。I.431 は ISDN PRI T1 アダプター上でのみ動作します。速度は 1.5 Mbps に固定されています。

注: マルチポイント ISDN PRI アダプターは、I.431 スイッチをサポートしません。PRI の全ラインを利用するためには、チャンネル化を選択し、すべてのタイム・スロットを 1 つのダイヤル回線に割り当てます。

例: Base ISDN net

```
Config> n 5
ISDN Config> set sw i431
ISDN Config> list all
ISDN Configuration
Maximum frame size in bytes    = 2048
Switch Variant                  = I431 PRI
```

例: Dial Circuit

```
Config> n 6
Circuit config: 6>set net 5
Circuit config: 6>list all
```

```
Base net = 5
```

ISDN の使用

第44章 ISDN インターフェースの構成および監視

この章では、ISDN コマンドおよび GWCON コマンドについて説明します。本章には、以下の節が含まれています。

- 『ISDN 構成コマンド』
- 735ページの『インターフェース監視プロセスへのアクセス』
- 735ページの『ISDN 監視コマンド』
- 740ページの『ISDN と GWCON コマンド』

注:

1. ISDN インターフェースは、ISDN 関連のアクティビティを監視するのに使用できる ELS メッセージおよび原因符号の両方を提供します。 イベント・ログ・システム・メッセージの手引き を参照してください。
2. ISDN、Q931、CEME、LAPD、および DIAL ELS サブシステムが使用可能です。

ISDN 構成コマンド

表98 は、ISDN 構成コマンドの要約を示しており、それに続く各節で個々のコマンドについて説明しています。これらのコマンドは `ISDN Config>` プロンプトで入力します。

表 98. ISDN 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Block-calls	特定のコーラーからの着信コールを妨害します。
Disable	BRI の場合にのみ有効です。電源 1 検出を使用不可にします。
Enable	BRI の場合にのみ有効です。電源 1 検出を使用可能にします。
List	ISDN 構成を表示します。
Remove	DN0 エントリーを ISDN 構成から除去します。
Set	フレーム・サイズ、ローカル・アドレス、無応答タイムアウト、無応答後の試行回数、ISDN スイッチのタイプ、ディレクトリー番号、SPIDS、and TEI.
Cause Code	インターフェースを介して接続を確立するための試行をそれ以上処理するのを停止します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Block-Calls

block-calls コマンドは、着信コールを妨害するのに使用します。妨害するコーラーの番号を認証リストに追加する必要があります。コールを妨害されるコーラーの最大数は、インターフェースにつき 16 です。

コールの妨害は、次のものに使用することができます。

- 常時受信される非勧誘型のコール

ISDN 構成コマンド

- 特定のコールを無視する必要があるネットワーク立ち上げ/テスト

構文:

```
block-calls          add
                        list
                        remove
```

Add 妨害されるコーラーの番号を追加します。

List 妨害されるコーラーの番号をリストします。

Remove

妨害されるコーラーの番号をリストから除去します。

List

list コマンドは、現行の ISDN 構成を表示します。

構文:

```
list
```

例: **list**

```
ISDN Configuration
Local Network Address Name      = local2210
Local Network Address:Subaddress = 2542210:
Maximum frame size in bytes     = 2048
Outbound call address Timeout   = 180 Retries = 2
Switch Variant                  = NT DMS-250
DN0 (Directory Number 0)       = 2542210
No circuit address accounting information being kept.

T1/J1 Interface Parameters:
LBO                             = 00.0 dB
Code                            = B8ZS
ZBTISI                          = Disabled
ESF-Data-Link                   = ANSI-IDLE
```

Remove

remove コマンドでは、以前に **set DN0** または **set DN1** コマンドを使って設定してあった DN0 または DN1 を除去することができます。

構文:

```
remove          DN0-entry...
```

例: **remove DN0**

Set

set コマンドは、フレーム・サイズ、アドレス、およびタイムアウトを構成します。スイッチの機種および TEI 番号も指定します。PRI の場合、端末終端点識別子 (TEI) は常にゼロ (0) です。

構文:

```

set
    framesize...
    frame-type1
    interface
    local-address-name...
    RAI-type1
    retries-call-address...
    switch-variant...
    dn0...

```

framesize 1024 or 2048 or 4096 or 8192

ISDN インターフェースで送受されるフレームの、ネットワーク・レイヤー部分のサイズを設定します。データ・リンクおよび MAC レイヤーのヘッダーは含まれません。ISDN フレーム・サイズは、ISDN インターフェースを使用するダイヤル回線に構成したフレーム・サイズ以上の値に設定する必要があります。

PPP ダイヤル回線インターフェースの場合、**set lcp options** コマンドを使用して、PPP MRU を変更することができます。ISDN フレーム・サイズは、PPP MRU および PPP ヘッダー用のバイトを十分に組み込める大きさであることが必要です。

注: 1024 のフレーム・サイズを選択した場合、PPP は ISDN ダイヤル回線上では動作しません。PPP の最小サイズは 1500 であるからです。

FR ダイヤル回線インターフェースの場合、**set framesize** コマンドを使用して、フレーム・サイズを変更することができます。ISDN フレーム・サイズは、FR フレーム・サイズ以上の値でなければなりません。

ダイヤル回線のフレーム・サイズが ISDN のフレーム・サイズより大きい場合、ルーターの初期化時に、ダイヤル回線のフレーム・サイズが削減されます。

例:

```

set framesize
Framesize in bytes (1024/2048/4096/8192) [1024]? 2048

```

frame-type

選択項目は、D4 または ESF です。これは T1 マルチ・フレーム・フォーマットを指定します。非チャンネル化モードの場合は、ESF しかサポートされません。フレーム・タイプは、基本 ISDN ネット・メニューのもとで構成します。

例:

```

set frame-type
Circuit config: 10>set frame type

```

ISDN 構成コマンド

interface

PRI の場合のみ。 T1 または E1 回線の以下のインターフェース・パラメータを設定します。

T1 PRI の場合:

lbo ルーターの T1 ポートによって送信される信号の減衰。この情報はサービス提供者によって提供されます。

有効値:

a= -00.0 dB

b= -07.5 dB

c= -15.0 dB

d= -22.5 dB

デフォルト値: a

code この情報はサービス提供者によって提供されます。

有効値: B8ZS または AMI

デフォルト値: B8ZS

ZBTSI ゼロ・バイト・タイム・スロット反転 (Zero Byte Time Slot Inversion)。この情報はサービス提供者によって提供されます。

有効値: 使用可能または使用不可

デフォルト値: 使用不可

esf-data-link

サービス契約。この情報はサービス提供者によって提供されます。

有効値:

ANSI-T1.403

ANSI-IDLE

AT&T-IDLE

デフォルト値: ANSI-T1.403

E1 PRI の場合:

code この情報はサービス提供者によって提供されます。

有効値: HDB3 または AMI

デフォルト値: HDB3

crc4 ルーターの E1 ポートが crc4 符号語を転送し、受信したフレーム内の crc4 符号語を検査するかどうかを指定します。この情報はサービス提供者によって提供されます。

有効値: 使用可能または使用不可

デフォルト値: 使用不可

local-address-name *address name*

これはローカル ISDN ポートのネットワーク・アドレス名です。このアドレス名は、Config> プロンプトで **add isdn-address** コマンドを使用して定義した名前の 1 つに一致している必要があります。

有効値: 任意の有効なアドレス

デフォルト値: なし

例:

```
set local-address-name
Assign local address name []? line-1-local
```

RAI-type

選択項目は ANSI または Japanese です。これは、D4 フレームを使用している場合、T1 回線上の RAI を示す方法を指定します。ANSI RAI は、すべてのチャンネルのビット 2 の値が 0 であることによって示されます。Japanese RAI は、フレーム 12 の S ビット位置の値が 1 であることによって示されます。フレーム・タイプは、基本 ISDN ネット・メニューのもとで構成します。

retries-call-address value

一部の電話サービス提供者は、自動リコール装置に対して、アクセス不能アドレスまたは自動リコールを拒否するアドレスへの連続コール回数を制限しています。**Retries-call-address** は、ルーターが一度に試みるコールの最大数を指定します。**retries-call-address** を 0 に設定すると、ルーターは同時にすべての回線を起動します。

switch-variant を INS64 に設定した場合は、**retries-call-address** のデフォルトを変更することはできません。デフォルトは 2 に固定されます。

有効値: 0 ~ 30

デフォルト値: 23 (BRI の場合は 2)

switch-variant 4ess or 5ess or auspri usni2 or ins1500 or dms250 or channel

ISDN インターフェースが接続されるスイッチのモデルを指定します。ISDN 1 次群インターフェースのスイッチの機種/サービス・タイプは、以下のリストから選択することができます。

ISDN 1 次群インターフェース (PRI)/チャンネル化 T1/E1 の有効値:

- AT&T 5ESS (北米)
- AT&T 4ESS (北米)
- Australia (AUSTEL)
- INS-Pri (日本、NTT)
- National ISDN 2 (北米)
- NET 5 (欧州 ISDN、ETSI)
- Northern Telecom 250 (DMSPRI)
- Native I.431
- Channelized T1/E1

デフォルト値: DMSPRI

dn0 directory number 0

インバウンドを受け入れるためには、DN0 が **set local-address-name** コマンドを使用して構成したネットワーク・ダイヤル・アドレス (電話番号) と一致していることが必要です。DN0 が構成されていない場合は、検査は行われず、すべてのコールが受け入れられます。スイッチがコール設定メッセージで発番号を提供しない場合は、DN0 を構成してはなりません。詳細については、734 ページを参照してください。

例:

ISDN 構成コマンド

```
set dn0
Enter DN0 (Directory-Number-0) [ ]? 5088981234
```

注: これは、基本速度 ISDN スイッチのすべての機種に適用されます。

- 着信コールが正しい ISDN あて先に送信されていることを検証するために DN0 および DN1 が使用されます。
- 送信中の ISDN コールのあて先番号 (コールされる側の番号) が DN0 または DN1 のいずれにも一致しない場合、そのコールはリジェクトされます。
- ユーザーがあて先検証の検査をう回したい場合は、DN0 または DN1 のいずれも構成しないでください。ISDN 回線の設備がもつ DN が 1 つしかなく、ユーザーがあて先検証を使用したい場合には、DN0 を構成する必要があります。ISDN 回線が 2 つの DN を用意していない場合は、DN1 を構成しないでください。
- SPID および TEI を構成する際は、必ず最初の SPID (SPID[0]) および TEI (TEI[0]) を構成してください。SPID[0] または TEI[0] を構成せずに SPID[1] または TEI[1] を構成すると、エラーが発生します。

Cause Code

Cause Code コマンドは、ルーターが 『specified』 (有効値) レスポンスを受信したときに、ISDN インターフェースを介して接続の確立を再試行するのを防止するのに使用します。これらのコマンドは Cause Config> プロンプトで入力します。

構文:

```
cause code          ? (Help)
                    _add
                    _list
                    _remove
                    _exit
```

表 99. ISDN Cause Codes コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Add	原因符号エントリーを ISDN 構成に追加します。
List	ISDN 構成の原因符号リストを表示します。
Remove	ISDN 構成から原因符号エントリーを除去します。
Exit	直前のコマンド・レベルに戻ります。13ページの『下位レベル環境の終了』を参照してください。

Add **add** コマンドは、原因符号を ISDN 構成に追加するのに使用します。

有効値: 01 ~ FF の間の任意の 16 進値

デフォルト値: なし

構文: cause code add value

例: **add FF**

List **list** コマンドは、ISDN 構成の原因符号リストを表示するのに使用します。

構文: cause code list

Remove

remove コマンドは、原因符号を ISDN 構成から除去するのに使用します。

有効値: 01 ~ FF の間の任意の 16 進値

デフォルト値: なし

構文: cause code remove value

例: **remove FF**

インターフェース監視プロセスへのアクセス

ISDN の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。

```
+ network #
```

ただし、# は、ISDN インターフェースの番号です。ダイヤル回線の監視プロセスに直接アクセスすることはできませんが、ISDN インターフェースにマップされたダイヤル回線を監視することができます。

ISDN 監視コマンド

以下の節では、ISDN インターフェースの料金計算エントリー、コール、回線、パラメーター、および統計を表示することができる ISDN 操作コマンドについて説明します。これらのコマンドは ISDN> プロンプトで入力します。

表 100. ISDN 監視コマンドの要約

監視コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Block-calls	特定のコーラーからの着信コールを妨害します。
Calls	前回にルーター上の統計がリセットされた以降に、このインターフェースにマップされた各ダイヤル回線に行われた、完了した接続および試行された接続の数を表示します。
Channels	ISDN 1 次群インターフェース上のチャンネルの統計を表示します。
Circuits	ISDN インターフェース上に構成されたすべてのデータ回線の状態を表示します。
Dial-dump	指定されたダイヤル回線の運用特性を表示します。
L2_counters	L2/L1 状態をいくつかの L2 カウンターとともにリストします。
L3_counters	送信/受信/受諾された設定のカウンターをリストします。
TEI	TEI の状態をリストします (BRI の場合のみ)。
Parameters	ISDN インターフェースの現行パラメーターを表示します。
Signaling-L3	このコマンドは、製品サポートの要員だけが使用するのためのものです。
Statistics	ISDN インターフェースの現行統計を表示します。

ISDN 監視コマンド

表 100. ISDN 監視コマンドの要約 (続き)

監視コマンド	機能
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Block-Calls

block-calls コマンドは、着信コールを妨害するのに使用します。妨害するコーラーの番号を認証リストに追加する必要があります。コールを妨害されるコーラーの最大数は、インターフェースにつき 16 です。

構文:

```
block-calls                add
                               list
                               remove
```

Add 妨害されるコーラーの番号を追加します。

List 妨害されるコーラーの番号をリストします。

Remove

妨害されるコーラーの番号をリストから除去します。

Calls

calls コマンドは、前回にルーター上の統計がリセットされた以降に、このインターフェースにマップされた各ダイヤル回線で行われた、完了した接続および試行された接続の数をリストするのに使用します。

構文:

```
calls
```

例:

```
calls
Net Interface Site Name      In   Out  Rfsd  Blckd
 4   PPP/1   v403                2    0    0     0
```

Unmapped connection indications: 0

Net このインターフェースにマップされたダイヤル回線の数

Interface

インターフェースのタイプとそのインスタンス番号

Site Name

ダイヤル回線のネットワーク・アドレス名

In このダイヤル回線で受け入れられたインバウンド接続

Out このダイヤル回線によって開始された、完了した接続の数

Rfsd ネットワークまたはリモートポートによってリジェクトされた、このダイヤル回線によって開始された接続の数

Blckd ルーターが妨害した接続試行。ルーターが接続試行をブロックするのは、すべての利用可能なチャネルが使用中の場合、最大試行回数を使い尽くされて

ルーターがタイマーのカウントダウンを待っている場合、あるいはレイヤー 1 はアップであるが、レイヤー 2 がダウンの場合です。

Unmapped connection indications:

着信コールを受け入れるように構成され、使用可能にされているダイヤル回線がないために、ルーターによってリジェクトされた接続試行の回数

Channels

channels コマンドは、ISDN 1 次群インターフェース上のチャンネルの統計をリストします。

構文:

channels

Circuits

circuits コマンドは、ISDN インターフェース上に構成されている『Up』または『Available』のダイヤル回線の状態を表示します。

構文:

circuits

例:

```

circuit
Net Interface  MAC/Data-Link  State    Reason    Duration
4   PPP/1   Point to Point  Up B1    SelfTest  91:24:03
5   PPP/2   Point to Point  Up B2    Inbound   91:24:00

```

Net このインターフェースにマップされたダイヤル回線の数

Interface

インターフェースのタイプとそのインスタンス番号

MAC/Data-Link

このダイヤル回線に構成されたデータ・リンク・プロトコルのタイプ

State ダイヤル回線の現行状態

Up 現在接続された状態です。

Available

現在は接続されていませんが、利用可能です。

Disabled

ダイヤル回線は使用不可にされています。

Down ダイヤル回線がビジーであるか、リンク・レイヤー・プロトコルがダウンしているために、接続に失敗しました。

Reason

現行状態の理由:

nnn_Data

(nnn はプロトコルの名前です。) プロトコルに送信するデータがあったので、回線はアップです。

ISDN 監視コマンド

Rmt Disc

リモート切断。リモートあて先がコールを切断したので、回線はダウンまたは利用可能のいずれかです。

Opr Req

オペレーター要求。前回のコールが監視コマンドによって切断されたので、回線は利用可能です。

Inbound

回線がインバウンド・コールに応答したので、回線はアップです。

Restoral

WAN 復元動作のため、回線はアップです。

Self Test

回線は静的として構成されており (アイドル・タイム = 0)、使用可能にされたときに正常に接続されました。

Duration

回線が現行状態にある時間の長さ

Dial-dump

dial-dump コマンドは、指定されたダイヤル回線の運用特性を表示するのに使用します。

構文:

dial-dump *circuitname*

L2_Counters

L2_counters コマンドは、L2/L1 状態をいくつかの L2 カウンターとともにリストするのに使用します。

構文:

L2_counters

L3_Counters

L3_counters コマンドは、送信/受信/受諾された設定のカウンターをリストするのに使用します。構文:

L3_counters

TEI

TEI コマンドは、TEI の状態をリストするのに使用します。 BRI の場合のみ。

構文:

parameters

例:

```

parameters
ISDN Port parameters:

Local Address Name:      v1233
Local Network Address:   20
Local Network Subaddress:
Frame Size:             2048
TEI 0:                  Automatic
TEI 1:                  Automatic

Switch Variant:        AT&T 5ESS (United States)
Multipoint Selection:   Multipoint
Directory Number 0:    20
Outbound call address Timeout: 180      Retries: 0

```

Parameters

parameters コマンドは、現行の ISDN 構成を表示するのに使用します。

構文:

```
parameters
```

例:

```

parameters
ISDN Port parameters:

Local Address Name:      v1233
Local Network Address:   20
Local Network Subaddress:
Frame Size:             2048
TEI 0:                  Automatic
TEI 1:                  Automatic

Switch Variant:        AT&T 5ESS (United States)
Multipoint Selection:   Multipoint
Directory Number 0:    20
Outbound call address Timeout: 180      Retries: 0

```

Statistics

statistics コマンドは、この ISDN インターフェースの現行統計を表示するのに使用します。

構文:

```
statistics
```

E1 による PRI の例:

```

statistics
Link: Active ISDN Firmware: 1.0 Handler State: Running

Transmit D Channel Receive D Channel
Packets 68422 Packets 68419
Bytes 411656 Bytes 413592
Overflow 23 Overflow 3
Underrun 0 Too Long 6
Abort 4
CRC error 8
Misaligned 3

Transmit B Channels Receive B Channels
Packets 1499094 Packets 1499228
Bytes 59955660 Bytes 59951780
Overflow 0 Overflow 90
Underrun 0 Too Long 171
Abort 139
CRC error 232

```

ISDN 監視コマンド

```

                                     Misaligned      72
E1 Status Register                   E1 Error Count Registers
Receive AIS      : Off  CRC6 Errors:      4
Receive RAI     : Off  LCV Errors:     38
Receive Carrier Loss: Off FEB Errors:    11
Receive Loss of Sync: Off FAS Errors:    24
```

I.431 を使用する T1 による PRI の例:

```

statistics
Transmit                               Receive
Packets      0      Packets      0
Bytes        0      Bytes        0
Overflow     68480  Overflow     0
Underrun     0      Too Long    0
                                     Abort      0
                                     CRC error  0
                                     Misaligned 0

T1 Status Register                   T1 Error Count Registers
Receive AIS      : Off  LCV Errors:      0
Receive RAI     : Off  CRC6 Errors:     0
Receive Carrier Loss: Off Sync Errors: 47937328
Receive Loss of Sync: On

T1 PRM Events                         Local      Remote
CRC Error                               0          0
Controlled Slip                         0          0
Line Code Violation                     0          0
Frame Sync Bit Error                    0          0
Severely Errored Frame                   0          0
Payload Loopback Active                  0          0
PRMs Processed (1/sec)                   0          0
```

ISDN と GWCON コマンド

ISDN には独自の監視用の監視プロセスがありますが、GWCON 環境から **interface**、**statistics**、および **error** コマンドを使用すれば、ルーターも構成情報と、装置および回線の完全な統計を表示します。また、GWCON **test** コマンドを使用して、DCE および回線をテストすることもできます。

注: ISDN インターフェースに対して **test** コマンドを出すと、現行のコールは除去され、再ダイヤルされます。

Interface -- ISDN インターフェースとダイヤル回線の統計

GWCON プロンプト (+) で **interface** コマンドを使用して、ISDN インターフェースおよびダイヤル回線の統計を表示します。

ダイヤル回線の統計を表示するには、**interface** コマンドに続けて、ダイヤル回線のインターフェース番号を入力します。ISDN インターフェースの場合、情報は D チャネルと B チャネルについて表示されます。(これは ISDN **statistics** コマンドで表示されるものと同じ情報です。)

例:

```
interface 2
```

```

                                     Self-Test  Self-Test  Maintenance
Nt Nt' Interface Slot-Port          Passed    Failed    Failed
2 2  ISDN/0   Slot: 8 Port: 1             1         0         0

ISDN Base Net MAC/data-link on ISDN Primary Rate interface
Link: Active ISDN Firmware: 1.0 Handler State: Running
```

Transmit	D Channel	Receive	D Channel
Packets	36	Packets	36
Bytes	214	Bytes	214
Overflow	0	Overflow	0
Underrun	0	Too Long	0
		Abort	0
		CRC error	0
		Misaligned	0

Transmit	B Channels	Receive	B Channels
Packets	0	Packets	0
Bytes	0	Bytes	0
Overflow	0	Overflow	0
Underrun	0	Too Long	0
		Abort	0
		CRC error	0
		Misaligned	0

T1 Status Register	T1 Error Count Registers
Receive AIS : Off	LCV Errors: 0
Receive RAI : Off	CRC6 Errors: 0
Receive Carrier Loss: Off	Sync Errors: 0
Receive Loss of Sync: Off	

T1 PRM Events	Local	Remote
CRC Error	0	0
Controlled Slip	0	0
Line Code Violation	0	0
Frame Sync Bit Error	0	0
Severely Errored Frame	0	0
Payload Looback Active	0	0
PRMs Processed (1/sec)	365	367

ダイヤル回線の以下の統計を表示するには、**interface** コマンドに続けてダイヤル回線のインターフェース番号を入力します。

例:

interface 3

Nt	Nt'	Interface	Self-Test Passed	Self-Test Failed	Maintenance Failed
3	2	PPP/1	1	0	0

Point to Point MAC/data-link on ISDN Primary Rate interface

下のリストは、ISDN とダイヤル回線の両方の出力を説明しています。

Nt シリアル・ライン・インターフェース番号またはダイヤル回線インターフェース番号

Nt' *Nt* がダイヤル回線の場合、これはダイヤル回線がマップされる ISDN インターフェースのインターフェース番号です。

Interface

インターフェース・タイプとそのインスタンス番号

Slot ISDN アダプターが入っているスロット

Port ISDN アダプター上のポート番号

Self-Test Passed

成功した自己テストの回数

Self-Test Failed

失敗した自己テストの回数

ISDN と GWCON コマンド

Maintenance: Failed

保守障害の数

Configuration - ルーターのハードウェアおよびソフトウェアに関する情報

ルーターのハードウェアおよびソフトウェアに関する情報を表示するには、GWCON (+) プロンプトから **configuration** コマンドを入力します。これには、ルーター上に構成されたインターフェースとそのインターフェースの状態を表示するセクションが含まれています。

ダイヤル回線がダイヤル・オンデマンドとして構成されている場合、ダイヤル回線の状態は、接続されているかどうかに関係なく、常に Up として表示されます。この場合、Up は、ダイヤル回線が接続状態または利用可能のいずれかであることを意味しています。

ダイヤル回線が静的回線として構成されている場合には、ダイヤル回線が接続されている場合のみ、状態は Up と示されます。(**configuration** コマンドの出力例については、152ページの『Configuration』を参照してください。)

第45章 ダイヤル回線の構成および監視

この章では、V.25bisまたは ISDN インターフェースにマップされたダイヤル回線インターフェース上のダイヤル回線の構成方法について説明します。本章には、以下の節が含まれています。

- 『ダイヤル回線構成コマンド』
- 750ページの『ダイヤル回線監視コマンド』

注:

1. PPP ダイヤル回線インターフェースは、ISDN または V.25bis ネットワークを基本ネットワーク・インターフェースとして使用することができます。
2. FR ダイヤル回線インターフェースは、ISDN または V.25bis ネットワークを基本ネットワーク・インターフェースとして使用することができます。
3. 交換 SDLC コール・イン・ダイヤル回線インターフェースは、V.25bis ネットワークを基本ネットワーク・インターフェースとして使用します。
4. BRI の場合、ISDN D チャネルを介して X.25 回線を使用することができます。

ダイヤル回線の構成方法については、以下を参照してください。

- ISDN インターフェースについては、713ページの『第43章 ISDN インターフェースの使用』を参照してください。
- V.25bis インターフェースについては、673ページの『第39章 V.25bis ネットワーク・インターフェースの使用』を参照してください。

ダイヤル回線構成コマンド

表101 は、ダイヤル回線構成コマンドを説明しています。ダイヤル回線構成コマンドは、Circuit Config> プロンプトで入力します。構成変更を有効にするためには、ルーターをリスタートする必要があります。

Circuit Config> プロンプトにアクセスするには、**network** コマンドに続けて『ダイヤル回線』のインターフェース番号を入力します。(ダイヤル回線番号は、**add device dial-circuit** コマンドを入力したときに割り当てられています。) Config> プロンプトで **list devices** コマンドを入力すると、ユーザーが追加したダイヤル回線のリストを表示することができます。

表 101. ダイヤル回線構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』を参照してください。
Delete	インバウンド・コールの設定をダイヤル回線構成から削除します。
Encapsulator	データ・リンク・プロトコル構成を変更することができます。
List	ダイヤル回線構成パラメーターを表示します。

ダイヤル回線の構成

表 101. ダイヤル回線構成コマンドの要約 (続き)

コマンド	機能
Set	ダイヤル回線をインバウンド・コール用またはアウトバウンド・コール用に構成したり、ダイヤル回線をシリアル・ライン・インターフェースにマップしたり、アドレス、アイドル・タイムアウト、優先順位、lid_out アドレス、インバウンドあて先、および自己テスト遅延を設定したりします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Delete

delete コマンドは、インバウンド・コールの設定をダイヤル回線構成から除去するのに使用します。

構文:

delete *inbound destination*

inbound destination

INBOUND あて先および ANY_INBOUND 設定値を、ダイヤル回線構成から除去します。これにより、ダイヤル回線は電話番号が *destination* パラメーターに一致するコーラーからのコールのみを受け入れるようになります。

Encapsulator

encapsulator コマンドは、ダイヤル回線インターフェース上で実行されているリンク・レイヤー・プロトコル (たとえば、PPP、フレーム・リレー、X.25SDLC) の構成プロセスに入るのに使用します。

注: **add device dial-circuit** コマンドによって作成されるダイヤル回線インターフェースのデフォルトは PPP になります。リンク・レイヤー・タイプを変更するには、Config> プロンプトで次のように入力します。

- フレーム・リレーの場合は、**set data-link frame-relay** と入力する。
- SDLC の場合は、**set data-link sdlc** と入力する。

構文:

encapsulator

次の例は、PPP ダイヤル回線インターフェースに対して **encapsulator** コマンドを使用して、PPP 構成プロセスに入ることを示しています。

例:

```
encapsulator
Point-to-Point user configuration
PPP Config>
```

V.25bis を基本ネットとして使用するダイヤル回線を構成する場合は、以下のことに注意してください。

- V.25bis インターフェースのクロックは外部として事前定義されています。モデム (DCE) がクロック速度を制御します。クロック、符号化、およびその他の HDLC パラメーターは、ダイヤル回線構成の一部として構成することはできません。

ISDN に対して PPP またはフレーム・リレーを構成するときは、ダイヤル回線構成の HDLC パラメーターは構成できないので注意してください。物理レイヤー・パラメーターは ISDN インターフェース上で構成します。

PPP プロトコルの構成については、365ページの『第23章 シリアル・ライン・インターフェースの構成』または 519ページの『第30章 ポイント・ポイント・プロトコル・インターフェースの使用』を参照してください。

フレーム・リレー・プロトコルの構成については、443ページの『第28章 フレーム・リレー・インターフェースの使用』または 465ページの『第29章 フレーム・リレー・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。

SDLC インターフェースの構成または監視については、621ページの『第35章 SDLC インターフェースの使用』または 625ページの『第36章 SDLC 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。

X.25 インターフェースの構成または監視については、377ページの『第25章 X.25 ネットワーク・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。

Circuit Config> プロンプトに戻るには、**exit** コマンドを使用します。

List

list コマンドは、現行のダイヤル回線構成を表示するのに使用します。

I.430 および I.431 についての詳細は、727ページの『I.431 スイッチの機種』を参照してください。

構文:

list

例:

注: リストされるオプションは、使用されるインターフェースのタイプによって異なります。すべてのインターフェース・タイプについてすべてのオプションが表示されるわけではありません。

```
list
Any inbound          set
Bandwidth:           64
Base net:             1
Callback:            yes
Calls:               inbound
Destination name:    remote-site-sanfrancisco
Idle char:           7E
Idle timer:          = 60 sec
Inbound calls        allowed
Inbound dst name:    local-1
LID out address:     1234
LID used:            enabled
Net #:               2
Outbound calls       allowed
Priority:             8
SelfTest Delay Timer: = 0 ms
Time slot:           1 4 5 8
```

ダイヤル回線の構成

Any inbound

他のどのダイヤル回線にも一致しないインバウンド・コールを、この回線にマップして、インバウンド・コールとして受け入れるときにこの設定値を表示します。

帯域幅 (Bandwidth)

帯域幅の値を Kbps 単位で表示します。

Base net

このダイヤル回線がマップされるシリアル・ライン・インターフェースの名前を表示します。

Callback

このオプションの設定値を表示します。

Calls このオプションの設定値を表示します。

Destination name

発信回線のコールされる側のネットワーク・アドレス名と、LID 機構がインバウンド・コールに対して使用するデフォルトの比較用アドレスを表示します。

Idle char

I.43x またはチャンネル化回線に使用されるアイドル文字を表示します。

Idle timer

アイドル・タイマーの設定値 (秒) を表示します。範囲は 0 ~ 65535 です。0 は、これが専用回線であることを示します。

Inbound calls allowed

回線がインバウンド・コールを受け入れるように構成されている場合に、このパラメーターを表示します。

Inbound dst name

他のアドレスのどれにも一致しないインバウンド・コールを受け入れるように回線が構成されている場合に、このパラメーターを表示します。これは、LID 機構がインバウンド・コールに対して使用する代替の比較用アドレス名です。

LID out address

ルーター同士を接続するダイヤル回線の名前を表示します。

LID used

このオプションの設定値を表示します。

Net # 基本回線番号を表示します。

Outbound calls allowed

回線がアウトバウンド・コールを開始するよう構成されている場合に、このパラメーターを表示します。

Priority

このパラメーターの設定値を表示します。

SelfTest Delay Timer

自己テスト遅延タイマーの設定値 (ミリ秒) を表示します。範囲は 0 ~ 65535 です。0 は遅延なしを示します。

Time slot

このダイヤル回線で使用するスロットのリストを表示します。

Set

set コマンドは、ダイヤル回線をインターフェース (たとえば、ISDNまたは V.25bis) にマップしたり、ダイヤル回線をアウトバウンド・コールまたはインバウンド・コール (あるいは、その両方) 用として構成したり、あて先アドレス、インバウンド・アドレス、アイドル・タイムアウト、および自己テスト遅延を設定するのに使用します。

注:

1. ダイヤル回線上で SDLC、I.430、I.431、チャンネル化、または X.25 を稼働している場合、以下のパラメータはソフトウェアが特定のデフォルト値を使用するので、**set** コマンドを使用して変更することはできません。
 - Any_inbound - any_inbound を設定
 - Calls - インバウンド
 - Destination - デフォルト・アドレス
 - Inbound destination - あて先インバウンド・アドレスなし
 - Idle - 0
 - Lid_out_addr - LID 名なし
 - Lid_used - 使用不可
 - Priority - 8
 - Self_test_delay

構文:

```
set                any_inbound
                    bandwidth...
                    callback...
                    calls...
                    destination...
                    idle...
                    idle-char...
                    inbound destination...
                    lid_out_addr...
                    lid_used...
                    net...
                    priority...
                    selftest-delay...
                    timeslot...
```

any_inbound

他のどのダイヤル回線にも一致しないインバウンド・コールは、この回線にマップして、インバウンド・コールとして受け入れることを指定します。

ダイヤル回線の構成

bandwidth *kbps*

I.430 およびチャネル化 T1/E1 回線の帯域幅 (Kbps) を設定します。

有効値:

I.430 の場合: 64 または 128

チャネル化の場合: 56 または 64

デフォルト値: 64

callback [*Yes or No*]

コールバック・フィーチャーは、コーラー電話番号を使用して、コールを認証テーブルと突き合わせて検証した後、着信コールを切断します。次に、コールバックは同じコーラーに発信コールを行います。コールバックは、常に使用不可にしておく必要があります。デフォルトは **no** です。

calls [*outbound または inbound または both*]

このダイヤル回線をアウトバウンド・コール発信専用、インバウンド・コール受信専用、またはコールの発信と着信の両方に指定します。デフォルトは「両方」です。

destination *address_name*

このパラメーターは、ダイヤル回線が動作するために必要です。これは、このダイヤル回線が接続するリモート・ルーターのネットワーク・ダイヤル・アドレスです。LID プロトコルは、このパラメーターを着信コールに対するデフォルトの比較用アドレスとして使用します。このパラメーターは、Config> プロンプトを使用して **add isdn address** コマンドまたは **add v25-bis address** コマンドのいずれかで割り当てたアドレス名に一致している必要があります。

例: set destination remote-site-sanfrancisco

idle # *of seconds*

回線のタイムアウト期間を指定します。この指定された期間、回線上にプロトコル・トラフィックがないと、ダイヤル回線は切断されます。範囲は 0 ~ 65535 秒で、デフォルトは 60 秒です。ゼロの設定値はタイムアウト期間がないことを意味し、この回線が専用回線であることを示します。

注:

1. WAN 復元動作の場合は、アイドル・タイムアウトを 0 に設定する必要があります。
2. I.43x、X.25、またはチャネル化回線の場合、ユーザーはこのパラメーターを設定することができません。

idle-char

I.43x またはチャネル化回線に使用されるアイドル文字を指定します。

注: 通常の ISDN 回線の場合は、このパラメーターは構成できません。

有効値: 7E または FF

デフォルト値: 7E

例: **set idle-char 7E**

inbound-destination *address_name*

このパラメーターは、ダイヤル回線がアウトバウンド・コールとインバウンド・コールの両方に設定されており、このルーターのローカル・ダイヤル・アドレスが、リモート・ルーターがダイヤルするあて先ダイヤル・アドレスと異なる場合に設定します。たとえば、ルーターの1つがPBX、国際、またはLATA間交換局を通す必要がある場合は、番号が異なることになります。このパラメーターは、`Config>` プロンプトで **add isdn address** コマンドまたは **add v25-bis address** コマンドのいずれかを使って割り当てたアドレス名に一致している必要があります。着信 LID または CallerID をダイヤル回線と突き合わせるためにインバウンドあて先番号が使用されます。一致がある場合は、ダイヤル回線はコールを受け取ります。

例: **set inbound remote-site-1**

lid_out_addr *address_name*

`lid_out_addr` は、2つのルーター間のダイヤル回線の名前です。2つのルーター間に複数の回線が構成されている場合(パラレル回線)、どちらのダイヤル回線が接続するのかをルーター間で明確に知る手段が必要です。この目的のために、一方の端のルーター(コラー側)から `lid_out_addr` が送信されます。受信側の他方のルーターは、同じストリングをインバウンドあて先名として構成します。`lid_out_addr` は、以前に `config>` プロンプトから **ADD ISDN-ADDRESS** を使用して追加したアドレス名でなければなりません。

lid_used [enabled or disabled]

論理 ID をサポートしない装置への回線の論理 ID 交換を抑制します。

有効値: 使用可能または使用不可

デフォルト値: 使用不可

net #

インターフェースの基本ネットワーク番号を、この回線にマップしたいシリアル・ライン・インターフェースの # に設定します。

例:

```
Circuit Config> set net
Base net for this circuit [ ]? 2
```

priority

優先順位フィールドは、利用可能なチャネルがないときに、ある回線を別の回線より優先させることを可能にします。コール・リクエストがあり、すべてのチャネルが使用中の場合、要求元のダイヤル・オンデマンド回線の優先順位を、通信中のすべてのダイヤル・オンデマンド回線と照合します。これより低い優先順位のアウトバウンド・ダイヤル・オンデマンド回線があった場合、その回線は切断され、高い優先順位のダイヤル・オンデマンド回線のコールが設定されます。接続のアウトバウンド側の優先順位のみが考慮されます。ダイヤル・オンデマンドのインバウンド・コールは、高い優先順位のアウトバウンド・コールのためにダウンにされることはありません。ダイヤル・オンデマンドのコールは、それより低い優先順位のコールをダウンにすることはできません。

selftest-delay # of milliseconds

このパラメーターを使用して、コールが設定されてから最初のパケットが送

ダイヤル回線の構成

信されるまでの間の時間を遅らせることができます。selftest-delay を設定することにより、最初のパケットが廃棄されるのを防止できます。範囲は 0 ～ 65535 で、デフォルトは 150 です。

V.25bis ダイヤル回線の場合、モデムの同期化に時間がかかる場合は、この設定値を調整します。

ISDN ダイヤル回線の場合、一部の ISDN 交換機はあて先側の回線の設定が完了したことが通知される前にデータ転送を開始するので、ダイヤル・オンデマンド・リンクでは、この設定値を調整することが必要になることがあります。

timeslot list of slots

このダイヤル回線で使用するスロットまたはスロットのリストを指定します。回線で利用できるスロットの番号は、サービス提供者が割り当てます。リストの指定は、スロット番号をブランクで区切って示します。

注: このパラメーターは、チャンネル化 T1/E1 回線の場合にのみ使用できます。

有効値:

チャンネル化 T1 の場合: 1 ～ 24

チャンネル化 E1 の場合: 1 ～ 31

デフォルト値: なし

例: `set timeslot 1 4 5 8`

ダイヤル回線監視コマンド

表102 は、ダイヤル回線監視コマンドを説明しています。ダイヤル回線監視コマンドは、Circuit Config> プロンプトで入力します。監視変更を有効にするためには、ルーターをリスタートする必要があります。

表 102. ダイヤル回線監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』を参照してください。
Callback Exit	認証キャッシュ内の情報を追加、削除、またはリストします。直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Callback

callback コマンドを使用して、認証キャッシュ内の情報を追加、削除、またはリストします。

構文:

```
callback          add  
                   delete  
                   list
```


- add** 認証リストにコールバック番号を追加します。
- delete** 認証リストからコールバック番号を削除します。
- list** 認証リスト内のコールバック番号およびその他の情報をリストします。

第4部 付録および後付け

付録A. クイック構成リファレンス

重要

IBM 2210 の構成および監視を試みているときに、サービス端末が読み取り不能の場合は、IBM 2210 Nways Multiprotocol Router Service and Maintenance Manual の“Service Terminal Display Unreadable”の項を参照してください。

クイック構成に関する注記

クイック構成プロセスを開始する前に、以下の注記をお読みください。

1. ASCII 端末を、クイック構成プログラムを実行するサービス・ポートに接続します。導入および初期構成の手引きを参照してください。
2. 特定の項目をクイック構成を通して構成する場合、その項目の既存の構成は除去されます。
3. 構成は、アダプター上の 1 つのポートに対応するインターフェース・レベルで行います。アダプターのタイプが異なると、ポートの数が異なるので、アダプター（たとえば、X.21 アダプター、FC 2291）上のすべてのインターフェースをアクティブにするには、最大 8 つのポートを構成する必要がある場合があります。

注: ESCON アダプターまたは PCA アダプターでは、1 つの物理インターフェースに最高 16 のバーチャル・インターフェースを構成することができます。このバーチャル・インターフェースはすべて、1 つのポートに対応します。

4. **add device** コマンドを使用して、IBM 2210 に導入されているアダプターに必要なすべての網インターフェースまたはバーチャル・インターフェースを『追加』する必要があります。これは、クイック構成を実行する前に行うことが必要です。インターフェースの追加については、59ページの『Add』を参照してください。
5. **network** コマンドを使用して、ネットワーク・インターフェース構成情報を入力する必要があります。85ページの『Network』を参照してください。

選択

クイック構成プログラムの使用時に表示されるパネルで、大括弧 [] で囲んで示されている情報は、デフォルト値です。たとえば、次のように入力します。

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

- デフォルト値の Yes を使用する場合は、**Enter** を押します。
- デフォルト以外の値 (No または Quit) を使用する場合は、小括弧の中の値から選択します。
- 大括弧の中に値が表示されない場合は、デフォルトがないので、値を入力する必要があります。

終了とリスタート

- **r** を入力すれば、いつでも現行のクイック構成セクションを最初からやり直すことができます。たとえば、インターフェース構成セクションにいるときに、**r** と入力して **Enter** を押すと、そのセクションの始めに戻ります。
- クイック構成を終了するには、**q** と入力して **Enter** を押します。Config> プロンプトが表示されます。
- Config> プロンプトからクイック構成をリスタートするには、**qc** と入力して **Enter** を押します。

完了

- 構成を完了したら、構成を有効にするために、IBM 2210 をリスタートする必要があります。クイック構成プログラムの終わりに、このオプションが与えられません。

クイック構成プログラムの開始

以下の節では、クイック構成プログラム (**qconfig**) を使用したサンプル構成について説明します。

クイック構成プログラムを開始するには、Config> プロンプトで **qc** と入力します。

開始すると、プログラムは次のようなパネルを表示します。

```
Router Quick Configuration for the following:
o Bridging
  Spanning Tree Bridge (STB)
  Source Routing Bridge (SRB)
  Source Routing Transparent Bridge (SRT)
o Protocols
  IP (including OSPF, RIP, and SNMP)
  IPX
  DNA (DECnet)

Event Logging will be enabled for all configured subsystems
with logging level 'Standard'

Note: Please be warned that any existing configuration for a particular item
will be removed if that item is configured through Quick Configuration
```

イベント・ログは、システム・アクティビティ、状態の変更、データの送受信、データ誤りと内部誤り、およびサービス要求を記録します。ログ・レベルは標準 (デフォルト) に設定されます。エラー・ログについての詳細は、イベント・ログ・システム・メッセージの手引きを参照してください。

クイック構成では、次のことが行えます。

1. ブリッジングを構成する
2. プロトコルを構成する
3. ルーターをリスタートする

LAN エミュレーションの構成

ATM 装置を追加した場合、次のようなプロンプトが表示されます。

```
*****
LAN Emulation Configuration
*****

Type 'Yes' to Configure LAN Emulation
Type 'No' to skip LAN Emulation Configuration
Type 'Quit' to exit Quick Config

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

この質問からトークンリングまたはイーサネット LAN エミュレーション・クライアントのいずれも構成することができます。

ブリッジングの構成

```
*****
Bridging Configuration
*****

Type 'Yes' to Configure Bridging
Type 'No' to skip Bridging Configuration
Type 'Quit' to exit Quick Config

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

1. Configure Bridging に応答して、以下の処置の 1 つを行います。
 - **y** と入力して、ブリッジング構成プロンプトを表示する。表示されるプロンプトは、ネットワーク構成によって異なります。
 - **n** と入力して、ブリッジング構成を飛ばし、クイック構成を継続する。
 - **q** と入力して、クイック構成を終了する。これにより、Config> プロンプトが表示されます。クイック構成に再び入るには、このプロンプトの後に **qc** と入力します。
2. ブリッジングを構成することを選択すると、すべての LAN インターフェース上のスパンニング・ツリー・ブリッジング (STB) が使用可能になります。次のようなパネルが表示されます。

```
Type 'r' any time at this level to restart Bridging Configuration
STB will be enabled on all LAN interfaces
```

SRT ブリッジングを構成する場合は、**y** と入力します。そうでない場合は、**n** と入力します。構成内の各トークンリング・インターフェースごとに、インターフェース上のソース・ルーティングを使用可能にするように求めるプロンプトが出ます。

```
Configure SRT Bridging? (Yes, No): [Yes]
You are now configuring the Source Routing part of SRT Bridging
Bridge Number (hex) of this Router (1-F): [A]
```

3. ブリッジ番号を入力します。これは、2 つの並列セグメント間で固有の 1 ~ F の 16 進値です。

```
Interface 0 (Port 1) is of type Token Ring
Configure Source Routing on this interface (Yes, No): [Yes]
```

4. **y** と入力して、インターフェース上のソース・ルーティングを構成します。コンソールに、次の 2 行が表示されます。

```
Configuring Interface 0 (Port 1)
Segment Number (hex) of this Interface (1-FFF): [A1]
```

注: ソース・ブリッジングではゼロのポート番号は使用できないので、ポート番号が 1 だけ増えます。

各インターフェースに、1 ~ FFF の固有の 16 進値が割り当てられます。各リング (セグメント) 上のインターフェースは同じセグメント番号を持ちますが、セグメント番号は各リングに固有です。

各トークンリング・インターフェースごとに、次のようなプロンプトが表示されます。

```
Interface 1 (Port 2) is of type Token Ring
Configure Source Routing on this interface? (Yes, No): [Yes]
Configuring Interface 1 (Port 2)
Segment Number (hex) of this Interface (1-FFF): [A2]
```

3 つ以上のインターフェースをソース・ルーティング用に構成する場合は、内部バーチャル・セグメントに対して固有の 1 ~ FFF の 16 進値を入力します。

```
Virtual Segment Number (hex) of this Router (1-FFF): [A4]
```

5. 次のようなパネルが表示されます。

```
This is all configured bridging information:

  Interfaces configured for STB:

  Interface #   Port #   Interface Type
      0         1         Token Ring
      1         2         Token Ring

The Source Routing part of SRT Bridging has been enabled

Bridge Number of this Router: A

Interfaces configured for Source Routing:

  Interface #   Port#   Segment #   Interface Type
      0         1         A1         Token Ring
      1         2         A2         Token Ring

Virtual Segment Number of this Router: A4

Save this Configuration? (Yes, No): [Yes]
```

6. ブリッジング構成を保管し、クイック構成を継続する場合は、**y** と入力します。ブリッジング構成プロンプトを再表示する場合は、**n** と入力します。

y と入力すると、次のようなメッセージが表示されます。


```
Bridging configuration saved
```

プロトコルの構成

ブリッジング構成を保管すると、次のようなパネルが表示されます。

```
*****
Protocol Configuration
*****
Type 'Yes' to Configure Protocols
Type 'No' to skip Protocol Configuration
Type 'Quit' to exit Quick Config
Configure Protocols? (Yes, No, Quit): [Yes]
```

次の処置のいずれかを行います。

- **y** と入力して、プロトコルを構成する。
- **n** と入力して、プロトコル構成を飛ばし、クイック構成を継続する。
- **q** と入力して、クイック構成を終了する。

最初に IP を構成し、次に IPX、その後で DECnet を構成します。

IP の構成

Configure Protocol パネルに **y** と応答すると、クイック構成は次のようなメッセージを表示します。

```
Type 'r' any time at this level to restart Protocol configuration
Configure IP? (Yes, No): [Yes]
```

1. 次の処置のいずれかを行います。
 - **y** と入力して、IP を構成する。
 - **n** と入力して、IP 構成を飛ばし、クイック構成を継続する。

各インターフェースごとに、次のような行が表示されます。

```
Configuring Per-Interface IP Information

Type 'Yes' to Configure IP on this interface
Type 'No' to skip to the next interface
Type '?' to list interfaces
Type an interface # to skip to that interface
Type 'Quit' to exit Per-Interface IP Configuration

Configure IP on Interface 0 (Token Ring)?
(Yes, No, #, ?, Quit) [Yes]
IP Address: [] 128.185.141.1
Address Mask: [255.255.0.0]
```

2. IP アドレスを 10 進表記法 (たとえば、128.185.142.20) で入力します。無効な IP アドレスを入力すると、以下のエラー・メッセージの 1 つがコンソールに表示されます。

Bad address, please try again.

This address has already been assigned. Enter a different address

アドレス・マスクは、このインターフェースが接続する IP ネットワークまたはサブネットワークを表す 10 進値です。

IP アドレッシングまたはアドレス・マスクについての詳細は、プロトコルの構成と監視 解説書 を参照するか、あるいはネットワーク管理者に相談してください。

```
Per-Interface IP Configuration complete
```

```
Configuring IP Routing Information  
Enable Dynamic Routing (Yes, No): [Yes]
```

3. ルーティング・プロトコル (RIP または OSPF) がルーティング・テーブルを作成する必要がある場合は、**y** と入力します。手動で IP アドレスをルーティング・テーブルに追加する場合 (静的ルート) は、**n** と入力します。

```
Enable OSPF? (Yes, No): [Yes]
```

4. OSPF ルーティング・プロトコルを 1 次動的 IP ルーティング・プロトコルとして使用可能にする場合は、**y** と入力します。RIP は、公示の受信ではなく、公示の送信についてのみ使用可能にされます。OSPF を使用したくない場合は、**n** と入力します。RIP は、公示の送信および受信に対して使用可能にされます。

```
OSPF Enabled with Max routes = 1000 and Max routers = 50
```

Max routes は、OSPF ルーティング・ドメインにインポートされる自律システム (AS) 外部ルートの最大数です。Max routers は、ルーティング・ドメイン内の OSPF ルーターの最大数です。

```

Routing Configuration Complete

SNMP will be configured with the following parameters:

Community: public
Access:    READONLY

If you plan to use the graphical configuration tool
to download a configuration, it requires the definition
of a community name with read_write_trap access.

Define community with read_write_trap access ? (Yes, No): [Yes]

This is the information you have entered:

      Interface #      IP Address    Address Mask
      -----
      0                128.185.141.1 255.255.255.0
      1                128.185.142.1 255.255.255.0
      2                128.185.143.1 255.255.255.0

OSPF is configured, and RIP is configured only for 'sending'

SNMP has been configured with the following parameters:

Community: public
Access:    read_trap

Community: dana
Access:    read_write_trap

Save this configuration? (Yes, No): [Yes]

```

5. IP 構成を保管し、クイック構成を継続する場合は、**y** と入力します。プロトコル構成プロンプトを再表示する場合は、**n** と入力します。

IPX の構成

IP 構成を保管すると、次のようなメッセージが表示されます。

```
Configure IPX? (Yes, No): [Yes]
```

1. IPX を構成する場合は、**y** と入力します。IPX 構成を飛ばして、クイック構成を継続する場合は、**n** と入力します。

次のようなメッセージが表示されます。

```
Type 'r' any time at this level to restart IPX Configuration
IPX Configuration is already present
Configure IPX anyway? (Yes, No): [No] yes
```

2. 既存の構成を置き換える場合は、**y** と入力します。現行の構成を保持し、継続する場合は、**n** と入力します。

Configuring Per-Interface IPX Information

Type 'Yes' to Configure IPX on this interface
Type 'No' to skip to the next interface
Type an interface # to skip to that interface
Type '?' to list interfaces
Type 'Quit' to exit Per-Interface IPX Configuration

Configure IPX on Interface 0 (Token Ring)?
(Yes, No, #, ?, Quit) [Yes]

3. 次のメッセージとユーザーの応答は、トークンリング、FDDI、またはイーサネットのいずれを構成しているかによって異なります。

Configuring Interface 0 (Token Ring):

- a. 次のようなプロンプトが表示されます。

```
Token Ring encapsulation (frame) type? (TOKEN--RING MSB, TOKEN--RING LSB,  
TOKEN--RING_SNAP MSB, TOKEN--RING_SNAP LSB): [TOKEN--RING MSB]
```

- b. トークンリング・エンド・ステーション上の IPX プロトコルが使用するカプセル化タイプを入力します。

Token--Ring MSB: これは最も一般的なカプセル化タイプで、これがデフォルトです。IBM 2210 は、3 バイト 802.2 ヘッダー (0xE0, 0xE0, 0x03) を付けて発信パケットを作成します。これは、発信元および先アドレスを MSB (最上位ビット) に入れて、つまり非標準フォーマット (トークンリングに固有のアドレス・フォーマット) で送信します。

Token--Ring LSB IBM 2210 がアドレスを LSB (最下位ビット) に入れて、つまり標準フォーマットで送信する点を除いて、Token-Ring MSB と同じです。

Token-Ring SNAP MSB IBM 2210 は、8 バイトの 802.2/SNAP ヘッダー (0xAA, 0xAA, 0x03, 0x00, 0x00, 0x00, 0x81, 0x37) を付けて発信パケットを作成します。これは、発信元および先アドレスを MSB (最上位ビット) に入れて、つまり、非標準フォーマットで送信します。

Token-Ring SNAP LSB IBM 2210 がアドレスを LSB (最下位ビット) に入れて、つまり標準フォーマットで送信する点を除いて、Token-Ring SNAP MSB と同じです。

イーサネットの IPX の構成:

- a. 次のようなプロンプトが表示されます。

```
Ethernet encapsulation type? (ETHERNET_8022, ETHERNET_8023, ETHERNET_ii,  
ETHERNET_SNAP): [ETHERNET_8023]
```

- b. イーサネット・エンド・ステーション上の IPX プロトコルが使用するカプセル化タイプを入力します。

Ethernet_8022 パケットには 802.2 ヘッダーが含まれています。

Ethernet_8023 802.2 ヘッダーが付かない IEEE 802.3 パケット・フォーマットを使用します。これがデフォルトで、NetWare バージョン 4.0 より前のバージョンのデフォルトです。イーサネット 802.3 は、802.2 ヘッダーを含まないので、IEEE 802 標準に合致しません。これは、ネットワーク上の他のノードとの問題の原因になることがあります。

This is the information you have entered:

Per-Interface Configuration Information

Cir	Ifc	IPX Net(hex)	Encapsulation	IPXWAN
1	1	10	ETHERNET_8023	Not Configured
2	3	300		Not Configured
3	5	400		Not Configured
4	6	600		Enabled

Host Number for Serial Lines: 0002210A0000
IPXWAN Node ID = 2210A
IPX Router Name = ipxwan_router-2210A

Save this configuration? (Yes, No): [Yes]

6. IPX 構成を保管し、クイック構成を継続する場合は、**y** と入力します。IPX 構成プロンプトを再表示する場合は、**n** と入力します。

y と入力すると、次のようなメッセージが表示されます。

IPX configuration saved

DECnet (DNA) の構成

IPX 構成を保管すると、次のようなメッセージが表示されます。

IPX Configuration saved

Configure DNA? (Yes, No): [Yes]

1. DNA を構成する場合は、**y** と入力します。DNA 構成を飛ばして、クイック構成を継続する場合は、**n** と入力します。

Type 'r' any time at this level to restart DNA Configuration

Configuring Global DNA information

Highest Node Number (decimal) (1-1023): [32]
Router Level (Level1, Level2, DEC Level1, DEC Level2):
[Level2]
Highest Area (decimal) (1-63): [63]
Node Address (area.node): (63.32)

上の構成フィールドは、以下を考慮して構成します。

Highest Node Number

ルーターのエリアの最高ノード・アドレス。これを高く設定しすぎると、ルーターの効率に悪影響を与え、余分な記憶域が必要になります。

Router Level

ルーターがレベル 1 またはレベル 2 のどちらのルーターであるかを識別します。レベル 1 のルーターは、そのエリア内のすべてのノードを追跡しますが、エリア外のノードには関与しません。レベル 2 のルーターは、エリア間のトラフィックをルートします。

通常は Level1 または Level2 を選択します。ただし、ルーターが X.25 ネットワークを介して DEC X.25 標準準拠のルーターと通信する必要がある場合は例外で、その場合にのみ DEC Level1 または DEC Level2 を選択します。

Highest Area

この番号は、少なくともネットワーク全体で最も高いエリア番号と同じ値にすることが必要です。

Node Address

このルーターのノード ID で、ネットワーク内で固有であることが必要です。

Enter を押すと、次のようなパネルが表示されます。

```
Configuring Per-Interface DNA Information
Configuring Max Routers on each interface

Configuring Interface 0 (Ethernet)
Configure DNA on this interface? (Yes, No) [YES]
Max Routers (decimal) (1-33): [16]

Configuring Interface 1 (WAN PPP)
Configure DNA on this interface? (Yes, No) [Yes]

Configuring Interface 2 (Token Ring)
Configure DNA on this interface? (Yes, No) [Yes]
Max Routers (decimal) (1-33): [16]
```

- DECnet ネットワークに接続されるすべてのインターフェースに対して **y** と入力します。LAN の場合、Max Routers はこの回線上に存在できる他のルーターの数を指定します。ルーターの効率とメモリー所要量を考慮して、この引き数はこの回線上の隣接ルーターの合計数より少し多めに設定します。

次のようなパネルが表示されます。

```
This is the information you have entered:

Global Configuration Information

Highest Node Number:      32
Router Level:             Level2
Highest Area:             63
Node Address:             63.32

Pre-Interface Configuration Information
Interface Number          Max Routers

0                          16
1                          1
2                          16

Save this configuration? (Yes, No): [Yes]
```

- DECnet 構成を保管し、クイック構成を継続する場合は、**y** と入力します。DECnet 構成プロンプトを再表示する場合は、**n** と入力します。

y と入力すると、次のようなメッセージが表示されます。

DNA Configuration Saved

IBM 2210 のリスタート

プロトコルを構成した後、次のメッセージを受け取ります。

```
Quick Config Done
Do you want to write this configuration? (Yes, No): [Yes]
```

y を押して変更を保管し、次の情報を表示させます。

```
Default config file written successfully.
Configuration was written.
The system must be restarted for this configuration to take effect.
```

OPCON プロンプト (*) で **reload** と入力し、新しい構成で IBM 2210 をリスタートします。現行の構成を変更または表示するには、**qc** と入力します。

付録B. X.25 ナショナル・パーソナリティー

この付録では、GTE-Telenet および DDN のデフォルト設定値をリストします。

GTE-Telenet

以下のパラメーターは GTE-Telenet のデフォルト設定値です。

- コール・リクエスト (Callreq): 20
- 復旧要求 (Clearreq):
 - 再試行 (Retries): 1
 - タイマー (Timer): 18
- 切断 (Disconnect): Passive
- DP タイマー (DP-timer): 500 ミリ秒
- フレーム・ウィンドウ・サイズ (Frame window size): 7
- ネットワーク・タイプ (Network Type): CCITT
- N2 タイムアウト (N2 timeouts): 20
- パケット (Packet):
 - デフォルト・サイズ (Default size): 128
 - 最大サイズ (Maximum size): 256
 - ウィンドウ・サイズ (Window size): 2
- リセット (Reset)
 - 再試行 (Retries): 1
 - タイマー (Timer): 18
- リスタート (Restart)
 - 再試行 (Retries): 1
 - タイマー (Timer): 18
- 標準 (Standard): 1984
- T1 タイマー (T1-timer): 4
- T2 タイマー (T2-timer): 2

DDN

以下のパラメーターは DDN のデフォルト設定値です。

- コール・リクエスト (Callreq): 20
- 復旧要求 (Clearreq):
 - 再試行 (Retries): 1
 - タイマー (Timer): 18
- 切断 (Disconnect): Passive
- DP タイマー (DP-timer): 500 ミリ秒
- フレーム・ウィンドウ・サイズ (Frame window size): 7
- ネットワーク・タイプ (Network Type): CCITT
- N2 タイムアウト (N2 timeouts): 20

- パケット (Packet):
 - デフォルト・サイズ (Default size): 128
 - 最大サイズ (Maximum size): 256
 - ウィンドウ・サイズ (Window size): 2
- リセット (Reset)
 - 再試行 (Retries): 1
 - タイマー (Timer): 18
- リスタート (Restart)
 - 再試行 (Retries): 1
 - タイマー (Timer): 18
- 標準 (Standard): 1984
- T1 タイマー (T1-timer): 4
- T2 タイマー (T2-timer): 2

付録C. 複数のディスクからのルーター・ロード・ファイルの作成

ソフトウェア・ロードが複数のディスクで到着した場合、以下の手順を使用して、ロードを結合して 1 つのロード・ファイルを作成し、ルーターがブート時に使用できるようにします。

最初のディスクには、既存のロードを分割して複数のディスクでトランスポートするのに必要な、次の 4 つのファイルが入っています。

cutup.c

(標準 C コンパイラを使用してコンパイルできる UNIX C ソース・ファイル)

cutup.exe

(DOS)

以下のファイルは、分割されたロードを再アセンブルして、DOS または UNIX サーバーにロードするのに使用します。

kopy.bat

(DOS)

kopy (UNIX シェル・スクリプト)

DOS でのロード・ファイルのアセンブル

2 枚のディスクからロードをアセンブルするには、ディスク 1 (KOPY.BAT) で提供された DOS バッチ・ファイルを使用し、次の構文を用いて行います。

```
kopy <installation_drive><destination_directory>
```

ロードをアセンブルする前に、あて先ディレクトリーを作成したこと、および `installation_diskette_drive` パラメーターで指定されたドライブに最初のディスクが挿入されていることを確認してください。次の例は、これらの手順を示しています。

```
B:\>kopy b: c:\source\cutup\tmp
B:\>copy c:\gw0/B c:\source\cutup\tmp\gw.tmp
1 file(s) copied
.
Please mount the second diskette
Press any key to continue . . .
Copying the second load file fragment
B:\>
B:\>copy c:\source\cutup\tmp\gw.tmp/B + b:\gw1
c:\source\cutup\tmp\gw.tmp c:\SOURCE\CUTUP\TMP\GW.TMP
B:\GW1
1 file(s) copied
B:\>rename c:\source\cutup\tmp\gw.tmp gw.ldc
Load file reassembly was successful
B:\>
```

UNIX でのロード・ファイルのアセンブル

2 枚の UNIX ディスクからロードをアセンブルするには、ディスク 1 で提供された UNIX Bourne シェル・スクリプト (`kopy`) を使用し、次の構文を用いて行うことができます。

```
kopy<installation_drive><diskette_directory><destination_directory>
```

ロードをアセンブルする前に、あて先ディレクトリーを作成したこと、および installation_diskette_drive パラメーターで指定されたドライブに最初のディスクが挿入されていることを確認してください。次の例は、これらの手順を示しています。

```
kopy /dev/fd0 /kew /pcfs
Please insert the first diskette
Copying the first load file fragment
Please mount the second diskette
Copying the second load file fragment
Load file reassembly was successful
# ls /kew
gw0 gw1 gw.ldc
```

UNIX Bourne シェル・スクリプトを使用できない場合は、以下の手順を使用して、手でロードをアセンブルすることができます。

1. 2 枚のディスク (gw0 および gw1) に分割されたロードを、UNIX ファイル・システム上のディレクトリーにコピーする。
2. 次の UNIX コマンドを入力する。

```
cat gw0 gw1 > gw.ldc
```

得られたファイル (gw.ldc) は、アセンブルされたルーター・ロードです。

DOS でのロード・ファイルの分割

DOS のもとでロードを分割するには、CUTUP.EXE ファイルを使用して、次のようにして行います。

```
cutup<file_extension><file_name><cut_length>
```

file_extension は、分割する必要がある各スライスの先頭に付加されます。 file_name は、分割されるファイルの DOS ファイル名です。 cut_length は、CUTUP.EXE がファイルを分割するときの各フラグメントの長さです。次の例は、これらの手順を示しています。

```
C: \source\cutup>dir
Volume in drive C has no label
Volume Serial Number is XXXXXXXX
Directory of C: \SOURCE\CUTUP
.0730934:46p
..0730934:46p
GW      LDC 10225660728931:22p
CUTUP   EXE 105410902939:38a
2 file(s) 1033107 bytes
14811136 bytes free
C: \source\cutup>cutup gw.ldc gw 1000000
.....
.....
c: \SOURCE\CUTUP>dir
Volume in drive C has no label
Volume Serial Number is XXXXXXXX
Directory of C: \SOURCE\CUTUP
.0730934:46p
..0730934:46p
GW      0 10000000801931:22p
GW      LDC 10225660728931:22p
```

```
CUTUP  EXE  105410902939:38a
GW      1   225660801931:22p
4 file(s) 2055673 bytes
14811136 bytes free
```

UNIX でのロード・ファイルの分割

ロードの分割は、cutup.c を使用して行います。始めに、UNIX コンパイラーを使用してプログラムをコンパイルし、分割実行可能ファイルを作成します。その後で、次の構文を使用します。

```
cutup<file_extension><file_name><cut_length>
```

file_extension は、分割する必要がある各スライスの先頭に付加されます。file_name は、分割されるファイルの DOS ファイル名です。cut_length は、ファイルを分割するのに使用される長さ CUTUP.EXE です。次の例は、これらの手順を示しています。

```
# ls -la
total 658
drwxrwxr-x 2 root  512 Aug 114:41 .
drwxrwxr-x 26 root 1024 Aug 114:41 ..
drwxrwxr-x 2 root 24576 Aug 114:41 cutup
drwxrwxr-r 2 root1022566 Aug 114:41 gw.ldc

# cutup gw.ldc gw 100000

# ls -la
total 658
drwxrwxr-x 2 root  512 Aug 114:41 .
drwxrwxr-x 26 root 1024 Aug 114:41 ..
drwxrwxr-x 2 root 24576 Aug 114:41 cutup
drwxrwxr-r 2 root1022566 Aug 114:41 gw.ldc
drwxrwxr-r 2 root1000000 Aug 114:41 gw0
drwxrwxr-r 2 root 22566 Aug 114:41 gw1
```


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)

lfc#	インターフェース番号 (interface number)
IGP	内部ゲートウェイ・プロトコル (interior gateway protocol)
ILMI	インターリム・ローカル管理インターフェース (Interim Local Management Interface)
InARP	逆アドレス解決プロトコル (Inverse Address Resolution Protocol)
IP	インターネット・プロトコル (Internet Protocol)
IPCP	IP 制御プロトコル (IP Control Protocol)
IPPN	IP プロトコル・ネットワーク (IP Protocol Network)
IPX	インターネットワーク・パケット交換 (Internetwork Packet Exchange)
IPXCP	IPX 制御プロトコル (IPX Control Protocol)
ISDN	サービス総合デジタル網 (integrated services digital network)
ISO	国際標準化機構 (International Organization for Standardization)
Kbps	キロビット / 秒 (kilobits per second)
LAC	L2TP ネットワーク・アクセス集線装置 (L2TP Network Access Concentrator)
LAN	ローカル・エリア・ネットワーク (local area network)
LAPB	平衡型リンク・アクセス・プロトコル (link access protocol-balanced)
LAT	ローカル・エリア・トランスポート (local area transport)
LCS	LAN チャネル・ステーション (LAN Channel Station)
LCP	リンク制御プロトコル (Link Control Protocol)
LE	LAN エミュレーション (LAN Emulation)
LEC	LAN エミュレーション・クライアント (LAN Emulation Client)
LED	発光ダイオード (light-emitting diode)
LECS	LAN エミュレーション構成サーバー (LAN Emulation Configuration Server)
LES	LAN エミュレーション・サーバー (LAN Emulation Server)
LES-BUS	LAN エミュレーション・サーバー - 同報通信および未知サーバー (LAN Emulation Server - Broadcast and Unknown Server)
LF	最大フレーム、改行 (largest frame; line feed)
LIS	論理 IP サブネット (Logical IP subnet)
LLC	論理リンク制御 (logical link control)
LLC2	論理リンク制御 2 (論理リンク制御 2)
LMI	ローカル管理インターフェース (local management interface)
LNS	L2TP ネットワーク・サーバー (L2TP Network Server)
LRM	LAN 報告機構 (LAN reporting mechanism)
LS	リンク状態 (link state)
LSA	リンク状態公示 (link state advertisement)

LSA リンク・サービス体系 (Link Services Architecture)

LSB 最下位ビット (least significant bit)

LSI LAN ショートカット・インターフェース (LAN shortcuts interface)

LSreq リンク状態要求 (link state request)

LSrxl リンク状態再送リスト (link state retransmission list)

LU 論理装置 (logical unit)

MAC 媒体アクセス制御 (medium access control)

Mb メガビット (megabit)

MB メガバイト (megabyte)

Mbps メガビット / 秒 (megabits per second)

MBps メガバイト / 秒 (megabytes per second)

MC マルチキャスト (multicast)

MCF MAC フィルター (MAC filtering)

MIB 管理情報ベース (Management Information Base)

MIB II 管理情報ベース II (Management Information Base II)

MILNET
軍事ネットワーク (military network)

MOS マイクロ・オペレーティング・システム (Micro Operating System)

MOSDBG
マイクロ・オペレーティング・システム・デバッグ・ツール (Micro Operating System Debugging Tool)

MOSDDT
マイクロ・オペレーティング・システム動的デバッグ・ツール (Micro Operating System Dynamic Debugging Tool)

MOSPF
マルチキャスト拡張付き最短パス最優先オープン (Open Shortest Path First with multicast extensions)

MPC マルチパス・チャネル (Multi-Path Channel)

MPC+ ハイパフォーマンス・データ転送 (HPDT) マルチパス・チャネル (High performance data transfer (HPDT) Multi-Path Channel)

MSB 最上位ビット (most significant bit)

MSDU MAC サービス・データ単位 (MAC service data unit)

MSS マルチプロトコル・スイッチ・サービス (Multiprotocol Switched Services)

MRU 最大受信単位 (maximum receive unit)

MTU 最大伝送単位 (maximum transmission unit)

nak 否定応答 (not acknowledged)

NAS Nways スイッチ管理ステーション (Nways Switch Administration station)

NBMA 非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)

Qos	サービス品質 (Quality of Service)
RAM	ランダム・アクセス・メモリー (random access memory)
RD	ルート記述子 (route descriptor)
REM	リング・エラー監視 (ring error monitor)
REV	受信 (receive)
RFC	コメント要求 (Request for Comments)
RI	リング標識、ルーティング情報 (ring indicator; routing information)
RIF	ルーティング情報フィールド (routing information field)
RII	ルーティング情報標識 (routing information indicator)
RIP	ルーティング情報プロトコル (Routing Information Protocol)
RISC	縮小命令セット・コンピューター (reduced instruction-set computer)
RNR	受信不可 (receive not ready)
ROM	読み取り専用メモリー (read-only memory)
ROpcon	リモート・オペレーター・コンソール (Remote Operator Console)
RPS	リング・パラメーター・サーバー (ring parameter server)
RTMP	ルーティング・テーブル保守プロトコル (Routing Table Maintenance Protocol)
RTP	ルーティング更新プロトコル (RouTing update Protocol)
RTS	送信要求 (request to send)
Rtype	ルート・タイプ (route type)
rxmits	再送 (retransmissions)
rxmt	再送する (retransmit)
s	秒 (second)
SAF	発信元アドレス・フィルター (source address filtering)
SAP	サービス・アクセス・ポイント (Service access point)
SAP	サービス公示プロトコル (Service Advertising Protocol)
SCR	持続セル速度 (Sustained cell rate)
SCSP	サーバー・キャッシュ同期プロトコル (Server Cache Synchronization Protocol)
sdel	開始区切り文字 (start delimiter)
SDLC	SDLC リレー、同期データ・リンク制御 (SDLC relay, synchronous data link control)
SDU	サービス・データ単位 (Service Data Unit)
seqno	シーケンス番号 (sequence number)
SGID	サーバー・グループ ID (sever group id)
SGMP	シンプル・ゲートウェイ監視プロトコル (Simple Gateway Monitoring Protocol)
SL	シリアル・ライン (serial line)

SLIP	シリアル・ライン IP (Serial Line IP)
SMP	待機モニター・プレゼント (standby monitor present)
SMTP	シンプル・メール転送プロトコル (Simple Mail Transfer Protocol)
SNA	システム・ネットワーク体系 (Systems Network Architecture)
SNAP	サブネットワーク・アクセス・プロトコル (Subnetwork Access Protocol)
SNMP	シンプル・ネットワーク管理プロトコル (Simple Network Management Protocol)
SNPA	サブネットワーク接続ポイント (subnetwork point of attachment)
SPF	OSPF エリア内ルート (OSPF intra-area route)
SPE1	OSPF 外部ルート・タイプ 1 (OSPF external route type 1)
SPE2	OSPF 外部ルート・タイプ 2 (OSPF external route type 2)
SPIA	OSPF エリア間ルート・タイプ (OSPF inter-area route type)
SPID	サービス・プロファイル ID (service profile ID)
SPX	順次パケット交換 (Sequenced Packet Exchange)
SQE	信号品質エラー (signal quality error)
SRAM	静的ランダム・アクセス・メモリー (static random access memory)
SRB	ソース・ルーティング・ブリッジ (source routing bridge)
SRF	特定ルート・フレーム (specifically routed frame)
SRLY	SDLC リレー (SDLC relay)
SRT	ソース・ルーティング透過型 (source routing transparent)
SR-TB	ソース・ルーティング - 透過型ブリッジ (source routing-transparent bridge)
STA	静的 (static)
STB	スパンニング・ツリー・ブリッジ (spanning tree bridge)
STE	スパンニング・ツリー探索 (spanning-tree explorer)
STP	シールド付き対より線、スパンニング・ツリー・プロトコル (shielded twisted pair; spanning tree protocol)
SVC	スイッチド・バーチャル・サーキット (switched virtual circuit)
SVN	スイッチド・バーチャル・ネットワーキング (Switched Virtual Networking)
TB	透過型ブリッジ (transparent bridge)
TCN	トポロジ変更通知 (topology change notification)
TCP	伝送制御プロトコル (Transmission Control Protocol)
TCP/IP	伝送制御プロトコル / インターネット・プロトコル (Transmission Control Protocol/Internet Protocol)
TEI	端末終端点識別子 (terminal point identifier)
TFTP	トリビアル・ファイル転送プロトコル (Trivial File Transfer Protocol)
TKR	トークンリング (token ring)

TLV	タイプ/長さ/値 (Type/Length/Value)
TMO	タイムアウト (timeout)
TOS	サービスのタイプ (type of service)
TSF	透過型スパンニング・フレーム (transparent spanning frames)
TTL	活動回数 (time to live)
TTY	テレタイプライター (teletypewriter)
TX	送信 (transmit)
UA	非番号制確認 (unnumbered acknowledgment)
UDP	ユーザー・データグラム・プロトコル (User Datagram Protocol)
UI	非番号制情報 (unnumbered information)
UNI	ユーザー・ネットワーク・インターフェース (User-Network Interface)
UTP	シールドなし対より線 (unshielded twisted pair)
VCC	バーチャル・チャネル・コネクション (Virtual Channel Connection)
VINES	バーチャル・ネットワーキング・システム (VirtuAl NETworking System)
VIR	可変情報速度 (variable information rate)
VL	バーチャル・リンク (virtual link)
VNI	バーチャル・ネットワーク・インターフェース (Virtual Network Interface)
VR	バーチャル・ルート (virtual route)
WAN	広域ネットワーク (wide area network)
WRS	WAN 復元 / 再ルート (WAN restoral/reroute)
X.25	パケット交換網 (packet-switched networks)
X.251	X.25 物理レイヤー (X.25 physical layer)
X.252	X.25 フレーム・レイヤー (X.25 frame layer)
X.253	X.25 パケット・レイヤー (packet layer)
XID	交換 ID (exchange identification)
XNS	Xerox ネットワーク・システム (Xerox Network Systems)
XSUM	チェックサム (checksum)
ZIP	AppleTalk ゾーン情報プロトコル (AppleTalk Zone Information Protocol)
ZIP2	AppleTalk ゾーン情報プロトコル 2 (AppleTalk Zone Information Protocol 2)
ZIT	ゾーン情報テーブル (Zone Information Table)

用語集

この用語集には、以下からの用語および定義が含まれています。

- *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990 (米国規格協会 (ANSI) が 1990 年に著作権を取得)。この複写版が米国規格協会 (ANSI: 11 West 42nd Street, New York, New York 10036) から発売されています。定義の後に記号 (A) を付けて出典を示してあります。
- ANSI/EIA Standard--440-A, *Fiber Optic Terminology*。この複写版が米国電子工業会 (2001 Pennsylvania Avenue, N.W., Washington, DC 20006) から発売されています。定義の後に記号 (E) を付けて出典を示してあります。
- *Information Technology Vocabulary*。国際標準化機構および国際電気標準会議の第 1 合同技術委員会第 1 分科会 (ISO/IEC JTC1/SC1) によって編さんされたものです。この語彙集の刊行部分から転載した定義については、その後に記号 (I) を付けて示してあります。また、ISO/IEC JTC1/SC1 で編さん中の国際規格草案、分科会草案、および作業文書から採用した定義については、その後に記号 (T) を付けて、SC1 の加盟各国諸団体間で最終合意がなされていないことを示してあります。
- *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users' Glossary*
- *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

この用語集では、以下の形で相互参照しています。

と対比:

反対の意味または実質的に異なる意味をもつ用語を示します。

の同義語:

この用語集の該当箇所に記述されている、優先的に使用してほしい、同じ意味をもつ用語を示します。

と同義:

逆方向参照として、定義の対象となっている用語から、同じ意味をもつ他の用語をすべて参照します。

を参照:

一部の語 (特に最後の語) が同じ複数語からなる用語を参照します。

も参照:

関連する意味 (同義ではない) をもつ用語を参照します。

A

AAL. ATM アダプテーション・レイヤー (ATM Adaptation Layer)。ヘッダーを追加/除去し、セルへからのデータを細分化/再組み立てすることにより、ATM ネットワークへからのユーザー・データを適応させるレイヤー。

AAL-5. ATM アダプター・レイヤー 5 (ATM Adaptation Layer 5)。複数ある標準 AAL の 1 つ。AAL-5 はデータ通信用に設計されたもので、LAN エミュレーションおよびクラシカル IP によって使用される。

抽象構文 (abstract syntax). データ伝送に必要な特性はすべて含んでいるが、その他の明細 (たとえば、特定のコンピューター・アーキテクチャーに依存する明細など) は省略 (抽象化) されているデータ仕様。抽象構文表記法 (ASN.1) (*abstract syntax notation 1 (ASN.1)*) および基本符号化規則 (BER) (*basic encoding rules (BER)*) も参照。

抽象構文表記法 1 (ASN.1) (abstract syntax notation 1 (ASN.1)). 次の標準で指定されている抽象構文の開放型システム間相互接続 (OSI) 方式。

- ITU-T 勧告 X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T 勧告 X.680 (1994) | ISO/IEC 8824-1: 1994

基本符号化規則 (BER) (*basic encoding rules (BER)*) も参照。

ACCESS. シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、管理ノードがオブジェクトに対して提供する最小レベルのサポートを定義する、管理情報ベース (MIB) モジュール内の文節。

確認応答 (acknowledgment). (1) 受信側が送信側に肯定応答として確認応答文字を伝送すること。(T) (2) 送信された項目が受信されたことを示すこと。

アクティブ (active). (1) 運用可。(2) 別のノードまたは装置に接続された、またはそれへの接続が利用可能なノードまたは装置に関する用語。

アクティブ・モニター (active monitor). トークンリング・ネットワークにおいて、一度に 1 つのリング・ステーションによって実行される機能で、トークンの伝送を開始し、トークン誤り回復機能を提供する。現在のアクティブ・モニターに障害が起こった場合、リング上の任意のアクティブ・アダプターが、アクティブ・モニター機能を提供することができる。

アドレス (address). データ通信において、通信ネットワークに接続された各装置、ワークステーション、またはユーザーに割り当てられる固有のコード。

アドレス・マッピング・テーブル (AMT) (address mapping table (AMT)). 現在のノード・アドレスとハードウェア・アドレスのマッピングを提供する、AppleTalk ルーター内に維持されているテーブル。

アドレス・マスク (address mask). インターネット・サブネットワークにおいて、IP アドレスのホスト部分のサブネットワーク・アドレス・ビットを識別するために使用される、32 ビットのマスク。サブネット・マスク (*subnet mask*) およびサブネットワーク・マスク (*subnetwork mask*) と同義。

アドレス解決 (address resolution). (1) ネットワーク・レイヤー・アドレスを媒体特有アドレスにマッピングする方法。(2) アドレス解決プロトコル (*ARP*) (*Address Resolution Protocol (ARP)*) および *AppleTalk* アドレス解決プロトコル (*AARP*) (*AppleTalk Address Resolution Protocol (AARP)*) も参照。

アドレス解決プロトコル (ARP) (Address Resolution Protocol (ARP)). (1) インターネット・プロトコルにおいて、サポートされる大都市圏ネットワークやローカル・エリア・ネットワーク (イーサネットやトークンリングなど) が使用するアドレスに、IP アドレスを動的にマップするプロトコル。(2) 逆アドレス解決プロトコル (*RARP*) (*Reverse Address Resolution Protocol (RARP)*) も参照。

アドレッシング (addressing). データ通信において、端末局がデータの送信先の端末局を選択する方法。

隣接ノード (adjacent nodes). 他のノードとは接続していない少なくとも 1 つのパスによって相互に接続されている 2 つのノード。(T)

管理ドメイン (Administrative Domain). 1 つの管理機関によって管理される、ホストとルーターおよび相互接続ネットワークの集合。

拡張ピアツーピア・ネットワーキング機能 (Advanced Peer-to-Peer Networking) (APPN). SNA の拡張機能で、次の特長を備えている。(a) 重大な階層間の依存関係を回避することによって、単一点の障害の影響を分離できるようにした、分散ネットワーク制御の機能強化。(b) 接続、再構成、および柔軟なルート選択を容易に実現できる、動的なネットワーク・トポロジー情報の交換。(c) ネットワークの資源の動的定義。(d) 資源の登録およびディレクトリー検索の自動化。APPN は、エンド・ユーザー・サービス向けの LU 6.2 ピア間通信機能をネットワークの制御に拡張し、LU 2、LU 3、および LU 6.2 を含む複数の LU タイプをサポートする。

拡張ピアツーピア・ネットワーキング機能 (APPN) エンド・ノード (Advanced Peer-to-Peer Networking (APPN) end node). 広範囲のエンド・ユーザー・サービスを提供し、そのローカル・コントロール・ポイント (CP) と隣接するネットワーク・ノード内の CP との間のセッションをサポートするノード。このノードは、これらのセッションを使用して、隣接 CP (ネットワーク・ノード・サーバー) に資源を動的に登録し、ディレクトリー検索要求を送受信し、管理サービスを受ける。APPN エンド・ノードは、サブエリア・ネットワークに周辺ノードまたは他のエンド・ノードとして接続することもできる。

拡張ピアツーピア・ネットワーキング機能 (APPN) ネットワーク (Advanced Peer-to-Peer Networking (APPN) network). 相互接続されたネットワーク・ノードとそれらのクライアント・エンド・ノードの集合。

拡張ピアツーピア・ネットワーキング機能 (APPN) ネットワーク・ノード (Advanced Peer-to-Peer Networking (APPN) network node). 広範囲のエンド・ユーザー・サービスを提供するノードで、次のものを提供することができる。

- 分散ディレクトリー・サービス (中央ディレクトリー・サーバーへのドメインの資源の登録を含む)
- トポロジー・データベースは他の APPN ネットワーク・ノードと交換し、そのネットワーク内のネットワークが、要求されたサービス・クラスに基づいて LU-LU セッションの最適ルートを選択できるようにする。
- そのローカル LU とクライアント・エンド・ノードのセッション・サービス
- APPN ネットワークの中間ルーティング・サービス

拡張ピアツーピア・ネットワーキング機能 (APPN) ノード (Advanced Peer-to-Peer Networking (APPN) node). APPN ネットワーク・ノードまたは APPN エンド・ノード。

エージェント (agent). エージェントの役割を果たすシステム。

アラート (alert). 問題または切迫した問題を識別するためにネットワーク内の管理サービス中心拠点に送られるメッセージ。

全ステーション・アドレス (all-stations address). 通信において、同報通信アドレス (*broadcast address*) の同義語。

米国規格協会 (ANSI) (American National Standards Institute (ANSI)). 認定組織が米国の自主業界標準を作成して維持するための手順を決める、生産者、消費者、および一般の関係団体から構成される組織。(A)

アナログ (analog). (1) 連続的に変化する物理量から構成されるデータに関する用語。(A) (2) デジタル (*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、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、ホスト入出力構成プログラム (IOCP) の CNTLUNIT マクロ命令の CUADD ステートメントによって定義される。制御装置アドレスは、同じホスト上で定義された各論理区画ごとに固有でなければならない。

D

D ビット (D-bit). 送達確認ビット (Delivery-confirmation bit)。X.25 通信において、受信側からのエンド・エンド確認 (送達確認) が必要な場合に 1 にセットされる、データ・パケットまたはコール・リクエスト・パケット内のビット。

デーモン (daemon). 標準サービスを行うために無人で実行されるプログラム。デーモンには、そのタスクを実行するために自動的に起動されるものと、定期的に動作するものがある。

データ・キャリア検出 (DCD) (data carrier detect (DCD)). 受信回線信号検出器 (RLSD) (received line signal detector (RLSD)) の同義語。

データ回線 (data circuit). (1) 両方向データ通信の手段を提供する、関連付けられた一対の送信チャネルと受信チャネル。(I) (2) SNA においては、リンク接続 (link connection) の同義語。(3) 物理回線 (physical circuit) およびバーチャル・サーキット (virtual circuit) も参照。

注:

1. データ交換装置相互間では、データ回線は、データ交換装置で使用するインターフェースのタイプによって、データ回線終端装置 (DCE) を含むことがある。
2. データ端末とデータ交換装置またはデータ集線装置との間では、データ回線は、データ装置側のデータ回線終端装置を含み、またデータ交換装置またはデータ集線装置側の DCE と類似の装置を含むことがある。

データ回線終端装置 (DCE) (data circuit-terminating equipment (DCE)). データ端末において、データ端末装置 (DTE) と回線の間で信号変換および符号化を行う装置。(I)

注:

1. DCE は、独立した機器であるか、DTE または中間装置に組み込まれている。
2. DCE は、伝送路のネットワーク側で一般的に必要とされる機能を果す。

データ・リンク接続識別子 (DLCI) (data link connection identifier (DLCI)). フレーム・リレー・サブポート、またはフレーム・リレー・ネットワークの PVC セグメントの数字識別子。1 つのフレーム・リレー・ポート内の各サブポートは、固有の DLCI を持っている。下表 (米国規格協会 (ANSI) 標準 T1.618 および国際電信電話諮問委員会 (ITU-T/CCITT) 標準 Q.922 から抜粋) は、特定の DLCI 値に関連する機能を示している。

DLCI 値	機能
0	チャネル内信号
1-15	未使用
16-991	フレーム・リレー接続手順を用いて割り当て
992-1007	フレーム・リレー・ベアラー・サービスのレイヤー 2 管理
1008-1022	未使用
1023	チャネル内のレイヤー管理

データ・リンク制御 (DLC) (data link control (DLC)). データ・リンク (SDLC リンクまたはトークンリングなど) 上のノードが、情報を正確に交換するために使用する規則。

データ・リンク制御 (DLC) レイヤー (data link control (DLC) layer). SNA において、2 つのノード間のリンクを介するデータ転送をスケジュールし、そのリンクの誤り制御を行うリンク・ステーションから構成されるレイヤー。データ・リンク制御の例としては、ビット順次リンク接続の SDLC や、システム/370 チャネルのデータ・リンク制御がある。

注: 通常、DLC レイヤーは物理トランスポート機構から独立しており、上位レイヤーに送るデータの健全性が確保される。

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、その後にネットワーク・レイヤーからの制御情報が続き、その後にアプリケーション・プロトコル・データが入っている。(2) データ・リンク交換 (*data link switching*) も参照。

コード化 (encode). 元の形に再び変換できるような方法で、規則を使用してデータを変換すること。(T)

エンド・ノード (EN) (end node (EN)). (1) 拡張ピアツーピア・ネットワークング (*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/遅延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、いくつかのロットで成り立ち、各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 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 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 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 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す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、特殊な形式の通報通信。

マルチパス・チャンネル (multipath channel) (MPC). VTAM-VTAM 間両方向通信用として複数の単一方向サブチャンネルを使用するチャンネル・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。パーマネント・バーチャル・サーキット (PVC) (*permanent virtual circuit (PVC)*) と対比。

同期 (synchronous). (1) 共通タイミング信号のような特定の事象の発生に依存する 2 つ以上のプロセス。(T) (2) 規則的または予測可能な時間的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・マネージメント・プロトコル (SNMP) において、例外条件を報告するために、管理ノード (エージェント機能) が管理ステーションに送るメッセージ。

トランク・アダプター (trunk adapter). トランク・ラインに NBBS 体系のトランスポート・サービスを提供するコードを実行する、Nways スイッチの 2216 以外の型式のモジュール。2216 では、ポート・アダプターとトランク・アダプターの機能が結合された多重化ポート/トランク・アダプター (MPTA) が使用されている。

トランク・ライン (trunk line). 2 つの Nways スイッチを接続する高速伝送路。同軸ケーブル、ファイバー・ケーブル、または無線を使用でき、通信会社からリースすることもできる。

Nways スイッチでは、各トランク・ラインは 1 つの NBBS トランクに関連付けられている。

トンネル (Tunnel). トンネルとは、LNS-LAC の対によって定義されるもので、LAC と LNS の間で PPP データグラムを伝える。単一のトンネルで多くのセッションを多重化することができる。制御接続が同じトンネルを介して作動する場合は、すべてのセッションおよびトンネル自体の設定、解放、および保守を制御する。

トンネル伝送 (tunneling). トランスポート・ネットワークを、単一の通信リンクまたは LAN のように扱うこと。カプセル化 (encapsulation) も参照。

T1. 米国では、1.544-Mbps の公衆アクセス回線。24 個の 64 Kbps チャネルで利用可能。欧州方式 (E1) は 2.048 Mbps で伝送する。

U

出荷時設定アドレス (universally administered address). ローカル・エリア・ネットワークにおいて、製造時にアダプターに永久的に符号化されるアドレス。出荷時設定アドレスは固有である。ローカル管理アドレス (locally administered address) と対比。

ユーザー・データグラム・プロトコル (UDP) (User Datagram Protocol (UDP)). インターネット・プロトコルにおいて、低信頼性のコネクションレス・データグラム・サービスを提供するプロトコル。このプロトコルを使用して、ある計算機またはプロセス上のアプリケーション

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、たとえば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
第 2 レベル 16, 18
プロトコル
構成プロセス 25
動作 (監視) プロセス 25
アクセス, 監視コマンドへの 599
アクセス, MP 構成プロンプトへの 595
アドレス
ISDN 715
アドレス項目
削除 120
変更 117
アドレス登録, LAN エミュレーションの 298
アドレスの入力
ATM 309
アドレス・レゾリューション, LAN エミュレーションの 298
アドレス・ワイルドカード, DTE 418
暗号化
構成 559
イーサネット
カプセル化タイプ 762
統計の表示 279
ネットワーク・インターフェース
構成 283
IPX のカプセル化タイプ 762
イーサネット監視コマンド 286
要約 285
collisions 286
イーサネット構成コマンド
アクセス 283
要約 283
connector-Type 284
ip-encapsulation 284, 336
list 284
physical-address 284
イーサネット・オペレーショナル・コマンド
アクセス 285
イーサネット・ネットワーク・インターフェース
使用 279
イベント
原因 170
イベント番号パラメーター 171

イベント・ログ
サブシステム 171
イメージ
指定時刻にロード 108
インターセプト文字 13
変更 37
インターフェース
プロセスのリスト 7
ユーザー 7
予備 256
予備の構成 50
ATM 監視コマンド 324, 327
ATM 構成コマンド 314
インターフェース装置
追加 59
変更 66
インターフェースの制約事項 52
エンド・システム識別子 289
オフファン・スイッチド・バーチャル・サーキット
フレーム・リレー 447
オフファン・パーマネント・バーチャル・サーキット
フレーム・リレー 447
オンライン・ヘルプ 27, 29

[カ行]

概説, LAN エミュレーションの 287
回線情報速度 (CIR) 454
回線速度 455
回線の競合
ISDN 716
回線輻輳 457
減速による対応 457
概要
ソフトウェアの 7
バーチャル・コネクション (VC) 535
バイナリー同期通信リレー (BRLY) 653
ELS ネット・フィルター監視コマンド 238
ELS ネット・フィルター構成コマンド 206
カプセル化タイプ 762
可変情報速度
フレーム・リレーの 456
環境, 下位レベルの
終了 13
監視
性能監視コマンド 249
ネットワーク・インターフェース 24
ATM 313
MP コマンドへのアクセス 599

監視コマンド

マルチリンク PPP プロトコル 600

LAN エミュレーション・クライアント (LEC) 331

完成を使用可能にする

CONFIG コマンド 78

完成を使用不可にする

CONFIG コマンド 77

キープアライブ・タイマー、XTP の設定 434

技術サポートへのアクセス 50

起動、予備インターフェースの 150

機能

構成プロセスとコンソール・プロセスへのアクセス
24

逆方向明示的輻輳回避 458

逆方向明示的輻輳通知 (BECN)

フレーム・リレー 450

クイック構成 9, 17

説明 48

ブリッジング構成 757

プロトコル構成

手順 759

IP ユーザー・インターフェース 759

IPX ユーザー・インターフェース 761

クイック構成リファレンス 756

グループ

削除 191

グループ名パラメーター 173

クロック、設定と変更 97

クロックとケーブルのタイプ 365

ケーブル・タイプ、クロックと 365

コードの導入 110

コールの検証

ISDN 716

コールバック制御プロトコル (CBCP)

PPP の 533

交換 SDLC コールイン・インターフェース

構成 621

更新

構成 14

構成

暗号化 559

既存の構成に基づく 14

更新 14

推奨事項 13

ネットワーク・インターフェース 21

バーチャル・コネクション (VC) 536

初めて 14

マルチリンク PPP インターフェース 591

シリアル・リンク上 592

ダイヤル回線で 591

マルチシャシー MP の 593

レイヤー 2 トンネル・ネット上で 593

構成 (続き)

メモリーの更新 98

ユーザー・アクセス 49

DECnet 764

IP 759

IPX 761

MP プロンプトへのアクセス 595

OPCON 33

PPP コールバック 530

XTP 429

構成、ブートの 101

構成、予備インターフェースの 50

起動 150

構成 50

制約事項 52

定義 256

構成コマンド

マルチリンク PPP プロトコル (mp) 595

GWCON プロンプト 25

set prompt-level

プレフィックスをホスト名に追加 94

構成情報の削除 73

構成ファイル

アクセス 106

構成ロード

妥当性検査 108

考慮事項

バーチャル・コネクション (VC) 535

マルチリンク PPP プロトコル (MP) 590

コプロセッサ

構成プロセスへのアクセス 19

コマンド

入力 11

exit 13

コマンド活動記録 29, 30

コンポーネント、LAN エミュレーションの 288

[サ行]

最小情報速度

フレーム・リレーの 456

最大情報速度

フレーム・リレーの 456

最大フレーム・サイズ・ポリシー 294, 296

再ロード 17

装置 6

識別、プロンプトの 12

時刻

イメージのロードの起動 108

システム・ダンプの使用 57

終了

下位レベルの環境 13

終了、装置の 6

- 終了、Telnet セッションの 44
- 出力
 - 他のコンソールに送信 35
 - 中断 37
 - 廃棄 36
- 順方向明示的輻輳回避 458
- 順方向明示的輻輳通知 (FECN)
 - フレーム・リレー 449
- 使用可能にする、メモリー・ダンプを 122
- 冗長度、LAN エミュレーション・サーバーの 304
- シリアル PPP リンク
 - MP の構成 592
- シリアル・ライン・インターフェース
 - 構成 365
 - 構成プロセスへのアクセス 365
- 信号バージョンの構成、LAN エミュレーションの 292
- 信頼性、LAN エミュレーションの 304
- 推奨事項
 - 構成 13
- スイッチの機種 727
 - ISDN の設定 733
- 性能
 - 構成 247
- 性能監視コマンド
 - アクセス 249
 - 要約 249
 - disable 250
 - enable 250
 - list 250
 - report 250
 - set 251
- 性能構成コマンド
 - 要約 248
 - disable 248
 - enable 248
 - list 249
 - set 249
- セキュリティー、LAN エミュレーションの 305
- セッション
 - 終了 38
- 接続要求タイマー 419
- 設定と変更、時刻、日付、およびクロックの 97
- 選択子 289
- 相互形閉域ユーザー・グループ
 - 概要 373
- 装置
 - 再ロード 6, 17
 - 時間統計の表示 166
 - 終了 6
 - リポート 40
- 装置コンソール
 - 使用 4

- 装置コンソール (続き)
 - リモート 5
 - ローカル 4
- 装置ソフトウェア
 - 再ロード 40
 - ユーザー・インターフェース 4
- 装置プロセス
 - 情報の表示 40
 - 接続 11, 42
- ソフトウェア
 - 概要 7
 - 導入 110
 - ユーザー・インターフェース 7
- ソフトウェア導入 110
- ソフトウェア/コードの導入 110

[夕行]

- 第 2 レベル
 - プロセス
 - アクセス 16, 18
 - タイプ/長さ値 296
 - ダイヤルイン回線
 - バーチャル・コネクション (VC) 535
 - 構成 536
 - 考慮事項 535
 - add device の例 20
 - ダイヤル回線
 - 構成 675, 696, 725
 - 追加 674, 694, 725
 - ISDN 714
 - MP の構成 591
 - ダイヤル回線監視コマンド
 - callback 750
 - ダイヤル回線構成コマンド
 - 要約 743
 - delete 744
 - encapsulator 744
 - list 745
 - set 747
 - ダンプ
 - 構成 109
 - ダンプ・ファイル
 - 説明 109
 - 中間ローカル管理インターフェース 291
 - 超過バースト・サイズ
 - 定義 455
 - フレーム・リレー用の設定 455
 - 重複ポリシー値 296
 - 追加 20
 - ダイヤルイン回線
 - 例 20

追加 20 (続き)

マルチリンク PPP 回線

例 20

データ・ダイレクト VCC 300

データ・リンク接続識別子 (DLCI)

フレーム・リレー 444, 449

ディレクトリー

ブートおよびダンプ 109

転送プロセス

例 104

トークンリング

IPX のカプセル化タイプ 762

トークンリング監視コマンド

アクセス 261

要約 261

dump 262

トークンリング構成コマンド

アクセス 257

要約 257

list 258

LLC 258

llc 262

LLC 用に使用可能化 260

media 259

packet-size 259

set 259

source-routing 260

speed 261

トークンリング・インターフェース

表示される統計 263

トークンリング・ネットワーク・インターフェース

構成 257

統計

消去 152

統合リンク・レイヤー・マネージメント (CLLM)

説明 453

動的ルーティング

OSPF 760

RIP 760

[ナ行]

ナショナル・パーソナリティーの設定 424

認証

リモート装置

使用する PPP インターフェースの構成 530

PPP インターフェースの構成 529

認定バースト・サイズ

最大フレーム・サイズとの関係 455

定義 454

ネットワーク制御プロトコル (NCP)

PPP インターフェースの 532

ネットワーク制御プロトコル (NCP) (続き)

コールバック制御プロトコル (CBCP) 533

ブリッジング制御プロトコル (BCP) 532

AppleTalk 制御プロトコル 532

APPN HPR 制御プロトコル 535

APPN ISR 制御プロトコル 535

Banyan VINES 制御プロトコル (BVCP) 532

DECnet 制御プロトコル (DNCP) 533

IP 制御プロトコル (IPCP) 533

IPv6 制御プロトコル (IPv6CP) 534

IPX 制御プロトコル (IPXCP) 535

OSI 制御プロトコル (OSICP) 535

ネットワーク・インターフェース

監視 24, 255

検査 165

構成 18, 255

構成の表示 21

構成プロセスへのアクセス 19

コンソール・プロセス 18, 255

コンソール・プロセスへのアクセス 23

削除 75

サポートされるインターフェース 21

使用可能にする 165

使用不可にする 156

情報の表示 81, 153, 158

GWCON インターフェース・コマンド 255

SDLC 650

X.25 411

ネットワーク・ソフトウェア

統計情報の表示 164

[ハ行]

バーチャル・コネクション (VC)

概要 535

構成 536

考慮事項 535

バイナリー同期通信リレー (BRLY)

概要 653

考慮事項 657

サンプル構成 654

パケット完了コード 173

パケット転送機能

CONFIG 環境に入る 89

パケット・トレース監視コマンド

パケット・トレース 222

off 236

on 236

reset 236

set 236

subsystems 237

trace-status 238

- パケット・トレース監視コマンド (続き)
 - view 238
- パケット・トレース・メッセージ
 - パケット・トレース 222
- 初めて
 - 構成 14
- パスワード 5
- パスワード、ユーザー用の設定 65
- バックアップ・ピア機能、XTP の 418
- パラメーター
 - イベント番号 171
 - 構成 90
 - 主要な LAN エミュレーション 287
 - LAN エミュレーションの 307
- パラメーターのデフォルト値
 - X.25 368
- 日付、設定と変更 97
- 表示、ホスト名をソフトウェア VPD と共に 94
- ブート
 - オプション 135
 - オプションへのアクセス 135
 - オプション・プロンプト 137
 - 統合ブート装置から 134
 - 方式 133
 - BOOTP 134
 - BOOTP の失敗 134
 - TFTP から 135
- ブート CONFIG コマンド
 - 要約 113
 - add 114
 - change 117
 - copy 119
 - delete 120
 - describe 121
 - disable 121
 - enable 122
 - erase 122
 - list 123
 - load 125
 - store 127
 - tftp 129
 - timedload 127
- ブート CONFIG プロセス
 - 使用可能なコマンド 113
 - 説明 101
 - 入る 113
- ブートおよびダンプ構成データベース
 - 表示 123
- ブートストラップ・プロトコル 102
- ブート・オプション
 - 説明 133
 - プロンプト 137
- ブート・オプション (続き)
 - B (ブート) 138
 - BC (Config-only モードでのブート) 138
 - BM (コンソール照会を使用したブート) 139
 - BN (コンソール照会を使用したブート、実行禁止) 141
 - BP (BOOTP を使用したブート) 141
 - CC (構成メモリの消去) 147
 - D (保管済み構成を使用したダンプ) 142
 - DIAG (IBM 拡張診断プログラムの実行) 143
 - DM (コンソール照会を使用したダンプ) 144
 - LC (構成メモリのロード) 145
 - UB (TFTP ブート構成の表示) 144
 - UC (ハードウェア構成の表示) 144
 - UG (RAM 内アドレスでの実行) 145
 - ZB (ZModem ブート) 147
 - ZC (ZModem 構成メモリのロード) 147
- ブート・ディレクトリー 109
- ブート・ファイル
 - 説明 101
 - メイン・メモリへのコピー 125
- フォーラム準拠 LEC
 - 特定クライアントの構成 333
 - ARP 構成 333
- 不揮発性構成メモリー
 - 置き換え 66
- 輻輳監視 457
- 輻輳通知と回避
 - 逆方向明示的輻輳回避 458
 - 順方向明示的輻輳回避 458
- ブリッジング、クイック構成を使用するの構成 757
- ブリッジング制御プロトコル (BCP)
 - PPP の 532
- フレーム・リレー 445
 - インターフェースの初期化 445
 - オーファン・スイッチド・バーチャル・サーキット 447
 - オーファン・パーマネント・バーチャル・サーキット 447
 - 回線情報速度 454
 - 回線速度 455
 - 拡張アドレス 449
 - 可変情報速度 456
 - 可変情報速度 (VIR) 456
 - 管理状態報告書 453
 - 説明 452
 - 全状態報告書 453
 - リンク整合性検証報告書 453
 - 逆方向明示的輻輳通知 450
 - 構成 462, 465
 - 構成へのアクセス 462
 - コマンド/レスポンス 449

- フレーム・リレー 445 (続き)
 - 最小情報速度 456
 - 最大情報速度 456
 - 順方向明示的輻輳通知 449
 - 使用 443
 - 紹介 443
 - 静的 ARP 469
 - 帯域幅予約 460
 - 超過バースト・サイズ 455
 - データ速度 454
 - データ・リンク接続識別子 (DLCI) 449
 - ネットワーク 444
 - ネットワーク管理 452
 - ネットワーク・インターフェース 465, 515
 - バーチャル・サーキット 443
 - パーマネント・バーチャル・サーキット 445
 - 廃棄可能性 450
 - 必須グループ 448
 - 輻輳通知と回避 458
 - フレーム転送の説明 450
 - フレーム・フォーマット 448
 - プロトコル・アドレス・マッピング 451
 - マルチキャスト・エミュレーション 451
 - ユーザー・データ 450
 - DLCI (データ・リンク接続識別子) 444
 - HDLC フラグ 449
 - LAPD データ・リンク・プロトコル 443, 448
 - LMI マネージメント・エンティティ 452
 - PVC および 448
 - PVC マネージメントの使用可能化 463
 - SVC
 - FRF 4 452
 - SVC マネージメントの使用可能化 464
- フレーム・リレー監視コマンド
 - 要約 500
 - clear 501
 - disable 501
 - cilm 501
 - notify-fecn-source 501
 - throttle-transmit-on-fecn 501
 - enable 501
 - cilm 502
 - notify-fecn-source 502
 - throttle-transmit-on-fecn 502
 - list 502
 - all 502
 - circuit 502
 - lmi 502
 - permanent-virtual-circuits 502
 - pvc-groups 502
 - llc 512
 - notrace 512

- フレーム・リレー監視コマンド (続き)
 - set 513
 - trace 514
- フレーム・リレー構成コマンド 476, 478
 - 要約 465
 - add 466
 - permanent-virtual-circuit 466
 - protocol-address 466
 - add protocol-address
 - IP プロトコル 469
 - add-protocol
 - AppleTalk2 プロトコル 469
 - DN プロトコル 469
 - IPX プロトコル 469
 - change 475
 - disable
 - 圧縮 476
 - 暗号化 476
 - 断片化 476
 - 輻輳 457
 - cir-monitor 476
 - cilm 476
 - congestion-monitor 476
 - dn-length-field 476
 - lmi 476
 - lower-dtr 476
 - multicast-emulation 476
 - notify-fecn-source 476
 - no-pvc 476
 - orphan-circuits 476
 - protocol-broadcast 476
 - throttle-transmit-on-fecn 476
 - enable
 - 圧縮 478
 - 暗号化 478
 - 輻輳 458
 - cir-monitor 478
 - cilm 478
 - congestion-monitor 478
 - dn-length-field 478, 480
 - lmi 479
 - lower-dtr 479
 - multicast-emulation 479
 - notify-fecn-source 479
 - no-pvc 479
 - orphan-circuits 479
 - protocol-broadcast 479
 - throttle-transmit-on-fecn 479
 - list 485
 - all 485
 - fragmentation-capable-pvcs 485
 - hdlc 485

フレーム・リレー構成コマンド 476, 478 (続き)
 lmi 485
 permanent-virtual-circuits 485
 protocol-address 485
llc 492
remove
 permanent-virtual-circuit 493
 protocol-address 493
remove protocol-address
 Appletalk2 プロトコル 493
 IP プロトコル 493
 IPX プロトコル 493
remove-protocol
 DN プロトコル 493
set
 転送遅延パラメーター 495
 cable 495
 clocking 495
 crc-type 495
 default cir 495
 frame-size 495
 lmi-type 495
 n1-parameter 495
 n2-parameter 495
 n3-parameter 495
 p1-parameter 495
 t1-parameter 495
フレーム・リレー・スイッチド・バーチャル・サーキット (SVC) 445
 除去 494
 追加 470
 変更 475
 リスト 491, 492, 511
フレーム・リレー・パーマネント・バーチャル・サーキット (PVC)
 変更 475
フレーム・リレー・フォーラム・インプリメンテーション合意 4 (FRF 4) 452
フロー制御
 パケット 152
ブロードキャストおよび不明サーバー 289, 299
ブロードキャスト・マネージャー 301
プロセス
 第 2 レベル
 アクセス 16, 18
 通信 7
 リスト 7
プロセスへの接続 11
プロトコル
 クイック構成を使用した構成 759
 構成および動作プロセス
 アクセス 25

プロトコル (続き)
 構成環境に入る 89
 構成プロセス 255, 256
 構成プロセスに入る 25
 コンソール・プロセス 17, 255, 256
 コンソール・プロセスに入る 25
 情報の表示 153
 リストの生成 89
プロトコル・コンソール・プロセス
 入る 25
プロンプト
 識別 12
 装置プロセス 12
 ブート・オプション 137
 CONFIG 12
 GWCON 12
 OPCON 12
閉域ユーザー・グループ
 概要 372
 拡張
 タイプ 373
 構成 374
 cug 0 オーバーライド 374
 XTP サポート
 概要 420
 X.25 回線の確立 373
ヘルプ
 コンソール・コマンド 13, 660
ヘルプの入手 13, 660
ポイント・ポイント構成コマンド
 アクセス 540
 要約 540
 list 544
 LLC 549
ポイント・ポイント・インターフェース
 構成 539
ポイント・ポイント・ネットワーク・インターフェース
 使用 519
ポイント・ポイント・プロトコル (PPP) 533
 アドレス・フィールド 521
 概要 519
 コールバック制御プロトコル (CBCP) 533
 構成プロセスへのアクセス 539
 情報フィールド 521
 制御フィールド 521
 認証 526
 ネットワーク制御プロトコル (NCP) 532
 フラグ・フィールド 521
 ブリッジング制御プロトコル (BCP) 532
 フレーム構造 520
 フレーム・チェック・シーケンス・フィールド 521
 プロトコル・フィールド 521

ポイント・ポイント・プロトコル (PPP) 533 (続き)

- リンク確立パケット 524
- リンク終了パケット 526
- リンク制御プロトコル (LCP) 522
- リンク保守パケット 526
- AppleTalk 制御プロトコル 532
- APPN HPR 制御プロトコル 535
- APPN ISR 制御プロトコル 535
- Banyan Vines 制御コントロール (BVCP) 532
- DECnet 制御プロトコル (DNCP) 533
- IPv6 制御プロトコル (IPv6CP) 534
- IPX 制御プロトコル (IPXCP) 535
- LCP パケット 523
- OSI 制御プロトコル (OSICP) 535

方法、プロトコルをリストする 89

- ホスト名の表示 94
- ホスト名を時刻と 共に表示 94
- ホスト名を日付と共に表示 94
- ホスト名を復帰と共に表示 94
- ホスト名を変更と共に表示 94
- ポリシー 287
 - 一致 294
- ポリシーとポリシー値 293

[マ行]

- マジック・ナンバー 108
- マルチシャシー MP 591
 - 構成 593
- マルチリンク PPP プロトコル (MP)
 - 概要 589
 - 監視コマンド 600
 - 構成
 - シリアル・リンク 592
 - ダイヤル回線 591
 - マルチシャシー MP 593
 - レイヤー 2 トンネル伝送ネット 593
 - 構成コマンド 595
 - 考慮事項 590
 - マルチシャシー 591
 - レイヤー 2 トンネル伝送との関係 591
- マルチリンク PPP プロトコル (mp) 監視コマンド
 - アクセス 599
- マルチリンク・プロトコル (MP) 構成プロンプト
 - アクセス 595
- メッセージ
 - 解釈 171
 - 受信 168
 - 説明 173
- メッセージ処理プロセス
 - 影響するコマンド 167
 - 説明 167
 - 出入り 167

メッセージ処理プロセス (続き)

- メッセージの受信 168
- OPCON コマンド 167
- メッセージ・バッファ
 - 概要 187
- ELS 監視コマンド 241
 - flush 242
 - list 242
 - log 242
 - nolog 243
 - read-file 244
 - set 244
 - tftp 245
 - view 246
 - write-buffer 246
- ELS 構成コマンド 209
 - list 209
 - log 209
 - nolog 210
 - set 211

メモリー

- 情報の消去 224
- メモリー・ダンプ
 - 使用可能にする 122
 - 使用不可にする 121

基づく、構成に

- 既存の 14

[ヤ行]

- ユーザー・アクセス
 - 構成 49
 - パスワードの設定 65
 - パスワードの変更 71
 - ユーザー情報のリスト 84
 - ユーザーの削除 76
 - ユーザーの追加 65
 - ユーザー変更 72
- ユーザー・インターフェース
 - ソフトウェア 7
 - プロセス 7

[ラ行]

- リスタート、IBM 2210 の 766
- リスト、構成の 89
- 利点、LAN エミュレーションの 287
- リモート DTE の検索 418
- リモート装置
 - 認証
 - 使用する PPP インターフェースの構成 530
 - PPP インターフェースの構成 529

- リモート端末 5
- リモート・コンソール 5
- リモート・ログイン 5
- リモート・ログ記録
 - 出力例 182
 - その他の考慮事項 186
 - 重複ログ記録 186
 - 反復シーケンス番号 186
 - IP アドレスを含むメッセージ 186
- リンク制御プロトコル (LCP)
 - パケット 523
 - PPP との関係 522
- ルーター
 - 情報の表示 81
- ルーター・ソフトウェア
 - 通信 162
- ルーター・ソフトウェアの導入 110
- ルーター・ロード・ファイル
 - 複数のディスクからの作成 769
 - DOS でのアセンブル 769
 - DOS での分割 770
 - UNIX でのアセンブル 769
 - UNIX での分割 771
- ルート記述子ポリシー 294
- 例、クイック構成 756
- レイヤー 2 トンネル伝送
 - マルチリンクとの関係 PPP (MP) 591
- レイヤー 2 トンネル伝送ネット
 - 構成 MP 593
- ローカル XTP
 - 説明 419
- ローカル端末 4
- ローカル・コンソール 4
- ロード・ファイル、ルーターの
 - 複数のディスクからの作成 769
 - DOS でのアセンブル 769
 - DOS での分割 770
 - UNIX でのアセンブル 769
 - UNIX での分割 771
- ログイン
 - リモート・コンソールからの 5
 - リモート・ログイン名 5
 - ローカル・コンソールからの 5

[ワ行]

ワイルドカード、DTE アドレス 418

[数字]

- 2210
 - ブート・サーバーとして 102
- 2210 の構成 148

2210 へのソフトウェア/コードのロード 110

A

- activate
 - GWCON コマンド 150
- add
 - ブート CONFIG コマンド 114
 - フレーム・リレー構成コマンド 466
 - add 640
 - ATM 構成コマンド 315
 - ATM バーチャル・インターフェース構成コマンド 322
 - BSC リレー構成コマンド 660
 - CONFIG コマンド 59
 - ELS 構成コマンド 190
 - SDLC 監視コマンド 640
 - SDLC 構成コマンド 627
 - SDLC リレー構成コマンド 608
 - XTP 監視コマンド 437
 - XTP 構成コマンド 429
 - X.25 構成コマンド 394
- add device の例
 - マルチリンク PPP 20
- advanced
 - ELS 監視コマンド 214
 - ELS 構成コマンド 190
- AppleTalk 制御プロトコル
 - PPP の 532
- APPN HPR 制御プロトコル
 - PPP の 535
- APPN ISR 制御プロトコル
 - PPP の 535
- ARP 構成
 - config 334
 - list 335
 - remove 335
 - set 335
- ATM
 - アドレスの入力方法 309
- ATM LLC 監視コマンド
 - list 327
- ATM アドレッシング 289
- ATM 監視コマンド
 - アクセス 323
 - インターフェース 324, 327
 - 要約 323
 - atm-llc 324
 - interface 323
 - list 324
 - trace 325
 - wrap 326

ATM 構成コマンド
 アクセス 313
 インターフェース 314
 要約 314
 add 315
 disable 321
 enable 320
 LE-Client 314
 LE-Services 314
 list 315
 qos 316
 remove 316
 set 316

ATM ネットワーク・インターフェース
 監視 313
 使用 309

ATM バーチャル・インターフェース監視コマンド
 要約 327

ATM バーチャル・インターフェース構成コマンド
 要約 321
 add 322
 list 322
 remove 322

atm-llc
 ATM 監視コマンド 324

B

Banyan VINES 制御プロトコル (BVCP)
 PPP の 532

BCM 301
 発信元ルート・ブリッジングのサポート 303
 IP のサポート 302
 IPX のサポート
 BCM IPX サーバー・ファーム 302
 LEC を防止 302
 NetBIOS のサポート 303
 NetBIOS ネーム・シェアリング 303

BCM IPX サーバー・ファーム
 LEC を防止 302

boot
 CONFIG コマンド 66

Boot CONFIG
 プロセス
 CONFIG から入る 66

BOOTP
 サーバー 104
 使用可能/使用不可 103
 転送プロセス 102
 BOOTP クライアントとしてのルーター 102
 BOOTP の失敗 142

BOOTP 転送
 説明 102
BOOTP 転送の使用可能/使用不可 103
BOOTP の失敗 134
BSC インターフェース
 構成 659
BSC インターフェース構成コマンド
 list 664
 set 665
BSC リレー
 概要 653
 監視環境へのアクセス 668
 構成 659
 組み合わせマルチポイント 654
 バーチャル・マルチポイント 654
 物理マルチポイント 653, 654
 ポイント・ポイント 653

 考慮事項 657
 サンプル構成 654
BSC リレー監視コマンド
 要約 669
 clear-port-statistics 669
 disable 669
 enable 670
 list 670

BSC リレー構成コマンド
 要約 660
 add 660
 delete 662
 disable 663
 enable 663
 list 665

buffer
 GWCON コマンド 151

BUS 287, 289
 機能 300
 接続 299

BUS の機能 300
BUS への接続 299

C

callback
 ダイヤル回線監視コマンド 750

calls
 監視コマンド 736
 V.25bis 監視コマンド 684
 V.34 監視コマンド 704

change
 ブート CONFIG コマンド 117
 フレーム・リレー構成コマンド 475
 CONFIG コマンド 66
 XTP 構成コマンド 432

- change (続き)
 - X.25 構成コマンド 401
- channels
 - 監視コマンド 737
- CHAP
 - 監視 560
 - 構成 540
 - PPP の認証 528
- CIR
 - オーファン・パーマネント・バーチャル・サーキット
 - CIR 454
 - 監視 456, 457
 - VIR に対する関係 456
- circuits
 - 監視コマンド 737
 - V.25bis 監視コマンド 685
 - V.34 監視コマンド 705
- clear
 - フレーム・リレー監視コマンド 501
 - BSC リレー監視コマンド 669
 - CONFIG コマンド 73
 - ELS 監視コマンド 214
 - ELS 構成コマンド 191
 - GWCON コマンド 152
 - PPP 監視コマンド 561
 - SDLC 監視コマンド 641
- clear-counters
 - LLC 監視コマンド 271
- clear-port-statistics
 - SDLC リレー監視コマンド 617
- CLLM
 - 説明 453
- CLLM サポート 459
- collisions
 - 監視コマンド 286
- CONFIG コマンド
 - 完成を使用可能にする 78
 - 完成を使用不可にする 77
 - 要約 58
 - add 59
 - boot 66
 - change 66
 - clear 73
 - delete 75
 - disable 77
 - enable 77
 - event 80
 - features 80
 - List 81
 - load 84
 - network 85
 - patch 86
 - CONFIG コマンド (続き)
 - protocol 89
 - qconfig 89
 - set 90
 - system retrieve 95
 - system view 96
 - time 97
 - unpatch 98
 - update 98
 - write 98
 - CONFIG プロセス
 - アクセス 16
 - システム・ダンプ 57
 - 終了 57
 - 使用可能なコマンド 58
 - 説明 47
 - 入る 17, 57
 - configuration
 - 情報の表示 153
 - GWCON コマンド 152
 - OPCON command 19
 - OPCON コマンド 34
 - Config-Only モード
 - 自動的に入る 48
 - 手動で入る 48
 - 説明 48
 - connector-Type
 - イーサネット構成コマンド 284
 - console
 - OPCON コマンド 35
 - copy
 - ブート CONFIG コマンド 119
 - copy-config コマンド
 - リモート・ホストから 119
 - リモート・ルーターから 119
 - ルーター内部で 119
 - CPU
 - メモリー使用量の表示 159
 - create
 - ELS ネット・フィルター監視コマンド 239
 - ELS ネット・フィルター構成コマンド 207

D

- DDN
 - デフォルト設定値 767
- DECnet 制御プロトコル (DNCP)
 - PPP の 533
- DECnet の構成 764
- default
 - ELS 構成コマンド 191

delete

- ダイヤル回線構成コマンド 744
- ブート CONFIG コマンド 120
- BSC リレー構成コマンド 662
- CONFIG コマンド 75
- delete 641
- ELS 構成コマンド 191
- ELS ネット・フィルタ監視コマンド 240
- ELS ネット・フィルタ構成コマンド 208
- ISDN 76
- SDLC 監視コマンド 641
- SDLC 構成コマンド 628
- SDLC リレー構成コマンド 610
- XTP 監視コマンド 437
- XTP 構成コマンド 433
- X.25 構成コマンド 403

describe

- ブート CONFIG コマンド 121

diags

- OPCON コマンド 35

disable

- 監視コマンド 250
- 性能構成コマンド 248
- データ圧縮 540
- 認証プロトコル 540
- ブート CONFIG コマンド 121
- フレーム・リレー監視コマンド 501
- フレーム・リレー構成コマンド
 - cir-monitor 476
- マルチリンク・プロトコル 540
- ATM 構成コマンド 321
- BSC リレー監視コマンド 669
- BSC リレー構成コマンド 663
- CONFIG コマンド 77
- ELS ネット・フィルタ監視コマンド 240
- ELS ネット・フィルタ構成コマンド 208
- GWCON コマンド 156
- Lower DTR 540
- SDLC 構成コマンド 628
- SDLC リレー監視コマンド 617
- SDLC リレー構成コマンド 610
- SDLC リンク確立コネクション 641
- XTP 構成コマンド 434
- X.25 構成コマンド 384

display

- ELS 監視コマンド 215
- ELS 構成コマンド 191

divert

- OPCON コマンド 35

DLCI (データ・リンク接続識別子)

- フレーム・リレー 444

DOS

- ロード・ファイルのアセンブル 769
- ロード・ファイルの分割 770

DTE アドレス・ワイルドカード 418

dump

- トークンリング監視コマンド 262

E

ELAN タイプ・ポリシー 296

ELAN ネーム・ポリシー 295

ELS

- 概念 170
- 監視 189
- 再ロード 224
- 障害追及の例 3 177
- 使用法 174
- 説明 169
- トラップ 227, 234
- トラップの設定 175
- トラブルシューティングのための使用 176
- トラブルシューティングの例 1 176
- トラブルシューティングの例 2 176
- 入る 80
- 保管 225
- メッセージの解釈 171
- メッセージ・バッファ
 - 概要 187
- リモート・ログ記録
 - 出力 182
 - その他の考慮事項 186
 - 重複ログ記録 186
 - 反復シーケンス番号 186
 - IP アドレスを含むメッセージ 186
- remote-logging 200, 225
- Telnet の使用による出力の取り込み 175
- tracing 202, 228

els

- OPCON コマンド 36

ELS 監視コマンド

- メッセージ・バッファ 241
- flush 242
- list 242
- log 242
- nolog 243
- read-file 244
- set 244
- tftp 245
- view 246
- write-buffer 246

要約 213

- advanced 214

ELS 監視コマンド (続き)

- clear 214
- display 215
- files 215
- filter 216
- list 216
- nodisplay 219
- noremove 219
- notrace 220
- notrap 221
- remote 222
- remove 224
- restore 224
- retrieve 224
- save 225
- set 225
- statistics 231
- trap 234
- view 235

ELS 構成

- 出入り 170

ELS 構成環境

- 出入り 189

ELS 構成コマンド

- メッセージ・バッファ 209

- list 209
- log 209
- nolog 210
- set 211

- 要約 189

- add 190
- advanced 190
- clear 191
- default 191
- delete 191
- display 191
- filter 192
- list 192
- nodisplay 194
- noremove 195
- notrace 196
- notrap 197
- remote 198
- set 199
- trace 233
- trap 205

ELS コンソール環境

- リモート・ログ記録 177
- リモート・ワークステーション
 - 構成 178
- レベル
 - 定義 178

ELS コンソール環境 (続き)

- 2210 リモート・ログ記録
 - 構成 180
- syslog ファシリテーター
 - 定義 178

ELS 動作環境

- 出入り 213

ELS ネット・フィルター監視コマンド

- 概要 238
- create 239
- delete 240
- disable 240
- enable 240
- list 241

ELS ネット・フィルター構成コマンド

- 概要 206
- create 207
- delete 208
- disable 208
- enable 208
- list 208

ELS メッセージ 173

- 回転の管理 174
- グループ 173
- 説明 173
- トラップ 205, 234
- トラップの抑制 197, 221
- トラップの抑制 (notrap) 221
- トレースの抑制 220
- ネットワーク情報 173
- 表示の抑制 194
- 表示の抑制 (nodisplay) 219
- リモート・ファイルへのログ記録の使用可能化 (Remote) 198, 222
- リモート・ログの抑制 (noremove) 195, 219
- ログ・レベル 172
- trace 204
- tracing 233

enable

- 監視コマンド 250
- 性能構成コマンド 248
- データ圧縮 542
- 認証プロトコル 542
- ブート CONFIG コマンド 122
- フレーム・リレー監視コマンド 501
- フレーム・リレー構成コマンド 478
- マルチリンク・プロトコル 542
- ATM 構成コマンド 320
- BSC リレー監視コマンド 670
- BSC リレー構成コマンド 663
- CHAP 542
- CONFIG コマンド 77

enable (続き)
 ELS ネット・フィルター監視コマンド 240
 ELS ネット・フィルター構成コマンド 208
 GWCON コマンド 156
 Lower DTR 542
 PAP 542
 SDLC 監視コマンド 641
 SDLC 構成コマンド 629
 SDLC リレー監視コマンド 618
 SDLC リレー構成コマンド 611
 XTP 構成コマンド 434
 X.25 構成コマンド 383
enable lmi 499
encapsulator
 ダイヤル回線構成コマンド 744
erase
 ブート CONFIG コマンド 122
error
 GWCON コマンド 157
ESI 289
event
 CONFIG コマンド 80
 GWCON コマンド 157
 OPCON コマンド 36
exit 660
 コンソール・コマンド 660
exit コマンド 13

F

features 80
 シン・サーバー機能 80
 帯域幅予約 80, 158
 符号化サブシステム 80
 CONFIG コマンド 80
 GWCON コマンド 158
 MAC フィルター 80, 158
 WAN 復元 158
 WAN 復元/再ルート 80
files
 ELS 監視コマンド 215
filter
 ELS 監視コマンド 216
 ELS 構成コマンド 192
flush
 OPCON コマンド 36

G

GTE-Telenet
 デフォルト設定値 767

828 MRS V3.3 ソフトウェア使用者の手引き

GWCON
 コマンド
 SDLC インターフェース 650
 X.25 インターフェース 411
 プロセス
 入る 17
GWCON コマンド
 インターフェース 255
 要約 150
 activate 150
 buffer 151
 clear 152
 configuration 152
 disable 156
 enable 156
 error 157
 event 157
 features 158
 interface 158
 memory 159
 network 161
 protocol 162
 queue 162
 reset 164
 statistics 164
 test 165
 uptime 166
GWCON プロセス
 説明 149
 出入り 149

H

halt
 OPCON コマンド 37
HDLC フラグ
 フレーム・リレー・フレーム内の 449
HSSI
 set
 cable 496, 552
 circuit congestion defaults 496
 clocking 496, 553
 crc type 497
 crc-type 495
 line speed 498

I

IBD
 ファイル転送の考慮事項 107
 ファイル名の定義 106

- IBM 2210
 - Config-Only モード 48
- ILMI 機能、LAN エミュレーションの 291
- ILMI の使用による LECS の探索 292
- intercept
 - OPCON コマンド 37
- interface
 - ATM 監視コマンド 323
 - GWCON コマンド 158
- IP
 - TFTP 104
- IP (インターネット・プロトコル)、クイック構成を使用した構成 759
- IP 監視コマンド
 - ping 39
- IP 制御プロトコル (IPCP)
 - PPP の 533
- IP の構成 759
- IPv6 制御プロトコル (IPv6CP)
 - PPP の 534
- IPX (インターネットワーク・パケット交換機能)
 - イーサネット・カプセル化タイプ 762
 - クイック構成を使用した構成クイック構成 761
 - トークンリング・カプセル化タイプ 762
- IPX 制御プロトコル (IPXCP)
 - PPP の 535
- IPX の構成 761
- ip-encapsulation
 - イーサネット構成コマンド 284, 336
- ISDN
 - アドレス 715
 - アドレスの削除 76
 - インターフェースの制約事項 721
 - 概説 713
 - 監視プロセスへのアクセス 735
 - コールの検証 716
 - 構成 722, 729
 - サポートされるスイッチ 721
 - サンプル構成 719
 - ダイヤル回線 714
 - ダイヤル回線の競合 716
 - デマンド回線を介したコスト制御 716
 - 要件と制約 721
 - GWCON コマンド 740
 - PPP 構成 721
- ISDN インターフェース
 - 使用 713
- ISDN 監視コマンド
 - 要約 735
 - calls 736
 - channels 737
 - circuits 737

- ISDN 監視コマンド (続き)
 - L2_Counters 738
 - L3_Counters 738
 - parameters 739
 - statistics 739
 - TEI 738
- ISDN 構成コマンド
 - 要約 729
 - list 730
 - remove 730
 - set 730
 - set switch variant 733
- I.431 スイッチ 727

L

- L2_Counters
 - 監視コマンド 738
- L3_Counters
 - 監視コマンド 738
- LAN あて先ポリシー (MAC アドレス・ポリシー) 295
- LAN エミュレーション 287
 - 概要 287
 - 関連 ILMI 機能の概説 291
 - クライアント 288
 - 構成サーバー 288
 - 構成サーバー、ポリシーとポリシー値 293
 - コンポーネント 288
 - コンポーネントの ATM アドレス 291
 - サーバー 288
 - 最大フレーム・サイズ・ポリシー 296
 - 主要な構成パラメーター 307
 - 冗長度 304
 - 信号バージョン 292
 - 信号バージョンの構成 292
 - 信頼性 304
 - セキュリティ 305
 - 重複ポリシー値 296
 - データ・ダイレクト VCC の確立 300
 - ブロードキャストおよび不明サーバー (BUS) 289
 - ブロードキャスト・マネージャー (BCM) 301
 - 利点 287
 - ATM アドレッシング 289
 - ATM でのアドレッシング 289
 - BUS 289
 - BUS の機能 300
 - BUS への接続 299
 - ELAN タイプ・ポリシー 296
 - ELAN ネーム・ポリシー 295
 - ILMI 機能、関連の 291
 - ILMI の使用による LECS の探索 292
 - LAN エミュレーション構成サーバーの概説 292

- LAN エミュレーション 287 (続き)
 - LAN エミュレーション用のルーター拡張機能の概説 301
 - LAN エミュレーション・コンポーネントの ATM アドレス 291
 - LECS LAN あて先ポリシー (MAC アドレス・ポリシー) 295
 - LECS TLV 296
 - LECS の概説 292
 - LECS の割り当てポリシー例 294
 - LECS、ポリシーとポリシー値 293
 - LES によるアドレス解決 298
 - LES へのアドレス登録 298
 - LES への接続 297
- LAN エミュレーション構成サーバー 292
- LAN エミュレーションの主要パラメーター 307
- LAN エミュレーション用のルーター拡張機能 301
- LAN エミュレーション・クライアント (LEC) 329
 - 構成 329, 331
- LAN エミュレーション・コンポーネントの ATM アドレス 291
- LAN エミュレーション・サーバー 297
- LE クライアント 288
- LEC 監視コマンド
 - アクセス 351
 - 要約 352
 - list 353
 - mib 357
- LECS 287
 - 最大フレーム・サイズ・ポリシー 296
 - 重複ポリシー値 296
 - とLAN エミュレーション 288
 - 割り当てポリシー例 294
 - ELAN タイプ・ポリシー 296
 - ELAN ネーム・ポリシー 295
 - LAN あて先ポリシー (MAC アドレス・ポリシー) 295
 - LAN エミュレーションのコンポーネント 292
 - LAN 拡張 292
 - TLV 296
- LES 287, 288
 - アドレス解決 298
 - アドレス登録 298
 - 接続 297
- LE-Client
 - ATM 構成コマンド 314
- LE-Services
 - ATM 構成コマンド 314
- list 25
 - イーサネット構成コマンド 284
 - 監視コマンド 250, 353
 - 性能構成コマンド 249
- list 25 (続き)
 - ダイヤル回線構成コマンド 745
 - トークンリング構成コマンド 258
 - ブート CONFIG コマンド 123
 - フレーム・リレー監視コマンド 502
 - フレーム・リレー構成コマンド 485
 - ポイント・ポイント構成コマンド 544
 - ATM LLC 監視コマンド 327
 - ATM 監視コマンド 324
 - ATM 構成コマンド 315
 - ATM バーチャル・インターフェース構成コマンド 322
 - BSC インターフェース構成コマンド 664
 - BSC リレー監視コマンド 670
 - BSC リレー構成コマンド 665
 - CONFIG コマンド 81
 - ELS 監視コマンド 216
 - ELS 構成コマンド 192
 - ELS ネット・フィルタ監視コマンド 241
 - ELS ネット・フィルタ構成コマンド 208
 - ISDN 構成コマンド 730
 - list 642
 - LLC 監視コマンド 271, 362
 - LLC 構成コマンド 350
 - PPP 監視コマンド 561
 - SDLC 監視コマンド 642
 - SDLC 構成コマンド 629
 - SDLC リレー監視コマンド 618
 - SDLC リレー構成コマンド 611, 612
 - V.25bis 構成コマンド 680
 - V.34 構成コマンド 700
 - XTP 監視コマンド 438
 - XTP 構成コマンド 434
 - X.25 監視コマンド 408
 - X.25 構成コマンド 404
- list devices 313
- list devices コマンド 20, 283, 539, 679, 699
- llc
 - トークンリング監視コマンド 262
 - トークンリング構成コマンド 258, 262
 - フレーム・リレー監視コマンド 512
 - フレーム・リレー構成コマンド 492
 - ポイント・ポイント構成コマンド 549
 - PPP 監視コマンド 585
 - PPP 構成コマンド 549
- LLC 監視コマンド
 - アクセス 271
 - 要約 271
 - clear-counters 271
 - list 271, 362
 - set 277, 362

LLC 構成コマンド
 アクセス 267
 要約 267, 350, 362
 list 268, 350
 set 269, 350
LLC ネットワーク・インターフェース
 構成 267
LMI マネージメント・エンティティ 452
load
 ブート CONFIG コマンド 125
 CONFIG コマンド 84
loading
 特定時刻に 108
login
 使用不可にする 77
logout
 OPCON コマンド 38

M

MAC アドレス・ポリシー (LAN あて先ポリシー) 295
media
 トークンリング構成コマンド 259
memory
 情報の入手 38
 情報の表示 159
 GWCON コマンド 159
 OPCON コマンド 38
mib
 監視コマンド 357
MONITR プロセス
 影響するコマンド 167
 説明 167
 出入り 167
 メッセージの受信 168
 OPCON コマンド 167
MPPE オプション
 リスト 545
msgsz
 SDLC 監視コマンド 645
MS-CHAP
 PPP の認証 528

N

national disable
 X.25 構成コマンド 387
national enable
 X.25 構成コマンド 385
national restore
 X.25 構成コマンド 393

national set
 X.25 構成コマンド 388
network
 環境 85, 161
 CONFIG コマンド 85
 GWCON コマンド 161
network コマンド 21, 283, 313, 352, 539, 679, 699
nodisplay
 ELS 監視コマンド 219
 ELS 構成コマンド 194
noremote
 ELS 監視コマンド 219
 ELS 構成コマンド 195
notrace
 フレーム・リレー監視コマンド 512
 ELS 監視コマンド 220
 ELS 構成コマンド 196
notrap
 ELS 監視コマンド 221
 ELS 構成コマンド 197

O

off
 パケット・トレース監視コマンド 236
on
 パケット・トレース監視コマンド 236
OPCON インターフェース
 構成 33
OPCON コマンド
 要約 34
 configuration 34
 console 35
 diags 35
 divert 35
 els 36
 event 36
 flush 36
 halt 37
 intercept 37
 logout 38
 memory 38
 reload 40
 status 40
 suspend 41
 talk 42
 telnet 42
OPCON の説明 33
OPCON プロセス
 アクセス 33
 使用可能なコマンド 34
 説明 33

OPCON プロセス (続き)

戻る 13

要約 7

OSI 制御プロトコル (OSICP)

PPP の 535

OSPF 760

P

packet trace

パケット・トレース監視コマンド 222

packet-size

トークンリング構成コマンド 259

parameters

監視コマンド 739

V.25bis 監視コマンド 686

V.34 監視コマンド 706

X.25 監視コマンド 408

patch

CONFIG コマンド 86

perf コマンド 248

physical-address

イーサネット構成コマンド 284

pin parameter

設定 200

ping

IP 監視コマンド 39

PPP

IP 制御プロトコル (IPCP) 533

PPP インターフェース監視プロセス

アクセス 560

PPP 監視コマンド

要約 560

clear 561

IPCP パラメーターのリスト 561

LCP パラメーターのリスト 561

list 561

dn 583

dncp 583

osi 584

osicp 583

llc 585

PPP コールバック

構成 530

PPP 構成コマンド

IPCP パラメーターの設定 549

LCP パラメーターの設定 549

list

ccp 545

ecp 545

set 549

PPP の PAP 認証 527

prompt-level

構成コマンド

プレフィックスをホスト名に追加 94

ホスト名の表示 94

追加機能

ホスト名を VPD と共に表示 94

ホスト名を時刻と共に表示 94

ホスト名を日付と共に表示 94

ホスト名を復帰と共に表示 94

ホスト名を変更と共に表示 94

protocol

CONFIG コマンド 89

GWCON コマンド 162

protocol コマンド 25, 26

Q

qconfig

CONFIG コマンド 89

QoS

ATM 構成コマンド 316

queue

GWCON コマンド 162

Quick Config モード 49

手動で入る 49

R

reload

OPCON コマンド 6, 40

remote

ELS 監視コマンド 222

ELS 構成コマンド 198

remove

フレーム・リレー構成コマンド 492

ATM 構成コマンド 316

ATM バーチャル・インターフェース構成コマンド
322

ELS 監視コマンド 224

ISDN 構成コマンド 730

report

監視コマンド 250

reset

パケット・トレース監視コマンド 236

GWCON コマンド 164

X.25 監視コマンド 409

restore

ELS 監視コマンド 224

retrieve

ELS 監視コマンド 224

RIP 760

S

save

ELS 監視コマンド 225

SDLC

交換コールイン・インターフェース
構成 621

構成 621, 625

構成手順 621

構成へのアクセス 625

構成要件 623

ネットワーク・インターフェース 650

SDLC 監視コマンド

アクセス 639

要約 640

clear 641

link counters 642

list 642

SDLC 構成コマンド

要約 626

add 627

delete 628

disable 628

enable 629, 641

list 629

msgsz 645

set 632

SDLC 接続

サポート 626

SDLC リレー

監視環境へのアクセス 616

構成 605, 607

構成へのアクセス 608

SDLC リレー監視コマンド

要約 617

clear-port-statistics 617

disable 617

enable 618

list 618

SDLC リレー構成コマンド

要約 608

add 608

delete 610

disable 610

enable 611

list 611, 612

set 614

set

監視コマンド 251

性能構成コマンド 249

ダイヤル回線構成コマンド 747

トークンリング構成コマンド 259

set (続き)

パケット・トレース監視コマンド 236

フレーム・リレー監視コマンド 513

フレーム・リレー構成コマンド 494

ATM 構成コマンド 316

BSC インターフェース構成コマンド 665

CONFIG コマンド 90

ELS 監視コマンド 225

ELS 構成コマンド 199

ISDN 構成コマンド 730

LLC 監視コマンド 277, 362

LLC 構成コマンド 350

PPP 構成コマンド 549

SDLC 監視コマンド 645

SDLC 構成コマンド 632

SDLC リレー構成コマンド 614

V.25bis 構成コマンド 681

V.34 構成コマンド 701

XTP 構成コマンド 434

X.25 構成コマンド 378

source-routing

トークンリング構成コマンド 260

speed

トークンリング構成コマンド 261

statistics

監視コマンド 739

ELS 監視コマンド 231

GWCON コマンド 164

V.25bis 監視コマンド 687

V.34 監視コマンド 707

X.25 監視コマンド 410

status

OPCON コマンド 40, 539

store

ブート CONFIG コマンド 127

subsystems

パケット・トレース監視コマンド 237

suspend

OPCON コマンド 41

system retrieve

CONFIG コマンド 95

system view

CONFIG コマンド 96

T

talk

OPCON コマンド 42, 248, 249

TCP/IP, X.25 トラフィックのトランスポート 415

TDM (時分割多重) 443

TEI

監視コマンド 738

telnet
 セッションの終了 44
 接続のクローズ 44
 OPCON コマンド 42
 Telnet セッションの状態の入手 43
telnet コマンド 43
telnet セッションの入手 43
telnet 接続 5
 クローズ 44
 状態の入手 43
test
 GWCON コマンド 165
 SDLC 監視コマンド 649
 test 649
TFTP
 からのブート 135
 説明 104
 IBD との間 106
 IBD に関する考慮事項 107
tftp
 ブート CONFIG コマンド 129
time
 設定と変更 97
 CONFIG コマンド 97
timedload
 ブート CONFIG コマンド 127
Tinygram 圧縮 550
TLV
 ELAN ベースで定義 296
trace
 フレーム・リレー監視コマンド 514
 ATM 監視コマンド 325
 ELS 構成コマンド 233
trace-status
 パケット・トレース監視コマンド 238
trap
 ELS 監視コマンド 234
 ELS 構成コマンド 205

U

UNIX
 ロード・ファイルのアセンブル 769
 ロード・ファイルの分割 771
unpatch
 CONFIG コマンド 98
update
 CONFIG コマンド 98
uptime
 GWCON コマンド 166

V

V25bis アドレス 84
VC
 フレーム・リレー 443
view
 パケット・トレース監視コマンド 238
 ELS 監視コマンド 235
V.25bis
 アドレスの追加 673
 監視プロセスへのアクセス 684
 構成 673, 679
 構成へのアクセス 679
 GWCON コマンド 689
V.25bis 監視コマンド
 要約 684
 calls 684
 circuits 685
 parameters 686
 statistics 687
V.25bis 構成コマンド
 要約 679
 list 680
 set 681
V.34
 アドレスの追加 693
 監視プロセスへのアクセス 703
 構成 693, 699
 構成へのアクセス 699
 GWCON コマンド 709
V.34 監視コマンド
 要約 704
 calls 704
 circuits 705
 parameters 706
 statistics 707
V.34 構成コマンド
 要約 699
 list 700
 set 701

W

wrap
 ATM 監視コマンド 326
write
 CONFIG コマンド 98

X

XTP

監視コマンド

- Add 437
- Delete 437
- List 438

キープアライブ・タイマーの設定 434

構成 429

構成コマンド 429

- Add 429
- Change 432
- Delete 433
- Disable 434
- Enable 434
- List 434
- Set 434

構成手順 420

使用 415

ナショナル・パーソナリティーの設定 424

バックアップ・ピア機能 418

閉域ユーザー・グループ

概要 420

ローカル XTP

説明 419

X.25

パラメーターのデフォルト値 368

X.25 インターフェース

相互形閉域ユーザー・グループ

概要 373

閉域ユーザー・グループ

回線の確立 373

概要 372

拡張タイプ 373

構成 374

cug 0 の処理のオーバーライド 374

X.25 監視コマンド

- 要約 407
- list 408
- parameters 408
- reset 409
- statistics 410

X.25 構成コマンド

- 要約 377
- add 394
- change 401
- delete 403
- disable 384
- enable 383
- list 404
- national disable 387
- national enable 385

X.25 構成コマンド (続き)

- national restore 393
- national set 388
- set 378

X.25 トランスポート・プロトコル (XTP) 415

X.25 ネットワーク・インターフェース

監視プロセスへのアクセス 407

構成 377

使用 367

統計 411

ナショナル・パーソナリティー 368, 767



Printed in Japan

SC88-6372-07



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:



Nways
マルチプロトコル・ルーティン
グ・サービス

MRS V3.3 ソフトウェア使用者の手引き