

INFONET3790
マルチポートブルータ
取扱説明書

古河電気工業株式会社

ご注意

この装置の耐用年数は6年です。それ以降の使用は弊社にご相談ください。

この装置の修理可能期間は、製造終了後6年間とさせていただきます。

本マニュアルには、「外国為替及び外国貿易管理法」に定める戦略物資関連技術が含まれています。従って、本マニュアルを輸出する場合には、同法に基づく許可が必要とされます。なお、本マニュアルを廃棄する場合は、完全に粉砕して下さい。

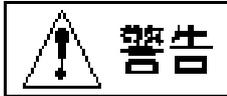
この装置は、第一種情報処理装置（商工業地域において使用されるべき情報処理装置）で商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会（VCCI）基準に適合しております。

従って、住宅地域またはその隣接した地域で使用すると、ラジオ、テレビジョン受信機等に受信障害を与えることがあります。

取扱説明書に従って正しい取り扱いをして下さい。



安全のために



下記の注意を守らないと火災・感電により死亡や大けがの原因となります。

設置

- 本装置の分解・解体・改造・再生を行わないでください。
火災・感電・故障の原因となります。

ケーブル

- 本装置のケーブル類の上には、絶対に重いものをのせたり、折り曲げたりしないでください。
重いものをのせると、ケーブルに傷がついて、感電や火災の原因となります。

使用上のご注意

- 電源ケーブルがACコンセントに接続されているときには、濡れた手で本装置に触れないでください。
感電の原因となります。
- 本装置の電源は、AC100V (50/60Hz) を使用してください。
異なる電圧で使用すると、感電、発煙、火災の原因となります。
- 本装置内部には、水などの液体を入れないでください。
感電の原因となります。
- 雷が鳴り出したら、ケーブルや電源ケーブルに触れないでください。
感電の原因となります。



下記の注意を守らないと、周辺の家電に損害を与えたり、本装置の故障の原因となります。

設置

- 本装置は、屋内に設置してください。
故障の原因となります。
- 極端な高温、あるいは低温状態や温度変化の激しい場所で使用しないでください。
故障の原因となります。
- 直射日光の当たる場所や発熱機器（ストーブ、コンロなど）のそばで使用しないでください。
故障の原因となります。
- 水や油などの液体がかかる場所、湯気がかかる場所、湿気やほこりの多い場所で使用しないでください。
火災・感電・故障の原因となります。
- 塩害地域では使用しないでください。
故障の原因となります。
- 衝撃や振動の加わる場所で使用しないでください。
故障の原因となります。
- 薬品の噴囲気中や薬品にふれる場所で使用しないでください。
故障の原因となります。
- モータなど、強い磁界を発生する装置のそばで使用しないでください。
故障の原因となります。
- ラジオやテレビジョン受信機等のそばで使用しないでください。
ラジオやテレビジョン受信機等に雑音が入る場合があります。
- 本装置は側面に内部の熱を逃がすための通気孔が設けてあるので、装置の側面に物を置いたりして、通気孔をふさがないようにください。
通気孔をふさぐと、内部の温度が上昇して、故障の原因となります。
- 本装置をならべて使用する場合、側面に3cm以上の間隔をあけてください。
故障の原因となります。
- 国内のみで使用してください。
本装置は国内仕様になっていますので、海外ではご使用になれません。

ケーブル

- 本装置のケーブル類を抜き差しする場合には、先に装置の電源ケーブルを抜いてください。
- 本装置のケーブル類は、足などを引っかかないように整理してください。
ケーブル類に足などを引っかけると、危険です。
また、本装置の使用中に電源ケーブルが抜けると、重要なデータが失われることもあります。

電源

- 安全のために、電源（AC100V）には、必ずアースを取ってください。また、電源ケーブルは添付品をご使用ください。添付品以外の電源ケーブルのご使用は避けてください。
アースを接続しないと、感電の原因となります。
- 本装置の電源ケーブルは、タコ足配線にしないでください。
コンセントが過熱し、火災の原因となることがあります。

使用上のご注意

- 内部に液体や金属類など異物が入った状態で使用しないでください。
故障の原因となります。
- 本装置を移動するときは、必ず電源ケーブルを抜いてください。
故障の原因となります。

本装置のお手入れ

- 汚れはやわらかい布によるからぶきか、水または中性の洗剤を含ませて固くしぼった布で軽く拭いてください。
水や中性洗剤は、絶対に本体に直接かけないでください。
- ベンジンやシンナーなど（揮発性のもの）は使用しないでください。
本装置の外装を傷めたり、故障の原因となったりします。
- 殺虫剤などをかけないでください。
故障の原因となります。

著作権および商標について

本装置のファームウェアには以下の著作権が含まれています。

GateD, Release 3. Copyright (c) 1990, 1991, 1992 by Cornell University. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Cornell University and its collaborators. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

GateDaemon Project
Information Technologies/Network Resources
143 Caldwell Hall
Cornell University
Ithaca, NY 14853-2602

GateD is maintained and developed by Cornell University and its collaborators.

商標

Internetwork Packet Exchange and IPX are registered trademarks of Novell, Inc.
NetWare is a registered trademark of Novell, Inc.

AppleTalk, EtherTalk, Macintosh, LaserWriterはアップルコンピュータ社の商標です。

DECnetはDEC社の商標です。

Stacker is a registered trademark and LZS is a trademark of Stac Electronics.

はじめに

このたびは、INFONET3790マルチポートブロータをお買い上げいただき、まことにありがとうございます。本取扱説明書は、INFONET3790マルチポートブロータの基本的な取扱いについて説明しています。ご使用の際には、本取扱説明書をお読みにになり、正しくご使用くださるようお願い申し上げます。また、本装置をご使用になる間は、本取扱説明書を大切に保管してください。

尚、本製品および本取扱説明書を正しくお使いいただく上で以下の前提知識を必要とします。

前提知識

- LAN (Local Area Network) IEEE802.3/Ethernet 規格、または同程度の知識を有していること。
- TCP/IP (Transmission Control Protocol / Internet Protocol) や、IPX (Internet Packet Exchange) およびAppleTalkなどのネットワークの知識を有していること。
- SNMP (Simple Network Management Protocol) およびMIB (Management Information Base) のネットワーク管理についての知識を有していること。
- コンピュータの一般知識を有し、キーボード操作ができること。

まず、梱包物をご確認ください。

梱包物

- INFONET3790マルチポートブロータ 1台
- 電源ケーブル (3m) 1本
- モジュラーケーブル (5m) 8本
- 取扱説明書 (本書) 1部
- ワークシート 1部
- ユーザ登録カード 1枚

本装置を接続する公衆回線の条件については、本取扱説明書「1.7 公衆回線網の加入契約条件」で説明しています。

万一不備な点がございましたら、恐れ入りますがお買い求めの販売店までお申し付けください。

保証について

弊社ではユーザ登録をお願いしております。お手数ですが「ユーザ登録カード」にご記入の上、弊社までご返送くださいますようお願いいたします。また、保証書は1年間大切に保管してください。

弊社ではお買い上げいただきました製品に対し、お買い上げ後1年間の無償保証を行っております。正常なご使用状態のもとで、保証期間内に万一故障が発生いたしました時は、下記の弊社技術サポート課にお問い合わせください。

その場合、保証書に従い故障の修理をさせていただきます。

保守サービス窓口

古河電気工業株式会社

ネットワーク機器部 開発部 技術サポート課

〒254 神奈川県平塚市東八幡5丁目1番9号

TEL:0463-24-8545 (ダイヤルイン) FAX:0463-24-8548

本書の構成と内容

本取扱説明書は、本装置の設置・設定・運用等に関して記述されています。本書は、以下のよう
に構成されています。

1章 装置に関する 基礎知識	装置の外観や取扱い上の注意事項等について説明しています。装置を設置する前にお読みください。
2章 装置の機能	装置の機能概要や、ネットワークへの接続形態について説明しています。ネットワーク接続形態の決定やシステム編集を行う前にお読みください。
3章 基本設定	別冊のワークシートの作成方法、またそのワークシートを利用して設定を行う項目の説明と設定方法について説明しています。システム編集を行う際にお読み下さい。
4章 拡張設定	装置に接続したコンソールから操作する場合の、拡張機能の設定方法について説明しています。システム編集を行う際にお読み下さい。
5章 オペレーション	コンソールより行う装置の運用方法のほかに、TELNETやリモートコンソールについて説明しています。本装置を運用する際にお読み下さい。
6章 インフォメーション	装置に接続したコンソールから操作する場合の、インフォメーションの参照方法や内容について説明しています。本装置に関する情報を得る際にお読み下さい。
付録	参照事項として、装置の仕様、装置の運用形態、設定情報一覧表、コマンド一覧表、MIB一覧表を記載しています。

本取扱説明書で使用される用語等について

- 用語の説明

(1) 構成定義情報

装置の運用に関する設定情報を示します。

(2) ISDNリモートターゲット

ISDNで接続する相手の名称を示します。

(3) フィルタリング

本取扱説明書でフィルタリングという表現があった場合は、中継するデータを限定する場合と、遮断するデータを限定する場合の2通りがあります。

(4) IPアドレス

本取扱説明書で使用しているIPアドレスは、ローカルなネットワークで使用されるアドレスとして推奨されているものです（RFC(Request For Comments)1597）。したがって、本取扱説明書中のアドレスを使用して、外部のネットワークと接続することはできませんので、ご注意ください。本取扱説明書のIPアドレスは、以下の範囲内のものです。

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

(5) MACアドレス

本取扱説明書で使用しているMACアドレスは、実際には存在しないMACアドレスを使用しています。したがって、本取扱説明書と同じMACアドレスは、装置に入力できません。本取扱説明書中のMACアドレスの例としては、以下のものがあります。

XX:XX:XX:XX:XX:XX
XX:XX:XX:XX:XX:XX
YY:YY:YY:YY:YY:YY
ZZ:ZZ:ZZ:ZZ:ZZ:ZZ

(6) ISDN番号

本取扱説明書で使用しているISDN番号は、実際には存在しないISDN番号を使用しています。したがって、本取扱説明書と同じISDN番号は、装置に入力できません。本取扱説明書中のISDN番号としては、以下のものがあります。

03xxxxxxxx
06xxxxxxxx

(7) ポート

AppleTalkでは、インタフェースをポートと呼びます。

(8) オンライン状態・オフライン状態

各WAN回線に関して本装置が持っている状態。

オンライン状態WAN回線が運用可能な状態。そのWAN回線に関する設定を行うためには、オフライン状態に移行する必要があります。

オフライン状態WAN回線に関する設定を行うことができる状態。設定を有効にし、そのWAN回線を運用可能な状態にするためには、オンライン状態に移行する必要があります。

本装置では、上記2つの状態を持つことにより、装置を再起動せずにすなわち、他のWAN回線の運用を妨げることなく、設定を変更することができます。

- 注釈マークの説明

本取扱説明書で使用している記号の意味は以下のとおりです。



メモ

装置の設定、運用に関する参照先や補足の説明を示します。



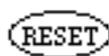
注意

装置の設定や運用上での特に意識すべき注意点を示します。



警告

行ってはならない装置の設定や運用を示します。



設定を行った後、装置をリセットしなければ有効にならない設定項目を示します。



ワークシートを参照しながら設定する項目を示します。

(→→*.*.*) 参照していただく章・節・項番号を示します。

目次

ご注意	ii
安全のために	iii
著作権および商標について	vi
はじめに	vii
保証について	viii
本書の構成と内容	ix
本取扱説明書で使用される用語等について	x
ご注意	ii
1章 装置に関する基礎知識	1-1
1.1 装置外観	1-2
1.2 各部の名称と機能	1-3
1.3 電源の投入 / 遮断	1-6
1.4 各種ケーブルの取扱い	1-6
1.4.1 コンソール	1-6
1.4.2 AUIケーブル	1-8
1.4.3 モジュラーケーブル	1-8
1.4.4 電源ケーブル	1-9
1.5 フロッピーディスクユニットの取扱い	1-9
1.6 フロントパネルのLED表示	1-10
1.7 公衆回線網の加入契約条件	1-12
1.7.1 HSDをご利用になる場合の契約条件について	1-12
1.7.2 ISDNをご利用になる場合の契約条件について	1-12
2章 装置の機能	2-1
2.1 運用形態	2-2
2.2 データリンクプロトコル	2-2
2.3 IPホスト機能	2-2
2.4 IPルーティング機能	2-3
2.4.1 RIPを利用したダイナミックルーティング	2-3
2.4.2 OSPFを利用したダイナミックルーティング	2-3
2.4.3 スタティックルーティング	2-5
2.4.4 ダイナミックルーティングとスタティックルーティングの関係	2-5
2.4.5 インタフェースタイプ	2-5
2.4.6 Proxy ARP機能	2-6
2.4.7 DHCPリレーエージェント機能	2-7
2.5 IPXルーティング機能	2-9
2.5.1 ダイナミックルーティング	2-9
2.5.2 スタティックルーティング	2-9

2.5.3	ダイナミックルーティングとスタティックルーティングの関係	2-9
2.5.4	インタフェースタイプ	2-10
2.5.5	IPXのKeepAliveパケットの代理応答 / 要求機能	2-10
2.6	IP,IPXパケットフィルタリング機能	2-10
2.6.1	送信元 / 宛先アドレスによるフィルタリング	2-11
2.6.2	プロトコル識別によるフィルタリング	2-12
2.6.3	上位プログラムによるフィルタリング	2-13
2.6.4	送信可 / 受信可インタフェースによるフィルタリング	2-13
2.7	AppleTalkルーティング機能	2-14
2.7.1	ダイナミックルーティング	2-14
2.7.2	スタティックルーティング	2-14
2.7.3	AURP	2-14
2.8	AppleTalkパケットフィルタリング機能	2-16
2.8.1	DDPフィルタリング	2-16
2.8.2	ゾーンフィルタリング	2-18
2.8.3	サービスフィルタリング	2-18
2.9	ブリッジング機能	2-19
2.9.1	STP機能	2-19
2.9.2	フィルタリング機能	2-20
2.9.3	WAN回線複数使用時のWAN-WANブリッジング機能	2-23
2.10	ISDNに関する機能	2-24
2.10.1	通常データ通信	2-24
2.10.2	トラヒックの分散	2-24
2.10.3	様々な回線の接続 / 切断方法	2-25
2.10.4	最大80箇所の相手との通信	2-29
2.10.5	チャンネルグループ機能	2-33
2.10.6	様々なISDN接続時間の制御方法	2-34
2.10.7	セキュリティ機能	2-35
2.10.8	呼確立リミッタ	2-37
2.11	ネットワーク管理機能	2-38
2.12	TELNETサーバ機能	2-39
2.13	リモートコンソール機能	2-39
2.14	簡易コマンド機能	2-40
2.15	データ圧縮機能	2-40
2.16	データ別優先制御機能	2-41
2.17	ルータグループ化機能	2-41
2.18	トラヒックロギング機能	2-43
3章	基本設定	3-1
3.1	基本設定の流れ	3-2
3.2	ワークシートの作成	3-4
3.2.1	ワークシート「基本設定編」	3-8
3.2.2	ワークシート「HSD編」	3-12
3.2.3	ワークシート「ISDNチャンネルグループ編」	3-13

3.2.4	ワークシート「ISDN運用形態編（グループ/チャンネル毎）」	3-15
3.2.5	ワークシート「ISDNリモートターゲット編（グループ/チャンネル毎）」	3-18
3.2.6	ワークシート「ISDN通常回線編」	3-21
3.2.7	ワークシート「IPホスト編」	3-26
3.2.8	ワークシート「IPルーティング編」	3-29
3.2.9	ワークシート「IPリモートターゲット編」	3-32
3.2.10	ワークシート「IPスタティックルーティング編」	3-34
3.2.11	ワークシート「DHCPリレーエージェント編」	3-37
3.2.12	ワークシート「IPパケットフィルタリング編」	3-39
3.2.13	ワークシート「IPXルーティング編」	3-45
3.2.14	ワークシート「IPXリモートターゲット編」	3-48
3.2.15	ワークシート「IPXパケットフィルタリング編」	3-50
3.2.16	ワークシート「IPXスタティックルーティング編」	3-55
3.2.17	ワークシート「IPXスタティックSAP編」	3-58
3.2.18	ワークシート「AppleTalkルーティング編」	3-60
3.2.19	ワークシート「AppleTalkリモートターゲット編」	3-64
3.2.20	ワークシート「外部AppleTalkルータ編」	3-66
3.2.21	ワークシート「AppleTalk DDP (forward) フィルタリング編」	3-68
3.2.22	ワークシート「AppleTalkゾーンリスト編」	3-71
3.2.23	ワークシート「AppleTalkスタティックルーティング編」	3-73
3.2.24	ワークシート「AppleTalkスタティックゾーン編」	3-76
3.2.25	ワークシート「MACアドレスリモートターゲット編」	3-78
3.2.26	ワークシート「ブリッジング編」	3-80
3.2.27	ワークシート「送信元フィルタリング編」	3-82
3.2.28	ワークシート「宛先フィルタリング編」	3-84
3.2.29	ワークシート「プロトコルフィルタリング編」	3-86
3.2.30	ワークシート「SNMP編」	3-89
3.3	コンソールの接続	3-92
3.4	メインメニュー	3-93
3.5	管理者資格(スーパーモード)への移行	3-95
3.6	一般資格への復帰	3-96
3.7	設定情報の表示	3-97
3.8	コンソールからの設定	3-98
3.9	運用形態の選択	3-100
3.10	現在時刻の設定	3-101
3.11	自ホスト名の設定	3-101
3.12	WAN回線の設定	3-102
3.12.1	HSDの設定	3-102
3.12.2	ISDNチャンネルグループの設定	3-103
3.12.3	ISDN運用形態の設定	3-104
3.12.4	ISDNリモートターゲットの設定	3-105
3.12.5	ISDN通常回線の設定	3-107
3.13	機能の選択	3-109
3.14	IPホスト/IPアドレスの設定	3-110

3.15	IPに関する基本設定	3-112
3.15.1	IPルーティングの設定	3-112
3.15.2	IPのISDNリモートターゲットの設定	3-113
3.15.3	IPスタティックルーティングの設定	3-114
3.15.4	DHCPリレーエージェントの設定	3-116
3.15.5	IPパケットフィルタリングの設定	3-117
3.16	IPXに関する基本設定	3-120
3.16.1	IPXルーティングの設定	3-120
3.16.2	IPXのISDNリモートターゲットの設定	3-121
3.16.3	IPXパケットフィルタリングの設定	3-123
3.16.4	IPXスタティックルーティングの設定	3-125
3.16.5	IPXスタティックSAPの設定	3-126
3.17	AppleTalkに関する基本設定	3-128
3.17.1	AppleTalkの設定	3-128
3.17.2	AppleTalkルーティングの設定	3-129
3.17.3	AppleTalkのISDNリモートターゲットの設定	3-130
3.17.4	外部AppleTalkルータの設定	3-131
3.17.5	AppleTalk DDP (forward) フィルタリングの設定	3-133
3.17.6	ゾーンリストの設定	3-135
3.17.7	AppleTalkスタティックルーティングの設定	3-137
3.17.8	AppleTalkスタティックゾーンテーブルの設定	3-138
3.18	ブリッジングに関する基本設定	3-142
3.18.1	MACアドレスのISDNリモートターゲットの設定	3-142
3.18.2	ブリッジング機能の設定	3-143
3.18.3	送信元 / 宛先フィルタリングの設定	3-145
3.18.4	プロトコルフィルタリングの設定	3-148
3.19	SNMPに関する基本設定	3-149
3.19.1	SNMPパラメータの設定	3-149
3.18.2	SNMPマネージャリストの設定	3-149
3.20	設定内容の確認	3-151
3.21	設定内容の適用	3-151
4章	拡張設定	4-1
4.1	拡張設定の流れ	4-2
4.2	データリンクに関する設定	4-5
4.3	ブリッジングに関する拡張設定	4-9
4.3.1	STPの設定	4-9
4.3.2	アドレス学習テーブルのエイジャウト時間	4-12
4.3.3	フレームの最大中継遅延時間	4-12
4.4	ICMPリダイレクトメッセージの設定	4-13
4.5	IPに関する拡張設定	4-15
4.5.1	RIP(IP)に関する拡張設定	4-16
4.5.2	RIP(IP)インタフェースの設定	4-19
4.5.3	RIP(IP)フィルタリング(accept gateway)の設定	4-21

4.5.4	RIP(IP)フィルタリング(propagate gateway)の設定	4-24
4.5.5	RIP(IP)フィルタリング(interface accept)の設定	4-26
4.5.6	RIP(IP)フィルタリング(interface propagate)の設定	4-28
4.5.7	Proxy ARPの設定	4-30
4.5.8	スタティックルーティングの設定	4-31
4.5.9	IPパケットフィルタリング(forward)の設定	4-31
4.5.10	IPパケットフィルタリング(discard)の設定	4-31
4.5.11	OSPFに関する設定	4-32
4.6	IPXに関する拡張設定	4-60
4.6.1	RIP(IPX)インタフェースの設定	4-62
4.6.2	RIP(IPX)フィルタリングの設定	4-64
4.6.3	RIP(IPX)スタティックルーティングの設定	4-66
4.6.4	SAP(IPX)インタフェースの設定	4-67
4.6.5	SAP(IPX)フィルタリングテーブルの属性の設定	4-69
4.6.6	SAP(IPX)フィルタリング(address)の設定	4-70
4.6.7	SAP(IPX)フィルタリング(server name)の設定	4-71
4.6.8	SAP(IPX)フィルタリング(service type)の設定	4-72
4.6.9	SAP(IPX)のスタティック設定	4-73
4.6.10	IPXパケットフィルタリング(forward)の設定	4-73
4.6.11	IPXパケットフィルタリング(discard)の設定	4-73
4.6.12	IPX frame typeの設定	4-74
4.6.13	KeepAliveパケットの代理応答 / 要求の設定	4-75
4.7	AppleTalkに関する拡張設定	4-78
4.7.1	AppleTalkインタフェースの設定	4-81
4.7.2	AppleTalkスタティックルーティングの設定	4-84
4.7.3	AppleTalkスタティックゾーンテーブルの設定	4-84
4.7.4	AppleTalk DDP(forward)フィルタリングの設定	4-84
4.7.5	AppleTalk DDP(discard)フィルタリングの設定	4-84
4.7.6	AppleTalkサービス(forward)フィルタリングの設定	4-85
4.7.7	AppleTalkサービス(discard)フィルタリングの設定	4-87
4.7.8	ゾーンフィルタリングの設定	4-87
4.7.9	ルーティング情報のフィルタリング(accept gateway)の設定	4-89
4.7.10	ルーティング情報のフィルタリング(propagate gateway)の設定	4-92
4.7.11	ルーティング情報のフィルタリング(accept port)の設定	4-92
4.7.12	ルーティング情報のフィルタリング(propagate port)の設定	4-94
4.7.13	AURP protocolの設定	4-94
4.7.14	外部AppleTalkルータの設定	4-98
4.8	SNMPに関する拡張設定	4-98
4.9	リモートファイルメンテナンスの設定	4-99
4.10	データ別優先制御に関する拡張設定	4-100
4.10.1	パラメータの設定	4-101
4.10.2	IPプロトコルの設定	4-102
4.10.3	IPアドレスの設定	4-104
4.10.4	IPXプロトコルの設定	4-106

4.10.5	IPXアドレスの設定	4-108
4.10.6	AppleTalkプロトコルの設定	4-110
4.10.7	AppleTalkアドレスの設定	4-111
4.10.8	ブリッジングデータの設定	4-113
4.10.9	MACアドレスの設定	4-114
4.11	トラヒックロギングに関する設定	4-116
4.11.1	トラヒックロギングテーブルの設定	4-116
4.12	呼確立リミッタの設定	4-119
4.12.1	連続接続時間呼確立リミッタの設定	4-119
4.12.2	トータル接続時間呼確立リミッタの設定	4-120
4.13	リモートターゲットの設定	4-122
4.14	ルータグループ化機能の設定	4-123
5章	オペレーション	5-1
5.1	オペレーションメニュー	5-2
5.2	通常回線の接続	5-3
5.3	通常回線の切断	5-3
5.4	トラヒック分散回線の接続	5-4
5.5	トラヒック分散回線の切断	5-4
5.6	グループ/チャネルのオンライン状態への遷移	5-5
5.7	グループ/チャネルのオフライン状態への遷移	5-5
5.8	呼確立リミッタのリスタート	5-6
5.9	リモートコンソール	5-7
5.10	エコーテスト	5-7
5.11	パスワードの変更	5-11
5.12	構成定義情報, ログ情報の保存	5-11
5.13	すべての設定情報の確認	5-12
5.14	フレームトレース機能	5-13
5.14.1	フレームトレース機能の操作	5-13
5.14.2	フレームトレース機能の種類の設定	5-13
5.14.3	フレームトレースの開始/終了	5-21
5.14.4	トレース結果の表示	5-22
5.14.5	トレース結果の消去	5-22
5.14.6	トレースデータの解析	5-23
5.15	障害復帰の確認	5-27
5.16	装置の再起動	5-27
5.17	保守用コマンド	5-29
5.17.1	回線接続診断試験 (Inktest)	5-29
5.17.2	スキャンアウト	5-33
5.17.3	ファイルメンテナンスモード (filemnt)	5-34
5.18	装置の遠隔操作	5-38
5.18.1	TELNETコンソール	5-38
5.18.2	遠隔装置への接続(リモートコンソール)	5-39

5.18.3	遠隔操作の終了	5-40
5.19	簡易コマンド機能	5-40
5.20	FTPを利用したメンテナンス	5-40
6章	インフォメーション	6-1
6.1	インフォメーションメニュー	6-2
6.2	IPに関するインフォメーション	6-5
6.2.1	IPインタフェースの情報	6-5
6.2.2	IPに関する統計情報	6-7
6.2.3	IPルーティングの情報	6-9
6.3	DHCPリレーエージェントに関する インフォメーション	6-10
6.3.1	廃棄フレーム	6-10
6.3.2	統計情報	6-10
6.4	IPXに関するインフォメーション	6-12
6.4.1	IPXインタフェースの情報	6-12
6.4.2	IPXに関する統計情報	6-13
6.4.3	IPXルーティング情報	6-14
6.4.4	SAP情報	6-15
6.5	ブリッジング機能に関するインフォメーション	6-16
6.5.1	ブリッジポートの情報	6-16
6.5.2	ブリッジング機能に関する統計情報	6-17
6.6	チャンネルに関するインフォメーション	6-18
6.6.1	チャンネルの情報	6-18
6.6.2	チャンネルの統計情報	6-19
6.7	OSPFに関するインフォメーション	6-21
6.7.1	OSPFに関する一般情報	6-22
6.7.2	OSPFエリアの情報	6-23
6.7.3	OSPFリンク状態の情報	6-24
6.7.4	OSPFインタフェースの情報	6-25
6.7.5	OSPFバーチャルリンクのインタフェース情報	6-26
6.7.6	OSPF隣接の情報	6-27
6.7.7	OSPFバーチャルリンクを確立した相手の情報	6-28
6.8	AppleTalkに関するインフォメーション	6-29
6.8.1	AppleTalkのポートの情報	6-29
6.8.2	統計情報	6-31
6.8.3	AppleTalkルーティング情報	6-33
6.8.4	ゾーンリスト	6-34
6.8.5	サービスの情報	6-35
6.8.6	AURPコネクション情報	6-36
6.9	呼確立リミッタに関するインフォメーション	6-38
6.10	ルータグループ化に関するインフォメーション	6-39
6.11	エラーログ	6-40
6.12	ラインログ	6-40

6.13	トラップログ	6-40.....
6.14	トラヒックロギングに関するインフォメーション	6-41.....
付録A 装置の仕様		A-1.....
A.1	仕様	A-1.....
A.2	使用環境	A-1.....
	A.2.1 電気的条件.....	A-1.....
	A.2.2 環境条件.....	A-2.....
A.3	インタフェース仕様	A-2.....
	A.3.1 AUIポート.....	A-2.....
	A.3.2 I430ポート.....	A-3.....
	A.3.3 コンソールポート.....	A-4.....
A.4	コンソール仕様	A-4.....
付録B 装置の運用形態		B-1.....
B.1	装置の運用形態 (HSD回線)	B-2.....
B.2	装置の運用形態 (ISDN回線)	B-3.....
	B.2.1 代表取扱いサービスを利用する場合	B-3.....
	B.2.2 代表取扱いサービスを利用しない場合	B-4.....
	B.2.3 トラヒック分散を利用する場合	B-4.....
付録C 設定情報一覧表		C-1.....
C.1	現在時刻	C-1.....
C.2	自ホスト名	C-1.....
C.3	HSDに関する設定	C-2.....
C.4	ISDNに関する設定	C-2.....
	C.4.1 ISDNチャンネルグループ.....	C-2.....
	C.4.2 ISDN運用形態.....	C-3.....
	C.4.3 ISDNリモートターゲット.....	C-3.....
	C.4.4 ISDN通常回線.....	C-4.....
	C.4.5 ISDN接続 / 切断時刻.....	C-4.....
	C.4.6 MACアドレスリモートターゲット.....	C-5.....
	C.4.7 IPアドレスリモートターゲット.....	C-5.....
	C.4.8 IPXアドレスリモートターゲット.....	C-5.....
	C.4.9 AppleTalkアドレスリモートターゲット.....	C-5.....
C.5	基本機能	C-6.....
C.6	IPホスト.....	C-6.....
C.7	datalink.....	C-7.....
C.8	SNMP.....	C-7.....
C.9	IPに関する設定.....	C-8.....
	C.9.1 IPルーティング.....	C-8.....
	C.9.2 IPフィルタリング (forward : 最大128エントリ)	C-9.....
	C.9.3 IPフィルタリング (discard : 最大64エントリ)	C-10.....

C.9.4	RIP motion.....	C-11.....
C.9.5	RIPインタフェース.....	C-11.....
C.9.6	スタティックルーティング (最大256エン트리)	C-12.....
C.9.7	RIPフィルタリング(accept GW : 最大32GW × 4エン트리).....	C-12.....
C.9.8	RIPフィルタリング(propagate GW : 最大32GW × 4エン트리)	C-13.....
C.9.9	RIPフィルタリング(IF accept : 最大40エン트리)	C-13.....
C.9.10	RIPフィルタリング(IF propagate : 最大40エン트리).....	C-14.....
C.9.11	Proxy ARP.....	C-14.....
C.10	OSPFに関する設定.....	C-14.....
C.10.1	OSPF機能使用有無.....	C-14.....
C.10.2	OSPFルータID	C-15.....
C.10.3	OSPFエリア.....	C-15.....
C.10.4	OSPFバックボーンエリア.....	C-15.....
C.10.5	OSPFネットワーク (最大32エン트리)	C-16.....
C.10.6	OSPFスタブホスト (最大16エン트리)	C-16.....
C.10.7	OSPFインタフェース.....	C-16.....
C.10.8	OSPF隣接ルータ (最大32エン트리)	C-17.....
C.10.9	OSPFバーチャルリンク隣接ルータ (最大8エン트리)	C-17.....
C.10.10	OSPFバーチャルリンク (最大8エン트리)	C-17.....
C.10.11	RIP export (最大20エン트리)	C-18.....
C.10.12	OSPF AS外のルーティング情報	C-18.....
C.10.13	OSPF AS外のルーティング情報の受信 (OSPF import : 最大20エン트리)	C-19.....
C.10.14	OSPF AS外のルーティング情報の送信 (OSPF export : 最大20エン트리)	C-19.....
C.11	IPXに関する設定	C-20.....
C.11.1	IPXルーティング.....	C-20.....
C.11.2	IPXフィルタリング (forward : 最大128エン트리)	C-21.....
C.11.3	IPXフィルタリング (discard : 最大64エン트리)	C-22.....
C.11.4	RIPインタフェース.....	C-23.....
C.11.5	RIPフィルタリング (最大64エン트리)	C-23.....
C.11.6	RIPスタティック (最大256エン트리)	C-24.....
C.11.7	SAPインタフェース.....	C-24.....
C.11.8	SAPフィルタリングモード.....	C-24.....
C.11.9	SAPフィルタリング(address) (最大64エン트리)	C-25.....
C.11.10	SAPフィルタリング(server name) (最大64エン트리)	C-25.....
C.11.11	SAPフィルタリング(server type) (最大64エン트리)	C-25.....
C.11.12	SAPスタティック (最大256エン트리)	C-26.....
C.11.13	IPX frame type	C-26.....
C.11.14	Keep Alive.....	C-27.....
C.12	AppleTalkに関する設定	C-28.....
C.12.1	AppleTalkルーティング.....	C-28.....
C.12.2	外部AppleTalkルータ.....	C-29.....
C.12.3	AppleTalk DDPフィルタリング (forward) (最大64エン트리).....	C-30.....

C.12.4	AppleTalk DDPフィルタリング (discard) (最大32エントリ)	C-31
C.12.5	AppleTalkゾーンリスト	C-32
C.12.6	AppleTalkスタティックルーティング	C-32
C.12.7	AppleTalkスタティックゾーン	C-33
C.12.8	AppleTalkインタフェース	C-33
C.12.9	サービスフィルタリング (forward) (最大64エントリ)	C-34
C.12.10	サービスフィルタリング (discard) (最大64エントリ)	C-34
C.12.11	ゾーンフィルタリング (最大128エントリ)	C-35
C.12.12	ルーティング情報のフィルタリング (accept gateway) (最大32GW × 7エントリ)	C-35
C.12.13	ルーティング情報のフィルタリング (propagate gateway) (最大32GW × 7エントリ)	C-36
C.12.14	ルーティング情報のフィルタリング (accept port) (最大40エントリ)	C-36
C.12.15	ルーティング情報のフィルタリング (propagate port) (最大40エントリ)	C-37
C.12.16	AURPプロトコル	C-37
C.13	ブリッジに関する設定	C-38
C.13.1	ブリッジング	C-38
C.13.2	アドレス学習テーブルのエイジャウト時間	C-38
C.13.3	ブリッジ最大中継遅延時間	C-38
C.13.4	アドレスフィルタリングのデフォルト	C-38
C.13.5	送信元アドレスフィルタリング (最大64エントリ)	C-39
C.13.6	宛先アドレスフィルタリング (最大64エントリ)	C-39
C.13.7	プロトコルフィルタリングのデフォルト	C-39
C.13.8	プロトコルフィルタリング (最大32エントリ)	C-40
C.13.9	STP	C-40
C.13.10	ICMPリダイレクト	C-41
C.14	リモートファイルメンテナンスに関する設定	C-41
C.15	データ圧縮に関する設定	C-41
C.16	データ別優先制御に関する設定	C-42
C.16.1	パラメータ	C-42
C.16.2	IPプロトコル	C-42
C.16.3	IPアドレス	C-43
C.16.4	IPXプロトコル	C-43
C.16.5	IPXアドレス	C-44
C.16.6	AppleTalkプロトコル	C-44
C.16.7	AppleTalkアドレス	C-45
C.16.8	ブリッジングデータ	C-45
C.16.9	MACアドレス	C-45
C.17	トラフィックロギングに関する設定	C-46
C.18	呼確立リミットに関する設定	C-46
C.18.1	連続接続時間呼確立リミット	C-46
C.18.2	トータル接続時間呼確立リミット	C-47

C.19 ルータグループ化機能の設定	C-47
付録D 簡易コマンド機能	D-1
付録E FTPを利用したメンテナンス	E-1
付録F MIB一覧表	F-1
F.1 MIB-II (RFC1213)	F-2
F.1.1 system グループ	F-2
F.1.2 interface グループ	F-2
F.1.3 at グループ	F-2
F.1.4 ip グループ	F-3
F.1.5 ipForward グループ	F-4
F.1.6 icmp グループ	F-4
F.1.7 tcp グループ	F-5
F.1.8 udp グループ	F-5
F.1.9 snmp グループ	F-6
F.2 dot3 (RFC1284)	F-6
F.2.1 the Ethernet-like Statistics グループ	F-6
F.2.2 the Ethernet-like Collision Statistics グループ	F-7
F.3 appletalk (RFC1243)	F-7
F.4 ospf (RFC1253)	F-8
F.5 dot1dBridge (RFC1286)	F-10
F.5.1 dot1dBase グループ	F-11
F.5.2 dot1dStp グループ	F-11
F.5.3 dot1dTp グループ	F-12
F.5.4 dot1dStatic グループ	F-12
F.6 装置拡張MIB	F-13
F.6.1 中継装置共通の拡張MIB	F-15
F.6.2 ブリッジ固有の拡張MIB	F-15
F.6.3 中継装置のインタフェース	F-17
F.6.4 中継装置のポート	F-18
F.6.5 中継装置の通信相手	F-18
F.6.6 呼確立リミッタのMIB	F-19
F.6.7 トラヒックロギング機能のMIB	F-19
F.6.8 中継装置の拡張インタフェース	F-19
F.6.9 中継装置のプロトコル	F-20
F.7 Trap	F-22
F.7.1 標準MIB-IIのTrap	F-22
F.7.2 装置拡張Trap	F-22

目次

図1-1	装置外観（単位：mm）	1-2
図1-2	装置前面	1-3
図1-3	装置後面	1-4
図1-4	装置底面	1-5
図1-5	コンソールの接続	1-7
図1-6	AUIケーブルの接続	1-8
図1-7	モジュラーケーブルの接続	1-8
図1-8	電源ケーブルの接続	1-9
図2-1	OSPF運用環境	2-4
図2-2	IPポイントツーポイント接続例	2-5
図2-3	IPブロードキャスト接続例	2-6
図2-4	Proxy ARP機能利用環境	2-7
図2-5	DHCP運用形態例 1	2-7
図2-6	DHCP運用形態例 2	2-8
図2-7	IPXブロードキャスト接続例	2-10
図2-8	送信元 / 宛先アドレスによるフィルタリング	2-11
図2-9	プロトコル識別によるフィルタリング	2-12
図2-10	上位プログラムによるフィルタリング	2-13
図2-11	送信可 / 受信可インタフェースによるフィルタリング	2-13
図2-12	AURPを使用している環境の例	2-15
図2-13	送信元 / 宛先アドレスによるフィルタリング	2-16
図2-14	プロトコル識別によるフィルタリング	2-17
図2-15	送信可 / 受信可インタフェースによるフィルタリング	2-17
図2-16	ゾーンフィルタリング	2-18
図2-17	サービスフィルタリング	2-18
図2-18	STP機能	2-19
図2-19	アドレス学習によるフィルタリング	2-21
図2-20	送信元アドレス，宛先アドレスによるフィルタリング	2-21
図2-21	プロトコル識別によるフィルタリング	2-22
図2-22	HSD2回線使用時のWAN-WANブリッジング機能	2-23
図2-23	手動による接続例	2-25
図2-24	指定時間内の中継データによる接続例	2-26
図2-25	手動接続例	2-27
図2-26	指定時間内でのデータ量による接続例	2-28
図2-27	IPパケットによる自動接続	2-29
図2-28	IPXパケットによる自動接続	2-30
図2-29	AppleTalkパケットによる自動接続	2-31
図2-30	ブリッジングフレームによる自動接続	2-32
図2-31	チャンネルグループ機能の利用例	2-33

図2-32	KeepAliveの代理応答 / 要求例	2-35.....
図2-33	CHAP機能を使用する場合の設定方法	2-36.....
図2-34	SNMPエージェント機能.....	2-38.....
図2-35	TELNETサーバ機能.....	2-39.....
図2-36	リモートコンソール機能.....	2-39.....
図2-37	ルータグループ化機能.....	2-42.....
図2-38	トラヒックロギング機能設定例.....	2-44.....
図3-1	基本設定の流れ.....	3-3.....
図3-2 (1)	ワークシートの構成 (1)	3-4.....
図3-2 (2)	ワークシートの構成 (2)	3-5.....
図3-2 (3)	ワークシートの構成 (3)	3-6.....
図3-2 (4)	ワークシートの構成 (4)	3-7.....
図3-3	基本設定編の形式と記入の手順.....	3-8.....
図3-4	HSD編の形式と記入の手順.....	3-12.....
図3-5	ISDNチャネルグループ編の形式と記入の手順	3-13.....
図3-6	ISDN運用形態編の形式と記入の手順	3-15.....
図3-7	ISDNリモートターゲット編の形式と記入の手順	3-18.....
図3-8	ISDN通常回線編の形式と記入の手順	3-21.....
図3-9	ISDNの接続方法によるIPXルーティング不能ケース	3-24.....
図3-10	IPホスト編の形式と記入の手順	3-26.....
図3-11	IPルーティング編の形式と記入の手順	3-29.....
図3-12	IPリモートターゲット編の形式と記入の手順	3-32.....
図3-13	IPスタティックルーティング編の形式と記入の手順	3-34.....
図3-14	DHCPリレーエージェント編の形式と記入の手順	3-37.....
図3-15	IPパケットフィルタリング編の形式と記入の手順	3-39.....
図3-16	IPXルーティング編の形式と記入の手順	3-45.....
図3-17	IPXリモートターゲット編の形式と記入の手順	3-48.....
図3-18	IPXパケットフィルタリング編の形式と記入の手順	3-50.....
図3-19	IPXスタティックルーティング編の形式と記入の手順	3-55.....
図3-20	IPXスタティックSAP編の形式と記入の手順	3-58.....
図3-21	AppleTalkルーティング編の形式と記入の手順.....	3-60.....
図3-22	AppleTalkリモートターゲット編の形式と記入の手順.....	3-64.....
図3-23	外部AppleTalkルータ編の形式と記入の手順.....	3-66.....
図3-24	AppleTalk DDP (forward) フィルタリング編の形式と記入の手順	3-68.....
図3-25	AppleTalkゾーンリスト編の形式と記入の手順.....	3-71.....
図3-26	AppleTalkスタティックルーティング編の形式と記入の手順.....	3-73.....
図3-27	AppleTalkスタティックゾーン編の形式と記入の手順.....	3-76.....
図3-28	MACアドレスリモートターゲット編の形式と記入の手順.....	3-78.....
図3-29	ブリッジング編の形式と記入の手順.....	3-80.....
図3-30	送信元フィルタリング編の形式と記入の手順.....	3-82.....
図3-31	宛先フィルタリング編の形式と記入の手順.....	3-84.....
図3-32	プロトコルフィルタリング編の形式と記入の手順.....	3-86.....

図3-33	SNMP編の形式と記入の手順	3-89
図3-34	メインメニュー例	3-93
図3-35	管理者資格への移行例	3-95
図3-36	一般資格への復帰例	3-96
図3-37	入力の流れ	3-98
図3-38	エラー表示例	3-99
図3-39	WAN回線選択例	3-100
図3-40	現在時刻設定例 (1995年6月18日14時52分00秒に設定)	3-101
図3-41	自ホスト名の設定例	3-101
図3-42	HSD回線の回線速度設定例	3-102
図3-43	ISDNチャンネルグループ機能設定例	3-103
図3-44	ISDNチャンネルグループ追加例	3-103
図3-45	グループおよびチャンネルの選択画面例	3-104
図3-46	運用形態の設定例 (「WAN topology」に「Usual」か 「Usual/Load split」を選択した場合) (グループの場合)	3-104
図3-47	運用形態の設定 (「WAN topology」に「Load split」を選択した場合)	3-105
図3-48	ISDNリモートターゲット設定選択画面	3-105
図3-49	ISDNリモートターゲット設定画面	3-106
図3-50	ISDN通常回線設定例	3-107
図3-51	接続時刻, 切断時刻設定メニュー	3-108
図3-52	ISDN接続 / 切断時刻の追加例	3-108
図3-53	基本機能画面 (設定値の表示)	3-109
図3-54	基本機能設定例	3-110
図3-55	IPホスト設定例	3-110
図3-56	IPアドレス設定例	3-111
図3-57	IPルーティング設定例 (ISDNを7本使用する場合)	3-112
図3-58	IPルーティング設定例 (ISDNを7本使用する場合)	3-113
図3-59	IPリモートターゲット例	3-113
図3-60	IPリモートターゲットデータ追加例	3-114
図3-61	IPスタティックルーティング設定メニュー	3-114
図3-62	IPスタティックルート追加例	3-115
図3-63	DHCPリレーエージェント機能の設定例	3-116
図3-64	IPパケットフィルタリングの設定メニュー	3-117
図3-65	IPパケットフィルタリングの追加例	3-118
図3-66	IPXルーティング設定例	3-120
図3-67	IPXルーティング設定例	3-121
図3-68	IPXリモートターゲットの設定メニュー	3-121
図3-69	IPXリモートターゲットテーブルの追加例	3-122
図3-70	IPXパケットフィルタリングの設定メニュー	3-123
図3-71	IPXパケットフィルタリングテーブルの追加例	3-124
図3-72	RIP(IPX)スタティックルーティングの設定例	3-125
図3-73	IPXスタティックルーティングテーブルの追加例	3-125

図3-74	スタティックSAPの設定例	3-126
図3-75	IPXスタティックSAPの追加例	3-126
図3-76	AppleTalk設定例	3-128
図3-77	AppleTalkルーティング設定例	3-129
図3-78	AppleTalkルーティング設定例	3-130
図3-79	AppleTalkリモートターゲットの設定メニュー	3-130
図3-80	AppleTalkリモートターゲットテーブルの追加例	3-131
図3-81	外部AppleTalkルータ設定画面	3-131
図3-82	外部AppleTalkルータテーブル追加例	3-132
図3-83	AppleTalk DDP (forward) フィルタリングの設定メニュー	3-133
図3-84	DDP(forward)フィルタリングの追加例	3-134
図3-85	ゾーンリストの設定メニュー	3-135
図3-86	AppleTalkゾーンリストの追加例	3-136
図3-87	AppleTalkスタティックルーティングの設定メニュー	3-137
図3-88	AppleTalkスタティックルーティングテーブル追加例	3-137
図3-89	スタティックゾーンの設定メニュー	3-138
図3-90	AppleTalkスタティックゾーンテーブルのネットワーク選択例	3-139
図3-91	AppleTalkスタティックゾーンテーブルの設定メニュー	3-139
図3-92	AppleTalkスタティックゾーンテーブルの変更例	3-139
図3-93	AppleTalkスタティックゾーンテーブルの削除例	3-140
図3-94	AppleTalkスタティックゾーンテーブルの追加例	3-140
図3-95	AppleTalkスタティックゾーンテーブルの表示例	3-140
図3-96	すべてのAppleTalkスタティックゾーンテーブルの表示例	3-141
図3-97	MACアドレスリモートターゲットの設定メニュー	3-142
図3-98	IPXリモートターゲットデータの追加例	3-142
図3-99	ブリッジング機能設定例 (ISDN選択時)	3-143
図3-100	ブリッジング機能設定例 (HSD選択時)	3-144
図3-101	アドレスフィルタリングパラメータ設定メニュー	3-145
図3-102	アドレスフィルタリングのデフォルトの設定例	3-146
図3-103	送信元アドレスフィルタリングテーブル設定メニュー	3-146
図3-104	送信元アドレスフィルタリングテーブルの追加例	3-147
図3-105	プロトコルフィルタリング設定メニュー	3-148
図3-106	SNMPパラメータ設定例	3-149
図3-107	SNMPマネージャリストの設定例	3-149
図3-108	SNMPマネージャリストの追加例	3-150
図3-109	設定内容確認の問い合わせメニュー	3-151
図3-110	設定後動作メニュー (1)	3-151
図3-111	設定後動作メニュー (2)	3-152
図4-1	拡張設定入力の流れ	4-2
図4-2	拡張設定メニュー	4-3
図4-3	データリンクの設定画面例(HSD選択時)	4-5
図4-4	データリンクの設定画面例(ISDN選択時)	4-6

図4-5	ブリッジング機能拡張設定メニュー	4-9
図4-6	STP（装置単位）の設定例	4-9
図4-7	STP（各回線）の設定例	4-11
図4-8	アドレス学習テーブルエージアウト時間設定例	4-12
図4-9	フレームの最大中継遅延時間設定例	4-12
図4-10	ICMPリダイレクトメッセージ設定例	4-13
図4-11	IPルーティング拡張設定メニュー	4-15
図4-12	RIP動作モード設定メニュー	4-16
図4-13	RIP動作モード設定例	4-17
図4-14	トラストゲートウェイ設定メニュー	4-18
図4-15	RIP(IP)インターフェース拡張設定例	4-19
図4-16	RIP(IP)フィルタリング(accept gateway)拡張設定例	4-21
図4-17	RIP(IP)フィルタリングテーブル(accept gateway)属性	4-22
図4-18	RIP(IP)フィルタリングテーブル(accept gateway)設定例	4-22
図4-19	RIP(IP)フィルタリング(propagate gateway)拡張設定例	4-24
図4-20	RIP(IP)フィルタリングテーブル(propagate gateway)属性	4-24
図4-21	RIP(IP)フィルタリングテーブル(propagate gateway)設定例	4-25
図4-22	RIP(IP)フィルタリング(interface accept)拡張設定例	4-26
図4-23	RIP(IP)フィルタリングテーブル(interface accept)属性	4-26
図4-24	RIP(IP)フィルタリングテーブル(interface accept)設定例(ISDN選択時)	4-27
図4-25	RIP(IP)フィルタリング(interface propagate)拡張設定例	4-28
図4-26	RIPフィルタリングテーブル(interface propagate)属性	4-28
図4-27	RIP(IP)フィルタリングテーブル(interface propagate)設定例(ISDN選択時)	4-29
図4-28	Proxy ARP設定例	4-30
図4-29	OSPF設定メニュー	4-32
図4-30	OSPF機能使用有無の設定画面	4-32
図4-31	OSPFルータID設定画面	4-33
図4-32	OSPFエリア設定メニュー	4-34
図4-33	OSPFエリア追加例	4-34
図4-34	OSPFバックボーンエリア設定例	4-36
図4-35	OSPFネットワーク範囲設定メニュー	4-37
図4-36	OSPFネットワーク範囲追加例	4-37
図4-37	OSPFスタブホスト設定メニュー	4-39
図4-38	OSPFスタブホスト追加例	4-39
図4-39	OSPFインタフェース設定例	4-41
図4-40	OSPF隣接ルータ設定メニュー例	4-43
図4-41	OSPF隣接ルータ追加例	4-43
図4-42	OSPFバーチャルリンク隣接ルータ設定メニュー	4-45
図4-43	OSPFバーチャルリンク隣接ルータ追加例	4-45
図4-44	OSPFバーチャルリンク設定例	4-47
図4-45	RIP export設定例	4-49
図4-46	AS外のルーティング情報の設定例	4-52
図4-47	AS外のルーティング情報の受信（OSPF import）設定例	4-54

図4-48	AS外のルーティング情報の送信（OSPF export）設定例.....	4-57.....
図4-49	IPXルーティングの拡張設定メニュー	4-60.....
図4-50	RIP(IPX)インタフェース拡張設定例	4-62.....
図4-51	RIP(IPX)フィルタリングテーブル拡張設定例	4-64.....
図4-52	RIP(IPX)フィルタリングテーブル(interface accept)属性.....	4-64.....
図4-53	SAP(IPX)インタフェース拡張設定例	4-67.....
図4-54	SAP(IPX)フィルタリングテーブルの属性の設定例	4-69.....
図4-55	アドレスによるSAP(IPX)フィルタリング設定例	4-70.....
図4-56	サーバ名によるSAP(IPX)フィルタリング設定例	4-71.....
図4-57	タイプによるSAP(IPX)フィルタリング設定例	4-72.....
図4-58	IPX frame type設定例	4-74.....
図4-59	IPX KeepAlive設定例	4-75.....
図4-60	AppleTalkルーティングの拡張設定メニュー（AURPを「not use」とした場合）	4-78
図4-61	AppleTalkルーティングの拡張設定メニュー （AURPを「use」とし、「IP Tunnel」を「not use」とした場合）.....	4-78....
図4-62	AppleTalkルーティングの拡張設定メニュー （AURPを「use」とし、「IP Tunnel」を「use」とした場合）.....	4-79.....
図4-63	AppleTalkインタフェースの設定メニュー.....	4-81.....
図4-64	AppleTalk動作（装置単位）の設定例.....	4-81.....
図4-65	AppleTalk動作（グループ/チャンネル毎）.....	4-83.....
図4-66	サービス(forward)フィルタリングテーブル設定メニュー	4-85...
図4-67	サービス(forward)フィルタリングテーブル追加例	4-85.....
図4-68	ゾーンフィルタリングテーブルの設定メニュー.....	4-87.....
図4-69	ゾーンフィルタリングテーブルの属性の設定例.....	4-87.....
図4-70	ゾーンフィルタリングテーブルの設定メニュー.....	4-88.....
図4-71	ゾーンフィルタリングテーブルの設定例.....	4-88.....
図4-72	accept gatewayの設定メニュー	4-89.....
図4-73	accept gatewayの属性の設定例	4-89.....
図4-74	accept gatewayフィルタリングテーブル設定メニュー	4-90.....
図4-75	accept gatewayフィルタリングテーブル設定例	4-90.....
図4-76	accept portの設定メニュー	4-92.....
図4-77	accept portの属性の設定例	4-92.....
図4-78	accept portフィルタリングテーブルの設定メニュー	4-93.....
図4-79	accept portフィルタリングテーブルの設定例	4-93.....
図4-80	AURPの設定例	4-95.....
図4-81	リモートファイルメンテナンス設定画面.....	4-99.....
図4-82	データ別優先制御設定メニュー.....	4-100.....
図4-83	パラメータの設定例.....	4-101.....
図4-84	データ優先制御IPプロトコル選択画面	4-102.....
図4-85	データ優先制御IPアドレス選択画面	4-104.....
図4-86	データ優先制御IPXプロトコル選択画面	4-106.....
図4-87	データ優先制御IPXアドレス設定画面	4-108.....
図4-88	データ優先制御AppleTalkプロトコル選択画面.....	4-110.....

図4-89	データ優先制御AppleTalkネットワーク番号設定画面.....	4-111....
図4-90	データ優先制御ブリッジング選択画面.....	4-113.....
図4-91	データ優先制御MACアドレス設定画面.....	4-114.....
図4-92	テーブルエントリ間の優先度.....	4-115.....
図4-93	トラヒックロギングテーブル表示例.....	4-116.....
図4-94	トラヒックロギングテーブルIPアドレス設定例.....	4-116.....
図4-95	トラヒックロギングテーブルインタフェース設定例.....	4-117....
図4-96	呼確立リミッタの設定選択画面.....	4-119.....
図4-97	連続接続時間呼確立リミッタの設定例.....	4-119.....
図4-98	トータル接続時間呼確立リミッタ設定画面例.....	4-120.....
図4-99	トータル接続時間呼確立リミッタの変更例.....	4-120.....
図4-100	リモートターゲット設定メニュー.....	4-122.....
図4-101	ルータグループ化機能の設定例.....	4-123.....
図5-1	オペレーションメニュー.....	5-2.....
図5-2	通常回線接続例.....	5-3.....
図5-3	通常回線切断例.....	5-3.....
図5-4	トラヒック分散回線接続例.....	5-4.....
図5-5	トラヒック分散回線切断例.....	5-4.....
図5-6	グループ/チャンネルのオンライン状態への遷移例.....	5-5.....
図5-7	グループ/チャンネルのオフライン状態への遷移例.....	5-5.....
図5-8	呼確立リミッタのスタート画面.....	5-6.....
図5-9	リモートコンソール接続例.....	5-7.....
図5-10	警告メッセージ例.....	5-7.....
図5-11	エコーテストメニュー.....	5-7.....
図5-12	IPエコーテスト例.....	5-8.....
図5-13	IPXエコーテスト例.....	5-9.....
図5-14	AppleTalkエコーテスト例.....	5-10.....
図5-15	パスワード設定例.....	5-11.....
図5-16	構成定義情報保存例.....	5-11.....
図5-17	設定情報確認例.....	5-12.....
図5-18	フレームトレースメニュー画面.....	5-13.....
図5-19	フレームトレースの種類の設定画面.....	5-13.....
図5-20	MACフレームのトレース設定例.....	5-15.....
図5-21	IPフレームのトレース設定例.....	5-17.....
図5-22	IPXフレームのトレース設定例.....	5-18.....
図5-23	AppleTalk フレームのトレース設定例.....	5-19.....
図5-24	Dチャンネルのトレース設定例.....	5-20.....
図5-25	フレームトレースの開始/終了.....	5-21.....
図5-26	フレームトレース結果の表示例.....	5-22.....
図5-27	フレームトレース結果の消去.....	5-22.....
図5-28	フレームトレース結果の解析例.....	5-23.....
図5-29	障害復帰の確認例.....	5-27.....

図5-30	装置リセット例	5-27
図5-31	リンクテストモード移行例	5-29
図5-32	PPP接続診断試験例	5-30
図5-33	LLC-type1接続診断試験例	5-31
図5-34	リンクテストのヘルプ情報	5-32
図5-35	スキャンアウトON時の設定状況画面	5-33
図5-36	スキャンアウトOFF時の設定状況画面	5-33
図5-37	スキャンアウトONの設定	5-33
図5-38	ファイルメンテナンスモードへの移行(自装置の場合)	5-34
図5-39	ファイルメンテナンスモードへの移行(遠隔装置の場合)	5-34
図5-40	ファームウェアの格納状況の表示例	5-35
図5-41	自装置からのファームウェアのダウンロード例	5-36
図5-42	ダウンロードしたファームウェアの起動	5-37
図5-43	有効とするフラッシュメモリの変更	5-37
図5-44	ヘルプ情報の表示画面例	5-37
図5-45	TELNETログイン後のメインメニュー例	5-38
図5-46	リモートコンソール選択後のメインメニュー例	5-39
図5-47	TELNETコンソールからの復帰例	5-40
図6-1	インフォメーションメニュー	6-2
図6-2	IPインタフェース情報例	6-5
図6-3	IPに関する統計情報例	6-7
図6-4	IPルーティング情報例	6-9
図6-5	DHCPリレーエージェントに関する廃棄フレーム	6-10
図6-6	DHCPリレーエージェントに関する統計情報例	6-10
図6-7	IPXインタフェース情報例	6-12
図6-8	IPXに関する統計情報例	6-13
図6-9	IPXルーティング情報例	6-14
図6-10	SAP情報例	6-15
図6-11	ブリッジポートの情報例	6-16
図6-12	ブリッジング機能に関する統計情報例	6-17
図6-13	チャンネル情報例	6-18
図6-14	チャンネル統計情報例	6-19
図6-15	OSPFに関する情報選択メニュー	6-21
図6-16	OSPFに関する一般情報例	6-22
図6-17	OSPFエリアの情報例	6-23
図6-18	OSPFリンクの情報例	6-24
図6-19	OSPFインタフェースの情報例	6-25
図6-20	OSPFバーチャルリンクのインタフェースの情報例	6-26
図6-21	OSPF隣接の情報例	6-27
図6-22	OSPFバーチャルリンクを確立した相手の情報例	6-28
図6-23	AppleTalkのポートの情報例	6-29
図6-24	AppleTalkに関する統計情報	6-31

図6-25	AppleTalkルーティング情報例.....	6-33.....
図6-26	ゾーンリスト表示例.....	6-34.....
図6-27	サービスの情報の取得例.....	6-35.....
図6-28	AURPコネクション情報表示例.....	6-36.....
図6-29	呼確立リミッタに関する情報例.....	6-38.....
図6-30	ルータグループ化に関する情報例.....	6-39.....
図6-31	エラーログ例.....	6-40.....
図6-32	ラインログ例.....	6-40.....
図6-33	トラップログ例.....	6-40.....
図6-34	トラヒックロギングに関する情報例.....	6-41.....
図B-1	HSDを使用する場合.....	B-2.....
図B-2	代表取扱いサービスを利用する場合.....	B-3.....
図B-3	代表取扱いサービスを利用しない場合.....	B-4.....
図B-4	トラヒック分散を利用する場合.....	B-4.....

表目次

表1-1	LED表示ランプの動作	1-10.....
表1-2	LEDの表示	1-11.....
表2-1	ブリッジングにおけるフィルタリングの中継方向.....	2-20.....
表2-2	マルチポートブルータAの内部テーブル.....	2-29.....
表2-3	マルチポートブルータAの内部テーブル.....	2-30.....
表2-4	マルチポートブルータAの内部テーブル.....	2-31.....
表2-5	マルチポートブルータAの内部テーブル.....	2-32.....
表2-6	圧縮の対象となるデータ種別.....	2-40.....
表3-1	ISDNの接続方法およびその他の条件とルーティング機能の関係	3-23.....
表3-2	IPのプロトコル番号例	3-40.....
表3-3	「source address」と「source mask」の組み合わせ例	3-41.....
表3-4	ウエルノウンポート番号.....	3-42.....
表3-5	WAN回線の推奨「ticks」値.....	3-47.....
表3-6	IPXのプロトコル番号例	3-51.....
表3-7	「source network number」と「source mask」の組み合わせ例	3-52.....
表3-8	IPXのソケット番号	3-52.....
表3-9	プロトコル番号表.....	3-87.....
表3-10	コンソールの通信機能設定.....	3-92.....
表3-11	一度オフライン状態にしなければならない設定項目.....	3-152.....
表4-1	「address」と「mask」の組み合わせ例	4-23.....
表4-2	エリアに所属するネットワーク範囲の設定例.....	4-38.....
表4-3	「network number」と「mask」の組み合わせ例	4-65.....
表4-4	アプリケーションとプロトコル.....	4-103.....
表4-5	「address」と「mask」の組み合わせ例	4-105.....
表4-6	IPXプロトコルのアプリケーションとプロトコル	4-106.....
表4-7	「network number」と「mask」の組み合わせ例	4-109.....
表5-1	トレースするフレームの種類.....	5-16.....
表5-2	選択デフォルト再設定項目.....	5-28.....
表A-1	仕様.....	A-1.....
表A-2	電気的条件.....	A-1.....
表A-3	環境条件.....	A-2.....
表A-4	AUIポートのインタフェース仕様.....	A-2.....
表A-5	I430ポートのインタフェース仕様.....	A-3.....
表A-6	コンソールポートのインタフェース仕様.....	A-4.....
表A-7	コンソール仕様.....	A-4.....

表D-1	インフォメーションコマンド一覧	1-1
表D-2	インフォメーションコマンド一覧(つづき)	1-2
表D-3	オペレーションコマンド一覧	1-3

1章 装置に関する基礎知識

この章では、本装置の各部の名称と機能、ケーブルの接続方法、取扱い上の注意、公衆回線網の加入契約条件等装置に関する基礎知識を説明します。装置を使用する前に必ずお読みください。

この章の内容を以下にまとめます。

- 装置外観
- 各部の名称と機能
- 電源の投入 / 遮断
- 各ケーブルの取扱い
- フロッピーディスクユニットの取扱い
- フロントパネルのLED表示
- 公衆回線網の加入契約条件

1.1 装置外観

本装置の外観を図1-1に示します。

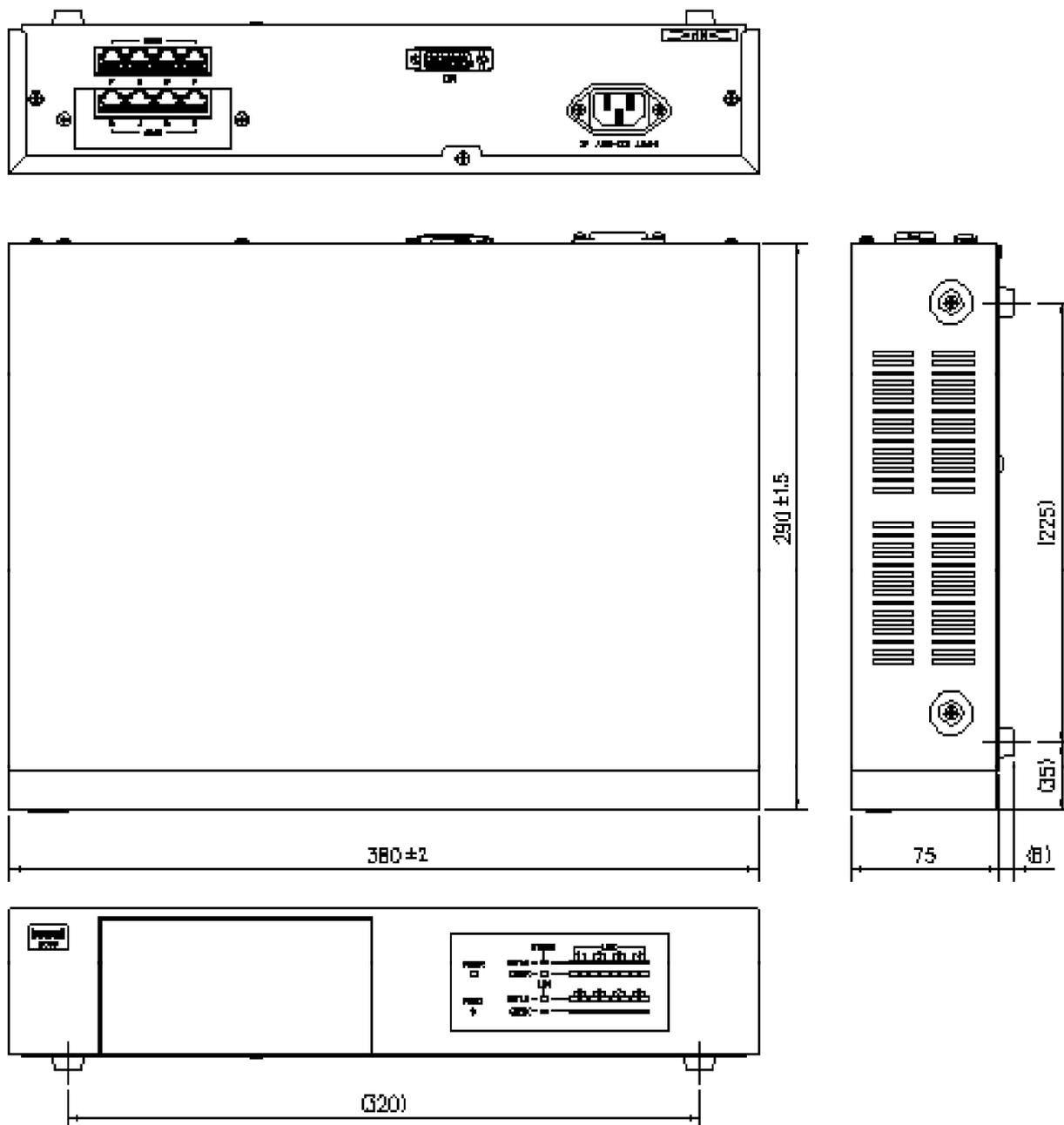


図1-1 装置外観 (単位 : mm)

1.2 各部の名称と機能

図1-2, 1-3, 1-4に本装置の各部の名称を示し, その機能を説明します。

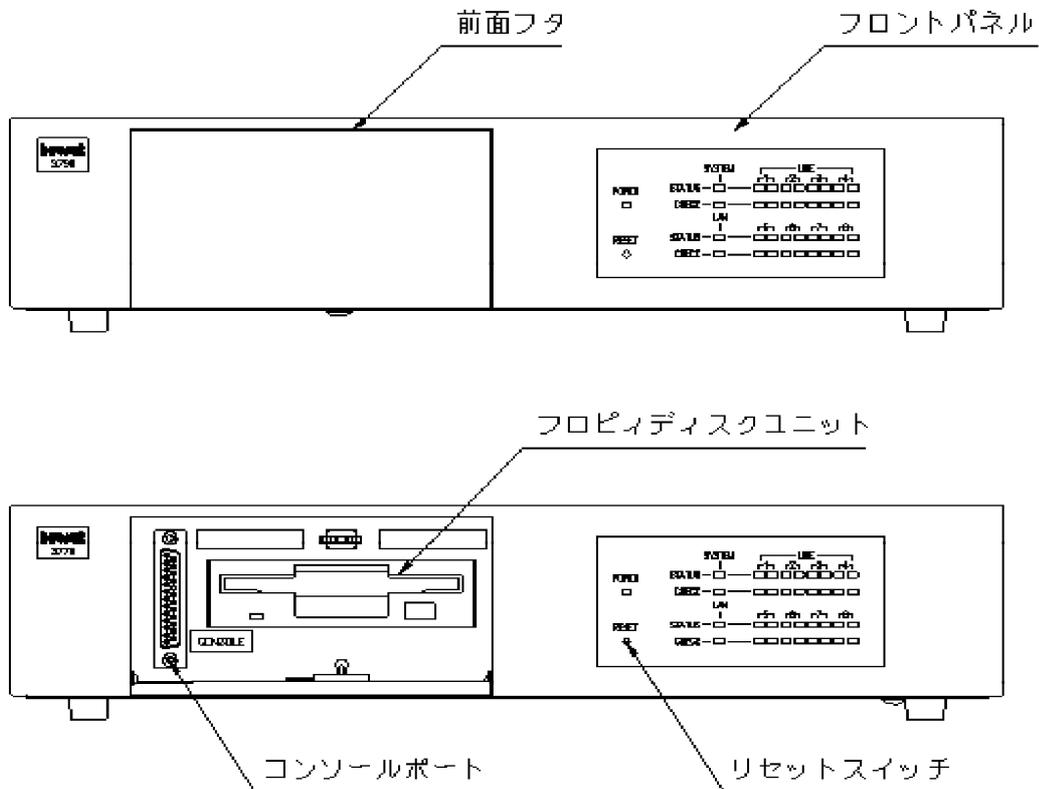


図1-2 装置前面

- フロントパネル
LED表示によって現在の運用状態を示します。



メモ：LED表示の詳細に関しては、「1.6 フロントパネルのLED表示」を参照してください。

- リセットスイッチ
装置をリセットするためのスイッチです。

- 前面フタ
装置の前面フタの内部には、フロッピーディスクユニットとコンソールポートがあります。フタを開けるときはフタの中央上部を軽く押してください。また、フタを閉めるときは、フタの中央上部を軽く押し込んでください。
- コンソールポート
装置の運用状態の表示、コマンドの操作、構成定義情報の表示、設定および変更を行うためにRS-232Cインタフェースを持つ端末を接続するためのポートです。
- フロッピーディスクユニット
装置の構成定義情報のバックアップ、保守に使用します。

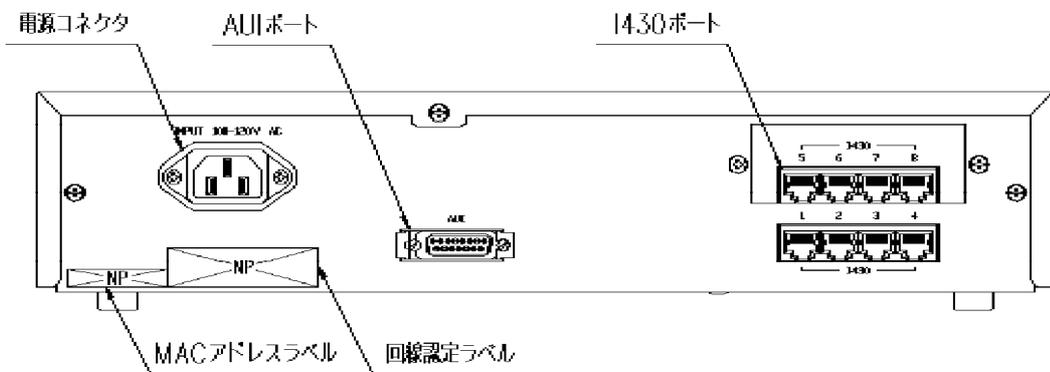


図1-3 装置後面

- 1430ポート
ISDN基本インタフェース、または高速デジタル回線（1インタフェース）を接続するポートです。付属のモジュラーケーブルを接続します。



メモ：本取扱説明書では高速デジタル回線（1インタフェース）をHSD、ISDN基本インタフェースをISDNと表現します。HSD、ISDNについては「1.7 公衆回線網の加入契約条件」を参照してください。



メモ：ISDNは1つのインタフェースで2つのチャネルを使用できる公衆回線網です。

- 電源コネクタ
電源ケーブルの接続コネクタです。
- AUIポート
ISO8802-3（10BASE5）規格のAUIケーブルを接続するためのポートです。
- MACアドレスラベル
装置のMACアドレスを示します。

- 回線認定ラベル
回線認定番号および本装置の機種名を示します。

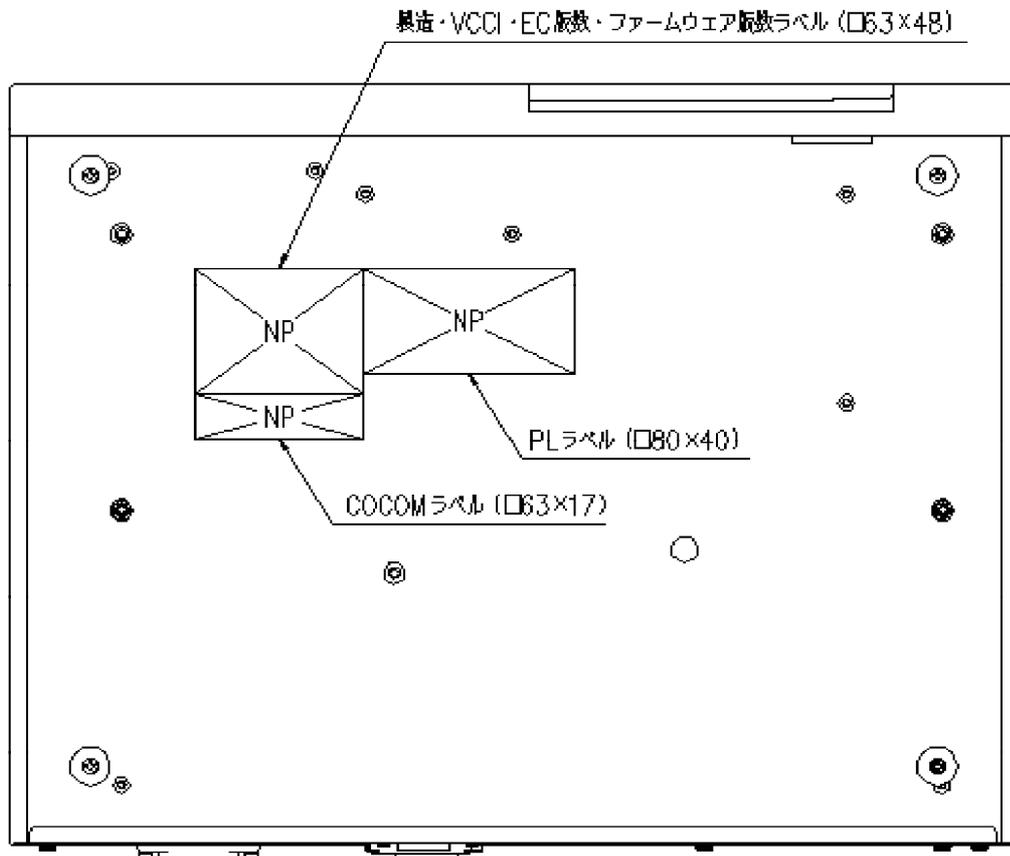


図1-4 装置底面

- 製造・VCCI・EC版数・ファームウェア版数ラベル
装置のシリアル番号，製造年月，装置版数，VCCI（情報処理装置等電波障害自主規制協議会）基準に関する注意書き，ファームウェア版数を示します。
- COCOMラベル
COCOM（対共産圏輸出調整委員会）基準に関する注意書きを示します。
- PLラベル
装置運用上の注意事項を示します。

1.3 電源の投入 / 遮断

電源ケーブルを接続した時点で、電源が投入されます（電源スイッチに相当するものではありません）。また、電源ケーブルを抜くことによって、電源は遮断されます。

1.4 各種ケーブルの取扱い

本装置を導入するためには、各種ケーブルを接続する必要があります。以下のケーブルの取扱い方法を説明します。

- コンソールケーブル（別売）
- AUIケーブル（別売）
- モジュラーケーブル
- 電源ケーブル



メモ：コンソールケーブル、AUIケーブル、モジュラーケーブルは、電源ケーブルを接続する前に接続してください。

1.4.1 コンソール

コンソールの接続は以下の方法で行ってください（図1-4 参照）。

- （1）コンソールポートにコンソールケーブル（RS-232C：ストレート）を接続します。
- （2）コンソールケーブルコネクタのスクリューロックを回し、コネクタを固定します。
- （3）お手持ちのコンソールに同様にしてコンソールケーブルを接続します。
- （4）コンソール使用終了後はコンソールケーブルを取り外し、装置前面のフタを閉めてください。



注意：コンソールには、RS-232C規格インタフェースを持った機器をご使用ください。コンソールポートに接続するコンソールの通信機能は、「付録A 装置の仕様」を参照してください。



メモ：本取扱説明書では、コンソールポートに接続したコンソールを「ローカルコンソール」と表現する場合もあります。

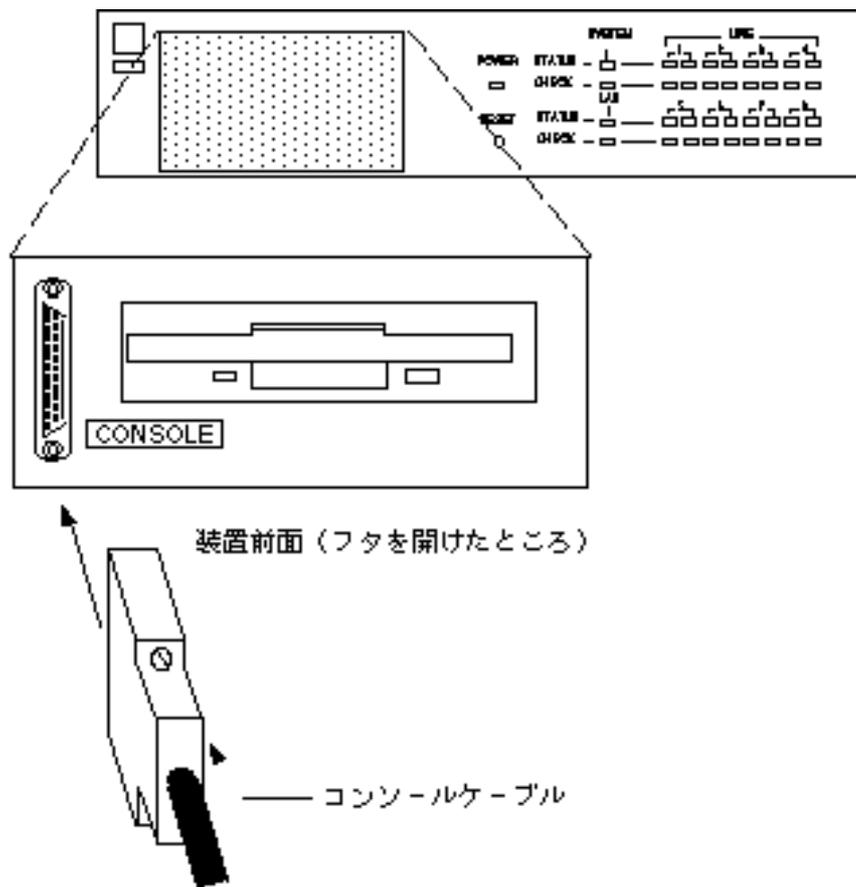


図1-5 コンソールの接続

1.4.2 AUIケーブル

AUIポートにトランシーバ（MAU）と接続しているAUIケーブルを接続してください（図1-5参照）。

AUIケーブルを接続する前にスライドラッチを左側にスライドさせ、ケーブルを接続後スライドラッチを右側にロックしてください。

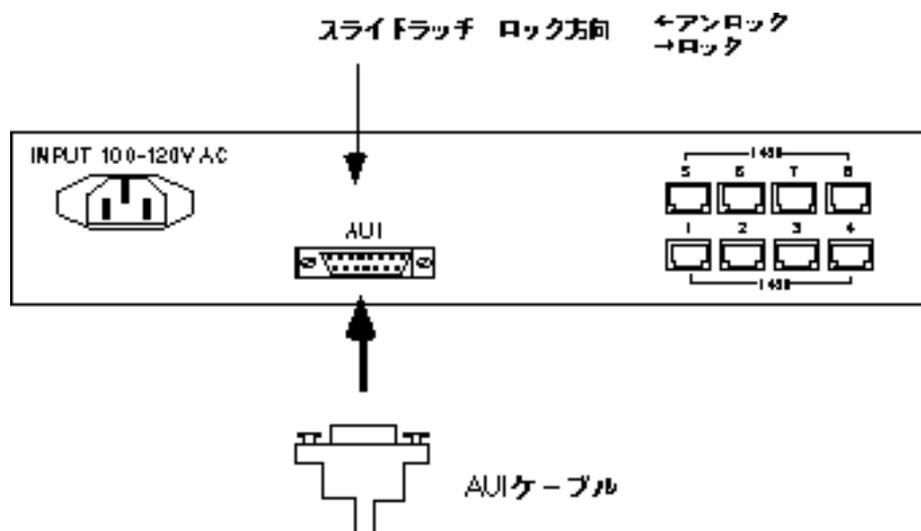


図1-6 AUIケーブルの接続

1.4.3 モジュラーケーブル

1430ポートに、付属のモジュラーケーブルのモジュラーコネクタを「カチン」と音がするまで差し込んでください（図1-7参照）。モジュラーケーブルは同時に最大8本まで接続することができます。

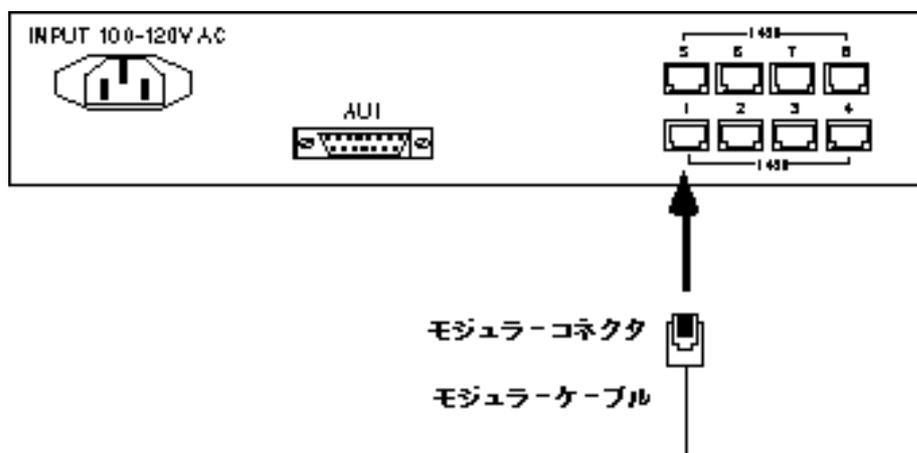


図1-7 モジュラーケーブルの接続

1.4.4 電源ケーブル

電源ケーブルは電源コネクタに差し込んでください（図1-8 参照）。本装置の電源投入は電源プラグの差し込みによって行われます。電源投入後は、LEDのPOWERランプが点灯します。



図1-8 電源ケーブルの接続

1.5 フロッピーディスクユニットの取扱い

本装置のフロッピーディスクユニットにフロッピーディスクを挿入することによって以下のことが実行できます。

- 構成定義情報の保存
- ログ情報の保存



メモ：操作方法については「5.12 構成定義情報，ログ情報の保存」を参照してください。



注意：フロッピーディスクは1.2Mフォーマットの3.5インチ2HDを使用してください。
フロッピーディスクユニットのLEDが点灯中は、絶対にフロッピーディスクを抜かないでください。

1.6 フロントパネルのLED表示

本装置の運用状態は、フロントパネルにあるLED表示ランプによって示されます。LED表示ランプのそれぞれの動作と意味を以下に示します。

表1-1 LED表示ランプの動作

LED		動作
POWER(緑)		電源投入中を示し、通電中は点灯する。
STATUS	SYSTEM (緑)	装置ファームウェアが動作中に点灯する。
	LAN (緑)	LANの状態を示す。データ転送中に点滅する。
	LINE1(緑) ~ LINE8(緑)	HSD (またはISDN) の状態を示す。HSD (またはISDN) が接続すると点灯し、データ転送中は点滅する。(ただし、HSDの場合左側のLEDのみ点灯もしくは点滅、ISDNの場合、チャンネル1の時左側、チャンネル2の時右側のLEDが点灯もしくは点滅する) HSD (またはISDN) 未接続時は消灯する。
	CHECK	a) 立ち上げ時の自己診断でエラーが発生した場合に点灯する。 b) 装置運用に関わる何らかの障害が発生した場合に点滅する。
CHECK	SYSTEM (橙)	a) 立ち上げ時の自己診断でエラーが発生した場合に点灯する。 b) 装置運用に関わる何らかの障害が発生した場合に点滅する。
	LAN(橙)	LANのエラー状態を示す。LANでエラーが発生した場合に点滅する。
	LINE1(橙) ~ LINE8(橙)	HSD (またはISDN) のエラーの状態を示す。HSD (またはISDN) でエラーが発生した場合に点滅する。また、ISDNでケーブル不良、ケーブル抜けの場合点灯する。



メモ：連続接続時間呼確立リミッタが作動した場合（「2.10.8 呼確立リミッタ」），LEDは以下のように点灯します。このような状態になった場合は，その後装置を正しく運用することはできなくなります。

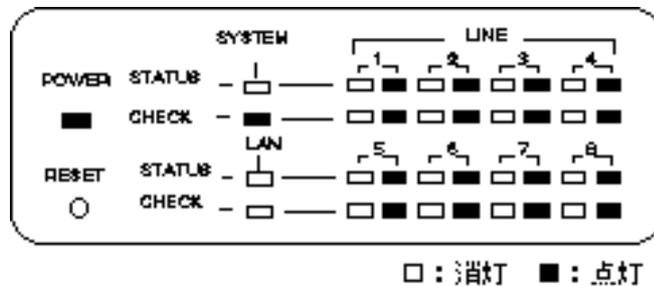


表1-2 LEDの表示

			SYSTEM	LAN	LINE1 ~ LINE8
正常動作	自己診断中 (LED 自己診断中を除く)	STATUS		×	×
		CHECK	×	×	×
	運用中	STATUS		-	-
		CHECK	×	×	×
自己診断でエラー		STATUS	×	-	-
		CHECK		-	-
自動リセット		STATUS		-	-
		CHECK		×	×
AUIポートの通信でエラー		STATUS		-	-
		CHECK	×		×
WAN回線の通信でエラー		STATUS		-	-
		CHECK	×	×	
ISDNケーブル不良・ケーブル抜け		STATUS		-	-
		CHECK	×	×	

表内の記号の説明

- : 点滅
- : 点灯
- × : 消灯
- : 運用形態による



注意： 自己診断テスト中は、フロントパネルのLED（POWERは除く）の点灯・消灯を行います。自己診断テスト中は、絶対にケーブルの抜き差しを行わないでください。



メモ： 自己診断でエラーが発生した場合は、担当営業または保守員までご連絡ください。

1.7 公衆回線網の加入契約条件

本装置は公衆回線網として以下の2種類のうちどちらかを使用することができます。

- 日本電信電話株式会社（以降NTTとする）スーパーデジタル（Iインタフェース）
- NTT INSネット64

これらの公衆網をご利用になる場合の加入契約条件について説明いたします。なお、本取扱説明書および本装置では、それぞれの回線を以下のように表現します。また、本取扱説明書では、これらの回線を総称してWAN回線と表現します。

- NTT スーパーデジタル : 高速デジタル回線またはHSD
- NTT INSネット64 : ISDN回線またはISDN

1.7.1 HSDをご利用になる場合の契約条件について

HSDを契約される際は、回線速度によって以下の2品目のうちどちらかを指定してください。

- スーパーデジタル（Iインタフェース） 64kbps
- スーパーデジタル（Iインタフェース） 128kbps

1.7.2 ISDNをご利用になる場合の契約条件について

ISDNをご利用になる場合の契約条件について説明します。以下の制限事項に従って契約条件をご確認ください。

(1) インタフェース形態およびレイヤ1 起動種別

- 本装置を使用する場合、**P-MP接続** で契約してください。
- レイヤ1 起動種別は、**呼毎起動** と**常時起動** のどちらでも動作します。

(2) 通信形態

- **通話モード・デジタル通信モード** で契約してください。
- 発信者番号通知は、**呼毎通知許可** で契約してください。



メモ：上記の契約条件を満たさない場合、本装置でISDNを運用することはできません。



メモ：本装置では、NTTのサービスである「代表取扱いサービス」に対応するための機能をサポートしています。詳細については、「2.10.5 チャンネルグループ機能」を参照してください。

2章 装置の機能

この章では、本装置の主な機能について説明します。
この章の内容を以下にまとめます。

- 運用形態
- データリンクプロトコル
- IPホスト機能
- IPルーティング機能
- IPXルーティング機能
- IP, IPXパケットフィルタリング機能
- AppleTalkルーティング機能
- ブリッジング機能
- ISDNに関する機能
- ネットワーク管理機能
- TELNETサーバ機能
- リモートコンソール機能
- 簡易コマンド機能
- データ圧縮機能
- データ別優先制御機能
- DHCPリレーエージェント機能
- ルータグループ化機能
- トラヒックロギング機能

2.1 運用形態

本装置は、HSDまたはISDNを複数利用して遠隔地のLANを接続することができるLAN間接続装置（マルチポートブロータ）です。

本装置を利用した運用形態を付録Bに示します。

2.2 データリンクプロトコル

本装置ではWAN回線の接続に利用するデータリンクプロトコルとして、PPPをサポートしています。PPPプロトコルを使用すると、PPPを使用した他社の装置との接続が可能となります。

2.3 IPホスト機能

本装置では、IPのルーティングを行わない場合でも、IPホストとして運用することができます。本装置をIPホストとして運用する場合には、ネットワーク管理機能、TELNETサーバ機能、リモートコンソール機能を利用することができます。

2.4 IPルーティング機能

本装置は、IPパケットのルーティング機能をサポートしています。本装置のIPルーティング機能で、RIP(Routing Information Protocol)を利用したダイナミックルーティング、またはOSPF(Open Shortest Path First)を利用したダイナミックルーティングとスタティックルーティングを併用して運用することができます。また接続相手によりネットワークの形態(以降インタフェースタイプ)を選択して運用することができます。

2.4.1 RIPを利用したダイナミックルーティング

本装置は、RIPによるダイナミックルーティング機能をサポートしています。この機能により、本装置の持っているルーティング情報をRIPでネットワークへ広告します。また、RIPで獲得したルーティング情報によってルーティングテーブル(最大3000エントリ)の更新を行います。

ダイナミックルーティングは、ルータ間でルーティング情報の交換を行い、経路を決定する方法です。ルータ間の情報交換により経路を決定しますので、ルータの故障やネットワークの故障を発見し、常に最適な経路をダイナミックに選択できます。

2.4.2 OSPFを利用したダイナミックルーティング

本装置は、OSPFを利用したダイナミックルーティング機能をサポートしています。この機能により、本装置の持っているルーティング情報をOSPFでネットワークへ広告します。また、OSPFで獲得したルーティング情報によってルーティングテーブル(最大3000エントリ)の更新を行います。

OSPFを利用したダイナミックルーティングはリンクステートアルゴリズムを基本としているので、比較的大規模なネットワークでの運用に有効です。またOSPFを利用したダイナミックルーティングでは、大規模なネットワークをいくつかのエリアに分けて、階層的にルーティングの制御を行うことができます。

本装置は、OSPFが定義するAS境界ルータ、エリア境界ルータ、内部ルータのいずれでも(あるいはいくつか兼ねて)運用することができます。

- AS境界ルータ..... 他のAS(Autonomous System: 自律システム)との境界として運用されるルータ
- エリア境界ルータ..... 複数のエリアの境界として運用されるルータ
- 内部ルータ エリア内で運用されるルータ

OSPFを運用している環境を図2-1で示します。

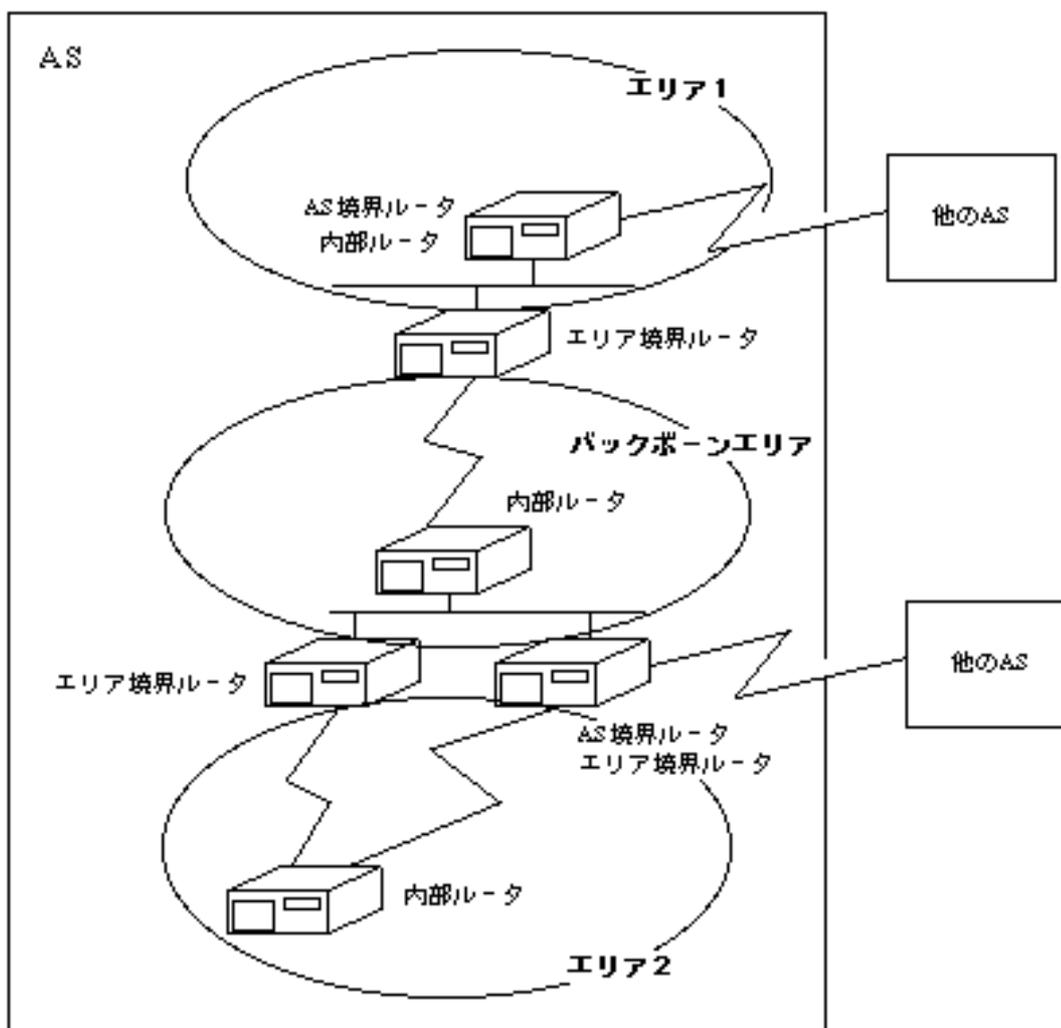


図2-1 OSPF運用環境



メモ：距離ベクタルーティングとリンクステートルーティング

距離ベクタルーティングでは、ルーティング情報として到達可能なネットワークとその距離（経由するルータ数）を交換します。この距離ベクタルーティングの代表例であるRIPは、ほとんどのルータで採用されています。しかし、RIPでは、扱うことができる距離に最大15という制限があり、経路情報が変化したときの収束が遅いなどの問題があるため、多数の経路情報からなる大規模なネットワークには不向きであるといわれています。

一方、リンクステートルーティングでは、ネットワーク全体の接続状態に関する情報を各ルータが保持し、それを同期させながらルーティングを行います。リンクステートルーティングの一つであるOSPFでは、ネットワークまでの距離として60000を越える値が定義されており、事実上距離による制限はありません。また、経路情報の収束が比較的短時間で行われます。このためRIPに比べ大規模なネットワークに適しているといわれています。

2.4.3 スタティックルーティング

本装置は、ルーティング情報を設定により有効にするスタティックルーティングをサポートしています。

スタティックルーティングは、装置に設定された経路情報に従って経路を決定する方法です。

2.4.4 ダイナミックルーティングとスタティックルーティングの関係

同じ宛先への経路が、ダイナミックルーティングで獲得したルーティング情報と、スタティックルーティングにより設定したルーティング情報で異なる場合、本装置ではどちらの情報を有効にするかを選択することができます。



メモ：同じ宛先への経路が、ダイナミックルーティングで獲得したルーティング情報と、スタティックルーティングにより設定したルーティング情報で異なる場合、それぞれの持つ優先度（「preference」値）によりどちらの情報を有効にするかを決定します。本装置では、スタティックルーティングの「preference」値を設定することができます（RIPは固定）。「preference」値が同じ場合には、宛先へ到達するために経由するルータの数（メトリック値）の少ない経路を有効とします。

2.4.5 インタフェースタイプ

本装置は、インタフェースタイプとして以下の2通りをサポートしています。

(1) ポイントツーポイント

HSDを介して本装置どうしを接続する場合、またはISDNを介して特定の相手と接続する場合には、インタフェースタイプにポイントツーポイントを選択します。ポイントツーポイントはWAN回線にネットワークを割り当てる必要の無いインタフェースタイプです。

図2-2に、IPポイントツーポイント接続例を示します。

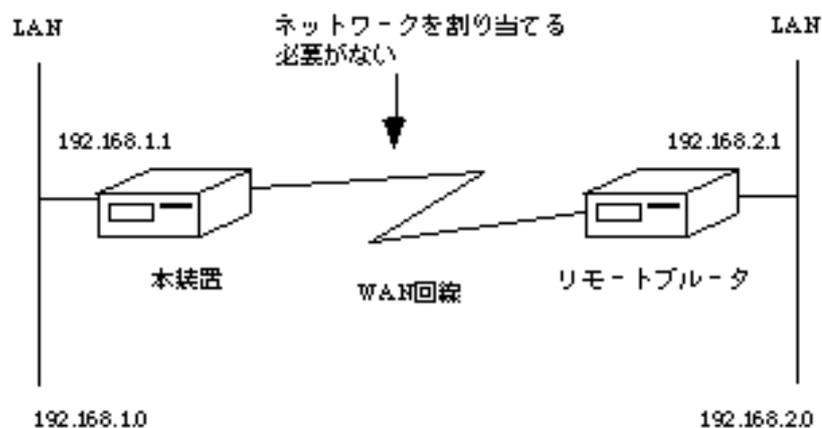


図2-2 IPポイントツーポイント接続例

(2) ブロードキャスト(broadcast)

HSDを介して本装置とブリッジまたはポイントツーポイントインタフェースをサポートしていないルータと接続する場合、またはISDNを介して複数の相手と接続する場合には、インタフェースタイプにブロードキャストを選択します。ブロードキャストはWAN回線にネットワークを割り当てなくてはならないインタフェースタイプです。

図2-3に、IPブロードキャスト接続例を示します。

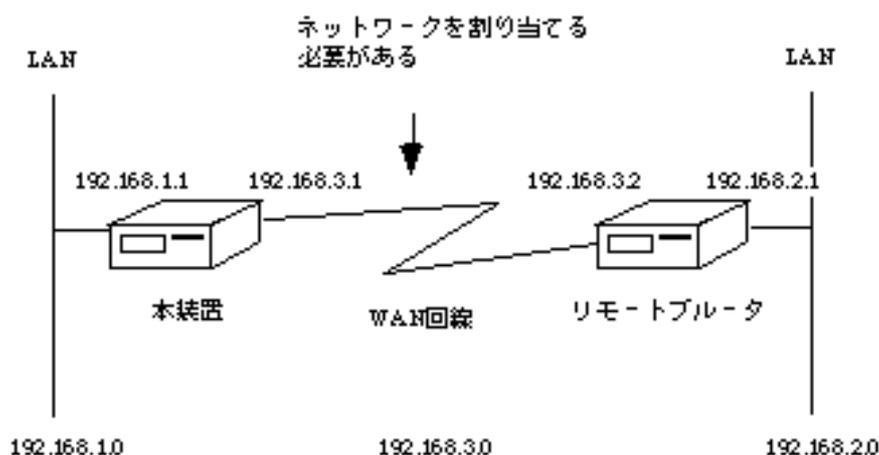


図2-3 IPブロードキャスト接続例

2.4.6 Proxy ARP機能

本装置は、サブネットの概念を持たない端末のARPの要求に対して、装置自身のMACアドレスを応答する機能（Proxy ARP機能）をサポートしています。

本装置のProxy ARP機能は、以下の2通りがあります。

- (1) 中継すべきアドレスへのARPの要求に対して代理応答する。
- (2) すべてのARPの要求に対して代理応答する。

図2-4にProxy ARP機能利用環境を示します。図2-4では、本装置をマルチポートブルートと表現します。ネットワークA, B, Cは同じネットワーク番号をサブネットに分けて運用しています。Proxy ARP機能(1)の場合、マルチポートブルートAは、端末からネットワークAまたはネットワークBにあるホスト宛のARPの要求に対して代理応答し、ネットワークCにあるホスト宛のARPの要求に対しては代理応答しません。Proxy ARP機能(2)の場合、マルチポートブルートAは、ネットワークA, B, CにあるホストへのARPの要求に対して代理応答します。本装置ではProxy ARP機能(1), (2)のどちらを利用するかを選択することができます。(2)は、ルータbがProxy ARPをサポートしていない場合に選択します。

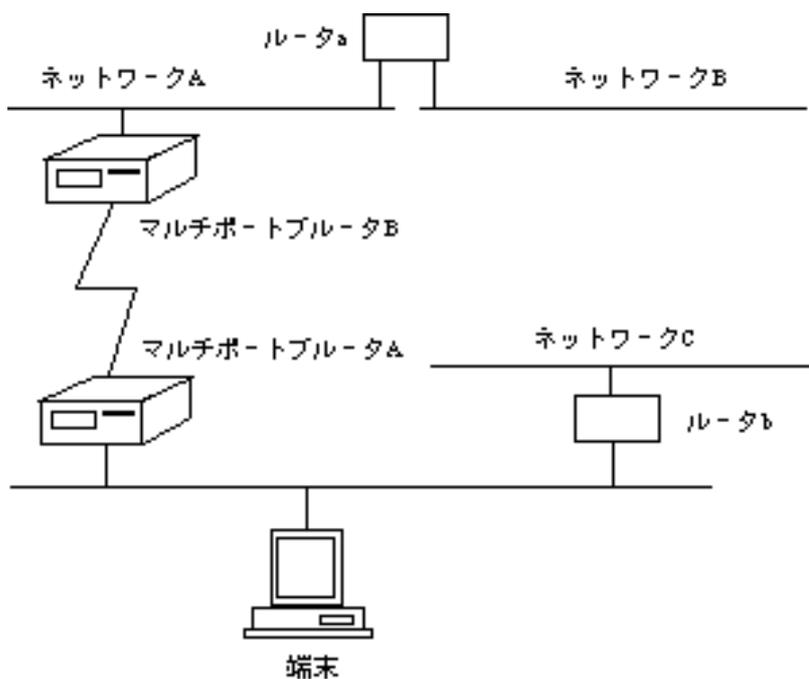


図2-4 Proxy ARP機能利用環境

2.4.7 DHCPリレーエージェント機能

本装置は、IPホストの自動設定に利用されるBOOTPおよびDHCPに関して、クライアント（IPホスト）とサーバ間でBOOTPおよびDHCPパケットを中継するためのリレーエージェント機能をサポートしています。

以下に運用形態例を示します。

(1) 形態1

LAN側のクライアントとWAN側のサーバ間で、BOOTP/DHCPパケットを転送します。

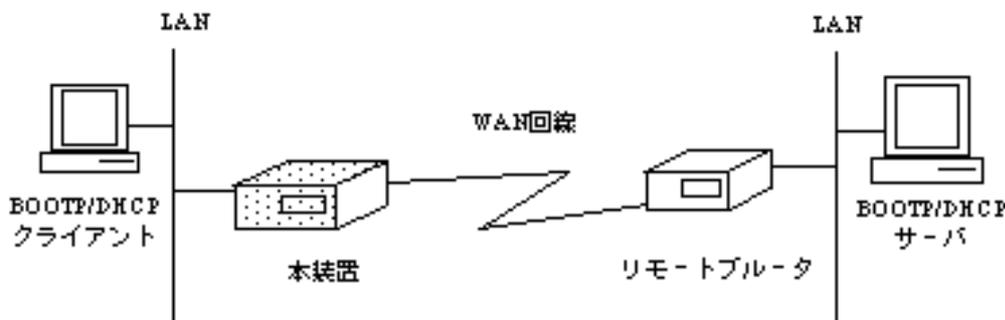


図2-5 DHCP運用形態例1

(2) 形態 2

LAN側のクライアントとLAN側のサーバ間で、BOOTP/DHCPパケットを転送します。

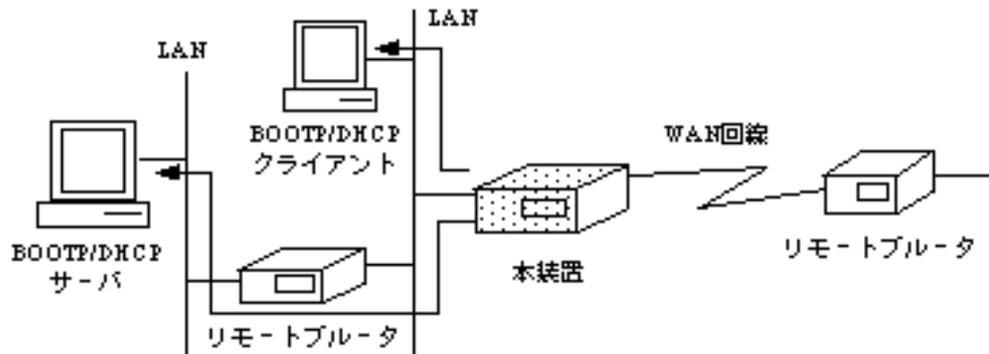


図2-6 DHCP運用形態例 2



メモ：DHCPリレーエージェント機能に関しては、以下のドキュメントを参考にしています。

- BOOTSTRAP PROTOCOL (BOOTP) : RFC951
- Dynamic Host Configuration Protocol : RFC1541
- Clarifications and Extensions for BOOTP : RFC1542

- DHCP Options and BOOTP Vendor Extensions : RFC1533
- Interoperation Between DHCP and BOOTP : RFC1534

2.5 IPXルーティング機能

本装置は、Novell社の開発したNetWareで利用されるIPXパケットをルーティングする機能をサポートしています。本装置のIPXルーティング機能は、RIP(Routing Information Protocol)を用いたダイナミックルーティングと、スタティックルーティングをサポートしています。またネットワークの形態（以降インタフェースタイプ）はブロードキャストタイプのみをサポートしています。

2.5.1 ダイナミックルーティング

本装置は、RIPを利用したダイナミックルーティング機能をサポートしています。この機能により、本装置の持っているルーティング情報をRIPでネットワークへ広告します。また、RIPで獲得したルーティング情報によってルーティングテーブル（最大500エントリ）の更新を行います。

ダイナミックルーティングは、ルータ間でルーティング情報の交換を行い、経路を決定する方法です。ルータ間の情報交換により経路を決定しますので、ルータの故障やネットワークの故障を発見し、ダイナミックに経路の変更を行うことができます。

2.5.2 スタティックルーティング

本装置は、ルーティング情報を設定により有効にするスタティックルーティングをサポートしています。

スタティックルーティングは、装置に設定された経路情報に従って経路を決定する方法です。

2.5.3 ダイナミックルーティングとスタティックルーティングの関係

同じ宛先への経路が、ダイナミックルーティングで獲得したルーティング情報と、スタティックルーティングにより設定したルーティング情報で異なる場合、本装置ではどちらの情報を有効にするかを選択することができます。



メモ：IPXルーティングでは、宛先への到達時間（「ticks」値）が最も少ない経路を最適経路とします。同じ宛先への経路が、ダイナミックルーティングで獲得したルーティング情報と、スタティックルーティングにより設定したルーティング情報で異なる場合、「ticks」値の小さい方を有効とします。「ticks」値が同じ場合は、宛先へ到達するために経由するネットワークの数（メトリック値）が最も少ない経路を有効とします。

2.5.4 インタフェースタイプ

本装置は、インタフェースタイプとして以下に示すブロードキャストタイプのみをサポートしています。ブロードキャストはWAN回線にネットワークを割り当てなくてはならないインタフェースタイプです。

図2-8にブロードキャスト接続例を示します。

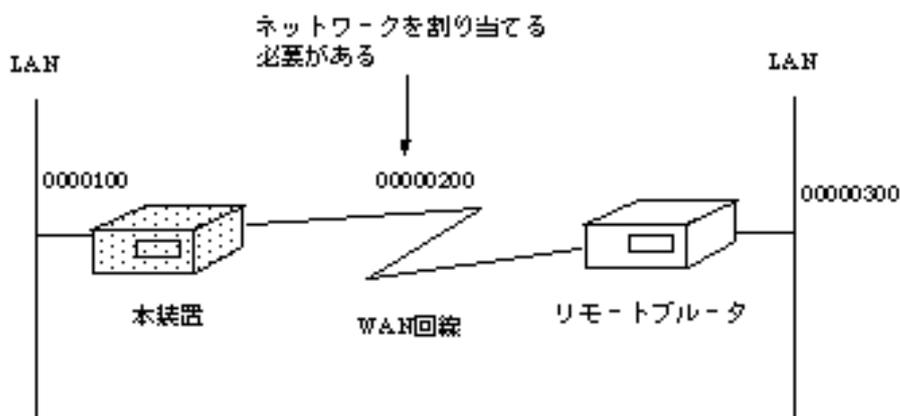


図2-7 IPXブロードキャスト接続例

2.5.5 IPXのKeepAliveパケットの代理応答 / 要求機能

本装置はISDNの課金を抑制する機能として、IPXのKeepAliveパケットに関して代理に回答 / 要求する機能をサポートしています。（ 2.8.5(2) KeepAliveの代理応答 / 要求」）

2.6 IP,IPXパケットフィルタリング機能

本装置は、主にセキュリティを強化する機能として、IP,IPXパケットをフィルタリング（中継 / 遮断）する機能をサポートしています。方法としては、以下の4種類があり、すべてを組み合わせる使用することができます。それぞれの方法をIPパケットを例として説明します。

- 送信元 / 宛先アドレスによるフィルタリング（ 2.6.1）
- プロトコル識別によるフィルタリング（ 2.6.2）
- 上位プログラムによるフィルタリング（IP:ポート，IPX:ソケット識別）（ 2.6.3）
- 送信可 / 受信可インタフェースによるフィルタリング（ 2.6.4）

2.6.1 送信元 / 宛先アドレスによるフィルタリング

図2-8にIPルーティング使用時の送信元アドレス、宛先アドレスフィルタリングの使用例を示します。図2-8のマルチポートブロータAは、送信元アドレスによるフィルタリングを行います。送信元が192.168.1.1のパケットは中継し、192.168.1.2のパケットは遮断する設定を行っています。この場合、図に示すように192.168.1.1からのパケットはWAN回線に中継し、192.168.1.2からのパケットはWAN回線に中継しません。マルチポートブロータBは宛先アドレスフィルタリングを行います。宛先が192.168.2.1のパケットは中継し、192.168.2.2のパケットは遮断する設定をしています。この場合、図に示すように192.168.2.1宛のパケットはLANに中継し、192.168.2.2宛のパケットはLANに中継しません。

送信元アドレス、宛先アドレスによるフィルタリングは同時に使用することができます。また、IPXルーティング時と同じ設定を行うことにより送信元アドレス、宛先アドレスによるフィルタリングを行うことができます。

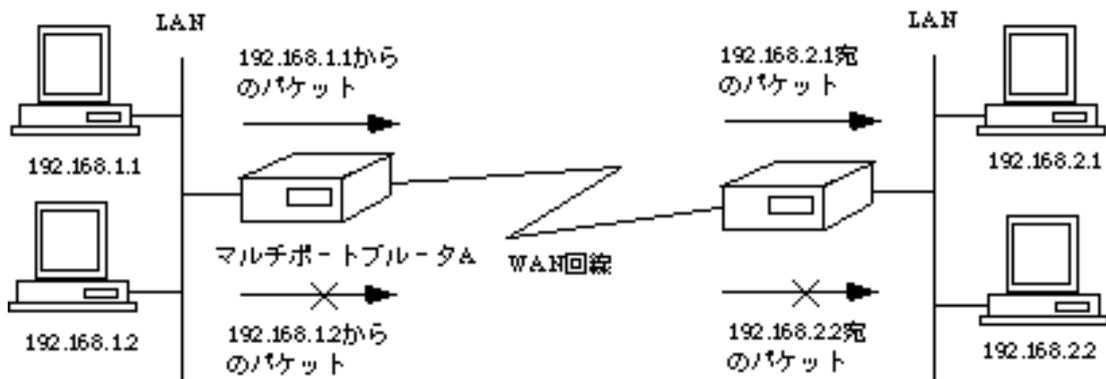


図2-8 送信元 / 宛先アドレスによるフィルタリング

2.6.2 プロトコル識別によるフィルタリング

図2-9にIPルーティング使用時のプロトコル識別によるフィルタリングの使用例を示します。図2-9のマルチポートブリュータAでは、TCPパケットは中継し、UDPパケットは遮断する設定を行っています。この場合、図に示すようにTCPパケットはWAN回線に中継し、UDPパケットはWAN回線に中継しません。IPルーティング時に識別できるプロトコルを以下に示します。

- TCP
- UDP
- その他（プロトコル番号（ 「3.2.12 ワークシート「IPパケットフィルタリング編」」）により指定）

IPXルーティング時も同様の設定を行うことによりプロトコル識別によるフィルタリングを行うことができます。IPXルーティング時に識別できるプロトコルを以下に示します。

- NCP
- SPX
- NetBIOS
- unknown
- その他（プロトコル番号（ 「3.2.15 ワークシート「IPXパケットフィルタリング編」」）により指定）

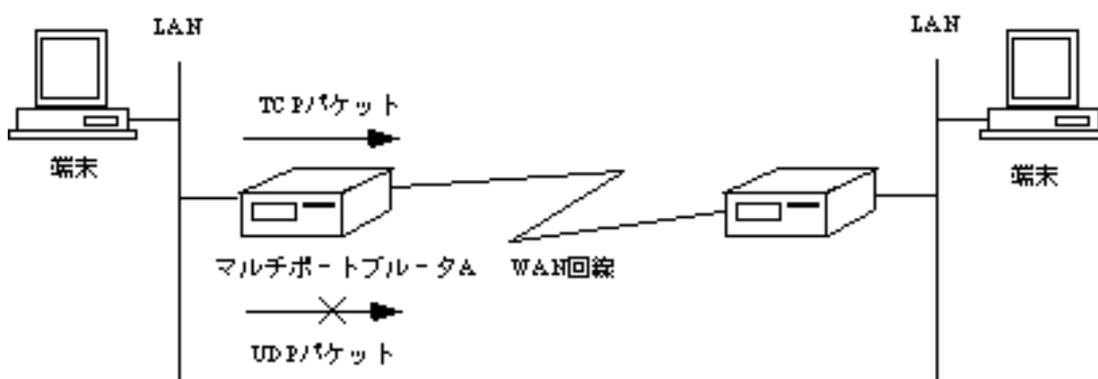


図2-9 プロトコル識別によるフィルタリング

2.6.3 上位プログラムによるフィルタリング

図2-10にIPルーティング時の上位プログラムによるフィルタリングの使用例を示します。IPルーティング時は上位プログラムをポート番号（「3.2.12 ワークシート「IPパケットフィルタリング編」」）で識別します。図2-10のマルチポートブルータAはポート番号'23'(TELNETポート)宛のパケットは中継し、ポート番号'21'(FTPポート)宛のパケットは遮断する設定を行っています。この場合、図に示すように端末間のTELNETは実行できますが、FTPは実行できません。

IPXルーティング時も同じ設定を行うことにより上位プログラムによるフィルタリングを行うことができます。IPXルーティング時は上位プログラムをソケット番号（「3.2.15 ワークシート「IPXパケットフィルタリング編」」）で識別します。

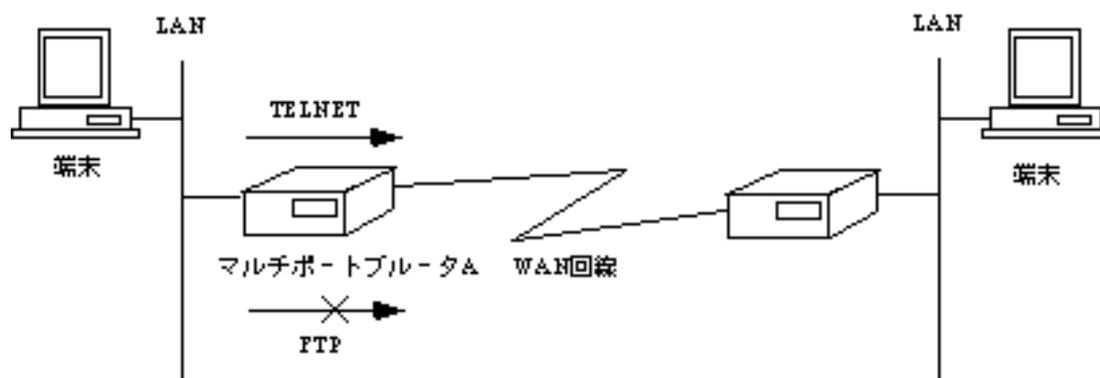


図2-10 上位プログラムによるフィルタリング

2.6.4 送信可 / 受信可インタフェースによるフィルタリング

図2-11にIPルーティング時の送信可インタフェース、受信可インタフェースによるフィルタリングの使用例を示します。図2-11のマルチポートブルータAは受信可インタフェースをLAN、送信可インタフェースをWAN回線に設定してあります。この場合、図に示すようにLANからWAN回線への中継は行いますが、WAN回線からLANへの中継は行いません。

IPXルーティング時も同じ設定を行うことにより送信可インタフェース、受信可インタフェースによるフィルタリングを行うことができます。

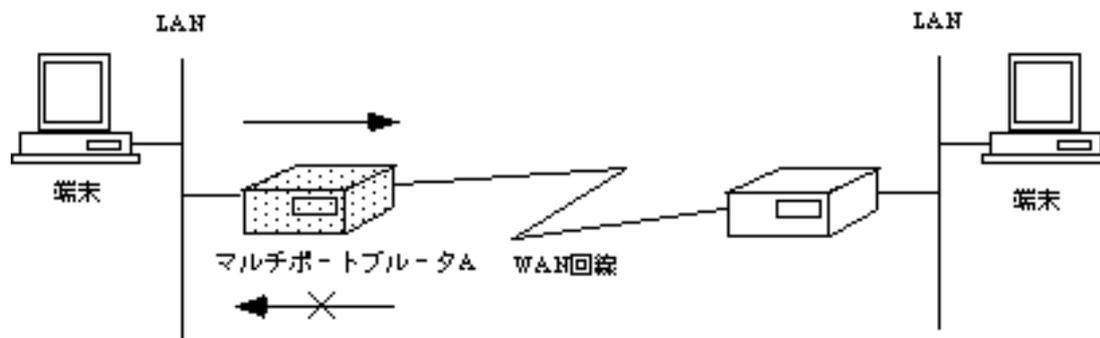


図2-11 送信可 / 受信可インタフェースによるフィルタリング

2.7 AppleTalkルーティング機能

本装置は、アップルコンピュータ社の開発したMacintoshで利用されるAppleTalkパケットをルーティングする機能をサポートしています。本装置のAppleTalkルーティング機能は、RTMP(Routing Table Maintenance Protocol)/ZIP(Zone Information Protocol)もしくはAURP(AppleTalkUpdate-based Routing Protocol)を用いたダイナミックルーティングと、スタティックルーティングをサポートしています。WANポートには特にネットワーク番号範囲を設定する必要はありません。

2.7.1 ダイナミックルーティング

本装置は、RTMP/ZIPおよびAURPを利用したダイナミックルーティング機能をサポートしています。この機能により、本装置の持っているルーティング情報をRTMPおよびAURPでネットワークへ広告します。また、RTMP/ZIPおよびAURPで獲得したルーティング情報によってルーティングテーブル(最大300エントリ)の更新を行います。

ダイナミックルーティングは、ルータ間でルーティング情報およびゾーン情報の交換を行い、経路を決定する方法です。ルータ間の情報交換により経路を決定しますので、ルータの故障やネットワークの故障を発見し、ダイナミックに経路の変更を行うことができます。

2.7.2 スタティックルーティング

本装置は、ルーティング情報を設定により有効にするスタティックルーティングをサポートしています。

スタティックルーティングは、装置に設定された経路情報に従って経路を決定する方法です。

2.7.3 AURP

本装置は、大規模ネットワークでのAppleTalkルーティングを可能とするAURPをサポートしています。この機能により、IP Tunnelをはじめ様々なオプションを使用したルーティングを行うことができます。

(1) Point-to-point Tunnel

AURPを使用した場合、Point-to-point Tunnelを行います。Point-to-point Tunnelでは、ポートがUPしたときの初期情報の交換と、ルーティング情報に変更があったときのみ交換を行い、ルーティング情報の定期送信は行いません。

AURPを使用している環境例と設定例を以下の図2-12に示します。

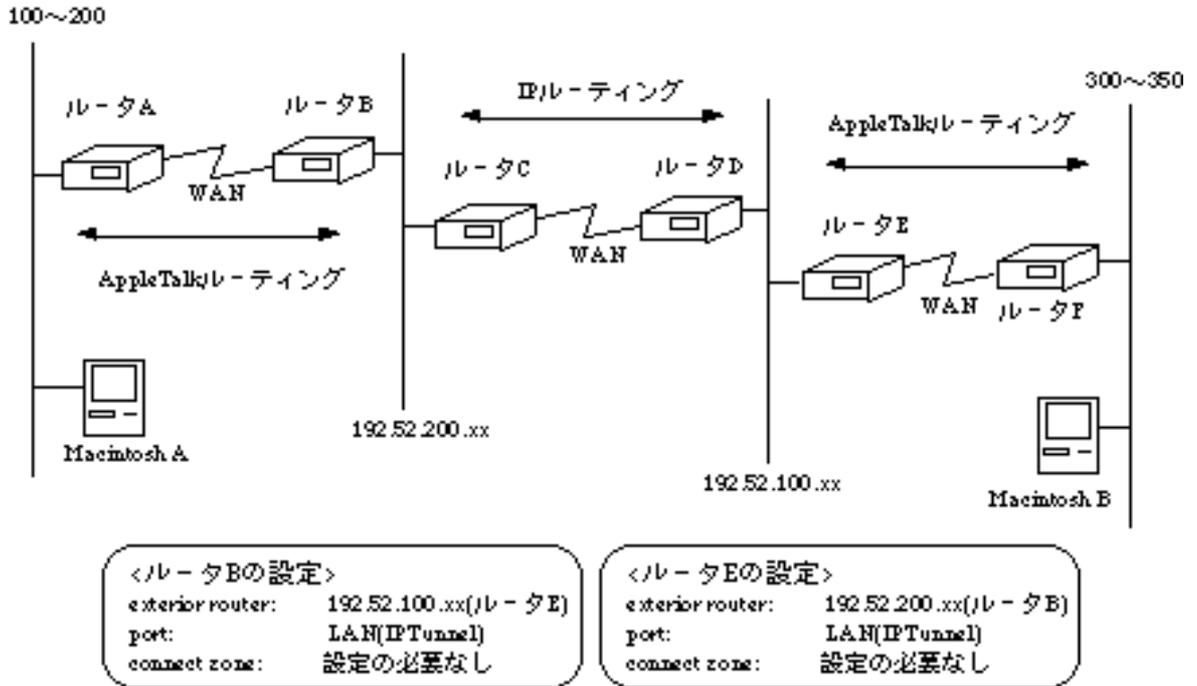


図2-12 AURPを使用している環境の例

(2) IP Tunnel

IP Tunnelを使用すると、通信したいMacintosh同士の経路にIPルーティングしか行わないネットワークが存在しても、AppleTalkパケットをIPパケットにカプセル化して送信するため通信が可能となります。

図2-12においてMacintosh AとMacintosh Bが通信を行う場合、ルータC、ルータDはIPルーティングの機能しか持たないため、IP Tunnelを利用して通信を行います。設定例として、ルータBおよびルータEはIP Tunnelを使用するとし、お互いのIPアドレスを設定します。

(3) リマッピング

AppleTalkネットワークでは、異なるネットワークのネットワーク番号範囲が重なる可能性があります。リマッピングを使用すればこの問題を解決することができます。リマッピングとは、AURPを使用しているポートから受信したルーティング情報は内部的にネットワーク番号範囲をふり直す機能です。ルータBでリマッピングを行うと、ルータAではルータBより先にあるAppleTalkのネットワークのネットワーク番号範囲をすべてリマッピングした値で受信します。

(4) クラスタリング

複数のルーティング情報を同時に受信した場合に、それを一つのルーティング情報として送信する機能です。

例えば、501~600のネットワークのルーティング情報と、101~200のネットワークのルーティング情報を受信した場合、それを5001~5200の1つのルーティング情報として扱うことで、これにより送信するデータ量を減少させることができます。

2.8 AppleTalkパケットフィルタリング機能

本装置は、主にセキュリティを強化する機能として、AppleTalkパケットをフィルタリング（中継／遮断）する機能をサポートしています。方法としては以下の3種類があり、すべてを組み合わせる使用することができます。それぞれの方法を以下に説明します。

- DDPフィルタリング（ 2.8.1）
- ゾーンフィルタリング（ 2.8.2）
- サービスフィルタリング（ 2.8.3）

2.8.1 DDPフィルタリング

DDPフィルタリングには、アドレス、プロトコルおよびポートの識別によるフィルタリングがあり、これらを組み合わせる使用することができます。

(1) 送信元／宛先アドレスによるフィルタリング

図2-13にAppleTalkルーティング使用時の送信元アドレス、宛先アドレスフィルタリングの使用例を示します。

図2-13のマルチポートルータAは、送信元アドレスによるフィルタリングを行います。送信元ネットワーク番号が100のパケットは中継し、ネットワーク番号105のパケットは遮断する設定を行っています。この場合、図に示すようにネットワーク番号100からのパケットはWAN回線に中継し、ネットワーク番号105からのパケットはWAN回線に中継しません。マルチポートルータBは宛先アドレスフィルタリングを行います。宛先がネットワーク番号200のパケットは中継し、ネットワーク番号205のパケットは遮断する設定をしています。この場合、図に示すようにネットワーク番号200宛のパケットはLANに中継し、ネットワーク番号205宛のパケットはLANに中継しません。

送信元アドレス、宛先アドレスによるフィルタリングは同時に使用することができます。

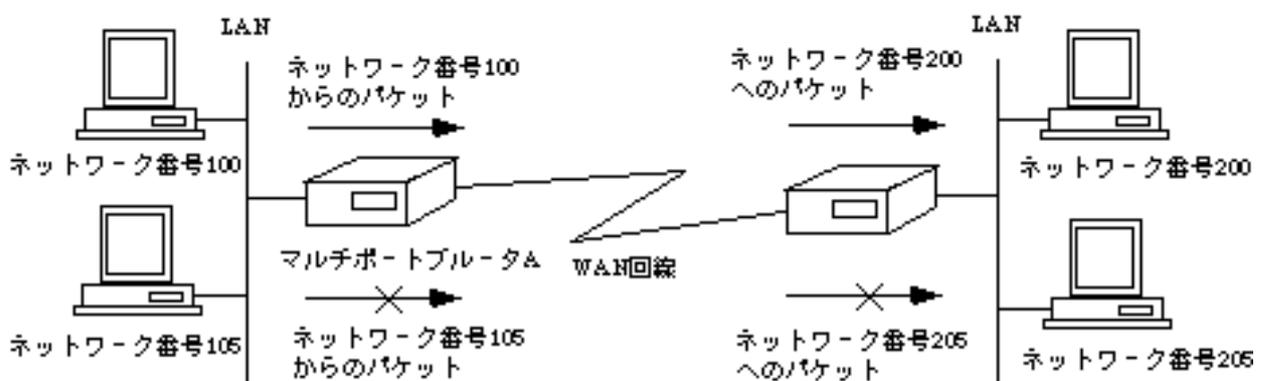


図2-13 送信元／宛先アドレスによるフィルタリング

(2) プロトコル識別によるフィルタリング

図2-14にAppleTalkルーティング使用時のプロトコル識別によるフィルタリングの使用例を示します。図2-14のマルチポートブルータAでは、ZIPパッケージは中継し、NBPパッケージは遮断する設定を行っています。この場合、図に示すようにZIPパッケージはWAN回線に中継し、NBPパッケージはWAN回線に中継しません。AppleTalkルーティング時に識別できるプロトコルを以下に示します。

- RTMP(Rp/Dt)
- NBP
- ATP
- AEP
- RTMP(Rq)
- ZIP
- ADSP

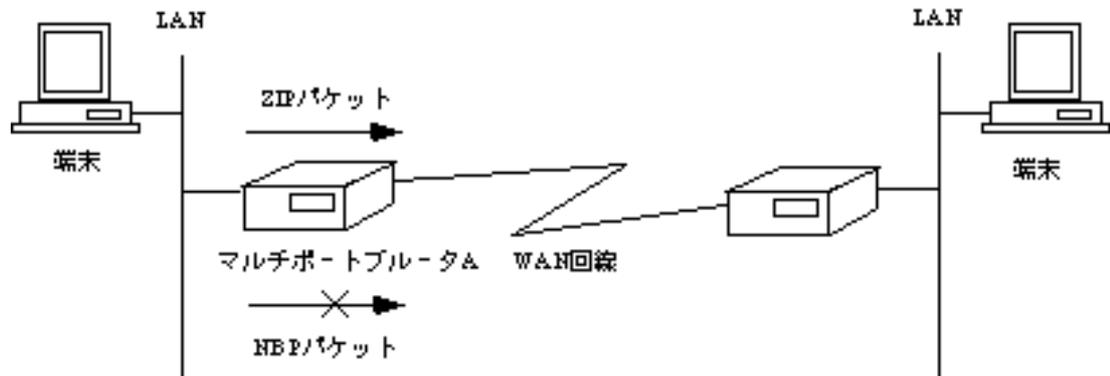


図2-14 プロトコル識別によるフィルタリング

(3) 送信可 / 受信可インタフェースによるフィルタリング

図2-15にAppleTalkルーティング時の送信可ポート、受信可ポートによるフィルタリングの使用例を示します。図2-15のマルチポートブルータAは受信可ポートをLAN、送信可ポートをWAN回線に設定してあります。この場合、図に示すようにLANからWAN回線への中継は行いますが、WAN回線からLANへの中継は行いません。

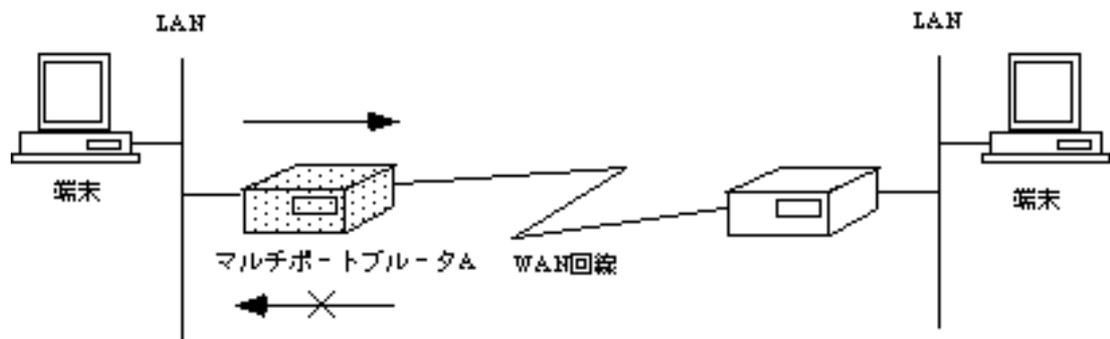


図2-15 送信可 / 受信可インタフェースによるフィルタリング

2.8.2 ゾーンフィルタリング

本装置では、ゾーンをフィルタリングする機能をサポートしています。図2-16にゾーンフィルタリングの使用例を示します。図2-16のマルチポートブルータAは、フィルタリングテーブルのゾーン名を「tokyo」、ポートを「WAN」に設定し、このテーブルに設定されたゾーンを他ポート側に見せるまたは見せないのどちらかを選択します。「見せる」を選択した場合、LAN側には「tokyo」のみが見えます。「見せない」を選択した場合、LAN側では「tokyo」を見ることができません。

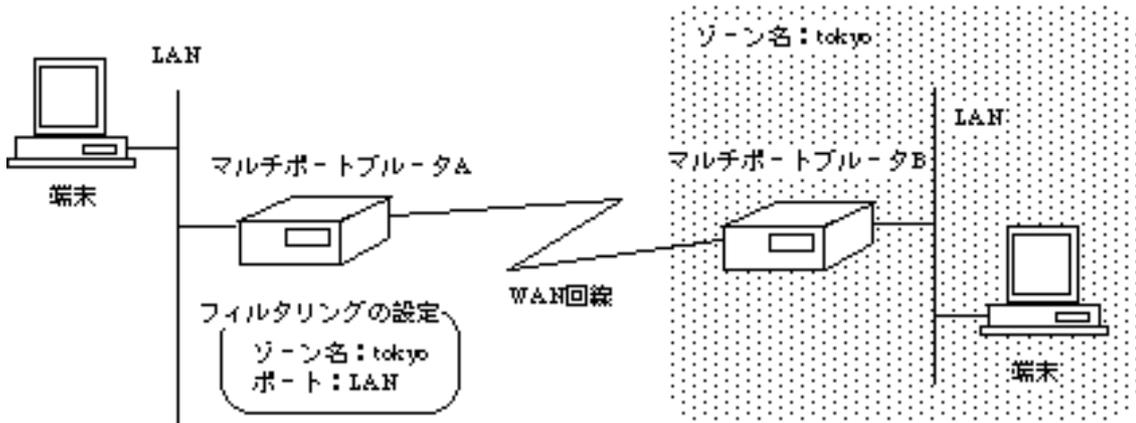


図2-16 ゾーンフィルタリング

2.8.3 サービスフィルタリング

本装置では、サービスをフィルタリングする機能をサポートしています。図2-17にサービスフィルタリング (forward) の使用例を示します。図2-17のマルチポートブルータAは、フィルタリングテーブルのノード名を「Printer1」、タイプを「LaserWriter」に設定しています。このテーブルで指定したサービスをどのポート側から受信するか、また、指定したサービスをどのポート側に送信するかを設定します。存在するポートを「WAN」、送信するポートを「LAN」とすればWAN側に存在する「Printer1」の情報のみがLANへ送信されます。

同様の設定をサービスのフィルタリング (discard) に設定すれば、「Printer1」の情報以外が送信されます。

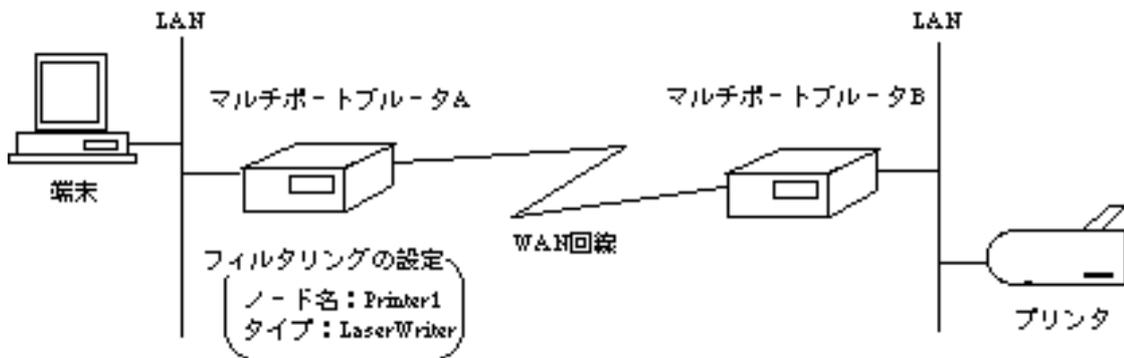


図2-17 サービスフィルタリング

2.9 ブリッジング機能

本装置は、IP、IPXおよびAppleTalk以外のプロトコルに対しては、ブリッジングする機能を持っています。設定によりIP、IPXおよびAppleTalkもブリッジングが可能です。

ブリッジング機能は以下の3通りがあります。

- STP(Spanning Tree Algorithm and Protocol)機能 (2.9.1)
- ブリッジングフレームのフィルタリング機能 (2.9.2)
- WAN回線複数使用時のWAN-WANブリッジング (2.9.3)

2.9.1 STP機能

STP機能は、マルチポートブリータでネットワークを構成した場合に、ネットワークの閉ループを発見し、内部的に閉ループを遮断する機能です。本装置はSTPに関連する各種の値を設定することにより、遮断する経路を決定することができます。図2-18にSTP機能の例を示します。

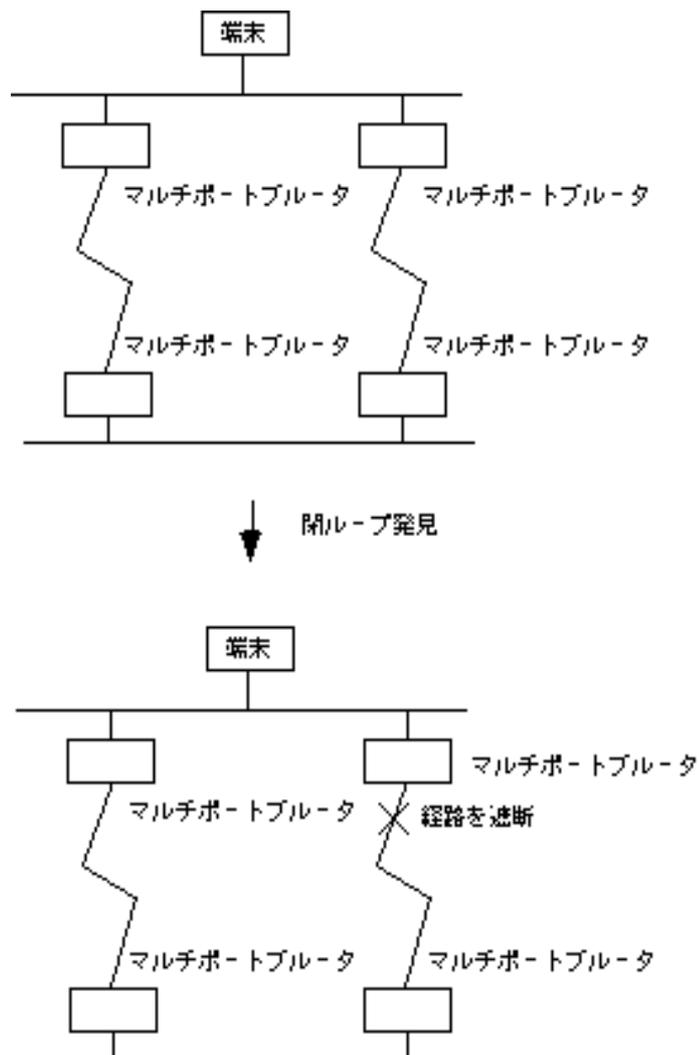


図2-18 STP機能

2.9.2 フィルタリング機能

本装置は、ブリッジングフレームによる無駄な回線の負荷を軽減するために、ブリッジングフレームに関してフィルタリング（中継／遮断）する機能をサポートしています。方法としては、以下の3種類があり、すべてを組み合わせ使用することができます。それぞれの方法を以下に示します。

- (1) アドレス学習によるフィルタリング
- (2) 送信元アドレス、宛先アドレスによるフィルタリング
- (3) プロトコル識別によるフィルタリング



注意：フィルタリングの対象となる中継方向を以下の表にまとめます。

表2-1 ブリッジングにおけるフィルタリングの中継方向

使用するWAN回線	ブリッジングでフィルタリングの対象となる中継方向	指定インタフェース
HSD	LAN WAN WAN LAN WAN WAN	受信インタフェース：LAN, HSD#1～HSD#8 （設定可） 送信インタフェース：LAN, HSD#1～HSD#8 （設定可）
ISDN	LAN WAN WAN LAN	受信インタフェース：LAN, ISDN#1～ISDN#8 （設定可） 送信インタフェース：LAN, ISDN#1～ISDN#8 （設定可）

(1) アドレス学習によるフィルタリング

図2-19にアドレス学習によるフィルタリング機能を示します。図2-20のマルチポートブリータAは、端末Aと端末Bが同じLAN上に存在することを端末Aと端末Bの通信より学習し、端末Aと端末B間の通信フレームはWAN回線に中継しません。本装置が学習できるアドレスは最大1024エントリです。

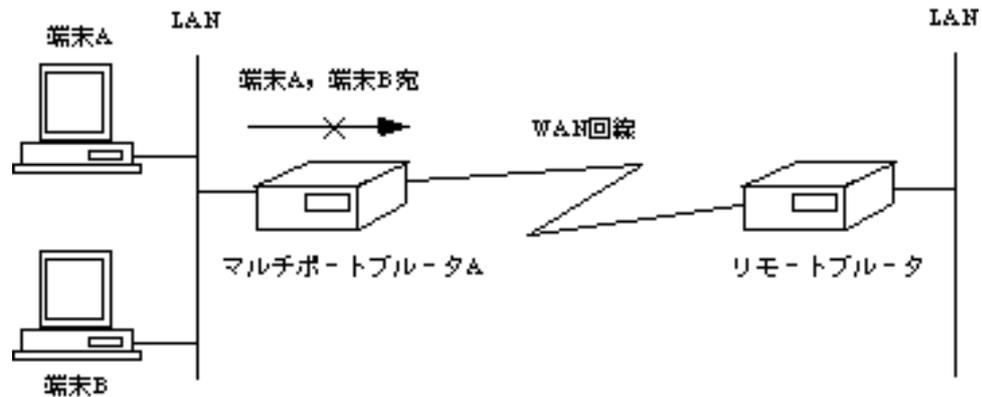


図2-19 アドレス学習によるフィルタリング



メモ：端末Aおよび端末Bのアドレスを学習していない場合は、マルチポートブリータは端末Aおよび端末B宛のフレームであってもWAN回線に中継します。

(2) 送信元アドレス、宛先アドレスによるフィルタリング

図2-20に送信元アドレス、宛先アドレスによるフィルタリングの使用例を示します。図2-20のマルチポートブリータAは、送信元アドレスによるフィルタリングを行い、送信元がXX:XX:XX:XX:XX:XXのフレームは中継し、YY:YY:YY:YY:YY:YYのフレームは遮断する設定を行っています。この場合、図に示すように端末AからのフレームはWAN回線に中継し、端末BからのフレームはWAN回線に中継しません。また、宛先アドレスによるフィルタリングも同時に行うことができます。宛先アドレスフィルタリングは、指定したアドレス宛のフレームの制御を行います。送信元、宛先アドレスは各々最大256エントリ登録することができます。

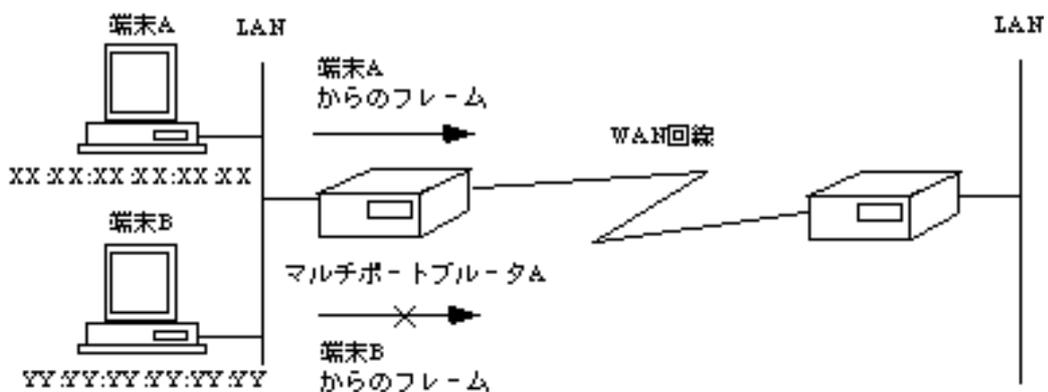


図2-20 送信元アドレス、宛先アドレスによるフィルタリング

(3) プロトコル識別によるフィルタリング

図2-21にプロトコル識別によるフィルタリングの使用例を示します。図2-21のマルチポートブルータAは、プロトコル識別によるフィルタリングを行います。マルチポートブルータAにはDECnetのフレームは中継し、OSIのフレームは遮断する設定を行っています。この場合、図に示すようにDECnetのフレームはWAN回線に中継し、OSIのフレームはWAN回線に中継しません。プロトコルは最大128エントリ登録することができます。（プロトコル番号「3.2.29 ワークシート「プロトコルフィルタリング編」」）

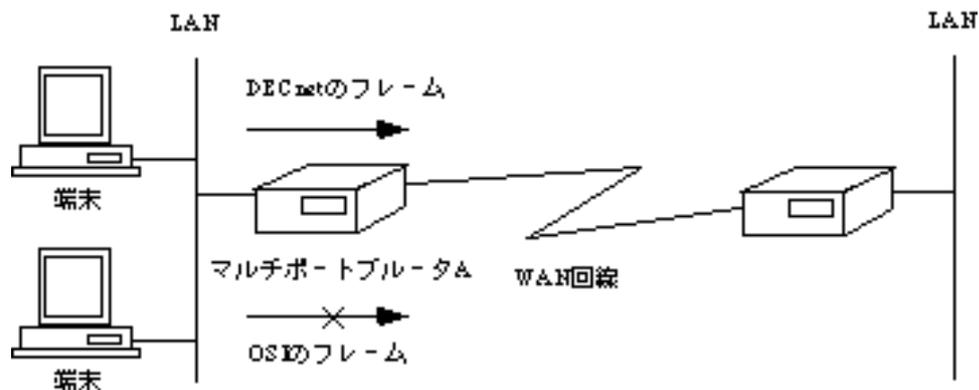


図2-21 プロトコル識別によるフィルタリング

2.9.3 WAN回線複数使用時のWAN-WANブリッジング機能

本装置は、WAN回線を複数使用する場合に、WAN回線より受信したブリッジングフレームをLANと他のWAN回線にブリッジングするWAN-WANブリッジング機能をサポートしています。図2-22にHSD2回線使用時のWAN-WANブリッジング機能の使用例を示します。この例は、マルチポートブルータAが、HSD#1回線より中継されてきた端末C宛のブリッジングフレームをHSD#2のみに中継しLANに中継しない様子を示します。

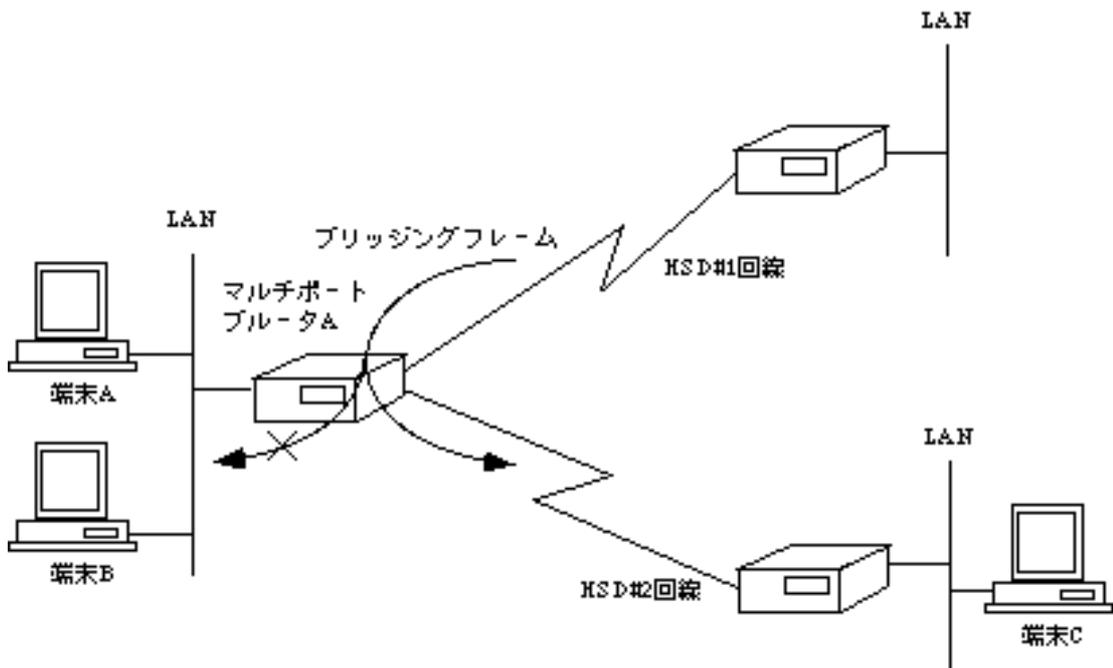


図2-22 HSD2回線使用時のWAN-WANブリッジング機能

2.10 ISDNに関する機能

本装置ではISDNを介して行うデータ通信において、以下に示す特徴を持っています。この節では、これらの特徴についてまとめます。

- 通常のデータ通信
- トラヒックの分散
- 様々な回線の接続 / 切断方法
- 最大80箇所の相手との通信
- チャンネルグループ化機能
- 様々なISDN使用料金の制御方法
- セキュリティ機能



メモ：ISDNは1つのインタフェースで2つのチャンネルを使用できる公衆回線網です。

2.10.1 通常のデータ通信

ISDN回線を介して遠隔地にあるISO8802-3のLANを接続することができます。本装置では、ISDNを利用して最大16箇所の相手と同時に通信を行うことができます。本取扱説明書では、通常のデータ通信を行う回線を「通常回線」と表現します。

2.10.2 トラヒックの分散

本装置では、1箇所の相手と通信を行う際に2つのチャンネルを利用し、データを分散して通信を行う（トラヒック分散機能）ことができます。本機能を利用すると、多量のデータ通信時に通信能力を高めることができます。本取扱説明書では、トラヒックの分散を行う回線を「トラヒック分散回線」と表現します。



メモ：トラヒック分散は、通常回線のデータリンクプロトコルがPPPである場合のみ行います。また、トラヒック分散はデータがIP,IPX,OSIプロトコルの場合に行います。

2.10.3 様々な回線の接続 / 切断方法

本装置のISDN接続 / 切断には様々な方法があります。接続 / 切断方法を適切に選択することにより、ISDNを効率よく運用することができます。

(1) 通常回線の接続 / 切断方法

ISDNを通常回線として使用する場合の接続 / 切断方法は、以下の3種類があります。

- 手動による接続 / 切断
- 指定時間内での中継データによる接続 / 切断
- 着信専用

- 手動による接続 / 切断

コンソールより接続コマンド（「5.2 通常回線の接続」）を入力する、またはSNMPマネージャから接続要求を行うことによりISDNを接続し、コンソールより切断コマンド（「5.3 通常回線の切断」）を入力する、またはSNMPマネージャから切断要求を行うことによりISDNを切断します。（SNMPマネージャ「2.11 ネットワーク管理機能」）図2-23に接続例を示します。

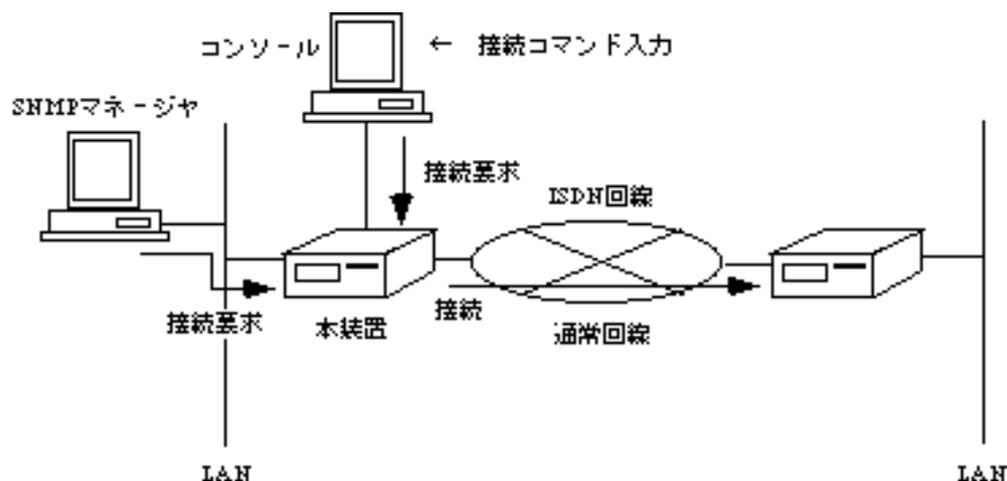


図2-23 手動による接続例

- 指定時間内での中継データによる接続 / 切断

指定した時間内にLANからISDNに中継すべきデータが発生した場合、接続すべき相手を選択してその相手に接続します。また、一定期間中継すべきデータが存在しなかった場合、または切断時刻になった場合はISDNを切断します。図2-24に接続例を示します。

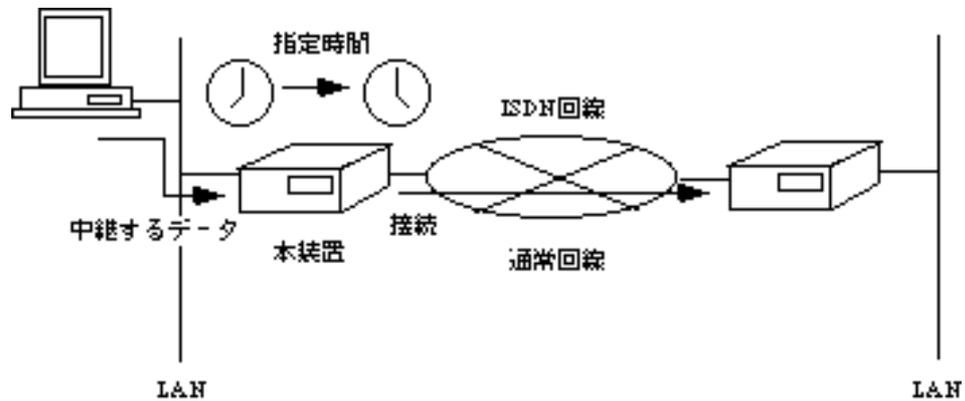


図2-24 指定時間内の中継データによる接続例

- 着信専用

相手からのISDN接続要求があったときのみ接続します。

(2) トラヒック分散回線の接続 / 切断方法

ISDNをトラヒック分散回線として使用する場合の接続 / 切断方法は、以下の4種類があります。

- 手動による接続 / 切断
- 指定時間内でのデータ量による接続 / 切断
- 手動による接続 / 切断

コンソールより接続コマンド（ 「5.4 トラヒック分散回線の接続」 ）を入力する、またはSNMPマネージャから接続要求を行ったときISDNを接続し、コンソールより切断コマンド（ 「5.5 トラヒック分散回線の切断」 ）を入力する、またはSNMPマネージャから切断要求を行ったとき、ISDNを切断します。（SNMPマネージャ 「2.9 ネットワーク管理機能」 ） 図2-25に接続例を示します。

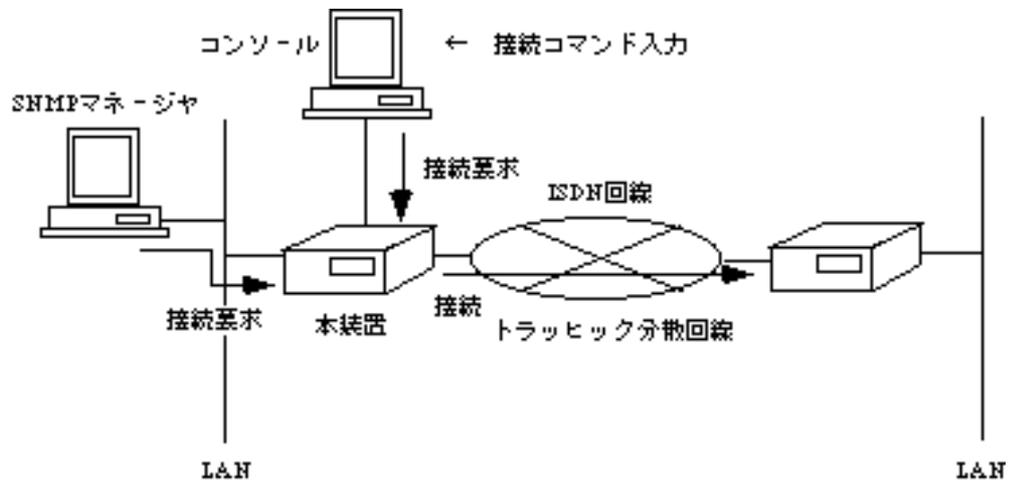


図2-25 手動接続例



メモ：輻輳とは回線の負荷が高くなり、データの中継できない状態を意味します。

- 指定時間内でのデータ量による接続 / 切断

指定した時間内に通常回線に輻輳が発生した場合、トラヒック分散回線を接続します。また、輻輳が終了し一定期間輻輳が発生しなかった場合、または切断時刻になった場合はISDN回線を切断します。図2-26に接続例を示します。

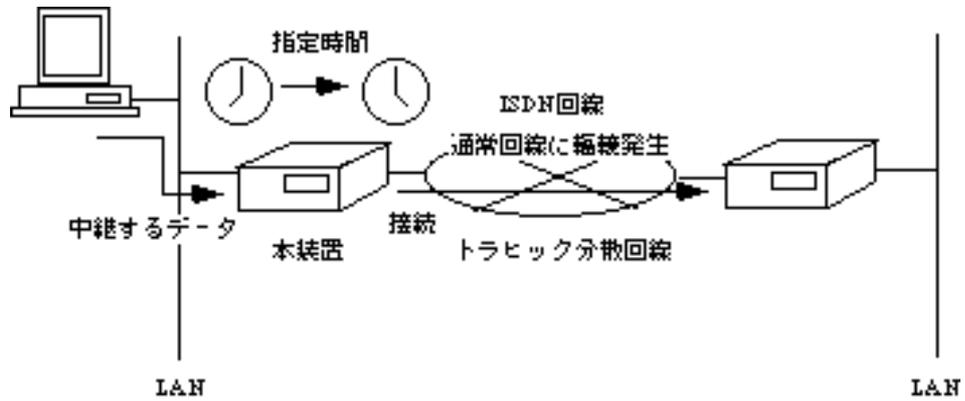


図2-26 指定時間内でのデータ量による接続例

2.10.4 最大80箇所の相手との通信

本装置はISDNを介して最大80箇所のLANと接続することができます。中継データによる接続を行う際は、本装置が中継データを解析して、接続すべき相手に接続を行います。

以下にIPパケット、IPXパケット、AppleTalkパケットおよびブリッジングフレームによる自動接続例を示します。

(1) IPパケットによる複数相手自動接続

図2-27に複数相手に対するIPパケットによる自動接続例を示します。マルチポートルータAは、表2-2に示すテーブルを保持しています。マルチポートルータAは中継すべきデータの宛先アドレス(192.168.3.1)をみて、保持しているテーブルからデータを中継するために接続するルータおよびそのルータのISDN番号を検索し、自動的にISDNを接続しデータを中継します。

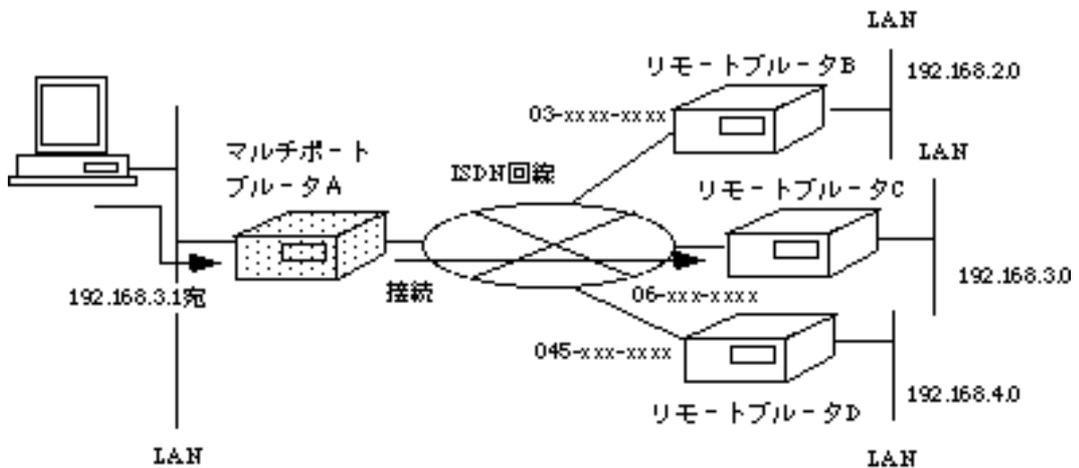


図2-27 IPパケットによる自動接続

表2-2 マルチポートルータAの内部テーブル

宛先ネットワーク番号	中継するルータ	接続する相手のISDN番号
192.168.2.0	リモートルータB	03-xxxx-xxxx
192.168.3.0	リモートルータC	06-xxx-xxxx
192.168.4.0	リモートルータD	045-xxx-xxxx

(2) IPXパケットによる複数相手自動接続

図2-28に複数相手に対するIPXパケットによる自動接続例を示します。マルチポートルータAは、表2-3に示すテーブルを保持しています。マルチポートルータAは、クライアントからサーバD（インターナルネットワーク番号が300）宛のパケットの宛先ネットワーク番号をみて、保持しているテーブルからデータを中継するために接続するルータおよびそのルータのISDN番号を検索し、自動的にISDNを接続しデータの中継します。

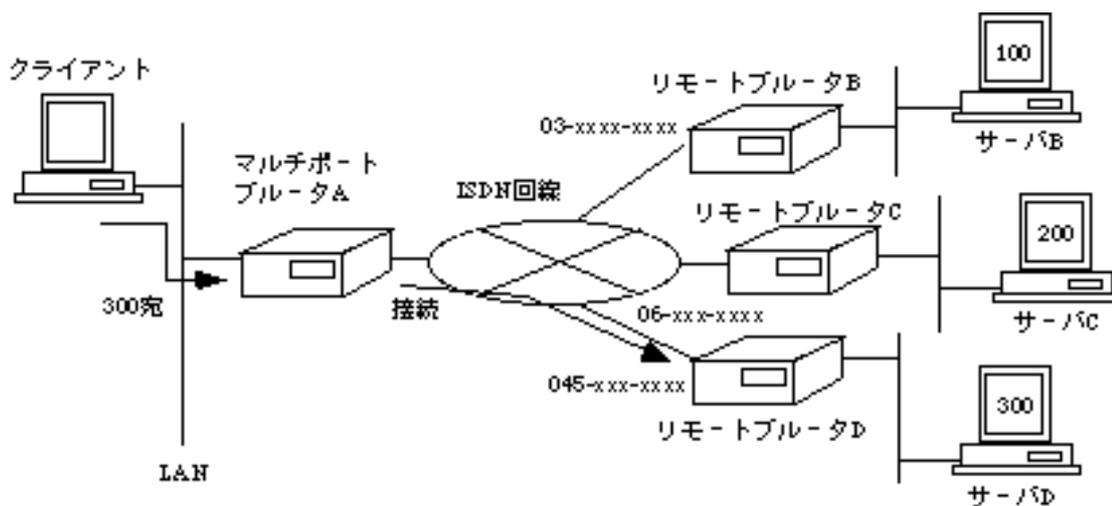


図2-28 IPXパケットによる自動接続

表2-3 マルチポートルータAの内部テーブル

宛先ネットワーク番号	中継するルータ	接続する相手のISDN番号
100 (サーバB)	リモートルータB	03-xxxx-xxxx
200 (サーバC)	リモートルータC	06-xxx-xxxx
300 (サーバD)	リモートルータD	045-xxx-xxxx

(3) AppleTalk packetsによる複数相手自動接続

図2-29に複数相手に対するAppleTalk packetsによる自動接続例を示します。マルチポートブロータAは、表2-4に示すテーブルを保持しています。マルチポートブロータAは、MacintoshAからMacintoshB（ネットワーク番号が450.5）宛の packetsの宛先ネットワーク番号を見て、保持しているテーブルからデータを中継するために接続するルータおよびルータのISDN番号を検索し、自動的にISDNを接続しデータを中継します。

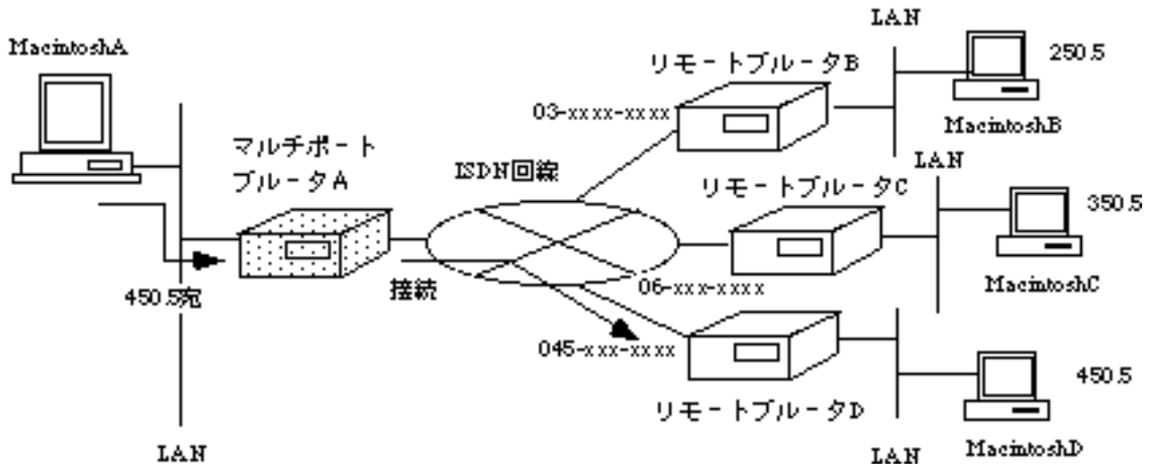


図2-29 AppleTalk packetsによる自動接続

表2-4 マルチポートブロータAの内部テーブル

宛先ネットワーク番号	中継するルータ	接続する相手のISDN番号
201 ~ 300	リモートブロータB	03-xxxx-xxxx
301 ~ 400	リモートブロータC	06-xxx-xxxx
401 ~ 500	リモートブロータD	045-xxx-xxxx

(4) ブリッジングフレームによる複数相手自動接続

図2-30に複数相手に対するブリッジングフレームによる自動接続例を示します。マルチポートブロータAは、表2-5に示すテーブルを保持しています。マルチポートブロータAは、ブリッジングフレームの宛先MACアドレス (XX:XX:XX:XX:XX:XX) をみて、保持しているテーブルからデータの中継のために接続するルータおよびそのルータのISDN番号を検索し、自動的にISDNを接続しデータの中継します。

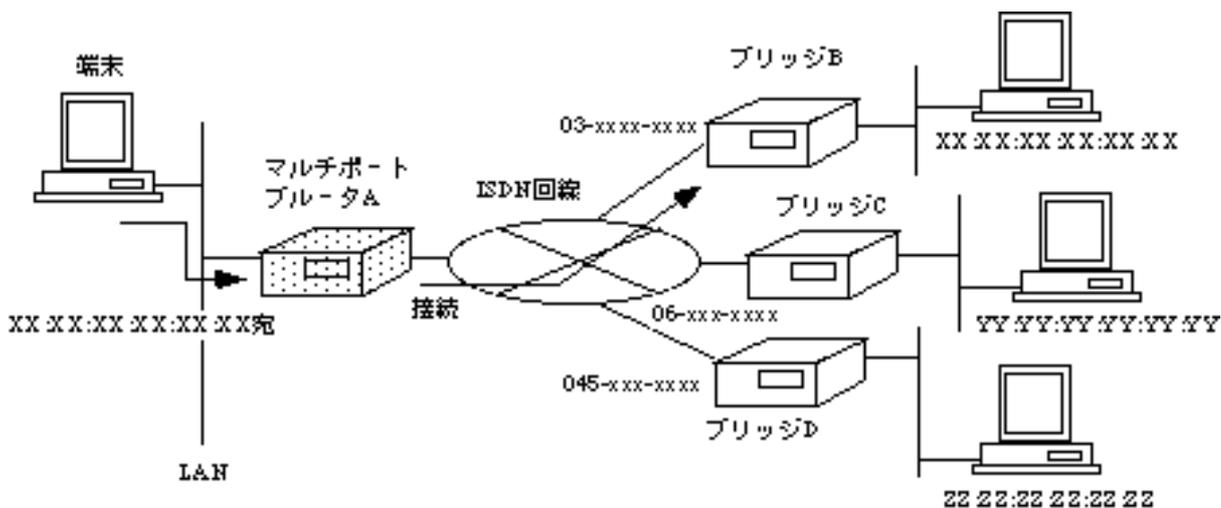


図2-30 ブリッジングフレームによる自動接続

表2-5 マルチポートブロータAの内部テーブル

宛先アドレス	接続する相手のISDN番号
XX:XX:XX:XX:XX:XX	03-xxxx-xxxx
YY:YY:YY:YY:YY:YY	06-xxx-xxxx
ZZ:ZZ:ZZ:ZZ:ZZ:ZZ	045-xxx-xxxx

2.10.5 チャンネルグループ機能

本装置では、NTTの無料のサービスである「代表取扱サービス」に対応するための、「チャンネルグループ機能」をサポートしています。



メモ：「代表取扱サービス」とは、複数のインタフェースグループで代表群を決め、あらかじめ決めた代表番号に着信があった場合、代表群から空いている回線を選んで着信するサービスです。最大20回線まで代表を組むことができ、代表選択の方法として、順次サーチ方式とラウンドロビン方式の2方式あります。本装置ではどちらの方式でも使用することができます。

本装置のチャンネルグループ機能を利用する場合は、「代表取扱サービス」で契約した複数のインタフェースを1つのグループとし、そのグループに代表番号を割り当てます。

図2-31に、チャンネルグループ機能の利用例を示します。

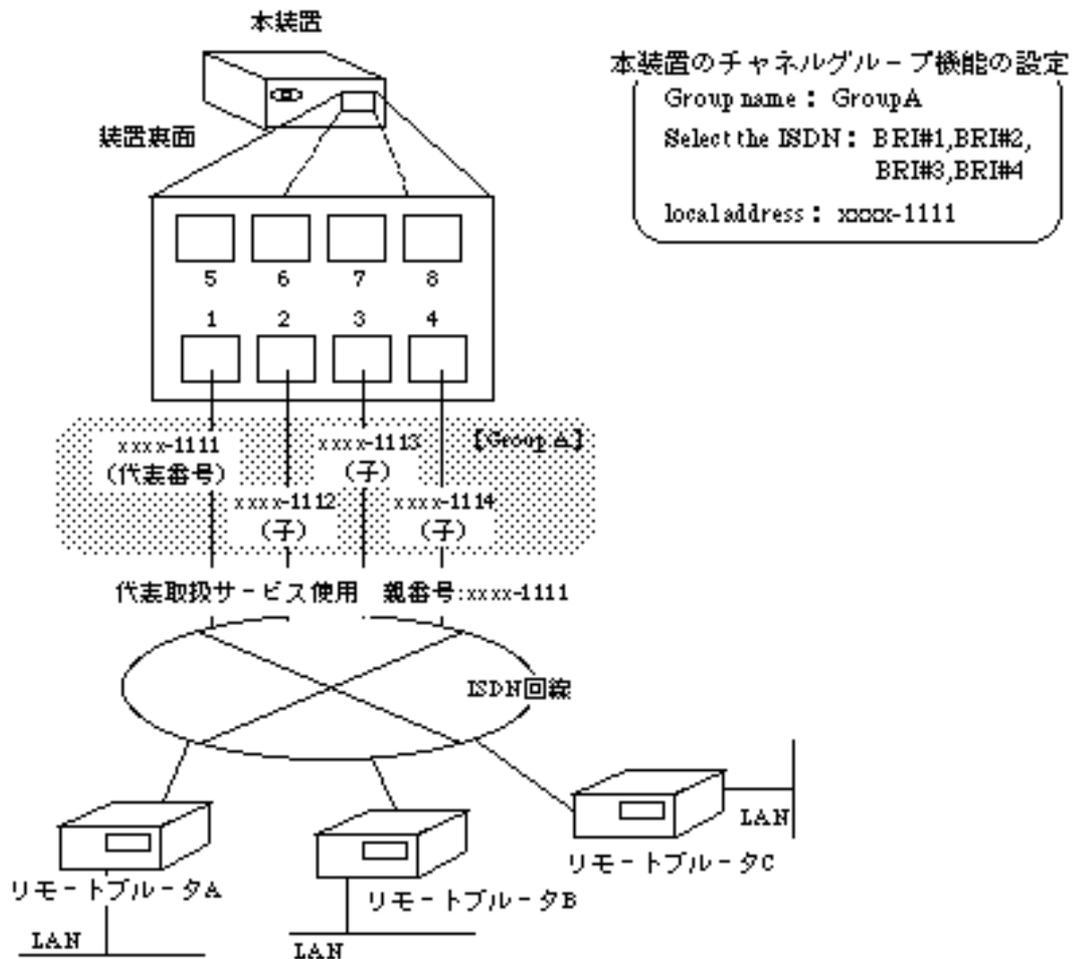


図2-31 チャンネルグループ機能の利用例

図2-31において、本装置は4つのインタフェースすなわち、BRI#1～BRI#4を一つのグループとし、代表番号をxxxx-1111と設定しています。

リモートブロータAが宛先ISDN番号xxxx-1111で発呼し、xxxx-1111が使用されていなければ、xxxx-1111と接続します。次に、リモートブロータBが宛先ISDN番号xxxx-1111で発呼すると、xxxx-1111は使用中なので、xxxx-1112にすべり接続します。

このように、接続相手にはあたかも1つのインタフェースであるかのように見せ、グループである4本の回線を、同時に接続することができます。



注意：xxxx-1112からxxxx-1114までの子番号宛に発呼することはできません。

また、本装置側から発呼する場合は、自動接続の場合、ISDN番号xxxx-1111から発呼し、もしxxxx-1111が使用されているかまたは回線の障害が発生している等の場合は、xxxx-1112にすべり発呼します。手動接続の場合は、ポートを選択して発呼することができます。

2.10.6 様々なISDN接続時間の制御方法

ISDNは、使用料金が接続時間に依存した公衆回線網です。したがって通常回線の接続/切断方法を中継データによる接続/切断にした場合、通常データ以外のデータ（ルーティング制御パケット等）を通信する場合にも、ISDNの使用料金がかかってしまいます。

本装置では以下に示す方法で、ISDN使用料金を節約することができます。

- (1) RIP(IP), RIP(IPX), SAP(IPX)の制御
- (2) KeepAliveの代理応答/要求

- (1) RIP(IP), RIP(IPX), SAP(IPX)の制御

通常RIP(IP)は毎30秒、RIP(IPX), SAP(IPX)は毎60秒に1回定期的に情報を送信し、ルーティングテーブルの更新を行っています。しかし、これらのルーティング制御パケットによりISDNが接続されISDN使用料金が加算されてしまいます。

本装置では、ルーティング制御パケットを定期送信する/しないの設定をすることができます。ルーティング制御パケットを送信しない場合、ISDNの接続を行わず、ルーティング制御パケットによりISDN使用料金が定期的に加算されることはありません。

- (2) IPXのKeepAliveの代理応答/要求

NetWareでは、サーバがクライアントにKeepAliveの要求を送信し、クライアントがサーバにKeepAliveの応答を送信することによりサーバがクライアントの存在を確認します。しかし、サーバとクライアントがISDNを介して接続している場合、KeepAliveパケットによりISDNが接続されISDN使用料金が加算されてしまいます。

本装置では、KeepAliveパケットに対して代理に応答/要求する機能をサポートしています。この機能によりISDN使用料金を節約することができます。図2-32にKeepAliveの代理応答/要求例を示します。マルチポートブロータAは、サーバからクライアントへのKeepAliveの要求に対してクライアントの代わりに応答し、マルチポートブロータBは、サーバの代わりにKeepAliveの要求をクライアントに送信します。この機能により、ISDNを接続せずにNetWareのKeepAlive機能を使用することができます。

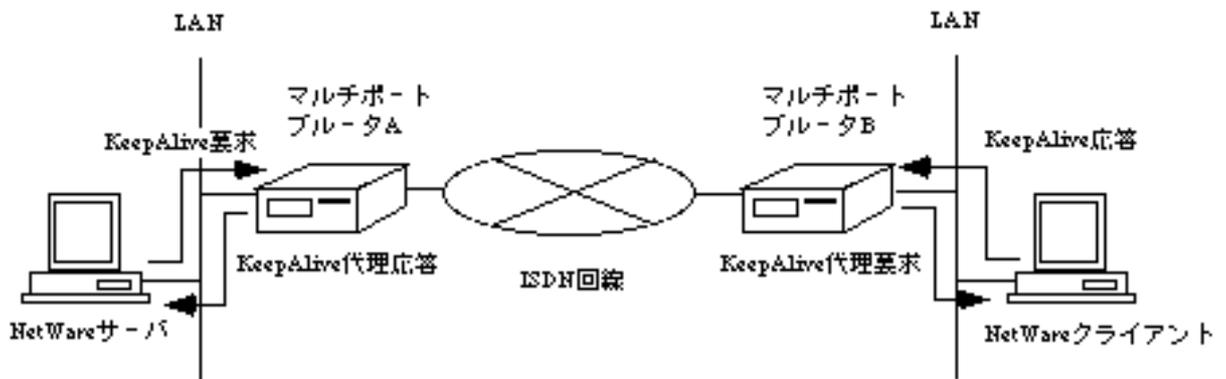


図2-32 KeepAliveの代理応答 / 要求例

2.10.7 セキュリティ機能

本装置では、ISDN回線が不本意な相手と接続されネットワークに進入されてしまうのを防ぐために、次の2つの方法をセキュリティ機能としてサポートしています。

- 着信時の相手ISDN番号の確認
- CHAP機能

(1) 着信時の相手ISDN番号確認

本装置では、ISDN回線を介して相手と接続する場合、接続相手の名前（リモートターゲット）とアドレスを登録します。

網からは、ISDNの発信者番号通知サービスにより、着信時に相手ISDN番号、サブアドレスが送信されるので、着信の際にその内容を確認し、登録していない相手からの着信は拒否することができます。（ 3.2.5 ワークシート「ISDNリモートターゲット編」）

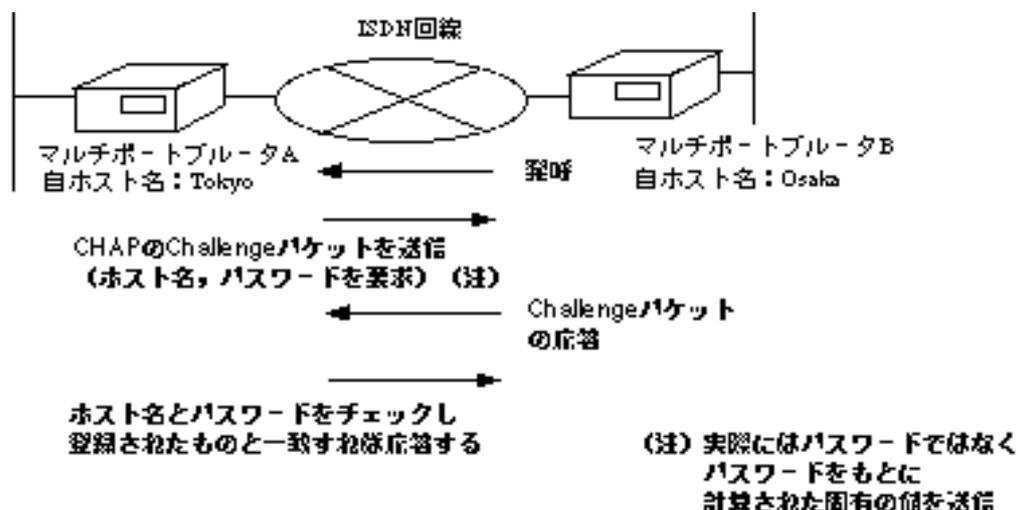
(2) CHAP機能

本装置は、接続相手を認証するCHAP機能（Challenge-Handshake Authentication Protocol）をサポートしています。

CHAP機能により「(1) 着信時の相手ISDN番号確認」の機能をサポートしていない他社装置と接続する場合でも、接続相手がCHAP機能をサポートしていれば認証することができます。

本装置のCHAP機能では、接続相手が登録された相手と異なる場合、リンクを切断します。

以下にCHAP機能を使用する場合の設定方法とその設定例を示します。



マルチポートブルータMの設定

設定項目	設定内容	参照項
自ホスト名	Tokyo	3.2.1
着信時の相手ISDN番号を 確認する/しない	する	3.2.4
リモートターゲット	Osaka	3.2.5
リモートターゲットに 対するパスワード	furukawa	3.2.5

マルチポートブルータBの設定

設定項目	設定内容	参照項
自ホスト名	Osaka	3.2.1
着信時の相手ISDN番号を 確認する/しない	する	3.2.4
リモートターゲット	Tokyo	3.2.5
リモートターゲットに 対するパスワード	furukawa	3.2.5

図2-33 CHAP機能を使用する場合の設定方法



メモ：CHAP機能に関しては、以下のドキュメントを参考にしています。

- PPP Authentication Protocol : RFC1334
- The Point-to-Point Protocol(PPP) : RFC1331
- MD5 Message-Digest Algorithm : RFC1321

2.10.8 呼確立リミッタ

本装置では、ISDN回線を使用する場合、運用、設定などのミスからISDNが長時間接続されたままになり、思わぬ課金が発生するのを防ぐための、呼確立リミッタを備えています。（「4.12 呼確立リミッタの設定」）

呼確立リミッタは、ISDNの接続時間の累計の方法により、次の2種類があります。

- 本装置がISDNを連続して接続した時間を基にする
（連続接続時間呼確立リミッタ）
- 接続相手毎に1ヶ月の接続累計時間を基にする
（トータル接続時間呼確立リミッタ）

(1) 連続接続時間呼確立リミッタ

本機能では、ISDNが接続され続けその時間が指定時間に達したとき、LEDが点灯し（「1.6 フロントパネルのLED表示」）、自動的に装置を停止し、ISDNを切断します。連続接続時間呼確立リミッタによりISDNが切断されたら、システムに異常が発生しています。その後、装置を正しく運用することはできなくなります。

長時間連続でISDN回線を使用する場合は、この機能をOFFとしておくか、設定時間を長く設定する必要があります。

接続時間は、呼をどちらから確立したか（自分が発呼したか着呼したか）やISDNの使用目的（通常回線、トラヒック分散）、また接続契機（手動による発呼や自動発呼など）に関係なく接続している時間を累計します。



注意：連続接続時間呼確立リミッタによりISDNが切断されたら、システムに異常が発生しています。本装置の設定をはじめ、周辺機器の運用を再度確認し、代理店もしくは弊社技術サポートまでご連絡ください。

(2) トータル接続時間呼確立リミッタ

本機能では、1ヶ月毎のISDN回線の接続時間（呼確立時間）の累計が指定した時間に達した場合に「作動」します。また、呼確立時間の累計がトータル接続時間呼確立リミッタが作動する指定の時間の90パーセントに達したときは「警告」が出されます。

【作動】

- 100パーセントを超えた時刻と接続相手の情報が「インフォメーション」の「elog」に記録されます。
- 装置前面のCHECK LEDが点滅します。
- 接続していた回線は切断されます。それ以降、その相手に対する着呼/発呼は行いません。

【警告】

- 90パーセントを超えた時刻と接続相手の情報が「インフォメーション」の「elog」に記録されます。
- 装置前面のCHECK LEDが点滅します。

呼確立時間は、呼をどちらから確立したか（自分が発呼したか着呼したか）やISDNの使用目的（通常回線，トラヒック分散），また接続契機（手動による発呼や自動発呼など）に関係なく，接続している時間を相手毎に累計します。

また，呼確立時間の累計はコマンド以外にも，装置電源投入時，装置リセット時および毎月1日にリセットされます。



注意：どちらか一方が先にリミッタが作動したときにISDNの呼は解放され，もう一方のルータでは「リミッタ作動直前」で止まってしまう。この状態で，リミッタが作動した方のルータを回復させてISDNを接続した途端，今度はもう一方のルータのリミッタが作動してしまいます。このような現象を防ぐためにも，呼確立リミッタの動作は，自装置を「on」にした場合相手装置は「off」にすることをおすすめします。



注意：トータル接続時間呼確立リミッタが「警告」を表す状態になっていたら，システムに異常が発生しています。本装置の設定をはじめ，周辺機器の運用を再度確認してください。トータル接続時間呼確立リミッタが「作動」するとリミッタをリセットしなければISDN回線を接続することはできません。

2.11 ネットワーク管理機能

本装置は，ネットワーク管理機能としてSNMP(Simple Network Management Protocol)のエージェント機能をサポートしています。本機能を利用することにより，遠隔地のSNMPマネージャによってISDNの接続/切断等，本装置の管理をすることができます。本装置は，最大8種類のマネージャを登録できます。

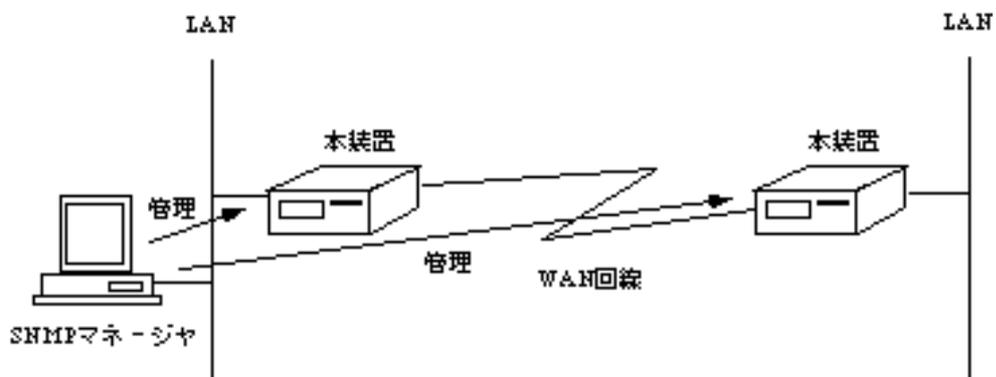


図2-34 SNMPエージェント機能

2.12 TELNETサーバ機能

本装置は、TELNETサーバ機能をサポートしています。遠隔のTELNETクライアントからネットワークを経由して本装置にログインし、システム編集および運用操作等、ローカルコンソールと同等の操作を行うことができます。ログインした後は、ローカルコンソールと同じ方法で操作します。

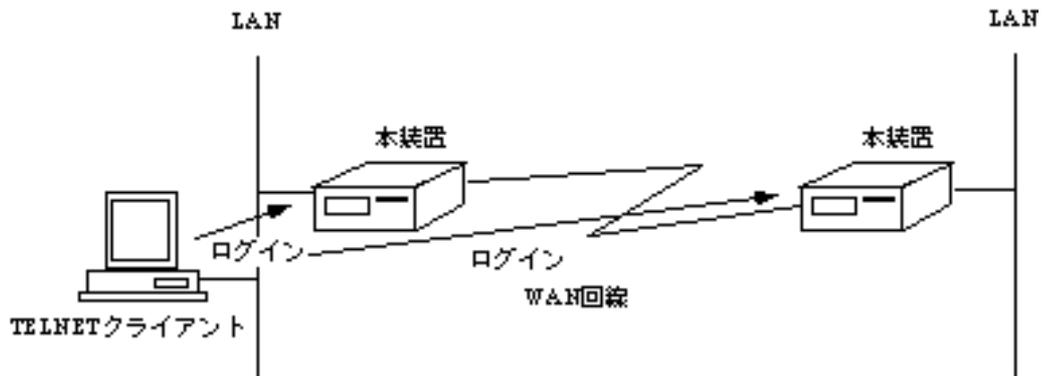


図2-35 TELNETサーバ機能

2.13 リモートコンソール機能

本装置は、ローカルコンソールにより遠隔地にある装置を操作できるリモートコンソール機能をサポートしています。本装置のコンソールを遠隔の装置のコンソールとして使用し、遠隔の装置のシステム編集および運用操作等、ローカルコンソールと同等の操作を行うことができます。リモートコンソール機能は、ローカルコンソールと同じ方法で操作します。

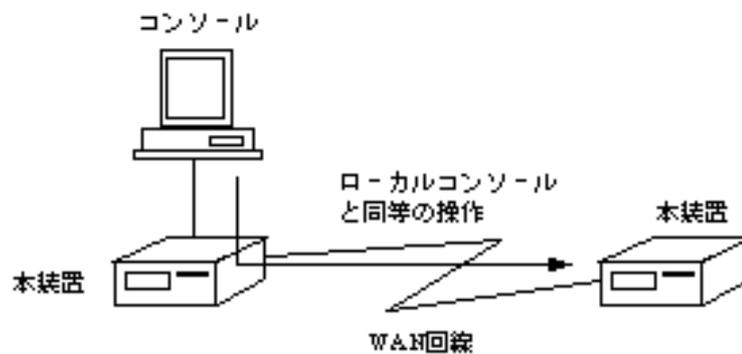


図2-36 リモートコンソール機能

2.14 簡易コマンド機能

本装置は、コンソールからメニューを選択して装置の操作を行う通常の方法の他に、コマンドを入力して直接操作を行う簡易コマンド機能をサポートしています。本機能を利用することにより、頻繁に使用する操作や参照する情報の取得を毎回メニューを選択しながら操作をすることなく行うことができます。簡易コマンド機能により実行できるコマンド名、実行内容、参照項を付録Dに記述します。

2.15 データ圧縮機能

本装置は、PPP上のデータを圧縮/復元する機能を持っています。LCPがPPPに関する基本的なネゴシエーションを行った後、CCPによってデータ圧縮のアルゴリズムのネゴシエーションを行います。データ圧縮のアルゴリズムには、Stacker LZSを使用します。

圧縮の対象となるデータ種別の一部を以下の表に示します。データ圧縮の対象とならないのは、個々のネットワーク制御プロトコル、圧縮制御プロトコルおよびLCPです。

表2-6 圧縮の対象となるデータ種別

データ種別	PPPプロトコル番号(16進数)
ブリッジングデータ	0031
IP	0021
IPX	002b



注意：データサイズが180バイト未満の時、データ圧縮は行われません。また、圧縮後のデータサイズが圧縮前のデータサイズより大きいまたは等しい場合、圧縮前のデータが送信されます。

2.16 データ別優先制御機能

本装置は、指定したデータをLANからWANに優先的にまたは非優先的に中継する機能を持っています。（データ別優先制御機能）

データの指定は以下の種類で行うことができます。

- プロトコル種別
- プロトコルアドレス
- アプリケーション
- MACアドレス

これにより、次のような問題を解決することができます。

- 遅延に弱いプロトコル（FNAなど）が、他のプロトコルのトラヒックによってタイムアウトしコネクションが切断される。
- 対話型処理のアプリケーションを利用した場合（telnetなど）に、一時的に大量のトラヒックが発生すると、対話型処理のアプリケーションの使い勝手が悪くなる。
- IPXルーティングを行うとき、NetWareのサーバへログインする時間が異常に長くなる。

2.17 ルータグループ化機能

本装置では、複数の本装置をグループ化し論理的に1台のルータとすることにより（グループルータ）、そのルータを1つの代表電話グループに接続し、空き回線を利用して通信を行うことができます。

本機能を使用することにより、NTTのサービスである「代表取扱いサービス」（2.10.5チャンネルグループ機能）の提供回線数の最大20回線を有効に利用することができます。



メモ：利用できる通信は、IPルーティングのみです。

グループ化された個々のルータは、互いにグループルータとして動作するルータを検出することにより、グループルータであることを認識します。

個々のルータには、回線を接続する優先度やグループルータ内の他のルータが回線を接続しているかどうかを確認するパケットの応答待ちタイム時間などを設定します。グループルータには、代表IPアドレスを設定します。

これにより、エンドユーザがルータが複数あることを意識することなく、複数の経路から最適経路を選択して通信を行うことができます。

図2-37にルータグループ化機能を利用している例を示します。

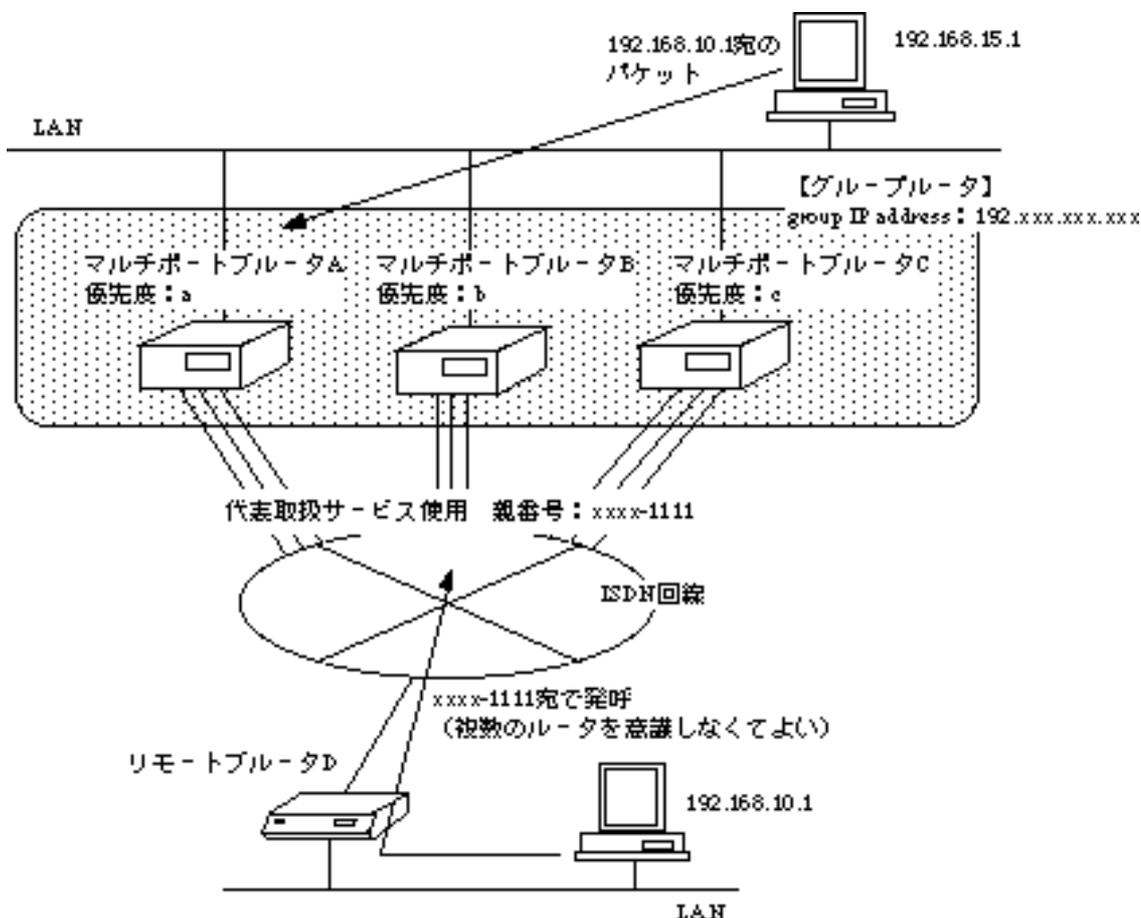


図2-37 ルータグループ化機能

図2-37において、ノード192.168.15.1が、ノード192.168.10.1宛の packetsを送信するとき、まず、優先度の高いマルチポートルータA宛に packetsを送信します。

マルチポートルータA～Cはグループルータであり、それぞれのチャネルは代表取扱サービス（2.10.5 チャネルグループ機能）を利用しています。マルチポートルータAはノード192.168.10.1宛の packetsを受信すると、

- 自身がリモートルータDと接続していれば、 packetsを中継します。
- 自身はリモートルータDと接続していなければ、グループルータ内の他のルータが接続していないか確認し、接続していればそのルータが packetsを中継します。
- グループルータ内のどのルータも、リモートルータDと接続していなければ、優先度の高いルータが回線を接続します。

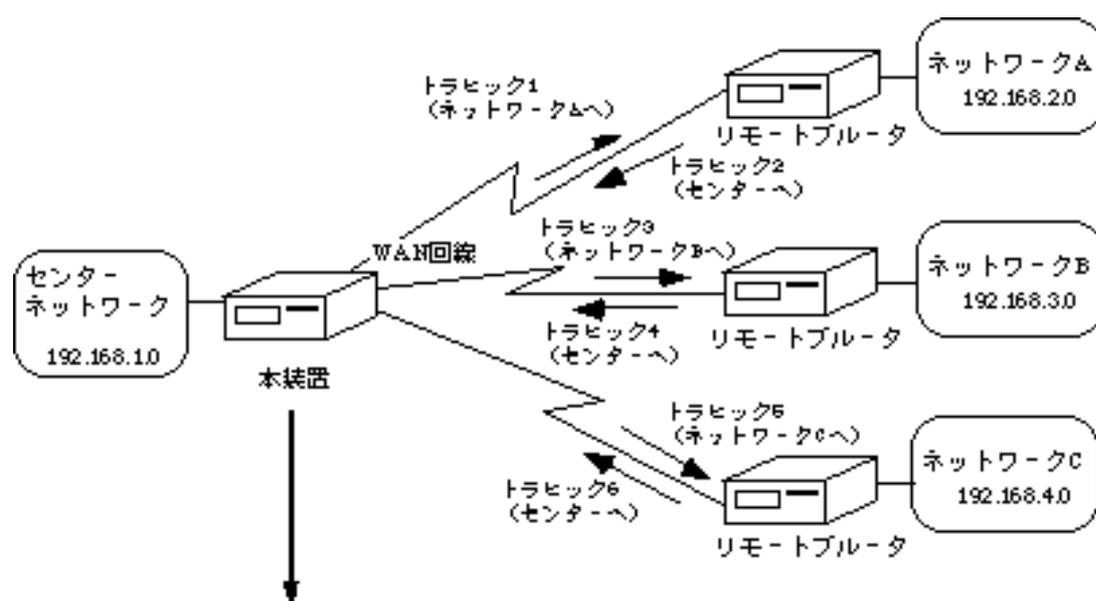
このような手順で、最適な経路を選択して、通信を行います。

2.18 トラフィックロギング機能

本装置では、IPルーティングにおけるIPパケットのトラフィック量のロギング機能を持っています。

これにより、特定の回線を使用するユーザ間でのトラフィック量を把握することができ、通信費、設備費の課金の分担等に利用できます。

図2-38にトラフィックロギング機能を使用している例を示します。



トラフィックロギングの設定例

トラフィック1
(センターネットワーク→ネットワークA間)

source data type	IP address
source IP address	192.168.1.0
source mask	255.255.255.0
destination data type	IP address
destination address	192.168.2.0
destination mask	255.255.255.0

トラフィック2
(ネットワークA→センターネットワーク間)

source data type	IP address
source IP address	192.168.2.0
source mask	255.255.255.255
destination data type	IP address
destination address	192.168.1.0
destination mask	255.255.255.255

トラフィック3
(センターネットワーク→ネットワークB間)

source data type	IP address
source IP address	192.168.1.0
source mask	255.255.255.0
destination data type	IP address
destination address	192.168.3.0
destination mask	255.255.255.0

トラフィック4
(ネットワークB→センターネットワーク間)

source data type	IP address
source IP address	192.168.3.0
source mask	255.255.255.0
destination data type	IP address
destination address	192.168.1.0
destination mask	255.255.255.0

トラフィック5
(センターネットワーク→ネットワークC間)

source data type	IP address
source IP address	192.168.1.0
source mask	255.255.255.0
destination data type	IP address
destination address	192.168.4.0
destination mask	255.255.255.0

トラフィック6
(ネットワークC→センターネットワーク間)

source data type	IP address
source IP address	192.168.4.0
source mask	255.255.255.0
destination data type	IP address
destination address	192.168.1.0
destination mask	255.255.255.0

図2-38 トラフィックロギング機能設定例

3章 基本設定

この章では、装置の基本設定について説明します。基本設定とは、装置の導入時やシステムの変更時に必ず設定する項目を指します。

この章の内容を以下にまとめます。

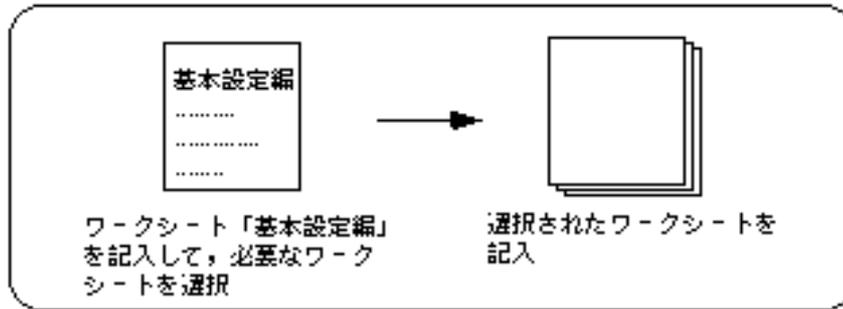
- 基本設定の流れ
- ワークシートの作成
- コンソールの接続
- メインメニュー
- 管理者資格(スーパーモード)への移行
- 一般資格への復帰
- 設定情報の表示
- コンソールからの設定

3.1 基本設定の流れ

基本設定の流れについて説明します。基本設定は、本取扱説明書に添付してあるワークシートを利用して行います。まずワークシートにあらかじめ必要な項目を記入します。その後、記入されたワークシートを見ながらコンソールより実際の装置に入力します。

基本設定の流れを図3-1にまとめます。

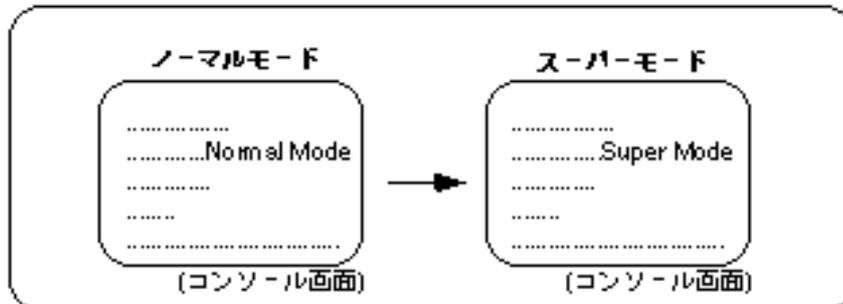
1.まずワークシートを作成します。(→「3.2 ワークシートの作成」)



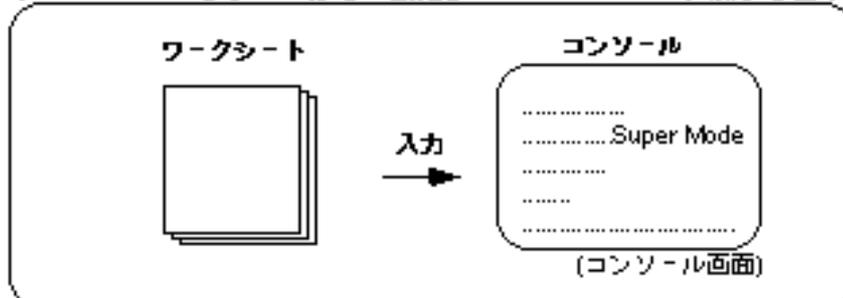
2次にコンソールを接続します。(→「3.3 コンソールの接続」)



3.コンソール上で管理者資格(スーパーモード)へ移行します。
(→「3.5 管理者資格(スーパーモード)への移行」)



4.各設定項目をワークシートを見ながらコンソールより装置に入力します。
(→「3.8 コンソールからの設定」～「3.19 SNMPに関する基本設定」)



5 設定を有効にするために、装置の再起上げを行います。
(→「3.21 設定内容の適用」)

図3-1 基本設定の流れ

3.2 ワークシートの作成

ワークシートの作成は次の手順で行います。

- (1) ワークシート「基本設定編」で、必要なワークシートを選択します。
- (2) (1)で選択された各ワークシートを記入します。

各ワークシートの簡単な説明を以下に示します。（記入方法 3.2.1以降）

【必要なワークシートを選択するためのワークシート】

必要なワークシートを
選択

基本設定編
.....
.....
.....

【装置で使用する回線と、回線に伴うワークシート】

・HSD

WAN回線にHSDを使用
する場合

HSD編
.....
.....
.....

・ISDN

WAN回線にISDNを使用
する場合

ISDN チャネル グループ編
.....

ISDN 運用形態編
.....
.....

ISDN リモート ターゲット編
.....
.....

ISDN 通常回線編
.....

図3-2 (1) ワークシートの構成 (1)

【装置で使用する機能と、機能に伴うワークシート】

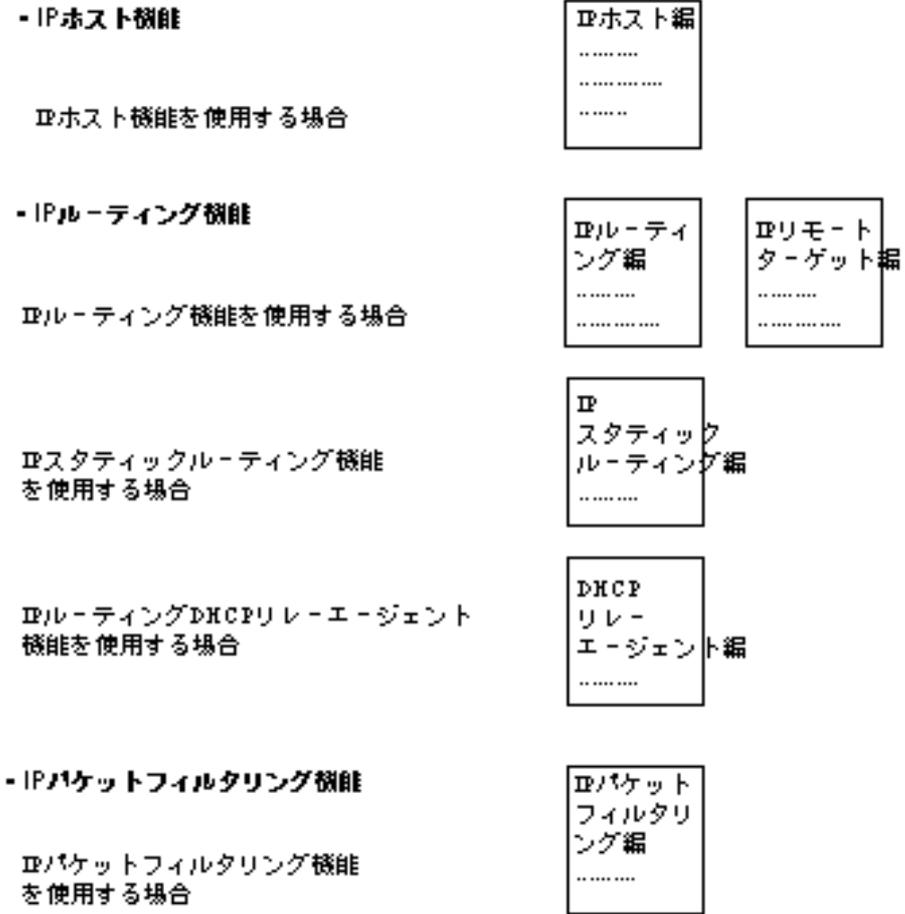


図3-2(2) ワークシートの構成(2)

【装置で使用する機能と、機能に伴うワークシート】

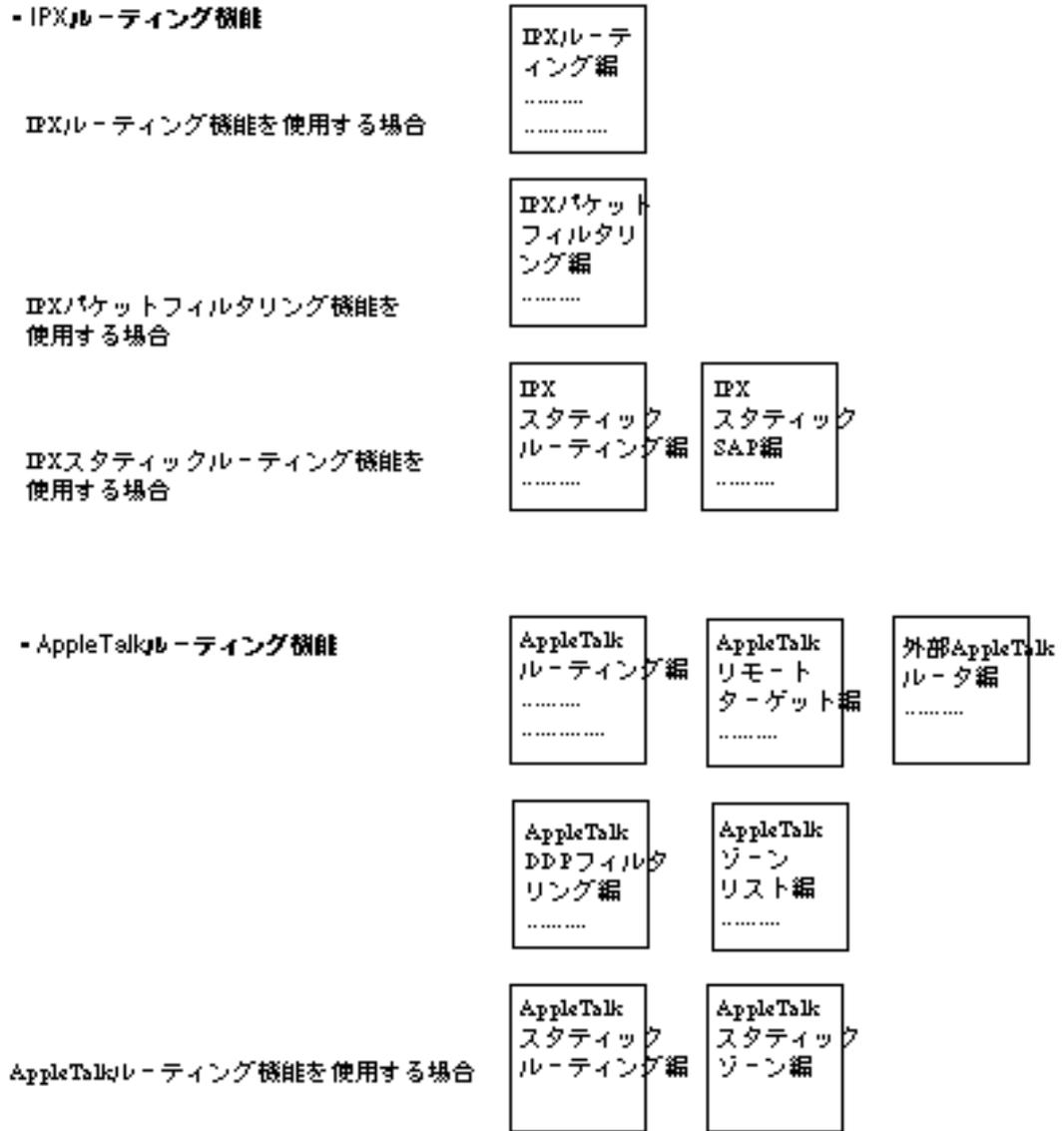


図3-2(3) ワークシートの構成(3)

【装置で使用する機能と、機能に伴うワークシート】

・ブリッジング機能

ブリッジング機能を使用する場合



ブリッジングフレームの
フィルタリング機能を使用する場合



・SNMPエージェント機能

SNMPエー ジェント機能を使用する場合



図3-2 (4) ワークシートの構成 (4)

3.2.1 ワークシート「基本設定編」

基本設定編のワークシートの形式と，記入の手順を図3-3に示します．

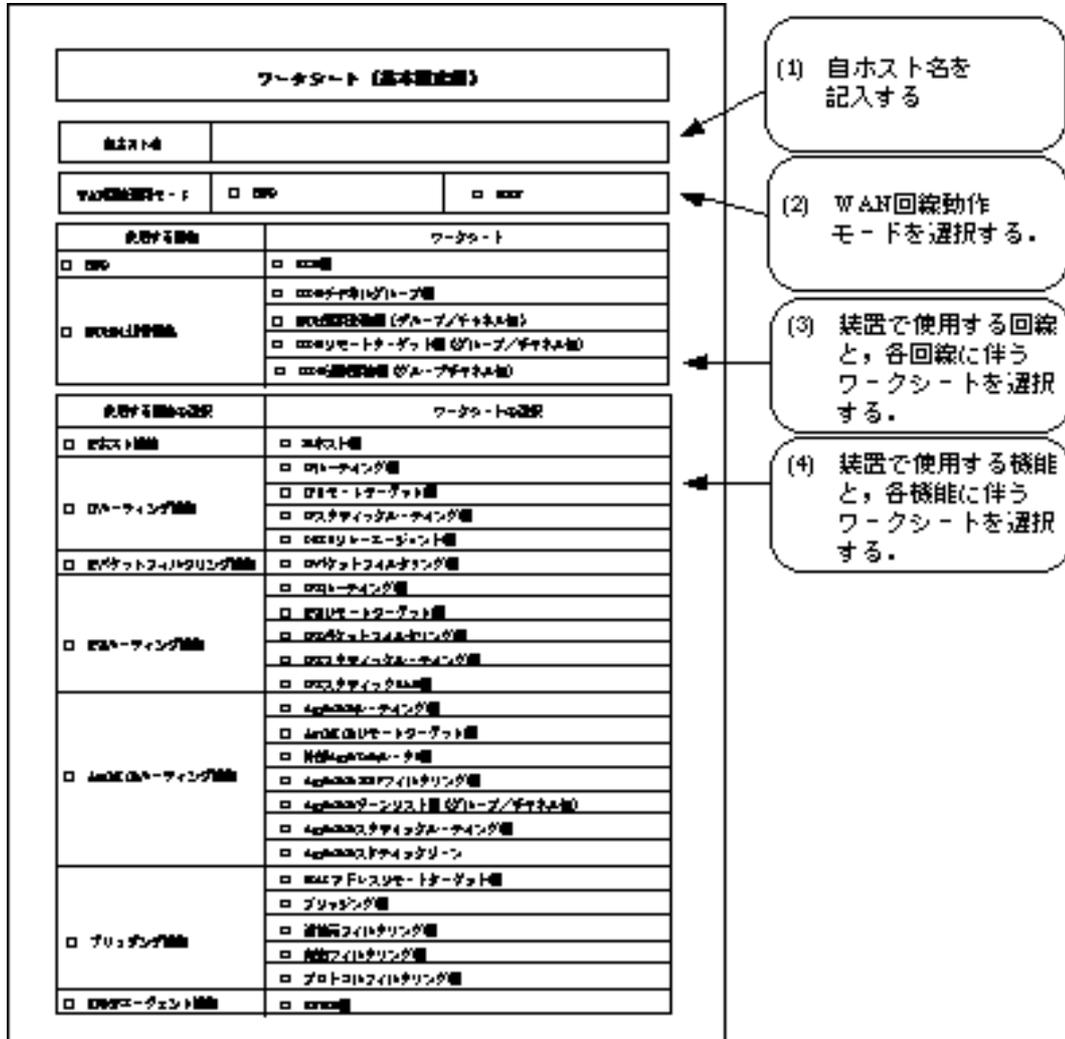


図3-3 基本設定編の形式と記入の手順

(1) 自ホスト名を記入する．

本装置の自ホスト名を記入します．

- host name
本装置の自ホスト名を記入します．
設定範囲： 最大6文字の英数字
導入時の設定： なし

(2) WAN回線動作モードを選択する。

装置で使用する回線の選択を行います。

- HSD
HSD回線を使用する場合に、欄をチェックします。
- ISDN
ISDN回線を使用する場合に、欄をチェックします。

(3) 装置で使用する回線と、各回線に伴うワークシートを選択する。

装置で使用する回線の種類を選択します。HSDを使用する場合は、使用する回線として、「HSD」の欄をチェックします。また、使用するワークシートとして「HSD編」の欄をチェックします。

ISDNを使用する場合は、グループまたはチャンネルの選択を行い、そのグループもしくはチャンネル毎に「ISDN運用形態編」、「ISDNリモートターゲット編」、「ISDN通常回線編」を選択します。

(4) 装置で使用する機能と、各機能に伴うワークシートを選択する。

選択できる機能は、「IPホスト機能」、「IPルーティング機能」、「IPパケットフィルタリング機能」、「IPXルーティング機能」、「AppleTalkルーティング機能」、「ブリッジング機能」、「SNMPエージェント機能」です。必要な機能を選択して、欄をチェックします。なお、各機能は複数重複して選択することができます。

装置で使用する機能を選択後、機能に伴うワークシートの欄をチェックします。以下に各機能と各ワークシートの概要を示します。

- IPホスト機能
この機能は、「IPルーティング機能」を選択しない場合に必ず選択します。この機能を選択する場合、ワークシート「IPホスト編」の欄をチェックします。
- IPルーティング機能
この機能は、IPルーティング機能を使用する場合に選択します。この機能を選択する場合、ワークシート「IPルーティング編」の欄をチェックします。その後、必要ならばワークシート「IPリモートターゲット編」、「DHCPリレーエージェント編」、「IPスタティックルーティング編」の欄をチェックします。
 - ・「IPリモートターゲット編」は、WAN回線にISDNを選択した場合に必要です。
 - ・IPスタティックルーティング機能は、ルーティング情報を静的(スタティック)に装置に設定する機能です。
 - ・DHCPリレーエージェント機能は、BOOTP/DHCPサーバとBOOTP/DHCPクライアントが本装置を介して遠隔地にある場合に、設定する機能です。

- IPパケットフィルタリング機能
この機能は、IPパケットフィルタリング機能の設定を行う場合に選択します。基本設定でのIPパケットフィルタリング機能は、指定したIPパケットを中継する機能です。この機能を選択する場合、ワークシート「IPパケットフィルタリング編」の 欄をチェックします。
- IPXルーティング機能
この機能は、IPXルーティングの設定を行う場合に選択します。この機能を選択する場合、ワークシート「IPXルーティング編」の 欄をチェックします。その後、必要ならばワークシート「IPXリモートターゲット編」, 「IPXパケットフィルタリング編」, 「IPXスタティックルーティング編」, 「IPXスタティックSAP編」の 欄をチェックします。
 - ・ 「IPXリモートターゲット編」は、WAN回線にISDNを選択した場合に必要です。
 - ・ IPXパケットフィルタリング機能は、指定したIPXパケットを中継する機能です。
 - ・ IPXスタティックルーティング機能、IPXスタティックSAP機能は、ルーティング情報、サーバの情報を静的(スタティック)に装置に設定する機能です。
- AppleTalkルーティング機能
この機能は、AppleTalkルーティングの設定を行う場合に選択します。この機能を選択する場合、ワークシート「AppleTalkルーティング編」および「AppleTalkゾーンリスト編」の 欄をチェックします。その後必要ならば、「AppleTalkリモートターゲット編」, 「外部AppleTalkルータ編」, 「AppleTalk DDPフィルタリング編」, 「AppleTalkスタティックルーティング編」, 「AppleTalkスタティックゾーン編」の 欄をチェックします。
 - ・ 「AppleTalkリモートターゲット編」は、WAN回線にISDNを選択した場合に必要です。
 - ・ 「外部AppleTalkルータ編」は、IP Tunnel機能を使用する場合（ 「3.2.18 AppleTalkルーティング編」 ）必要です。
 - ・ AppleTalk DDPフィルタリング機能は、指定したAppleTalkパケットを中継する機能です。
 - ・ AppleTalkスタティックルーティング機能は、ルーティング情報を静的（スタティック）に装置に設定する機能です。
- ブリッジング機能
この機能は、ブリッジングの設定を行う場合に選択します。この機能を選択する場合、必要ならばワークシート「MACアドレスリモートターゲット編」の 欄をチェックします。その後、ワークシート「ブリッジング編」の 欄をチェックします。さらに必要ならば「送信元フィルタリング編」, 「宛先フィルタリング編」, 「プロトコルフィルタリング編」の 欄をチェックします。各項目に関する説明を以下にまとめます。

- ・ 送信元フィルタリング機能は、指定した送信元MACアドレスのフレームを中継する機能です。
 - ・ 宛先フィルタリング機能は、指定した宛先MACアドレスのフレームを中継する機能です。
 - ・ プロトコルフィルタリング機能は、指定したプロトコルのフレームを中継する機能です。
- SNMPエージェント機能
この機能はSNMPエージェント機能を使用する場合に選択します。この機能を選択する場合、ワークシート「SNMP編」の 欄をチェックします。

このシートの記入はこれで終了です。

「3.2.2 ワークシート「HSD編」」から「3.2.29 ワークシート「SNMP編」」では、各ワークシートの記入方法を説明しています。ワークシート「基本設定編」で選択したワークシートに関する項を読んでください。

3.2.2 ワークシート「HSD編」

HSD編のワークシートの形式と、記入の手順を図3-4に示します。

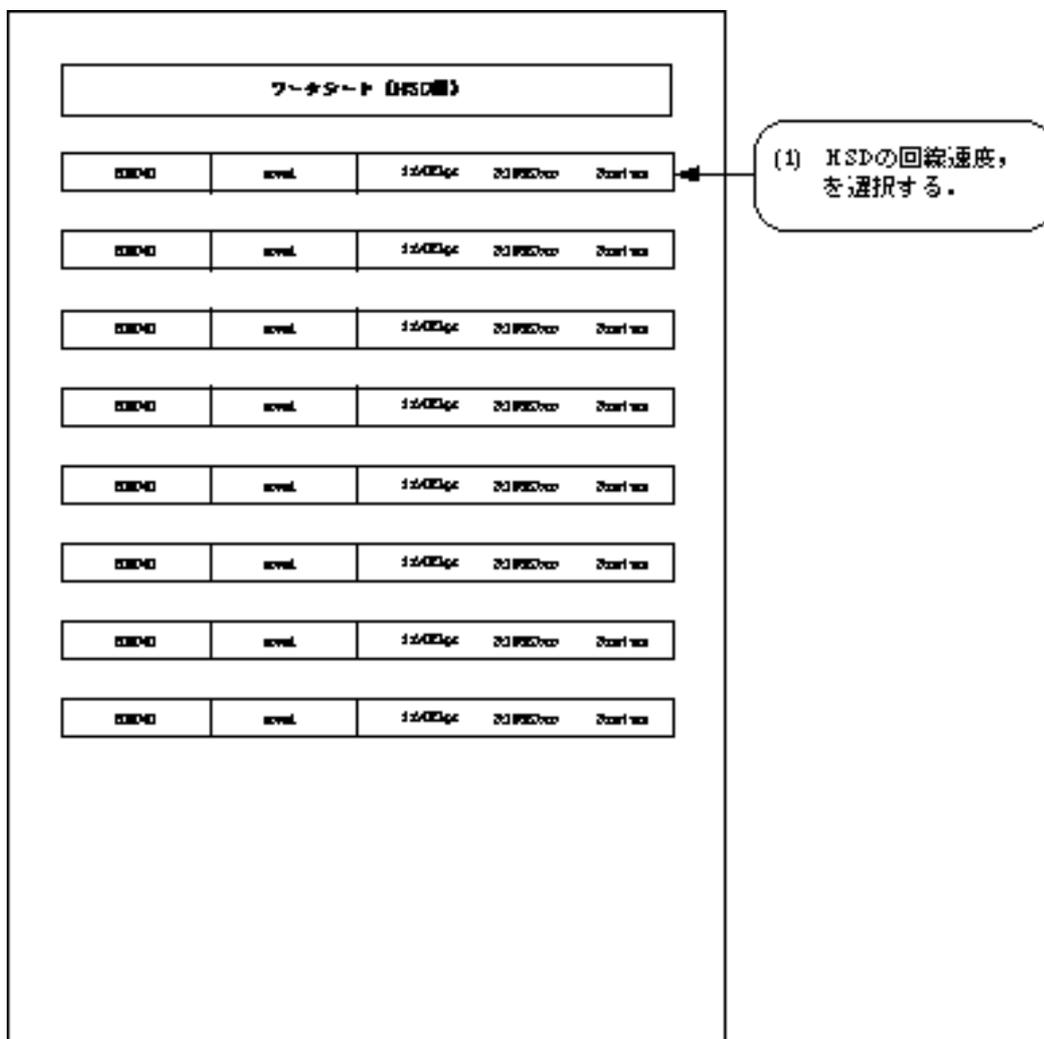


図3-4 HSD編の形式と記入の手順

(1) 回線速度を選択する。

記入項目を示します。

- speed
各回線毎にHSDの回線速度を選択します。
設定範囲： 1:64Kbps
 2:128Kbps
 3:not use
導入時の設定： 3:not use

このシートの記入はこれで終了です。

3.2.3 ワークシート「ISDNチャンネルグループ編」

ISDNチャンネルグループ編のワークシートの形式と、記入の手順を図3-5に示します。

ワークシート「ISDNチャンネルグループ編」				
ISDNグループ名	2300MHz	2300MHz	2300MHz	4700MHz
ISDNグループ名	2300MHz	2300MHz	2300MHz	2300MHz
ISDNグループ名	2300MHz	2300MHz	2300MHz	4700MHz
ISDNグループ名	2300MHz	2300MHz	2300MHz	4700MHz
ISDNグループ名	2300MHz	2300MHz	2300MHz	4700MHz
ISDNグループ名	2300MHz	2300MHz	2300MHz	4700MHz
ISDNグループ名	2300MHz	2300MHz	2300MHz	4700MHz
ISDNグループ名	2300MHz	2300MHz	2300MHz	4700MHz
ISDNグループ名	2300MHz	2300MHz	2300MHz	4700MHz
ISDNグループ名	2300MHz	2300MHz	2300MHz	4700MHz

(1) グループ名と使用するポートを選択する。

図3-5 ISDNチャンネルグループ編の形式と記入の手順

(1) グループ名と使用するポートを選択する。

NTTのサービスである「代表取扱サービス」を利用する場合の、チャンネルグループ機能におけるグループを定義します。グループは最大8エン트리設定できます。

- group name

ISDNのポートをグループとして定義する場合のグループ名を記入します。

設定範囲： 最大6文字の英数字

導入時の設定： なし

- Select the ISDN

「group name」に属するISDNのポートを選択します。

設定範囲： 1:BRI#1
 2:BRI#2
 3:BRI#3
 4:BRI#4
 5:BRI#5
 6:BRI#6
 7:BRI#7
 8:BRI#8

導入時の設定： なし



メモ：同じポートを複数のグループに割り当てることはできません。また、グループには必ず連続したポートを選択してください。

このシートの記入はこれで終了です。

3.2.4 ワークシート「ISDN運用形態編（グループ/チャンネル毎）」

ISDN運用形態編のワークシートの形式と、記入の手順を図3-6に示します。



メモ：ISDN運用形態編は、グループもしくはチャンネル毎に必要です。不足する場合は、必要枚数コピーしてください。

ワークシート「ISDN運用形態編」(グループ/チャンネル毎)				
グループ名/チャンネル名				
運用形態	ISDN	ISDN	ISDN	ISDN
運用形態1	ISDN	ISDN	ISDN	ISDN
運用形態2	ISDN	ISDN	ISDN	ISDN
運用形態3	ISDN	ISDN	ISDN	ISDN
運用形態4	ISDN	ISDN	ISDN	ISDN
運用形態5	ISDN	ISDN	ISDN	ISDN
運用形態6	ISDN	ISDN	ISDN	ISDN
運用形態7	ISDN	ISDN	ISDN	ISDN
運用形態8	ISDN	ISDN	ISDN	ISDN
運用形態9	ISDN	ISDN	ISDN	ISDN
運用形態10	ISDN	ISDN	ISDN	ISDN
運用形態11	ISDN	ISDN	ISDN	ISDN
運用形態12	ISDN	ISDN	ISDN	ISDN
運用形態13	ISDN	ISDN	ISDN	ISDN
運用形態14	ISDN	ISDN	ISDN	ISDN
運用形態15	ISDN	ISDN	ISDN	ISDN
運用形態16	ISDN	ISDN	ISDN	ISDN
運用形態17	ISDN	ISDN	ISDN	ISDN
運用形態18	ISDN	ISDN	ISDN	ISDN
運用形態19	ISDN	ISDN	ISDN	ISDN
運用形態20	ISDN	ISDN	ISDN	ISDN

(1) グループ名もしくはチャンネルを記入する。

(2) 運用形態等を記入する。

(3) トラヒック分散回線とする場合、どのグループもしくはチャンネルのトラヒック分散回線とするか記入する。

図3-6 ISDN運用形態編の形式と記入の手順

(1) グループ名もしくはチャンネルを記入する。

設定項目を以下に示します。

- Selecting group/channel

設定を行うグループ（3.2.3 ワークシート「ISDNチャンネルグループ編」で設定したもの）もしくはチャンネル（どのグループにも属さないポートのうち1もしくは2を選択する）を記入します。

設定範囲： 有効なグループ名もしくはチャンネル名

導入時の設定： なし



メモ：本装置および本取扱説明書では、ISDNのポートの名称を「BRI#1」～「BRI#8」、また、チャンネルの名称は「BRI#1-1」のように「-1」「-2」を付加した形式で示します。

(2) 運用形態等を記入する。

設定項目を以下に示します。

- WAN topology

本グループもしくはチャンネルの運用形態を選択します。

設定範囲： 1:Usual (通常回線として使用)
2:Load split (トラヒック分散回線として使用)
3:Usual/Load split (通常回線またはトラヒック分散回線として使用)
(グループの場合のみ)
4:not use (チャンネルの場合のみ)

導入時の設定： 1:Usual



注意：「Usual」として運用するグループもしくはチャンネルが他にない場合は、「Load split」は選択できません。

- multi target (チャンネルの場合のみ)

本チャンネルを複数の相手(最大80箇所)と接続するかどうかを選択します。

設定範囲： 1:use (複数の相手と接続する)
2:not use (複数の相手と接続しない)

導入時の設定： 2:not use

- receive address check mode

着信時に相手アドレスをチェックするかどうかを選択します。

設定範囲： 1:on (チェックする)
2:off (チェックしない)

導入時の設定： 1:on

- receive address check skip length

「receive address check mode」を「on」とした場合、チェック時のアドレススキップ長を記入します。

設定範囲： 0 ~ 19

導入時の設定： 0



メモ：本設定は、0発信により外線に接続する私設網などで発信番号と着信番号が異なる場合に設定します。例えば、PBX経由で0発信により外線と接続する場合、設定番号の最初の1桁(0)を、チェックの対象外とします。

設定相手番号：0-03-xxx-xxxx，着信番号:03-xxxx-xxxx

「check skip length」を1に設定する。

(3) トラヒック分散回線とする場合，どのグループもしくはチャンネルのトラヒック分散回線とするか記入する．

本グループもしくはチャンネルをトラヒック分散回線（Load split）とする場合，どのグループもしくはチャンネルのトラヒック分散回線とするのが設定します．

- Usual line

本グループもしくはチャンネルをトラヒック分散回線とする場合，どのグループもしくはチャンネルのトラヒック分散回線とするのが記入します．

設定範囲： 「WAN topology」で「Usual」が選択されたグループもしくはチャンネル
導入時の設定： なし

このシートの記入はこれで終了です．

3.2.5 ワークシート「ISDNリモートターゲット編（グループ/チャンネル毎）」

ISDNリモートターゲット編のワークシートの形式と、記入の手順を図3-7に示します。

本ワークシートは、「WAN topology」で「Usual」もしくは「Usual/Load split」を選択した場合のみ記入します。

➡ メモ：ISDNリモートターゲット編は、グループもしくはチャンネル毎に必要です。不足する場合は、必要枚数コピーしてください。

The diagram shows a worksheet form titled "ワークシート「ISDNリモートターゲット編」". It contains several input fields and tables. Two callouts on the right indicate the input steps: (1) "グループ名もしくはチャンネルを記入する。" (Enter group name or channel) pointing to the "Group/channel" field, and (2) "リモートターゲットテーブルを記入する。" (Enter remote target table) pointing to the "Remote target table" section.

ワークシート「ISDNリモートターゲット編」			
Group/channel			
name			
remote address			
channel			
Do you want to use Load split for ISDN??		Yes	No
input	12345 5678901234 56789	remote	
Load split 動作時			
all lines			
channel			

図3-7 ISDNリモートターゲット編の形式と記入の手順

(1) グループ名もしくはチャンネルを記入する。

設定項目を以下に示します。

- Selecting group/channel
設定を行うグループ (3.2.3 ワークシート「ISDNチャンネルグループ編」で設定したもの) もしくはチャンネル (どのグループにも属さないポートのうち1もしくは2を選択する) を記入します。
設定範囲: 「WAN topology」で「Usual」もしくは「Usual/Load split」を選択したグループもしくはチャンネル
導入時の設定: なし

(2) リモートターゲットテーブルを記入する。

ISDNリモートターゲットを記入します。本装置では運用上、ISDN番号のかわりにISDNリモートターゲットを使用します。1つのエントリーに関する記入項目を以下に示します。

- target
ISDNリモートターゲットを記入します。
設定範囲: 最大6文字の英数字
導入時の設定: なし
- remote address
宛先のISDN番号を市外局番から記入します。
設定範囲: 最大20桁の10進数
導入時の設定: なし
- remote subaddress
宛先のISDNサブアドレスを記入します。ISDNサブアドレスを使用している場合のみ、記入を行います。
設定範囲: 最大19桁の10進数
導入時の設定: なし
- preference
同一の「target」が複数ある場合に、宛先ISDN番号に発呼の優先度を指定します。
設定範囲: 0 ~ 4 (小さいほど優先度が高い)
導入時の設定: 0



メモ: 「target」に対して発呼要求があった場合、優先度の高い宛先ISDN番号に発呼します。接続が失敗した場合、次に優先度の高い宛先ISDN番号に発呼します。

3章 基本設定

- Do you connect Load split line to XXXXXX?
設定しているグループもしくはチャンネルが負荷分散回線を接続する設定になっている場合で、「preference」を「0」とした場合、「target」で指定した接続相手に対して、トラヒック分散するかどうか選択します。
設定範囲： 1:yes (トラヒック分散する)
2:no (トラヒック分散しない)
導入時の設定： 2:no

- load split line address
「Do you connect Load split line to XXXXXX?」で「yes」とした場合、トラヒック分散回線の相手ISDN番号を記入します。
設定範囲： 最大20桁の10進数
導入時の設定： 通常回線における接続相手のISDN番号 (「remote address」の値)

- load split line subaddress
「Do you connect Load split line to XXXXXX?」で「yes」とした場合、トラヒック分散回線の相手ISDNサブアドレスを記入します。
設定範囲： 最大19桁の10進数
導入時の設定： 通常回線における接続相手のISDNサブアドレス
(「remote subaddress」の値)

- speed
発呼するユーザ速度を選択します。
設定範囲： 1:64K (64kbpsで発呼する)
2:64K/56K (最初に64kbpsで発呼し、理由コードが伝達能力で切断された場合、56kbpsで再発呼する)
3:56K (56kbpsで発呼する)
導入時の設定： 1:64K

- password
リモートターゲットに対するパスワードを記入します。ISDN回線を使用する場合、不本意な相手と接続されることを防ぐためにセキュリティ機能としてパスワードを設定します。(「2.10.7 セキュリティ機能」)
設定範囲： 8文字以内の英数字
導入時の設定： なし

このシートの記入はこれで終了です。

3.2.6 ワークシート「ISDN通常回線編」

ISDN通常回線編のワークシートの形式と、記入の手順を図3-8に示します。



メモ：ISDN通常回線編は、グループもしくはチャンネル毎に必要です。不足する場合は、必要枚数コピーしてください。

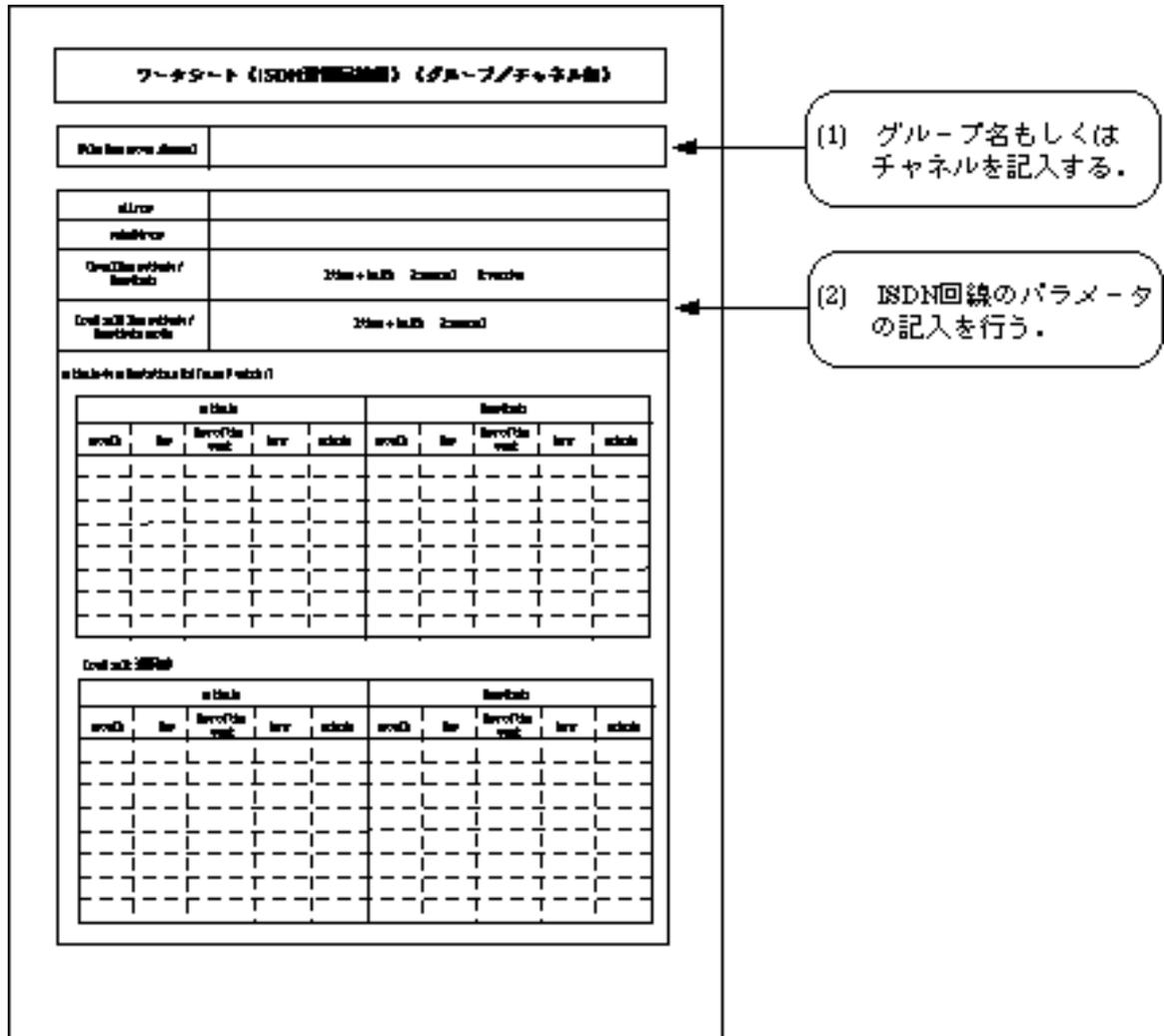


図3-8 ISDN通常回線編の形式と記入の手順

(1) グループ名もしくはチャンネルを記入する。

設定項目を以下に示します。

- Selecting group/channel

設定を行うグループ (3.2.3 ワークシート「ISDNチャンネルグループ編」で設定したもの) もしくはチャンネル (どのグループにも属さないポートのうち1もしくは2を選択する) を記入します。

設定範囲： 「WAN topology」で「Usual」, 「Usual/Load split」もしくは「Load split」を選択したグループもしくはチャンネル

導入時の設定： なし

(2) ISDN回線のパラメータの記入を行う。

設定項目を示します。

- address
自局のISDN番号を記入します。
設定範囲： 最大20桁の10進数
導入時の設定： なし



メモ：自局のISDN番号には市外局番を含めないでください。

- subaddress
自局のISDNサブアドレスを記入します。
設定範囲： 最大19桁の10進数
導入時の設定： なし
- Usual line activate/deactivate
本グループを通常回線として使用する場合（3.2.4 ワークシート「ISDN運用形態編」の「WAN topology」で「Usual」または「Usual/Load split」を選択した場合）、接続(activate) / 切断(deactivate)の方法を選択します。
設定範囲： 1:time + traffic (指定時刻の回線の自動接続, 指定時刻の回線の自動切断又は中継データがなくなったことによる自動切断)
2: manual (手動による回線の接続)
3: passive (着信専用)
導入時の設定： 3: passive
- Load split line activate/deactivate
本グループをトラヒック分散回線として使用する場合（3.2.4 ワークシート「ISDN運用形態編」の「WAN topology」で「Load split」または「Usual/Load split」を選択した場合）、接続(activate) / 切断(deactivate)の方法を選択します。
設定範囲： 1:time + traffic (指定時刻の回線の自動接続, 指定時刻の回線の自動切断又は中継データがなくなったことによる自動切断)
2: manual (手動による回線の接続)
導入時の設定： 2: manual



メモ：実際の接続および切断は、手動による動作を優先します（passive/passiveを除く）。例えば、時刻指定の自動接続 / 切断を選択した場合でも、指定時刻外に手動による接続および切断が可能です。



注意：time+trafficを選択して時間外に手動で接続した場合は、一定時間（「4.2 データリンクに関する設定」の「idle timer」）中継データがなくなると自動切断します。



注意：ISDNの接続方法とその他の条件によって、IP/IPXのダイナミックルーティング機能が使用できない場合があります。ISDNの接続方法およびその他の条件と、ルーティング機能の関係を表3-1にまとめます。

表3-1 ISDNの接続方法およびその他の条件とルーティング機能の関係

ISDNの接続方法	interface up mode (4.2を参照)	mult target (3.24を参照)	IP/IPX/AppleTalkルーティング		
			ダイナミック (RIP(IP),RIP(IPX),SAP(IPX), RTMP(AppleTalk), AURP(AppleTalk))		スタティック (IP/IPX/AppleTalk スタティック, スタティックSAP)
			triggered update	定期 update	
time+traffic	- (適用外)	not use	○	○	○
		use	◎	◎	○
manual, passive	always	not use	○	○	○
		use	◎	◎	○
	normal	not use	○	○	○
		use	◎	◎	○

上記の表に関する注意事項を以下にまとめます。

- 図中の ○ と ◎ はルーティング機能が使用できることを示します。◎ は、ISDN回線の接続を契機としてルーティング情報の交換を行う本装置の独自機能によってルーティングが使用できることを示します。
- IP/IPX/AppleTalkダイナミックルーティング機能を使用する場合は、ISDN回線の両側の装置の設定が上記の表の「ダイナミックルーティング：」の条件を満たしている必要があります。
- 装置導入時のダイナミックルーティングの「triggered update」/「定期update」の種別はRIP(IP)、RIP(IPX)、SAP(IPX)、RTMP(AppleTalk)、AURP(AppleTalk)のいずれも「triggered update」です（「4.5.1 RIP(IP)インタフェースに関する設定」、「4.6.1 RIP(IPX)インタフェースの設定」、「4.6.4 SAP(IPX)インタフェースの設定」、「4.7.1 AppleTalkインタフェースの設定」、「4.7.13 AURPプロトコルの設定」）。そのため、ダイナミックルーティングの方法として「定期update」を使用したい時は、拡張設定のRIP(IP)、RIP(IPX)、SAP(IPX)、RTMP(AppleTalk)、AURP(AppleTalk)の「triggered update」/「定期update」の種別を「定期update」に変更する必要があります。ただし、ダイナミックルーティングの方法として「定期update」を選択した場合は、RIP(IP)、RIP(IPX)、SAP(IPX)、RTMP(AppleTalk)、AURP(AppleTalk)の制御パケットが一定時間おきにISDN回線に送信されます（4.5.1、4.6.1、4.6.4、4.7.1、4.7.13）。そのため、ISDN回線の切断方法として「time+traffic」を選択しても、中継データがなくなったことによるISDN回線の自動切断を行わない場合があります。

3章 基本設定

- 装置導入時の「interface up mode」の設定は「normal」です。（「4.2 データリンクに関する設定」）

また、ISDNの接続方法の組み合わせによってはIPXルーティング機能を使用できないケースがあります。図3-9にそのケースを示します。

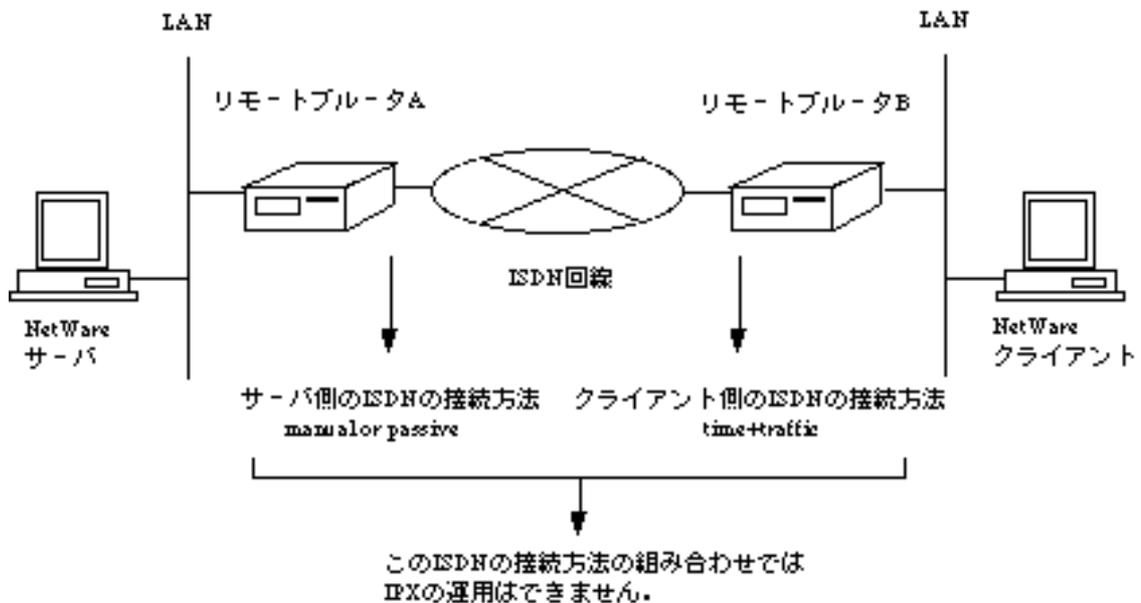


図3-9 ISDNの接続方法によるIPXルーティング不能ケース

- activate-deactivate time list
「Usual line activate/deactivate」で「time + traffic」を選択した場合は、接続時刻、切断時刻を記入します。接続時刻、切断時刻とも通常回線およびトラフィック分散回線でそれぞれ8エン트리記入できます。
設定範囲：
month (1 ~ 12, *)
day (1 ~ 31, *)
day of the week (1:Sun., 2:Mon., 3:Tue., 4:Wed., 5:Thu., 6:Fri., 7:Sat., 8:any(すべての曜日))
hour (0 ~ 23, *)
minute (0 ~ 59, *)
導入時の設定： 「deactivate minute」は00, 「day of the week」はany, それ以外は**

時刻を記入する時の注意事項を以下に示します。

- 時刻(hour)は24時間制で記入します。
- *(アスタリスク)は、各々の項目の全てを網羅することを示します。
- 「activate」のすべてに「*」を指定した場合は、常時接続されます。

- 「deactivate」のすべてに「*」を入力することはできません。
- 「activate」と「deactivate」を同一に指定した場合は、切断が優先され接続しません。
- 日と曜日を同時に記入することはできません。もし同時に記入して装置に設定した場合、日を指定されている方を優先します。



メモ：「*」で設定されたエントリと他の明示的に値を指定したエントリが重複した場合は、「*」のエントリは無視されます（特定日優先機能）。



注意：切断時刻に2月29日を設定した場合には、次のうるう年まで接続状態が継続することがあります。

3.2.7 ワークシート「IPホスト編」

IPホスト編のワークシートの形式と、記入の手順を図3-10に示します。

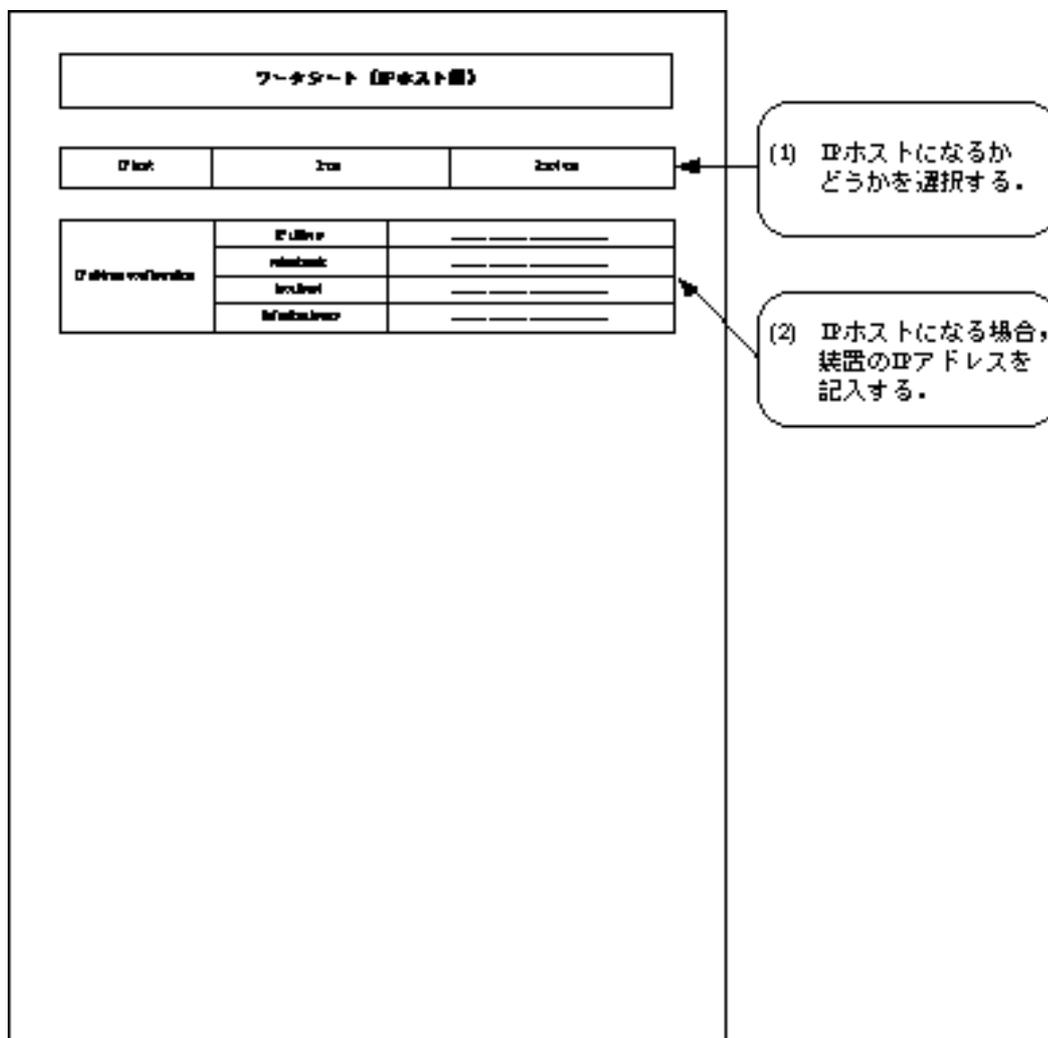


図3-10 IPホスト編の形式と記入の手順

(1) IPホストになるかどうかを選択する。

記入項目を示します。

- IP host
IPホストとして運用する / しないを選択します。
設定範囲： 1:use (IPホストとして運用する)
 2:not use (IPホストとして運用しない)
導入時の設定： 2:not use

「IPルーティング機能」を選択しない場合で、装置がIPホストになる必要があるのは、以下のような場合です。

- 「SNMPエージェント機能」を使用する場合。
- 「IPフィルタリング機能」を使用する場合。
- 「TELNETサーバ機能」を使用する場合。
- 「リモートコンソール機能」を使用する場合。
- 装置の所在を確認するエコーテストの対象とする場合。

上記の条件に当てはまる場合には、IPホスト「use」を選択します。この場合、次にIPアドレスの記入を行います。

また上記に当てはまらない場合には、IPホスト「not use」を選択します。この場合、このシートの記入はこれで終了です。

(2) IPホストになる場合、装置のIPアドレスを記入する。

「IP host」で「use」を選択した場合には、本装置のIPアドレスを記入します。

- IP address
装置のIPアドレスを記入します。
設定範囲： xxx.xxx.xxx.xxxの形式(マーシャンアドレスを除く)
導入時の設定： なし
-  注意：装置に設定するIPアドレスとして、以下のアドレスが適用できます。その他のアドレスはマーシャンアドレスと呼ばれるアドレスで、特別な用途のために予約されています。
1.0.0.0 ~ 126.255.255.255
128.0.0.0 ~ 255.255.239.255
- subnetmask
装置のサブネットマスクを記入します。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： クラスA:255.0.0.0, クラスB:255.255.0.0, クラスC:255.255.255.0
- broadcast
装置のブロードキャストアドレスを記入します。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： ホスト部がオール1のアドレス

3章 基本設定

- default gateway

デフォルトゲートウェイを使用する場合、デフォルトゲートウェイのIPアドレスを記入します。

設定範囲： xxx.xxx.xxx.xxxの形式

導入時の設定： なし



メモ：デフォルトゲートウェイは中継先の分からないパケットを転送するゲートウェイを示します。

このシートの記入はこれで終了です。

3.2.8 ワークシート「IPルーティング編」

IPルーティング編の、ワークシートの形式と記入の手順を図3-11に示します。

ワークシート「IPルーティング編」

LAN

interface name	IP
Ethernet	_____
serial	_____
loopback	_____

WAN

interface name	Serial	IP	interface name	Serial	IP
Ethernet	_____	_____	Ethernet	_____	_____
serial	_____	_____	serial	_____	_____
loopback	_____	_____	loopback	_____	_____
serial DCE	_____	_____	serial DCE	_____	_____
serial DTE	_____	_____	serial DTE	_____	_____

このワークシートは、IPルーティングテーブルを生成するためのテンプレートです。ネットワーク構成に応じて、必要に応じて修正してください。

図3-11 IPルーティング編の形式と記入の手順

(1) 各インタフェースのIPアドレスを記入する

始めに、LANインタフェースの項目の記入を行います。

- IP address

LANインタフェースのIPアドレスを記入します。

設定範囲： xxx.xxx.xxx.xxxの形式(マージャンアドレスを除く)

導入時の設定： なし



注意：装置に設定するIPアドレスとして、以下のアドレスが適用できます。その他のアドレスはマージャンアドレスと呼ばれるアドレスで、特別な用途のために予約されています。

1.0.0.0 ~ 126.255.255.255

128.0.0.0 ~ 255.255.239.255

- subnetmask

LANインタフェースのサブネットマスクを記入します。

設定範囲： xxx.xxx.xxx.xxxの形式

導入時の設定： クラスA:255.0.0.0, クラスB:255.255.0.0, クラスC:255.255.255.0

- broadcast

LANインタフェースのブロードキャストアドレスを記入します。

設定範囲： xxx.xxx.xxx.xxxの形式

導入時の設定： ホスト部がオール1のアドレス

次に、WANインタフェース(HSDまたはISDN)の項目の記入を行います。

- routing interface

ISDN選択時には、ルーティングに使用するインタフェースを選択します。IPルーティングを行うグループもしくはチャンネルを記入します。(実際の設定では、IPルーティングを行うかどうかの問い合わせがあります。行うのであれば「y」を、行わないのであれば「n」を選択します。)

設定範囲： 「WAN topology」で「Usual」または「Usual/Load split」を選択したグループもしくはチャンネル

導入時の設定： なし

- interface type

WAN回線のインタフェースタイプを選択します。

設定範囲： 1:broadcast (ブロードキャスト)

2:point to point (ポイントツーポイント)

導入時の設定： 2:point to point



注意：接続相手がルータ以外(パーソナルコンピュータなど)の時のみ「interface type」で「point to point」選択してください。その場合、そのグループの接続/切断の方法(3.2.6 「ISDN通常回線編」)は「passive」にしてください。

- IP address

WANインタフェースのIPアドレスを記入します。ただし、WAN回線のインタフェースタイプとしてポイントツーポイントを選択した場合は、LANと同じ値を記入することを推奨します。この場合、LANと異なる値を記入して装置に設定することも可能ですが、余計なIPアドレスを消費してしまいます。

設定範囲： xxx.xxx.xxx.xxxの形式(マージャンアドレスを除く)

導入時の設定： なし

- subnetmask
WANインタフェースのサブネットマスクを記入します。ただし、専用線のインタフェースタイプとしてポイントツーポイントを選択した場合で、上記の「IPaddress」でLANインタフェースで設定したIPアドレスと同じ値を記入した場合は、「subnetmask」を記入する必要はありません。上記の「IPaddress」でLANインタフェースで設定したIPアドレスと異なる値を記入した場合は、適切なサブネットマスクを設定する必要があります。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： クラスA:255.0.0.0, クラスB:255.255.0.0, クラスC:255.255.255.0

- broadcast
WAN回線のインタフェースタイプとしてブロードキャストを選択した場合は、ブロードキャストアドレスを記入します。WAN回線のインタフェースタイプとしてポイントツーポイントを選択した場合、記入する必要はありません。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： ホスト部がオール1のアドレス

- remote IP address
WAN回線のインタフェースタイプとしてポイントツーポイントを選択した場合は、接続相手のIPアドレスを記入します。WAN回線のインタフェースタイプとしてブロードキャストを選択した場合、記入する必要はありません。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： なし

- remote subnetmask
WAN回線のインタフェースタイプとしてポイントツーポイントを選択した場合は、接続相手のサブネットマスクを記入します。WAN回線のインタフェースタイプとしてブロードキャストを選択した場合、記入する必要はありません。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： 255.255.255.255



メモ：「routing interface」でグループを選択した場合、グループに含まれるチャンネルの「interface type」を「point to point」として運用することができます。この場合は、すべてのチャンネルに関して項目を記入してください。

このシートの記入はこれで終了です。

3.2.9 ワークシート「IPリモートターゲット編」

IPリモートターゲット編の、ワークシートの形式と記入の手順を図3-12に示します。

ワークシート「IPリモートターゲット編」

	address	mask		address	mask
1			11		
2			12		
3			13		
4			14		
5			15		
6			16		
7			17		
8			18		
9			19		
10			1A		
11			1B		
12			1C		
13			1D		
14			1E		
15			1F		
16			20		
17			21		
18			22		
19			23		
20			24		
21			25		
22			26		
23			27		
24			28		
25			29		
26			2A		
27			2B		
28			2C		
29			2D		
30			2E		

IPリモートターゲットテーブルは最大80件まで登録できます。エントリは最大80件記入できます。1エントリに関する設定項目を以下に示します。

(1) IPのISDNリモートターゲットを記入する。

図3-12 IPリモートターゲット編の形式と記入の手順

(1) IPのISDNリモートターゲットを記入する。

ISDNを選択した場合でISDNで複数の相手と接続する（ 3.2.4(2) ）場合、宛先のIPアドレスとそれに対応するISDNリモートターゲットのテーブルを記入します。ISDNの接続相手を固定して使用する場合、記入の必要はありません。エントリは最大80件記入できます。1エントリに関する設定項目を以下に示します。

- address
宛先のIPアドレスを記入します。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： なし

- target index
宛先のIPアドレスに対応した、ISDNリモートターゲットを記入します。
設定範囲： ISDNリモートターゲット（最大80エントリから1エントリ選択）
導入時の設定： なし



メモ：IPリモートターゲットテーブルは、最大80エントリ設定が可能です。本ワークシートをもう一枚コピーしてください。

このシートの記入はこれで終了です。

3.2.10 ワークシート「IPスタティックルーティング編」

IPスタティックルーティング編のワークシートの形式と、記入の手順を図3-13に示します。

ワークシート「IPスタティックルーティング編」

destination IP	net	network	width	priority
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		
-----	-----	-----		

(1) IPスタティックルーティングテーブルを記入する。

テーブルは最大256エントリが登録可能です。 設定するテーブルのエントリより大きい場合は、設定可能なエントリ数にしてください。

図3-13 IPスタティックルーティング編の形式と記入の手順

➡ **メモ**：スタティックルーティングで設定するIPアドレスには、0.0.0.0から255.255.255.255のすべてのIPアドレスが設定可能です。

(1) IPスタティックルーティングテーブルを記入する。

IPスタティックルーティングテーブルには、最大256エントリの登録が可能です。1つのエントリに関する記入項目を以下に示します。

- destination address
宛先IPアドレスを記入します。もし、ここのアドレスを「0.0.0.0」と記入した場合、このエントリはデフォルトルートの設定となります。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： 0.0.0.0(デフォルトルート)



メモ：デフォルトルートとは、中継先の分からないパケットを装置が受信した場合に、装置がそのパケットを転送するゲートウェイを指定する機能です。

- mask

宛先IPアドレスのサブネットマスクを記入します。

設定範囲： xxx.xxx.xxx.xxxの形式

導入時の設定： 0.0.0.0 (destination addressがホストを示す場合は、255.255.255.255)



メモ：ホストルートを設定する場合は、「mask」に「255.255.255.255」を設定します。

- gateway

「destination address」で指定された宛先へパケットを送信する場合の、中継先ゲートウェイアドレスを記入します。「destination address」が「0.0.0.0」(デフォルトルートの設定)の場合、この値は宛先の分からないパケットを転送するゲートウェイ(デフォルトゲートウェイ)を示します。

設定範囲： xxx.xxx.xxx.xxxの形式

導入時の設定： 0.0.0.0

- metric

このエントリをRIPで送信する場合のメトリック値を記入します。またメトリック値を16とすると、このエントリに記入してあるネットワークに関する情報はRIPで送信しません。

設定範囲： 1 ~ 16

導入時の設定： 16

基本的にメトリック値には「destination address」に到達するために経由するルータの数を記入します。ただし、メトリック値を実際に経由するルータの数と異なる値として記入することで、記入中のスタティックルートに重みをつけることが可能となります。次に例を示します。

- ・ メトリック値を実際に経由するルータの数より大きな値にする場合
この場合、相手の装置はこのルートを現実より到達が困難であると判断します。例えば、回線の課金が高いのでそのルートはなるべく使用したくない等の場合に、このような記入を行います。
- ・ メトリック値を実際に経由するルータの数より小さな値にする場合
この場合、相手の装置はこのルートを現実より到達が容易であると判断します。例えば、回線の課金が安いのでそのルートをなるべく使用したい等の場合に、このような記入を行います。

- preference

ルーティング情報がRIP，スタティックルート，ICMPリダイレクトメッセージによって学習した情報などと重複した場合，どのルートを優先するかを決定する優先順位の値を記入します．経路を選択する際，「preference」値の小さな値の経路が有効となります．本装置では，RIPで学習したルーティング情報の「preference」値は100固定，スタティックルートの「preference」値の導入時の設定が50です．

設定範囲： 0 ~ 255

導入時の設定： 50



メモ：メトリック値と「preference」値の関係

同じネットワークに対する経路が重複したとき，本装置は経路選択の値として「preference」値のみ使用します．メトリック値は，装置が広告するルート情報に添付する値として使用されません．本装置は，同じネットワークに対する「preference」値の等しいルート情報を複数保持していた場合，先に検索されたルート情報を有効とします．



メモ：IPスタティックルーティングテーブルは，最大256エントリ設定が可能です．本ワークシートを必要枚数コピーしてください．

このシートの記入はこれで終了です．

3.2.11 ワークシート「DHCPリレーエージェント編」

DHCPリレーエージェント編のワークシートの形式と、記入の手順を図3-14に示します。

ワークシート「DHCPリレーエージェント編」		
insert ISDN address	yes	no
insert ISDN address		
no insert ISDN address		
insert ISDN address		
no insert ISDN address		
DHCP relay 2nd	.	.
	.	.
	.	.

(1) DHCPリレーエージェント機能に関する項目を記入する。

図3-14 DHCPリレーエージェント編の形式と記入の手順

(1) DHCPリレーエージェント機能に関する項目を記入する。

DHCPリレーエージェント機能は、BOOTP/DHCPサーバとBOOTP/DHCPクライアントが本装置を介して遠隔地にある場合に、設定する機能です。本機能を使用しない場合は、本ワークシートの記入は必要ありません。以下に設定項目を示します。

- insert ISDN address
DHCPパケット内に接続相手のISDN番号を入れて送信するかどうか選択します。
設定範囲： 1: yes
2: no
導入時の設定： 2: no



メモ：ISDNを介してサーバが存在する形態を使用する場合，DHCPサーバがISDN番号でクライアントを意識するためにはサーバ側ルータは「insert ISDN address」を「yes」に設定します．

- max hops value
DHCPパケット内の「hops」領域の最大値を記入します．「hops」は，リレーする毎に1ずつインクリメントされる値です．
設定範囲： 1 ~ 16
導入時の設定： 4

- send request interface
DHCPリクエストパケットを送信するインタフェースを記入します．
設定範囲： LAN, 「routing interface」で選択されたグループもしくはチャンネル
導入時の設定： LAN, 「routing interface」で選択されたグループもしくはチャンネル

- recv request interface
DHCPリクエストパケットを受信するインタフェースを記入します．
設定範囲： LAN, 「routing interface」で選択されたグループもしくはチャンネル
導入時の設定： LAN, 「routing interface」で選択されたグループもしくはチャンネル

- DHCP server list
リレー先のDHCPサーバのIPアドレスを記入します．
設定範囲： xxx.xxx.xxx.xxxの値
導入時の設定： なし

このシートの記入はこれで終了です．

3.2.12 ワークシート「IPパケットフィルタリング編」

IPパケットフィルタリング編のワークシートの形式と、記入の手順を図3-15に示します。

ワークシート「IPパケットフィルタリング編」

No.	IPアドレス	ポート	プロトコル	宛先	動作
1	192.168.1.1	80	TCP	192.168.1.2	許可
2	192.168.1.1	80	TCP	192.168.1.2	拒否
その他の設定					有効

No.	IPアドレス	ポート	プロトコル	宛先	動作
1	192.168.1.1	80	TCP	192.168.1.2	許可
2	192.168.1.1	80	TCP	192.168.1.2	拒否
その他の設定					有効

No.	IPアドレス	ポート	プロトコル	宛先	動作
1	192.168.1.1	80	TCP	192.168.1.2	許可
2	192.168.1.1	80	TCP	192.168.1.2	拒否
その他の設定					有効

No.	IPアドレス	ポート	プロトコル	宛先	動作
1	192.168.1.1	80	TCP	192.168.1.2	許可
2	192.168.1.1	80	TCP	192.168.1.2	拒否
その他の設定					有効

データは最大128エントリまで登録可能です。既定するデータのエントリより少ない場合は、空白欄をコピーしてください。

(1) IPパケットフィルタリングテーブルを記入する。

図3-15 IPパケットフィルタリング編の形式と記入の手順

(1) IPパケットフィルタリングテーブルを記入する。

IPパケットフィルタリングテーブルには、最大128エントリの登録が可能です。1つのエントリに関する記入項目を以下に示します。



メモ：フィルタリングで設定するIPアドレスには、0.0.0.0から255.255.255.255のすべてのIPアドレスが設定可能です。

3章 基本設定

- protocol

フィルタリングの対象とするパケットのプロトコルを選択します。

設定範囲： 1:tcp (TCPプロトコル)
2:udp (UDPプロトコル)
3:tcp+udp (TCP , UDPプロトコル)
4:all (すべてのプロトコル)
5:other (TCP, UDP以外のプロトコルを0～255の10進で指定)

導入時の設定： 4:all

「other」を選択した場合には、プロトコル番号を10進数で記入します。TCPとUDP以外の主なプロトコル番号を表3-2に示します。

表3-2 IPのプロトコル番号例

プロトコル	設定値(16進数)
IP	0800(type)
ARP	0806(type)
トレーラプロトコル	10XX(type) (XXは00～10の値)
リバースARP	8035(type)
IPX	8137(type), 8138(type), e0(dlsap), ff(dlsap)
DECnet	60XX(type) (XXは00～09の値), 80XX(type) (XXは38～42の値)
AppleTalk	809b(type), 80f3(type)
XNS	0807(type)
XEROX PUP	0200(type), 0201(type), 0a00(type), 0a01(type)
XEROX NS IDP	0600(type)
OSI	fe(dlsap)
FNA	80(dlsap)

- source address

フィルタリングの対象とするパケットの送信元のIPアドレスを記入します。"*" (アスタリスク) を記入した場合は、すべての送信元アドレスが対象となります。

設定範囲： xxx.xxx.xxx.xxxの形式、または*(すべてのIPアドレス)

導入時の設定： *(すべてのIPアドレス)

- source mask

「source address」に対するマスクパターンを記入します。

設定範囲： xxx.xxx.xxx.xxxの形式

導入時の設定： 255.255.255.255

「source mask」は上記の「source address」と組み合わせて設定することによって、複数のIPアドレスを同時に指定することができます。ただし、「source address」で"*"を記入した場合には、「source mask」を記入する必要はありません。
 ここでのマスクパターンはサブネットマスクとは異なり、クラスにこだわらずに設定が可能です。表3-3に例を示します。

表3-3 「source address」と「source mask」の組み合わせ例

source address	source mask	フィルタリングの適用されるIPアドレス
172.16.1.1	255.255.255.255	172.16.1.1のみ
172.17.0.0	255.255.0.0	172.17.0.0 ~ 172.17.255.255の全てのIPアドレス
0.0.0.1	0.0.0.255	XXX.XXX.XXX.1の形式のIPアドレス

- source port(A)

フィルタリングの対象とするパケットがTCPあるいはUDPの場合、送信元ポートを記入します。ポート番号は範囲指定で設定する必要があります。ここでは、送信元フィルタリングの対象となるポートの最小ポート番号を記入します。

設定範囲： 0 ~ 65535

導入時の設定： 0



メモ：TCPやUDPで使用されるポート番号は、TCPやUDPより上位に位置する各プログラム(プロセス)の識別子のことをさします。IPアドレスとポート番号の組み合わせで、データを送信するプロセスが正確に決定されます。ポート番号には、統一的に割り当てられている番号(ウエルノウンポート番号)と、動的に割り当てられる番号の2種類があります。ウエルノウンポート番号の例を表3-4にまとめます。

表3-4 ウェルノウンポート番号

ポート番号	種別	ポート番号	種別
0(UDP/TCP)	Reserved	25(TCP)	SMTP
5(TCP)	Remote Job Entry	37(UDP)	Time
7(UDP/TCP)	Echo	42(UDP)	Host Name Server
9(UDP/TCP)	Discard	43(UDP)	NICNAME (WhoIs)
11(UDP/TCP)	Active Users	53(UDP)	Domain Name Server
13(UDP/TCP)	Daytime	69(UDP)	Trivial File Transfer
15(UDP/TCP)	Who is up or NETSTAT	79(TCP)	Finger (Name)
17(UDP/TCP)	Quote of the Day	95(TCP)	SUPDUP
19(UDP/TCP)	Character Generator	101(TCP)	NIC Host Name Server
21(TCP)	File Transfer (Control)		
23(TCP)	Telnet		

- source port(B)
送信元フィルタリングの対象となるポートの最大ポート番号を記入します。
設定範囲： 「source port(A)」の値 ~ 65535
導入時の設定： 65535



メモ： source port(A), source port(B)は，以下の関係を満たすように記入してください。
0 source port(A) source port(B) 65535



メモ： 1つのポートのみをフィルタリングの対象にする場合は，source port(A)およびsource port(B)に同じポート番号を記入してください。
(例) TELNETポートのみをフィルタリングの対象にする
source port(A) = 23, source port(B) = 23

- destination address
フィルタリングの対象とするパケットの宛先のIPアドレスを記入します。"*" (アスタリスク) を記入した場合はすべての宛先アドレスが対象となります。
設定範囲： xxx.xxx.xxx.xxxの形式，または*(すべてのIPアドレス)
導入時の設定： *(すべてのIPアドレス)
- destination mask
「destination address」に対するマスクパターンを記入します。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： 255.255.255.255

「destination mask」は上記の「destination address」と組み合わせて設定することによって、複数のIPアドレスを同時に指定することができます。ただし、「destination address」で"*"を記入した場合には、「destination mask」を記入する必要はありません。ここでのマスクパターンとアドレスの関係は「source mask」と同じです。

- destination port(A)
宛先フィルタリングの対象となるポートの最小ポート番号を0から65535の範囲の10進数で記入します。
設定範囲： 0 ~ 65535
導入時の設定： 0
- destination port(B)
宛先フィルタリングの対象となるポートの最大ポート番号を記入します。
設定範囲： 「destination port(A)」の値 ~ 65535
導入時の設定： 65535



メモ： destination port(A), destination port(B)は、以下の関係を満たすように記入してください。
0 destination port(A) destination port(B) 65535



メモ： 1つのポートのみをフィルタリングの対象にする場合は、source port(A)およびsource port(B)に同じポート番号を記入してください。

- receive interface
上記で指定したパケットの受信インタフェースを、LANとWAN回線のなかで指定します(複数選択可)。上記で指定したパケットはここで指定したインタフェースから受信した場合のみ対象となります。
設定範囲： LAN, 「routing interface」で選択されたグループもしくはチャンネル
導入時の設定： LAN, 「routing interface」で選択されたグループもしくはチャンネル
- send interface
上記で指定したパケットの中継を許可する送信インタフェースを、LANとWAN回線のなかで指定します(複数選択可)。
設定範囲： LAN, 「routing interface」で選択されたグループもしくはチャンネル
導入時の設定： LAN, 「routing interface」で選択されたグループもしくはチャンネル



メモ： 「receive interface」および「send interface」では、グループに属するチャンネルの指定はできません。

- mode
指定したパケットに対する応答パケットをフィルタリングの対象とする場合は、「full」を指定します。指定したパケットに対する応答パケットをフィルタリングの対象としない場合は、「half」を指定します。
設定範囲： 1:full (応答パケットを対象とする)
2:half (応答パケットを対象としない)
導入時の設定： 1:full



メモ：TCP/IPで広く利用されているクライアント - サーバ間の通信では、送信したパケットに対する応答パケットが必ず存在します。特定の相手との通信全体をフィルタリング対象とする場合には、送信と受信の両方のパケットを同時に指定する必要があります。ここで「mode」を「full」と選択することで、1つのエントリで送信と受信の両方のパケットを指定することができます。



メモ：IPパケットフィルタリングは、最大128エントリまで設定が可能です。本ワークシートを必要枚数コピーしてください。

3.2.13 ワークシート「IPXルーティング編」

IPXルーティング編のワークシートの形式と、記入の手順を図3-16に示します。

ワークシート「IPXルーティング編」

router name

LAN 1

interface	IPX アドレス
ethernet 0	XXXXXXXX.XX.X
ethernet 1	XXXXXXXX.XX.X
ethernet 2	XXXXXXXX.XX.X
ethernet 3	XXXXXXXX.XX.X
ethernet 4	XXXXXXXX.XX.X
ethernet 5	XXXXXXXX.XX.X
ethernet 6	XXXXXXXX.XX.X
ethernet 7	XXXXXXXX.XX.X
ethernet 8	XXXXXXXX.XX.X
ethernet 9	XXXXXXXX.XX.X
ethernet 10	XXXXXXXX.XX.X
ethernet 11	XXXXXXXX.XX.X
ethernet 12	XXXXXXXX.XX.X
ethernet 13	XXXXXXXX.XX.X
ethernet 14	XXXXXXXX.XX.X
ethernet 15	XXXXXXXX.XX.X

LAN 2

interface	IPX アドレス	interface	IPX アドレス
ethernet 0	XXXXXXXX.XX.X	ethernet 0	XXXXXXXX.XX.X
ethernet 1	XXXXXXXX.XX.X	ethernet 1	XXXXXXXX.XX.X
ethernet 2	XXXXXXXX.XX.X	ethernet 2	XXXXXXXX.XX.X
ethernet 3	XXXXXXXX.XX.X	ethernet 3	XXXXXXXX.XX.X
ethernet 4	XXXXXXXX.XX.X	ethernet 4	XXXXXXXX.XX.X
ethernet 5	XXXXXXXX.XX.X	ethernet 5	XXXXXXXX.XX.X
ethernet 6	XXXXXXXX.XX.X	ethernet 6	XXXXXXXX.XX.X
ethernet 7	XXXXXXXX.XX.X	ethernet 7	XXXXXXXX.XX.X
ethernet 8	XXXXXXXX.XX.X	ethernet 8	XXXXXXXX.XX.X
ethernet 9	XXXXXXXX.XX.X	ethernet 9	XXXXXXXX.XX.X
ethernet 10	XXXXXXXX.XX.X	ethernet 10	XXXXXXXX.XX.X
ethernet 11	XXXXXXXX.XX.X	ethernet 11	XXXXXXXX.XX.X
ethernet 12	XXXXXXXX.XX.X	ethernet 12	XXXXXXXX.XX.X
ethernet 13	XXXXXXXX.XX.X	ethernet 13	XXXXXXXX.XX.X
ethernet 14	XXXXXXXX.XX.X	ethernet 14	XXXXXXXX.XX.X
ethernet 15	XXXXXXXX.XX.X	ethernet 15	XXXXXXXX.XX.X

LAN 3

interface	IPX アドレス	interface	IPX アドレス
ethernet 0	XXXXXXXX.XX.X	ethernet 0	XXXXXXXX.XX.X
ethernet 1	XXXXXXXX.XX.X	ethernet 1	XXXXXXXX.XX.X
ethernet 2	XXXXXXXX.XX.X	ethernet 2	XXXXXXXX.XX.X
ethernet 3	XXXXXXXX.XX.X	ethernet 3	XXXXXXXX.XX.X
ethernet 4	XXXXXXXX.XX.X	ethernet 4	XXXXXXXX.XX.X
ethernet 5	XXXXXXXX.XX.X	ethernet 5	XXXXXXXX.XX.X
ethernet 6	XXXXXXXX.XX.X	ethernet 6	XXXXXXXX.XX.X
ethernet 7	XXXXXXXX.XX.X	ethernet 7	XXXXXXXX.XX.X
ethernet 8	XXXXXXXX.XX.X	ethernet 8	XXXXXXXX.XX.X
ethernet 9	XXXXXXXX.XX.X	ethernet 9	XXXXXXXX.XX.X
ethernet 10	XXXXXXXX.XX.X	ethernet 10	XXXXXXXX.XX.X
ethernet 11	XXXXXXXX.XX.X	ethernet 11	XXXXXXXX.XX.X
ethernet 12	XXXXXXXX.XX.X	ethernet 12	XXXXXXXX.XX.X
ethernet 13	XXXXXXXX.XX.X	ethernet 13	XXXXXXXX.XX.X
ethernet 14	XXXXXXXX.XX.X	ethernet 14	XXXXXXXX.XX.X
ethernet 15	XXXXXXXX.XX.X	ethernet 15	XXXXXXXX.XX.X

Filtering

Filtering	Yes	No
-----------	-----	----

ワークシート「IPXルーティング編」の記入方法は、以下の通りです。記入するワークシートは、必ずしもこの順番で記入してください。

(1) 装置のルータ名を記入する

(2) 各インターフェースのIPXアドレスを記入する。

(3) フィルタリングを行う／行わないを選択する。

図3-16 IPXルーティング編の形式と記入の手順

(1) 装置のルータ名を記入する。

- router name

IPXルータの名称を記入します。この項目は省略可能です。

設定範囲： 最大47文字の英数字

導入時の設定： 自ホスト名（「3.2.1 ワークシート「基本設定編」」）

(2) 各インタフェースのIPXアドレスを記入する。

始めに、LANインタフェースの項目の記入を行います。

- network NO
LANインタフェースに接続されるネットワークのネットワーク番号を記入します。
設定範囲： 8桁の16進数
導入時の設定： 00000000

- frame type
LANインタフェースに接続されるネットワークで使用するMACフレームのタイプを選択します。
設定範囲： 1:ETHERNET_II
2:ETHERNET_802.3
3:ETHERNET_802.2
4:ETHERNET_SNAP
導入時の設定： 2:ETHERNET_802.3



注意：「frame type」の記入は同一ネットワーク上にNetWareサーバ、クライアントが接続される場合、サーバ、クライアントと同じMACフレームのタイプを選択する必要があります。MACフレームのタイプが異なっている場合、通信は不能です。

- ticks
LANインタフェースの「ticks」値を記入します。LANインタフェースの場合、1を推奨値としています。
設定範囲： 1 ~ 65535
導入時の設定： 1



メモ：IPXにおける「ticks」とは、該当するネットワークに到達する時間を示します。「1tick」は約1/18秒です。本装置は、該当するネットワークに到達するルートがいくつか存在する場合、「ticks値」が1番小さなルートを選択します。

次に、WAN回線インタフェース(HSDまたはISDN)の項目の記入を行います。

- routing interface
ISDN選択時には、ルーティングに使用するインタフェースを選択します。IPXルーティングを行うグループもしくはチャンネルを記入します。（実際の設定では、IPXルーティングを行うかどうかの問い合わせがあります。行うのであれば「y」を、行わないのであれば「n」を選択します。）
設定範囲： 「WAN topology」で「Usual」または「Usual/Load split」を選択したグループもしくはチャンネル
導入時の設定： なし

- network NO
WAN回線インタフェースに接続されるネットワークのネットワーク番号を記入します。
設定範囲： 8桁の16進数
導入時の設定： 00000000
- node ID.
特別な値の記入は不要です（0000.0000.0000と記入されています）。0000.0000.0000以外の値は、将来の拡張用です。
設定範囲： xxxx.xxxx.xxxxの形式(16進数)
導入時の設定： 0000.0000.0000
- ticks
WAN回線インタフェースの「ticks」値を記入します。
設定範囲： 1 ~ 65535
導入時の設定： 1



メモ：WAN回線インタフェースの「ticks」値として、回線スピード毎の推奨値を表3-5にまとめます。

表3-5 WAN回線の推奨「ticks」値

回線種別	HSD		ISDN
回線 スピード	64Kbps	128Kbps	64Kbps
推奨tick値 [ticks]	18	11	85

(3) フィルタリングを行う / 行わないを選択する。

- IPX filtering
IPXパケットのフィルタリング機能の使用の有無を記入します。フィルタリング機能を使用しない場合は、すべてのIPXパケットを中継します。
設定範囲： 1:use (使用する)
2:not use (使用しない)
導入時の設定： 1:use

このシートの記入はこれで終了です。

3.2.14 ワークシート「IPXリモートターゲット編」

IPXリモートターゲット編の、ワークシートの形式と記入の手順を図3-17に示します。

ワークシート「IPXリモートターゲット編」

	MINC	MISC		MINC	MISC
1			11		
2			12		
3			13		
4			14		
5			15		
6			16		
7			17		
8			18		
9			19		
10			20		
11			21		
12			22		
13			23		
14			24		
15			25		
16			26		
17			27		
18			28		
19			29		
20			30		

IPXリモートターゲットテーブルは最大80エントリーを扱えます。既定するエントリーが40エントリーより多い場合は、必要に応じてコピーしてください。

(1) IPXのISDNリモートターゲットを記入する。

図3-17 IPXリモートターゲット編の形式と記入の手順

(1) IPXのISDNリモートターゲットを記入する。

ISDNを選択した場合でISDNで複数の相手と接続する（ 3.2.4(2) ）場合、宛先のIPアドレスとそれに対応するISDNリモートターゲットのテーブルを記入します。ISDNの接続相手を固定して使用する場合、記入の必要はありません。エントリーは最大80件記入できます。1エントリーに関する設定項目を以下に示します。

- address
宛先のIPXアドレスを記入します。
設定範囲： 12桁の16進数
導入時の設定： なし

- target

宛先のIPXアドレスに対応した，ISDNリモートターゲットを記入します．

設定範囲： ISDNリモートターゲット（最大80エントリから1エントリ選択）

導入時の設定： なし



メモ：IPXリモートターゲットテーブルは，最大80エントリ設定が可能です．本ワークシートを必要枚数コピーしてください．

このシートの記入はこれで終了です．

3.2.15 ワークシート「IPXパケットフィルタリング編」

IPXパケットフィルタリング編のワークシートの形式と、記入の手順を図3-18に示します。

ワークシート「IPXパケットフィルタリング編」

Protocol: Lan 2 over 700000 4 000000 0 00 0 0000 1 0000					
IPV4	local number	network number	mask	protocol	protocol
Destination	local number	network number	mask	protocol	protocol
receive interface					action
read data size					L:POL 0 0 0 0 0 0

Protocol: Lan 2 over 700000 4 000000 0 00 0 0000 1 0000					
IPV4	local number	network number	mask	protocol	protocol
Destination	local number	network number	mask	protocol	protocol
receive interface					action
read data size					L:POL 0 0 0 0 0 0

Protocol: Lan 2 over 700000 4 000000 0 00 0 0000 1 0000					
IPV4	local number	network number	mask	protocol	protocol
Destination	local number	network number	mask	protocol	protocol
receive interface					action
read data size					L:POL 0 0 0 0 0 0

Protocol: Lan 2 over 700000 4 000000 0 00 0 0000 1 0000					
IPV4	local number	network number	mask	protocol	protocol
Destination	local number	network number	mask	protocol	protocol
receive interface					action
read data size					L:POL 0 0 0 0 0 0

データは最大128エントリ登録可能です。既定するデータがエントリを超過した場合、自動的に
コピーしていただきます。

(1) IPXパケットフィルタリングテーブルを記入する。

図3-18 IPXパケットフィルタリング編の形式と記入の手順

(1) IPXパケットフィルタリングテーブルを記入する。

IPXパケットフィルタリングテーブルには、最大128エントリの登録が可能です。1つのエントリに関する記入項目を以下に示します。

- protocol

フィルタリングの対象とするパケットのプロトコルを選択します。

設定範囲： 1:ncp (NCPプロトコル)
 2:spx (SPXプロトコル)
 3:netbios (NetBIOSプロトコル)
 4:unknown (unknownとして予約されているプロトコル)
 5:all (すべてのプロトコル)
 6:other (上記のプロトコル以外のプロトコルを0～ffの範囲
 の16進で 指定)
 導入時の設定： 4:unknown

「other」を選択した場合には、プロトコル番号を16進数で記入します。NCP、SPX、NetBIOS以外の主なプロトコル番号を表3-6に示します。

表3-6 IPXのプロトコル番号例

プロトコル	設定値(16進数)
Routing Information Protocol(RIP)	01
Service Advertising Protocol(SAP)	04

- source host number

フィルタリングの対象とするパケットの送信元ホストIDを16進数で記入します。"*" (アスタリスク) 記入した場合はすべての送信元ホストが対象となります。

設定範囲： 12桁の16進数，あるいは*(すべてのホストID)

導入時の設定： *(すべてのホストID)

- source network number

フィルタリングの対象とする送信元のネットワーク番号を16進数で記入します。"*" (アスタリスク) を記入した場合はすべての送信元ネットワークが対象となります。

設定範囲： 8桁の16進数，あるいは*(すべてのネットワーク番号)

導入時の設定： *(すべてのネットワーク番号)

- source mask

「source network number」に対するマスクパターンを記入します。

設定範囲： 8桁の16進数

導入時の設定： ffffffff

「source mask」は上記の「source network number」と組み合わせて設定することによって、複数のネットワーク番号を同時に指定することができます。ただし、「source network number」で"*" (アスタリスク) を記入した場合には、「source mask」を記入する必要はありません。表3-7に「source mask」の例を示します。

表3-7 「source network number」と「source mask」の組み合わせ例

source network number	source mask	フィルタリングの適用されるネットワーク番号
00000001	ffffff	00000001のみ
00010000	ffff0000	00010000 ~ 0001ffffの全てのネットワーク番号
00000001	000000ff	XXXXXX01の形式のネットワーク番号

- source sock(A)
 フィルタリングの対象とするパケットの送信元ソケット番号を記入します。ソケット番号は範囲指定で設定する必要があります。ここでは、フィルタリングの対象となる送信元ソケットの最小ソケット番号を記入します。
 設定範囲： 0000 ~ ffff (16進数)
 導入時の設定： 0000



メモ：IPXで使用されるソケット番号は、IPXより上位に位置する各プログラム(プロセス)の識別子のことをさします。ソケット番号には、統一的に割り当てられている番号(ウエルノウンソケット番号)と、動的に割り当てられる番号の2種類があります。ソケット番号の例を表3-8にまとめます。

表3-8 IPXのソケット番号

ソケットプロセス	ソケット番号(16進)
NetWare Core Protocol (NCP) Process	0451
Service Advertising Protocol (SAP) Process	0452
Routing Information Protocol (RIP) Process	0453
Novell NetBIOS Process	0455
Diagnostics Process	0456
動的に割り当てられるソケット	4000 ~ 7fff

- source sock(B)
 フィルタリングの対象となる送信元ソケットの最大ソケット番号を指定します。
 設定範囲： 「source sock(A)」の値 ~ ffff (16進数)
 導入時の設定： ffff



メモ：source sock(A), source sock(B)は、以下の関係を満たすように記入してください。
 0 source sock(A) source sock(B) ffff



メモ：1つのポートのみをフィルタリングの対象にする場合は、source sock(A)およびsource sock(B)に同じソケット番号を記入してください。
 (例) NCPのみをフィルタリングの対象にする
 source port(A) = 451, source port(B) = 451

- destination host number
フィルタリングの対象とするパケットの宛先ホストIDを16進数で記入します。"*" (アスタリスク) を記入した場合はすべての送信元ネットワークが対象となります。
設定範囲： 12桁の16進数, あるいは*(すべてのホストID)
導入時の設定： *(すべてのホストID)
 - destination network number
フィルタリングの対象とするパケットの宛先ネットワーク番号を16進数で記入します。
"*" (アスタリスク) を記入した場合はすべてのネットワーク番号が対象となります
設定範囲： 8桁の16進数, あるいは*(すべてのネットワーク番号)
導入時の設定： *(すべてのネットワーク番号)
 - destination mask
「destination network number」に対するマスクパターンを記入します。マスクの適用方法は「source mask」と同じです。
設定範囲： 8桁の16進数
導入時の設定： ffffffff
 - destination sock(A)
フィルタリングの対象となる宛先ソケットの最小ソケット番号を指定します。
設定範囲： 0000 ~ ffff (16進数)
導入時の設定： 0000
 - destination sock(B)
フィルタリングの対象となる宛先ソケットの最大ソケット番号を指定します。
設定範囲： 「destination sock(A)」の値 ~ ffff (16進数)
導入時の設定： ffff
-  メモ： source sock(A), source sock(B)は、以下の関係を満たすように記入してください。
0 source sock(A) source sock(B) ffff
-  メモ： 1つのポートのみをフィルタリングの対象にする場合は、source sock(A)およびsource sock(B)に同じソケット番号を記入してください。
- receive interface
上記で指定したパケットの受信インタフェースを、LANとWAN回線のなかで指定します(複数選択可)。上記で指定したパケットはここで指定したインタフェースから受信した場合のみ対象となります。
設定範囲： LAN, 「routing interface」で選択されたグループもしくはチャネル
導入時の設定： LAN, 「routing interface」で選択されたグループもしくはチャネル

- send interface

上記で指定したパケットの中継を許可する送信インタフェースを、LANとWAN回線のなかで指定します(複数選択可)。

設定範囲： LAN, 「routing interface」で選択されたグループもしくはチャンネル

導入時の設定： LAN, 「routing interface」で選択されたグループもしくはチャンネル

- mode

指定したパケットに対する応答パケットをフィルタリングの対象とする場合は、「full」を指定します。指定したパケットに対する応答パケットをフィルタリングの対象としない場合は、「half」を指定します。

設定範囲： 1:full (応答パケットを対象とする)

2:half (応答パケットを対象としない)

導入時の設定： 1:full



メモ：IPXで広く利用されているクライアント - サーバ間の通信では、送信したパケットに対する応答パケットが必ず存在します。特定の相手との通信全体をフィルタリング対象とする場合には、送信と受信の両方のパケットを同時に指定する必要があります。この項目で「mode」を「full」と指定することで、1つのエントリで送信と受信の両方のパケットを指定することができます。



メモ：IPXパケットフィルタリングは、最大128個まで設定が可能です。ワークシート「IPXパケットフィルタリング編」を必要枚数コピーしてください。

このシートの記入はこれで終了です。

3.2.16 ワークシート「IPXスタティックルーティング編」

IPXスタティックルーティング編のワークシートの形式と、記入の手順を図3-19に示します。

ワークシート「IPXスタティックルーティング編」

destination host	width	time delay	network address IP	network locID

テーブル形式のエントリを複数登録できます。既定のテーブルのエントリより多くの場合は、ご利用ください。

図3-19 IPXスタティックルーティング編の形式と記入の手順

(1) IPXスタティックルーティングテーブルを記入する。

IPXスタティックルーティングテーブルには、最大256エントリの登録が可能です。1つのエントリに関する記入項目を以下に示します。

- destination network

スタティックルーティング情報の宛先IPXネットワーク番号を記入します。接続先がサーバの場合は、ここには接続するサーバのインターナルネットワーク(内部ネットワーク)のネットワーク番号を記入します。

設定範囲： 8桁の16進数

導入時の設定： なし

- metric

このエントリをRIPで送信する場合のメトリック値を記入します。メトリック値を16とすると、このエントリに記入してあるネットワークに関するルート情報を送信しません（設定していない場合と同じになります）。

設定範囲： 1 ~ 16

導入時の設定： 16 (到達不能)

メトリック値を利用して、記入中のスタティックルートに重みをつけることが可能となります。重みのつけ方は、次に示す「tick」値の場合と同じです。

- time ticks

「destination network」までの「ticks」値を記入します。

設定範囲： 1 ~ 65535

導入時の設定： 15

「ticks」値は、「destination network」に到達するために経由する時間で、1tick=1/18秒です。ただし、「ticks」値を実際の時間と異なる値として記入することで、記入中のスタティックルートに重みをつけることが可能となります。次に例を示します。

- ・ 「ticks」値を実際の値より大きくする場合

この場合、装置はこのルートを実際より到達が困難であると判断します。例えば、回線の課金が高いのでそのルートはなるべく使用したくない等の場合に、このような記入を行います。

- ・ 「ticks」値を実際の値より小さくする場合

この場合、装置はこのルートを実際より到達が容易であると判断します。例えば、回線の課金が安いのでそのルートをなるべく使用したい等の場合に、このような記入を行います。



メモ：IPXにおけるメトリック値と「ticks」値について

IPXにおけるメトリック値と「ticks」値は、両方とも同じ宛先のネットワークに対するルートが複数存在した場合に、最適なルートを選択するために使用される値です。本装置は、まず「ticks」値の小さいルートを選択します。もし「ticks」値の等しいルートが複数存在するならば、装置はメトリック値の小さいルートを選択します。更にメトリック値も等しい場合、装置は先に登録されたルートを選択します。

- gateway network NO

中継先ゲートウェイのネットワーク番号を記入します。

設定範囲： 8桁の16進数

導入時の設定： なし

- gateway host ID
中継先ゲートウェイのホストIDを記入します。
設定範囲： 12桁の16進数
導入時の設定： なし



メモ：最大256エントリ設定できます。必要な枚数コピーして使用してください。

このシートの記入はこれで終了です。

3.2.17 ワークシート「IPXスタティックSAP編」

IPXスタティックSAP編のワークシートの形式と、記入の手順を図3-20に示します。

ワークシート「IPXスタティックSAP編」

server name	network.library	local address	remote address	remote server
server1	192.168.1.1	192.168.1.1	192.168.1.2	server2
server2	192.168.1.2	192.168.1.2	192.168.1.1	server1
server3				

server name	network.library	local address	remote address	remote server
server1	192.168.1.1	192.168.1.1	192.168.1.2	server2
server2	192.168.1.2	192.168.1.2	192.168.1.1	server1
server3				

server name	network.library	local address	remote address	remote server
server1	192.168.1.1	192.168.1.1	192.168.1.2	server2
server2	192.168.1.2	192.168.1.2	192.168.1.1	server1
server3				

server name	network.library	local address	remote address	remote server
server1	192.168.1.1	192.168.1.1	192.168.1.2	server2
server2	192.168.1.2	192.168.1.2	192.168.1.1	server1
server3				

テーブルの最大256エントリを登録できます。 既定するテーブルのエントリより多くの場合は、自動的に
コピーしていただきます。

(1) IPXスタティックSAP
テーブルを記入する。

図3-20 IPXスタティックSAP編の形式と記入の手順



メモ：WAN回線にHSDを使用している場合は、このシートの記入は必要ありません。

(1) IPXスタティックSAPテーブルを記入する。

IPXスタティックSAPテーブルには、最大256エントリの登録が可能です。1つのエントリに関する記入項目を以下に示します。

- server name
サーバのサーバ名を設定します。
設定範囲： 最大47文字の英数字
導入時の設定： なし

- network address
サーバのインターナルネットワーク番号を設定します。
設定範囲： 8桁の16進数
導入時の設定： なし

- host address
サーバのホストIDを設定します。ファイルサーバの場合は"000000000001"と記入します。
設定範囲： 12桁の16進数
導入時の設定： なし

- socket
サーバのソケット番号を設定します。ファイルサーバの場合は"0451"と記入します。
設定範囲： 4桁の16進数
導入時の設定： なし

- service type
フィルタリングの対象とするSAP情報のサービスタイプを設定します。
設定範囲： 1 : print queue
2 : file server
3 : job server
4 : print server
5 : archive server
6 : remote bridge server
7 : advertising print server
8 : other (16進4桁で任意のサービスタイプ番号を入力する)
導入時の設定： なし

- hop to server
サーバまでのメトリック値を設定します。
設定範囲： 1 ~ 16
導入時の設定： 16



メモ：IPXスタティックSAPテーブルは、最大256エントリ設定が可能です。本ワークシートを必要枚数コピーしてください。

このシートの記入はこれで終了です。

3.2.18 ワークシート「AppleTalkルーティング編」

AppleTalkルーティング編のワークシートの形式と、記入の手順を図3-21に示します。

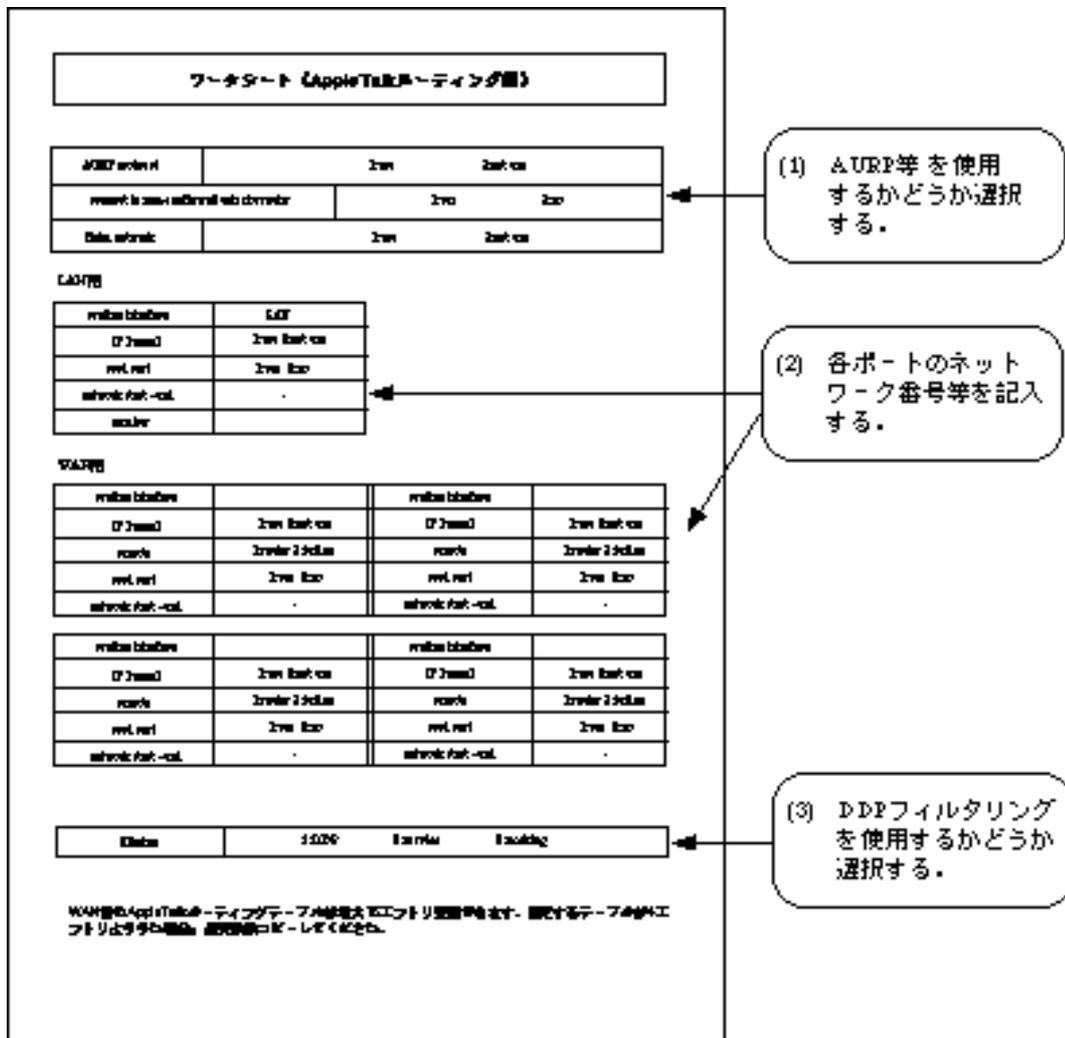


図3-21 AppleTalkルーティング編の形式と記入の手順

(1) AURP等を使用するかどうか選択する。

AppleTalkネットワークを用いた大規模なネットワークを構築する場合、AURPを動作します。

- AURP protocol
AURPを動作するかどうか選択します。
設定範囲： 1:use
2:not use
導入時の設定： 1:use

- connect to non-configured exterior router
「IP Tunneling exterior router」テーブル（ 3.2.20 ワークシート「外部AppleTalkルー
タ編」）または「remote target」に設定されていない外部ルー
タとAURPの接続を行うか
どうかを選択します。
設定範囲： 1:yes
2:no
導入時の設定： 2:no

- Extra network
Extra network（発呼用ネットワーク動作制御）を使用するかどうか
を選択します。ISDN使用時に、接続方法を「time + traffic」（指
定された時間内の中継データによる自動発呼）にした場合は、
必ず「use」にします。
設定範囲： 1:use
2:not use
導入時の設定： 2:not use

(2) 各ポートのネットワーク番号等を記入する。

始めに、LANインタフェースの項目の記入を行います。

- IP Tunnel
IP Tunnel機能を使用するかどうかを選択します。「IP routing」を「use」にしたときのみ
設定可能です。
設定範囲： 1:use
2:not use
導入時の設定： 2:not use

- seed port
LANポートに接続されるネットワークで本装置をシードルー
タとして運用するかどうか
を選択します。
設定範囲： 1:yes
2:no
導入時の設定： 1:yes



注意： AppleTalkのネットワークを構築する場合、1つのネットワークにシードルー
タとして運用され
ているルー
タが1台以上必要です。

すでにLAN側にシードルー
タが存在するネットワークに本装置をシードルー
タとして立ちあげ
た場合で、そのシードルー
タとゾーンリストおよびネットワーク番号範囲が異なる場合、本装置
はノンシードルー
タとして運用されます。

- network start - end

LANポートに接続されるネットワークのネットワーク番号範囲を記入します。「seed port」で「no」を選択した場合は、ネットワーク番号範囲の設定は必要ありません。また、ネットワーク番号範囲の終わりは、ネットワーク番号範囲の始めと等しいか大きい値でなければいけません。

設定範囲： start : 1 ~ 65279

end : 1 ~ 65279

導入時の設定： start : 1

end : 1

- number

LANポートに接続されるネットワークのネットワーク番号を記入します。ただし、ネットワーク番号範囲内にある番号を割り当てます。

設定範囲： 1 ~ 65279

導入時の設定： 1

次に、WAN回線ポート（HSD、ISDN）に接続されるネットワークの項目を記入します。

- routing interface

ISDN選択時には、ルーティングに使用するインタフェースを選択します。AppleTalkルーティングを行うグループもしくはチャネルを記入します。（実際の設定では、AppleTalkルーティングを行うかどうかの問い合わせがあります。行うのであれば「y」を、行わないのであれば「n」を選択します。）

設定範囲： 「WAN topology」で「Usual」または「Usual/Load split」を選択したグループもしくはチャネル

導入時の設定： なし

- IP Tunnel

IP Tunnel機能を使用するかどうかを選択します。「IP routing」を「use」にしたときのみ設定可能です。

設定範囲： 1:use

2:not use

導入時の設定： 2:not use



注意：HSD選択時に「IP Tunneling」を使用する場合は、そのポートをrouting interfaceに指定しないでください。

- remote

WAN回線で接続される相手の装置形態を選択します。

設定範囲： 1:router

2:bridge

導入時の設定： 1:router



注意：「remote」で「router」が選択された場合、「3.2.22 ワークシート「AppleTalkゾーンリスト編」」での設定は必要ありません。

- seed port

WANポートに接続されるネットワークで本装置をシードルータとして運用するかどうかを選択します。この項目は、「remote」で「bridge」を選択したときのみ記入します。

設定範囲： 1:yes
2:no

導入時の設定： 1:yes



注意：AppleTalkのネットワークを構築する場合、1つのネットワークにシードルータとして運用されているルータが1台以上必要です。

すでにLAN側にシードルータが存在するネットワークに本装置をシードルータとして立ちあげた場合で、そのシードルータとゾーンリストおよびネットワーク番号範囲が異なる場合、本装置はノンシードルータとして運用されます。

- network start - end

WANポートに接続されるネットワークのネットワーク番号範囲を記入します。「seed port」で「no」を選択した場合、または「remote」で「router」を選択した場合は、ネットワーク番号範囲の設定は必要ありません。また、ネットワーク番号範囲の終わりは、ネットワーク番号範囲の始めと等しいか大きい値でなければいけません。

設定範囲： start : 1 ~ 65279
end : 1 ~ 65279

導入時の設定： start : 1
end : 1

(3) DDPフィルタリングを使用するかどうか選択する。

- Select the filtering

DDPのフィルタリングを行う場合「DDP」を、サービスのフィルタリングを行う場合「service」を選択します。この設定は、複数選択することが可能です。

設定範囲： 1:DDP
2:service
3:nothing

導入時の設定： 3:nothing

このシートの記入はこれで終了です。

3.2.19 ワークシート「AppleTalkリモートターゲット編」

AppleTalkリモートターゲット編の、ワークシートの形式と記入の手順を図3-22に示します。

	minnc	nsgc		minnc	nsgc
1			11		
2			12		
3			13		
4			14		
5			15		
6			16		
7			17		
8			18		
9			19		
10			20		
11			21		
12			22		
13			23		
14			24		
15			25		
16			26		
17			27		
18			28		
19			29		
20			30		

AppleTalkリモートターゲットテーブルは最大8000エントリを登録できます。既定するエントリ数が4000エントリより多い場合は、設定範囲を拡張してください。

図3-22 AppleTalkリモートターゲット編の形式と記入の手順

(1) AppleTalkのISDNリモートターゲットを記入する。

ISDNを選択した場合でISDNで複数の相手と接続する（ 3.2.4(2)）場合、宛先のネットワーク番号とそれに対応するISDNリモートターゲットのテーブルを記入します。ISDNの接続相手を固定して使用する場合、記入の必要はありません。エントリは最大80件記入できます。1エントリに関する設定項目を以下に示します。

- address

宛先のネットワーク番号を記入します。この項目はAURPを使用する場合記入する必要はありません。

設定範囲： 1 ~ 65279

導入時の設定： なし

- target index

宛先のネットワーク番号に対応した、ISDNリモートターゲットを記入します。

設定範囲： ISDNリモートターゲット（最大80エントリから1エントリ選択）

導入時の設定： なし



メモ：AppleTalkリモートターゲットテーブルは、最大80エントリ設定が可能です。本ワークシートを必要枚数コピーしてください。

このシートの記入はこれで終了です。

- port

上記で指定した相手と接続するポートを選択します。WAN回線に関しては、「基本設定編」のWAN回線動作モードで選択した回線が設定範囲になります。

設定範囲： LAN, 「IP Tunnel」で「use」を選択されたグループもしくはチャンネル
導入時の設定： なし

このシートの記入はこれで終了です。

3.2.21 ワークシート「AppleTalk DDP (forward) フィルタリング編」

AppleTalk DDP (forward) フィルタリング編のワークシートの形式と、記入の手順を図3-24に示します。本装置のDDP (forward) フィルタリング機能では、中継を許可するすべてのパケットをフィルタリングテーブルに設定します。テーブルに設定されていないパケットを受信した場合は廃棄されます。

ワークシート (AppleTalk DDP (forward) フィルタリング編)

Del network #xxx		re network #xxx	
Del network col.		re network col.	
Del network net		re network net	
DDP key	23E74E78a554 21E1F 7:5A7F 4:5A67 8:87E478a1 8:8E7 7:6547 9:13		
net	2540	254E	
network net			
net net			

Del network #xxx		re network #xxx	
Del network col.		re network col.	
Del network net		re network net	
DDP key	23E74E78a554 21E1F 7:5A7F 4:5A67 8:87E478a1 8:8E7 7:6547 9:13		
net	2540	254E	
network net			
net net			

Del network #xxx		re network #xxx	
Del network col.		re network col.	
Del network net		re network net	
DDP key	23E74E78a554 21E1F 7:5A7F 4:5A67 8:87E478a1 8:8E7 7:6547 9:13		
net	2540	254E	
network net			
net net			

Del network #xxx		re network #xxx	
Del network col.		re network col.	
Del network net		re network net	
DDP key	23E74E78a554 21E1F 7:5A7F 4:5A67 8:87E478a1 8:8E7 7:6547 9:13		
net	2540	254E	
network net			
net net			

テーブルは最大400エントリ容量があります。既定するテーブルのエントリより多い場合は、品質低下を
 コピーしていただく。

(1) フィルタリング
 テーブルを記入する。

図3-24 AppleTalk DDP (forward) フィルタリング編の形式と記入の手順



メモ：「AppleTalkルーティング編」で、「filtering」で「DDP」を選択した場合以外は記入の必要はありません。

(1) フィルタリングテーブルを記入する。

AppleTalk DDP (forward) フィルタリングテーブルには、最大128エントリの登録が可能です。1つのエントリに関する記入項目を以下に示します。

- dst network start
フィルタリングの対象とするパケットの宛先ネットワーク番号範囲の始めを記入します。
設定範囲： 0 ~ 65535
導入時の設定： 0
- dst network end
フィルタリングの対象とするパケットの宛先ネットワーク番号範囲の終わりを記入します。ネットワーク番号範囲の終わりは、ネットワーク番号範囲の始めと等しいか大きい値でなければいけません。
設定範囲： 0 ~ 65535
導入時の設定： 65535
- dst network node
フィルタリングの対象とするパケットの宛先ノードIDを記入します。0はすべてのノードを表します。
設定範囲： 0 ~ 255
導入時の設定： 0
- src network start
フィルタリングの対象とするパケットの送信元ネットワーク番号範囲の始めを記入します。
設定範囲： 0 ~ 65535
導入時の設定： 0
- src network end
フィルタリングの対象とするパケットの送信元ネットワーク番号範囲の終わりを記入します。ネットワーク番号範囲の終わりは、ネットワーク番号範囲の始めと等しいか大きい値でなければいけません。
設定範囲： 0 ~ 65535
導入時の設定： 65535
- src network node
フィルタリングの対象とするパケットの送信元ノードIDを記入します。0はすべてのノードを表します。
設定範囲： 0 ~ 255
導入時の設定： 0

- DDP type
フィルタリングの対象とするパケットのプロトコルを選択します。この項目は複数選択することはできません。

設定範囲： 1:RTMP(Rp/Dt)
2:NBP
3:ATP
4:AEP
5:RTMP(Rq)
6:ZIP
7:ADSP
8:all

導入時の設定： 8:all

- mode
指定したパケットに対する応答パケットをフィルタリングの対象とする場合は、「full」を指定します。指定したパケットに対する応答パケットをフィルタリングの対象としない場合は、「half」を指定します。

設定範囲： 1:full (応答パケットを対象とする)
2:half (応答パケットを対象としない)

導入時の設定： 1:full



メモ：AppleTalkを利用した通信では、送信したパケットに対する応答パケットが存在することがあるため、フィルタリング対象とする場合には両方のパケットを指定する必要があります。「mode」を「full」に指定することで1つのエントリで両方のパケットを指定することができます。

- receive port
上記で指定したパケットの受信ポートを、LANとWAN回線のなかで指定します（複数選択可）。上記で指定したパケットはここで指定したポートから受信した場合のみ対象となります。

設定範囲： LAN (AppleTalk),LAN (IP Tunnel)および「routing interface」で選択されたグループもしくはチャンネル

導入時の設定： LANおよび通常回線として使用する回線

- send port
上記で指定したパケットの中継を許可する送信ポートを、LANとWAN回線のなかで指定します（複数選択可）。

設定範囲： LAN (AppleTalk),LAN (IP Tunnel)および「routing interface」で選択されたグループもしくはチャンネル

導入時の設定： LANおよび通常回線として使用する回線



メモ：AppleTalkパケットフィルタリングは、最大64エントリまで設定が可能です。本ワークシートを必要枚数コピーしてください。

このシートの記入はこれで終了です。

3.2.22 ワークシート「AppleTalkゾーンリスト編」

AppleTalkゾーンリスト編のワークシートの形式と、記入の手順を図3-25に示します。



メモ：AppleTalkゾーンリスト編は、グループもしくはチャンネル毎に必要です。不足する場合は、必要枚数コピーしてください。

The diagram shows a worksheet titled "ワークシート (AppleTalkゾーンリスト編)". At the top, there are two fields: "AppleTalkグループ名" and "チャンネル". Below these is a large table with two columns, each labeled "ゾーン名". To the right of the form, two callout boxes with arrows point to the respective fields:

- (1) グループ名もしくはチャンネルを記入する。
- (2) ゾーン名を記入する。

At the bottom of the worksheet, there is a small note: "ゾーン名はすべて大文字で入力してください。"

図3-25 AppleTalkゾーンリスト編の形式と記入の手順

(1) グループ名もしくはチャンネルを記入する .

設定項目を以下に示します .

- Selecting group/channel
設定を行うグループ (3.2.3 ワークシート「ISDNチャンネルグループ編」で設定したもの) もしくはチャンネル (どのグループにも属さないポートのうち1もしくは2を選択する) を記入します .
設定範囲 : 「WAN topology」で「Usual」, 「Usual/Load split」もしくは「Load split」を選択したグループもしくはチャンネル
導入時の設定 : なし

(2) ゾーン名を記入する .

本装置に接続されるネットワークで本装置をシードルータとして運用する場合ゾーンを設定する必要があります .



注意 : すでにシードルータが存在するネットワークに本装置をシードルータとして立ちあげた場合で、他のシードルータとゾーンリストおよびネットワーク番号範囲が異なる場合、本装置はノンシードルータとして運用されます .

- zone name
ポートに設定するゾーン名を記入します . ゾーン名は最大32文字まで設定ができます . 大文字と小文字の区別はしていません .
設定範囲 : 最大32文字の英数字
導入時の設定 : なし



注意 : " * (アスタリスク) " というゾーン名を設定することはできません .



メモ : ゾーン名はすべてのポート合わせて最大256エン트리, 1ポートでは最大255エン트리まで設定が可能です . 本ワークシートを必要枚数コピーしてください .

- default zone
他のゾーン名が選択されるまで使用されるゾーン名です . ゾーン名を設定する場合、ポート毎に必ず1つのゾーンをデフォルトゾーンとしなければなりません . ゾーン名を1つしか設定しなかった場合は、そのゾーンがデフォルトゾーンになります .
設定範囲 : 1:yes
2:no
導入時の設定 : 2:no

このシートの記入はこれで終了です .

3.2.23 ワークシート「AppleTalkスタティックルーティング編」

AppleTalkスタティックルーティング編のワークシートの形式と、記入の手順を図3-26に示します。

ワークシート「AppleTalkスタティックルーティング編」

dst network start	
dst network end	
type	2:AppleTalk 255.255.255.0:157 address
address network number	
mask 32	
hop	
recall val	

dst network start	
dst network end	
type	2:AppleTalk 255.255.255.0:157 address
address network number	
mask 32	
hop	
recall val	

dst network start	
dst network end	
type	2:AppleTalk 255.255.255.0:157 address
address network number	
mask 32	
hop	
recall val	

dst network start	
dst network end	
type	2:AppleTalk 255.255.255.0:157 address
address network number	
mask 32	
hop	
recall val	

テーブルは最大256エントリを登録可能です。指定するテーブルのエントリは必ずしも同じ値に設定してください。

(1) AppleTalkスタティックルーティングテーブルを記入する。

図3-26 AppleTalkスタティックルーティング編の形式と記入の手順

(1) AppleTalkスタティックルーティングテーブルを記入する。

本装置でAppleTalkデータ中継のための自動接続機能を利用する場合、スタティックルーティングテーブルを設定する必要があります。しかし、「AURP protocol」を「use」にしたときは、自動接続機能を利用する場合でもスタティックルーティングテーブルの設定は必要ありません。AppleTalkスタティックルーティングテーブルには、最大256エントリの登録が可能です。1つのエントリに関する記入項目を以下に示します。

- dst network start
スタティックルーティング情報の宛先ネットワーク番号の始めを記入します。
設定範囲： 1 ~ 65535
導入時の設定： なし

3章 基本設定

- dst network end
スタティックルーティング情報の宛先ネットワーク番号の終わりを記入します。ネットワーク番号範囲の終わりは、ネットワーク番号範囲の始めと等しいか大きい値でなければいけません。
設定範囲： 1 ~ 65535
導入時の設定： 「dst network start」で設定した数値



注意：ネットワーク番号範囲を重なって設定することはできません。

- type
スタティックルーティング情報の中継先ルータのアドレスのタイプを選択します。
「ISDN index」はWAN回線動作モードでISDNを選択し、さらに「AppleTalkリモートターゲット編」で「target」を記入した場合、「IP Address」は「AppleTalkルーティング編」の「IP Tunnel」を「use」にした場合にそれぞれ選択します。
設定範囲： 1:AppleTalk
2:ISDN index
3:IP Address
導入時の設定： なし
- gateway network number
スタティックルーティング情報の中継先ルータのアドレスを記入します。上記の「type」で選択した番号により、設定範囲は異なります。
(AppleTalk選択時)
設定範囲： 0 ~ 65535
導入時の設定： なし
(ISDN index選択時)
設定範囲： ISDNリモートターゲット（最大80エン트리から1エン트리選択）
導入時の設定： なし



メモ：「multi target」を「not use」にした場合は、ISDNリモートターゲットの「target index」の中から1エン트리選択します。

- (IP Address選択時)
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： なし
- node ID
スタティックルーティング情報の中継先ルータの node IDを記入します。上記の「type」で「AppleTalk」を選択したときのみ必要です。
設定範囲： 0 ~ 254
導入時の設定： 0

- hop
スタティックルーティング情報の中継先ルータまでのホップ数を記入します。
設定範囲： 1 ~ 15
導入時の設定： 1

- send port
スタティックルーティング情報の中継先ルータが存在するポートを選択します。上記の「type」で選択した番号により、設定範囲は異なります。WAN回線に関しては、「基本設定編」のWAN回線動作モードで選択した回線が設定範囲になります。
設定範囲： LAN(AppleTalk),LAN(IP Tunnel)および「routing interface」で選択されたグループもしくはチャンネル
導入時の設定： なし



メモ：AppleTalkスタティックルーティングテーブルは、最大128エントリ設定できます。必要な枚数コピーしてください。



注意：AppleTalkスタティックルーティングを使用する場合は、必ず次の「AppleTalkスタティックゾーン編」の記入が必要です。

このシートの記入はこれで終了です。

(1) スタティックゾーンを記入する。

AppleTalkスタティックゾーンテーブルには、すべてのネットワーク合わせて最大128エントリの登録が可能です。1つのエントリに関する記入項目を以下に示します。

- dst network start
スタティックゾーンが所属するルーティング情報の宛先ネットワーク番号の始めを記入します。ワークシート「AppleTalkスタティックルーティング編」に記入されているネットワーク全てに1つ以上のゾーンが必要です。
設定範囲： 0 ~ 65535
導入時の設定： 0

- dst network end
スタティックゾーンが所属するルーティング情報の宛先ネットワーク番号の終わりを記入します。
設定範囲： 0 ~ 65535
導入時の設定： 65535

- zone
スタティックに設定するゾーン名を記入します。ゾーン名は最大32文字まで設定ができます。大文字と小文字の区別はしていません。
設定範囲： 最大32文字の英数字
導入時の設定： なし



注意：” * (アスタリスク) ” というゾーン名を設定することはできません。



メモ：スタティックゾーンテーブルは、最大128エントリ設定が可能です。本ワークシートを必要枚数コピーしてください。

このシートの記入はこれで終了です。

3.2.25 ワークシート「MACアドレスリモートターゲット編」

MACアドレスリモートターゲット編のワークシートの形式と、記入の手順を図3-28に示します。

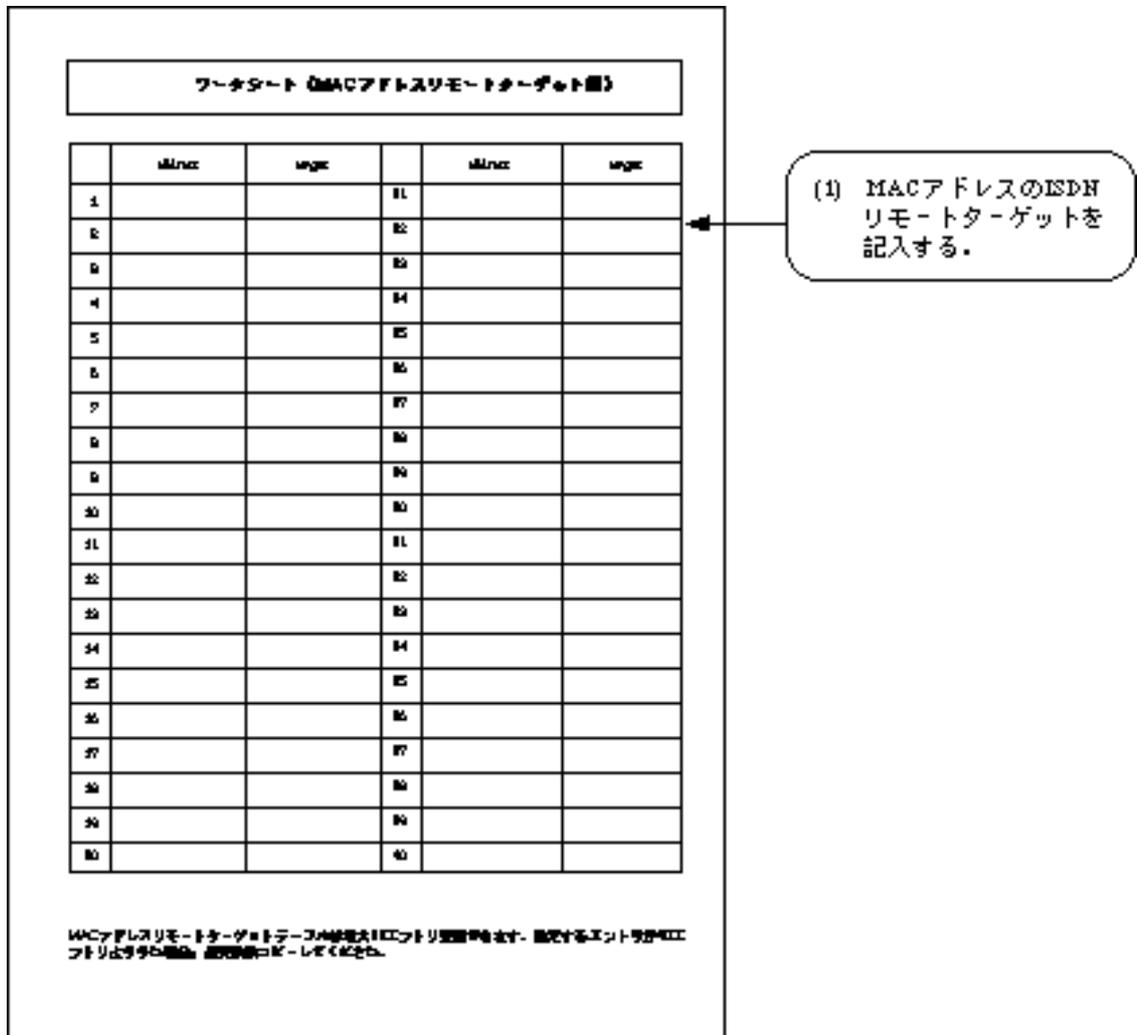


図3-28 MACアドレスリモートターゲット編の形式と記入の手順

(1) MACアドレスのISDNリモートターゲットを記入する。

ISDNを選択した場合でISDNで複数の相手と接続する(3.2.4(2)) 場合、宛先のMACアドレスとそれに対応するISDNリモートターゲットのテーブルを記入します。ISDNの接続相手を固定して使用する場合、記入の必要はありません。エントリは最大80件記入できます。1エントリに関する設定項目を以下に示します。

- address
宛先MACアドレスを記入します。
設定範囲： 12桁の16進数
導入時の設定： なし

- target

宛先MACアドレスに対応した、ISDNリモートターゲットを記入します。

設定範囲： ISDNリモートターゲット（最大80エン트리から1エン트리選択）

導入時の設定： なし



メモ：MACアドレスリモートターゲットテーブルは、最大80エン트리設定が可能です。本ワークシートを必要枚数コピーしてください。

このシートの記入はこれで終了です。

3.2.26 ワークシート「ブリッジング編」

ブリッジング編のワークシートの形式と、記入の手順を図3-29に示します。

	idmac	idipc		idmac	idipc
1			11		
2			12		
3			13		
4			14		
5			15		
6			16		
7			17		
8			18		
9			19		
10			20		
11			21		
12			22		
13			23		
14			24		
15			25		
16			26		
17			27		
18			28		
19			29		
20			30		

MACアドレスリモートターゲットは最大1000まで登録可能です。設定するエントリが1000より多い場合は、複数回登録してください。

図3-29 ブリッジング編の形式と記入の手順

(1) ブリッジングに関する基本事項を記入する。

記入項目を以下に示します。

- bridging interface

ISDN選択時には、ルーティングに使用するインタフェースを選択します。ブリッジングを行うグループもしくはチャンネルを記入します。（実際の設定では、ブリッジングを行うグループもしくはチャンネルを選択します。）

設定範囲： 「WAN topology」で「Usual」または「Usual/Load split」を選択したグループもしくはチャンネル

導入時の設定： なし

- STP

STP機能を使用するかどうか選択します。WAN回線にHSDを使用している場合に記入が必要です。

設定範囲： 1:use (使用する)
2:not use (使用しない)

導入時の設定： 2:not use



注意：STP機能の設定を「not use」から「use」に変更した場合には、STPに関するパラメータがデフォルト値に設定されます。STPのパラメータを変更する場合は拡張設定の「4.3.1 STPの設定」を参照してください。

- static filtering

スタティック設定によるフィルタリング機能を使用するかどうかを選択します。

設定範囲： 1:use (使用する)
2:not use (使用しない)

導入時の設定： 2:not use

このシートの記入はこれで終了です。

3.2.27 ワークシート「送信元フィルタリング編」

送信元フィルタリング編のワークシートの形式と，記入の手順を図3-30に示します．

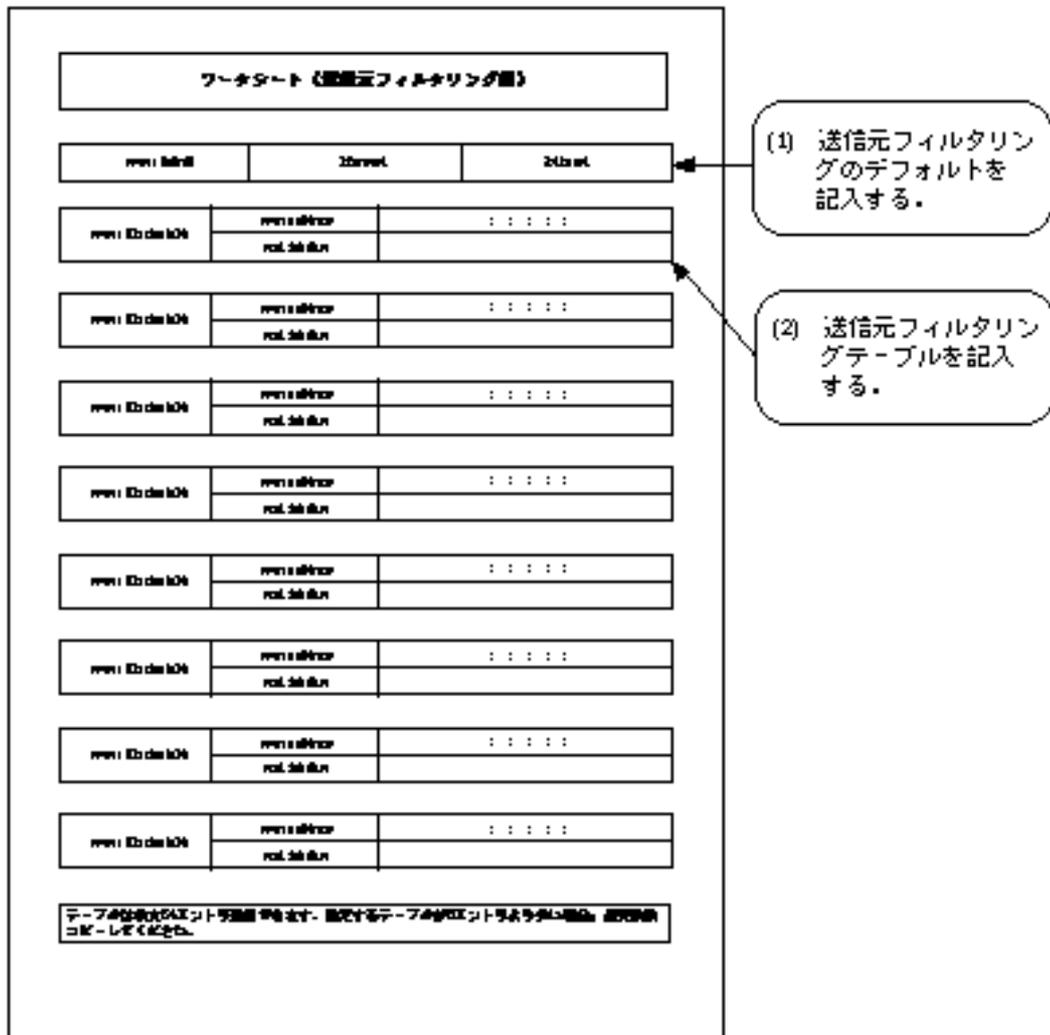


図3-30 送信元フィルタリング編の形式と記入の手順

(1) 送信元フィルタリングのデフォルトを記入する．

記入事項を以下に示します．

- source default
 テーブルに記入されていない送信元アドレスを持ったフレームを受信した場合の処理方法を選択します．
 設定範囲： 1:forward (中継する)
 2:discard (廃棄する)
 導入時の設定： 1:forward

(2) 送信元フィルタリングテーブルを記入する。

送信元フィルタリングテーブルには、最大64エントリの登録が可能です。1つのエントリに関する記入項目を以下に示します。

- source address

フィルタリングの対象となる送信元MACアドレスを記入します。

設定範囲： xx:xx:xx:xx:xx:xxの形式(16進数)

導入時の設定： 00:00:00:00:00:00

- send interface

「source address」で記入したMAC アドレスを持つフレームの、送信インタフェースを記入します。

設定範囲： LAN, 「bridging interface」で選択されたグループもしくはチャネル,
 nothing (なし：指定したフレームは廃棄される)

導入時の設定： LAN, 「bridging interface」で選択されたグループもしくはチャネル



メモ：テーブルは最大64エントリ設定できます。必要な場合は、用紙をコピーして使用してください。

このシートの記入はこれで終了です。

3.2.28 ワークシート「宛先フィルタリング編」

宛先フィルタリング編のワークシートの形式と、記入の手順を図3-31に示します。

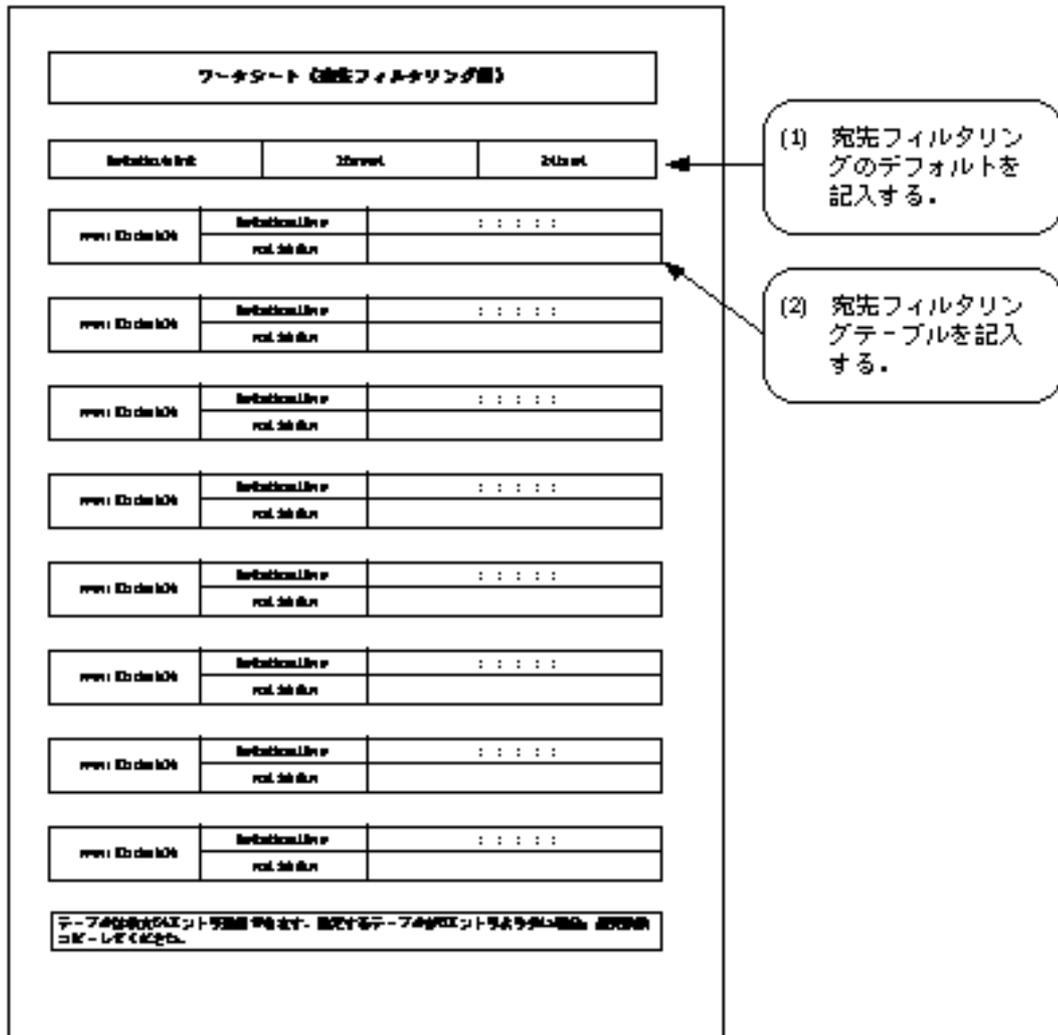


図3-31 宛先フィルタリング編の形式と記入の手順

(1) 宛先フィルタリングのデフォルトを記入する。

記入事項を以下に示します。

- destination default
 テーブルに記入されていない宛先アドレスを持ったフレームを受信した場合の処理方法を選択します。
 設定範囲： 1:forward (中継する)
 2:discard (廃棄する)
 導入時の設定： 1:forward

(2) 宛先フィルタリングテーブルを記入する。

宛先フィルタリングテーブルには、最大64エントリの登録が可能です。1つのエントリに関する記入項目を以下に示します。

- destination address

フィルタリングの対象となる宛先MACアドレスを記入します。

設定範囲： xx:xx:xx:xx:xx:xxの形式(16進数)

導入時の設定： 00:00:00:00:00:00

- send interface

「destination address」で記入したMAC アドレスを持つフレームの、送信インタフェースを選択します。

設定範囲： LAN, 「bridging interface」で選択されたグループもしくはチャンネル,
 nothing (なし：指定したフレームは廃棄される)

導入時の設定： LAN, 「bridging interface」で選択されたグループもしくはチャンネル



メモ：テーブルは最大64エントリ設定できます。必要な場合は、用紙をコピーして使用してください。

このシートの記入はこれで終了です。

3.2.29 ワークシート「プロトコルフィルタリング編」

プロトコルフィルタリング編のワークシートの形式と、記入の手順を図3-32に示します。

The worksheet is titled "ワークシート「プロトコルフィルタリング編」". It contains a table with columns for "Invert", "Match", and "Mismatch". Below this are several rows for "protocol filter table" with sub-columns for "protocol", "port", and "action".

Callout (1) points to the "Invert" column: (1) プロトコルフィルタリングのデフォルトを記入する。

Callout (2) points to the "protocol" column: (2) プロトコルフィルタリングテーブルを記入する。

At the bottom, there is a note: データは最大32エントリで制限されます。既定するデータのエントリより多い場合は、既定値のコピーしてください。

図3-32 プロトコルフィルタリング編の形式と記入の手順

(1) プロトコルフィルタリングのデフォルトを記入する。

記入事項を以下に示します。

- default
 テーブルに記入されていないプロトコルのフレームを受信した場合の、処理方法を選択します。
 設定範囲： 1:forward (中継する)
 2:discard (廃棄する)
 導入時の設定： 1:forward

(2) プロトコルフィルタリングテーブルを記入する。

プロトコルフィルタリングテーブルには、最大32エントリの登録が可能です。1つのエントリに関する記入項目を以下に示します。

- protocol
フィルタリングの対象とするプロトコルのタイプを選択します。
設定範囲： 1:type (プロトコルをイーサネット形式フレームのTYPEの値で識別)
2:dlsap (プロトコルをLLC形式フレームのDLSAPの値で識別)
導入時の設定： 1:type
- number
プロトコル番号を記入します。
設定範囲： 「type」の時は4桁の16進、「dlsap」の時は2桁の16進数
導入時の設定： 「type」の時は0000、「dlsap」の時は00

表3-9にプロトコル番号を示します。

表3-9 プロトコル番号表

プロトコル	設定値(16進数)
IP	0800(type)
ARP	0806(type)
トレーラプロトコル	10XX(type) (XXは00～10の値)
リバースARP	8035(type)
IPX	8137(type), 8138(type), e0(dlsap), ff(dlsap)
DECnet	60XX(type) (XXは00～09の値), 80XX(type) (XXは38～42の値)
AppleTalk	809b(type), 80f3(type)
XNS	0807(type)
XEROX PUP	0200(type), 0201(type), 0a00(type), 0a01(type)
XEROX NS IDP	0600(type)
OSI	fe(dlsap)
FNA	80(dlsap)

3章 基本設定

- send interface

中継するインタフェースを指定します。

設定範囲： LAN, 「bridging interface」で選択されたグループもしくはチャンネル,
nothing (なし：指定したフレームは廃棄される)

導入時の設定： LAN, 「bridging interface」で選択されたグループもしくはチャンネル



メモ：テーブルは最大16エントリ設定できます。必要な場合は、用紙をコピーして使用してください。

このシートの記入はこれで終了です。

3.2.30 ワークシート「SNMP編」

SNMP編のワークシートの形式と、記入の手順を図3-33に示します。

The diagram shows a worksheet titled "ワークシート (SNMP編)". It contains five main sections:

- SNMP parameters:** A table with three rows for "sysName", "sysLocation", and "sysCommunity".
- SNMP manager (1):** A table with four rows: "sysName", "sysLocation", "sysCommunity", and "sysPort". The last two rows have "1.7.1.1" and "1.610" in the columns.
- SNMP manager (2):** A table with four rows: "sysName", "sysLocation", "sysCommunity", and "sysPort". The last two rows have "1.7.1.1" and "1.610" in the columns.
- SNMP manager (3):** A table with four rows: "sysName", "sysLocation", "sysCommunity", and "sysPort". The last two rows have "1.7.1.1" and "1.610" in the columns.
- SNMP manager (4):** A table with four rows: "sysName", "sysLocation", "sysCommunity", and "sysPort". The last two rows have "1.7.1.1" and "1.610" in the columns.

Callout (1) points to the "sysName" field in the first section. Callout (2) points to the "sysName" field in the second section.

図3-33 SNMP編の形式と記入の手順

(1) 装置のSNMPパラメータの値を記入する。

記入事項を以下に示します。

- sysName

本装置をSNMPエージェントとして使用する場合の装置の名称を英数字32文字以内で記入します（必ずしも記入する必要はありません）。

設定範囲： 最大32文字の英数字

導入時の設定： 自ホスト名（「3.2.1 ワークシート「基本設定編」」）

- sysContact
本装置をSNMPエージェントとして使用する場合の管理者名を英数字32文字以内で記入します（必ずしも記入する必要はありません）。
設定範囲： 最大32文字の英数字
導入時の設定： なし

- sysLocate
本装置をSNMPエージェントとして使用する場合の設置場所を英数字64文字以内で記入します（必ずしも記入する必要はありません）。
設定範囲： 最大64文字の英数字
導入時の設定： なし

(2) SNMPマネージャテーブルの値を記入する。

SNMPマネージャテーブルには、最大8エントリの登録が可能です。SNMPマネージャとは、本装置のSNMPエージェント機能を利用して本装置の情報を取得したり、本装置を操作する資格を持つ外部の装置のことをさします。1つのエントリに関する記入項目を以下に示します。



メモ：SNMPマネージャテーブルで設定するIPアドレスには、0.0.0.0から255.255.255.255のすべてのIPアドレスが設定可能です。

- IP address
SNMPマネージャのIPアドレスを記入します。IPアドレス0.0.0.0は、デフォルトマネージャ(すべての装置が本装置のSNMPエージェント機能を使用可能)のエントリを示します。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： 0.0.0.0

- community name
SNMPマネージャと通信する場合のコミュニティ名を英数字32文字以内で記入します。
設定範囲： 最大32文字の英数字
導入時の設定： public

- set enable
SNMPマネージャからの設定を許可するかどうかを選択します。
設定範囲： 1:YES (SNMPマネージャからの設定を許可する)
2:NO (SNMPマネージャからの設定を許可しない)
導入時の設定： 2:NO

- alarm
SNMPマネージャにトラップを送信するかどうかを選択します。ただし本装置では、デフォルトマネージャにトラップ送信はできません。この場合「2:NO」を選択します。
設定範囲： 1:YES (SNMPマネージャにトラップを送信する)
2:NO (SNMPマネージャにトラップを送信しない)
導入時の設定： 2:NO



メモ：SNMPマネージャは最大8エン트리登録できます。必要な場合は本シートをコピーして使用してください。

このシートの記入はこれで終了です。

3.3 コンソールの接続

システム編集を行うには、本装置にコンソールを接続する必要があります。出荷後初めての設定は、必ずコンソールケーブル(RS-232C)を介したコンソール(ローカルコンソール)で行います。

本装置の後面にある「CONSOLE」と表示されたコンソールポートに、コンソールケーブルを介してコンソールを接続します。

コンソールポートに接続するコンソールの通信機能は、表3-10の値に設定します。

表3-10 コンソールの通信機能設定

項目	設定
同期方式	調歩同期
通信速度	9600bps
キャラクタ長	8ビット
ストップビット長	1
パリティ	無し
フロー制御	Xon / Xoff



注意：コンソールを本装置にコンソールケーブルを介して接続する場合は、装置の電源スイッチがOFF（「」側に押されている状態）であることを確認してください。また、コンソール側でも、コンソールケーブルを接続する際には電源を落としてから接続します。

3.4 メインメニュー

コンソールで装置に接続後、最初に出てくる画面が装置のメインメニューです。

コンソール上での操作は、メインメニューから画面を数字でたどるメニュー形式になっています。図3-34に、ローカルコンソールを接続した際のメインメニューの例と、それぞれの項目の概要を示します。

```
INFONET 3790 Remote Router  B V01.00 1995.04.01
WAN topology (ISDN) 1995/04/01 12:00:00 (  1 12:34:56)  Normal Mode
1. configuration display
2. configuration set (normal)
3. configuration set (expert)
4. operation
5. information
6. shift to super mode
7. exit from remote console or current mode
Select the number. :
```

図3-34 メインメニュー例

まず、メインメニューの初めの2行について説明します。

- INFONET 3790 Remote Router
本装置の名称を示します。
- B
本装置のハードウェア版数を示します。
- V01.00 1995.04.01
ファームウェア版数と作成日を示します。
- WAN topology (ISDN)
本装置の運用回線を示します。HSD選択時は「WAN topology(HSD)」と表示されます。
- 1995/04/01 12:00:00
現在の日時を示します（「3.10 現在時刻の設定」を参照）。
- (1 12:34:56)
本装置の運用を開始してからの日時を示します。上記の例では運用を開始してから1日と12時間34分56秒経過したことを示しています。

3章 基本設定

- Normal Mode
現在のモードを示します。(「3.5 管理者資格への移行」, 「3.6 一般資格への復帰」)

次に, 1から7の選択メニューについて説明します。

- configuration display
装置に基本設定で設定された内容を表示します。(「3.7 設定情報の表示」)
- configuration set (normal)
装置の基本設定を行います。(「3.8 コンソールからの設定」)
- configuration set (expert)
装置の拡張設定を行います。(「4章 拡張設定」)
- operation
エコーテストやリセット等の, 装置の操作を行います。(「5章 オペレーション」)
- information
統計情報や回線状態等の, 情報の表示を行います。(「6章 インフォメーション」)
- shift to super mode
管理者資格(スーパーモード)へ移行します。(「3.5 管理者資格(スーパーモード)への移行」)
- exit from remote console or current mode
遠隔操作の終了, および一般資格への復帰を行います。(「3.6 一般資格への復帰」, 「5.18.3 遠隔操作の終了」)

3.5 管理者資格(スーパーモード)への移行

メインメニューの「configuration set (normal)」、**「configuration set (expert)」**および「operation」は、管理者資格(スーパーモード)でないと実行することができません。現在のモードはメインメニューの2行目の右端に表示されています。「Normal mode」は、一般資格を表わし、「Super mode」は管理者資格を表わします。

一般資格から管理者資格への移行は、メインメニューの「shift to super mode」を選択します。その後、パスワードを入力すると管理者資格へ移行します。図3-35に例を示します。

```

INFONET 3790 Remote Brouter  B V02.04 1995.04.01
WAN topology (ISDN) 1995/04/01 12:00:00 ( 3 00:01:21) Normal Mode
ノーマルモード

1. configuration display
2. configuration set (normal)
3. configuration set (expert)
4. operation
5. information
6. shift to super mode
7. exit from remote console or current mode
Select the number. : 6 「shift to super mode」を選択
Password: パスワードを入力
INFONET 3790 Remote Brouter  B V02.04 1995.04.01
WAN topology (ISDN) 1995/04/01 12:00:00 ( 3 00:01:21) Super Mode
スーパーモード

:
:

```

図3-35 管理者資格への移行例



メモ：装置の導入時はパスワードが設定されていません。パスワードが設定されていない状態では、「リターン」キーのみの入力ですーパーモードへ移行できます。

3.6 一般資格への復帰

現在のモードが管理者資格の場合，メインメニューで「exit from remote console or current mode」を実行すると一般資格へ復帰します．図3-36に例を示します．

```
INFONET 3790 Remote Brouter  B V02.04 1995.04.01
WAN topology (ISDN) 1995/04/01 12:00:00 ( 3 00:01:21)  Super Mode
                                                         スーパーモード

1. configuration display
2. configuration set (normal)
3. configuration set (expert)
4. operation
5. information
6. shift to super mode
7. exit from remote console or current mode
Select the number. : 7      「exit from remote console or current mode」
                             を選択

INFONET 3790 Remote Brouter  B V02.04 1995.04.01
WAN topology (ISDN) 1995/04/01 12:00:00 ( 3 00:01:21)  Normal Mode
                                                         ノーマルモード

:
:
```

図3-36 一般資格への復帰例

3.7 設定情報の表示

メインメニューで「configuration display」を選択することで、運用に必要な基本設定の情報を確認することができます。

設定項目ごとに順に設定情報を表示しますが、各項目の最後では

```
== q:quit      return key:next      ESC:previous ==
```

と表示します。ここで、キー入力に応じて以下の動作をします。

- 「q」キーを入力した場合、メインメニューに戻ります。
- 「リターン」キーを入力した場合、次の設定項目を表示します。
- 「ESC」（エスケープ）キーを入力した場合、前の設定項目を再表示します。



メモ：上記のキー以外を入力した場合、「リターン」キーと同様の動作をします。

3.8 コンソールからの設定

基本設定は、メインメニューの「configuration set (normal)」で行います。設定を行うためには、管理者資格（スーパーモード）になっている必要があります。（「3.5 管理者資格への移行」）一般資格（ノーマルモード）のまま「configuration set (normal)」を選択した場合には、「User mode mismatch!」と表示され設定できません。

「configuration set (normal)」では設定項目を順番に設定します。設定項目は関連したグループに分かれており、ワークシートを使用して各グループを設定することによって、運用に必要な設定を行うことができます。設定動作は、図3-37の流れで行います。

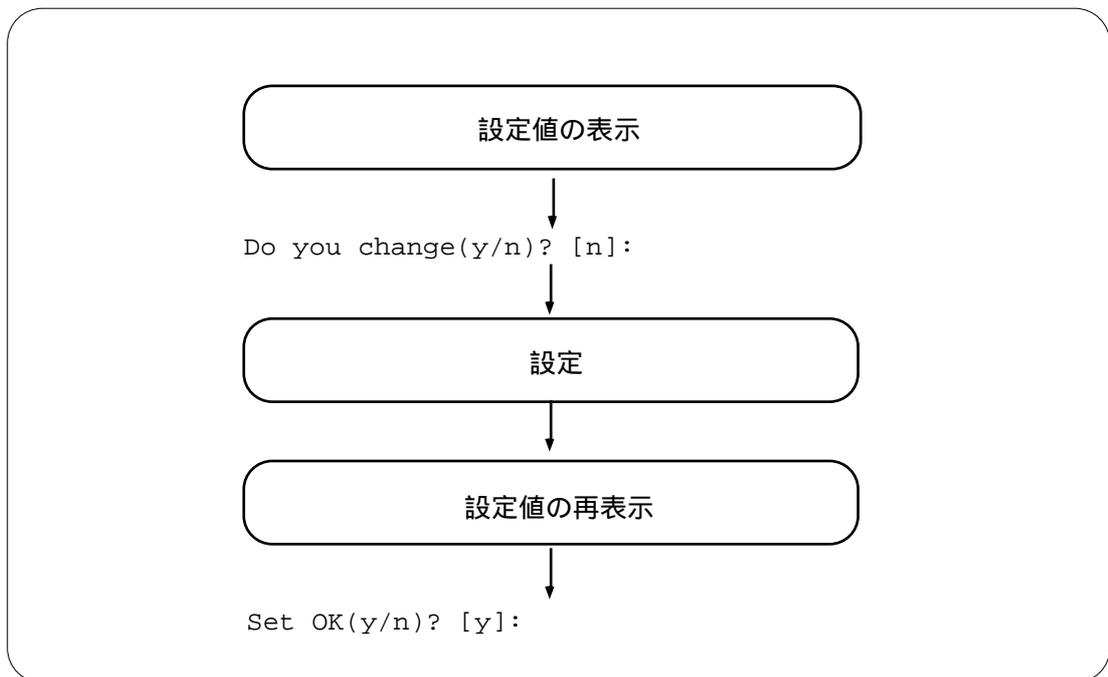


図3-37 入力の流れ

- 「設定値の表示」の部分では、設定を行う項目の現在の値を表示します。表示されている項目を設定する場合は、「Do you change(y/n)? [n]:」で「y」キーを入力すると、「設定」の部分が表示されます。「n」キーまたは「リターン」キーを入力した場合は、次のグループの「設定値の表示」に進みます。
- 「設定」の部分で設定を行います。入力を間違った場合、「Set OK(y/n)? [y]:」で「n」キーを入力してください。「設定」に戻って再度設定することができます。
- グループ内の設定が終了すると、現在設定した内容を「設定値の再表示」の部分に表示し、「Set OK(y/n)? [y]:」が表示されます。設定内容を確認し、「Set OK(y/n)? [y]:」で「y」キーまたは「リターン」キーを入力すると次の設定グループに進みます。

- 設定を変更しない場合
現在設定されている値，または，設定時の省略値は，[]内に表示されます．[]内の値を変更しない場合は，「リターン」キーを入力します．
- 設定内容を消去したい場合
文字列を設定しなければならない項目（SNMPエージェント機能の設定におけるsysName, sysContact, sysLocate, CommunityNameなど）において，設定内容を消去する場合（何も設定しない状態にする場合）「"」（ダブルクォーテーション2回）を入力します．
- 設定を間違えて先に進んだ場合
「ESC」キーの入力により，その入力された場所によって次のように動作します．
 - ・ 現在，選択しているメニューの先頭で「ESC」キーが入力された場合には，確認の後に一段上の（メインメニューの方向）メニューに移動します．
 - ・ 現在，選択しているメニュー内の設定をしているところで「ESC」キーが入力された場合には，もう一度，その選択しているメニューの最初の項目に移動します．この時，今までに入力されていたものが再設定をする際の省略の値となります．
- 入力ミスをした場合
データの入力ミスに対しては，エラー表示を行います．例えば，現在時刻の設定で不正な入力をした場合には図3-38のように表示し，再入力を促します．

```
year[1995]: 1995
month[12]: 13
Limit error (1 =< value =< 12) !
month[12]:
```

図3-38 エラー表示例

- 「- MORE -」表示
1画面で該当する項目の全ての情報が表示できない場合，本装置のコンソール画面では「- MORE -」表示を行います．「- MORE -」表示では，まず1画面に収まるだけの情報を表示します．この状態でさらに情報が必要ならば，「リターン」キーまたは「スペース」キーを押します．「リターン」キーおよび「スペース」キーでは次の1画面を表示します．また，表示を中断する場合は「q」キーを押します．

3.9から3.21に，コンソールからの基本設定の入力方法を示します．基本設定の入力は，「3.2 ワークシートの作成」で作成したワークシートを参照しながら行います．

3.9 運用形態の選択



本設定は、ワークシート「基本設定編」を参照して設定を行います。（「3.2.1 ワークシート「基本設定編」」）

まず、装置で使用する回線を、HSDとISDNより選択します。「*」が左側に記されている回線は、現在選択されていることを示します。この設定は、装置をリセットした後有効になりますので、設定後必ず装置のリセットを行ってください。

```
*** Selecting PORT way ***
* 1 HSD
  2 ISDN
Select the number. [1]: 2
Execute system reset.
Do you want to continue ? [y/n]: y
```

図3-39 WAN回線選択例



メモ：使用する回線を変更した後、「Do you want to continue ? [y/n]」と表示されます。装置のリセットを行う場合は、設定を確認して「y」を入力します。もう1度設定をやり直す場合は、「n」を入力します。



注意：装置導入時にWAN回線を選択した場合や、運用中にWAN回線の運用形態を切り替えた場合は、使用するWAN回線の詳細設定は、リセット動作の後に行います。また、運用中にWAN回線の運用形態を切り替えた場合は、再設定が必要となる項目がありますので必ずすべての設定項目を確認してください。

3.10 現在時刻の設定

現在時刻の設定を行います。導入時に現在時刻を設定していますが確認願います。年は西暦で、また時間は24時間制で設定します。

```

*** Set current time parameter(s) ***
1995/08/19 15:50:53
Do you change (y/n)? [n]: y
year [1995]:
month [08]: 6
day [19]: 18
hour [15]: 14
minute [50]: 52
second [53]: 0
Current time parameter(s) are set to the following values.
1995/06/18 14:52:00
Set OK (y/n)? [y]:

```

図3-40 現在時刻設定例 (1995年6月18日14時52分00秒に設定)

3.11 自ホスト名の設定

本装置の自ホスト名の設定を行います。

```

*** Set host name configuration ***
<host name configuration parameter(s)>
  host name:
Do you change (y/n)? [n]:y
host name []: Tokyo

host name parameter(s) are set to the following values.
<host name configuration parameter(s)>
  host name: Tokyo
Set OK (y/n)? [y]:

```

図3-41 自ホスト名の設定例



メモ：自ホスト名は、次の2点に関して未登録の場合、その内容が適用されます。

- IPXルーティングのルータ名 (IPX router name) (「3.16.1 IPXルーティングの設定」)
- SNMPマネージャのsysName (「3.19.1 SNMPパラメータの設定」)

3.12 WAN回線の設定

3.12.1 HSDの設定



本設定は、ワークシート「HSD編」を参照して設定を行います。(「3.2.2 ワークシート「HSD編」」)

HSDを選択している場合は、HSDの設定を行います。

```
*** Set HSD speed configuration ***
<Main HSD speed parameter(s)>
[HSD#1] [HSD#2] [HSD#3] [HSD#4] [HSD#5] [HSD#6] [HSD#7] [HSD#8]
128kbps 128kbps 128kbps 128kbps 128kbps 128kbps 128kbps 128kbps
Do you change (y/n)? [n]: y
HSD#1 speed(1:64k 2:128k 3:not use) [3]: 1
HSD#2 speed(1:64k 2:128k 3:not use) [3]: 2
HSD#3 speed(1:64k 2:128k 3:not use) [3]: 1
HSD#4 speed(1:64k 2:128k 3:not use) [3]: 1
HSD#5 speed(1:64k 2:128k 3:not use) [3]: 2
HSD#6 speed(1:64k 2:128k 3:not use) [3]: 2
HSD#7 speed(1:64k 2:128k 3:not use) [3]: 1
HSD#8 speed(1:64k 2:128k 3:not use) [3]: 2
Main HSD parameter(s) are set to the following values.
<Main HSD parameter(s)>
[HSD#1] [HSD#2] [HSD#3] [HSD#4] [HSD#5] [HSD#6] [HSD#7] [HSD#8]
64kbps 128kbps 64kbps 64kbps 128kbps 128kbps 64kbps 128kbps
Set OK (y/n)? [y]:
```

図3-42 HSD回線の回線速度設定例

3.12.2 ISDNチャンネルグループの設定



本設定は、ワークシート「ISDNチャンネルグループ編」を参照して設定を行います。また、各機能に関する詳細は、「3.2.3 ワークシート「ISDNチャンネルグループ編」」を参照してください。

ISDNを使用する場合、NTTのサービスである「代表取扱サービス」を利用するために、チャンネルグループ機能におけるグループを定義します。

```
*** Set ISDN group configuration ***
1. change 2. delete 3. add 4. display 5. end
Select the number. [5]: 1
```

図3-43 ISDNチャンネルグループ機能設定例

本設定では、グループ名を設定し、その後そのグループに属するポートを選択します。



メモ：本装置および本取扱説明書では、ISDNのポートの名称を「BRI#1」～「BRI#8」、また、チャンネルの名称は「BRI#1-1」のように「-1」「-2」を付加した形式で示します。

```
<Add group configuration>
group name [] :GroupB
1.BRI#1 2.BRI#2 3.BRI#3 4.BRI#4 5.BRI#5 6.BRI#6 7.BRI#7
Select the ISDN : 2,3,4

[GroupB] :BRI#2,BRI#3,BRI#4
Add OK (y/n)? [y]:
```

図3-44 ISDNチャンネルグループ追加例

チャンネルグループのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

3.12.3 ISDN運用形態の設定



本設定は、ワークシート「ISDN運用形態編（グループ/チャンネル毎）」を参照して設定を行います。また、各機能に関する詳細は、「3.2.4 ワークシート「ISDN運用形態編」（グループ/チャンネル毎）」を参照してください。

本設定では、「3.12.2 ISDNチャンネルグループ編」で設定されたグループおよびチャンネルに関して運用形態、マルチターゲット、相手チェック方式の設定を行います。

```

*** Selecting group/channel ***
1. [GroupA]
2. [Kinki]
3. [GroupB]
4. BRI#6-1
5. BRI#6-2
6. BRI#7-1
7. BRI#7-2
Do you change (y/n)? [n]: y
Select the number : 1
    
```

図3-45 グループおよびチャンネルの選択画面例

```

Group/Channel WAN topology      multi target check mode  check skip length
-----+-----+-----+-----+
[GroupA]      Usual/Load split  use          on          0

Do you change {y/n}? [n]: y
Select the WAN topology (1.Usual 2.Load split 3.Usual / Load split) [3]: 1
receive address check mode (1:on 2:off) [1]:
                check skip length [0]: 5

Group/Channel WAN topology      multi target check mode  check skip length
-----+-----+-----+-----+
[GroupA]      Usual                use          on          5
Set OK (y/n) [y]:
    
```

図3-46 運用形態の設定例（「WAN topology」に「Usual」か「Usual/Load split」を選択した場合）
（グループの場合）

```

Group/Channel WAN topology      multi target check mode  check skip length
-----+-----+-----+-----+-----
[GroupA]      Usual/Load split  use          on          0

Select the WAN topology (1.Usual 2.Load split 3.Usual / Load split) [3]: 2
receive address check mode (1:on 2:off) [1]:
                check skip length [0]: 5

Usual line
    1.GroupA      2.GroupB      3.BRI#6-1      4.BRI#6-2
    5.BRI#7-1     6.BRI#7-2

Select the number []: 1

Group/Channel WAN topology      multi target check mode  check skip
length
-----+-----+-----+-----+-----
[GroupA]      Load split(GroupA) use          on          5
Set OK (y/n)? [y]

```

図3-47 運用形態の設定（「WAN topology」に「Load split」を選択した場合）



注意：グループの場合、「muliti target」は「use」固定となります。チャンネルの場合で、「multi target」を「use」から「not use」に変更する場合、あらかじめ設定されていたISDNリモートターゲット（ 3.2.5）、IP、IPX、AppleTalkリモートターゲット（ 3.2.9, 3.2.14, 3.2.19）、MACアドレスターゲット（ 3.2.25）の各エンタリは消去されてしまいます。本設定を変更する前には必ず構成定義情報の保存（ 5.12）を行ってください。

3.12.4 ISDNリモートターゲットの設定



本設定は、ワークシート「ISDNリモートターゲット編（グループ/チャンネル毎）」を参照して設定を行います。また、各機能に関する詳細は、「3.2.5 ワークシート「ISDNリモートターゲット編」（グループ/チャンネル毎）」を参照してください。

```

*** Set GroupA remote address list configuration ***
    1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:5

```

図3-48 ISDNリモートターゲット設定選択画面



注意：装置を新規に購入した場合、あるいは装置に対してなにも設定をしていない状態（デフォルトの設定をロードした状態）においては、必ず宛先ISDN番号を設定します。

```

<Add GroupA remote address data>
target [t-0001]: Tokyo
address []: 0333333333
subaddress []:
preference [0]:
Do you connect Load split line to Tokyo? (1.yes 2.no) [2]: 1
load split line address [0333333333]:
    subaddress []: 1
speed (1.64k 2.64k/56k 3.56k) [2]:
Do you change the password? [n]: y
New password: xxxxxxxx
Retype New password: xxxxxxxx
New password is accepted.

no target address          pref line      Load split  speed  password
    subaddress
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1. Tokyo 0333333333          0 Usual      yes      64k/56k  *****
    Load split address      : 0333333333
    subaddress : 1
Add OK (y/n)? [y]:
    
```

図3-49 ISDNリモートターゲット設定画面



注意：同じ名称のターゲットのエントリを設定する場合、必ずどれか一つのエントリの「preference」を「0」にしてください。



メモ：サブアドレスを削除する場合は、「""」（ダブルクォーテーション2回）を入力します。

ISDNリモートターゲットのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

3.12.5 ISDN通常回線の設定



本設定は、ワークシート「ISDN通常回線編」を参照して設定を行います。（各機能に関する詳細 「3.2.6 ワークシート「ISDN通常回線編」」）

ISDNを選択した場合は、ISDNの通常回線の設定を行います。以下に1チャンネルに関する設定例を示します。複数ISDNを選択されている場合、さらに同様の設定を行います。

```

*** Set ISDN configuration ***
GroupA configuration:
no. group/channel address          connection activate/deactivate
              subaddress          Usual      Load split
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1. [GroupA]    223333              time+traffic manual

address [223333] :
subaddress [] :
<Select Usual line activate/deactivate mode>
1.time+traffic
2.manual
3.passive
Select the number. [1]: 2
<Select Load split line activate/deactivate mode>
1.time+traffic
2.manual
Select the number. [2]: 1

no. group/channel address          connection activate/deactivate
              subaddress          Usual      Load split
-----+-----+-----+-----+-----+-----+-----+-----+-----+
1. [GroupA]    223333              manual      time+traffic

Set OK (y/n)? [y]:

```

図3-50 ISDN通常回線設定例



注意：実際の接続および切断は、手動による動作を優先します。例えば、時刻指定の自動接続 / 切断を選択した場合でも、指定時刻外に手動による接続および切断が可能です。



注意：中継データによる自動接続 / 切断の場合、手動により回線を切断できますが、その後中継データが発生した場合は自動接続します。

接続 / 切断の方法として「time」を含む方法を選択した場合は、時刻の設定が必要となります。以下に接続時刻，切断時刻の設定メニューを示します。

```
*** Set GroupA connection activate/deactivate time configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図3-51 接続時刻，切断時刻設定メニュー

以下に時刻設定の追加例を示します。

```
<Add activate-deactivate time>
line (1.Usual 2.Load split) [1]:
activate month [**]: 6
    day [**]: 18
    day of the week[***]
    hour [**]: 14
    minute [00]:
deactivate month [**]: 6
    day [**]: 18
    day of the week[***]
    hour [**]: 15
    minute [00]:
time value:06/18(***)14:00 - 06/18(***)15:00 (Usual line)
Add OK (y/n)? [y]:
```

図3-52 ISDN接続 / 切断時刻の追加例

ISDN接続 / 切断時刻のエントリの設定は，設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。表示したいエントリの「target」を入力します。
- end 設定を終了します。

ただし，エントリが1つも無い状態で「change」，「delete」を選択すると「Input error!」と表示され，設定できません。また，「display」を選択すると「no entry.」と表示されます。

3.13 機能の選択



本設定は、ワークシート「基本設定編」を参照して設定を行います。（「3.2.1 ワークシート「基本設定編」」）

「IPルーティング機能」、「IPパケットフィルタリング機能」、「IPXルーティング機能」、「AppleTalkルーティング機能」、「ブリッジング機能」および「SNMPエージェント機能」に関して、それぞれの機能を使用する／しないの設定を行います。

```

*** Set basic configuration ***
<Basic configuration parameter(s)>
  IP routing      : not use
  IP filtering    : not use
  IPX routing     : not use
  AppleTalk routing: not use
  bridging       : not use
  SNMP           : use
Do you change (y/n)? [n]:

```

図3-53 基本機能画面 (設定値の表示)

- IP routing
IPルーティング機能を使用するかどうかを選択します。
- IP filtering
IPパケットフィルタリング機能を使用するかどうかを選択します。
- IPX routing
IPXルーティング機能を使用するかどうかを選択します。
- AppleTalk routing
AppleTalkルーティング機能を使用するかどうかを選択します。
- bridging
ブリッジング機能を使用するかどうかを選択します。
- SNMP
SNMPエージェント機能を使用するかどうかを選択します。

```
Do you change (y/n)? [y]: y
IP routing (1:use 2:not use) [2]: 1
IP filtering (1:use 2:not use) [2]:
IPX routing (1:use 2:not use) [2]: 1
AppleTalk routing (1:use 2:not use) [2]: 1
bridge (1:use 2:not use) [2]: 1
SNMP (1:use 2:not use) [1]:
Basic parameter(s) are set to the following values.
<Basic configuration parameter(s)>
  IP routing      : use
  IP filtering    : not use
  IPX routing     : use
  AppleTalk routing: use
  bridging       : use
  SNMP           : use
Set OK (y/n)? [y]:
```

図3-54 基本機能設定例

3.14 IPホスト / IPアドレスの設定



本設定は、ワークシート「IPホスト編」を参照して設定を行います。(「3.2.7 ワークシート「IPホスト編」」)

「IPルーティング機能」を使用しない状態で、装置をIPホストとして動作させるかどうかを選択します。「IPフィルタリング機能」を使用する場合または「SNMPエージェント機能」を使用する場合は、必ずIPホストとして動作するため、図3-55の画面は表示されません。装置をIPホストとして動作させない場合は、「Do you change (y/n)?」で「n」を選択し次のメニューに移動します。

```
*** Set IP host configuration ***
<IP host configuration parameter(s)>
  IP host: not use
Do you change (y/n)? [n]: y
  IP host (1:use 2:not use) [2]: 1
IP host parameter(s) are set to the following values.
<IP host configuration parameter(s)>
  IP host: use
Set OK (y/n)? [y]:
```

図3-55 IPホスト設定例

装置をIPホストとする場合には、装置のIPアドレスの設定を行います。

```
*** Set IP address configuration ***
<IP address configuration parameter(s)>
  IP address      :0.0.0.0
  subnetmask     :0.0.0.0
  broadcast       :0.0.0.0
  default gateway:
Do you change (y/n)? [n]: y
IP address[0.0.0.0]: 192.168.1.1
subnetmask[255.255.255.0]:
broadcast[192.168.1.255]:
default gateway[]:
IP address parameter(s) are set to the following values.
<IP address configuration parameter(s)>
  IP address      :192.168.1.1
  subnetmask     :255.255.255.0
  broadcast       :192.168.1.255
  default gateway:
Set OK(y/n)? [y]:
```

図3-56 IPアドレス設定例



メモ：「default gateway」を設定したあとで設定を削除したい場合には「"」（ダブルクォーテーション2回）を入力します。

3.15 IPに関する基本設定

3.15.1 IPルーティングの設定



本設定は、ワークシート「IPルーティング編」を参照して設定を行います。（「3.2.8 ワークシート「IPルーティング編」」）

ISDNを選択し、IPルーティング機能を使用する場合の、設定例を図3-57に示します。

```

*** Set IP router configuration ***
<IP router configuration parameter(s)>
                                     broadcast or interface
no  group  interface IP address      subnetmask      remote address type
---+-----+-----+-----+-----+-----+-----+
 1. ----- LAN          192.52.1.1      255.255.255.0   192.52.1.255    bcast
 2. GroupA -----          192.168.2.1     255.255.255.0   195.168.2.255   bcast
 3. GroupB BRI#5-1  ---.---.---.--- 255.255.255.0   192.169.1.213   ptop
 4.          BRI#5-2  ---.---.---.--- 255.255.255.0   192.169.30.214  ptop
 5. ----- BRI#6-1  ---.---.---.--- 255.255.255.0   192.169.2.100   ptop
 6. ----- BRI#6-2  not use IP routing
 7. ----- BRI#7-1  192.169.4.100   255.255.255.0   192.169.4.2     ptop
 8. ----- BRI#7-2  ---.---.---.--- 255.255.255.0   192.169.5.100   ptop
Do you change (y/n)? [n]: y
routing interface:
GroupA (y/n) [y]: y
GroupB (y/n) [y]: y
BRI#6-1 (y/n) [y]: n
BRI#6-2 (y/n) [n]: n
BRI#7-1 (y/n) [y]: y
BRI#7-2 (y/n) [y]: y
Select the group/channel to change
  1.LAN
  2.GroupA   3.GroupB   4.BRI#7-1   5.BRI#7-2
Select the number : 2,4
GroupA interface type (1:broadcast) [1]:
  IP address [192.168.2.1]: 192.168.55.1
  subnetmask [255.255.255.0]:
  broadcast [192.190.1.255]:
BRI#7-1 interface type (1:broadcast 2:point to point) [2]:
  IP address [192.169.4.100]:
  remote IP address [192.169.4.2]: 192.52.33.3
  remote subnetmask [192.52.33.255]:

```

図3-57 IPルーティング設定例（ISDNを7本使用する場合）



メモ：変更するグループおよびチャネルは複数同時に選択することができます。

```

IP router parameter(s) are set to the following values.
<IP router configuration parameter(s)>
                                     broadcast or interface
no  group  interface IP address      subnetmask      remote address type
-----+-----+-----+-----+-----+-----+-----
1.  ----- LAN          192.52.1.1      255.255.255.0  192.52.1.255    bcast
2.  GroupA -----  192.168.55.1   255.255.255.0  195.168.2.255   bcast
3.  GroupB BRI#5-1   ---.---.---.--- 255.255.255.0  192.169.1.213   ptop
4.           BRI#5-2   ---.---.---.--- 255.255.255.0  192.169.30.214  ptop
5.  ----- BRI#6-1   not use IP rouing
6.  ----- BRI#6-2   not use IP rouing
7.  ----- BRI#7-1   192.169.4.100  255.255.255.0  192.169.33.3    ptop
8.  ----- BRI#7-2   ---.---.---.--- 255.255.255.0  192.169.5.100   ptop
Set OK (y/n)? [y]:

```

図3-58 IPルーティング設定例（ISDNを7本使用する場合）

3.15.2 IPのISDNリモートターゲットの設定



本設定は、ワークシート「IPリモートターゲット編」を参照して設定を行います。また、設定項目に関する詳細は、「3.2.9 ワークシート「IPリモートターゲット編」」を参照してください。

ISDNを選択した場合、宛先IPアドレスとISDNリモートターゲットの対応テーブルを設定します。最大80エントリ設定できます。

```

*** Set IP address target configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]: 3

```

図3-59 IPリモートターゲット例

以下にIPリモートターゲットの追加例を示します。テーブルは、最大80エントリ登録できません。

```
<Add IP address target>
address []: 192.168.1.1
<Target index>
  1. Tokyo
  2. Osaka
Select the number of target index []: 2
      address      target
      192.168.1.1  Osaka
Add OK (y/n)? [y]:
```

図3-60 IPリモートターゲットデータ追加例

IPリモートターゲットのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。表示したいエントリの「target」を入力します。
- end 設定を終了します。

ただし、エントリが1つもない状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。

すでに最大エントリ（80エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。

3.15.3 IPスタティックルーティングの設定



本設定は、ワークシート「IPスタティックルーティング編」を参照して設定を行います。
(「3.2.10 ワークシート「IPスタティックルーティング編」」)

IPのスタティックルーティングの設定を行います。IPスタティックルーティング機能を使用する場合の、設定例を図3-61に示します。

```
*** Set IP static routing configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図3-61 IPスタティックルーティング設定メニュー

以下にIPのスタティックルーティングの追加例を示します。テーブルは、最大256エントリ設定できます。

```
<Add IP static routing data>
destination address [0.0.0.0]: 192.168.2.0
mask [255.255.255.0]:
gateway [0.0.0.0]: 192.168.1.10
metric [1]: 2
preference [50]:
static routing data:
  no  dst address      mask                gateway             metric preference
  ---+-----+-----+-----+-----+-----
  1.  192.168.2.0      255.255.255.0      192.168.1.10       2                50
Add OK (y/n)? [y]:
```

図3-62 IPスタティックルート追加例

IPスタティックルートのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

ただし、エントリが1つもない状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。

すでに最大エントリ（256エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。

3.15.4 DHCPリレーエージェントの設定



本設定は、ワークシート「DHCPリレーエージェント編」を参照して設定を行います。
 (「3.2.11 ワークシート「DHCPリレーエージェント編」」)

DHCPリレーエージェント機能を使用する場合に本設定を行います。DHCPリレーエージェント機能は、BOOTP/DHCPサーバとBOOTP/DHCPクライアントが本装置を介して遠隔地にある場合に、設定を行います。

```

*** Set BOOTP/DHCP relay agent configuration ***
<BOOTP/DHCP relay agent configuration parameter(s)>

relay agent          : use
insert ISDN address  : yes
max hops value       : 4
send request interface: LAN,GroupA,GroupB,BRI#7-1,BRI#7-2
recv request interface: LAN,GroupA,GroupB,BRI#7-1,BRI#7-2

DHCP server list :
no IP address
---+-----
1. 192.52.128.1
2. 158.202.232.3
3. 100.100.100.100
4. 200.200.200.200
Do you change (y/n)? [n]: y
DHCP relay agent (1.use 2.not use) [1]:
MAX hops value [4]:
send request interface:
1.LAN
2.GroupA    3.GroupB    4.BRI#7-1    5.BRI#7-2
Select the number [1,2,3,4,5] :
recv request interface:
1.LAN
2.GroupA    3.GroupB    4.BRI#7-1    5.BRI#7-2
Select the number [1,2,3,4,5] :
DHCP server list (max 4 entries)
no IP address
---+-----
1. 192.52.128.1
2. 158.202.232.3
3. 100.100.100.100
4. 200.200.200.200
Do you change (y/n)? [n]: y

1. change 2. delete 3. add 4. end
Select the number. :

```

図3-63 DHCPリレーエージェント機能の設定例

3.15.5 IPパケットフィルタリングの設定



本設定は、ワークシート「IPパケットフィルタリング編」を参照して設定を行います。
(「3.2.12 ワークシート「IPパケットフィルタリング編」」)

IPパケットフィルタリング機能を使用する場合に本設定によりIPパケットフィルタリングテーブルの設定を行います。本装置のIPパケットフィルタリング機能では、中継を許可するすべてのパケットをフィルタリングテーブルに設定します。テーブルに設定されていないパケットを受信した場合は廃棄されます。

IPパケットフィルタリング機能を使用する場合の、設定例を図3-64に示します。

```
*** Set IP packet filtering configuration (forward) ***  
1. change 2. delete 3. add 4. display 5. end  
Select the number. [5]:
```

図3-64 IPパケットフィルタリングの設定メニュー

以下に、IPパケットフィルタリングの追加例を示します。テーブルは、最大128エントリ登録できます。



メモ：「receive interface」「send interface」を複数選択するときは、「,」で区切って同時に選択します。

```
<Add IP filtering data>
protocol (1:tcp 2:udp 3:tcp+udp 4:all 5:other) [4]: 3
source address [*]:
    mask [255.255.255.255]:
    A=<port<=B A [0]:
        B [65535]: 1024
destination address [*]:
    A=<port<=B A [0]:
        B [65535]:

receive interface :
    1.LAN
    2.GroupA    3.GroupB    4.BRI#7-1    5.BRI#7-2
select the number [1,2,3,4,5]:
send interface :
    1.LAN
    2.GroupA    3.GroupB    4.BRI#7-1    5.BRI#7-2
select the number [1,2,3,4,5]:
mode (1:full 2:half) [1]: 1
IP filtering data:
  2. src address      : *                mask          : 255.255.255.255
     dst address     : *                mask          : 255.255.255.255
     A=<s port<=B    : 0,65535          A=<d port<=B  : 0,65535
     protocol        : tcp+udp          mode          : full
     rcv interface  : LAN,GroupA,GroupB,BRI#7-1,BRI#7-2
     send interface : LAN,GroupA,GroupB,BRI#7-1,BRI#7-2

Add OK (y/n)? [y]:
```

図3-65 IPパケットフィルタリングの追加例

IPパケットフィルタリングのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。表示したいエントリの「src address」を入力します。
- end 設定を終了します。

ただし、エントリが1つもない状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。すでに最大エントリ（128エントリ）登録されているところへ新規エントリを追加しようとする時、「Input error!」と表示され設定できません。

3.16 IPXに関する基本設定

3.16.1 IPXルーティングの設定



本設定は、ワークシート「IPXルーティング編」を参照して設定を行います。（「3.2.13 ワークシート「IPXルーティング編」」）

IPXのルーティングの設定例を以下に示します。

```

*** Set IPX router configuration ***
<IPX router parameter(s)>
  router name:
  routing interface list
  Group/channel network NO.   frame type   tick
  -----+-----+-----+-----
  LAN           00000200   ETHERNET_802.3   1
  [GroupA]     00000111   ETHERNET_802.3   1
  [GroupB]     00000222   ETHERNET_802.3   1
  BRI#6-1      not use IPX routing
  BRI#6-2      00000444   ETHERNET_802.3   1
  BRI#7-1      00000666   ETHERNET_802.3   1
  BRI#7-2      00000777   ETHERNET_802.3   1
  IPX filtering:use
  Do you change (y/n) [n]: y
  router name []: FURU
  routing interface:
  GroupA (y/n) [y]: y
  GroupB (y/n) [y]: y
  BRI#6-1 (y/n) [n]: n
  BRI#6-2 (y/n) [y]: y
  BRI#7-1 (y/n) [y]: n
  BRI#7-2 (y/n) [y]: y
  Select the group/channel to change
    1.LAN
    2.GroupA    3.GroupB    4.BRI#6-2    5.BRI#7-2
  Select the number : 2,4
  GroupA network NO. [00000111]: aaaaaaaa
    node ID.[0000.0000.0000]:
    ticks [1]: 18
  BRI#6-2 network NO. [00000444]: cccccccc
    node ID.[0000.0000.0000]:
    ticks [1]: 85

```

図3-66 IPXルーティング設定例

```

IPX router parameter(s) are set to the following values ***
<IPX router parameter(s)>
  router name:INFONET3790
  routing interface list
  Group/channel network NO.   frame type      tick
  -----+-----+-----+-----
LAN          00000100      ETHERNET_802.3    1
[GroupA]     aaaaaaaaa      ETHERNET_802.3   18
[GroupB]     bbbbbbbbb      ETHERNET_802.3   18
BRI#6-1     not use IPX routing
BRI#6-2     cccccccc      ETHERNET_802.3   85
BRI#7-1     not use IPX routing
BRI#7-2     dddddddd      ETHERNET_802.3   85
  IPX filtering:use
  Set OK (y/n)? [y]:

```

図3-67 IPXルーティング設定例

3.16.2 IPXのISDNリモートターゲットの設定



本設定は、ワークシート「IPXリモートターゲット編」を参照して設定を行います。また、設定項目に関する詳細は、「3.2.14 ワークシート「IPXリモートターゲット編」」を参照してください。

ISDNを選択した場合、宛先IPXのホストIDとISDNリモートターゲットの対応テーブルを設定します。最大80エントリ設定できます。

```

*** Set IPX address target configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]: 3

```

図3-68 IPXリモートターゲットの設定メニュー

以下に、IPXリモートターゲットの追加例を示します。テーブルは、最大80エントリ登録できます。

```
<Add IPX address target>
address []: 222222222222
<Target index>
  1. Osaka
  2. Tokyo
Select the number of target index []: 1

      address      target
      222222222222  Osaka
Add OK (y/n)? [y]:
```

図3-69 IPXリモートターゲットテーブルの追加例

IPXリモートターゲットのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。表示したいエントリの「target」を入力します。
- end 設定を終了します。

ただし、エントリが1つもない状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。すでに最大エントリ（80エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。

3.16.3 IPXパケットフィルタリングの設定



本設定は、ワークシート「IPXパケットフィルタリング編」を参照して設定を行います。
(「3.2.15 ワークシート「IPXパケットフィルタリング編」」)

本装置のIPXパケットフィルタリング機能では、中継を許可するすべてのパケットをフィルタリングテーブルに設定します。テーブルに設定されていないパケットを受信した場合は廃棄されます。IPXパケットフィルタリングの設定例を図3-71に示します。

```
*** Set IPX packet filtering configuration (forward) ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図3-70 IPXパケットフィルタリングの設定メニュー

以下に、IPXパケットフィルタリングテーブルの追加例を示します。テーブルは、最大128エントリ登録できます。



メモ：「receive interface」「send interface」を複数選択するときは、「,」で区切って同時に選択します。

```

<Add IPX filtering data>
protocol (1:ncp 2:spx 3:netbios 4:unknown 5:all 6:other) [5]:
source host number [*]:
    network number [*]:
        A=<sock<=B A [0000]:
            B [ffff]:
destination host number [*]:
    network number [*]:
        A=<sock<=B A [0000]:
            B [ffff]:
receive interface :
    1.LAN
    2.GroupA    3.GroupB    4.BRI#6-2    5.BRI#7-2
select the number [1,2,3,4,5]:
send interface :
    1.LAN
    2.GroupA    3.GroupB    4.BRI#6-2    5.BRI#7-2
select the number [1,2,3,4,5]:
mode (1:full 2:half) [1]:

Selected IPX filtering data:
  2. src host      : *          net          : *          mask: *
     dst host      : *          net          : *          mask: *
     A=<src sock<=B: 0000,ffff  A=<dst sock<=B: 0000,ffff
     protocol      : *          mode         : full
     recv interface: LAN,GroupA,GroupB,BRI#6-2,BRI#7-2
     send interface: LAN,GroupA,GroupB,BRI#6-2,BRI#7-2
Add OK (y/n)? [y]:

```

図3-71 IPXパケットフィルタリングテーブルの追加例

IPXパケットフィルタリングテーブルのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

ただし、エントリが1つも無い状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。すでに最大エントリ（128エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。

3.16.4 IPXスタティックルーティングの設定



本設定は、ワークシート「IPXスタティックルーティング編」を参照して設定を行います。
(「3.2.16 ワークシート「IPXスタティックルーティング編」」)

IPXのスタティックルーティングの設定を行います。IPXスタティックルーティング機能を使用する場合の、設定例を図3-73に示します。

```
*** Set RIP(IPX) static configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図3-72 RIP(IPX)スタティックルーティングの設定例

以下に、IPXスタティックルーティングテーブルの追加例を示します。テーブルは、最大256エントリ登録できます。

```
<Add RIP(IPX) static data>
destination network []: dddd
metric [16]: 2
time ticks [15]:
gateway network NO []: bbbb
      host ID []: eeee

RIP(IPX) static data:
no  dst network metric time ticks gateway
                                (network NO)  (host ID)
----+-----+-----+-----+-----+-----
  2. 0000dddd          2          15    0000bbbb 00000000eeee
Add OK (y/n)? [y]:
```

図3-73 IPXスタティックルーティングテーブルの追加例

IPスタティックルートのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

ただし、エントリが1つもない状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。すでに最大エントリ（256エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。

3.16.5 IPXスタティックSAPの設定



本設定は、ワークシート「IPXスタティックSAP編」を参照して設定を行います。（「3.2.17 ワークシート「IPXスタティックSAP編」」）

IPXのスタティックSAPの設定を行います。IPXスタティックSAP機能を使用する場合の、設定例を図3-75に示します。



メモ：WAN回線にHSDを使用している場合は、本設定は表示されません。

```
*** Set SAP(IPX) static configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図3-74 スタティックSAPの設定例

以下に、IPXスタティックSAPテーブルの追加例を示します。テーブルは、最大256エントリ登録できます。

```
<Add SAP static data>
server name []
:SAKURA
network address []: bb
host address []: b
socket []: b
1. print queue  4. print server          7. advertising print server  10.
other
2. file server  5. archive server        8. unknown
3. job server   6. remote bridge server  9. all
Select the number of service type. [8]: 2
hop to server [16]:4
Add OK (y/n)? [y]:
```

図3-75 IPXスタティックSAPの追加例

IPXスタティックSAPテーブルのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

ただし、エントリが1つもない状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。

すでに最大エントリ（256エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。

3.17 AppleTalkに関する基本設定

3.17.1 AppleTalkの設定



本設定は、ワークシート「AppleTalkルーティング編」を参照して設定を行います。（「3.2.18 ワークシート「AppleTalkルーティング編」」）

AppleTalkの設定例を以下に示します。AppleTalkを用いた大規模なネットワークを構築する場合には、「AURP」を「use」にします。

```
*** Set AppleTalk configuration ***
<AppleTalk parameter(s)>
  AURP protocol: not use
  connect to non-configured exterior router : no
  extra network : use
Do you change (y/n)? [n]: y
AURP protocol (1:use 2:not use) [2]: 1
connect to non-configured exterior router (1:yes 2:no) [2]:
extra network (1.use 2.not use) [1]:
AppleTalk parameter(s) are set to the following values.
<AppleTalk parameter(s)>
  AURP protocol: use
  connect to non-configured exterior router : no
  extra network : use
Set OK (y/n)? [y]:
```

図3-76 AppleTalk設定例

3.17.2 AppleTalkルーティングの設定



本設定は、ワークシート「AppleTalkルーティング編」を参照して設定を行います。（「3.2.18 ワークシート「AppleTalkルーティング編」」）

AppleTalkルーティングの設定例を以下に示します。

```

*** Set AppleTalk routing configuration ***
<AppleTalk routing parameter(s)>

                                seed  network
group/channel routing          remote port  start  end    number
-----+-----+-----+-----+-----+-----
LAN          AppleTalk,IP Tunnel  ----- no    -----  -----  1
GroupA       AppleTalk           router  ---   -----  -----  -----
GroupB       AppleTalk,IP Tunnel  router  ---   -----  -----  -----
ISDN#6-1     AppleTalk           router  ---   -----  -----  -----
ISDN#6-2     not use AppleTalk routing
ISDN#7-1     AppleTalk           router  ---   -----  -----  -----
ISDN#7-2     not use AppleTalk routing
filtering:  not use
Do you change (y/n)? [n]:  y
routing interface:
GroupA (y/n) [y]:  y
GroupB (y/n) [y]:  y
BRI#6-1 (y/n) [y]:  n
BRI#6-2 (y/n) [n]:  n
BRI#7-1 (y/n) [y]:  y
BRI#7-2 (y/n) [n]:  y
Select the group/channel to change
  1.LAN
  2.GroupA   3.GroupB   4.BRI#7-1   5.BRI#7-2
Select the number :  2,4
GroupA IP Tunnel (1.use 2.not use) [2] :  1
      remote (1:router 2:bridge) [1]:
BRI#7-1 IP Tunnel (1.use 2.not use) [2] :  2
      remote (1:router 2:bridge) [1]:
Selected the filtering (1:DDP 2:service 3:nothing) [3]:

```

図3-77 AppleTalkルーティング設定例

```

AppleTalk routing parameter(s) are set to the following values.
<AppleTalk routing parameter(s)>

                                seed  network
                                remote port  start  end    number
-----+-----+-----+-----+-----+-----
LAN          AppleTalk,IP Tunnel  ----- yes    1     10    2
GroupA      AppleTalk,IP Tunnel  router ---  -----  -----
GroupB      AppleTalk,IP Tunnel  bridge yes    100   100   -----
ISDN#6-1    not use AppleTalk routing
ISDN#6-2    not use AppleTalk routing
ISDN#7-1    AppleTalk            router ---  -----  -----  -----
ISDN#7-2    AppleTalk,IP Tunnel  bridge yes    10000 10001 -----
filtering:  not use
Set OK (y/n)? [y]:

```

図3-78 AppleTalkルーティング設定例

3.17.3 AppleTalkのISDNリモートターゲットの設定



本設定は、ワークシート「AppleTalkリモートターゲット編」を参照して設定を行います。
 (「3.2.19 ワークシート「AppleTalkリモートターゲット編」」)

ISDNを選択した場合、AppleTalkルーティングを行うISDNリモートターゲットの対応テーブルを設定します。最大80エントリ設定できます。

```

*** Set AppleTalk address target configuration ***
1. change 2. delete 3. add 4. display 5. end
Select the number. [5]:

```

図3-79 AppleTalkリモートターゲットの設定メニュー

以下に、AppleTalkリモートターゲットテーブルの追加例を示します。

```
<Add AppleTalk address target>
address []: 30
<Target index>
  1. Osaka
  2. Tokyo
Select the number of target index []: 1

      address      target
      30           Osaka
Add OK (y/n)? [y]:
```

図3-80 AppleTalkリモートターゲットテーブルの追加例

AppleTalkリモートターゲットのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。表示したいエントリの「target」を入力します。
- end 設定を終了します。

ただし、エントリが1つもない状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。

すでに最大エントリ（80エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。

3.17.4 外部AppleTalkルータの設定



本設定は、ワークシート「外部AppleTalkルータ編」を参照して設定を行います。また、設定項目に関する詳細は、「3.2.20 ワークシート「外部AppleTalkルータ編」」を参照してください。

外部AppleTalkルータの設定例を以下に示します。

```
*** Set AppleTalk routing IP Tunneling exterior router table ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図3-81 外部AppleTalkルータ設定画面

外部AppleTalkルータテーブルの追加例を以下に示します。テーブルは、最大128エントリ登録できます。

```
<Add AppleTalk routing IP Tunneling exterior router data>
IP Address []: 192.168.1.1
port:
  1.LAN
  2.GroupA    3.GroupB    4.BRI#7-1    5.BRI#7-2
Select the number [1]: 3
AppleTalk routing IP Tunneling exterior router data:
no  IP address      port
----+-----+-----
  2. 192.168.1.1    GroupB
Add OK (y/n)? [y]:
```

図3-82 外部AppleTalkルータテーブル追加例

外部AppleTalkルータテーブルのエントリの設定は、設定メニュー画面では以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

ただし、エントリが1つも無い状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。

すでに最大エントリ（128エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。

3.17.5 AppleTalk DDP (forward) フィルタリングの設定



本設定は、ワークシート「AppleTalk DDP フィルタリング編」を参照して設定を行います。（「3.2.21 ワークシート「AppleTalk DDP (forward) フィルタリング編」」）

DDP (forward) フィルタリングの設定例を以下に示します。

本装置のDDP (forward) フィルタリング機能では、中継を許可するすべてのパケットをフィルタリングテーブルに設定します。テーブルに設定されていないパケットを受信した場合は廃棄されます。DDP(forward)フィルタリングの設定メニューを図3-83に示します。

```
*** Set AppleTalk routing DDP (forward) filtering ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図3-83 AppleTalk DDP (forward) フィルタリングの設定メニュー

以下に、AppleTalk DDP (forward) フィルタリングテーブルの追加例を示します。テーブルは、最大64エントリまで設定できます。



メモ：「receive port」「send port」を複数選択するときは、「，」で区切って同時に選択します。

```

<Add AppleTalk routing DDP (forward) filtering data>
dst network start [0]: 1
      end [65535]: 2
      node [0]: 1
src network start [0]: 1
      end [65535]: 2
      node [0]: 2
DDP type (1:RTMP(Rp/Dt) 2:NBP 3:ATP 4:AEP 5:RTMP(Rq) 6:ZIP 7:ADSP 8:all)
[8]: 1
mode (1:full 2:half) [1]: 1
receive port:
  1.LAN(AppleTalk)      2.LAN(IP tunnel)
  3.GroupA      4.GroupB      5.BRI#7-1      6.BRI#7-2
Select the number [1,2,3,4,5,6]: 1,2
send port :
  1.LAN(AppleTalk)      2.LAN(IP tunnel)
  3.GroupA      4.GroupB      5.BRI#7-1      6.BRI#7-2
Select the number [1,2,3,4,5,6]: 1,2,3,4

AppleTalk routing DDP (forward) filtering data:
  1. dst network start,end: 1,2      host: 1
      dst network start,end: 1,2      host: 2
      DDP type : RTMP
      mode : full
      recv interface: LAN(AppleTalk),LAN(IP tunnel)
      send interface: LAN(AppleTalk),LAN(IP tunnel),GroupA,GroupB
Add OK (y/n)? [y]:

```

図3-84 DDP(forward)フィルタリングの追加例

IPスタティックルートのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

ただし、エントリが1つも無い状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。すでに最大エントリ（64エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。

3.17.6 ゾーンリストの設定



本設定は、ワークシート「AppleTalkゾーンリスト編」を参照して設定を行います。（「3.2.22 ワークシート「AppleTalkゾーンリスト編」」）

本装置のポートが属するネットワークにおいて、本装置をシードルータとして運用する場合、ゾーンリストを設定する必要があります。ゾーンリストはすべてのポート合わせて256個設定できます。

```
*** Set AppleTalk routing zone list configuration ***
1. LAN
2. GroupA
3. BRI#7-2
3. end
Select the number. [3]: 1

*** Set AppleTalk routing zone name (LAN) ***
1. change 2. delete 3. add 4. display 5. end
Select the number. [5]:
```

図3-85 ゾーンリストの設定メニュー

ゾーンリストの追加例を以下に示します。



注意：すでにシードルータが存在するネットワークに本装置をシードルータとして立ちあげた場合で他のシードルータとゾーンリストが異なる場合、本装置はノンシードルータとして運用されます。



メモ：ゾーン名は大文字と小文字を区別していないので、設定時の入力文字と確認時の表示文字は必ずしも同じではありません。

初めての登録の場合は、「default zone」にするかどうかの問い合わせはありません。また、すでに最大ゾーンリスト(256個)登録されているところへ新規ゾーンリストを追加しようとすると、「Input error!」と表示され、設定できません。

ゾーン名を設定する場合、ポート毎に必ず1つのゾーンをデフォルトゾーンとしなければなりません。ゾーン名を1つしか設定しなかった場合は、そのゾーンがデフォルトゾーンになります。

```
<Add AppleTalk routing zone data>
zone name []: Honsha
default zone (1:yes 2:no) [2]:

AppleTalk routing zone data:
  no   zone name
  ----+-----
      3. Honsha
Add OK (y/n)? [y]:
```

図3-86 AppleTalkゾーンリストの追加例

AppleTalkゾーンリストのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

ただし、エントリが1つもない状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。

すでに最大エントリ（256エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。

3.17.7 AppleTalkスタティックルーティングの設定



本設定は、ワークシート「AppleTalkスタティックルーティング編」を参照して設定を行います。
(「3.2.23 ワークシート「AppleTalkスタティックルーティング編」」)

本装置でAppleTalkデータ中継のための自動接続機能を利用する場合、スタティックルーティングテーブルを設定する必要があります。しかし、「AURP protocol」を「use」にしたときは、自動接続機能を利用する場合でもスタティックルーティングテーブルの設定は必要ありません。

```
*** Set AppleTalk static routing configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図3-87 AppleTalkスタティックルーティングの設定メニュー

以下に、AppleTalk スタティックルーティングテーブルの追加例を示します。テーブルは最大128エントリまで登録できます。

```
<Add AppleTalk static routing data>
dst network start []: 200
      end [100]: 299
type(1.AppleTalk 2.ISDN index 3.IP address) []: 1
gateway network number [0]: 10
      node ID [0]: 20
hop [1]:
send port :
  1.LAN(AppleTalk)      2.LAN(IP tunnel)
  3.GroupA      4.GroupB      5.BRI#7-1      6.BRI#7-2
Select the number [] : 3

AppleTalk static routing data:
  no dst network next router
      (str end) type gateway hop send port
-----+-----+-----+-----+-----+-----
  2. 200 299 AppleTalk 10 20 1 GroupA
Add OK (y/n)? [y]:
```

図3-88 AppleTalkスタティックルーティングテーブル追加例

AppleTalkスタティックルーティングテーブルのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

ただし、エントリが1つもない状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。

すでに最大エントリ（128エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。

3.17.8 AppleTalkスタティックゾーンテーブルの設定



本設定は、ワークシート「AppleTalkスタティックゾーン編」を参照して設定を行います。（「3.2.24 ワークシート「AppleTalkスタティックゾーン編」」）



注意：スタティックルーティングで設定されたネットワークには、必ず1つ以上スタティックゾーンを設定する必要があります。正しく設定されていない場合は通信できません。

```
*** Set AppleTalk routing static zone table ***
  1. change  2. display  3. end
Select the number. [3]:
```

図3-89 スタティックゾーンの設定メニュー

(1) 設定の変更

現在設定されているエントリの変更を行う場合は、「change」を選択します。ゾーンリストの変更は、まず変更するゾーンリストが所属するネットワーク番号範囲を選択し、次にそのゾーンリストの内容を変更する順で行います。ただし、ゾーンリストが1つもない状態で「change」を選択するとスタティックルーティングで設定されたネットワーク番号範囲が表示されます。



メモ：スタティックゾーンが所属するネットワーク番号範囲は、スタティックルーティングテーブルに設定されたものから選択します。

```
<AppleTalk routing static zone>
      dst network      dst network      dst network      dst network
      no. (str end)    no. (str end)    no. (str end)    no. (str end)
-----+-----+-----+-----+-----+-----+-----+-----+-----
      1.      1      255
      2.     500     599
Select the number. : 1
```

図3-90 AppleTalkスタティックゾーンテーブルのネットワーク選択例

```
<Set AppleTalk routing static zone table>
<dst network (start: 1 end: 255)>
      1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図3-91 AppleTalkスタティックゾーンテーブルの設定メニュー

- 設定されたエントリの変更

現在設定されているエントリを変更する場合、「change」を選択します。ただし、ゾーンリストが1つもない状態で「change」を選択すると「Input error!」と表示されます。

```
<Change AppleTalk routing static zone data>
Select the entry number. : 1

Selected AppleTalk routing static zone data:
      no  zone
      ----+-----
      1. hiratsuka
zone [hiratsuka]: hiratuka

AppleTalk routing static zone data:
      no  zone
      ----+-----
      1. hiratuka
Change OK (y/n)? [y]:
```

図3-92 AppleTalkスタティックゾーンテーブルの変更例

- 設定されたエントリの削除

現在設定されているエントリを削除する場合、「delete」を選択します。

```
<Delete AppleTalk routing static zone data>
Select the entry number. : 2

Selected AppleTalk routing static zone data:
  no   zone
-----+-----
      2. sapporo
Delete OK (y/n)? [n]:
```

図3-93 AppleTalkスタティックゾーンテーブルの削除例

- 設定されたエントリの追加

現在設定されているエントリを追加する場合、「add」を選択します。

```
<Add AppleTalk routing static zone data>
zone []: kobe

AppleTalk routing static zone data:
  no   zone
-----+-----
      2. kobe
Add OK (y/n)? [y]:
```

図3-94 AppleTalkスタティックゾーンテーブルの追加例

- 設定されたエントリの表示

現在設定されているエントリを表示する場合、「display」を選択します。

```
<AppleTalk routing static zone table (max 128 entries)>
  no   zone
-----+-----
      1. hiratuka
      2. kobe
```

図3-95 AppleTalkスタティックゾーンテーブルの表示例

- 設定の終了

設定を終了する場合、「end」を選択します。すると、「図3-90 AppleTalk スタティックゾーンテーブルのネットワーク選択例」の画面に戻ります。

さらに、「図3-90 AppleTalk スタティックゾーンテーブルのネットワーク選択例」の画面を終了する場合は、「ESC」キーを押します。

(2) 設定されたすべてのエントリの表示

現在設定されているすべてのエントリを表示する場合、スタティックゾーン設定画面（*** Set AppleTalk routing static zone table ***）において「display」を選択します。

```
<AppleTalk routing static zone table (max 128 entries)>
dst network (start:    1 end:  255)
no    zone
-----+-----
      1. hiratuka
      2. kobe
```

図3-96 すべてのAppleTalkスタティックゾーンテーブルの表示例

(3) 設定の終了

AppleTalkスタティックゾーンの設定を終了する場合、「end」を選択します。

3.18 ブリッジに関する基本設定

3.18.1 MACアドレスのISDNリモートターゲットの設定



本設定は、ワークシート「MACアドレスリモートターゲット編」を参照して設定を行います。
(「3.2.25 ワークシート「MACアドレスリモートターゲット編」」)

ISDNを選択した場合、宛先MACアドレスとISDNリモートターゲットの対応テーブルを設定します。最大80エントリ設定できます。

```
*** EXP.: Set MAC address target configuration ***
  1. change  2. delete  3. add  4. display  5.end
Select the number. :
```

図3-97 MACアドレスリモートターゲットの設定メニュー

以下に、MACアドレスリモートターゲットの追加例を示します。テーブルは、最大80エントリ登録できます。

```
<Add MAC address target>
address []: xx:xx:xx:xx:xx:xx
<Target index>
  1. Tokyo   2. Osaka   3. Nagoya
Select the number of target index [1]: 2
      address          target
      xx:xx:xx:xx:xx:xx Osaka
Add OK (y/n)? [y]:
```

図3-98 IPXリモートターゲットデータの追加例

MACアドレスリモートターゲットテーブルのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

ただし、エントリが1つもない状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。すでに最大エントリ（80エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。

3.18.2 ブリッジング機能の設定



本設定は、ワークシート「ブリッジング編」を参照して設定を行います。
 (「3.2.26 ワークシート「ブリッジング編」」)

ブリッジング機能の設定例を図3-99、図3-100に示します。

```

*** Set bridging configuration ***
<Bridging parameter(s)>
  bridging interface:GroupA,GroupB,BRI#6-1
  STP                :not use
  static filtering   :not use
Do you change (y/n)? [n]: y
bridging interface :
  1.GroupA      2.GroupB      3.BRI#6-1      4.BRI#6-2
  5.BRI#7-1     6.BRI#7-2
Select the number [1,2,3]: 1,2,3,4,5,6
static filtering (1:use 2:not use) [1]: 1

Bridging parameter(s) are set to the following values.
<Bridging parameter(s)>
  bridging interface:GroupA,GroupB,BRI#6-1,BRI#6-2,BRI#7-1,BRI#7-2
  STP                :use
  static filtering   :use
Set OK (y/n)? [y]:

```

図3-99 ブリッジング機能設定例 (ISDN選択時)

```
*** Set bridging configuration ***
<Bridging parameter(s)>
  bridging interface:
    STP                :not use
    static filtering   :not use
Do you change (y/n)? [n]: y
bridging interface :
  1.HSD#1
Select the number []: 1
STP (1:use 2:not use) [2]: 1
static filtering (1:use 2:not use) [2]: 1

Bridging parameter(s) are set to the following values.
<Bridging parameter(s)>
  bridging interface:HSD#1
  STP                :use
  static filtering   :use
Set OK (y/n)? [y]:
```

図3-100 ブリッジング機能設定例 (HSD選択時)

3.18.3 送信元 / 宛先フィルタリングの設定



送信元フィルタリングの設定は、ワークシート「送信元フィルタリング編」を参照して設定を行います。（「3.2.27 ワークシート「送信元フィルタリング編」」）



宛先フィルタリングの設定は、ワークシート「宛先フィルタリング編」を参照して設定を行います。（「3.2.28 ワークシート「宛先フィルタリング編」」）

送信元 / 宛先フィルタリング機能の設定例を図3-101に示します。

```
*** Set static address filtering configuration ***
1. default (handling of the other address that not include the filtering
table)
2. source filtering data
3. destination filtering data
4. end
Select the number. [4]:
```

図3-101 アドレスフィルタリングパラメータ設定メニュー

- default
フィルタリングテーブルに設定されていないMACフレームを受信した場合の処理方法を選択します。
- source filtering data
送信元MACアドレスによるフィルタリングテーブルの設定を行います。
- destination filtering data
宛先MACアドレスによるフィルタリングテーブルの設定を行います。
- end
MACアドレスによるフィルタリングの設定を終了します。

(1) アドレスフィルタリングのデフォルトの設定

「default」では、フィルタリングテーブルに設定されていないフレームの処理方法を選択します。送信元アドレスによるフィルタリングテーブルと宛先アドレスによるフィルタリングテーブルのそれぞれに対して選択します。

```
<Static address filtering parameter(s)>
  source default      :forward
  destination default:forward
Do you change (y/n)? [n]: y
source default (1:forward 2:discard) [1]:2
destination default (1:forward 2:discard) [1]:

Static address filtering parameter(s) are set to the following values.
<Static address filtering parameter(s)>
  source default      :discard
  destination default:forward
Set OK (y/n)? [n]:y
```

図3-102 アドレスフィルタリングのデフォルトの設定例

(2) 送信元アドレスフィルタリングの設定

「source filtering data」では、送信元フィルタリングテーブルの設定を行います。

```
*** Set source filtering configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. :
```

図3-103 送信元アドレスフィルタリングテーブル設定メニュー

以下に、送信元アドレスフィルタリングテーブルの追加例を示します。テーブルは、最大64エントリ登録できます。

```
<Add source filtering data>
source address [00:00:00:00:00:00]: xx:xx:xx:xx:xx:xx
send interface:
  1.GroupA      2.GroupB      3.BRI#6-1      4.BRI#6-2
  5.BRI#7-1     6.BRI#7-2     7.nothing
Select the number [1,2,3]: 1,2,3
source filtering data:
  1. source address : xx:xx:xx:xx:xx:xx
     send interface : GroupA,GroupB,BRI#6-1
Add OK (y/n)? [y]:
```

図3-104 送信元アドレスフィルタリングテーブルの追加例

送信元アドレスフィルタリングのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

ただし、エントリが1つもない状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。

すでに最大エントリ（64エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。



メモ：エントリを表示する場合、「send interface」に「nothing」が設定されている場合、「send interface」には何も表示されません。

(3) 宛先アドレスフィルタリングテーブルの設定

設定方法は、「(2) 送信元アドレスフィルタリングの設定」と同じです。

3.18.4 プロトコルフィルタリングの設定



プロトコルフィルタリングの設定は、ワークシート「プロトコルフィルタリング編」を参照して設定を行います。（「3.2.29 ワークシート「プロトコルフィルタリング編」」）

プロトコルフィルタリング機能の設定方法は「3.18.3 送信元/宛先フィルタリングの設定」と最大エントリ数を除いて同じです。プロトコルフィルタリングは、最大32エントリ設定できます。

```
*** Set protocol filtering configuration ***
1. default (handling of the other protocol that not include the filtering
table)
2. filtering table
3. end
Select the number. [3]:
```

図3-105 プロトコルフィルタリング設定メニュー

- default
フィルタリングテーブルに設定されていないIMACフレームを受信した場合の処理方法を選択します。
- filtering table
プロトコルによるフィルタリングテーブルの設定を行います。
- end
プロトコルによるフィルタリングの設定を終了します。

3.19 SNMPに関する基本設定



SNMPエージェント機能に関する設定は、ワークシート「SNMP編」を参照して設定を行います。（「3.2.30 ワークシート「SNMP編」」）

3.19.1 SNMPパラメータの設定

SNMPパラメータの設定例を図3-106に示します。

```

*** Set SNMP manager configuration ***
<SNMP configuration parameter(s)>
sysName      :
sysContact   :
sysLocate    :
  SNMP manager list (max 8 entries)
  IP address  community name      set enable alarm
  -+-----+-----+-----+-----+
  1  0.0.0.0      public          NO          NO
Do you change (y/n)? [n]:y
sysName []
: remote brouter
sysContact []
: honsya
sysLocate []
: kaihatsuka

```

図3-106 SNMPパラメータ設定例

3.18.2 SNMPマネージャリストの設定

SNMPマネージャリストの設定例を図3-107に示します。

```

SNMP manager list (max 8 entries)
  IP address  community name      set enable alarm
  -+-----+-----+-----+-----+
  1  0.0.0.0      public          NO          NO
Do you change (y/n)? [n]: y

  1. change  2. delete  3. add  4. end
Select the number. : 3

```

図3-107 SNMPマネージャリストの設定例



注意：SNMPマネージャを設定するときは以下の点に注意してください。

- SNMPマネージャのエントリは、IPアドレスの昇順に並べ替えられますので、入力した順番には表示されません。
- IPアドレスとコミュニティ名が同じエントリは登録できません。新規登録の場合に、すでに存在するエントリと同じIPアドレスを入力し、すでに存在するエントリと同じコミュニティ名を入力すると「Input error!」と表示され、設定できません。

以下に、SNMPマネージャリストの追加例を示します。テーブルは、最大8エントリ登録できます。

```
<Add SNMP manager>
IP address [0.0.0.0]: 192.168.5.1
community name [public]
:
set enable(1:YES 2:NO) [2]: 1
alarm(1:YES 2:NO) [2]:
SNMP manager:
      IP address      community name      set enable alarm
-----+-----+-----+-----+-----
      192.168.5.1    public                YES          NO
Add OK (y/n)? [y]:
```

図3-108 SNMPマネージャリストの追加例

SNMPマネージャリストのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change エントリを変更します。変更したいエントリの番号を入力します。
- delete エントリを削除します。削除したいエントリの番号を入力します。
- add エントリを追加します。
- display エントリを表示します。表示したいエントリの「dst address」を入力します。
- end 設定を終了します。

ただし、エントリが1つもない状態で「change」、「delete」を選択すると「Input error!」と表示され、設定できません。また、「display」を選択すると「no entry.」と表示されます。すでに最大エントリ（8エントリ）登録されているところへ新規エントリを追加しようとすると、「Input error!」と表示され設定できません。

3.20 設定内容の確認

すべての設定が完了すると、設定内容の確認を行うことができます。確認を行う場合には、次のメニューにおいて「y」キーを入力します。「n」キーを入力すると、次のメニューに移ります。（ 「3.7 設定情報の表示」 ）

```
Now you have set all configurations!  
Do you display the configurations (y/n)? [y]:
```

図3-109 設定内容確認の問い合わせメニュー

3.21 設定内容の適用

最後に設定後の動作を選択します。

```
Do you display the configurations (y/n)? [n]:  
  
1. Save new parameter(s) and reset      3. Configurations set again  
2. Save new parameter(s) only          4. Quit (no save and no reset)  
Select the number. :
```

図3-110 設定後動作メニュー（1）

- Save new parameter(s) and reset
設定内容を保存後、装置をリセットします。
- Save new parameter(s) only
設定内容の保存のみを行います。
- Configurations set again
これまで入力した値をデフォルト値として再度最初のメニューより設定を行います。
- Quit (no save and no reset)
入力したデータを無効にしてメインメニューへ移行します。

4章 拡張設定

この章では、装置の拡張設定について説明します。
拡張設定とは、基本設定で設定できない細かな設定をさします。
この章の内容を以下にまとめます。

- 拡張設定の流れ
- データリンクに関する設定
- ブリッジングに関する拡張設定
- ICMPリダイレクトメッセージの設定
- IPに関する拡張設定
- IPXに関する拡張設定
- AppleTalkに関する拡張設定
- SNMPに関する拡張設定
- リモートファイルメンテナンスの設定
- データ別優先制御に関する拡張設定
- トラヒックロギング
- 呼確立リミッタの設定
- リモートターゲットの設定
- ルータグループ機能の設定



注意：基本設定の前に拡張設定を行ってはいけません。

4.1 拡張設定の流れ

拡張設定は、メインメニューの「configuration set (expert)」で行います。設定を行うためには、管理者資格（スーパーモード）になっている必要があります。（「3.5 管理者資格への移行」）一般資格（ノーマルモード）のまま「configuration set (expert)」を選択した場合には、「User mode mismatch!」と表示され設定できません。

拡張設定は、設定項目が関連したグループに分かれています。必要な部分を各グループ単位で設定を行います。グループ単位の設定動作を図4-1に示します。

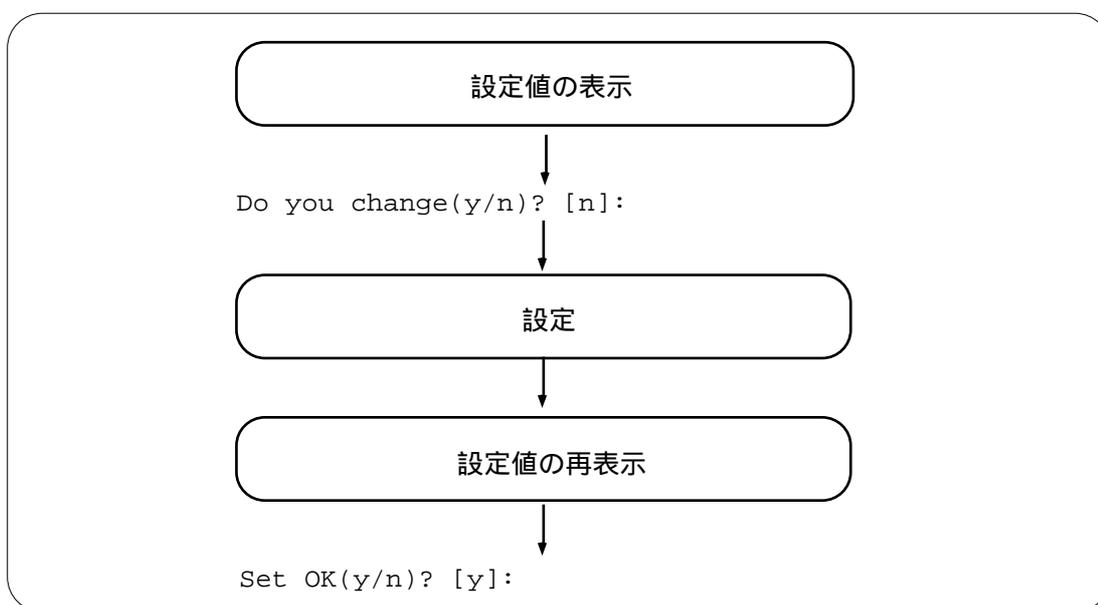


図4-1 拡張設定入力の流れ

- 「設定値の表示」の部分では、設定を行う項目の現在の値を表示します。表示されている項目を設定する場合は、「Do you change(y/n)? [n]:」で「y」キーを入力します。「設定」の部分が表示されます。「n」キーを入力した場合は、拡張設定のメニューに戻ります。
- 「設定」の部分で設定を行います。
- グループ内の設定が終了すると、設定した内容を「設定値の再表示」の部分に表示し、「Set OK(y/n)? [y]:」が表示されます。設定内容を確認し、「y」キーまたは「リターン」キーを入力すると拡張設定のメニューに戻ります。この時、設定値は装置内メモリに保存されます。「設定値の再表示」で「n」キーを入力することで、再度設定することができます。「n」キーを入力した場合は設定値は装置内メモリには保存されません。
- 各々のメニューの設定が終了し、メインメニューへ戻る場合は、「ESC」キーを押します。

拡張設定のメニューを図4-2に示します。

```
*** Expert mode (configuration) menu ***
1. datalink
2. bridging
3. ICMP redirect
4. IP routing
5. IPX routing
6. AppleTalk routing
7. SNMP
8. remote file maintenance
9. packet priority control
10. traffic logging
11. limitation of ISDN connection period      ISDN選択時のみ
12. remote target                            ISDN選択時のみ
13. router grouping                          ISDN選択時のみ
Select the number. :
```

図4-2 拡張設定メニュー

- datalink
WAN回線に関する設定を行います。(「4.2 データリンクに関する設定」)
- bridging
ブリッジング機能に関する設定を行います。(「4.3 ブリッジングに関する拡張設定」)
- ICMP redirect
ICMP リダイレクト機能に関する設定を行います。(「4.4 ICMPリダイレクトメッセージの設定」)
- IP routing
IPルーティングに関する設定を行います。(「4.5 IPに関する拡張設定」)
- IPX routing
IPXルーティングに関する設定を行います。(「4.6 IPXに関する拡張設定」)
- AppleTalk routing
AppleTalkルーティング機能に関する設定を行います。(「4.7 AppleTalkに関する拡張設定」)

- SNMP
SNMPエージェント機能に関する設定を行います。(「4.8 SNMPに関する拡張設定」)

- remote file maintenance
システムのアップデート等保守に関する設定を行います。(「4.9 リモートファイルメンテナンスの設定」)

- packet priority control
データ別優先制御機能に関する設定を行います。(「4.10 データ別優先制御に関する拡張設定」)

- traffic logging
トラフィックロギング機能に関する設定を行います。(「4.11 トラフィックロギングに関する設定」)

- limitation of ISDN connection period (ISDN選択時のみ)
呼確立リミッタに関する設定を行います。(「4.12 呼確立リミッタの設定」)

- remote target (ISDN選択時のみ)
リモートターゲットの設定を行います。(「4.13 リモートターゲットの設定」)

- router grouping (ISDN選択時のみ)
ルータグループ化機能に関する設定を行います。(「4.14 ルータグループ化機能の設定」)

4.2 データリンクに関する設定

WAN回線のデータリンクの設定を行います。WAN回線に関する拡張設定は、メニュー画面で「configuration set (expert)」を選択後「datalink」を選択することで設定できます。

```
*** EXP.: Set datalink extension configuration ***
      1.HSD#1      2.HSD#2      3.HSD#3
Select the number. : 1

<Datalink extension parameter(s)>
                                     HSD#1
-----+-----
watching line                        on
data compress                         no
PPP send retry                       10
PPP restart timer (10ms)             100
PPP loop timer (sec)                 10
Do you change (y/n)? [n]: y
```

図4-3 データリンクの設定画面例(HSD選択時)

```

*** EXP.: Set datalink extension configuration ***
  1.GroupA      2.TetsuG      3.GroupB      4.BRI#6-1      6.BRI#7-2
  5.BRI#6-2     6.BRI#7-1
Select the number : 1
<Datalink extension parameter(s)>
                                     GroupA
-----+-----
watching line                          on
interface up mode                       always
data compress                           no
congestion timer (sec)                   1
max retry calling                        8
PPP send retry                           10
PPP restart timer (10ms)                 100
PPP loop timer (sec)                     10
idle timer (sec)                         60
Do you change (y/n)? [n] : y
watching line(1:on 2:off) [1]:
interface up mode (1:always 2:normal) [1]:
data compress (1:auto 2:no 3:fixed) [2]:
congestion timer (sec) [1]:
max retry calling [8]:
PPP send retry [10]:
PPP restart timer (10ms)[100]:
PPP loop timer (sec)[10]:
idle timer (sec)[60]:
EXP.: Datalink extension parameter(s) are set to the following values.
                                     GroupA
-----+-----
watching line                          on
interface up mode                       always
data compress                           no
congestion timer (sec)                   1
max retry calling                        8
PPP send retry                           10
PPP restart timer (10ms)                 100
PPP loop timer (sec)                     10
idle timer (sec)                         60
Set OK (y/n)? [y]:

```

図4-4 データリンクの設定画面例(ISDN選択時)

(1) WAN回線(HSDまたはISDN)の設定

- watching line
 WAN回線上のフラグ同期監視モード。
 設定範囲： 1: on (監視する)
 2: off (監視しない)
 導入時の設定： 1: on

- interface up mode (ISDN選択時のみ)
 ISDN回線インタフェース状態。
 設定範囲： 1: always ISDN回線の接続 / 切断にかかわらずISDN回線から
 得た ルーティング情報を常に有効とする。
 2: normal ISDNの回線接続時のみISDN回線から得たルーティング情
 報を常に有効とする。
 導入時の設定： 2: normal

- メモ：本設定はISDNを利用してIPルーティングを行う場合で、ISDNを着信専用、手動、指定時刻による接続にした場合に必要となります。


- 注意：「interface up mode」とその他の条件によって、IP/IPXのダイナミックルーティング機能が使用できない場合があります（「3.2.6 ワークシート「ISDN通常回線編」」）。


- data compress
 データ圧縮の方法を設定します。「auto」を選択すると、接続相手と圧縮アルゴリズムのネゴシエーションを行います。ネゴシエーションが完了すれば圧縮データの送受信を行います、完了できなければ圧縮データの送受信は行いません。「no」を選択するとネゴシエーションを行いません（データ圧縮の動作を行いません）。「fixed」を選択すると、ネゴシエーションは行いますが、その結果にかかわらず圧縮データの送受信を行います。データ圧縮の設定は、接続相手と同じものを選択してください。
 設定範囲： 1:auto (実行)
 2:no (非実行)
 3:fixed (圧縮固定)
 導入時の設定： 2:no

- congestion timer (ISDN#1のみ)
 輻輳継続許容時間。設定された時間以上輻輳状態が継続した場合、自動トラヒック分散機能を開始します。
 設定範囲： 1 ~ 3600 [sec]
 導入時の設定： 1

- max retry calling (ISDN選択時のみ)

RESET 相手あるいは網の障害により接続している回線が切断された場合に行うリトライの回数。
設定範囲： 0 (リトライなし)
1 ~ 254 (リトライ回数)
255 (無限回)
導入時の設定： 8



メモ：手動、中継データによるISDN接続失敗時にはリトライは行いません。

- PPP send retry
RESET PPP最大パケット再送回数。PPPのリンク確立に失敗した場合、リンク確立要求を設定された回数分再送します。
設定範囲： 0 ~ 255
導入時の設定： 10

- PPP restart timer
RESET PPP リスタートタイマ値。リンク確立要求を再送する場合のタイマ値。
設定範囲： 100 ~ 6000 [10msec]
導入時の設定： 100

- PPP loop timer
RESET PPPのネゴシエーションの無限ループを検出するタイマ値。タイマが満了するまでPPPのネゴシエーションを継続します。
設定範囲： 1 ~ 60 [sec]
導入時の設定： 10

- idle timer (ISDN選択時のみ)
RESET ISDN回線の無通信監視タイマ。中継データによる自動切断を行う場合、タイマが満了するまで無通信状態が継続した時に回線を切断します。また、トラヒック分散を自動終了する場合、トラヒックが減少してトラヒック分散回線で無通信状態が継続した時にトラヒック分散を終了します。
設定範囲： 1 ~ 3600 [sec]
導入時の設定： 60



メモ：idle timerの設定は、相手先との距離により課金単位を目安にして設定すると効率的です。以下に設定の目安を記述しますので参考にしてください。

例：3分毎に10円ずつ課金される場合 idle timer : 180
1分毎に100円ずつ課金される場合 idle timer : 60

4.3 ブリッジングに関する拡張設定

ブリッジングに関する拡張設定を行います。ブリッジング機能の拡張機能はメニュー画面で「configuration set (expert)」を選択後「bridging」を選択することで設定できます。

```
*** EXP.: Bridging configuration menu ***
1. STP(general)
2. STP(each line)
3. filtering database agetime
4. bridge max forward delay
Select the number. :
```

図4-5 ブリッジング機能拡張設定メニュー

4.3.1 STPの設定

(1) STP (装置単位) の設定

図4-5で「STP(General)」を選択すると以下の画面が表示されます。

```
*** EXP.: Set STP configuration ***
<STP general parameter(s)>
  bridge priority          : 32768
    max age (sec)         : 20
    hello time (sec)     : 2
    forward delay (sec)  : 15
Do you change (y/n)? [n]:
bridge priority [32768]:
  max age (sec) [20]:
  hello time (sec) [2]:
  forward delay (sec) [15]:
Set OK (y/n)? [y]:
```

図4-6 STP (装置単位) の設定例

- RESET** - bridge priority
ルートブリッジ(Root Bridge)を決定するために使用するブリッジ優先度(Bridge Priority)を設定します。
設定範囲： 0 ~ 65535
導入時の設定： 32768

- RESET** - max age
本装置がルートブリッジになった場合に送信するBPDU内の最大エージ時間(Max age)として使用する値を設定します。
設定範囲： 6 ~ 40[sec]
導入時の設定： 20
- RESET** - hello time
本装置がルートブリッジになった場合に送信するBPDU内のハロータイム(Hello Time)として使用する値を設定します。本装置がルートブリッジの場合はBPDUはこの時間間隔で送信されます。
設定範囲： 1 ~ 10[sec]
導入時の設定： 2
- RESET** - forward delay
本装置がルートブリッジになった場合に送信するBPDU内のフォワード遅延(Forward Delay)として使用する値を設定します。本装置がルートブリッジの場合は、ポートの状態がフォワードに遷移する時のフィルタリングデータベース(アドレス学習テーブル)のエージングタイマに使用されます。
設定範囲： 4 ~ 30[sec]
導入時の設定： 15



メモ：max age, hello timeおよびforward delayの設定は以下の関係式を満たすように設定します。
$$2 \times (\text{forward delay} - 1) \leq \text{max age} \leq 2 \times (\text{hello time} + 1)$$

(2) STP (各回線) の設定

図4-5で「STP(each line)」を選択すると以下の画面が表示されます。ここでは、変更するチャンネルを選択し、そのチャンネルに関する設定を行います。チャンネルの選択肢は、LANと「bridging interface」で選択されたグループ/チャンネルとする。

```

*** EXP.: Set STP configuration ***
<STP each line parameter(s)>
  1.LAN
  2.GroupA    3.GroupB    4.BRI#6-1    5.BRI#6-2
  6.BRI#7-1   7.BRI#7-2
Select the number : 2
  interface priority path cost domain
  -----+-----+-----+-----
  GroupA    128      15625      off
Do you change (y/n)? [n]: y
priority [128]:
path cost [15625]:
domain (1:on 2:off) [2]: on
  interface priority path cost domain
  -----+-----+-----+-----
  GroupA    128      15625      on

```

図4-7 STP (各回線) の設定例

- RESET** - priority

ポートの優先度(Port Priority)を設定する .

設定範囲 : 0 ~ 255

導入時の設定 : 128
- RESET** - pathcost

ポートのパスコスト(Path Cost)を設定する .

設定範囲 : 1 ~ 65535

導入時の設定 : LAN:100

HSD (64Kbps) :15625 (128Kbps) :7813

ISDN:15625
- RESET** - domain

STPドメインを分離するかどうかを選択します . 分離する場合はBPDUを中継しない .

(LANでは設定不可)

設定範囲 :

1 : on (分離する)

2 : off (分離しない)

導入時の設定 : 2 : off

4.3.2 アドレス学習テーブルのエイジアウト時間

アドレス学習テーブルのエイジアウト時間を設定します。

```
*** EXP.: Set filtering database agetime parameter(s) ***
    agetime (sec): 300
Do you change (y/n)? [n]: y
    agetime (sec) [300]: 200

EXP.: Filtering database agetime parameter(s) is set to the following
values.
    agetime (sec): 200
Set OK (y/n)? [y]:
```

図4-8 アドレス学習テーブルエイジアウト時間設定例

- RESET** - agetime
アドレス学習テーブルのエイジアウト時間を設定する。
設定範囲： 10 ~ 1000000[sec]
導入時の設定： 300

4.3.3 フレームの最大中継遅延時間

フレームの最大中継遅延時間を設定します。

```
*** EXP.: Set bridge max forward delay parameter(s) ***
    bridge max forward delay (10msec): 200
Do you change (y/n)? [n]: y
    bridge max forward delay (10msec) [200]: 50

EXP.: Bridge max forward delay parameter(s) is set to the following values.
    bridge max forward delay (10msec): 50
Set OK (y/n)? [y]:
```

図4-9 フレームの最大中継遅延時間設定例

- RESET** - bridge max forward delay
ブリッジングフレームの最大中継遅延時間を設定します。ブリッジングフレームの受信後中継するまでに最大中継遅延時間以上の時間が経過した場合にはそのフレームを廃棄します。
設定範囲： 50 ~ 400 [10msec]
導入時の設定： 400

4.4 ICMPリダイレクトメッセージの設定

ICMPリダイレクト機能に関する設定を行います。ICMPリダイレクト機能はメインメニューで「configuration set (expert)」を選択後「ICMP redirect」を選択して設定します。

```

*** EXP.: Set ICMP redirect configuration ***
<ICMP redirect parameter(s)>
mode      : on
preference: 20
interface : LAN,GroupA,GroupB,BRI#7-1,BRI#7-2
trust gateways list (max 10 entries)
    All gateways
Do you change (y/n)? [n]: y
mode (1:on 2:off) [1]:
preference [20]:
interface :
    1.LAN
    2.GroupA    3.GroupB    4.BRI#6-1    5.BRI#6-2
    6.BRI#7-1    7.BRI#7-2
Select the number [1,2,3,4,5]
<Set trust gateways list>
    trust gateways list (max 10 entries)
        All gateways
Do you change (y/n)? [n]: y

    1. change  2. delete  3. add  4. end
Select the number. : 3

<Add trust gateway data>
trust gateway []: 192.168.1.1
trust gateway data:
    1. 192.168.1.1
Add OK (y/n)? [y]:

```

図4-10 ICMPリダイレクトメッセージ設定例

RESET

- mode

ICMPリダイレクトメッセージを受信する/しないを設定します。「受信する」に設定した場合は、ICMPリダイレクトメッセージによりルーティング情報の学習を行います。

設定範囲： 1: on (受信する)
2: off (受信しない)

導入時の設定： 1: on



注意：本設定はIPルーティング動作をしない場合のみ有効となります。IPルーティング動作をする場合は、設定値に関係無く、ICMPリダイレクトメッセージ受信によるルーティング情報の学習は行いません。

RESET

- preference

ICMPリダイレクトメッセージによるルーティング情報の優先順位を設定します。同じ宛先に対するルーティング情報がRIP、スタティックルート、またはICMPリダイレクトメッセージ受信で重複した場合、この「preference」値で有効とするルート情報の優先順位をつけます。経路を選択する際は、「preference」値の小さな値のルーティング情報が有効となります。「preference」値はRIPが100固定、スタティックルートが導入時の設定で50です。（「3.2.10 ワークシート「IPスタティックルーティング編」」）また、直接インタフェースに接続されたネットワークに対するルーティング情報の場合は、インタフェースで設定したルーティング情報の場合は、インタフェースで設定したルーティング情報に対する「preference」値（導入時の設定が0）も考慮する必要があります。（4.5.2 RIPインタフェースの設定）

設定範囲： 0 ~ 255

導入時の設定： 20

RESET

- interface

ICMPリダイレクトメッセージを受信するインタフェースを設定します。設定されていないインタフェースからICMPリダイレクトメッセージを受信してもルーティング情報の学習は行いません。

設定範囲： LAN, 「bridging interface」で選択されたグループおよびチャンネル

導入時の設定： LAN, 「bridging interface」で選択されたグループおよびチャンネル

RESET

- trust gateway

ICMPリダイレクトメッセージを受信する送信元ゲートウェイのIPアドレスを設定します。設定されたゲートウェイ以外からのICMPリダイレクトメッセージは受信しません。

設定範囲： xxx.xxx.xxx.xxxの形式 (最大10エントリ)

導入時の設定： All gateways (すべてのゲートウェイから、ICMPリダイレクトメッセージを受信する)

「trust gateway」のエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。

4.5 IPに関する拡張設定

IPルーティング機能に関する拡張設定を行います。IPルーティングの拡張機能はメインメニューで「configuration set (expert)」を選択後「IP routing」を選択することで設定できます。

```
*** EXP.: IP routing configuration menu ***
 1. RIP motion
 2. RIP interface
 3. RIP filtering (accept gateway)
 4. RIP filtering (propagate gateway)
 5. RIP filtering (interface accept)
 6. RIP filtering (interface propagate)
 7. proxy ARP
 8. static routing
 9. IP filtering (forward)
10. IP filtering (discard)
11. OSPF configuration
Select the number. :
```

図4-11 IPルーティング拡張設定メニュー

- RIP motion
RIPの動作に関する拡張設定を行います。
- RIP interface
RIPのインタフェースに関する動作を設定します。
- RIP filtering(accept gateway)
送信元ゲートウェイ単位で受信するルーティング情報を制限します。
- RIP filtering(propagate gateway)
送信元ゲートウェイ単位で送信するルーティング情報を制限します。
- RIP filtering(interface accept)
送信元インタフェース単位で受信するルーティング情報を制限します。
- RIP filtering(interface propagate)
送信元インタフェース単位で送信するルーティング情報を制限します。
- proxy ARP
Proxy ARP (代理ARP) に関する設定を行います。

- static routing
スタティックルーティングテーブルを設定します。この設定は基本設定で行う「3.15.2 IPスタティックルーティングの設定」と同じです。
- IP filtering(forward)
中継パケットのフィルタリングテーブルの設定を行います。この設定は基本設定で行う「3.15.3 IPパケットフィルタリングの設定」と同じです。
- IP filtering(discard)
中継パケットのフィルタリングテーブルの設定を行います。IPパケットフィルタリング機能を使用する場合、「IP filtering(forward)」で設定されたパケットでも本テーブルに設定されたパケットは中継しません。
- OSPF configuration
OSPFに関する設定を行います。
- DHCP relay agent
DHCPリレーエージェント機能に関する設定を行います。

4.5.1 RIP(IP)に関する拡張設定

RIPの動作に関する拡張設定を行います。

```
*** EXP.: Set RIP(IP) motion configuration ***
1. motion parameter(s)
2. trust gateways
3. source gateways
4. end
Select the number. [4]: 1
```

図4-12 RIP動作モード設定メニュー

(1) RIPの動作モードの設定

「motion parameter(s)」を選択して、RIPの動作モードの設定を行います。

```

*** EXP.: Set RIP(IP) motion configuration ***
<RIP(IP) motion parameter(s)>
  mode          : supplier
  default metric: 16
Do you change (y/n)? [n]: y
mode (1:supplier 2:point to point 3:quiet 4:off) [1]:
default metric [16]:

EXP.: RIP(IP) motion parameter(s) are set to the following values.
<RIP(IP) motion parameter(s)>
  mode          : supplier
  default metric: 16
Set OK (y/n)? [y]:

```

図4-13 RIP動作モード設定例

RESET

- mode

RIPの動作モードを設定します。

設定範囲：	1: supplier	(ブロードキャストのインタフェースにはブロードキャスト、ポイントツーポイントのインタフェースには相手アドレス宛てにRIPの定期 updateおよび triggered update を送信する。)
	2: point to point	(source gateway (下記) で設定されたゲートウェイ宛てにRIPの定期 updateおよびtriggered updateを送信する。)
	3: quiet	(RIPの定期updateおよびtriggered updateを送信しない)
	4: off	(RIPを動作しない。)

導入時の設定： 1: supplier

- default metric

OSPFで獲得したルーティング情報をRIPで送信する場合のメトリック値。これは、OSPFを使用する場合に必要な項目ですので、OSPFを使用しない場合は、導入時の設定のままにかまいません。

設定範囲： 0 ~ 16

導入時の設定： 16

(2) トラストゲートウェイの設定

「trust gateways」を選択して、有効なルーティング情報を提供してくれるゲートウェイ(トラストゲートウェイ)を登録します。

```
*** EXP.: Set RIP(IP) motion (trust gateways) configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. :
```

図4-14 トラストゲートウェイ設定メニュー

RESET

- trust gateway

有効なルーティング情報を提供してくれるゲートウェイのIPアドレスを登録します(最大20エン트리)。登録されたゲートウェイからのRIP情報のみ有効とします。登録が無い場合はすべてのゲートウェイからのRIP情報を有効とします。

設定範囲： xxx.xxx.xxx.xxxの形式

導入時の設定： なし

「trust gateway」のエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

(3) ソースゲートウェイの設定

「source gateways」を選択して、ルーティング情報を提供するゲートウェイ(ソースゲートウェイ)を登録します。設定メニューはトラストゲートウェイと同じ形式です。

RESET

- source gateway

「mode」が「point to point」の場合、ルーティング情報を提供するゲートウェイのIPアドレスを登録します(最大40エン트리)。RIPの定期アップデートおよびトリガードアップデートを登録されたゲートウェイのみに送信します。登録がない場合は、どのゲートウェイにもRIPの定期updateおよびtriggered updateを送信しません。

設定範囲： xxx.xxx.xxx.xxxの形式

導入時の設定： なし

「source gateway」のエントリの設定方法は、「(2) トラストゲートウェイの設定」と同じです。

4.5.2 RIP(IP)インタフェースの設定

RIPのインタフェースに関する動作を設定します。

```

*** EXP.: Set RIP(IP) interface configuration ***
<RIP(IP) interface parameter(s)>
  1.LAN
  2.BRI#1-1
Select the number. : 2
      send   rcv   metric pre-   broad- interval   ageout time
      control control   ference   cast   (sec)   (sec)
-----+-----+-----+-----+-----+-----+-----+-----
BRI#1-1 RIP2   RIP2   0     0     off   30     off   180
<RIP2 password>
  BRI#1-1:pass
Do you change (y/n)? [n]: y
BRI#1-1 RIP send control (1:RIP1 2:RIP2 3:RIP1,2 4:off) [2]: 3
      rcv control (1:RIP1 2:RIP2 3:RIP1,2 4:off) [2]: 2
  password [pass]:
  metric [0]:
  preference [0]:
  broadcast (1:on 2:off) [2]:
  broadcast interval (sec) [30]:
  RIP entry ageout (1:on 2:off) [2]:
  ageout time (sec) [180]:

EXP.: RIP(IP) interface parameter(s) are set to the following values.
<RIP(IP) interparameter(s)>

      send   rcv   metric pre-   broad- interval   ageout time
      control control   ference   cast   (sec)   (sec)
-----+-----+-----+-----+-----+-----+-----+-----
BRI#1-1 RIP1,2 RIP2   0     0     off   30     off   180
<RIP2 password>
  BRI#1-1:pass
Set OK (y/n)? [y]:

```

図4-15 RIP(IP)インターフェース拡張設定例

以下に示す設定はインタフェース毎に設定します。ただし、ISDN回線については基本設定の運用形態で定義されている回線のみ問い合わせます。

4章 拡張設定

- RESET** - send control
RIP情報の送信方法を選択します。
設定範囲： 1:RIP1 (RIP1で送信)
2:RIP2 (RIP2で送信)
3:RIP1,2 (RIP2をブロードキャスト宛に送信)
4:off (送信しない)
導入時の設定： 1:RIP1
- RESET** - recv control
RIP情報の受信方法を選択します。
設定範囲： 1:RIP1 (RIP1を受信)
2:RIP2 (RIP2を受信)
3:RIP1,2 (RIP1およびRIP2を受信)
4:off (受信しない)
導入時の設定： 1:RIP1
- RESET** - password
上記で「RIP2」または「RIP1,2」を選択した場合、認証を行うためのパスワードを設定します。パスワードを消去する場合は「"」を入力します。
設定範囲： 最大16文字の英数字
導入時の設定： なし
- RESET** - metric
インタフェースのメトリック値を設定します。RIPの受信時、「"RIPパケットに設定されたメトリック" + 1 + "本設定値"」をルーティング情報として保持します。
設定範囲： 0 ~ 16
導入時の設定： 0
- RESET** - preference
直接インタフェースに接続されたネットワークに対するルーティング情報がRIP、スタティック設定、ICMPリダイレクトメッセージによって学習したルーティング情報と重複した場合、どのルーティング情報を優先するかを決定する優先順位を設定します。
「preference」値は、値の小さい方が優先されます。本装置の「preference」値はRIPが100固定、スタティック設定の値が導入時の設定で50 (3.2.10 ワークシート「IPスタティックルーティング編」)、ICMPリダイレクトメッセージの値が導入時の設定で20 (「4.4 ICMPリダイレクトメッセージの設定」) です。
設定範囲： 0 ~ 255
導入時の設定： 0
- RESET** - broadcast
send controlがonのときのRIPの送信方法を選択します。
設定範囲： 1: on (定期update)
2: off (triggered update)
導入時の設定： 2: off

- RESET** - broadcast interval
ISDN回線にRIPの定期アップデートの送信する場合の、定期送信間隔を設定します。
設定範囲： 30 ~ 2147483647[sec]
導入時の設定： 30
- RESET** - RIP entry ageout
RIPにより学習したルーティング情報のエージアウトする/しないを選択します。
設定範囲： 1: on (エージアウトする)
2: off (エージアウトしない)
導入時の設定： 2: off
- RESET** - ageout time
RIPにより学習したルーティング情報のエージアウトする場合のエージアウト時間を設定します。
設定範囲： 30 ~ 2147483647[sec]
導入時の設定： 180



注意：ISDN回線にRIPの定期アップデートの送信する場合、本装置とISDN回線を介して接続している相手側の装置の「ageout time」を、「broadcast interval」より大きい値に設定してください(約6倍)。

4.5.3 RIP(IP)フィルタリング(accept gateway)の設定

RIPパケット受信(accept)時、相手先ゲートウェイにより有効にする(あるいは無効にする)ルーティング情報を限定することができます。

```
*** EXP.: Set RIP(IP) filtering (accept GW) configuration ***
1. filtering mode
2. filtering table
3. end
Select the number. [3]:1
```

図4-16 RIP(IP)フィルタリング(accept gateway)拡張設定例

(1) フィルタリングテーブルの属性の設定

図4-16に示した画面で「filtering mode」を選択し、フィルタリングテーブルの属性を選択します。フィルタリングテーブルの属性を有効にするとした場合、テーブルに設定されているエントリに一致したRIP情報は、ルーティングテーブルに登録します。無効にするとした場合、テーブルに設定されているエントリに一致したRIP情報はルーティングテーブルには登録しません。

```
RIP(IP) filtering (accept gateway) parameter(s)>
  mode: exclude
Do you change (y/n)? [n]:
```

図4-17 RIP(IP)フィルタリングテーブル(accept gateway)属性

RESET

- mode

テーブルに設定されているエントリに一致したものを有効にするか、無効にするかを選択します。

設定範囲： 1: include (有効にする)

2: exclude (無効にする)

導入時の設定： 2: exclude

(2) フィルタリングテーブルの設定

図4-16に示した画面で「filtering table」を選択し、有効にする（あるいは無効にする）ルーティング情報として、宛先IPアドレスと相手ゲートウェイのIPアドレスを設定します。ゲートウェイが最大32個、1ゲートウェイあたりの宛先アドレスとして最大4エントリ、総計128エントリのテーブルが登録できます。

```
<RIP(IP) filtering (accept gateway) table>
  1. change 2. delete 3. add 4. display 5. end
Select the number. [5]: 3

destination address [0.0.0.0]: 192.168.1.1
mask []: 255.255.255.0
gateway address []: 192.168.2.1
RIP(IP) filtering (propagate gateway) data:
  no  dst address      mask                gateway address
  ----+-----+-----+-----
  1. 192.168.1.1      255.255.255.0     192.168.2.1
Add OK (y/n)? [y]:
```

図4-18 RIP(IP)フィルタリングテーブル(accept gateway)設定例

- RESET** - destination address
 ルーティング情報の宛先IPアドレスを設定します。
 設定範囲： xxx.xxx.xxx.xxxの形式
 導入時の設定： 0.0.0.0

- RESET** - mask
 destination addressに対するマスクパターンを設定します。上記のdestination addressと組み合わせることで設定することによって、ホストアドレス以外にネットワークアドレスやサブネットアドレスを指定することができます。
 設定範囲： xxx.xxx.xxx.xxxの形式（0.0.0.0を除く）
 導入時の設定： なし

ここでのマスクパターンはサブネットマスクとは異なり、クラスにこだわらずに設定が可能です。以下に例を示します。

表4-1 「address」と「mask」の組み合わせ例

address	mask	フィルタリングの適用されるIPアドレス
172.16.1.1	255.255.255.255	172.16.1.1のみ
172.17.0.0	255.255.0.0	172.17.0.0 ~ 172.17.255.255の全てのIPアドレス

- RESET** - gateway address
 destination addressとmaskで指定された宛先に対するルーティング情報の送信元として有効な（あるいは無効な）ゲートウェイのIPアドレスを設定します。
 設定範囲： xxx.xxx.xxx.xxxの形式（0.0.0.0を除く）
 導入時の設定： なし



メモ：図4-17，図4-18の画面から図4-16の画面に移行するには「ESC」キーを入力してください。

「accept gateway」のエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

4.5.4 RIP(IP)フィルタリング(propagate gateway)の設定

RIPパケット送信(propagate)時、相手先ゲートウェイ毎に送信するルーティング情報を限定することができます。この設定は、「4.5.1 RIP(IP)に関する拡張設定」のRIPの動作モードの設定で「point to point」を選択した場合のみ有効です。

```
*** EXP.: Set RIP(IP) filtering (propagate GW) configuration ***
1. filtering mode
2. filtering table
3. end
Select the number. [3]:
```

図4-19 RIP(IP)フィルタリング(propagate gateway)拡張設定例

(1) フィルタリングテーブルの属性の設定

図4-19に示した画面で「filtering mode」を選択し、フィルタリングテーブルの属性を選択します。フィルタリングテーブルの属性を有効にするとした場合、テーブルに設定されているエントリに一致したRIP情報を送信します。無効にするとした場合、テーブルに設定されているエントリに一致したRIP情報は送信しません。

```
RIP(IP) filtering (propagate gateway) parameter(s)>
mode: exclude
Do you change (y/n)? [n]:
```

図4-20 RIP(IP)フィルタリングテーブル(propagate gateway)属性

RESET

- mode

テーブルに設定されているエントリに一致したものを有効にするか、あるいは無効にするかを選択します。

設定範囲： 1: include (有効にする)

2: exclude (無効にする)

導入時の設定： 2: exclude

(2) フィルタリングテーブルの設定

図4-19に示した画面で「filtering table」を選択し、有効にする（あるいは無効にする）ルーティング情報として、宛先IPアドレスと相手ゲートウェイのIPアドレスを設定します。ゲートウェイが最大32個、1ゲートウェイあたりの宛先アドレスとして最大4エントリ、総計128エントリのテーブルが登録できます。

```
<RIP(IP) filtering (propagate gateway) table>
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]: 3

<Add RIP(IP) filtering (propagate gateway) data>
destination address [0.0.0.0]: 192.168.1.1
mask []: 255.255.255.0
gateway address []: 192.168.2.1
RIP(IP) filtering (propagate gateway) data:
  no  dst address      mask                gateway address
  ----+-----+-----+-----+
  1.  192.168.1.1      255.255.255.0      192.168.2.1
Add OK (y/n)? [y]:
```

図4-21 RIP(IP)フィルタリングテーブル(propagate gateway)設定例

- RESET** - destination address
ルーティング情報の宛先IPアドレスを設定します。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： 0.0.0.0
- RESET** - mask
destination addressに対するマスクパターンを設定します。上記のdestination addressと組み合わせて設定することによって、ホストアドレス以外にネットワークアドレスやサブネットワークアドレスを指定することができます。ここでのマスクパターンとアドレスの関係は表4-1と同じです。
設定範囲： xxx.xxx.xxx.xxxの形式（0.0.0.0を除く）
導入時の設定： なし
- RESET** - gateway address
destination addressとmaskで指定された宛先に対するルーティング情報の宛先として有効な（あるいは無効な）ゲートウェイのIPアドレスを設定します。
設定範囲： xxx.xxx.xxx.xxxの形式（0.0.0.0を除く）
導入時の設定： なし



メモ：図4-20，図4-21の画面から図4-19の画面に移行するには「ESC」キーを入力してください。

「propagate gateway」のエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

4.5.5 RIP(IP)フィルタリング(interface accept)の設定

RIPパケット受信(accept)時、インタフェース毎に有効にする（あるいは無効にする）ルーティング情報を限定することができます。

```
*** EXP.: Set RIP(IP) filtering (IF accept) configuration ***
1. filtering mode
2. filtering table
3. end
Select the number. [3]:
```

図4-22 RIP(IP)フィルタリング(interface accept)拡張設定例

(1) フィルタリングテーブルの属性の設定

図4-22に示した画面で「filtering mode」を選択し、フィルタリングテーブルの属性を選択します。フィルタリングテーブルの属性を有効にするとした場合、テーブルに設定されているエントリに一致したRIP情報は、ルーティングテーブルに登録します。無効にするとした場合、テーブルに設定されているエントリに一致したRIP情報はルーティングテーブルには登録しません。

```
<RIP(IP) filtering (interface accept) parameter(s)>
mode: exclude
Do you change (y/n)? [n]:
```

図4-23 RIP(IP)フィルタリングテーブル(interface accept)属性

- RESET** - mode
テーブルに設定されているエントリに一致したものを有効にするか、あるいは無効にするかを選択します。
設定範囲： 1: include (有効にする)
2: exclude (無効にする)
導入時の設定： 2: exclude

(2) フィルタリングテーブルの設定

図4-22に示した画面で「filtering table」を選択し、有効にする（あるいは無効にする）ルーティング情報として、宛先アドレスとインタフェースを設定します。テーブルには最大40エントリが登録できます。

```
<RIP(IP) filtering (interface accept) table>
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]: 3

<Add RIP(IP) filtering (interface accept) data>
destination address [0.0.0.0]: 192.168.1.1
mask [0.0.0.0]: 255.255.255.0
interface:
  1.LAN
  2.GroupA   3.GroupB   4.BRI#7-1   5.BRI#7-2
Select the number [1,2,3,4,5,6]:
RIP(IP) filtering (interface accept) data:
  no  dst address      mask                interface
  ---+-----+-----+-----+
  1.  192.168.1.1      255.255.255.0      LAN,GroupA,BRI#5-1,BRI#5-2
                                     BRI#7-1,BRI#7-2
Add OK (y/n)? [y]:
```

図4-24 RIP(IP)フィルタリングテーブル(interface accept)設定例(ISDN選択時)

- RESET** - destination address
ルーティング情報の宛先IPアドレスを設定します。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： 0.0.0.0
- RESET** - mask
destination addressに対するマスクパターンを設定します。上記のdestination addressと組み合わせて設定することによって、ホストアドレス以外にネットワークアドレスやサブネットワークアドレスを指定することができます。ここでのマスクパターンとアドレスの関係は表4-1と同じです。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： 0.0.0.0
- RESET** - interface
destination addressとmaskで指定された宛先に対するルーティング情報を受信するインタフェースを設定します。受信インタフェースは、「 , 」で区切って複数同時に設定することが可能です。
設定範囲： LAN, 「IP routing」で選択されたグループもしくはチャンネル
導入時の設定： LAN, 「IP routing」で選択されたグループもしくはチャンネル

➡ メモ：図4-23，図4-24の画面から図4-22の画面に移行するには「ESC」キーを入力してください。

「interface accept」のエントリの設定は，設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

4.5.6 RIP(IP)フィルタリング(interface propagate)の設定

RIPパケット送信(propagate)時，インタフェース毎に有効にする（あるいは無効にする）ルーティング情報を限定することができます。

```
*** EXP.: Set RIP(IP) filtering (IF propagate) configuration ***
1. filtering mode
2. filtering table
3. end
Select the number. [3]:
```

図4-25 RIP(IP)フィルタリング(interface propagate)拡張設定例

(1) フィルタリングテーブルの属性の設定

図4-25に示した画面で「1.filtering mode」を選択し，フィルタリングテーブルの属性を選択します。フィルタリングテーブルの属性を有効にするとした場合，テーブルに設定されているエントリに一致したRIP情報は，指定したインタフェースに送信します。無効にするとした場合，テーブルに設定されているエントリに一致したRIP情報は指定したインタフェースには送信しません。

```
<RIP(IP) filtering (interface propagate) parameter(s)>
mode: exclude
Do you change (y/n)? [n]:
```

図4-26 RIPフィルタリングテーブル(interface propagate)属性

- RESET** - mode
 テーブルに設定されているエントリに一致したものを有効にするか、あるいは無効にするかを選択します。
 設定範囲： 1: include (有効にする)
 2: exclude (無効にする)
 導入時の設定： 2: exclude

(2) フィルタリングテーブルの設定

図4-25に示した画面で「filtering table」を選択し、有効にする（あるいは無効にする）ルーティング情報として、宛先のIPアドレスとインタフェースを設定します。テーブルには最大40エントリが登録できます。

```
<RIP(IP) filtering (interface propagate) table>
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]: 3

<Add RIP(IP) filtering (interface propagate) data>
destination address [0.0.0.0]: 192.168.1.1
mask [0.0.0.0]: 255.255.255.0
interface:
  1. LAN
  2. GroupA   3. GroupB   4. BRI#7-1   5. BRI#7-2
Select the number [1,2,3,4,5,6]:
RIP(IP) filtering (interface propagate) data:
  no  dst address      mask                interface
  ---+-----+-----+-----+-----+-----+-----+-----+-----+
  1. 192.168.1.1      255.255.255.0     LAN,GroupA,BRI#5-1,BRI#5-2
                                     BRI#7-1,BRI#7-2
Add OK (y/n)? [y]:
```

図4-27 RIP(IP)フィルタリングテーブル(interface propagate)設定例 (ISDN選択時)

- RESET** - destination address
 ルーティング情報の宛先IPアドレスを設定します。
 設定範囲： xxx.xxx.xxx.xxxの形式
 導入時の設定： 0.0.0.0

- RESET** - mask
destination addressに対するマスクパターンを設定します。上記のdestination addressと組み合わせることで設定することによって、ホストアドレス以外にネットワークアドレスやサブネットワークアドレスを指定することができます。ここでのマスクパターンとアドレスの関係は表4-1と同じです。

設定範囲： xxx.xxx.xxx.xxxの形式

導入時の設定： 0.0.0.0

- RESET** - interface
destination addressとmaskで指定された宛先に対するルーティング情報を送信するインタフェースを設定します。送信インタフェースは、「,」で区切って複数同時に設定することが可能です。

設定範囲： LAN, 「IP routing」で選択されたグループもしくはチャンネル

導入時の設定： LAN, 「IP routing」で選択されたグループもしくはチャンネル



メモ：図4-26，図4-27の画面から図4-25の画面に移行するには「ESC」キーを入力してください。

「interface propagate」のエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

4.5.7 Proxy ARPの設定

Proxy ARP (代理ARP) に関する設定をします。

```
*** EXP.: Set proxy ARP parameter(s) ***
mode: off
Do you change (y/n)? [n]:
(1:off 2:response only forwarding packets 3:response all packets) [1]:

EXP.: Proxy ARP parameter(s) is set to the following values.
mode: off
Set OK (y/n)? [y]:
```

図4-28 Proxy ARP設定例

RESET

- mode

Proxy ARPの動作モードを設定します。

設定範囲： 1: off (Proxy ARPの動作をしない)
2: response only forwarding packets (本装置がフォワーディングすべきパケットに対してのみProxy ARPの動作をする)
3: response all packets (すべてのパケットに対してProxy ARPの動作をする)

導入時の設定： 1: off

4.5.8 スタティックルーティングの設定

設定方法は「3.15.3 IPスタティックルーティングの設定」と同じです。ここでの設定は、基本設定で行う設定とまったく同じです。

4.5.9 IPパケットフィルタリング(forward)の設定

設定方法は「3.15.5 IPパケットフィルタリングの設定」と同じです。ここでの設定は、基本設定で行う設定とまったく同じです。

4.5.10 IPパケットフィルタリング(discard)の設定

本テーブルに設定されたパケットを受信した場合は「4.5.9 IPパケットフィルタリング(forward)の設定」により中継を許可されたものであっても廃棄されます。

設定方法は「3.15.5 IPパケットフィルタリングの設定」と同じです。

4.5.11 OSPFに関する設定

OSPFに関する設定は拡張設定のメニューで、「OSPF configuration」を選択することにより行います。

```
*** EXP.: Set OSPF configuration(s) ***
 1. OSPF mode
 2. OSPF router ID
 3. OSPF area (except backbone area)
 4. OSPF backbone area
 5. OSPF network range
 6. OSPF stub host
 7. OSPF interface
 8. OSPF neighbor list
 9. OSPF virtual neighbor list
10. OSPF virtual link
11. RIP export
12. OSPF AS external route default
13. OSPF AS external import
14. OSPF AS external export
Select the number. :
```

図4-29 OSPF設定メニュー

(1) OSPF機能使用有無の設定

OSPFを使用したダイナミックルーティング機能を使用するかどうかを設定します。

```
*** EXP.: Set OSPF mode configuration ****
<OSPF mode parameter(s)>
  OSPF mode: not use
Do you change (y/n)? [n]: y
OSPF mode (1:use 2:not use) [2]: 1
EXP.: OSPF mode parameter(s) are set to the following values.
<OSPF mode parameter(s)>
  OSPF mode: use
Set OK (y/n)? [y]:
```

図4-30 OSPF機能使用有無の設定画面

- RESET** - OSPF mode
OSPFを利用したルーティングを行うかどうかを選択します。
設定範囲： 1.use (使用する)
 2.not use (使用しない)
導入時の設定： 2.not use

(2) OSPFルータIDの設定

OSPFの設定メニューで「OSPF router ID」を選択することにより、OSPFを利用したIPルーティングを行う上で必要なルータIDを設定します。他のルータのルータIDと重複しないように設定してください。

```
*** Set OSPF router ID. configuration ***
<OSPF router ID. parameter(s)>
  router ID. :3232235777(192.168.1.1)
Do you change (y/n)? [n]: y
router ID [192.168.1.1] : 192.168.2.1
  router ID. :3232236033(192.168.2.1)
Set OK (y/n)? [y]:
```

図4-31 OSPFルータID設定画面

RESET

- router ID

OSPFを利用したルーティングを行う上で必要なルータIDを設定します。

設定範囲： xxx.xxx.xxx.xxxの形式（0.0.0.0を除く）

または、1～4294967295（10進数）

導入時の設定： LANインタフェースのIPアドレスと同じ値



メモ：ルータIDにはLANインタフェースのIPアドレスを設定することをおすすめします。

(3) OSPFエリアの設定

OSPFの設定メニューで「OSPF area (except backbone area)」を選択することにより、OSPFで定義するバックボーンエリア以外のエリアの設定を行います。

```
*** EXP.: Set OSPF area configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図4-32 OSPFエリア設定メニュー

以下にOSPFエリアの追加例を示します。



メモ：「interface」を複数選択するときは、「,」で区切って同時に選択します。

```
<Add OSPF area data>
area ID. []: 1
authtype (1:none 2:simple) [1]: 2
attribute (1:not stub 2:stub 3:stub default) [1]:
interface:
  1.LAN
  2.GroupA   3.GroupB   4.BRI#7-1   5.BRI#7-2
Select the number [1,2]: 1,2,3,4,5
Selected OSPF area data:
                                attribute or
no area ID.                    authtype default cost interface
-----+-----+-----+-----+-----+-----+-----+-----+-----+
  1(0.0.0.1)                    simple  not stub   LAN,GroupA,GroupB
                                BRI#7-1,BRI#7-2
Add OK (y/n)? [y]:
```

図4-33 OSPFエリア追加例

RESET

- area ID

インタフェースが属するエリアのエリアIDを設定します。

設定範囲： xxx.xxx.xxx.xxxの形式（0.0.0.0を除く）

または、1～4294967295（10進数）

導入時の設定： なし

- RESET** - authtype
 ルータ間の認証の有無を選択します。
 設定範囲： 1:none (認証を行わない)
 2:simple (認証をルータに設定するパスワードで行う)
 導入時の設定： 1:none



メモ：パスワードに関しては、「(7) OSPFインタフェースの設定」を参照してください。

- RESET** - attribute
 エリアの属性を選択します。
 設定範囲： 1:not stub (スタブエリア以外)
 2:stub (スタブエリア)
 3:stub default (本装置がエリア境界ルータでAS外のルーティング情報を
 デフォルトルートとして広告する場合)
 導入時の設定： 1:not stub

- RESET** - cost
 「attribute: stub default」を選択した場合のみ、デフォルトルートを広告するときのコストの値を設定します。
 設定範囲： 1 ~ 16777215 (10進数)
 導入時の設定： なし

- RESET** - interface
 エリアに属するインタフェースを選択します。複数のインタフェースが同じエリアに属する場合は、同時に選択します。
 設定範囲： LAN,IPルーティングするグループ/チャンネル
 導入時の設定： LAN,IPルーティングする全てのインタフェース

OSPFエリアの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

ただし、エントリが一つもない状態で「change」、「delete」を選択しようとするとき、「Input error!」と表示され設定できません。また、各インタフェースに既にいずれかのエリアに所属している場合に新規エントリを追加しようとするとき、「Input error!」と表示され設定できません。

(4) OSPFバックボーンエリアの設定

OSPF設定メニューで「OSPF backbone area」を選択することにより、OSPFで定義するバックボーンエリアの設定を行います。

内部ルータがバックボーンエリアに属する場合か、あるいはエリア境界ルータの場合は、バックボーンエリアの設定が必ず必要です。この場合、いずれかのインタフェースが直接あるいはバーチャルリンクを介して間接的にバックボーンエリアに接していなければなりません。バックボーンエリア以外の内部ルータでは、バックボーンエリアの設定は必要ありません。

```

*** EXP.: Set OSPF backbone configuration ***
<OSPF backbone configuration parameter(s)>
  backbone :not use
Do you change (y/n)? [n]: y
backbone (1:use 2:not use) [2]: 1
authtype (1:none 2:simple) [1]: 2
interface
  1.LAN
  2.GroupA      3.GroupB      4.BRI#7-1      5.BRI#7-2
  6.VirtualLink
Select the number [1]: 1,2,3,4,5,6

OSPF backbone parameter(s) are set to the following values.
<OSPF backbone configuration parameter(s)>
  backbone :use
  authtype :simple
  interface:LAN,GroupA,BRI#5-1,BRI#5-2,BRI#7-1,BRI#7-2,VirtualLink
Set OK (y/n)? [y]:

```

図4-34 OSPFバックボーンエリア設定例

- RESET - backbone
 バックボーンエリアの使用の有無を選択します。
 設定範囲： 1:use (バックボーンエリアを使用する)
 2:not use (バックボーンエリアを使用しない)
 導入時の設定： 2:not use

- RESET - authtype
 ルータ間の認証の有無を選択します。
 設定範囲： 1:none (認証を行わない)
 2:simple (認証をルータに設定するパスワードで行う)
 導入時の設定： 1:none



メモ：パスワードの設定は、「(7) OSPFインタフェースの設定」を参照してください。

- RESET** - interface
 バックボーンエリアに属するインタフェースを選択します。複数のインタフェースがバックボーンエリアに属する場合は、同時に選択します。
 設定範囲： LAN,IPルーティングするグループ/チャンネル,Virtual link
 導入時の設定： LAN,IPルーティングする全てのグループ/チャンネル

➡ メモ：「interface」として選択可能なのは、「(2) OSPFエリアの設定」で選択しないインタフェースおよびバーチャルリンクです。

➡ メモ：「interface」を複数選択するときは、「,」で区切って同時に選択します。

(5) OSPFネットワーク範囲の設定

OSPF設定メニューで「OSPF network range」を選択することにより、隣接するエリアに所属するネットワーク範囲を全て登録します。

```
*** EXP.: Set OSPF networks configuration ***
1. change 2. delete 3. add 4. display 5. end
Select the number. [5]:
```

図4-35 OSPFネットワーク範囲設定メニュー

以下に、エントリの追加例を示します。1エリアに対して、複数のネットワーク範囲を設定することが可能です。ネットワーク範囲は、最大32エントリの登録が可能です。

```
<Add OSPF networks data>
address []: 192.169.10.0
mask []: 255.255.255.0

<Area ID.>
1. backbone 2. 1(0.0.0.1)
Select the number of area ID. [1]:

OSPF networks data:
no address mask area ID.
-----+-----+-----+-----
1. 192.169.10.0 255.255.255.0 backbone
Add OK (y/n)? [y]:
```

図4-36 OSPFネットワーク範囲追加例

- RESET** - address
 エリアに所属するネットワーク範囲のIPアドレスを設定します。
 設定範囲： xxx.xxx.xxx.xxxの形式
 導入時の設定： なし

4章 拡張設定

- RESET** - mask
IPアドレスの範囲を指定するためのマスクを設定します。
設定範囲：xxx.xxx.xxx.xxxの形式
導入時の設定： なし

「address」と「mask」の組み合わせによって設定されたネットワーク範囲の例を表4-2に示します。

表4-2 エリアに所属するネットワーク範囲の設定例

address	mask	ネットワーク範囲
172.16.0.0	255.255.0.0	172.16.0.0 ~ 172.16.255.255
192.168.1.0	255.255.255.0	192.168.1.0 ~ 192.168.1.255

- RESET** - area ID
「address」と「mask」の組み合わせによって設定されたネットワーク範囲が所属するエリアの、エリアIDを選択します。
設定範囲： 「(2) OSPFエリアID」で設定したエリアID
(バックボーンエリア含む)
導入時の設定： なし

OSPFネットワーク範囲の設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

ただし、エントリが一つもない状態で「change」、「delete」を選択しようとする、「Input error!」と表示され設定できません。また、既に最大エントリ（32エントリ）登録されている場合に新規エントリを追加しようとする、「Input error!」と表示され設定できません。

(6) OSPFスタブホストの設定

OSPF設定メニューで「OSPF stub host」を選択することにより、OSPFスタブホストの設定を行います。OSPFが動作していないホスト（スタブホスト）のルーティング情報をOSPFで広告する場合に、そのホストのIPアドレスを登録します。

本設定は、本装置を内部ルータとして使用する場合とエリア境界ルータとして使用する場合の両方で設定が必要です。また、本設定は、インタフェースタイプがポイントツーポイントで、接続相手がOSPFの動作をしていないホストの場合に必要となります。

```
*** EXP.: Set OSPF stubhosts configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図4-37 OSPFスタブホスト設定メニュー

以下に、OSPFスタブホストの追加例を示します。
テーブルは最大16エントリ設定が可能です。

```
<Add OSPF stubhost data>
address []: 192.168.20.1
cost []: 100

<Area ID.>
  1. backbone                2. 1(0.0.0.1)
Select the number of area ID. [1]:
OSPF stubhost data:
  no  address          cost          area ID.
  ---+-----+-----+-----
  1. 192.168.20.1     100          1(0.0.0.1)
Add OK (y/n)? [y]:
```

図4-38 OSPFスタブホスト追加例

- RESET** - address
スタブホストのIPアドレスを設定します。
設定範囲： xxx.xxx.xxx.xxxの形式（0.0.0.0を除く）
導入時の設定： なし
- RESET** - cost
本装置から設定したスタブホストまでのコスト値を設定します。
設定範囲： 1 ~ 16777215
導入時の設定： なし

- RESET** - area ID
スタブホストの所属するエリアIDを設定します。
設定範囲：エリアID（バックボーンエリア含む）
導入時の設定： なし

OSPFスタブホストの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。

ただし、エントリが一つもない状態で「change」、「delete」を選択しようとするとき、「Input error!」と表示され設定できません。また、既に最大エントリ（16エントリ）登録されている場合に新規エントリを追加しようとするとき、「Input error!」と表示され設定できません。

(7) OSPFインタフェースの設定

OSPF設定メニューで「OSPF interface」を選択することにより、OSPFインタフェースの設定を行います。

本設定は、本装置を内部ルータとして使用する場合とエリア境界ルータとして使用する場合の両方で設定が必要です。

```

*** Set OSPF interface configuration ***
  1.LAN
  2.GroupA   3.GroupB   4.BRI#7-1   5.BRI#7-2
Select the number. [4]: 4
[BRI#7-1]
  type      :non broadcast   cost      :781
  priority  :1               authkey   :area1           transit delay(sec):1
                                retransmit hello   dead       poll
  -----+-----+-----+-----+-----
  interval (sec) |5         10         40         -----
Do you change (y/n)? [n]:
type (1:broadcast 2:non-broadcast) [1]: 2
cost [781]:
priority [1]:
authkey [area1]: area2
transit delay(sec) [1]:
retransmit interval(sec) [5]:
hello interval(sec) [10]:
dead interval(sec) [40]:
  type      :non broadcast   cost      :781
  priority  :1               authkey   :area2           transit delay(sec):1
                                retransmit hello   dead       poll
  -----+-----+-----+-----+-----
  interval (sec) |5         10         40         -----
Set OK (y/n)? [y]:

```

図4-39 OSPFインタフェース設定例

- RESET** - type
 OSPFパケットの送信タイプを選択します。
 設定範囲： 1:broadcast (OSPFパケットをマルチキャスト宛に送信)
 2:non broadcast (OSPFパケットを隣接ルータ宛に送信)
 導入時の設定： 1:broadcast

4章 拡張設定

- RESET** - cost
インタフェースに設定するコスト値を設定します。
設定範囲： 1 ~ 65535 (65535は到達不能を示す)
導入時の設定： LAN: 10, HSD: 781, ISDN: 1562
- RESET** - priority
本装置を指定ルータとして運用するかどうかを決定するための優先度を設定します。この値の大きいほうが優先度が高くなります。
設定範囲： 0 ~ 255 (0は指定ルータとして運用不能を示す)
導入時の設定： 1
- RESET** - authkey
インタフェースの属するエリアの認証タイプ (「(3) OSPFエリアの設定」, 「(4) OSPFバックボーンエリアの設定」) を「simple」にした場合に、パスワードを設定します。
設定範囲： 8文字以内の英数字
導入時の設定： なし
- RESET** - transit delay
リンクステートアップデートの送信遅延時間を設定します。
設定範囲： 1 ~ 65535 [sec]
導入時の設定： 1
- RESET** - retransmit interval
隣接ルータとの情報交換パケット (database description, link state update) の再送間隔を設定します。
設定範囲： 1 ~ 65535 [sec]
導入時の設定： 5
- RESET** - hello interval
Helloパケットの送信間隔を設定します。
設定範囲： 1 ~ 65535 [sec]
導入時の設定： 10
- RESET** - dead interval
本装置が隣接ルータからの定期的なHelloパケットを受信しなくなった場合に、本装置が隣接ルータをダウンしたと判断するまでの時間を設定します。
設定範囲： 1 ~ 65535 [sec]
導入時の設定： 40

RESET - poll interval

本装置が隣接ルータをダウンしたと判断した後、その隣接ルータへHelloパケットを送信する間隔を設定します。本設定は、OSPFパケットの送信タイプが「non broadcast」の場合のみ設定します。

設定範囲： 1 ~ 65535 [sec]

導入時の設定： 120

(8) OSPF隣接ルータの設定

インタフェースタイプが「broadcast」（ 3.15.1 IPルーティングの設定）で、OSPFパケットの送信タイプが「non broadcast」の場合（ (7) OSPFインタフェースの設定）に、隣接ルータを登録します。

```
*** OSPF interface neighbor list (max 32 entries) ***
  1.LAN
  2.GroupA   3.GroupB   4.BRI#7-1   5.BRI#7-2
Select the number. [4]: 4
  no neighbor      priority
-----+-----
  1. 192.168.10.1  eligible
  2. 192.168.11.1  not eligible
  1. change  2. delete  3. add  4. end
Select the number. :
```

図4-40 OSPF隣接ルータ設定メニュー例

以下に、OSPF隣接ルータの設定追加例を示します。
隣接ルータは最大32エントリ登録できます。

```
<Add OSPF interface neighbor>
neighbor []: 192.168.12.1
priority (1:eligible 2:not eligible) [2]: 1

OSPF interface neighbor data:
  no neighbor      priority
-----+-----
      192.168.12.1  eligible
Add OK (y/n)? [y]:
```

図4-41 OSPF隣接ルータ追加例

RESET - neighbor

隣接ルータのIPアドレスを設定します。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： なし

RESET - priority

「neighbor」で記入した隣接ルータを、指定ルータとして運用しても良いかどうかを選択します。

設定範囲： 1:eligible (指定ルータとして運用可)
2:not eligible (指定ルータとして運用不可)
導入時の設定： 2:not eligible

OSPF隣接ルータの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。

ただし、エントリが一つもない状態で「change」、「delete」を選択しようとするとき、「Input error!」と表示され設定できません。また、既に最大エントリ（32エントリ）登録されている場合に新規エントリを追加しようとするとき、「Input error!」と表示され設定できません。

(9) OSPFバーチャルリンク隣接ルータの設定

OSPF設定メニューで「OSPF virtual neighbor list」を選択することにより、バーチャルリンクを確立する必要がある際の隣接ルータを登録します。

本設定は、本装置をエリア境界ルータとして使用する場合のみ設定が必要です。

バックボーンエリアに属するインタフェースとして「Virtual link」を選択した場合（(4) OSPFバックボーンエリアの設定）のみバーチャルリンクテーブルを登録します。

```

*** EXP.: Set OSPF virtual neighbor list (max 8 entries) ***
<OSPF virtuallink list>
  no neighbor ID.      transitarea
  ---+-----+-----
  1. 192.168.10.1      1(0.0.0.1)
  2. 192.168.12.1      2(0.0.0.2)

  1. change  2. delete  3. add  4. end
Select the number. :

```

図4-42 OSPFバーチャルリンク隣接ルータ設定メニュー

以下に、OSPFバーチャルリンク隣接ルータの追加例を示します。
テーブルは最大8エントリまで設定できます。

```

<Add OSPF Virtual link data>
neighbor ID. [192.168.10.1]:192.168.11.1
transitarea [1(0.0.0.1)]:

Virtual link data:
  no neighbor ID.      transitarea
  ---+-----+-----
  1. 192.168.11.1      1(0.0.0.1)
Add OK (y/n)? [y]:

```

図4-43 OSPFバーチャルリンク隣接ルータ追加例

RESET - neighbor ID

本装置とバーチャルリンクを確立するエリア境界ルータのルータIDを設定します。

設定範囲： xxx.xxx.xxx.xxxの形式

導入時の設定： なし

RESET

- transitarea

バーチャルリンクを確立するエリア境界ルータと本装置の間の、エリアIDを設定します。

設定範囲： xxx.xxx.xxx.xxxの形式（0.0.0.0を除く）

または、1～4294967295（10進数）

導入時の設定： なし

OSPFバーチャルリンク隣接ルータの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。

ただし、エントリが一つもない状態で「change」、「delete」を選択しようとする、「Input error!」と表示され設定できません。また、既に最大エントリ（8エントリ）登録されている場合に新規エントリを追加しようとする、「Input error!」と表示され設定できません。

(10) OSPFバーチャルリンクの設定

OSPF設定メニューで「OSPF virtual link」を選択することにより、バーチャルリンクを確立する隣接ルータの諸設定を行います。「(7) OSPFバーチャルリンク隣接ルータ」で設定されたテーブルの諸設定を行います。

```

*** OSPF virtual link configuration ***
no neighbor ID.
---+-----
1. 192.168.10.1
2. 192.168.12.1
Select the entry number. : 1
Selected Virtual link data:
<Neighbor ID.[192.168.10.1] virtual link detail parameter(s)>
authkey          :area1
transit delay(sec):1
                    retransmit hello      dead
-----+-----+-----+-----
interval (sec)    5          10          40
authkey [area1]:area2
transit delay(sec) [1]:
retransmit interval(sec) [5]:
hello interval(sec) [10]:
dead interval(sec) [40]:

<Neighbor ID.[192.168.10.1] virtual link detail parameter(s)>
authkey          :area2
transit delay(sec):1
                    retransmit hello      dead
-----+-----+-----+-----
interval (sec)    |5          10          40
Set OK (y/n)? [y]:

```

図4-44 OSPFバーチャルリンク設定例

- RESET** - authkey
 バーチャルリンクを確立するルータ間で認証を行うための、パスワードを設定します。
 設定範囲： 8文字以内の英数字
 導入時の設定： なし
- RESET** - transit delay
 リンクステートアップデートの送信遅延時間を設定します。
 設定範囲： 1 ~ 65535 [sec]
 導入時の設定： 1

- RESET** - retransmit interval
バーチャルリンクを確立するルータ間の情報交換パケット（database description, link state update）の送信間隔を設定します。
設定範囲： 1 ~ 65535 [sec]
導入時の設定： 5

- RESET** - hello interval
Helloパケットの送信間隔を設定します。
設定範囲： 1 ~ 65535 [sec]
導入時の設定： 10

- RESET** - dead interval
本装置がバーチャルリンクを確立するルータからの定期的なHelloパケットを受信しなくなった場合に、本装置がそのルータをダウンしたと判断するまでの時間を設定します。
設定範囲： 1 ~ 65535 [sec]
導入時の設定： 40



注意：「authkey」、 「hello interval」 および 「dead interval」 は、バーチャルリンクを確立するルータと同じ値でなければいけません。

(11) RIP exportの設定

OSPF設定メニューで「RIP export」を選択することにより、RIP以外で受信したルーティング情報をRIPで通知する（あるいは通知しない）場合の設定を行います。RIPで通知する（あるいは通知しない）ルーティング情報のテーブルは最大20エントリ登録できます。

```

*** EXP.: Set RIP(IP) export configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]: 3

<Add RIP(IP) export data>
Select the configuration (1:metric 2:restrict): 1
metric [1]:
protocol (1:ospf 2:ospf ase) [1]:

<Announce list>
no entry.
Do you change (y/n)? [n]: y
  1. change  2. delete  3. add  4. end
Select the number. : 3

<Add RIP(IP) export destination data>
Select the address format (1:all 2:network 3:host): 2
dst address [0.0.0.0]: 192.168.1.0
mask [0.0.0.0]: 255.255.255.0

OSPF RIP export destination data:
  no dst address      mask
  ---+-----+-----
  1. 192.168.1.0      255.255.255.0
Add OK (y/n)? [y]:

<Announce list>
  no dst address      mask          no dst address      mask
  ---+-----+-----+-----+-----
  1. 192.168.1.0      255.255.255.0
  1. change  2. delete  3. add  4. end
Select the number. : 4

<Announce list>
  no dst address      mask          no dst address      mask
  ---+-----+-----+-----+-----
  1. 192.168.1.0      255.255.255.0
Set OK (y/n)? [y]:

OSPF RIP export data:
  1. metric:1      protocol:ospf
  no dst address      mask          no dst address      mask
  ---+-----+-----+-----+-----
  1. 192.52.0.0      255.255.0.0
Add OK (y/n)? [y]:

```

図4-45 RIP export設定例

RIPで通知する（あるいは通知しない）ルーティング情報のテーブル1エントリに関する項目を以下に示します。

RESET - configuration
あとで設定する「Announce list」に一致したルーティング情報をRIPにより送信するかどうかを選択します。
設定範囲： 1:metric（一致した情報をRIPにより送信する）
2:restrict（一致した情報をRIPにより送信しない）
導入時の設定： なし

RESET - metric
RIP以外のルーティング情報をRIPとして受信するときのメトリック値を設定します。
設定範囲： 1 ~ 16
導入時の設定： 16

RESET - protocol
RIPとして受信するRIP以外のルーティング情報を選択します。
設定範囲： 1:ospf（OSPFによるルーティング情報）
2:ospf ase（OSPFのAS外のルーティング情報）
導入時の設定： 1:ospf

RIPで通知する（あるいは通知しない）ルーティング情報のテーブル1エントリ毎に、該当するルーティング情報のリスト（「Announce list」）を設定します。最大20エントリ設定できます。

RESET - address format
「Announce list」に登録するルーティング情報のアドレス形式を選択します。
設定範囲： 1:all（すべてのIPアドレス）
2:network（複数のIPアドレス）
3:host（1つのIPアドレス）
導入時の設定： なし

RESET - dst address
「Announce list」に登録するルーティング情報のアドレスを選択します。「address format」で「all」を選択したときは、この設定の問い合わせはありません。
設定範囲： 0.0.0.0 ~ 255.255.255.255
導入時の設定： 0.0.0.0

RESET - mask

「dst address」で登録したアドレスの範囲を指定するマスクパターンを設定します。
「address format」で「all」か「host」を選択したときは、この設定の問い合わせはありません。

設定範囲：0.0.0.1 ~ 255.255.255.255

導入時の設定： 255.255.255.255

「RIP export」のエントリの設定と、「RIP export」内の「Announce list」の設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリを表示します。（「RIP export」の場合のみ）
- end 設定を終了します。

(12) AS外のルーティング情報の設定

OSPF設定メニューで「OSPF AS external route default」を選択することにより、AS外のルーティング情報をルーティングテーブルに登録する、あるいは送信する場合のAS外のルーティング情報についての諸設定を行います。OSPFによるダイナミックルーティング機能をしようする場合で、AS境界ルータとして運用する場合に設定が必要です。

```
*** EXP.: Set OSPF AS external route default configuration ***
<OSPF AS external route default parameter(s)>
  import preference   : 110
    interval(sec): 1
    max route    : 100
  export cost        : 0
    OSPF tag     : 0
    type        : 1
Do you change (y/n)? [n]: y
import preference [110]:
  interval(sec) [1]:
  max route [100]:
export cost []: 11
  OSPF tag [0]:
  type (1:type1 2:type2) [1]:

<OSPF AS external route default parameter(s)>
  import preference   : 110
    interval(sec): 1
    max route    : 100
  export cost        : 11
    OSPF tag     : 0
    type        : 1
Set OK (y/n)? [y]:
```

図4-46 AS外のルーティング情報の設定例

RESET

- import preference

AS外のルーティング情報が重なった場合の優先度を設定します。「preference」の値は、値の小さい方が優先されます。本装置の「preference」値はRIPが100固定、スタティック設定の値が導入時の設定で50（3.2.10 ワークシート「IPスタティックルーティング編」）、ICMPリダイレクトメッセージの値が導入時の設定で20（4.4 ICMPリダイレクトメッセージの設定）です。

設定範囲： 0 ~ 255

導入時の設定： 110

- RESET** - import interval
AS外のルーティング情報を受信する場合に、その情報を有効にするタイミングを設定します。
設定範囲： 1 ~ 65535 [sec]
導入時の設定： 1
- RESET** - import max route
AS外の情報を受信する場合に、「import interval」の間に有効にする最大のルート数を設定します。
設定範囲： 1 ~ 65535 [sec]
導入時の設定： 100
- RESET** - export cost
AS外のルーティング情報を送信する際の、そのルートへのコストを設定します。
設定範囲： 1 ~ 65535 [sec]
導入時の設定： 100
- RESET** - export tag OSPF
AS外のルーティング情報を送信パケットにつけるtagの値を設定します。
設定範囲： 0 ~ 2147483647
導入時の設定： 0
- RESET** - export type
AS外のルーティング情報を送信する際、そのルーティング情報を送信するタイプを設定します。
設定範囲： 1:type1（内部ルータが宛先へのコストを計算する場合にAS境界ルータまでのコストを加算）
2:type2（内部ルータが宛先へのコストを計算する場合にAS境界ルータまでのコストを無視）
導入時の設定： 1:type1

(13) AS外のルーティング情報の受信(OSPF import)の設定

「OSPF AS external import」を選択することにより、AS境界ルータで、OSPFのAS外のルーティング情報をルーティングテーブルに登録するかどうかを設定します。本設定を行わない場合、AS外のすべてのルーティング情報を受け入れます。

```

*** EXP.: Set OSPF import configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]: 3

<Add OSPF import data>
tag [*]:
Select the configuration (1:preference 2:restrict): 1
preference [0]: 1

<Announce list>
no entry.
Do you change (y/n)? [n]: y
  1. change  2. delete  3. add  4. end
Select the number. : 3

<Add OSPF import destination data>
Select the address format (1:all 2:network 3:host): 2
dst address [0.0.0.0]: 192.168.1.0
mask [0.0.0.0]: 255.255.255.0

OSPF import destination data:
      no  dst address      mask
-----+-----+-----
      1. 192.168.1.0      255.255.255.0
Add OK (y/n)? [y]:

<Announce list>
      no  dst address      mask          no  dst address      mask
-----+-----+-----+-----+-----
      1. 192.168.1.0      255.255.255.0
  1. change  2. delete  3. add  4. end
Select the number. :

```

図4-47 AS外のルーティング情報の受信 (OSPF import) 設定例

- RESET** - tag
 AS外のルーティング情報のtagの値を設定します。
 設定範囲: 0 ~ 2147483647, または* (すべてのtag)
 導入時の設定: *

- RESET** - configuration
 あとで設定する「Announce list」に一致したAS外のルーティング情報を、ルーティングテーブルに登録するかどうかを選択します。
 設定範囲： 1:preference (一致した情報をルーティングテーブルに登録する)
 2:restrict (一致した情報をルーティングテーブルに登録しない)
 導入時の設定： なし

- RESET** - preference
 AS外のルーティング情報をルーティングテーブルに登録するときの優先度を設定します。上記の「configuration」で「restrict」を選択した場合は、この問い合わせは行われません。
 設定範囲： 0 ~ 255
 導入時の設定： 0

AS外のルーティング情報の受信(OSPF import)のテーブル1エン트리毎に、該当するルーティング情報のリスト(「Announce list」)を設定します。「Announce list」は各エントリの合計で最大20エン트리設定できます。1エン트리に関する項目を以下に示します。

- RESET** - address format
 「Announce list」に登録するルーティング情報のアドレス形式を選択します。
 設定範囲： 1:all (すべてのIPアドレス)
 2:network (複数のIPアドレス)
 3:host (1つのIPアドレス)
 導入時の設定： なし

- RESET** - dst address
 「Announce list」に登録するルーティング情報のアドレスを選択します。「address format」で「all」を選択したときは、この設定の問い合わせは行われません。
 設定範囲： 0.0.0.0 ~ 255.255.255.255
 導入時の設定： 0.0.0.0

- RESET** - mask
 「dst address」で登録したアドレスの範囲を指定するマスクパターンを設定します。「address format」で「all」か「host」を選択したときは、この設定の問い合わせは行われません。
 設定範囲： 0.0.0.0 ~ 255.255.255.255
 導入時の設定： 0.0.0.0

「OSPF import」のエントリの設定と、「OSPF import」内の「Announce list」の設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリを表示します。

(14) AS外のルーティング情報の送信(OSPF export)の設定

OSPF設定メニューで「OSPF AS external import」を選択することにより、AS境界ルータで、AS外のルーティング情報をAS内へ送信するための設定を行います。

```

*** EXP.: Set OSPF export configuration ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]: 3

<Add OSPF export data>
type (1:type1 2:type2) [1]:
tag [0]:
Select the configuration (1:cost 2:restrict): 1
cost []: 1
protocol (1:rip 2:static 3:default) [1]: 1

<Announce list>
no entry.
Do you change (y/n)? [n]: y
  1. change  2. delete  3. add  4. end
Select the number. : 3

<Add OSPF export destination data>
Select the address format (1:all 2:network 3:host): 2
dst address [0.0.0.0]: 192.168.1.0
mask [0.0.0.0]: 255.255.255.0

OSPF export destination data:
  no dst address      mask
  ---+-----+-----
  1. 192.168.1.0      255.255.255.0
Add OK (y/n)? [y]:

<Announce list>
  no dst address      mask          no dst address      mask
  ---+-----+-----+-----+-----
  1. 192.168.1.0      255.255.255.0
  1. change  2. delete  3. add  4. end
Select the number. :

```

図4-48 AS外のルーティング情報の送信 (OSPF export) 設定例

AS外のルーティング情報の送信(OSPF export)のテーブル1エントリに関する項目を以下に示します。

4章 拡張設定

- RESET** - type
AS外のルーティング情報を送信する際の、そのルーティング情報を送信するタイプを設定します。
設定範囲： 1:type1 (内部ルータが宛先へのコストを計算する場合AS境界ルータまでのコストを加算)
2:type2 (内部ルータが宛先へのコストを計算する場合AS境界ルータまでのコストを無視)
導入時の設定： 1:type1
- RESET** - tag
AS外のルーティング情報を送信するときのtagの値を設定します。
設定範囲： 0 ~ 2147483647
導入時の設定： 0
- RESET** - configuration
あとで設定する「Announce list」に一致したAS外のルーティング情報を、AS内に送信するかどうかを選択します。
設定範囲： 1:cost (一致した情報をAS内に送信する)
2:restrict (一致した情報をAS内に送信しない)
導入時の設定： なし
- RESET** - cost
AS外のルーティング情報のコストを設定します。上記「configuration」で「restrict」を選択した場合は、この問い合わせは行われません。
設定範囲： 1 ~ 16777215
導入時の設定： なし
- RESET** - protocol
AS外のルーティング情報を得たプロトコルを指定します。
設定範囲： 1:rip (RIP)
2:static (スタティックルーティング)
3:default (デフォルトルーティング)
導入時の設定： 1:rip

AS外のルーティング情報の送信(OSPF export)のテーブル1エン트리毎に、該当するルーティング情報のリスト(「Announce list」)を設定します。「Announce list」は各エントリの合計で最大20エン트리設定できます。

- RESET** - address format
AS外のルーティング情報を得たプロトコルを指定する。
設定範囲： 1:all (すべてのIPアドレス)
2:network (複数のIPアドレス)
3:host (1つのIPアドレス)
導入時の設定： なし
- RESET** - dst address
「Announce list」に登録するルーティング情報のアドレスを選択します。「address format」で「all」を選択したときは、この設定の問い合わせは行われません。
設定範囲： 0.0.0.0 ~ 255.255.255.255
導入時の設定： 0.0.0.0
- RESET** - mask
「dst address」で登録したアドレスの範囲を指定するマスクパターンを設定します。
「address format」で「all」か「host」を選択したときは、この設定の問い合わせは行われません。
設定範囲： 0.0.0.0 ~ 255.255.255.255
導入時の設定： 0.0.0.0

「OSPF export」のエントリの設定と、「OSPF export」内の「Announce list」の設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更する。
- delete エントリを削除する。
- add エントリを追加する。
- display エントリを表示する。

4.6 IPXに関する拡張設定

IPXルーティング機能に関する拡張設定を行います。IPXルーティングの拡張機能は、メインメニューで「configuration set (expert)」を選択後「IPX routing」を選択して設定します。

```
*** EXP.: IPX routing configuration menu ***
 1. RIP interface
 2. RIP filtering
 3. RIP static
 4. SAP interface
 5. SAP filtering mode
 6. SAP filtering (address)
 7. SAP filtering (server name)
 8. SAP filtering (service type)
 9. SAP static
10. IPX filtering (forward)
11. IPX filtering (discard)
12. frame type
13. keep alive
Select the number. :
```

図4-49 IPXルーティングの拡張設定メニュー

- RIP interface
RIPのインタフェースに関する動作を設定します。
- RIP filtering
RIPのフィルタリングテーブルを設定します。
- RIP static
スタティックルーティングを設定します。
- SAP interface
SAPのインタフェースに関する動作を設定します。
- SAP filtering mode
SAPのフィルタリングテーブルの属性を設定します。
- SAP filtering(address)
SAP情報のネットワークアドレスによるフィルタリングテーブルを設定します。
- SAP filtering(server name)
SAP情報のサーバ名によるフィルタリングテーブルを設定します。

- SAP filtering(service type)
SAP情報のサーバタイプによるフィルタリングテーブルを設定します。
- SAP static
スタティックなSAP情報を設定します。
- IPX filtering(forward)
中継するパケットのフィルタリングテーブルの設定を行います。IPXパケットフィルタリング機能を使用する場合、本テーブルに設定されたエントリのみを中継します。テーブルに設定されていないパケットは全て遮断します。
- IPX filtering(discard)
遮断するパケットのフィルタリングテーブルの設定を行います。IPXパケットフィルタリング機能を使用する場合、「IPX filtering(forward)」で設定されたパケットでも本テーブルに設定されたパケットは中継しません。
- frame type
インタフェースのフレームタイプの設定を行います。
- keep alive (ISDN選択時のみ)
「KeepAlive」に関する情報を設定します。

4.6.1 RIP(IPX)インタフェースの設定

RIPのインタフェースに関する動作を設定します。

```

*** EXP.: Set RIP(IPX) interface configuration ***
<RIP(IPX) interface parameter(s)>
  1.LAN
  2.BRI#1-1
Select the number. : 2

      interface send      rcv      broadcast interval(sec) ageout time(sec)
                control control
-----+-----+-----+-----+-----+-----+-----+-----+-----+
BRI#1-1  on      on      off      60              off      180
Do you change (y/n)? [n]: y
send control (1:on 2:off) [1]:
rcv control (1:on 2:off) [1]:
broadcast (1:on 2:off) [2]:
broadcast interval (sec) [60]:
entry ageout (1:on 2:off) [2]:
ageout time (sec) [180]:

EXP.: RIP(IPX) interface parameter(s) are set to the following values.
<RIP(IPX) interface parameter(s)>

      interface send      rcv      broadcast interval(sec) ageout time(sec)
                control control
-----+-----+-----+-----+-----+-----+-----+-----+-----+
BRI#1-1  on      on      off      60              off      180
Set OK (y/n)? [y]:

```

図4-50 RIP(IPX)インタフェース拡張設定例

- RESET** - send control
RIP情報を送信する / しないを選択します。
設定範囲： 1:on
 2:off
導入時の設定： 1:on

- RESET** - rcv control
RIP情報を受信する / しないを選択します。
設定範囲： 1:on
 2:off
導入時の設定： 1:on

- RESET** - broadcast
send controlがonのときのRIPの送信方法を選択します。
設定範囲： 1: on (定期update)
 2: off (triggered update)
導入時の設定： 2: off
- RESET** - broadcast interval
ISDN回線にRIPの定期アップデートを送信する場合の、定期送信間隔を設定します。
設定範囲： 60 ~ 2147483647[秒]
導入時の設定： 60
- RESET** - entry ageout
RIPによりISDN回線から学習したルーティング情報のエージアウトする / しないを選択します。
設定範囲： 1: on (エージアウトする)
 2: off (エージアウトしない)
導入時の設定： 2: off
- RESET** - ageout time
RIPによりISDN回線から学習したルーティング情報がエージアウトする場合の、エージアウト時間を設定します。
設定範囲： 30 ~ 2147483647[秒]
導入時の設定： 180
-  注意：ISDN回線にRIPの定期アップデートをする場合、本装置とISDN回線を介して接続している相手側の装置の「ageout time」を、「broadcast interval」より大きい値に設定してください(約3倍)。

4.6.2 RIP(IPX)フィルタリングの設定

RIPのフィルタリングテーブルを設定します(最大64エントリ)。

```
*** EXP.: Set RIP(IPX) filtering configuration ***
<RIP(IPX) filtering parameter(s)>
  mode                : exclude
  exclude max hop count: 16
  RIP(IPX) filtering table (max 16 entries)
    no entry
Do you change (y/n)? [n]: y
mode (1:include 2:exclude) [2]:
exclude max hop count [16]:

<Set RIP(IPX) filtering table>
  RIP(IPX) filtering table (max 16 entries)
    no entry
Do you change (y/n)? [n]: y

  1. change  2. delete  3. add  4. end
Select the number. : 3

<Add RIP(IPX) filtering data>
network []: 11223344
mask []: ffffff
RIP(IPX) filtering data:
  no network mask
  ----+-----+-----+
  1. 11223344  ffffffff
Add OK (y/n)? [y]:
```

図4-51 RIP(IPX)フィルタリングテーブル拡張設定例

(1) フィルタリングテーブルの属性の設定

フィルタリングテーブルの属性を選択します。フィルタリングテーブルの属性を有効にするとした場合、テーブルに設定されているエントリに一致したRIP情報は、ルーティングテーブルに登録します。無効にするとした場合、テーブルに設定されているエントリに一致したRIP情報はルーティングテーブルには登録しません。

```
<RIP(IP) filtering (interface accept) parameter(s)>
  mode: exclude
Do you change (y/n)? [n]:
```

図4-52 RIP(IPX)フィルタリングテーブル(interface accept)属性

- RESET** - mode
 テーブルに設定されているエントリに一致したものを有効にするか、あるいは無効にするかを選択します。
 設定範囲： 1: include (有効にする)
 2: exclude (無効にする)
 導入時の設定： 2: exclude
- RESET** - exclude max hop count
 設定値以上のホップカウントのRIPのエントリを受信した場合は、そのエントリを廃棄します。
 設定範囲： 1 ~ 16
 導入時の設定： 16

(2) フィルタリングテーブルの設定

有効にする(あるいは無効にする)ルーティング情報として、宛先アドレスを設定します。テーブルには最大64エントリが登録できます。

- network
 ルーティング情報の宛先ネットワーク番号を設定します。
 設定範囲： 8桁の16進数(00000000を除く)
 導入時の設定： なし
- mask
 networkに対するマスクパターンを設定します。上記のnetworkと組み合わせて設定することによって、単一のネットワーク番号だけではなく共通部分を持った複数のネットワーク番号を指定することができます。
 設定範囲： 8桁の16進数(00000000を除く)
 導入時の設定： なし

ここでのマスクパターンとネットワーク番号の組み合わせ例を以下に示します。

表4-3 「network number」と「mask」の組み合わせ例

network number	mask	フィルタリングの適用されるネットワーク番号
00000001	fffffff	00000001のみ
00010000	ffff0000	00010000 ~ 0001ffffの全てのネットワーク番号
00000001	000000ff	XXXXXX01の形式のネットワーク番号

RIPフィルタリングテーブルのエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。

4.6.3 RIP(IPX)スタティックルーティングの設定

スタティックルーティングの設定をします。本設定は基本設定で行うこともできます。設定方法は「3.16.3 IPXスタティックルーティングの設定」と同じです。

4.6.4 SAP(IPX)インタフェースの設定

SAPのインタフェースに関する動作を設定します。

```

*** EXP.: Set SAP(IPX) interface configuration ***
<SAP(IPX) interface parameter(s)>
  1.LAN
  2.BRI#1-1
Select the number. : 2

      interface send      rcv      broadcast interval(sec) ageout time(sec)
                control control
-----+-----+-----+-----+-----+-----+-----+-----+
BRI#1-1  on      on      off      60              off      180
Do you change (y/n)? [n]: y
send control (1:on 2:off) [1]:
rcv control (1:on 2:off) [1]:
broadcast (1:on 2:off) [2]:
broadcast interval (sec) [60]:
entry ageout (1:on 2:off) [2]:
ageout time (sec) [180]:

EXP.: SAP(IPX) interface parameter(s) are set to the following values.
<SAp(IPX) interface parameter(s)>

      interface send      rcv      broadcast interval(sec) ageout time(sec)
                control control
-----+-----+-----+-----+-----+-----+-----+
BRI#1-1  on      on      off      60              off      180
Set OK (y/n)? [y]:

```

図4-53 SAP(IPX)インタフェース拡張設定例

- RESET** - send control
 SAP情報を送信する/しないを選択します。
 設定範囲： 1:on
 2:off
 導入時の設定： 1:on
- RESET** - rcv control
 SAP情報を受信する/しないを選択します。
 設定範囲： 1:on
 2:off
 導入時の設定： 1:on

4章 拡張設定

- RESET** - broadcast
SAPの送信方法を選択します。
設定範囲： 1 : on (定期update)
 2 : off (triggered update)
導入時の設定： 2 : off
- RESET** - broadcast interval
ISDN回線にSAPの定期アップデートを送信する場合の、定期送信間隔を設定します。
設定範囲： 60 ~ 2147483647[秒]
導入時の設定： 60
- RESET** - entry ageout
SAPによりISDN回線から学習したSAP情報の、エージアウトする / しないを選択します。
設定範囲： 1 : on (エージアウトする)
 2 : off (エージアウトしない)
導入時の設定： 2 : off
- RESET** - ageout time
SAPによりISDN回線から学習したSAP情報がエージアウトする場合の、エージアウト時間を設定します。
設定範囲： 30 ~ 2147483647[秒]
導入時の設定： 180



注意：ISDN回線にSAPの定期アップデートの送信する場合、本装置とISDN回線を介して接続している相手側の装置の「ageout time」を、「broadcast interval」より大きい値に設定してください(約3倍)。

4.6.5 SAP(IPX)フィルタリングテーブルの属性の設定

SAPのフィルタリングについて設定します。

```

*** EXP.: Set SAP(IPX) filtering mode configuration ***
<SAP(IPX) filtering mode parameter(s)>
  mode                : exclude
  exclude max hop count: 16
Do you change (y/n)? [n]: y
mode(1:include 2:exclude) [2]:
exclude max hop count [16]:

EXP.: SAP(IPX) filtering mode parameter(s) are set to the following values.
<SAP(IPX) filtering mode parameter(s)>
  mode                : exclude
  exclude max hop count: 16
Set OK (y/n)? [y]:

```

図4-54 SAP(IPX)フィルタリングテーブルの属性の設定例

RESET

- mode

テーブルに設定されているエントリに一致したものを有効にするか、あるいは無効にするかを選択します。有効にするを選択した場合、エントリに一致したSAPを、SAPテーブルに登録します。無効にするを選択した場合、エントリに一致したSAPは、SAPテーブルに登録しません。

設定範囲： 1: include (有効にする)
2: exclude (無効にする)

導入時の設定： 2: exclude



注意：「mode」で設定した項目は、「4.6.6 SAP(IPX)フィルタリング(address)の設定」, 「4.6.7 SAP(IPX)フィルタリング(server name)の設定」および「4.6.8 SAP(IPX)フィルタリング(service type)の設定」で設定するすべてのテーブルに有効となります。

RESET

- exclude max hop count

設定値より大きいホップカウントのSAPのエントリを受信した場合は、そのエントリを廃棄します。

設定範囲： 1 ~ 16

導入時の設定： 16

4.6.6 SAP(IPX)フィルタリング(address)の設定

ネットワーク番号によるSAPのフィルタリングテーブルを設定します。フィルタリングテーブルには最大64エントリが登録できます。

```
*** EXP.: Set SAP(IPX) filtering (addr) configuration ***
<SAP(IPX) filtering (address) parameter(s)>
  SAP(IPX) filtering (address) table (max 16 entries)
    no entry
Do you change (y/n)? [n]: y

<Set SAP(IPX) filtering (address) table>

  1. change  2. delete  3. add  4. end
Select the number. : 3

<Add SAP(IPX) filtering (address) data>
network []: 11223344
mask []: ffffff
SAP(IPX) filtering (address) data:
  no network  mask
  ----+-----+-----+
  1. 11223344  fffffff
```

図4-55 アドレスによるSAP(IPX)フィルタリング設定例

- network
SAP情報のサーバのネットワーク番号を設定します。
設定範囲： 8桁の16進数（00000000を除く）
導入時の設定： なし
- mask
networkに対するマスクパターンを設定します。上記のnetworkと組み合わせて設定することによって、単一のネットワーク番号だけではなく共通部分を持った複数のネットワーク番号を指定することができます。networkとマスクパターンの関係は「4.6.2 RIP(IPX)フィルタリングの設定」と同じです。
設定範囲： 8桁の16進数（00000000を除く）
導入時の設定： なし

SAPフィルタリングテーブル(address)のエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。

4.6.7 SAP(IPX)フィルタリング(server name)の設定

サーバ名によるSAPのフィルタリングテーブルを設定します。フィルタリングテーブルには最大64エントリを登録することができます。

```

*** EXP.: Set SAP(IPX) filtering (name) configuration ***
<SAP(IPX) filtering (server name) parameter(s)>
    SAP(IPX) filtering (server name) table (max 16 entries)
        no entry
Do you change (y/n)? [n]: y
<Set SAP(IPX) filtering (server name) table>

    1. change  2. delete  3. add  4. end
Select the number. : 3

<Add SAP(IPX) filtering (server name) data>
server name []: server1
SAP(IPX) filtering (server name) data:
    no server name
    ----+-----
        1. server1
Add OK (y/n)? [y]:

```

図4-56 サーバ名によるSAP(IPX)フィルタリング設定例

- server name
SAP情報のサーバ名を設定します。
設定範囲： 最大47文字の英数字
導入時の設定： なし

SAPフィルタリングテーブル(server name)のエントリの設定は、設定メニュー画面で以下のコマンドをして行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。

4.6.8 SAP(IPX)フィルタリング(service type)の設定

サービスタイプによるSAPのフィルタリングテーブルを設定します。フィルタリングテーブルには最大64エントリが登録できます。

```

*** EXP.: Set SAP(IPX) filtering (type) configuration ***
<SAP(IPX) filtering (service type) parameter(s)>
  SAP(IPX) filtering (service type) table (max 16 entries)
    no entry
Do you change (y/n)? [n]: y

<Set SAP(IPX) filtering (service type) table>

  1. change  2. delete  3. add  4. end
Select the number. : 3

<Add SAP(IPX) filtering (service type) data>
  1. print queue  4. print server      7. advertising print server
  2. file server  5. archive server     8. all
  3. job server   6. remote bridge server  9. other
Select the number of service type [9]: 2
SAP(IPX) filtering (service type) data:
  no service type
  ----+-----
      1. file server
Add OK (y/n)? [y]:

```

図4-57 タイプによるSAP(IPX)フィルタリング設定例

- service type

SAP情報のサービスタイプを設定します。

設定範囲： 1 : print queue
 2 : file server
 3 : job server
 4 : print server
 5 : archive server
 6 : remote bridge server
 7 : advertising print server
 8 : all
 9 : other (16進4桁で任意のサービスタイプ番号を入力する)

導入時の設定： 9 : other

SAPフィルタリングテーブル(service type)のエントリの設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。

4.6.9 SAP(IPX)のスタティック設定

「3.16.5 IPXスタティックSAPの設定」と同じです。ここでの設定は、基本設定で行うものとまったく同じです。

4.6.10 IPXパケットフィルタリング(forward)の設定

「3.16.3 IPXパケットフィルタリングの設定」と同じです。ここでの設定は、基本設定で行うものとまったく同じです。

4.6.11 IPXパケットフィルタリング(discard)の設定

本設定では、中継を許可しないパケットを指定します。特に「4.6.7 IPXパケットフィルタリング(forward)の設定」により中継を許可されたパケットであっても、このテーブルに設定されたパケットは廃棄されます。設定方法は「3.15.3 IPXパケットフィルタリングの設定」と同じです。



メモ：本装置は導入時に「ソケット番号"457"を使用するパケットを中継しない」エントリを設定してあります。

4.6.12 IPX frame typeの設定

インタフェースのフレームタイプの設定を行います。

```
*** EXP.: Set frame type configuration ***
<frame type parameter(s)>
  1.LAN
  2.BRI#1-1    3.BRI#1-2
Select the number. : 1
frame type: ETHERNET_802.3

frame type:
(1:ETHERNET_II 2:ETHERNET_802.3 3:ETHERNET_802.2 4:ETHERNET_SNAP) [2] : 1

frame type: ETHERNET_II
Set OK (y/n) [y]:
```

図4-58 IPX frame type設定例

- frametype
インタフェースに接続されるネットワークのMACフレームのタイプを選択します。WAN
インタフェースについてはブリッジ接続する場合のみ設定が必要です。ブリッジ接続
する場合、ブリッジ側のMACフレームタイプと同じタイプを選択します。
設定範囲： 1: ETHERNET_II
 2: ETHERNET_802.3
 3: ETHERNET_802.2
 4: ETHERNET_SNAP
導入時の設定： 2: ETHERNET_802.3

4.6.13 KeepAliveパケットの代理応答 / 要求の設定

KeepAliveパケットの代理応答 / 要求の設定をします(ISDN選択時のみ)。「mode」以外の設定は、導入時の設定で運用します(設定は特に必要ありません)。

```

*** EXP.: Set Proxy keep alive(IPX) configuration ***
<Proxy keep alive(IPX) parameter(s)>
  mode                                     : not use
Do you change (y/n)? [n]: y
mode (1:use 2:not use) [2]: 1
request  start  indicate timer (sec) [3]:
          retry count [10]:
          send   timer normal (min) [5]:
          timer retry (min) [1]:
          retry count [10]:
response stop  indicate timer (sec) [3]:
          retry count [10]:
          restart indicate timer (sec) [3]:
          retry count [10]:
          end    indicate timer (sec) [3]:
          retry count [2]:
          end timer (min) [10]:

EXP.: Proxy keep alive(IPX) parameter(s) are set to the following values.
<Proxy keep alive(IPX) parameter(s)>
  mode                                     : use
request  start  indicate timer (sec): 3
          retry count          : 10
          send   timer normal (min) : 5
          timer retry (min)      : 1
          retry count          : 10
response stop  indicate timer (sec): 3
          retry count          : 10
          restart indicate timer (sec): 3
          retry count          : 10
          end    indicate timer (sec): 3
          retry count          : 2
          end timer (min)       : 10
Set OK (y/n)? [y]:

```

図4-59 IPX KeepAlive設定例

4章 拡張設定

- RESET** - mode
KeepAliveパケットの代理応答 / 要求機能の動作する / しないを選択します。
設定範囲： 1 : use (動作する)
2 : not use (動作しない)
導入時の設定： 1 : use
- RESET** - request start indicate timer
代理要求開始指示パケット送信失敗時の再送タイマを設定します。
設定範囲： 1 ~ 255 [sec]
導入時の設定： 3
- RESET** - request start retry count
代理要求開始指示パケット送信失敗時の再送回数を設定します。
設定範囲： 1 ~ 255
導入時の設定： 10
- RESET** - request send timer normal
KeepAlive代理要求パケットの送信間隔 (通常時) を設定します。
設定範囲： 1 ~ 255 [min]
導入時の設定： 5
- RESET** - request send timer retry
KeepAlive代理要求パケットの送信間隔 (リトライ時) を設定します。
設定範囲： 1 ~ 255 [min]
導入時の設定： 1
- RESET** - request send retry count
KeepAlive代理要求パケットのリトライ回数を設定します。
設定範囲： 1 ~ 255
導入時の設定： 10
- RESET** - response stop indicate timer
代理応答停止指示パケット送信失敗時の再送タイマを設定します。
設定範囲： 1 ~ 255 [sec]
導入時の設定： 3
- RESET** - response stop retry count
代理応答停止指示パケット送信失敗時の再送回数を設定します。
設定範囲： 1 ~ 255
導入時の設定： 10
- RESET** - response restart indicate timer
代理応答再開指示パケット送信失敗時の再送タイマを設定します。
設定範囲： 1 ~ 255 [sec]
導入時の設定： 3

- RESET** - response restart retry count
代理応答再開指示パケット送信失敗時の再送回数を設定します。
設定範囲： 1 ~ 255
導入時の設定： 10
- RESET** - response end indicate timer
代理応答終了指示パケット送信失敗時の再送タイマを設定します。
設定範囲： 1 ~ 255 [sec]
導入時の設定： 3
- RESET** - response end retry count
代理応答終了指示パケット送信失敗時の再送回数を設定します。
設定範囲： 1 ~ 255
導入時の設定： 2
- RESET** - response end timer
代理応答終了指示を受信してから代理応答エントリ解放までのタイマを設定します。
設定範囲： 1 ~ 255 [min]
導入時の設定： 10

4.7 AppleTalkに関する拡張設定

AppleTalkルーティング機能に関する拡張設定を行います。AppleTalkルーティングの拡張機能は、メインメニューで「configuration set (expert)」を選択後「AppleTalk routing」を選択して設定します。

拡張設定メニューは、基本設定で選択した機能により次の3種類の表示があります。

1.AURPを「not use」とした場合（図4-60参照）

2.AURPを「use」とし、「IP Tunnel」を「not use」とした場合（図4-61参照）

2.AURPを「use」とし、「IP Tunnel」を「use」とした場合（図4-62参照）

```
*** EXP.: AppleTalk routing configuration menu ***
1. AppleTalk interface
2. static routing
3. static zone
4. DDP (forward) filtering
5. DDP (discard) filtering
6. service (forward) filtering
7. service (discard) filtering
8. zone filtering
9. accept gateway
10. propagate gateway
11. accept port
12. propagate port
Select the number. :
```

図4-60 AppleTalkルーティングの拡張設定メニュー（AURPを「not use」とした場合）

```
*** EXP.: AppleTalk routing configuration menu ***
1. AppleTalk interface
2. static routing
3. static zone
4. DDP (forward) filtering
5. DDP (discard) filtering
6. service (forward) filtering
7. service (discard) filtering
8. zone filtering
9. accept gateway
10. propagate gateway
11. accept port
12. propagate port
13. AURP protocol
Select the number. :
```

図4-61 AppleTalkルーティングの拡張設定メニュー（AURPを「use」とし、「IP Tunnel」を「not use」とした場合）

```
*** EXP.: AppleTalk routing configuration menu ***
1. AppleTalk interface
2. static routing
3. static zone
4. DDP (forward) filtering
5. DDP (discard) filtering
6. service (forward) filtering
7. service (discard) filtering
8. zone filtering
9. accept gateway
10. propagate gateway
11. accept port
12. propagate port
13. AURP protocol
14. IP Tunneling exterior router table
Select the number. :
```

図4-62 AppleTalkルーティングの拡張設定メニュー（AURPを「use」とし、
「IP Tunnel」を「use」とした場合）

- AppleTalk interface
AppleTalkのインタフェースに関する動作を設定します。
- static routing
AppleTalkスタティックルーティングテーブルを設定します。
- static zone
AppleTalkスタティックゾーンを設定します。
- DDP (forward) filtering
中継するDDPパケットのフィルタリングテーブルを設定します。DDPフィルタリング機能を使用する場合、本テーブルに設定されたエントリのみを中継します。テーブルに設定されていないパケットはすべて廃棄します。
- DDP (discard) filtering
遮断するDDPパケットのフィルタリングテーブルを設定します。DDPフィルタリング機能を使用する場合、「DDP(forward) filtering」で設定されたパケットでも本テーブルに設定されたパケットは中継しません。
- service (forward) filtering
中継するサービスのフィルタリングテーブルを設定します。サービスフィルタリング機能を使用する場合、本テーブルに設定されたエントリのみを中継します。テーブルに設定されていないパケットはすべて廃棄します。

- service (discard) filtering
遮断するサービスのフィルタリングテーブルを設定します。サービスフィルタリング機能を使用する場合、「service (forward) filtering」で設定されたパケットでも本テーブルに設定されたパケットは中継しません。
- zone filtering
ゾーン名によるフィルタリングテーブルを設定します。
- accept gateway
ルーティング情報のパケットを送信元ゲートウェイアドレスによりフィルタリングします。
- propagate gateway
ルーティング情報別に宛先ゲートウェイを限定します。
- accept port
ルーティング情報のパケットを受信ポートによりフィルタリングします。
- propagate port
ルーティング情報別に宛先ポートを限定します。
- AURP protocol
AURPに関する動作を設定します。
- IP Tunneling exterior router table
IP Tunneling exterior routerのテーブルを設定します。

4.7.1 AppleTalkインタフェースの設定

「AppleTalk interface」を選択することにより、AppleTalkインタフェースに関する動作を設定します。

```
*** EXP.: Set AppleTalk routing configuration ***
<AppleTalk routing interface parameter(s)>
1. general configuration
2. interface configuration
3. end
Select the number. [3]:
```

図4-63 AppleTalkインタフェースの設定メニュー

(1) AppleTalk動作（装置単位）の設定

図4-63で、「general configuration」を選択し、装置単位のAppleTalkの動作の設定を行います。

```
<AppleTalk routing general parameter(s)>
DDP checksum                :not use
AMT ageout timer (sec)      :1
AARP request (reply timer (sec): 1 retry count: 5)
ATP TReq (reply timer (sec): 3 retry count: 5)
phase 1 bridge              :not use
Do you change (y/n)? [n]:  y
DDP checksum (1:use 2:not use) [2]:
AMT ageout timer (sec) [1]:
AARP request reply timer (sec) [1]:
        retry count [5]:
ATP TReq reply timer (sec) [3]:
        retry count [5]:
phase 1 bridge (1:use 2:not use) [2]:

<AppleTalk routing interface general parameter(s)>
DDP checksum                :not use
AMT ageout timer (sec)      :1
AARP request (reply timer (sec): 1 retry count: 5)
ATP TReq (reply timer (sec): 3 retry count: 5)
phase 1 bridge              :not use
Set OK (y/n)? [y]:
```

図4-64 AppleTalk動作（装置単位）の設定例

RESET

- DDP checksum

DDPパケットにチェックサムをつけて送信するかどうか設定します。

設定範囲： 1:use

2:not use

導入時の設定： 2:not use

4章 拡張設定

- RESET** - AMT ageout timer
AMT (アドレスマッピングテーブル) のタイムアウト時間を設定します。
設定範囲: 1 ~ 255[sec]
導入時の設定: 1
- RESET** - AARP request reply timer
AARPリクエストの応答を監視するタイマのタイムアウト値を設定します。
設定範囲: 1 ~ 255[sec]
導入時の設定: 1
- RESET** - AARP request retry count
AARPリクエストの再送回数を設定します。
設定範囲: 1 ~ 100[回]
導入時の設定: 5
- RESET** - ATP TReq reply timer
トランザクションリクエストの応答を監視するタイマのタイムアウト値を設定します。
設定範囲: 1 ~ 255[sec]
導入時の設定: 3
- RESET** - ATP TReq retry count
トランザクションリクエストの再送回数を設定します。
設定範囲: 1 ~ 100[回]
導入時の設定: 5
- RESET** - phase 1 bridge
AppleTalk phase 1 のブリッジングを行うかどうかを設定します。
設定範囲: 1:use
2:not use
導入時の設定: 2:not use

(2) AppleTalk動作（グループ/チャンネル毎）の設定

図4-63で、「interface configuration」を選択し、グループ/チャンネル毎のAppleTalkの動作の設定を行います。

```
<AppleTalk routing interface parameter(s)>
      1.GroupA      2.GroupB      3.BRI#6-2      4.BRI#7-2
Select the number : 1

      ATPC      routing info      routing table
port      Prot.      offer interval aging validity
-----+-----+-----+-----
GroupA RTMP      no              10 no              20

Do you change (y/n)? [n]: y
ATCP routing protocol (1:not use 2:RTMP) [2]:
routing information offering (1:yes 2:no) [2]:
              interval (sec) [10]:
routing table aging (1:yes 2:no) [2]:
              validity (sec) [20]:

      ATPC      routing info      routing table
port      Prot.      offer interval aging validity
-----+-----+-----+-----
GroupA RTMP      no              10 no              20
Set OK (y/n)? [y]:
```

図4-65 AppleTalk動作（グループ/チャンネル毎）



メモ：本設定で選択できるポートは、LAN以外のAppleTalkルーティングを行うポートです。

RESET

- ATPC routing protocol

WAN回線を介してルータを接続した場合に、RTMPによりルーティング情報の送受信を行う/行わないを設定します。本設定は、ルーティングインタフェースに選択したポート毎に設定を行います。

設定範囲： 1:not use

2:RTMP

導入時の設定： 2:RTMP

RESET

- routing information offering

ISDN回線にルーティング情報を定期的に送信するかどうかを選択します。

設定範囲： 1:yes

2:no

導入時の設定： 2:no

- RESET** - routing information interval
上記の「routing information offering」で、「yes」とした場合、定期的に送信する間隔を設定します。
設定範囲： 10 ~ 4294967[sec]
導入時の設定： 10

- RESET** - routing table aging
ISDN回線からのルーティング情報のエージアウトを行うかどうかを選択します。
設定範囲： 1:yes
 2:no
導入時の設定： 2:no

- RESET** - routing table validity
上記の「routing table aging」で「yes」とした場合、エージアウトする時間を設定します。
設定範囲： 20 ~ 4294967[sec]
導入時の設定： 20

4.7.2 AppleTalkスタティックルーティングの設定

スタティックルーティングテーブルの設定をします。本設定は基本設定で行うこともできます。設定方法は「3.17.6 AppleTalkスタティックルーティングの設定」と同じです。

4.7.3 AppleTalkスタティックゾーンテーブルの設定

スタティックゾーンの設定をします。本設定は基本設定で行うこともできます。設定方法は「3.17.7 AppleTalkスタティックゾーンテーブルの設定」と同じです。

4.7.4 AppleTalk DDP(forward)フィルタリングの設定

AppleTalk DDP(forward)フィルタリングの設定をします。本設定は基本設定で行うこともできます。設定方法は「3.17.4 AppleTalk DDP(forward)フィルタリングの設定」と同じです。

4.7.5 AppleTalk DDP(discard)フィルタリングの設定

AppleTalk DDP(discard)フィルタリングの設定をします。
本装置のDDP(discard)フィルタリング機能では、遮断するすべてのパケットをフィルタリングテーブルに設定します。本テーブルに設定されたパケットを受信した場合は、「4.7.4 DDP(forward) filtering」により中継を許可されたものであっても廃棄されます。本テーブルには、最大32エントリ登録できます。

設定方法は、「4.7.4 AppleTalk DDP(forward)フィルタリングの設定」と同じです。

4.7.6 AppleTalkサービス(forward)フィルタリングの設定

サービス(forward)フィルタリングの設定をします。

本装置のサービス(forward)フィルタリング機能では、中継を許可するすべてのサービスをフィルタリングテーブルに設定します。テーブルに設定されていないサービスに関するNBPパケットを受信した場合は廃棄されます。

```
*** EXP.: Set AppleTalk routing service filtering configuration (forward)
***
    1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図4-66 サービス(forward)フィルタリングテーブル設定メニュー

以下に、サービス(forward)フィルタリングテーブルの追加例を示します。

中継を許可するサービスをフィルタリングテーブルに設定します。テーブルには最大64エントリが登録できます。

```
<Add AppleTalk routing service filtering data>
object name []: =
type name []: =
filter port
    1.LAN(AppleTalk)      2.LAN(IP tunnel)
    2.GroupA             4.GroupB             5.BRI#7-1             6.BRI#7-2
Select the number [1,2,3,4,5,6]: 1
receive port
    1.LAN(AppleTalk)      2.LAN(IP tunnel)
    2.GroupA             4.GroupB             5.BRI#7-1             6.BRI#7-2
Select the number [1,2,3,4,5,6]: 2

AppleTalk routing service filtering data:
    2. object name :=
       type name :=
       filter port :LAN(AppleTalk)
       receive port :LAN(IP tunnel)
Add OK (y/n)? [y]:
```

図4-67 サービス(forward)フィルタリングテーブル追加例

- object name

オブジェクト名を設定します。何も設定しないと無効になります。「=」を設定するとすべてのノードを表します。

設定範囲： 最大32文字の英数字，=（すべてのオブジェクト）

導入時の設定： なし

- type name
タイプ名を設定します。何も設定しないと無効になります。「=」を設定すると、すべてのタイプを表します。
設定範囲： 最大32文字の英数字，=（すべてのタイプ）
導入時の設定： なし

- filter port
上記で指定したサービスを送信するポートを指定します。WAN回線の設定範囲は、通常回線として選択している回線から選択します。また、「LAN(IP Tunnel)」は、基本設定で、「AURP」を「use」さらにLANポートの「IP Tunnel」を「use」とした時のみ表示されます。
設定範囲： LAN(AppleTalk),LAN(IP Tunnel),AppleTalkルーティングを使用するすべてのポート
導入時の設定： なし

- receive port
上記で指定したサービスの受信ポートを指定します。上記で指定したサービスはここで指定したポート側に存在するもののみフィルタリングの対象となります。WAN回線の設定範囲は、通常回線として選択している回線から選択します。また、「LAN(IP Tunnel)」は、基本設定で、「AURP」を「use」さらにLANポートの「IP Tunnel」を「use」とした時のみ表示されます。
設定範囲： LAN(AppleTalk),LAN(IP Tunnel),AppleTalkルーティングを使用するすべてのポート
導入時の設定： なし



メモ：「object name」「type name」で指定したサービスのうち「filtering port」で指定したポート側に存在するものが「receive port」で指定したポート側に提供されます。

サービス(forward)フィルタリングテーブルのエントリの設定は、設定メニュー画面では以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリの表示を行います。
- end 設定を終了します。

4.7.7 AppleTalkサービス(discard)フィルタリングの設定

サービス(discard)フィルタリングの設定をします。

サービス(forward)フィルタリングにより中継を許可された中から中継を許可しないサービスを指定することにより、より細かなフィルタリングを行うことができます。

本テーブルに設定されたサービスは、サービス(forward)フィルタリングにより中継を許可されたものであっても廃棄されます。テーブルには最大64エントリが登録できます。

設定方法は、「4.7.6 AppleTalkサービス(forward)フィルタリングの設定」と同じです。

4.7.8 ゾーンフィルタリングの設定

ゾーンフィルタリングテーブルの設定とそのエントリを有効にするか無効にするかの設定を行います。テーブルには最大32エントリが登録できます。

```
*** EXP.: Set AppleTalk routing zone filtering ***
1. table attribute
2. filtering data
Select the number. :
```

図4-68 ゾーンフィルタリングテーブルの設定メニュー

(1) ゾーンフィルタリングテーブルの属性の設定

「table attribute」を選択してフィルタリングテーブルの属性を設定します。

```
<AppleTalk routing zone filtering attribute>
  attribute: exclude
Do you change (y/n)? [n]: y
attribute (1:include 2:exclude) [2]:
AppleTalk routing zone filtering attribute
parameter(s) are set to the following values.
<AppleTalk routing zone filtering attribute>
  attribute: exclude
Set OK (y/n)? [y]:
```

図4-69 ゾーンフィルタリングテーブルの属性の設定例

- attribute

フィルタリングテーブルに設定されているエントリに一致したゾーンを見せるか見せないかを選択します。

設定範囲： 1:include (見せる)

2:exclude (見せない)

導入時の設定： 2:exclude (見せない)

(2) フィルタリングテーブルの設定

「filtering data」を選択して、見せる（または見せない）ゾーンを設定します。

```
*** Set AppleTalk routing zone filtering data ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図4-70 ゾーンフィルタリングテーブルの設定メニュー

以下に、ゾーンフィルタリングテーブルの追加例を示します。
テーブルには最大128エントリ登録できます。

```
<Add AppleTalk routing zone filtering data>
zone name []: support
filter port
  1.LAN(AppleTalk)      2.LAN(IP tunnel)
  2.GroupA             34.GroupB      5.BRI#7-1      6.BRI#7-2
Select the number []: 3

AppleTalk routing zone filtering data:
no  zone name
    filter port
-----+-----
  1. support
     GroupA
Add OK (y/n)? [y]:
```

図4-71 ゾーンフィルタリングテーブルの設定例

- zone name
フィルタリングを行うゾーンの名前を設定します。何も設定しないと無効になります。
ただし、「*」を設定するとすべてのゾーンを示します。
設定範囲： 1～32文字の英数字，*（すべてのゾーン）
導入時の設定： なし
- filter port
上記で指定したゾーンのフィルタリングを行うポートを指定します。「filter port」で指定したポート側において、他ポート側に存在するゾーンのうち「zone name」で指定したゾーンを見せる（または見せない）ようにします。WAN回線の設定範囲は、通常回線として選択している回線から選択します。また、「LAN(IP Tunnel)」は、基本設定で、「AURP」を「use」さらにLANポートの「IP Tunnel」を「use」とした時のみ表示されません。
設定範囲： LAN(AppleTalk),LAN(IP Tunnel),AppleTalkルーティングを使用するポート
導入時の設定： なし

フィルタリングテーブルの設定は以下のメニューコマンドを選択することによって行ってください。

- change..... フィルタリングテーブルの変更を行います。
- delete フィルタリングテーブルの削除を行います。
- add フィルタリングテーブルの追加を行います。
- display フィルタリングテーブルの表示を行います。
- end 設定を終了します。

4.7.9 ルーティング情報のフィルタリング(accept gateway)の設定

ルーティング情報の受信フィルタリング(中継ルータによる)テーブルの設定とそのエントリを有効にするか無効にするかの設定を行います。

```
*** EXP.: Set AppleTalk routing information accept filtering (GW) ***
1. table attribute
2. filtering data
Select the number. :
```

図4-72 accept gatewayの設定メニュー

(1) フィルタリングテーブルの属性の設定

「table attribute」を選択してフィルタリングテーブルの属性を設定します。

```
<AppleTalk routing information accept filtering (GW) attribute>
attribute: exclude
Do you change (y/n)? [n]: y
attribute (1:include 2:exclude) [2]:

AppleTalk routing information accept filtering (GW) attribute
parameter(s) are set to the following values.
<AppleTalk routing information accept filtering (GW) attribute>
attribute: exclude
Set OK (y/n)? [y]:
```

図4-73 accept gatewayの属性の設定例

- attribute
フィルタリングテーブルに設定されているエントリに一致したエントリを有効にするか無効にするか選択します。
設定範囲： 1:include (有効にする)
 2:exclude (無効にする)
導入時の設定： 2:exclude (無効にする)

(2) フィルタリングテーブルの設定

「filtering data」を選択して、有効にする（または無効にする）エントリを設定します。

```
*** Set AppleTalk routing information accept filtering (GW) data ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]:
```

図4-74 accept gatewayフィルタリングテーブル設定メニュー

以下に、accept gatewayフィルタリングテーブルの追加例を示します。ゲートウェイが最大32個、1ゲートウェイあたりの宛先アドレスとして最大7エントリ、総計224エントリのテーブルが登録できます。

```
<Add AppleTalk routing information accept filtering (GW) data>
dst network start [0]: 2
      end [2]: 3
type(1:AppleTalk 2:other) []: 1
gateway network number [0]: 12
      node ID [0]: 1

AppleTalk routing information accept filtering (GW) data:
  no  dst network
      (str  end) type      gateway
-----+-----+-----+-----
      2.    2    3 AppleTalk    12    1
Add OK (y/n)? [y]:
```

図4-75 accept gatewayフィルタリングテーブル設定例

- dst network start
ルーティング情報の宛先ネットワークのネットワーク番号範囲の始めを設定します。
設定範囲： 0 ~ 65535
導入時の設定： 0
- dst network end
ルーティング情報の宛先ネットワークのネットワーク番号範囲の終わりを設定します。
ただし、ネットワーク番号範囲の始めより等しいか大きい値でなければいけません。
設定範囲： 0 ~ 65535
導入時の設定： 0

- type
ルーティング情報の送信元ルータのアドレスのタイプを選択します。「AppleTalk」は対象とするルータがAppleTalkルータの場合、「ISDN index」はWAN回線動作モードでISDNを選択し、さらに「AppleTalk リモートターゲット編」で「target index」を記入した場合、「IP Address」は「AppleTalkルーティング編」の「IP Tunnel」を「use」とした場合にそれぞれ選択が可能です。「other」は他のエントリで指定されないすべてのゲートウェイを対象にします。

設定範囲： 1:AppleTalk
2:ISDN index
3:IP Address
4:other

導入時の設定： なし

- gateway network number
ルーティング情報の送信元ルータのネットワーク番号を設定します。AppleTalk 選択時のみ入力します。上記の「type」で選択した番号により、設定範囲は異なります。「other」を選択した場合は、設定の必要はありません。

(AppleTalk選択時)

設定範囲： 0 ~ 65535

導入時の設定： なし

(ISDN index選択時)

設定範囲： AppleTalkリモートターゲット (最大80エントリから1エントリ選択)

導入時の設定： なし



メモ：「multi target」を「not use」にした場合は、ISDNリモートターゲットの「target index」の中から1エントリ選択します。

(IP address選択時)

設定範囲： xxx.xxx.xxx.xxxの形式

導入時の設定： なし

フィルタリングテーブルの設定は以下のメニューコマンドを選択することによって行ってください。

- change..... フィルタリングテーブルの変更を行います。
- delete フィルタリングテーブルの削除を行います。
- add フィルタリングテーブルの追加を行います。
- display フィルタリングテーブルの表示を行います。
- end 設定を終了します。

4.7.10 ルーティング情報のフィルタリング(propagate gateway)の設定

ルーティング情報の送信フィルタリング（中継ルータによる）テーブルの設定とそのエントリを有効にするか無効にするかの設定を行います。ゲートウェイが最大32個、1ゲートウェイあたりの宛先アドレスとして最大7エントリ、総計224エントリのテーブルが登録できます。

設定方法は、「4.7.9 ルーティング情報のフィルタリング(accept gateway)の設定」と同じです。

4.7.11 ルーティング情報のフィルタリング(accept port)の設定

ルーティング情報の受信フィルタリング（中継ポートによる）テーブルの設定とそのエントリを有効にするか無効にするかの設定を行います。

```
*** EXP.: Set AppleTalk routing information accept filtering (port) ***
1. table attribute
2. filtering data
Select the number. : 1
```

図4-76 accept portの設定メニュー

(1) フィルタリングテーブルの属性の設定

「table attribute」を選択してフィルタリングテーブルの属性を設定します。

```
<AppleTalk routing information accept filtering (port) attribute>
attribute: exclude
Do you change (y/n)? [n]: y
attribute (1:include 2:exclude) [2]:

AppleTalk routing information accept filtering (port) attribute
parameter(s) are set to the following values.
<AppleTalk routing information accept filtering (port) attribute>
attribute: exclude
Set OK (y/n)? [y]:
```

図4-77 accept portの属性の設定例

- attribute
フィルタリングテーブルに設定されているエントリに一致したエントリを有効にするか無効にするか選択します。
設定範囲： 1:include（有効にする）
 2:exclude（無効にする）
導入時の設定： 2:exclude（無効にする）

(2) フィルタリングテーブルの設定

「filtering data」を選択して、有効にする（または無効にする）エントリを設定します。

```
*** Set AppleTalk routing information accept filtering (port) data ***
  1. change  2. delete  3. add  4. display  5. end
Select the number. [5]: 3
```

図4-78 accept portフィルタリングテーブルの設定メニュー

以下に、accept portフィルタリングテーブルの追加例を示します。

テーブルは、最大40エントリまで登録できます。

```
<Add AppleTalk routing information accept filtering (port) data>
dst network start [0]: 100
      end [100]:
receive port
  1.LAN(AppleTalk)      2.LAN(IP tunnel)
  2.GroupA      34.GroupB      5.BRI#7-1      6.BRI#7-2
Select the number []: 1,2,3,4,5,6

AppleTalk routing information accept filtering (port) data:
no dst network
      (str end) receive port
-----+-----+-----+-----+-----+-----+-----+-----+-----+
  2.   100   100 LAN(ETalk2),LAN(IP tunnel),GroupA,GroupB,BRI#7-1
      BRI#7-2
Add OK (y/n)? [y]:
```

図4-79 accept portフィルタリングテーブルの設定例

- dst network start
ルーティング情報の宛先ネットワークのネットワーク番号範囲の始めを設定します。
設定範囲： 0 ~ 65535
導入時の設定： 0
- dst network end
ルーティング情報の宛先ネットワークのネットワーク番号範囲の終わりを設定します。
ただし、ネットワーク番号範囲の始めより等しいか大きい値でなければいけません。
設定範囲： 0 ~ 65535
導入時の設定： 0

- send port

フィルタリングを行うポートを指定します。WAN回線の設定範囲は、通常回線として選択している回線から選択します。また、「LAN(IP Tunnel)」は、基本設定で、「AURP」を「use」さらにLANポートの「IP Tunnel」を「use」とした時のみ表示されます。

設定範囲： LAN(AppleTalk),LAN(IP Tunnel),AppleTalkルーティングを使用するポート

導入時の設定： なし

フィルタリングテーブルの設定は以下のメニューコマンドを選択することによって行ってください。

- change..... フィルタリングテーブルの変更を行います。
- delete フィルタリングテーブルの削除を行います。
- add フィルタリングテーブルの追加を行います。
- display フィルタリングテーブルの表示を行います。
- end 設定を終了します。

4.7.12 ルーティング情報のフィルタリング(propagate port)の設定

ルーティング情報の送信ポートによるフィルタリングテーブルの設定とそのエントリを有効にするか無効にするかの設定を行います。テーブルには最大40エントリが登録できます。

設定方法は、「4.7.11 accept port」と同じです。

4.7.13 AURP protocolの設定

AURPに関する設定を行います。この項目は基本設定で「AURP」を「use」とした時のみ表示されます。

```

*** EXP.: Set AppleTalk routing AURP protocol configuration ***
 1.LAN
 2.GroupA      3.GroupB      4.BRI#6-2      5.BRI#7-2
Select the number : 2

<AppleTalk routing AURP protocol configuration parameter(s)>
[GroupA]
  protocol                : AURP
  Tickle packet           : not use
      send time           : 90
  send AURP packet any time : yes
  resend open request      : yes
  remapping                : not use
  remapping range start    : -----
      end                  : -----
  clustering               : -----
  hop count reduction      : -----

Do you change (y/n)? [n]: y
protocol (1:AURP/RTMP 2:static 3:AURP) [3]:
Tickle packet (1:use 2:not use) [2]: 1
      send time [90]:
send AURP packet any time (1:yes 2:no) [1]:
resend open request (1:yes 2:no) [1]:
remapping (1:use 2:not use) [2]: 1
remapping range start []: 5000
      end []: 6000
clustering (1:use 2:not use) [2]: 1
hop count reduction (1:use 2:not use) [2]: 1

AppleTalk routing AURP protocol parameter(s) are set to the following
values.
<AppleTalk routing AURP protocol configuration parameter(s)>
[GroupA]
  protocol                : AURP
  Tickle packet           : use
      send time           : 90
  send AURP packet any time : yes
  resend open request      : yes
  remapping                : use
  remapping range start    : 5000
      end                  : 6000
  clustering               : use
  hop count reduction      : use

Set OK (y/n)? [y]:

```

図4-80 AURPの設定例

(1) AURPの設定を行う

AURPに関する拡張機能の設定を行います。

- RESET** - protocol
ルーティングプロトコルを選択します。この項目はWAN回線の場合にのみ設定します。WAN回線にFRを選択した場合は、「RTMP」は選択可能で「AURP/RTMP」は選択不可能です。「AURP/RTMP」を選択すると、回線を接続した相手が「AURP」を使わない場合でも「RTMP」でルート情報交換が可能です。
設定範囲： 1:AURP/RTMP
2:RTMP
3:static
4:AURP
導入時の設定： 4:AURP
- RESET** - Tickle packet
Tickle packetを送信するかどうか設定します。Tickle packetを送信してそれに対する応答で相手のルータがupしているかどうか確認することができます。ISDNを選択している場合、Tickle packetを定期的に送信すると回線が接続されてしまうので、送信するかしないかを設定します。
設定範囲： 1:use
2:not use
導入時の設定： 2:not use
- RESET** - Tickle packet send time
Tickle packetの定期送信間隔を設定します。
設定範囲： 30 ~ 4294967[sec]
導入時の設定： 90
- RESET** - send AURP packet any time (ISDN選択時のみ)
回線が接続されていないときにAURPのルーティングパケットを送信するかどうか設定します。「yes」とした場合は、ルート情報に変化があった際に回線を接続して変更内容を相手ルータに通知します。「no」とした場合は、回線が接続した際にルート情報交換を行います。
設定範囲： 1:yes
2:no
導入時の設定： 2:no



メモ：「yes」とした場合は、必ず相手ルータでの設定も「yes」にします。



注意：ISDN選択時で、「IP Tunnel」を使用する場合、「send AURP packet any time」は「yes」を選択します。

- RESET** - resend open request
 相手ルータとAURPのコネクションが解放された後，Open-Reqパケットを再送するかどうか設定します．
 設定範囲： 1:yes
 2:no
 導入時の設定： 1:yes
- RESET** - remapping
 リマッピングを行うかどうか設定します．リマッピングを行うと，そのポート側に存在するネットワークについて内部的にネットワーク番号範囲を割り当て直します．
 設定範囲： 1:use
 2:not use
 導入時の設定： 2:not use
- RESET** - remapping range start
 リマッピングするネットワーク番号範囲の始めを設定します．リマッピングするネットワーク番号範囲は，リマッピングを行っていないポート側に存在するネットワークで使用されていない値にします．また，他のポートのリマッピングレンジでも使用されていない値にします．この項目は「remapping」を「use」にした場合のみ設定します．
 設定範囲： 1 ~ 65279
 導入時の設定： 0
- RESET** - remapping range end
 リマッピングを行うネットワーク番号範囲の終わりを設定します．ただし，ネットワーク番号範囲の始めより等しいか大きい値でなければいけません．この項目は「remapping」を「use」にした場合のみ設定します．
 設定範囲： 1 ~ 65279
 導入時の設定： 0
- !** 注意：ネットワークにループが存在すると，リマッピングしたルーティング情報を再び受信して再度リマッピングしてしまうため，リマッピングを行う場合は，ネットワークにループが存在しないことを確認します．
- !** 注意：ネットワーク上にリマッピングを行わないルータが存在すると，ルータ間でループが生じたときに発見することができないため，リマッピングの設定はすべてのルータで統一する必要があります．
- clustering
 クラスタリングを行うかどうか設定します．クラスタリングを行うと複数にリマッピングされたネットワーク番号範囲を一つのネットワークとして扱うため，ルーティング情報やNBPのパケットによるトラフィックを削減することができます．この項目は，「remapping」を「use」にした場合のみ「use」に設定できます．
 設定範囲： 1:use
 2:not use
 導入時の設定： 2:not use

RESET - hop count reduction

大規模なネットワークを構築するときに、DDPとRTMPのホップカウントの制限(15hops)を無視するかどうか設定します。この項目は、「remapping」を「use」にした場合のみ「use」に設定できます。

設定範囲： 1:use
 2:not use
導入時の設定： 2:not use

4.7.14 外部AppleTalkルータの設定

設定方法は「3.17.3 外部AppleTalkルータの設定」と同じです。ここでの設定は、基本設定で行う設定とまったく同じです。

4.8 SNMPに関する拡張設定

SNMPに関する設定は、「3.19 SNMPに関する基本設定」と同じです。

4.9 リモートファイルメンテナンスの設定

本設定では、システムのアップデート等に関する設定を行います。リモートファイルメンテナンスの設定画面を図4-81に示します。

```
*** EXP.: Set Remote file maintenance configuration ***
<Remote file maintenance parameter(s)>
    server timer11 (sec): 5
        timer12 (sec):25
    client timer11 (sec): 5
        timer12 (sec):25
Do you change (y/n)? [n]:
```

図4-81 リモートファイルメンテナンス設定画面

- server timer11
サーバの、クライアントからの応答待ちタイマを設定します。サーバは、ここで設定された時間内にクライアントから応答がないと、通信のリトライを行います。
設定範囲：1 ~ 655 [秒]
導入時の設定： 5
- server timer12
サーバの、クライアントに対するリトライタイマを設定します。サーバは、ここで設定された時間だけクライアントに対して、「server timer11」間隔でリトライを続けます。
設定範囲： 1 ~ 655 [秒]
導入時の設定： 25
- client timer11
クライアントの、サーバからの応答待ちタイマを設定します。クライアントは、ここで設定された時間内にサーバから応答がないと、通信のリトライを行います。
設定範囲： 1 ~ 655 [秒]
導入時の設定： 5
- client timer12
クライアントの、サーバに対するリトライタイマを設定します。クライアントは、ここで設定された時間だけサーバに対して、「client timer11」間隔でリトライを続けます。
設定範囲： 1 ~ 655 [秒]
導入時の設定： 25

4.10 データ別優先制御に関する拡張設定

データ別優先制御機能に関する拡張設定を行います。データ別優先制御機能は、メインメニューで「configuration set (expert)」を選択後「packet priority control」を選択して設定します。

```
*** EXP.: Data priority configuration menu ****
1. motion parameter(s)
2. IP protocol
3. IP address
4. IPX protocol
5. IPX address
6. AppleTalk protocol
7. AppleTalk address
8. bridging
9. MAC address
Select the number. :
```

図4-82 データ別優先制御設定メニュー

- motion parameter(s)
データ優先制御に関する動作を設定します。
- IP protocol
データ別優先制御を行うIPプロトコルを設定します。
- IP address
データ別優先制御を行うIPアドレスを設定します。
- IPX protocol
データ別優先制御を行うIPXプロトコルを設定します。
- IPX address
データ別優先制御を行うIPXアドレスを設定します。
- AppleTalk protocol
データ別優先制御を行うAppleTalkプロトコルを設定します。
- AppleTalk address
データ別優先制御を行うAppleTalkアドレスを設定します。
- bridging
データ別優先制御を行うブリッジングデータテーブルを設定します。

- MAC address
データ別優先制御を行うMACアドレスを設定します。

4.10.1 パラメータの設定

図4-82で「motion parameter(s)」を選択して、データ別優先制御に関する動作を設定します。

```

*** EXP.: Set Packet priority control motion configuration ****
<Packet priority control motion parameter(s)>
  packet priority control: not use
Do you change (y/n)? [n]: y
packet priority control (1:use 2:not use) [2]: 1
band rate high [70]:
  normal [20]:
EXP.: Packet priority control motion parameter(s) are
  set to the following values.
<Packet priority control motion parameter(s)>
  packet priority control: use
  band rate high          : 70
  normal                  : 20
Set OK (y/n)? [y]:

```

図4-83 パラメータの設定例

(1) データ優先制御の動作の設定

データ優先制御の動作を選択します。本機能では優先度を「優先」、「通常」、「非優先」の3段階とし、各優先度を割り当てられたデータをどの割合で送信するかを比率を設定します。一定時間内に送信するデータのバイト数を比率で管理することにより、各優先度の送信帯域を保証します。

- RESET** - packet priority control
データ優先制御を行うかどうかを選択します。
設定範囲： 1:use
 2:not use
導入時の設定： 2:not use

以下の項目は、「packet priority control」で「use」としたときのみ設定可能です。

- band rate high
優先度が「優先」の場合の比率を設定します。
設定範囲： 0 ~ 100
導入時の設定： 70

- band rate normal
優先度が「通常」の場合の比率を設定します。
設定範囲： 0 ~ 100 - [band rate highの値]
導入時の設定： 20
(この値が範囲外になる場合は、範囲内の最大値)



メモ：「非優先」の比率の設定項目はありませんが、100 - (「優先」+「通常」)の値が自動的に設定されます。



メモ：いずれかの優先度に該当するデータが存在しない場合は、それ以外の優先度のデータのみでデータを送信します。例えば、比率が優先 = 70%、通常 = 20%、非優先 = 10%と設定されている場合で、「優先」のデータがない時は、「通常」と「非優先」の比率20:10で送信します。

4.10.2 IPプロトコルの設定

データ別優先制御を行うIPプロトコルの選択とその優先度を設定します。「packet priority」が「not use」の場合に「IP protocol」を選択すると「Input error!」となり、設定を行うことはできません。最大8エン트리設定することができます。

```
*** EXP.: Set IP protocol table configuration ***
<Protocol table (max 8 entries)>
no entry.

1. change 2. delete 3. add 4. end
Select the number. [4]: 3
application (1:telnet 2:ftp-data 3:ftp 4:snmp 5:all 6:other) [5]:
protocol (1:tcp 2:udp 3:icmp 4:ospf 5:all 6:other) [5]:
priority (1:high 2:normal 3:low) [1]:

IP protocol table data:
no application protocol priority
-----+-----+-----
1. *           *           high
Add OK (y/n)? [y]:
```

図4-84 データ優先制御IPプロトコル選択画面

- application
データ優先制御を行うアプリケーションを選択します。複数選択はできません。
設定範囲： 1:telnet
2:ftp-data
3:ftp
4:snmp
5:all
6:other
導入時の設定： 5:all



メモ：「application」で次の値を選択すると、自動で「protocol」が設定されますので、設定の必要はありません。

表4-4 アプリケーションとプロトコル

application	protocol
telnet	tcp
ftp-data	tcp
ftp	tcp
snmp	udp

- application number
「application」で「other」を選択した場合、アプリケーションの番号を設定してください。
設定範囲： 0 ~ 65535
導入時の設定： 0
- protocol
「application」で「all」を選択した場合、上位プロトコルを選択してください。複数選択はできません。「application」で「other」を選択した場合は、「tcp」「udp」が設定範囲になります。
設定範囲： 1:tcp
2:udp
3:icmp
4:ospf
5:all
6:other
導入時の設定： 5:all
- protocol number
「protocol」で「other」を選択した場合、プロトコル番号を設定してください。
設定範囲： 0 ~ 255
導入時の設定： 0
- priority
優先度を選択します。
設定範囲： 1:high
2:normal
3:low
導入時の設定： 1:high

IPプロトコルの優先度の設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。



メモ：テーブルに設定されたエントリに該当しない中継データは、すべて「通常」として扱います。このため、実際の「通常」に設定されたデータの優先制御については、「通常」に設定されたデータのエントリとテーブルに設定されたエントリ以外のデータの両方を対象とします。優先度の設定を行う場合は、テーブルに設定されていないデータのトラフィック量も考慮して設定を行ってください。

4.10.3 IPアドレスの設定

データ別優先制御を行うIPアドレスとその優先度を設定します。設定されたアドレスは送信元、宛先に関係なく優先度が適用されます。「packet priority」が「not use」の場合に「IP address」を選択すると「Input error!」となり、設定を行うことはできません。最大8エントリ設定することができます。

```
*** EXP.: Set IP address table configuration ****
<IP address table (max 8 entries)>
  no entry.

  1. change  2. delete  3. add  4. end
Select the number. [4]: 3
IP address [0.0.0.0]: 10.10.10.10
mask [0.0.0.0]: 10.10.10.10
priority (1:high 2:normal 3:low) [1]:

IP address table data:
no  IP address      mask                priority
---+-----+-----+-----
  1. 10.10.10.10    10.10.10.10        high
Add OK (y/n)? [y]:
```

図4-85 データ優先制御IPアドレス選択画面

- IP address
データ優先制御を行う送信元および宛先IPアドレスを設定します。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： なし

- mask
データ優先制御を行うマスクを設定します。
設定範囲： xxx.xxx.xxx.xxxの形式
導入時の設定： なし

ここでのマスクパターンはサブネットマスクと異なり、クラスにこだわらずに設定が可能です。以下に例を示します。

表4-5 「address」と「mask」の組み合わせ例

address	mask	優先制御の適用されるIPアドレス
172.16.1.1	255.255.255.255	172.16.1.1のみ
172.17.0.0	255.255.0.0	172.17.0.0 ~ 172.17.255.255の全てのIPアドレス
0.0.0.1	0.0.0.255	4バイト目が1である全てのIPアドレス

- priority
優先度を選択します。
設定範囲： 1:high
 2:normal
 3:low
導入時の設定： 1:high

IPアドレスの優先度の設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。



メモ：テーブルに設定されたエントリに該当しない中継データは、すべて「通常」として扱います。このため、実際の「通常」に設定されたデータの優先制御については、「通常」に設定されたデータのエントリとテーブルに設定されたエントリ以外のデータの両方を対象とします。優先度の設定を行う場合は、テーブルに設定されていないデータのトラフィック量も考慮して設定を行ってください。

4.10.4 IPXプロトコルの設定

データ別優先制御を行うIPXプロトコルとその優先度を設定します。「packet priority」が「not use」の場合に「IPX protocol」を選択すると「Input error!」となり、設定を行うことはできません。最大8エントリ設定することができます。

```

*** EXP.: Set IPX protocol table configuration ****
<IPX protocol table (max 8 entries)>
  no entry.

  1. change  2. delete  3. add  4. end
Select the number. [4]: 3
application (1:ncp 2:sap 3:rip 4:netbios 5:diagnostic 6:all 7:other) [6]:
protocol (1:ncp 2:spx 3:netbios 4:all 5:other) [4]:
priority (1:high 2:normal 3:low) [1]:

IPX protocol table data:
no application protocol priority
-----+-----+-----+-----
  1. *           *           high
Add OK (y/n)? [y]:
    
```

図4-86 データ優先制御IPXプロトコル選択画面

- application
データ優先制御を行うアプリケーションを選択します。複数選択はできません。
設定範囲： 1:ncp
2:sap
3:rip
4:netbios
5:diagnostic
6:all
7:other
導入時の設定： 6:all



メモ：「application」で次の値を選択すると、自動で「protocol」が設定されますので、設定の必要はありません。

表4-6 IPXプロトコルのアプリケーションとプロトコル

application	protocol
ncp	ncp
sap	all
rip	all
netbios	netbios
diagnostic	all

- application number
「application」で「other」を選択した場合、アプリケーションの番号を設定してください。
設定範囲： 0 ~ ffff
導入時の設定： 0
- protocol
「application」で「all」を選択した場合、上位プロトコルを選択してください。複数選択はできません。
設定範囲： 1:ncp
2:spx
3:netbios
4:all
5:other
導入時の設定： 4:all
- protocol number
「protocol」で「other」を選択した場合、プロトコル番号を設定してください。
設定範囲： 0 ~ ff
導入時の設定： 0
- priority
優先度を選択します。
設定範囲： 1:high
2:normal
3:low
導入時の設定： 1:high

IPXプロトコルの優先度の設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。



メモ：テーブルに設定されたエントリに該当しない中継データは、すべて「通常」として扱います。このため、実際の「通常」に設定されたデータの優先制御については、「通常」に設定されたデータのエントリとテーブルに設定されたエントリ以外のデータの両方を対象とします。優先度の設定を行う場合は、テーブルに設定されていないデータのトラフィック量も考慮して設定を行ってください。

4.10.5 IPXアドレスの設定

データ別優先制御を行うIPXアドレスとその優先度を設定します。設定されたアドレスは送信元、宛先に関係なく優先度が適用されます。「packet priority」が「not use」の場合に「IPX address」を選択すると「Input error!」となり、設定を行うことはできません。最大8エントリ設定することができます。

```

*** EXP.: Set IPX address table configuration ****
<IPX address table (max 8 entries)>
  no entry.

      1. change  2. delete  3. add  4. end
Select the number. [4]: 3
host number [*]: 100000000000
network number [*]: 11001100
mask [ffffffff]:
priority (1:high 2:normal 3:low) [1]:

IPX address table data:
no host          network mask      priority
----+-----+-----+-----+-----
  1. 100000000000 11001100 ffffffff high
Add OK (y/n)? [y]:

```

図4-87 データ優先制御IPXアドレス設定画面

- host number
データ優先制御を行うホスト番号を設定します。ただし、「*」を設定するとすべてのホスト番号を示します。
設定範囲： 12桁の16進数，*（すべてのホスト番号）
導入時の設定： *
- network number
データ優先制御を行うIPXネットワーク番号を設定します。ただし、「*」を設定するとすべてのIPXネットワーク番号を示します。
設定範囲： 8桁の16進数，*（すべてのIPXネットワーク番号）
導入時の設定： *
- mask
データ優先制御を行うネットワーク番号マスクを設定します。
設定範囲： 8桁の16進数
導入時の設定： ffffffff

ここでのマスクパターンとネットワーク番号の組み合わせの例を以下に示します。

表4-7 「network number」と「mask」の組み合わせ例

network number	mask	フィルタリングの適用されるネットワーク番号
00000001	ffffff	00000001のみ
00010000	ffff0000	00010000 ~ 0001ffffの全てのネットワーク番号
00000001	000000ff	XXXXXXXX01の形式のネットワーク番号

- priority
優先度を選択します。
設定範囲： 1:high
 2:normal
 3:low
導入時の設定： 1:high

IPXアドレスの優先度の設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。



メモ：テーブルに設定されたエントリに該当しない中継データは、すべて「通常」として扱います。このため、実際の「通常」に設定されたデータの優先制御については、「通常」に設定されたデータのエントリとテーブルに設定されたエントリ以外のデータの両方を対象とします。優先度の設定を行う場合は、テーブルに設定されていないデータのトラフィック量も考慮して設定を行ってください。

4.10.6 AppleTalkプロトコルの設定

データ別優先制御を行うAppleTalkプロトコルとその優先度を設定します。「packet priority」が「not use」の場合に「AppleTalk protocol」を選択すると「Input error!」となり、設定を行うことはできません。最大8エントリ設定することができます。

```
*** EXP.: Set AppleTalk protocol table configuration ****
<AppleTalk protocol table (max 8 entries)>
  no entry.

  1. change  2. delete  3. add  4. end
Select the number. [4]: 3
protocol
(1:RTMP(Rp/Dt) 2:NBP 3:ATP 4:AEP 5:RTMP(Rq) 6:ZIP 7:ADSP 8:all 9:other)
[8]:
priority (1:high 2:normal 3:low) [1]:

AppleTalk protocol table data:
no protocol  priority
-----+-----
  1. *          high
Add OK (y/n)? [y]:
```

図4-88 データ優先制御AppleTalkプロトコル選択画面

- protocol

データ優先制御を行うプロトコルを選択します。複数選択はできません。

設定範囲： 1:RTMP(Rq/Dt)
2:NBP
3:ATP
4:AEP
5:RTMP(Rq)
6:ZIP
7:ADSP
8:all
9:other

導入時の設定： 8:all

- protocol number

「protocol」で「other」を選択した場合、アプリケーションの番号を設定してください。

設定範囲： 0 ~ 255

導入時の設定： 0

- priority
優先度を選択します。
設定範囲： 1:high
 2:normal
 3:low
導入時の設定： 1:high

AppleTalkプロトコルの優先度の設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。



メモ：テーブルに設定されたエントリに該当しない中継データは、すべて「通常」として扱います。このため、実際の「通常」に設定されたデータの優先制御については、「通常」に設定されたデータのエントリとテーブルに設定されたエントリ以外のデータの両方を対象とします。優先度の設定を行う場合は、テーブルに設定されていないデータのトラフィック量も考慮して設定を行ってください。

4.10.7 AppleTalkアドレスの設定

データ別優先制御を行うネットワーク番号とその優先度を設定します。設定されたアドレスは送信元、宛先に関係なく優先度が適用されます。「packet priority」が「not use」の場合に「AppleTalk address」を選択すると「Input error!」となり、設定を行うことはできません。最大8エントリ設定することができます。

```

*** EXP.: Set AppleTalk address table configuration ****
<AppleTalk address table (max 8 entries)>
  no entry.

  1. change  2. delete  3. add  4. end
Select the number. [4]: 3
network start [0]: 10
                end [10]: 12
host [*]:
priority (1:high 2:normal 3:low) [1]:

AppleTalk address table data:
  network
no  start end  host priority
---+-----+-----+-----
  1.   10  12  *   high
Add OK (y/n)? [y]:

```

図4-89 データ優先制御AppleTalkネットワーク番号設定画面

- network start
データ優先制御を行うネットワーク番号範囲の始めを設定します。
設定範囲： 0 ~ 65535
導入時の設定： 0

- end
データ優先制御を行うネットワーク番号範囲の終わりを設定します。この値はネットワーク番号範囲の始めと等しいか大きい値でなければいけません。
設定範囲： 0 ~ 65535
導入時の設定： 0

- host
データ優先制御を行うノードIDを設定します。ただし、「*」を設定するとすべてのノードIDを示します。
設定範囲： 0 ~ 255, *(すべてのノードID)
導入時の設定： *

- priority
優先度を選択します。
設定範囲： 1:high
 2:normal
 3:low
導入時の設定： 1:high

AppleTalkアドレスの優先度の設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。



メモ：テーブルに設定されたエントリに該当しない中継データは、すべて「通常」として扱います。このため、実際の「通常」に設定されたデータの優先制御については、「通常」に設定されたデータのエントリとテーブルに設定されたエントリ以外のデータの両方を対象とします。優先度の設定を行う場合は、テーブルに設定されていないデータのトラフィック量も考慮して設定を行ってください。

4.10.8 ブリッジングデータの設定

データ別優先制御を行うブリッジングデータとその優先度を設定します。「packet priority」が「not use」の場合に「bridging」を選択すると「Input error!」となり、設定を行うことはできません。最大8エントリ設定できます。

```

*** EXP.: Set bridge table configuration ****
<bridge table (max 4 entries)>
  no entry.

      1. change  2. delete  3. add  4. end
Select the number. [4]: 3
datalink(1:ethertype 2:dlsap 3:fna) [1]:
protocol [0]:
priority (1:high 2:normal 3:low) [1]:

bridge table data:
no  datalink  protocol  priority
----+-----+-----+-----
  1. ethertype 0          high
Add OK (y/n)? [y]:

```

図4-90 データ優先制御ブリッジング選択画面

- datalink
データ優先制御を行うプロトコルを選択します。複数選択はできません。
設定範囲： 1:ethertype
 2:dlsap
 3:fna
導入時の設定： なし
- protocol
「datalink」で「ethertype」または「dlsap」を選択した場合、プロトコルの番号を設定してください。
設定範囲： 0 ~ ffff (「ethertype」選択時)
 0 ~ ff (「dlsap」選択時)
導入時の設定： なし
- priority
優先度を選択します。
設定範囲： 1:high
 2:normal
 3:low
導入時の設定： 1:high

ブリッジングデータの優先度の設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。



メモ：テーブルに設定されたエントリに該当しない中継データは、すべて「通常」として扱います。このため、実際の「通常」に設定されたデータの優先制御については、「通常」に設定されたデータのエントリとテーブルに設定されたエントリ以外のデータの両方を対象とします。優先度の設定を行う場合は、テーブルに設定されていないデータのトラフィック量も考慮して設定を行ってください。

4.10.9 MACアドレスの設定

データ別優先制御を行うブリッジングデータのMACアドレスとその優先度を設定します。「packet priority」が「not use」の場合に「MAC address」を選択すると「Input error!」となり、設定を行うことはできません。最大8エントリ設定できます。

```
*** EXP.: Set MAC address table configuration ****
<MAC address table (max 8 entries)>
  no entry.

  1. change  2. delete  3. add  4. end
Select the number. [4]: 3
MAC address [00:00:00:00:00:00]:
priority (1:high 2:normal 3:low) [1]:

MAC address table data:
no MAC address      priority
----+-----+-----
  1. 00:00:00:00:00:00 high
Add OK (y/n)? [y]:
```

図4-91 データ優先制御MACアドレス設定画面

- MAC address
データ優先制御を行うMAC addressを設定します。
設定範囲： xx:xx:xx:xx:xx:xxの形式
導入時の設定： なし

- priority
優先度を選択します。
設定範囲： 1:high
 2:normal
 3:low
導入時の設定： 1:high

MACアドレスの優先度の設定は、設定メニュー画面で以下のコマンドを選択して行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- end 設定を終了します。



メモ：テーブルに設定されたエントリに該当しない中継データは、すべて「通常」として扱います。このため、実際の「通常」に設定されたデータの優先制御については、「通常」に設定されたデータのエントリのデータとテーブルに設定されたエントリ以外のデータの両方を対象とします。優先度の設定を行う場合は、テーブルに設定されていないデータのトラフィック量も考慮して設定を行ってください。



メモ：中継データが優先制御テーブル内の複数のエントリに一致する場合の、プロトコルおよびアドレステーブルの各エントリ間の優先度を、以下に示します。

IPアドレス					IPXアドレス			AppleTalk アドレス	MACアドレス	
TELNET	FTP	...	RIP	...	File Server	Print Server				
TCP			UDP		NCP		SPX			
IP					IPX			NBP ZIP AEP	EtherType	LLC

↑ 高
優先度

ルーティング
ブリッジング

図4-92 テーブルエントリ間の優先度

4.11 トラヒックロギングに関する設定

拡張設定のメニューで「traffic logging」を選択してトラヒックロギングに関する設定を行います。トラヒックロギングの対象とするエントリの送信元および宛先のIPアドレス、マスクまたはインタフェースを登録します。最大16エントリ登録できます。

```
<traffic logging table (max 16 entries)>
no. src address      mask                recv interface
    dst address      mask                dst interface
-----+-----+-----+-----
  1. 192.52.128.20    255.255.255.255    -----
     192.52.127.200  255.255.255.128    -----
-----+-----+-----+-----
  2. 192.52.128.39    255.255.255.0      -----
     . . . . .      . . . . .          LAN
-----+-----+-----+-----
  3. . . . . .        . . . . .          GroupA
     192.52.127.118  255.255.255.255    -----
-----+-----+-----+-----
  4. . . . . .        . . . . .          GroupA
     . . . . .        . . . . .          GroupB
```

図4-93 トラヒックロギングテーブル表示例

4.11.1 トラヒックロギングテーブルの設定

トラヒックロギングの対象となるエントリの設定を行います。

```
source data type (1:IP address 2:recv interface) [1]:
source IP address []: 192.52.128.20
      mask [255.255.255.255]:
destination data type (1:IP address 2:dst interface) [1]:
destination address []: 192.52.127.200
      mask [255.255.255.255]: 255.255.255.128

traffic logging table data:
no. src address      mask                recv interface
    dst address      mask                dst interface
-----+-----+-----+-----
  1. 192.52.128.20    255.255.255.255    -----
     192.52.127.200  255.255.255.128    -----
Add OK (y/n)? [y]:
```

図4-94 トラヒックロギングテーブルIPアドレス設定例

```

<Add traffic log table data>
source data type (1:IP address 2:recv interface) [1]: 2
receive interface
    1.LAN          4.BRI#5-2
    2.GroupA       5.BRI#7-1
    3.BRI#5-1     6.BRI#7-2
Select the number []: 2
destination data type (1:IP address 2:dst interface) [1]: 1
destination IP address []: 192.52.33.44
    mask [255.255.255.255]:

traffic log table data:
no  src address      mask                recv interface
   dst address      mask                dst interface
-----+-----+-----+-----
2.  ----.----.----.----  ----.----.----.----  GroupA
   192.52.33.44      255.255.255.255  -----
Add OK (y/n)? [y]:

```

図4-95 トラフィックロギングテーブルインタフェース設定例

- source data type
 トラフィックロギングの対象を接続相手の送信元アドレスにするか、受信インタフェースにするか選択します。
 設定範囲： 1: IP address
 2: recv interface
 導入時の設定： 1: IP address
- source IP address
 「source data type」で「IP address」を選択した場合に、送信元IPアドレスを設定します。
 設定範囲： 0.0.0.1 ~ 255.255.255.255
 導入時の設定： なし
- source mask
 「source data type」で「IP address」を選択した場合に、送信元マスクを設定します。
 設定範囲： 128.0.0.0 ~ 255.255.255.255
 導入時の設定： 255.255.255.255
- receive interface
 「source data type」で「recv interface」を選択した場合に、受信するインタフェースを選択します。複数の選択はできません。
 設定範囲： LAN,IPルーティングを使用するグループもしくはチャネル
 導入時の設定： なし

- destination data type
トラフィックロギングの対象を接続相手の宛先アドレスにするか、宛先インタフェースにするか選択します。
設定範囲： 1: IP address
 2: dst interface
導入時の設定： 1: IP address

- destination IP address
「destination data type」で「IP address」を選択した場合に、宛先IPアドレスを設定します。
設定範囲： 0.0.0.1 ~ 255.255.255.255
導入時の設定： なし

- destination mask
「destination data type」で「IP address」を選択した場合に、宛先マスクを設定します。
設定範囲： 128.0.0.0 ~ 255.255.255.255
導入時の設定： 255.255.255.255

- destination interface
「destination data type」で「dst interface」を選択した場合に、送信するインタフェースを選択します。複数の選択はできません。
設定範囲： LAN,IPルーティングを使用するグループもしくはチャンネル
導入時の設定： なし



メモ：中継するパケットが設定されたエントリに重複して該当する場合、すべてのエントリでロギングが行われます。

トラフィックロギングテーブルのエントリの設定は、設定メニュー画面で以下のコマンドにより行います。

- change..... エントリを変更します。
- delete エントリを削除します。
- add エントリを追加します。
- display エントリを表示します。
- end 設定を終了します。



注意：すでに登録されているエントリの再設定を行いますと、「5.6 トラフィックロギングに関するインフォメーション」において累計フレーム数、累計オクテット数が0にクリアされます。

4.12 呼確立リミッタの設定

拡張設定のメニューで「limitation of ISDN connection period」を選択して呼確立リミッタの設定を行います。

ISDN回線を接続する場合、運用、設定などのミスからISDNの呼が長時間接続されたままになる可能性があります。それを事前に防ぐために、呼確立リミッタを使用します。呼確立リミッタには、ISDNを連続して接続した時間を基にする「連続接続時間呼確立リミッタ」と接続相手毎に1ヶ月の接続累計時間を基にする「トータル接続時間呼確立リミッタ」の2種類があります。（「2.10.8 呼確立リミッタ」）

```
*** EXP.: limitation of ISDN connection period ***
 1. consecutive time
 2. monthly total time
Select the number. :
```

図4-96 呼確立リミッタの設定選択画面

4.12.1 連続接続時間呼確立リミッタの設定

図4-96で、「consecutive time」を選択することにより、連続接続時間呼確立リミッタの設定を行います。連続接続時間呼確立リミッタの設定では、使用の有無および連続接続時間の上限値を設定します。

```
<consecutive time parameter(s)>
 mode      : on
 time(hour): 12
Do you change (y/n)? [n]: y
mode (1.on 2.off) [1]:
time (hour) [12]:

EXP.: consecutive time parameter(s) are set to the following values.
<consecutive time parameter(s)>
 mode      : on
 time(hour): 12
Set OK (y/n)? [y]:
```

図4-97 連続接続時間呼確立リミッタの設定例

- mode
連続接続時間呼確立リミッタを動作させるかどうか選択します。
設定範囲： 1:on
 2:off
導入時の設定： 1:on

- time
ISDNの連続接続時間の上限値を設定します。この時間を越えて呼が接続されていると回線は切断され、その後、装置を正常に運用することはできなくなります。この項目は、「mode」を「on」にした場合のみ設定可能です。
設定範囲： 1 ~ 168[hour]
導入時の設定： 12

4.12.2 トータル接続時間呼確立リミッタの設定

図4-96で、「monthly total time」を選択することにより、トータル接続時間呼確立リミッタの設定を行います。トータル接続時間呼確立リミッタでは、呼確立時間の累計が接続相手毎に行われるので、リモートターゲット毎に設定を行います。

```
<monthly total time>

1. change 2.display 3.end
Select the number: 1
```

図4-98 トータル接続時間呼確立リミッタ設定画面例

(1) 設定を変更する場合(change)

現在設定されているエントリの変更を行う場合は、「change」を選択します。エントリの変更方法は、まず変更するエントリを番号で指定し、次にそのエントリの内容を変更する順で行います。

```
<Change manthly total time>
Select the entry number.: 1

no target mode time (hour)
---+-----+-----+-----
1. tokyo off 300
mode (1.on 2.off) [2]:1
time (hour) [300]: 744

no target mode time (hour)
---+-----+-----+-----
1. tokyo on 744
Change OK (y/n)? [y]:
```

図4-99 トータル接続時間呼確立リミッタの変更例

- mode
トータル接続時間呼確立リミッタを動作させるかどうか選択します。
設定範囲： 1:on
2:off
導入時の設定： 2:off
- time
1ヶ月間におけるISDNの呼確立時間累計の上限値を設定します。この累計時間の90%を越えて呼が接続されていると警告が行われ、100%になると呼確立リミッタが作動します。
設定範囲： 1 ~ 744[hour]
導入時の設定： 300



注意：呼確立時間は、呼をどちらから確立したか（自分が発呼したか着呼したか）やISDNの使用目的（通常回線、トラヒック分散）また、接続契機（手動による発呼や自動発呼など）に関係なく、接続している時間を相手毎に累計します。
どちらか一方が先にリミッタが作動したときにISDNの呼は解放され、もう一方のルータでは「リミッタ作動直前」で止まってしまう。この状態で、リミッタが作動した方のルータを回復させてISDNを接続した途端、今度はもう一方のルータのリミッタが作動してしまいます。このような現象を防ぐためにも、トータル接続時間呼確立リミッタの動作は、自装置を「on」にしたら相手装置は「off」にすることをおすすめします。



メモ：1ヶ月間におけるISDNの呼確立時間累計の上限値の90%を越えて呼が接続されていると、以下の警告により異常を知ることができます。

- 90%を越えた時刻と接続相手の情報が「インフォメーション」の「elog」に記録されます。
- 装置前面のCHECK LEDが点滅します。

また、リミッタが作動すると、以下の状況により異常を知ることができます。

- 100%を越えた時刻と接続相手の情報が「インフォメーション」の「elog」に記録されます。
- 装置前面のCHECK LEDが点滅します。
- 接続していた回線は切断されます。それ以降、着呼/発呼は行いません。



メモ：呼確立時間累計の上限値を変更しても、それまでの累計時間はクリアされません。累計時間をクリアするにはリミッタの再スタートを行ってください。（「5.8 呼確立リミッタのリセットコマンド」）

(2) 設定を終了する場合(end)

設定を終了する場合は、「図4-96 呼確立リミッタ設定画面例」で、「end」を選択してください。

4.13 リモートターゲットの設定

ISDNを利用して複数の相手と接続する場合に、リモートターゲットの設定を行います。

```
*** EXP.: remote target configuration menu ***
1. MAC address target
2. IP address target
3. IPX address target
4. AppleTalk network NO.target
Select the number. :
```

図4-100 リモートターゲット設定メニュー

- MAC address target
ブリッジ中継フレームによりISDN回線を自動接続する場合の、宛先MACアドレスとISDNリモートターゲットのテーブルを設定します。この設定は基本設定の「3.18.2 MACアドレスのISDNリモートターゲットの設定」と同じです。
- IP address target
IP中継パケットによりISDN回線を自動接続する場合の、宛先IPアドレスとISDNリモートターゲットのテーブルを設定します。この設定は基本設定の「3.15.2 IPのISDNリモートターゲットの設定」と同じです。
- IPX address target
IPX中継パケットによりISDN回線を自動接続する場合の、宛先IPXアドレスとISDNリモートターゲットのテーブルを設定します。この設定は基本設定の「3.16.2 IPXのISDNリモートターゲットの設定」と同じです。
- AppleTalk network NO. target
AppleTalk中継パケットによりISDN回線を自動接続する場合の、宛先AppleTalkネットワーク番号とISDNリモートターゲットのテーブルを設定します。この設定は基本設定の「3.17.2 AppleTalkのISDNリモートターゲットの設定」と同じです。

4.14 ルータグループ化機能の設定

拡張設定のメニューで「router grouping」を選択して、ルータグループ化機能に関する設定を行います。

本設定では、複数のISDN対応ルータをグループ化し論理的に1台のルータとすることにより（グループルータ）、そのルータを1つの代表電話グループに接続し、空き回線を利用して通信を行うことができます。通信を行えるのはIPルーティングです。

```

*** EXP.: Set router grouping configuration ***
  router grouping      : not use
Do you change (y/n) [n]: y
router grouping (1.use 2.not use) [2]: 1
preference [xxxxxxxx] :
UDP port number [] : 100
group IP address [] : 192.52.168.99
duplication check timer [3]:
Group name :
  1.GroupA
Select the number [1]:
RIP send count [0]: 10

EXP.: router grouping configuration is set to the following values.
  router grouping      : use
  preference            : xxxxxxxxx
  UDP port number      : 100
  group IP address     : 192.52.168.99
  duplication check timer: 3[sec]
  Group name           : GroupA
  RIP send count       : 10
Set OK (y/n) [y]:

```

図4-101 ルータグループ化機能の設定例

- RESET** - router grouping
ルータグループ化機能を使用するかどうかを選択します。
設定範囲： 1:use（使用する）
 2:not use（使用しない）
導入時の設定： 2:not use

- RESET** - preference
グループルータの個々のルータの優先度を設定します。優先度の高いルータが着呼発呼を優先的に行います。「preference」は、値が小さいほど優先度が高いことを示します。
設定範囲： 00000000 ~ ffffffff
導入時の設定： MACアドレスの下位4バイト

4章 拡張設定

- RESET** - UDP port number
UDPポート番号を設定します。
設定範囲： 1024 ~ 65535
導入時の設定： 55555

- RESET** - group IP address
グループルータの代表IPアドレスを設定します。ここでは、LAN側の代表として使用するIPアドレスを設定します。
設定範囲： 0.0.0.0 ~ 255.255.255.255 (マージャンアドレスを除く)
導入時の設定： なし

- RESET** - duplication check timer
重複確認応答パケット待ちタイマを設定します。中継データを受信した時、グループ内の他のルータがその中継データの送信先と接続しているかを確認するパケット(重複確認応答パケット)の応答待ち時間を設定します。
設定範囲： 1 ~ 100 [sec]
導入時の設定： 3

- RESET** - Group name
本装置のどのグループがルータグループに属するのかが設定します。
設定範囲： IPルーティングを使用するグループ
導入時の設定： なし

- RESET** - RIP send count
RIPパケットの連続送信数を設定します。
設定範囲： 0 ~ 127
導入時の設定： 10



メモ：ルータグループ化機能を使用する場合、グループを形成するルータのWAN側のIPアドレスは同じものを設定してください。



メモ：ルータグループ化機能を使用する場合、負荷分散機能を使用することはできません。

5章 オペレーション

この章では、装置のオペレーションについて説明します。オペレーションのコマンドを選択して、本装置の運用や保守に関する機能を実行します。

この章の内容を以下にまとめます。

- オペレーションメニュー
- 通常回線の接続 / 切断
- トラヒック分散回線の接続 / 切断
- グループ / チャネルのオンライン / オフライン
- 呼確立リミッタのリスタート
- リモートコンソール
- エコーテスト
- パスワードの変更
- 構成定義情報、エラーログの保存
- すべての設定情報の確認
- フレームトレース機能
- 障害復帰の確認
- 装置の再起動
- 保守用コマンド
- 装置の遠隔操作
- 簡易コマンド機能
- FTPを利用したメンテナンス



注意：装置のオペレーションの実行は、管理者資格(スーパーモード)で行います（「3.5 管理者資格 (スーパーモード)への移行」を参照）。

5.1 オペレーションメニュー

メインメニューの、「operation」を選択することにより以下のオペレーションメニューが表示されます。

```
*** Operation menu ***
1. connect main line
2. disconnect main line
3. connect load split line
4. disconnect load split line
5. group/channel online
6. group/channel offline
7. reset limitation of ISDN connection period
8. remote console
9. echo test
10. change password
11. save
12. dump all configurations
13. frame trace
14. put out system check LED
15. reset
Select the number. :
```

図5-1 オペレーションメニュー

オペレーションメニューからメインメニューへ移行する際は、「ESC」キーを入力します。



注意：HSD回線の使用を選択している場合は、「connect main line」から「disconnect load split line」と「reset limitation of ISDN connection period」のISDN回線関連のメニューは表示されません。

5.2 通常回線の接続

オペレーションメニューで、「connect main line」を選択した後、接続するターゲットインデックスを選択すると、ISDN通常回線を接続します。

```
*** Connect main line ***
 1.GroupA      2.GroupB      3.BRI#2-1    4.BRI#2-2
Select the number. : 1
      1.tokyo      2.osaka
Select the number of target index. : 2
Command OK.
Hit return or ESC or 'q' key:
```

図5-2 通常回線接続例



メモ：すでに接続されている回線について接続動作を行った場合"Input error!"と表示されます。

5.3 通常回線の切断

オペレーションメニューで、「disconnect main line」を選択後、切断するターゲットインデックスを選択すると、ISDN通常回線を切断します。

```
*** Disconnect main line ***
 1.Osaka      2.Tokyo
Select the number : 1
Command OK.
Hit return or ESC or 'q' key:
```

図5-3 通常回線切断例

5.4 トラヒック分散回線の接続

トラヒック分散回線を使用する形態の場合、オペレーションメニューで「connect load split line」を選択後、接続する相手を選択して、トラヒック分散回線を接続します。接続する相手には、現在通常回線が接続されている相手のターゲットインデックスが表示されます。

```
*** Connect load split line ***
 1.Osaka      2.Tokyo
Select the number : 1
Command OK.
Hit return or ESC or 'q' key:
```

図5-4 トラヒック分散回線接続例

5.5 トラヒック分散回線の切断

トラヒック分散回線を使用する形態の場合、オペレーションメニューで「disconnect load split line」を選択後、トラヒック分散を切断する相手を選択し、トラヒック分散回線を切断します。

```
*** Disconnect load split line ***
 1.Osaka      2.Tokyo
Select the number :
Command OK.
Hit return or ESC or 'q' key:
```

図5-5 トラヒック分散回線切断例



メモ：すでに切断されている回線について切断動作を行った場合"command error."と表示されます。

5.6 グループ / チャンネルのオンライン状態への遷移

オペレーションメニューで「group/channel online」を選択した後、オンライン状態にするグループ / チャンネルを選択し、グループ / チャンネルをオンライン状態にします。

```
<group/channel>

  1.GroupA      2.GroupB      3.BRI#6-1
Select the number : 1
Command OK.
Hit return or ESC or 'q' key:
```

図5-6 グループ / チャンネルのオンライン状態への遷移例

5.7 グループ / チャンネルのオフライン状態への遷移

オペレーションメニューで「group/channel offline」を選択した後、オフライン状態にするグループ / チャンネルを選択し、グループ / チャンネルをオフライン状態にします。オフライン状態に遷移すると接続されていたISDN回線は切断されます。

```
<group/channel>

  1.BRI#6-2    2.BRI#7-1    3.BRI#6-1
Select the number : 1
Command OK.
Hit return or ESC or 'q' key:
```

図5-7 グループ / チャンネルのオフライン状態への遷移例

5.8 呼確立リミッタのリスタート

オペレーションメニューで「reset limitation of ISDN connection period」を選択して、呼確立リミッタのリスタートを行います。呼確立リミッタのリスタートとは、トータル接続時間呼確立リミッタで現在のステータスが、「alerted」か「bombarded」の場合「normal」にする、これまでの累計を0にする、の2点です。呼確立リミッタを動作するかどうかの設定については、「4.12 呼確立リミッタの設定」を参照してください。

```

*** reset limitation of ISDN connection period ***
no  index  status      no  index  status
-----+-----+-----+-----+-----+-----
 1. Tokyo  bombarded  2. Osada  alerted
 3. Kyoto  normal
      .
      .
      .
-More-
Select the number. : 1

Command OK.
Hit return or ESC or 'q' key:

```

図5-8 呼確立リミッタのスタート画面

以下に表示内容を示します。

- index リモートターゲットテーブルに設定されたターゲットインデックス
- status トータル接続時間呼確立リミッタの状態
 - normal..... 正常状態（警告前）
 - alerted 警告後
 - bombarded..... 呼確立リミッタ作動後
 - not-work 呼確立リミッタ未動作

トータル接続時間呼確立リミッタをリスタートしたいターゲットの番号を選択します。リスタートすると「Command OK.」と表示されます。



メモ：本コマンド以外に、トータル接続時間呼確立リミッタは次の時にスタートします。

- 電源投入時
- 装置リセット時

また、次の時にリスタートします。

- 現在のステータスが「normal」および「alerted」で、内蔵カレンダーの現在の日付が「1日」になった時

5.9 リモートコンソール

オペレーションメニューで「remote console」を選択すると、遠隔装置のリモートコンソールになることができます。遠隔装置のリモートコンソールになるためには、パスワードの入力が必要です。

```
*** Remote console ***
Input remote IPaddress: 192.168.2.1
Connecting .... (192.168.2.1)
Password:
```

図5-9 リモートコンソール接続例

リモート装置のコンソールの操作は、ローカルコンソールの操作と同じです。リモートの設定等を終了しローカルコンソールに戻るときは、メインメニューの「exit from remote console or current mode」を選択します。



注意：対象の装置で、既にローカルのコンソール、TELNETで接続されたコンソールあるいはリモートコンソールが使用されている場合、以下の警告が表示されリモートコンソールに入れません。

```
Remote console(ipaddress 192.168.2.1) is using now!
```

図5-10 警告メッセージ例



メモ：IPルーティングを使用しない場合で本装置をIPホストとして運用しない場合、リモートコンソール機能は使用できません。

5.10 エコーテスト

オペレーションメニューで「echo test」を選択して、IP、IPXおよびAppleTalk接続を確認することができます。

```
*** Echo test menu ***
1. IP
2. IPX
3. AppleTalk
Select the number. : 1
```

図5-11 エコーテストメニュー

(1) IP

確認したいホストのIPアドレスを入力することにより、指定したホストの応答を確認することができます（UNIXのpingコマンドと類似の機能）。

```
*** Ping ***
Input target IPaddress []: 1111
*** Illegal parameter                不正なIPアドレス
Input target IPaddress []: 192.168.1.1
[1011] Network is unreachable.      到達不能
Input target IPaddress []: 192.168.2.1
[000] Ping TimeOut.                 タイムアウト
Input target IPaddress [192.168.1.1]: 192.168.3.1
[000] Ping Stop.                    「コントロール」キーと「c」キーを同時入力
Input target IPaddress [192.168.2.1]: 192.168.4.1
64 bytes from 192.168.3.1: icmp_seq=0.

---- PING Statistics ----
1 packets transmitted, 1 packets received.   エコーテストの応答の受信を示す
Input target IPaddress [192.168.3.1]:
```

図5-12 IPエコーテスト例

- 不正なIPアドレス(xxx.xxx.xxx.xxxの形式以外のアドレス)を入力した場合、「Illegal parameter」と表示され、コマンドライン(「Input target IPaddress []:」)に戻ります。また、到達不能なネットワークを入力した場合、「Network is unreachable.」と表示され、コマンドラインに戻ります。
- ホストの応答が20秒間ない場合、「Ping TimeOut」と表示され、コマンドラインに戻ります(リトライは行われません)。
- ホストの応答がない状態で「コントロール」キーと「c」キーを同時に押すと、エコーテストを中断できます。この場合コンソールには「Ping Stop」と表示されます。
- エコーテストの画面からオペレーションのメニュー画面にもどるには、「ESC」キーを入力します。

(2) IPX

確認したいIPXルータ、サーバおよびクライアントのネットワーク番号とノードIDを入力することにより、その相手の応答を確認することができます。

```

*** Echo test menu ***
  1. IP
  2. IPX
  3. AppleTalk
Select the number. : 2
*** IPX echo test ***
IPX network number []: xxx
   node ID []: 1
*** Illegal parameter
IPX network number []: 100
   node ID []: 1
[1011] Network is unreachable.
IPX network number []: 120
   node ID []: 1
[000] Echo TimeOut.
IPX network number [120]:50
   node ID [1]:
[000] Echo test Stop
IPX network number [50]:60
   node ID [1]:
network-number=60 node-ID=1 Alive
IPX network number [60]:

```

不正なネットワーク番号

到達不能

タイムアウト

「コントロール」キーと「c」キーを同時入力

図5-13 IPXエコーテスト例

- 不正なネットワーク番号を入力した場合、「Illegal parameter」と表示され、コマンドライン（IPX network number []）に戻ります。また、到達不能なネットワークを入力した場合、「Network is unreachable.」と表示され、コマンドラインに戻ります。
- 相手の応答が20秒間ない場合、「Echo TimeOut.」と表示され、コマンドラインに戻りません（リトライは行われません）。
- 相手の応答がない状態で「コントロール」キーと「c」キーを同時に押すと、エコーテストを中断できます。この場合コンソールには「Echo test Stop」と表示されます。
- エコーテストの画面からオペレーションのメニュー画面に戻るには、「ESC」キーを入力します。

(3) AppleTalk

確認したいノードのネットワーク番号を入力することにより、指定したノードにAEPエコーリクエストのデータを送信することができます。

```
*** AppleTalk echo test ***
AppleTalk network number []: abc
      node ID []: 1
*** Illegal parameter
AppleTalk network number []: 100
      node ID []: 1
[1011] Network is unreachable.
AppleTalk network number []: 120
      node ID []: 1
[000] Echo TimeOut.
AppleTalk network number [120]:50
      node ID [1]:
[000] Echo test Stop
AppleTalk network number [50]:60
      node ID [1]:
network-number=60 node-ID=1 Alive
AppleTalk network number [60]:
```

不正なネットワーク番号

到達不能

タイムアウト

「コントロール」キーと「c」キーを同時入力

図5-14 AppleTalkエコーテスト例

- 不正なAppleTalkネットワーク番号を入力した場合、「Illegal parameter」と表示され、コマンドライン（AppleTalk network number []）に戻ります。また、到達不能なネットワークを入力した場合、「Network is unreachable.」と表示され、コマンドラインに戻ります。
- ノードの応答が20秒間ない場合、「Echo TimeOut.」と表示され、コマンドラインに戻ります（リトライは行われません）。
- ノードの応答がない状態で「コントロール」キーと「c」キーを同時に押すと、エコーテストを中断できます。この場合コンソールには「Echo test Stop」と表示されます。
- エコーテストの画面からオペレーションのメニュー画面に戻るには、「ESC」キーを入力します。

5.11 パスワードの変更

オペレーションメニューで「change password」を選択すると、装置のパスワードを設定できます。管理者資格になるためのパスワードと、TELNETおよびremote consoleによるログインを許可するパスワードの設定および変更を、それぞれ独立して実行できます。



メモ：パスワードは8文字以内の英数字で入力します。

```

*** Change password ***
Change password (1:super user 2:telnet/remote console) [1]:
New password:                新しいパスワードの入力
Retype new password:         再度新しいパスワードの入力
New password is accepted.
Hit return or ESC or 'q' key:

```

図5-15 パスワード設定例

5.12 構成定義情報，ログ情報の保存

オペレーションメニューで「save」を選択すると、現在運用している構成定義情報またはログ情報をフロッピーディスクに保存できます。「save」の操作を行う前に、フロッピーディスクを装置前面フタ内部のフロッピーディスクユニットに差し込みます。フロッピーディスクがフロッピーディスクユニットに差し込まれていない状態で「save」の操作を行うと、「Command error」と表示されて「save」の操作が実行されません。



メモ：フロッピーディスクは1.2Mフォーマットの3.5インチ2HDを使用してください。また、すでに使用していたフロッピーディスクで構成定義情報やログ情報の保存を行うと、あらかじめフロッピーディスクが持っていた情報はすべて消去されてしまいます。

```

*** Save ***
Select Save (1.configurations 2.log) [1]: 1
command OK.
Hit return or ESC or 'q' key:

```

図5-16 構成定義情報保存例

- configuration
構成定義情報をフロッピーディスクにセーブします。このフロッピーディスクを利用して構成定義の読み込みが可能です。（「5.16 装置の再起動」）
- log
装置のエラーログ，ラインログ，トラップログをフロッピーディスクにセーブします。

5.14 フレームトレース機能

フレームトレース機能では、以下に示す種類のフレームをトレースすることができます。

- MACフレーム
- IPルーティングのフレーム（IPルーティング機能使用時）
- IPXルーティングのフレーム（IPXルーティング機能使用時）
- AppleTalkルーティングのフレーム（AppleTalkルーティング機能使用時）
- ISDN Dチャンネルのフレーム

フレームトレース機能は、1フレームあたり最大96バイトで、256フレームまでトレースすることができます。また、フレームトレース機能は、フレームトレース種類の設定、開始/終了、トレースデータの表示および消去ができます。

5.14.1 フレームトレース機能の操作

フレームトレース機能を実行するときは、オペレーションメニューで「frame trace」を選択します。フレームトレースメニュー画面を図5-18に示します。

```
*** Frame trace ***
1. start
2. display
3. configuration
4. clear
Select the number
```

図5-18 フレームトレースメニュー画面

5.14.2 フレームトレース機能の種類の設定

フレームトレース機能の種類を設定するときは、フレームトレースメニュー画面で「configuration」を選択します。

```
*** Frame trace configuration ***
<Frame trace current mode>
  trace :off
  trace frame type :MAC
Select the trace frame type (1.MAC 2.IP 3.IPX 4.Apple 5.ISDN Dch *.all) []:
```

図5-19 フレームトレースの種類の設定画面

- trace
現在，フレームトレース機能が動作しているかどうかを表示します。「on」の時は動作状態，「off」の時は停止を示します。

- trace protocol
現在トレースが指定されているフレームの種類を表示します。フレーム種類は以下の3通りから設定できます。
 - MAC..... MACフレーム
 - IP IPフレーム
 - IPX..... IPXフレーム
 - APPLE..... AppleTalkフレーム
 - ISDN Dch..... ISDNのDチャンネルのフレーム

- Select the trace frame type
トレースするフレーム種類を指定します。トレースするフレームの種類は複数指定できます。
 - 1.MAC..... MACフレーム
 - 2.IP IPフレーム
 - 3.IPX..... IPXフレーム
 - 4.APPLE..... AppleTalkフレーム
 - 5.ISDN Dch.. ISDNのDチャンネルのフレーム
 - *.all MAC , IP , IPX , AppleTalk , ISDN Dチャンネルフレーム

(1) MACフレームのトレースの設定

MACフレームのトレースの設定例を示します。MACフレームのトレースでは、トレースモード（表5-1を参照）、MACアドレス（宛先/送信元）およびインタフェースにより、トレースするMACフレームを限定することができます。

```
*** Frame trace configuration ***
<Frame trace current mode>
  trace off
  trace frame type :MAC
Select the trace protocol (1.MAC 2.IP 3.IPX 4.Apple 5.ISDN Dch*.all) []: 1

<MAC>
  mode :local
  local address      remote address      remote interface
-----+-----+-----+-----
      00:00:00:00:00:00  00:00:00:00:00:00
Do you change (y/n)? [n]: y
mode (1.remote 2.local 3.broadcast 4.any) [4]:
local address [00:00:00:00:00:00]:
remote address [00:00:00:00:00:00]:
remote interface
  1.LAN
  2.BRI#1-1      3.BRI#1-2
Select the number. :
```

図5-20 MACフレームのトレース設定例

- mode
トレースするモードを指定します。本設定は複数設定可能です(表5-1を参照)。

表5-1 トレースするフレームの種類

mode	トレースするフレームの種類
1	WAN側のノード(remote addressで指定)宛に送信するフレーム, およびそのノードから受信したフレームをトレースします.
2	LAN側のノード(local addressで指定)宛に送信するフレーム, およびそのノードから受信したフレームをトレースします.
3	ブロードキャストのフレームをトレースします.
1, 2	WAN側のノード(remote addressで指定)からLAN側のノード(local addressで指定)宛に送信するフレーム, およびLAN側のノードからWAN側のノード宛に送信するフレームをトレースします.
1, 2, 3	WAN側のノード(remote addressで指定)からLAN側のノード(local addressで指定)宛に送信するフレーム, LAN側のノードからWAN側のノード宛に送信するフレーム, およびブロードキャストのフレームをトレースします.
1, 3	WAN側のノード(remote addressで指定)宛に送信するフレーム, そのノードから受信したフレーム, およびブロードキャストのフレームをトレースします.
2, 3	LAN側のノード(local addressで指定)宛に送信するフレーム, そのノードから受信したフレーム, およびブロードキャストのフレームをトレースします.
4	ブロードキャストを除く全てのフレームをトレースします.

- local address
モードを「local」に選択する場合に, トレース対象とするLAN側のノードのMACアドレスを指定します.
- remote address
モードを「remote」に選択する場合に, トレース対象とするWAN側のノードのMACアドレスを指定します.
- remote interface
トレースするインタフェースを指定します. インタフェースは複数設定可能です. インタフェースを複数選択するときは, 「, 」で区切って同時に選択します.

(2) IPフレームのトレースの設定

IPフレームのトレースの設定例を示します。IPフレームのトレースでは、プロトコル種別（TCP, UDP, ICMP等）、IPアドレス（宛先/送信元）およびTCP/UDPのポート番号によりトレースするIPフレームを限定することができます。トレースするIPフレームの設定方法は、「3.15.5 IPパケットフィルタリングの設定」と同じです。

（ 「3.2.12 ワークシート「IPパケットフィルタフィルタリング編」」 ）

```

<IP>
  src address      : *                mask          : *
  dst address      : *                mask          : *
  A<=s port<=B    : 0,0              A<=d port<=B : 0,0
  protocol         : 0
  recv interface:
Do you change (y/n)? [n]: y
protocol (1:tcp 2:udp 3:tcp+udp 4:all 5:other) [5]:
protocol number [0]:
source address [*]:
destination address [*]:
receive interface :
  1.LAN
  2.BRI#1-1      3.BRI#1-2      4.BRI#2-1      5.BRI#2-2
  6.BRI#3-1      7.BRI#7-1      8.BRI#7-2      9.BRI#8-1
 10.BRI#8-2
Select the number. :

```

図5-21 IPフレームのトレース設定例

(3) IPXフレームのトレースの設定

IPXフレームのトレースの設定例を示します。IPXフレームのトレースでは、プロトコル種別（NCP, SPX, 等）、IPXアドレス（宛先 / 送信元）およびsocket番号によりトレースするIPXフレームを限定することができます。トレースするIPXフレームの設定方法は、「3.16.3 IPXパケットフィルタリングの設定」と同じです。（「3.2.15 ワークシート「IPXパケットフィルタフィルタリング編」」）

```
*** Frame trace configuration ***
<Frame trace current mode>
  trace off
  trace frame type :MAC
Select the trace frame type (1.MAC 2.IP 3.IPX 4.APPLE 5.ISDN Dch*.all)
[1]:3

<IPX>
  src host      : *          net      : *          mask: *
  dst host      : *          net      : *          mask: *
  A=<src sock<=B: 0000,ffff   A=<dst sock<=B: 0000,ffff
  protocol      : *
  recv interface: LAN,GroupA,GroupB,BRI#6-2,BRI#7-2
Do you change (y/n)? [n]: y
protocol (1:ncp 2:spx 3:netbios 4:unknown 5:all 6:other) [5]:
source host number [*]:
  network number [*]:
  A=<sock<=B A [0000]:
  B [ffff]:
destination host number [*]:
  network number [*]:
  A=<sock<=B A [0000]:
  B [ffff]:
receive interface :
  1.LAN
  2.GroupA   3.GroupB   4.BRI#6-2   5.BRI#7-2
select the number :
```

図5-22 IPXフレームのトレース設定例

(4) AppleTalkフレームのトレースの設定

AppleTalk フレームのトレースの設定例を示します。AppleTalk フレームのトレースでは、プロトコル種別 (RTMP, NBP, ATP, ZIP等) およびAppleTalk アドレス (宛先/送信元) によりトレースするAppleTalk フレームを限定することができます。トレースするAppleTalk フレームの設定方法は、「3.17.4 AppleTalk DDP(forward)フィルタリングの設定」と同じです。

(「3.2.21 ワークシート「AppleTalk DDP(forward)フィルタリング編」」)

```

*** Frame trace configuration ***
<Frame trace current mode>
  trace off
  trace frame type :APPLE
Select the trace frame type (1.MAC 2.IP 3.IPX 4.Apple 5.ISDN Dch *.all)
[1]: 4

<APPLE>
  1. dst network start,end: 1,2          host: 1
     dst network start,end: 1,2          host: 2
     DDP type : RTMP
     recv interface:
Do you change (y/n)? [n]: y
dst network start [0]: 1
     end [65535]: 2
     node [0]: 1
src network start [0]: 1
     end [65535]: 2
     node [0]: 2
DDP type (1:RTMP(Rp/Dt) 2:NBP 3:ATP 4:AEP 5:RTMP(Rq) 6:ZIP 7:ADSP 8:all)
[8]: 1
receive port:
  1.LAN(AppleTalk)      2.LAN(IP tunnel)
  3.GroupA              4.GroupB          5.BRI#7-1          6.BRI#7-2
Select the number :
```

図5-23 AppleTalk フレームのトレース設定例

(5) ISDN Dチャンネルフレームのトレースの設定

「ISDN Dch」を選択することにより、ISDN Dチャンネルのフレームをトレースすることができます。

```
*** Frame trace configuration ***
<Frame trace current mode>
  trace off
  trace frame type :APPLE
Select the trace frame type (1.MAC 2.IP 3.IPX 4.Apple 5.ISDN Dch *.all)
[3]: 5

<ISDN Dch>
trace line: BRI#1,BRI#2,BRI#3,BRI#4,BRI#5,BRI#6,BRI#7,BRI#8

Do you change (y/n)? [n]: y
  1.BRI#1      2.BRI#2      3.BRI#3      4.BRI#4
  5.BRI#5      6.BRI#6      7.BRI#7      8.BRI#8
Select the trace line : 1,2,3

<ISDN Dch>
trace line: BRI#1,BRI#2,BRI#3
Change OK (y/n)? [y]:
```

図5-24 Dチャンネルのトレース設定例

5.14.3 フレームトレースの開始/終了

フレームトレースを開始するときは、フレームトレースメニュー画面で「start」を選択します。フレームトレースが開始されると、フレームトレースメニュー画面で「start」が「stop」に変わります。フレームトレースを終了させるときは、「stop」を選択します。

```
*** Frame trace ***
1. start
2. display
3. configuration
4. clear
Select the number. : 1                                フレームトレース開始

*** Frame trace ***
1. stop
2. display
3. configuration
4. clear
Select the number. : 1                                フレームトレース終了
```

図5-25 フレームトレースの開始/終了

5.14.4 トレース結果の表示

フレームトレース結果を表示するときは、フレームトレースメニュー画面で「display」を選択します。フレームトレースの表示例を図5-26に示します。

```
*** Frame trace ***
1. start
2. display
3. configuration
4. clear
Select the number. : 2

*** Frame trace display ***
Select the trace frame type (1.MAC 2.IP 3.IPX 4.Apple 5.ISDN Dch*.all)
[*]:
  0 050c4ef1:00001620 data=0x00ba1d38(90) type=mcb+mbuf
    id   =(00800000) ,ip,,,,
    subid=(08008000) ip,recv,
      00 ba 1d 38 00 ba 1d 38 00 bf 37 00 20 00 00 00 ...8...8..7....
      00 04 80 00 05 0c 4e ef 00 00 00 00 00 80 00 00.....N.....
      40 00 00 00 00 00 00 32 45 00 00 29 05 77 00 00@.....2E..).w..
      3b 06 7b 90 9e ca e0 26 9e ca e1 0c 0d 81 00 17 ;.{.....
      47 21 42 3a 3b 27 1a 77 50 10 10 7d a9 fc 00 00G!B:;' .wP..}....
      0a 00 00 00 00 00 8f 28 0b 30 34 ec 00 00 02 04.....(.04.....
  1 050c4ef6:0000046e data=0x00ba16d0(90) type=mcb+mbuf
```

図5-26 フレームトレース結果の表示例

5.14.5 トレース結果の消去

フレームトレース結果を消去するときは、フレームトレースメニュー画面で「clear」を選択します。

```
*** Frame trace ***
1. start
2. display
3. configuration
4. clear
Select the number. : 4
```

図5-27 フレームトレース結果の消去

5.14.6 トレースデータの解析

フレームトレースしたデータの解析方法について説明します。

```

_0 03991326:00000fcc data=0x00b9eb88(96) type=mcb+mbuf
(a)   (b)       (c)           (d)           (e)
      id   =(80000000) lan,,,,,
              (f)
subid=(8000 8000) land,recv,
      (g) (h)
00 b9 eb 88 00 b9 eb 88 00 be e8 00 80 00 00 00 .....
              (i)           (j)           (k)
00 04 80 00 03 99 13 26 00 00 00 00 80 00 00 00 .....%.....
              (l)           (m)
40 00 00 00 00 00 00 40 80 00 00 01 ff ff ff ff @.....@.....
              (n)           (o)           (p)
ff ff 08 00 20 0b a6 24 08 06 00 01 08 00 06 04 ..$......
              (p)
00 01 08 00 20 0b a6 24 9e ca e1 02 00 00 00 00 ..$......
              (p)
00 00 9e ca e1 01 3e 02 25 e2 3e 02 25 e3 38 01 ..>.%.>.%.>.%.>.
              (p)

```

図5-28 フレームトレース結果の解析例

図5-28の例を元にしてトレースデータの解析方法を説明します。下線で示した部分はトレースしたデータの属性を表し、以下の様な内容を示します。表示は、(a)のみ10進数で、(b)~(p)は16進数です。

- (a)
トレースデータ番号を示します。
- (b)
データをトレースした時のタイムスタンプを16進数で示します。これは装置を起動してからの時間で、単位は10msecです。例の値を10進数で表すと、以下のようになります。
3991326[10msec] (16進数) = 60363558[10msec] (10進数) = 603635.58[sec] (10進数)
- (c), (d), (e)
内部情報を示します。

- (f)

トレースの種類を示します。

0x00000001.....	IPトレース
0x00000002.....	IPXトレース
0x00000004.....	AppleTalkトレース
0x00000040.....	ISDN Dchトレース
0x00008000.....	line#16回線から受信したMACトレース
0x00010000.....	line#15回線から受信したMACトレース
0x00020000.....	line#14回線から受信したMACトレース
0x00040000.....	line#13回線から受信したMACトレース
0x00080000.....	line#12回線から受信したMACトレース
0x00100000.....	line#11回線から受信したMACトレース
0x00200000.....	line#10回線から受信したMACトレース
0x00400000.....	line#9回線から受信したMACトレース
0x00800000.....	line#8回線から受信したMACトレース
0x01000000.....	line#7回線から受信したMACトレース
0x02000000.....	line#6回線から受信したMACトレース
0x04000000.....	line#5回線から受信したMACトレース
0x08000000.....	line#4回線から受信したMACトレース
0x10000000.....	line#3回線から受信したMACトレース
0x20000000.....	line#2回線から受信したMACトレース
0x40000000.....	line#1回線から受信したMACトレース
0x80000000.....	LAN回線から受信したMACトレース

- (g)

トレースした場所(ファームウェア)を示します。

0x8000.....	LANドライバ
0x4000.....	WANドライバ
0x2000.....	WAN制御部
0x1000.....	ブリッジ制御部
0x0800.....	IP制御部
0x0400.....	IPX制御部
0x0100.....	AppleTalk制御部

- (h)

トレースしたフレームの処理情報を示します。

0x8000.....	受信したデータ
0x4000.....	送信したデータ
0x0800.....	フィルタリングしたデータ
0x0400.....	タイムアウトしたデータ
0x0200.....	廃棄したデータ
0x0210.....	リソースが原因で廃棄したデータ
0x0220.....	回線が原因で廃棄したデータ
0x0230.....	I/Fが原因で廃棄したデータ

0x0240..... mbufが原因で廃棄したデータ
 0x0250..... mcbが原因で廃棄したデータ
 0x0260..... プロトコルが原因で廃棄したデータ

- (i), (j)
内部情報を示します。
- (k)
どの回線のフレームであるかを示します。フレームにより2種類の意味を持ちます。

0xWWWWWWWWW

WWWWWWWWW:回線の種類

8000000..... LAN
 4000000..... line#1
 2000000..... line#2
 1000000..... line#3
 0800000..... line#4
 0400000..... line#5
 0200000..... line#6
 0100000..... line#7
 0080000..... line#8
 0040000..... line#9
 0020000..... line#10
 0010000..... line#11
 0008000..... line#12
 0004000..... line#13
 0002000..... line#14
 0001000..... line#15
 0000800..... line#16

0x00XXYYZZ (LANの送信, WANの送受信の場合)

XX:デバイスサブクラス

00 ISDN#1 (HSD#1)
 }

0f..... ISDN#16 (HSD#16)

YY:デバイスクラス

00 Ethernet
 10 SD (高速デジタル回線)
 20 ISDN回線

ZZ:プリミティブID

80 受信データ
 03 送信データ

- (l)
ドライバがデータを受信した時のタイムスタンプです。これは装置を起動してからの時間で、単位は10msecです。

- (m)
フレームのタイプ、各種コントロール情報を示します。複数組み合わせることにより、さまざまな状態を示します。
 - 0x00000001..... IPデータ・トレースが必要なフレーム
 - 0x00000002..... IPXデータ・トレースが必要なフレーム
 - 0x00000004..... AppleTalkデータ・トレースが必要なフレーム
 - 0x00000040..... ISDN Dchデータ・トレースが必要なフレーム

 - 0x00008000..... MACデータ (line#16) ・トレースが必要なフレーム
 - 0x00010000..... MACデータ (line#15) ・トレースが必要なフレーム
 - 0x00020000..... MACデータ (line#14) ・トレースが必要なフレーム
 - 0x00040000..... MACデータ (line#13) ・トレースが必要なフレーム
 - 0x00080000..... MACデータ (line#12) ・トレースが必要なフレーム
 - 0x00100000..... MACデータ (line#11) ・トレースが必要なフレーム
 - 0x00200000..... MACデータ (line#10) ・トレースが必要なフレーム
 - 0x00400000..... MACデータ (line#9) ・トレースが必要なフレーム
 - 0x00800000..... MACデータ (line#8) ・トレースが必要なフレーム
 - 0x01000000..... MACデータ (line#7) ・トレースが必要なフレーム
 - 0x02000000..... MACデータ (line#6) ・トレースが必要なフレーム
 - 0x04000000..... MACデータ (line#5) ・トレースが必要なフレーム
 - 0x08000000..... MACデータ (line#4) ・トレースが必要なフレーム
 - 0x10000000..... MACデータ (line#3) ・トレースが必要なフレーム
 - 0x20000000..... MACデータ (line#2) ・トレースが必要なフレーム
 - 0x40000000..... MACデータ (line#1) ・トレースが必要なフレーム
 - 0x80000000..... MACデータ (LAN) ・トレースが必要なフレーム

- (n)
ドライバでの制御情報を示します。
 - 0x80KKLLLL 遅延タイムアウトによるフレームの廃棄禁止
 - 0x40KKLLLL FCS有りのフレーム

 - KK: データ別優先制御機能の優先順位
 - 00: 優先 (high)
 - 01: 通常 (normal)
 - 02: 非優先 (low)
 - LLLL: 無意味な数値

- (o)
フレームの総バイト数を示します。

- (p)
トレースしたフレームの最初の56バイト分のデータを示します。



メモ：ISDN Dチャネルのトレースでは、(i)の部分からデータが入ります。(i),(j),(k),(l),(m),(n),(o)のような制御データはありません。

5.15 障害復帰の確認

装置や回線上で障害が発生した場合、フロントパネルのCHECK LEDが点滅します。

CHECK LEDは、オペレーションメニューの「put out system check LED」を実行して、強制的に消灯することができます。このコマンドを実行後、LEDの点滅がなくなったら障害はなくなったと考えられます。

```
*** Put out system check LED ***
Execute OK (y/n)? [y]:
Hit return or ESC or 'q' key:
```

図5-29 障害復帰の確認例

5.16 装置の再起動

オペレーションメニューで「reset」を選択すると、装置を再起動できます。

```
*** Reset ***
1:normal restart          2:loading restart
3:all default restart    4:limited default restart
Reset mode : 1
Do you want to continue(y/n)?[y]:
```

図5-30 装置リセット例

- normal restart
通常のリセット動作を行います。
- loading restart
フロッピーディスクに保存された構成定義情報を読み込んで、リセット動作を行います。



- 注意：-
- フロッピーディスクが挿入されていない場合や、構成定義情報が保存されていないフロッピーディスクが挿入されている場合は、通常のリセット動作を行います。
 - 本装置の構成的情報が保存されており、かつ、書き込み禁止（ライトプロテクトがかかっている）フロッピーディスクが挿入されている場合は、選択したメニューによらず「loading restart」を実行します。

5章 オペレーション

- 「loading restart」を行う場合以外は、フロッピーディスクを挿入した状態でリセット動作を行わないでください。



警告：他機種リモートブロータ装置の構成定義情報が保存されたフロッピーディスクを挿入した状態で「loading restart」を行わないでください。

- all default restart

パスワードを除いたすべての設定を、装置導入時の設定(デフォルト設定)に戻しリセット動作を行います。このコマンドは、機能の選択や各テーブルの登録などをすべて初めからやり直す際に使用します。

- limited default restart

表5-2に示す設定を、装置導入時の設定(デフォルト設定)に戻しリセット動作を行います。このコマンドは、表5-2に示す項目をデフォルト設定に戻し、各テーブルに登録した値はデフォルト設定に戻さずにリセット動作を行います。

表5-2 選択デフォルト再設定項目

設定項目	参照項
運用形態の選択	3.9
HSDの設定	3.12.1
ISDNチャンネルグループの設定	3.12.2
ISDN運用形態の設定	3.12.3
ISDNリモートターゲットの設定	3.12.4
ISDN通常回線の設定	3.12.5
機能の選択	3.13
IPホスト / IPアドレスの設定	3.14
IPルーティングの設定	3.15.1
IPXルーティングの設定	3.16.1
AppleTalkルーティングの設定	3.17.1
ブリッジング機能の設定	3.18.2
SNMPパラメータの設定	3.19.1
データリンクに関する設定	4.2
アドレス学習テーブルのエージアウト時間	4.3.2
ICMPリダイレクト	4.4
RIP(IP)に関する拡張設定	4.5.1
RIP(IP)インタフェースの設定	4.5.2
ProxyARPの設定	4.5.7
RIP(IPX)インタフェースの設定	4.6.1
SAP(IPX)インタフェースの設定	4.6.4
KeepAliveパケットの代理応答 / 要求の設定	4.6.13
データ別優先制御のパラメータの設定	4.10.1
データ圧縮の設定	4.2

5.17 保守用コマンド

管理者資格(スーパーモード)のメインメニューで実行できる保守用コマンドと、その使用方法について説明します。保守用コマンドで行う機能は、以下の3種類です。

- lnktest 回線接続診断試験の操作
- scanout スキャンアウト機能の設定
- filemnt ファームウェアの交換の操作

コマンドの入力方法は、以下の形式で表します。

コマンド形式：command(abbrev)[arg1,arg2・・・]

- command 入力するコマンドを示します。
- abbrev 短縮形を示します。
- arg..... 引数を示します。なお引数の数はコマンドにより異なり、省略可能な場合があります。



メモ：コマンドの入力は大文字と小文字の両方で可能です。またコマンドと引数の間、および引数と引数の間はスペースで区切ります。

【例】

コマンド形式：ppp(p) [HSD#1]

- ppp コマンド名
- (p) 短縮形
- [HSD#1] 引数

5.17.1 回線接続診断試験 (lnktest)

回線接続診断試験を実行する場合には、管理者資格(スーパーモード)のメインメニューで以下のコマンドを入力してリンクテストモードへ移行します。

コマンド形式：lnktest(l)

リンクテストモードへの移行画面を以下に示します。

```
Select the number.:lnktest
Super:lnktest>
```

図5-31 リンクテストモード移行例

リンクテストモードでは、PPPの接続およびLLC-type1の接続に関する接続診断試験を行うことができます。リンクテストモードで使用できるコマンドは以下のとおりです。

- ppp PPPの接続診断試験を実行
- llc LLC-type1の接続診断試験を実行
- ? 使用できるコマンドまたはコマンド形式を表示
- exit リンクテストモードの終了

(1) PPPの接続診断試験 (ppp)

WAN回線を経由してPPP接続する場合、PPPの接続診断試験を行います。

コマンド形式 : ppp(p) [type] [count]

[type] : 接続診断試験を行うグループ/チャンネル名を指定します。
設定例 : GroupA, BRI#1-1, HSD#1等

[count] : フレームの送信回数を指定します。
設定範囲 : 1 ~ 255 (省略時は10が設定される)

PPPの接続診断試験の画面を以下に示します。

```
Super:lnktest>ppp HSD#1
[001] PPP Lnktest OK.
[002] PPP Lnktest OK.
[003] PPP Lnktest OK.
.
.
[010] PPP Lnktest OK.
PPP Lnktest Total count : 010
Normal count : 010
Error count : 000
TimeOut count : 000
```

図5-32 PPP接続診断試験例

- Total count..... 接続診断試験を行った回数
- Normal count..... 正常にフレーム送受信した回数
- Error count..... レングス異常の受信回数
- TimeOut count..... タイムアウトの回数

PPPの接続診断試験でエラーまたはタイムアウトが発生した場合、回線による障害が考えられます。回線の接続を確認してください。

(2) LLC-type1の接続診断試験

WAN回線を経由してLLC接続する場合，LLC-type1による接続診断試験を行います．

コマンド形式：llc(l) [type][DstMACAddress][count]

[type] : 接続診断試験を行うグループ/チャンネル名を指定します．
設定例： GroupA, BRI#1-1, HSD#1等

[DstMACAddress] : 接続診断試験を行う相手装置の物理アドレスを設定します．
設定範囲： xx:xx:xx:xx:xx:xxの形式

[count] : フレームの送信回数を指定します．
設定範囲： 1～255（省略時は10が設定される）

LLC-type1の接続診断試験の画面を以下に示します．

```
Mainte:lnktest>llc HSD#1 xx:xx:xx:xx:xx:xx
[001] LLC Lnktest OK.
[002] LLC Lnktest OK.
[003] LLC Lnktest OK.
.
.
[010] LLC Lnktest OK.
LLC Lnktest Total count : 010
Normal count : 010
Error count : 000
TimeOut count : 000
```

図5-33 LLC-type1接続診断試験例

- Total count..... 接続診断試験を行った回数
- Normal count..... 正常にフレーム送受信した回数
- Error count..... レングス異常の受信回数
- TimeOut count..... タイムアウトの回数

LLC-type1の接続診断試験でタイムアウトまたはエラーが発生した場合，相手装置のMACアドレスが正しいことを確認してください．相手装置のMACアドレスが正しい場合，回線による障害が考えられます．回線の接続を確認してください．

(3) ヘルプ情報の表示 (?)

リンクテストモードで使用できるコマンドを表示します。また、引数にコマンド名を指定するとそのコマンドの使用形式を表示します。

コマンド形式 : ? [command] あるいは [command]?

ヘルプ情報の表示画面を以下に示します。

```
Super:lnktest> ?  
  (?), exit(e), ppp(p), llc(l)           使用できるコマンドの表示  
Super:lnktest> ? exit                    使用形式の表示  
usage: exit(e)  
Super:lnktest> ppp ?                    使用形式の表示  
usage: ppp(p) <type> [<count>]
```

図5-34 リンクテストのヘルプ情報

(4) リンクテストモードの終了

リンクテストモードを終了し、メインメニューに戻ります。

コマンド形式 : exit(e)

5.17.2 スキャンアウト

スキャンアウトは、装置のメモリ情報をフロッピーディスクに書き込む機能です。実行されると、フロッピーディスクにメモリ情報を書き込みます。フロッピーディスクは約2~4枚必要です（状況によっては最大17枚必要となります）。スキャンアウトの設定は電源のOFF/ON(ケーブルの抜き差し)で解除されます。

(1) スキャンアウトの設定状態の確認

スキャンアウトの設定状況の表示を行います。

コマンド形式：scanout(s)

スキャンアウトの設定状況の表示画面を以下に示します。

```
Select the number.:scanout
Scanout ON
```

図5-35 スキャンアウトON時の設定状況画面

```
Select the number.:scanout
Scanout OFF
```

図5-36 スキャンアウトOFF時の設定状況画面

(2) スキャンアウトの設定

引数として"on"を指定すると、次回装置リセット時にスキャンアウトを実行します。

コマンド形式：scanout(s) [on]

```
Select the number.:scanout on
Command OK.
```

図5-37 スキャンアウトONの設定

5.17.3 ファイルメンテナンスモード (filemnt)

ファイルメンテナンスモードへ移行するには、管理者資格(スーパーモード)のメインメニューで以下のコマンドを入力します。ファイルメンテナンスモードでは、格納されているファームウェアの格納状況の表示やファームウェアのダウンロードの実行ができます。



注意：本コマンドは、TELNETコンソールおよびリモートコンソールでは使用できません。

コマンド形式：filemnt(f) [IPAddr]

- 自装置でファイルメンテナンスモードへ移行する場合

```
Select the number.: filemnt
filemnt>
```

図5-38 ファイルメンテナンスモードへの移行(自装置の場合)

- 遠隔装置のファイルメンテナンスモードへ移行する場合
ファームウェアの交換を行う装置のIPアドレスを指定します。

```
Select the number.: filemnt 192.168.1.1 IPアドレスを指定
remote[192.168.1.1] filemnt> 遠隔装置のファイルメンテナンスモードへ移行
```

図5-39 ファイルメンテナンスモードへの移行(遠隔装置の場合)

ファイルメンテナンスモードで使用できるコマンドは以下のとおりです。

filestat	格納されているファームウェアの格納状況の表示
putsys.....	ファームウェアのダウンロードの実行
chgsys	アクティブなフラッシュメモリの変更(本装置では未使用)
startsys.....	ダウンロードしたファームウェアの起動
?	使用できるコマンドまたはコマンドの使用形式の表示
exit	ファイルメンテナンスモードの終了

(1) ファームウェアの格納状況の表示 (filestat)

本装置に格納されているファームウェアのバージョン等を表示します。

コマンド形式 : filestat(f)

格納状況の表示画面とその説明を以下に示します。

```
filemnt> filestat
SIDE-A: VALID (Active) ID:WAKATO EXTID: MEDU      FIRM VER:V01.00 FILE
VER:180695
SIDE-B: VALID (Inactive) ID:WAKATO EXTID: MEDU    FIRM VER:V01.01 FILE
VER:280995
```

図5-40 ファームウェアの格納状況の表示例

ID..... 装置識別子を示します。WAKATOと表示されます。

EXTID 拡張識別子を示します。MEDUと表示されます。

FIRM VER ファームウェアのバージョンを示します。上のSIDE-Aの例はファームウェアのバージョンがV01.00であることを示します。

FILE VER ファームウェアの作成年月日を示します。上のSIDE-Aの例はファームウェアが1995年6月18日に作成されたことを示します。

Active リセット後起動されるシステムを示します。

Inactive リセット後には起動されないシステムを示します。

(2) ファームウェアのダウンロード (startsys)

ファームウェアのバージョンアップは、弊社より提供するフロッピーディスクをご使用ください。ダウンロードの実行中は"#"の表示を行います。

コマンド形式：putsys(p)

```
filemnt> putsys
#####
#####
.
.
.
First file has been put, put second file continuously   1枚目ダウンロードの
終了
```

*** 1枚目のフロッピーディスクを外し、2枚目続いて3枚目を挿入する ***

```
#####
#####
.
.
.
Command OK.                                     ダウンロード 終了
```

図5-41 自装置からのファームウェアのダウンロード例



メモ：フロッピーディスクからのファームウェアのダウンロードの操作を失敗した場合、状況に応じて以下のようなエラーメッセージがでます。エラーメッセージを確認のうえで、正しい操作を行ってください。

- フロッピーディスクを装置に挿入せずに「putsys」を実行する、またはファームウェアの入っていないフロッピーディスクを装置に挿入して「putsys」を実行すると「Floppy disk open error」と表示され動作しません。
- フロッピーディスクの順番を間違えて装置に挿入して「putsys」を実行すると、「Put first (またはsecond) FD to drive」と表示され動作しません。

ファームウェアのダウンロードがエラーとなった場合、ファームウェアの不具合が考えられます。再度ダウンロードを行ってエラーが発生した場合は弊社までご連絡ください。

(3) ファームウェアのダウンロード後の適用 (startsys)

ダウンロードされたファームウェアの起動を行います。この場合、装置はリセットされます。

コマンド形式 : startsys(s)

```
filemnt> startsys  
Command OK.
```

図5-42 ダウンロードしたファームウェアの起動

(4) 有効とするフラッシュメモリの変更 (chgsys)

有効とするフラッシュメモリの変更を行います。

コマンド形式 : chgsys(c)

```
filemnt> chgsys  
Command OK.
```

図5-43 有効とするフラッシュメモリの変更

(5) ヘルプ情報の表示 (?)

ファイルメンテナンスモードで使用できるコマンドを表示します。また、引数にコマンド名を指定するとそのコマンドの使用形式を表示します。

コマンド形式 : ? [command]あるいは[command]?

ヘルプ情報の表示画面を以下に示します。

```
filemnt> ?  
  (?), putsys(p), chgsys(c), startsys(s), filestat(f), exit(e)  
filemnt>? putsys  
usage: putsys(p) [[devname:]][filename]]
```

図5-44 ヘルプ情報の表示画面例

5.18 装置の遠隔操作

本装置には、遠隔地から本装置のシステム編集および運用操作する方法が2種類あります（TELNETコンソール、リモートコンソール）。

5.18.1 TELNETコンソール

本装置を、ネットワークに接続し、遠隔の装置とIPのネットワークとして通信が可能となった状態において、遠隔の端末から本装置にTELNETでログインし、コンソール機能を実行することができます（TELNETコンソール）。本装置にTELNETでログインするためには、パスワードの入力が必要となります。なお、導入時はパスワード無しに設定されていますので、パスワード入力時はリターンの入力によりログインすることができます。パスワードを変更するときは「5.11 パスワードの変更」を参照してください。

TELNETでログインした場合と、ローカルコンソールでは、装置の最初の画面(メニュー画面)が一部異なります。TELNETでログインした場合、メインメニューのコマンドライン(「Select the number. :」)の左にTELNETで接続している装置のIPアドレスが表示されます。図5-40に例を示します。

```
Password:xxxxxx
INFONET 3790 Remote Brouter  D V01.00 1995.04.01
WAN topology (ISDN) 1995/04/01 12:00:00 ( 0 00:00:00) Normal Mode
1. configuration display
2. configuration set (normal)
3. configuration set (expert)
4. operation
5. information
6. shift to super mode
7. exit from remote console or current mode
remote[192.168.0.1] Select the number. :
```

図5-45 TELNETログイン後のメインメニュー例

TELNETでログインしてからの操作方法は、ローカルコンソールの操作方法と同じです。



注意：TELNETコンソールによりシステム編集を行う場合、TELNET接続に使用している回線の定義をOFFにはしてはいけません。TELNET接続に使用している回線の定義をOFFにした場合には、回線が切断され以後TELNET接続が不可能となります。



注意：TELNETコンソールから、さらに他の遠隔装置に対してリモートコンソールで接続はできません。

5.18.2 遠隔装置への接続(リモートコンソール)

本装置をネットワークに接続し、遠隔装置とIPのネットワークとして通信が可能となった状態において、ローカルコンソールからオペレーションメニュー（メインメニューで「operation」を選択した後のメニュー）中の「remote console」を選択し、その後遠隔装置のIPアドレスを入力することにより、遠隔の装置のコンソール機能を実行することができます。（「5.9 リモートコンソール」）リモートコンソールと、ローカルコンソールでは、装置の最初の画面(メニュー画面)が一部異なります。リモートコンソールでは、メインメニューのコマンドラインの左にリモートで接続している遠隔装置のLANインタフェースのIPアドレスが表示されます。以下に例を示します。

```
INFONET 3790 Remote Brouter  D V01.00 1995.04.01
WAN topology (ISDN) 1995/04/01 12:00:00 ( 0 00:00:00) Normal Mode
1. configuration display
2. configuration set (normal)
3. configuration set (expert)
4. operation
5. information
6. shift to super mode
7. exit from remote console or current mode
remote[192.168.0.1] Select the number. :
```

図5-46 リモートコンソール選択後のメインメニュー例

リモートコンソールの操作方法は、ローカルコンソールの操作方法と同じです。



注意：リモートコンソールによりシステム編集を行う場合、リモートコンソールの接続に使用している回線の定義をOFFにしてはいけません。リモートコンソールの接続に使用している回線の定義をOFFにした場合には、回線が切断され以後リモートコンソールの接続が不可能となります。



注意：リモートコンソールから、さらに他の遠隔装置に対してリモートコンソールで接続はできません。遠隔装置にリモートコンソールで接続する操作は、必ずローカルコンソールで行います。

5.18.3 遠隔操作の終了

リモートコンソール、TELNETコンソールを終了させる際は、現在のモードが一般資格の状態では、「exit from remote console or current mode」を選択します。このコマンドを選択すると、リモートコンソールで遠隔装置に接続していた場合は自装置のローカルコンソールに、TELNETコンソールで遠隔装置に接続していた場合は接続している端末の画面に復帰します。

```
INFONET 3790 Remote Brouter  A V02.04 1995.04.01
WAN topology (ISDN) 1995/04/01 12:00:00 ( 3 00:01:21) Normal Mode
1. configuration display
2. configuration set (normal)
3. configuration set (expert)
4. operation
5. information
6. shift to super mode
7. exit from remote console or current mode
remote[192.168.1.1] Select the number. : 7      TELNETコンソールで7を選択
Connection closed by foreign host.             TELNETを終了したときの表示
local%
```

図5-47 TELNETコンソールからの復帰例



メモ：リモートコンソール、TELNETコンソールで管理者資格の場合、ローカルコンソールに復帰するためには「exit from remote console or current mode」を2回実行する必要があります。

5.19 簡易コマンド機能

本装置は、コンソールからメニューを選択して装置の操作を行う通常の方法の他に、コマンドを入力して直接操作を行う簡易コマンド機能をサポートしています。本機能を利用することにより、頻繁に使用する操作や参照する情報の取得を毎回メニューを選択しながら操作をすることなく行うことができます。簡易コマンド機能により実行できるコマンド名、実行内容、参照項を付録Dに記述します。

5.20 FTPを利用したメンテナンス

本装置では、リモートメンテナンスとして、同一LAN上のホスト（FTPクライアント）からFTPでログインすることができます。FTPを利用したリモートメンテナンスの使用方法を付録Eに記述します。

6章 インフォメーション

この章では、装置に関する各種情報の表示機能について説明します。この章の内容を以下にまとめます。

- インフォメーションメニュー
- IPに関するインフォメーション
- DHCPリレーエージェントに関するインフォメーション
- IPXに関するインフォメーション
- ブリッジング機能に関するインフォメーション
- チャネルに関するインフォメーション
- OSPFに関するインフォメーション
- AppleTalkに関するインフォメーション
- 呼確立リミッタに関するインフォメーション
- エラーログ
- ラインログ
- トラップログ
- トラヒックロギングに関するインフォメーション

6.1 インフォメーションメニュー

メインメニューの「information」を選択することにより、図6-1のインフォメーションメニューが表示されます。インフォメーションメニューの中から、必要な情報を選択します。

```
*** Information menu ***
 1. IP interface status
 2. IPX interface status
 3. bridge port status
 4. channel information
 5. statistics information
 6. IP routing information
 7. BOOTP/DHCP relay information
 8. IPX routing information
 9. SAP information
10. OSPF information
11. AppleTalk information
12. limitation of ISDN connection period
13. error log
14. line log
15. trap log
16. traffic log
Select the number. :
```

図6-1 インフォメーションメニュー

インフォメーションメニューからメインメニューへ移行する際は、「ESC」キーを入力します。

- IP interface status
インフォメーションメニューで「IP interface status」を選択すると、IPルーティング機能のインタフェースの情報が表示されます。（「6.2 IPに関するインフォメーション」）
- IPX interface status
インフォメーションメニューで「IPX interface status」を選択すると、IPXルーティング機能のインタフェースが情報が表示されます。（「6.3 IPXに関するインフォメーション」）
- bridge port status
インフォメーションメニューで「bridge port status」を選択すると、ブリッジング機能のポートに関する情報が表示されます。（「6.4 ブリッジングに関するインフォメーション」）

- channel information
インフォメーションメニューで「channel information」を選択すると、現在使用しているチャンネルの情報が表示されます。（「6.5 チャンネルに関するインフォメーション」）
- statistics information
インフォメーションメニューで「statistics information」を選択すると、各種統計情報が表示されます。（「6.2 IPに関するインフォメーション」～「6.6 ISDNに関するインフォメーション」）
- IP routing information
インフォメーションメニューで「IP routing information」を選択すると、IPのルーティング情報が表示されます。（「6.2 IPに関するインフォメーション」）
- IP routing information
インフォメーションメニューで「IP routing information」を選択すると、IPのルーティング情報が表示されます。（「6.2 IPに関するインフォメーション」）
- BOOTP/DHCP relay information
インフォメーションメニューで「BOOTP/DHCP relay information」を選択すると、DHCPリレーエージェント機能の情報が表示されます。（「6.3 DHCPリレーエージェント機能に関するインフォメーション」）
- IPX routing information
インフォメーションメニューで「IPX routing information」を選択すると、IPXのルーティング情報が表示されます。（「6.4 IPXに関するインフォメーション」）
- SAP routing information
インフォメーションメニューで「SAP routing information」を選択すると、IPXのSAP情報が表示されます。（「6.4 IPXに関するインフォメーション」）
- OSPF information
インフォメーションメニューで「OSPF information」を選択すると、OSPFに関する情報が表示されます。（「6.7 OSPFに関するインフォメーション」）
- AppleTalk information
インフォメーションメニューで「AppleTalk information」を選択すると、AppleTalkに関する情報が表示されます。（「6.8 AppleTalkに関するインフォメーション」）
- limitation of ISDN connection period
インフォメーションメニューで「limitation of ISDN connection period」を選択すると、呼確立リミットに関する情報が表示されます。（「6.9 呼確立リミットに関するインフォメーション」）

- error log
インフォメーションメニューで「error log」を選択すると、装置全体の中度 / 軽度障害情報が表示されます。（ 「6.10 エラーログ」 ）

- line log
インフォメーションメニューで「line log」を選択すると、回線に関する障害情報等が表示されます。（ 「6.11 ラインログ」 ）

- trap log
インフォメーションメニューで「trap log」を選択すると、装置全体の重度障害情報が表示されます。（ 「6.12 トラップログ」 ） 重度障害とは装置にリセットがかかる、または一部の機能が全く使用できなくなる状態となる障害を意味します。

- traffic log
インフォメーションメニューで「traffic log」を選択すると、IPルーティングにおけるIPパケットのトラフィック量が表示されます。（ 「6.13 トラフィックロギングに関するインフォメーション」 ）

6.2 IPに関するインフォメーション

インフォメーションメニュー内でIPに関する情報は「IP interface status」, 「statistics information」, 「IP routing information」の3箇所にて取得できます。

6.2.1 IPインタフェースの情報

インフォメーションメニューで「IP interface status」を選択すると、IPルーティング機能に関するインタフェースの情報が表示されます。図6-2にISDN使用時の表示例を示します。

```

1.LAN
2.BRI#1-1    3.BRI#1-2    4.BRI#2-1    5.BRI#2-2
6.BRI#3-1    7.BRI#3-2    8.BRI#4-1    9.BRI#4-2
10.BRI#5-1   11.BRI#5-2   12.BRI#6-1   13.BRI#6-2
14.BRI#7-1   15.BRI#7-2   16.BRI#8-1   17.BRI#8-2
Select the number : 1
<LAN>
interface status:up
IP address      :192.168.1.1
subnetmask     :255.255.255.0
broadcast      :192.168.1.255
Hit return or ESC or 'q' key:
:
1.LAN
2.BRI#1-1    3.BRI#1-2    4.BRI#2-1    5.BRI#2-2
6.BRI#3-1    7.BRI#3-2    8.BRI#4-1    9.BRI#4-2
10.BRI#5-1   11.BRI#5-2   12.BRI#6-1   13.BRI#6-2
14.BRI#7-1   15.BRI#7-2   16.BRI#8-1   17.BRI#8-2
Select the number : 2
<BRI#1-1>
interface status :up
channel status  :connect
interface type  :broadcast
IP address      :192.168.2.1
subnetmask     :255.255.255.0
broadcast      :192.168.2.255
Hit return or ESC or 'q' key:
:

```

図6-2 IPインタフェース情報例

以下に表示内容を示します。

- interface status..... インタフェースの状態 .
 - up WAN回線に障害がないとき (LANは常にup)
 - down WAN回線に障害が発生しているとき

- channel status チャネルの状態 (ISDNのみ) .
 - connect..... 正常に接続中
 - failure..... 異常
 - notconnected..... 正常に切断中
 - calling 接続動作中
 - disconnecting..... 切断動作中
 - other..... その他の状態

- interface type WAN回線のインタフェースタイプ .
 - point to point ポイントツーポイントインタフェース
 - broadcast..... ブロードキャストインタフェース

- IP address そのインタフェースのIPアドレス .

- subnetmask そのインタフェースのサブネットマスク (インタフェースタイプがポイントツーポイントの場合にはリモートサブネットマスク) .

- broadcast..... そのインタフェースのブロードキャストアドレス (インタフェースタイプがポイントツーポイントの場合にはリモートサブネットマスク)

- remote IP address そのインタフェースと接続する相手のIPアドレス (インタフェースタイプがブロードキャストの場合には、表示されません)

6.2.2 IPに関する統計情報

インフォメーションメニューで「statistics information」を選択後、サブメニュー「IP」を選択すると、IPに関する統計情報が表示されます。

```

<IP>
in packet          :0          in discard packet    :0
in header error packet :0      in address error packet:0
out request packet  :0          out discard packet   :0
forward packet     :0          no route packet      :0

<ICMP>
in message packet  :0          in error packet      :0
out message packet:0          out error packet:0

<UDP>
in datagram packet:0          in error packet      :0
no port packet    :0          out datagram packet:0

<TCP>
in segment packet:0          out segment packet:0
in error packet   :0          passive open count:0

<RIP>
in packet          :0          sent packet          :0
out request packet :0          in reply packet      :0
flash update packet:0        send error packet:0
bad receive packet :0

<SNMP>
in packet          :0          out packet:0
out trap packet:0

```

図6-3 IPに関する統計情報例

以下に表示内容を示します。

(1) IP

- in packet 総入力IPパケット数
- in discard packet..... 廃棄された入力パケット数
- in header error packet..... IPヘッダエラー受信パケット数
- in address error packet IPアドレスエラー受信パケット数
- out request packet..... 送信要求パケット数
- out discard packet..... 内部資源不足のため廃棄された送信要求パケット数
- forward packet..... フォワーディングの必要のある受信パケット数
- no route packet 送信経路がないため廃棄された送信要求パケット数

(2) ICMP

- in message packet..... 受信ICMPパケット数 (エラー含む)
- in error packet 受信ICMPエラーパケット数
- out message packet..... 送信ICMPパケット数 (エラー含む)
- out error packet 送信ICMPエラーパケット数

(3) UDP

- in datagram packet 受信UDPデータグラム数
- in error packet 受信エラーUDPデータグラム数 (チェックサムエラー等)
- no port packet 受信エラーUDPデータグラム数 (不正宛先ポート)
- out datagram packet 送信UDPデータグラム数

(4) TCP

- in segment packet 受信TCPセグメント数
- out segment packet..... 送信TCPセグメント数
- in error packet 受信エラーTCPセグメント数 (チェックサムエラー等)
- passive open count 受動オープンした回数

(5) RIP

- in packet 受信RIPパケット数
- sent packet 送信RIPパケット数
- out request packet..... 送信RIP要求パケット数
- in reply packet 受信RIPリプライパケット数
- flash update packet..... 「triggered update」した回数
- send error packet 送信エラーパケット数
- bad receive packet 受信エラーパケット数

(6) SNMP

- in packet 受信SNMPメッセージ数
- out packet 送信SNMPメッセージ数
- out trap packet 送信SNMPトラップ数

6.2.3 IPルーティングの情報

インフォメーションメニューで「IP routing information」を選択すると、IPのルーティング情報が表示されます。ただし、IPルーティング機能が動作していない場合、表示は行われません。

protocol	dst host	mask	metric	gateway
rip	192.168.2.0	255.255.255.0	3	192.168.1.1

図6-4 IPルーティング情報例

- protocol..... ルーティング情報を得た手段
 rip..... RIPにより有効になったルーティング情報
 local スタティックにより有効になったルーティング情報
 other..... 装置が直接属しているネットワークの情報
- dst host..... 宛先ネットワーク（ホスト）番号
- mask..... dst hostに対するマスク
- metric..... dst hostに到達するために経由するルータの数
- gateway..... dst hostに到達するために送信するゲートウェイのIPアドレス

6.3 DHCPリレーエージェントに関する

インフォメーション

インフォメーションメニュー内でDHCPリレーエージェントに関する情報は、「discard frame」、「statistics」の2箇所で取得できます。

6.3.1 廃棄フレーム

インフォメーションメニューで「BOOTP/DHCP relay information」を選択後、サブメニュー「discard frame」を選択すると、廃棄フレームに関する情報を表示することができます。

ここでは、「BOOTREQUEST」フレームと「BOOTREPLY」フレームの表示を選択します。

```
*** INF. : discard frame menu ****
  1. BOOTREQUEST frame
  2. BOOTREPLY frame
Select the number. : 1
```

図6-5 DHCPリレーエージェントに関する廃棄フレーム

表示は16進数のダンプで表示されます。

6.3.2 統計情報

インフォメーションメニューで「BOOTP/DHCP relay information」を選択後、サブメニュー「statistics」を選択すると、DHCPリレーエージェント機能に関する統計情報を表示することができます。

```
received request : 0000000001      received reply : 0000000001
relayed request  : 0000000001      relayed reply  : 0000000001
discarded request: 0000000001      discarded reply: 0000000001
```

図6-6 DHCPリレーエージェントに関する統計情報例

表示内容を以下に示します。

- received request..... BOOTP/DHCPリレーエージェント機能全体が受信したBOOTREQUESTメッセージ数
- received reply BOOTP/DHCPリレーエージェント機能全体が受信したBOOTREPLYメッセージ数
- relayed request BOOTP/DHCPリレーエージェント機能全体がリレーしたBOOTREQUESTメッセージ数

6.3 DHCPリレーエージェントに関するインフォメーション

- relayed reply..... BOOTP/DHCPリレーエージェント機能がリレーした
BOOTREPLYメッセージ数
- discarded request..... BOOTP/DHCPリレーエージェント機能が廃棄した
BOOTREQUESTメッセージ数
- discarded reply BOOTP/DHCPリレーエージェント機能が廃棄した
BOOTREPLYメッセージ数

6.4 IPXに関するインフォメーション

インフォメーションメニュー内でIPXに関する情報は「IPX interface status」, 「statistics information」, 「IPX routing information」, 「SAP information」の4箇所で取得できます。

6.4.1 IPXインタフェースの情報

インフォメーションメニューで「IPX interface status」を選択すると、IPXルーティング機能に関するインタフェースの情報が表示されます。ただし、IPXルーティング機能が動作していない場合、表示は行われません。図6-7にISDN使用時の表示例を示します。

```
1.LAN
2.GroupA      3.GroupB      4.BRI#6-2      5.BRI#7-2
Select the number : 1
<GroupA>
interface status :up
IPX frame type   :ETHERNET_802.3
IPX network NO.  :00000b00

1.LAN
2.GroupA      3.GroupB      4.BRI#6-2      5.BRI#7-2
Select the number :
```

図6-7 IPXインタフェース情報例

以下に表示内容を示します。

- interface status..... インタフェースの状態
 - up WAN回線に障害がないとき (LANは常にup)
 - down WAN回線に障害が発生しているとき
- IPX frame type データリンク層のフレームのタイプ
- IPX node ID. WAN回線に割り当てられたIPXノード番号
- IPX network NO. そのインタフェースの持つIPXネットワーク番号

6.4.2 IPXに関する統計情報

インフォメーションメニューで「statistics information」を選択後、サブメニュー「IPX」を選択すると、IPXに関する統計情報が表示されます。

```

<IPX>
in packet          :0          in discard packet      :0
in format error packet :0      in bad hop count packet :0
out generated packet :0          out forwarded packet   :0
no route packet     :0          local destination packet:0
broadcast receive packet:0      broadcast send packet  :0

<RIP>
in packet          :0          sent packet            :0
out request packet :0          in reply packet        :0
flash update packet:0          send errors packet     :0
bad receive packet :0

<SAP>
in packet          :0          sent packet            :0
out request packet :0          in reply packet        :0
flash updates packet:0          send error packet     :0
bad receive packet :0
Hit return or ESC or 'q' key:

```

図6-8 IPXに関する統計情報例

以下に表示内容を示します。

(1) IPX

- in packet 受信IPXパケット数
- in discard packet..... 受信エラーIPXパケット数
- in format error packet..... 廃棄された受信パケット数
- in bad hop count packet ホップカウントの誤った受信IPXパケット数
- out generated packet..... 装置が発生した送信IPXパケット数
- out forwarded packet..... 中継した送信IPXパケット数
- no route packet 廃棄された送信要求パケット数（送信経路がない）
- local destination packet..... 自局あてIPXパケット数
- broadcast receive packet 受信ブロードキャストIPXパケット数
- broadcast send packet..... 送信ブロードキャストIPXパケット数

(2) RIP

- in packet 受信RIPパケット数
- sent packet 送信RIPパケット数
- out request packet..... 送信RIP要求パケット数
- in reply packet 受信RIPリプライパケット数
- flash update packet..... 「triggered update」した回数
- send errors packet..... 送信エラーパケット数
- bad receive packet 受信エラーパケット数

(3) SAP

- in packet 受信SAPパケット数
- sent packet 送信SAPパケット数
- out request packet..... 送信SAP要求パケット数
- in reply packet 受信SAPリプライパケット数
- flash update packet..... 「triggered update」した回数
- send errors packet..... 送信エラーパケット数
- bad receive packet 受信エラーパケット数

6.4.3 IPXルーティング情報

インフォメーションメニューで「IPX routing information」を選択すると、IPXのルーティング情報が表示されます。ただし、IPXルーティング機能が動作していない場合、表示は行われません。

```

Router name:
  dst network metric time ticks gateway
                                (network NO)  (host ID)
-----+-----+-----+-----+-----+-----+-----+-----+-----+
12345678          1          1      0000000a 001122334455
Hit return or ESC or 'q' key:
    
```

図6-9 IPXルーティング情報例

- dst network 宛先ネットワーク番号
- metric..... dst networkに到達するために経由するルータの数（本装置を1としてカウントする）
- time ticks dst networkに到達するための時間（1tick = 1/18秒）

- gateway (network NO)..... dst networkに到達するために送信するゲートウェイのネットワーク番号
- gateway (host ID)..... dst networkに到達するために送信するゲートウェイのノードID

6.4.4 SAP情報

インフォメーションメニューで「SAP information」を選択すると、IPXのSAPに関する情報が表示されます。ただし、IPXルーティング機能が動作していない場合、表示は行われません。

```

server name           :Server1
  address (network)  :00000ddd
                    (host) :0000000000001
  socket             :0451
  type                :file server
  hop to server      :4

Hit return or ESC or 'q' key:
    
```

図6-10 SAP情報例

- server name サーバの名称
- address (network) サーバのインターナルネットワーク番号
- address (host) サーバのノードID
- socket..... サーバが通信に利用するためのソケット番号
- type サーバのサービスタイプ
- hop to server サーバに到達するために経由するルータの数（本装置を1としてカウントする）

6.5 ブリッジ機能に関するインフォメーション

インフォメーションメニュー内でブリッジ機能に関する情報は「bridge port status」と「statistics information」の2箇所で取得できます。

6.5.1 ブリッジポートの情報

インフォメーションメニューで「bridge port status」を選択すると、ブリッジ機能のポートに関する情報が表示されます。図6-9にISDN使用時の表示例を示します。

```

1.LAN
2.GroupA      3.BRI#5-1    4.BRI#5-2    5.BRI#6-1
6.BRI#7-2
Select the number : 1
<LAN>
interface      :ISO8802-3
port status    :forwarding

1.LAN
2.GroupA      3.BRI#5-1    4.BRI#5-2    5.BRI#6-1
6.BRI#7-2
Select the number : 2
<GroupA>
operation status :add-loadsplit
port status      :forwarding
lsplit           :GroupB

```

図6-11 ブリッジポートの情報例

以下に表示内容を示します。

- interface インタフェース仕様（現在はISO8802-3のみ，表示はLANのみ）
- operation status..... チャンネルまたはリンクコネクションの現在の使用状態
 - clear 切断状態
 - only-usual 通常回線のみで運用
 - add-loadsplit..... トラヒック分散動作中
 - other..... その他

- port status 中継動作の状態
 - disable..... 使用しない
 - blocking 中継を行わない (BPDUの中継は行う)
 - listening 受信のみを行う
 - learning..... 受信したMACアドレスの学習を行う
 - forwarding 中継を行う

- Isplit トラヒック分散回線として使用するグループ

6.5.2 ブリッジング機能に関する統計情報

インフォメーションメニューで「statistics information」を選択後、サブメニュー「bridge port」を選択すると、ブリッジングのポートの統計情報が表示されます。図6-12にISDN使用時の表示例を示します。

```

1.LAN
2.GroupA      3.BRI#5-1    4.BRI#5-2    5.BRI#6-1
6.BRI#7-2
Select the number : 1

<LAN>
port in frames      :0    port out frames:0
filtered frames     :0
error frames        :0
FCS error frames    :0    collision count :0
delay discard frames:0
Hit return or ESC or 'q' key:
  
```

図6-12 ブリッジング機能に関する統計情報例

以下に表示内容を示します。

- port in frames ポートに届いたフレームの数
- port out frames ポートから出たフレームの数
- filtered frames フィルタリングで廃棄されたフレーム数
- error frames フレームのフォーマットエラー (LANのみ)
- FCS error frames FCSエラーで廃棄されたフレーム数
- collision count 衝突検出回数 (LANのみ)
- delay discard frames..... 最大中継遅延時間を超えたため、廃棄されたフレームの数

6.6 チャネルに関するインフォメーション

6.6.1 チャネルの情報

インフォメーションメニューで「channel information」を選択すると、現在使用しているチャネルの情報が表示されます。チャネルとは、HSDまたはISDNのような物理的な回線をさします。図6-13にISDN使用時の表示例を示します。

```

1.BRI#1-1    2.BRI#1-2    3.BRI#2-1    4.BRI#2-1
5.BRI#3-1    6.BRI#3-2    7.BRI#4-1    8.BRI#4-2
9.BRI#5-1   10.BRI#5-2   11.BRI#6-1   12.BRI#6-2
13.BRI#7-1  14.BRI#7-2

Select the number : 1

<BRI#1-1>
local address      :03xxxxxxxx
local subaddress   :1000
channel usage      :normal
line status        :up
channel status     :notconnected
Hit return or ESC or 'q' key:

```

図6-13 チャネル情報例

以下に表示内容を示します。

line speed..... 専用線の色度 (HSDのみ...64Kbps, 128Kbps)

local address 自装置のISDN番号 (ISDNのみ)

local subaddress 自装置のサブアドレス (ISDNのみ)

channel usage ISDN回線の属性

off 未使用

normal..... 通常 (HSDのみ)

main 通常回線として運用中 (ISDNのみ)

loadsplit トラヒック分散として運用 (ISDNのみ)

line status..... 回線の状態

up 運用中 (HSD), 正常動作状態 (ISDN)

down 停止 (HSD), 通信不可状態 (ISDN)

```

testing ..... 試験中 (HSDのみ)
normal-stop..... 正常停止状態
other..... その他

channel status ..... チャンネルの状態 (ISDNのみ)
connect ..... 正常に接続中
failure ..... 異常
notconnected..... 正常に切断中
calling ..... 接続動作中
disconnecting..... 切断動作中
other..... その他の状態
    
```



注意：チャンネルがグループに属している場合、情報が表示されるのは必ずしも実際に接続しているチャンネルとは限りません。

6.6.2 チャンネルの統計情報

インフォメーションメニューで「statistics information」を選択後サブメニューの「channel」を選択すると、現在使用しているチャンネルの統計情報が表示されます。図6-12にISDN使用時の表示例を示します。

```

      1.GroupA      2.GroupB      3.BRI#5-1      4.BRI#5-2
Select the number : 1

<GroupA>
congestion count:269
load split count:0                load split error count:0
total time(sec) :0                total charge(yen):0
call setup count:0                call error count :0
call busy count :0
Hit return or ESC or 'q' key:
    
```

図6-14 チャンネル統計情報例

以下に表示内容を示します。

- congestion count..... 通常回線障害発生回数
- load split count トラヒック分散の接続回数 (ISDNのみ)
- load split error count トラヒック分散回線の障害発生回数 (ISDNのみ)
- total time (sec)..... ISDNの接続時間の合計 (秒) (ISDN, 発呼した時のみ)

6章 インフォメーション

- total charge (yes) ISDNの使用料金の合計（円）（ISDN，発呼した時のみ）



注意：ISDNを回線スピード56kbpsで海外と接続している場合、「total charge」の値は加算されません。

- call setup count..... ISDNを使用した回数（ISDNのみ）
- call error count ISDNを接続した際エラーで解放された回数（ISDNのみ）
- call busy count..... ISDNを接続した際相手ビジーで解放された回数（ISDNのみ）



メモ：グループを選択した場合，グループに属するチャンネルの情報の累計を表示します。

6.7 OSPFに関するインフォメーション

インフォメーションメニュー内でOSPFに関する情報は「OSPF information」で取得できます。「OSPF information」を選択すると、図6-15の選択メニューが表示されます。

```
*** INF.: OSPF information menu ***
 1. general
 2. area table
 3. link state data base
 4. interface table
 5. virtual interface table
 6. neighbor table
 7. virtual neighbor table
Select the number. :
```

図6-15 OSPFに関する情報選択メニュー

- general OSPFに関する一般情報（6.6.1を参照）
- area table OSPFエリアの情報（6.6.2を参照）
- link state data base OSPFリンク状態の情報（6.6.3を参照）
- interface table OSPFインターフェースの情報（6.6.4を参照）
- virtual interface table OSPFバーチャルリンクのインタフェース情報（6.6.5を参照）
- neighbor table OSPF隣接の情報（6.6.6を参照）
- virtual neighbor table OSPFバーチャルリンクを確立した相手の情報（6.6.7を参照）

6.7.1 OSPFに関する一般情報

インフォメーションメニューで「OSPF information」を選択後サブメニューの「general」を選択すると、OSPFに関する一般情報が表示されます。図6-16に表示例を示します。

```
area border router status:false
AS border router status  :false
external LSA count       :0
external LSA checksum    :0
originate new LSA count  :0
receive new LSA count    :0
Hit return or ESC or 'q' key:
```

図6-16 OSPFに関する一般情報例

以下に表示内容を示します。

- area border router status 本装置のエリア境界ルータとしての状態
true..... エリア境界ルータとして動作中
false エリア境界ルータとして動作していない
- AS border router status 本装置のAS境界ルータとしての状態
true..... AS境界ルータとして動作中
false AS境界ルータとして動作していない
- external LSA count link-state databaseの中のexternal link-state advertisementsの数
- external LSA checksum link-state databaseの中のexternal link-state advertisementsのチェックサムの総和
- originate new LSA count OSPFのlink-state advertisementsを送信した回数
- receive new LSA count OSPFのlink-state advertisementsを受信した回数

6.7.2 OSPFエリアの情報

インフォメーションメニューで「OSPF information」を選択後サブメニューの「area table」を選択すると、現在使用しているOSPFエリアの情報を表示します。図6-17に表示例を示します。

```

area ID                :0.0.0.0
spf runs               :1
area border router count:0
AS border router count :0
area LSA count         :1
area LSA checksum      :45438

area ID                :0.0.0.1
spf runs               :2
area border router count:0
AS border router count :0
area LSA count         :1
area LSA checksum      :13335

Hit return or ESC or 'q' key:

```

図6-17 OSPFエリアの情報例

以下に表示内容を示します。

- area ID 本装置が属しているエリアのエリアID
- spf runs OSPFのリンクの情報からルーティングテーブルを更新した回数
- area border router count エリア内の到達可能なエリア境界ルータの総数
- AS border router count..... エリア内の到達可能なAS境界ルータの総数
- area LSA count..... エリア内のlink-state databaseの中のlink-state advertisementsの総数
- area LSA checksum..... エリア内のlink-state databaseの中のlink-state advertisementsのチェックサムの総和

6.7.3 OSPFリンク状態の情報

インフォメーションメニューで「OSPF information」を選択後サブメニューの「link state data base」を選択すると、現在のリンク状態の情報を表示します。図6-18に表示例を示します。

```
area ID      :0.0.0.0
type        :routerLink
link state ID:192.168.2.1
router ID   :192.168.2.1
sequence    :2147483651
age         :1433
checksum    :45691

area ID      :0.0.0.0
type        :summaryLink
link state ID:192.168.3.0
router ID   :192.168.2.1
sequence    :2147483649
age         :1464
checksum    :16434

Hit return or ESC or 'q' key:
```

図6-18 OSPFリンクの情報例

以下に表示内容を示します。

- area ID link-state advertisementを受信したエリアID
- type link-state advertisementのタイプ
 - routerLink..... ルータのインタフェースの情報
 - networkLink 指定ルータが送信するトランジットネットワークの情報
 - summaryLink エリア境界ルータが送信するエリア外のネットワークの情報
 - asSummaryLink AS境界ルータのAS内の情報
 - asExternalLink AS境界ルータが送信するAS外のネットワーク情報
- link state ID link-state advertisementの中に入っていたlink-state ID
- router ID link-state advertisementを生成したルータのルータID
- sequence 受信したlink-state advertisementのシーケンス番号
- age そのlink-state advertisementを受信してからの時間[sec]
- checksum 受信したlink-state advertisementのチェックサム

6.7.4 OSPFインタフェースの情報

インフォメーションメニューで「OSPF information」を選択後サブメニューの「interface table」を選択すると、OSPFインタフェースの情報を表示します。図6-19に表示例を示します。

```

IP address           :192.168.1.1
address less interface :0
state                :designateRouter
designated router     :192.168.1.1
backup designated router:0.0.0.0
event count          :2

IP address           :192.168.1.1
address less interface :3
state                :pointToPoint
designated router     :0.0.0.0
backup designated router:0.0.0.0
event count          :1

Hit return or ESC or 'q' key:

```

図6-19 OSPFインタフェースの情報例

以下に表示内容を示します。

- IP address インタフェースに設定されたIPアドレス
- address less interface..... WAN側にアドレスを設定していないルータの数
- state..... インタフェースの状態
 - down インタフェースが使用できない
 - loopback インタフェースがループバックされている
 - waiting..... designated router,backup designated routerを決定中である
 - pointToPoint..... インタフェースタイプがポイントツーポイントである
 - designatedRouter..... そのインタフェースが属しているネットワークで本装置が指定ルータとして運用されている
 - backupDesignatedRouter そのインタフェースが属しているネットワークで本装置がバックアップ指定ルータとして運用されている
 - otherDesignatedRouter..... そのインタフェースが属しているネットワークで本装置が指定ルータでもバックアップ指定ルータでもない
- designated router 指定ルータのルータID
 - 0.0.0.0..... 指定ルータが存在しない

- backup designated router バックアップ指定ルータのルータID
0.0.0.0..... バックアップ指定ルータが存在しない
- events count..... インタフェースの状態が変化した回数

6.7.5 OSPFバーチャルリンクのインタフェース情報

インフォメーションメニューで「OSPF information」を選択後サブメニューの「virtual interface table」を選択すると、OSPFバーチャルリンクのインタフェース情報を表示します。図6-20に表示例を示します。

```
transit area ID   :0.0.0.1
neighbor         :5.5.5.5
state            :down
event count:0

Hit return or ESC or 'q' key:
```

図6-20 OSPFバーチャルリンクのインタフェースの情報例

以下に表示内容を示します。

- transit area ID バーチャルリンクを確立しているエリア境界ルータ間のエリアID
- neighbor..... バーチャルリンクを確立している相手のエリア境界ルータのルータID
- state..... バーチャルリンクの状態
down バーチャルリンクのインタフェースが使えない
pointToPoint..... インタフェースタイプがポイントツーポイントである
- events count..... バーチャルリンクの状態が変化した回数

6.7.6 OSPF隣接の情報

インフォメーションメニューで「OSPF information」を選択後サブメニューの「neighbor table」を選択すると、OSPF隣接の情報を表示します。図6-21に表示例を示します。

```
IP address      :192.168.10.1
neighbor router:0.0.0.0
state          :down
event count    :0

Hit return or ESC or 'q' key:
```

図6-21 OSPF隣接の情報例

以下に表示内容を示します。

- IP address 隣接のIPアドレス
- neighbor router 隣接のルータのルータID
- state..... 隣接との関係の状態
 - down 隣接ルータとの通信がなされていない
 - attempt..... 隣接ルータにhelloパケットを送信
 - init..... 隣接ルータのhelloパケットを受信
 - twoWay 隣接ルータとの双方向の通信が可能
 - exchangeStart 近隣(adjacencies)を形成している初期段階
 - exchange..... 隣接にdatabase descriptionパケットを送信
 - loading..... 隣接にlink-state requestパケットを送信
 - full 隣接ルータとの近隣が確立
- event count 隣接との関係の状態が変化した回数

6.7.7 OSPFバーチャルリンクを確立した相手の情報

インフォメーションメニューで「OSPF information」を選択後サブメニューの「virtual neighbor」を選択すると、OSPFバーチャルリンクを確立した相手の情報を表示します。図6-22に表示例を示します。

```
transit area ID      :192.168.1.1
router ID           :192.168.10.1
IP address          :192.168.10.1
option              :1
state                :down
event count         :0

Hit return or ESC or 'q' key:
```

図6-22 OSPFバーチャルリンクを確立した相手の情報例

以下に表示内容を示します。

- transit area ID バーチャルリンクを確立しているエリア境界ルータ間のエリアID
- IP address バーチャルリンクを確立している相手のエリア境界ルータのIPアドレス
- state..... 隣接との関係の状態
 - down 隣接ルータとの通信がなされていない
 - attempt..... 隣接ルータにhelloパケットを送信
 - init..... 隣接ルータのhelloパケットを受信
 - twoWay 隣接ルータとの双方向の通信が可能
 - exchangeStart 近隣(adjacencies)を形成している初期段階
 - exchange..... 隣接にdatabase descriptionパケットを送信
 - loading..... 隣接にlink-state requestパケットを送信
 - full 隣接ルータとの近隣が確立
- event count バーチャルリンクの状態が変化した回数

6.8 AppleTalkに関するインフォメーション

AppleTalkに関する情報は、インフォメーションメニュー内で「AT port group」、 「statistics information」、 「routing information」、 「ZIT table」、 「service information」、 「AURP information」の6項目が取得できます。

6.8.1 AppleTalkのポートの情報

「AppleTalk information」で「AT port group」を選択すると、AppleTalkルーティング機能に関するインタフェースの情報が表示されます。ただし、AppleTalkルーティング機能が動作していない場合、表示は行われません。

```
*** AppleTalk port group information ***
  1.LAN
  2.GroupA      3.GroupB      4.BRI#6-2      5.BRI#7-2
Select the number : 1

<LAN>
descriptor      :AppleTalk
type             :EtherTalk2
network number start :100
network number end   :199
network address    :100      1
status            :operational
network configuration:configured
zone configuration  :configured
zone              :hiratsuka
physical interface :LAN

Hit return or ESC or 'q' key:
```

図6-23 AppleTalkのポートの情報例

以下に表示内容を示します。

- descriptor ポートの識別子
 - AURPを使用しない場合
 - AppleTalk
 - AURPを使用している場合
 - AURP: ポート OFF
 - AURP: point-to-point..... WANでIP Tunnelを使用していない
 - AURP: IP..... LANおよびWANのISDN以外でIP Tunnelを使用している
 - AURP: point-to-point IP .. WANでISDNでIP Tunnelを使用している

- type ポートの下位層の種別
 - EtherTalk2..... ポートをEtherTalk2で運用
 - serial-ppp..... ポートをPPPで運用
 - serial-nonstandard 特にtypeが定まっていない

- network number start..... ポートのネットワーク番号範囲の始め

- network number end..... ポートのネットワーク番号範囲の終わり

- network address..... ポートのノードアドレス

- status ポートの現在の状態
 - operational..... ポート UP
 - off ポート DOWN

- network configuration ポートのネットワークの設定の状態
 - configured..... ネットワークを本装置の設定で運用している
 - garnered..... ネットワークを他の装置の情報で運用している
 - unconfigured..... 設定されていない

- zone configuration..... ポートのゾーンの設定の状態
 - configured..... ゾーンを本装置の設定で運用している
 - garnered..... ゾーンを他の装置の情報で運用している
 - unconfigured..... 設定されていない



メモ：ポートを「EtherTalk2」で運用していないとき、「network number start」, 「network number end」および「network address」の値は「0」と表示されます。

- zone ポートが属しているネットワークのデフォルトゾーン

- physical interface 物理インタフェース

6.8.2 統計情報

「AppleTalk information」で「statistics information」を選択すると、AppleTalkに関する統計情報が表示されます。

```

<AARP>
send request packets      :0          send reply packets      :0
receive packets          :0          send probe packets     :0
discard packets          :0

<DDP>
out request packets      :2          in receive packets     :0
forward requests        :0          out no route packets   :2
too short error packets :0          too long error packets :0
broad cast error packets:0          short DDP error packets:0
hop count error packets :0          checksum error packets :0

<RTMP>
receive packets          :0          send packets           :0
request send packets     :0          reply receive packets  :0
discard packets          :0          send error packets     :0

<ZIP>
receive packets          :0          discard packets        :0
send packets             :0          ZIP GetNetInfo port requests:0

<NBP>
receive packets          :0          discard packets        :0
BrRq receive packets    :0          FwdRq send packets    :0
LkUp send packets       :0

<AEP>
echo request packets     :0          echo reply packets     :0
Hit return or ESC or 'q' key:

```

図6-24 AppleTalkに関する統計情報

以下に表示内容を示します。

(1) AARP

- send request packets..... AARP Request送信パケット数
- send reply packets AARP Reply送信パケット数
- receive packets 受信パケット数
- send probe packets AARP Probe送信パケット数
- discard packets 受信不正パケット数 (廃棄パケット数)

(2) DDP

- out request packets 本装置が送信したDDPパケット数（中継パケットは含まない）
- in receive packets DDPによって受信されたパケット数（エラーパケットを含む）
- forward requests 中継したDDPパケット数
- out no route packets 宛先が見つからず廃棄されたDDPパケット
- too short error packets..... DDPヘッダが短すぎて廃棄されたパケット数
- too long error packets..... DDPヘッダが長すぎて廃棄されたパケット数
- broad cast error packets..... 宛先が本装置でないため廃棄されたブロードキャストパケット数
- short DDP error packets 宛先が本装置でなくショートDDPパケットであったため廃棄されたパケット数
- hop count error packets 宛先が本装置でなく距離が15を越えるため廃棄されたパケット数
- checksum error packets チェックサムエラーによって廃棄されたパケット数

(3) RTMP

- receive packets 受信パケット数
- send packets..... 送信パケット数
- request send packets..... 要求パケット送信数
- reply receive packets 応答パケット受信数
- discard packets 受信不正パケット数（廃棄パケット数）
- send error packets..... 送信エラーパケット数

(4) ZIP

- receive packets 受信パケット数
- discard packets 受信不正パケット数（廃棄パケット数）
- send packets..... 送信パケット数
- ZIP GetNetInfo port requests.... ZIP GetNetInfoパケット送信数

(5) NBP

- receive packets 受信パケット数
- discard packets 受信不正パケット数（廃棄パケット数）
- BrRq receive packets..... BrRq受信数
- FwdRq send packets..... FwdRq送信数
- LkUp send packets LkUp送信数

(6) AEP

- echo request packets..... エコーリクエストパケット受信数
- echo reply packets エコー応答パケット送信数

6.8.3 AppleTalkルーティング情報

「AppleTalk information」で「routing information」を選択すると、AppleTalkルーティング情報が表示されます。ただし、AppleTalkルーティング機能が動作していない場合、またルーティング情報がない場合は「no entry」と表示されます。

```

range start:100
  end   :199
  next hop   :0      0
  port      :1
  hops      :0
range start:200
  end   :299
  next hop  :10     1
  port     :4
  hops     :0
range start:1780
  end   :1780
  next hop  :0      0
  port     :0
  hops     :0
Hit return or ESC or 'q' key:

```

図6-25 AppleTalkルーティング情報例

以下に表示内容を示します。

- range start 宛先ネットワークのネットワーク番号の始め
- range end 宛先ネットワークのネットワーク番号の終わり
- next hop 中継先ルータのノードアドレス
(宛先ネットワークが本装置に直接接続するネットワークである場合「0 0」と表示されます。)
- port..... 中継先ルータの接続しているポート番号
- hops 宛先ネットワークまでのホップ数



メモ：「range start」および「range end」以外が全て「0」のルーティング情報は、「extra network」を「use」にした場合に自動的に作成される発呼用ゾーンのためのルーティング情報です。

6.8.4 ゾーンリスト

「AppleTalk information」で「ZIT table」を選択すると、ゾーンリストが表示されます。ただし、AppleTalkルーティング機能が動作していない場合、またゾーンリストがない場合は「no entry」と表示されます。

```
name:kobe
  index      :1
  network start:100
  network end  :199
name:nagoya
  index      :2
  network start:200
  network end  :299
name:tokyo
  index      :3
  network start:1780
  network end  :1780
```

図6-26 ゾーンリスト表示例

以下に表示内容を示します。

- index ゾーンリストに必ず1つ割り当てられる番号
- network start..... このゾーンが属しているネットワーク番号範囲の始め
- network end このゾーンが属しているネットワーク番号範囲の終わり

6.8.5 サービスの情報

「AppleTalk information」で「service information」を選択すると、サービスの情報を表示します。ゾーン名、タイプ、オブジェクト名を入力することによって、指定したゾーンに存在するサービスの情報を取得することができます。

```

Input zone []: tokyo
      type [=]:
      object [=]:
*** Illegal parameter                不正なゾーン名
Input zone []: osaka
      type [=]:
      object [=]:
zone:osaka                            30秒後もしくは「コントロール」キーと
type:AFPServer                        「c」キーを同時入力
object:jun
      node:60      251      socket:130enumerator:0

```

図6-27 サービスの情報の取得例

以下に入力する項目を示します。

- Input zone 情報を取得したいゾーン名
- Input type..... 情報を取得したいタイプ（「=」はすべてのタイプの検索を行います）
- Input object..... 情報を取得したいオブジェクト（「=」はすべてのタイプの検索を行います）

次に表示内容を示します。

- 不正なゾーン名を入力した場合、「*** Illegal parameter」と表示されコマンドライン（「Input zone []」）に戻ります。
- 検索は30秒間行われその後表示されます。「コントロール」キーと「c」キーを同時に押すと検索を中断できます。中断した場合は、その時間内で取得できたサービスを表示します。
- 同時に取得できるサービスは100個までです。
- zone 上で入力されたゾーン名
- type サービスのタイプ
- object そのサービスのオブジェクト名
- node そのサービスのノードアドレス
- socket..... そのサービスのソケット番号
- enumerator..... そのサービスのエヌメレータ値（列挙子）

6.8.6 AURPコネクション情報

「AppleTalk information」で「AURP information」を選択すると、AURPコネクション情報を表示します。

```
remote address   :1001
      subaddress:
local condition  :receiver and sender
port             :GroupA
send RI packet   :800
receive RI packet:890
send ZI packet   :900
receive ZI packet:990

remote address   :100.100.100.100
local condition  :receiver
port             :LAN IPTunneling
send RI packet   :150
receive RI packet:60
send ZI packet   :550
receive ZI packet:560
```

図6-28 AURPコネクション情報表示例

以下に表示内容を示します。

- remote address..... AURPのコネクション相手のアドレス（相手のタイプがISDNリモートターゲットの時、またはAppleTalkで「IP Tunnel」が「use」の時）
- subaddress AURPのコネクション相手のアドレス（相手のタイプがISDNリモートターゲットの時）

- local condition .. AURPのコネクションの種類
 - sender..... 相手に情報を提供する
 - receiver 相手から情報を取得する
 - receiver and sender..... 上記の両者

- port..... コネクションを確立しているポート
- send RI packet RIパケットの送信数
- receive RI packet..... RIパケットの受信数
- send ZI packet ZIパケットの送信数
- receive ZI packet ZIパケットの受信数

6.9 呼確立リミッタに関するインフォメーション

インフォメーションメニューで「limitation of ISDN connection period」を選択するとトータル接続時間呼確立リミッタに関する情報が表示されます。

```
<tokyo>
status          : normal
remote address  : 0311112222
remote subaddress :
limiter max period : 300:00:00
limiter current period: 20:00:00
limiter last period : 5:00:00

<t-0001>
status          : alerted
remote address  : 0457778888
remote subaddress :
limiter max period : 300:00:00
limiter current period: 299:59:59
limiter last period : 50:00:00
```

図6-29 呼確立リミッタに関する情報例

以下に表示内容を示します。

- status トータル接続時間呼確立リミッタの現在の状態
 - normal..... 正常状態（警告前）
 - alerted 警告後
 - bombarded..... トータル接続時間呼確立リミッタ作動後
 - not-work 呼確立リミッタ未動作
- remote address..... ISDNリモートアドレス
- remote subaddress ISDNリモートサブアドレス
- limiter max period 呼確立時間累計の上限値（時間：分：秒）
- limiter current period 現在の呼確立時間の累計（時間：分：秒）
- limiter last period 前回トータル接続時間呼確立リミッタが再スタートする直前の呼確立時間累計（時間：分：秒）



注意：トラヒック分散で2回線使用している場合は、2回線分の呼確立時間の累計が表示されます。また、ISDNリモートアドレスとリモートサブアドレスは通常回線のものが表示されます。

6.10 ルータグループ化に関するインフォメーション

インフォメーションメニューで「router grouping information」をグループルータリストを表示します。

no.	IP address	MAC address	free channel	connected IP address
1.	192.168.1.1	00.80.bd.f0.00.8c	0B	
2.	192.168.1.2	00.80.bd.f0.00.05	0B	

Hit return or ESC or 'q' key:

図6-30 ルータグループ化に関する情報例

以下に表示内容を示します。

- IP address グループルータのIPアドレス
- MAC address..... グループルータのMACアドレス
- free channel 使用できるISDNの本数
- connected IP address..... 現在の接続相手のIPアドレス

6.11 エラーログ

インフォメーションメニューで「error log」を選択すると、装置全体の中度 / 軽度障害情報を表示します。

```
seq uptime          date                      tid logid    ecode
-----
000 0000:00:00.00  94/04/01 (thu) 17:22:22    0 00000000 00000000
                                     # P_ON [V01.00-040194]

Hit return or ESC or 'q' key:
```

図6-31 エラーログ例

6.12 ラインログ

インフォメーションメニューで「line log」を選択すると、回線に関する障害情報等を表示します。サブメニューで回線を選択します。

```
1.LAN
2.BRI#1-1      3.BRI#1-2      4.BRI#5-1      5.BRI#5-2
Select the number : 1
seq uptime          date                      channel  ecode
-----
000 0000:00:00.00  94/04/01 (thu) 17:22:22  LAN      00000000
                                     # P_ON [V01.00-040194]

Hit return or ESC or 'q' key:
```

図6-32 ラインログ例

6.13 トラップログ

インフォメーションメニューで「trap log」を選択すると、装置全体の重度障害情報を表示します。

```
seq uptime          date                      tid logid    ecode
-----
000 0000:00:00.00  94/04/01 (thu) 17:22:22    0 00000000 00000000
                                     # P_ON [V01.00-040194]

Hit return or ESC or 'q' key:
```

図6-33 トラップログ例

6.14 トラフィックロギングに関するインフォメーション

インフォメーションメニューで「traffic logging」を選択した場合、トラフィックロギングに関する情報を表示することができます。

```

*** traffic logging information ***
source IP address      : 192.52.128.20          mask      : 255.255.255.255
destination IP address: 192.52.127.200          mask      : 255.255.255.128
total frames          : 10                      total octets: 10

source IP address      : 192.52.128.20          mask      : 255.255.255.255
destination interface  : ISDN#1
total frames          : 15                      total octets: 15

receive interface     : LAN
destination IP address: 192.52.127.200          mask      : 255.255.255.128
total frames          : 20                      total octets: 20

receive interface     : ISDN#1
destination interface  : ISDN#2
total frames          : 25                      total octets: 25

```

図6-34 トラフィックロギングに関する情報例

以下に表示内容を示します。

- source IP address..... 送信元アドレス
- source mask..... 送信元アドレスマスク
- receive interface 受信インタフェース
- destination IP address..... 宛先アドレス
- destination mask..... 宛先アドレスマスク
- destination interface 宛先インタフェース
- total frames..... 累計フレーム数
- total octets 累計オクテット数



メモ：中継するパケットが設定されたエントリに重複して該当する場合、すべてのエントリでロギングが行われます。



メモ：累計フレーム数、累計オクテット数を0にクリアしたい場合、「4.11 トラフィックロギングに関する設定」で対応するエントリの再設定を行ってください。

付録A 装置の仕様

A.1 仕様

表A-1 仕様

	ポート名	ポート数	仕様
回線構成	AUI	1	ISO8802-3 10BASE5
	I430	1または2	高速デジタル回線（Iインタフェース） 回線速度：64Kbps, 128Kbps
		0または1	ISDN基本インタフェース（2B+D） 回線交換モード
	CONSOLE	1	Dsub25ピンコネクタ
外形寸法			380（W）× 290（D）× 75（H）mm
重量			6 Kg
モジュラーケーブル			10Mbps対応UTPケーブル

A.2 使用環境

A.2.1 電気的条件

表A-2 電気的条件

電源電圧	AC100V ± 10%
周波数	50 / 60Hz + 2% - 4%
消費電力	20W
電源コード	2極アース付き 3Pストレート, 3m



メモ：第3種接地工事を行った電源設備に、この装置を接続してください。

A.2.2 環境条件

表A-3 環境条件

温度	動作時	0～40℃	
	休止時	0～50℃	
湿度	動作時	20～80%	結露しないこと
	休止時	8～90%	
浮遊塵埃		0.15mg/m ³ 以下	

A.3 インタフェース仕様

A.3.1 AUIポート

ポート数：1

コネクタ：D-sub 15P メスコネクタ

表A-4 AUIポートのインタフェース仕様

ピン番号	信号名称	信号方向	ピン番号	信号名称	信号方向
		ブルータ			トランシーバ
1	CI-S		9	CI-B	
2	CI-A		10	DO-B	
3	DO-A		11	DO-S	
4	DI-S		12	DI-B	
5	DI-A		13	VP	
6	Vc		14	VS	
7			15		
8					

A.3.2 I430ポート

ポート数：8

コネクタ：8ピン モジュラーコネクタ（RJ45）

表A-5 I430ポートのインタフェース仕様

ピン番号	信号名称	信号方向	
		ブルータ	網終端装置
1			
2			
3	TA+		
4	RA+		
5	RB-		
6	TB-		
7			
8			

A.3.3 コンソールポート

ポート数：1

コネクタ：D-sub 25P メスコネクタ M2.6 勘合固定台付

表A-6 コンソールポートのインタフェース仕様

ピン番号	信号名称	信号方向	
		ブルータ	DTE
1	FG		
2	SD		
3	RD		
5	CS		
6	DR		
7	GND		
20	ER		

A.4 コンソール仕様

コンソールポートに接続するコンソールの通信機能は、次のような設定にしてください。

表A-7 コンソール仕様

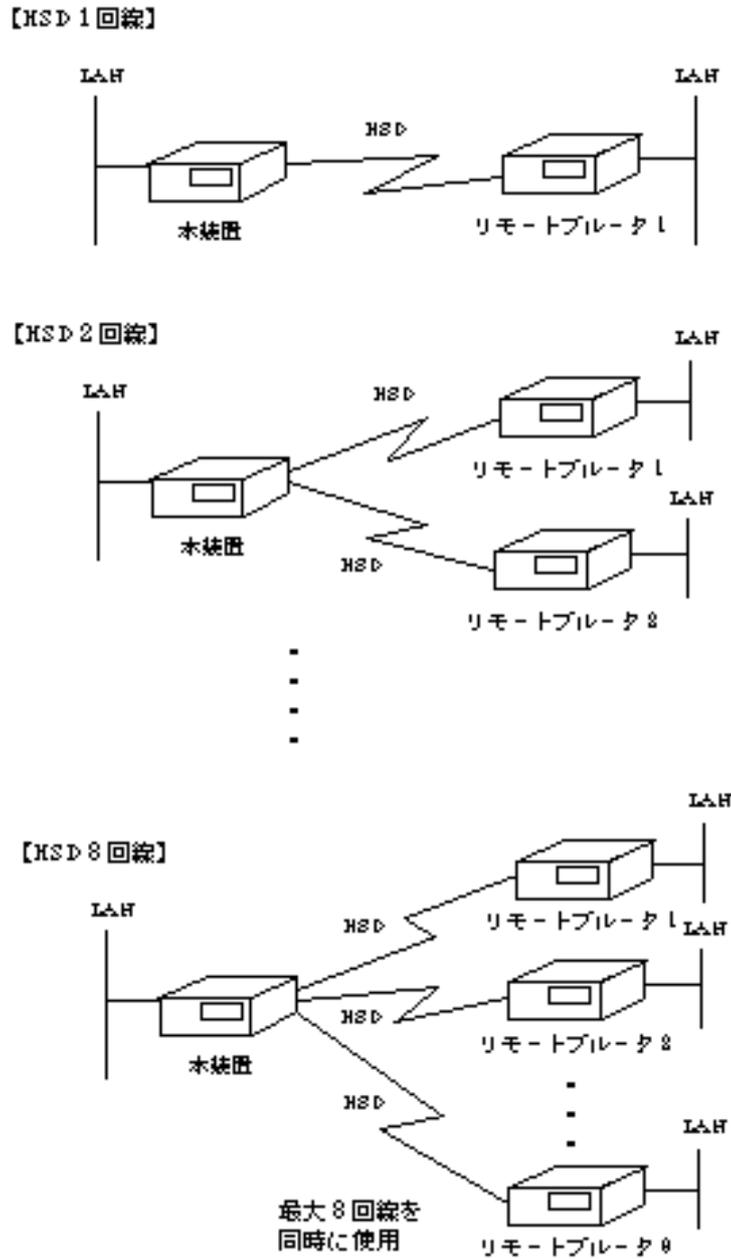
項目	設定
同期方式	調歩同期
通信速度	9600bps
キャラクタ長	8ビット
ストップビット長	1
パリティ	無し
フロー制御	Xon/Xoff

付録B 装置の運用形態

本装置を使用した装置の運用形態について説明します。本装置ではHSD回線を同時に8回線、もしくは、ISDNを同時に8回線（Bチャンネル16回線）使用することができます。それぞれの場合の、利用形態をこの付録で図解します。

B.1 装置の運用形態（HSD回線）

複数の遠隔地にあるLANを，1～8本のHSD回線を通常回線として接続します。

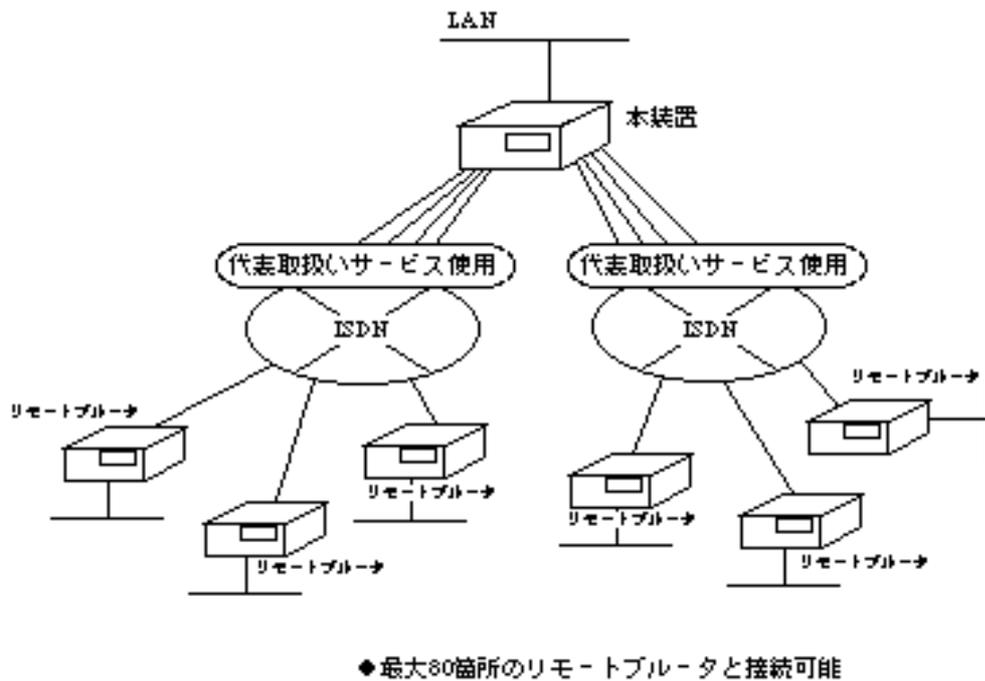


図B-1 HSDを使用する場合

B.2 装置の運用形態（ISDN回線）

B.2.1 代表取扱いサービスを利用する場合

複数の遠隔地にあるLANを、チャンネルをグループと設定して、NTTの代表取扱いサービス（「2.10.5 チャンネルグループ機能」）を利用して接続します。



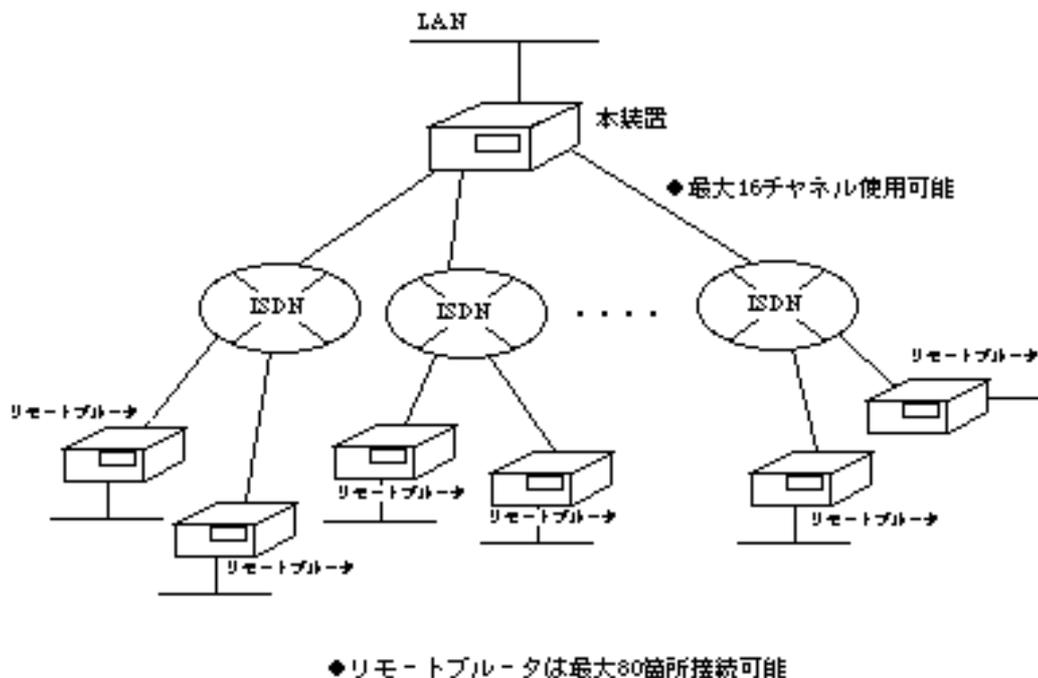
図B-2 代表取扱いサービスを利用する場合

代表取扱いサービスを利用する場合、複数のISDNのBチャンネルを1つのグループと定義し、1つの親番号を割り当てます。本装置は最大80箇所との接続が可能です。

接続相手は親番号に発呼しますが、本装置では同じ番号で同時に複数のISDN回線を着呼することができます。

B.2.2 代表取扱いサービスを利用しない場合

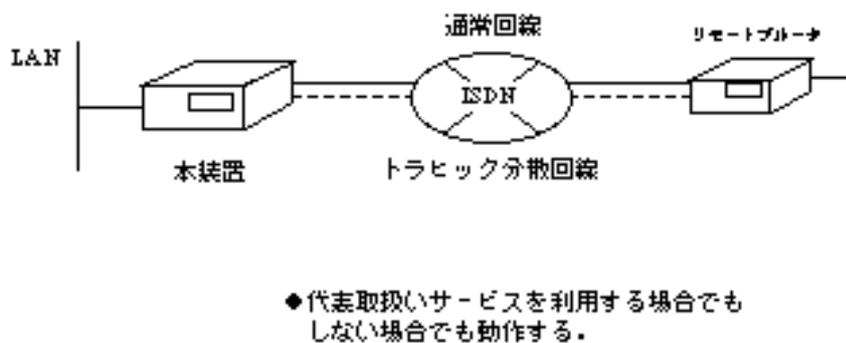
複数の遠隔地にあるLANを、NTTの代表取扱いサービス（「2.10.5 チャンネルグループ機能」）を利用しないで、接続します。



図B-3 代表取扱いサービスを利用しない場合

B.2.3 トラフィック分散を利用する場合

複数の遠隔地にあるLANを、通常回線およびトラフィック分散回線として接続します。



図B-4 トラフィック分散を利用する場合

付録C 設定情報一覧表

本装置での設定情報を示します。備考欄では設定レベルおよび有効タイミングを示します。設定レベルおよび有効タイミングの表記内容は以下の通りです。

< 設定レベル（備考欄左側） >

：必ず設定が必要。

：運用条件によっては設定が必要。

×：導入時の設定のまま運用（通常は設定の必要はない）。

< 有効タイミング（備考欄右側） >

R：リセット後設定値が有効となる。

S：セーブ後有効となる（リセットの必要はない）。

C.1 現在時刻

参照項 3.10

項目	内容	設定範囲	導入時の設定	備考	
year	年	1995 ~ 2094	現在時刻		S
month	月	1 ~ 12	現在時刻		S
day	日	1 ~ 31	現在時刻		S
hour	時	0 ~ 23	現在時刻		S
minute	分	0 ~ 59	現在時刻		S
second	秒	0 ~ 59	現在時刻		S

C.2 自ホスト名

参照項 3.2.1,3.11

項目	内容	設定範囲	導入時の設定	備考	
host name	自ホスト名	最大6文字の英数字	なし	⊙	R

C.3 HSDに関する設定

参照項 3.2.2, 3.12.1

項目	内容	設定範囲	導入時の設定	備考
speed	回線の速度	64Kbps 128Kbps not use	not use	R

C.4 ISDNに関する設定

C.4.1 ISDNチャネルグループ

参照項 3.2.3, 3.12.2

項目	内容	設定範囲	導入時の設定	備考
group name	ISDNをグループとする時のグループ名	最大6文字の英数字	なし	R
Select the ISDN	「group name」に属するISDNのポート	BRI#1 BRI#2 BRI#3 BRI#4 BRI#5 BRI#6 BRI#7 BRI#8	なし	R

C.4.2 ISDN運用形態

参照項 3.2.4,3.12.3

項目	内容	設定範囲	導入時の設定	備考
WAN topology	グループ/チャンネルの運用形態	Usual Load split Usual/Load split (グループのみ) not use (チャンネルのみ)	Usual	R
multi target	複数の相手と接続する/しない	use not use	not use	R
receive address check mode	着信時に相手アドレスをチェックする/しない	on off	on	R
receive address check skip length	チェック時のアドレススキップ長	0 ~ 19	0	R
Usual line	トラヒック分散回線使用時のメイン回線	「WAN topology」で「Usual」が選択されたグループ/チャンネル	なし	R

C.4.3 ISDNリモートターゲット

参照項 3.2.5,3.12.4

項目	内容	設定範囲	導入時の設定	備考
target	ISDNリモートターゲット	最大6文字の英数字	なし	R
remote address	宛先ISDN番号	最大20桁の10進数	なし	R
remote subaddress	宛先ISDNサブアドレス	最大19桁の10進数	なし	R
preference	宛先ISDN番号の発呼の優先度	0 ~ 4	0	R
Do you connect Load split line to XXXXXX	トラヒック分散の使用の有無	yes (トラヒック分散する) no (トラヒック分散しない)	no	R
load split line address	トラヒック分散回線の相手ISDN番号	最大20桁の10進数	「remote address」の値	R
speed	発呼するユーザ速度	64K 64K/56K 56K	64K	R
password	リモートターゲットに対するパスワード	8文字以内の英数字	なし	R

C.4.4 ISDN通常回線

参照項 3.2.6,3.12.5

項目	内容	設定範囲	導入時の設定	備考
local ISDN address	自局のISDN番号	最大20桁の10進数	なし	R
local ISDN subaddress	自局のISDNサブアドレス	最大19桁の10進数	なし	R
Usual line activate/deactivate	通常回線の接続 / 切断の方法	time + traffic manual passive	passive	R
Load split line activate/deactivate	トラヒック分散回線の接続 / 切断の方法	time + traffic manual	manual	R

C.4.5 ISDN接続 / 切断時刻

参照項 3.2.6,3.12.5

項目	内容	設定範囲	導入時の設定	備考	
activate/ deactivate	month	月	1 ~ 12 または*	*	S
	day	日	1 ~ 31 または*	*	S
	day of the week	曜日	Sun. Mon. Tue. Wed. Thu. Fri. Sat. any (すべての曜日)	any	S
	hour	時	0 ~ 23 または*	manual	S
	minute	分	0 ~ 59 または*	manual	S

C.4.6 MACアドレスリモートターゲット

参照項 3.2.25,3.18.1

項目	内容	設定範囲	導入時の設定	備考	
address	宛先MACアドレス	xx:xx:xx:xx:xx:xxの形式	なし	○	§
target	接続相手のターゲットインデックス	1~80のターゲットインデックス	なし	○	§

C.4.7 IPアドレスリモートターゲット

参照項 3.2.9,3.15.2

項目	内容	設定範囲	導入時の設定	備考	
address	中継ルータのIPアドレス	xxx.xxx.xxx.xxxの形式	なし	○	§
target	接続相手のターゲットインデックス	1~80のターゲットインデックス	なし	○	§

C.4.8 IPXアドレスリモートターゲット

参照項 3.2.14,3.16.2

項目	内容	設定範囲	導入時の設定	備考	
address	中継ルータのIPXノードアドレス	12桁の16進数	なし	○	§
target	接続相手のターゲットインデックス	1~80のターゲットインデックス	なし	○	§

C.4.9 AppleTalkアドレスリモートターゲット

参照項 3.2.19,3.17.2

項目	内容	設定範囲	導入時の設定	備考	
address	中継ルータのネットワーク番号	1 ~ 65279	なし	○	§
target	接続相手のターゲットインデックス	1~80のターゲットインデックス	なし	○	§

C.5 基本機能

参照項 3.13

項目	内容	設定範囲	導入時の設定	備考	
IP routing	IPルーティング機能の使用の有無	use : 使用する not use : 使用しない	not use	⊙	R
IP filtering	IPフィルタリング機能の使用の有無	use : 使用する not use : 使用しない	not use	⊙	R
IPX routing	IPXルーティング機能の使用の有無	use : 使用する not use : 使用しない	not use	⊙	R
AppleTalk routing	AppleTalkルーティング機能の使用の有無	use : 使用する not use : 使用しない	not use	⊙	R
bridging	ブリッジング機能の使用の有無	use : 使用する not use : 使用しない	not use	⊙	R
SNMP	SNMP機能の使用の有無	use : 使用する not use : 使用しない	use	⊙	R

C.6 IPホスト

参照項 3.2.7, 3.14

項目	内容	設定範囲	導入時の設定	備考	
IP host	IPホストとして運用する / しない	use : IPホストとして 運用する not use : IPホストとして 運用しない	not use		R
IP address	装置自身のIPアドレス	xxx.xxx.xxx.xxxの形式 (マージャンアドレス を除く)	なし		R
subnetmask	サブネットマスク	xxx.xxx.xxx.xxxの形式	クラスA:255.0.0.0 クラスB:255.255.0.0 クラスC:255.255.255.0		R
broadcast	ブロードキャスト制御	xxx.xxx.xxx.xxxの形式	ホスト部がオール1のアドレス		R
default gateway	ゲートウェイのIPアドレス	xxx.xxx.xxx.xxxの形式	なし		R



注意：装置に設定するIPアドレスとして、以下のアドレスが適用できます。その他のアドレスはマージャンアドレスと呼ばれるアドレスで、特別な用途のために予約されています。

1.0.0.0 ~ 126.255.255.255

128.0.0.0 ~ 255.255.239.255

C.7 datalink

参照項 4.2

項目	内容	設定範囲	導入時の設定	備考	
load split interval timer	輻線監視を行う時間間隔	1~65535 [sec]	300	×	R
watching line	PPP回線上のフラグ同期監視	on:監視する off:監視しない	on	○	R
interface up mode	常にルーティング可能状態とする/接続したときのみ可能状態とする	always:可能にする normal:接続したときのみ可能にする。	normal	○	R
congestion timer	輻線継続監視時間 (トラヒック分散回線の回線接続契機)	1~3600 [sec]	1	×	R
max retry calling	発呼のリトライ回数	0:リトライなし 1~254:リトライ回数 255:無限回	8	×	R
PPP send retry	PPPリンク確立パケット再送回数	0~255	10	×	R
PPP restart timer	PPPリンク確立要求再送タイマ値	100~6000 [10msec]	100	×	R
PPP loop timer	PPPのネゴシエーションの無限ループを検出するタイマ値	1~60 [sec]	10	×	R
idle timer	データ有無型のトラヒック分散および通常回線の終了契機となる無通信監視タイマ値	1~3600 [sec]	60	×	R

C.8 SNMP

参照項 3.2.3,3.19,4.8

項目	内容	設定範囲	導入時の設定	備考	
sysName	管理ノード名	最大32文字の英数字	自ホスト名	×	S
sysContact	管理者名	最大32文字の英数字	なし	×	S
sysLocation	管理ノードの物理的位置	最大64文字の英数字	なし	×	S
IP address	マネージャのIPアドレス	xxx.xxx.xxx.xxxの形式	0.0.0.0	○	S
communityname	マネージャのコミュニティ名	最大32文字の英数字	public	○	S
set enable	マネージャからのset要求の許容	YES NO	NO	○	S
send alarm	マネージャへのトラップ送信有無	YES NO	NO	○	S

マネージャに関する設定は最大8エントリまで設定できます。

C.9 IPに関する設定

C.9.1 IPルーティング

参照項 3.2.8, 3.15.1

項目	内容	設定範囲	導入時の設定	備考	
LAN	IP address	LANのIPアドレス xxx.xxx.xxx.xxxの形式 (マシヤンアドレスを 除く)	なし	○	R
	subnetmask	LANのサブネットマスク	クラスA:255.0.0.0 クラスB:255.255.0.0 クラスC:255.255.255.0	○	R
	broadcast	LANのブロードキャストアドレス	xxx.xxx.xxx.xxxの形式	○	R
WAN	routing interface	ルーティングに使用する インタフェース	「Usual」または 「Usual/load split」を選択 したグループもしくは チャネル	○	R
	interface type	インタフェースのタイプ	point to point broadcast	○	R
	IP address	WANのIPアドレス	xxx.xxx.xxx.xxxの形式 (マシヤンアドレスを 除く)	○	R
	subnetmask	WANのサブネットマスク	xxx.xxx.xxx.xxxの形式	○	R
	broadcast	WANのブロードキャスト アドレス	xxx.xxx.xxx.xxxの形式	○	R
	remote IP address	接続先のIPアドレス	xxx.xxx.xxx.xxxの形式	○	R
	remote subnet mask	接続先のサブネットマスク	xxx.xxx.xxx.xxxの形式	○	R



注意：装置に設定するIPアドレスとして、以下のアドレスが適用できます。その他のアドレスはマシヤンアドレスと呼ばれるアドレスで、特別な用途のために予約されています。

1.0.0.0 ~ 126.255.255.255

128.0.0.0 ~ 255.255.239.255

C.9.2 IPフィルタリング (forward : 最大128エントリ)

参照項 3.2.12,3.15.5,4.5.9

項目	内容	設定範囲	導入時の設定	備考	
protocol	フィルタリングの対象とするプロトコル	tcp udp tcp+udp all other	all	○	§
source address	フィルタリングの対象とする送信元アドレス	xxx.xxx.xxx.xxxの形式 または*	*(1)	○	§
source mask	送信元アドレスに対するマスク	xxx.xxx.xxx.xxxの形式	255.255.255.255	○	§
source port(A)	フィルタリングの対象とする送信元ポートの開始番号	0~65535	0	○	§
source port(B)	フィルタリングの対象とする送信元ポートの終了番号	Aの値~65535	65535	○	§
destination address	フィルタリングの対象とする宛先アドレス	xxx.xxx.xxx.xxxの形式 または*	*(1)	○	§
destination mask	宛先アドレスに対するマスク	xxx.xxx.xxx.xxxの形式	255.255.255.255	○	§
destination port(A)	フィルタリングの対象とする宛先ポートの開始番号	0~65535	0	○	§
destination port(B)	フィルタリングの対象とする宛先ポートの終了番号	Aの値~65535	65535	○	§
receive interface	フィルタリング対象の受信インタフェース	LAN, 「routing interface」で 選択されたグループも しくはチャネル	LAN, 「routing interface」で 選択されたグループも しくはチャネル	○	§
send interface	フィルタリング対象の送信インタフェース	LAN, 「routing interface」で 選択されたグループも しくはチャネル	LAN, 「routing interface」で 選択されたグループも しくはチャネル	○	§
mode	エントリモード	half full	full	○	§

(1): 「*」は各々の項目の設定範囲の全てを網羅することを示します。

C.9.3 IPフィルタリング (discard : 最大64エントリ)

参照項 4.5.10

項目	内容	設定範囲	導入時の設定	備考	
protocol	フィルタリングの対象とするプロトコル	tcp udp tcp+udp all other	all	○	S
source address	フィルタリングの対象とする送信元アドレス	xxx.xxx.xxx.xxxの形式 または*	*(1)	○	S
source mask	送信元アドレスに対するマスク	xxx.xxx.xxx.xxxの形式	255.255.255.255	○	S
source port(A)	フィルタリングの対象とする送信元ポートの開始番号	0~65535	0	○	S
source port(B)	フィルタリングの対象とする送信元ポートの終了番号	Aの値~65535	65535	○	S
destination address	フィルタリングの対象とする宛先アドレス	xxx.xxx.xxx.xxxの形式 または*	*(1)	○	S
destination mask	宛先アドレスに対するマスク	xxx.xxx.xxx.xxxの形式	255.255.255.255	○	S
destination port(A)	フィルタリングの対象とする宛先ポートの開始番号	0~65535	0	○	S
destination port(B)	フィルタリングの対象とする宛先ポートの終了番号	Aの値~65535	65535	○	S
receive interface	フィルタリング対象の受信インタフェース	LAN, 「routing interface」で 選択されたグループも しくはチャネル	LAN, 「routing interface」で 選択されたグループも しくはチャネル	○	S
send interface	フィルタリング対象の送信インタフェース	LAN, 「routing interface」で 選択されたグループも しくはチャネル	LAN, 「routing interface」で 選択されたグループも しくはチャネル	○	S
mode	エントリモード	half full	full	○	S

(1): 「*」は各々の項目の設定範囲の全てを網羅することを示します。

C.9.4 RIP motion

参照項 4.5.1

項目	内容	設定範囲	導入時の設定	備考	
mode	RIPの動作モード	supplier: 送受信 point to point: 送受信 quiet: 受信のみ off: 動作しない	supplier	×	R
trust gateways list	有効なルーティング情報を提供してくれるゲートウェイ	xxx.xxx.xxx.xxxの形式 (最大20エントリー)	なし	×	S
source gateways list	point to pointの場合ルーティング情報を提供するゲートウェイ	xxx.xxx.xxx.xxxの形式 (最大40エントリー)	なし	×	S

C.9.5 RIPインタフェース

参照項 4.5.2

項目	内容	設定範囲	導入時の設定	備考		
各 イ ン タ フ ェ ー ス	send control	RIP情報の送信方法	RIP1: RIP1で送信 RIP2: RIP2で送信 RIP1,2: RIP2をブロード キャスト宛に送信 off: 送信しない	RIP1	×	R
	recv control	RIP情報の受信方法	RIP1: RIP1を受信 RIP2: RIP2を受信 RIP1,2: RIP1およびRIP2 を受信 off: 受信しない	RIP1	×	R
	password	RIP2での認証パスワード	最大16文字の英数字	なし	×	R
	metric	interfaceの加算メトリック値	0~16	0	×	R
	preference	interfaceごとの優先順位	0~255	0	×	R
	broadcast*	WANへのRIP送信方法	on: 定期アップデート off: triggered update	off	×	R
	broadcast interval*	定期アップデートする場合のRIP送信間隔	30~2147483647	30	×	R
	entry ageout*	ルーティング情報をエージアウトする/しない	on: エージアウトする off: エージアウトしない	off	×	R
broadcast interval*	エージアウト時間	30~2147483647	180	×	R	

*はLANでは設定なし。

C.9.6 スタティックルーティング (最大256エントリ)

参照項 3.2.10,3.15.3,4.5.8

項目	内容	設定範囲	導入時の設定	備考	
destination address	宛先ネットワーク番号	xxx.xxx.xxx.xxxの形式 0.0.0.0 : default route	0.0.0.0	○	§
mask	マスク	xxx.xxx.xxx.xxxの形式	0.0.0.0	○	§
gateway	ゲートウェイアドレス	xxx.xxx.xxx.xxxの形式	0.0.0.0	○	§
metric	メトリック値	1~16	16	○	§
preference	優先順位	0~255	50	○	§

C.9.7 RIPフィルタリング(accept GW : 最大32GW x 4エントリ)

参照項 4.5.3

項目	内容	設定範囲	導入時の設定	備考	
mode	テーブルのエントリに一致した情報を有効にする／一致しない情報を有効にする	include : 一致した情報 exclude : 一致しない情報	exclude	○	R

項目	内容	設定範囲	導入時の設定	備考	
destination address	宛先アドレス	xxx.xxx.xxx.xxxの形式	0.0.0.0	○	R
mask	マスク	xxx.xxx.xxx.xxxの形式 (0.0.0.0を除く)	なし	○	R
gateway address	ゲートウェイのアドレス	xxx.xxx.xxx.xxxの形式 (0.0.0.0を除く)	なし	○	R

C.9.8 RIPフィルタリング(propagate GW : 最大32GW × 4エントリ)

参照項 4.5.4

項目	内容	設定範囲	導入時の設定	備考	
mode	テーブルのエントリに一致した情報をRIPで送信する／一致しない情報をRIPで送信する	include : 一致した情報 exclude : 一致しない情報	exclude	○	R

項目	内容	設定範囲	導入時の設定	備考	
destination address	宛先アドレス	xxx.xxx.xxx.xxxの形式	0.0.0.0	○	R
mask	マスク	xxx.xxx.xxx.xxxの形式 (0.0.0.0を除く)	なし	○	R
gateway address	ゲートウェイのアドレス	xxx.xxx.xxx.xxxの形式 (0.0.0.0を除く)	なし	○	R

C.9.9 RIPフィルタリング(IF accept : 最大40エントリ)

参照項 4.5.5

項目	内容	設定範囲	導入時の設定	備考	
mode	テーブルのエントリに一致した情報を有効にする／一致しない情報を有効にする	include : 一致した情報 exclude : 一致しない情報	exclude	○	R

項目	内容	設定範囲	導入時の設定	備考	
destination address	宛先アドレス	xxx.xxx.xxx.xxxの形式	0.0.0.0	○	R
mask	マスク	xxx.xxx.xxx.xxxの形式	0.0.0.0	○	R
interface	受信するインタフェース	LAN, 「IP routing」で選択されたグループもしくはチャネル	LAN, 「IP routing」で選択されたグループもしくはチャネル	○	R

C.9.10 RIPフィルタリング(IF propagate : 最大40エントリ)

参照項 4.5.6

項目	内容	設定範囲	導入時の設定	備考
mode	テーブルのエントリに一致した情報をRIPで送信する／一致しない情報をRIPで送信する	include : 一致した情報 exclude : 一致しない情報	exclude	○ R
項目	内容	設定範囲	導入時の設定	備考
destination address	宛先アドレス	xxx.xxx.xxx.xxxの形式	0.0.0	○ R
mask	マスク	xxx.xxx.xxx.xxxの形式	0.0.0	○ R
interface	送信するインタフェース	LAN, 「IP routing」で選択されたグループもしくはチャネル	LAN, 「IP routing」で選択されたグループもしくはチャネル	○ R

C.9.11 Proxy ARP

参照項 4.5.7

項目	内容	設定範囲	導入時の設定	備考
mode	proxy ARPの動作モード	off : 動作しない response only- forwarding packets : 中継パケットに対してのみ送信 response all packets : 全てのパケットに対して送信	off	R

C.10 OSPFに関する設定

C.10.1 OSPF機能使用有無

参照項 4.5.11(1)

項目	内容	設定範囲	導入時の設定	備考
OSPF mode	OSPF機能の使用の有無	1 use (使用する) 2 not use (使用しない)	2 not use	○ R

C.10.2 OSPFルータID

参照項 4.5.11(2)

項目	内容	設定範囲	導入時の設定	備考
routerID	ルータID	xxx.xxx.xxxxの形式 (0.0.0を除く) または 1~4294967295	LANのIPアドレス と同じ値	○ R

C.10.3 OSPFエリア

参照項 4.5.11(3)

項目	内容	設定範囲	導入時の設定	備考
area ID	エリアID	xxx.xxx.xxxxの形式 (0.0.0を除く) または 1~4294967295	なし	○ R
authtype	ルータ間の認証の有無	none simple	none	○ R
attribute	エリアの属性	not stub stub stub default	not stub	○ R
cost	デフォルトルートのコスト	1~16777215	なし	○ R
interface	エリアに属するインタフェース	LAN, 「IP routing」で 選択されたグループ もしくはチャネル	LAN, 「IP routing」 で選択された グループもしくは チャネル	○ R

C.10.4 OSPFバックボーンエリア

参照項 4.5.11(4)

項目	内容	設定範囲	導入時の設定	備考
backbone	バックボーンエリアの使用の有無	use not use	not use	○ R
authtype	ルータ間の認証の有無	none simple	none	○ R
interface	バックボーンエリアに属する インタフェース	LAN, 「IP routing」で選択され たグループもしくは チャネル, Virtual link	LAN, 「IP routing」で 選択された グループもしくは チャネル	○ R

C.10.5 OSPFネットワーク（最大32エントリ）

参照項 4.5.11(5)

項目	内容	設定範囲	導入時の設定	備考
address	エリアに所属するネットワーク範囲のIPアドレス	xxx.xxx.xxx.xxxの形式	なし	○ R
mask	addressに対するマスク	xxx.xxx.xxx.xxxの形式	なし	○ R
Area ID	エリアID	設定したエリアID (バックボーンエリア含む)	なし	○ R

C.10.6 OSPFスタブホスト（最大16エントリ）

参照項 4.5.11(6)

項目	内容	設定範囲	導入時の設定	備考
address	スタブホストのIPアドレス	xxx.xxx.xxx.xxxの形式	なし	○ R
cost	スタブホストまでのコスト値	1~16777215	なし	○ R
Area ID	エリアID	設定したエリアID (バックボーンエリア含む)	なし	○ R

C.10.7 OSPFインタフェース

参照項 4.5.11(7)

項目	内容	設定範囲	導入時の設定	備考
type	インタフェースのタイプ	broadcast non broadcast	broadcast	○ R
cost	インタフェースのコスト値	1~65535	LAN:10 MSD:781 ISDN:1562	○ R
priority	インタフェースの優先度	0~255	1	○ R
authkey	認証に使用するパスワード	8文字以内の英数字	なし	○ R
transit delay	リンクステートアップデートの送信遅延時間	1~65535 [sec]	1	× R
retransmit interval	隣接ルータとの情報交換パケットの再送間隔	1~65535 [sec]	5	× R
hello interval	Helloパケットの送信間隔	1~65535 [sec]	10	× R
dead interval	隣接ルータがダウンしたと判断するまでの時間	1~65535 [sec]	40	× R
pollinterval	隣接ルータがダウンしたと判断した後のHelloパケットの送信間隔	1~65535 [sec]	120	× R

C.10.8 OSPF隣接ルータ (最大32エントリ)

参照項 4.5.11(8)

項目	内容	設定範囲	導入時の設定	備考	
neighbor	隣接ルータのIPアドレス	xxx.xxx.xxx.xxxの形式	なし	○	R
polalky	隣接ルータを指定ルータとして 運用可/運用不可	eligible not eligible	not eligible	○	R

C.10.9 OSPFバーチャルリンク隣接ルータ (最大8エントリ)

参照項 4.5.11(9)

項目	内容	設定範囲	導入時の設定	備考	
neighbor	隣接ルータのIPアドレス	xxx.xxx.xxx.xxxの形式	なし	○	R
priority	隣接ルータを指定ルータとして 運用可/運用不可	eligible not eligible	not eligible	○	R

C.10.10 OSPFバーチャルリンク (最大8エントリ)

参照項 4.5.11(10)

項目	内容	設定範囲	導入時の設定	備考	
neighbor ID	バーチャルリンクを確立するルータの IPアドレス	xxx.xxx.xxx.xxxの形式	なし	○	R
transit area	バーチャルリンクを確立するルータと の間のエリアID	xxx.xxx.xxx.xxxの形式 (0.0.0.0を除く) または 1~4294967295	なし	○	R
authkey	バーチャルリンクを確立するルータと のパスワード	8文字以内の英数字	なし	○	R
transit delay	リンクステートアップデートの 送信遅延時間	1~65535 [sec]	1	×	R
retransmit interval	バーチャルリンクを確立するルータと の情報交換パケットの再送間隔	1~65535 [sec]	5	×	R
hello interval	Helloパケットの送信間隔	1~65535 [sec]	10	×	R
dead interval	バーチャルリンクを確立するルータが ダウンしたと判断する時間	1~65535 [sec]	40	×	R

C.10.11 RIP export (最大20エントリ)

参照項 4.5.11(11)

項目	内容	設定範囲	導入時の設定	備考	
configuration	ルーティング情報を送信する/ 送信しない	metric:送信する restrict:送信しない	なし	×	R
metric	RIPとして受信するときの メトリック値	1~16	16	×	R
protocol	RIP以外のルーティング情報の プロトコル	ospf ospf ase	ospf	×	R
address format	Announce listのアドレス形式	all network host	なし	×	R
dst address	Announce listの宛先アドレス	0.0.0.0~255.255.255.255	0.0.0.0	×	R
mask	宛先アドレスに対するマスク	0.0.0.1~255.255.255.255	255.255.255.255	×	R

C.10.12 OSPF AS外のルーティング情報

参照項 4.5.11(12)

項目	内容	設定範囲	導入時の設定	備考	
import preference	AS外のルーティング情報が重なった 場合の優先度	0~255	110	×	R
import interval	ルーティング情報を有効にする タイミング	1~65535	1	×	R
import max route	import intervalの間に有効にする 最大ルート数	1~65535	100	×	R
export cost	AS外のルートへのコスト	1~16777215	100	×	R
export tag ospf	AS外のルーティング情報を送信する ときのtagの値	0~2147483647	0	×	R
type	AS外のルーティング情報の 送信タイプ	type1 type2	type1	×	R

C.10.13 OSPF AS外のルーティング情報の受信 (OSPF import : 最大20エントリ)

参照項 4.5.11(13)

項目	内容	設定範囲	導入時の設定	備考	
tag	ルーティング情報を登録するtagの値	0~2147483647, または*(すべてのtag)	*	○	R
configuration	ルーティング情報を登録する/しない	preference restrict	なし	○	R
preference	ルーティング情報の優先度	0~255	0	○	R
address format	Announce listのアドレス形式	all network host	なし	○	R
dst address	Announce listの宛先アドレス	xxx.xxx.xxx.xxxの形式	0.0.0.0	○	R
mask	宛先アドレスに対するマスク	xxx.xxx.xxx.xxxの形式	0.0.0.0	○	R

C.10.14 OSPF AS外のルーティング情報の送信 (OSPF export : 最大20エントリ)

参照項 4.5.11(14)

項目	内容	設定範囲	導入時の設定	備考	
type	AS外のルーティング情報の送信タイプ	type1 type2	type1	○	R
tag	AS外のルーティング情報を送信するときのtagの値	0~2147483647	0	○	R
configuration	AS外のルーティング情報を送信する/しない	cost restrict	なし	○	R
cost	AS外のルーティング情報のコスト	1~16777215	なし	○	R
protocol	AS外のルーティング情報のプロトコル	rip static default	rip	○	R
address format	Announce listのアドレス形式	all network host	なし	○	R
dst address	Announce listの宛先アドレス	xxx.xxx.xxx.xxxの形式	0.0.0.0	○	R
mask	宛先アドレスに対するマスク	xxx.xxx.xxx.xxxの形式	0.0.0.0	○	R

C.11 IPXに関する設定

C.11.1 IPXルーティング

参照項 3.2.13

項目	内容	設定範囲	導入時の設定	備考	
router name	ルータの名称	最大47文字の英数字	自ホスト名	○	R
LAN	network NO	LANのネットワーク番号	8桁の16進数	00000000	○ R
	frame type	LANのフレーム形式	ETHERNET_II ETHERNET_802.3 ETHERNET_802.2 ETHERNET_SNAP	ETHERNET_802.3	○ R
	ticks	LANのtick値	1~65535	1	○ R
WAN	routing interface	ルーティングに使用するインタフェース	「Usual」または「UsualLoad split」を選択したグループもしくはチャネル	通常回線に使用する回線	○ R
	network NO	WAN回線のネットワーク番号	8桁の16進数	00000000	○ R
	frame type	WAN回線のフレーム形式	ETHERNET_II ETHERNET_802.3 ETHERNET_802.2 ETHERNET_SNAP	ETHERNET_802.3	○ R
	ticks	WAN回線のtick値	1~65535	1	○ R
IPX filtering	IPXフィルタリング機能の使用の有無	use : 使用する not use : 使用しない	1	○	R

C.11.2 IPXフィルタリング (forward : 最大128エントリ)

参照項 3.2.15,3.16.3,4.6.10

項目	内容	設定範囲	導入時の設定	備考	
protocol	フィルタリングの対象とするプロトコル	ncp spx netbios unknown all other	unknown	○	§
source host number	フィルタリングの対象とする送信元アドレス	12桁の16進数 または*	*(1)	○	§
source network number	フィルタリングの対象とする送信元ネットワーク番号	8桁の16進数 または*	*(1)	○	§
source mask	送信元ネットワーク番号に対するマスク	8桁の16進数	00000000	○	§
source sock(A)	フィルタリングの対象とする送信元ソケットの開始番号	0000~ffff	0000	○	§
source sock(B)	フィルタリングの対象とする送信元ソケットの終了番号	Aの値~ffff	ffff	○	§
destination host number	フィルタリングの対象とする宛先アドレス	12桁の16進数 または*	*(1)	○	§
destination network number	フィルタリングの対象とする宛先ネットワーク番号	8桁の16進数 または*	*(1)	○	§
destination mask	宛先ネットワーク番号に対するマスク	8桁の16進数	00000000	○	§
destination sock(A)	フィルタリングの対象とする宛先ソケットの開始番号	0000~ffff	0000	○	§
destination sock(B)	フィルタリングの対象とする宛先ソケットの終了番号	Aの値~ffff	ffff	○	§
receive interface	フィルタリング対象の受信インタフェース	LAN, 「IPX routing」で選択されたグループもしくはチャネル	LAN, 「IPX routing」で選択されたグループもしくはチャネル	○	§
send interface	フィルタリング対象の送信インタフェース	LAN, 「IPX routing」で選択されたグループもしくはチャネル	LAN, 「IPX routing」で選択されたグループもしくはチャネル	○	§
mode	エントリモード	half full	full	○	§

導入時にIPXフィルタリング (forward) テーブルに「全てを中継する」エントリを設定してあります。

(1): 「*」は各々の項目の設定範囲の全てを網羅することを示します。

C.11.3 IPXフィルタリング (discard : 最大64エン트리)

参照項 4.6.11

項目	内容	設定範囲	導入時の設定	備考	
protocol	フィルタリングの対象とするプロトコル	nop spx netbios unknown all other	unknown	○	S
source host number	フィルタリングの対象とする送信元アドレス	12桁の16進数 または*	*(1)	○	S
source network number	フィルタリングの対象とする送信元ネットワーク番号	8桁の16進数 または*	*(1)	○	S
source mask	送信元ネットワーク番号に対するマスク	8桁の16進数	00000000	○	S
source sock(A)	フィルタリングの対象とする送信元ソケットの開始番号	0000~ffff	0000	○	S
source sock(B)	フィルタリングの対象とする送信元ソケットの終了番号	Aの値~ffff	ffff	○	S
destination host number	フィルタリングの対象とする宛先アドレス	12桁の16進数 または*	*(1)	○	S
destination network number	フィルタリングの対象とする宛先ネットワーク番号	8桁の16進数 または*	*(1)	○	S
destination mask	宛先ネットワーク番号に対するマスク	8桁の16進数	00000000	○	S
destination sock(A)	フィルタリングの対象とする宛先ソケットの開始番号	0000~ffff	0000	○	S
destination sock(B)	フィルタリングの対象とする宛先ソケットの終了番号	Aの値~ffff	ffff	○	S
receive interface	フィルタリング対象の受信インタフェース	LAN, 「IPX routing」で選択されたグループもしくはチャネル	LAN, 「IPX routing」で選択されたグループもしくはチャネル	○	S
send interface	フィルタリング対象の送信インタフェース	LAN, 「IPX routing」で選択されたグループもしくはチャネル	LAN, 「IPX routing」で選択されたグループもしくはチャネル	○	S
mode	エン트리モード	half full	full	○	S

導入時にIPXフィルタリング (discard) テーブルに「ソケット番号"457"を使用するパケットを中継しない」エントリを設定してあります。

(1): 「*」は各々の項目の設定範囲の全てを網羅することを示します。

C.11.4 RIPインタフェース

参照項 4.6.1

項目	内容	設定範囲	導入時の設定	備考	
send control	interfaceにRIP情報を送信するかどうか	on: 送信する off: 送信しない	off	×	R
recv control	interfaceからRIP情報を受信するかどうか	on: 送信する off: 送信しない	60	×	R
broadcast	RIPの送信方法	on: 定期update off: triggered update	off	×	R
interval	broadcast onの場合RIP送信間隔	60~2147483647 [sec]	60	×	R
ageout	ISDN回線から学習したRIP情報のエージアウト	on: エージアウトする off: エージアウトしない	off	×	R
time	ageout onの場合のエージアウト時間	30~2147483647 [sec]	180	×	R

C.11.5 RIPフィルタリング (最大64エン트리)

参照項 4.6.2

項目	内容	設定範囲	導入時の設定	備考	
mode	テーブルのエン特里に一致した情報を有効にする/一致しない情報を有効にする	include: 一致した情報 exclude: 一致しない情報	exclude	○	R
exclude hop count	この数以上のホップカウントのRIPのエン特里を受信したときはそのエン特里を廃棄	1~16	16	○	R

項目	内容	設定範囲	導入時の設定	備考	
network	ネットワーク番号	8桁の16進数 (00000000を除く)	なし	○	S
mask	マスク	8桁の16進数 (00000000を除く)	なし	○	S

C.11.6 RIPスタティック（最大256エントリ）

参照項 3.2.16,3.16.4,4.6.3

項目	内容	設定範囲	導入時の設定	備考
destination address	宛先ネットワーク番号	8桁の16進数	なし	S
metric	メトリック値	1～16	16	S
time ticks	tick値	1～65535	15	S
gateway network NO.	ゲートウェイのネットワーク番号	8桁の16進数	なし	S
gateway host ID	ゲートウェイのノードID	12桁の16進数	なし	S

C.11.7 SAPインタフェース

参照項 4.6.4

項目	内容	設定範囲	導入時の設定	備考
I S D N 回 線	broadcast	SAPの送信方法 on：定期update off：triggered update	off	× R
	interval	broadcast on の場合SAP送信間隔	60	× R
	ageout	ISDN回線から学習した SAP情報のエージアウト on：エージアウトする off：エージアウトしない	off	× R
	time	ageout on の場合のエージアウト時間	180	× R

C.11.8 SAPフィルタリングモード

参照項 4.6.5

項目	内容	設定範囲	導入時の設定	備考
mode	テーブルのエントリに一致した情報を有効にする / 一致しない情報を有効にする	include：一致した情報 exclude：一致しない情報	exclude	R
exclude hop count	この数以上のホップカウントのSAPのエントリを受信したときはそのエントリを廃棄	1～16	16	R

C.11.9 SAPフィルタリング(address) (最大64エントリ)

参照項 4.6.6

項目	内容	設定範囲	導入時の設定	備考	
network	ネットワーク番号	8桁の16進数 (00000000を除く)	なし	○	S
mask	マスク	8桁の16進数 (00000000を除く)	なし	○	S

C.11.10 SAPフィルタリング(server name) (最大64エントリ)

参照項 4.6.7

項目	内容	設定範囲	導入時の設定	備考	
server name	サーバ名	最大47文字の英数字	なし	○	S

C.11.11 SAPフィルタリング(server type) (最大64エントリ)

参照項 4.6.8

項目	内容	設定範囲	導入時の設定	備考	
service type	フィルタリングの対象とする サーバのサービスタイプ	print queue file server job server print server archive server remote bridge server advertising print server all other (4桁の16進)	other	○	S

C.11.12 SAPスタティック (最大256エントリ)

参照項 3.2.17,3.16.5,4.6.9

項目	内容	設定範囲	導入時の設定	備考	
server name	サーバの名称	47文字以内の英数字	なし	○	§
address(network)	サーバのネットワーク番号 (インターナル)	8桁の16進数	なし	○	§
address(host)	サーバのホスト番号 (インターナル)	12桁の16進数	なし	○	§
socket	ソケット番号	4桁の16進数	なし	○	§
service type	フィルタリング対象とする サーバのサービスタイプ	print queue file server job server print server archive server remote bridge server advertising print server other (4桁の16進数)	なし	○	§
hop to server	サーバまでのホップ数	1~16	16	○	§

C.11.13 IPX frame type

参照項 4.6.12

項目	内容	設定範囲	導入時の設定	備考	
frame type	IPXフレームタイプ	1-ETHERNET-II 2-ETHERNET_802.3 3-ETHERNET_802.2 4-ETHERNET_SNAP	2-ETHERNET_802.2	○	§

C.11.14 Keep Alive

参照項 4.6.13

項目	内容	設定範囲	導入時の設定	備考	
mode	KeepAliveパケットの代理応答 / 要求の動作	use : 動作する not use : 動作しない	use		R
request start indicate timer	代理要求開始指示パケット送信失敗時の再送タイマ	1 ~ 255 [sec]	3	×	R
request start retry count	代理要求開始指示パケット送信失敗時の再送回数	1 ~ 255	10	×	R
request send timer normal	正常時の代理要求送信タイマ	1 ~ 255 [min]	5	×	R
request send timer retry	リトライ時の代理要求送信タイマ	1 ~ 255 [min]	1	×	R
request send retry count	代理要求送信時のリトライ回数	1 ~ 255	10	×	R
response stop indicate timer	代理応答停止指示パケット送信失敗時の再送タイマ	1 ~ 255 [sec]	3	×	R
response stop retry count	代理応答停止指示パケット送信失敗時の再送回数	1 ~ 255	10	×	R
response restart indicate timer	代理応答再開指示パケット送信失敗時の再送タイマ	1 ~ 255 [sec]	3	×	R
response restart retry count	代理応答再開指示パケット送信失敗時の再送回数	1 ~ 255	10	×	R
response end indicate timer	代理応答終了指示パケット送信失敗時の再送タイマ	1 ~ 255 [sec]	3	×	R
response end retry count	代理応答終了指示パケット送信失敗時の再送回数	1 ~ 255	2	×	R
response end timer	代理応答終了のタイマ値	1 ~ 255 [min]	10	×	R

C.12 AppleTalkに関する設定

C.12.1 AppleTalkルーティング

参照項 3.2.18,3.17.1,3.17.2

項目	内容	設定範囲	導入時の設定	備考		
AURP protocol	AURPを使用する／しない	use not use	not use	○	R	
connect to non-configured exterior router	設定されていない外部ルータとAURPの接続を行う／行わない	yes no	no	○	R	
Extra network	突呼用ネットワーク動作制御を使用する／しない	use not use	not use	○	R	
LAN	IP Tunnel	IP Tunnel機能を使用する／しない	use not use	not use	○	R
	seed port	LANをseed portとして動作する／しない	yes no	yes	○	R
	network start	LANのネットワーク番号範囲の始め	1~65279	1	○	R
	network end	LANのネットワーク番号範囲の終わり	1~65279	1	○	R
	number	LANのネットワーク番号	1~65279	1	○	R
WAN	routing interface	ルーティングに使用するインタフェース	「Usual」または「UsualLoad split」を選択したグループもしくはチャネル	「Usual」または「UsualLoad split」を選択したグループもしくはチャネル	○	R
	IP Tunnel	IP Tunnel機能を使用する／しない	use not use	not use	○	R
	remote	WAN回線で接続される相手の形態	router bridge	router	○	R
	seed port	WANをseed portとして動作する／しない	yes no	yes	○	R
	network start	WANのネットワーク番号範囲の始め	1~65279	1	○	R
	network end	WANのネットワーク番号範囲の終わり	1~65279	1	○	R
Select the filtering	DDPフィルタリングを使用する／しない	DDP service nothing	nothing	○	R	

C.12.2 外部AppleTalkルータ

参照項 3.2.20,3.17.4

項目	内容	設定範囲	導入時の設定	備考	
IP Address	IP Tunnelを使用して接続する相手のIPアドレス	xxx.xxx.xxx.xxxの形式	0.0.0.0		R
port	上記相手のポート	LAN, 「IP Tunnel」を使用する グループもしくは チャンネル	なし		R

C.12.3 AppleTalk DDPフィルタリング (forward) (最大64エン트리)

参照項 3.2.21,3.17.5,4.7.6

項目	内容	設定範囲	導入時の設定	備考	
dst network start	フィルタリング対象の宛先ネットワーク番号の始め	0~65535	0	○	§
dst network end	フィルタリング対象の宛先ネットワーク番号の終わり	0~65535	65535	○	§
dst network node	フィルタリング対象の宛先ノードID	0~255	0	○	§
src network start	フィルタリング対象の送信元ネットワーク番号の始め	0~65535	0	○	§
src network end	フィルタリング対象の送信元ネットワーク番号の終わり	0~65535	65535	○	§
src network node	フィルタリング対象の送信元ノードID	0~255	0	○	§
DDP type	フィルタリング対象のプロトコル	RTMP(Rp/Dt) NBP ATP AEP RTMP(Rj) ZIP ADSP all	all	○	§
mode	エン트리モード	full half	full	○	§
receive port	フィルタリング対象の受信ポート	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkレーティングを使用するグループ もしくはチャネル	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkレーティングを使用するグループ もしくはチャネル	○	§
send port	フィルタリング対象の送信ポート	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkレーティングを使用するグループ もしくはチャネル	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkレーティングを使用するグループ もしくはチャネル	○	§

C.12.4 AppleTalk DDPフィルタリング (discard) (最大32エントリ)

参照項 4.7.7

項目	内容	設定範囲	導入時の設定	備考	
dst network start	フィルタリング対象の宛先ネットワーク番号の始め	0~65535	0	○	Ⓢ
dst network end	フィルタリング対象の宛先ネットワーク番号の終わり	0~65535	65535	○	Ⓢ
dst network node	フィルタリング対象の宛先ノードID	0~255	0	○	Ⓢ
src network start	フィルタリング対象の送信元ネットワーク番号の始め	0~65535	0	○	Ⓢ
src network end	フィルタリング対象の送信元ネットワーク番号の終わり	0~65535	65535	○	Ⓢ
src network node	フィルタリング対象の送信元ノードID	0~255	0	○	Ⓢ
DDP type	フィルタリング対象のプロトコル	RTMP(Rp/Dt) NBP ATP AEP RTMP(Rq) ZIP ADSP all	all	○	Ⓢ
mode	エントリモード	full half	full	○	Ⓢ
receive port	フィルタリング対象の受信ポート	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkレーディングを使用するグループ もしくはチャネル	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkレーディングを使用するグループ もしくはチャネル	○	Ⓢ
send port	フィルタリング対象の送信ポート	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkレーディングを使用するグループ もしくはチャネル	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkレーディングを使用するグループ もしくはチャネル	○	Ⓢ

C.12.5 AppleTalkゾーンリスト

参照項 3.2.22,3.17.6

項目	内容	設定範囲	導入時の設定	備考	
zone name	ゾーン名	最大32文字の英数字	なし	○	S
default zone	デフォルトゾーンとする/しない	yes: デフォルトゾーンとする no: デフォルトゾーンとしない	no	○	S

C.12.6 AppleTalkスタティックルーティング

参照項 3.2.23,3.17.7,4.7.2

項目	内容	設定範囲	導入時の設定	備考	
dst network start	宛先ネットワーク番号範囲の始め	1~65535	なし	○	S
dst network end	宛先ネットワーク番号範囲の終わり	1~65535	「dst network start」で設定した数値	○	S
type	中継先ルータのアドレスのタイプ	AppleTalk ISDN index IP Address	なし	○	S
gateway network number	中継先ルータのアドレス	AppleTalk: 選択時 0~65535 ISDN index: 選択時 ISDNリモート ターゲット (最大80エン トリから1エントリ選択) IP Address xxx.xxx.xxx.xxxの形式	なし	○	S
node ID	中継先ルータのノードID	0~254	0	○	S
hop	中継先ルータまでのホップ数	1~15	1	○	S
send port	中継先ルータが存在するポート	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkルーティングを 使用するグループもしくは チャネル	なし	○	S

C.12.7 AppleTalkスタティックゾーン

参照項 3.2.24,3.17.8,4.7.3

項目	内容	設定範囲	導入時の設定	備考	
dst network start	宛先ネットワーク番号の始め	0~65535	0	○	§
dst network end	宛先ネットワーク番号の終わり	0~65535	65535	○	§
zone	スタティックに設定するゾーン名	最大32文字の英数字	なし	○	§

C.12.8 AppleTalkインタフェース

参照項 4.7.1

項目	内容	設定範囲	導入時の設定	備考	
DDP checksum	DDPのチェックサムをつける／つけない	use: チェックサムをつける not use: チェックサムをつけない	not use	×	R
AMT ageout timer	AMTのエージアウトタイマ	1~255 [sec]	1	×	R
AAARP request reply timer	AAARPリクエスト応答監視タイマ	1~255 [sec]	1	×	R
AAARP request retry count	AAARPリクエストの再送回数	1~100 [回]	5	×	R
ATP TReq reply timer	ATPリクエストの応答監視タイマ	1~255 [sec]	3	×	R
ATP TReq reply count	ATPリクエストの再送回数	1~100 [回]	5	×	R
phase 1 bridge	AppleTalk phase 1ブリッジングを行う／行わない	use not use	not use	×	R
ATCP routing protocol	RTMPの送受信を行う／行わない	not use RTMP	RTMP	×	R
routing information offering	ISDN回線に定期的に送信する／送信しない	yes: 送信する no: 送信しない	no	×	R
routing information interval	定期的に送信する間隔	10~4294967 [sec]	10	×	R
routing table aging	エージアウトを行う／行わない	yes no	no	×	R
routing table validity	エージアウトする時間	40~4294967 [sec]	20	×	R

C.12.9 サービスフィルタリング (forward) (最大64エントリ)

参照項 4.7.6

項目	内容	設定範囲	導入時の設定	備考
object name	フィルタリング対象のオブジェクト名	最大32文字の英数字 または「=」	なし	○ S
type name	フィルタリング対象のタイプ名	最大32文字の英数字 または「=」	なし	○ S
filtering port	送信を許可するポート	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkレレーティング を使用するグループ もしくはチャネル	なし	○ S
receive port	受信を許可するポート	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkレレーティング を使用するグループ もしくはチャネル	なし	○ S

C.12.10 サービスフィルタリング (discard) (最大64エントリ)

参照項 4.7.7

項目	内容	設定範囲	導入時の設定	備考
object name	フィルタリング対象のオブジェクト名	最大32文字の英数字 または「=」	なし	○ S
type name	フィルタリング対象のタイプ名	最大32文字の英数字 または「=」	なし	○ S
filtering port	送信を許可するポート	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkレレーティング を使用するグループ もしくはチャネル	なし	○ S
receive port	受信を許可するポート	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkレレーティング を使用するグループ もしくはチャネル	なし	○ S

C.12.11 ゾーンフィルタリング (最大128エン트리)

参照項 4.7.8

項目	内容	設定範囲	導入時の設定	備考	
attribute	エントリに一致したゾーンを見せる/見せない	include: 見せる exclude: 見せない	exclude	○	S
zone name	フィルタリングを行うゾーンの名前	最大32文字の英数字 または「*」	なし	○	S
filter port	フィルタリングを行うポート	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkルーティングを 使用するグループ もしくはチャネル	なし	○	S

C.12.12 ルーティング情報のフィルタリング (accept gateway) (最大32GW × 7エン트리)

参照項 4.7.9

項目	内容	設定範囲	導入時の設定	備考	
attribute	設定された情報を有効にする/ 有効にしない	include: 有効にする exclude: 有効にしない	exclude	○	S
dst network start	宛先ネットワーク番号範囲の 先頭番号	0~65535	なし	○	S
dst network end	宛先ネットワーク番号範囲の 最終番号	0~65535	なし	○	S
type	送信元ルータのアドレスのタイプ	AppleTalk ISDN index IP address other	なし	○	S
gateway network number	ゲートウェイのネットワーク番号	AppleTalk選択時 0~65535 ISDN index選択時 AppleTalkリモート ターゲット (最大80エン トリから1エントリ選択) IP address選択時 xxx.xxx.xxx.xxxの形式	なし	○	S

C.12.13 ルーティング情報のフィルタリング (propagate gateway) (最大32GW x 7エン트리)

参照項 4.7.10

項目	内容	設定範囲	導入時の設定	備考	
attribute	設定された情報を有効にする/ 有効にしない	include : 有効にする exclude : 有効にしない	exclude	○	S
dst network start	宛先ネットワーク番号範囲の 先頭番号	0~65535	なし	○	S
dst network end	宛先ネットワーク番号範囲の 最終番号	0~65535	なし	○	S
type	送信元ルータのアドレスのタイプ	AppleTalk ISDN index IP address other	なし	○	S
gateway network number	ゲートウェイのネットワーク番号	AppleTalk選択時 0~65535 ISDN index選択時 AppleTalkリモート ターゲット (最大80エン トリから1エントリ選択) IP address選択時 xxx.xxx.xxx.xxxの形式	なし	○	S

C.12.14 ルーティング情報のフィルタリング (accept port) (最大40エン트리)

参照項 4.7.11

項目	内容	設定範囲	導入時の設定	備考	
attribute	設定された情報を有効にする/ 有効にしない	include : 有効にする exclude : 有効にしない	exclude	○	S
dst network start	宛先ネットワーク番号範囲の 先頭番号	0~65535	なし	○	S
dst network end	宛先ネットワーク番号範囲の 最終番号	0~65535	なし	○	S
send port	フィルタリング対象の受信 インタフェース	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkルーティングを 使用するグループ もしくはチャネル	なし	○	S

C.12.15 ルーティング情報のフィルタリング (propagate port) (最大40エントリ)

参照項 4.7.12

項目	内容	設定範囲	導入時の設定	備考	
attribute	設定された情報を有効にする/ 有効にしない	include : 有効にする exclude : 有効にしない	exclude	○	S
dst network start	宛先ネットワーク番号範囲の 先頭番号	0~65535	なし	○	S
dst network end	宛先ネットワーク番号範囲の 最終番号	0~65535	なし	○	S
send port	フィルタリング対象の受信 インタフェース	LAN(AppleTalk), LAN(IP Tunnel), AppleTalkルーティングを 使用するグループ もしくはチャネル	なし	○	S

C.12.16 AURPプロトコル

参照項 4.7.13

項目	内容	設定範囲	導入時の設定	備考	
protocol	ルーティングプロトコルを選択	AURP/RTMP RTMP static AURP	AURP	○	R
Tickle packet	Tickle packetを送信する/ 送信しない	use 送信する not use 送信しない	not use	○	R
Tickle packet send time	Tickle packetの定期送信間隔	30~4294967[sec]	90	○	R
send AURP packet any time	AURPパケットを送信する/ しない	yes no	no	○	R
resend openrequest	Open-Reqパケットを再送する/ しない	yes no	yes	○	R
remapping	リマッピングを行う/ 行わない	use not use	not use	○	R
remapping range start	リマッピングをするネットワーク 番号範囲の始め	1 ~ 65279	0	○	R
remapping range end	リマッピングをするネットワーク 番号範囲の終わり	1 ~ 65279	0	○	R
clustering	クラスタリングを行う/ 行わない	use not use	not use	○	R
hop count reduction	ホップカウントの制限 (15hops) を 無視する/ しない	use not use	not use	○	R

C.13 ブリッジに関する設定

C.13.1 ブリッジング

参照項 3.2.26,3.18.2

項目	内容	設定範囲	導入時の設定	備考	
bridging interface	ブリッジングを行うグループもしくはチャンネル	「Usual」または「Usual/Loadsplit」を選択したグループもしくはチャンネル	なし		R
STP	STP機能の使用の有無	use not use	not use		R
static filtering	スタティックフィルタリングの使用の有無	use not use	not use		R

C.13.2 アドレス学習テーブルのエイジアウト時間

参照項 4.3.2

項目	内容	設定範囲	導入時の設定	備考	
agetime	アドレス学習テーブルのエイジアウト時間	10 ~ 1000000 [sec]	300	×	R

C.13.3 ブリッジ最大中継遅延時間

参照項 4.3.3

項目	内容	設定範囲	導入時の設定	備考	
bridge max forward delay	ブリッジングフレームの中継遅延時間	50~400 [10msec]	400	×	R

C.13.4 アドレスフィルタリングのデフォルト

参照項 3.2.27,3.18.3

項目	内容	設定範囲	導入時の設定	備考	
source default	未定義送信元アドレスの処理	forward : 中継する discard : 遮断する	forward		R
destination default	未定義宛先アドレスの処理	forward : 中継する discard : 遮断する	forward		R

C.13.5 送信元アドレスフィルタリング (最大64エントリ)

参照項 3.2.27,3.18.3

項目	内容	設定範囲	導入時の設定	備考
src address	送信元アドレス	xx:xx:xx:xx:xx:xxの形式	00:00:00:00:00:00	○ S
send interface	中継WAN回線	LAN, ブリッジングを使用する グループもしくは チャネル	LAN, ブリッジングを 使用する グループもし くはチャネル	○ S

C.13.6 宛先アドレスフィルタリング (最大64エントリ)

参照項 3.2.28,3.18.3

項目	内容	設定範囲	導入時の設定	備考
destination address	宛先MACアドレス	xx:xx:xx:xx:xx:xxの形式	00:00:00:00:00:00	○ S
send interface	中継WAN回線	LAN, ブリッジングを使用する グループもしくは チャネル	LAN, ブリッジングを 使用する グループもし くはチャネル	○ S

C.13.7 プロトコルフィルタリングのデフォルト

参照項 3.2.29,3.18.4

項目	内容	設定範囲	導入時の設定	備考
default	未定義プロトコルの処理	forward : 中継する discard : 遮断する	forward	R

C.13.8 プロトコルフィルタリング (最大32エントリ)

参照項 3.2.29,3.18.4

項目	内容	設定範囲	導入時の設定	備考	
protocol	プロトコルのタイプ	type dloop	type	○	S
number	プロトコル番号	typeの時は4桁の16進数 dloopの時は2桁の16進数	0000または00	○	S
send interface	中継WAN回線	LAN, ブリッジングを使用する グループもしくは チャネル	LAN, ブリッジングを 使用するグルー プもしくはチャ ネル	○	S

C.13.9 STP

参照項 4.3.1

項目	内容	設定範囲	導入時の設定	備考	
bridge priority	ブリッジ優先度	0~65535	32768	○	R
max age	STP機能のタイムアウト時間	6~40 [sec]	20	×	R
hello time	BPDUPケットの送信タイミング	1~10 [sec]	2	×	R
forward delay	BPDUPケットの監視時間	4~30 [sec]	15	×	R
port priority	各ポートの優先度	0~255	128	×	R
port pathcost	各インタフェースの重み	0~65535	LAN:100 MSD(64Kbps): 15625 MSD(128Kbps): 7813 ISDN:15625	×	R
domain	STPドメインの分離	on: 分離する off: 分離しない	off	×	R

C.13.10 ICMPリダイレクト

参照項 4.4

項目	内容	設定範囲	導入時の設定	備考	
mode	ICMPリダイレクトメッセージによりルーティングテーブルを更新する/しない	on: 更新する off: 更新しない	on	×	R
preference	ICMPリダイレクトメッセージに関する優先順位	0~255	20	×	R
interface	ICMPリダイレクトメッセージを受信するインタフェース	LAN, ブリッジングを使用する グループもしくは チャネル	LAN, ブリッジングを 使用する グループもしくは チャネル	×	S
trust gateways	ICMPリダイレクトメッセージの送信元ゲートウェイ	xxx.xxx.xxx.xxxの形式 (最大10エントリ)	All gateways	○	S

C.14 リモートファイルメンテナンスに関する設定

参照項 4.9

項目	内容	設定範囲	導入時の設定	備考	
server timer11	サーバの、クライアントからの応答待ちタイム	1 ~ 655	5	○	S
server timer12	サーバの、クライアントからの応答リトライタイム	1 ~ 655	25	○	S
client timer11	クライアントの、サーバからの応答待ちタイム	1 ~ 655	5	○	S
client timer12	クライアントの、サーバからの応答リトライタイム	1 ~ 655	25	○	S

C.15 データ圧縮に関する設定

参照項 4.2

項目	内容	設定範囲	導入時の設定	備考	
data compress	データ圧縮の方法	auto (実行) no (非実行) fixed (圧縮固定)	no	○	R

C.16 データ別優先制御に関する設定

C.16.1 パラメータ

参照項 4.10.1

項目	内容	設定範囲	導入時の設定	備考	
packet priority control	データ別優先制御機能の使用の有無	use not use	not use	○	R
band rate high	優先度が「優先」の場合の比率	0 ~ 100	70	○	S
band rate normal	優先度が「通常」の場合の比率	0 ~ 100 - [band rate highの値] 範囲外になる場合は、 範囲内の最大値	20	○	S

C.16.2 IPプロトコル

参照項 4.10.2

項目	内容	設定範囲	導入時の設定	備考	
application	データ別優先制御を行うアプリケーション	telnet ftp-data ftp snmp all other	all	○	S
application number	アプリケーションの番号	0 ~ 65535	0	○	S
protocol	データ別優先制御を行う上位プロトコル	tcp udp icmp ospf all other	all	○	S
protocol number	プロトコルの番号	0 ~ 255	0	○	S
priority	優先度	high normal low	high	○	S

C.16.3 IPアドレス

参照項 4.10.3

項目	内容	設定範囲	導入時の設定	備考	
IP address	データ別優先制御を行うIPアドレス	xxx.xxx.xxx.xxxの形式	なし	○	§
mask	データ別優先制御を行うマスク	xxx.xxx.xxx.xxxの形式	なし	○	§
priority	優先度	high normal low	high	○	§

C.16.4 IPXプロトコル

参照項 4.10.4

項目	内容	設定範囲	導入時の設定	備考	
application	データ別優先制御を行うアプリケーション	nop sap rip netbios diagnostic all other	all	○	§
application number	アプリケーションの番号	0~ffff	0	○	§
protocol	データ別優先制御を行う上位プロトコル	nop spx netbios all other	all	○	§
protocol number	プロトコルの番号	0~ff	0	○	§
priority	優先度	high normal low	high	○	§

C.16.5 IPXアドレス

参照項 4.10.5

項目	内容	設定範囲	導入時の設定	備考	
host number	データ別優先制御を行うホスト番号	12桁の16進数または「*」	*	○	S
network number	データ別優先制御を行うIPXネットワーク番号	8桁の16進数または「*」	*	○	S
mask	データ別優先制御を行うマスク	8桁の16進数	fffffff	○	S
priority	優先度	high normal low	high	○	S

C.16.6 AppleTalkプロトコル

参照項 4.10.6

項目	内容	設定範囲	導入時の設定	備考	
protocol	データ別優先制御を行うプロトコル	RTMP(Rq/Dt) NBP ATP AEP RTMP(Rq) ZIP ADSP all other	all	○	S
protocol number	データ別優先制御を行うアプリケーション番号	0~255	0	○	S
priority	優先度	high normal low	high	○	S

C.16.7 AppleTalkアドレス

参照項 4.10.7

項目	内容	設定範囲	導入時の設定	備考	
network start	データ別優先制御を行うネットワーク番号範囲の始め	0~65535	0	○	§
network end	データ別優先制御を行うネットワーク番号範囲の終わり	0~65535	0	○	§
host	データ別優先制御を行うノードID	0~255または「*」	*	○	§
priority	優先度	high normal low	high	○	§

C.16.8 ブリッジングデータ

参照項 4.10.8

項目	内容	設定範囲	導入時の設定	備考	
dsalink	データ別優先制御を行うデータリンクプロトコル	ethertype dlcap fna	なし	○	§
protocol	プロトコル番号	0 ~ ffff [ethertype選択時] 0 ~ ff [dlcap選択時]	なし	○	§
priority	優先度	high normal low	high	○	§

C.16.9 MACアドレス

参照項 4.10.9

項目	内容	設定範囲	導入時の設定	備考	
MAC address	データ別優先制御を行うMACアドレス	xx:xx:xx:xx:xx:xxの形式	なし	○	§
priority	優先度	high normal low	high	○	§

C.17 トラフィックロギングに関する設定

参照項 4.11.1

項目	内容	設定範囲	導入時の設定	備考	
source traffic log	トラフィックログの対象の選択	IP address recv interface	IP address	○	S
source IP address	送信元IPアドレス	0.0.0.1~255.255.255.255	なし	○	S
source mask	送信元マスク	128.0.0.0~ 255.255.255.255	255.255.255.255	○	S
receive interface	受信するインタフェースの選択	LAN, IPルーティングを使用 するグループもしくは チャネル	なし	○	S
destination traffic log	トラフィックログの対象の選択	IP address dst interface	IP address	○	S
destination IP address	宛先IPアドレス	0.0.0.1~255.255.255.255	なし	○	S
destination mask	宛先マスク	128.0.0.0~ 255.255.255.255	255.255.255.255	○	S
destination interface	送信するインタフェースの選択	LAN, IPルーティングを使用 するグループもしくは チャネル	なし	○	S

C.18 呼確立リミッタに関する設定

C.18.1 連続接続時間呼確立リミッタ

参照項 4.12.1

項目	内容	設定範囲	導入時の設定	備考	
mode	連続呼確立リミッタの動作の有無	on off	on		S
time	連続接続時間の上限值	1 ~ 168 [hour]	12		S

C.18.2 トータル接続時間呼確立リミッタ

参照項 4.12.2

項目	内容	設定範囲	導入時の設定	備考	
mode	呼確立リミッタの使用の有無	on off	off	○	§
time	1ヶ月のISDNの呼確立時間の累計の上限値	1 ~ 744 [hour]	300	○	§

C.19 ルータグループ化機能の設定

参照項 4.14

項目	内容	設定範囲	導入時の設定	備考	
router grouping	ルータグループ化機能の使用の有無	use not use	not use		R
preference	グループルータの個々のルータの優先度	00000000 ~ ffffffff	MACアドレスの下位4バイト		R
UDP port number	UDPポート番号	0 ~ 65535	55555		R
group IP address	グループルータの代表IPアドレス	0.0.0.0 ~ 255.255.255.255 (マージャンアドレスを除く)	なし		R
duplication check timer	重複確認応答パケット待ちタイマ	1 ~ 1000 [100msec]	10		R
Group name	ルータグループに属するグループ	IPルーティングを使用するグループ	なし		R
RIP send count	RIPパケットの連続送信数	0 ~ 127	10		R

付録D 簡易コマンド機能

簡易コマンドには、インフォメーションコマンドとオペレーションコマンドがあります。本付録では、簡易コマンド機能により実行できるコマンド名、実行内容、参照項を表D-1に示します。

表D-1 インフォメーションコマンド一覧

コマンド名	実行内容	参照項
?inf	インフォメーションコマンド名の表示	
ipst	IPインタフェースの情報の表示	6.2.1
ipstt	IPに関する統計情報の表示	6.2.2
iprt	IPルーティングの情報の表示	6.2.3
ipxst	IPXインタフェースの情報の表示	6.4.1
ipxstt	IPXに関する統計情報の表示	6.4.2
ipxrt	IPXルーティング情報の表示	6.4.3
sapinfo	SAP情報の表示	6.4.4
atport	AppleTalkのポートの情報の表示	6.8.1
atstt	AppleTalkに関する統計情報の表示	6.8.2
atrtmp	AppleTalkルーティング情報の表示	6.8.3
atzit	ゾーンリストの表示	6.8.4
atserv	サービスの情報の表示	6.8.5
brist	ブリッジポートの情報の表示	6.5.1
bristt	ブリッジング機能に関する統計情報の表示	6.5.2
chinfo	チャンネルの情報の表示	6.6.1
chstt	チャンネルの統計情報の表示	6.6.2

表D-2 インフォメーションコマンド一覧(つづき)

ospfgen	OSPFに関する一般情報の表示	6.7.1
ospfarea	OSPFエリアの情報の表示	6.7.2
ospflink	OSPFリンク状態の情報の表示	6.7.3
ospfif	OSPFインタフェース情報の表示	6.7.4
ospfvif	OSPFバーチャルリンクのインタフェースの情報の表示	6.7.5
ospfnei	OSPF隣接の重宝の表示	6.7.6
ospfvnei	OSPFバーチャルリンクを確立した相手の情報の表示	6.7.7
limiter	呼確立リミッタの情報の表示	6.9
elog	エラーログの表示	6.10
llog	ラインログの表示	6.11
tlog	トラップログの表示	6.12
trafficlog	トラヒックロギングの情報の表示	6.13

表D-3 オペレーションコマンド一覧

コマンド名	実行内容	参照項
?ope	オペレーションコマンドの表示	
conn	ISDN通常回線の接続	5.2
dconn	ISDN通常回線の切断	5.3
lsplon	ISDNトラヒック分散回線の接続	5.4
lsploff	ISDNトラヒック分散回線の切断	5.5
online	offlineからonlineへの移行	5.6
offline	onlineからofflineへの移行	5.7
limreset	呼確立リミッタのリセットコマンド	5.8
rc	リモートコンソール	5.9
ping	IPのエコーテスト	5.10
ipxecho	IPXのエコーテスト	5.10
atecho	AppleTalkのエコーテスト	5.10
passwd	パスワードの変更	5.11
save	構成定義情報, エラーログの保存	5.12
dump	すべての設定情報の確認	5.13
ftrace	フレームトレース	5.14
led	LEDの消灯制御	5.15
reset	装置の再起動	5.16

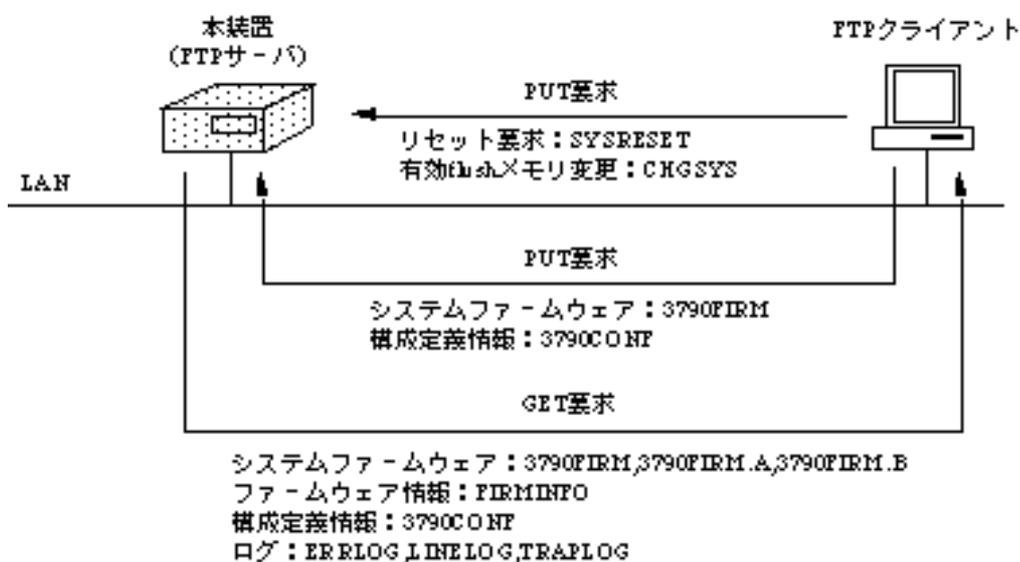
付録E FTPを利用したメンテナンス

本装置では、リモートメンテナンスとして、同一LAN上のホスト（FTPクライアント）からFTPでログインすることができます。FTPでログインすることにより以下の作業を行うことができます。

- システムファームウェアの転送（リードおよびライト）
- 構成定義情報の転送（リードおよびライト）
- ログ（エラーログ、ラインログ、トラップログ）の取得
- 装置のリセット

FTPクライアントから本装置にログインする場合、ログイン名は”root”，パスワードには本装置の管理者資格になるためのパスワードを使用します。パスワードが違う場合、すでに別のクライアントによりログインされている場合および管理者資格になるためのパスワードが設定されていない場合は、ログインすることはできません。

ログインした状態で300秒間何も操作が行われなかった場合、本装置はコネクションを切断します。



本装置とFTPクライアント間で転送できるファイル名およびそのデータの種別を以下に示します。

データファイルの種類	ファイル名	GET	PUT
システムファームウェア	3790FIRM		
システムファームウェア (A面)	3790FIRM.A		×
システムファームウェア (B面)	3790FIRM.B		×
ファームウェア情報	FIRMINFO		×
構成定義情報	3790CONF		
エラーログ	ERRLOG		×
ラインログ	LINELOG		×
トラップログ	TRAPLOG		×
システムリセット	SYSRESET	×	
有効flushメモリ変更	CHGSYS	×	

：使用可能
 ×：使用不可能

ファームウェアのバージョンアップを行う場合の、FTPクライアントの操作方法を示します。

1. FTPクライアントよりFTPで本装置にログインします。
2. 転送モードをバイナリにします。
3. 新しいファームウェアのファイル「3790FIRM」をPUTします。転送されたファームウェアは装置のInactive側のflushメモリに格納されます。
4. 本装置内のファイル「FIRMINFO」をGETしファームウェアが正しいことを確認します（以下の図を参照）。

```
SIDE-A: VALID (Active)
      ID: WAKATO
      EXTID: MEDU
FIRM VER: V01.00
FILE VER: 022096

SIDE-B: VALID (Inactive)
      ID: WAKATO
      EXTID: MEDU
FIRM VER: VN1.00
FILE VER: 121295
```



注意：Inactive側のflushメモリの情報がINVALIDになっているときは、ファームウェアの転送に失敗しています。再度ファームウェアの転送を行ってください。

5. ファイル「SYSRESET」をPUTして装置をリセットしシステムを立ち上げます。
6. 装置が正しく起動されたら、再度FTPでログインした後ファイル「CHGSYS」をPUTし、有効にするflushメモリを変更します。この操作を行わないと、再度装置をリセットしたとき、古いファームウェアが起動されます。



メモ：システムファームウェア（3790FIRM）を装置にPUTする場合、転送を開始するまでに20～30秒かかります。これは、本装置側で、転送されてきたファイルが正しいかの判断や、書き込みの準備をしている時間ですので、そのままにしてお待ちください。



メモ：flushメモリのA側、B側のファームウェアをダウンロードする場合は、それぞれファイル「3790FIRM.A」「3790FIRM.B」をGETします。ファイル「3790FIRM」をGETするとInactive側のファームウェアがダウンロードされます。

付録F MIB一覧表

本装置でサポートを行うMIBのオブジェクト識別子を以下に示します。

internet	OBJECT IDENTIFIER ::= { iso org(3) dod(6) 1 }
directory	OBJECT IDENTIFIER ::= { internet 1 }
mgmt	OBJECT IDENTIFIER ::= { internet 2 }
mib-2	OBJECT IDENTIFIER ::= { mgmt 1 }
system	OBJECT IDENTIFIER ::= { mib-2 1 }
interfaces	OBJECT IDENTIFIER ::= { mib-2 2 }
at	OBJECT IDENTIFIER ::= { mib-2 3 }
ip	OBJECT IDENTIFIER ::= { mib-2 4 }
ipforward	OBJECT IDENTIFIER ::= { ip 24 }
icmp	OBJECT IDENTIFIER ::= { mib-2 5 }
tcp	OBJECT IDENTIFIER ::= { mib-2 6 }
udp	OBJECT IDENTIFIER ::= { mib-2 7 }
transmission	OBJECT IDENTIFIER ::= { mib-2 10 }
dot3	OBJECT IDENTIFIER ::= { transmission 7 }
frame-relay	OBJECT IDENTIFIER ::= { transmission 32 }
snmp	OBJECT IDENTIFIER ::= { mib-2 11 }
appletalk	OBJECT IDENTIFIER ::= { mib-2 13 }
ospf	OBJECT IDENTIFIER ::= { mib-2 14 }
dot1dBridge	OBJECT IDENTIFIER ::= { mib-2 17 }
experimental	OBJECT IDENTIFIER ::= { internet 3 }
private	OBJECT IDENTIFIER ::= { internet 4 }
enterprises	OBJECT IDENTIFIER ::= { private 1 }
furukawa	OBJECT IDENTIFIER ::= { enterprises 246 }



メモ：表の中の「ACCESS」の意味は以下のとおりです。

- R : SNMPマネージャより取得可能な情報
- R/W : SNMPマネージャより取得と設定が可能な情報
- R (CIP) : SNMPマネージャおよびコンソールより取得可能な情報
- R/W (CIP) : SNMPマネージャおよびコンソールより取得および設定が可能な情報



メモ：テーブルのMIBでアンダーラインが引いてあるテーブルは、エントリの追加/削除があることを示します。したがって、エントリの登録がない場合はSNMPマネージャより情報の取得ができません。

F.1 MIB-II (RFC1213)

F.1.1 system グループ

MIB	OID	SYNTAX	ACCESS
sysDescr	system.1	DisplayString	R(CIP)
sysObjectID	system.2	ObjectID	R
sysUpTime	system.3	TimeTicks	R
sysContact	system.4	DisplayString	R/W(CIP)
sysName	system.5	DisplayString	R/W(CIP)
sysLocation	system.6	DisplayString	R/W(CIP)
sysServices	system.7	INTEGER	R

F.1.2 interface グループ

MIB	OID	SYNTAX	ACCESS
ifNumber	interfaces.1	INTEGER	R
ifTable	interfaces.2	Aggregate	--
ifEntry	ifTable.1	Aggregate	--
ifIndex	ifEntry.1	INTEGER	R
ifDescr	ifEntry.2	DisplayString	R
ifType	ifEntry.3	INTEGER	R
ifMtu	ifEntry.4	INTEGER	R
ifSpeed	ifEntry.5	Gauge	W(CIP)
ifPhysAddress	ifEntry.6	OctetString	R(CIP)
ifAdminStatus	ifEntry.7	INTEGER	R/W
ifOperStatus	ifEntry.8	INTEGER	R
ifLastChange	ifEntry.9	TimeTicks	R
ifInOctets	ifEntry.10	Counter	R
ifInUcastPkts	ifEntry.11	Counter	R
ifInNUcastPkts	ifEntry.12	Counter	R
ifInDiscards	ifEntry.13	Counter	R
ifInErrors	ifEntry.14	Counter	R
ifInUnknownProtos	ifEntry.15	Counter	R
ifOutOctets	ifEntry.16	Counter	R
ifOutUcastPkts	ifEntry.17	Counter	R
ifOutNUcastPkts	ifEntry.18	Counter	R
ifOutDiscards	ifEntry.19	Counter	R
ifOutErrors	ifEntry.20	Counter	R
ifOutQLen	ifEntry.21	Gauge	R
ifSpecific	ifEntry.22	ObjectID	R

F.1.3 at グループ

MIB	OID	SYNTAX	ACCESS
atTable	at.1	Aggregate	--
atEntry	atTable.1	Aggregate	--
atIfIndex	atEntry.1	INTEGER	R/W
atPhysAddress	atEntry.2	OctetString	R/W
atNetAddress	atEntry.3	NetworkAddress	R/W

F.1.4 ip グループ

MIB	OID	SYNTAX	ACCESS
ipForwarding	ip.1	INTEGER	R
ipDefaultTTL	ip.2	INTEGER	R
ipInReceives	ip.3	Counter	R(CIP)
ipInHdrErrors	ip.4	Counter	R(CIP)
ipInAddrErrors	ip.5	Counter	R(CIP)
ipForwDatagrams	ip.6	Counter	R(CIP)
ipInUnknownProtos	ip.7	Counter	R
ipInDiscards	ip.8	Counter	R(CIP)
ipInDelivers	ip.9	Counter	R
ipOutRequests	ip.10	Counter	R(CIP)
ipOutDiscards	ip.11	Counter	R(CIP)
ipOutNoRoutes	ip.12	Counter	R(CIP)
ipReasmTimeout	ip.13	INTEGER	R
ipReasmReqds	ip.14	Counter	R
ipReasmOKs	ip.15	Counter	R
ipReasmFails	ip.16	Counter	R
ipFragOKs	ip.17	Counter	R
ipFragFails	ip.18	Counter	R
ipFragCreates	ip.19	Counter	R
ipAddrTable	ip.20	Aggregate	--
ipAddrEntry	ipAddrTable.1	Aggregate	--
ipAdEntAddr	ipAddrEntry.1	IpAddress	R(CIP)
ipAdEntIfIndex	ipAddrEntry.2	INTEGER	R
ipAdEntNetMask	ipAddrEntry.3	IpAddress	R(CIP)
ipAdEntBroadcastAddr	ipAddrEntry.4	INTEGER	R
ipAdEntReasmMbxSize	ipAddrEntry.5	INTEGER	R
<u>ipRouteTable</u>	ip.21	Aggregate	--
ipRouteEntry	ipRouteTable.1	Aggregate	--
ipRouteDest	ipRouteEntry.1	IpAddress	R/W
ipRouteIfIndex	ipRouteEntry.2	INTEGER	R/W
ipRouteMetric1	ipRouteEntry.3	INTEGER	R/W
ipRouteMetric2	ipRouteEntry.4	INTEGER	R/W
ipRouteMetric3	ipRouteEntry.5	INTEGER	R/W
ipRouteMetric4	ipRouteEntry.6	INTEGER	R/W
ipRouteNextHop	ipRouteEntry.7	IpAddress	R/W
ipRouteType	ipRouteEntry.8	INTEGER	R/W
ipRouteProto	ipRouteEntry.9	INTEGER	R
ipRouteAge	ipRouteEntry.10	INTEGER	R/W
ipRouteMsk	ipRouteEntry.11	IpAddress	R/W
ipRouteMetric5	ipRouteEntry.12	INTEGER	R/W
ipRouteInfo	ipRouteEntry.13	ObjectID	R
<u>ipNetToMediaTable</u>	ip.22	Aggregate	--
ipNetToMediaEntry	ipNetToMediaTable.1	Aggregate	--
ipNetToMediaIfIndex	ipNetToMediaEntry.1	INTEGER	R/W
ipNetToMediaPhysAddress	ipNetToMediaEntry.2	OctetString	R/W
ipNetToMediaNetAddress	ipNetToMediaEntry.3	IpAddress	R/W
ipNetToMediaType	ipNetToMediaEntry.4	INTEGER	R/W
ipRoutingDiscards	ip.23	Counter	R(CIP)

F.1.5 ipForward グループ

MIB	OID	SYNTAX	ACCESS
ipForwardNumber	ipForward.1	Gauge	R
ipForwardTable	ipForward.2	Aggregate	--
ipForwardEntry	ipForwardTable.1	Aggregate	--
ipForwardDest	ipForwardEntry.1	IpAddress	R(CIP)
ipForwardMask	ipForwardEntry.2	IpAddress	R(CIP)
ipForwardPolicy	ipForwardEntry.3	INTEGER	R
ipForwardNextHop	ipForwardEntry.4	IpAddress	R(CIP)
ipForwardIfIndex	ipForwardEntry.5	INTEGER	R
ipForwardType	ipForwardEntry.6	INTEGER	R
ipForwardProto	ipForwardEntry.7	INTEGER	R(CIP)
ipForwardAge	ipForwardEntry.8	INTEGER	R
ipForwardInfo	ipForwardEntry.9	ObjectID	R
ipForwardNextHopAS	ipForwardEntry.10	INTEGER	R
ipForwardMetric1	ipForwardEntry.11	INTEGER	R(CIP)
ipForwardMetric2	ipForwardEntry.12	INTEGER	R
ipForwardMetric3	ipForwardEntry.13	INTEGER	R
ipForwardMetric4	ipForwardEntry.14	INTEGER	R
ipForwardMetric5	ipForwardEntry.15	INTEGER	R

F.1.6 icmp グループ

MIB	OID	SYNTAX	ACCESS
icmpInMsgs	icmp.1	Counter	R(CIP)
icmpInErrors	icmp.2	Counter	R(CIP)
icmpInDestUnreschs	icmp.3	Counter	R
icmpInTimeExcds	icmp.4	Counter	R
icmpInParmProbs	icmp.5	Counter	R
icmpInSrcQuenchs	icmp.6	Counter	R
icmpInRedirects	icmp.7	Counter	R
icmpInEchos	icmp.8	Counter	R
icmpInEchoReps	icmp.9	Counter	R
icmpInTimestamps	icmp.10	Counter	R
icmpInTimestampReps	icmp.11	Counter	R
icmpInAddrMasks	icmp.12	Counter	R
icmpInAddrMaskReps	icmp.13	Counter	R
icmpOutMsgs	icmp.14	Counter	R(CIP)
icmpOutErrors	icmp.15	Counter	R(CIP)
icmpOutDestUnreschs	icmp.16	Counter	R
icmpOutTimeExcds	icmp.17	Counter	R
icmpOutParmProbs	icmp.18	Counter	R
icmpOutSrcQuenchs	icmp.19	Counter	R
icmpOutRedirects	icmp.20	Counter	R
icmpOutEchos	icmp.21	Counter	R
icmpOutEchoReps	icmp.22	Counter	R
icmpOutTimestamps	icmp.23	Counter	R
icmpOutTimestampReps	icmp.24	Counter	R
icmpOutAddrMasks	icmp.25	Counter	R
icmpOutAddrMaskReps	icmp.26	Counter	R

F.1.7 tcp グループ

MIB	OID	SYNTAX	ACCESS
tcpRtoAlgorithm	tcp.1	INTEGER	R
tcpRtoMin	tcp.2	INTEGER	R
tcpRtoMax	tcp.3	INTEGER	R
tcpMaxConn	tcp.4	INTEGER	R
tcpActiveOpens	tcp.5	Counter	R
tcpPassiveOpens	tcp.6	Counter	R(CIP)
tcpAttemptFails	tcp.7	Counter	R
tcpIstabResets	tcp.8	Counter	R
tcpCurrIstab	tcp.9	Gauge	R
tcpInSegs	tcp.10	Counter	R(CIP)
tcpOutSegs	tcp.11	Counter	R(CIP)
tcpRetransSegs	tcp.12	Counter	R
tcpConnTable	tcp.13	Aggregate	--
tcpConnEntry	tcpConnTable.1	Aggregate	--
tcpConnState	tcpConnEntry.1	INTEGER	R
tcpConnLocalAddress	tcpConnEntry.2	IpAddress	R
tcpConnLocalPort	tcpConnEntry.3	INTEGER	R
tcpConnRemAddress	tcpConnEntry.4	IpAddress	R
tcpConnRemPort	tcpConnEntry.5	INTEGER	R
tcpInErrs	tcp.14	Counter	R(CIP)
tcpOutRsts	tcp.15	Counter	R

F.1.8 udp グループ

MIB	OID	SYNTAX	ACCESS
udpInDatagrams	udp.1	Counter	R(CIP)
udpNoPorts	udp.2	Counter	R(CIP)
udpInErrors	udp.3	Counter	R(CIP)
udpOutDatagrams	udp.4	Counter	R(CIP)
udpTable	udp.5	Aggregate	--
udpEntry	udpTable.1	Aggregate	--
udpLocalAddress	udpEntry.1	IpAddress	R
udpLocalPort	udpEntry.2	INTEGER	R

F.1.9 snmp グループ

MIB	OID	SYNTAX	ACCESS
snmpInPkts	snmp.1	Counter	R(CIP)
snmpOutPkts	snmp.2	Counter	R(CIP)
snmpInBadVersions	snmp.3	Counter	R
snmpInBadCommunityNames	snmp.4	Counter	R
snmpInBadCommunityUses	snmp.5	Counter	R
snmpInASNParseErrs	snmp.6	Counter	R
snmpInTooBig	snmp.8	Counter	R
snmpInNoSuchNames	snmp.9	Counter	R
snmpInBadValues	snmp.10	Counter	R
snmpInReadOnly	snmp.11	Counter	R
snmpInGenErrs	snmp.12	Counter	R
snmpInTotalReqVars	snmp.13	Counter	R
snmpInTotalSetVars	snmp.14	Counter	R
snmpInGetRequests	snmp.15	Counter	R
snmpInGetNexts	snmp.16	Counter	R
snmpInSetRequests	snmp.17	Counter	R
snmpInGetResponses	snmp.18	Counter	R
snmpInTraps	snmp.19	Counter	R
snmpOutTooBig	snmp.20	Counter	R
snmpOutNoSuchNames	snmp.21	Counter	R
snmpOutBadValues	snmp.22	Counter	R
snmpOutGenErrs	snmp.24	Counter	R
snmpOutGetRequests	snmp.25	Counter	R
snmpOutGetNexts	snmp.26	Counter	R
snmpOutSetRequests	snmp.27	Counter	R
snmpOutGetResponses	snmp.28	Counter	R
snmpOutTraps	snmp.29	Counter	R(CIP)
snmpEnableAuthenTraps	snmp.30	INTEGER	R

F.2 dot3 (RFC1284)

F.2.1 the Ethernet-like Statistics グループ

MIB	OID	SYNTAX	ACCESS
dot3StatsTable	dot3.2	Aggregate	--
dot3StatsEntry	dot3StatsTable.1	Aggregate	--
dot3StatsIndex	dot3StatsEntry.1	INTEGER	R
dot3StatsAlignmentErrors	dot3StatsEntry.2	Counter	R(CIP)
dot3StatsFCSErrors	dot3StatsEntry.3	Counter	R(CIP)
dot3StatsSingleCollisionFrames	dot3StatsEntry.4	Counter	R
dot3StatsMultipleCollisionFrames	dot3StatsEntry.5	Counter	R
dot3StatsSQETestErrors	dot3StatsEntry.6	Counter	R
dot3StatsDeferredTransmissions	dot3StatsEntry.7	Counter	R
dot3StatsLateCollisions	dot3StatsEntry.8	Counter	R
dot3StatsExcessiveCollisions	dot3StatsEntry.9	Counter	R
dot3StatsInternalMacTransmitErrors	dot3StatsEntry.10	Counter	R
dot3StatsCarrierSenseErrors	dot3StatsEntry.11	Counter	R
dot3StatsExcessiveDeferrals	dot3StatsEntry.12	Counter	R
dot3StatsFrameTooLong	dot3StatsEntry.13	Counter	R
dot3StatsInRangeLengthErrors	dot3StatsEntry.14	Counter	R
dot3StatsOutOfRangeLengthFields	dot3StatsEntry.15	Counter	R
dot3StatsInternalMacReceiveErrors	dot3StatsEntry.16	Counter	R

F.2.2 the Ethernet-like Collision Statistics グループ

MIB	OID	SYNTAX	ACCESS
dot3CollTable	dot3.5	Aggregate	--
dot3CollEntry	dot3CollTable.1	Aggregate	--
dot3CollIndex	dot3CollEntry.1	INTEGER	R
dot3CollCount	dot3CollEntry.2	INTEGER	R(CIP)
dot3CollFrequencies	dot3CollEntry.3	Counter	R(CIP)

F.3 appletalk (RFC1243)

MIB	OID	SYNTAX	ACCESS
arpTable	arp.1	Aggregate	--
arpEntry	arpTable.1	Aggregate	--
arpIfIndex	arpEntry.1	INTEGER	R
arpPhysAddress	arpEntry.2	OctetString	R
arpNetAddress	arpEntry.3	OctetString	R
atportTable	atport.1	Aggregate	--
atportEntry	atportTable.1	Aggregate	--
atportIndex	atportEntry.1	INTEGER	R(CIP)
atportDescr	atportEntry.2	DisplayString	R(CIP)
atportType	atportEntry.3	INTEGER	R/W(CIP)
atportNetStart	atportEntry.4	OctetString	R/W(CIP)
atportNetEnd	atportEntry.5	OctetString	R/W(CIP)
atportNetAddress	atportEntry.6	OctetString	R/W(CIP)
atportStatus	atportEntry.7	INTEGER	R/W(CIP)
atportNetConfig	atportEntry.8	INTEGER	R(CIP)
atportZoneConfig	atportEntry.9	INTEGER	R(CIP)
atportZone	atportEntry.10	OctetString	R/W(CIP)
atportIfIndex	atportEntry.11	INTEGER	R/W(CIP)
ddpOutRequests	ddp.1	Counter	R(CIP)
ddpOutShorts	ddp.2	Counter	R
ddpOutLongs	ddp.3	Counter	R
ddpInReceives	ddp.4	Counter	R(CIP)
ddpForwRequests	ddp.5	Counter	R(CIP)
ddpInLocalDatagrams	ddp.6	Counter	R
ddpNoProtocolHandlers	ddp.7	Counter	R
ddpOutNoRoutes	ddp.8	Counter	R(CIP)
ddpTooShortErrors	ddp.9	Counter	R(CIP)
ddpTooLongErrors	ddp.10	Counter	R(CIP)
ddpBroadcastErrors	ddp.11	Counter	R(CIP)
ddpShortDDPErrors	ddp.12	Counter	R(CIP)
ddpHopCountErrors	ddp.13	Counter	R(CIP)
ddpChecksumErrors	ddp.14	Counter	R(CIP)
rtmpTable	rtmp.1	Aggregate	--
rtmpEntry	rtmpTable.1	Aggregate	--
rtmpRangeStart	rtmpEntry.1	OctetString	R/W(CIP)
rtmpRangeEnd	rtmpEntry.2	OctetString	R/W(CIP)
rtmpNextHop	rtmpEntry.3	OctetString	R/W(CIP)
rtmpType	rtmpEntry.4	INTEGER	R/W
rtmpPort	rtmpEntry.5	INTEGER	R/W(CIP)
rtmpHops	rtmpEntry.6	INTEGER	R/W(CIP)
rtmpState	rtmpEntry.7	INTEGER	R/W

MIB	OID	SYNTAX	ACCESS
zipTable	zip.1	Aggregate	--
zipEntry	zipTable.1	Aggregate	--
zipZoneName	zipEntry.1	OctetString	R/W
zipZoneIndex	zipEntry.2	INTEGER	R
zipZoneNetStart	zipEntry.3	OctetString	R/W
zipZoneNetEnd	zipEntry.4	OctetString	R/W
zipZoneState	zipEntry.5	INTEGER	R/W
stechoRequests	stecho.1	Counter	R(CIP)
stechoReplies	stecho.2	Counter	R(CIP)

F.4 ospf (RFC1253)

MIB	OID	SYNTAX	ACCESS
ospfRouterId	ospfGeneralGroup.1	IpAddress	R/W
ospfAdminStat	ospfGeneralGroup.2	INTEGER	R/W
ospfVersionNumber	ospfGeneralGroup.3	INTEGER	R
ospfAreaBdrRtrStatus	ospfGeneralGroup.4	INTEGER	R
ospfASBdrRtrStatus	ospfGeneralGroup.5	INTEGER	R/W
ospfExternLSACount	ospfGeneralGroup.6	Gauge	R(CIP)
ospfExternLSACksumSum	ospfGeneralGroup.7	INTEGER	R(CIP)
ospfTOSsupport	ospfGeneralGroup.8	INTEGER	R/W
ospfOriginateNewLSAs	ospfGeneralGroup.9	Counter	R(CIP)
ospfRxNewLSAs	ospfGeneralGroup.10	Counter	R(CIP)
ospfAreaTable	ospf.2	Aggregate	--
ospfAreaEntry	ospfAreaTable.1	Aggregate	--
ospfAreaId	ospfAreaEntry.1	IpAddress	R/W(CIP)
ospfAuthType	ospfAreaEntry.2	INTEGER	R/W
ospfImportASExtern	ospfAreaEntry.3	INTEGER	R/W
ospfSpfRuns	ospfAreaEntry.4	Counter	R(CIP)
ospfAreaBdrRtrCount	ospfAreaEntry.5	Gauge	R(CIP)
ospfASBdrRtrCount	ospfAreaEntry.6	Gauge	R(CIP)
ospfAreaLSACount	ospfAreaEntry.7	Gauge	R(CIP)
ospfAreaLSACksumSum	ospfAreaEntry.8	INTEGER	R(CIP)
ospfStubAreaTable	ospf.3	Aggregate	--
ospfStubAreaEntry	ospfStubAreaTable.1	Aggregate	--
ospfStubAreaID	ospfStubAreaEntry.1	IpAddress	R/W
ospfStubTOS	ospfStubAreaEntry.2	INTEGER	R/W
ospfStubMetric	ospfStubAreaEntry.3	INTEGER	R/W
ospfStubStatus	ospfStubAreaEntry.4	INTEGER	R/W

MIB	OID	SYNTAX	ACCESS
ospfLsdbTable	ospf.4	Aggregate	--
ospfLsdbEntry	ospfLsdbTable.1	Aggregate	--
ospfLsdbAreaId	ospfLsdbEntry.1	IpAddress	R(CIP)
ospfLsdbType	ospfLsdbEntry.2	INTEGER	R(CIP)
ospfLsdbLSID	ospfLsdbEntry.3	IpAddress	R(CIP)
ospfLsdbRouterId	ospfLsdbEntry.4	IpAddress	R(CIP)
ospfLsdbSequence	ospfLsdbEntry.5	INTEGER	R(CIP)
ospfLsdbAge	ospfLsdbEntry.6	INTEGER	R(CIP)
ospfLsdbChecksum	ospfLsdbEntry.7	INTEGER	R(CIP)
ospfLsdbAdvertisement	ospfLsdbEntry.8	OctetString	R
ospfAreaRangeTable	ospf.5	Aggregate	--
ospfAreaRangeEntry	ospfAreaRangeTable.1	Aggregate	--
ospfAreaRangeAreaID	ospfAreaRangeEntry.1	IpAddress	R/W
ospfAreaRangeNet	ospfAreaRangeEntry.2	IpAddress	R/W
ospfAreaRangeMask	ospfAreaRangeEntry.3	IpAddress	R/W
ospfAreaRangeStatus	ospfAreaRangeEntry.4	INTEGER	R/W
ospfHostTable	ospf.6	Aggregate	--
ospfHostEntry	ospfHostTable.1	Aggregate	--
ospfHostIpAddress	ospfHostEntry.1	IpAddress	R/W
ospfHostTOS	ospfHostEntry.2	INTEGER	R/W
ospfHostMetric	ospfHostEntry.3	INTEGER	R/W
ospfHostStatus	ospfHostEntry.4	INTEGER	R/W
ospfIfTable	ospf.7	Aggregate	--
ospfIfEntry	ospfIfTable.1	Aggregate	--
ospfIfIpAddress	ospfIfEntry.1	IpAddress	R/W(CIP)
ospfAddressLessIf	ospfIfEntry.2	INTEGER	R/W(CIP)
ospfIfAreaId	ospfIfEntry.3	IpAddress	R/W
ospfIfType	ospfIfEntry.4	INTEGER	R/W
ospfIfAdminStat	ospfIfEntry.5	INTEGER	R/W
ospfIfRtrPriority	ospfIfEntry.6	INTEGER	R/W
ospfIfTransitDelay	ospfIfEntry.7	INTEGER	R/W
ospfIfRetransInterval	ospfIfEntry.8	INTEGER	R/W
ospfIfHelloInterval	ospfIfEntry.9	INTEGER	R/W
ospfIfRtrDeadInterval	ospfIfEntry.10	INTEGER	R/W
ospfIfPollInterval	ospfIfEntry.11	INTEGER	R/W
ospfIfState	ospfIfEntry.12	INTEGER	R(CIP)
ospfIfDesignatedRouter	ospfIfEntry.13	IpAddress	R(CIP)
ospfIfBackupDesignatedRouter	ospfIfEntry.14	IpAddress	R(CIP)
ospfIfEvents	ospfIfEntry.15	Counter	R(CIP)
ospfIfAuthKey	ospfIfEntry.16	OctetString	R/W
ospfIfMetricTable	ospf.8	Aggregate	--
ospfIfMetricEntry	ospfIfMetricTable.1	Aggregate	--
ospfIfMetricIpAddress	ospfIfMetricEntry.1	IpAddress	R/W
ospfIfMetricAddressLessIf	ospfIfMetricEntry.2	INTEGER	R/W
ospfIfMetricTOS	ospfIfMetricEntry.3	INTEGER	R/W
ospfIfMetricMetric	ospfIfMetricEntry.4	INTEGER	R/W
ospfIfMetricStatus	ospfIfMetricEntry.5	INTEGER	R/W

MIB	OID	SYNTAX	ACCESS
ospfVirtIfTable	ospf.9	Aggregate	--
ospfVirtIfEntry	ospfVirtIfTable.1	Aggregate	--
ospfVirtIfAreaID	ospfVirtIfEntry.1	IpAddress	R/W(CIP)
ospfVirtIfNeighbor	ospfVirtIfEntry.2	IpAddress	R/W(CIP)
ospfVirtIfTransitDelay	ospfVirtIfEntry.3	INTEGER	R/W
ospfVirtIfRetransInterval	ospfVirtIfEntry.4	INTEGER	R/W
ospfVirtIfHelloInterval	ospfVirtIfEntry.5	INTEGER	R/W
ospfVirtIfRtrDeadInterval	ospfVirtIfEntry.6	INTEGER	R/W
ospfVirtIfState	ospfVirtIfEntry.7	INTEGER	R(CIP)
ospfVirtIfEvents	ospfVirtIfEntry.8	Counter	R(CIP)
ospfVirtIfAuthKey	ospfVirtIfEntry.9	OctetString	R/W
ospfVirtIfStatus	ospfVirtIfEntry.10	INTEGER	R/W
ospfNbrTable	ospf.10	Aggregate	--
ospfNbrEntry	ospfNbrTable.1	Aggregate	--
ospfNbrIpAddr	ospfNbrEntry.1	IpAddress	R/W(CIP)
ospfNbrAddressLessIndex	ospfNbrEntry.2	INTEGER	R/W
ospfNbrRtrId	ospfNbrEntry.3	IpAddress	R(CIP)
ospfNbrOptions	ospfNbrEntry.4	INTEGER	R
ospfNbrPriority	ospfNbrEntry.5	INTEGER	R/W
ospfNbrState	ospfNbrEntry.6	INTEGER	R(CIP)
ospfNbrEvents	ospfNbrEntry.7	Counter	R(CIP)
ospfNbrLSRetransQLen	ospfNbrEntry.8	Gauge	R
ospfNbrMbrStatus	ospfNbrEntry.9	INTEGER	R/W
ospfVirtNbrTable	ospf.11	Aggregate	--
ospfVirtNbrEntry	ospfVirtNbrTable.1	Aggregate	--
ospfVirtNbrArea	ospfVirtNbrEntry.1	IpAddress	R(CIP)
ospfVirtNbrRtrId	ospfVirtNbrEntry.2	IpAddress	R(CIP)
ospfVirtNbrIpAddr	ospfVirtNbrEntry.3	IpAddress	R(CIP)
ospfVirtNbrOptions	ospfVirtNbrEntry.4	INTEGER	R
ospfVirtNbrState	ospfVirtNbrEntry.5	INTEGER	R(CIP)
ospfVirtNbrEvents	ospfVirtNbrEntry.6	Counter	R(CIP)
ospfVirtNbrLSRetransQLen	ospfVirtNbrEntry.7	Gauge	R

F.5 dot1dBridge (RFC1286)

RFC1286に定義されているMIBを以下に示します。

```
dot1dBridge OBJECT IDENTIFIER ::= { mib-2 17 }

-- groups in the Bridge MIB

dot1dBase OBJECT IDENTIFIER ::= { dot1dBridge 1 }

dot1dStp OBJECT IDENTIFIER ::= { dot1dBridge 2 }

dot1dTp OBJECT IDENTIFIER ::= { dot1dBridge 4 }

dot1dStatic OBJECT IDENTIFIER ::= { dot1dBridge 5 }
```

F.5.1 dot1dBase グループ

MIB	OID	SYNTAX	ACCESS
dot1dBaseBridgeAddress	dot1dBase.1	OctetString	R(NV)
dot1dBaseNumPorts	dot1dBase.2	INTEGER	R
dot1dBaseType	dot1dBase.3	INTEGER	R
dot1dBasePortTable	dot1dBase.4	Aggregate	--
dot1dBasePortEntry	dot1dBasePortTable.1	Aggregate	--
dot1dBasePort	dot1dBasePortEntry.1	INTEGER	R
dot1dBasePortIfIndex	dot1dBasePortEntry.2	INTEGER	R
dot1dBasePortCircuit	dot1dBasePortEntry.3	ObjectID	R
dot1dBasePortDelayExceededDiscards	dot1dBasePortEntry.4	Counter	R(CIP)
dot1dBasePortMtuExceededDiscards	dot1dBasePortEntry.5	Counter	R

F.5.2 dot1dStp グループ

MIB	OID	SYNTAX	ACCESS
dot1dStpProtocolSpecification	dot1dStp.1	INTEGER	R
dot1dStpPriority	dot1dStp.2	INTEGER	R/W(CIP)
dot1dStpTimeSinceTopologyChange	dot1dStp.3	TimeTicks	R
dot1dStpTopChanges	dot1dStp.4	Counter	R(CIP)
dot1dStpDesignatedRoot	dot1dStp.5	OctetString	R
dot1dStpRootCost	dot1dStp.6	INTEGER	R
dot1dStpRootPort	dot1dStp.7	INTEGER	R
dot1dStpMaxAge	dot1dStp.8	INTEGER	R/W
dot1dStpHelloTime	dot1dStp.9	INTEGER	R/W
dot1dStpHoldTime	dot1dStp.10	INTEGER	R
dot1dStpForwardDelay	dot1dStp.11	INTEGER	R/W
dot1dStpBridgeMaxAge	dot1dStp.12	INTEGER	R/W(CIP)
dot1dStpBridgeHelloTime	dot1dStp.13	INTEGER	R/W(CIP)
dot1dStpBridgeForwardDelay	dot1dStp.14	INTEGER	R/W(CIP)
dot1dStpPortTable	dot1dStp.15	Aggregate	--
dot1dStpPortEntry	dot1dStpPortTable.1	Aggregate	--
dot1dStpPort	dot1dStpPortEntry.1	INTEGER	R
dot1dStpPortPriority	dot1dStpPortEntry.2	INTEGER	R/W(CIP)
dot1dStpPortState	dot1dStpPortEntry.3	INTEGER	R(CIP)
dot1dStpPortInable	dot1dStpPortEntry.4	INTEGER	R/W
dot1dStpPortPathCost	dot1dStpPortEntry.5	INTEGER	R/W(CIP)
dot1dStpPortDesignatedRoot	dot1dStpPortEntry.6	OctetString	R
dot1dStpPortDesignatedCost	dot1dStpPortEntry.7	INTEGER	R
dot1dStpPortDesignatedBridge	dot1dStpPortEntry.8	OctetString	R
dot1dStpPortDesignatedPort	dot1dStpPortEntry.9	OctetString	R
dot1dStpPortForwardTransitions	dot1dStpPortEntry.10	Counter	R

F.5.3 dot1dTp グループ

MIB	OID	SYNTAX	ACCESS
dot1dTpLearnedEntryDiscards	dot1dTp.1	Counter	R(CIP)
dot1dTpAgingTime	dot1dTp.2	INTEGER	R/W(CIP)
dot1dTpFdbTable	dot1dTp.3	Aggregate	--
dot1dTpFdbEntry	dot1dTpFdbTable.1	Aggregate	--
dot1dTpFdbAddress	dot1dTpFdbEntry.1	OctetString	R
dot1dTpFdbPort	dot1dTpFdbEntry.2	INTEGER	R
dot1dTpFdbStatus	dot1dTpFdbEntry.3	INTEGER	R
dot1dTpPortTable	dot1dTp.4	Aggregate	--
dot1dTpPortEntry	dot1dTpPortTable.1	Aggregate	--
dot1dTpPort	dot1dTpPortEntry.1	INTEGER	R
dot1dTpPortMaxInfo	dot1dTpPortEntry.2	INTEGER	R
dot1dTpPortInFrames	dot1dTpPortEntry.3	Counter	R(CIP)
dot1dTpPortOutFrames	dot1dTpPortEntry.4	Counter	R(CIP)
dot1dTpPortInDiscards	dot1dTpPortEntry.5	Counter	R(CIP)

F.5.4 dot1dStatic グループ

MIB	OID	SYNTAX	ACCESS
<u>dot1dStaticTable</u>	dot1dStatic.1	Aggregate	--
dot1dStaticEntry	dot1dStaticTable.1	Aggregate	--
dot1dStaticAddress	dot1dStaticEntry.1	OctetString	R/W(CIP)
dot1dStaticReceivePort	dot1dStaticEntry.2	INTEGER	R/W(CIP)
dot1dStaticAllowedToGoTo	dot1dStaticEntry.3	OctetString	R/W(CIP)
dot1dStaticStatus	dot1dStaticEntry.4	INTEGER	R/W(CIP)

F.6 装置拡張MIB

装置拡張MIBのツリー構造を以下に示します。

```

furukawa    OBJECT IDENTIFIER ::= { enterprises 246 }

products    OBJECT IDENTIFIER ::= { furukawa 1 }
temporary   OBJECT IDENTIFIER ::= { furukawa 2 }

infonet     OBJECT IDENTIFIER ::= { products 1 }

tmpTransmission OBJECT IDENTIFIER ::= { temporary 1 }
tmpProtocol  OBJECT IDENTIFIER ::= { temporary 2 }

infonetBase      OBJECT IDENTIFIER ::= { infonet 1 }
infonetBrouter   OBJECT IDENTIFIER ::= { infonet 2 }
infonetBridge    OBJECT IDENTIFIER ::= { infonet 3 }
infonetRepeater  OBJECT IDENTIFIER ::= { infonet 4 }
infonetChannel   OBJECT IDENTIFIER ::= { infonet 5 }
infonetPort      OBJECT IDENTIFIER ::= { infonet 6 }
infonetTarget    OBJECT IDENTIFIER ::= { infonet 7 }
infonetFrames    OBJECT IDENTIFIER ::= { infonet 8 }

infonetSystem      OBJECT IDENTIFIER ::= { infonetBase 1 }
infonetSystemError OBJECT IDENTIFIER ::= { infonetBase 2 }

infonetBridgeBase  OBJECT IDENTIFIER ::= { infonetBridge1 }
infonetBridgePort  OBJECT IDENTIFIER ::= { infonetBridge2 }
infonetBridgeStatic OBJECT IDENTIFIER ::= { infonetBridge3 }
infonetBridgeProtocol OBJECT IDENTIFIER ::= { infonetBridge4 }

infChannel          OBJECT IDENTIFIER ::= { infonetChannel1 }

infPortExt1         OBJECT IDENTIFIER ::= { infonetPort 1 }
infTarget           OBJECT IDENTIFIER ::= { infonetTarget1 }
infCallLimiter      OBJECT IDENTIFIER ::= { infonetTarget2 }

infAddress          OBJECT IDENTIFIER ::= { infonetFrames 4 }
infAdlp             OBJECT IDENTIFIER ::= { infAddress 1 }

tmpHighSuperDigital OBJECT IDENTIFIER ::= { tmpTransmission 1 }
tmpIsdn-c           OBJECT IDENTIFIER ::= { tmpTransmission 3 }

tmpPpp             OBJECT IDENTIFIER ::= { tmpProtocol 1 }
exttmpPpp          OBJECT IDENTIFIER ::= { tmpProtocol 2 }

tmpPppLinkControlTable OBJECT IDENTIFIER ::= { tmpPpp 1 }
tmpPppLinkStatusTable  OBJECT IDENTIFIER ::= { tmpPpp 2 }
tmpPppLinkErrorsTable  OBJECT IDENTIFIER ::= { tmpPpp 3 }
tmpPppTests             OBJECT IDENTIFIER ::= { tmpPpp 6 }

tmpPppEchoTest       OBJECT IDENTIFIER ::= { tmpPppTests 1 }

exttmpPppLinkControlTable OBJECT IDENTIFIER ::= { exttmpPpp 1 }
exttmpPppLcpTable      OBJECT IDENTIFIER ::= { exttmpPpp 2 }
exttmpPppBncpTable     OBJECT IDENTIFIER ::= { exttmpPpp 3 }
exttmpPppMbcTable      OBJECT IDENTIFIER ::= { exttmpPpp 4 }
exttmpPppDotldTable    OBJECT IDENTIFIER ::= { exttmpPpp 5 }

```

```

tmpPpp                OBJECT IDENTIFIER ::= { tmpProtocol 1 }
extmpPpp              OBJECT IDENTIFIER ::= { tmpProtocol 2 }

tmpPppLinkControlTable OBJECT IDENTIFIER ::= { tmpPpp 1 }
tmpPppLinkStatusTable OBJECT IDENTIFIER ::= { tmpPpp 2 }
tmpPppLinkErrorsTable OBJECT IDENTIFIER ::= { tmpPpp 3 }
tmpPppTests           OBJECT IDENTIFIER ::= { tmpPpp 6 }

tmpPppIchoTest        OBJECT IDENTIFIER ::= { tmpPppTests 1 }

extmpPppLinkControlTable OBJECT IDENTIFIER ::= { extmpPpp 1 }
extmpPppLcpTable      OBJECT IDENTIFIER ::= { extmpPpp 2 }
extmpPppBcpTable      OBJECT IDENTIFIER ::= { extmpPpp 3 }
extmpPppMbcTable      OBJECT IDENTIFIER ::= { extmpPpp 4 }
extmpPppDotldTable    OBJECT IDENTIFIER ::= { extmpPpp 5 }

```

F.6.1 中継装置共通の拡張MIB

(1) infonetSystem グループ

MIB	OID	SYNTAX	ACCESS
infResetSystem	infonetSystem.1	INTEGER	R/W
infSaveConfig	infonetSystem.2	INTEGER	R/W
infSlotCapacity	infonetSystem.4	INTEGER	R
infSlotMbp	infonetSystem.5	OctetString	R
infCurrentTime	infonetSystem.6	DisplayString	R/W
<u>infMgrTable</u>	infonetSystem.11	Aggregate	--
infMgrEntry	infMgrTable.1	Aggregate	--
infMgrIndex	infMgrEntry.1	INTEGER	R/W
infMgrIpAddress	infMgrEntry.2	IpAddress	R/W(CIP)
infMgrCommunityName	infMgrEntry.3	DisplayString	R/W(CIP)
infMgrType	infMgrEntry.4	INTEGER	R/W(CIP)
infMgrStatus	infMgrEntry.5	INTEGER	R/W

(2) infonetSystemError グループ

MIB	OID	SYNTAX	ACCESS
infSystemErrorPoint	infonetSystemError.1	OctetString	R
infSystemErrorText1	infonetSystemError.2	DisplayString	R
infSystemErrorText2	infonetSystemError.3	DisplayString	R
infSystemErrorText3	infonetSystemError.4	DisplayString	R
infSystemErrorText4	infonetSystemError.5	DisplayString	R
infSystemErrorText5	infonetSystemError.6	DisplayString	R
infSystemErrorText6	infonetSystemError.7	DisplayString	R
infSystemErrorText7	infonetSystemError.8	DisplayString	R
infSystemErrorText8	infonetSystemError.9	DisplayString	R
infSystemErrorText9	infonetSystemError.10	DisplayString	R
infSystemErrorText10	infonetSystemError.11	DisplayString	R
infSystemErrorText11	infonetSystemError.12	DisplayString	R
infSystemErrorText12	infonetSystemError.13	DisplayString	R
infSystemErrorText13	infonetSystemError.14	DisplayString	R
infSystemErrorText14	infonetSystemError.15	DisplayString	R
infSystemErrorText15	infonetSystemError.16	DisplayString	R
infSystemErrorText16	infonetSystemError.17	DisplayString	R
infSystemErrorText17	infonetSystemError.18	DisplayString	R
infSystemErrorText18	infonetSystemError.19	DisplayString	R
infSystemErrorText19	infonetSystemError.20	DisplayString	R
infSystemErrorText20	infonetSystemError.21	DisplayString	R

F.6.2 ブリッジ固有の拡張MIB

(1) infonetBridgeBase グループ

MIB	OID	SYNTAX	ACCESS
infBriBaseStpStatus	infonetBridgeBase.1	INTEGER	R/W(CIP)
infBriBaseMaxForwardDelay	infonetBridgeBase.2	INTEGER	R/W(CIP)

(2) infonetBridgePort グループ

MIB	OID	SYNTAX	ACCESS
<u>infBriPortTable</u>	infonetinfBridgePort.1	Aggregate	--
infBriPortEntry	infBriPortTable.1	Aggregate	--
infBriPortIndex	infBriPortEntry.1	INTEGER	R
infBriPortStatus	infBriPortEntry.2	INTEGER	R/W
infBriPortDatalinkProtocol	infBriPortEntry.3	INTEGER	R
infBriPortReservedDatalinkProtocol	infBriPortEntry.4	INTEGER	R/W
infBriPortSnapTranslation	infBriPortEntry.5	INTEGER	R/W
infBriPortSelectiveTranslation	infBriPortEntry.6	OctetString	R/W

(3) infonetBridgeStatic グループ

MIB	OID	SYNTAX	ACCESS
<u>infBriStaticTable</u>	infonetStatic.1	Aggregate	--
infBriStaticEntry	infBriStaticTable.1	Aggregate	--
infBriStaticSourceAddress	infBriStaticEntry.1	PhysAddress	R/W
infBriStaticReceivePort	infBriStaticEntry.2	INTEGER	R/W
infBriStaticAllowedToGoTo	infBriStaticEntry.3	OctetString	R/W
infBriStaticStatus	infBriStaticEntry.4	INTEGER	R/W
infBriStaticDefault	infBridgeStatic.2	INTEGER	R/W
<u>infBriStaticG1Table</u>	infBridgeStatic.3	Aggregate	--
infBriStaticG1Entry	infBriStaticG1Table.1	Aggregate	--
infBriStaticG1ReceivePort	infBriStaticG1Entry.1	INTEGER	R/W
infBriStaticG1aAllowedToGoTo	infBriStaticG1Entry.2	OctetString	R/W
infBriStaticG1bAllowedToGoTo	infBriStaticG1Entry.3	OctetString	R/W
infBriStaticG1Status	infBriStaticG1Entry.4	INTEGER	R/W

(4) infonetBridgeProtocol グループ

MIB	OID	SYNTAX	ACCESS
<u>infBriProtocolTable</u>	infonetProtocol.1	Aggregate	--
infBriProtocolEntry	infBriProtocolTable.1	Aggregate	--
infBriProtocol	infBriProtocolEntry.1	OctetString	R/W
infBriProtocolReceivePort	infBriProtocolEntry.2	INTEGER	R/W
infBriProtocolAllowedToGoTo	infBriProtocolEntry.3	OctetString	R/W
infBriProtocolStatus	infBriProtocolEntry.4	INTEGER	R/W
infBriProtocolDefault	infBridgeProtocol.2	INTEGER	R/W

F.6.3 中継装置のインタフェース

(1) infChannel グループ

MIB	OID	SYNTAX	ACCESS
infChTable	infChannel.1	Aggregate	--
infChEntry	infChTable.1	Aggregate	--
infChIndex	infChEntry.1	INTEGER	R
infChTypeExtension	infChEntry.2	OctetString	R
infChSlotNumber	infChEntry.3	INTEGER	R
infChLinesetStatus	infChEntry.4	INTEGER	R
infChLinesetErrorCounter	infChEntry.5	Counter	R
infChLocalSnpaAddress	infChEntry.6	OctetString	R
infChReservedLocalSnpaAddress	infChEntry.7	OctetString	R/W
infChLocalSubAddress	infChEntry.8	OctetString	R
infChReservedLocalSubAddress	infChEntry.9	OctetString	R/W
infChUsage	infChEntry.10	OctetString	R/W
infChErrorTime	infChEntry.11	INTEGER	R
infChBackupCounter	infChEntry.12	Counter	R
infChBackupFailureCounter	infChEntry.13	Counter	R
infChCongestionTime	infChEntry.14	INTEGER	R/W
infChCongestionCounter	infChEntry.15	Counter	R
infChLoadsplitCounter	infChEntry.16	Counter	R
infChLoadsplitFailureCounter	infChEntry.17	Counter	R
infChErrorText1	infChEntry.18	DisplayString	R
infChErrorText2	infChEntry.19	DisplayString	R
infChErrorText3	infChEntry.20	DisplayString	R
infChErrorText4	infChEntry.21	DisplayString	R
infChErrorText5	infChEntry.22	DisplayString	R
infChErrorText6	infChEntry.23	DisplayString	R
infChErrorText7	infChEntry.24	DisplayString	R
infChErrorText8	infChEntry.25	DisplayString	R
infChErrorText9	infChEntry.26	DisplayString	R
infChErrorText10	infChEntry.27	DisplayString	R
infChErrorText11	infChEntry.28	DisplayString	R
infChErrorText12	infChEntry.29	DisplayString	R
infChErrorText13	infChEntry.30	DisplayString	R
infChErrorText14	infChEntry.31	DisplayString	R
infChErrorText15	infChEntry.32	DisplayString	R
infChErrorText16	infChEntry.33	DisplayString	R
infChErrorText17	infChEntry.34	DisplayString	R
infChErrorText18	infChEntry.35	DisplayString	R
infChErrorText19	infChEntry.36	DisplayString	R
infChErrorText20	infChEntry.37	DisplayString	R

F.6.4 中継装置のポート

(1) infPortExt1グループ

MIB	OID	SYNTAX	ACCESS
infPortExt1Table	infPortExt1.1	Aggregate	--
infPortExt1Entry	infPortExt1Table.1	Aggregate	--
infPortExt1Index	infPortExt1Entry.1	INTEGER	R
infPortExt1UsualTarget	infPortExt1Entry.2	OctetString	R
infPortExt1BackupTarget	infPortExt1Entry.3	OctetString	R/W
infPortExt1LoadsplitTarget	infPortExt1Entry.4	OctetString	R/W
infPortExt1CurrentTarget	infPortExt1Entry.5	OctetString	R
infPortExt1UsualChannel	infPortExt1Entry.6	OctetString	R/W
infPortExt1BackupChannel	infPortExt1Entry.7	OctetString	R
infPortExt1LoadsplitChannel	infPortExt1Entry.8	OctetString	R/W
infPortExt1CurrentChannel	infPortExt1Entry.9	OctetString	R
infPortExt1CallOperStatus	infPortExt1Entry.10	INTEGER	R
infPortExt1CallAdminStatus	infPortExt1Entry.11	INTEGER	R/W

F.6.5 中継装置の通信相手

(1) infTargetグループ

MIB	OID	SYNTAX	ACCESS
infTargetTable	infTarget.1	Aggregate	--
infTargetEntry	infTargetTable.1	Aggregate	--
infTargetIndex	infTargetEntry.1	INTEGER	R
infTargetRemoteSnpsAddress	infTargetEntry.2	OctetString	R
infTargetReservedRemoteSnpsAddress	infTargetEntry.3	OctetString	R/W(NV)
infTargetRemoteSubAddress	infTargetEntry.4	OctetString	R
infTargetReservedRemoteSubAddress	infTargetEntry.5	OctetString	R/W(NV)
infTargetMaxRetryCalling	infTargetEntry.6	INTEGER	R/W(NV)
infTargetCallingPriority	infTargetEntry.7	INTEGER	R/W(NV)
infTargetIdleStatusTime	infTargetEntry.8	INTEGER	R/W(NV)
infTargetCallSetupTime	infTargetEntry.9	DisplayString	R/W(NV)
infTargetCallClearTime	infTargetEntry.10	DisplayString	R/W(NV)
infTargetTotalTime	infTargetEntry.11	INTEGER	R
infTargetTotalCharge	infTargetEntry.12	INTEGER	R
infTargetCallSetupCounter	infTargetEntry.13	Counter	R
infTargetCallErrorCounter	infTargetEntry.14	Counter	R
infTargetCallBusyCounter	infTargetEntry.15	Counter	R

F.6.6 呼確立リミッタのMIB

(1) infCallLimiter グループ

MIB	OID	SYNTAX	ACCESS
infCallLimiterTable	infCallLimiter.1	Aggregate	--
infCallLimiterEntry	infCallLimiterTable.1	Aggregate	--
infCallLimiterIndex	infCallLimiterEntry.1	INTEGER	R
infCallLimiterRemoteSnpaAddress	infCallLimiterEntry.2	OCTET STRING	R(CIP)
infCallLimiterRemoteSnpaSubAddress	infCallLimiterEntry.3	OCTET STRING	R(CIP)
infCallLimiterMaxPeriod	infCallLimiterEntry.4	INTEGER	R(CIP)
infCallLimiterCurrentPeriod	infCallLimiterEntry.5	INTEGER	R/W(CIP)
infCallLimiterLastPeriod	infCallLimiterEntry.6	INTEGER	R(CIP)
infCallLimiterStatus	infCallLimiterEntry.7	INTEGER	R/W(CIP)

F.6.7 トラヒックロギング機能のMIB

(1) infAdIpグループ

MIB	OID	SYNTAX	ACCESS
infAdIpTable	infAdIp.1	Aggregate	--
infAdIpEntry	infAdIpTable.1	Aggregate	--
infAdIpSourceAddress	infAdIpEntry.1	IpAddress	R/W(CIP)
infAdIpSourceMask	infAdIpEntry.2	IpAddress	R/W(CIP)
infAdIpRecvIf	infAdIpEntry.3	INTEGER	R/W(CIP)
infAdIpDestAddress	infAdIpEntry.4	IpAddress	R/W(CIP)
infAdIpDestMask	infAdIpEntry.5	IpAddress	R/W(CIP)
infAdIpDestIf	infAdIpEntry.6	INTEGER	R/W(CIP)
infAdIpTotalFrames	infAdIpEntry.7	Counter	R(CIP)
infAdIpTotalOctets	infAdIpEntry.8	Counter	R(CIP)
infAdIpStatus	infAdIpEntry.9	INTEGER	R/W

F.6.8 中継装置の拡張インタフェース

(1) tmpHighSuperDigital グループ

MIB	OID	SYNTAX	ACCESS
tmpHSDTable	tmpHighSuperDigital.1	Aggregate	--
tmpHSDEntry	tmpHSDTable.1	Aggregate	--
tmpHSDChIndex	tmpHSDEntry.1	INTEGER	R(CIP)
tmpHSDStatus	tmpHSDEntry.2	INTEGER	R(CIP)
tmpHSDSpeed	tmpHSDEntry.3	INTEGER	R(CIP)
tmpHSDErrorCounter	tmpHSDEntry.4	Counter	R(CIP)

(2) tmpIsdn-c グループ

MIB	OID	SYNTAX	ACCESS
tmpIsdn-cTable	tmpIsdn-c.1	Aggregate	--
tmpIsdn-cEntry	tmpIsdn-cTable.1	Aggregate	--
tmpIsdn-cChIndex	tmpIsdn-cEntry.1	INTEGER	R
tmpIsdn-cStatus	tmpIsdn-cEntry.2	INTEGER	R(CIP)
tmpIsdn-cChannelType	tmpIsdn-cEntry.3	INTEGER	R
tmpIsdn-cChannelStatus	tmpIsdn-cEntry.4	INTEGER	R(CIP)

F.6.9 中継装置のプロトコル

(1) tmpPppグループ

- tmpPpp Link Control Tableグループ

MIB	OID	SYNTAX	ACCESS
tmpPppLinkControlTable	tmpPpp.1	Aggregate	--
tmpPppLinkControlEntry	tmpPppLinkControlTable.1	Aggregate	--
tmpPppLinkControlIndex	tmpPppLinkControlEntry.1	INTEGER	R
tmpPppLinkCRCSize	tmpPppLinkControlEntry.2	INTEGER	R/W
tmpPppLinkRestartTimerValue	tmpPppLinkControlEntry.3	INTEGER	R/W
tmpPppLinkMaxRestarts	tmpPppLinkControlEntry.4	INTEGER	R/W
tmpPppLinkLocalMRU	tmpPppLinkControlEntry.5	INTEGER	R/W
tmpPppLinkRemoteMRU	tmpPppLinkControlEntry.6	INTEGER	R

- tmpPpp Link Status Tableグループ

MIB	OID	SYNTAX	ACCESS
tmpPppLinkStatusTable	tmpPpp.2	Aggregate	--
tmpPppLinkStatusEntry	tmpPppLinkStatusTable.1	Aggregate	--
tmpPppLinkStatusIndex	tmpPppLinkStatusEntry.1	INTEGER	R
tmpPppLinkVersion	tmpPppLinkStatusEntry.2	INTEGER	R
tmpPppLinkCurrentState	tmpPppLinkStatusEntry.3	INTEGER	R
tmpPppLinkPreviousState	tmpPppLinkStatusEntry.4	INTEGER	R
tmpPppLinkChangeTime	tmpPppLinkStatusEntry.5	TimeTicks	R
tmpPppLinkPhysical	tmpPppLinkStatusEntry.13	ObjectID	R

- tmpPpp Link Errors Tableグループ

MIB	OID	SYNTAX	ACCESS
tmpPppLinkErrorsTable	tmpPpp.3	Aggregate	--
tmpPppLinkErrorsEntry	tmpPppLinkErrorsTable.1	Aggregate	--
tmpPppLinkErrorsIndex	tmpPppLinkErrorsEntry.1	INTEGER	R
tmpPppLinkBadAddresses	tmpPppLinkErrorsEntry.2	Counter	R
tmpPppLinkLastBadAddress	tmpPppLinkErrorsEntry.3	OctetString	R
tmpPppLinkBadControls	tmpPppLinkErrorsEntry.4	Counter	R
tmpPppLinkLastBadControl	tmpPppLinkErrorsEntry.5	OctetString	R
tmpPppLinkLastUnknownProtocol	tmpPppLinkErrorsEntry.6	OctetString	R
tmpPppLinkInvalidProtocols	tmpPppLinkErrorsEntry.7	Counter	R
tmpPppLinkLastInvalidProtocol	tmpPppLinkErrorsEntry.8	OctetString	R
tmpPppLinkPacketTooLongs	tmpPppLinkErrorsEntry.9	Counter	R
tmpPppLinkBadCRCs	tmpPppLinkErrorsEntry.10	Counter	R
tmpPppLinkConfigTimeouts	tmpPppLinkErrorsEntry.11	Counter	R
tmpPppLinkTerminateTimeouts	tmpPppLinkErrorsEntry.12	Counter	R

(2) extmpPppグループ

MIB	OID	SYNTAX	ACCESS
extmpPppLinkControlTable	extmpPpp.1	Aggregate	--
extmpPppLinkControlEntry	extmpPppLinkControlTable.1	Aggregate	--
extmpPppLinkControlIndex	extmpPppLinkControlEntry.1	INTEGER	R
extmpPppLinkControlLoopTime	extmpPppLinkControlEntry.2	INTEGER	R/W(CIP)
extmpPppLcpTable	extendedPpp.2	Aggregate	--
extmpPppLcpEntry	extmpPppLcpTable.1	Aggregate	--
extmpPppLcpIndex	extmpPppLcpEntry.1	INTEGER	R
extmpPppLcpStatus	extmpPppLcpEntry.2	INTEGER	R
extmpPppLcpFcsPreserve	extmpPppLcpEntry.3	INTEGER	R(NV)
extmpPppLcpSetupCounter	extmpPppLcpEntry.4	Counter	R
extmpPppLcpErrorCounter	extmpPppLcpEntry.5	Counter	R
extmpPppBncpTable	extendedPpp.3	Aggregate	--
extmpPppBncpEntry	extmpPppBncpTable.1	Aggregate	--
extmpPppBncpIndex	extmpPppBncpEntry.1	INTEGER	R
extmpPppBncpStatus	extmpPppBncpEntry.2	INTEGER	R
extmpPppBncpReceiveFrames	extmpPppBncpEntry.3	Counter	R
extmpPppBncpReceiveOctets	extmpPppBncpEntry.4	Counter	R
extmpPppBncpSendFrames	extmpPppBncpEntry.5	Counter	R
extmpPppBncpSendOctets	extmpPppBncpEntry.6	Counter	R
extmpPppBncpLocalMbcType	extmpPppBncpEntry.7	OctetString	R
extmpPppBncpRemoteMbcType	extmpPppBncpEntry.8	OctetString	R
extmpPppBncpTinygramComp	extmpPppBncpEntry.9	INTEGER	R(NV)
extmpPppBncpLinkSetupCounter	extmpPppBncpEntry.10	Counter	R
extmpPppBncpLinkErrorCounter	extmpPppBncpEntry.11	Counter	R
extmpPppBncpRejCounter	extmpPppBncpEntry.12	Counter	R
extmpPppMbcTable	extendedPpp.4	Aggregate	--
extmpPppMbcEntry	extmpPppMbcTable.1	Aggregate	--
extmpPppMbcIndex	extmpPppMbcEntry.1	INTEGER	R
extmpPppMbcRejCounter	extmpPppMbcEntry.2	Counter	R
extmpPppDotldTable	extendedPpp.5	Aggregate	--
extmpPppDotldEntry	extmpPppDotldTable.1	Aggregate	--
extmpPppDotldIndex	extmpPppDotldEntry.1	INTEGER	R
extmpPppDotldRejCounter	extmpPppDotldEntry.2	Counter	R

F.7 Trap

F.7.1 標準MIB-IIのTrap

TRAP-TYPE	ENTERPRISE	VARIABLES
coldStart	brouter	--
linkDown	brouter	ifIndex
linkUp	brouter	ifIndex
authenticationFailure	brouter	--
newRoot	dot1dBridge	--
topologyChange	dot1dBridge	--
frDLCIStatusChange	frame-relay	frCircuitIfIndex, frCircuitDlci, frCircuitState
xptrHealth	snmpDot3RptrMgt	xptrOperStatus, xptrHealthText
xptrResetEvent	snmpDot3RptrMgt	xptrOperStatus, xptrHealthText
xpMauJabberTrap	snmpDot3MauMgt	xpMauJabberState

F.7.2 装置拡張Trap

TRAP-TYPE	ENTERPRISE	VARIABLES
infError	infonetBase	--
infBriCongestion	infonetBridge	--
infCallLimiter	infCallLimiter	--



メモ：Trapに関連した表の中の「TRAP-TYPE」はトラップの種類を、「ENTERPRISE」はTrapの属するグループを示します。またTrapに関連した表の中の「VARIABLES」は、Trapに含まれる情報の種類を示します。「--」は、そのTrapに含まれる情報がないことを示します。

A

AppleTalkルーティング 2-14, 3-10, 3-60, 3-128, 3-129, 4-78, 6-29

AURP 2-14, 3-23, 3-60, 3-66, 3-128, 3-137, 4-78, 4-94, 6-29

C

CHAP 2-35, 2-37

D

DHCPリレーエージェント 3-9-3-91, 3-37, 6-10-6-40

DHCPリレーエージェント機能 2-7, 3-116

H

HSD 1-12, 2-2, 3-9, 3-12, 3-102, B-2

I

ICMPリダイレクトメッセージ 4-13

IP Tunnel 2-14, 3-10, 3-61

IPXアドレス 3-46, 4-112, 4-124

IPXルーティング 2-9, 3-10, 3-24, 3-45, 3-120, 4-60, 6-12

IPアドレス 3-27, 3-110, 5-8

IPホスト 2-2, 3-26, 3-110

IPルーティング 2-3, 3-9, 3-29, 3-112, 4-15, 4-33, 4-123, 6-5

ISDN 2-24

ISDNリモートターゲット 3-18, 3-32, 3-48, 3-64, 3-78, 3-105, 3-113, 3-121, 3-130, 3-142

ISDN回線 2-35, 3-9, B-3

ISDN番号 3-105

K

KeepAlive 2-10, 2-34, 4-75

L

LED 1-10, 5-27

O

OSPF 2-3, 4-32, 6-21

OSPFインタフェース 4-41, 6-25

OSPFエリア 4-34, 6-23

OSPFスタブホスト 4-39

OSPFネットワーク 4-37

OSPFバーチャルリンク 4-47, 6-26, 6-28

OSPFバーチャルリンク隣接ルータ 4-45

OSPFバックボーン 4-36

OSPF隣接 4-43, 6-27

OSPFルータID 4-32, 4-33

P

Proxy ARP 2-6, 4-30

R

RTMP 2-14, 3-23, 5-19

S

SAP 3-10, 3-23, 3-58, 3-126, 6-15

SNMP 2-38, 3-11, 3-89, 3-149, 4-98

STP 2-19, 3-81, 4-9

イ

一般資格 3-95, 5-40

エ

エラーログ 6-39

オ

オフライン 5-5

オンライン 5-5

カ

簡易コマンド 2-40, 5-40, D-1

管理者資格 3-95, 5-1, 5-11, 5-40

ク

クラスタリング 2-15

コ

呼確立リミッタ 4-119, 5-6, 6-38

コンソール 1-4, 1-6, 2-39, 3-92, 3-98, A-4

サ

再起動 5-27. *リセットも参照*

シ

自ホスト名 3-8, 3-45, 3-89, 3-101

ス

スーパーモード. *管理者資格を参照*

スタティックルーティング 2-5

スタティックルーティング (AppleTalk) 2-14, 3-10, 3-73, 3-137

スタティックルーティング (IP) 3-9

スタティックルーティング (IPX) 2-9, 3-10, 3-55, 3-125

スタティックルーティングIP) 3-114

ソ

ゾーンフィルタリング 2-18

ゾーンリスト 3-61, 3-71, 3-135

タ

ダイナミックルーティング 2-3

ダイナミックルーティング (AppleTalk) 2-14

ダイナミックルーティング (IPX) 2-9

代表取扱いサービス 2-41, B-3, B-4

チ

チャンネルグループ 2-33, 3-13

テ

データリンク 4-5

データ圧縮 2-40, 4-7

データ別優先制御 2-41, 4-100, 5-26

ト

トラップログ 6-39

トラヒックロギング 2-43, 4-116, 6-40

トラヒック分散 2-24, 5-4, B-4

ネ

ネットワーク番号 5-10

ネットワーク番号範囲 3-61

ノ

ノーマルモード. 一般資格を参照

ハ

パケットフィルタリング 2-10

パケットフィルタリング (IP) 3-10, 3-39, 3-117

パケットフィルタリング (IPX) 3-10, 3-50, 3-123

パスワード 3-20, 3-95, 5-11

フ

ブリッジング 2-19, 3-10, 3-80, 3-142, 4-9, 6-16

フレームトレース 5-13

ブロードキャスト (IP) 2-6

ホ

ポイントツーポイント (IP) 2-5

ラ

ラインログ 6-39

リ

リセット 1-3, 2-2, 2-24, 3-151, E-1. 再起動も参照

リマッピング 2-15

リモートコンソール 2-39, 5-7, 5-39

リモートファイルメンテナンス 4-99

ル

ルーティンググループ化 2-41, 4-123

ロ

ローカルコンソール. コンソールを参照

ログイン 5-40, E-1

INFONET3790 マルチポートブルータ

取扱説明書 5 版

発行日 1997年8月

発行責任 古河電気工業株式会社

Printed in Japan

本書は改善のため事前連絡なしに変更することがあります。

本書に記載されたデータの使用に起因する第三者の特許権その他の権利については、当社はその責を負いません。

無断転載を禁じます。

落丁・乱丁本はお取り替えいたします。