AX2000R ソフトウェアマニュアル

解説書 Vol.2

Ver. 8.4 対応

AX-10-158-10

AlaxalA

■対象製品

このマニュアルは AX2000R モデルを対象に記載しています。また，AX2000R のソフトウェア Ver. 8.4 の機能について記載しています。ソフトウェア機能は，ソフトウェア ROUTE-OS8B でサポートする機能について記載します。

■輸出時の注意

本製品を輸出される場合には，外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上，必要な手続きをお取りください。
なお，ご不明な場合は，弊社担当営業にお問い合わせください。

■商標一覧

Ethernet は，米国 Xerox Corp. の商品名称です。
HP OpenView は米国 Hewlett-Packard Company の米国及び他の国々における商品名称です。
IPX は米国 Novell, Inc. の登録商標です。
JP1 は，（株）日立製作所の日本における商品名称（商標又は，登録商標）です。
Microsoft は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
NetWare は，米国 Novell,Inc. の登録商標です。
PolicyXpert は，米国 Hewlett-Packard Company の商品名称です。
SNA は，米国 International Business Machines Corp. のプロトコル名称です。
Solaris は，米国及びその他の国における Sun Microsystems, Inc. の商標又は登録商標です。
UNIX は，X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。
Windows は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
イーサネットは，富士ゼロックス（株）の商品名称です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■マニュアルはよく読み，保管してください。

製品を使用する前に，安全上の説明をよく読み，十分理解してください。
このマニュアルは，いつでも参照できるよう，手近な所に保管してください。

■ご注意

このマニュアルの内容については，改良のため，予告なく変更する場合があります。

■電波障害について

この装置は，情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

■高調波規制について

高調波電流規格　JIS　C　61000-3-2 適合品
適合装置：
ＡＸ－６５３１－１Ｒ（ＡＸ ２００１ Ｒ）
ＡＸ－６５３１－２Ｒ（ＡＸ ２００２ Ｒ）
ＡＸ－６５３１－２ＲＸ（ＡＸ ２００２ ＲＸ）

■発行

２００５年　１２月 （第2版） ＡＸ－１０－１５８－１０

変更来歴

【Ver. 8.4】

表　変更来歴

章・節・項・タイトル	追加・変更内容
1.6　優先度指定	•「表 1-9　64VLL 帯域制御指定時のパケット種別ごとの優先度」の記述を追加しました。
1.7　廃棄制御	• B モデル用新規サポート NIF である NEB100-1TC の記述を追加しました。
1.8.1　完全優先	• B モデル用新規サポート NIF である NEB100-1TC の記述を追加しました。
1.8.6　帯域制御（トラフィック指定）	• Tag-VLAN 連携回線に対する帯域制御（トラフィック指定）の説明を追加しました。 • 16VLL 帯域制御の記述を追加しました。 • 64VLL 帯域制御の記述を追加しました。
1.10.4　キュー仕様	• B モデル用新規サポート NIF である NEB100-1TC の記述を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

はじめに

■対象製品およびソフトウェアバージョン

このマニュアルはAX2000Rモデルを対象に記載しています。また，AX2000Rのソフトウェア ROUTE-OS8B Ver. 8.4の機能について記載しています。

操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。また，このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。

■対象読者

AX2000Rを利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。

また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

■このマニュアルの記述内容について

このマニュアル中には，AX2000Rでサポートしていない機能に関する用語・文言が一部に記載されております。以下に挙げます機能に関する用語・文言につきましては，AX2000Rでサポートしていない機能とご理解くださいますようお願い致します。

(1)BCUの二重化

(2) 電源の冗長構成

(3) オンライン中のボード交換（NIFの活栓挿抜）

(4) 以下のネットワークインタフェース

・イーサネットインタフェースのうち，100BASE-FX

・WANインタフェースのうち，J2(6.3Mbit/s)，T1，T3，E1，E3，OC-3c，OC-12c，OC-48c。
また，APS機能および各種関連コマンドパラメータのsubline指定。

・ATMインタフェースのうち，OC-12c。また，OC-3cの8ポートNIF

(5)RMイーサネット（BCUにある管理用イーサネットポート）

(6)AUXポートおよびダイアルアップIP接続

(7) 階層化シェーパ

また，AX2000Rでサポートする構成定義コマンドの入力形式をCLIタイプ1階層入力形式，構成定義コマンドをCLIタイプ1コマンドと記載する場合があります。

■このマニュアルの訂正について

このマニュアルに記載の内容は，ソフトウェアと共に提供する「リリースノート」および「マニュアル訂正資料」で訂正する場合があります。

■マニュアルの構成

「AX2000Rソフトウェアマニュアル　解説書」はVol.1およびVol.2に分かれています。

「AX2000Rソフトウェアマニュアル　解説書 Vol.2」は，次に示す五つの編と付録から構成されています。

第1編　QoS

AX2000Rが行っているQoS制御，Diff-serv機能などについて説明しています。

第 2 編　マルチプロトコル通信

IPX ルーティング，ブリッジについて説明しています。

第 3 編　高信頼性機能

高信頼性機能として VRRP について説明しています。

第 4 編　運用

ネットワーク管理，運用機能について説明しています。

第 5 編　システム構築のためのポイント

システム構築時に必要な，他機種および網・各種専用線サービスとの接続について説明しています。

付録 A　準拠規格

準拠している規格について説明しています。

付録 B　謝辞 (Acknowledgments)

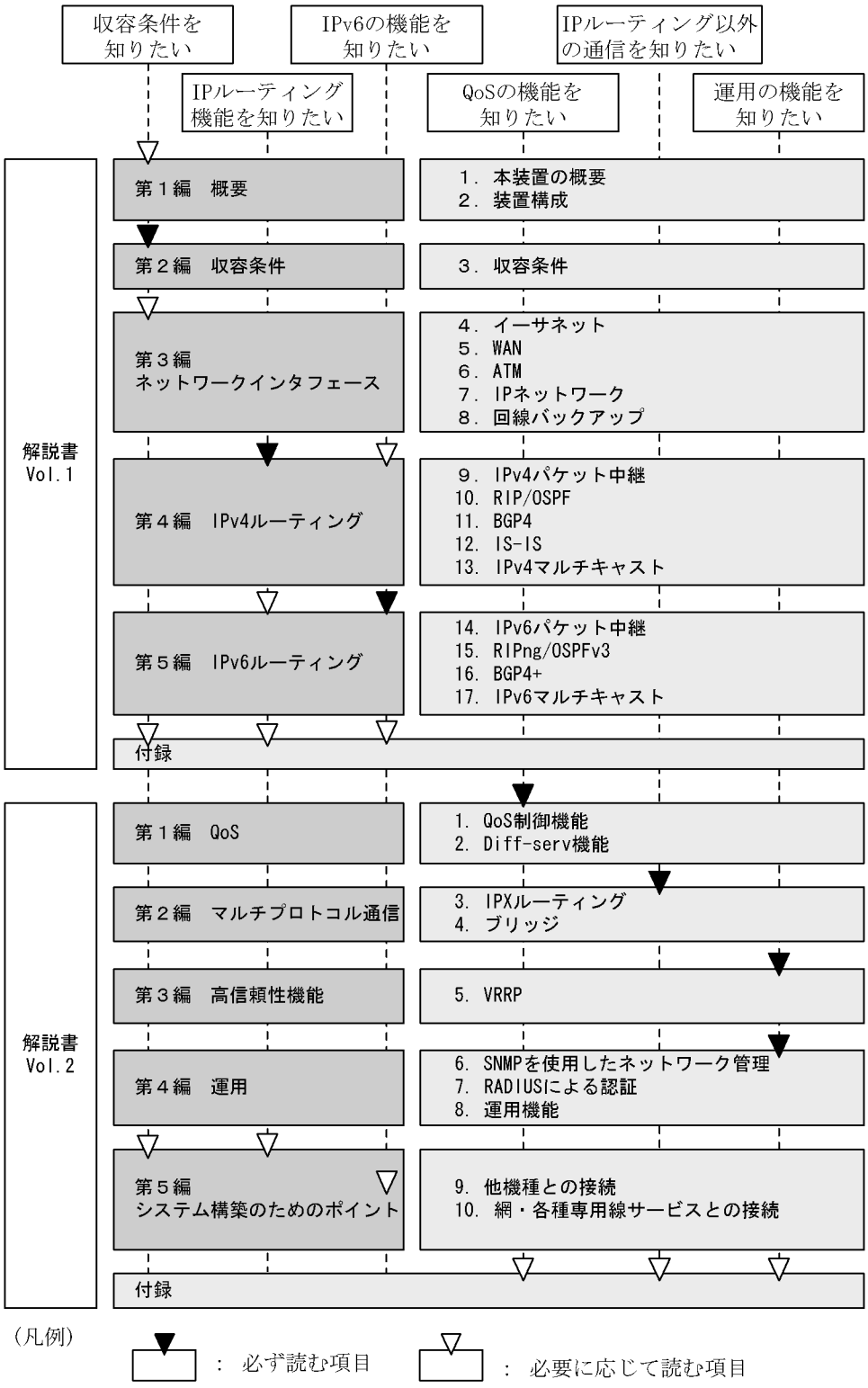
謝辞 (Acknowledgments) を掲載しています。

付録 C　用語解説

このマニュアルで使用している用語の意味を説明しています。

■読書手順

このマニュアルは次の手順でお読みいただくことをお勧めします。



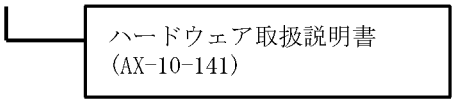
■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しております。

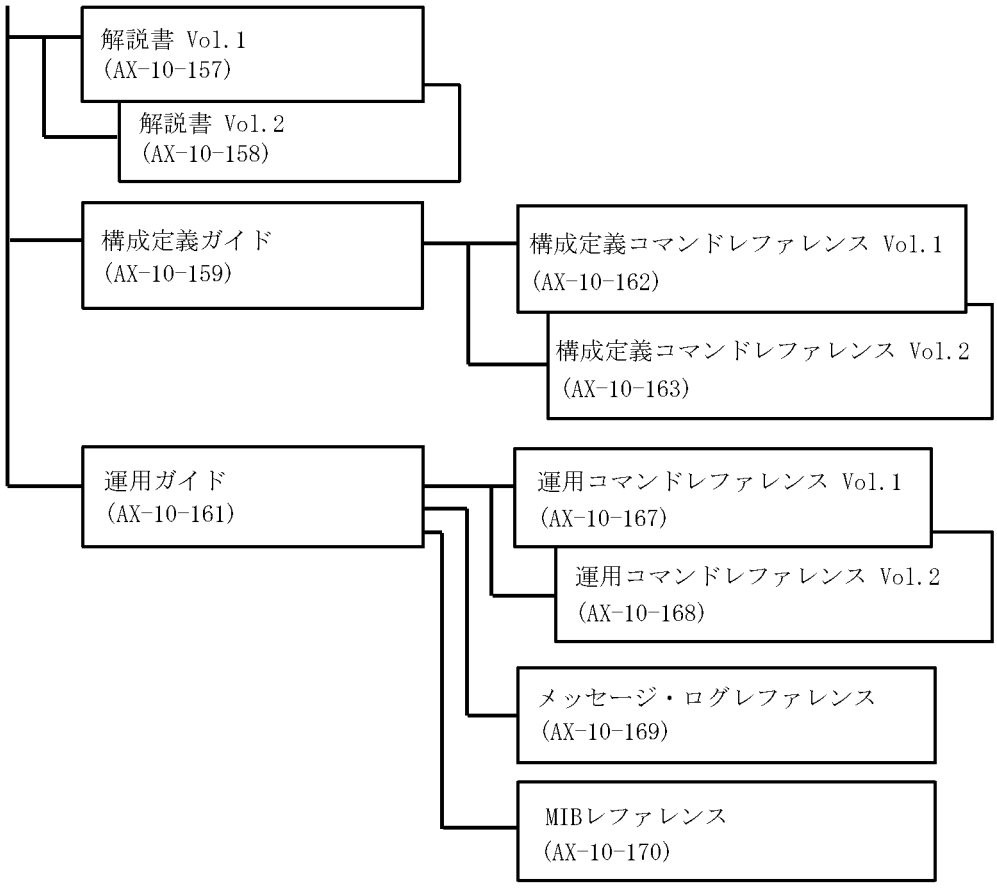
http://www.alaxala.com

■ AX2000R マニュアル体系

●ハードウェアマニュアル



●ソフトウェアマニュアル



■ AX2000R シリーズマニュアルの読書手順

本装置の導入，セットアップ，日常運用までの作業フローに従って，それぞれの場合に参照するマニュアルを次に示します。かっこ内はマニュアル番号です。

●ハードウェアの構成，およびソフトウェアの機能を知りたい

解説書 Vol.1
(AX-10-157)

解説書 Vol.2
(AX-10-158)

●ハードウェアの設備条件，取扱方法を調べる

ハードウェア取扱説明書
(AX-10-141)

●構成定義情報の作成方法，定義例 （各コマンドの入力シンタックス，パラメータ詳細）

構成定義ガイド
(AX-10-159)

構成定義コマンドレファレンス Vol.1
(AX-10-162)

構成定義コマンドレファレンス Vol.2
(AX-10-163)

●運用管理方法，トラブルシュート →各コマンドの入力シンタックス，パラメータ詳細

運用ガイド
(AX-10-161)

運用コマンドレファレンス Vol.1
(AX-10-167)

運用コマンドレファレンス Vol.2
(AX-10-168)

→運用ログ詳細

メッセージ・ログレファレンス
(AX-10-169)

→MIB詳細

MIBレファレンス
(AX-10-170)

■このマニュアルでの表記

AAL	ATM Adaptation Layer
ABR	Available Bit Rate
AC	Access Concentrator
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
AIS	Alarm Indication Signal
ALG	Application Level Gateway
ANSI	American National Standards Institute
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
AS	Autonomous System
ATM	Asynchronous Transfer Mode
AUX	Auxiliary
BAP	Bandwidth Allocation Protocol
BAS	Broadband Access Server
BECN	Backward Explicit Congestion Notification
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second　　*bpsと表記する場合もあります。
BOD	Bandwidth On Demand
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
BSR	BootStrap Router
CBR	Constant Bit Rate
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CLLM	Consolidated Link Layer Management
CLNP	Connectionless Network Protocol
CLNS	ConnectionLess Network System
CLP	Cell Loss Priority
CNTL	CoNTroL
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
DA	Destination Address
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
Diff-serv	Differentiated Services
DIS	Draft International Standard/Designated Intermediate System
DLCI	Data Link Connection Identifier
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSU	Digital Service Unit
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
ES	End System
FCS	Frame Check Sequence
FDB	Filtering DataBase
FDDI	Fiber Distributed Data Interface
FECN	Forward Explicit Congestion Notification
FERF	Far End Receive Failure
FQDN	Fully Qualified Domain Name
FR	Frame Relay
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GFR	Guaranteed Frame Rate
HDLC	High level Data Link Control
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IIH	IS-IS Hello

ILMI	Interim Local Management Interface
INS	Information Network System
IP	Internet Protocol
IPsec	Security Architecture for IP
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IPv6 Control Protocol
IPX	Internetwork Packet Exchange
ISDN	Integrated Services Digital Network
IS	Intermediate System
IS-IS	Information technology - Telecommunications and Information exchange between systems - Intermediate system to Intermediate system Intra-Domain routeing information exchange protocol for use in conjunction with the Protocol for providing the Connectionless-mode Network Service (ISO 8473)
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU-T	International Telecommunication Union - Telecommunication, Standardization Sector
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LIS	Logical IP Subnetwork
LLB	Local Loop Back
LLC	Logical Link Control
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LQR	Link Quality Report
LSP	Link State PDU
MAC	Media Access Control
MC	Memory Card
MCR	Media Access Control
MD5	Message Digest 5
MIB	Management Information Base
MLD	Multicast Listener Discovery
MMF	Multi Mode Fiber
MRU	Maximum Receive Unit
MSS	Maximum Segment Size
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAPT	Network Address Port Translation
NAPT-PT	Network Address Port Translation - Protocol Translation
NAT	Network Address Translation
NAT-PT	Network Address Translation - Protocol Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NetBIOS	Network Basic Input/Output System
NIF	Network Interface board
NLA ID	Next-Level Aggregation Identifier
NLP	Network Layer Protocol
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OAM	Operation Administration and Management
OC-12c	Optical Carrier level 12 concatetenation
OC-3c	Optical Carrier level 3 concatenation
OC-48c	Optical Carrier level 48 concatetenation
ONU	Optical Network Unit
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packet per second　　*ppsと表記する場合もあります。
PAD	PADding
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADR	PPPoE Active Discovery Request
PADS	PPPoE Active Discovery Session-confirmation
PADT	PPPoE Active Discovery Terminate
PC	Personal Computer
PCI	Protocol Control Information
PCR	Peak Cell Rate
PDU	Protocol Data Unit
PHY	PHYsical layer protocol
PICS	Protocol Implementation Conformance Statement

PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
POS	PPP over SONET/SDH
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PRI	Primary Rate Interface
PSNP	Partial Sequence Numbers PDU
PSS	Product Support Service
PVC	Permanent Virtual Channel (Connection)/Permanent Virtual Circuit
QoS	Quality of Service
RA	Router Advertisement
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RLB	Remote Loop Back
RM	Routing Manager
RMON	Remote Network Monitoring MIB
RP	Routing Processor
RPF	Reverse Path Forwarding
RQ	ReQuest
SA	Source Address
SAP	Service Access Point
SD	Start Delimiter
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SD-I	Super Digital I interface
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SMF	Single Mode Fiber
SMTP	Simple Mail Transfer Protocol
SNA	Systems Networking Architecture
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SONET	Synchronous Optical Network
SPF	Shortest Path First
SPT	Spanning Tree
SPX	Sequenced Packet Exchange
SSAP	Source Service Access Point
SVC	Switched Virtual Channel (Connection)
TA	Terminal Adapter
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTC	the Telecommunication Technology Committee
TTL	Time To Live
UBR	Unspecified Bit Rate
UBR+	Unspecified Bit Rate plus
UDP	User Datagram Protocol
UNI	User Network Interface
UPC	Usage Parameter Control
VBR	Variable Bit Rate
VC	Virtual Channel/Virtual Call/Virtual Circuit
VCI	Virtual Channel Identifier
VLAN	Virtual LAN
VLL	Virtual Leased Line
VP	Virtual Path
VPI	Virtual Path Identifier
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WFQ	Weighted Fair Queueing
WS	Work Station
WWW	World-Wide Web

■図中で使用する記号の説明

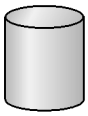
このマニュアルの図中で使用する記号を，次のように定義します。

●ﾜｰｸｽﾃｰｼｮﾝ，端末

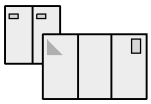
●入出力の動作

●サーバ

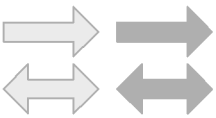
●ファイル



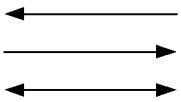
●ホストセンタ



●データの流れ

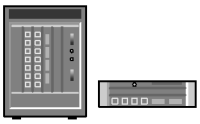


●その他の流れ

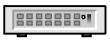


●工程，作業項目の流れ

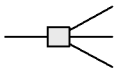
●AX2000R



●一般ルータ



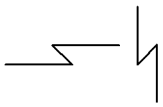
●イーサネットまたはギガビットイーサネット



●ネットワーク

●論理回線

●通信回線



■常用漢字以外の漢字の使用について

このマニュアルでは，常用漢字を使用することを基本としていますが，次に示す用語については，常用漢字以外を使用しています。

- 宛て（あて）
- 宛先（あてさき）
- 迂回（うかい）
- 個所（かしょ）
- 活栓挿抜（かっせんそうばつ）
- 筐体（きょうたい）
- 桁 （けた）
- 毎 （ごと）
- 閾値（しきいち）
- 嗜好（しこう）
- 芯（しん）
- 必須（ひっす）
- 輻輳（ふくそう）
- 閉塞（へいそく）
- 漏洩（ろうえい）

■ kB(バイト) などの単位表記について

1kB(キロバイト)，1MB(メガバイト)，1GB(ギガバイト)，1TB(テラバイト) はそれぞれ 1,024 バイト，1,024 ^{2}バイト，1,024 ^{3}バイト，1,024 ^{4}バイトです。

目次

第 1 編　QoS

1 QoS 制御機能 1

1.1 QoS 制御概説 2
1.1.1 QoS 制御の必要性 2
1.1.2 トラフィック種別と要求品質 2
1.1.3 QoS 制御のメリット 3
1.2 QoS 制御構造 4
1.3 フロー検出 5
1.4 帯域監視 7
1.5 マーカー 9
1.6 優先度指定 10
1.7 廃棄制御 16
1.8 シェーパ 18
1.8.1 完全優先 18
1.8.2 最低帯域保証 19
1.8.3 ラウンドロビン 19
1.8.4 均等最低帯域保証 19
1.8.5 最低帯域保証 (kbit/s 指定) 19
1.8.6 帯域制御 (トラフィック指定) 20
1.8.7 グループ帯域制御 28
1.9 QoS 制御機能の適用例 31
1.9.1 QoS ネットワーク構成例 31
1.9.2 QoS ネットワークの運用 35
1.10 QoS 制御機能の仕様一覧 37
1.10.1 QoS 制御機能とメディア種別との対応 37
1.10.2 エントリ数の仕様 38
1.10.3 QoS 制御機能とプロトコル種別とのサポート仕様 38
1.10.4 キュー仕様 39
1.10.5 レイヤ 2 連携機能 41
1.11 QoS 制御使用時の注意事項 42
1.11.1 RP 処理負荷と QoS 制御の関係 42
1.11.2 TCP パケットに対する帯域監視機能の使用 43
1.11.3 そのほかの注意事項 43

2 Diff-serv 機能 45

2.1 Diff-serv 概説 46
2.1.1 Diff-serv の機能 46
2.1.2 Diff-serv の QoS サービス 49

2.1.3 Diff-serv の制御仕様 50
2.2 Diff-serv の機能ブロック 51
2.2.1 フロー制御 51
2.2.2 廃棄制御 52
2.2.3 シェーパ 52
2.2.4 機能ブロックと構成定義コマンドの対応 52
2.3 構成定義作成時の注意事項 55
2.3.1 構成定義作成パターン 55
2.3.2 適用例 55

第 2 編　マルチプロトコル通信

3 IPX ルーティング 59
3.1 IPX ルーティング概説 60
3.1.1 フレームタイプ 60
3.1.2 ノードアドレス 60
3.1.3 ネットワークアドレス 61
3.1.4 インタフェース 61
3.1.5 IPX ルーティングの機能 61
3.2 通信処理機能 62
3.3 中継機能 64
3.4 経路制御機能 67
3.4.1 RIP プロトコル 67
3.4.2 スタティックルーティング 68
3.5 特殊制御パケット処理機能 69
3.5.1 SAP パケット処理 69
3.5.2 ウォッチドッグ・パケットの制御 72
3.5.3 そのほかの特殊パケット処理 74
3.5.4 SAP フィルタリング 74
3.5.5 RIP フィルタリング 75
3.5.6 Ping 機能 75
3.6 ネットワーク設計の考え方 77
3.6.1 中継性能 77
3.6.2 制御パケットのトラフィック 77
3.6.3 WAN または ATM 接続 79

4 ブリッジ 81
4.1 サポート仕様 82
4.1.1 フレーム・フォーマット 82

4.1.2 インタフェース 82
4.2 トランスペアレント・ブリッジ 83
4.3 スパニングツリー・アルゴリズム 84
4.4 トランスレーション 87
4.4.1 トランスレーション適用構成 87
4.4.2 フレーム・フォーマットのトランスレーション 88
4.4.3 MAC アドレスのビット順序反転 89
4.5 ブリッジ機能 90
4.5.1 インタフェースのブリッジ動作モード 90
4.5.2 スパニングツリー・トポロジ管理 90
4.5.3 フィルタリング 92
4.5.4 拡張フィルタリング 93
4.6 ネットワーク設計の考え方 95
4.6.1 禁止トポロジ 95
4.6.2 中継性能 96
4.6.3 HDLC パススルーと優先度制御 96
4.6.4 WAN または ATM 接続 96

第 3 編　高信頼性機能

5 VRRP 99
5.1 VRRP 概説 100
5.2 仮想ルータの MAC アドレスと IP アドレス 101
5.3 障害監視インタフェース 103
5.4 VRRP ポーリング 104
5.4.1 VRRP ポーリングの概要 104
5.4.2 VRRP ポーリング使用時の注意事項 105
5.5 VRRP ポーリングの障害検出の仕組み 107
5.6 障害検出の仕組み 109
5.7 パケットの認証 110
5.8 マスタルータの選出方法 111
5.8.1 優先度 111
5.8.2 自動切り戻し 111
5.9 ネットワーク構成例 112
5.9.1 VRRP による構成例 112
5.9.2 負荷分散の例 112
5.10 VRRP 使用時の注意事項 114

第 4 編　運用

6 SNMP を使用したネットワーク管理 117

6.1 SNMP 概説 118

6.1.1 ネットワーク管理 118

6.1.2 SNMP エージェント機能 118

6.2 MIB 概説 120

6.2.1 MIB 構造 120

6.2.2 MIB オブジェクトの表し方 120

6.2.3 インデックス 121

6.2.4 本装置のサポート MIB 121

6.3 SNMP オペレーション 122

6.3.1 GetRequest オペレーション 122

6.3.2 GetNextRequest オペレーション 123

6.3.3 GetBulkRequest オペレーション 124

6.3.4 SetRequest オペレーション 124

6.3.5 SNMP オペレーションの制限事項 126

6.3.6 SNMP オペレーションのメッセージフォーマット 127

6.4 トラップ 129

6.4.1 トラップ概説 129

6.4.2 トラップフォーマット 129

6.4.3 サポートトラップ 129

6.4.4 PVC Trap 130

6.5 RMON MIB 134

7 RADIUS による認証 135

7.1 RADIUS 概説 136

7.2 RADIUS の適用機能および範囲 137

7.3 RADIUS を使用した認証 139

7.4 RADIUS 認証でのログインユーザの扱い 141

8 運用機能 143

8.1 運用管理 144

8.1.1 運用端末 144

8.2 立ち上げ 146

8.2.1 立ち上げおよび再起動 146

8.2.2 自己診断テスト 146

8.3 ログイン制御 147

8.3.1 ログイン制御 147

8.3.2 ログインセキュリティ制御 147
8.4 構成定義 149
8.4.1 構成定義情報 149
8.4.2 構成定義情報ファイルの種類 150
8.4.3 構成定義情報の運用方法 150
8.4.4 構成定義情報の表示と編集 151
8.5 運用コマンド 152
8.6 MC 162
8.6.1 バックアップ MC の運用 162
8.6.2 MC 保守コマンド 162
8.7 管理情報の収集 163
8.7.1 時計および時刻情報 163
8.7.2 装置およびインタフェース状態表示 163
8.7.3 統計情報 164
8.7.4 運用メッセージおよび運用ログ 165
8.8 LED および FAULT CODE の表示 166
8.8.1 LED 166
8.8.2 FAULT CODE 166
8.9 ネットワーク障害切り分け機能 167
8.9.1 経路確認 167
8.9.2 疎通テスト 167
8.9.3 回線テスト 169
8.9.4 トレース (フレームトレース) 169
8.10 障害時の復旧および情報収集 171
8.10.1 障害部位と復旧内容 171
8.10.2 ログ 172
8.10.3 スイッチ 172
8.10.4 メモリダンプ 172
8.11 ソフトウェアのアップデート 173
8.11.1 リモート運用端末からのソフトウェアのアップデート 173
8.11.2 コンソールからのソフトウェアのアップデート 173
8.11.3 ソフトウェアアップデート時の注意事項 173
8.12 ファイル属性 174

第 5 編　システム構築のためのポイント

9 他機種との接続 175
9.1 イーサネットインタフェース 176
9.1.1 インタフェース種別の設定 176
9.1.2 Tag-VLAN 連携の LAN スイッチ接続 176

9.1.3 Tag-VLAN 連携の PC 接続 178
9.2 WAN インタフェース 179
9.2.1 フレームリレー 179
9.3 ATM インタフェース 180
9.3.1 Cisco 社製ルータ接続 180
9.4 IP ルータとの接続 181
9.4.1 他機種との接続 181
9.4.2 他装置との置き換え 183
9.5 IPv6 ルータとの接続 185
9.5.1 他機種との接続 185
9.6 SNMP マネージャとの接続 187
9.6.1 推奨 SNMP マネージャ 187
9.6.2 MIB 情報収集周期のチューニング 187
9.7 RADIUS サーバとの接続 189
9.7.1 推奨 RADIUS サーバ 189
9.7.2 RADIUS サーバの設定 189

10 網・各種専用線サービスとの接続 191
10.1 イーサネット，ギガビット・イーサネット 192
10.1.1 広域イーサネット 192
10.1.2 フレッツ・ADSL および B フレッツ接続 (PPPoE での接続) 192
10.2 専用線・フレームリレー・ISDN 194
10.2.1 WAN のサービス 194
10.2.2 フレームリレー網の加入条件 194
10.2.3 ISDN 回線契約条件 196
10.2.4 インバースマックス　ターミナルアダプタ接続条件 199
10.3 ATM サービス 204
10.3.1 ATM メガリンクサービス 204
10.3.2 セルリレーサービス 209
10.3.3 メガデータネッツ 210

付録 215
付録 A　準拠規格 216
付録 A.1 イーサネット 216
付録 A.2 WAN 217
付録 A.3 ATM 219
付録 A.4 IPv4 ネットワーク 219
付録 A.5 RIP/OSPF 220
付録 A.6 BGP4 221
付録 A.7 IS-IS 221

付録 A.8　IPv4 マルチキャスト 222
付録 A.9　IPv6 ネットワーク 222
付録 A.10　RIPng/OSPFv3 223
付録 A.11　BGP4+ 223
付録 A.12　IPv6 マルチキャスト 224
付録 A.13　Diff-serv 224
付録 A.14　ブリッジ 224
付録 A.15　SNMP 224
付録 A.16　RADIUS 226
付録 A.17　VRRP 226
付録 B　謝辞 (Acknowledgments) 227
付録 C　用語解説 245

索引 255

目次

解説書 Vol . 1

第 1 編　概要

1 本装置の概要 1

1.1 本装置のコンセプト 2

1.2 本装置の特長 3

1.2.1 先進技術を取り入れたハードウェア・ルーティング 3

1.2.2 先進 IP プロトコル IPv6 に対応 3

1.2.3 QoS 制御機能による高度な通信品質 4

1.2.4 高信頼性 5

1.2.5 優れた運用性 5

1.3 本装置の機能 6

2 装置構成 9

2.1 本装置のシリーズの種類 10

2.1.1 収容インタフェース数 10

2.1.2 装置の外観 10

2.2 装置の構成要素 12

2.2.1 ハードウェアの構成要素 12

2.2.2 ソフトウェア 14

2.3 接続形態 16

2.4 ネットワーク構成例 17

2.4.1 エンタープライズへの適用例 17

第 2 編　収容条件

3 収容条件 21

3.1 搭載条件 22

3.1.1 機器搭載条件 22

3.1.2 ハードウェア搭載に関する注意事項 23

3.2 収容条件 24

3.2.1 ROUTE-OS8B の収容条件 24

第 3 編　ネットワークインタフェース

4 イーサネット 41

4.1 イーサネット 42
4.1.1 接続インタフェース 42
4.1.2 MAC ／ LLC 副層制御 43
4.1.3 対象プロトコル 45
4.1.4 イーサネット接続時の注意事項 45
4.2 ギガビット・イーサネット 46
4.2.1 接続インタフェース 46
4.2.2 MAC ／ LLC 副層制御 46
4.2.3 中継対象プロトコル 47
4.2.4 オートネゴシエーション 47
4.2.5 ギガビット・イーサネット接続時の注意事項 48
4.2.6 ネットワーク構成例 49
4.3 Tag-VLAN 連携 51
4.3.1 プロトコル仕様 51
4.3.2 サポート仕様 51
4.3.3 ネットワーク構成例 53
4.3.4 Tag-VLAN 連携使用時の注意事項 54
4.4 PPP over Ethernet クライアント機能 56
4.4.1 サポート仕様 56
4.4.2 ネットワーク構成例 63
4.4.3 PPPoE 使用時の注意事項 64
4.5 イーサネット使用時の注意事項 66
4.5.1 禁止トポロジ 66

5 WAN 67

5.1 物理インタフェース 68
5.1.1 物理インタフェース条件 68
5.1.2 回線速度についての注意事項 71
5.1.3 WAN の回線ハードウェアでの送信遅延 72
5.2 PPP 75
5.2.1 PPP 概説 75
5.2.2 データリンクコネクション 76
5.2.3 認証 76
5.2.4 ネットワークコネクション 78
5.2.5 カプセル化 79
5.2.6 PPP 制御パケット 80
5.2.7 マルチリンク PPP(MP) 83

5.2.8 BACP と BAP 86
5.2.9 PPP 関係タイマ値，リトライ値 92
5.3 フレームリレー 102
5.3.1 フレームリレー概説 102
5.3.2 インタフェースの設定 104
5.3.3 パラレル PVC 108
5.3.4 トラフィック制御 109
5.3.5 アドレス解決 114
5.3.6 カプセル化フォーマット 115
5.3.7 プロトコルオプション 116
5.4 ISDN 接続 119
5.4.1 ISDN 概説 119
5.4.2 ISDN チャネルとインタフェース 120
5.4.3 ISDN ユーティリティ機能 123
5.4.4 ISDN 使用時の注意事項 124
5.5 オーバーロード 127
5.5.1 BOD サポート方式 127
5.5.2 オーバーロード開始 / 停止 128
5.5.3 オーバーロード接続形態 130
5.5.4 オーバーロード使用時の注意事項 132

6 ATM 135
6.1 ATM 概説 136
6.2 物理層 137
6.2.1 25M ATM インタフェース 137
6.2.2 OC-3c SONET/STM-1 SDH インタフェース 137
6.3 ATM/AAL 層 138
6.3.1 接続制御 138
6.3.2 トラフィック制御 142
6.3.3 OAM 制御 156
6.4 Classical IP over ATM 161
6.4.1 ATM 上の IP フォワーディング 161
6.5 IPv6 パケット中継 163
6.5.1 ATM 上の IPv6 フォワーディング 163
6.6 IPX およびブリッジのパケット中継 165
6.6.1 ATM 上の IPX パケットの扱い 165
6.6.2 ATM 上のブリッジフレームの扱い 166
6.7 ATM 使用時の注意事項 168
6.7.1 帯域設計時の注意事項 168
6.7.2 機能項目別の接続条件 170

7 IP ネットワーク 171
7.1 アドレッシング 172
7.1.1 IP アドレス 172
7.1.2 サブネットマスク 172
7.1.3 IP アドレス付与単位 173
7.1.4 ホスト名情報 177
7.2 アドレッシングとパケット中継動作 178
7.2.1 イーサネットのマルチホーム接続 178
7.2.2 イーサネットの Tag-VLAN 連携回線接続 178
7.2.3 フレームリレー，ATM のネットワーク 178

8 回線バックアップ 185
8.1 インタフェースバックアップ 186
8.1.1 回線バックアップ仕様 187
8.1.2 バックアップ切り替え条件 188
8.2 物理ポートバックアップ 191
8.2.1 回線バックアップ仕様 191
8.2.2 バックアップ切り替え条件 192
8.3 バックアップ接続構成 193
8.4 回線バックアップ使用時の注意事項 197

第 4 編 IPv4 ルーティング

9 IPv4 パケット中継 199
9.1 IP レイヤ機能 200
9.2 通信機能 201
9.2.1 インターネットプロトコル (IP) 201
9.2.2 ICMP 202
9.2.3 ARP 204
9.3 中継機能 206
9.3.1 IP パケットの中継方法 206
9.3.2 ブロードキャストパケットの中継方法 206
9.3.3 MTU とフラグメント 211
9.3.4 包含サブネットの注意事項 212
9.4 フィルタリング 216
9.4.1 フィルタリング項目 216
9.4.2 フィルタリング制御使用時の注意事項 217

9.5 ロードバランス 218
9.5.1 ロードバランス概説 218
9.5.2 ロードバランス仕様 219
9.5.3 出力インタフェースの決定 220
9.5.4 ロードバランス使用時の注意事項 222
9.6 Null インタフェース 223
9.7 ポリシールーティング 225
9.7.1 ポリシールーティング機能 225
9.7.2 ポリシールーティング制御 225
9.7.3 ポリシールーティング項目 227
9.7.4 ポリシールーティング使用時の注意事項 228
9.8 DHCP/BOOTP リレーエージェント機能 229
9.8.1 サポート仕様 229
9.8.2 DHCP/BOOTP パケットを受信したときのチェック内容 229
9.8.3 中継時の設定内容 229
9.8.4 ネットワーク構成例 230
9.8.5 DHCP/BOOTP リレーエージェント機能使用時の注意事項 234
9.9 DHCP サーバ機能 235
9.9.1 サポート仕様 235
9.9.2 接続構成 235
9.9.3 サポート DHCP オプション 237
9.9.4 DHCP サーバ機能使用時の注意事項 240
9.10 DHCP クライアント機能 242
9.10.1 サポート仕様 242
9.10.2 接続構成 242
9.10.3 サポート DHCP オプション 243
9.10.4 ネットワーク構成例 246
9.11 DNS リレー機能 247
9.11.1 サポート仕様 247
9.11.2 接続構成 247
9.11.3 構成定義情報による動作内容 247
9.11.4 ネットワーク構成例 248
9.12 NAT，NAPT 機能 249
9.12.1 サポート仕様 249
9.12.2 接続構成 249
9.12.3 NAT，NAPT のアドレス変換方式 251
9.12.4 サポートプロトコル 252
9.12.5 ネットワーク構成例 253
9.12.6 NAT と他機能併用時の注意事項 253

10 RIP ／ OSPF 257
10.1 IPv4 ルーティング 258
10.1.1 スタティックルーティングとダイナミックルーティング 258
10.1.2 経路情報 258
10.1.3 ルーティングプロトコルごとの適用範囲 259
10.2 ネットワーク設計の考え方 260
10.2.1 アドレス設計 260
10.2.2 直結経路の取り扱い 260
10.2.3 アドレス境界の設計 261
10.2.4 共用アドレスインタフェース 262
10.2.5 パーシャルメッシュ・ネットワークの設計 264
10.2.6 マルチホーム・ネットワークの設計 265
10.3 経路制御 (RIP/OSPF) 266
10.3.1 スタティックルーティング 266
10.3.2 ダイナミックルーティング (RIP/OSPF) 269
10.3.3 スタティックルーティングとダイナミックルーティング (RIP/OSPF) の同時動作 269
10.3.4 経路削除保留機能 270
10.4 RIP 271
10.4.1 RIP 概説 271
10.4.2 経路選択アルゴリズム 272
10.4.3 RIP-1 での経路情報の広告 272
10.4.4 RIP-2 の機能 277
10.4.5 RIP による経路広告／切り替えタイミング 278
10.4.6 メッセージ送受信相手の限定 281
10.4.7 RIP 使用時の注意事項 281
10.5 OSPF 284
10.5.1 OSPF 概説 284
10.5.2 経路選択アルゴリズム 285
10.5.3 イコールコストマルチパス 287
10.5.4 エリア分割 288
10.5.5 ルータ間の接続の検出 292
10.5.6 AS 外経路と AS 境界ルータ 294
10.5.7 認証 297
10.5.8 OSPF マルチバックボーン機能 297
10.5.9 経路選択の優先順位 299
10.5.10 OSPF 使用時の注意事項 300
10.6 経路フィルタリング (RIP/OSPF) 302
10.6.1 インポート・フィルタ (RIP/OSPF) 302
10.6.2 エキスポート・フィルタ (RIP/OSPF) 303
10.7 経路集約 (RIP/OSPF) 306
10.8 複数プロトコル同時動作時の注意事項 308

10.8.1 OSPF または RIP-2 と RIP-1 の同時動作 308
10.8.2 複数のプロトコルで同じ宛先の経路を学習する場合の注意事項 310
10.8.3 RIP による経路情報広告時の注意事項 310

11 BGP4 313

11.1 BGP4 概説 314
11.1.1 経路情報 314
11.1.2 BGP4 の適用範囲 315
11.1.3 ネットワーク設計の考え方 315
11.2 経路制御 (BGP4) 316
11.2.1 スタティックルーティング 316
11.2.2 ダイナミックルーティング (BGP4) 316
11.2.3 スタティックルーティングとダイナミックルーティング (BGP4) の同時動作 316
11.2.4 経路削除保留機能 317
11.3 BGP4 319
11.3.1 BGP4 の基礎 319
11.3.2 経路選択アルゴリズム 320
11.3.3 コミュニティ 328
11.3.4 ルート・フラップ・ダンピング 329
11.3.5 ルート・リフレクション 330
11.3.6 コンフィデレーション 332
11.3.7 BGP4 マルチパス 335
11.3.8 サポート機能のネゴシエーション 337
11.3.9 ルート・リフレッシュ 338
11.3.10 TCP MD5 認証 339
11.3.11 グレースフル・リスタート 339
11.3.12 BGP4 使用時の注意事項 340
11.4 経路フィルタリング (BGP4) 343
11.4.1 インポート・フィルタ (BGP4) 343
11.4.2 エキスポート・フィルタ (BGP4) 346
11.5 経路集約 (BGP4) 349

12 IS-IS 351

12.1 IS-IS 概説 352
12.2 IS-IS 356
12.2.1 経路情報広告の基礎 356
12.2.2 エリア分割とレベル 359
12.2.3 経路選択アルゴリズム 363
12.2.4 経路学習 365
12.2.5 認証 (IS-IS) 365
12.2.6 IS-IS 詳細 368

12.3 経路フィルタリング 376
12.3.1 インポート・フィルタ (IS-IS) 376
12.3.2 エキスポート・フィルタ (IS-IS) 376
12.4 経路集約 (IS-IS) 378
12.5 制限事項 379

13 IPv4 マルチキャスト 381
13.1 マルチキャスト概説 382
13.1.1 マルチキャストアドレス 382
13.1.2 マルチキャストのインタフェース種別 383
13.1.3 マルチキャストルーティング機能 383
13.2 グループマネージメント機能 385
13.2.1 IGMP メッセージサポート仕様 385
13.2.2 IGMP 動作 385
13.2.3 Querier の決定 386
13.2.4 グループメンバの管理 388
13.2.5 IGMP V1 ルータとの混在 389
13.2.6 IGMP V1 ホストとの混在 389
13.2.7 PIM-DM の Querier 決定動作 389
13.2.8 IGMP タイマ 389
13.3 マルチキャスト中継機能 390
13.4 経路制御機能 391
13.4.1 マルチキャストルーティングプロトコル概説 391
13.4.2 PIM-DM 391
13.4.3 DVMRP 400
13.4.4 PIM-SM 408
13.4.5 PIM-SSM 414
13.5 マルチキャストトンネル機能 417
13.5.1 マルチキャストトンネリング 417
13.6 ネットワーク設計の考え方 418
13.6.1 マルチキャスト中継 418
13.6.2 冗長経路 (障害などによる経路切り替え) 419
13.6.3 適応ネットワーク構成 419

第 5 編 IPv6 ルーティング

14 IPv6 パケット中継 425
14.1 IPv6 概説 426
14.2 アドレッシング 427

14.2.1 IPv6 アドレス 427
14.2.2 アドレス表記方法 429
14.2.3 アドレスフォーマットプレフィックス 429
14.2.4 ユニキャストアドレス 430
14.2.5 マルチキャストアドレス 433
14.2.6 IPv6 アドレス付与単位 435
14.2.7 本装置で使用する IPv6 アドレスの扱い 436
14.2.8 ステートレスアドレス自動設定機能 437
14.2.9 ホスト名情報 438
14.3 IPv6 レイヤ機能 439
14.4 通信機能 440
14.4.1 インターネットプロトコル　バージョン 6 (IPv6) 440
14.4.2 ICMPv6 442
14.4.3 NDP 443
14.5 中継機能 445
14.5.1 ルーティングテーブルの内容 445
14.5.2 ルーティングテーブルの検索 445
14.6 フィルタリング 446
14.6.1 フィルタリング項目 446
14.6.2 拡張ヘッダ追跡機能 447
14.7 ロードバランス 449
14.7.1 ロードバランス概説 449
14.7.2 ロードバランス仕様 449
14.7.3 出力インタフェースの決定 450
14.7.4 Hash 値の計算方法 450
14.7.5 ロードバランス使用時の注意事項 451
14.8 Null インタフェース 452
14.9 IPv6 DHCP サーバ機能 453
14.9.1 サポート仕様 453
14.9.2 サポート DHCP オプション 454
14.9.3 配布プレフィクスの経路情報 456
14.9.4 DHCP サーバ機能使用時の注意事項 457
14.10 NAT-PT 機能 458
14.10.1 サポート仕様 458
14.10.2 NAT-PT プレフィックス 460
14.10.3 動的 NAPT-PT 460
14.10.4 静的 NAT-PT および静的 NAPT-PT 461
14.10.5 ALG 463
14.10.6 NAT-PT 機能使用時の注意事項 466
14.11 トンネル 472
14.11.1 IPv6 over IPv4 トンネル 472
14.11.2 IPv4 over IPv6 トンネル 472

14.11.3 6to4 トンネル 473
14.11.4 トンネル機能使用時の注意事項 474
14.12 RA 481
14.12.1 RA によるアドレス情報配布 481
14.12.2 RA 情報変更時の例 484
14.13 IPv6 使用時の注意事項 485

15 RIPng/OSPFv3 487

15.1 IPv6 ルーティング 488
15.1.1 スタティックルーティングとダイナミックルーティング 488
15.1.2 経路情報 488
15.1.3 ルーティングプロトコルごとの適用範囲 488
15.2 ネットワーク設計の考え方 489
15.2.1 アドレス設計 489
15.2.2 直結経路の取り扱い 489
15.2.3 マルチホーム・ネットワークの設計 490
15.3 経路制御 (RIPng/OSPFv3) 491
15.3.1 スタティックルーティング 491
15.3.2 ダイナミックルーティング (RIPng/OSPFv3) 492
15.3.3 スタティックルーティングとダイナミックルーティングの同時動作 (RIPng/OSPFv3) 492
15.3.4 経路削除保留機能 493
15.4 RIPng 494
15.4.1 RIPng 概説 494
15.4.2 経路選択アルゴリズム 495
15.4.3 RIPng での経路情報の広告 495
15.4.4 RIPng の機能 496
15.4.5 RIPng による経路広告／切り替えのタイミング 496
15.4.6 RIPng 使用時の注意事項 499
15.5 OSPFv3 501
15.5.1 OSPFv3 概説 501
15.5.2 経路選択アルゴリズム 502
15.5.3 エリア分割 504
15.5.4 ルータ間の接続の検出 508
15.5.5 AS 外経路と AS 境界ルータ 509
15.5.6 OSPFv3 マルチバックボーン機能 511
15.5.7 経路選択の優先順位 512
15.5.8 OSPFv3 使用時の注意事項 512
15.6 経路フィルタリング (RIPng/OSPFv3) 513
15.6.1 インポート・フィルタ (RIPng/OSPFv3) 513
15.6.2 エキスポート・フィルタ (RIPng/OSPFv3) 513
15.7 経路集約 (RIPng/OSPFv3) 517

16 BGP4+ 519
16.1 BGP4+ 概説 520
16.1.1 経路情報 520
16.1.2 BGP4+ の適用範囲 521
16.1.3 ネットワーク設計の考え方 521
16.2 経路制御 (BGP4+) 522
16.2.1 スタティックルーティング (BGP4+) 522
16.2.2 ダイナミックルーティング (BGP4+) 522
16.2.3 スタティックルーティングとダイナミックルーティング (BGP4+) の同時動作 522
16.2.4 経路削除保留機能 523
16.3 BGP4+ 524
16.3.1 BGP4+ の基礎概念 524
16.3.2 経路選択アルゴリズム 525
16.3.3 サポート機能のネゴシエーション 529
16.3.4 ルート・リフレクション 530
16.3.5 コミュニティ 530
16.3.6 コンフィデレーション 530
16.3.7 ルート・リフレッシュ 530
16.3.8 BGP4+ マルチパス 531
16.3.9 ルート・フラップ・ダンピング 531
16.3.10 TCP MD5 認証 531
16.3.11 グレースフル・リスタート 532
16.3.12 BGP4+ 使用時の注意事項 532
16.4 経路フィルタリング (BGP4+) 535
16.4.1 インポート・フィルタ (BGP4+) 535
16.4.2 エキスポート・フィルタ (BGP4+) 536
16.5 経路集約 (BGP4+) 539
17 IPv6 マルチキャスト 541
17.1 IPv6 マルチキャスト概説 542
17.1.1 IPv6 マルチキャストアドレス 542
17.1.2 IPv6 マルチキャストのインタフェース種別 542
17.1.3 IPv6 マルチキャストルーティング機能 543
17.2 IPv6 グループマネージメント機能 544
17.2.1 MLD の概要 544
17.2.2 MLD の動作 544
17.2.3 Querier の決定 545
17.2.4 IPv6 グループメンバの管理 546
17.2.5 MLD タイマ値 547
17.3 IPv6 マルチキャスト中継機能 548

17.3.1 中継対象アドレス 548
17.3.2 IPv6 マルチキャストパケット中継処理 548
17.4 IPv6 経路制御機能 550
17.4.1 IPv6 PIM-SM の動作 550
17.4.2 近隣検出 554
17.4.3 Forwarder の決定 555
17.4.4 DR の決定および動作 555
17.4.5 冗長経路時の注意事項 556
17.4.6 IPv6 PIM-SM タイマ仕様 556
17.4.7 IPv6 PIM-SM 使用時の注意事項 557
17.4.8 IPv6 PIM-SSM 558
17.5 ネットワーク設計の考え方 560
17.5.1 IPv6 マルチキャスト中継 560
17.5.2 IPv6 PIM-SM 560
17.5.3 冗長経路 (障害などによる経路切り替え) 560
17.5.4 適応ネットワーク構成 561

付録 565
付録 A 準拠規格 566
付録 A.1 イーサネット 566
付録 A.2 WAN 567
付録 A.3 ATM 569
付録 A.4 IPv4 ネットワーク 569
付録 A.5 RIP/OSPF 570
付録 A.6 BGP4 571
付録 A.7 IS-IS 571
付録 A.8 IPv4 マルチキャスト 572
付録 A.9 IPv6 ネットワーク 572
付録 A.10 RIPng/OSPFv3 573
付録 A.11 BGP4+ 573
付録 A.12 IPv6 マルチキャスト 574
付録 A.13 Diff-serv 574
付録 A.14 ブリッジ 574
付録 A.15 SNMP 574
付録 A.16 RADIUS 576
付録 A.17 VRRP 576
付録 B 謝辞 (Acknowledgments) 577
付録 C 用語解説 595

索引 605

1 QoS 制御機能

ネットワークを利用したサービスの多様化に伴い，通信品質を保証しないベストエフォート型のトラフィックに加え，実時間・帯域保証型のトラフィックが増加しています。本装置の QoS 制御を使用することにより，トラフィック種別に応じた通信品質を提供することができます。この章では本装置の QoS 制御機能について説明します。

1.1　QoS 制御概説

1.2　QoS 制御構造

1.3　フロー検出

1.4　帯域監視

1.5　マーカー

1.6　優先度指定

1.7　廃棄制御

1.8　シェーパ

1.9　QoS 制御機能の適用例

1.10　QoS 制御機能の仕様一覧

1.11　QoS 制御使用時の注意事項

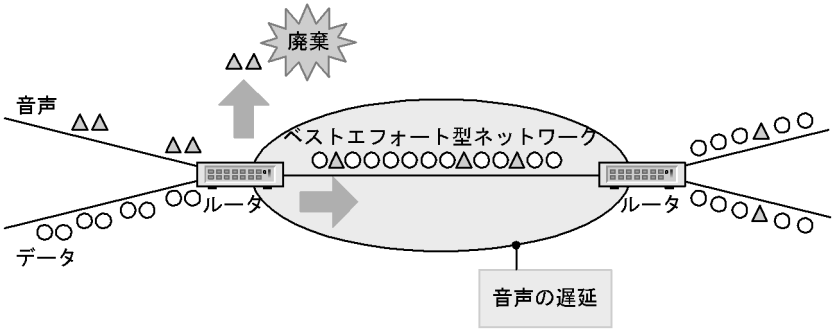
1.1 QoS 制御概説

QoS 制御とは，回線の帯域やキューのバッファ容量などの限られたネットワーク資源を有効に使用する機能です。アプリケーションごとに要求される様々な通信品質を満たすために，QoS 制御を使いネットワーク資源を適切に分配する必要があります。

1.1.1 QoS 制御の必要性

なぜ QoS 制御が必要なのか，まずこの点を考えます。次の図に QoS 制御を使用しないベストエフォート型のネットワークを示します。

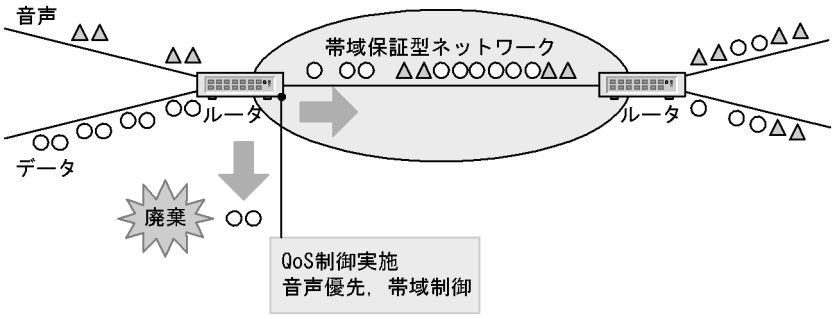
図 1-1 ベストエフォート型ネットワークの概念



ベストエフォート型の場合，ルータはトラフィックを「早い者順」に送信します。「図 1-1 ベストエフォート型ネットワークの概念」のようにデータトラフィックの負荷が高いと，データトラフィックの送信量が多くなるため，音声トラフィックの廃棄や遅延が発生します。

一方，次の図に示す QoS 制御を使用した帯域保証型ネットワークでは，音声トラフィックを優先的に送信したり，帯域制御を使用してデータトラフィックの出力量を制限したりできます。この結果，音声トラフィックの遅延を最小限に抑え，また，データトラフィックを帯域に応じて適切に送信できます。

図 1-2 帯域保証型ネットワークの概念



1.1.2 トラフィック種別と要求品質

トラフィック種別に対応する代表的な用途および通信品質を次の表に示します。

表 1-1 トラフィック種別と要求される通信品質

トラフィック種別	用途	要求品質
音声	IP 電話	低遅延，低揺らぎ（実時間型）
映像	VoD	低遅延，最低帯域保証
データ （帯域保証型）	基幹業務，重要データ	最低帯域保証
データ （ベストエフォート型）	Web アクセス，ファイル転送， バックアップ処理	余剰帯域

1.1.3 QoS 制御のメリット

QoS 制御を使用することで，次に示すメリットがあります。

● 通信品質の向上

トラフィックの要求品質に応じた QoS 制御を適用することによって，優先トラフィックの通信品質を向上できます。例えば，データトラフィックより遅延に敏感な音声トラフィックを優先的に出力することによって，音声通信の品質を良くすることができます。

● 装置・回線コストの低減

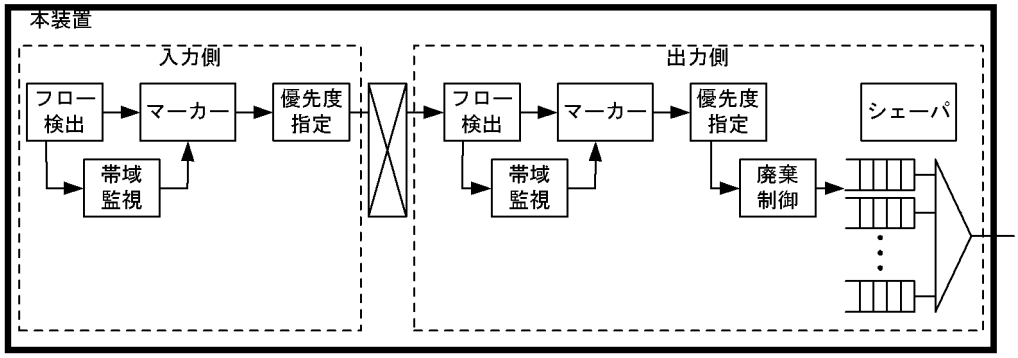
トラフィック量が増大しても，現状の装置・回線を維持したまま，重要なトラフィックの通信品質を向上できます。

今までは通信品質を改善するために，輻輳ポイントで回線を増強する方法を取ってきました。しかし，ネットワークの大規模化が進み，トラフィック量が増え続ける状況を考慮すると，回線増強だけでは限界があります。そこで，回線増強だけなく QoS 制御も併用するという方法が必要になります。

1.2 QoS 制御構造

本装置の QoS 機能のブロック図を次に示します。

図 1-3 QoS 制御の機能ブロック図



図に示した機能ブロックの概要を次の表に示します。

表 1-2 機能ブロックの概要

機能ブロック	機能概要
フロー検出	プロトコル種別や IP アドレス，ポート番号などの条件に一致するフローを検出します。
帯域監視	フローごとに帯域を監視して，帯域を超えたフローに対してペナルティを与えます。
マーカー	IP ヘッダ内の DSCP や Tag-VLAN 連携ヘッダのユーザ優先度の値を書き換える機能です。
優先度指定	フローをキューイングするキュー番号や，廃棄され易さを示すキューイング優先度を指定します。
廃棄制御	パケットの優先度とキューの状態に応じて，該当パケットをキューイングするか廃棄するかを制御します。廃棄制御は出力側だけの機能です。
シェーパ	各キューからのパケットの出力順序および出力帯域を制御します。シェーパは出力側だけの機能です。

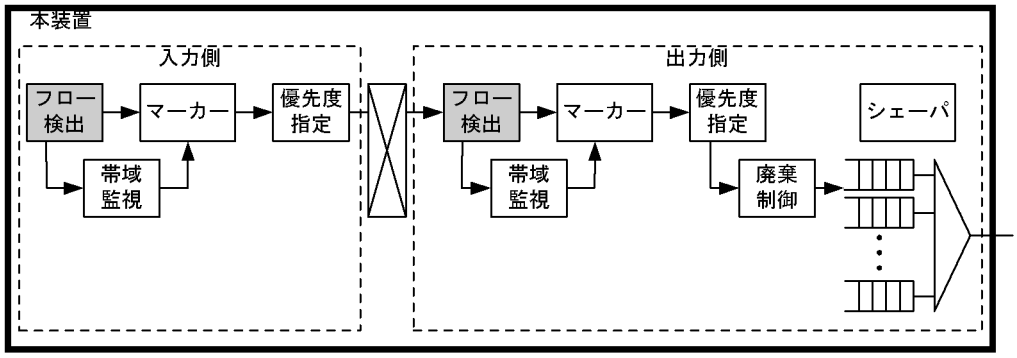
機能ブロックの詳細について，次の節から説明します。

1.3 フロー検出

フロー検出は，パケットの一連の流れであるフローを IP ヘッダや TCP ヘッダなどの条件に基づいて検出する機能です。

この節で説明する機能ブロックの位置を次の図に示します。

図 1-4 フロー検出の位置づけ



（凡例）：この節で説明する機能ブロック

(1) IP フロー検出

本装置は QoS 制御のために IP フローを検出しますが，検出するためには，あらかじめ構成定義情報で IP フローを識別するための条件を指定しておく必要があります。IP フロー識別条件とその指定方法を次の表に示します。

表 1-3 IP フロー識別条件と指定方法

条件		内容
分類	項目	
インタフェース	－	インタフェース名
Tag-VLAN 連携	VLAN ID	VLAN 番号
	ユーザ優先度	ユーザ優先度を指定します
IP ヘッダ	ユーザデータ長	上限値または下限値を指定します
	DSCP 値	TOS フィールドまたはトラフィッククラスフィールドの上位 6 ビット
	プレシデンス	TOS フィールドまたはトラフィッククラスフィールドの上位 3 ビット
	上位プロトコル	TCP ／ UDP ／ ICMP ／ IGMP などを示す番号を指定します
	送信元 IP アドレス	下限値から上限値の範囲で指定します※1
	宛先 IP アドレス	下限値から上限値の範囲で指定します※1
ICMP ヘッダ	ICMP タイプ	番号を指定します
	ICMP コード	番号を指定します
UDP ／ TCP ヘッダ	送信元ポート番号	下限値から上限値の範囲で指定します※1

条件		内容
分類	項目	
	宛先ポート番号	下限値から上限値の範囲で指定します※1
IGMP ヘッダ	IGMP タイプ	番号を指定します
ICMP6 ヘッダ	ICMPv6 タイプ	番号を指定します
	ICMPv6 コード	番号を指定します

（凡例） －：該当しない

(2) ハードウェア中継機能使用時の注意事項

ハードウェア処理による IPv6 中継での，拡張ヘッダ付きのパケットに対する 4 層情報の検索処理は，基本ヘッダのすぐ次が 4 層ヘッダになる場合にだけ，4 層ヘッダの情報を条件一致の対象にします。

ハードウェア処理時に，拡張ヘッダ付きのパケットに対し 4 層情報（TCP，UDP または ICMPv6）を条件とする IP フローを検出するには，フィルタリング検索で動作パラメータとして「拡張ヘッダ追跡」を指定したフローに条件一致させます。QoS 機能単独では 4 層情報を条件とする IP フローを検出できません。

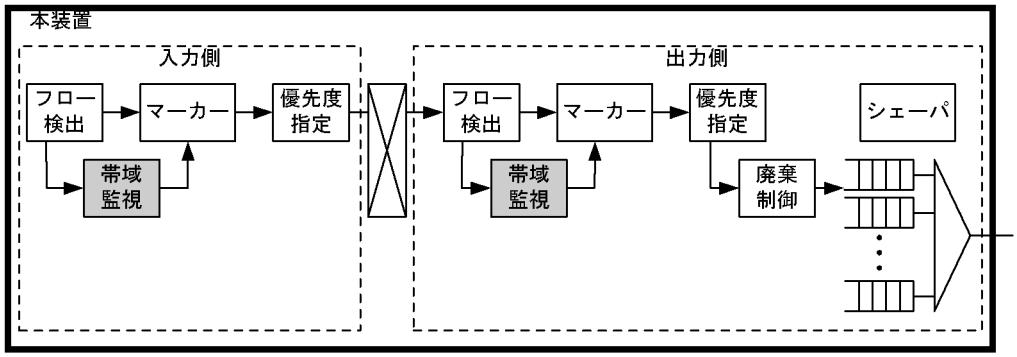
(3) IPX ／ブリッジ／ HDLC パススルーフロー検出

本装置は IPX，ブリッジ，HDLC パススルーについてもフローを検出し，QoS 制御の対象にできます。この場合も，あらかじめ構成定義情報で指定しておきます。ただし，IP のようにパケットの内容による識別は行わず，対象とするインタフェースだけを指定します。

1.4 帯域監視

この節で説明する機能ブロック図の位置を次の図に示します。

図 1-5 帯域監視の位置づけ



（凡例）：この節で説明する機能ブロック

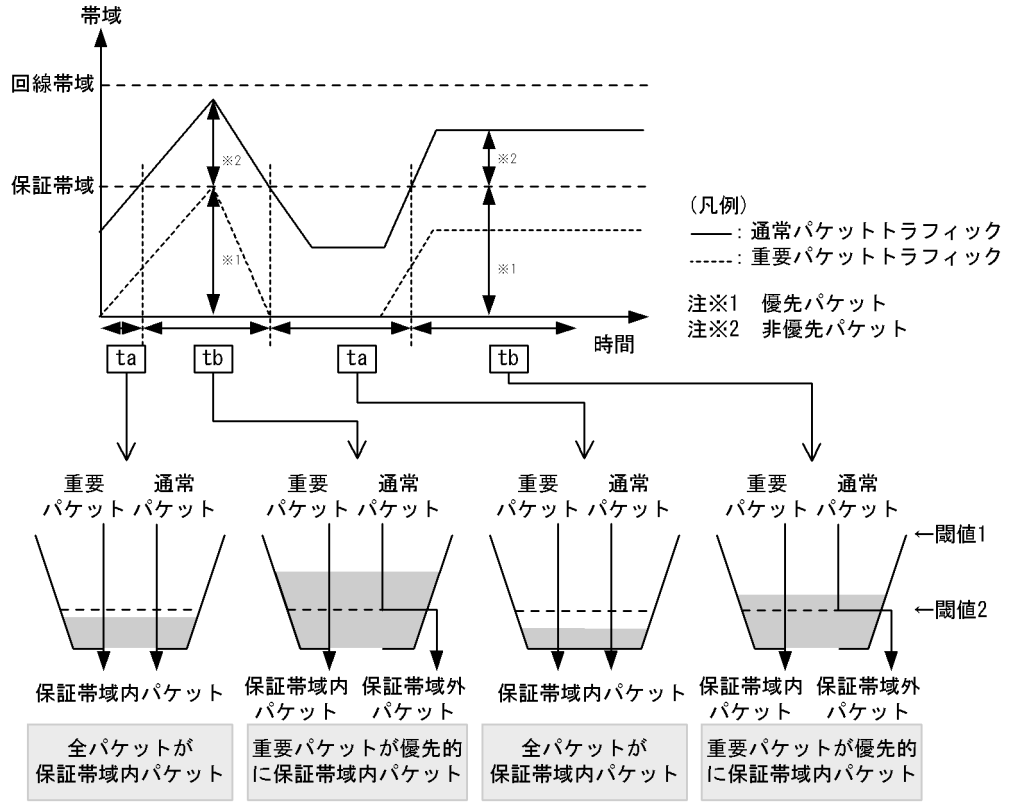
入力フローと出力フローの帯域を監視する機能です。帯域を監視するには，指定した帯域以上のフローを受信したときにどのような処理を行うかで設定します。設定できる処理を次に示します。

- パケットを廃棄します。
- パケットが廃棄しやすくなるように指定したキューイング優先度に変更します。
- パケットが廃棄しやすくなるように指定した DSCP 値に変更します。

本装置での帯域監視の方式は，Leaky Bucket アルゴリズムです。精度は± 10%です。また，**重要パケット保護機能**に対応しています。重要パケット保護機能とは，保証帯域の帯域内で，重要なパケットは優先的に保証帯域内パケットとして転送し，通常のパケットは重要なパケットが全保証帯域を使用して転送していない場合に保証帯域内パケットとして転送する機能です。重要パケット保護機能は，二つの閾値を所持する Leaky Bucket アルゴリズムで実現しています。

二つの閾値を持つ Leaky Bucket アルゴリズムの動作概要を次の図に示します。

図 1-6　二つの閾値を持つ Leaky Bucket アルゴリズムの動作概要



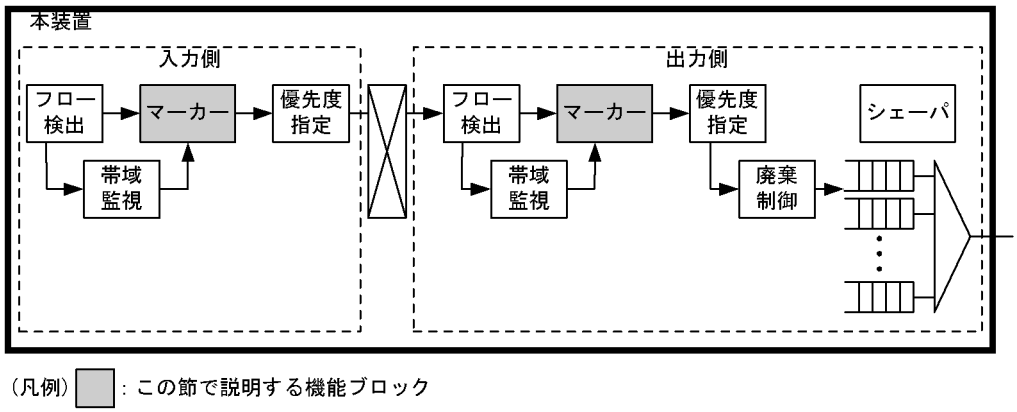
二つの閾値を持つ場合も Leaky Bucket アルゴリズムと同様の考え方です。重要パケット保護機能を，「図 1-6　二つの閾値を持つ Leaky Bucket アルゴリズムの動作概要」に示すように水とバケツの関係で説明します。バケツの深さは重要なパケットのバケツの深さ閾値 2 とそれ以外の通常パケット用の閾値 1 を持ちます。バケツにはパケット到着時にパケット長に応じた水を加えます。

- すべてのパケットが保証帯域内パケットと判定される場合
  パケット到着時にそれぞれの閾値に対して水が溢れない (受信する帯域が保証帯域以下) 場合に保証帯域内パケットと判定します。
- 重要なパケットが優先的に保証帯域内パケットとして送信される場合
  送信帯域が保証帯域を超えて閾値 2 以上の水が蓄積されると，重要なパケットが優先的に保証帯域内パケットとして送信されます。

1.5 マーカー

マーカーは，Tag-VLAN 連携ヘッダ内のユーザ優先度および IP ヘッダ内の DSCP を書き換える機能です。この節で説明するマーカーの位置づけを次の図に示します。

図 1-7 マーカーの位置づけ



(1) DSCP 書き換え

検出したフローの TOS フィールド（IPv4 ヘッダ）またはトラフィッククラスフィールド（IPv6 ヘッダ）の上位 6 ビットを書き換えます。ユニキャストは，入力側と出力側で DSCP 書き換えを設定できます。マルチキャストは，入力側だけ DSCP 書き換えを設定できます。

この機能を利用することによって，検出したフローのユーザ優先度を DSCP 値に対応づけることができます。例えば，ユーザ優先度が 7 のフローに対して DSCP を 63 に設定できます。

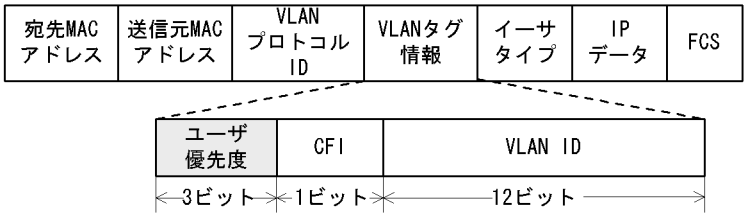
また，帯域監視機能ブロックからの指示によって，最低帯域を超えたフローの DSCP を書き換えることができます。例えば，最低帯域を超えたフローに対して，DSCP を 0 に設定できます。

(2) ユーザ優先度書き換え

検出したフローの Tag-VLAN 連携ヘッダ内にあるユーザ優先度を書き換えます。ユーザ優先度は次の図に示すように，VLAN タグ情報フィールドの先頭の 3 ビットを指します。この機能は，出力側だけ設定できます。

この機能を利用することによって，検出したフローの DSCP 値をユーザ優先度に対応付けることができます。例えば，DSCP が 63 のフローに対してユーザ優先度を 7 に設定できます。

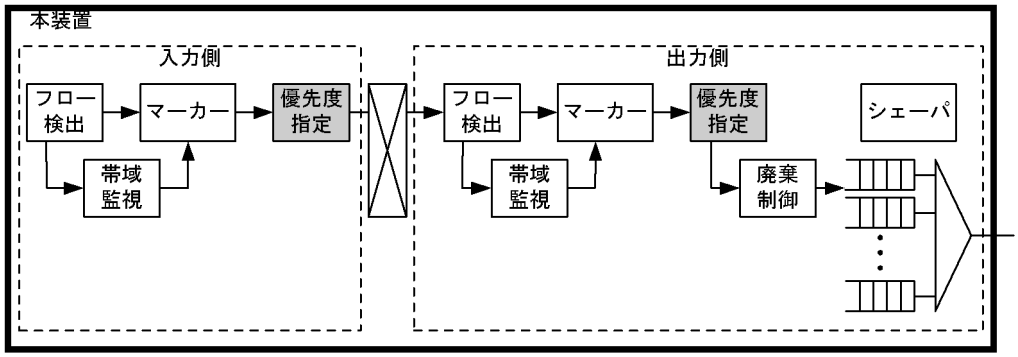
図 1-8 Tag-VLAN 連携のヘッダフォーマット



1.6 優先度指定

この節で説明する機能ブロックの位置を次の図に示します。

図 1-9 優先度指定の位置づけ



（凡例）：この節で説明する機能ブロック

(1) フロー単位による優先度決定

入力パケットが属するフローを検出し，該当するフローに対応する出力優先度とキューイング優先度を決定し QoS 制御を実施します。

(2) DSCP 値による優先度決定

入力 IP パケットの DSCP フィールドの値によって出力優先度とキューイング優先度を決定して QoS 制御を実施します。DSCP は IPv4 パケットでは TOS フィールドの上位 6 ビット，IPv6 パケットではトラフィッククラスフィールドの上位 6 ビットに当たります。

表 1-4 TOS 値に対応する優先度

precedence	TOS 値	出力優先度	キューイング優先度
0	0 ～ 31	1	4
1	32 ～ 39	2	1
	40 ～ 47	2	4
	48 ～ 55	2	3
	56 ～ 63	2	2
2	64 ～ 71	3	1
	72 ～ 79	3	4
	80 ～ 87	3	3
	88 ～ 95	3	2
3	96 ～ 103	4	1
	104 ～ 111	4	4
	112 ～ 119	4	3
	120 ～ 127	4	2
4	128 ～ 135	5	1
	136 ～ 143	5	4

precedence	TOS 値	出力優先度	キューイング優先度
	144 ～ 151	5	3
	152 ～ 159	5	2
5	160 ～ 191	6	1
6	192 ～ 223	7	1
7	224 ～ 255	8	1

(3) ユーザ優先度による優先度決定

Tag-VLAN 連携のユーザ優先度フィールドの値によって出力優先度を決定して，QoS 制御を実施します。

(4) 構成定義情報で優先度を決定できるパケット

IP パケット種別ごとに構成定義情報によって優先度を決定できるパケットと，構成定義情報の設定内容に関係なく固定的に優先度が決定するパケットがあります。

パケット種別ごとの優先度を「表 1-5　パケット種別ごとの優先度」,「表 1-8　グループ帯域制御・16VLL 帯域制御指定時のパケット種別ごとの優先度」,「表 1-9　64VLL 帯域制御指定時のパケット種別ごとの優先度」に示します。

表 1-5　パケット種別ごとの優先度

パケット種別	全 IP パケット優先度指定機能※1	RP 種別	IP フロー検出条件の状態	出力回線のキュー数ごとの出力優先度※2							キューイング優先度
				4	8	16	32	64	250	1000	
本装置が生成する ARP(ARP Request/ ARP Response) パケット	有効・無効	―	―	4	8	16	32	64	250	1000	4
本装置が生成するレイヤ 2 パケット (WAN)	有効・無効	―	―	4	8	16	32	64	250	1000	4
本装置が生成する IPv4 パケット※5 (RIP，OSPF，BGP，telnet，ftp，snmp，igmp，pim など)	無効	―	一致・不一致	4	8	16	32	64	250	1000	4※4
	有効	―	一致	※3※5							
			不一致	4	8	16	32	64	250	1000	4※4
本装置が生成するエラーを通知するための IPv4 ICMP パケット	無効	―	一致・不一致	2	4	7	13	25	98	392	1
	有効	―	一致	※3							
			不一致	2	4	7	13	25	98	392	4

パケット種別	全 IP パケット優先度指定機能※1	RP 種別	IP フロー検出条件の状態	出力回線のキュー数ごとの出力優先度※2							キューイング優先度
				4	8	16	32	64	250	1000	
本装置が中継する次の IPv4 パケット • オプション (IP ヘッダ) 付きパケット • フラグメントしたパケット • 方向転換 (Redirect) したパケット • ARP 未解決パケット • DVMRP トンネルインタフェースに送出する DVMRP カプセル化パケット	無効	―	一致・不一致	2	4	7	13	25	98	392	4
	有効※5	―	一致	※3							
			不一致	2	4	7	13	25	98	392	4
上記以外の IPv4 パケット	有効・無効	―	一致	※3							
			不一致	2	4	7	13	25	98	392	4
本装置が生成する IPv6 パケット	有効・無効	―	一致	※3							
			不一致	4	8	16	32	64	250	1000	4
本装置が中継する IPv6 パケット	有効・無効	―	一致	※3							
			不一致	2	4	7	13	25	98	392	4

(凡例) ―：該当しない

注※ 1　全 IP パケットの優先度を flow 構成定義によって指定できるようにする機能です。

注※ 2　出力優先度はパケットを積むキュー番号を意味します。

注※ 3　flow qos 構成定義で指定した優先度です。

注※ 4　本条件でパケットを中継する場合，パケットを受信した RP と送信した RP の組み合わせごとの優先度指定方式を「表 1-6　受信した RP と送信した RP の組み合わせごとの優先度指定方式」に示します。

注※ 5　本装置が生成する IPv4 パケットの一覧を「表 1-7　本装置が生成する主な IPv4 パケット」に示します。

表 1-6　受信した RP と送信した RP の組み合わせごとの優先度指定方式

RP 種別		優先度指定方式
入力側	出力側	
AX2000R 内蔵 RP	AX2000R 内蔵 RP	入力側，出力側で指定した優先度を両側で指定した場合は出力側で指定した優先度

表 1-7　本装置が生成する主な IPv4 パケット

パケット名称	プロトコル (番号)	ポート番号	タイプ番号	備考
Echo Reply	ICMP(1)	―	0	エコー応答 (ping)
Echo		―	8	エコー要求 (ping)
Membership Query	IGMP(2)	―	17※3	メンバーシップ要求

パケット名称	プロトコル (番号)	ポート番号	タイプ番号	備考
Version1 Membership Report	IGMP(2)	―	18 ※3	バージョン 1 のメンバーシップ報告
ftp	TCP(6)	20，21 ※1	―	―
telnet		23 ※1	―	―
time		37 ※1	―	―
www		80 ※1	―	―
bgp		179 ※1	―	―
rlogin		513 ※1	―	―
echo	UDP(17)	7 ※2	―	―
time		37 ※2	―	―
bootps/bootpc		67,68 ※2	―	DHCP
ntp		123 ※2	―	―
snmp		161 ※2	―	―
sysylog		514 ※2	―	―
rip		520 ※2	―	―
ospf	89	―	―	―

(凡例) ―：該当しない

注※ 1　送信元ポート番号および宛先ポート番号の片方がこのポート番号です。

注※ 2　送信元ポート番号がこのポート番号です。

注※ 3　IGMP バージョンと IGMP タイプを合わせたものがこのタイプ番号です。

表 1-8　グループ帯域制御・16VLL 帯域制御指定時のパケット種別ごとの優先度

パケット種別	全 IP パケット優先度指定機能※1	IP フロー検出条件の状態	出力グループ番号と出力優先度※2		キューイング優先度
			グループ数 2 まで	グループ数 3 以上	
本装置が生成する ARP(ARP Request/ ARP Response) パケット	有効・無効	―	(グループ 1) 4	(グループ 16) 4	4
本装置が生成するレイヤ 2 パケット (WAN)	有効・無効	―	(グループ 1) 4	(グループ 16) 4	4
本装置が生成する IPv4 パケット※5 (RIP，OSPF，BGP，telnet，ftp，snmp，igmp，pim など)	無効	一致・不一致	(グループ 1) 4	(グループ 16) 4	4 ※4
	有効	一致	※3※5		
		不一致	(グループ 1) 4	(グループ 16) 4	4 ※4
本装置が生成するエラーを通知するための IPv4 ICMP パケット	無効	一致・不一致	(グループ 1) 2	(グループ 8) 1	1
	有効	一致	※3		
		不一致	(グループ 1) 2	(グループ 8) 1	4

パケット種別	全 IP パケット優先度指定機能※1	IP フロー検出条件の状態	出力グループ番号と出力優先度※2		キューイング優先度
			グループ数 2 まで	グループ数 3 以上	
本装置が中継する次の IPv4 パケット • オプション (IP ヘッダ) 付きパケット • フラグメントしたパケット • 方向転換 (Redirect) したパケット • ARP 未解決パケット • DVMRP トンネルインタフェースに送出する DVMRP カプセル化パケット	無効	一致・不一致	(グループ 1) 2	(グループ 8) 1	4
	有効※5	一致	※3		
		不一致	(グループ 1) 2	(グループ 8) 1	4
上記以外の IPv4 パケット	有効・無効	一致	※3		
		不一致	(グループ 1) 2	(グループ 8) 1	4
本装置が生成する IPv6 パケット	有効・無効	一致	※3		
		不一致	(グループ 1) 4	(グループ 16) 4	4
本装置が中継する IPv6 パケット	有効・無効	一致	※3		
		不一致	(グループ 1) 2	(グループ 8) 1	4

(凡例) －：該当しない

注※ 1　全 IP パケットの優先度を flow 構成定義によって指定できるようにする機能です。

注※ 2　出力優先度はパケットを積むキュー番号を意味します。出力グループのキュー数は 4 固定です。

注※ 3　flow qos 構成定義で指定した優先度です。

注※ 4　本条件でパケットを中継する場合，パケットを受信した RP と送信した RP の組み合わせごとの優先度指定方式を「表 1-6　受信した RP と送信した RP の組み合わせごとの優先度指定方式」に示します。

注※ 5　本装置が生成する IPv4 パケットの一覧を「表 1-7　本装置が生成する主な IPv4 パケット」に示します。

注※ 6　16VLL 帯域制御の場合は，出力グループ番号は出力 VLL 番号となります。16VLL 帯域制御については，「1.8.6　帯域制御 (トラフィック指定)」を参照してください。

表 1-9　64VLL 帯域制御指定時のパケット種別ごとの優先度

パケット種別	全 IP パケット優先度指定機能※1	IP フロー検出条件の状態	出力 VLL 番号と出力優先度※2※7	キューイング優先度
本装置が生成する ARP(ARP Request/ARP Response) パケット	有効・無効	－	(VLL64)4	4
本装置が生成するレイヤ 2 パケット (WAN)	有効・無効	－	(VLL64)4	4
本装置が生成する IPv4 パケット※5 (RIP，OSPF，BGP，telnet，ftp，snmp，igmp，pim など)	無効	一致・不一致	(VLL64)4	4※4
	有効	一致	※3※5	4※6
		不一致	(VLL64)4	4※4
本装置が生成するエラーを通知するための IPv4 ICMP パケット	無効	一致・不一致	(VLL25)1	1
	有効	一致	※3	4※6
		不一致	(VLL25)1	4

パケット種別	全 IP パケット優先度指定機能※1	IP フロー検出条件の状態	出力 VLL 番号と出力優先度※2※7	キューイング優先度
本装置が中継する次の IPv4 パケットオプション(IP ヘッダ)付きパケット フラグメントしたパケット 方向転換 (Redirect) したパケット ARP 未解決パケット DVMRP トンネルインタフェースに送出する DVMRP カプセル化パケット	無効	一致・不一致	(VLL25)1	4
	有効※5	一致	※3	4※6
		不一致	(VLL25)1	4
上記以外の IPv4 パケット	有効・無効	一致	※3	4※6
		不一致	(VLL25)1	4
本装置が生成する IPv6 パケット	有効・無効	一致	※3	4※6
		不一致	(VLL64)4	4
本装置が中継する IPv6 パケット	有効・無効	一致	※3	4※6
		不一致	(VLL25)1	4

(凡例) －：該当しない

注※1　全 IP パケットの優先度を flow 構成定義によって指定できるようにする機能です。

注※2　出力優先度はパケットを積むキュー番号を意味します。出力 VLL のキュー数は 4 固定です。

注※3　flow qos 構成定義で指定した出力優先度です。ユーザ優先度と送信キュー番号の対応を「表 1-10　ユーザ優先度と送信キュー番号およびキューイング優先度の関係 (NEB100-1TC)」に示します。

注※4　本条件でパケットを中継する場合，パケットを受信した RP と送信した RP の組み合わせごとの優先度指定方式を「表 1-6　受信した RP と送信した RP の組み合わせごとの優先度指定方式」に示します。

注※5　本装置が生成する IPv4 パケットの一覧を「表 1-7　本装置が生成する主な IPv4 パケット」に示します。

注※6　flow qos 構成定義で指定したキューイング優先度にかかわらず，設定値はすべて 4 固定となります。

注※7　出力 VLL は帯域制御を設定した Tag-VLAN 連携回線となります。また，64VLL 帯域制御については，「1.8.6　帯域制御 (トラフィック指定)」を参照してください。

(5) 優先度設定時の注意事項

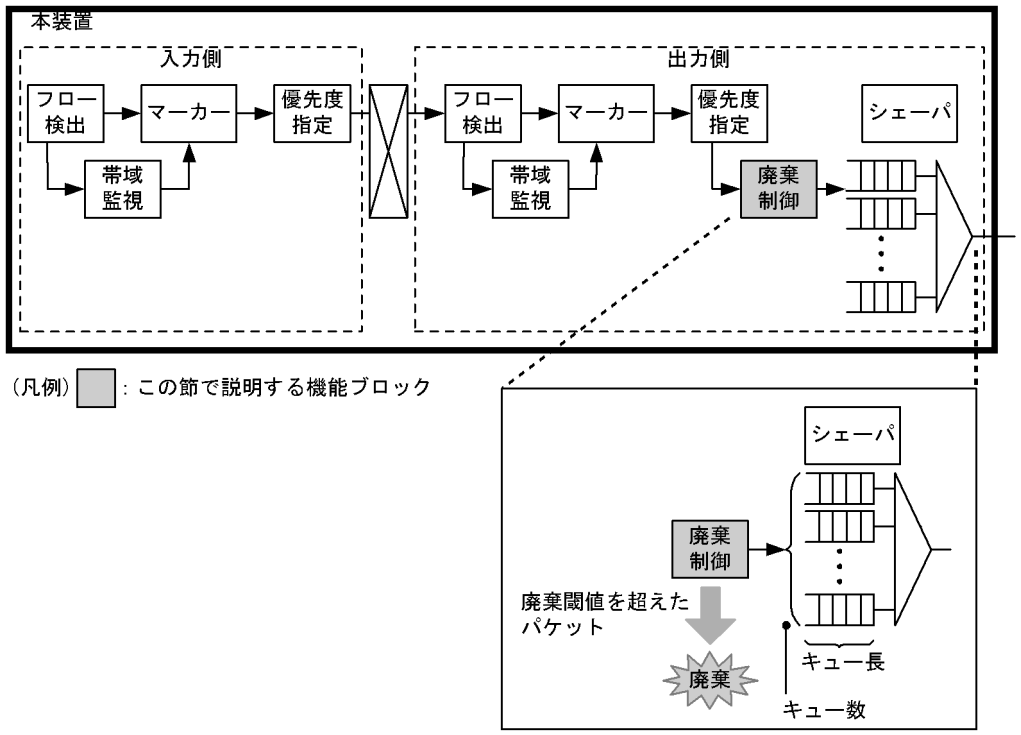
双方向通信に対して完全優先を行う場合は，両方向のフローに対して優先度の設定をする必要があります。

1.7 廃棄制御

廃棄制御は，パケットの優先度とキューの状態に応じて，該当パケットをキューイングするか廃棄するかを制御します。キューにパケットが滞留している場合，同じ出力優先度でもキューイング優先度を変えることによって，さらに木目細かい QoS を実現できます。

この節で説明する機能ブロックの位置とその拡大図を次の図に示します。廃棄制御は出力側だけの機能です。また，「図 1-10　廃棄制御の位置づけとその拡大図」に示すとおり，一つのキューにキューイングできる最大のパケット数を「キュー長」，一つのインタフェースが保有するキューの最大数を「キュー数」と呼びます。

図 1-10　廃棄制御の位置づけとその拡大図



キューにパケットが滞留している場合，キューイング優先度に従って出力キューにあるパケットを廃棄します。キューイング優先度に従って廃棄を開始するキュー長を NIF ごとに設定できます。キューイング優先度は 1(低)～4(高)の範囲で指定します。キューイング優先度が高いパケットほど廃棄しません。
キューイング優先度の考え方を，例を使用して説明します。

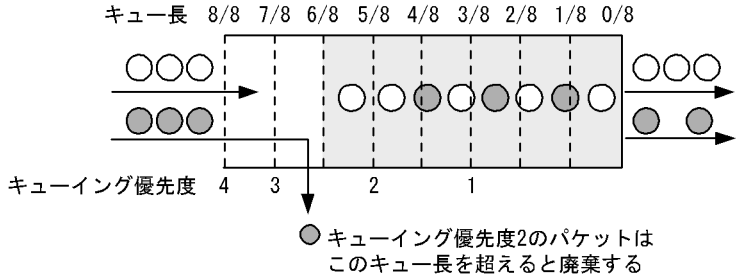
(例)

キューイング優先度ごとのキュー長を，次に示すように設定します。キュー長は最大キュー長を 8 としたときの割合で設定します。

- キューイング優先度 1 のとき 3/8
- キューイング優先度 2 のとき 5/8
- キューイング優先度 3 のとき 7/8
- キューイング優先度 4 のとき 8/8

パケットをキューイングしようとしたときのキュー長が 6/8 の場合は，該当するパケットのキューイング優先度が 3 の場合は廃棄されませんが，2 の場合は廃棄されます。キューイング制御の概念を次の図に示します。

図 1-11　キューイング制御の概念



（凡例）● ：キューイング優先度2のパケット
○ ：キューイング優先度3のパケット

NEB100-1TC で 64VLL 帯域制御を行っている場合は，キューイング優先度は設定値にかかわらず常に 4 となります。64VLL 帯域制御については，「1.8.6　帯域制御（トラフィック指定）」を参照してください。また，ユーザ優先度と送信キュー番号は固定的になっています。ユーザ優先度と送信キュー番号の関係を次の表に示します。

表 1-10　ユーザ優先度と送信キュー番号およびキューイング優先度の関係 (NEB100-1TC)

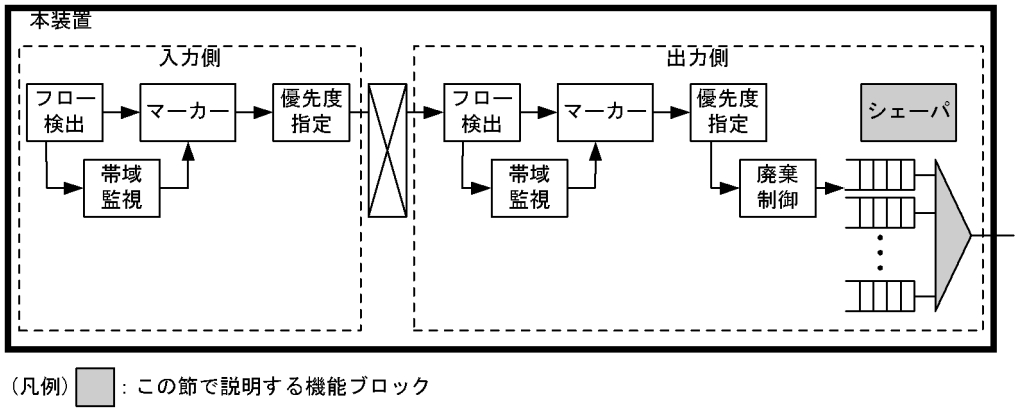
ユーザ優先度	送信キュー番号※	キューイング優先度
0	1	4
1		
2	2	
3		
4	3	
5		
6	4	
7		

注※　番号の大きいほうが高い優先度となります。

1.8 シェーパ

シェーパは，パケットの出力順序や出力帯域を制御する機能です。この節で説明するシェーパの位置づけを次の図に示します。

図 1-12 シェーパの位置づけ



本装置はシェーパとして完全優先，最低帯域保証，ラウンドロビン，均等最低帯域保証，最低帯域保証(kbit/s 指定)，帯域制御(トラフィック指定)，グループ帯域制御をサポートします。ただし，インタフェースごとに選択できるのは，1 種類だけです。

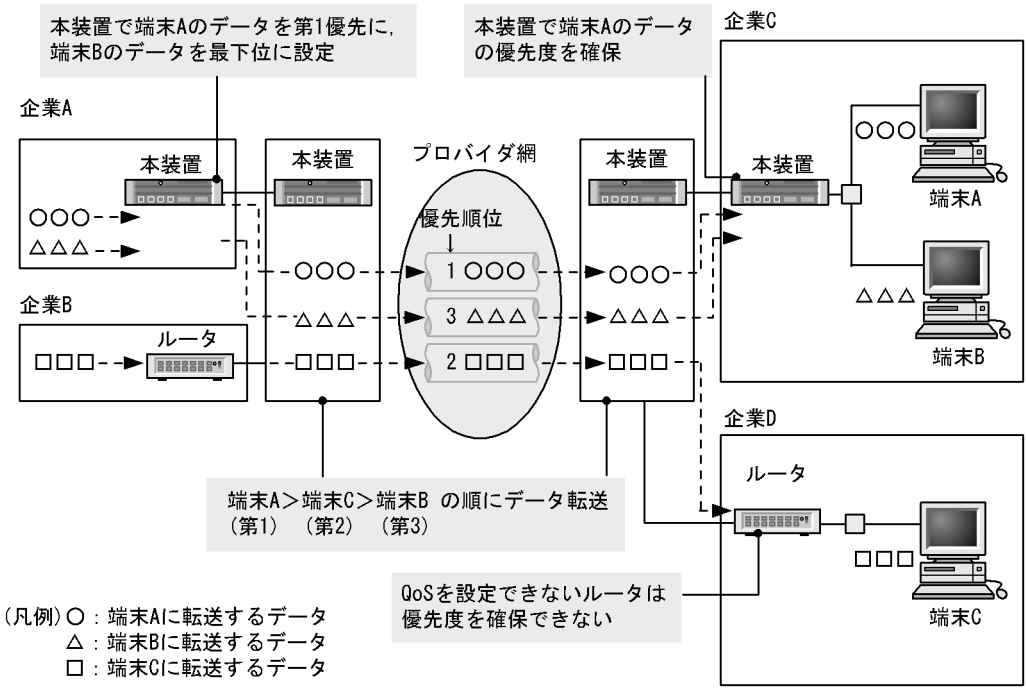
1.8.1 完全優先

優先度の高いキューにあるパケットを送信してから，優先度の低いキューにあるパケットを送信します。出力優先度の高いキューにパケットが積まれていると低いキューに積まれたパケットは送信されません。出力優先度を次に示します。

1（低）≦出力優先度≦ 8（高）

ISP のプロバイダ網を使用したデータ伝送の場合を例にして，優先制御の概要を次の図に示します。

図 1-13 優先制御の概要



1.8.2 最低帯域保証

送信帯域の最低保証を行う機能です。キューごとに指定された帯域分だけを送信します。ただし，回線の帯域が空いていれば，空いている帯域も使用して送信します。帯域は回線の帯域の%で指定します。

1.8.3 ラウンドロビン

複数のキューにパケットが存在する場合，順番にキューを参照し，パケットを送信します。パケット長に関わらず，パケット数が均等になるように制御します。

1.8.4 均等最低帯域保証

送信帯域の均等最低保証を行う機能です。キューごとに均等に割り当てられた帯域分だけを送信します。ただし，回線の帯域が空いていれば，空いている帯域も使用して送信します。設定方法は均等な帯域を割り当てるキュー数を指定します。各キューの帯域は，回線の全帯域を指定したキュー数で割った値になります。

1.8.5 最低帯域保証 (kbit/s 指定)

送信帯域の最低保証を行う機能です。キューごとに指定された帯域分だけを送信します。ただし，回線の帯域が空いていれば，空いている帯域も使用して送信します。帯域は kbit/s 単位で指定します。

最低帯域保証 (kbit/s 指定) を指定したインタフェースでは，フロー制御で優先度指定機能によって出力優先度を決定した場合だけ，最低帯域保証 (kbit/s 指定) 機能が実行できます。フロー制御で DSCP 書き換え指定または入力パケット DSCP 値指定によって出力優先度の決定を行った場合は，最低帯域保証 (kpbs 指定) 機能は実行できません。最低帯域保証 (kbit/s 指定) とフロー制御の出力優先度決定の関係を次の表に示します。

表 1-11 最低帯域保証 kbit/s と指定フロー制御の出力優先度決定の関係

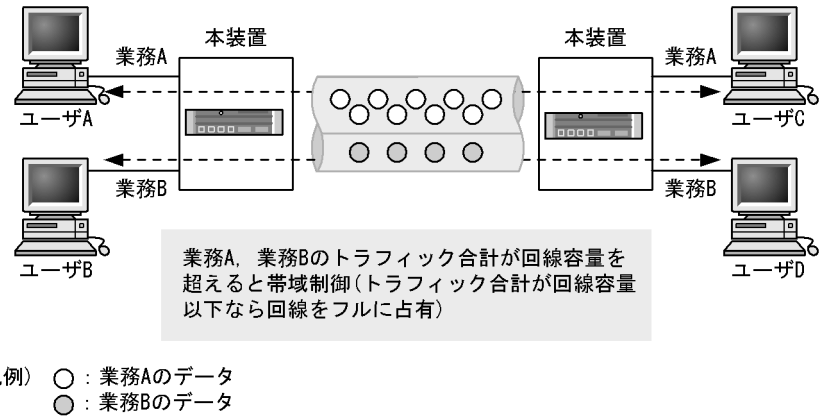
フロー制御での優先度決定方法	最低帯域保証 kbit/s 指定機能の実行
出力優先度指定	○
DSCP 書き換え指定	－
入力パケット DSCP 値指定	－

（凡例） ○：実行できる －：実行できない

1.8.6 帯域制御（トラフィック指定）

トラフィックに対して帯域を割り当てることによって，輻輳時も該当トラフィックは設定した帯域を確保することができます。また，この制御を使用して広域イーサネットサービスへ接続できます。例えば，回線帯域が 100Mbit/s で ISP との契約帯域が 50Mbit/s の場合，あらかじめ回線帯域を 50Mbit/s 以下に抑えてパケットを送信することができます。物理帯域と契約帯域の差による輻輳を回避することができます。帯域制御の概要を次の図に示します。

図 1-14 帯域制御の概要



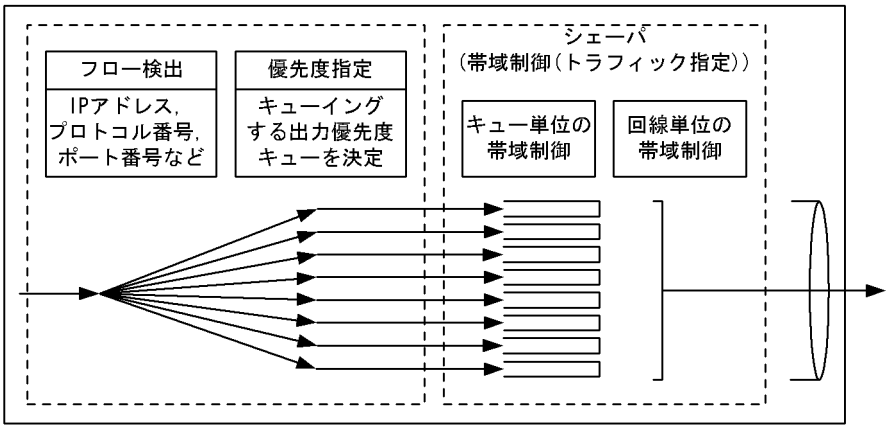
帯域制御（トラフィック指定）には，次の 2 種類があります。

- LINE 回線に対する帯域制御（トラフィック指定）
- Tag-VLAN 連携回線に対する帯域制御（トラフィック指定）

（1） LINE 回線に対する帯域制御（トラフィック指定）

帯域制御（トラフィック指定）の構造を次の図に示します。

図 1-15 帯域制御 (トラフィック指定) の仕組み



フロー検出によって検出したフローを，指定したキューにキューイングします。その後シェーパによってキューごとに帯域を確保しつつ，回線全体をシェーピングします。帯域の確保には大きく二つの制御方法があります。一つは設定した最大帯域を固定的に確保する**固定帯域制御**です。もう一つは設定した最低帯域は輻輳時でも確保しつつ，回線内に帯域が余っている場合 (**余剰帯域**)，最大帯域の範囲内で帯域を確保する**可変帯域制御**です。

なお，シェーパの動作仕様は，モデルおよび NIF 種別に応じて異なります。以降に動作仕様とサポート仕様をモデルごとに説明します。

(a) AX2001R，AX2002R，AX2002RX

AX2001R，AX2002R および AX2002RX における仕様を説明します。

● キューの状態と帯域開放

帯域制御を行うキューには，キューにパケットが全くないインアクティブ状態とパケットがキューに存在するアクティブ状態という二つの状態があります。
インアクティブ状態のとき，キューは帯域をすべて開放します。このため帯域を必要とするほかのキューが開放された帯域を利用することができます。
一方アクティブ状態のときは，固定帯域制御では最大帯域を，可変帯域制御では最低帯域を確保します。実際に使用する帯域が確保した帯域より小さい場合，未使用分の帯域は開放されません。またアクティブ状態のキューは，パケットがなくなっても一定時間経過するまでアクティブ状態を維持して，かつ帯域も確保し続けます。一定時間以内に新たなパケットがキューにキューイングされなければ，キューは帯域を開放します。

● 帯域制御 (トラフィック指定) を実行できる優先度

帯域制御 (トラフィック指定) を指定したインタフェースは，優先度指定機能によって出力優先度を決定した場合だけ，帯域制御 (トラフィック指定) が実行できます。DSCP 書き換え指定または入力パケット DSCP 値指定によって出力優先度を決定した場合は，帯域制御 (トラフィック指定) は実行できません。帯域制御 (トラフィック指定) と優先度指定機能の関係を次の表に示します。

表 1-12 帯域制御 (トラフィック指定) と優先度指定機能の関係

優先度指定機能	帯域制御 (トラフィック指定) 機能の実行
出力優先度指定	○
DSCP 書き換え指定	－
入力パケット DSCP 値指定	－

（凡例） ○：実行できる　－：実行できない

● 帯域制御サポート仕様

NIF 種別ごとの帯域制御のサポート仕様を次の表に示します。

表 1-13　NIF 種別ごとのサポート仕様

項目		NIF 種別		
		10BASE-T	100BASE-TX	1000BASE-X
		内臓イーサネット※5 NEB100-TB		NEB1G-1B
回線当たりのキュー数		4，8，64 キュー		
回線ごとの最大送信帯域※2※3※4	4 キューの場合	320kbit/s ～ 10Mbit/s	320kbit/s ～ 100Mbit/s	320kbit/s ～ 590Mbit/s
	8 キューの場合	640kbit/s ～ 10Mbit/s	640kbit/s ～ 100Mbit/s	640kbit/s ～ 590Mbit/s
	64 キューの場合	5120kbit/s ～ 10Mbit/s	5120kbit/s ～ 100Mbit/s	5120kbit/s ～ 590Mbit/s
キューごとのトラフィック種別が固定帯域制御の場合※1	キューごとの最大送信帯域※2※4	80kbit/s ～ 10Mbit/s ※3	80kbit/s ～ 100Mbit/s ※3	80kbit/s ～ 590Mbit/s ※3
キューごとのトラフィック種別が可変帯域制御の場合※1	キューごとの最低保証帯域※2※4			
	キューごとの最大送信帯域※2※4			
	最大帯域割り当て重み	1 ～ 63		

注※ 1　各キューには帯域が未設定時は最低保証帯域 80kbit/s が割り当てられます。

注※ 2　誤差は最大 2%程度です。

注※ 3　範囲外の帯域を割り当てた場合は完全優先で動作します。

注※ 4　理論限界値を考慮して設定してください。

< 理論限界値算出式 >

フレーム長 (byte：FCS 含む)*8(bit) ／
((フレーム長 (byte：FCS 含む)*8(bit) ／回線速度 (bit/s))
＋フレーム間ギャップ時間 (ns))

フレーム間ギャップ時間を次の表に示します。

回線速度 (bit/s)	フレーム間ギャップ時間 (ns)
10000000	16000
100000000	1600
1000000000	160

注※ 5　AX2001R，AX2002R，AX2002RX で内蔵されたイーサネットのことです。

（2） Tag-VLAN 連携回線に対する帯域制御 (トラフィック指定)

AX2001R，AX2002R および AX2002RX では，Tag-VLAN 連携ごとに帯域制御 (トラフィック指定) を行うことができます。一つの回線に Tag-VLAN 連携を多重化して使用している際に回線が輻輳状態となっても，Tag-VLAN 連携ごとに帯域を保証することができます。さらに Tag-VLAN 連携内のアプリケーショ

ン種別ごとに帯域制御が可能です。帯域制御設定を行っている Tag-VLAN 連携回線を VLL と呼びます。

(a) 16VLL 帯域制御

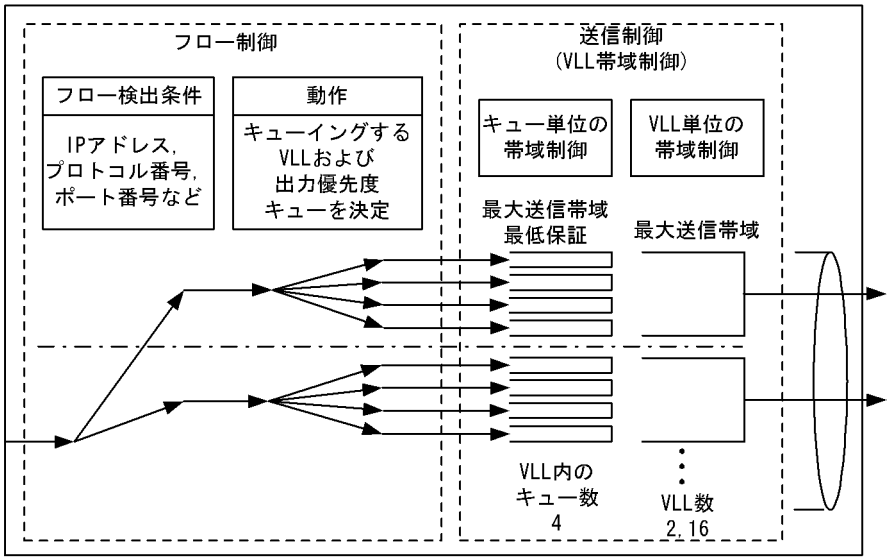
16VLL 帯域制御は，NIF 当たり，最大で 16VLL の設定が可能です。NIF は，内蔵 Ether，NEB100-4TB，NEB1G-1B で使用できます。

16VLL 帯域制御では，キューごとに以下の設定ができます。

- 固定帯域制御
- 可変帯域制御 (最低帯域保証・最大帯域保証・余剰帯域)

16VLL 帯域制御に対する帯域制御の構造を次の図に示します。

図 1-16 Tag-VLAN 連携回線に対する帯域制御 (トラフィック指定) の仕組み



フロー制御部では，フロー検出条件に一致するパケットに対してキューイングする VLL および出力優先度キューを決定します。送信制御部では，キューごとに固定帯域制御または可変帯域制御によって出力する帯域を制御し，VLL ごとに帯域制御を行います。16VLL 帯域制御では，最大 16 個の Tag-VLAN 連携回線を同時に制御可能です。なお固定帯域制御および可変帯域制御は，前述の LINE 回線に対する帯域制御 (トラフィック指定) の機能と同様です。

● キューの状態と帯域開放

帯域制御を行うキューには，キューにパケットが全くないインアクティブ状態とパケットがキューに存在するアクティブ状態という二つの状態があります。

インアクティブ状態のとき，キューは帯域をすべて開放します。このため帯域を必要とするほかのキューが開放された帯域を利用することができます。

一方アクティブ状態のときは，固定帯域制御では最大帯域を，可変帯域制御では最低帯域を確保します。実際に使用する帯域が確保した帯域より小さい場合，未使用分の帯域は開放されません。またアクティブ状態のキューは，パケットがなくなっても一定時間経過するまでアクティブ状態を維持して，かつ帯域も確保し続けます。一定時間以内に新たなパケットがキューにキューイングされなければ，キューは帯域を開放します。

● 16VLL 帯域制御を実行できる優先度

16VLL 帯域制御を指定した Tag-VLAN 連携回線は，優先度指定機能によって出力優先度を決定した場合だけ，帯域制御 (トラフィック指定) が実行できます。ユーザ優先度書き換え，DSCP 書き換え指定

または入力パケット DSCP 値指定によって出力優先度を決定した場合は，16VLLL 帯域制御は実行できません。16VLL 帯域制御と優先度指定機能の関係を次の表に示します。

表 1-14　16VLL 帯域制御と優先度指定機能の関係

優先度指定機能	16VLL 帯域制御機能の実行
出力優先度指定	○
ユーザ優先度書き換え	－
DSCP 書き換え指定	－
入力パケット DSCP 値指定	－

（凡例）　○：実行できる　－：実行できない

定義した Tag-VLAN 連携の数と帯域制御（トラフィック指定）を設定できる数との関係を次の表に示します。

表 1-15　帯域制御を設定する物理回線ごとの Tag-VLAN 連携数

Tag － VLAN 連携数		16VLL 帯域制御
物理回線当たり	NIF 当たり	設定可否
1 ～ 2	1 ～ 8	○
3 ～ 16※	3 ～ 16	○
17 以上	17 以上	－

（凡例）　○：設定可　－：設定不可

注※　Line 番号 0 だけに設定可能です。

「表 1-15　帯域制御を設定する物理回線ごとの Tag-VLAN 連携数」は，物理回線当たり二つの Tag-VLAN 連携，かつ NIF 全体として 8 個の Tag-VLAN 連携（＝二つの Tag-VLAN 連携× 4 回線）を定義する場合，帯域制御（トラフィック指定）をすべての Tag-VLAN 連携に設定することができます。

また，物理回線に対して 3 ～ 16 個の Tag-VLAN 連携を定義する場合，該当回線が Line 番号 0 に定義されているときだけ，帯域制御（トラフィック指定）をすべての Tag-VLAN 連携に設定し，16VLL として動作させることができます。例えば，Line 番号 0 に三つの Tag-VLAN 連携を定義して，Line 番号 1 に一つの TagVLAN 連携を定義した場合，帯域制御（トラフィック指定）を Tag-VLAN 連携に設定することはできません。(Ver.08-04 以降では，17 個以上の Tag-VLAN 連携の定義は可能ですが，定義された場合は帯域制御（トラフィック指定）を行わずに，17 個以上の Tag-VLAN 連携回線が定義されている LINE 回線が完全優先で動作します。)

● 16VLL 帯域制御サポート仕様

表 1-16　NIF 種別ごとのサポート仕様

項目	NIF 種別		
	10BASE-T	100BASE-TX	1000BASE-X
	内臓イーサネット※5 NEB100-4TB		NEB1G-1B
NIF 当たりの VLL 数	16 VLL		
VLL 当たりのキュー数	4 キュー		

項目		NIF 種別		
		10BASE-T	100BASE-TX	1000BASE-X
		内臓イーサネット※5 NEB100-4TB		NEB1G-1B
VLL ごとの最大送信帯域※2※3※4		320kbit/s ～ 10Mbit/s	320kbit/s ～ 100Mbit/s	320kbit/s ～ 590Mbit/s
キューごとのトラフィック種別が固定帯域制御の場合※1	キューごとの最大送信帯域※2※4	80kbit/s ～ 10Mbit/s※3	80kbit/s ～ 100Mbit/s※3	80kbit/s ～ 590Mbit/s※3
キューごとのトラフィック種別が可変帯域制御の場合※1	キューごとの最低保証帯域※2※4			
	キューごとの最大送信帯域※2※4			
	最大帯域割り当て重み	1 ～ 63		

注※1　各キューには帯域が未設定時は最低保証帯域 80kbit/s が割り当てられます。
注※2　誤差は最大 2%程度です。
注※3　範囲外の帯域を割り当てた場合は LINE 回線内の完全優先で動作します。
注※4　理論限界値を考慮して設定してください。

< 理論限界値算出式 >
　フレーム長 (byte：FCS 含む)*8(bit) ／
　((フレーム長 (byte：FCS 含む)*8(bit) ／回線速度 (bit/s))
　＋フレーム間ギャップ時間 (ns))
フレーム間ギャップ時間を次の表に示します。

回線速度 (bit/s)	フレーム間ギャップ時間 (ns)
10000000	16000
100000000	1600
1000000000	160

注※5　AX2001R，AX2002R，AX2002RX で内蔵されたイーサネットのことです。

(b) 64VLL 帯域制御

64VLL 帯域制御は「16VLL 帯域制御」を拡張しており，NIF 当たり最大で 64VLL まで設定可能にしています。

64VLL 帯域制御では，キューごとに以下の設定が行えます。

- 可変帯域制御 (最低帯域保証)

注　VLL 単位で 4 キューの完全優先として動作させることも可能です。

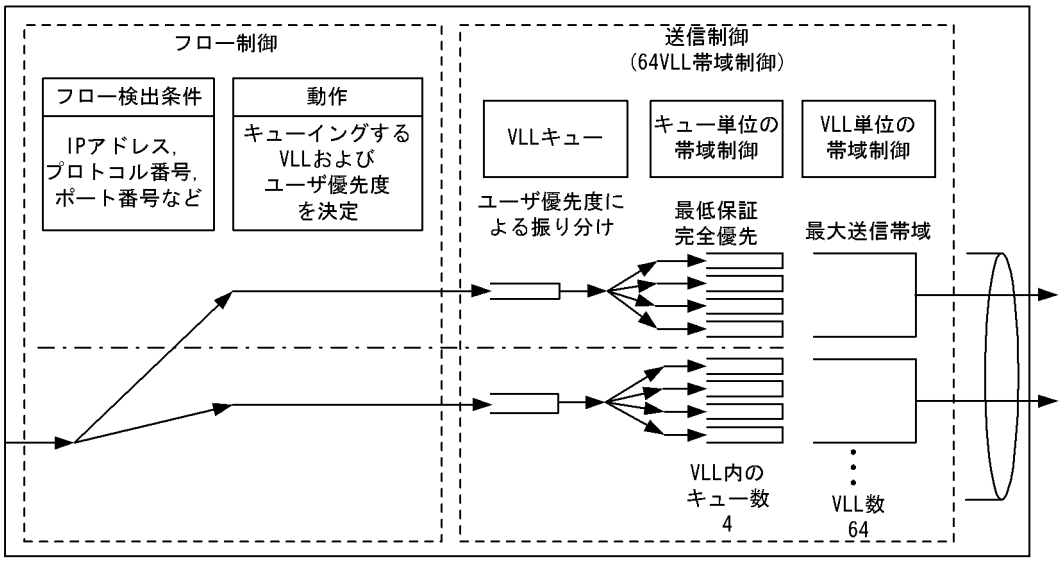
以下に 64VLL 帯域制御の特徴を記載します。

- NEB100-1TC で使用可能です。
- VLL 単位での帯域制御は 4 キューでのトラフィック指定と 4 キューでの完全優先として動作可能です。
- 優先度を指定する場合はユーザ優先度書き換えで行います。
- NEB100-1TC では NIF 上にキューが存在するため，キューごとの統計情報を確認する場合は，show vll コマンドを使用して下さい。

- Tag ヘッダありの Ethernet V2 フォーマット形式フレームのみサポートしています。サポート外のフレームは該当 VLL の最低優先度キュー (キュー 1) から送信されます。

64VLL 帯域制御の構造を次の図に示します。

図 1-17　64VLL 帯域制御の仕組み



フロー制御部では，フロー検出条件に一致するパケットに対してキューイングする VLL および出力優先度キューを決定します。送信制御部では，ユーザ優先度の設定値に応じて VLL 内のキューの振り分けを行った後，キューごとに可変帯域制御または 4 キューの完全優先によって出力する帯域を制御し，VLL ごとに帯域制御を行います。64VLL 帯域制御では，最大 64 個の Tag-VLAN 連携回線を同時に制御可能です。なお可変帯域制御は，前述の LINE 回線に対する帯域制御 (トラフィック指定) の機能と同様です。4 キューの完全優先の仕様を以下に示します。

● VLL 内完全優先動作について

64VLL では，一つの VLL に対して 4 キューの完全優先で制御することが可能です。VLL 内完全優先動作では，複数のキューにパケットが存在する場合，優先度の高いキューから常にパケットを送信します。トラフィックの優先順を完全に遵守する場合に適用できます。優先度は 1 (低) ≦出力優先度≦ 4 (高) となります。

● キューの状態と帯域開放

帯域制御を行うキューには，キューにパケットが全くないインアクティブ状態とパケットがキューに存在するアクティブ状態という二つの状態があります。
インアクティブ状態のとき，キューは帯域をすべて開放します。このため帯域を必要とするほかのキューが開放された帯域を利用することができます。
一方アクティブ状態のときは，可変帯域制御では最低帯域を確保します。実際に使用する帯域が確保した帯域より小さい場合は，未使用分の帯域は余剰帯域として開放し，帯域を必要とするほかのキューが開放された帯域を利用することができます。またアクティブ状態のキューは，パケットがなくなっても一定時間経過するまでアクティブ状態を維持して，かつ帯域も確保し続けます。一定時間以内に新たなパケットがキューにキューイングされなければ，キューは帯域を開放します。

● 64VLL 帯域制御を実行できる優先度

64VLL 帯域制御を指定した Tag-VLAN 連携回線は，ユーザ優先度書き換えによってユーザ優先度を書き換えた場合のみ，64VLL 帯域制御が実行できます。出力優先度指定，DSCP 書き換え指定または入力パケット DSCP 値指定によって出力優先度を決定した場合は，64VLL 帯域制御は実行できません。

64VLL 帯域制御と優先度指定機能の関係を次の表に示します。

表 1-17 64VLL 帯域制御と優先度指定機能の関係

優先度指定機能	64VLL 帯域制御機能の実行
出力優先度指定	－
ユーザ優先度書き換え	○
DSCP 書き換え指定	－
入力パケット DSCP 値指定	－

（凡例） ○：実行できる －：実行できない

● 64VLL 帯域制御サポート仕様

表 1-18 64VLL 帯域制御のサポート仕様

項目		NIF 種別	
		10BASE-T	100BASE-TX
		NEB100-1TC	
NIF 当たりのグループ数		64 グループ	
ユーザ当たりのキュー数		4 キュー	
ユーザごとの最大送信帯域※2※3		320kbit/s ～ 10Mbit/s	320kbit/s ～ 100Mbit/s
キューごとのトラフィック種別が固定帯域制御の場合※1	キューごとの最大送信帯域	―※6	
キューごとのトラフィック種別が可変帯域制御の場合※1	キューごとの最低保証帯域※2※5	80kbit/s ～ 10Mbit/s※3	80kbit/s ～ 100Mbit/s※3
	キューごとの最大送信帯域	―※7	
	最大帯域割り当て重み	―※7	

（凡例） －：設定不可

注※1 各キューに一つも帯域設定を行っていない場合，その VLL は完全優先 VLL として動作します。キューの優先度は 1（低）≦出力優先度≦ 4（高）となります。

また，VLL 内のいずれかのキューに帯域制御を設定している場合，該当 VLL 内の帯域制御未設定キューには最低保証帯域 80kbit/s が割り当てられます。

注※2 誤差は最大 2%程度です。

注※3 範囲外の帯域を割り当てた場合は帯域制御を行わずに LINE 回線が完全優先で動作します。

注※4 65 個以上の Tag-VLAN 連携を定義する場合，帯域制御（トラフィック指定）を行わずに 65 個以上 Tag-VLAN 連携回線を定義した LINE 回線内が完全優先で動作します。

注※5 理論限界値を考慮して設定してください。

< 理論限界値算出式 >

フレーム長 (byte：FCS 含む)*8(bit) ／
((フレーム長 (byte：FCS 含む)*8(bit) ／回線速度 (bit/s))
＋フレーム間ギャップ時間 (ns))

フレーム間ギャップ時間を次の表に示します。

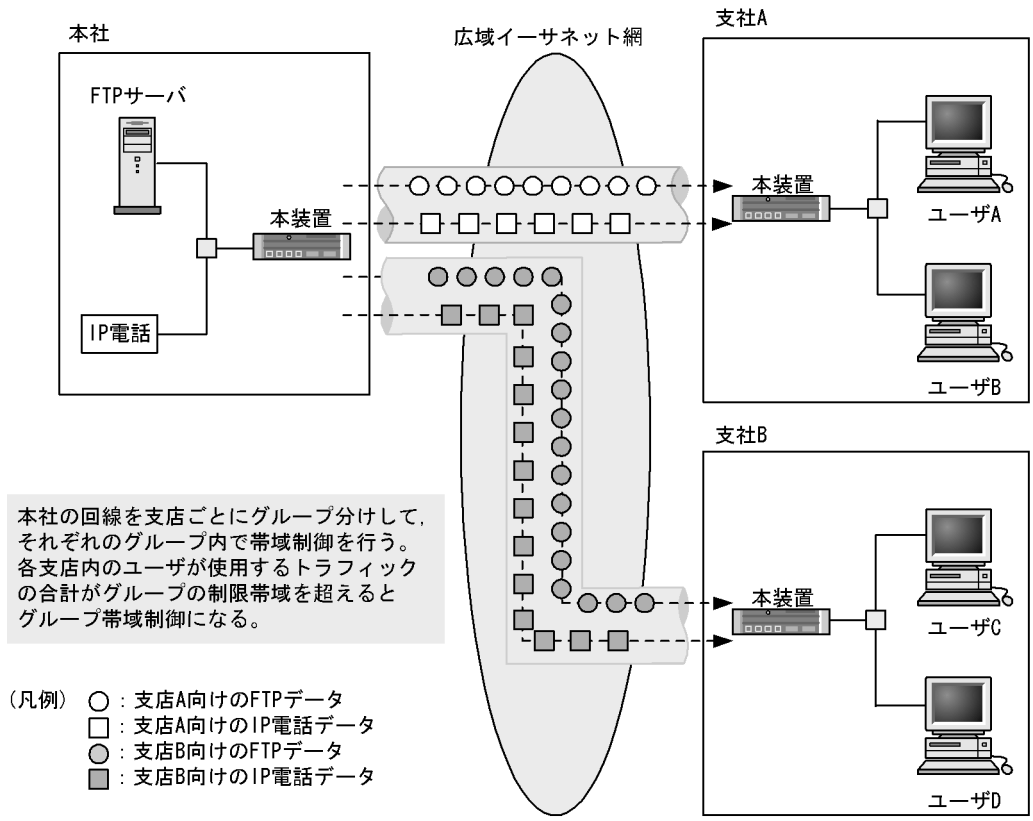
回線速度 (bit/s)	フレーム間ギャップ時間 (ns)
10000000	16000
100000000	1600
1000000000	160

注※ 6　設定された場合は，未設定時と同様の帯域（最低保証帯域 80kbit/s）が割り当てられます。
注※ 7　設定された場合は，設定不可項目（キューごとの最大送信帯域および最大帯域割り当て重み）だけを無視して帯域制御を行います。

1.8.7　グループ帯域制御

物理回線をグループ単位に分割し，グループ内で一定の帯域を確保するための制御です。本社と複数の支店を結ぶネットワークで，拠点ごとに優先する業務がある場合に，輻輳時もその業務のための帯域を確保したいときに有効です。企業ネットワークの広域イーサネット網を使用したデータ転送を例にして，グループ帯域制御の概要を次の図に示します。

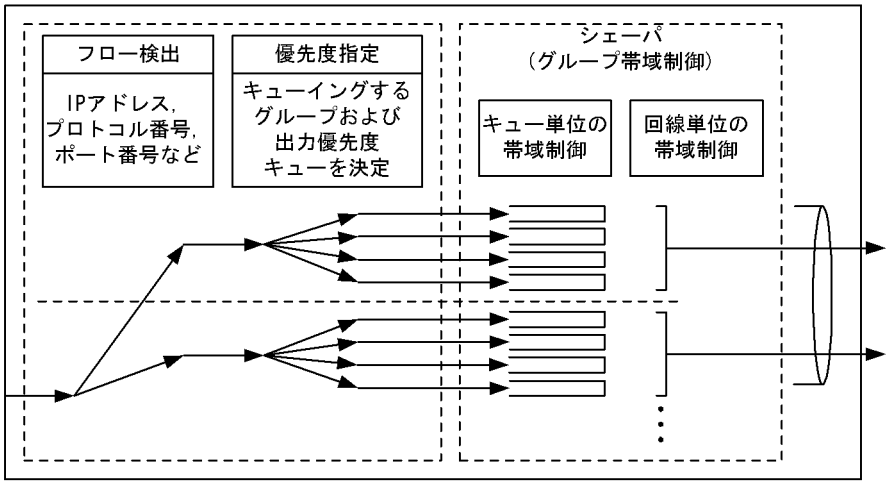
図 1-18　グループ帯域制御の概要



(1) グループ帯域制御の構造

グループ帯域制御の構造を次の図に示します。

図 1-19 グループ帯域制御の構造



フロー検出により検出したフローを，指定したグループおよびキューへキューイングします。その後グループ帯域制御により，1 段目でキューごとに固定帯域制御または可変帯域制御を行い，2 段目で各キューを束ねたグループに対して帯域制御を行います。なお固定帯域制御および可変帯域制御は，前述の機能と同様です。

(2) 帯域制御のサポート仕様

グループ帯域制御を実行できる NIF ごとのサポート仕様を次の表に示します。

表 1-19 NIF 種別ごとのサポート仕様

項目		NIF 種別		
		10BASE-T	100BASE-TX	1000BASE-X
		内蔵イーサネット※5 NEB100-4TB		NEB1G-1B
NIF 当たりのグループ数		16 グループ		
グループ当たりのキュー数		4 キュー		
グループごとの最大送信帯域 ※2※3※4		320kbit/s ～ 10Mbit/s	320kbit/s ～ 100Mbit/s	320kbit/s ～ 590Mbit/s
キューごとのトラフィック種別が固定帯域制御の場合 ※1	キューごとの最大送信帯域※2※4	80kbit/s ～ 10Mbit/s※3	80kbit/s ～ 100Mbit/s※3	80kbit/s ～ 590Mbit/s※3
キューごとのトラフィック種別が可変帯域制御の場合 ※1	キューごとの最低保証帯域 ※2※4			
	キューごとの最大送信帯域※2※4			
	最大帯域割当重み	1 ～ 63		

注※ 1 各キューには帯域が未設定時は最低保証帯域 80kbit/s が割り当てられます。

注※ 2 誤差は最大 2%程度です。

注※ 3　範囲外の帯域を割り当てた場合は完全優先で動作します。
注※ 4　理論限界値を考慮して設定してください。

< 理論限界値算出式 >
　フレーム長 (byte：FCS 含む)*8(bit) ／
　((フレーム長 (byte：FCS 含む)*8(bit) ／回線速度 (bit/s))
　＋フレーム間ギャップ時間 (ns))
フレーム間ギャップ時間を次の表に示します。

回線速度 (bit/s)	フレーム間ギャップ時間 (ns)
10000000	16000
100000000	1600
1000000000	160

注※ 5　AX2000R で内蔵されたイーサネットのことです。

(3) グループ帯域制御を実行できる優先度

グループ帯域制御を指定したインタフェースでは，出力優先度指定によって出力優先度を決定した場合だけ，グループ帯域制御が実行できます。マーカーで DSCP 書き換え指定または入力パケット DSCP 値指定によって出力優先度を決定した場合は，グループ帯域制御は実行できません。グループ帯域制御とフロー制御の出力優先度決定の関係を次の表に示します。

表 1-20　帯域制御 (トラフィック指定) とフロー制御の出力優先度決定の関係

フロー制御での優先度決定方法	帯域制御 (トラフィック指定) 機能の実行
出力優先度指定	○
DSCP 書き換え指定	―
入力パケット DSCP 値指定	―

(凡例)　○：実行できる　―：実行できない

(4) グループ番号の設定範囲

同一 NIF 内でグループ帯域制御を設定する物理回線数と Line 番号によって，使用できるグループ番号の範囲が異なります。次の表に使用する物理回線数と Line 番号に対するグループ番号の範囲を示します。

表 1-21　使用する物理回線数・Line 番号に対するグループ番号の範囲

使用する物理回線数	Line 番号	使用可能なグループ番号
1 回線だけ	0	1 ～ 16
	0 以外	1 ～ 2
2 回線以上	0 ～ 3	1 ～ 2

表に示すとおり，1 回線かつ Line 番号 0 にグループ帯域制御を設定する場合，グループ番号 1 から 16 を使用できます。1 回線かつ Line 番号 0 以外の場合，および 2 回線以上にグループ帯域制御を設定する場合，グループ番号は 1 ～ 2 だけ使用できます。

1.9 QoS 制御機能の適用例

この節では QoS 制御機能を適用したネットワーク構成例について説明します。

1.9.1 QoS ネットワーク構成例

トラフィック量がネットワークの転送容量を上回ると，ネットワーク内でパケットが滞留する場所（輻輳ポイント）が生じます。この項では，この輻輳ポイントに QoS 制御を適用し，通信品質を改善する QoS 制御の適用例を示します。

(1) 企業ネットワークへの適用例

自ネットワークを構成する装置ごとに装置単体レベルで QoS 制御（簡易的 QoS 制御）を行う企業ネットワークに本装置の QoS 制御を適用した場合の例について説明します。

(a) 企業ネットワークへ QoS 制御を適用する場合のメリット

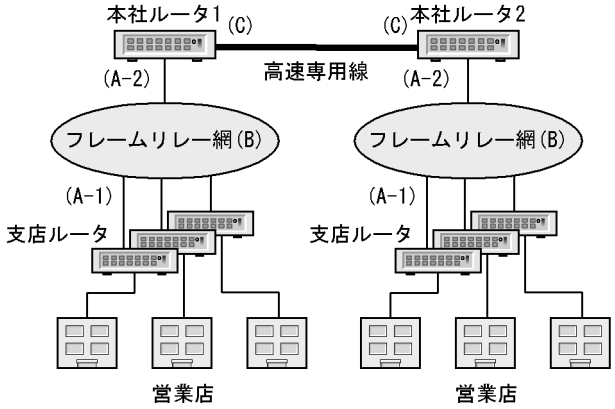
企業ネットワークに本装置の QoS 制御を適用した場合には，次に示すような要求を実現できます。

- **最低帯域保証**
  各営業店宛てのトラフィックの最低帯域を保証できます。この要求を実現するため，本装置では最低帯域保証をサポートしています。
- **高度な通信品質**
  特定のアプリケーションに対して高度な通信品質を提供できます。この要求を実現するためには，該当するアプリケーションに高い優先度を割り当てます。本装置では完全優先で高度な通信品質を提供しています。

(b) 適用例

輻輳ポイントごとに通信品質の改善方法を示します。企業ネットワークへの適用例を次の図に示します。企業ネットワークの構成は，本社間に高速専用線を使用し，本社－支店間にフレームリレー網を使用します。

図 1-20 企業ネットワークへの適用例



構成の説明

支店ルータは，直接営業店の回線を収容するルータで，IP パケットのフローを検出し，出力優先度ごとに最低帯域保証を行います。

本社ルータは，支店ルータからのトラフィックを集約して，ネットワークの基幹部分を構成するルー

タです。支店ルータ配下の営業店宛ての IP パケットのフローを検出して，出力優先度ごとに最低帯域保証を行います。また，本社－本社間ではトラフィック種別ごとに完全優先を行います。
本装置は，本社ルータ，支店ルータのどちらにも適用できます。

輻輳ポイント

- 複数の営業店から本社向けのパケットが集中する支店ルータの本社ルータ向けの出力インタフェース (A-1)
- 本社から複数の営業店へのパケットが集中する本社ルータの支店ルータ向けの出力インタフェース (A-2)
- フレームリレー網内 (B)
- 高速専用線が集中する本社ルータの本社 1 －本社 2 間の高速専用線網への出力インタフェース (C)

通信品質の改善方法

1. 輻輳ポイント (A-1，A-2) で最低帯域保証
   (A-1)(A-2) の輻輳ポイントで営業店ごとにトランザクションデータに対し最低帯域保証制御を行うことによって，輻輳ポイントで輻輳が発生した場合にトランザクションデータの低遅延，低廃棄を実現できます。
2. 輻輳ポイント (B) でレイヤ 2 連携機能
   フレームリレー網が輻輳した場合に，トランザクションデータ以外のデータの廃棄を網の輻輳制御機能 (DE ビット) を使用することによって，通信品質を改善できます。
3. 輻輳ポイント (C) で完全優先
   輻輳ポイント (C) では，トラフィック種別ごとに要求される通信品質にで完全優先を行うことによって，通信品質を改善できます。トラフィック種別に対する要求通信品質は，「表 1-1　トラフィック種別と要求される通信品質」を参照してください。

(2) プロバイダ網への適用例 (DSCP 値を使用した QoS 制御)

本装置の DSCP 値を使用した QoS 制御をプロバイダ網に適用した場合の例について説明します。

(a) 実現できるサービス

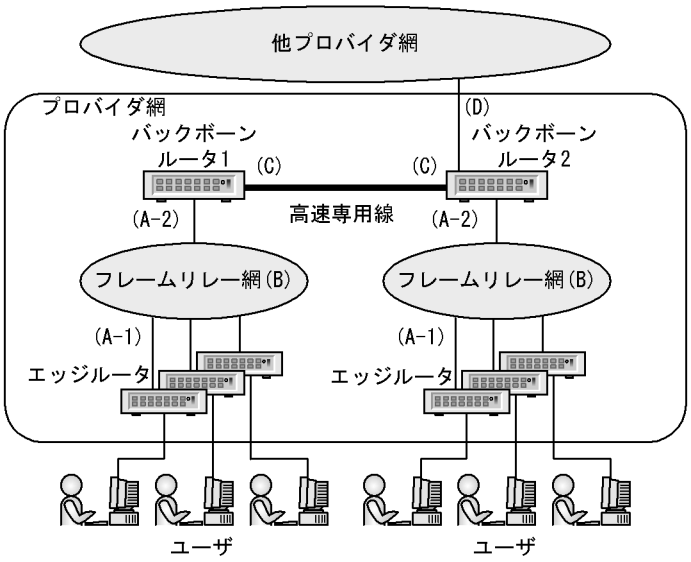
DSCP 値を使用した QoS 制御をプロバイダ網に適用すると，次のようなサービスを実現できます。

- **最低帯域保証サービス**
  帯域を遵守するユーザが，意図的である／意図的でないに関係なく契約帯域違反のユーザからの過剰トラフィックの流入による影響を受けないサービスです。このサービスを実現するため，本装置では最低帯域保証と帯域監視機能をサポートしています。
- **通信品質サービス**
  優先契約をしたユーザにはその優先度に従った通信品質を提供するサービスです。アプリケーションによって発生するトラフィックはさまざまですが，それぞれのトラフィックの特徴に応じた QoS 制御を行うことによって通信品質を確保します。

(b) 適用例

輻輳ポイントごとに通信品質の改善方法を示します。プロバイダ網への適用例を次の図に示します。プロバイダ網の構成はバックボーンルータ間，バックボーンルータとそのほかのプロバイダ網間に高速専用線を使用し，バックボーンルーター－エッジルータ間にフレームリレー網を使用します。

図 1-21 プロバイダ網への適用例 (DSCP 値を使用した QoS 制御)



構成の説明

エッジルータは，直接ユーザの回線を収容するルータです。IP パケットのフローを検出して，フローごとに帯域監視を行い，優先度を割り当てます。割り当てられた優先度に対応する DSCP 値で IP パケットの DSCP フィールドを書き換え，IP パケットごとに優先度情報を反映します。

バックボーンルータは，エッジルータからのトラフィックを集約して，ネットワークの基幹部分を構成するルータです。エッジルータが IP パケットごとに設定した DSCP 値の優先度情報に応じてパケットを転送します。

このようにすることでプロバイダはユーザに対して通信品質を提供できます。本装置は，バックボーンルータ，エッジルータのどちらにも適用できます。

輻輳ポイント

- 複数のユーザからバックボーン向けのパケットが集中するエッジルータのバックボーンルータ向けの出力インタフェース (A-1)
- バックボーンルータから複数のユーザへのパケットが集中するバックボーンルータのエッジルータ向けの出力インタフェース (A-2)
- フレームリレー網内 (B)
- 高速専用線が集中するバックボーンルータのバックボーンルータ 1 ―バックボーンルータ 2 間の高速専用線への出力インタフェース (C)
- バックボーンルータから他プロバイダ網への出力インタフェース (D)

通信品質の改善方法

1. 輻輳ポイント (A-1) で完全優先，帯域監視

   エッジルータはユーザからのパケットに対し，ユーザが契約した優先度に対応する DSCP 値をパケットの IP ヘッダの TOS フィールドに書き込み，その DSCP 値で完全優先を行います。高い優先度で契約したユーザのトラフィックが低い優先度のトラフィックよりも優先して中継され，優先度に応じた通信品質を実現できます。

   さらにエッジルータは各ユーザから，またはユーザへのパケットに対して，ユーザが契約した帯域を監視する帯域監視を行います。契約帯域を超えた違反パケットを廃棄することで，そのほかのユーザの過剰トラフィックによる帯域使用を防止し，各ユーザの通信品質を保持します。
2. 輻輳ポイント (B) でレイヤ 2 連携機能

   フレームリレー網が輻輳した場合に，プロバイダのポリシーに従い，網の輻輳制御機能 (DE ビッ

ト) を使用してトランザクションデータ以外のデータの廃棄を行うことによって，通信品質を改善できます。

3. 輻輳ポイント (A-2，C) で完全優先
   パケットの IP ヘッダ内の DSCP 値に基づいて完全優先を行うことによって，高い優先度で契約したユーザのトラフィックが低い優先度のトラフィックよりも優先して中継され，優先度に応じた通信品質を実現できます。
4. 輻輳ポイント (D) で帯域監視
   プロバイダ間接続の場合は特に相互の契約帯域を守ることと相手からの契約帯域以上のトラフィックが来ていないか監視 (帯域監視) することが重要です。相手からのトラフィックを監視し，契約帯域を超えた違反パケットを廃棄することで，自網内への予期しないトラフィックの流入を防止し，自網内の通信品質を保持します。

(3) プロバイダ網への適用例 (最低帯域保証 (kbit/s 指定) を使用した QoS 制御)

本装置の 1000 キューモード (最低帯域保証 (kbit/s 指定)) を使用した QoS 制御をプロバイダ網に適用した場合の例について説明します。

(a) 実現できるサービス

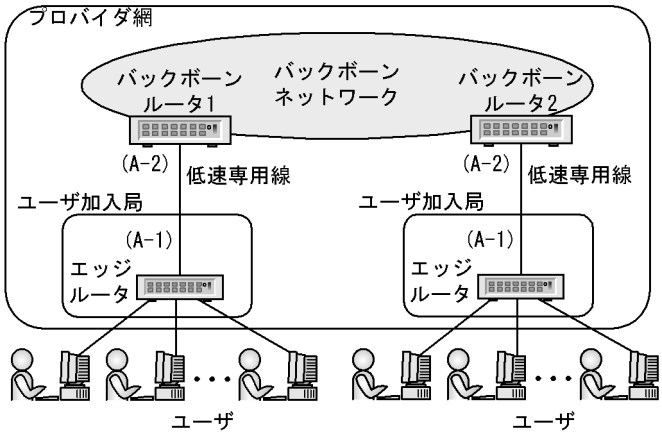
最低帯域保証 (kbit/s 指定) を使用した QoS 制御をプロバイダ網に適用すると，次のようなサービスを実現できます。

- **1000 ユーザ最低帯域保証サービス**
  ユーザ加入局とバックボーンネットワークの間を 6Mbit/s 以下の低速専用線で接続する場合に，低速専用線で各ユーザの最低帯域を保証するサービスです。このサービスを実現するため，本装置では回線当たり最大 1000 個のパケット送信キューを使用できる最低帯域保証をサポートしています。

(b) 適用例

輻輳ポイントとなる低速専用線での通信品質の改善方法を示します。プロバイダ網への適用例を次の図に示します。

図 1-22 プロバイダ網への適用例 (最低帯域保証 (kbit/s 指定) を使用した QoS 制御)



構成の説明

エッジルータは，直接ユーザの回線を収容するルータで，ユーザからの IP パケットのフローを検出し，フローごとに最低帯域保証を行います。

バックボーンルータは，エッジルータからのトラフィックを集約し，ネットワークの基幹部分を構成するルータです。また，基幹部分からユーザへ向けた IP パケットのフローを検出し，フローごとに

最低帯域保証を行います。
このようにすることでプロバイダはユーザに対して通信品質を提供できます。本装置は，バックボーンルータ，エッジルータのどちらにも適用できます。

輻輳ポイント

- 複数のユーザからバックボーン向けのパケットが集中するエッジルータのバックボーンルータ向けの出力インタフェース (A-1)
- バックボーンルータから複数のユーザへのパケットが集中するバックボーンルータのエッジルータ向けの出力インタフェース (A-2)

通信品質の改善方法

1. 輻輳ポイント (A-1，A-2) で最低帯域保証
   (A-1)(A-2) の輻輳ポイントで，ユーザごとに個別の送信待ちキューを使用して最低帯域保証制御を行います。こうすれば，輻輳ポイントで輻輳が発生した場合に，ユーザの使用帯域を保証するサービスが実現できます。また，輻輳が発生していないときには，各ユーザが専用線の空き帯域を有効に利用できます。

1.9.2 QoS ネットワークの運用

QoS ネットワークの運用を，簡易的 QoS 制御，網レベル QoS 制御，隣接ネットワーク間 QoS 制御の 3 レベルに分類して説明します。

● 簡易的 QoS 制御

自ネットワークを構成する装置ごとに，装置単体レベルでの QoS 制御を行う運用形態です。現状ルータでは送信遅延時間が発生するなど通信品質が劣化しますが，本装置の QoS 制御を適用すれば，通信品質の劣化を防ぐことができます。
この運用形態では，それぞれの装置単位に，例えば，telnet，http，ftp，インターネット電話といったアプリケーションのフローごとの QoS 制御をあらかじめ構成定義で指定しておきます。本装置はフローを検出し，指定された QoS 制御を実行します。QoS 制御は自ネットワークを構成するすべての装置への適用が望ましいですが，トラフィックの集中するルータだけに適用しても効果があります。

● 網レベル QoS 制御

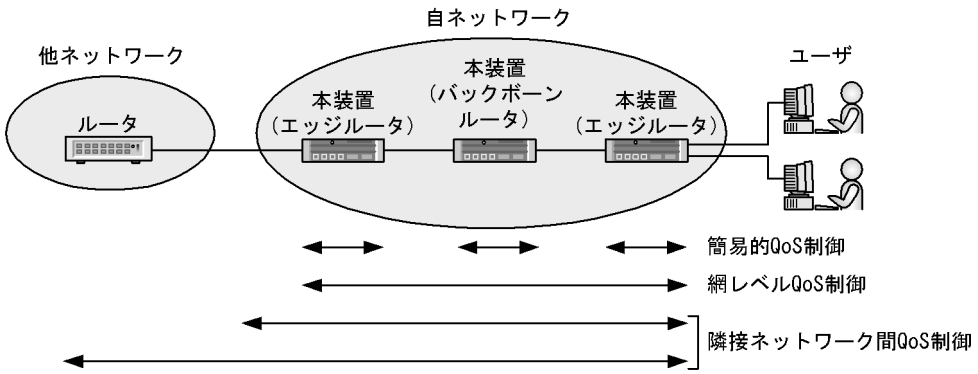
自ネットワークの範囲で，一貫した QoS 制御を行う運用形態です。エッジルータでは，フローを検出し，帯域監視と DSCP 値の書き換えを行います。バックボーンルータでは，DSCP 値に従った QoS 制御を行います。これらの QoS 制御によって，特定ユーザのフローを検出し網の中で一貫した QoS 制御を行うといった通信品質サービスを提供できます。

● 隣接ネットワーク連携 QoS 制御

他ネットワークとの接続点で IP パケットの DSCP 値を監視し，自ネットワークの QoS 制御のポリシーに違反するパケットの DSCP 値を適宜書き換えることによって，自ネットワーク内の通信品質を確保します。なお，隣接するネットワークが自ネットワークと同じ QoS 制御のポリシーで運用されている場合には，IP パケットの DSCP 値を書き換えないで，その DSCP 値による QoS 制御を行い，隣接ネットワークと相互に連携した QoS 制御ができます。

運用形態ごとの QoS 制御範囲を次の図に示します。

図 1-23 運用形態ごとの QoS 制御範囲



また，それぞれの運用形態について，QoS 機能の企業ネットワークへの適用例を「表 1-22 運用形態ごとの QoS 機能の適用 (企業ネットワーク)」に，プロバイダ網への適用例を「表 1-23 運用形態ごとの QoS 機能の適用 (プロバイダ網)」に示します。

表 1-22 運用形態ごとの QoS 機能の適用 (企業ネットワーク)

運用形態	適用する QoS 制御	
	支店ルータ機能	本社ルータ機能
簡易的 QoS 制御	フロー検出 帯域監視 最低帯域保証／完全優先	フロー検出 完全優先
網レベル QoS 制御	フロー検出 帯域監視 DSCP 値書き換え 完全優先	DSCP 値に従って 完全優先

表 1-23 運用形態ごとの QoS 機能の適用 (プロバイダ網)

運用形態		QoS 制御	
		エッジルータ機能	バックボーン ルータ機能
簡易的 QoS 制御		フロー検出 帯域監視 最低帯域保証／完全優先	フロー検出 完全優先
網レベル QoS 制御		フロー検出 帯域監視 完全優先 DSCP 値書き換え	DSCP 値に従って 完全優先
隣接ネットワーク連携 QoS 制御	隣接ネットワークの QoS 制御ポリシーが異なる	フロー検出 帯域監視 最低帯域保証／完全優先 DSCP 値監視および書き換え	DSCP 値に従って 完全優先
	隣接ネットワークの QoS 制御ポリシーが同じ	帯域監視 DSCP 値に従って完全優先	DSCP 値に従って 完全優先

1.10 QoS 制御機能の仕様一覧

1.10.1 QoS 制御機能とメディア種別との対応

メディア種別と QoS 制御機能との対応を次の表に示します。入力側および出力側それぞれについて示します。

表 1-24 メディア種別と QoS 制御機能との対応

項目		概要	メディア種別					
			イーサネット		WAN		ATM	
			in	out	in	out	in	out
レイヤ 3 機能	フロー検出	IP の場合は，IP アドレスなどで指定されたフローを検出します。IPX，ブリッジ，HDLC パススルーの場合はプロトコル単位でフローを検出します。	○	○	○	○	○	○※1
	帯域監視	フローごとに帯域を監視して，帯域を超えたフローに対してペナルティを与えます。	○	○	○	○	○	○
	マーカー	DSCP を書き換えます。	○	○	○	○	○	○※1
		ユーザ優先度書き換えます。	－	○	－	－	－	－
	優先度指定	指定されたフローを検出後，対応した出力優先度，キューイング優先度を決定します。	○	○	○	○	○	○※2
	廃棄制御	パケットの優先度とキューキューの状態に応じて，該当パケットをキューイングするか廃棄するかを制御します。	－	○	－	○	－	○※2
	シェーパ	パケットの出力順序や出力帯域を制御します。	－	○	－	○	－	○※2
レイヤ 2 機能	DE ビット制御	フレームリレーの DE ビットを設定します。	－	－	－	○	－	－
	CLP ビット制御	ATM セルの CLP ビットを設定します。	－	－	－	－	－	○
	シェーパ	ATM トラフィックを ATM サービスカテゴリ（CBR，UBR，VBR，ABR，GFR など）ごとに出力制御します。※2	－	－	－	－	－	○

（凡例） in：Inbound 制御　out：Outbound 制御　○：対象にする　－：該当しない

注※ 1　フィルタリングによる指定が必要になります。

注※ 2　ATM 機能で行います。フローを CBR，VBR，ABR，UBR，GFR のトラフィックタイプにマッピングし，廃

棄制御，完全優先，およびシェーピングによる帯域制御を行います。詳細は，「解説書 Vol.1　6. ATM」参照してください。

1.10.2 エントリ数の仕様

表 1-25　モデルおよび RM 実装メモリサイズごとに定義できる最大エントリ数

モデル	RM 実装メモリサイズ	RP 種別	エントリ数※1※2		トンネルフィルタ数※2
			装置当たり	RP 当たり	装置当たり
AX2001R AX2002R AX2002RX	128MB	—	1000	1000	1000
	256MB	—	2000	2000	2000

（凡例）　—：該当しない

注※1　フィルタエントリ，QoS エントリ，トンネルエントリの合計値です。

注※2　構成定義 flow でフロー制御情報を設定する場合，設定内容によって 1 リスト当たりに使用するエントリ数を次の表に示します。

表 1-26　1 リスト当たりに使用するエントリ数

機能	設定内容	エントリ数
フィルタ	トンネルフィルタ	1
	トンネルフィルタ以外	1
QoS	設定なし	1
	最大帯域制限	1
	最低帯域保証	1
	最大帯域制限＋最低帯域保証	2
	最大帯域制限＋重要パケット保護	2
	最低帯域保証＋重要パケット保護	2
	最大帯域制限＋最低帯域保証＋重要パケット保護	4

1.10.3 QoS 制御機能とプロトコル種別とのサポート仕様

本装置がサポートするプロトコルによる QoS 制御の相違点を次の表に示します。

表 1-27　プロトコルによる QoS 制御の相違点

機能項目		プロトコル	
		IP	IPX/ ブリッジ / HDLC パススルー
フロー検出		○	—
帯域監視		○	—
マーカー	DSCP 書き換え	○	—
	ユーザ優先度書き換え	○	—
	EXP 書き換え	○	—
優先度指定		○	—

機能項目		プロトコル	
		IP	IPX/ ブリッジ / HDLC パススルー
コネクション分岐		○	－
シェーパ	最低帯域保証	○	○
	ラウンドロビン	○	○
	均等最低帯域保証	○	○
	最低帯域保証 (kbit/s 指定)	○	○
	帯域制御 (トラフィック指定)	○	○
	グループ帯域制御	○	○
	階層化シェーパ	○	－
フレームリレーの DE ビット制御		○	○
ATM セルの CLP ビット制御		○	○
サービスカテゴリごとのシェーパ		○	○

(凡例) ○：サポートする　－：サポートしない

1.10.4 キュー仕様

メディアおよびレイヤ 2 プロトコルごとのキュー仕様をモデルごとに以下に示します。インタフェース単位に完全優先，最低帯域保証，ラウンドロビン，均等最低帯域保証，最低帯域保証 (kbit/s 指定)，帯域制御 (トラフィック指定)，グループ帯域制御，階層化シェーパのどれかを選択します。

(1) イーサネット

イーサネットでは，シェーパをサポートします。次の表にメディアと NIF 略称ごとにサポートするシェーパ種別を示します。

表 1-28　イーサネットのキュー仕様

メディア	NIF 略称	シェーパ種別
		レガシーシェーパ
10BASE-T 100BASE-TX	内蔵イーサネット※1 NEB100-4TB NEB100-1TC※2	○
ギガビット・イーサネット	NEB1G-1B	○

(凡例) ○：使用できる　－：使用できない

注※ 1　AX2000R で内蔵されたイーサネットのことです。

注※ 2　NEB100-1TC では，Tag-VLAN 連携回線だけ帯域制御できます。このため，VLAN 以外のパケットは帯域制御できません。該当する VLAN 以外のパケットが出力されるキューは「1.6　優先度指定」を参照してください。

レガシーシェーパは 5 種類あり，メディア種別によりサポート内容が変わります。メディア種別に対応するレガシーシェーパの種別を次の表に示します。

表 1-29 イーサネットのキュー仕様

メディア	NIF 略称	キュー仕様			レガシーシェーパ				
		1	2	3	4	5※2	6	7※2	8※2
10BASE-T 半二重 100BASE-TX 半二重	内蔵イーサネット※1, NEB100-4TB	Line	8	4	○	―	―	―	―
	NEB100-1TC	Line	8	4	_※4	―	―	―	―
10BASE-T 全二重	内蔵イーサネット※1, NEB100-4TB	Line	4	4	―	―	―	○	○
100BASE-TX 全二重		Line	8	4	○	○	―	○	―
		Line	64	4	―	―	―	○	―
	NEB100-1TC※5	Line	64	4	_※4	―	―	○※3	―
ギガビット・イーサネット	NEB1G-1B	Line	4	4	―	―	―	○	○
		Line	8	4	○	○	○	○	―
		Line	64	4	―	―	―	○	―

(凡例)

1：キューを持つ単位　2：キュー個数　3：キューイング優先度数
4：完全優先　5：最低帯域保証　6：ラウンドロビン
7：帯域制御(トラフィック指定)　8：グループ帯域制御
○：使用できる
―：使用できない(構成定義情報に関係なく，デフォルト値(完全優先)で動作)

注※1　AX2000R で内蔵されたイーサネットのことです。

注※2　10BASE-T/100BASE-TX の全二重設定から半二重設定(オートネゴシエーション含む)に変更された場合，最低帯域保証，帯域制御(トラフィック指定)およびグループ帯域制御では指定された帯域を保証しません。

注※3　Tag-VLAN 連携にだけ設定できます。物理回線に対して設定を行った場合は，構成定義情報に関係なく，デフォルト値(完全優先)で動作します。

注※4　明示的な設定はできませんが，帯域制御を行っていない場合，または物理回線に対して帯域制御設定を行った場合に完全優先として動作します。

注※5　キューイング優先度は構成定義情報に関係なく 4 固定となります。

(2) WAN

表 1-30 WAN のキュー仕様

メディアおよびレイヤ 2 プロトコル	キュー仕様			シェーパ				
	1	2	3	4	5	6	7	8※
低速 WAN(～6M)PPP	Line	8	4	○	○	○	―	○
		16	4	―	―	―	―	○
		32	4	○	○	―	―	○
		250	4	―	―	―	―	○
		1000	2	―	―	―	―	○
低速 WAN(～6M)	DLCI	8	4	○	○	○	○	―
フレームリレー		16	4	―	○	―	○	―

メディアおよびレイヤ 2 プロトコル	キュー仕様			シェーパ				
	1	2	3	4	5	6	7	8 ※
		32	4	―	―	―	○	―
ISDN	peer	8	4	○	○	○	―	―

(凡例)

1：キューを持つ単位　2：キュー個数　3：キューイング優先度数
4：完全優先　5：最低帯域保証　6：ラウンドロビン
7：均等最低帯域保証　8：最低帯域保証 (kbit/s 指定)
○：使用できる
－：使用できない(構成定義情報に関係なく，デフォルト値(完全優先)で動作)

注※　PPP 情報に bod オプションが設定されている場合は，デフォルト値(完全優先)で動作します。PPP のインタフェースに IPX ルーティングインタフェースまたはブリッジインタフェースが設定されている場合は，デフォルト値(完全優先)で動作します。最大キュー数が未設定，または無効な値を設定した場合は，最大キュー数 8 として動作します。

(3) ATM

ATM 機能で行います。CBR，VBR，ABR，UBR 等の ATM サービスカテゴリによる制御を行います。詳細は，「解説書 Vol.1　6. ATM」を参照してください。

1.10.5 レイヤ 2 連携機能

フレームリレーの場合，QoS 制御で決定されたキューイング優先度を DE ビットにマッピングして，レイヤ 2 の廃棄制御と連携できます。また，ATM の場合は QoS 制御で決定されたキューイング優先度を CLP ビットにマッピングして，レイヤ 2 の廃棄制御と連携できます。

1.11　QoS 制御使用時の注意事項

1.11.1　RP 処理負荷と QoS 制御の関係

収容条件以内で使用する場合，「図 1-24　通常のケース (収容条件以内で，性能範囲内での使用)」に示すような QoS 制御 (廃棄制御，シェーパなど) を行います。しかし，収容条件を超えた状況で RP に高負荷が発生した場合，「図 1-25　高負荷によるパケット廃棄発生で QoS 制御が機能しないケース」に示すように送信パケットが廃棄されて期待する QoS 制御結果が得られないケースがあります。

図 1-24　通常のケース (収容条件以内で，性能範囲内での使用)

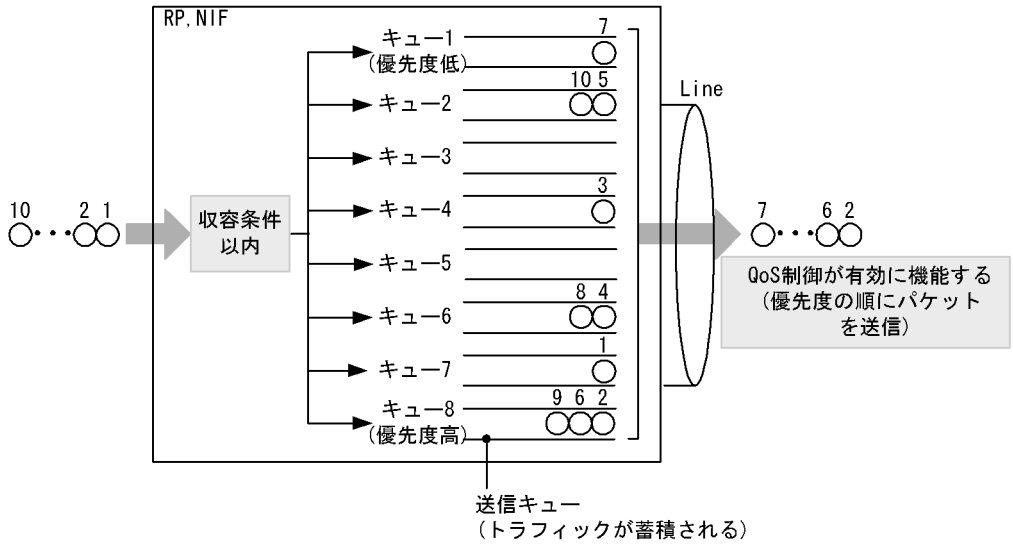
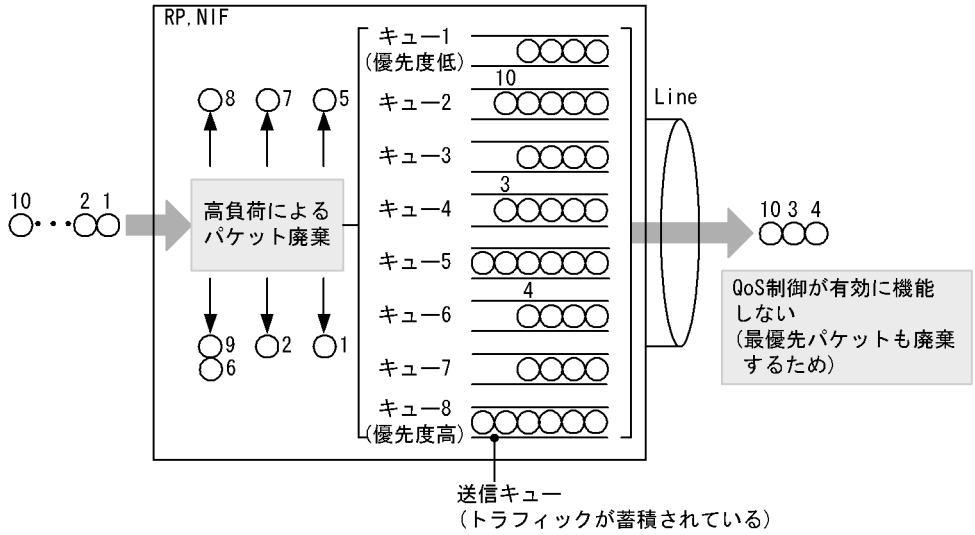


図 1-25　高負荷によるパケット廃棄発生で QoS 制御が機能しないケース



RP に高負荷が発生する要因を次に示します。大・中・小型モデル共通 NIF で共通に当てはまります。これら要因によって RP に高負荷が発生すると，QoS 制御が機能しなくなる場合があるので注意してください。

- RP のソフトウェア処理によるもの
  - IPX ルーティングを使用し，2500packet/s 以上のトラフィックが発生する場合
  - ブリッジを使用し，3500packet/s 以上のトラフィックが発生する場合
  - IP フラグメントが多発する場合
  - IP ヘッダ オプションを利用したパケットを多数受信および中継する場合
- 収容条件を超えた状況で使用している場合

本装置の収容条件は，「解説書 Vol.1　3. 収容条件」を参照してください。

1.11.2　TCP パケットに対する帯域監視機能の使用

帯域監視によって契約帯域を超えるパケットを廃棄する，という設定をした場合には，TCP のスロー・スタートが繰り返されデータ転送速度が極端に遅くなります。TCP を使用したデータ系通信に対して帯域を制限したい場合は，「1.10.5　レイヤ 2 連携機能」に示した各種帯域保証機能を使用することをお勧めします。

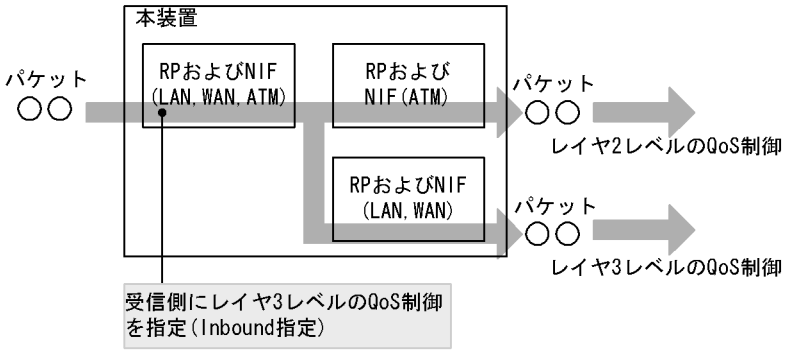
帯域保証機能を使用できず，帯域監視機能を使用する場合には，帯域監視の結果，「パケットを廃棄する」ではなく，「パケットが廃棄しやすくなるように指定したキューイング優先度に変更する」ようにしてください。このモードにすると，契約帯域を超えてもすぐ廃棄されず，出力回線が混んできたときだけに廃棄されるようになります。なお，帯域保証機能はキューごとの帯域保証になるので，帯域制御を行いたいフロー数がキュー数を超える場合など，帯域保証機能が使えない場合があります。

1.11.3　そのほかの注意事項

（1）受信 QoS 制御指定 (Inbound 指定) したトラフィックを ATM インタフェースで送信する場合の注意事項

イーサネット，WAN，ATM インタフェースから受信したトラフィックに対してレイヤ 3 レベルの受信 QoS 制御を指定しても，ATM インタフェースで送信するレイヤ 2 レベルで QoS が動作してしまうので注意してください。ATM インタフェースでの QoS 制御を次の図に示します。

図 1-26　ATM インタフェースでの QoS 制御 (受信トラフィックを Inbound 指定して ATM インタフェースへ送信する場合)



この図に示すように，受信 QoS 制御指定したトラフィックを ATM インタフェースで送信する場合，送信先の ATM インタフェースはレイヤ 2 レベルの QoS 制御 (CBR，UBR などのサービスカテゴリ) に従って QoS 制御 (完全優先，シェーピングなど) をします。

2 Diff-serv 機能

Diff-serv 機能は IP ネットワーク上の QoS 制御技術の一つです。この章では Diff-serv 機能について説明します。

2.1 Diff-serv 概説

2.2 Diff-serv の機能ブロック

2.3 構成定義作成時の注意事項

2.1 Diff-serv 概説

2.1.1 Diff-serv の機能

Diff-serv(Differentiated Services) 機能は，IP ネットワーク上の QoS 制御技術の一つです。従来の QoS 技術はパケットの TCP/IP ヘッダからフローを検出して優先度を決定していましたが，この技術ではインターネットのバックボーンのように多数のユーザのフローが集中する大規模な IP ネットワークには適用できませんでした。しかし，Diff-serv 機能を使用すれば，ネットワークの境界ルータで設定した条件に一致する IP フローを検出し，このフローの IP ヘッダ内 DS Field の上位 6 ビットである DSCP(Differentiated Services Code Point) に，ドメイン内で行う制御の内容をビットパターンとして集約し転送します。後続のルータは，DSCP だけを参照して優先制御などを行うため，高速にパケット転送を行うことができます。このようなシンプルなアーキテクチャを使用し，ISP での契約サービスの差別化や，各種アプリケーションのサービスの差別化などの，ポリシーベースのサービスを行えます。

(1) Diff-serv のネットワークモデル

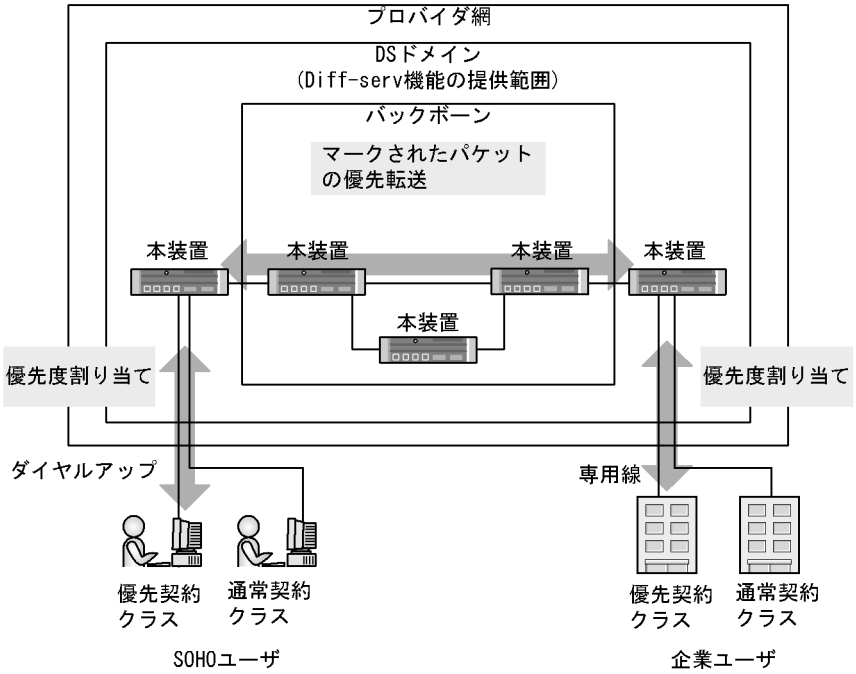
Diff-serv 機能を使用するネットワークを DS **ドメイン**と呼びます。この DS ドメインは境界に位置する**バウンダリノード**とコアに位置する**インテリアノード**から構成されます。フロー数が少なく回線速度が比較的低速のバウンダリノードは Diff-serv 機能の全機能を備えています。一方，高速で多数のフロー数を抱えるインテリアノードは簡易な機能を備えます。

バウンダリノードはネットワークの境界ルータに当たり，フローを識別して DSCP へ集約して DSCP に基づいて転送動作を行います。ここでバウンダリノードがパケットに対して行うマーキングを**ネットワークマーキング**と呼びます。また，ユーザがあらかじめパケットに DSCP を付けて転送する場合は，バウンダリノードが契約帯域の監視および送信制御だけを行います。この，ユーザがあらかじめパケットに対して行うマーキングを**ユーザマーキング**と呼びます。

インテリアノードはネットワークのバックボーンのルータに当たり，DSCP に基づいた転送動作だけを行います。この優先転送動作を，PHB(Per Hop Behavior) と呼びます。

Diff-serv 機能の概要を次の図に示します。

図 2-1 Diff-serv 機能の概要



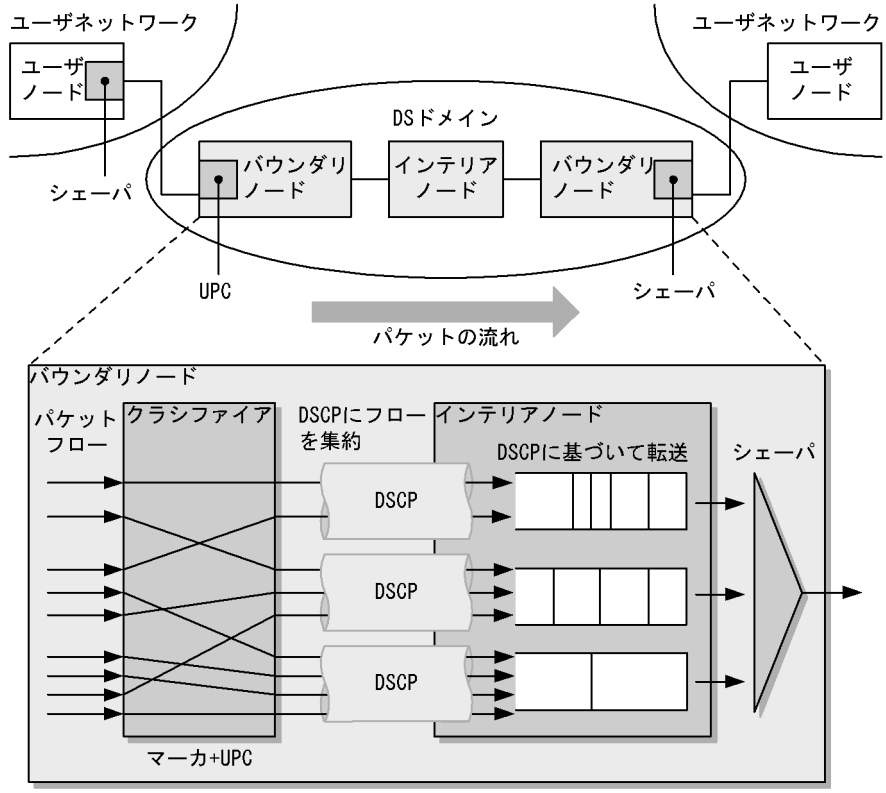
(2) バウンダリノードおよびインテリアノードの機能

バウンダリノードおよびインテリアノードでの，Diff-serv の機能について説明します。

- バウンダリノードの機能
  TCP/IP ヘッダからフローを識別し，個々のユーザとの契約に基づいて DSCP へ分類・集約する**クラシファイア**，IP ヘッダの DS フィールドに DSCP 値を書き込む**マーカ**，ユーザとの契約帯域を DSCP ごとに監視する UPC，送信帯域を制御する**シェーパ**機能があります。
- インテリアノードの機能
  インテリアノードはパケットヘッダ内の DSCP に基づいて優先転送だけを行います。

バウンダリノードおよびインテリアノードの機能を次の図に示します。

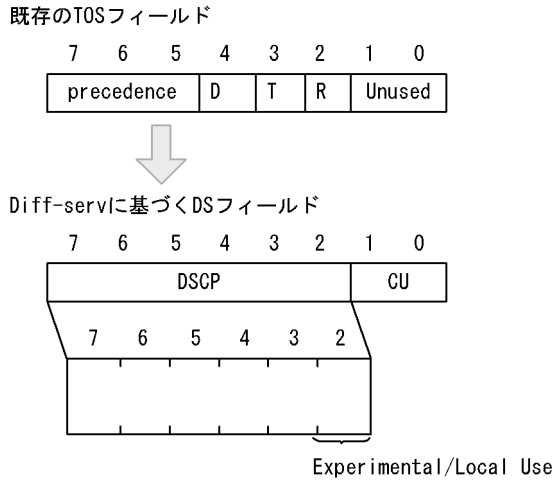
図 2-2 バウンダリノードおよびインテリアノードの機能



(3) DS フィールドと DSCP

Diff-serv では，既存の IP ヘッダ内の TOS フィールドを DS フィールドとして再定義しています。既存の TOS フィールドのフォーマットと，Diff-serv で使用する DS フィールドのフォーマットを次の図に示します。

図 2-3 TOS フィールドと DS フィールド



（凡例） D : Delay
T : Throughput
R : Reliability
DSCP : Differentiated Services Code Point
CU : Current Unused

Diff-serv の DSCP は，6 ビットのフィールドを持っていますが，最下位ビットは，RFC で Experimental/Local Use と規定しています。また，DSCP 値の上位 3 ビットを Class selector として使用することで，既存の TOS フィールドとの互換性を取っています。

(4) Diff-serv の導入手順

Diff-serv の導入時に必要な情報について概要を示します。DS ドメイン内には，バウンダリノードとインテリアノードの 2 種類のルータがあります。DS ドメイン内で一貫したサービスを行うためには，次に示す項目を決定する必要があります。

- STEP1
  バウンダリノードでは次の項目を決定します。
  - DS ドメイン内の DSCP と転送動作の対応づけ
  - 各ルータの転送動作
  - 各出力インタフェースの優先制御方法

  インテリアノードでは，DS ドメイン内の DSCP と転送動作の対応づけを決定します。これらの決定項目は DS ドメイン全体に対するものです。
- STEP2
  バウンダリノードでは各フローの DSCP との対応づけと帯域制御を決定します。これは，ユーザごとに決定します。インテリアノードでは決定する項目はありません。

2.1.2 Diff-serv の QoS サービス

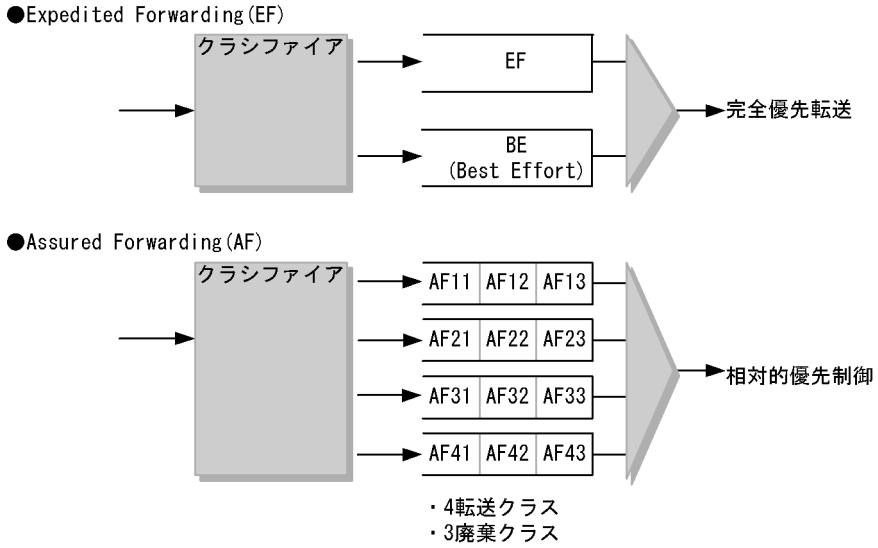
Diff-serv 機能が目標とする QoS サービスは，PHB と対応して標準化されています。Diff-serv の目標とする QoS サービスを次の表に示します。

表 2-1 Diff-serv の目標とする QoS サービス

サービス	特長	説明	対応する PHB
仮想専用線サービス	固定帯域保証	仮想専用線サービスの実現を目標とし，EF の DSCP を持ったパケットを他 DSCP のパケットより優先して転送し，固定帯域を保証します。	Expedited Forwarding (EF) 完全優先転送 (RFC 2598)
オリンピックサービス	相対的 QoS	オリンピックサービスの実現を目標とし，金，銀，銅の 3 種類のクラスを持ち，クラス間で相対的な QoS サービスを使用できます。	Assured Forwarding (AF) 相対的優先転送 (RFC 2597)

Diff-serv の目標とする QoS サービスを次の図に示します。

図 2-4 Diff-serv の目標とする QoS サービス



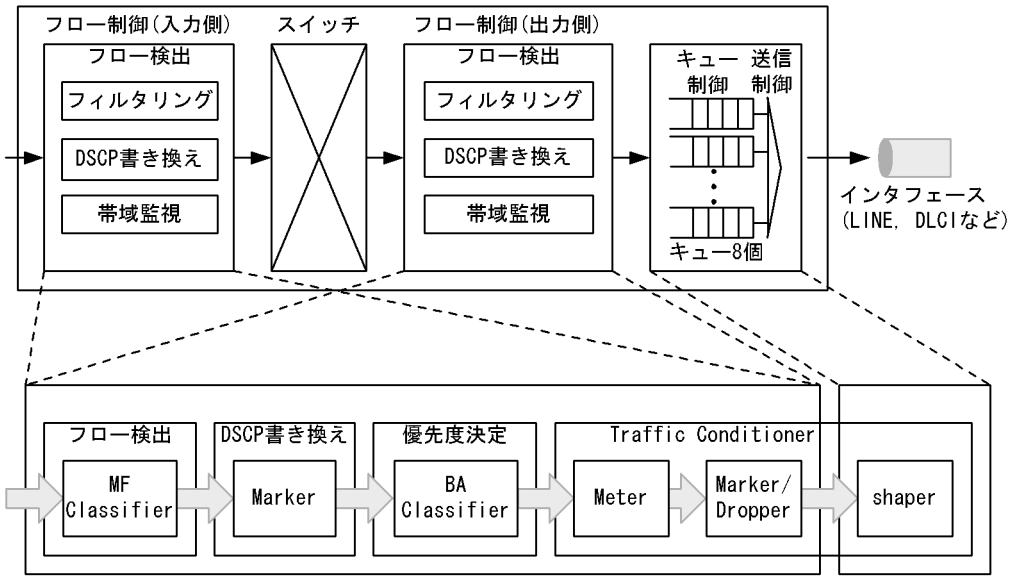
2.1.3 Diff-serv の制御仕様

本装置の Diff-serv の制御仕様は，「1.10 QoS 制御機能の仕様一覧」と同様で，RFC2475 に準拠しており，対象プロトコルは IP です。

2.2 Diff-serv の機能ブロック

本装置の Diff-serv の機能は，「1.2 QoS 制御構造」で示した，フロー制御，キュー制御，送信制御の 3 ブロックを使用して実現します。これらのブロックの内 RFC で Diff-serv ノードの必要機能として規定している MF Classifier(Multi Field Classifier)，Marker，BA Classifier(Behavior Aggregate Classifier)，Meter，Dropper は，フロー制御ブロックで，Shaper はキュー制御ブロックと送信制御ブロックで制御します。また，キュー制御および送信制御は，PHB(Per Hop Behavior) を決定します。本装置の Diff-serv 機能ブロックを次の図に示します。

図 2-5 本装置の Diff-serv 機能ブロック



各機能ブロックの説明を次の表に示します。

表 2-2 各機能ブロックの説明

機能ブロック		機能
MF Classifier		構成定義で指定するフロー識別条件によって IP フローの検出を行います。
Marker		MF Classifier で検出した IP フローのすべてのパケットに対して，構成定義で指定した DSCP 値のマーキングを行います。
BA Classifier		入力パケットの DSCP 値によって，出力優先度とキューイング優先度を決定します。
TrafficConditioner	Meter	IP フロー単位または DSCP 単位に使用している帯域の監視を行い，使用中の帯域を Marker，Shaper，Dropper に通知します。
	Marker	違反帯域のパケットに対して，構成定義で指定した DSCP 値のマーキングを再度行います。
	Dropper Shaper	Meter から通知される使用中帯域の状態に基づいて，違反帯域のパケットに対して帯域の調整動作を行います。

2.2.1 フロー制御

フロー制御は入力側と出力側の 2 か所で行います。

（1） MF Classifier(Multi Field Classifier)

MF Classifier は，あらかじめ構成定義で指定された条件で IP フローを検出します。構成定義で指定できる IP フローの識別条件と指定方法については，「1.3　フロー検出」を参照してください。

（2） Marker

Marker は，MF Classifier で検出した IP フローの 6 ビットの DS フィールドを書き換えます。また，帯域監視中の違反パケットに対するペナルティ動作としても DS フィールドを書き換えます。

（3） BA Classifier(Behavior aggregate Classifier)

BA Classifier は，入力インタフェースからのパケットか，装置内の Marker によってマーキングされたパケットの DS フィールドの値によって出力優先度とキューイング優先度を決定します。

（4） Traffic Conditioner

Traffic Conditioner には Meter，Marker，Shaper，Dropper の機能があります。これらの機能は，IP フローの帯域を監視して，違反帯域のパケットに対して帯域の調整動作を行います。具体的な調整動作を次に示します。

● Meter
IP フローの帯域を監視し，現在使用中の帯域を Marker，shaper，Dropper に通知します。

● Marker，Dropper
Meter から通知される現在使用中の帯域に対して，構成定義で設定した契約帯域以上のフローを受信したときに調整動作を行います。

● Shaper
帯域分配などの送信制御を行います。詳細は，「1.8　シェーパ」を参照してください。

中継動作はあらかじめ構成定義で設定しておきます。

- パケットを廃棄する。
- パケットの優先度を下げるために DSCP 値に変更する。
- パケットのキューイング優先度に変更する。

Traffic Conditioner の帯域監視は，構成定義で設定する監視帯域レートによって，監視時間が一意に決まります。このため，契約帯域に違反したフローは出力が契約帯域以下になる場合があります。詳細については「1.4　帯域監視」を参照してください。

2.2.2　廃棄制御

「1.7　廃棄制御」を参照してください。

2.2.3　シェーパ

「1.8　シェーパ」を参照してください。

2.2.4　機能ブロックと構成定義コマンドの対応

本装置で Diff-serv を行うには，構成定義の filter フロー情報および QoS フロー情報を使用して各機能ブロックに情報を設定します。機能ブロックに対応する構成定義コマンドを次の表に示します。

表 2-3 機能ブロックに対応する構成定義コマンド

Diff-serv の機能ブロック		本装置の構成定義コマンド	
ブロック名称	**機能**	**エントリ名称**	**パラメタ名称**
MFClassifier	フロー検出	flow filter	protocol {ip | <protocol No.> | tcp | udp | icmp | igmp |icmp6}
			upper
			lower
			dscp
			ip_source
			ip_destination
			port_source
			port_destination
			icmp_type
			icmp_code
			igmp_type
Marker	DSCP マーキング		replace_dscp
BA Classifier	フロー検出	flow qos	dscp
	優先度指定		priority
			discard
Meter/Dropper	違反検出		upc ※1
	違反パケットへの対応		penalty_drop penalty_discard penalty_dscp
Shaper	シェーパ	qos-queue-list	queue ○ _bandwidth ※2

注※1 upc 指定時は，監視帯域を設定します。
注※2 ○は，キュー番号を指定します。

DSCP 値と各クラスのマッピング例を次の図に示します。

図 2-6　DSCP 値と各クラスのマッピング例

	出力優先度	高 ← キューイング優先度 → 低			
		Discard クラス4	Discard クラス3	Discard クラス2	Discard クラス1
高	Priorityクラス8				
	Priorityクラス7				
	Priorityクラス6				101110
					46
	Priorityクラス5	100010	100100	100110	
		34	36	38	
	Priorityクラス4	011010	011100	011110	
		26	28	30	
	Priorityクラス3	010010	010100	010110	
		18	20	22	
	Priorityクラス2	001010	001100	001110	
		10	12	14	
低	Priorityクラス1	000000			
		0			

（凡例）

DSCP値(2進数)
DSCP値(10進数)

□：EFの推奨値　　■：Best Effortの推奨値

▒：AFの推奨値

注1　出力優先度が大きいほど，パケットを優先的に送出する。
注2　キューイング優先度が高いパケットほど廃棄しない。

2.3 構成定義作成時の注意事項

本装置は,「表 2-3 機能ブロックに対応する構成定義コマンド」で示したように，Filter 情報および QoS 情報の構成定義コマンドによって Diff-serv に対応できます。しかし，DS ドメイン内の本装置の位置づけと，本装置内を通過するフローのポリシーによって，構成定義の設定を Filter 情報または QoS 情報のどちらから行うかを決定する必要があります。

2.3.1 構成定義作成パターン

Filter 情報および QoS 情報の Diff-serv の代表的な設定パターンを次に示します。

- パターン 1：ネットワークマーキングでの入力側バウンダリノード
- パターン 2：ユーザマーキングでの入力側バウンダリノード
- パターン 3：インテリアノードおよび出力側バウンダリノード

Diff-serv の構成定義作成パターンを次の表に示します。

表 2-4 Diff-serv の構成定義作成パターン

定義パターン	inbound					outbound
	MF	Marker	BA	Meter	Dropper	
パターン 1	F	F	Q	Q	Q	－
パターン 2	－	－	Q	Q	Q	－
パターン 3	－	－	Q	－	－	－

（凡例） F：flow filter で定義する Q：flow qos で定義する －：規格外である

Diff-serv の構成定義を行う場合は，フローに対して Inbound 側の各エントリを使用しますが，次の場合は，Outbound 側エントリを使用してください。

- Outbound 側でメディアごとおよびレイヤ 2 プロトコルごとの QoS 機能を連携する場合 (index を用います。)
- Outbound 側でユーザごとに QoS 制御する場合

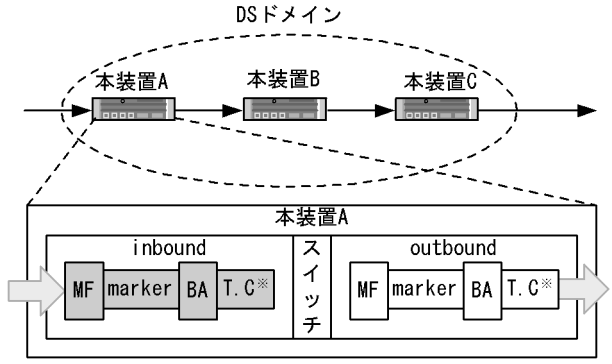
2.3.2 適用例

設定パターンごとの DS ドメイン内の本装置の位置づけと想定される適用例を，次に示します。

(1) パターン 1 の適用例

ネットワークマーキングを行うときの入力側バウンダリノードで，DS ドメイン外からのフローに対して対応する DSCP をマーキングし，マーキングした単位に帯域監視を行う場合に，パターン 1 を使用します。本装置の位置づけと適用例を次の図に示します。

図 2-7　本装置の位置づけと適用例 (パターン 1)

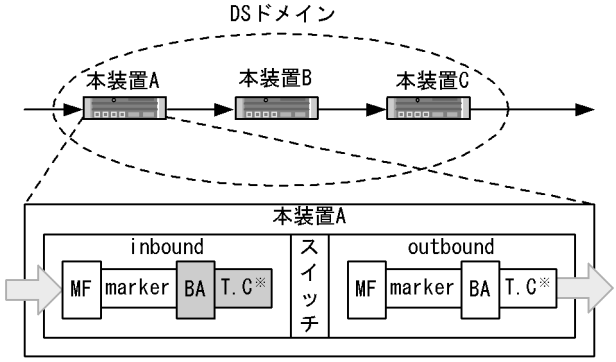


注※　T.C：Traffic Conditioner

(2) パターン 2 の適用例

ユーザマーキングを行うときの入力側バウンダリノードで，DSCP 単位に帯域監視を行う場合に，パターン 2 を使用します。また，ネットワークマーキングで DSCP のマーキングを行わない場合もこのパターンを使用します。本装置の位置づけと適用例を次の図に示します。

図 2-8　本装置の位置づけと適用例 (パターン 2)

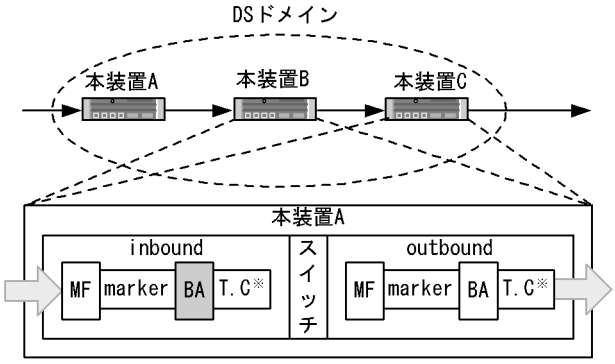


注※　T.C：Traffic Conditioner

(3) パターン 3 の適用例

ユーザマーキングを行うときの入力側バウンダリノードで，DSCP 単位に帯域監視を行う場合に，パターン 3 を使用します。また，ネットワークマーキングで DSCP のマーキングを行わない場合もこのパターンを使用します。本装置の位置づけと適用例を次の図に示します。

図 2-9　本装置の位置づけと適用例 (パターン 3)



注※　T.C：Traffic Conditioner

3 IPX ルーティング

IPX は Novell 社のネットワーク OS である NetWare で使用されている通信プロトコルであり，ネットワーク層のプロトコルです。この章では IPX を使用したルーティングについて説明します。

3.1　IPX ルーティング概説

3.2　通信処理機能

3.3　中継機能

3.4　経路制御機能

3.5　特殊制御パケット処理機能

3.6　ネットワーク設計の考え方

3.1 IPX ルーティング概説

本装置では NetWare の 3.11J，3.12J および 4.1J に対応した RIP/SAP ルーティング機能を実装しています。IPX および NetWare は Novell 社独自のプロトコルであるため，準拠する国際標準／規約はありません。NetWare で一般に使用される用語，プロトコル，サーバおよびクライアントの設定項目などは，NetWare のマニュアルを参照してください。

3.1.1 フレームタイプ

本装置でサポートするイーサネット上での IPX のフレームタイプは 4 種類です。本装置では 4 種類のフレームタイプを同一のイーサネット上に混在できます。その場合，異なるフレームタイプごとにネットワークアドレスを設定する必要があります。

FDDI については SNAP 型だけをサポートしています。したがって，FDDI 直結のマシンで NetWare を使用する場合には SNAP 型で運用する必要があります。ただし，本装置は FDDI を直接接続できないので注意してください。イーサネット上のフレームタイプを次の図に示します。

図 3-1 イーサネット上のフレームタイプ

●Ethernet 802.3(802.3RAWとも呼ばれる)

DA (6)	SA (6)	LEN (2)	IPXヘッダ

（凡例）LEN：LENより後のフィールドのバイト数。最小は46(0x2E)，最大は1500。

●Ethernet II

DA (6)	SA (6)	タイプ (2)	IPXヘッダ

（凡例）タイプ：0x8137，タイプより後のフィールドの最小は46(0x2E)，最大は1500。

●Ethernet 802.2

DA (6)	SA (6)	LEN (2)	LLC (3)	IPXヘッダ

（凡例）LEN：LENより後のフィールドのバイト数。最小は46(0x2E)，最大は1500。
LLC：0xe0e003

●Ethernet SNAP

DA (6)	SA (6)	LEN (2)	LLC (3)	SNAP (5)	IPXヘッダ

（凡例）LEN：LENより後のフィールドのバイト数。最小は46(0x2E)，最大は1500。
LLC:0xAAAA03
SNAP：0x0000008137

（ ）内の数字はバイト数を示す。

3.1.2 ノードアドレス

6 バイト (16 進数で 12 桁) のアドレスです。本装置では，イーサネットの場合は各ポートの MAC アドレスを使用しますので IPX での設定は不要ですが，WAN および ATM の場合は設定が必要です。同じネットワークアドレスでは各ノードアドレスはユニークな値を設定してください。全ビットが 1 または 0 のアドレスは使用できません。

3.1.3 ネットワークアドレス

4 バイト (32 ビット) のアドレスです。接続するネットワークシステム内でユニークな値を設定する必要があります。全ビットが 1 または 0 のアドレスは使用できません。ただし，ISDN バックアップを行う場合，バックアップ元とバックアップ先に同じアドレスを定義できます。

3.1.4 インタフェース

IPX ルーティング機能を行うインタフェース定義は，IP インタフェースが定義されたインタフェース (rmEthernet，AUX，トンネル，vlan は除く) に付加する形態で定義します。したがって，IPX インタフェース単独の定義はできません。

3.1.5 IPX ルーティングの機能

本装置は受信した IPX パケットをルーティングテーブルに従って中継します。この中継処理は大きく分けて次の四つの機能から構成されています。

- 通信処理機能
  IPX レイヤ (ネットワークレイヤ) の送信および受信処理を行う機能です。
- 中継機能
  ルーティングテーブルに従って IPX パケットを中継する機能です。
- 経路制御機能
  経路情報の送受信や，中継経路を決定しルーティングテーブルを作成する機能です。
- 特殊制御パケット処理機能
  IPX プロトコルで特徴的な制御パケットについてルータが処理を行う機能です。

3.2 通信処理機能

IPX(Internetwork Packet Exchange) プロトコルについて説明します。

(1) IPX パケットのヘッダフォーマット

IPX パケットのヘッダフォーマットを次の図に示します。

図 3-2 IPX パケットのヘッダフォーマット

(2) パケット長

最大 1500 バイトのパケットを送受信できます。これによって Netware3.12J で使用される LIP(Large Internet Packet) に対応できます。LIP はイーサネットでユーザデータ長が最大 1436 バイト長です。なお，本装置では IPX の最大パケット長は FDDI も 1500 バイトですので，サーバとクライアントがすべて FDDI 直結の場合はサーバのパケット長を調整してください。

(3) IPX パケットヘッダ有効性チェック

IPX パケット受信時に IPX パケットのヘッダの有効性をチェックします。チェック内容を次の表に示します。

表 3-1 IPX パケットヘッダチェック内容

IPX パケット ヘッダフィールド	チェック内容	チェック NG 時 のパケット廃棄
チェックサム	0xffff であること※	○
レングス (長さ)	実際に受信したレングスが 1500 以下であること このフィールド自体はチェックしない	○
トランスポート制御	0x0f 以下であること	○
パケットタイプ	0x00，0x01，0x02，0x04，0x05，0x11 のどれかであること	○
宛先ネットワークアドレス	RIP，SAP でなければ受信ポートのネットワークアドレスでないこと，または RIP，SAP でなければ 0x0000 でないこと	○
宛先ノードアドレス	RIP，SAP でなければ本装置のポートのアドレスでないこと	○
宛先ソケット	0x0455 以外であること NetBIOS の廃棄	○
送信元ネットワークアドレス	チェックしない	−
送信元ノードアドレス	チェックしない	−
送信元ソケット	0x0455 以外であること NetBIOS の廃棄	○

（凡例） ○：行う　－：該当しない
注※　Netware3.12J を使用する場合，NetWare サーバ／クライアント側の設定でチェックサムを使用しないことを設定してください。

（4） ノードアドレスフィールドのビットの順番

IPX パケットヘッダのノードアドレスフィールド（宛先，送信元）のデータはキャノニカル表現（低位ビットが先頭となる順番）です。

3.3 中継機能

中継機能は受信したパケットをルーティングテーブルに従ってフォワーディングする処理です。

(1) ルーティングテーブルの内容

ルーティングテーブルは複数個のエントリで構成されており，各エントリは次に示す内容を含んでいます。本装置のルーティングテーブル内容は show ipx route コマンドで表示できます。

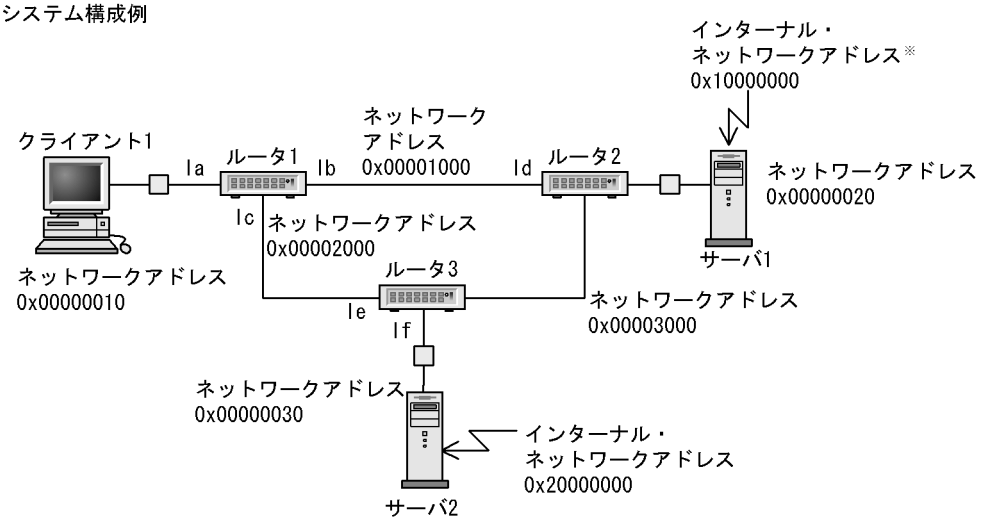
- Dest. Net ：宛先ネットワークアドレス
- Next Hop Net ：ネクストホップのネットワークアドレス
- Next Hop Host ：ネクストホップのノードアドレス
- IF Name ：送出インタフェース名称
- Hops ：ホップ数
- Ticks ：ティック数
  宛先のネットワークにパケットを届けるのに必要な時間。単位は 1/18 秒。ただし，中継経路の各ネットワークのティック数を加算した値。
- Flags ：このエントリの作成が，ダイナミックルーティングによって学習されたもの／スタティック定義されたもの。

(2) ルーティングテーブルの例

システム構成例を次の図に示します。

図 3-3　システム構成例

●システム構成例



注※　インターナル・ネットワークアドレスとは，サーバに定義された内部的なネットワークアドレスである。サーバと通信する場合，このネットワークアドレスが使用される。

●インタフェースla～lfのノードアドレス

la : 00-00-87-40-0A-E0
lb : 00-00-87-40-0B-E0
lc : 00-00-87-40-0C-E0
ld : 00-00-87-40-0D-E0
le : 00-00-87-40-0E-E0
lf : 00-00-87-40-0F-E0

●ルータ1のルーティングテーブル

Dest.Net	Next Hop Net	Next Hop Host	IF Name	Hop	Ticks	Flags
00000010	00000010	00-00-87-40-0A-E0	la	1	1	static
00001000	00001000	00-00-87-40-0B-E0	lb	1	1	static
00002000	00002000	00-00-87-40-0C-E0	lc	1	1	static
00000020	00001000	00-00-87-40-0D-E0	lb	2	2	rip
00000030	00002000	00-00-87-40-0E-E0	lc	2	2	rip
00003000	00001000	00-00-87-40-0D-E0	lb	2	2	rip
10000000	00001000	00-00-87-40-0D-E0	lb	3	3	rip
20000000	00002000	00-00-87-40-0E-E0	lc	3	3	rip

NetWare ではネットワークの時間評価値（早い／遅い）としてティック数を使用します。「図 3-3　システム構成例」でルータ間のネットワークのティック数が 3 本とも等しい値と仮定します。この場合，ルータ 1 はクライアント 1 からサーバ 1 への経路として，ルータ 1 →ルータ 2 の経路をルーティングテーブルに作成します。ルータ 1 →ルータ 3 →ルータ 2 の経路はルーティングテーブルに作成しません。

(3) ルーティングテーブルの検索とパケット中継

本装置は受信した IPX パケットの宛先ネットワークアドレスに該当するエントリをルーティングテーブルから検索します。一致したエントリ内のネクストホップのネットワークアドレスと受信パケットの宛先ネットワークアドレスが一致した場合は，ルータに直接接続されたネットワークアドレスであると判断します。

- 直接接続されたネットワークアドレス宛ての場合
  受信パケットの宛先ノードアドレスを MAC ヘッダの宛先アドレスとして直接接続されたネットワークに送信します。これによって，パケットは宛先のノードに到着します。
- 直接接続されたネットワークアドレス宛てでない場合
  一致したエントリ内にあるネクストホップのノードアドレスを MAC ヘッダの宛先アドレスとして，ネ

クストホップへのネットワークアドレスに接続しているインタフェースからパケットを送信することによって中継します。

3.4 経路制御機能

3.4.1 RIP プロトコル

各ルータは RIP(Routing Information Protocol) によって経路情報を交換し，ダイナミックにルーティングテーブルを作成します。IPX ルーティングを使用する RIP は，IP ルーティングで使用する RIP とはまったく異なるパケットです。RIP パケットの種類を次の表に示します。

表 3-2 RIP パケットの種類

パケットの種類	パケット送出元	機能	パケットの送出先
要求	サーバ／ルータ	経路情報収集の要求※1	ブロードキャスト
	クライアント	最短経路情報の要求	
応答	サーバ／ルータ	要求に対する応答※1	要求パケット発行者
		周期的な経路情報の通知※2※3	ブロードキャスト
		経路変更時の情報の通知※1	

注※1 non_Periodic RIP
注※2 Periodic RIP
注※3 周期 RIP と呼びます。

(1) RIP パケット送信／受信の制御

各サーバ／ルータはサーバ／ルータの存在を周期的に通知するために，**周期** RIP(Periodic RIP) と呼ばれるブロードキャストパケットを送信します。本装置ではこの周期 RIP の送信間隔 (Periodic RIP Interval) をインタフェース単位に構成定義情報で変更できます。値を 0 に設定すると周期 RIP パケットは送信しません。また，そのほかの RIP パケット (**非周期** RIP：non-Periodic RIP) の送信はインタフェース単位で抑止するように設定できます。

RIP パケット受信に対しては，構成定義情報の指定に関係なく学習を行い，エントリを更新します。構成定義情報の指定と RIP 送信／受信制御の関係を次の表に示します。

表 3-3 構成定義情報の指定と RIP 送信／受信制御の関係

RIP パケット	構成定義情報の指定	送信	受信
周期 RIP	Periodic_rip_interval 0(分)	周期 RIP を送信しない	構成定義情報の指定に関係なく，RIP パケット受信による学習は行います。
	Periodic_rip_Interval n(分)	周期 RIP を送信する	
非周期 RIP	non_periodic_rip_send_off	非周期 RIP を送信しない	
	non_periodic_rip_send	非周期 RIP を送信する	

通常，各インタフェースの RIP は次に示すどちらかの設定をします。

- 周期／非周期ともに送信する (ダイナミック)
- スタティックルーティングを設定した場合に周期／非周期ともに送信しないように設定する

(2) 最適経路の決定とルーティングテーブルへの登録

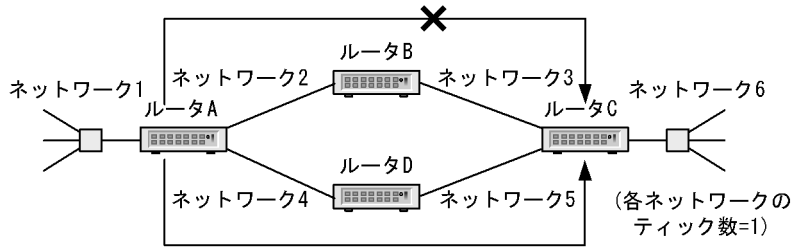
本装置では複数の経路から最適経路を決定するときに，ティック数の合計が小さい経路を選択し，ルーティングテーブルのエントリを作成します。一つのネットワークのティック数はイーサネットでは固定的に 1，WAN および ATM ではインタフェースごとに設定できます。

しかし，そのほかのルータの中にはホップ数 (中継するルータの数) で最適経路を決定するものもあるため，通常ティック数は 1 に設定することをお勧めします。また，本装置では同じティック数の経路が複数あれば，先に学習した方をルーティングテーブル中に保持します。

(a) 経路の決定

経路の決定を次の図に示します。

図 3-4 経路の決定



ルータ A では，ネットワーク 1 からネットワーク 6 への経路として，ルータ A → B → C の経路をルータ A → D → C の経路より先に学習した場合，ティック数が同じであるのでルータ A → B → C の経路が有効になります。

A → B → C の経路に障害が発生した場合，RIP の再学習によってルータ A の経路は A → D → C に切り替わりますが，経路交替までの間，ネットワーク 1 からネットワーク 6 への通信は中断されます。

(3) ルーティングエントリのエージング

ルーティングエントリのエージング時間は，構成定義情報で指定した周期 RIP の送信間隔の 3 倍です。指定値が 0 の場合，エージングは行いません。なお，スタティック定義されたルーティングエントリはエージングの対象となりません。

(4) IPX ルーティングエントリ数

本装置は IPX ルーティングエントリを最大 1000 個持つことができます。ただし，この値はダイナミックに学習した数とスタティックに定義された数の合計です。

3.4.2 スタティックルーティング

スタティックルーティングは構成定義情報でルーティングのエントリを設定することで実現できます。スタティックルーティングで複数の経路を設定した場合，またはダイナミックルーティングと混在した場合，ルーティングテーブルエントリのティック数が小さい経路が優先されます。

3.5 特殊制御パケット処理機能

IPX ルーティングにはいくつかの特殊制御パケット処理機能がありますが，SAP パケット処理およびウォッチドッグ・パケット処理について説明します。

3.5.1 SAP パケット処理

本装置は NetWare のサーバではありませんが，SAP パケットを処理し，SAP テーブルを作成することによってサーバの情報をまとめて別ネットワークに通知します。SAP パケットの種類を次の表に示します。

表 3-4 SAP パケットの種類

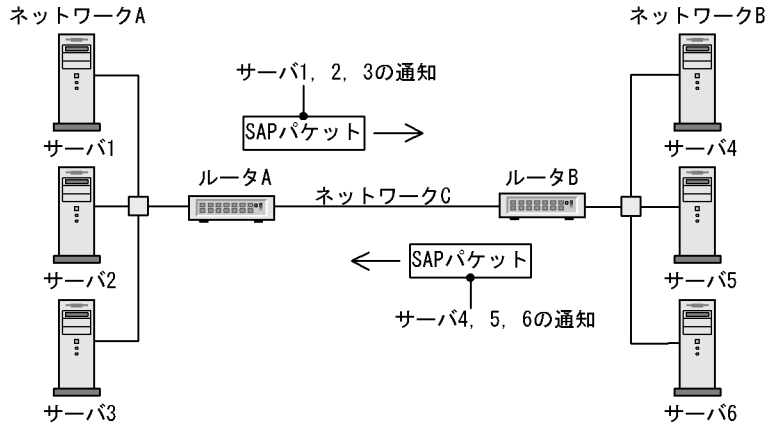
パケットの種類	パケット送出元	機能	パケットの送出先
一般要求 (General SAP)	サーバ／ルータ	サーバ情報収集の要求※1	ブロードキャスト
一般応答 (General SAP)	サーバ／ルータ	周期的なサーバ情報の通知※2	ブロードキャスト
		変更サーバ情報の通知※1	
		サーバ情報収集要求に対する応答※1	要求パケット発行者
最短要求 (Nearest SAP)	クライアント	最短サーバ情報の要求	ブロードキャスト
最短応答 (Nearest SAP)	サーバ／ルータ	最短サーバ情報要求に対する応答※1	要求パケット発行者

注※1 non-Periodic SAP

注※2 Periodic SAP

SAP パケット処理を次の図に示します。

図 3-5 SAP パケット処理



この図で，ルータ A はサーバ 4，5，6 の存在をルータ B からの SAP パケットで認識して，サーバ 1，サーバ 2，サーバ 3 に通知します。これによって，ネットワーク C 上はルータ A，B 間の SAP パケットだけが伝送されることになります。

(1) SAP パケット送信の制御

本装置では SAP パケットの送信も RIP パケットの送信と同様，周期的な SAP パケットの送信間隔 (Periodic SAP Interval) をインタフェース単位で変更できます。値を 0 に設定すると周期 SAP パケットは送信しません。そのほかの SAP パケット (non-Periodic SAP) の送信はインタフェース単位で抑止するように設定できます。

SAP パケット受信に対しては，構成定義情報の指定に関係なく学習を行い，エントリを更新します。構成定義情報の指定と SAP 送信／受信制御の関係を次の表に示します。

表 3-5 構成定義情報の指定と SAP 送信／受信制御の関係

SAP パケット分類	構成定義情報の指定	送信	受信
周期 SAP (Periodic SAP)	Periodic_sap_Interval 0(分)	周期 SAP を送信しない	構成定義情報の指定に関係なく，SAP パケット受信による学習は行います。
	Periodic_sap_Interval n(分)	周期 SAP を送信する	
非周期 SAP (non-Periodic SAP)	non_periodic_sap_send_off	非周期 SAP を送信しない	
	non_periodic_sap_send	非周期 SAP を送信する	

通常，各インタフェースの SAP は次に示すどちらかの設定をします。

- 周期／非周期ともに送信する (ダイナミック)
- スタティックルーティングを設定した場合に周期／非周期ともに送信しないように設定する

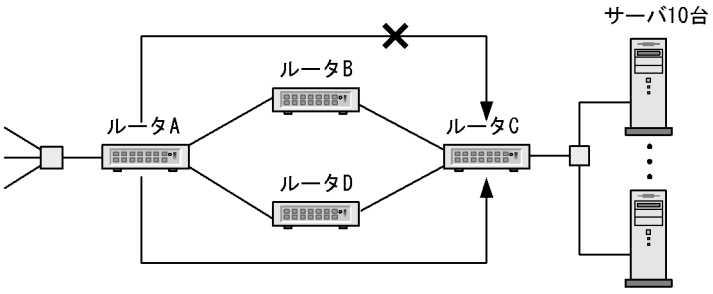
(2) SAP テーブルエントリの登録と経路

本装置では SAP パケットの処理の結果，サーバ情報を SAP テーブルに登録します。サーバ情報ごとにエントリを作成します。SAP テーブルエントリの内容は show ipx servers コマンドで表示できます。なお，SAP テーブルエントリの各エントリは該当するサーバへの経路情報がルーティングテーブルに学習，または設定されていなければ学習できません。各サーバには内部ネットワークアドレスが設定され，そのアドレスへの経路情報がルーティングテーブルエントリに作成されている必要があります。このため，スタティックルーティングの場合などは注意が必要です。なお，それぞれのサーバには，接続するネットワークシステムでユニークなサーバ名を使用してください。

(a) 経路の決定 (経路切り替え)

経路切り替えの場合の経路決定を次の図に示します。

図 3-6 経路の決定 (経路切り替え)



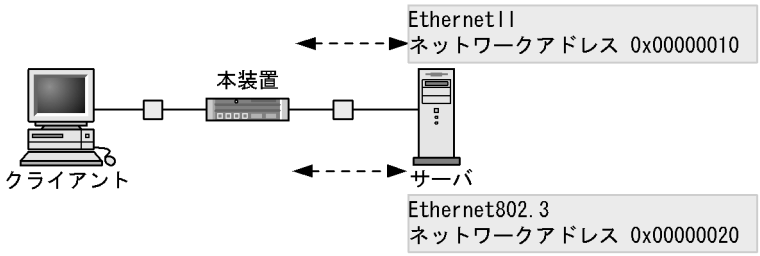
この図で，ルータ A のように冗長経路がある場合，先に学習したサーバ情報だけを SAP テーブルエントリに登録します。このため，例えば，ルータ A → B → C の経路で 10 個の SAP 情報をルータ A は保持します。この経路に障害が発生した場合は，再学習してルータ A → D → C の経路で SAP 情報が登録されると通信が復旧します。

(b) 経路の決定 (論理的な冗長構成 (複数フレームタイプの混在))

複数のフレームタイプが混在するネットワークでは，物理的には一つのネットワークであっても，論理的にはフレームタイプごとに異なる経路が存在します。この場合も，先に学習した経路で SAP 情報エントリを登録します。

複数フレームタイプの混在する場合の例を次の図に示します。

図 3-7 複数フレームタイプの混在する場合の例



この図では，本装置とサーバ間は一つのネットワークで接続されていますが，異なるフレームタイプである EthernetII と Ethernet802.3 に対して，それぞれ経路が存在します。本装置が先に学習した経路が EthernetII である場合，SAP 情報の経路も EthernetII になります。

(3) SAP テーブルエントリのエージング

SAP テーブルエントリのエージング時間は，構成定義情報で指定した周期 SAP の送信間隔の 3 倍です。指定値が 0 の場合，エージングは行いません。なお，スタティック定義された SAP テーブルエントリはエージングの対象になりません。

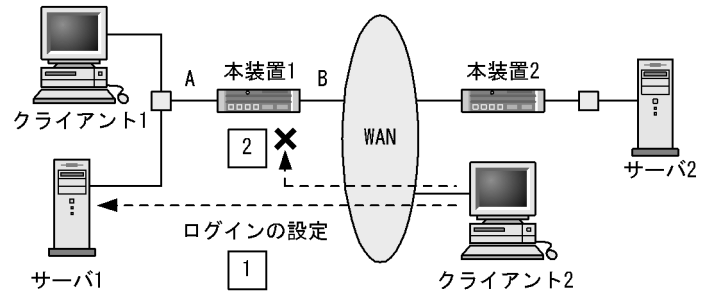
(4) SAP エントリ数

本装置の登録できる SAP エントリ数は，1000 個です。ただし，この値はダイナミックに学習した数とスタティックに定義された数の合計です。

(5) SAP テーブルのスタティック設定

本装置は構成定義情報で SAP テーブルエントリを設定できます。SAP テーブルエントリを使用したネットワーク構成を次の図に示します。

図 3-8　SAP テーブルエントリを使用したネットワーク構成



1. クライアント2がサーバ1にログインする設定をする。
2. 本装置1にサーバ2のスタティックサーバ情報を設定(ネクストポップはB)すると，
   クライアント2がサーバ1にログインできなくなることがある。

本装置 1 がクライアント 2 からの Nearest SAP(ブロードキャスト) に対して単純には応答しないように動作するため，クライアント 2 がサーバ 1 にログインするための構成定義情報の設定には注意が必要です。クライアントのサーバログイン条件を次の表に示します。

表 3-6　クライアントのサーバログイン条件

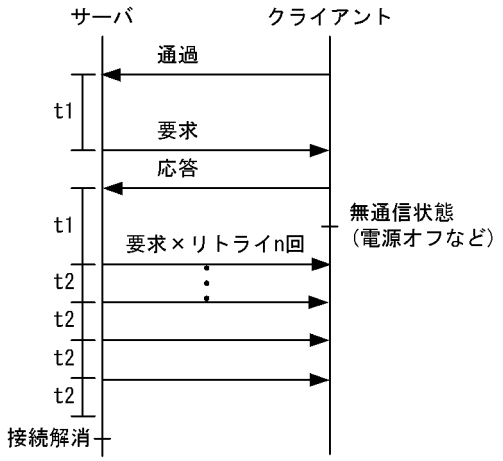
項目	ポートの構成定義情報	ログイン
Nearest SAP に対する応答動作	ポート B の定義の Nearest SAP Reply を off に設定	できない
	ポート B の定義の Nearest SAP Reply を on に設定	できる

3.5.2　ウォッチドッグ・パケットの制御

NetWare ではサーバにログインしたクライアントが無通信状態となったとき，サーバからクライアントに対して接続状態 (クライアントの電源オフも含む) を確認するため周期的に**ウォッチドッグ・パケット** (要求) を送信します。

クライアントはウォッチドッグ・パケット (要求) を受信すると，ウォッチドッグ・パケット (応答) をサーバ宛てに返信します。しかし，クライアントがログアウトしないで電源オフした場合は応答パケットは返信されません。このため，サーバはさらに周期的にウォッチドッグ・パケット (要求) を再送信し，応答パケットの返信がない場合，サーバはその無応答のクライアントの接続を解消します。ウォッチドッグ・プロトコルのシーケンスを次の図に示します。

図 3-9　ウォッチドッグ・プロトコルのシーケンス



ウォッチドッグ・プロトコルは NCP(Netware Core Protocol) の機能で，要求パケットの送信を中止することはできませんが，Netware3.12J 以降のバージョンでは送信開始時間，送信周期，送信回数をサーバの設定によって変更できます。ウォッチドッグ・プロトコルのパラメータ値を次の表に示します。

表 3-7　ウォッチドッグ・プロトコルのパラメータ値

パラメータ	NetWare3.11J	NetWare3.12J，4.1J
ウォッチドッグ送信開始時間 (t1)	約 5 分 (固定)	約 16 秒～約 21 分 (可変)
ウォッチドッグリトライ間隔 (t2)	約 1 分 (固定)	約 10 秒～約 10.5 分 (可変)
最大リトライ回数 (n)	10 回 (固定)	5 回～ 100 回 (可変)

(凡例) t1，t2，n：「図 3-9　ウォッチドッグ・プロトコルのシーケンス」を参照のこと。

(1) ウォッチドッグ代理応答機能

ウォッチドッグ代理応答機能とは，ウォッチドッグの要求に対し，ルータがクライアントに代わって代理応答することで，サーバとルータ間のネットワークのトラフィックを低減させる機能です。この機能は一般にキープアライブ代理応答とも呼ばれることがありますが，本装置ではウォッチドッグ代理応答 (Watchdog Spoofing) 機能と称します。なお，本装置では SPX プロトコルによる定期的な接続確認に対する代理応答機能はありません。これらの定期接続確認フレームは単に IPX フレームとして中継されます。

本装置のウォッチドッグ代理応答機能はポートごとに次の中から選択できます。

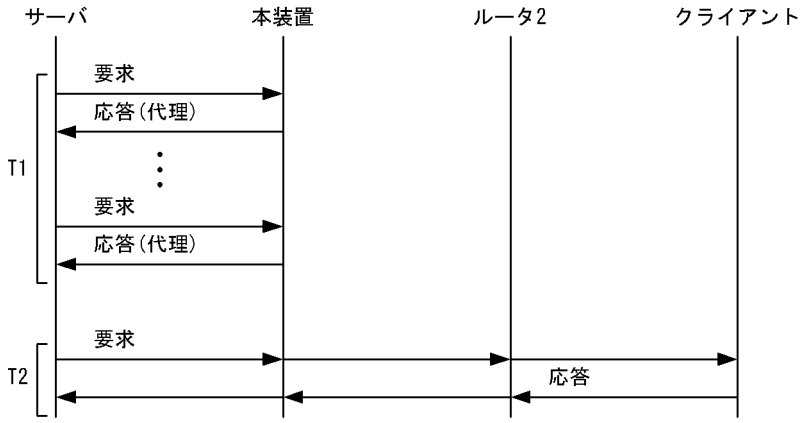
- ウォッチドッグ・パケットを周期的に代理応答する。(間引き方式)
  通常の設定としてお勧めします。
- クライアントの状態に関係なくウォッチドッグ・パケットの代理応答をする。
  課金などの関係で余計なパケットをすべて他ネットワークに送信したくないときに設定してください。
  クライアントをログオフしないで停止する (電源スイッチオフなど) と，サーバ上はそのクライアントとのコネクションが残り続けるので運用上注意が必要です。
- ウォッチドッグ・パケットの代理応答はしない。
  通常の設定としてお勧めします。

これらの設定を行うインタフェースは出力インタフェース側です。

(a) ウォッチドッグ代理応答 (間引き方式)

間引き方式によるウォッチドッグ代理応答を次の図に示します。

図 3-10　間引き方式によるウォッチドッグ代理応答



この図ではサーバからの要求に対して，一定時間 (T1) は本装置がサーバに代理応答します。その後一定時間 (T2) は本装置のウォッチドッグ・パケットを中継して，サーバ・クライアント間でウォッチドッグ・プロトコルを行わせます。T1，T2 は構成定義によって設定できますが，T2 ではサーバークライアント間でウォッチドッグ・プロトコルを実現させるために，次に示す条件を満足させる必要があります。

```
T2 > t1+t2×n
 (t1,t2の値は「表3-7　ウォッチドッグ・プロトコルのパラメータ値」参照)
```

これによって回線使用は低減します。また，クライアントがログオフしないで停止した場合は，サーバは最大 (T1 ＋ T2) 後，クライアントの停止を認識します。なお，T1，T2 の設定は各インタフェース単位ではなく，本装置の装置単位です。

3.5.3　そのほかの特殊パケット処理

- **シリアライゼーションパケットのフィルタリング**
  NetWare では，各サーバは固有の製造番号 (シリアル番号) をほかの全サーバに対して定期的に通知します。このトラフィックを低減するために，本装置ではシリアライゼーションパケットのフィルタリング (廃棄) を行うように設定できます。
- **ダイアグノスティックパケットのフィルタリング**
  ノベル社のプロトコル解析ソフトである LANalyzer が使用するダイアグノスティック (診断) パケットをトラフィック低減のためにフィルタリング (廃棄) できます。本装置宛てのダイアグノスティックパケットを受信した場合は廃棄します。
- **NETBIOS パケットのフィルタリング**
  NETBIOS は，ルーティングできるプロトコルではないですが，NetWare では IPX でカプセル化すれば IPX ネットワーク上を通過させることができます。しかし，実際にはルーティングではなく同報としてネットワーク間を中継し，高トラフィックによるネットワーク運用への支障が起こることが考えられます。このため，本装置では IPX でカプセル化された NETBIOS は中継しないで，受信時に廃棄します。

3.5.4　SAP フィルタリング

本装置は，学習したある特定の SAP エントリだけを送信 (Forwarding) したり，抑止 (Filtering) したりする SAP **フィルタリング機能**をサポートしています。本装置では最大 100 の SAP フィルタリングエントリが設定できます。

フィルタリング処理は，各エントリを構成定義情報に定義された順に調べ，SAP フィルタリングエントリの条件に SAP エントリが一致したら SAP フィルタリング動作 (送信／抑止) の指定によって，その SAP エントリを送信，または抑止します。最後の SAP フィルタリングエントリまで調べ条件に一致するものがない場合は送信します。

- SAP フィルタリング項目
  次に示す三つの SAP フィルタリング項目を任意に組み合わせて設定します。ある SAP フィルタリングエントリの設定項目をすべて満たした場合 (AND 条件)，その SAP フィルタリングエントリの条件が満たされたと判定します。
  条件一致時のパケットの処理は，Forward(その SAP エントリを送信)，Drop(その SAP エントリを抑止) のどちらかを指定します。さらに，フィルターモードとして Output(出力条件)，Input(入力条件) のどちらかを指定します。
  - Server type
    SAP エントリのサービスタイプに対してフィルタリングを行うサービスタイプを指定します。全タイプ指定をする場合は，「ffff」をご使用ください。
  - Server NetWork
    SAP エントリのネットワークアドレスに対してフィルタリングを行うネットワークアドレスを指定します。全ネットワークアドレスを指定する場合は，「ffffffff」をご使用ください。
  - Port Network
    フィルタリングを行うインタフェースを，ネットワークアドレスで指定します。全インタフェースを指定する場合は，「ffffffff」をご使用ください。

3.5.5 RIP フィルタリング

本装置は，学習したある特定の RIP エントリだけを送信 (Forwarding) したり，抑止 (Filtering) したりする RIP フィルタリング機能をサポートします。本装置では最大 100 の RIP フィルタリングエントリを設定できます。動作の概要は SAP フィルタリングと同様です。

- RIP フィルタリング項目
  次に示す二つの RIP フィルタリング項目を任意に組み合わせて設定します。フィルタリング動作／フィルタリングモードの考え方は SAP フィルタリングと同様です。
  - Network
    フィルタリングを行うネットワークアドレスを指定します。
  - Port Network
    フィルタリングを行うインタフェースをネットワークアドレスで指定します。

3.5.6 Ping 機能

IP と同様に IPX レベルでの Ping(経路情報疎通) 機能をサポートします。ping ipx コマンドを使用して実施します。目的装置のネットワークアドレス・ホストアドレスを指定してコマンドを実行し，相手からの応答の有無を確認することで経路疎通を確認できます。

なお，IPX-Ping は IPX の ECHO パケットを使用して実現していますが，ECHO パケットの応答をサポートしていない機種の場合は，Ping の応答が返りません。また，ECHO パケットの扱いについては次の仕様で動作します。相手機種によっては応答しない場合があるので注意してください。パケットサイズはコマンド実行時に指定できます。

受信時

パケットタイプ＝ 1，ソケット＝ 2 の ECHO パケットに対しパケットタイプ＝ 2，ソケット＝ 2 で応

答する。
パケットタイプ＝ 2，ソケット＝ 2 の ECHO パケットに対しパケットタイプ＝ 2，ソケット＝ 2 で応答する。

送信時

IPX-Ping コマンド実行時に，パケットタイプ＝ 1，ソケット＝ 2 の ECHO パケットと，パケットタイプ＝ 2，ソケット＝ 2 の ECHO パケットを同時に送信し，どちらか一方の応答があれば正常とみなす。

3.6 ネットワーク設計の考え方

3.6.1 中継性能

(1) 中継性能

本装置は IP 中継処理に最適化しています。IPX 中継処理は IP 中継処理のように最適化を行っていません。IPX を使用するネットワークを構築する場合，IPX の中継性能は RP 当たり 2500packet/s の中継性能を超えないように設計してください。また，IPX とブリッジを混在して使用する場合は IPX とブリッジを合わせて，RP 当たり 2500packet/s の中継性能を超えないように設計してください。

IPX 使用時のネットワーク構成の目安を次に示します。クライアント端末は RP 当たり 50 台以下に配分されるようにネットワークを構築してください。なお，同時に 6 台以上のクライアントがログイン動作を行ったとき，すべてのログイン完了まで数秒間かかる場合があります。

また，QoS 機能については IPX 中継性能以内のトラフィックの場合には効果があります。しかし，それを超えたトラフィックの場合は，内部でパケット廃棄が生じて，出力の優先制御が機能していないように見えることがあります。

(2) 過剰トラフィック発生時

過剰トラフィックおよび RM CPU 過負荷が継続して発生した場合，プロトコルデータの廃棄によって RIP/SAP のエージングタイムアウトが発生し，経路やサーバ情報が削除されることがあるので注意してください。この現象が継続する場合は，トラフィックを考慮してネットワーク構成を再考してください。

3.6.2 制御パケットのトラフィック

(1) RIP 情報

本装置ではルーティング情報について，次に示す設定ができます。

- ダイナミックルーティング設定だけ
- スタティックルーティング設定だけ
- 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混在した設定

これらを設定するためにはインタフェースごとに RIP 制御パケットの送信を制御する指定があります。デフォルトの設定は RIP を 1 分間隔で送出する設定となっています。このため，スタティックルーティングで動作させる場合や，WAN 回線で RIP の制御パケットが送出されると問題がある (課金など) 場合は，これらの設定を変更してください。

周期 RIP のトラフィック

周期的にブロードキャストしている RIP のトラフィックモデルを次に示します。これらはプロトコルの制御データですが，RIP のエントリ数に依存して増加します。低速 WAN 回線などはネットワーク構築上これらの制御データだけで負荷が過多にならないようにキュー長を考慮し，制御データのトラフィックを回線使用率の 10%以下になるように注意してください。
制御データだけでトラフィックが過多になるような場合は，周期 RIP を止めてスタティックで定義することをお勧めします。

一度に送信するパケット数(インタフェース当たり)＝
n÷50パケット(1パケット432バイト)

n：保持しているRIPエントリ数

エントリ数50以下の場合は1パケット。1000(max)の場合は20パケットになります。

(2) SAP 情報

本装置では IPX サーバ情報を次のように設定できます。

- ダイナミック SAP 情報設定だけ
- スタティック SAP 情報設定だけ
- ダイナミック SAP 情報とスタティック SAP 情報の混在した設定

これらを設定するためにはインタフェースごとに SAP 制御パケットの送信を制御する指定があります。デフォルトの設定は SAP を 1 分間隔で送出する設定となっています。このため，スタティック SAP で動作させる場合や，WAN 回線で SAP の制御パケットが送出されると問題がある (課金など) 場合は，これらの設定を変更してください。

周期 SAP のトラフィック

周期的にブロードキャストしている SAP のトラフィックモデルを次に示します。これらはプロトコルの制御データですが，SAP のエントリ数に依存して増加します。低速 WAN 回線などはネットワーク構築上これらの制御データだけで負荷が過多にならないようにキュー長を考慮し，制御データのトラフィックを回線使用率の 10%以下になるように注意してください。
制御データだけでトラフィックが過多になるような場合は，周期 SAP を止めてスタティックで定義することをお勧めします。

一度に送信するパケット数(インタフェース当たり)＝
n÷7パケット(1パケット480バイト)

n：保持しているSAPエントリ数

エントリ数7以下の場合は1パケット。1000(max)の場合は143パケットになります。

NetWare4.1J 使用時の注意

- SAP 情報中のサーバ名称にキャラクタコード以外のコードを使用した場合，該当するコードによる SAP スタティックは使用できないので注意してください。
- サーバの利用形態によっては周期パケットが発生する場合があるので，ISDN などの課金の影響を考慮する必要があります。

(3) そのほかの制御パケット

IPX ではユーザデータ以外に次のパケットを送信します。

- ウォッチドックパケット
- シリアライゼーションパケット
- ダイアグノスティックパケット
- NETBIOS パケット

これらのパケットに対する本装置での扱いについて次に説明します。

(a) ウォッチドックパケット

ウォッチドックパケットは，サーバがクライアントの状態 (電源オフも含む) を確認するために周期的に送信するパケットです。本装置ではサーバが送信したウォッチドックパケットに対して，次に示す設定がインタフェースごとにできます。

- クライアントの代わりに「無条件代理応答する」(Proxy 設定)
- クライアントの代わりに「周期的に代理応答する」(Periodic 設定)

• クライアントの代わりの「代理応答しない」(Forward 設定)

ISDN 回線などの課金やトラフィックを考慮して，どの設定にするかを決定してください。

(b) シリアライゼーションパケットとダイアグノスティックパケット

これらのパケットについては「中継する」または「廃棄する」の設定となっています。それぞれについてインタフェースごとにスイッチがあり定義で設定できます。これらは特別なことがないかぎり中継は不要なので，課金やトラフィックを考慮して，デフォルトはどれも廃棄するように設定されています。

(c) NETBIOS パケット

本装置では，IPX でカプセル化された NETBIOS パケットは中継しないで受信時に廃棄されますので注意してください。

3.6.3 WAN または ATM 接続

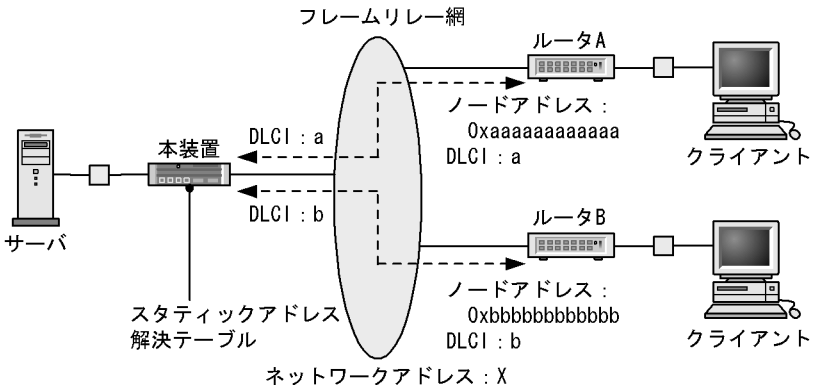
(1) フレームリレー網または ATM ネットワークへの接続

フレームリレー網または ATM ネットワークに接続する場合，該当するインタフェースの構成定義情報で次に示す項目を設定する必要があります。

• ノードアドレスの設定
• スタティックアドレス解決テーブルの設定
• ウォッチドッグ代理応答機能は，強制代理応答を推奨

フレームリレー網で IPX パケット中継を行うときに接続相手のノードアドレスと DLCI の対応を示すスタティックアドレス解決テーブルが必要です。したがって，接続相手装置はノードアドレスを任意に設定でき，送信先アドレスと DLCI の対応づけができる装置になります。なお，ATM ネットワークへの接続の場合はこの説明中の DLCI を VC と読み替えてください。フレームリレー網への接続例を次の図に示します。

図 3-11 フレームリレー網への接続例



ネットワークアドレス＋ノードアドレス	DLCI
X ＋ 0xaaaaaaaaaaaa	a
X ＋ 0xbbbbbbbbbbbb	b

(a) フレームタイプの設定

NetWare サーバ／クライアント，本装置で設定するフレームタイプを合わせてください。Windows 95 な

どでは IPX フレームタイプに "AUTO" という設定があります。この場合，クライアントは 4 種類のフレームタイプで順に要求を出し，応答が来たフレームで動作するというものです。本装置にはこのようなタイプの設定はありませんが，一つのポートに 4 種類のフレームタイプを設定しておくことができます。

(2) Group 化されたインタフェース

複数 VC または DLCI を Group 化したインタフェースに IPX インタフェースを設定した場合，周期 RIP/SAP は配下の全 VC，または DLCI にブロードキャストされます。既存の Group インタフェースに IPX インタフェースを追加するような場合，Group 配下に ip 以外は使用しない VC または DLCI が存在すると，むだなトラフィックを流すことになるので注意してください。

むだなトラフィック流出を防ぐためには，ipx を使用する VC または DLCI と，ip だけを使用する VC または DLCI に Group を分割し，別々にインタフェースを設定することをお勧めします。さらに，ブリッジが混在した場合も同様です。

(3) ISDN 接続

- ブロード型の ISDN 接続では RIP/SAP のブロードキャストができないため，スタティックで RIP/SAP を定義し，RIP/SAP のブロードキャストを停止して運用してください。
- ISDN バックアップを行う場合，バックアップ元とバックアップ先に同じ IPX アドレスを定義しておくことができます。

(4) その他

SAP，RIP をダイナミックで使用する場合，対応装置間の送信周期を同じ値で運用してください。

4 ブリッジ

この章ではブリッジ機能について説明します。

4.1 **サポート仕様**

4.2 **トランスペアレント・ブリッジ**

4.3 **スパニングツリー・アルゴリズム**

4.4 **トランスレーション**

4.5 **ブリッジ機能**

4.6 **ネットワーク設計の考え方**

4.1 サポート仕様

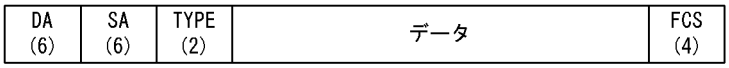
本装置は IEEE 802.1 で規定されるトランスペアレント・ブリッジとしての中継動作を行います。なお，IEEE 802.1 規格ではイーサネット間のブリッジ接続だけを示しており，WAN または ATM を介したブリッジ接続（リモート・ブリッジ）は扱っていません。しかし，本装置では WAN（専用線）または ATM についてもブリッジ接続を適用しています。WAN を介したブリッジ接続はブリッジ用 PPP によって，また，ATM を介したブリッジ接続はブリッジ用 LLC カプセル化 (RFC1483) によって行います。

4.1.1 フレーム・フォーマット

本装置がサポートするフレーム・フォーマットを次の図に示します。

図 4-1 本装置がサポートするフレーム・フォーマット

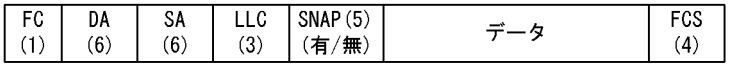
●イーサネット型（イーサネットおよびギガビット・イーサネット）



●IEEE802.3型（イーサネットおよびギガビット・イーサネット）

SNAPはOUI(3)とPID(2)から構成される。

●FDDI型



SNAPはOUI(3)とPID(2)から構成される。

（ ）内の数字はバイト数を示す。

なお，WAN および ATM フレームの場合，カプセル化ヘッダを外したフレーム・フォーマットもこの図と同じです。本装置は FDDI に接続するインタフェースを持ちませんが，WAN または ATM を介したカプセル化された FDDI 型フレームを扱うことはできます。

4.1.2 インタフェース

本装置はブリッジだけのインタフェースを定義できません。常に IP インタフェース（rmEthernet，AUX，トンネル，vlan を除く）に付ける形態となり，IP パケット以外をブリッジ中継します。なお，ブリッジは上位プロトコルを意識しないため，中継が不要なパケットを中継する場合があります。ネットワーク全体の負荷が増大する欠点がありますので，できる限りルータ機能を利用してください。

4.2 トランスペアレント・ブリッジ

トランスペアレント・ブリッジは MAC 副層によって中継を行う中継装置です。WAN および ATM 接続の場合はイーサネットフレームをカプセル化し中継します。トランスペアレント・ブリッジによってエンドシステム (ES) は，ほかのすべての ES が同一イーサネット上に存在するように見えます。また，トランスペアレント・ブリッジは FDDI やイーサネットなどの異種メディア間のフレーム・フォーマット変換 (トランスレーション) も行うため，ES は通信相手 ES の接続するメディアの違いを意識する必要がありません。この結果，ES から見て通信相手 ES は MAC アドレスで認識するだけでよいのでネットワークを意識する必要がありません。

本装置のトランスペアレント・ブリッジは次に示す三つの機能を持っています。

- ES の MAC アドレスを学習してフィルタリング・データベース (FDB) に登録する機能と，これに基づいたフレームのフィルタリング
- スパニングツリー・アルゴリズムに基づいた論理的木構造 (スパニングツリー) の生成
- 異種メディア間のフレーム・フォーマット変換 (トランスレーション)

トランスペアレント・ブリッジはフレームを受信すると，送信元 MAC アドレス (SA) をフィルタリング・データベース (FDB) と呼ばれるテーブルに登録します。FDB の各エントリには，MAC アドレスとフレームを受信したポートおよび監視時刻 (エイジングタイマ値) が記録されます。フレームを受信するごとに送信元 MAC アドレスに対応する FDB のエントリが更新されます。

トランスペアレント・ブリッジは，FDB のエントリに従ってフレームのフィルタリングを行います。フレームを受信するとブリッジは宛先 MAC アドレス (DA) と FDB 内の MAC アドレスを比較します。一致するエントリがないとフレームを受信したインタフェース以外のすべてのインタフェースにフレーム中継を行います。これを**フラッディング**といいます。

宛先 MAC アドレスに一致するエントリが FDB にあると，ブリッジはフレームを受信したインタフェースと FDB のエントリのインタフェースを比較します。インタフェースが同一であれば送信元 ES と宛先 ES が同一イーサネット上に存在していることになります。この場合フレーム中継は不要であるため，ブリッジはフレームを廃棄 (フィルタリング) します。インタフェースが異なっていれば，FDB のエントリに示されたインタフェースへフレームを中継します。それ以外のインタフェースへはフレーム中継は行われません (フィルタリングされます)。

本装置はスパニングツリー・アルゴリズムによって冗長的にブリッジ接続されたイーサネット /WAN 上のほかのブリッジと連携して論理的木構造を形成します。このアルゴリズムによって，任意の二つの ES 間で単一の経路を決定でき，フレームのループ周回を防ぐことができます。スパニングツリー・アルゴリズムはブリッジ間で BPDU と呼ばれる特別なフレームとやり取りすることで行われます。

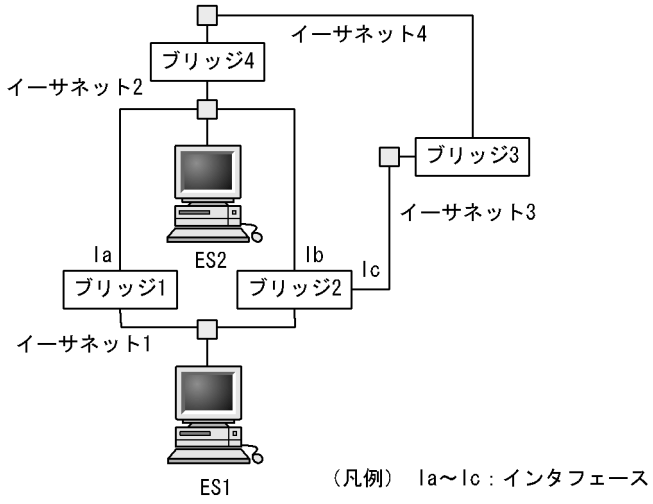
4.3 スパニングツリー・アルゴリズム

本装置の MAC ブリッジ機能は IEEE 802.1 の規格に基づいて実装されています。この規格は複数のイーサネット間を相互に接続したブリッジ接続イーサネット環境で，同一のイーサネット間を複数のブリッジで結ぶ並列ブリッジ接続構成を許したものです。ただし，並列接続によるループ周回の問題を，トランスペアレント・ブリッジ・サービス自体が解決しているわけではありません。ブリッジの並列接続を実現するためには，スパニングツリー・アルゴリズムを使用することが前提になります。

なお，スパニングツリープロトコルを使用する場合は，ブリッジ接続を使用するすべてのルータまたはブリッジで同一規格 (IEEE 802.1) のスパニングツリープロトコルを使用してください。

並列ブリッジ・トポロジを次の図に示します。

図 4-2 並列ブリッジ・トポロジ



(1) フレームを最初に送信した場合の処理

イーサネット 1 とイーサネット 2 は，二つの並列ブリッジ (ブリッジ 1 とブリッジ 2) で接続されています。イーサネット 1 の ES1 が，イーサネット 2 の ES2 にフレームを最初に送信した場合の処理を考えてみます。

1. ES1 によって送信され，ES2 宛てに送信されたフレームは，ブリッジ 1 とブリッジ 2 によって読み込まれます。これが ES1 と ES2 の間でやり取りされる最初のフレームであるため，どちらのブリッジのフィルタリング・データベース (FDB) にも ES1 または ES2 に対するエントリの登録はまだ行われていません。
2. 各ブリッジは ES1 がイーサネット 1 側の方向 (インタフェースで識別) にいるということを FDB に登録します。FDB を更新したあと，各ブリッジはフレームをフラッディングします。つまり，ブリッジ 1 はフレームを Ia に送り，ブリッジ 2 もそのフレームを Ib に送ります。このとき，ブリッジ 2 はフレームを Ic にも送ります。
3. ES2 は ES1 から発信されたフレームの二つのコピーを受け取ります。

(2) 重複フレームの受信

重複フレームの受信は ES では重大な問題にはなりません。また，転送効率もほとんど影響はありません。ただし，重複フレームをブリッジ 1 とブリッジ 2 で受け取ると問題が発生します。ブリッジ 1 によって Ia にフラッディングされたフレームは，Ib のブリッジ 2 によって受信されます。ブリッジ 2 はこのフレーム

を受信したときに，ES1 がイーサネット 2 側の方向にいるということを FDB に登録します。同様にブリッジ 1 はブリッジ 2 よりフラッディングされたフレームを受信したときに，ES1 がイーサネット 2 側の方向にいるということを FDB に登録します。その結果，両方のブリッジの FDB が矛盾してしまい，どちらのブリッジもフレームを ES1 に正しく転送できなくなってしまいます。この矛盾は，ES 間に代替の経路があるために生じます。このような現象のことを一般にループ周回といいます。スパニングツリー・アルゴリズムを使うことで，並列ブリッジを含むネットワークでループ周回を起さない構成が実現できます。

(3) スパニングツリー・トポロジの決定

このアルゴリズムによって，ブリッジ接続イーサネット内にある二つの ES 間でブリッジと中継のイーサネットから成る単一の経路を確保できます。また，ブリッジや伝送路に障害が発生してもスパニングツリー・アルゴリズムが自動的に再起動されるため，システムの構成の冗長性は広がります。スパニングツリー・トポロジは次のパラメータによって決定されます。

- 各ブリッジを識別するためのブリッジ ID。ブリッジ ID の一部はプライオリティ部として設定できます。
- 各インタフェースを識別するためのポート ID。ポート ID の一部はプライオリティ部として設定できます。
- 各インタフェースに対するコスト

これらのパラメータに従ってブリッジが BPDU のやり取りを行うことで，ブリッジ接続イーサネット内に論理的木構造が構築されます。

(4) 論理的木構造の構築

論理的木構造の構築を行うときには，まず**ルート・ブリッジ**というブリッジ接続イーサネット内で優先度が最も高い (値が最も小さい) ブリッジを決定する必要があります。このブリッジを中心に，論理的木構造が構築されていくことになります。

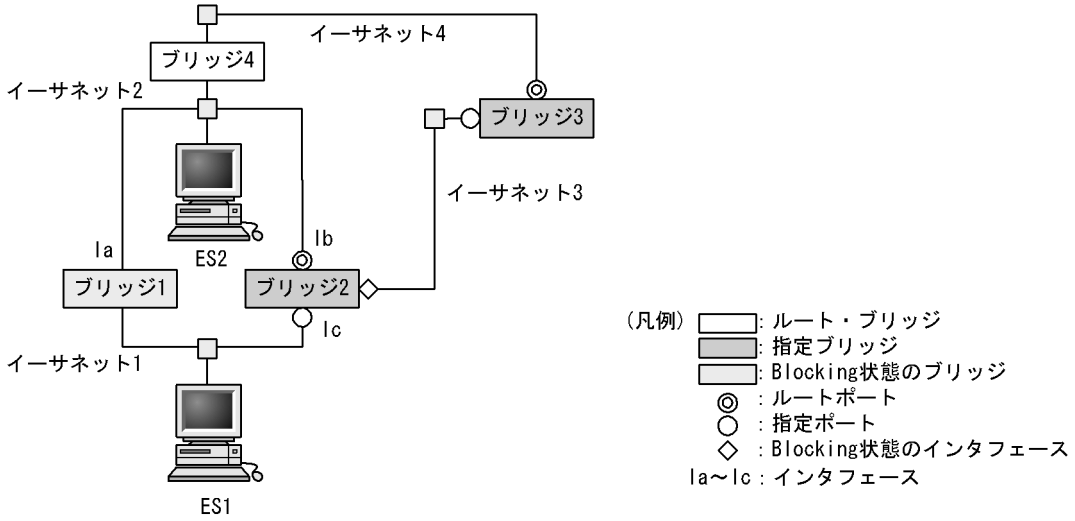
ルート・ブリッジが決まると，ほかのすべてのブリッジは経路コストを計算します。このコストは，各ブリッジ・インタフェースからルート・ブリッジまでの経路コストです。各ブリッジは，ルート・ブリッジまでの経路コストが最小であるインタフェースをルート・ポートとして指定します。経路コストが同じである場合，ブリッジは優先度が最も高い (値が最も小さい) ポートをルート・ポートとして指定します。

ブリッジ接続イーサネット内の各イーサネットでは，一つのブリッジが**指定ブリッジ** (Designated Bridge) として選択されます。このブリッジはルート・ブリッジまでの経路コストが最小であるルート・ポートを持っている必要があります。また，イーサネットを指定ブリッジに接続するインタフェースが**指定ポート** (Designated Port) として選択されます。このインタフェースはブリッジ接続イーサネット内でトラフィックの送信／受信を行い，Fowarding 状態にあるとみなされます。

これらのプロセスによって，並列接続を行うすべての冗長となるインタフェースがサービスから除外され，Blocking 状態になります。トポロジに変更が生じたり，ブリッジまたは伝送路に障害が発生したりすると，再度新しいスパニングツリーが構築され，Blocking 状態にあるインタフェースの一部を Fowarding 状態に戻します。

スパニングツリーの論理トポロジを次の図に示します。

図 4-3　スパニングツリーの論理トポロジ



この図では，スパニングツリー・アルゴリズムによってブリッジ 1 をサービスから除外し，ブリッジ 2 の Ic を Blocking 状態にできます。この図では論理的木構造の構築によって，ES 間で単一の経路となるスパニングツリーの論理トポロジを示しています。

4.4 トランスレーション

4.4.1 トランスレーション適用構成

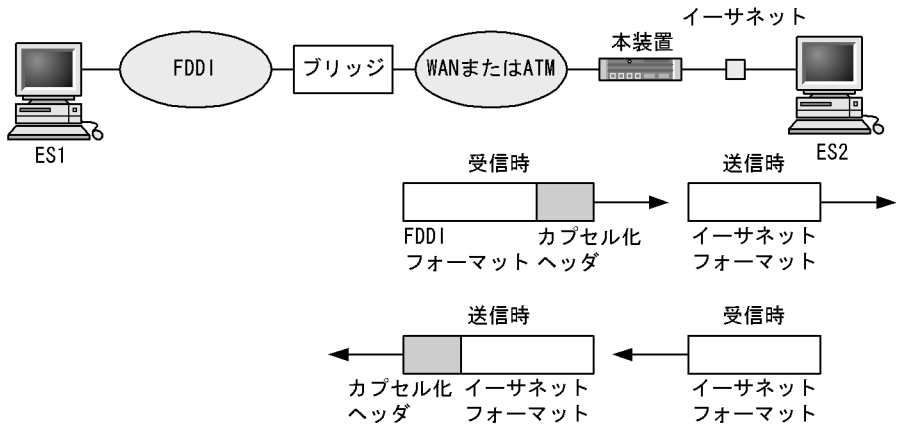
WAN または ATM を介したブリッジ接続では，一般にイーサネットから受信したフレームを WAN または ATM に中継する場合に，イーサネット上のフレームをカプセル化して送信します。また，WAN または ATM から受信したフレームはカプセル化ヘッダをはずし，さらに中継先のイーサネットメディアに合ったフレーム・フォーマットにトランスレーションして送信します。

本装置は FDDI に接続するインタフェースを持ちませんが，FDDI のフレームをイーサネットのフレームに変換するトランスレーション機能をサポートしています。これによって，WAN や ATM を介して FDDI に接続するネットワーク構成の場合にもブリッジ中継できます。

(1) WAN または ATM を介して FDDI に接続

WAN または ATM を介して FDDI に接続する場合のトランスレーションを次の図に示します。

図 4-4 WAN または ATM を介して FDDI に接続する場合のトランスレーション



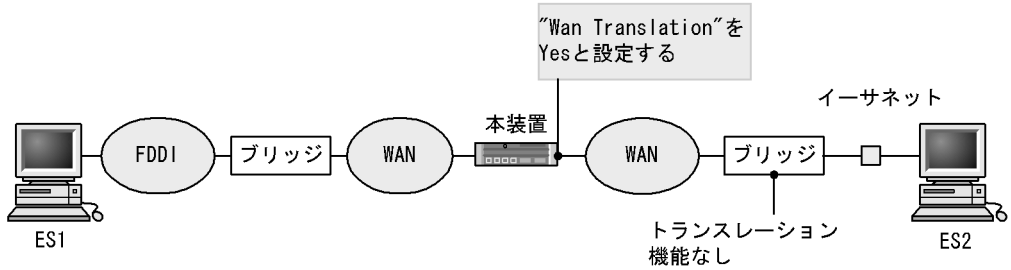
なお，この図の構成で WAN または ATM を介して本装置と接続するブリッジは，本装置と同等の機能を持つトランスペアレント・ブリッジである必要があります。

(2) トランスレーションをサポートしないブリッジとのリモート接続

本装置では WAN および ATM インタフェースで，フレームのトランスレーションを行う独自の機能をサポートしており，トランスレーションをサポートしないブリッジとのリモート接続もできます。

トランスレーションをサポートしないブリッジとのリモート接続を次の図に示します。

図 4-5 トランスレーションをサポートしないブリッジとのリモート接続

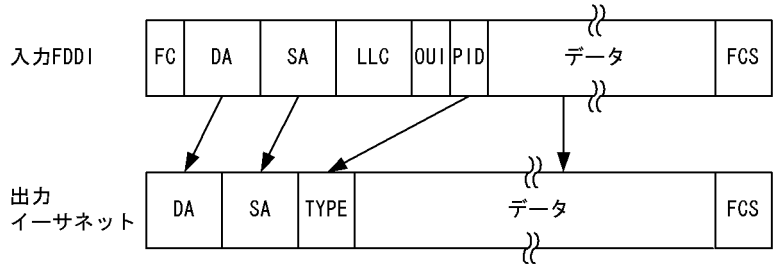


一般的にこの図のようなネットワーク構成で，イーサネットに接続されたブリッジが FDDI からイーサネットフォーマットへのトランスレーション機能を持たない場合，ES1 と ES2 間の通信ができません。この場合，本装置ではイーサネット側の WAN インタフェースの構成定義情報を設定することで，FDDI からイーサネットフォーマットへのトランスレーションを行ったあとに送信でき，ES1 と ES2 間の通信ができるようになります。

4.4.2 フレーム・フォーマットのトランスレーション

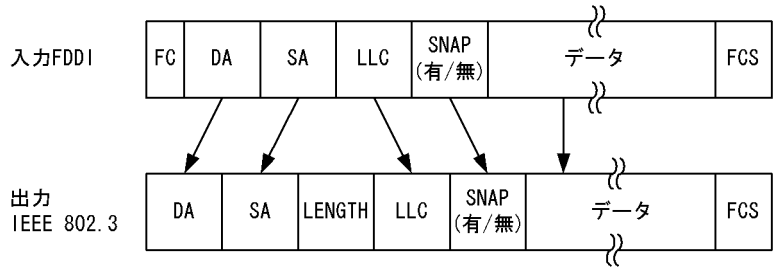
本装置は異なるメディア間のフレーム・フォーマット変換 (トランスレーション) を行います。FDDI → イーサネットのトランスレーションを「図 4-6　トランスレーション (FDDI →イーサネット)」に，FDDI → IEEE802.3 のトランスレーションを「図 4-7　トランスレーション (FDDI → IEEE802.3)」に示します。

図 4-6　トランスレーション (FDDI →イーサネット)



注　FDDIのFC情報は失われる。

図 4-7　トランスレーション (FDDI → IEEE802.3)



注　FDDIのFC，LLC情報は失われる。
　　LENGTH値は本装置が生成する。

FDDI 上のフレームをイーサネットに送信するときのトランスレーション条件を次の表に示します。

表 4-1　FDDI 上のフレームをイーサネットに送信するときのトランスレーション条件

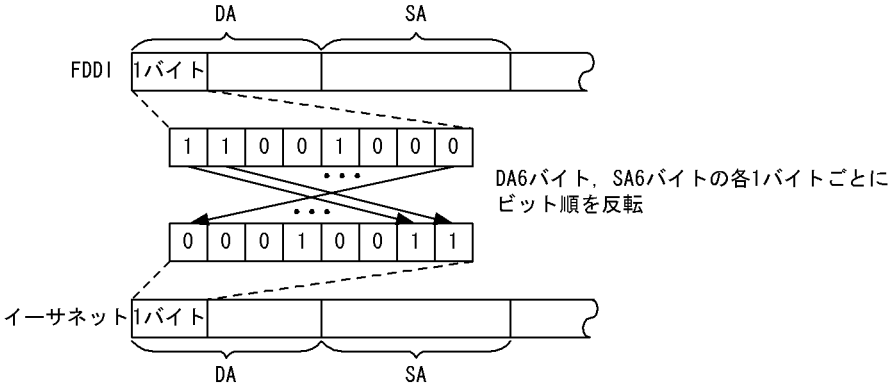
受信 FDDI フレーム			イーサネット上に送信するフレームフォーマット
DSAP/SSAP	OUI	PID	
0xaa	0x000000	0x80f3	802.3 型
		0x80f3 以外	イーサネット型
	0x0000f8	0x80f3	イーサネット型
		0x80f3 以外	イーサネット型
	その他	—	802.3 型
その他	—	—	802.3 型

（凡例） －：該当しない

4.4.3 MAC アドレスのビット順序反転

FDDI とイーサネットでは伝送路上にフレームを送信するときのビット順序が異なります。FDDI では各オクテットの最上位ビットから送信し，イーサネットではフレームの各オクテットの最下位ビットから送信します。この結果 FDDI とイーサネットとでは MAC アドレスのビット順序が異なるため，本装置は FDDI とイーサネット間のトランスレーションの場合，MAC アドレスのビット順序反転を行います。MAC アドレスのビット順序反転を次の図に示します。

図 4-8 MAC アドレスのビット順序反転



4.5 ブリッジ機能

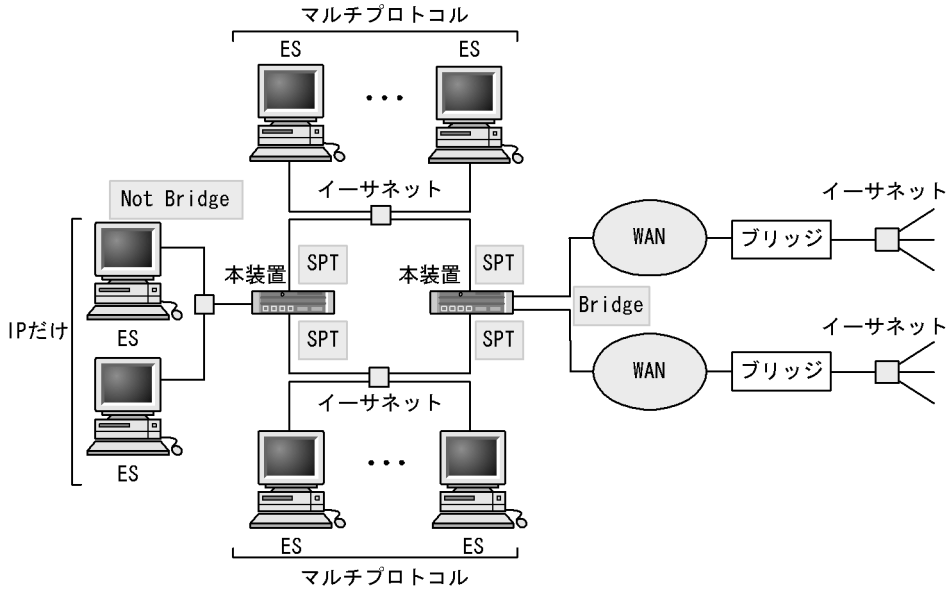
4.5.1 インタフェースのブリッジ動作モード

本装置はインタフェースごとにブリッジ機能を有効にするか無効にするか，スパニングツリー・アルゴリズムを実行するか実行しないかを指定できます。各インタフェースのブリッジ動作モードには次の 3 種類があります。

- SPT
  スパニングツリー・アルゴリズムを実行し，ブリッジ中継を行うインタフェース
- Bridge
  スパニングツリー・アルゴリズムは実行しないが，ブリッジ中継を行うインタフェース
- Not Bridge
  まったくブリッジとして動作しないインタフェース

これらのブリッジ動作モードはインタフェースごとに独立して設定できます。ブリッジインタフェースの動作モード設定例を次の図に示します。

図 4-9 ブリッジインタフェースの動作モード設定例



この図では，イーサネット側は並列ブリッジ接続としスパニングツリー・アルゴリズムを実行してネットワーク障害に対処します。WAN 側で並列ブリッジ接続がないネットワーク構成では，スパニングツリー・アルゴリズムを実行しません。これによって余分な BPDU が WAN 上に送信されません。また，IP フレームだけを流してほかの上位プロトコルのフレームを流したくないネットワーク側はブリッジインタフェースを定義しないか，または「Not Bridge」(デフォルトは Not Bridge) を設定しておけば，このインタフェースで IP ルーティングだけを行います。

4.5.2 スパニングツリー・トポロジ管理

(1) スパニングツリー・トポロジの変更

構成定義情報をデフォルトに設定してスパニングツリー・アルゴリズムを実行してもブリッジ接続された

イーサネット /WAN に論理的木構造 (スパニングツリー) は構築されます。しかし，意図的にあるトポロジにしたい場合には次の三つのパラメータによって調整できます。

1. ブリッジ・プライオリティ
   どのブリッジがルート・ブリッジになるかを決定するパラメータです。ブリッジ・プライオリティの値が最も小さいブリッジがルート・ブリッジになります。
2. 各ポートに対するコスト
   各ポートからルート・ブリッジまでの経路コストを計算するためのパラメータです。ルート・ブリッジまでの経路コストが最小であるポートがルート・ポートになります。
3. ポート・プライオリティ
   ルート・ブリッジまでの経路コストが同一の場合，ポート・プライオリティの値が小さいインタフェースがルート・ポートになります。

これらのパラメータは本装置のリスタートなしで変更できます。ただし，すべての ES 間の通信は一時中断しますので注意してください。

(2) スパニングツリー・インタフェースのイネーブル／ディスエーブル

スパニングツリー・アルゴリズムを実行しているポートについて，ブリッジ中継動作をイネーブルまたはディスエーブルできます。

このパラメータは本装置のリスタートなしで変更できます。ただし，すべての ES 間の通信は一時中断しますので注意してください。

(3) スパニングツリー情報の表示

show spanning-tree コマンドによって現在のスパニングツリー・トポロジを表示できます。なお，スパニングツリー・アルゴリズムは分散処理アルゴリズムであるため，このコマンドで表示されるのは該当する装置の情報だけです。ネットワーク全体のスパニングツリー・トポロジはほかのブリッジの情報と合わせて見てください。このコマンドの実行は，スパニングツリー・アルゴリズムの実行または ES 間の通信には影響ありません。

(4) スパニングツリーの初期化

restart bridge コマンドの入力によって，スパニングツリー・トポロジを再計算します。通常このコマンドを使用する必要はありません。しかし，何らかの原因でネットワーク上のほかのブリッジとの間でスパニングツリー・トポロジの矛盾が生じた場合などに使用できます。このコマンドを使用すれば，本装置のリスタートなしでスパニングツリー・トポロジを再計算できます。ただし，このコマンドの実行によって ES 間の通信は一時中断しますので注意してください。

(5) タイマ値

スパニングツリープロトコルを使用する場合は，ブリッジ接続するすべてのルータおよびブリッジで同一の規格 (IEEE802.1) のスパニングツリープロトコルを使用してください。また，本装置のスパニングツリーに使用するタイマ値は，デフォルトでは通常のブリッジ装置より早めに動作するように設定されています。本装置以外のブリッジ装置と混在させたネットワークで運用する場合，他装置との関係で不都合があれば spanningtree 構成定義でタイマ値を調整してください。スパニングツリーに使用するタイマ値を次の表に示します。

表 4-2　スパニングツリーに使用するタイマ値

タイマー種別	本装置のデフォルト値	通常のデフォルト値
Max age time	18	20
Forward delay time	10	15

4.5.3 フィルタリング

「4.2 トランスペアレント・ブリッジ」で示したようにブリッジ中継されるフレームは FDB によってフィルタリングされ，余分なトラフィックがネットワーク上を流れないようになっています。MAC アドレスは受信したフレームからの学習によって FDB に登録されます。この学習によって登録されたエントリをダイナミック・エントリと呼びます。また，構成定義情報としてあらかじめ設定しておくこともできます。構成定義情報によるエントリをスタティック・エントリと呼びます。ダイナミック・エントリはエイジアウト対象であり，構成定義情報で設定したエージングタイマ値（デフォルト 300 秒）を過ぎてもその MAC アドレスのエントリ更新がないと無効になります。

FDB の最大エントリ数は 2000 です。その中で最大 500 エントリまでスタティック・エントリとして設定できます。残りがダイナミック・エントリの登録エリアになります。なお，この FDB はインタフェースごとの指定ではなく，本装置の全インタフェースの指定になります。

次に，構成定義情報としてスタティック・エントリを設定する例を示します。FDB によるフィルタリングは MAC アドレスをキーとしたものなので，それ以外の複雑なフィルタリングの設定を行いたい場合には，拡張フィルタリングを使用してください。

（1） フィルタリング Action が Forward の適用例

特定の MAC アドレスを持つ ES が接続されるインタフェースがあらかじめわかっている場合には，その MAC アドレスをスタティック・エントリとして登録しておき，フィルタリング Action を Forward に設定します。スタティック・エントリはエイジアウトしないので，フラッディングによって余分なフレームがネットワーク上を流れるのを防止できます。ただし，並列ブリッジ接続してスパニングツリー・アルゴリズムを実行している場合には，スパニングツリー・トポロジの変化で ES が接続されるインタフェースが交替する場合もあるので，設定時に十分に注意してください。

（2） フィルタリング Action が Drop の適用例

セキュリティなどの目的から，既知のいくつかの MAC アドレスを持つ ES 発／宛てのフレームをブリッジ中継させない場合，またはブロードキャスト・アドレスや特定のマルチキャスト・アドレスのフレームをブリッジ中継したくない場合などには，それらの MAC アドレスをスタティック・エントリとして登録しておき，フィルタリング Action を Drop に設定します。これによって，本装置が受信したフレームで宛先 MAC アドレスまたは送信元 MAC アドレスが FDB の該当するスタティック・エントリの MAC アドレスと一致する場合，ブリッジ中継しないで廃棄（フィルタリング）されます。

（3） ダイナミック・エントリの制限事項

FDB は中継性能を向上させるため，MAC アドレスに対応する FDB のエントリ位置をある範囲に限定して処理しています。つまりあるダイナミック・エントリのエイジングがエージングタイマ値以下であっても，新しく学習フレームが該当する FDB エントリ範囲（MAC アドレスによって計算されたある範囲）に空きがない場合は，既存のダイナミック・エントリを無効にして新しくダイナミック・エントリを登録することがあります。

したがって，FDB は n 個の異なるフレームを学習しても必ずしも n 個のダイナミック・エントリが作成されない場合があるので注意してください。

また，FDB はスタティック・エントリとダイナミック・エントリを合わせて最大 2000 エントリですが，スタティック・エントリが 0 の場合はダイナミック・エントリは最大 1950 エントリになります。また，スタティック・エントリが 500 の場合，ダイナミック・エントリの最大は 1450 ～ 1500 の範囲になります。

4.5.4 拡張フィルタリング

本装置では，ブリッジ中継対象フレームの MAC ヘッダの各フィールドまたは MAC ヘッダの先頭からフレーム中の任意フィールドの値が指定したパターンと一致するかを調べてフィルタリングできます。これをすでに説明した FDB によるフィルタリングと区別するために**拡張フィルタリング**と呼びます。

(1) 拡張フィルタリングの比較項目

拡張フィルタリングでは，次に示すフレームのフィールドを指定できます。

- DA　：宛先 MAC アドレス (6 バイト)
- SA　：送信元 MAC アドレス (6 バイト)
- DSAP：宛先 SAP(サービスアクセスポイント)(1 バイト)
- SSAP：送信元 SAP(サービスアクセスポイント)(1 バイト)
- CTL　：コントロールフィールド (1 バイト)
- OUI　：組織コード (3 バイト)
- PID　：プロトコル ID(2 バイト)
- TYPE：イーサネットタイプ (2 バイト)
- ユーザ定義の任意フィールド指定：
  フレームの宛先 MAC アドレスの先頭をゼロとしたオフセット値 m
  (バイト数) から n バイトのフィールド
  (m：0 ～ 54，n：1 ～ 6)

これらの指定方法はいろいろな上位プロトコルについて柔軟なフィルタリングを行うことを想定しています。各比較項目は比較値とマスクの組み合わせで指定します。フレームの指定されたフィールドの値とマスクのビット AND をとったあとに比較値と一致するかを調べます。

拡張フィルタリングの 1 エントリで最大三つの比較項目を設定できます。すべての比較項目が一致した場合に，そのエントリの拡張フィルタリングの条件が一致したとみなします。

(2) 拡張フィルタリング指定対象

全インタフェースを指定すると，すべてのインタフェースで受信時または送信時にフレームが条件に一致するかを調べます。

特定インタフェースを指定すると，指定したインタフェースで，受信時または送信時にフレームが条件に一致するかを調べます。

(3) 条件一致時の動作

Forward を指定するとそのフレームを中継します。Drop を指定すると，そのフレームを廃棄します。

拡張フィルタリングの最大エントリ数は 200 です。各エントリは先にあるエントリから順に調べられ，条件が一致するエントリがあるとそれ以後のエントリは無視されます。最後のエントリまで調べて条件に一致するものがない場合に，そのフレームは中継されます。

(4) 拡張フィルタリングの設定例

拡張フィルタリングの設定例を次の表に示します。この例では次のフィルタリング条件を設定しています。

1. 全インタフェースで，送信元 MAC アドレスがローカルアドレスであるフレームを廃棄する (Entry No.1)。
2. interface1 では宛先 MAC アドレスがマルチキャスト・アドレスで，宛先／送信元 SAP が特定の値であるフレームを廃棄し，それ以外のフレームをブリッジ中継する (Entry No.2)。

3. interface2 では特定 DA を持つフレームだけをブリッジ中継し，それ以外のフレームを廃棄する (Entry No.3，4，5)。

表 4-3 拡張フィルタリングの設定例

構成定義情報の設定項目							意味
Entry No.	Interface	Action	Item No.	Type	Value(16 進)	Mask(16 進)	
1	all	Drop	1	SA	400000000000	400000000000	SA がローカル・アドレス (U/L=1) のフレームを廃棄 (全インタフェース)
			2	OFF	—	—	
			3	OFF	—	—	
2	Interface1	Drop	1	DA	800000000000	800000000000	DA がマルチキャスト・アドレス (I/G=1) で，DSAP/SSAP が FE のフレームを廃棄 (特定インタフェース)
			2	DSAP	fe	ff	
			3	SSAP	fe	ff	
3	Interface2	Forward	1	DA	006097c010c7	ffffffffff	特定 DA のフレームをブリッジ中継 (特定インタフェース)
			2	OFF	—	—	
			3	OFF	—	—	
4	Interface2	Forward	1	DA	0000e2081390	ffffffffff	特定 DA のフレームをブリッジ中継 (特定インタフェース)
			2	OFF	—	—	
			3	OFF	—	—	
5	Interface2	Drop	1	TYPE	0000	0000	すべてのフレームを廃棄 (特定インタフェース)
			2	OFF	—	—	
			3	OFF	—	—	

(凡例) —：該当しない

特定のフレームだけを中継してそれ以外のフレームを廃棄したい場合には，この表に示すように中継条件のエントリを先に設定し (Entry No.3，4)，最後に廃棄条件のエントリを設定する (Entry No.3，4，5) のが望ましい設定です。

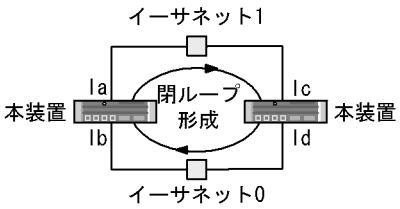
4.6 ネットワーク設計の考え方

4.6.1 禁止トポロジ

ブリッジ接続の場合，いくつか禁止トポロジがあります。ネットワーク構成が複雑になると禁止トポロジの判別が難しくなりますが，禁止トポロジは次に示す点を考慮して判断してください。

- 閉ループを形成していないこと
  ネットワークにループが形成されている場合，そのループ上のポートはすべてスパニングツリーを実行している必要があります。一つでもスパニングツリーを実行していないポートが存在すると閉ループを形成してしまいます。
- ルータと並列接続していないこと
  このような接続を行うとルータのネットワークアドレス定義でシステム矛盾が発生します。ネットワーク上にこのような構成がないか注意してください。閉ループの禁止トポロジの例を「図 4-10　閉ループ形成例 1」および「図 4-11　閉ループ形成例 2」に，ルータとの並列接続の禁止トポロジの例を「図 4-12　ルータとの並列接続例」に示します。

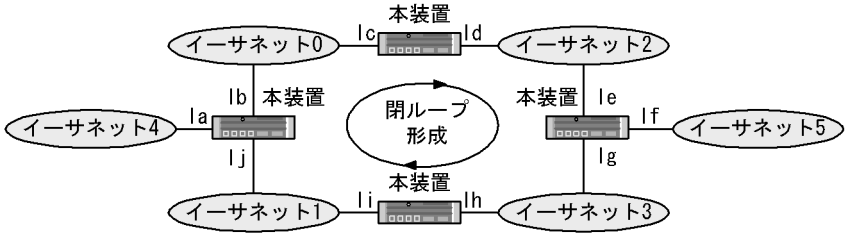
図 4-10　閉ループ形成例 1



禁止構成
インタフェースla～ld中で一つでもスパニングツリーを実行しないインタフェースがある場合

（凡例）　la～ld：インタフェース

図 4-11　閉ループ形成例 2

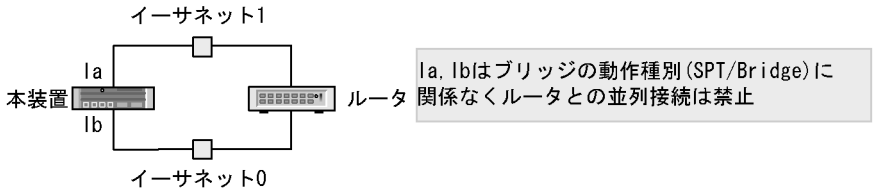


（凡例）　la～lj：インタフェース

禁止構成
インタフェースlb, lc, ld, le, lg, lh, li, ljの中で一つでもスパニングツリーを実行しないポートがある場合

禁止構成ではない
インタフェースla, lfはループを形成しないため，単純なブリッジ中継ポートで問題ない

図 4-12 ルータとの並列接続例



（凡例） la，lb：インタフェース

4.6.2 中継性能

(1) 中継性能

本装置は IP 中継処理に最適化しています。ブリッジ中継処理は IP 中継処理のように最適化を行っていません。ブリッジを使用するネットワークを構築する場合，ブリッジの中継性能は RP 当たり 3500 packet/s の中継性能を超えないように設計してください。また，IPX とブリッジを混在して使用する場合は，IPX とブリッジを合わせて RP 当たり 2500 packet/s の中継性能を超えないように設計してください。

また，QoS 機能については IPX 中継性能以内のトラフィックの場合には効果があります。しかし，それを超えたトラフィックの場合は内部でパケット廃棄が生じて，出力の優先制御が機能していないように見えることがあります。

(2) 過剰トラフィック発生時

過剰トラフィックおよび RM CPU 過負荷が継続して発生した場合，プロトコルデータの廃棄が発生します。スパニングツリーを実施している場合は BPDU のエージングアウトによって Blocking していたインタフェースが Forwarding されることがあるので注意してください。この現象が継続するような場合はトラフィックを考慮してネットワーク構成を再考してください。

4.6.3 HDLC パススルーと優先度制御

本装置では HDLC パススルーの WAN ポートを直接接続できませんが，MAC フレームでカプセル化された HDLC パススルーのフレームをブリッジ中継できます。

また，このとき WAN インタフェースの優先度制御は HDLC パススルーとほかのブリッジフレームを個々に設定できます。優先度は構成定義の HDLC QoS 情報，Bridge QoS 情報でそれぞれ設定でき，個々に遅延クラス，廃棄クラスをインタフェース単位に設定します。イーサネット，ATM インタフェースの場合は，Bridge QoS 情報で設定された値で一律に優先度制御します。

4.6.4 WAN または ATM 接続

(1) Cisco 社製ルータとの PPP 接続

Cisco 社製ルータと本装置を PPP 接続した回線上でブリッジを転送する場合，PPP 回線の MTU 長が 1516 バイトを超えるように Cisco 社製ルータの MTU 長を調整してください。

(2) フレームリレー網接続

(a) インタフェースの定義

フレームリレーでのブリッジインタフェースの設定は 1DLCI に IP インタフェースが定義されているとこ

ろにブリッジインタフェースが定義できます。

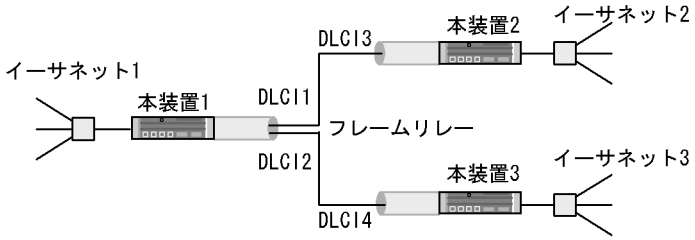
この場合，IP インタフェースは Point-To-Point 型およびブロード型のどちらかを設定できます。例えば，相手装置がブロード型だけをサポートしている場合は，1DLCI-1 インタフェースであってもブロード型で定義してください。

なお，タイムスロットやグループ化したインタフェースにブリッジインタフェースを定義できません。

(b) ネットワーク構成

フレームリレーでのブリッジ接続を次の図に示します。ブリッジのフレーム中継は，設定されたインタフェース間でフレームを中継します。

図 4-13 フレームリレーでのブリッジ接続



・DLCI1～4はすべて個々にIPインタフェースを付ける。
・本装置1でLAN1から受信したブリッジフレームはDLCI1,2に中継する。
またDLCI1から受信したブリッジフレームはDLCI2とLAN1に中継する。
・スパニングツリープロトコルも可能なので，フルメッシュ構成の場合などではインタフェースはSPTにする必要がある。

パーシャルメッシュやフルメッシュで構築されたネットワークで後からインタフェースにブリッジを設定する場合，複数 DLCI を 1 インタフェースとしている個所は 1DLCI ごとにインタフェースを分ける必要があります。逆にブリッジインタフェースを設定する予定の場合はあらかじめ 1DLCI-1 インタフェースのネットワークを構築するようにしてください。

(3) ATM 接続でのスパニングツリーの使用

ATM を使用してブリッジ接続をする場合，本装置は RFC1483 で規定されている BPDU フォーマットだけをサポートしています。本装置がサポートしている BPDU フレームフォーマットを次の図に示します。

図 4-14 本装置がサポートしている BPDU フレームフォーマット

LLC	OUI	PID	BPDU as defined by 802.1(d) or 802.1(g)

LLC : 0xaaaa03
OUI : 0x0080c2
PID : 0x000e

このフォーマット以外で BPDU を送受信動作する装置との接続では，該当する接続ポートはそれぞれの装置でスパニングツリーを動作させないので，明示的にループ構成にならないようにシステムを構成して運用してください。

規格外のフォーマット (PID に 0x00-01 や 0x00-07 を設定し MAC ヘッダを付随しているもの) を使用している装置と ATM ブリッジ接続した場合は，正しくスパンニングツリーデータをやり取りできないので注意してください。

(4) Group 化されたインタフェース

複数 VC を Group 化したインタフェースにブリッジインタフェースを設定した場合，BPDU または学習されていない中継フレームは配下の全 VC にブロードキャストされます。既存の Group インタフェースにブリッジインタフェースを追加するような場合，もし Group 配下に ip 以外は使用しない VC が存在するとむだなトラフィックを流すことになるので注意してください。

むだなトラフィック流出を防ぐためには，ブリッジを使用する VC と，ip だけを使用する VC に Group を分割し，別々にインタフェースを設定することをお勧めします。さらに，ipx が混在した場合も同様です。

(5) ISDN 接続

ISDN インタフェースへのブリッジ設定は，1Peer に IP インタフェースが定義されている個所だけにブリッジインタフェースを設定できます。この場合，IP インタフェースはポイントーポイント型になります。なお，Peer をグループ化したインタフェースにブリッジインタフェースは定義できません。

また，ISDN インタフェース上ではスパニングツリーを動作させることはできないので，インタフェースは yes または no のどちらかを設定できます。ネットワーク構築する場合は，明示的にループ構成とならないように注意してください。

5 VRRP

VRRP(Virtual Router Redundancy Protocol) はルータに障害が発生した場合でも，同一イーサネット上の別ルータを経由してエンドホストの通信経路を確保することを目的としたホットスタンバイ機能です。この章では VRRP の機能について説明します。

5.1　VRRP 概説

5.2　仮想ルータの MAC アドレスと IP アドレス

5.3　障害監視インタフェース

5.4　VRRP ポーリング

5.5　VRRP ポーリングの障害検出の仕組み

5.6　障害検出の仕組み

5.7　パケットの認証

5.8　マスタルータの選出方法

5.9　ネットワーク構成例

5.10　VRRP 使用時の注意事項

5.1 VRRP 概説

VRRP を使用すると，同一イーサネット上の複数のルータから構成される仮想的なルータを定義できます。デフォルトゲートウェイとしてこの仮想ルータを設定しておくことによって，ルータに障害が発生したときの別ルータへの切り替えを意識することなく，通信を継続できます。

(1) VRRP でサポートしている項目

VRRP でサポートしている項目を次の表に示します。

表 5-1 VRRP でサポートしている項目

項目		内容
対象インタフェース		イーサネット，VLAN
対象プロトコル		IPv4，IPv6
装置当たりの仮想ルータ最大数		255
インタフェース当たりの仮想ルータ最大数		255※1
仮想ルータ当たりの IP アドレス数		1
パケット認証方式	なし	○
	テキストパスワード	○
	IP 認証ヘッダ	－
優先度制御		○
自動切り戻し (Preempt Mode)		○ (on/off で設定する)
制御パケット送信間隔		1 ～ 255 秒の範囲で指定できる
装置切り替え時間		4 秒※2

(凡例) ○：サポートしている －：サポートしていない

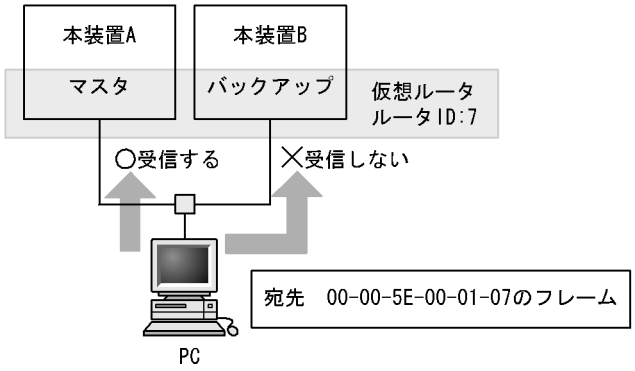
注※ 1 仮想ルータが使用する MAC アドレスは仮想ルータごとに自動的に割り当てられます。

注※ 2 制御パケットの送信間隔が 1 秒 (デフォルト) の場合の装置切り替え時間。装置の切り替え時間は (パケット送信間隔× 3 ＋ 1) 秒になります。エンド－エンド間の通信再開には，通信経路上のルータ装置で経路情報の再計算時間の設定が必要です。

5.2 仮想ルータの MAC アドレスと IP アドレス

仮想ルータは自身の物理的な MAC アドレスとは別に，仮想ルータ用の MAC アドレスを持ちます。仮想ルータの MAC アドレスは，00-00-5E-00-01-{仮想ルータの ID} に決められており，仮想ルータの ID から自動的に生成されます。マスタ状態のルータは仮想 MAC アドレス宛てのイーサネットフレームを受信してパケットをフォワーディングする能力を持ちますが，バックアップ状態のルータは仮想 MAC アドレス宛てのフレームを受信しません。VRRP は仮想ルータの状態に応じて仮想 MAC アドレス宛てイーサネットフレームを受信するかどうかを制御します。マスタ状態のルータは仮想 MAC 宛てフレームを受信すると，自ルーティングテーブルに従って IP パケットのフォワーディング処理を行います。仮想 MAC アドレス宛てフレームの受信を次の図に示します。

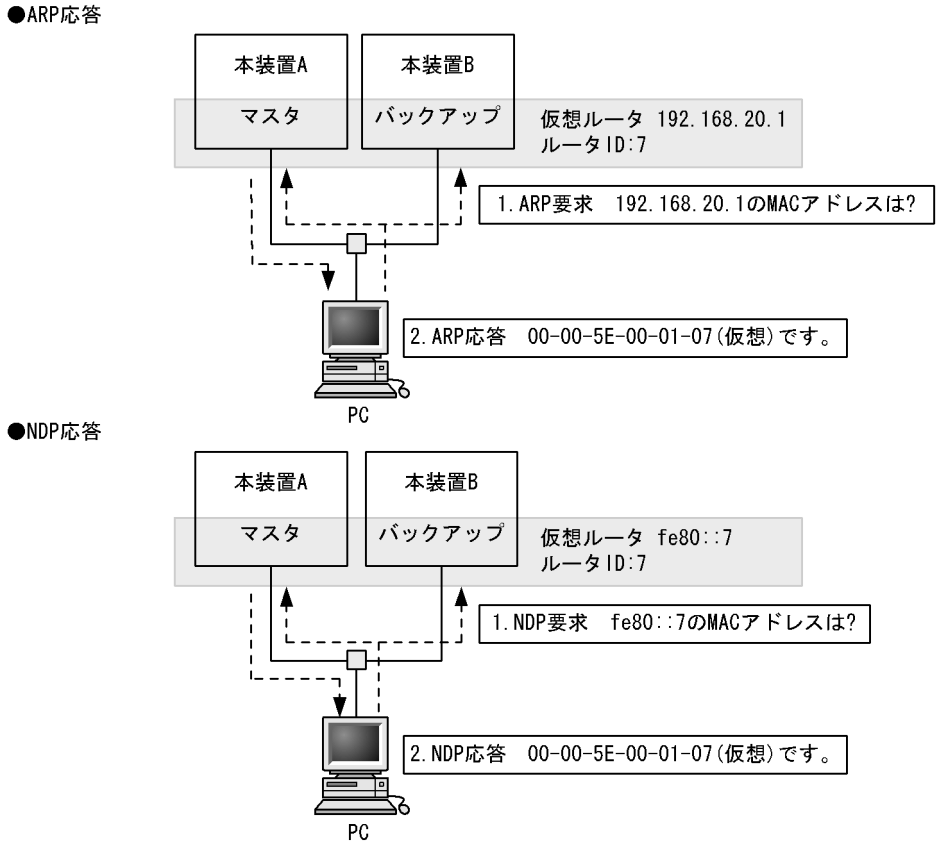
図 5-1　仮想 MAC 宛てフレームの受信



VRRP では仮想 MAC アドレス宛てフレームが切り替えの対象になります。マスタとバックアップが切り替わった後で通信を継続できるのは仮想 MAC アドレス宛てフレームに限定されます。「図 5-1　仮想 MAC 宛てフレームの受信」の場合，PC は仮想 MAC アドレスを宛先としてフレームの送出を行わなければなりません。

仮想ルータは仮想ルータの IP アドレスを持ちます。マスタ状態のルータは，仮想ルータの IP アドレスに対する ARP 要求パケットまたは NDP 要求パケットを受信すると，常に仮想ルータの MAC アドレスを使用して ARP 応答または NDP 応答します。仮想 MAC アドレスによる ARP 応答および NDP 応答を次の図に示します。

図 5-2　仮想 MAC アドレスによる ARP 応答および NDP 応答



仮想ルータをデフォルトルータとして使用する PC などのホストは，自 ARP キャッシュテーブル内に仮想ルータの IP アドレス宛てのフレームは仮想 MAC アドレス宛てに送出するように学習します。このように学習されたホストは常に仮想ルータへ送出するときに仮想 MAC アドレスを宛先に指定してフレームの送出を行うようになるため，VRRP のマスタ／バックアップの切り替えが発生した場合でも，通信を継続できます。

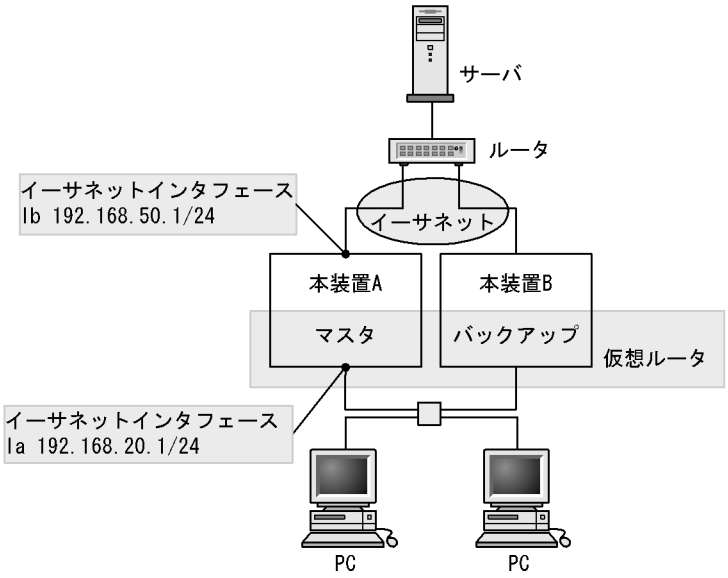
5.3 障害監視インタフェース

VRRP では仮想ルータを設定したインタフェースの障害時に，マスタルータを装置単位で切り替えます。しかし，仮想ルータが設定されていないそのほかのインタフェースに障害が発生した場合には切り替えません。本装置では独自の付加機能として他インタフェースを監視して，他インタフェースがダウンした場合に，仮想ルータの優先度を下げて運用する機能を使用できます。このインタフェースを障害監視インタフェースといいます。

障害監視インタフェースがダウンしたとき，仮想ルータの優先度の扱いは 2 通りあります。一つは , 障害監視インタフェースがダウンしたときに仮想ルータの優先度をあらかじめ設定しておいた優先度 (Critical Priority) に変更して運用します。もう一つは，障害監視インタフェースがダウンしたときにあらかじめ障害監視インタフェースに設定された，優先度減算値 (Down Priority) を仮想ルータの優先度から減算し運用します。前者の場合，障害監視インタフェースは一つしか設定できませんが，VRRP ポーリング機能を使用することができます。後者の場合，障害監視インタフェースを複数設定することができます。ただし，VRRP ポーリング機能は使用できません。

障害監視インタフェースを次の図に示します。

図 5-3　障害監視インタフェース



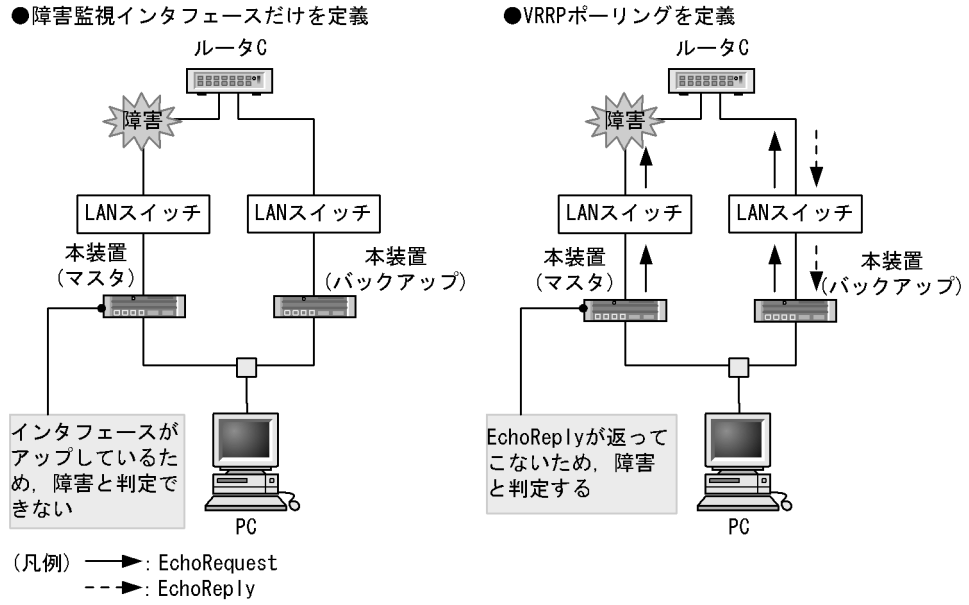
この図を例にして説明します。本装置 A には Ia というイーサネットインタフェースと Ib というイーサネットインタフェースの二つが定義されています。仮想ルータはインタフェース Ia に設定されています。通常の VRRP の動作ではイーサネット回線の障害によってインタフェース Ib がダウンしても，仮想ルータの動作には影響を与えません。しかし，本装置では障害監視インタフェース (Critical Interface) と障害監視インタフェースダウン時の優先度 (Critical Priority)，または優先度を下げる値 (Down Priority) を指定することによって，仮想ルータの動作状態を変更させることができます。

本装置 A の仮想ルータの障害監視インタフェースを Ib，そして障害監視インタフェースダウン時の優先度を 0 に設定した場合，インタフェース Ib のダウン時には自動的マスタが本装置 A から本装置 B へ切り替わります。

5.4 VRRP ポーリング

障害監視インタフェースでは，インタフェースのダウンで検出できるレベルの障害しか監視することができないため，ルータをまたいだ先の障害は検出できません。本装置では，障害監視インタフェースに対して VRRP **ポーリング**を使用することで，ルータをまたいだ先の障害でも検出できます。なお，VRRP ポーリングは障害インタフェースを複数設定した場合は使用できません。VRRP ポーリングを定義した場合と定義していない場合の比較を次の図に示します。

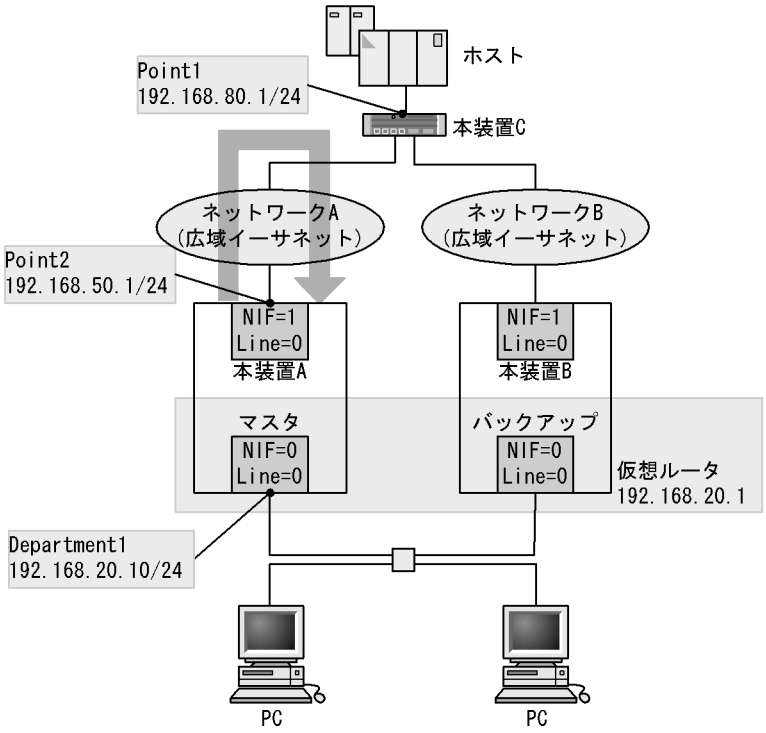
図 5-4 VRRP ポーリングを定義した場合と定義していない場合の比較



5.4.1 VRRP ポーリングの概要

VRRP ポーリングは，構成定義によって指定された IP アドレス宛てに ICMP Echo パケットによるポーリングを行い，疎通状態を監視します。ICMP Echo パケットは RFC 標準であるため，宛先 IP アドレスに指定する相手装置が本装置である必要はありません。ただし，ICMP Echo パケットに対して応答を返す必要があります。応答確認は ping コマンドを使用して行えます。応答がないため障害と判定した場合は，障害監視インタフェースと同様に仮想ルータの優先度を下げて運用します。VRRP ポーリングを次の図に示します。

図 5-5 VRRP ポーリング



「図 5-5 VRRP ポーリング」を例にして説明します。本装置 A には Department1 というイーサネットインタフェースと Point2 というイーサネットインタフェースの二つが定義されています。仮想ルータは Department1 に設定されています。通常の障害監視インタフェースでは，ネットワーク上で発生した障害は検出できません。しかし，本装置では宛先 IP アドレス (target address) を指定して VRRP ポーリングを有効にすることによって，ネットワーク上で発生した障害をすぐ検出できます。また，ホスト側の本装置 C は static ポーリングを使用し，経路切り替えを行います。static ポーリングについては，「解説書 Vol.1 10.3.1(3) スタティック経路の動的監視」を参照してください。

「図 5-5 VRRP ポーリング」の，本装置 A の仮想ルータの障害監視インタフェースを Point2，障害監視インタフェースダウン時の優先度を 0，ポーリングの宛先 IP アドレスをルータ 1 の Point1 の IP アドレス (192.168.80.1) に設定した場合，ネットワーク上で障害が発生し応答が返らなくなると，自動的にマスタが本装置 A から本装置 B へ切り替わります。なお，障害検出時間または障害回復検出時間は構成定義によって変更できます。

障害監視インタフェースがダウンした場合，VRRP ポーリングは疎通不可能状態と判断し，インタフェースがアップするまで待機します。障害監視インタフェースがアップした時，再度ポーリングを始め，障害復旧検証によって疎通可能状態と判定した場合，切り戻しを行います。

5.4.2 VRRP ポーリング使用時の注意事項

VRRP ポーリングの宛先 IP アドレスが，ルータをまたいだ先のネットワーク上にある場合は，各ルータのルーティングテーブルに依存します。このため，「図 5-6 送受信インタフェースが一致しない場合」のように VRRP ポーリングの応答を受信するインタフェースが VRRP ポーリングを送信したインタフェースと一致しない場合があります。この場合，受信インタフェースチェックオプション (構成定義パラメータの check-reply-interface) を指定することで，送信インタフェースと受信インタフェースをチェックできます。送信インタフェースと受信インタフェースが不一致の場合に該当するパケットを廃棄します。なお，

「図 5-7　自装置配下ではないネットワーク上のインタフェース不一致」のような自装置配下でないネットワーク上のインタフェースが不一致の場合は，保証しません。

図 5-6　送受信インタフェースが一致しない場合

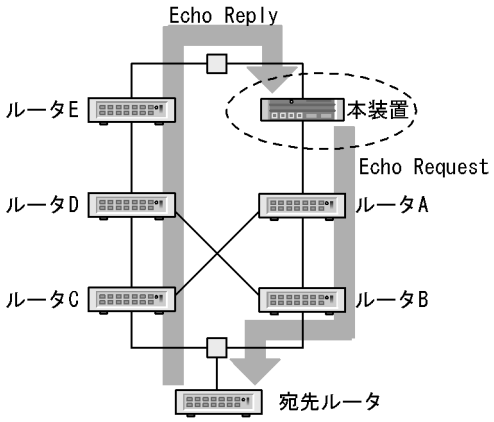
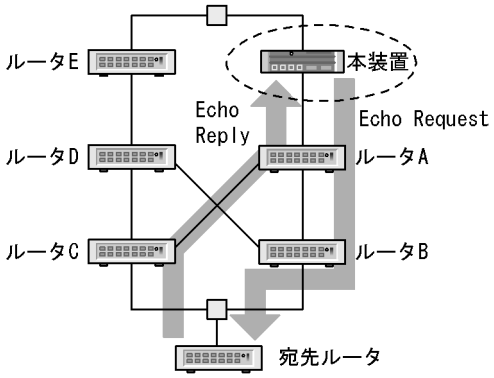


図 5-7　自装置配下ではないネットワーク上のインタフェース不一致

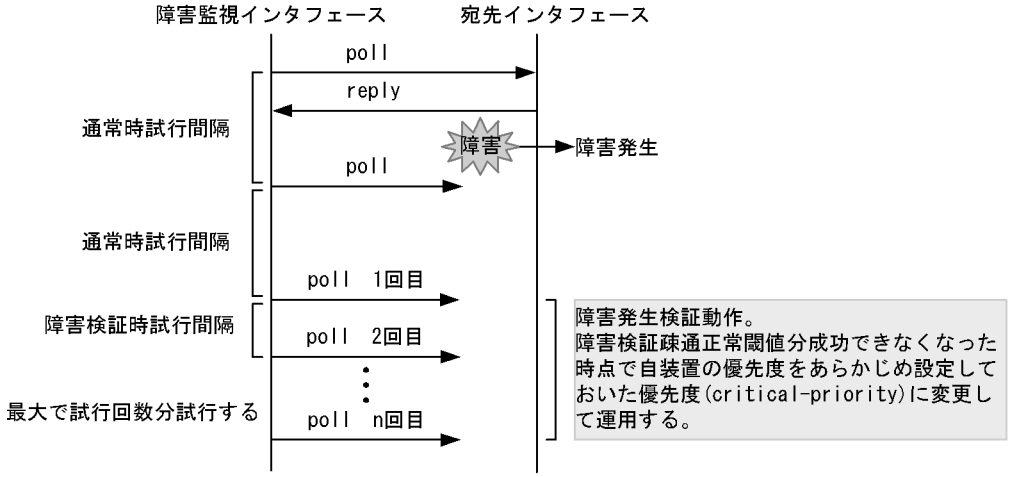


5.5 VRRP ポーリングの障害検出の仕組み

VRRP ポーリングの障害検出の仕組みについて説明します。VRRP ポーリングは通常時，通常時試行間隔（構成定義パラメータの check-status-interval）の指定値（単位：秒）でポーリングを行います。疎通可能状態である場合，応答が返らないままタイムアウトすると，障害発生検証を行います。

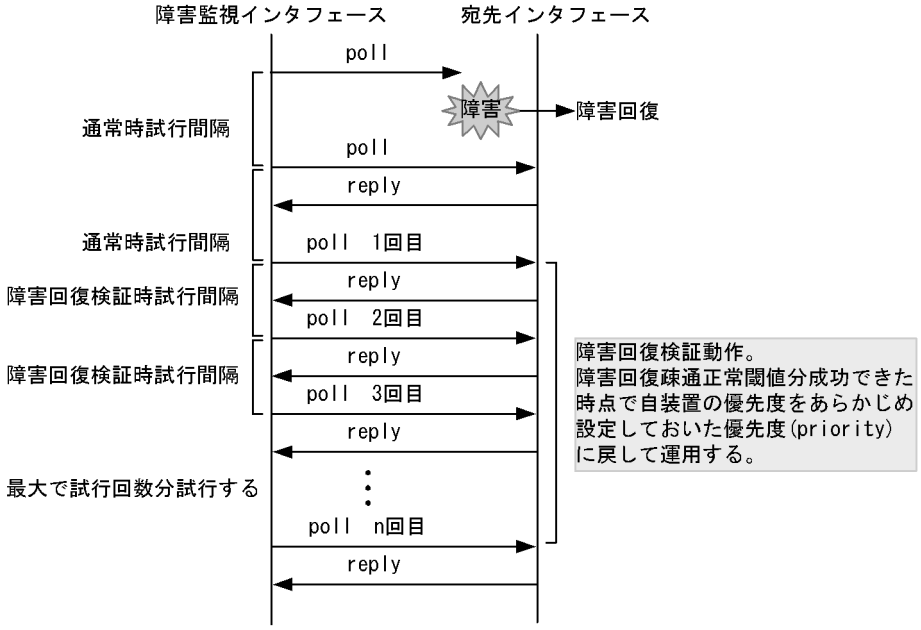
障害発生検証では，障害検証時試行間隔（構成定義パラメータの failure-detection-interval）の指定値（単位：秒）で，試行回数（構成定義パラメータの check-trial-times）のポーリングを行います。このときに，障害検出疎通正常判定閾値（構成定義パラメータの failure-detection-times）で指定した回数分応答が返ってくるか判定し，この回数を満たせなくなった時点で障害と判定します。障害検出動作シーケンスを次の図に示します。

図 5-8　障害検出動作シーケンス



VRRP ポーリングの障害回復検出の仕組みについて説明します。VRRP ポーリングは通常時，通常時試行間隔で指定した間隔でポーリングを行います。疎通不可能状態である場合，応答が返ってくると障害回復検証を行います。障害回復検証では，障害回復検証時試行間隔（構成定義パラメータの recovery-detection-interval）の指定値（単位：秒）で，試行回数分ポーリングを行います。このとき，障害回復疎通正常判定閾値（構成定義パラメータの recovery-detection-times）で指定した回数分応答が返ってくるか判定し，この回数を満たした時点で障害回復と判定します。障害回復動作のシーケンスを次の図に示します。

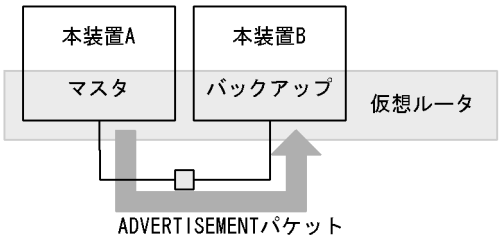
図 5-9　障害回復動作シーケンス



5.6 障害検出の仕組み

マスタ状態の本装置は定期的な周期（デフォルト 1 秒）で ADVERTISEMENT パケットと呼ばれる稼働状態確認用のパケットを，仮想ルータを設定したイーサネットインタフェースから送出します。バックアップ状態のルータはマスタ状態のルータが送出する ADVERTISEMENT パケットを受信することによって，マスタ状態のルータに障害がないことを確認します。ADVERTISEMENT パケットの送出を次の図に示します。

図 5-10 ADVERTISEMENT パケットの送出



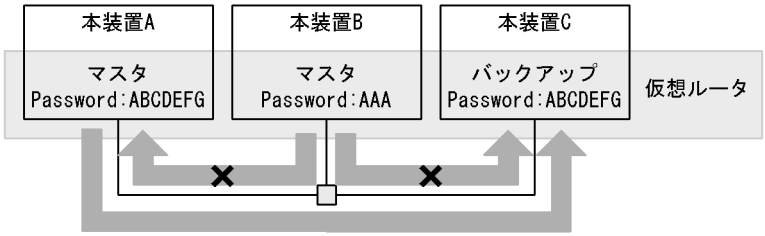
マスタ状態となっている本装置に障害が発生した場合，ADVERTISEMENT パケットを送出できません。例えば，本装置全体がダウンしてしまった場合や，仮想ルータが設定されているイーサネットインタフェースからパケットを送出できなくなるような障害が発生した場合，ケーブルの抜けなどの場合です。

バックアップ状態の本装置は一定の間 ADVERTISEMENT パケットをマスタ状態のルータから受信しなかった場合に，マスタルータに障害が発生したと判断し，バックアップからマスタへと状態を変化させます。

5.7 パケットの認証

ADVERTISEMENT パケットはリンクローカルスコープのマルチキャストアドレス (IPv4 では 224.0.0.18，IPv6 では ff02::12) を使用します。また，VRRP ルータは IP ヘッダの TTL または HopLimit が 255 以外のパケットを受信しないため，(ルータ超えを伴う) 遠隔からの攻撃を防ぐことができます。また，本装置ではテキストパスワードによる VRRP の ADVERTISEMENT パケットの認証をサポートします。8 文字以内のパスワードを仮想ルータに設定すると，パスワードが異なる ADVERTISEMENT パケットを廃棄します。パスワードの不一致を次の図に示します。

図 5-11 パスワードの不一致



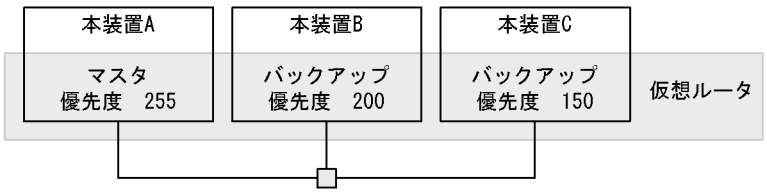
この図の例では本装置 B のパスワードが本装置 A および本装置 C と異なっているため，本装置 B から送出された ADVERTISEMNET パケットを本装置 A や本装置 C が受け取っても廃棄します。この場合，本装置 C は本装置 A からの ADVERTISEMENT パケットだけを受信して処理します。

5.8 マスタルータの選出方法

5.8.1 優先度

複数の VRRP ルータの中からマスタ状態になるルータを選出するために，VRRP では優先度を使用します。この優先度は装置ごとに設定できます。設定できる値は 1 から 255 までの数値で，デフォルトは 100 です。この数値が大きいほど優先度は高くなります。インタフェースに付与されている IP アドレスと仮想ルータの IP アドレスが等しい (IP アドレスの所有者) 場合，最も優先度が高い 255 に自動的に設定されます。マスタ状態のルータの選出を次の図に示します。

図 5-12　マスタ状態のルータの選出



この図の場合，優先度が最も高い本装置 A がマスタ状態になります。本装置 A がダウンした場合は，次に優先度の高い本装置 B がマスタ状態へと変化します。本装置 A と本装置 B の両方がダウンした場合にだけ本装置 C がマスタ状態になります。

5.8.2 自動切り戻し

VRRP では自ルータよりも優先度の低い VRRP ルータがマスタ状態になっていることを検出すると，優先度の高いバックアップルータが自動的にマスタへ状態を変化させます。逆に，マスタ状態のルータが自分より優先度の高いルータの存在を検出したときは自動的にバックアップへと状態を変化させます。

「図 5-12　マスタ状態のルータの選出」の構成を例にしてみると，本装置 A と本装置 B がダウンした状態で本装置 C がマスタ状態になっている状態から，本装置 B が復旧すると，本装置 C よりも優先度の高い本装置 B がマスタ状態に変化し，本装置 C がマスタ状態からバックアップ状態を変化させることになります。

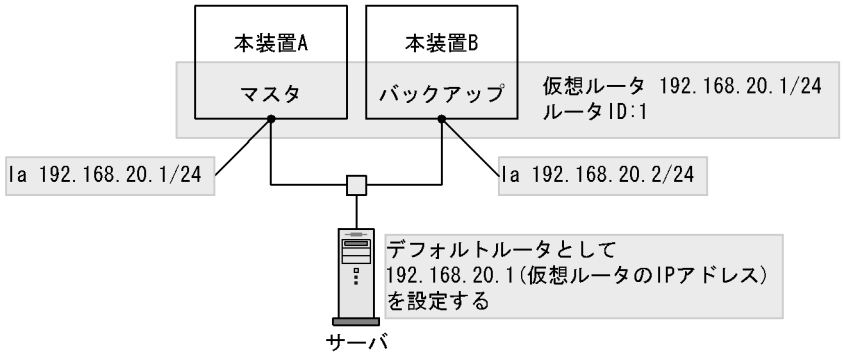
この自動切り戻しの機能を抑止する設定もできます。自動的に切り戻しさせたくない場合には PREEMPT モードを OFF に設定してください。PREEMPT モードを OFF に設定すれば，バックアップ状態のルータが自ルータよりも優先度の低いルータがマスタ状態になっていることを検出しても，マスタ状態へと変化させることはありません。ただ，自装置が IP アドレスの所有者 (優先度が 255 のとき) は切り戻しの抑止は有効になりません。

5.9 ネットワーク構成例

5.9.1 VRRP による構成例

VRRP によるネットワーク構成例を次の図に示します。

図 5-13 VRRP によるネットワーク構成例



この図の構成では同一のイーサネットセグメント内に設置された本装置 2 台を使用して，仮想的なルータを設定しています。実際には 2 台のルータのどちらかがマスタ状態となり，マスタ状態のルータが仮想ルータをシミュレートします。

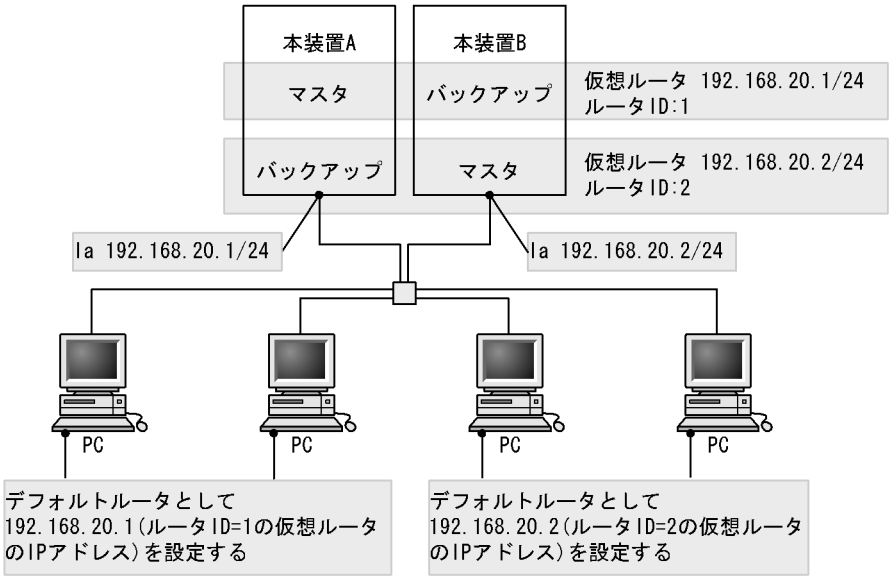
一方，バックアップ状態となったルータはマスタ状態のルータを監視します。マスタ状態のルータに障害が発生して通信を継続させることができなくなった場合，バックアップ状態で待機しているルータがマスタ状態のルータの障害を検出して，自身がマスタに状態を変化させて仮想ルータをシミュレートします。

仮想ルータには IP アドレスが設定されます。仮想ルータの IP アドレスをデフォルトルータとして指定しているサーバはマスタ状態のルータの切り替えを意識しないで通信を継続できます。

5.9.2 負荷分散の例

負荷分散の例を次の図に示します。

図 5-14　負荷分散の例



この図の例では同一のイーサネットセグメントに対して 2 個の仮想ルータを設定しています。配下の 4 台の PC のうち，2 台は仮想ルータ 1(ルータ ID:1 の仮想ルータ) をデフォルトルータに設定し，残りの 2 台は仮想ルータ 2(ルータ ID:2 の仮想ルータ) をデフォルトルータに設定しています。仮想ルータ 1 のマスタルータは本装置 A，仮想ルータ 2 のマスタルータは本装置 B になっているため，通常の運用時 (どちらのルータにも障害がない場合) には 2 台の本装置を使用して負荷分散を行えます。

本構成では，どちらかの装置に障害が発生しても，配下の 4 台の PC にすべて通信経路を確保できます。例えば，本装置 A に障害が発生した場合には仮想ルータ 1 のマスタが本装置 A から本装置 B へ移り，逆に本装置 B に障害が発生した場合には仮想ルータ 2 のマスタが本装置 B から本装置 A へ移ります。デフォルトルータをどちらかの仮想ルータに設定している PC はマスタ状態のルータが存在する間，通信を継続できます。

5.10 VRRP 使用時の注意事項

(1) サポートプロトコル

VRRP 機能を使用できるプロトコルは IPv4 および IPv6 だけです。また，仮想ルータを構成する複数のルータ間は VRRP を使用するプロトコルによって相互に通信できる必要があります。

(2) VRRP ルータに対する通信

VRRP ルータに対する通信 (ping，ping ipv6，telnet，ftp など) はルータのインタフェースに割り当てられている実 IP アドレス宛てで行う必要があります。仮想ルータの IP アドレスの場合，実 IP アドレスと仮想ルータの IP アドレスが同一であるアドレス所有者のルータがマスタ状態のときには通信できますが，それ以外の場合には通信できません。

(3) traceroute，traceroute ipv6

VRRP ルータから送出される IP パケットの送信元アドレスは仮想ルータの IP アドレスではなく，ルータの実 IP アドレスです。そのため，配下のホストから仮想ルータを通過する宛先アドレスに対して traceroute または traceroute ipv6 を実行した場合，マスタ状態となっている VRRP ルータの実 IP アドレスが経路中のルータの IP アドレスとして表示されます。

(4) proxy ARP

VRRP を設定しているイーサネットインタフェースから proxy ARP による応答を行う場合，仮想ルータの MAC アドレスを使用して応答します。物理的に割り当てられる MAC アドレスでは応答しません。

(5) proxyNDP

VRRP を設定しているイーサネットインタフェースから proxyNDP による応答を行う場合，物理的に割り当てられる MAC アドレスを使用して応答します。

(6) ICMP Redirect，ICMPv6 Redirect

VRRP を設定しているインタフェース上では ICMP Redirect および ICMPv6 Redirect メッセージの送出は抑止されます。

(7) 仮想 IP アドレスでの RIP 使用

VRRP で設定した仮想 IP アドレスで RIP を使用することはできません。

(8) 障害監視インタフェース

障害監視インタフェースには IP の定義を行ってください。障害監視インタフェースダウン時の優先度を 0(デフォルト) に設定した場合に障害監視インタフェースがダウンすると，VRRP を設定しているインタフェースもダウン状態になります。また，障害監視インタフェースを複数設定している場合，仮想ルータの優先度からダウンした障害インタフェースの優先度を下げる値の合計を減算した結果，優先度が 0 となった場合も同様に，VRRP を設定しているインタフェースもダウン状態になります。

一つのインタフェースに複数の VRRP 定義を行う場合で，各 VRRP 定義に対してそれぞれ個別の障害監視インタフェースを定義し，その障害監視インタフェースダウン時の優先度を 0 とした場合，該当するインタフェースに定義されている VRRP の障害インタフェースのうち一つでもダウン状態になると，そのインタフェースはそのほかの障害監視インタフェースの状態に関係なくダウン状態になります。その場合，

同一インタフェースに定義されているそのほかの VRRP の動作にも影響が発生するため，障害監視インタフェースダウン時の優先度を 0 とする障害監視インタフェースの指定を行う場合，一つのインタフェースには一つの VRRP を定義することをお勧めします。

一つのインタフェースに複数の VRRP を定義し，障害監視インタフェースダウン時の優先度を 0 とする障害監視インタフェースを指定する場合，各 VRRP の障害監視インタフェース定義にはすべて同一のインタフェースを指定してください。

また，障害監視インタフェースがアップしている場合，VRRP を設定しているインタフェースを close nif <NIF 番号 > line <Line 番号 > でダウンさせた場合でも自動的にアップ状態となります。VRRP を設定しているインタフェースをダウンさせる場合，障害監視インタフェースもダウンさせてください。

(9) VRRP ポーリング

VRRP ポーリングは，障害監視インタフェースを送信インタフェースとします。障害監視インタフェースの IP アドレスと宛先 IP アドレスは，相互に通信できる IP アドレスを設定してください。相互に通信できない IP アドレスを設定した場合は，VRRP ポーリングは障害と判定します。

構成定義で指定する障害監視インタフェースと，宛先 IP アドレスまでの経路は，ルーティングテーブルに依存します。ルーティングプロトコルによって正しい経路を設定してください。

受信インタフェースチェックオプション (構成定義パラメータの check-reply-interface) を指定している場合，送信インタフェースと受信インタフェースが不一致の場合はパケットを破棄します。このため，通信可能状態でも障害と判定する場合があります。受信インタフェースチェックオプションはデフォルトでは無効です。

VRRP ポーリングが送信する ICMP パケットは自装置内では優先されますが，他ルータでは優先されません。このため，ネットワーク過負荷時に障害と判定する場合があります。これを回避するには，VRRP ポーリングのパケットを QoS などで優先するように設定してください。

(10) DHCP/BOOTP リレーエージェント機能との共存

DHCP/BOOTP リレーエージェント機能と VRRP 機能を同一インタフェースで同時に運用する場合は，DHCP/BOOTP サーバで，DHCP/BOOTP クライアントゲートウェイアドレス (ルータオプション) を本装置に設定した仮想ルータアドレスに設定する必要があります。設定方法の詳細については，マニュアル「構成定義ガイド　7.4.6 DHCP/BOOTP リレーと VRRP 連携」を参照してください。

(11) IP-VPN 機能との共存

IP-VPN 機能と VRRP 機能を同一装置内で同時に使用できません。VRRP を使用する場合，IP-VPN 機能を定義しないでください。

(12) IP フィルタリング

VRRP を設定したインタフェースで，VRRP の ADVERTISEMENT パケットを廃棄するフィルタリングを設定しないでください。VRRP の ADVERTISEMENT パケットは，IPv4 の場合，宛先アドレスが ff02::12，送信元アドレスがマスタルータの実 IPv6 アドレス，プロトコル番号 112 になります。

(13) 高負荷時

設定する仮想ルータの数は 2 をお勧めします。仮想ルータの数が 3 以上の場合は VRRP 使用中にアドレス重複のログメッセージが表示されることがあります。2 の場合，装置が過負荷状態になっていることが考えられます。VRRP のパケット送出間隔を大きい値に設定して運用してください。

また，copy mc コマンドや ppupdate コマンド実行時には，RM の CPU 使用率が上昇しマスタ／バックアップの関係が切り替わる場合があります。CPU 高負荷時の切り替えを抑止したい場合は，ADVERTISEMENT パケットの送出間隔を調整してください。

（14）相互運用

Cisco 社ルータに搭載されている HSRP(Hot Standby Router Protocol) とは相互運用できません。

6 SNMP を使用したネットワーク管理

この章では本装置の SNMP エージェント機能についてサポート仕様を中心に説明します。

6.1　SNMP 概説

6.2　MIB 概説

6.3　SNMP オペレーション

6.4　トラップ

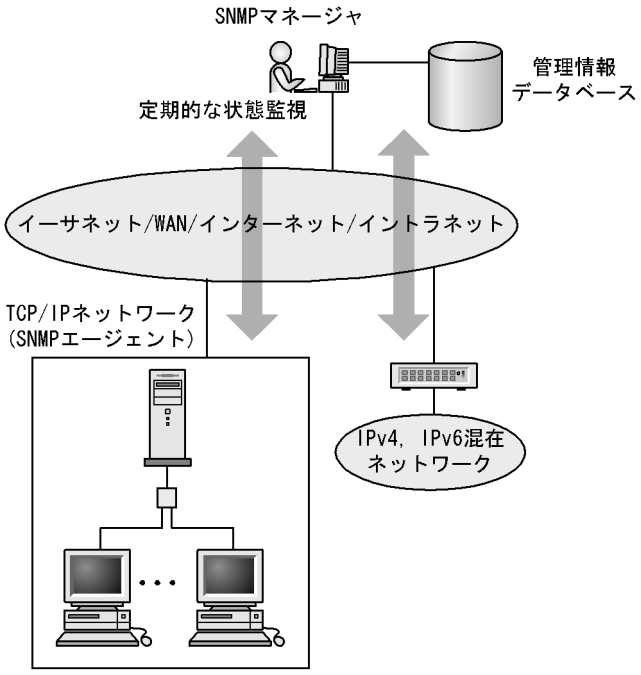
6.5　RMON MIB

6.1 SNMP 概説

6.1.1 ネットワーク管理

ネットワークシステムの稼働環境や性能を維持するためには，高度なネットワーク管理が必要です。SNMP(simple network management protocol) は業界標準のネットワーク管理プロトコルです。SNMP をサポートしているネットワーク機器で構成されたマルチベンダーネットワークを管理できます。管理情報を収集して管理するサーバを SNMP マネージャ，管理される側のネットワーク機器を SNMP エージェントといいます。ネットワーク管理の概要を次の図に示します。

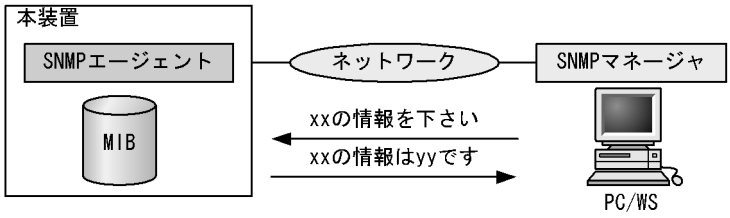
図 6-1 ネットワーク管理の概要



6.1.2 SNMP エージェント機能

本装置の SNMP エージェントは，ネットワーク上の装置内部に組み込まれたプログラムです。装置内の情報を SNMP マネージャに提供する機能があります。装置内にある各種情報を MIB(Management Information Base) と呼びます。SNMP マネージャは，装置の情報を取り出して編集・加工し，ネットワーク管理を行うための各種情報をネットワーク管理者に提供するソフトウェアです。MIB 取得の例を次の図に示します。

図 6-2 MIB 取得の例

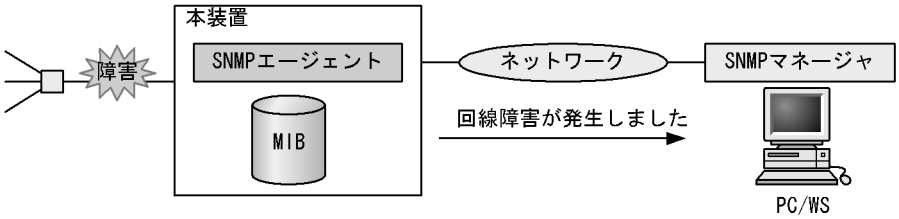


本装置の運用コマンドには MIB 情報を表示するための SNMP コマンドがあります。このコマンドは，自装置およびリモート装置の SNMP エージェントの MIB を表示します。ただし，ネットワーク管理を効率よく行うためには，JP1/Cm2/Network Node Manager などの SNMP マネージャを購入して運用することをお勧めします。

本装置では，SNMPv1(RFC1157) および SNMPv2(RFC1901) をサポートしています。SNMP マネージャを使用してネットワーク管理を行う場合は，SNMPv1 または SNMPv2 プロトコルで使用してください。

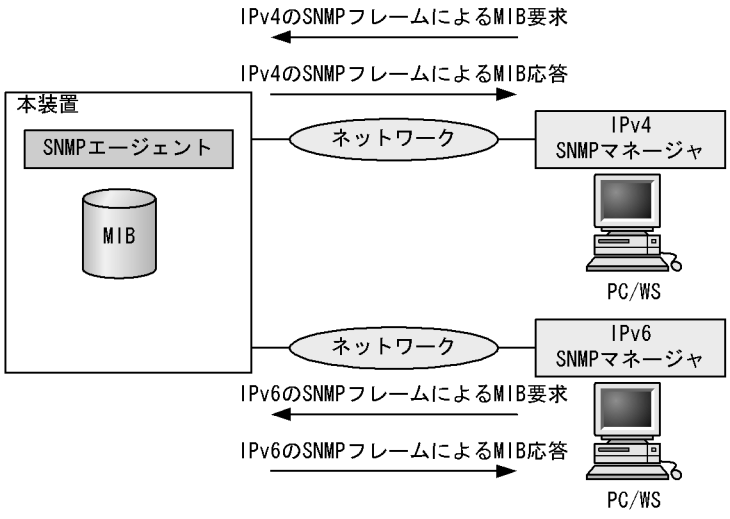
また，SNMP エージェントは**トラップ** (Trap) と呼ばれるイベント通知 (主に障害発生の情報など) 機能があります。SNMP マネージャは，トラップを受信することで定期的に装置の状態変化を監視しなくても変化を知ることができます。ただし，トラップは UDP を使用しているため，装置から SNMP マネージャに対するトラップが到達確認できません。そのため，ネットワークの輻輳などによって，トラップがマネージャに到達しない場合があります。トラップの例を次の図に示します。

図 6-3　トラップの例



本装置の SNMP プロトコルは IPv6 に対応しています。構成定義情報に設定した SNMP マネージャの IP アドレスによって，IPv4 または IPv6 アドレスが設定されている SNMP マネージャからの MIB 要求や，SNMP マネージャへのトラップ送信を行うことができます。IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例を次の図に示します。

図 6-4　IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例



6.2 MIB 概説

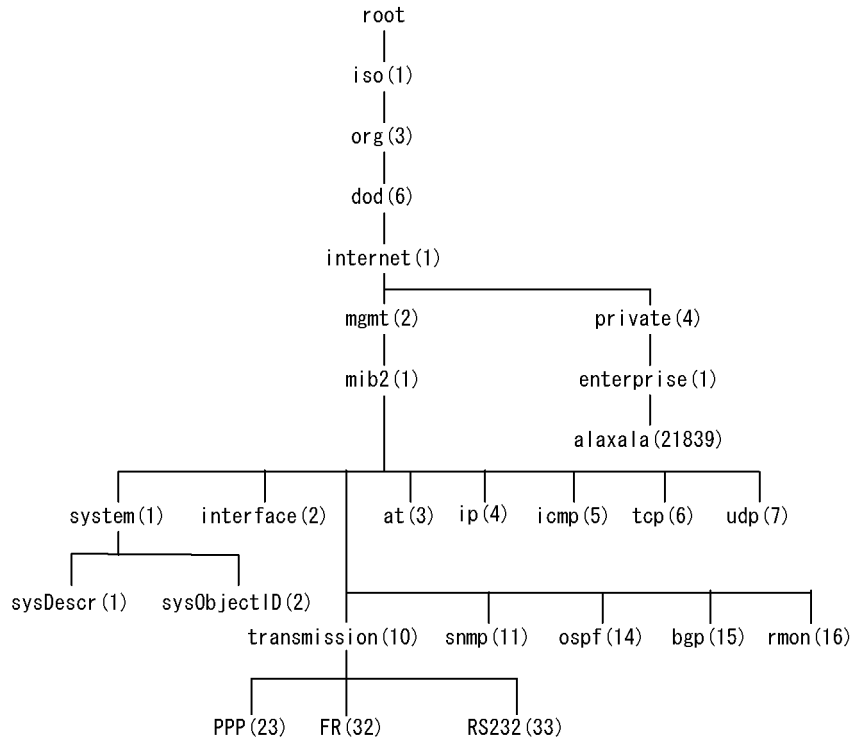
装置が管理し，SNMP マネージャに提供する MIB は，RFC で規定されたものと，装置の開発ベンダーが独自に用意する情報の 2 種類があります。

RFC で規定された MIB を**標準 MIB** と呼びます。標準 MIB は規格化されているため提供情報の内容の差はあまりありません。装置の開発ベンダーが独自に用意する MIB を**プライベート MIB** と呼び，装置によって内容が異なります。ただし，MIB のオペレーション（情報の採取・設定など）は，標準 MIB，プライベート MIB で共通です。オペレーションは，装置と目的の MIB 情報を指定するだけです。装置は IP アドレスで，MIB 情報はオブジェクト ID で指定します。

6.2.1 MIB 構造

MIB の構造はツリー構造になっています。MIB はツリー構造のため，各ノードを識別するために番号を付けて表す決まりになっています。root から各ノードの数字を順番にたどって番号を付けることで個々の MIB 情報を一意に識別できます。この番号列をオブジェクト ID と呼びます。オブジェクト ID は root から下位のオブジェクトグループ番号をドットで区切って表現します。例えば，sysDescr という MIB をオブジェクト ID で示すと 1.3.6.1.2.1.1.1 になります。MIB ツリーの構造例を次の図に示します。

図 6-5 MIB ツリーの構造例



6.2.2 MIB オブジェクトの表し方

オブジェクト ID は数字と．（ドット）(例：1.3.6.1.2.1.1.1) で表現します。しかし，数字の羅列ではわかりにくいため，マネージャによっては，sysDescr というニーモニックで指定できるものもあります。ニーモニックで指定する場合，SNMP マネージャがどの MIB のニーモニックを使えるか確認してから使用し

てください。また，本装置の SNMP コマンドで使用できるニーモニックについては，SNMP サブコマンド lookup を実行することで確認できます。

6.2.3 インデックス

MIB を指定するときのオブジェクト ID を使用しますが，一つの MIB に一つの意味だけある場合と一つの MIB に複数の情報がある場合があります。MIB を特定するためにはインデックス (INDEX) を使用します。インデックスは，オブジェクト ID の後ろに数字を付加して表し，何番目の情報かなどを示すために使用します。

一つの MIB に一つの意味だけがある場合，MIB のオブジェクト ID に ".0" を付加して表します。一つの MIB に複数の情報がある場合，MIB のオブジェクト ID の後ろに数字を付加して何番目の情報であるか表します。例えば，インタフェースのタイプを示す MIB に ifType (1.3.6.1.2.1.2.2.1.2) があります。本装置には複数のインタフェースがあります。特定のインタフェースのタイプを調べるには，"2 番目のインタフェースのタイプ " というように具体的に指定する必要があります。MIB で指定するときは，2 番目を示すインデックス .2 を MIB の最後に付加して ifType.2(1.3.6.1.2.1.2.2.1.2.2) と表します。

インデックスの表し方は，各 MIB によって異なります。RFC などの MIB の定義で，INDEX{ xxxxx,yyyyy,zzzzzz } となっている MIB のエントリは，xxxxx と yyyyy と zzzzzz をインデックスに持ちます。それぞれの MIB について，どのようなインデックスを取るか確認して MIB のオペレーションを行ってください。

6.2.4 本装置のサポート MIB

本装置では，装置の状態，インタフェースの統計情報，ルーティング情報，装置の機器情報など，ルータの管理に必要な MIB を提供しています。なお，プライベート MIB の定義 (ASN.1) ファイルは，ソフトウェアの CD-ROM 内にあります。

各 MIB の詳細についてマニュアル「MIB レファレンス　1. サポート MIB の概要」を参照してください。

6.3 SNMP オペレーション

管理データ (MIB:management information base) の収集や設定を行うため，SNMP では次に示す 4 種類のオペレーションがあります。

- GetRequest　　：指定した MIB の情報を取り出します。
- GetNextRequest：指定した次の MIB の情報を取り出します。
- GetBulkRequest：GetNextRequest の拡張版です。
- SetRequest　　：指定した MIB に値を設定します。

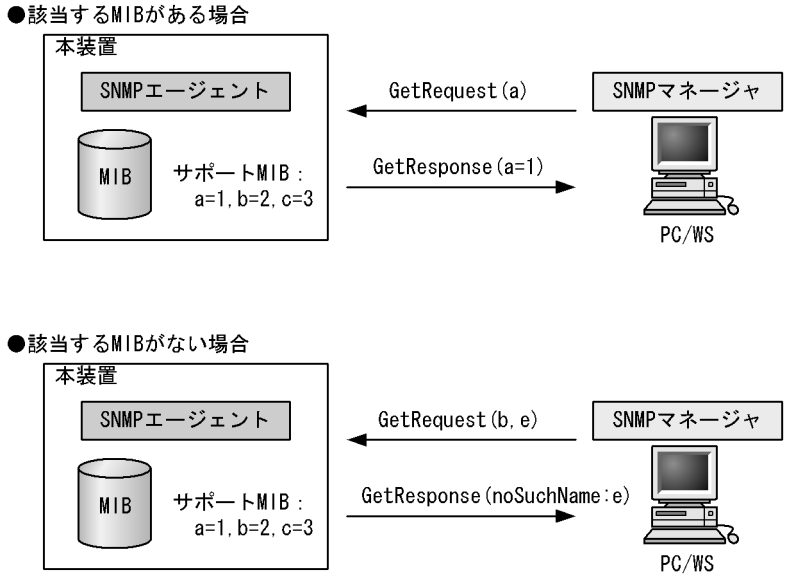
各オペレーションは SNMP **マネージャ**から装置 (SNMP エージェント) に対して行われます。各オペレーションについて説明します。

6.3.1 GetRequest オペレーション

GetRequest オペレーションは，SNMP マネージャから装置 (エージェント機能) に対して MIB の情報を取り出すときに使用します。このオペレーションでは，一つまたは複数 MIB を指定できます。

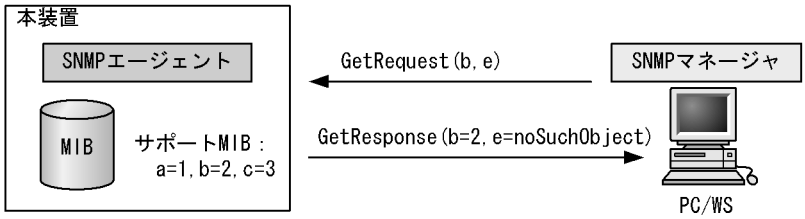
装置が該当する MIB を保持している場合，GetResponse オペレーションで MIB 情報を応答します。該当する MIB を保持していない場合は，GetResponse オペレーションで noSuchName を応答します。
GetRequest オペレーションを次の図に示します。

図 6-6　GetRequest オペレーション



SNMPv2c では，装置が該当する MIB を保持していない場合は，GetResponse オペレーションで MIB 値に noSuchObject を応答します。SNMPv2 の場合の GetRequest オペレーションを次の図に示します。

図 6-7 GetRequest オペレーション (SNMPv2c)

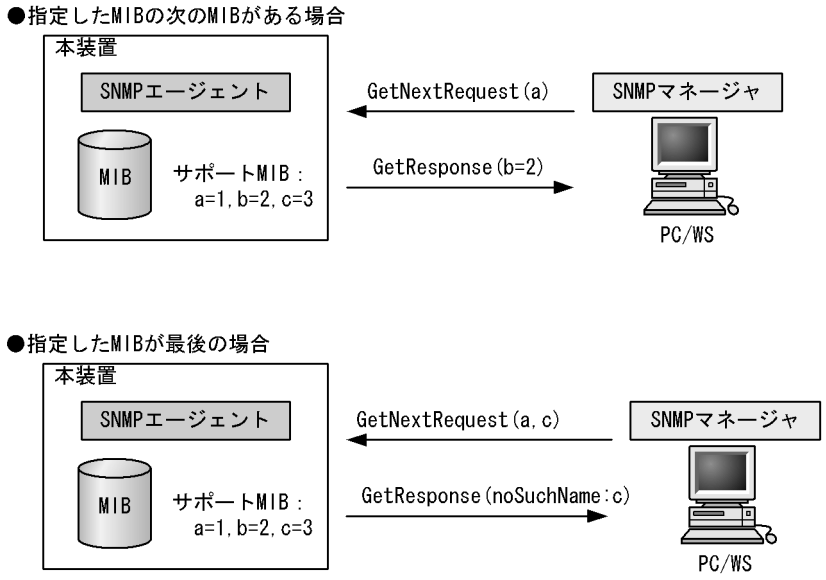


6.3.2 GetNextRequest オペレーション

GetNextRequest オペレーションは，GetRequest オペレーションに似たオペレーションです。GetRequest オペレーションは，指定した MIB の読み出しに使用しますが，GetNextRequest オペレーションは，指定した MIB の次の MIB を取り出すときに使用します。このオペレーションも一つまたは複数の MIB を指定できます。

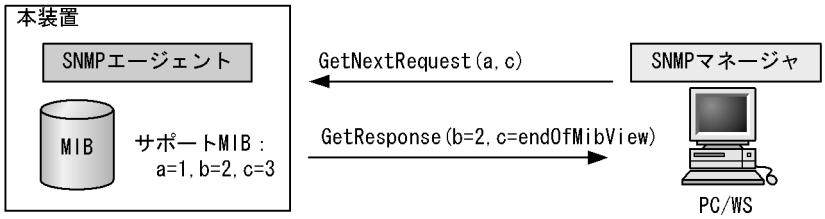
装置が指定した次の MIB を保持している場合は，GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合は，GetResponse で noSuchName を応答します。GetResponse オペレーションを次の図に示します。

図 6-8 GetNextRequest オペレーション



SNMPv2c の場合，指定した MIB が最後の場合は GetResponse で MIB 値に endOfMibView を応答します。SNMPv2 の場合の GetNextRequest オペレーションを次の図に示します。

図 6-9 GetNextRequest オペレーション (SNMPv2c)

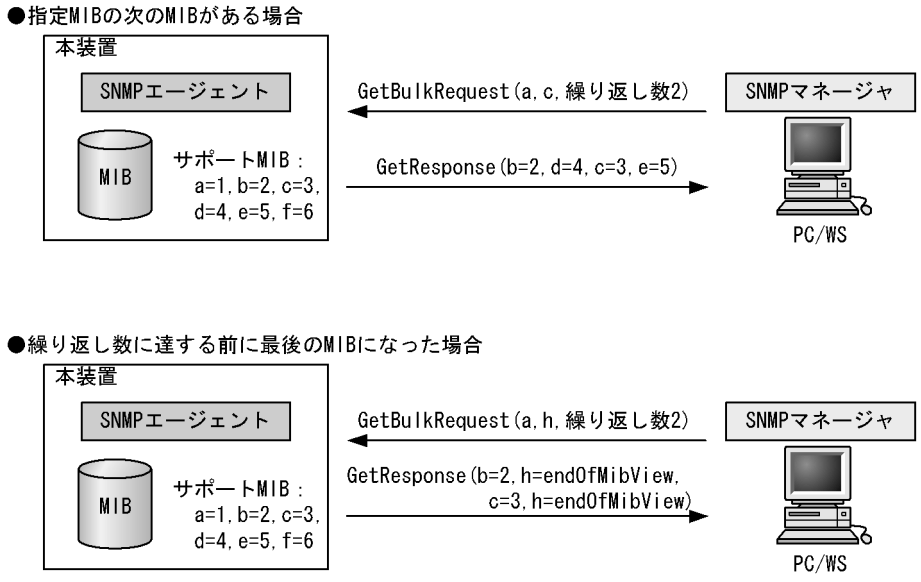


6.3.3 GetBulkRequest オペレーション

GetBulkRequest オペレーションは，GetNextRequest オペレーションを拡張したオペレーションです。このオペレーションでは繰り返し回数を設定し，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を取得できます。このオペレーションも，一つまたは複数の MIB を指定できます。

装置が，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を保持している場合は，GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合，または繰り返し数に達する前に最後の MIB になった場合，GetResponse オペレーションで MIB 値に endOfMibView を応答します。GetNextRequest オペレーションを次の図に示します。

図 6-10 GetBulkRequest オペレーション

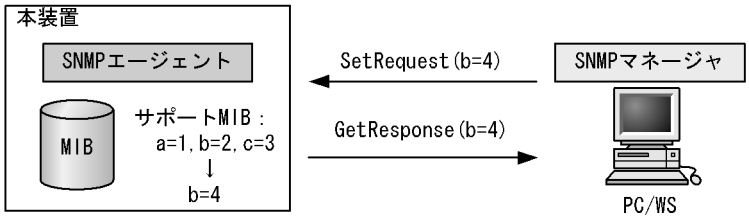


6.3.4 SetRequest オペレーション

SetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して行うオペレーションという点で GetRequest，GetNextRequest，GetBulkRequest オペレーションと似ていますが，値の設定方法が異なります。

SetRequest オペレーションでは，設定する値と MIB を指定します。値を設定すると，GetResponse オペレーションで MIB と設定値を応答します。なお，本装置で SetRequest オペレーションが実行できる MIB は，MIB-II の system グループの MIB と RMON の MIB の一部です。SetRequest オペレーションを次の図に示します。

図 6-11 SetRequest オペレーション



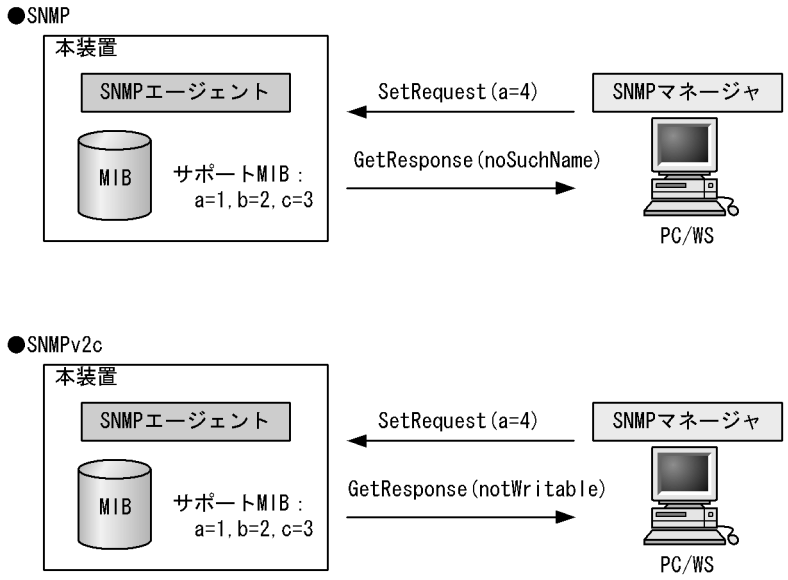
(1) MIB を設定できない場合の応答

MIB を設定できないケースは，次に示す 3 通りです。

- MIB が読み出し専用の場合（読み出し専用コミュニティに属するマネージャの場合も含む）
- 設定値が正しくない場合
- 装置の状態によって設定できない場合

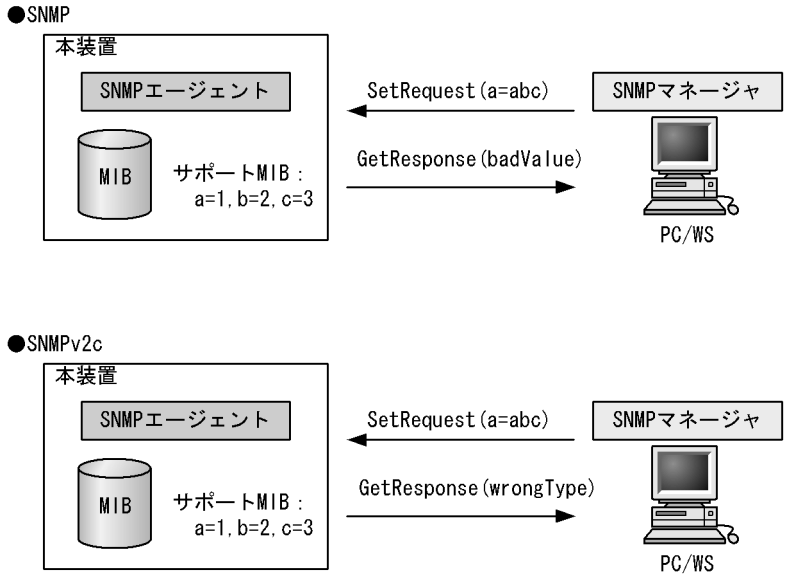
各ケースによって，GetResponse 応答が異なります。MIB が読み出し専用の場合，noSuchName の GetResponse 応答をします。SNMPv2c の場合，MIB が読み出し専用の時は notWritable の GetResponse 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 6-12 MIB 変数が読み出し専用の場合の SetRequest オペレーション



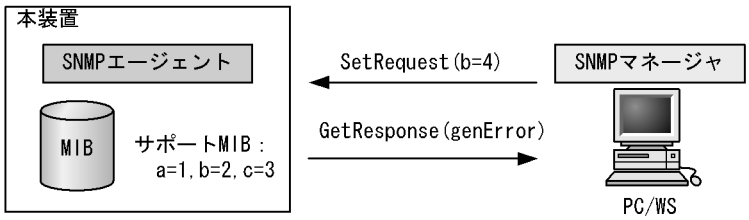
設定値のタイプが正しくない場合，badValue の GetResponse 応答をします。SNMPv2c の場合，設定値のタイプが正しくない時は wrongType の GetResponse 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 6-13 設定値のタイプが正しくない場合の SetRequest オペレーション例



装置の状態によって設定できない場合，GenError の GetResponse を応答します。例えば，装置内で値を設定しようとしたときに，装置内部で設定タイムアウトを検出した場合などがこれに当てはまります。装置の状態によって設定できない場合の SetRequest オペレーションを次の図に示します。

図 6-14 装置の状態によって設定できない場合の SetRequest オペレーション



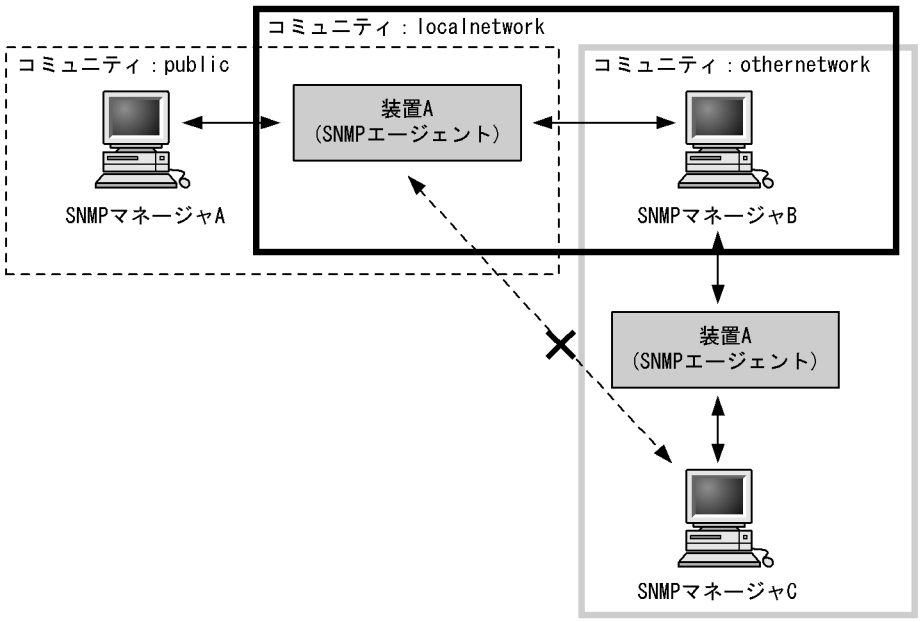
6.3.5 SNMP オペレーションの制限事項

SNMP オペレーションを実行するときには，次に示す制限事項に留意してください。

(1) コミュニティによるオペレーション制限

SNMP ではオペレーションを実行する SNMP マネージャを限定するため，**コミュニティ**という概念があります。コミュニティはオペレーションを実行する SNMP マネージャと SNMP エージェントを一つのグループとして割り当てる名称です。MIB に対してオペレーションする場合は，SNMP マネージャと SNMP エージェントは，同一のグループ（コミュニティ）に属する必要があります。コミュニティによるオペレーションを次の図に示します。

図 6-15 コミュニティによるオペレーション



装置 A はコミュニティ (public) およびコミュニティ (localnetwork) に属しています。コミュニティ (othernetwork) には属していません。この場合，装置 A はコミュニティ (public) およびコミュニティ (localnetwork) の SNMP マネージャ A，B から MIB のオペレーションを受け付けますが，コミュニティ (othernetwork) の SNMP マネージャ C からのオペレーションは受け付けません。

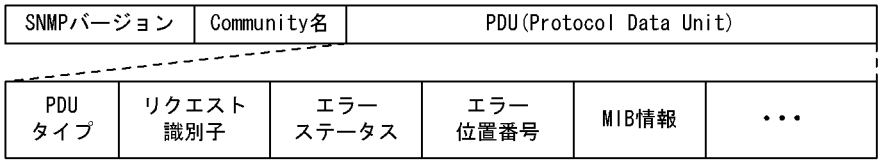
(2) IP アドレスによるオペレーション制限

本装置では，セキュリティを考慮し，コミュニティと SNMP マネージャの IP アドレスの組み合わせが合わないときは MIB のオペレーションを受け付けないようにしています。本装置で SNMP を使用するときは，コミュニティと SNMP マネージャの IP アドレスを構成定義コマンドで登録する必要があります。なお，コミュニティは文字列で設定します。また，一般的にコミュニティ名称は，public を使用している場合が多いです。

6.3.6 SNMP オペレーションのメッセージフォーマット

SNMP のオペレーションを行うメッセージフォーマットは，RFC1157 で規定されています。メッセージフォーマットの概要を次の図に示します。

図 6-16 SNMP オペレーションメッセージフォーマット



GetRequest，GetNextRequest，GetBulkRequest，SetRequest，GetResponse の各オペレーションのメッセージフォーマットは同じです。PDU タイプの値によってメッセージが区別されます。

オペレーション時は，オペレーションの種別を区別するために次の項目に値を設定して SNMP エージェントにメッセージを送信します。

- PDU タイプに種別を設定する
- フレーム送信シーケンス番号をリクエスト識別子に設定する
- オペレーションする MIB のオブジェクト ID を MIB 情報に設定する

PDU タイプコードを次の表に示します。

表 6-1　PDU タイプコード

オペレーション	コード
GetRequest	0xA0
GetNextRequest	0xA1
SetRequest	0xA2
GetResponse	0xA3
GetBulkRequest	0xA5

オペレーションの結果エラーが発生した場合，SNMP エージェントはエラーステータスにエラーコードを設定し，何番目の MIB 情報でエラーが発生したかをエラー位置番号に設定した GetResponse オペレーションの応答を返します。オペレーションの結果が正常なら，エラーステータスにエラーなしのコードを設定し，MIB 情報内にオペレーションした MIB 情報を設定した GetResponse オペレーションの応答を返します。エラーステータスコードを次の表に示します。

表 6-2　エラーステータスコード

エラーステータス	コード	内容
noError	0	エラーはありません。
tooBig	1	データサイズが大きく PDU に値を設定できません。
noSuchName	2	指定 MIB がない，または書き込みできませんでした。
badValue	3	設定値が不正です。
readOnly	4	書き込みできませんでした（本装置では応答することはありません）。
GenError	5	コード 0 ～ 4 以外のエラーが発生しました。
noAccess	6	アクセスできない MIB に対して set を行おうとしました。
wrongType	7	MIB で必要なタイプと異なるタイプが指定されました。
wrongLength	8	MIB で必要なデータ長と異なる長さが指定されました。
wrongEcoding	9	ASN.1 符号が不正でした。
wrongValue	10	MIB 値が不正でした。
noCreation	11	該当する MIB が存在しません。
inconsistentValue	12	現在何か理由があって値が設定できません。
resourceUnavailable	13	値の設定のためにリソースが必要だが，リソースが利用できません。
commitFaild	14	値の更新に失敗しました。
undoFaild	15	値の更新に失敗したときに，更新された値を元に戻すのに失敗しました。
notWriteable	17	セットできません。
inconsistentName	18	該当する MIB が存在しないため，現在は作成できません。

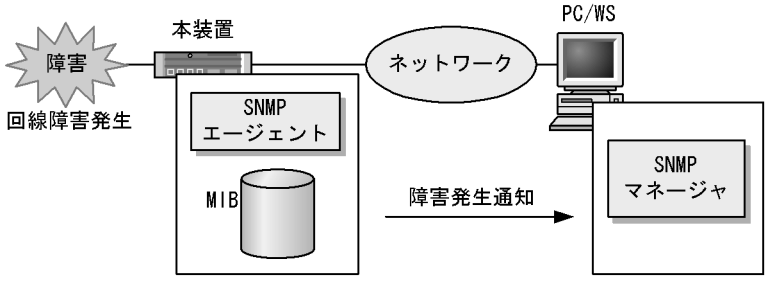
6.4 トラップ

6.4.1 トラップ概説

SNMP エージェントは**トラップ** (Trap) と呼ばれるイベント通知（主に障害発生の情報など）機能があります。トラップは重要なイベントを SNMP エージェントから SNMP マネージャに非同期に通知する機能です。SNMP マネージャは，トラップを受信することで定期的に装置の状態変化を検知できます。この通知を基に，装置内の MIB を取得して，さらに詳細な情報を得ることができます。

なお，トラップは UDP を使用しているため，装置から SNMP マネージャに対するトラップの到達が確認できません。そのため，ネットワークの輻輳などによってトラップがマネージャに到達しない場合があります。トラップの例を次の図に示します。

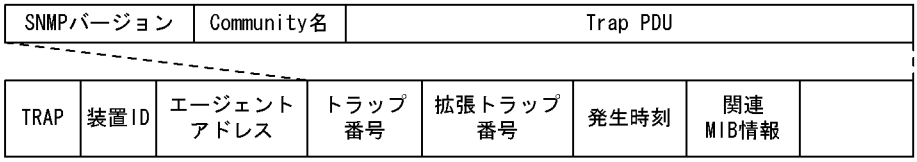
図 6-17 トラップの例



6.4.2 トラップフォーマット

トラップフレームには，どの IP アドレスの装置で，いつ，何が発生したかを示す情報を含みます。トラップフォーマットを次の図に示します。

図 6-18 トラップフォーマット



装置ID　：装置の識別ID（通常MIB-IIのsysObjectIDの値が設定される）
エージェントアドレス：トラップが発生した装置のIPアドレス
トラップ番号　：トラップの種別を示す識別番号
拡張トラップ番号　：トラップ番号の補足をするための番号
発生時刻　：トラップが発生した時間（装置が起動してからの経過時間）
関連MIB情報　：このトラップに関連するMIB情報

6.4.3 サポートトラップ

本装置では，MIB-II Trap，GBP Trap，RMON Trap，プライベート Trap の 4 種類をサポートしています。本装置がマネージャにトラップを通知するためには，構成定義コマンドでトラップを受信する SNMP マネージャのコミュニティ名，IP アドレスおよび受信するトラップのレベル（標準トラップだけか，プライベート Trap を含むか）を登録する必要があります。また，MIB-II Trap は使用している機能に関係なく，常に有効です。ほかのトラップは，機能を有効にすることでトラップが発行されます。

本装置が通知するトラップを次の表に示します。

表 6-3 本装置が通知するトラップ

トラップ種別	イベント通知概要
MIB-II Trap	• 装置が起動しました。 • 装置の構成変化を検出しました。 • 回線のリンクダウンを検出しました。 • 回線のリンクダウンの回復を検出しました。 • 不正な SNMP マネージャからのアクセスを検出しました。
BGP Trap	• BGP リンク確立を検出しました。 • BGP リンク断を検出しました。
RMON Trap	• 特定の MIB の値が上方閾値超えを検出しました。 • 特定の MIB の値が下方閾値下回りを検出しました。
プライベート Trap	• システム障害または警告メッセージの出力を検出しました。 • 待機系 RM の状態変化を検出しました。

各トラップの詳細についてはマニュアル「MIB レファレンス　4. サポート MIB トラップ」を参照してください。

6.4.4 PVC Trap

プライベート Trap の一つである PVC Trap は，ATM インタフェース上の VC が，新しく一つ以上通信できない状態になったときに送信されるトラップです。また，ATM インタフェースごとに PVC Trap の送信間隔を示す PVC Trap インターバルタイムを構成定義コマンドで設定できます。PVC Trap が送信されると，同一 ATM インタフェースの PVC Trap がインターバルタイム内に新しく発行されることはありません。

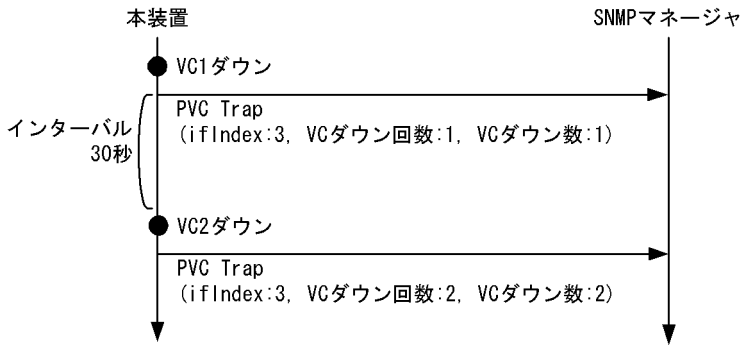
PVC Trap が SNMP マネージャに通知されると，次の三つの MIB 情報がトラップ情報として付加されています。

- ifIndex(ATM 物理インタフェースを示す ATM の物理層の ifIndex 値）
- grAtmIntfPVcFailures(該当する ATM 物理インタフェースに含まれる PVC が通信できない状態になった回数）
- grAtmIntfCurrentlyFailingPVcls(該当する ATM 物理インタフェースに含まれる，通信できない状態の PVC の総数）

ATM 回線 (ifIndex 値：3) に VC が 3 本 (VC1，VC2，VC3) 設定されている状態を例にして，PVC Trap の動作例を説明します。PVC Trap の送信間隔である PVC Trap インターバルタイムは 30 秒とします。

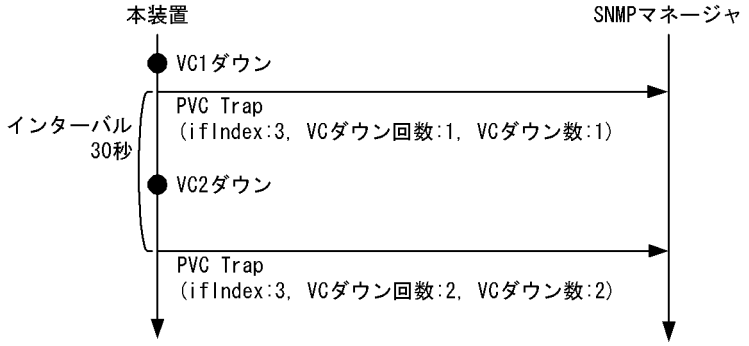
PVC Trap を SNMP マネージャに送信後，インターバルタイム以上経過したあとで新しく VC のダウンが発生した場合は，ダウン発生と同時に PVC Trap を送信します。この場合の PVC Trap 動作例 (VC のダウン間隔がインターバルタイム以上の場合 PVC Trap 動作例を次の図に示します。

図 6-19　PVC Trap 動作例 (VC のダウン間隔がインターバルタイム以上の場合)



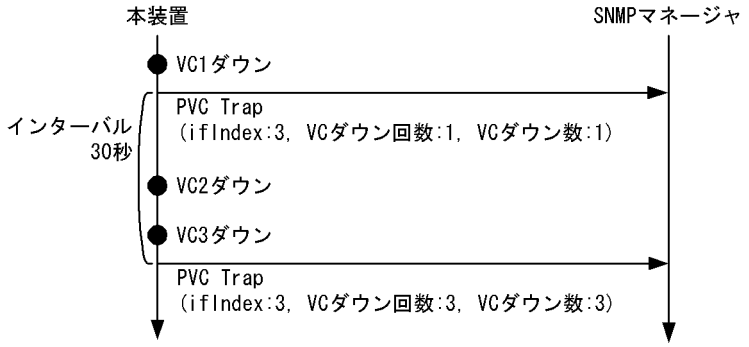
PVC Trap を SNMP マネージャに送信後，インターバルタイムが経過しないうちに新しく VC のダウンが発生した場合は，インターバルタイムが経過したあとに PVC Trap を送信します。VC のダウン間隔がインターバルタイム以内の場合の PVC Trap 動作例を次の図に示します。

図 6-20　PVC Trap 動作例 (インターバルタイム以内に VC のダウンが発生した場合)



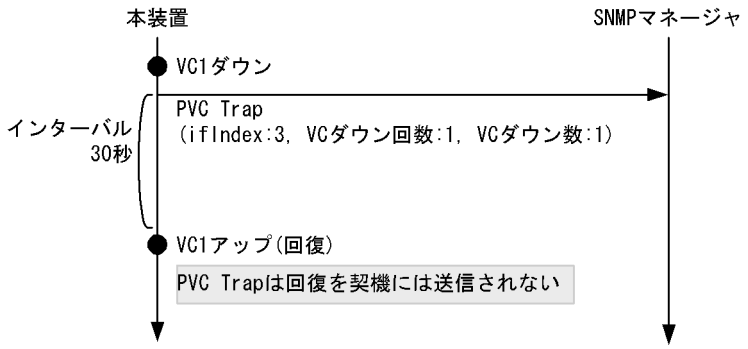
PVC Trap を SNMP マネージャに送信後，インターバルタイムが経過しないうちに新しく複数 VC のダウンが発生した場合は，インターバルタイムが経過したあとに 1 回だけ PVC Trap を送信します。この場合の PVC Trap 動作例を次の図に示します。

図 6-21　PVC Trap 動作例 (インターバルタイム以内に複数 VC のダウンが発生した場合)



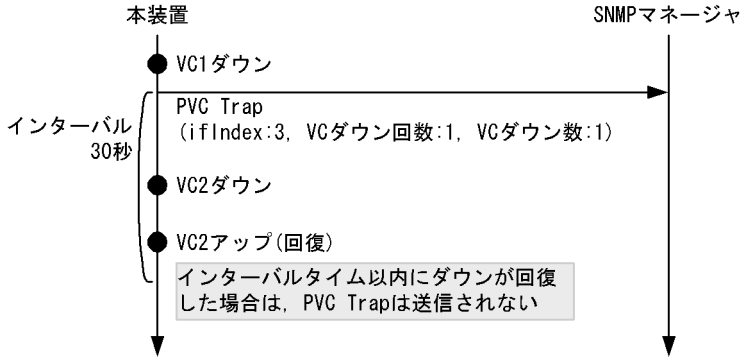
PVC Trap を SNMP マネージャに送信後，インターバルタイムが経過したあとに該当する VC が回復した場合は，PVC Trap は送信されません。PVC Trap は VC の回復を契機としては送信されません。この場合の PVC Trap 動作例を次の図に示します。

図 6-22　PVC Trap 動作例 (VC の回復間隔がインターバルタイム以上の場合)



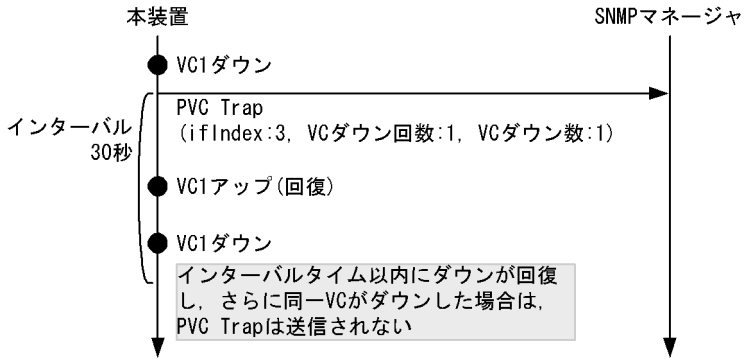
PVC Trap を SNMP マネージャに送信後，インターバルタイムが経過しないうちに新しく VC のダウンが発生し，さらにインターバルタイム以内に新しくダウンした VC が回復した場合は，インターバルタイムが経過しても PVC Trap は送信されません。この場合の PVC Trap 動作例を次の図に示します。

図 6-23　PVC Trap 動作例 (VC のダウン，回復がインターバルタイム以内に発生した場合)



PVC Trap を SNMP マネージャに送信後，インターバルタイムが経過しないうちに該当する VC が回復し，さらにインターバルタイム以内に該当する VC がダウンした場合は，インターバルタイムが経過しても PVC Trap は送信されません。この場合の PVC Trap 動作例を次の図に示します。

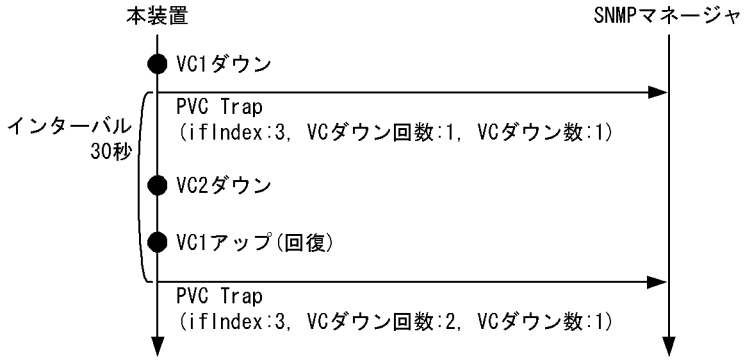
図 6-24　PVC Trap 動作例 (該当する VC の回復，ダウンがインターバルタイム以内に発生した場合)



PVC Trap を SNMP マネージャに送信後，インターバルタイムが経過しないうちに新しく VC がダウンし，さらにインターバルタイム以内に該当する VC が回復した場合は，インターバルタイムが経過したあ

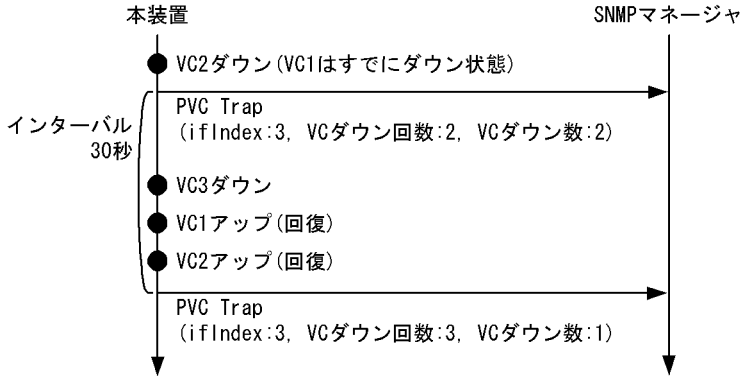
と，PVC Trap が送信されます。この場合の PVC Trap 動作例を次の図に示します。

図 6-25 PVC Trap 動作例 (該当する VC の回復，新しい VC のダウンがインターバルタイム以内に発生した場合)



PVC Trap を SNMP マネージャに送信後，インターバルタイムが経過しないうちに新しく VC がダウンし，さらにインターバルタイム以内に該当する VC がすべて回復した場合は，インターバルタイムが経過したあと，PVC Trap が送信されます。この場合の PVC Trap 動作例を次の図に示します。

図 6-26 PVC Trap 動作例 (該当する VC の全回復，新しい VC のダウンがインターバルタイム以内に発生した場合)



6.5 RMON MIB

RMON(Remote Network Monitoring) とは，イーサネット統計情報を提供する機能，収集した統計情報の閾値チェックを行ってイベントを発生させる機能，パケットをキャプチャする機能などを持ちます。この RMON は RFC1757 で規定されています。

RMON MIB のうち，statistics，history，alarm，event の各グループについて概要を説明します。

(1) statistics グループ

監視対象のサブネットワークについての，基本的な統計情報を収集します。例えば，サブネットワーク中の総パケット数，ブロードキャストパケットのような各種類ごとのパケット数，CRC エラー，コリジョンエラーなどのエラー数などです。statistics グループを使うと，サブネットワークのトラフィック状況や回線状態などの統計情報を取得できます。本装置では，イーサネット，ギガビット・イーサネットの回線で情報を取得します。

(2) history グループ

statistics グループで収集する情報とほぼ同じ統計情報をサンプリングし，来歴情報として保持できます。

history グループには historyControlTable という制御テーブルと，etherHistoryTable というデータテーブルがあります。historyControlTable はサンプリング間隔や来歴記録数の設定を行うための MIB です。

etherHistoryTable は，サンプリングした統計情報の来歴記録の MIB です。history グループは，一定期間の統計情報を装置内で保持しています。このため，SNMP マネージャなどが定期的にポーリングして統計情報を収集するのと比較して，ネットワークに負荷をかけることが少なく，連続した一定期間の統計情報を取得できます。

(3) alarm グループ

監視対象とする MIB のチェック間隔，閾値などを設定して，その MIB が閾値に達した時にログを記録したり，SNMP マネージャにトラップを発行したりすることを指定する MIB です。

この alarm グループは，例えば，サンプルタイムとして設定した 5 分間のうちに，パケットを取りこぼすという状態が 10 回以上検出したときにログを収集したり，SNMP マネージャにトラップを発行したりできます。この alarm グループを使用するときは，event グループも設定する必要があります。

(4) event グループ

event グループには alarm グループで設定した MIB の閾値を超えたときの動作を指定する eventTable グループ MIB と閾値を超えた時にログを記録する logTable グループ MIB があります。

eventTable グループ MIB は，閾値に達した時にログを記録するのか，SNMP マネージャにトラップを発行するのか，またはその両方するか何もしないかを設定するための MIB です。

logTable グループ MIB は，eventTable グループ MIB でログの記録を指定したときに，装置内にログを記録します。装置内のログのエントリ数は決まっているので，エントリをオーバーした場合，新しいログ情報の追加によって，古いログ情報が消去されていきます。定期的に SNMP マネージャに記録を退避しないと，前のログが消されてしまう可能性がありますので注意してください。

RMON は，JP1/Cm2 や HP OpenVeiw などの SNMP マネージャでも使用できますが，専用の RMON マネージャを使用すれば，より有効に RMON を活用できます。ただし，RMON マネージャによっては，本装置で使用できないものがありますので事前にテストしてから利用してください。

7 RADIUS による認証

この章では RADIUS サーバに対して本装置が要求する認証機能について説明します。

7.1 RADIUS 概説

7.2 RADIUS の適用機能および範囲

7.3 RADIUS を使用した認証

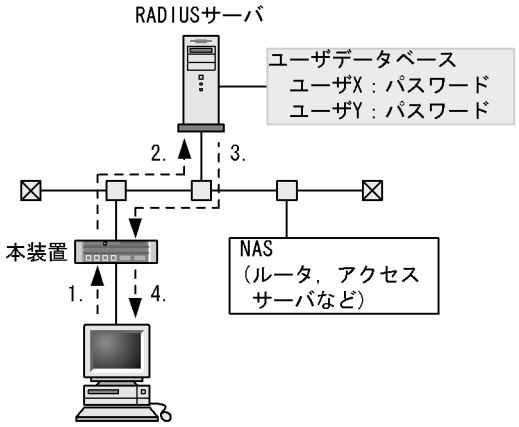
7.4 RADIUS 認証でのログインユーザの扱い

7.1 RADIUS 概説

RADIUS (Remote Authentication Dial In User Service) とは，NAS(Network Access Server) に対して認証・課金機能を提供するプロトコルです。NAS は RADIUS のクライアントとして動作するリモートアクセスサーバ，ルータなどの装置のことです。NAS は構築されている RADIUS サーバに対してユーザ認証，課金などのサービスを要求します。RADIUS サーバはその要求に対して，サーバ上に構築された管理情報データベースに基づいて要求に対する応答を返します。

RADIUS を使用すると一つの RADIUS サーバだけで，複数 NAS でのユーザパスワードなどの認証情報や課金情報を一元管理することができるようになります。本装置では，RADIUS サーバに対してユーザ認証を要求できます。RADIUS 認証の流れを次の図に示します。

図 7-1 RADIUS 認証の流れ



1. リモート運用端末よりユーザXが本装置にtelnetを実行する。
2. 本装置は構成定義で指定したRADIUSサーバに対して認証を要求する。
3. RADIUSサーバはユーザデータベースに基づいてユーザXを認証し，本装置にユーザXを認証したことを通知する。
4. 本装置はRADIUS認証に基づいて、ユーザXのリモート運用端末からのtelnetを許可する。

7.2 RADIUS の適用機能および範囲

本装置では，RADIUS をリモート運用端末からのログイン時のユーザ認証に使用します。RADIUS 機能のサポート範囲を次に示します。ログインについては，「8.3 ログイン制御」も参照してください。

(1) RADIUS の適用範囲

RADIUS 認証を適用できる操作を次に示します。

- 本装置への telnet(IPv4/IPv6)
- 本装置への rlogin(IPv4/IPv6)
- 本装置への ftp(IPv4/IPv6)

次に示す操作は RADIUS 認証を適用できません。

- RS232C からのログイン
- モデムを経由してのログイン
- ルータ管理者になるためのコマンド実行 (enable，admin)

(2) RADIUS のサポート範囲

RADIUS のサポート範囲を次の表に示します。

表 7-1 RADIUS のサポート範囲

分類	内容
文書全体	NAS に関する記述だけを対象にする
パケットタイプ	ログイン認証で使用する次のタイプ • Access-Request (送信) • Access-Accept (受信) • Access-Reject (受信)
属性	ログイン認証で使用する次の属性 • User-Name • User-Password • Service-Type • NAS-IP-Address • NAS-Identifier • Reply-Message

(3) 使用する RADIUS 属性の内容

使用する RADIUS 属性の内容を次の表に示します。

表 7-2 使用する RADIUS 属性の内容

属性名	パケットタイプ	内容
User-Name (属性値 =1)	Access-Request	認証するユーザの名前。
User-Password (属性値 =2)	Access-Request	認証ユーザのパスワード。 送信時には暗号化されます。
Service-Type (属性値 =6)	Access-Request	Login(値 =1)。 Access-Accept および Access-Reject に添付された場合は無視します。

属性名	パケットタイプ	内容
NAS-IP-Address (属性値 =4)	Access-Request	本装置の IP アドレス。 ローカルアドレスが設定されている場合はローカルアドレス，ローカルアドレスが設定されていない場合は，送信インタフェースの IP アドレスになります。
NAS-Identifier (属性値 =32)	Access-Request	本装置のルータ名。 ルータ名が設定されていない場合は添付されません。
Reply-Message (属性値 =18)	Access-AcceptAccess-Reject	サーバからのメッセージ。 添付されている場合は，運用ログとして出力されます。

注 1　この表で示す以外の属性については，本装置が送信する Access-Request タイプパケットには添付しません。
注 2　RADIUS サーバから送信される Access-Accept および Access-Reject タイプパケットにこの表で示す以外の属性が添付されている場合，本装置ではそれらを無視します。

7.3 RADIUS を使用した認証

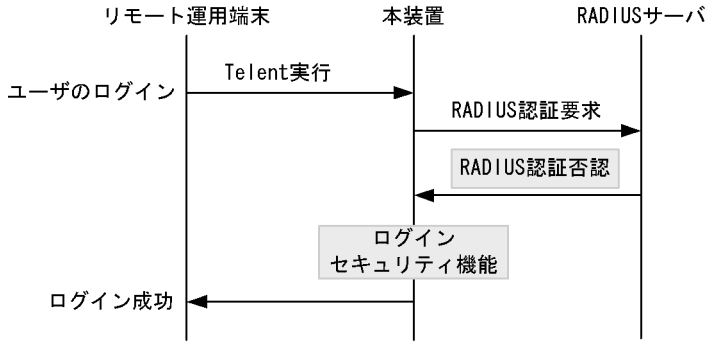
RADIUS を使用した認証方法について説明します。

(1) ログイン認証方式の指定

リモートログインの認証に使用するサービスは複数指定できます。指定できるサービスは RADIUS および password コマンドによる本装置単体でのログインセキュリティ機能です。これらの認証方式は単独でも同時でも指定でき，同時に指定された場合は先に指定された方式で認証に失敗した場合に，次に指定された方式で認証できます。

認証方式として RADIUS，単体でのログインセキュリティの順番で指定した場合の認証方式シーケンスを次の図に示します。

図 7-2 認証方式シーケンス



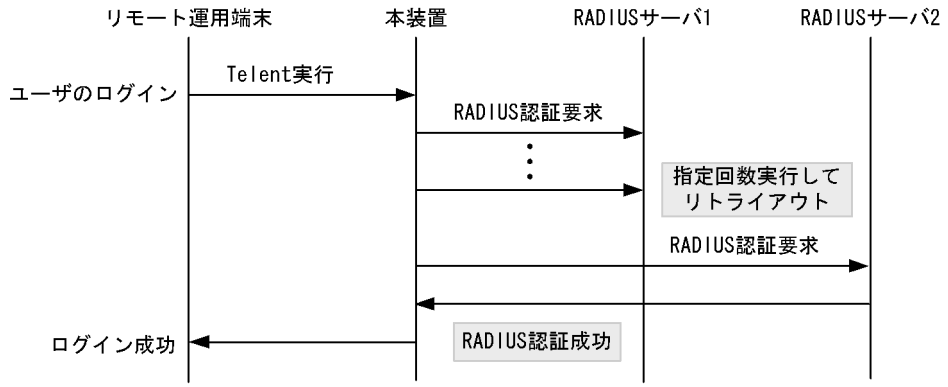
この図で端末からユーザが本装置に telnet を実行すると，RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS サーバと通信不可または RADIUS サーバでの認証に失敗すると，次に本装置のログインセキュリティ機能での認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

(2) RADIUS サーバの選択

RADIUS サーバは最大四つまで指定できます。一つのサーバと通信できないで認証サービスが受けられない場合は，順次これらのサーバに接続を試行します。

RADIUS サーバと通信不可を判断するタイムアウト時間を設定できます。デフォルト値は 5 秒です。また，各 RADIUS サーバでタイムアウトした場合は，再接続を試行します。この再試行回数も設定でき，デフォルト値は 2 回です。このため，ログイン方式として RADIUS が使用できないと判断するまでの最大時間は，タイムアウト時間×リトライ回数× RADIUS サーバ設定数になります。RADIUS サーバ選択のシーケンスを次の図に示します。

図 7-3 RADIUS サーバ選択のシーケンス



この図でリモート端末からユーザが本装置に telnet を実行すると，RADIUS サーバ 1 に対し本装置から RADIUS 認証を要求します。RADIUS サーバ 1 と通信できなかった場合は，続いて RADIUS サーバ 2 に対して RADIUS 認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

7.4 RADIUS 認証でのログインユーザの扱い

RADIUS 認証機能を使用するには，RADIUS サーバにユーザ名およびパスワードを登録します。
RADIUS サーバへ登録するユーザ名には次に示す 2 種類があります。

- 本装置に adduser コマンドを使用して登録済みのユーザ名
  本装置に登録されたユーザ情報を使用してログイン処理を行います。
- 本装置に未登録のユーザ名
  次に示す共通のユーザ情報でログイン処理を行います。
  - ユーザ名：remote_user
  - ホームディレクトリ：/usr/home/share/remote_user

RADIUS による認証を行う場合でも，RADIUS サーバおよび本装置の両方に同一ユーザ名を登録することをお勧めします。

本装置に未登録のユーザでログインした場合の注意点を示します。

- ファイルの管理
  ファイルを作成した場合，すべて remote_user 管理となり，別の RADIUS ユーザが作成したファイルの読み込みおよび書き込みができます。重要なファイルは ftp などで外部に保管するなど，ファイルの管理に注意してください。

8 運用機能

この章は，本装置の管理対象の考え方，管理情報および運用に使用する機能の概要について説明します。なお，リモート運用端末から本装置の運用管理を行うためには IP ネットワークへ接続されていることが必要です。

8.1 **運用管理**

8.2 **立ち上げ**

8.3 **ログイン制御**

8.4 **構成定義**

8.5 **運用コマンド**

8.6 MC

8.7 **管理情報の収集**

8.8 LED **および** FAULT CODE **の表示**

8.9 **ネットワーク障害切り分け機能**

8.10 **障害時の復旧および情報収集**

8.11 **ソフトウェアのアップデート**

8.12 **ファイル属性**

8.1 運用管理

本装置はセットアップ作業が終了すると，コンソールまたはリモート運用端末を使用して運用管理します。本装置には同時に複数の運用端末を接続し複数のユーザがログインできますが，構成定義情報の編集は「ルータ管理者」となった 1 ユーザに制限しています。運用管理の種類を次の表に示します。

表 8-1 運用管理

運用機能	概要
コマンド入力機能	コマンドラインによる入力を受け付けます。
ログイン制御機能	不正アクセス防止，パスワードチェックを行います。
構成定義情報編集機能	運用のための構成定義情報を設定します。設定された情報はすぐ運用に反映されます。
ネットワークコマンド機能	IP，IPv6，IPX，ブリッジ情報表示，リモート操作コマンドなどをサポートします。
ログ・統計情報	過去に発生した障害情報および回線使用率などの統計情報を表示します。
LED および FAULT CODE の表示	LED および 7 セグによって本装置の状態を参照します。
MIB 情報収集	SNMP マネージャによるネットワーク管理が行います。
装置保守機能	装置を保守するための状態表示，装置とネットワークの障害を切り分けるための回線診断，およびパッケージの取り替えなどのコマンドを持ちます。
MC 保守機能	MC のコピー，フォーマットなどを行います。

8.1.1 運用端末

本装置は運用端末として初期導入時にコンソールが必要です。そのあとの運用にはコンソールまたはリモート運用端末が必要です。コンソールは RS232C に接続する端末，リモート運用端末は IP ネットワーク経由で接続する端末です。運用端末は telnet や rlogin で本装置にリモートログインします。運用端末は IP ネットワーク経由で SNMP マネージャによるネットワーク管理にも対応しています。運用端末の接続形態を「図 8-1 運用端末の接続形態」に，リモート運用端末接続ポートと運用端末の条件を「表 8-2 運用端末の条件」に示します。

図 8-1 運用端末の接続形態

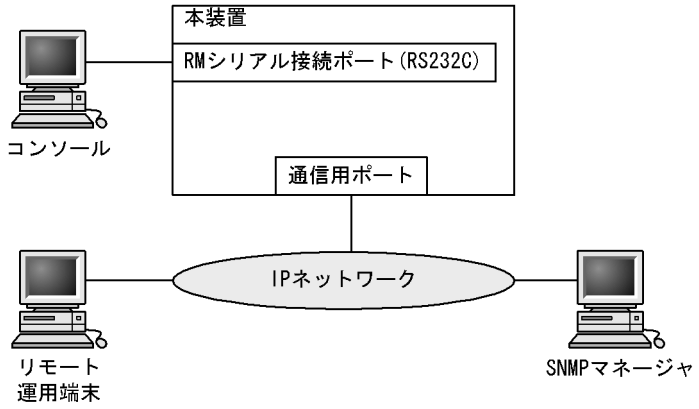


表 8-2 運用端末の条件

端末種別	接続形態	必要機能
コンソール	RM シリアル接続 (RS232C)	RS232C(回線速度：19200，9600，4800，2400，1200) ZMODEM 手順 CD-ROM(ISO-9660) ※
	RM シリアル接続 (モデム)	RS232C(回線速度：9600)
リモート運用端末	通信用ポート接続 (NIF 接続)	TCP/IP telnet または rlogin ftp CD-ROM(ISO-9660) ※

注※ 本端末を使用してソフトウェアの入れ替えを行う場合に必要です。

(1) コンソール

コンソールは RM シリアル接続 (RS232C) と RM シリアル接続 (モデム) があります。RM シリアル接続 (RS232C) の本装置のシリアルインタフェースは D-Sub9 ピンです。コンソールと接続する場合にはクロスケーブルを使用してください。例えば，AT 互換機と本装置を接続する場合には，AT 互換機同士をシリアルで接続するための D-Sub9 ピンクロスケーブルを使用してください。クロスケーブルの結線仕様を次の図に示します。

図 8-2 クロスケーブルの結線仕様

本装置側9ピン(メス)		接続	セットアップ端末側9ピン(メス)	
ピン番号	信号名		ピン番号	信号名
5	SG		5	GND
3	SD		2	RX
2	RD		3	TX
7	RS		1	DCD
8	CS		8	CTS
1	CD		7	RTS
6	DR		4	DTR
4	ER		6	DSR

RM シリアル接続 (モデム) およびダイアルアップ IP 接続のコンソールを本装置の RM シリアルインタフェースにモデムを接続する場合には，AT 互換機とモデムを接続するためのストレートケーブルを使用してください。また，本装置に接続するモデムは自動着信に設定してください。本装置ではモデムを設定できないので，PC などに接続して設定してください。

8.2 立ち上げ

本章は本装置の立ち上げについての仕様および使用する上での注意点を中心に説明します。

8.2.1 立ち上げおよび再起動

(1) 立ち上げ

本装置は，まず MC から RM 用ソフトウエアをローディングして RM の運用を開始したあとで，RP の運用を開始します。2 枚の MC がスロットに実装されている場合は，一方のスロット (通常はスロット 0) で立ち上げを行いますが，起動に失敗したときには自動的に他方 (通常はスロット 1) での立ち上げに切り替わります。また，RP の運用開始には RP 初期導入と定常運用の 2 種類の立ち上げ処理があり，それぞれで動作が異なります。

(a) RP 初期導入

本装置では RP 導入時に RP のフラッシュメモリにソフトウェアが書き込まれていない場合，または現在の運用バージョンと異なるバージョンのソフトウェアが書き込まれている場合は，自動的に RP 用ソフトウェアを同 RP に書き込みます。書き込まれたソフトウェアは通常 RP の障害が発生しないかぎり消えることはありません。この書き込み処理のために RP のフラッシュメモリ上のソフトウェアで起動する定常運用時よりも初期化時間が長くかかります。装置として初期化にかかる時間は RP の実装枚数に依存します。

(b) 定常運用

定常運用状態での立ち上げは，RP 初期導入時に行う RP へのソフトウェアの書き込み処理がないため，個々の RP は独立して初期化処理を行います。初期化にかかる時間は RP の実装枚数にほとんど影響を受けません。

(2) 再起動

本装置の再起動には管理者が手動で行う再起動と装置が自立して行う自動再起動があります。

(a) マニュアル再起動

管理者はコマンドを使用するか，装置上のリセットスイッチを操作することで本装置の再起動を行えます。

(b) 障害回復による再起動

本装置に重度の障害が発生した場合は，装置は自動的に障害復旧のために再起動を行います。詳細は「8.10　障害時の復旧および情報収集」を参照してください。

8.2.2 自己診断テスト

本装置では立ち上げ時に，RM と RP で自己診断テスト (ハードウェアの診断) をします。ハードウェアに異常が発見された場合は FAULT CODE を表示し，ログを採取します。RM で障害を検出した場合，二重化構成の時は系を切り替えます。また，RP で障害を検出した場合，障害検出した RP 以外は立ち上がります。

8.3 ログイン制御

本装置にはローカルログイン (RS232C 接続) と IP および IPv6 ネットワーク経由のリモートログイン機能が (rlogin または telnet) あります。

8.3.1 ログイン制御

本装置ではログイン時およびログイン中に次に示す制御を行っています。

1. 複数の運用端末から同時にログインできます。
2. コマンド実行結果はログインした端末だけに表示します。運用メッセージはログインしているすべての運用端末に表示されます。
3. キー入力が 60 分間ない場合は自動的にログアウトします。
4. killuser コマンドを使用してユーザを強制ログアウトできます。
5. ログイン時に不正アクセスを防止するためパスワードによるチェックやユーザ ID によるコマンドの使用範囲の制限を設けています。
6. 入力したコマンドとその応答メッセージおよび運用メッセージを運用ログとして収集します。運用ログは show logging コマンドで参照できます。
7. ログインできるユーザ数は 5 ユーザです。
8. 構成定義情報でログインできるユーザ数を制限できます。
9. 本装置にアクセスできるプロトコル (telnet，rlogin，http，ftp) を構成定義情報で制限できます。

8.3.2 ログインセキュリティ制御

(1) ユーザ ID 管理

ユーザ ID を adduser コマンドで作成できます。また，rmuser コマンドで削除できます。

システムが二重化運用されている場合，待機系の現用 MC に自動的にアカウントの同期を行います。また，運用系および待機系に予備 MC が実装されている場合，確認後アカウントの同期を行います。

(2) パスワード管理

本装置ログイン時のコマンドレベルの制御およびセキュリティレベル機能としてパスワードによるアクセス権制御機能を持ちます。パスワードは管理端末から本装置を操作する場合のアクセス制限と認証に使用します。パスワードは password コマンドによって変更できるので，セキュリティのために，定期的に変更されることをお勧めします。

システムが冗長構成で運用されている場合，待機系の現用 MC に自動的にパスワードの同期を行います。また，運用系および待機系に予備 MC が実装されている場合，確認後パスワードの同期を行います。

(3) アクセスできる端末の制限

リモート運用端末から本装置へアクセス制限を行います。アクセスを許可するリモート運用端末の IP アドレスおよびサブネットマスク，または IPv6 アドレスおよびプレフィックスを構成定義情報に登録し，登録外の端末からの使用を防止します。なお，サブネットマスクおよびプレフィックスは省略できます。アクセス許可するアドレスは IP と IPv6 を合計して最大 128 個登録できます。なお，初期導入時にはリモート運用端末からのアクセスができない設定になっています。

(4) ルータ管理者

本装置では一般ユーザとルータ管理者とユーザのレベル分けを行っています。

- 一般ユーザ　：コマンドなどでルータの保守ができます。
- ルータ管理者：構成定義情報の編集やユーザの追加・削除が行えます。

一般ユーザは enable コマンド実行によってルータ管理者になります。また，ルータ管理者にもパスワードが設定および変更ができるので，password コマンドを使用してパスワードを設定し，定期的に変更されることをお勧めします。

8.4 構成定義

本装置にはネットワークの運用環境に合わせて，構成および動作条件などの構成定義情報を定義しておく必要があります。初期導入時は構成定義情報を定義していません。

8.4.1 構成定義情報

構成定義情報の項目を次の表に示します。

表 8-3 構成定義情報

情報グループ名	内容
ルータ管理情報	ルータ名，設置場所などの管理情報 リモート運用端末の IP アドレス，IPv6 アドレス定義
SNMP 情報	コミュニティ名，SNMP マネージャアドレスなどの SNMP セッションに関する定義 リアルタイムモニタに関する定義
回線 (Line，Subline) 情報	回線の種別，回線速度などのレイヤ 1 の定義
リンクレイヤプロトコル情報	PPP プロトコルやフレームリレープロトコルの各種パラメータ定義 (レイヤ 2 の情報)
トンネル情報	トンネルインタフェースに関する定義
IP インタフェース情報	IPv4 アドレスやスタティック ARP の定義 IPv6 アドレスやスタティック NDP，RA の定義 IP パケットフィルタリングに関する定義 Tag-VLAN 連携に関する定義 アドレス変換機能に関する定義
IP ルーティングプロトコル情報	RIP，OSPF，BGP，RIPng，OSPFv3，BGP4+，IS-IS のプロトコルに関する定義 スタティックルーティングに関する定義
IP マルチキャストルーティングプロトコル情報	PIM-DM，PIM-SM，DVMRP，IGMP のプロトコルに関する定義
フロー情報	フロー制御に関する定義
QoS 情報	最低帯域保証などのサービス品質保証 (QoS) に関する定義
IPX 情報	IPX プロトコルに関する定義
ブリッジ情報	ブリッジに関する定義
デフォルト情報	構成定義※での初期値に関する定義
VRRP 情報	VRRP に関する定義
RA 情報	RA に関する定義
ホスト名情報	ホスト名称に関する定義
ログ情報	ログの運用方法に関する定義
NTP 情報	NTP に関する定義
Disable 情報	H ／ W ボードの閉塞に関する定義

注※ ルータ管理情報，SNMP 情報，回線 (Line，Subline) 情報，リンクレイヤプロトコル情報，トンネル情報，IP インタフェース情報，IP ルーティングプロトコル情報，IP マルチキャストルーティングプロトコル情報，フロー情報の各構成定義を示します。

8.4.2 構成定義情報ファイルの種類

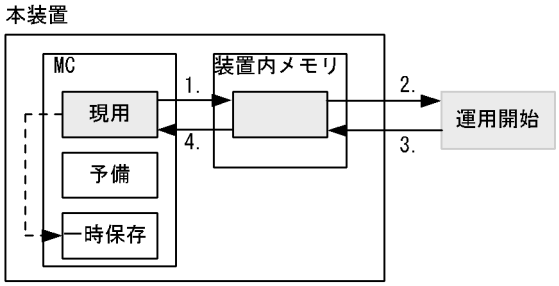
本装置は通信ポート中継機能の動作条件などを構成定義情報としてテキストファイル形式で MC に記憶します。構成定義情報には次に示すファイルの種類があります。

- **現用構成定義情報ファイル**
  本装置の立ち上げ時に使用し，その構成定義情報に従って運用されます。
- **予備構成定義情報ファイル**
  現用構成定義情報ファイルのコピーまたは将来のネットワークの変更に備えた編集用構成定義情報として利用します。
  予備構成定義情報ファイルは MC の中に複数記憶できますが，MC の残容量によって記憶できる量が変わります。予備構成定義情報ファイルを作成する前に運用コマンドの show mc コマンドを使用して MC の残容量を確認してください。
- **一時保存構成定義情報ファイル**
  運用中に構成定義を変更して MC に格納した場合に，編集前の現用構成定義情報ファイルを一時保存したファイルです。
  本装置の電源投入時，現用構成定義情報ファイルが正しく読み出せない場合は，一時保存構成定義情報ファイルで運用を開始します。

8.4.3 構成定義情報の運用方法

構成定義情報の運用方法を次の図に示します。

図 8-3 構成定義情報の運用方法



1. 本装置を起動すると，MC内の現用構成定義情報ファイルの内容が装置内メモリにロードされる。
2. 装置内メモリの内容で運用を開始する。
3. 構成定義情報が変更された場合は，装置内メモリの構成定義情報を編集する。
4. 変更された構成定義情報をMCに格納する。このとき，編集前の現用構成定義情報ファイルの内容を一時保存構成定義情報ファイルとして保存する。

MC 故障に備えてリモート端末に構成定義情報ファイルのバックアップを取ることをお勧めします。本装置は MC1 枚でも運用できますが，運用中に MC が故障した場合には，リモート装置にアクセスするための構成定義情報の設定，バックアップ構成定義情報ファイルの転送などに時間がかかり，迅速に復旧できません。迅速に復旧させるために MC は 2 枚で運用することをお勧めします。

MC を 2 枚で運用した場合，構成定義情報を編集したあとに必ず運用コマンドの copy mc コマンドを使用して，現用スロットから予備スロットにコピーすることをお勧めします。これは，本装置は MC 故障時にブートする MC を自動的に切り替えることができますが，現用スロットの構成定義情報ファイルより予備スロットの構成定義情報ファイルが古い場合には，故障後に古い構成定義情報に従って運用するためです。

8.4.4 構成定義情報の表示と編集

(1) 表示

構成定義コマンドの show コマンドで構成定義情報を表示できます。また，MC に格納した構成定義情報ファイルは運用コマンドの cat コマンドで表示することもできます。

(2) 編集

本装置は導入時および運用中のネットワーク構成変更時に使用する構成定義情報の編集機能を持ちます。現用／予備構成定義情報共に同一の操作で編集できます。編集はコンソールからだけでなく，導入後には IP ／ IPv6 ネットワークで接続したリモート運用端末からでも行えます。

8.5 運用コマンド

本装置で使用できる運用コマンドとその用途を次の表に示します。各コマンドの詳細は，マニュアル「運用コマンドレファレンス Vol.1」および「運用コマンドレファレンス Vol.2」を参照してください。

表 8-4 運用コマンドとその用途

分類	コマンド名	用途
モード切換	cli	CLI の起動
	enable	ルータ管理者へのモード変更
	disable	ルータ管理者モード終了
	quit(exit)	現在のユーザモード，コマンド入力モード終了
	logout	装置ログアウト
	configure(configure terminal)	構成定義コマンドモード開始
	end	構成定義コマンドモード終了
ログインユーザ管理	adduser	新規ユーザの追加
	rmuser	ユーザの削除
	password	パスワード設定・変更
	clear password	パスワード削除
	show sessions	ログインしている全ユーザの表示
	show whoami	ログインしている自ユーザの表示
	killuser	指定ユーザの強制ログアウト
ターミナル	set terminal warning-level	「警告があることを示すメッセージ」出力レベル設定
	set exec-timeout	「自動ログアウト」実行までの時間設定
	set terminal command-literal	CLI 運用コマンドコマンド入力モード変更
	set terminal help	ヘルプメッセージに表示するコマンド一覧の設定
	set terminal pager	ページング処理の有無設定
	show history	コマンド履歴表示
	stty	端末属性表示
リモート操作	telnet	他装置への遠隔ログイン
	rlogin	他装置への遠隔ログイン
	ftp	ファイル転送
ソフトウェア管理	show version	バージョン表示
	ppupdate	ソフトウェアのバージョンアップ
	ftpbackup	ftp サーバへのソフトウェア保存
	ftprestore	ftp サーバからのソフトウェア回復
	synchronize	MC の内容をコピー
MC 保守	copy mc	MC のコピー
	format mc	MC の初期化
	show mc	MC の情報表示
	set mc disable	MC のアクセス禁止
	set mc enable	MC のアクセス禁止解除

分類	コマンド名	用途
ファイル操作	show running-config (show configuration)	運用構成定義情報表示
	show startup-config	現用構成定義情報表示
	copy running-config	運用構成定義情報コピー
	erase startup-config	現用構成定義情報全削除
	cd	カレントディレクトリ移動
	pwd	カレントディレクトリのパス名の表示
	ls	ディレクトリ内容の表示
	dir	MC ファイルの表示
	cat	ファイルの連結・出力
	cp	ファイルのコピー
	mkdir	ディレクトリの作成
	mv	ファイルの移動，ファイル名の変更
	rm	ファイルの削除
	rmdir	ディレクトリの削除
	delete	回復可能な MC ファイルの削除
	undelete	回復可能な MC 上の削除ファイルの回復
	squeeze	回復可能な MC 上の削除ファイルの消去
	chmod	ファイルの許可モード変更
	zmodem	RS232C でのファイル転送
ユーティリティ	diff	テキストファイル間の行内容の相違表示
	grep	ファイルからのパターン検索
	egrep	ファイルからの拡張パターン検索
	fgrep	ファイルからの固定文字列検索
	more	テキストファイルの表示，ページング
	less	テキストファイルの表示，ページング
	vi	テキストエディタ
	sort	ファイルのソート
	tail	ファイルの最後の部分の表示
	hexdump	ヘキサダンプ表示
装置管理	show router	装置運用状態 / 統計情報表示
	clear counters router	本装置全体の統計情報カウンタクリア
	clear control-counter	リトライカウンタのクリア
	reload	再立ち上げ
	show tech-support	本装置の保守情報採取
RP/NIF 管理	close rp	RP 閉塞状態指示，活栓挿抜レジスタセット
	free rp	RP 閉塞状態解除，活栓挿抜レジスタ解除
	show nif	NIF 運用情報
	clear counters nif	統計情報カウンタクリア
	close nif	NIF 閉塞状態指示，活栓挿抜レジスタセット

分類	コマンド名	用途
	free nif	NIF 閉塞状態解除，活栓挿抜レジスタ解除
メッセージ・ログ	show logging	運用ログ表示
	clear logging	運用ログ消去
	show logging console	システムメッセージレベル表示
	set logging console	システムメッセージレベル設定
	show warning	警告メッセージ表示
リソース情報	show rm cpu	RM CPU 使用率表示
	show rp cpu	RP CPU 使用率 / バッファ使用率表示
	show rp buffer	RP バッファ統計情報表示
	clear rp buffer	RP バッファ統計情報カウンタクリア
	show processes	プロセス情報表示
	show memory	メモリ情報表示
	df	ディスクの空き容量表示
	du	ディスクの使用容量表示
RP 保守情報	show trace	RP トレース表示
	debug trace	RP トレース採取開始
	no debug trace	RP トレース採取停止
	clear trace	RP トレース削除
	show registor	RP レジスタ内容表示
	set registor	RP レジスタ内容設定
ダンプ情報	dump rp	RP ダンプ採取
	dump nif	NIF ダンプ採取
	set dump	RP ダンプ採取範囲設定
	show dump status	RP ダンプ採取範囲表示
	erase dumpfile	ダンプファイル消去
時刻管理	show calendar	日付・時間の表示
	set calendar	日付・時間の設定
	rdate	日付・時間をリモートホストから設定
	show ntp status	ntp サーバの状態表示
	restart ntp	ntp サーバの再初期化
MIB 情報	snmp lookup	サポート MIB オブジェクト名称およびオブジェクト ID を表示
	snmp get	指定した MIB の値を表示
	snmp getnext	指定した次の MIB の値を表示
	snmp walk	指定した MIB ツリーを表示
	snmp getif	interface グループの MIB 情報を表示
	snmp getroute	ipRouteTable（IP ルーティングテーブル）を表示
	snmp getarp	ipNetToMediaTable（IP アドレス変換テーブル）を表示

分類	コマンド名	用途
	snmp getforward	ipForwardTable および grVpnIpForwardTable（IP フォワーディングテーブル）を表示
	snmp rget	指定したリモート装置の MIB の値を表示
	snmp rgetnext	指定したリモート装置の次の MIB の値を表示
	snmp rwalk	指定したリモート装置の MIB ツリーを表示
	snmp rgetroute	指定したリモート装置の ipRouteTable（IP ルーティングテーブル）を表示
	snmp rgetarp	指定したリモート装置の ipNetToMediaTable（IP アドレス変換テーブル）を表示
イーサネット	show interfaces	回線運用状態 / 統計情報表示
	clear counters	回線統計情報カウンタクリア
	close	閉塞状態指示
	free	閉塞状態解除
	show vlan	Tag-VLAN 連携統計表示
	show vlans	Tag-VLAN 連携統計表示
	clear counters	Tag-VLAN 連携回線の統計情報カウンタクリア
	clear-vlan statistics	Tag-VLAN 連携統計情報カウンタクリア
	test interfaces	回線テスト開始
	no test interfaces	回線テスト終了
イーサネット (PPPoE)	show interfaces	回線運用状態 / 統計情報表示
	clear counters	回線統計情報カウンタクリア
	close	閉塞状態指示
	free	閉塞状態解除
	show trace pppoe	PPPoE フレームトレース表示
	clear trace pppoe	PPPoE フレームトレース削除
WAN(物理インタフェース)	show interfaces	回線運用状態 / 統計情報表示
	clear counters	回線統計情報カウンタクリア
	close	閉塞状態指示
	free	閉塞状態解除
	show statistics	WAN 回線使用率情報表示
	execute statistics	WAN 回線使用率情報収集開始
	no execute statistics	WAN 回線使用率情報収集停止
	clear statistics	WAN 回線使用率情報カウンタクリア
	show trace wanframe	WAN フレームトレース表示
	debug trace wanframe	WAN フレームトレース採取開始
	no debug trace wanframe	WAN フレームトレース採取停止
	clear trace wanframe	WAN フレームトレース削除
	show trace wancontrol	WAN レイヤ 2 制御フレームトレース表示
	debug trace wancontrol	WAN レイヤ 2 制御フレームトレース採取開始

分類	コマンド名	用途
	no debug trace wancontrol	WAN レイヤ 2 制御フレームトレース採取停止
	clear trace wancontrol	WAN レイヤ 2 制御フレームトレース削除
	test interfaces	回線テスト開始
	no test interfaces	回線テスト終了
WAN(フレームリレー)	show frame-relay	フレームリレー運用状態 / 統計情報表示
	clear counters	回線統計情報カウンタクリア
	close	閉塞状態指示
	free	閉塞状態解除
	ping frame-relay	フレームリレーエコーテスト
WAN(ISDN)	show interfaces	回線運用状態 / 統計情報表示
	show isdn-pool	ISDN プール運用状態 / 統計情報表示
	show peer	通信相手運用状態 / 統計情報表示
	clear counters	回線統計情報カウンタクリア
	close peer	閉塞状態指示
	free peer	閉塞状態解除
	show trace wanframe	D-ch フレームトレース表示
	debug trace wanframe	D-ch フレームトレース採取開始
	no debug trace wanframe	D-ch フレームトレース採取停止
	clear trace wanframe	D-ch フレームトレース削除
	show trace wanpeer	通信相手単位フレームトレース表示
	debug trace wanpeer	通信相手単位フレームトレース採取開始
	no debug trace wanpeer	通信相手単位フレームトレース採取停止
	clear trace wanpeer	通信相手単位フレームトレース削除
	show trace wancall	発呼契機フレームトレース表示
	show isdn history	ISDN 履歴情報表示
	clear isdn history	ISDN 履歴情報削除
ATM	show interfaces	回線運用状態 / 統計情報表示
	show atm	ATM 回線運用状態 / 統計情報表示
	clear counters	統計情報カウンタクリア
	close	閉塞状態指示
	free	閉塞状態解除
	ping atm	OAM F5 ループバックテスト
	show trace atmvc	ATM トレース表示
	debug trace atmvc	ATM トレース採取開始
	no debug trace atmvc	ATM トレース採取停止
	clear trace atmvc	ATM トレース削除
	test interfaces	回線テスト開始
	no test interfaces	回線テスト終了
IP ネットワーク情報	show ip-dual interface	ネットワークインタフェース・パラメータの表示

分類	コマンド名	用途
	show ip interface	IPv4 ネットワークインタフェース・パラメータの表示
	show ipv6 interface	IPv6 ネットワークインタフェース・パラメータの表示
	clear counters null-interface	NULL インタフェース廃棄パケット数カウンタクリア
	ping	エコーテスト
	ping ipv6	ICMP6 エコーテスト
	traceroute	ルート表示
	traceroute ipv6	IPv6 経由ルータの表示
	show ip arp	ARP 表示
	clear arp-cache	ARP 削除
	show ipv6 neighbors	NDP 表示
	clear ipv6 neighbors	ダイナミック NDP 情報クリア
	show netstat (netstat)	ネットワークのステータス表示
	clear netstat	ネットワーク統計情報カウンタクリア
	clear tcp	TCP コネクションの切断
	show vrrpstat	VRRP の運用状態表示
	clear vrrpstat	VRRP の統計情報カウンタクリア
	show ip policy	ポリシールーティング条件定義済み Filter リスト番号表示
	show ip local policy	ポリシールーティング条件，出力先情報表示
	show ip cache policy	ポリシーグループ情報の表示
	show dhcp traffic	DHCP サーバの統計情報の表示
	clear dhcp traffic	DHCP サーバの統計情報カウンタクリア
	show dhcp giaddr	インタフェースに対する giaddr 情報の表示
	show ip dhcp binding	DHCP サーバの結合情報表示
	clear ip dhcp binding	DHCP サーバの結合情報削除
	show ip dhcp import	DHCP サーバのオプション情報表示
	show ip dhcp conflict	DHCP サーバ検出の矛盾アドレス表示
	clear ip dhcp conflict	DHCP サーバの矛盾アドレス情報削除
	show ip dhcp server statistics	DHCP サーバの統計情報表示
	clear ip dhcp server statistics	DHCP サーバの統計情報カウンタクリア
	show dhcp lease	DHCP クライアントのリース情報表示
	show ip dhcp client statistics	DHCP クライアントの統計情報表示
	clear ip dhcp client statistics	DHCP クライアントの統計情報カウンタクリア
	dhcp server monitor	DHCP サーバパケット送受信ログ採取開始
	no dhcp server monitor	DHCP サーバパケット送受信ログ採取終了
	restart dhcp	DHCP サーバプログラム再起動

分類	コマンド名	用途
	restart dhcp client	DHCP クライアントプログラム再起動
	dump protocols dhcp	DHCP 情報のダンプ
	show dns-relay	DNS リレーの動作状況表示
	clear counters dns-relay	DNS リレーのエラー統計情報カウンタクリア
	show ip sat	アドレス変換情報表示
	clear ip sat	アドレス変換情報統計情報カウンタクリア
	show filter-flow	フィルタ IP フロー統計情報表示
	clear filter-flow	フィルタ IP フロー統計情報カウンタクリア
	show ip nat statistics	NAT 統計情報表示
	clear ip nat statistics	NAT 統計情報カウンタクリア
	show ip nat log	NAT 変換ログ表示
	clear ip nat log	NAT 変換ログ削除
	show ip nat translations	NAT バインディング情報表示
	clear ip nat translation	NAT バインディング情報削除
IP ユニキャストルーティングプロトコル情報	show ip route	すべての経路の一覧表示
	clear ip route	経路情報の再インストール，再評価
	show ip entry	特定経路の詳細情報の表示
	show ip rip	RIP プロトコル情報の表示
	clear counters rip ipv4-unicast	RIP プロトコル情報のクリア
	show ip ospf	OSPF プロトコル情報の表示
	clear ip ospf	OSPF プロトコル情報のクリア
	show ip bgp	BGP プロトコル情報の表示
	clear ip bgp	BGP プロトコル情報のクリア BGP 経路の再広告・再学習
	show isis	IS-IS プロトコル情報の表示
	clear isis	IS-IS プロトコル情報のクリア
	debug isis	IS-IS ルーティング・パケットのリアルタイム表示の制御
	show ip static	static 経路情報の表示
	clera ip static-gatewayclear ip static-gateway	static 経路情報のクリア
	show ip vpn	VPN サイト情報の表示
	show ip interface ipv4-unicast	IP ルーティングプログラムが認識するインタフェース情報の表示
	show processes memory ipv4-unicast	IP ルーティングプログラムのメモリ使用状況の表示
	show processes cpu ipv4-unicast	IP ルーティングプログラムの CPU 使用率表示
	show processes task ipv4-unicast	IP ルーティングプログラムのタスク情報の表示

分類	コマンド名	用途
	show processes timer ipv4-unicast	IP ルーティングプログラムのタイマ情報の表示
	debug protocols ipv4-unicast	IP ルーティングプログラムのイベントログ情報表示の開始
	no debug protocols ipv4-unicast	IP ルーティングプログラムのイベントログ情報表示の停止
	debug ip	IP ルーティング・パケットのリアルタイム表示の制御
	restart ipv4-unicast	IP ルーティングプログラムの再起動
	dump protocols ipv4-unicast	IP ルーティングプログラムの制御テーブル情報・イベントトレース情報のダンプ採取
	erase protocol-dump ipv4-unicast	IP ルーティングプログラムの制御テーブル情報・イベントトレース情報・コア情報のダンプ削除
IP マルチキャストルーティングプロトコル情報	show ip mcache	マルチキャスト経路情報の表示
	show ip mstatic	マルチキャスト静的グループ加入情報の表示
	show ip pim	PIM プロトコル情報の表示
	show ip mroute	PIM-SM マルチキャストルート情報
	show ip igmp	IGMP プロトコル情報の表示
	show ip dvmrp	DVMRP プロトコル情報の表示
	show ip rpf	RPF 情報の表示
	restart ipv4-multicast	IP マルチキャストルーティングプログラムの再起動
	dump protocols ipv4-multicast	IP マルチキャストルーティングプログラムの制御テーブル情報・イベントトレース情報のダンプ採取
	erase protocol-dump ipv4-multicast	IP マルチキャストルーティングプログラムの制御テーブル情報・イベントトレース情報・コア情報のダンプ削除
IPv6 ユニキャストルーティングプロトコル情報	show ipv6 route	すべての経路の一覧表示
	clear ipv6 route	経路情報の再インストール，再評価
	show ipv6 entry	特定経路の詳細情報の表示
	show ipv6 rip	RIPng プロトコル情報の表示
	clear counters rip ipv6-unicast	RIPng プロトコル情報のクリア
	show ipv6 ospf	OSPFv3 プロトコル情報の表示
	clear ipv6 ospf	OSPFv3 プロトコル情報のクリア
	show ipv6 bgp	BGP4+ プロトコル情報の表示
	clear ipv6 bgp	BGP4+ プロトコル情報のクリア BGP4+ 経路の再広告・再学習
	show isis	IS-IS プロトコル情報の表示
	clear isis	IS-IS プロトコル情報のクリア
	show ipv6 static	static 経路情報の表示
	clear ipv6 static-gateway	static 経路情報のクリア

分類	コマンド名	用途
	show ipv6 routers	RA 情報の表示
	show ipv6 interface ipv6-unicast	IPv6 ルーティングプログラムが認識するインタフェース情報の表示
	show processes memory ipv6-unicast	IPv6 ルーティングプログラムのメモリ使用状況の表示
	show processes cpu ipv6-unicast	IPv6 ルーティングプログラムの CPU 使用率の表示
	show processes task ipv6-unicast	IPv6 ルーティングプログラムのタスク情報の表示
	show processes timer ipv6-unicast	IPv6 ルーティングプログラムのタイマ情報の表示
	restart ipv6-unicast	IPv6 ルーティングプログラムの再起動
	debug protocols ipv6-unicast	IPv6 ルーティングプログラムのイベントログ情報表示開始
	no debug protocols ipv6-unicast	IPv6 ルーティングプログラムのイベントログ情報表示終了
	debug ipv6 packet-monitor	IPv6 ルーティング・パケットのリアルタイム表示の制御
	dump protocols ipv6-unicast	IPv6 ルーティングプログラムの制御テーブル情報・イベントトレース情報のダンプ採取
	erase protocol-dump ipv6-unicast	IPv6 ルーティングプログラムの制御テーブル情報・イベントトレース情報・コア情報のダンプ削除
IPv6 マルチキャストルーティングプロトコル情報	show ipv6 mcache	IPv6 マルチキャスト経路情報表示
	show ipv6 pim	IPv6 PIM プロトコル情報表示
	show ipv6 mroute	IPv6 PIM-SM マルチキャスト経路情報表示
	show ipv6 mld	IPv6 MLD プロトコル情報の表示
	show ipv6 rpf	RPF 情報の表示
	restart ipv6-multicast	IPv6 マルチキャストルーティングプログラムの再起動
	dump protocols ipv6-multicast	IPv6 マルチキャストルーティングプログラムの制御テーブル情報のダンプ採取
	erase protocol-dump ipv6-multicast	IPv6 マルチキャストルーティングプログラムの制御テーブル情報・コア情報のダンプ削除
QoS 情報	show qos ip-flow	QoS IP フロー統計情報表示
	clear qos ip-flow	QoS IP フロー統計情報カウンタクリア
	show qos flow	IPX，ブリッジ，HDLC パススルー，特殊 IP フロー統計情報表示
	clear qos flow	IPX，ブリッジ，HDLC パススルー，特殊 IP フロー統計情報カウンタクリア
	show qos queueing	出力インタフェースの優先度キューごとの統計情報表示
	clear qos queueing	出力インタフェースの優先度キューごとの統計情報カウンタクリア
IPX 情報	show ipx route	IPX ルーティング情報の表示
	show ipx servers	IPX サーバ情報の詳細表示

分類	コマンド名	用途
	show ipx interface	IPX ルーティングプログラムに関連するインタフェース情報の表示
	show ipx traffic	IPX ルーティングプログラムの統計情報の表示
	clear ipx traffic	IPX ルーティングプログラムの統計情報カウンタクリア
	restart ipx	IPX ルーティングプログラムの再起動
	ping ipx	IPX 経路情報疎通確認
	dump protocols ipx	IPX ルーティングプログラムの制御情報のダンプ
	ipx monitor	IPX ルーティングプログラムのイベントログ情報表示開始
	no ipx monitor	IPX ルーティングプログラムのイベントログ情報表示終了
ブリッジ情報	show spanning-tree	スパニングツリー情報の表示
	show bridge fdb	フィルタリングデータベース情報の表示
	show bridge interface	ブリッジプログラムに関連するインタフェース情報の表示
	show bridge traffic	ブリッジの統計情報の表示
	clear bridge traffic	ブリッジの統計情報カウンタクリア
	restart bridge	ブリッジプログラムの再起動
	dump protocols bridge	ブリッジプログラムの制御情報のダンプ
	bridge monitor	ブリッジプログラムのイベントログ情報表示開始
	no bridge monitor	ブリッジプログラムのイベントログ情報表示停止

8.6 MC

本装置では本装置のソフトウェアおよび構成定義情報を MC に保持します。装置起動時はこのカードからソフトウェアをローディングし，構成定義情報に従って装置を初期化します。

8.6.1 バックアップ MC の運用

MC で運用中に MC の故障が発生した場合には，本装置を起動できなくなります。また，MC の故障の状態によっては構成定義情報の再入力が必要になる場合があります。本装置では同一内容の 2 枚の MC を用意して BCU のスロット 0，スロット 1 の両方のスロットにそれぞれ MC を挿入して運用することで，一方の MC 障害時には自動的に装置がブートする MC を切り替えることができます。これによって，迅速な運用を再開できます。ただし，この場合に現用 MC と予備 MC の構成定義情報が不一致だと運用に支障をきたすので，常に copy mc コマンドでコピーしておくことをお勧めします。この時ログ情報なども copy mc コマンドを実行したときの時点の状態を予備 MC に保存できます。

8.6.2 MC 保守コマンド

次に示すコマンドで MC を保守できます。サポートする保守機能を次に示します。

- MC のコピー　　：copy mc コマンド
- MC の初期化　　：format mc コマンド
- MC の情報表示　　：show mc コマンド
- MC のアクセス禁止　：set mc disable コマンド
- MC のアクセス禁止解除：set mc enale コマンド

8.7 管理情報の収集

8.7.1 時計および時刻情報

1. set calendar コマンドで現在の時刻を表示および設定ができます。
2. rdate コマンドで現在の時刻の設定をできます。rdate コマンドは遠隔のホストから時刻を得て，その時刻を本装置に設定するコマンドです。
3. NTP プロトコルを使用して，ネットワーク上の NTP サーバと時刻同期を行えます。本装置は RFC1305 NTP バージョン 3 に準拠しています。

8.7.2 装置およびインタフェース状態表示

(1) 管理情報表示コマンド

本装置の管理情報を表示する主な管理情報表示コマンドと表示する管理情報を次の表に示します。各コマンドの詳細についてはマニュアル「運用コマンドレファレンス Vol.1」および「運用コマンドレファレンス Vol.2」を参照してください。

表 8-5 管理情報表示コマンドと表示する管理情報

コマンド名	用途	表示する管理情報
show ip interface show ipv6 interface show ip-dual interface	IP インタフェースの状態および各インタフェースに対応するメディアの情報を表示します。	• インタフェース名 • インタフェースのステータス • IP アドレス • IPv6 アドレス • サブネットマスク • MAC アドレス
show router show nif show interfaces show frame-relay show isdn-pool show peer show atm	router，nif，line など，本装置について指定された部位ごとの情報を表示します。	• 装置構成 • 装置 (部位) のステータス 表示項目は指定単位によって異なります。
show version	本装置に実装されているボードとソフトウェアについての情報を表示します。	• 実装されているボードの型名 • インストールされているソフトウェアのバージョン

(2) 装置の状態情報

装置の部位ごとの状態情報を次の表に示します。これらの管理情報は show router コマンド，show interfaces コマンド，show frame-relay コマンド，show isdn-pool コマンド，show peer コマンドおよび show nif コマンドで確認できます。

表 8-6 装置の部位ごとの状態情報

部位	状態情報	
	ステータス名称	意味
電源	active	運用中
	fault	障害
	disconnect	未実装

部位	状態情報	
	ステータス名称	意味
RM	active	運用系として運用中
	standby	待機系として運用中
	fault	障害中
	close	コマンド閉塞中
	disconnect	未実装
	configuration discord	構成定義情報不一致によって運用系と非同期中
	software version discord	ソフトウェアバージョン不一致によって運用系と非同期中
RM イーサネット接続ポート	active	運用中
	fault	障害中
	unused	未使用（構成定義情報未設定）
	test	回線テスト中
RP	active	運用中
	initialize	初期化中
	fault	障害中
	close	コマンド閉塞中
	unused	未使用（構成定義情報未設定）
NIF	active	運用中
	initialize	初期化中
	fault	障害中
	closed	コマンド閉塞中
	unused	未使用（構成定義情報未設定）
	mismatch	構成定義情報不一致
	locked	構成定義で運用停止中
Line	active up	運用中（正常動作中）
	active down	運用中（ネットワーク障害発生中）
	initialize	初期化中
	test	回線テスト中
	looped by remote	相手要求によりループ中
	fault	障害中
	closed	コマンド閉塞中
	unused	未使用（構成定義情報未設定）
	mismatch	構成定義情報不一致

8.7.3 統計情報

本装置では運用に必要な情報を統計情報として取得します。統計情報は show rm cpu コマンド，show rp cpu コマンドで本装置の CPU 使用率，show rp buffer コマンドでバッファ使用率などを取得できます。また，show router コマンド，show interfaces コマンド，show nif コマンド，show frame-relay コマンド，show isdn-pool コマンドおよび show peer コマンドで各ネットワークインタフェースのトラフィックカウ

ント，エラーカウントなどを参照できます。また，これらの情報はSNMPのMIB情報として参照することもできます。

8.7.4 運用メッセージおよび運用ログ

本装置は動作情報や障害情報などを運用メッセージとして通知します。同メッセージは運用端末に出力するほか，運用ログとして装置内に保存します。この情報で装置の運用状態や障害の発生を管理できます。運用ログは装置運用中に発生した事象（イベント）を発生順に記録したログ情報で，運用メッセージと同様の内容が格納されます。

種別ログは装置内で発生した障害や警告についての情報をメッセージIDごとに分類した上で，同事象が最初に発生した日時および最後に発生した日時と累積回数をまとめた情報です。

運用ログに格納する情報には次に示すものがあります。

- オペレータの操作および応答メッセージ
- 運用メッセージ
- ルーティングプログラムのイベント情報
- SNMPのイベント情報

これらのログは装置内にテキスト形式で格納しています。管理者はこれらの情報を，表示コマンドで参照できます。また，必要に応じてMCに格納したあとにファイルとして扱うこともできます。

8.8 LED および FAULT CODE の表示

本装置には装置の状態を示すために LED ランプ（以降 LED と略す）と 7 セグメント表示器による FAULT CODE を使用しています。LED および FAULT CODE の仕様について示します。

8.8.1 LED

LED ランプは装置のパネル面にあり，障害状態（赤・黄）と，動作状態表示（緑）およびネットワーク障害について表示します。LED の表示内容を次の表に示します。なお，LED の表示詳細については「ハードウェア取扱説明書」を参照してください。

表 8-7 LED の表示内容

機器種別	LED 名	状態
装置	STATUS(Ethernet)	内蔵イーサの動作状態を示す
	STATUS(RMP)	RMP の動作状態を示す
	POST	STATUS CODE が RM － CPU の初期診断コードを表示している状態を示す
	ALARM	装置障害発生を示す
	ERROR	装置の部分障害発生を示す
	READY	装置の動作可能状態を示す
	POWER	電源の投入状態を示す
	PRIMARY 0	MEM CARD 0 の状態を示す
	ACCESS 0	
	PRIMARY 1	MEM CARD 1 の状態を示す
	ACCESS 1	
	T ／ R	LINE の動作状態を示す
	LNK	
ネットワークインタフェース機構 (NIF) 共通	STATUS	NIF の動作状態を示す

8.8.2 FAULT CODE

FAULT CODE は 7 セグメント表示器で示す 10 進数のコードです。装置起動中の処理経過，または装置内で故障が発生した場合の故障部位をコードで示します。POST DISP LED が点灯中に表示されるコードは装置の初期診断の経過を示すもので，障害ではありません。また，RM の STATUS LED が緑点滅中に表示されるコードは装置の初期化処理経過を示すコードで，障害ではありません。FAULT CODE は ALARM LED または ERROR LED が点灯している場合に限って故障部位を示すコードになります。

8.9 ネットワーク障害切り分け機能

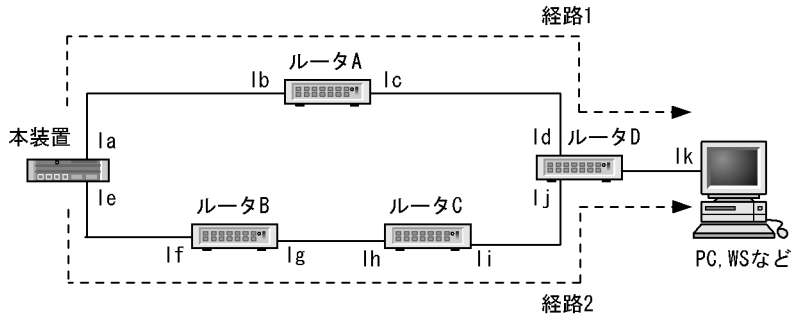
8.9.1 経路確認

経路確認コマンドとして，traceroute と traceroute ipv6 があります。

(1) traceroute コマンド

パケットの宛先の装置までの経路情報を確認するコマンドです。TTL(Time To Live) 値を 1 から順次増加したテスト用 IP パケットを送信して，経路途中のルータからの ICMP エラー応答を受け取ることで，宛先の装置までの経路情報を取得して，運用端末に表示します。このコマンドを使用してパケットの宛先の装置まで疎通確認できます。本装置から宛先の装置までの経路が複数あるような場合に，期待した経路で IP パケットが中継されるかどうかを確認するのに有効です。traceroute コマンドの使用例を次の図に示します。

図 8-4 traceroute コマンドの使用例



経路1でIPパケットが中継された場合：IPアドレスIb，Id，Ikと応答待ち時間を表示する
経路2でIPパケットが中継された場合：IPアドレスIf，Ih，Ij，Ikと応答待ち時間を表示する

(2) traceroute ipv6 コマンド

traceroute コマンドと同様の機能を持ち，IPv6 パケットの宛先の装置までの経路情報を確認するコマンドです。Hop Limit 値を 1 から順次増加したテスト用 IPv6 パケットを送信して，経路途中のルータからの ICMPv6 エラー応答を受け取ることで宛先の装置までの経路情報を取得し，運用端末に表示します。

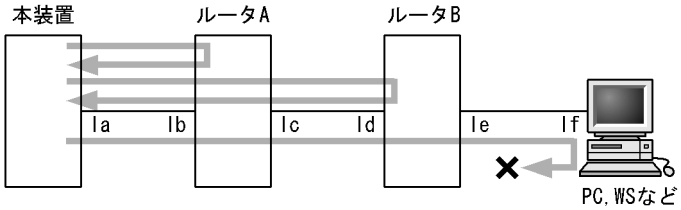
8.9.2 疎通テスト

疎通テスト確認のコマンドとして，ping，ping ipv6，ping ipx，ping frame-relay，ping atm があります。

(1) ping コマンド (ICMP エコー)

IP ネットワークでの障害切り分けに有効なコマンドです。このコマンドは指定した IP アドレスを持つ装置が ICMP エコーを返す機能を利用しています。宛先アドレスまでの経路途中のルータに対して順番に ping コマンドで疎通を確認していくことで，通信ができなくなっている範囲を絞り込むことができます。ping コマンドの使用例を次の図に示します。

図 8-5 ping コマンドの使用例



IPアドレスlb，ld，lfを宛先としてpingコマンドを実行したところ，lfからの応答がなかった。
この場合，ルータBのle，lfを持つ装置，le-lf間のネットワークに要因があると考えられる。

(2) ping ipv6 コマンド (ICMPv6 エコー)

ping コマンドと同様の機能を持ち，IPv6 ネットワークでの障害切り分けに有効なコマンドです。本コマンドは指定した IPv6 アドレスを持つ装置が ICMPv6 エコーを返す機能を利用しています。宛先アドレスまでの経路途中のルータに対して順番に ping ipv6 コマンドで疎通を確認していくことで，通信ができなくなっている範囲を絞り込むことができます。

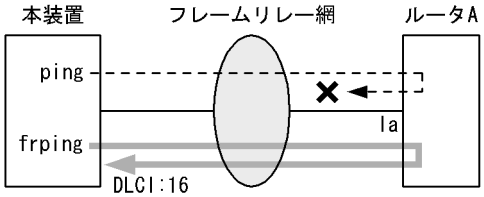
(3) ping ipx コマンド

NetWare プロトコルで接続する装置との間の疎通を確認するコマンドです。このコマンドは指定したネットワークアドレスおよびノードアドレスを持つ装置が IPX の ECHO パケットを返す機能を利用しています。ping コマンドと同じ使い方をすることで，通信ができなくなっている範囲を絞り込むことができます。

(4) ping frame-relay コマンド

フレームリレー網を介して接続する装置との間の疎通を確認するコマンドです。このコマンドは指定した DLCI の接続相手装置がフレームリレーの Inverse ARP 要求パケット受信に対し，Inverse ARP 応答パケットを返す機能を利用しています。また，同じ宛先の装置に対して ping コマンドとこのコマンドで疎通確認を行うことで，通信できない要因が IP レベルであるか，データリンクレイヤ以下 (フレームリレープロトコルでの相手装置との接続性，またはフレームリレー網) であるか切り分けることができます。ping frame-relay コマンドの使用例を次の図に示します。

図 8-6 ping frame-relay コマンドの使用例



IPアドレスlaを宛先としてpingコマンドを実行したところ，応答がなかった。
IPアドレスlaへのDLCI:16にping frame-relayコマンドを実行して応答がある場合はIPレベルに要因があり，逆にping frame-relayコマンドの応答がない場合はデータリンクレイヤ以下に要因があると考えられる。

(5) ping atm コマンド

ATM ネットワークを介して接続する装置との間の疎通を確認するコマンドです。このコマンドは指定した VC の接続相手装置が OAM Loopback セルを返す機能を利用しています。また，同じ宛先の装置に対し ping コマンドと本コマンドで疎通確認を行うことで，通信できない要因が IP レベルであるか，データリ

ンクレイヤ以下（ATM レイヤ以下での相手装置との接続性，または ATM ネットワーク）であるか切り分けることができます。

8.9.3 回線テスト

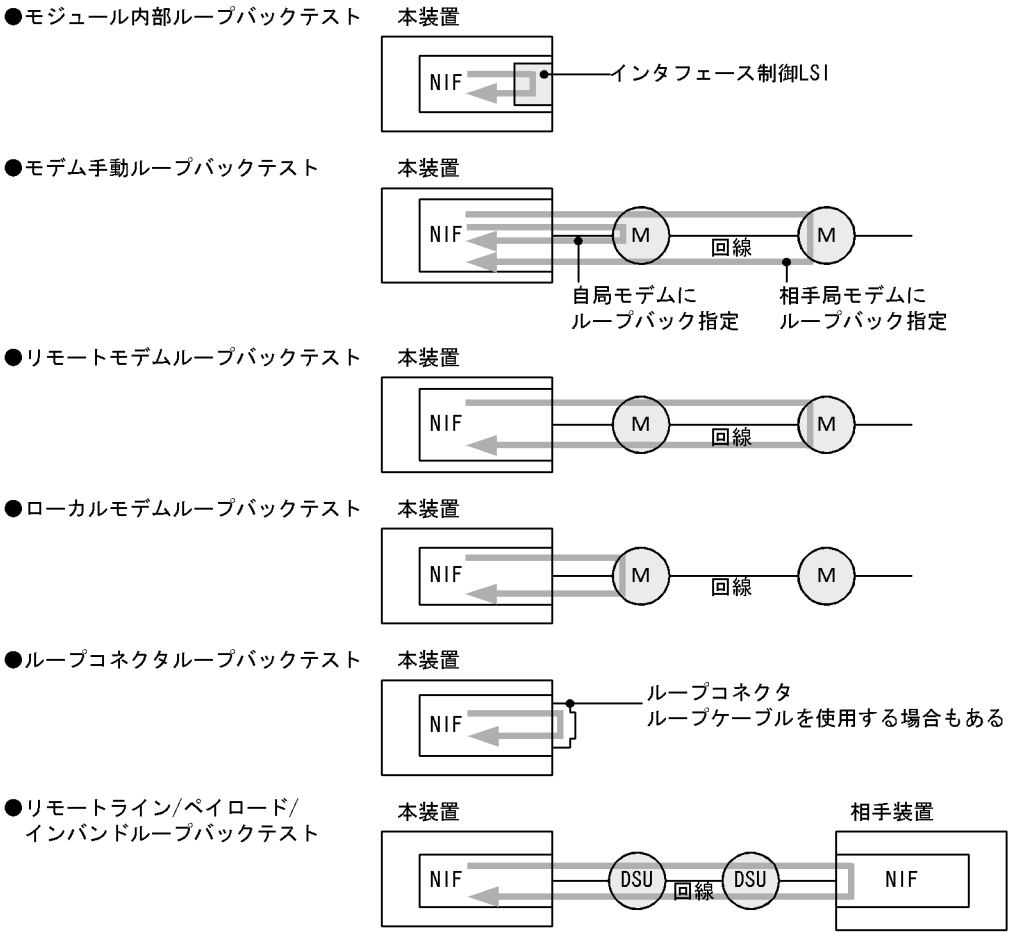
回線テストには次に示すコマンドを使用します。

- 回線テストの開始　　：test interfaces コマンド
- 回線テストの終了，およびその結果表示：no test interfaces コマンド

（1） test interfaces コマンド，no test interfaces コマンド

回線障害が発生した場合に，障害の要因が本装置にあるか，接続するネットワーク側にあるかを切り分けるコマンドです。ネットワークインタフェースの種別によってサポートするテスト種別が異なるので，詳細はマニュアル「運用コマンドレファレンス Vol.1」の test interfaces コマンド，no test interfaces コマンドを参照してください。テスト種別とテスト対象範囲を次の図に示します。

図 8-7　テスト種別とテスト対象範囲



8.9.4 トレース（フレームトレース）

フレームトレースに使用するコマンドを次に示します。

- 採取したフレームトレース情報の表示：show trace コマンド

- フレームトレース情報の採取開始　　：debug trace コマンド
- フレームトレース情報の採取の停止　：no debug trace コマンド
- 採取したフレームトレース情報の消去：clear debug trace コマンド

対象とするフレームは各ネットワークインタフェースに固有の制御フレームおよび一般の通信フレームです。主としてデータリンクレイヤのレベルでのネットワーク障害の切り分けのため，特定のフレームを採取してフレームのヘッダ情報などを確認する場合に有効です。収集対象とするフレームは各ネットワークインタフェースによって違いがあります。各ネットワークインタフェースについて主な収集フレームと指定方法を次の表に示します。

表 8-8　収集フレームと指定方法

ネットワークインタフェース	制御フレーム		通信フレーム	
	サポート	指定方法	サポート	指定方法
WAN	○	制御フレーム収集モードを指定	○	• タイムスロット • パターンとオフセット
ATM	○	Inverse ARP	×	―

（凡例）○：サポートする　―：該当なし

8.10 障害時の復旧および情報収集

本装置では運用中に障害が発生した場合は自動的に復旧処理を行います。障害部位に応じて復旧処理を局所化して行い，復旧処理による影響範囲を狭めることによって，正常運用部分が中断しないようにします。

8.10.1 障害部位と復旧内容

障害発生時，障害の内容によって復旧内容が異なります。障害部位と復旧内容を次の表に示します。

表 8-9 障害部位と復旧内容

障害部位	装置の対応	復旧内容	影響範囲
回線障害	自動復旧を無限回行います。	該当する回線の再初期化。	該当する回線を介する通信の中断。
ネットワークインタフェースボード障害(NIF)	自動復旧を 3 回／ 1Hr 行います。 障害継続中は 1 時間経過後に再度復旧処理を実行します。	該当する NIF の再初期化。	該当する NIF が収容する全回線を介する通信の中断。
ルーティング処理機構ボード障害(RP)	RP 初期化中の障害。 再初期化を 3 回行います。 復旧処理後も障害継続中の場合，障害要因によって次に示す対応を行います。 HardWare 障害の場合： 以降は停止 SoftWare 障害の場合： 1 時間経過後に再度復旧処理実行 なお，この障害での再初期化回数は，RP が運用状態に遷移した時点，または 1 時間経過後の復旧処理で初期化されます。	該当する RP の再初期化。	該当する RP が収容する全 NIF を介する通信の中断。
	RP 運用中の障害。 自動復旧を 3 回／ 1Hr 行います。 復旧処理後も障害継続中の場合，障害要因によって次に示す対応を行います。 HardWare 障害の場合： 以降は停止 SoftWare 障害の場合： 1 時間経過後に再度復旧処理実行 なお，この障害での自動復旧回数は，最初の障害発生から 1 時間経過後に初期化されます。	該当する RP の再初期化。	該当する RP が収容する全 NIF を介する通信の中断。
基本制御機構ボード障害 (BCU)	自動復旧を 7 回行います。 以降は停止。 1 時間以上運用時，自動復旧回数を初期化。	該当する BCU の再初期化。 なお，二重化されている場合は系交替による復旧処理を行います。	装置内の全回線を介する通信の中断。
装置筐体障害	停止。	装置再起動。	装置内の全回線を介する通信の中断。
電源機構障害 (PS)	停止。 なお，電源機構が冗長化されている場合は停止しません。	装置再起動。 なお，電源機構が冗長化されている場合は停止しません。	装置内全回線を介する通信の中断。 なお，電源機構が二重化されている場合は通信は中断しません。

8.10.2 ログ

障害発生時，障害の内容を機能別ログへ採取します。これによって障害の履歴を管理できます。障害の内容を把握すれば，障害に対する対策のほか，予防保守を行うための判断資料として使用します。

8.10.3 スイッチ

本装置にはリセットスイッチがあり，同スイッチを押して手動で装置の再起動を実行できます。通常，このスイッチを押す必要はありません。

8.10.4 メモリダンプ

本装置で RM や RP がリブートするなどの重度障害が発生した場合，障害の詳細調査に使用するために RM，RP および NIF のメモリダンプ情報を MC 上のダンプ専用ディレクトリにファイルとして格納します。

8.11 ソフトウェアのアップデート

本装置ではネットワーク接続したリモート運用端末またはコンソールからの操作で MC 内蔵のソフトウェアをアップデートできます。この機能はソフトウェアのインストールにも使用できます。

8.11.1 リモート運用端末からのソフトウェアのアップデート

ソフトウェアのアップデート機能を使用するためには前提条件として次のものが必要です。

- リモート運用端末
  TCP/IP ネットワーク接続要，CD-ROM 要，ftp 機能要
- 本装置のソフトウェア CD-ROM

8.11.2 コンソールからのソフトウェアのアップデート

ソフトウェアのアップデート機能を使用するためには前提条件として次のものが必要です。

- コンソール
  PC/AT 互換機，RS232C インタフェース要，CD-ROM 要，ZMODEM 手順サポートの通信プログラム要
- 本装置のソフトウェア CD-ROM

8.11.3 ソフトウェアアップデート時の注意事項

1. ソフトウェアのアップデートを行ったあと，装置を再起動するため，ネットワークの運用が一時停止します。
2. コンソールから ZMODEM 手順を使用してソフトウェアのアップデート／インストールを行うには長時間を必要とします。所要時間の詳細についてはソフトウェア添付資料をご参照ください。

8.12 ファイル属性

ファイルはファイルの所有者，所有者グループ，所有者・所有者グループ以外のその他についてそれぞれリード，ライト，実行の属性を持ちます。

これらの属性を使用して，例えば，所有者だけ読み書き可能とし，そのほかの者には読み書き不可にすれば，所有者以外への秘特性や所有者以外がファイルを誤って削除するなどを防止できます。

ファイルの所有者はファイルを作成したユーザとなります。所有者グループはファイルを作成したユーザが属するグループ名となります。ユーザ登録を行ったユーザのグループは user となります。所有者以外のユーザは所有者，所有者グループ以外のユーザを示します。

ファイルの属性は 1s コマンドで確認できます。また，属性は chmod コマンドで変更できます。

9 他機種との接続

この章では，システム構築時に検討が必要な他機種との接続について説明します。

9.1　イーサネットインタフェース

9.2　WAN インタフェース

9.3　ATM インタフェース

9.4　IP ルータとの接続

9.5　IPv6 ルータとの接続

9.6　SNMP マネージャとの接続

9.7　RADIUS サーバとの接続

9.1 イーサネットインタフェース

9.1.1 インタフェース種別の設定

本装置と他機種をイーサネットで接続する場合には次の点に注意してください。

(1) 10BASE-T/100BASE-TX 接続

次に示すように本装置の構成定義指定値と相手装置のインタフェース状態が不一致の場合，接続できないので注意してください。

- 10BASE-T/100BASE-TX のインタフェース種別が不一致の場合。
- 10BASE-T/100BASE-TX のインタフェース種別は一致しているが，全二重／半二重が不一致の場合。

(2) 1000BASE-SX/1000BASE-LX/1000BASE-LH 接続

本装置はオートネゴシエーション，または全二重固定接続です。

(3) オートネゴシエーション接続 (10BASE-T，100BASE-TX，1000BASE-SX，1000BASE-LX，1000BASE-LH)

本装置と相手装置の両方をオートネゴシエーションで使用する場合，接続する相手装置が IEEE802.3u オートネゴシエーションで接続できるか確認してください。この場合，設定されるモードは本装置および接続相手装置がサポートしている中で最も高速なモードが設定されます。相手装置が全二重固定設定の場合，本装置はオートネゴシエーションでなく全二重固定設定にしてください。

また，相手装置によってはオートネゴシエーションが正しく完了しないで通信ができない場合があります。この場合，本装置は次に示すシステムメッセージを表示します。このような問題は，本装置の設定を接続する相手装置に合わせた固定のモードにすると回避できます。

```
E4 LINELAN NIF:X LINE:X 41000201 1350:XXXXXXXXXXXX The interface faild in
autonegotiation
```

(4) フローコントロール

本装置はギガビット・イーサネットでフローコントロールを行います。本装置は相手装置からポーズパケットを受信した場合，送信規制を行います。また，本装置からポーズパケットを送信することによって，相手装置に送信規制を行います。

(5) タグによる仮想 LAN および優先制御

本装置は IEEE802.1Q(Tag-VLAN) をサポートしていますが，IEEE802.1p(優先制御) はサポートしていません。

9.1.2 Tag-VLAN 連携の LAN スイッチ接続

本装置と LAN スイッチを Tag-VLAN 連携で接続する場合の設定について説明します。

(1) VLAN 種別

本装置がサポートする VLAN は，IPv4 および IPv6 パケットに関する Tag-VLAN だけです。本装置を接続する LAN スイッチがそれ以外の VLAN(例えば，IPX などのプロトコル VLAN) をサポートしている場

合でも，LAN スイッチに設定する VLAN は，次に示すどちらかにしてください。

- LAN スイッチが中継する IPv4 および IPv6 パケットに関する Tag-VLAN
- LAN スイッチの送受信ポートに関する Tag-VLAN

(2) Tag-VLAN 連携設定

本装置と，本装置に接続する LAN スイッチの Tag-VLAN の設定は一致させてください。LAN スイッチと Tag-VLAN の設定を一致させるときは，次に示す点に注意してください。

- VLAN 設定をしたインタフェース (vlan オプションで指定) は，Tag 付きパケットだけを送受信できます。
- Tag なしパケットを受信した場合，そのパケットを廃棄します。
- VLAN 設定をしていないインタフェースは，Tag なしパケットだけを送受信できます。Tag 付きパケットを受信した場合，そのパケットを廃棄します。
- TPID(Tag Protocol Identifier) 値は "0x8100" または "0x9100" です。

(3) 中継できるパケット

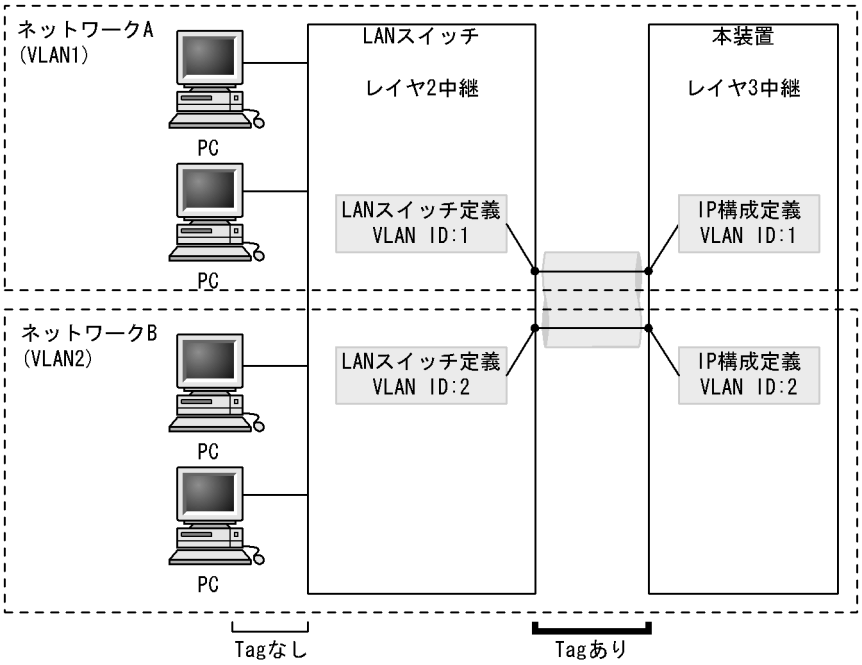
VLAN 設定をしたインタフェース (構成定義コマンドの vlan オプションで指定) は，IPv4 および IPv6 パケット ARP パケットが送受信できます。本装置を接続する LAN スイッチがそれ以外のパケットをサポートしている場合でも，次に示すパケットに関する VLAN は使用しないでください。

- IPX パケット
- ブリッジ中継パケット
- IPv4 マルチキャスト中継パケット
- IPv6 マルチキャスト中継パケット

(4) VLAN ID

VLAN ID は本装置，LAN スイッチから構成される仮想ネットワークの識別子のため，接続する LAN スイッチの VLAN ID と一致させる必要があります。VLAN ID の不一致が発生した場合，パケットの廃棄などが発生して正しい通信が行えません。二つの VLAN を LAN スイッチ経由で本装置に設定する例を次の図に示します。

図 9-1 二つの VLAN を LAN スイッチ経由で本装置に設定する例



- LAN スイッチに設定する VLAN ID(「図 9-1 二つの VLAN を LAN スイッチ経由で本装置に設定する例」の LAN スイッチ定義)と，本装置に設定する IP 構成定義の VLAN ID は同じ値にしてください。マルチホーミング接続の場合は，それぞれの IP に対して同じ値にしてください。
- Static ARP エントリを作成する場合は，本装置に設定する IP 構成定義の VLAN ID と，ARP(Static) 構成定義の VLAN ID は同じ値にしてください。複数の ARP エントリを作成する場合(接続する装置が複数存在する場合)は，全エントリについて同じ値にしてください。マルチホーミング接続の場合は，それぞれの IP に対して同じ値にしてください。

9.1.3 Tag-VLAN 連携の PC 接続

本装置と PC を Tag-VLAN で接続する場合には次の点に注意してください。

- Tag-VLAN のサポート
  Tag-VLAN をサポートしている PC はほとんどありません。本装置と PC を Tag-VLAN として接続する場合は，LAN スイッチ経由で接続してください。
- Layer2 中継
  本装置の Tag-VLAN 連携は IPv4 または IPv6 限定の Layer3 中継だけをサポートします。VLAN ドメイン内の Layer2 中継を PC 間で行う場合は，LAN スイッチで中継するように設定してください。

9.2 WAN インタフェース

9.2.1 フレームリレー

(1) DLCI グループを使用した他社接続

DLCI グループは，同一ネクストホップに対して，複数の PVC を設定するオプションであり，dlci-group コマンドで設定します。類似の機能をサポートしている他社製品がありますが，パケット送出時の DLCI の選択方式，障害検出時の動作など，機種によって異なります。

本装置以外の機種と接続する場合は，機種ごとの動作を確認してから使用してください。なお，Cisco 社製ルータでは，frame-relay priority-dlci-group コマンドでの構成設定が該当します。

(2) フレームリレー接続でのパケットフォーマット

本装置のフレームリレーでは，RFC1490/RFC2427 に準拠したフレームフォーマットを使用しています。機種によって，RFC 準拠のフレームフォーマットを使用するための設定が必要なものがある注意してください。Cisco 社製ルータでは，encapsulation frame-relay の指定時に "IETF" オプションが必要です。

(3) frping コマンド

frping コマンドは，RFC1293/RFC2390 規定の InverseARP プロトコルを利用した疎通確認コマンドです。Inverse ARP プロトコルは実装が必須ではありません。このため，疎通できる状態であっても，接続相手装置が Inverse ARP を行わない場合は，コマンド実行結果で相手装置からの応答タイムアウトを表示するので注意してください。

(4) パケット長

本装置と接続相手装置で，最大情報フィールド長 (MTU) の設定が異なっていると，転送フレームを廃棄する場合があるので，接続相手装置との間で最大情報フィールド長 (MTU) の設定値を一致させて使用してください。フレームの廃棄は，フレーム送信側装置の最大情報フィールド長の設定値が，フレーム受信側装置の設定値より大きいときに受信側の装置で発生します。

本装置を Cisco 社製ルータと接続するときは，dlci コマンドの -max_packet_size オプションで 1502 を設定してください。IP フラグメントで使用する MTU 長は dlci コマンドの -max_packet_size -2 となります。IP フラグメントの方法については「解説書 Vol.1　9.3.3 MTU とフラグメント」を参照してください。

9.3 ATM インタフェース

本装置と他機種との接続の場合に接続条件となる構成定義情報の設定について説明します。

9.3.1 Cisco 社製ルータ接続

本装置と Cisco 社製ルータのうち ATM インタフェースを持つ製品との接続の場合について，Cisco 社製ルータ接続時の構成定義情報を次の表に示します。

表 9-1 Cisco 社製ルータ接続時の構成定義情報

本装置の構成定義情報設定値		Cisco 社製ルータの構成定義情報設定値	
構成定義項目	設定値	構成定義項目	設定値
vc コマンド mtu	4470	mtu	4470(デフォルト)
		ip mtu	4470(デフォルト)

最大情報フィールド長 (MTU) の設定が異なっていると転送フレームを廃棄する場合があるので，本装置との間で設定値を一致させて使用してください。フレームの廃棄は，フレーム送信側装置の最大情報フィールド長の設定が，フレーム受信側装置の設定値より大きいときに受信側の装置で発生します。

9.4 IP ルータとの接続

9.4.1 他機種との接続

本装置と他機器を IP ルーティングで接続する場合について説明します。

(1) ポイントーポイント型回線のインタフェースアドレス

本装置はポイントーポイント型回線 (ブロードキャスト型で定義された ATM やフレームリレー以外の WAN 回線) の経路情報 (直結経路) を二つのホスト経路として扱います。したがって，本装置だけで構成されたネットワークでは，ポイントーポイント型の回線にインタフェースアドレスを割り当てることができます。ほかの機器間とでは使用しないでください。

ポイントーポイント型の回線に割り当てられるインタフェースアドレスを次に示します。詳細は「解説書 Vol.1　10.2 ネットワーク設計の考え方」を参照してください。

- 複数のポイントーポイント型回線に同一のネットワークまたはサブネットワークの IP アドレス
- ポイントーポイント型回線の両端に異なるネットワークまたはサブネットワークの IP アドレス

注意事項

本装置ではポイントーポイント型回線の経路情報を二つのホスト経路として扱いますが，Cisco 社製ルータでは一つのネットワーク経路として扱います。したがって，ルーティングプロトコルで広告される経路情報に差異が生じるので注意してください。

(2) フレームリレー／ ATM 上で RIP-1 を使用する場合の設定

本装置では構成定義情報で設定すれば，フレームリレー／ ATM・インタフェースをポイントーポイント型インタフェース，またはブロードキャスト型インタフェースとして取り扱うことができます。デフォルトではブロードキャスト型となっています。

本装置をフレームリレー／ ATM 経由で接続する場合は，本装置のフレームリレー／ ATM・インタフェースの接続形態をデフォルトのブロードキャスト型にして，ポイントーポイント型の定義はしないでください。

本装置以外と接続する場合には，接続する機器の仕様を確認してください。

(3) フレームリレー／ ATM 上で RIP-2 を使用する場合の設定

RIP-2 はネットワーク負荷の軽減のため，ブロードキャスト型インタフェースではマルチキャストアドレスによってルーティング・パケットを送信します。

本装置以外と接続する場合には，接続する機器の仕様を確認してください。

(4) フレームリレー／ ATM 上で OSPF を使用する場合の注意事項

OSPF はネットワーク負荷の軽減のため，ブロードキャスト型インタフェースではマルチキャストアドレスによってルーティング・パケットを送信します。

本装置以外と接続する場合には，接続する機器の仕様を確認してください。

(5) ポイントーポイント回線上で RIP-1 を使用する場合の設定

本装置ではポイントーポイント回線上に RIP パケットを送信する場合，送信先アドレスをユニキャストアドレス (相手装置のインタフェースアドレス) で送信します。また，ポイントーポイント回線上から RIP パケットを受信する場合，送信先アドレスがユニキャスト・アドレス (自装置のインタフェースアドレス)，または制限付きブロードキャストアドレス (すべて 1 のアドレス) のパケットを受け入れます。

Cisco 社製ルータでは「ip broadcast-address」の設定によって，RIP パケットの送信先アドレスが異なります。本装置と Cisco 社製ルータを接続する場合は，「ip broadcast-address」を設定しないでください。

(6) ポイントーポイント回線上で OSPF を使用する場合の設定

本装置ではポイントーポイント回線上で OSPF を動作させた場合，HelloInterval のデフォルト値は 10 秒，Routerdeadinterval のデフォルト値は 40 秒となっています。

本装置と他装置をポイントーポイント回線で接続する場合には，接続する他装置の仕様を確認の上，両ルータ間で HelloInterval 値および Routerdeadinterval 値を合わせてください。

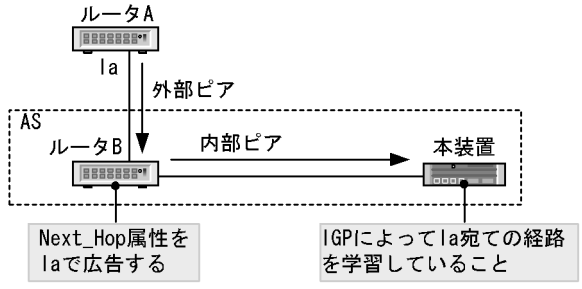
(7) OSPF を使用するときの注意事項

- HelloInterval のデフォルト値
  本装置の HelloInterval のデフォルト値は 10 秒です。本装置と接続されるルータに設定された HelloInterval を確認して，両ルータ間で HelloInterval 値を合わせてください。
- priority のデフォルト値
  本装置の priority のデフォルト値は 1 です。ただし，NBMA(ospf interface コマンドで nonbroadcast パラメータを指定したインタフェース) では 0 です。本装置を指定ルータの選択対象とさせたくない場合は，priority 値を 0 に設定してください。

(8) BGP-4 を使用するときの注意事項

- NextHop 解決
  本装置では同一 AS 内の BGP スピーカへ経路を広告するとき，NEXT_HOP 属性にその BGP スピーカとのピアリングに使用している自側のピアリングアドレスを設定します。また，本装置が受信する経路情報の NEXT_HOP 属性は IGP 経路を基に解決しています。したがって，NEXT_HOP 属性に相手側のピアリングアドレスが設定されている必要はなく，IGP によって NEXT_HOP 属性に対応するアドレス宛ての経路が学習されていれば，Next_Hop 解決は正常に行われます。
  なお，bgp コマンドの resolve-nexthop all オプションを指定すると，Next-Hop 解決に使用する経路情報を IGP 経路および BGP 経路に拡張できます。
  この Next_Hop 解決処理は，すべてのピアタイプ (外部ピア，メンバー AS 間ピア，内部ピア) に適用されます。Next_Hop 解決を次の図に示します。

図 9-2 Next_Hop 解決



(9) RFC1583 に準拠していない装置と OSPF で接続するときの注意事項

本装置と本装置以外の装置とで，同じ宛先の AS 外経路またはエリア間経路を，RFC1583 に準拠していない装置に広告するネットワーク構成にしないでください。

これは，OSPF の AS 外経路情報とエリア間経路情報の経路情報識別子 (LSID) フィールドの値は，RFC1247 の規格と RFC1583 以降の規格で異なるためです。

RFC1247 では，宛先アドレスを経路情報識別子として使用します。一方，RFC1583 以降 (本装置が該当) では，宛先アドレス以外の値を経路情報識別子として使用する場合があります (仕様は装置によって異なる)。このため，同一宛先の経路情報でも本装置とそのほかの装置が異なる経路情報識別子を使用することがあります。本装置同士では，同一宛先の経路情報の経路情報識別子は必ず同じ値になります。

RFC1583 に準拠していない装置では，同じ宛先の経路情報を異なる経路情報識別子で学習した場合，最短経路を選択しないか，または経路を学習しません。なお，RFC1583 以降の規格に準拠している装置では，正しく経路を選択します。

9.4.2 他装置との置き換え

次に示す機種は RIP-1 の実装が異なるので，注意が必要です。

- Cisco 社製ルータ

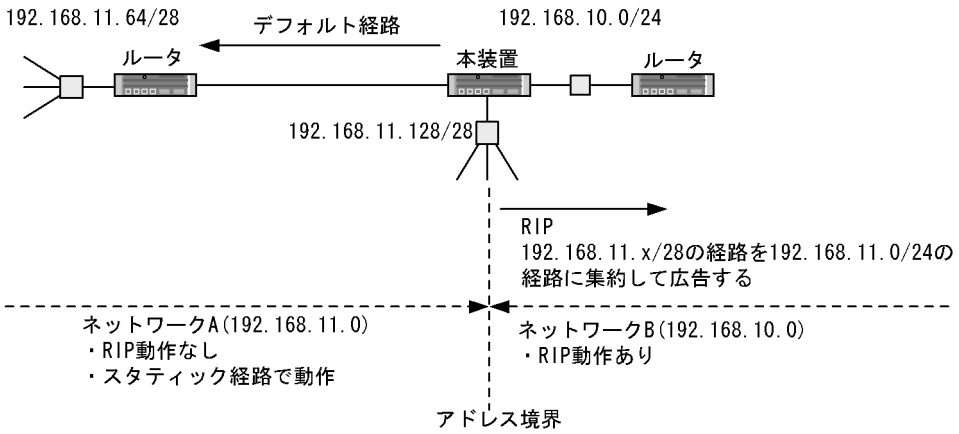
これら以外の装置と本装置を置き換える場合には，旧装置の仕様を確認してください。

本装置では，インタフェースアドレスがサブネット化されている場合，該当するインタフェースに対するネットワーク経路 (ナチュラル・マスク経路) を自動生成しません。ブロードキャスト接続ではサブネット経路を，ポイントーポイント接続ではホスト経路を生成します。RIP-1 ではアドレス境界をまたがるサブネット経路は広告しないため，構成定義情報によって経路集約 (サブネット経路およびホスト経路をネットワーク経路に集約する) 設定が必要になります。詳細は「解説書 Vol.1　10.4.3(3)(a) IP インタフェースが一つの場合の RIP 広告について」を参照してください。

Cisco 社製ルータなど RIP-1 の実装が異なる機種では，サブネット経路を自動的にネットワーク経路に集約し広告する装置もあり，通常該当する集約経路はフォワーディング・テーブルに登録されません。本装置ではサブネット経路をネットワーク経路に集約するためには経路集約の定義が必要です。また，集約経路はアクティブ経路としてフォワーディング・テーブルに登録されます。

集約経路をフォワーディング・テーブルに登録しないような装置と互換性を持って動作させるためには，経路集約の定義 (aggregate コマンド) に noinstall オプションの設定が必要です。noinstall オプションが必要な構成例を次の図に示します。

図 9-3 noinstall オプションが必要な構成例



本装置に集約経路192.168.11.0/24をインストールした場合，192.168.11.64/28宛てのIPパケットは本装置で廃棄される。
(本装置に192.168.11.64/28の経路がなく，デフォルト経路で動作させるような場合)

9.5 IPv6 ルータとの接続

本装置と他機器を IPv6 ルーティングで接続する場合には次の点に注意してください。

9.5.1 他機種との接続

(1) ポイントーポイント型回線のインタフェースアドレス

本装置はポイントーポイント型回線の経路情報(直結経路)を二つのホスト経路として扱います。したがって，本装置だけで構成されたネットワークでは，ポイントーポイント型の回線に次のインタフェースアドレスを割り当てることができます。他機種間では使用しないでください。詳細は「解説書 Vol.1　10.2 ネットワーク設計の考え方」を参照してください。

- 複数のポイントーポイント型回線に同一プレフィックスの IPv6 アドレス
- ポイントーポイント型回線の両端に異なるプレフィックスの IPv6 アドレス

ただし，ポイントーポイント型回線のインタフェースにこれらのアドレスを割り当てた場合，経路情報の集約設定などが複雑になります。本装置はリンク内だけで有効なリンクローカルアドレスを各インタフェースに割り当てることができるため，ポイントーポイント型回線のインタフェースにはできるだけリンクローカルアドレスだけを割り当てるようにしてください。

注意事項

本装置ではポイントーポイント型回線の経路情報を二つのホスト経路として扱いますが，Cisco 社製ルータでは一つのネットワーク経路として扱います。したがって，ルーティングプロトコルで広告される経路情報に差異が生じますので注意してください。

(2) ポイントーポイント型回線による BGP4+ 接続での注意事項

本装置では，BGP4+ 接続をリンクローカルアドレスで行うことができます。また，ポイントーポイント型回線の経路情報を二つのホスト経路として扱います。このため，本装置とポイントーポイント型回線で接続を行うルータの BGP4+ が次に示す動作条件に該当する場合，本装置は接続先ルータからの経路情報が受信できないことがあります。

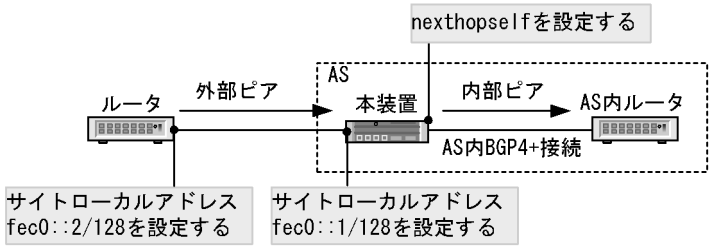
- グローバルアドレスだけで BGP4+ と接続するルータ
- ポイントーポイント型回線のグローバルアドレスを，ブロードキャストアドレス型回線と同様に一つのネットワーク経路として解釈するルータ

このようなルータとポイントーポイント型回線で接続し BGP4+ で経路情報の交換を行う場合には，ポイントーポイント型回線にサイトローカルアドレスを割り当ててください。

Cisco 社ルータと接続する場合は，これらの設定が必要となります。

また，受信した経路情報を本装置で内部 BGP4+ ピアに送信する場合は，該当するピアの構成定義情報に nexthopself パラメータを指定してください。nexthopself パラメータ指定の例を次の図に示します。

図 9-4 nexthopself パラメータ指定の例



注意事項

割り当てたサイトローカルアドレスは外部へ広告しないようにしてください。

9.6 SNMP マネージャとの接続

9.6.1 推奨 SNMP マネージャ

本装置では，次に示す SNMP マネージャで動作確認をしています。これら以外の SNMP マネージャを使用する場合は，十分評価の上，使用してください。

- SNMP マネージャ
  - HP OpenView Network Node Manager Ver4.0x (HP-UX 版)
  - HP OpenView Network Node Manager Ver5.01 (HP-UX 版)
  - HITACHI　JP1/Cm2/Network Node Manager
- RMON マネージャ
  - NetScout Systems　NetScout Manager Plus　Ver5.2
  - 3Com　Transcend LANsentry Manager　ver3.0

9.6.2 MIB 情報収集周期のチューニング

SNMP マネージャは，ネットワーク上の新しい装置を検出したり，トラフィック状況を監視したりするため，SNMP エージェントサポート機器に対して定期的に MIB の取得処理を行います。この定期的な MIB 取得処理間隔が短いとネットワーク機器やネットワークに負荷をかけることになります。また，装置の状態や回線速度などによって MIB 取得時にマネージャ側でタイムアウトが発生する可能性があります。次に示すことを考慮し，ネットワーク管理を行ってください。

(1) SNMP マネージャ側の応答監視タイマ値の考慮

SNMP マネージャ側で MIB 取得時の応答監視タイマ値を変更できる場合は，5 秒以上に設定してください。なお，本装置が次に示す場合に，マネージャ側で応答タイムアウトが頻発します。応答タイムアウトが頻発する場合は，応答監視タイマ値をさらに延ばす必要があります。

- ネットワークのレスポンスが悪い場合
  例えば，SNMP マネージャと本装置間に多数の接続装置（ブリッジ，ルータなど）がある，または回線速度が低い場合。
- 接続 IP ネットワーク数や接続インタフェース数が多い場合
  例えば，本装置のインタフェース数が多い場合，IP 関連の MIB 情報の検索時間で時間がかかる場合。
- ルーティングテーブルのエントリが多い場合
  例えば，本装置の IP ルーティングエントリ数が多い場合にルーティング関連の MIB 情報の検索時間で時間がかかります。または，経路計算などで MIB 情報の検索する CPU 割当時間の減少による，MIB レスポンス低下が発生する場合。
- ARP 数が多い場合
  例えば，本装置の ARP 数が多い場合，ARP 関連の MIB 情報の検索時間で時間がかかる場合。
- 接続 SNMP マネージャ数が多い場合
  例えば，本装置に接続する SNMP マネージャが多く，一定時間内に MIB 情報の収集が集中する場合。

SNMP マネージャのチューニングパラメータ

- ポーリング周期
- 応答監視タイマ
- 応答監視タイムアウト時のリトライ回数

(2) SNMP マネージャによる MIB 情報の収集周期の見直し

本装置は，ネットワークの規模に伴い管理情報 (MIB) 量も増大します。このため，大規模ネットワークに接続する場合，SNMP マネージャからの問い合わせに対する管理情報の収集に長時間を必要とし，一時的に装置が過負荷状態になる場合があります。

過負荷状態が発生した場合，ルーティング情報の取りこぼしや，ルーティング情報を本装置から他装置に配布できなくなり，一時的に IP フレームの中継ができなくなることが発生します。このような場合，SNMP マネージャの各種パラメータのチューニングをお勧めします。

BCU を二重化構成で運用しているとき

SNMP マネージャから MIB を設定すると，待機系 RM へ現用構成定義情報ファイルの内容を自動的にコピーするため，時間がかかることがあります。このときは，応答監視タイマ値を少なくとも 20 秒以上に設定してください。

(3) VRRP 構成でのネットワーク監視の注意事項

VRRP 構成のネットワークを JP1/Cm2 で管理する場合，VRRP の状態がマスタからスレーブ状態に遷移したときに，"xx.xx.xx.xx が報告された yy.yy.yy.yy の物理アドレス 0xXXXXXXXXXXXX は SNMP が zz.zz.zz.zz から得たアドレス 0xVVVVVVVVVVVV と異なる " というメッセージを出力します。

これは，JP1/Cm2 内のデータベース情報 (IP アドレスと物理アドレスの対応情報) と SNMP の MIB から取得した IP アドレスと物理アドレスの対応情報が異なるために発生します。このため，VRRP の状態がマスタからスレーブ状態に遷移したときに，このメッセージを出力した場合は問題ありません。xx.xx.xx.xx,yy.yy.yy.yy,zz.zz.zz.zz の部分は IP アドレス値になります。0xXXXXXXXXXXXX の部分は仮想アドレスの値，0xVVVVVVVVVVVV の部分は物理 MAC アドレスになります。

9.7 RADIUS サーバとの接続

9.7.1 推奨 RADIUS サーバ

本装置では，次に示す RADIUS サーバで動作確認をしています。これら以外の RADIUS サーバを使用する場合は，十分評価の上，使用してください。本装置でサポートしているのは RADIUS を使用したリモートログインのユーザ認証です。

- Lucent Technologies NavisRadius（Windows NT/Solaris 版）

9.7.2 RADIUS サーバの設定

本装置が RADIUS サーバと接続するための注意点を次に示します。

（1） RADIUS サーバでの本装置の識別

RADIUS プロトコルでは NAS を識別するキーとして，要求パケットの発信元 IP アドレスを使用するよう規定されています。本装置では要求パケットの発信元 IP アドレスに次に示すアドレスを使用します。

- 構成定義コマンドの router コマンドによるローカルアドレスが設定されている場合は，ローカルアドレスを発信元 IP アドレスとして使用します。
- ローカルアドレスが設定されていない場合は，送信インタフェースの IP アドレスを使用します。

このため，ローカルアドレスが設定されている場合は，RADIUS サーバに本装置を登録するためにローカルアドレスで指定した IP アドレスを使用する必要があります。これによって，RADIUS サーバと通信するインタフェースが特定できない場合には，ローカルアドレスを設定することで RADIUS サーバを確実に識別できる本装置の情報を登録することができるようになります。

（2） RADIUS サーバのメッセージ

RADIUS サーバは応答に Reply-Message 属性を添付して要求元にメッセージを送付する場合があります。本装置では，RADIUS サーバからの Reply-Message 属性の内容を運用ログに出力します。RADIUS サーバとの認証に失敗する場合は，運用ログを参照してください。

（3） RADIUS サーバのポート番号

RADIUS の認証サービスのポート番号は，RFC 2865 で 1812 と規定されています。本装置では特に指定しないかぎり，RADIUS サーバへの要求に 1812 のポート番号を使用します。しかし，一部の RADIUS サーバで 1812 ではなく初期の実装時に使用されていた 1645 のポート番号を使用している場合があります。このとき構成定義の auth_port オプションで 1645 を指定してください。-auth_port オプションでは 1 ～ 65535 の任意の値が指定できるので，RADIUS サーバが任意のポート番号で待ち受けできる場合にも対応できます。-auth_port オプションについては，マニュアル「構成定義コマンドレファレンス Vol.2　9. RADIUS」を参照してください。

10 網・各種専用線サービスとの接続

この章では，システム構築時に検討が必要な網・各種専用線サービスとの接続について説明します。

10.1 **イーサネット，ギガビット・イーサネット**

10.2 **専用線・フレームリレー・**ISDN

10.3 ATM **サービス**

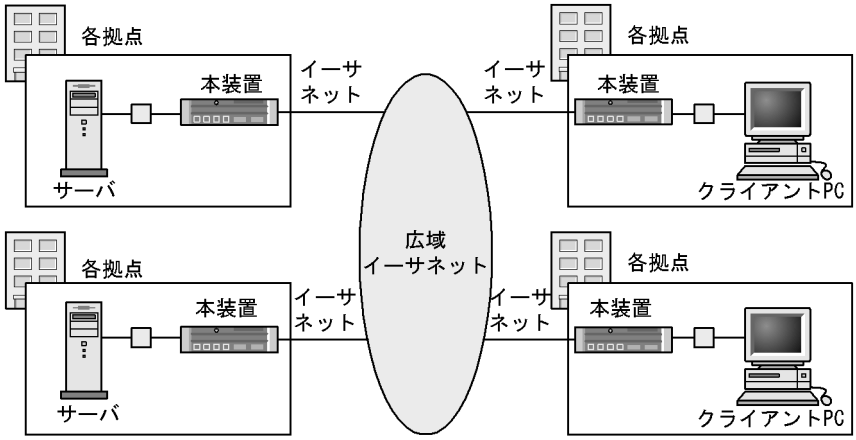
10.1 イーサネット，ギガビット・イーサネット

本装置と各イーサネットサービスの接続について説明します。

10.1.1 広域イーサネット

イーサネットで実現できるサービスとしては，日本電信電話株式会社をはじめとした通信事業者が提供する**広域イーサネット**が挙げられます。企業の多くは構内イーサネットを構築しており，複数の拠点や取引先との間でイーサネットを統合して業務を円滑に進めることが必要です。広域イーサネットは複数拠点のイーサネットを一つに統合するサービスです。広域イーサネットは，従来サービスよりも比較的安価で，高速バックボーンの共有によって，動画や画像によるトラフィックの増大にも対応できます。広域イーサネットを使用したネットワーク構成例を次の図に示します。

図 10-1 広域イーサネットを使用したネットワーク構成例



10.1.2 フレッツ・ADSL および B フレッツ接続 (PPPoE での接続)

(1) 適用サービス

本装置と接続できる PPPoE サービスを次の表に示します。

表 10-1 本装置と接続できる PPPoE サービス

サービス種別	品目	本装置と接続する回線終端装置
フレッツ・ADSL	1.5M タイプ	ADSL モデム
	8M タイプ	ADSL モデム
B フレッツ	ビジネスタイプ (100M)	ONU
	ベーシックタイプ (100M)	ONU
	ファミリータイプ (10M)	ONU
	マンションタイプ (100M)	ONU

なお，回線終端装置である ADSL モデムや ONU の動作環境設定，および本装置との接続方法は，使用する各製品の説明を参照してください。

(2) 本装置の構成定義情報

PPPoE の使用時，接続先プロバイダから指定される情報としてユーザ名，ドメイン名，パスワード，認証プロトコル，検索サービス名，AC 名があります。検索サービス名，AC 名は特に指定されない場合があります。これらは本装置の構成定義情報で設定します。これ以外の PPPoE の構成定義情報については，デフォルトの値で最適な接続ができるように設定されているので，サービス提供事業者から特に提示がないかぎり，値の変更は不要です。これらの値を変更した場合，通信のレスポンスが遅くなったり，通信できなくなったりする場合があります。ただし，特定 HP の閲覧ができないなどの現象が発生した場合，MRU，MSS のチューニングを行うことで，この現象を回避できる場合があります。チューニングの詳細については「運用ガイド　7.5.3(6) mru（MTU）の設定値」,「運用ガイド　7.5.3(7) mss 情報の設定値」を参照してください。

10.2 専用線・フレームリレー・ISDN

10.2.1 WAN のサービス

日本電信電話株式会社が提供している WAN のサービスを次の表に示します。

表 10-2 WAN のサービス

分類	サービス	特長
専用線	高速デジタル専用線	• 回線を専用で使用できる • サービス品目が豊富
	デジタルアクセス デジタルリーチ	• 回線を専用で使用できる • 低価格（サービス品目は 3 種類）
POS 回線	メトロハイリンク	• 最高 600M の超高速専用サービス • 低価格（サービス品目は 2 種類）
ISDN	INS ネット	• 従量制の料金設定 • バックアップ回線などに利用できる
フレームリレー	スーパーリレー FR	• 専用線と比較して低価格だが，通信品質は落ちる

10.2.2 フレームリレー網の加入条件

フレームリレー公衆網へ加入を申し込むときは，接続条件について指定する場合があります。また，指定した条件に合わせて本装置の構成定義情報を設定する必要があります。フレームリレー網の加入条件と本装置の構成定義情報を次の表に示します。

表 10-3 フレームリレー網の加入条件と本装置の構成定義情報

申込書の記入欄		本装置		備考
接続条件	一般的な選択肢	接続時の申し込み指定	構成定義情報の設定	
アクセス回線速度	64kbit/s ～ 6Mbit/s	6Mbit/s 以下の速度※1	物理インタフェースの種別が V.24 ／ V.35 ／ X.21(serial) の場合は，設定は不要。 高速デジタル回線の場合は，timeslot コマンドで設定します。詳細はマニュアル「構成定義コマンドレファレンス Vol.1」を参照してください。	－
PVC 状態確認手順 (LMI) のプロトコル規格	ITU-T Q.933(または TTC JT-Q933)ANNEX A	「ITU-T Q.933」，「ANSI TI.617aANNEX D」，「なし」の 3 種類から任意に選択します。	デフォルト動作のため，設定は不要。明示的に設定する場合は，frame-relay コマンドの local_management オプションで q933 を指定します。	－
	ANSI T1.617a ANNEX D		frame-relay コマンドの local_management オプションで ansi を指定します。	－

申込書の記入欄			本装置		備考
接続条件		一般的な選択肢	接続時の申し込み指定	構成定義情報の設定	
		フレームリレーフォーラム 4 社仕様 (FRF.1.1)		―	―
		なし		frame-relay コマンドの local_management オプションで no を指定します。	―
PVC 状態確認手順 (LMI) のプロトコル動作		端末 (DTE)	端末 (DTE)，網 (DCE)，双方向の 3 種類から任意に選択します。	デフォルト動作のため，設定は不要。明示的に設定する場合は，frame-relay コマンドの poll_direction オプションで dte を指定します。	最も一般的に使用されます。
		網 (DCE)		frame-relay コマンドの poll_direction オプションで dce を指定します。	公衆フレームリレー網への加入では，一般には使用しません。
		双方向		frame-relay コマンドの poll_direction オプションで both を指定します。	本装置では，メンテナンス作業などで PVC の運用が停止しているとき，該当する PVC の停止中状態を，双方向手順によって網へ通知します。これによって接続相手のルータは経路変更など適切なアクションをとることができます。※2
PVC 状態確認手順 (LMI) のプロトコルパラメータ	N391	1 ～ 255(回)	「6」	特に設定なし。	本装置では 6 固定。
	N392	1 ～ 10(回)	3	特に設定なし。	本装置では 3 固定。
	N393	1 ～ 10(回)	4	特に設定なし。	本装置では 4 固定。
	T391	5 ～ 30(秒)	10	特に設定なし。	本装置では 10 固定。
	T392	5 ～ 30(秒)	15	特に設定なし。	本装置では 15 固定。
PVC 状態確認手順 (LMI) の非同期単一 PVC 状態通知オプション		サポート	サポート，非サポートのどちらかを選択します。	特に設定なし。	PVC 状態確認手順のプロトコル動作で「端末 (DTE)」または「双方向」を行うときは，本装置は非同期単一 PVC 状態通知を常に受信できます。
		非サポート		特に設定なし。	―
CLLM メッセージ		サポート	サポート，非サポートのどちらかを選択します。	frame-relay コマンドの cllm_sustain オプションで，受信監視時間を指定します。指定値は網が CLLM を周期的に送出する時間間隔と一致させます。	CLLM は輻輳レベルの表示コードについて，プロトコル規定が明確でなく，使用時に注意が必要です。本装置では，日本電信電話株式会社のスーパーリレー FR に照応した表示コードを採用しています。

申込書の記入欄		本装置		備考
接続条件	一般的な選択肢	接続時の申し込み指定	構成定義情報の設定	
	非サポート		デフォルト動作のため，設定は不要。明示的に設定する場合は，frame-relay コマンドの cllm_sustain オプションで no を指定します。	－
DLCI(番号)	16 ～ 991	16 ～ 991 の範囲で指定します。	16 ～ 991 の値を使用できます。DLCI(番号) は該当する DLCI の DLCI 情報を設定するときに指定します。	同一のフレームリレー回線内で DLCI(番号) が重複しないように指定します。
CIR	0kbit/s ～ 3Mbit/s	アクセス回線速度以下の値を指定します。	特に指定しないで接続できます。また，dlci コマンドの cir オプションで加入条件の CIR を指定することで，送信データバッファが適正なサイズに調整されます。	本装置で輻輳検出時にルータから網への送出レートを規制する場合は，dlci コマンドの congestion_management オプションを指定します。
アドレス長	2 オクテット※3	－	特に設定なし。	本装置は 2 オクテット固定。
最大情報フィールド長	網によって固定 (1600 ～ 4500 オクテット)	－	frame-relay コマンドおよび dlci コマンドの max_packet_size オプション指定を，網の最大情報フィールド長以下にします。	－

(凡例) －：該当しない

注※ 1　本装置での接続時に指定できる値は，「解説書 Vol.1　5.1 物理インタフェース」を参照してください。

注※ 2　PVC 状態確認手順の「プロトコル動作」が「双方向」，および網がルータからの非同期通知を受信できる場合は，frame-relay コマンドの provide_single_pvc_status オプションを指定することで，ルータから網への PVC 状態通知を速やかに行うことができます。

注※ 3　ITU-T Q922 では 3，4 オクテット長の拡張アドレス形式が規定されていますが，一般には 2 オクテット形式を使用します。

10.2.3　ISDN 回線契約条件

本装置でサポートする ISDN 回線を「表 10-4　本装置でサポートする ISDN 回線」に，ISDN 基本回線の契約条件・付加サービスを「表 10-5　ISDN 基本回線の契約条件・付加サービス」に，ISDN 一次群回線の契約条件・付加サービス「表 10-6　ISDN 一次群回線の契約条件・付加サービス」にそれぞれ示します。

表 10-4　本装置でサポートする ISDN 回線

サポート ISDN 回線	備考
基本インタフェース（Point-Point）	－
基本インタフェース（Point-Multipoint 常時起動）	－
1 次群速度インタフェース（mH0+nB+D）	－

サポート ISDN 回線	備考
1 次群速度インタフェース（mH0+nB/D）	同一 RP 内の別回線に D チャネル共用を行う基本または 1 次群の回線が必要です。
1 次群速度インタフェース (H1/D)	

(凡例) －：該当しない

表 10-5 ISDN 基本回線の契約条件・付加サービス

区分	サービス名	契約条件／サポート	備考
契約条件	インタフェース形態およびレイヤ 1 起動種別	P-MP 常時または P-P	一次群回線の呼制御を基本回線の D チャネルで行う場合は P-P だけ指定できます。
基本サービス	発信者番号通知	通常通知（通話ごと非通知，呼毎通知許可※1※2	発信者番号によって，接続相手の識別，接続認証を行うため。
	ユーザ間情報通知	着信拒否※1	－
	サブアドレス通知	○	契約手続きは不要。網から自動的に通知されます。
	料金情報通知	○	
	通信中機器移動	×	－
付加サービス※4	任意チャネル着信 (「インタフェース形態およびレイヤ 1 起動種別」が P-P の場合だけのサービス)	◎	着信時のチャネル指定は本装置側から行うため。
	代表取扱 (代表電話番号)	○	D チャネル共用をさせないで Line Group を組む場合は必須です。
	グループセキュリティ	×	※3

(凡例)

◎：契約必須
○：サポートする (契約してもしなくてもよい)
×：サポートしない (契約できない)
－：該当しない

注※ 1　日本電信電話株式会社の ISDN 回線申込票で使用されている用語です。

注※ 2 「呼毎通知許可」は旧申込票で使用されていた用語です。

注※ 3　次に示す条件をすべて満たす場合だけ契約できます。

- 1 回線当たり最大 1 グループだけ利用できます。
- 発着信の規制パターンは,「グループ内通信」だけ契約できます。

次に示す発着信の規制パターンは契約できません。

- グループ内通信＋グループ外着信（グループ外からの着信だけ許容する）
- グループ内通信＋グループ外発信（グループ外への発信だけ許容する）
- グループ内通信＋グループ外着信＋グループ外発信
  （グループ外からの着信，グループ外への発信の両方を許容する）

注※ 4　この表にない付加サービスについては「×：サポートしない（契約できない)」になります。

表 10-6　ISDN 一次群回線の契約条件・付加サービス

区　分	サービス名			契約条件／サポート	備考
契約条件	インタフェース形態			23B+D または 24B 利用	－
	－	24B 利用の場合	(ア) インタフェース ID 番号	1-126 の任意の値を指定	本装置の構成定義情報の値と一致させる必要があります。
			(イ) 本回線を制御する D チャネルを持つ契約者回線番号	本回線を制御する D チャネルを持つ契約者回線番号	－
			(ウ)(イ) が基本回線の場合の呼番号長	1 オクテットまたは 2 オクテット※5	本装置の構成定義情報の値と一致させる必要があります。
基本サービス	発信者番号通知			通常通知（通話ごと非通知，呼毎通知許可※1※2	発信者番号によって，接続相手の識別，接続認証を行います。
	ユーザ間情報通知			着信拒否※1	－
	サブアドレス通知			○	契約手続きは不要（網から自動的に通知されます）。
	料金情報通知			○	
	通信中機器移動			×	－
付加サービス※4	任意チャネル着信			◎	着信時のチャネル指定は本装置側から行います。
	代表取扱 (代表電話番号)			○	D チャネル共用をさせないで Line Group を組む場合は必須です。
	グループセキュリティ			×	※3

(凡例)

◎：契約必須

○：サポートする (契約してもしなくてもよい)

×：サポートしない (契約できない)

－：該当しない

注※1　日本電信電話株式会社の ISDN 回線申込票で使用されている用語です。

注※2　「呼毎通知許可」は旧申込票で使用されていた用語です。

注※3　次に示す条件をすべて満たす場合だけ，契約できます。

- 1 回線当たり最大 1 グループだけ利用できます。
- 発着信の規制パターンは，「グループ内通信」だけ契約できます。

次に示す発着信の規制パターンは契約できません。

- グループ内通信＋グループ外着信（グループ外からの着信だけ許容する）
- グループ内通信＋グループ外発信（グループ外への発信だけ許容する）
- グループ内通信＋グループ外着信＋グループ外発信
  （グループ外からの着信，グループ外への発信の両方を許容する）

注※4　この表にない付加サービスについては「×：サポートしない（契約できない)」となります。

注※5　1 オクテットの場合，本装置の line_group 構成定義情報で "dch_line <Line-Name>" パラメータで D チャネル共用を定義できる ISDN 一次群回線の回線数は最大 4 になります。2 オクテットの場合はこのような制限はありません。ただし，回線業者によって，D チャネル共用を定義できる ISDN 一次群回線の回線数に上限があります。日本電信電話株式会社の場合，D チャネルを持つ回線を除いて，最大 8 になります。したがって，ISDN 回線を新規に契約する場合は，拡張性を考慮して 2 オクテットにしてください。特に申し出ない場合は 1 オクテットとなるので注意が必要です。

呼番号長が 1 オクテットとなっている既存の ISDN 回線を本装置に使用する場合で，契約を変更したくない場合，契約は 1 オクテットのままとして，本装置の line 構成定義情報の "call_reference_length {1 | 2}" パラメータで 1 を設定します。
本装置の line_group 構成定義情報についてはマニュアル「構成定義コマンドレファレンス Vol.1」の line-group コマンド，line コマンドを参照してください。

10.2.4 インバースマックス　ターミナルアダプタ接続条件

本装置と，インバースマックス　ターミナルアダプタ日本電信電話株式会社 INS メイト V － 1500(以降，TA) を接続し，バルク伝送接続を行う場合は，次に示す点に注意してください。なお，TA の設定方法，仕様などについては TA の取扱説明書を参照してください。

(1) 本装置の構成定義情報

本装置と TA の接続時に注意する必要がある本装置の構成定義情報を次の表に示します。

表 10-7　本装置の構成定義情報

構成定義情報※1		設定内容		
コマンド名	設定項目 / オプション名	ISDN 一次群回線 (23B ＋ D)	ISDN 基本群回線と ISDN 一次群回線の D チャネル共用 (24B ／ D)	
			基本群回線側	一次群回線側
line	物理インタフェース	priisdn	briisdn	priisdn
	bri_topology (インタフェース形態)	－	p-p	－
	phone_number (自電話番号)	本回線の電話番号	本回線の電話番号	－
	interface_id (インタフェース ID)	－	－	1※2
isdn-pool※3	channels(チャネル数)	※4	※4	
isdn-PPP※5	phone_number1 (相手電話番号)※6	相手電話番号	相手電話番号	
	channel_type (チャネル種別)	hO(HO チャネル)	hO(HO チャネル) または hl(Hl チャネル)	

(凡例) －：設定しない
注※ 1　この表の構成定義情報の詳細は，マニュアル「構成定義コマンドレファレンス Vol.1　4. ライン情報～構成定義コマンドレファレンス Vol.1　11. バックアップ情報」の line，isdn-ppp，isdn-pool コマンドを参照してください。
注※ 2　TA の「インタフェース ID(TE 側)」の設定 (「表 10-8　TA の基本設定内容」参照) と同じにする必要があります。
注※ 3 「ISDN 基本群回線と ISDN 一次群回線の D チャネル共用」の場合，line-group コマンドでこれら二つの line をグループ化しますが，この line-group に対して設定してください。line-group については，マニュアル「構成定義コマンドレファレンス Vol.1」を参照してください。
注※ 4　通信相手との通信速度分の B チャネルの個数を設定します。
H0 チャネル (384kbit/s) の場合，B チャネル (64kbit/s) × 6 であるため「6」を設定します。
Hl チャネル (1536kbit/s) の場合，B チャネル (64kbit/s) × 24 であるため「24」を設定します。HO チャネルで複数対地に接続する場合，これらのチャネル数の合計を設定します。

例えば，HO チャネルで 2 対地接続する場合，6 チャネル× 2 ＝ 12 であるため「12」を設定します。
注※ 5　isdn-pool に対して設定します。
注※ 6　phone_number2，phone_number3 は設定します。

(2) TA の設定内容

(a) 基本設定

本装置と TA の接続時に必要な TA の基本設定内容を次の表に示します。なお，表中の各設定項目の説明については，TA の取扱説明書を参照してください。

表 10-8　TA の基本設定内容

設定項目		設定内容		TA のデフォルト値
項目名	コマンド名	ISDN 一次群回線 (23B ＋ D)	ISDN 基本群回線と ISDN 一次群回線の D チャネル共用 (24B ／ D)	
回線設定	PRI	23B ＋ D	24B ／ D	23B ＋ D
受付ダイヤル (モード A/B) ※ 1	ADDI	相手電話番号	相手電話番号	－
呼番号長 (網側)	CRSN	2 ※ 2	※ 3	2
呼番号長 (TE 側)	CRSU	2 ※ 2	※ 3	2
インタフェース ID(網側)	IFDN	－	本回線の契約時に指定したインタフェース ID を設定	1
インタフェース ID(TE 側)	IFDU	－	1 ※ 4	1
任意チャネル着信サービス	SAV	On ※ 5	On ※ 5	Off

(凡例)　－：設定しない
注※ 1　モード A/B については「表 10-9　使用条件によって異なる設定」も参照してください。
注※ 2　呼番号長は 2 固定です。
注※ 3　「呼番号長 (網側)」は，この回線契約時に指定した呼番号長 (1 または 2) を設定します。「呼番号長 (TE 側)」は，本装置の line 構成定義情報の「call_reference_length」で設定された値 (1 または 2) を設定します。本装置で「call_reference_length」が設定されていない場合は 2 の設定となります。ただし，通常は「呼番号 (網側)」と「呼番号 (TE 側)」は同じ設定をしてください。つまり，回線契約時に指定した呼番長と，本装置の「call_reference_length」の設定値は同じにする必要があります。
障害切り分けなどのために，TA を介さないで本装置を網に直接接続する場合，網の「呼番号長」の契約を変更，または本装置「call_reference_length」の構成定義情報を変更しないでそのまま直接接続できるためです。
注※ 4　本装置の line 構成定義情報の「interface_id(インタフェース ID)」の設定 (「表 10-7　本装置の構成定義情報」参照) と同じにする必要があります。
注※ 5　回線契約時，「任意チャネル着信サービス」を申し込む必要があります。

(b) 使用条件による設定

使用条件によって異なる TA の設定を次の表に示します。なお，表中の各設定項目の説明については，TA の取扱説明書を参照してください。

表 10-9 使用条件によって異なる設定

設定項目		設定範囲	TA のデフォルト値
項目名	コマンド名		
バルク伝送方式モード A/ モード B	BMOD	ModeA/ModeB	ModeA
呼接続時間短縮	CMOD	Single/Dual	Single
着信タイミング	SLOW	Fast/Slow	Fast
識別着信	DISC	Off/On	Off

● バルク伝送方式モード A/ モード B の注意事項

「ModeB」の場合は，1 本余分に B チャネルを接続するため，その分通信料金も課金されるので注意が必要です。

● 呼接続時間短縮の注意事項

- 「Dual」の場合は，着信側にも約半分の通信料金が課金されるので注意が必要です。なお，「isdn-ppp」の構成定義情報の「channel_type」を「h1」(1536kbit/s) で使用する場合，TA-TA 間で計 24 個の B チャネルを接続します。しかし，接続する距離が遠距離，または使用回線業者の ISDN 回線の仕様によって，全チャネル接続完了までに時間がかかり，着信側の本装置で PPP リンク切断を検出する場合があります。

  発信側の TA は全 24 個の B チャネルが接続完了後，端末 (本装置) 宛てに通信できることを通知するのに対し，着信側の TA は 1B チャネルが接続完了後，端末 (本装置) 宛てに通信できることを通知します。このため，発信／着信側の本装置で PPP のリンク設定を開始するまでの時間に差が出ます。

  PPP リンク切断を検出したときに着信側の本装置で表示するログ情報を次に示します。

  ・イベント発生部位：PPP

  ・メッセージ認識子：17010006

  ・メッセージテキスト：

  The PPP connection has been terminated via peer's request.

  Make the peer router open the connection if you need it.(PPP リンク切断)

  このような場合は，この設定項目を「Dual」に設定してください。着信側にも課金されるので注意が必要です。

  着信側に課金できない場合，「着信タイミング」を「Slow」に変更してください。「Slow」の場合，着信側の TA も全 24 個の B チャネルが接続完了後，端末 (本装置) 宛てに通信できることを通知するため，発信／着信側の本装置で PPP のリンク設定を開始するまでの時間に差が出ません。

  なお，「Slow」で使用する場合，「着信タイミングの注意事項」の内容を確認してから使用してください。「Slow」に設定すると，TA-ISDN 網間で全 B チャネルを接続後，着信側端末に対して着信を通知するため，着信側端末が接続を許可しない相手 (電話番号) からの着信などを拒否した場合は，ISDN がいったん接続したあとに切断することになり，課金が発生します。この場合は「識別着信」を「On」に設定することで回避できます。

● 着信タイミングの注意事項

次に示す理由から，「Fast」に設定してください。

- 着信タイミングを「Slow」に設定した場合，TA-ISDN 網間で全 B チャネルを接続後，着信側端末に対して着信を通知するため，着信側端末が接続を許可しない相手 (電話番号) からの着信などを拒否した場合は，ISDN がいったん接続したあとに切断することになり，課金が発生します。
- 「Slow」に設定すると ISDN がいったん接続します。しかし，このとき着信側の端末が切断理由を「通信拒否」として着信を拒否しても，着信側の TA は (ISDN が接続済みであることから) 発信側に対して切断理由を「正常切断」として切断します。このため，発信側の端末 (本装置) で，相手局か

ら切断された本当の理由が不明になります。例えば，相手局が「接続を許可しない相手 (電話番号) からの着信」の理由で，切断理由を「通信拒否」として着信を拒否した場合，自局 (本装置) で表示するログ情報は次に示すように異なります。

・着信タイミング＝ Slow の場合：
  ・イベント発生部位：LINEWAN
  ・メッセージ識別子：ObOlOOO4
  ・メッセージテキスト：
    The peer router has disconnected the ISDN call.(相手局からの切断)
  ・付加情報 (切断理由)：正常切断
・着信タイミング＝ Fast の場合：
  ・イベント発生部位：LINEWAN
  ・メッセージ識別子：ObO90001
  ・メッセージテキスト：
    The originating call from this router has been refused.
      Check phone number configuration of this router and the peer.(相手局着信拒否)

各ログ情報の詳細は，マニュアル「メッセージ・ログレファレンス　3. 装置関連の障害およびイベント情報」を参照してください。

● 識別着信の注意事項

着信側の端末が，着信に対する応答 (許可) を着信側 TA に対して返したあとに初めて TA が ISDN を接続します。このため，「着信タイミング」を「Fast」に設定している場合は，課金が発生するという問題は発生しません。また，本装置には接続を許可する相手をチェックする認証機能があるので，識別着信を「On」にする必要はありません。

本装置の認証機能については，「解説書 Vol.1　5.2.3 認証」を参照してください。また，認証を行うための構成定義情報については，マニュアル「構成定義コマンドレファレンス Vol.1」の isdn-ppp コマンドを参照してください。

(c) ISDN 回線契約条件

TA に接続する ISDN 回線の契約条件は，TA を介さないで本装置を直接 ISDN 回線に接続する場合の契約条件と同じにしてください。本装置を直接 ISDN 回線に接続する場合の契約条件は，「10.2.3　ISDN 回線契約条件」を参照してください。

(d) 接続時間

この TA はバルク伝送を行うために，通信速度に相当する B チャネルの個数分対向の TA と呼接続するため (例：Hl チャネル (1536kbit/s) で通信する場合，B チャネル (64kbit/s) × 24)，端末から発信を行ってから通信相手と通信できる状態になるまでに時間がかかります。通信相手との接続時間を次の表に示します。なお，使用する回線業者の ISDN 回線の仕様，通信相手との距離などによってこの表の接続時間は増減しますので，表中の時間は目安です。

表 10-10　通信相手との接続時間

TA の「呼接続時間短縮」の設定	端末 (本装置) から発信するときのチャネル種別 (通信速度)	通信可能までのおよその時間※
Single	HO チャネル (384kbit/s)	14 秒
	Hl チャネル (1536kbit/s)	27 秒
Dual	HO チャネル (384kbit/s)	12 秒
	Hl チャネル (1536kbit/s)	18 秒

注※　本装置が ISDN 呼切断状態中に，本装置から通信相手に ping を発行してから，通信相手との間で PPP のデータリンクが確立するまでの時間を指します。

(e) 発着信についての注意事項

● TA 間の発着信衝突

この TA は仕様上，TA 間で ISDN の発着信が衝突した場合は通信できません。
このため，本装置で発着信の方向を制限する (発信専用／着信専用) など，TA 間で ISDN の発着信衝突が発生しないように注意してください。特にこの TA を専用線のバックアップの ISDN 回線に使用する場合は，バックアップ時に発着信衝突が発生する可能性が高くなります。
本装置で発着信の方向を制限する (発信専用／着信専用) 場合は，isdn － ppp 構成定義情報の「call － direction」オプションを設定してください。デフォルト値は「発着両用」です。設定方法については，マニュアル「構成定義コマンドレファレンス Vol.1」の isdn-ppp コマンドを参照してください。

● 発着信中の別の通信相手からの着信

この TA は仕様上，発着信中に別の端末 (発着信を行っている相手以外の相手) から着信があった場合，通信できなくなります。
この相手が通信を許可しない相手の場合は，TA の「識別着信」の設定を「On」にして，通信を許可する相手以外の相手からの着信を受けないようにしてください。
この相手が通信を許可する相手の場合は，本装置で発着信の方向を制限する (発信専用／着信専用) など，発着信中に別の通信相手からの着信が発生しないようにしてください。

10.3 ATM サービス

本装置が接続できる ATM サービスを次の表に示します。

表 10-11 接続できる ATM サービス

分類	サービス名称	会社名	備考
固定帯域保証型の VP サービス	ATM 専用サービス (ATM メガリンクサービス)	• 日本電信電話株式会社東日本 • 日本電信電話株式会社西日本 • エヌ・ティ・ティコミュニケーションズ	• サービス品目 0.5Mbit/s, 1Mbit/s ～ 135Mbit/s ※2 • 3 クラスのサービスクラス (デュアル，エクストラ，シングル) • 回線内速度設定サービスあり
セルリレーサービス	スーパーリレー CR	• 日本電信電話株式会社東日本 • 日本電信電話株式会社西日本 • エヌ・ティ・ティコミュニケーションズ	• サービスカテゴリ CBR, VBR，UBR • サービス品目 CBR PCR 16kbit/s ～ 10Mbit/s ※1※2 VBR SCR 16kbit/s ～ 6Mbit/s ※1※2 PCR 16kbit/s ～ 48Mbit/s ※1※2 UBR PCR 16kbit/s ～ 10Mbit/s ※1※2 • フレームリレーインターワーク
VC サービス	ATM データ通信網サービス (メガデータネッツ)	• 日本電信電話株式会社東日本 • 日本電信電話株式会社西日本	• 網加入型契約 • 保証型 (CBR)，一部保証型 (GFR)

注※ 1 本装置の通信速度 (PCR，SCR など) の設定範囲は 38kbit/s ～ 149760kbit/s です。16kbit/s ～は指定できないので注意が必要です。
注※ 2 契約した通信速度でシェーピングしたい場合は，契約通信速度を設定してください。本装置は，設定された通信速度に対してシェーピング精度は 0.3%の誤差がありますが，ソフトウェアで自動的に 0.3% 程度小さく設定しています。

10.3.1 ATM メガリンクサービス

本装置が固定帯域保証型の VP サービスに接続する場合について，日本電信電話株式会社 (日本電信電話株式会社) の ATM 専用サービスである ATM メガリンクサービスを例として示します。本装置が接続できるサービス品目を次の表に示します。

表 10-12 接続できるサービス品目 (ATM メガリンクサービス)

端末回線の種類	物理インタフェース	サービス品目	備考
1 芯式 (PDS 方式)	光 155.52Mbit/s ITU-T G.957	0.5Mbit/s 1 ～ 44Mbit/s(1Mbit/s 単位)	ONU に接続
	メタル 25.6Mbit/s TTC JT-I432.5	0.5Mbit/s 1Mbit/s ～ 24Mbit/s(1Mbit/s 単位)	ONU に接続
2 芯式 (SS 方式)	光 155.52Mbit/s ITU-T G.957	0.5Mbit/s 1 ～ 135Mbit/s(1Mbit/s 単位)	DSU に接続

(1) ケーブルおよびコネクタの設定

回線のタイプが OC-3c/STM-1 ATM の場合，マルチモード光ファイバで接続します。ONU，DSU 側コネクタは単芯 SC です。また，回線のタイプが 25Mbit/s ATM の場合，UTP ケーブルで接続します。ONU，DSU 側コネクタは RJ-45 です。

(2) 構成定義条件

回線のタイプが OC-3c/STM-1 ATM の場合の，接続時の構成定義条件を次の表に示します。

表 10-13 接続時の構成定義条件

構成定義コマンド	パラメータ	設定値	備考
line	clock	external (デフォルト値)	2 芯式 (SS 方式) で接続の場合だけ，1 芯式 (PDS 方式) で接続の場合は don't care
	frame_format	sdh_idle (デフォルト値)	―

(凡例) ―：該当しない

接続上の条件となる項目についてはデフォルト値の状態であれば特に設定する必要はありません。また，回線のタイプが 25Mbit/s ATM の場合は接続上の条件となる構成定義パラメータはありません。

(3) サービスカテゴリの設定

本装置は同一の VP 内の各 VC について指定されたサービスカテゴリおよびプライオリティに従って出力優先制御を行います。このため，同一の VP 内で使用する VC 数に応じた設定をすれば，効率の良い通信が実現できます。次に基本的な考え方および設定例を示します。

- VP サービスを介して通信するトラフィックを分けないで 1VC に通す場合，サービスカテゴリは CBR が適しています。同一 VP 内の VC 数が 1 本の場合，出力優先制御は関係ありません。
- VP 内に複数の VC を設定し，トラフィックの特徴に応じたサービスカテゴリおよびプライオリティを設定する場合，最も優先度の高いフローに対し CBR を，優先度の低いフローには，ABR や UBR などのレート制御を行うサービスカテゴリを設定します。こうすれば，空き帯域を有効利用できます。
  なお，サービスカテゴリ GFR/GFR2 を設定することもできます。ただし，トラフィックパラメータの設定範囲には，サービスカテゴリパターンに応じた制約があるので注意が必要です。サービスカテゴリ GFR/GFR2 設定時の制約条件を次の表に示します。

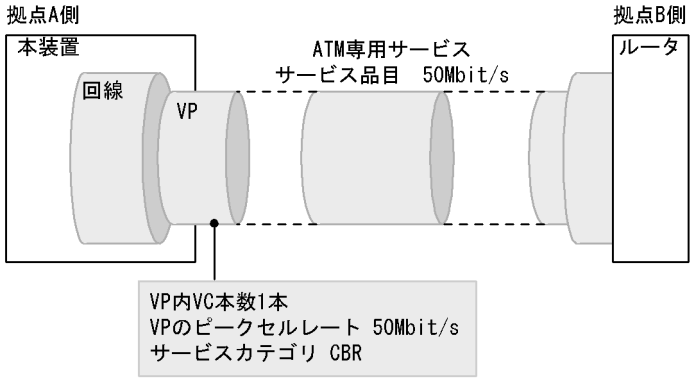
表 10-14 サービスカテゴリ GFR/GFR2 設定時の制約条件

GFR(サービスカテゴリパターン =gfr_clp_priority)		GFR2(サービスカテゴリパターン =gfr2s)			GFR2(サービスカテゴリパターン =gfr2m)		
mcr	pcr	mcr	pcr	priority4_pcr	mcr	pcr	priority4_pcr
250kbit/s ～	～ 135Mbit/s	250kbit/s ～ 500kbit/s	～ 500kbit/s	250kbit/s ～ 500kbit/s	3Mbit/s ～	～ 135Mbit/s	2.5Mbit/s ～
		250kbit/s ～ 135Mbit/s	501kbit/s ～ 135Mbit/s	500kbit/s ～ 135Mbit/s			

(4) VP 単位に帯域を確保する場合

拠点 A，B 間を ATM 専用サービスを利用して接続します。ATM 専用サービスは VP サービスなので，拠点 A，B 間のトラフィックに対し 50Mbit/s を用意する場合，50Mbit/s の VP を 1 本契約します。この場合，本装置は VP のピークセルレートを 50Mbit/s に設定すると，指定帯域について VP シェーピングします。また，ATM 専用サービスは固定の帯域を保証しますので，本装置のサービスカテゴリは CBR が適しています。本装置の設定項目を次の図に示します。

図 10-2　本装置の設定項目 (VP 単位に帯域を確保する場合)



(5) フローごとに固定の帯域を割り当てる場合

拠点 A，B 間を ATM 専用サービスを利用して接続します。拠点 A，B 間のトラフィック全体に対し 50Mbit/s の帯域を用意し，三つの業務部門にそれぞれ 20Mbit/s，20Mbit/s，10Mbit/s の固定の帯域を割り当てる例について示します。

この場合，50Mbit/s の契約帯域を 20Mbit/s，20Mbit/s，10Mbit/s の 3 本の VP に分けて設定します。本装置は VP のピークセルレートをそれぞれ 20Mbit/s，20Mbit/s，10Mbit/s に設定すると，指定された帯域で VP シェーピングします。さらに ATM 専用サービスの回線内速度設定サービスを利用すると，ATM ネットワーク内でも VP ごとの帯域が保証されます。本装置の設定項目を「図 10-3　本装置の設定項目 (フローごとに固定の帯域を割り当てる場合)」に示します。また，各 VC の設定内容例を「表 10-15　各 VC の設定内容 (フローごとに固定の帯域を割り当てる場合)」に示します。

なお，同一対地間のトラフィックをフローごとに異なる VC を使用して通信するためにパラレル PVC を設定する必要があります。しかし，この機能は本装置独自の機能なので，ATM ネットワークを介して接続する相手装置が本装置である場合だけに使用してください。

図 10-3　本装置の設定項目（フローごとに固定の帯域を割り当てる場合）

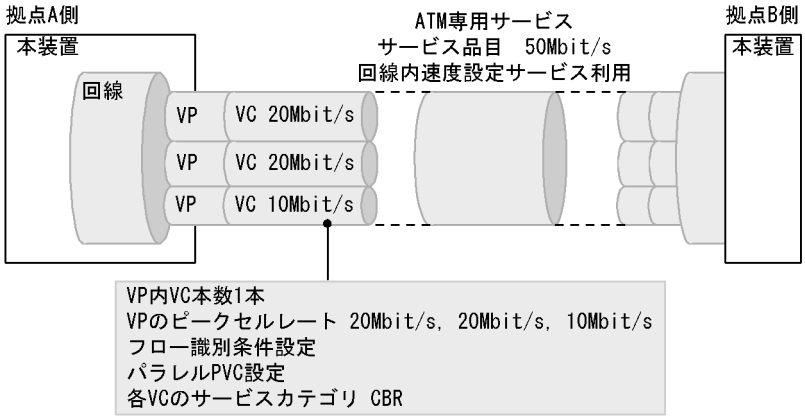


表 10-15　各 VC の設定内容（フローごとに固定の帯域を割り当てる場合）

VPI ／ VCI	帯域	サービスカテゴリ	用途
0 ／ 32	20Mbit/s	CBR	研究開発部門
1 ／ 32	20Mbit/s	CBR	営業部門
2 ／ 32	10Mbit/s	CBR	総務部門

(6) フローのトラフィック特性に応じた優先制御を行う場合

拠点 A，B 間を，ATM 専用サービスを利用して接続します。拠点 A，B 間のトラフィックに対し 30Mbit/s の帯域を用意します。CBR，UBR の VC を設定し，フローをトラフィック特性に応じた VC 割り当て，出力優先制御を行います。

また，UBR の動的なレート制御によって空き帯域を有効利用します。本装置の設定項目を「図 10-4　本装置の設定項目（フローのトラフィック特性に応じた優先制御を行う場合）」に示します。また，各 VC の設定内容を「表 10-16　各 VC の設定内容（フローのトラフィック特性に応じた優先制御を行う場合）」に示します。

図 10-4　本装置の設定項目（フローのトラフィック特性に応じた優先制御を行う場合）

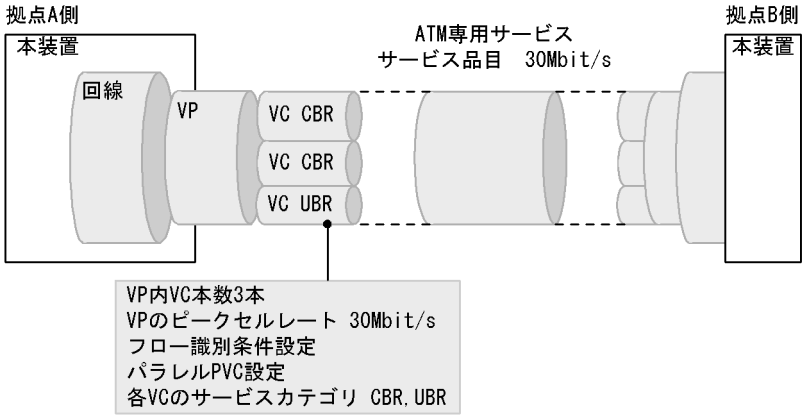


表 10-16 各 VC の設定内容 (フローのトラフィック特性に応じた優先制御を行う場合)

VPI ／ VCI	帯域	サービスカテゴリ および出力優先度	用途
0 ／ 32	ピークセルレート 10Mbit/s	CBR 最高位優先度	映像系 AP
0 ／ 33	ピークセルレート 20Mbit/s	CBR 第 2 位優先度	基幹業務 AP
0 ／ 34	ピークセルレート 30Mbit/s	UBR	メール

(7) 優先度によるフロー分けを使ったエクストラクラス利用

エクストラクラスは日本電信電話株式会社 (日本電信電話株式会社) の ATM メガリンクサービスのサービスクラス名称です。契約帯域をメインパス，サブパスの 2 本の VP に分割して使用し，故障時にメインパス帯域を保証することを特徴としています。このようなサービス形態をとることによってデュアルクラス (通常クラス) より割安な通信料金となっています。

次に本装置に接続した場合のエクストラクラスの利用例を示します。

- 拠点 A，B 間を ATM 専用サービスを利用し，サービスクラスはエクストラクラスとします。
- 拠点 A，B 間のトラフィックに対しメインパス 15Mbit/s，サブパス 15Mbit/s とします。
- 優先度の高いフローをメインパスに，優先度の低いフローをサブパスに流すよう設定すれば，ATM サービスの故障時にもメインパス側の帯域は保証されます。

本装置の設定項目を「図 10-5 本装置の設定項目 (優先度によるフロー分けを使ったエクストラクラス利用)」に示します。また，各 VC の設定内容を「表 10-17 各 VC の設定内容 (優先度によるフロー分けを使ったエクストラクラス利用)」に示します。

図 10-5 本装置の設定項目 (優先度によるフロー分けを使ったエクストラクラス利用)

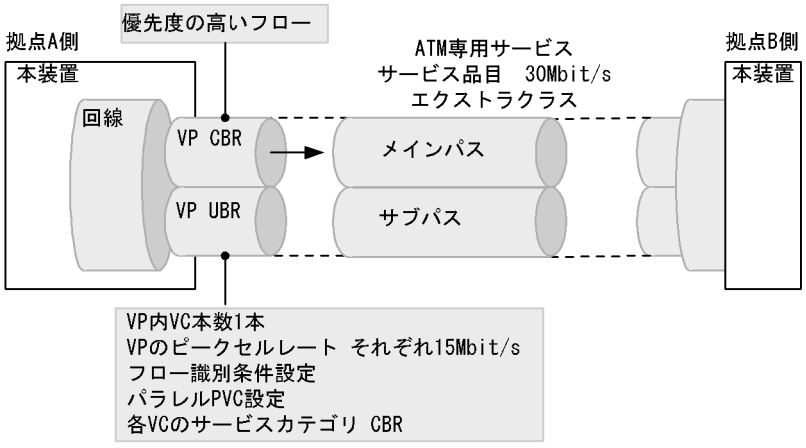


表 10-17 各 VC の設定内容 (優先度によるフロー分けを使ったエクストラクラス利用)

VPI ／ VCI	帯域	サービスカテゴリ	用途
0 ／ 32	ピークセルレート 15Mbit/s	CBR	メインパス 優先度の高いフローを割り当て
1 ／ 32	ピークセルレート 15Mbit/s	CBR	サブパス 優先度の低いフローを割り当て

10.3.2 セルリレーサービス

本装置がセルリレーサービスに接続する場合について，日本電信電話株式会社 (NTT) のセルリレーサービスであるスーパーリレー CR を例として示します。本装置が接続できるサービス品目について「表 10-18　接続できるサービス品目 (セルリレーサービス)」に示します。また，サービスカテゴリごとの接続性を「表 10-19　サービスカテゴリごとの接続性」に示します。

表 10-18　接続できるサービス品目 (セルリレーサービス)

アクセス方式	物理インタフェース	サービス品目	備考
第 2 種 PDS 方式	光 155.52Mbit/s ITU-T G.957	0.5Mbit/s 1 ～ 44Mbit/s(1Mbit/s 単位)	ONU に接続
	メタル 25.6Mbit/s TTC JT-I432.5	0.5Mbit/s 1Mbit/s ～ 24Mbit/s(1Mbit/s 単位)	ONU に接続
第 2 種 SS 方式	光 155.52Mbit/s ITU-T G.957	0.5Mbit/s 1 ～ 135Mbit/s(1Mbit/s 単位)	DSU に接続
第 3 種	光 155.52Mbit/s ITU-T G.957	45Mbit/s 135Mbit/s	―

(凡例)　― : 該当しない

表 10-19　サービスカテゴリごとの接続性

サービスカテゴリ	接続制御	フレームリレーインターワーク	本装置の接続性
CBR	PVC	―	○
	SVC	―	×
VBR	PVC	インターワークあり	△
		インターワークなし	△
UBR	PVC	―	○

(凡例)　○ : サポートする　△ : 計画中　× : サポートしない　― : 該当しない

(1) 構成定義条件

「10.3.1　ATM メガリンクサービス (2) 構成定義条件」を参照してください。

(2) サービスカテゴリの設定

セルリレーサービスは利用するサービスによって，VP サービスの場合と VC サービスの場合があります。それぞれについてのサービスカテゴリ設定の考え方を次に示します。

- VP サービスに接続する場合
  「10.3.1　ATM メガリンクサービス (3) サービスカテゴリの設定」を参照してください。
- VC サービスに接続する場合
  接続するサービスのサービスカテゴリに合わせて本装置のサービスカテゴリを設定してください。
- サービスカテゴリ VBR 使用上の注意事項
  スーパーリレー CR の VC サービスのように VC 単位で UPC が行われるサービスに接続する場合は，セル廃棄が行われる可能性があるため，次に示す範囲で設定してください。
  - サステーナブルセルレートはピークセルレートの 65%以下
  - MBS は 5 以上 (デフォルト値は 30)

10.3.3 メガデータネッツ

本装置が VC サービスに接続する場合について，日本電信電話株式会社 (NTT) の ATM データ通信網サービスであるメガデータネッツを例として示します。本装置が接続できるサービス品目を次の表に示します。

表 10-20 接続できるサービス品目 (メガデータネッツ)

物理インタフェース	基本帯域	サービス品目			
		PVC(相手固定通信) メニュー		CUG(グループ内通信) メニュー	
		速度保証タイプ	一部速度保証タイプ	速度保証タイプ	一部速度保証タイプ
光 155.52Mbit/sITU-T G.957	3Mbit/s ～ 42Mbit/s (3Mbit/s 単位)	※ 1	※ 2	※ 1	※ 2
メタル 25.6Mbit/sTTC JT-I432.5	3Mbit/s ～ 24Mbit/s (3Mbit/s 単位)				

注※ 1 「表 10-21 各サービスメニューの本装置の設定情報 (速度保証タイプ)」を参照してください。
注※ 2 「表 10-22 各サービスメニューの本装置の設定情報 (一部速度保証タイプ)」を参照してください。

(1) 構成定義条件

「10.3.1 ATM メガリンクサービス (2) 構成定義条件」を参照してください。

サービスカテゴリパターンは gfr2s を必ず使用してください。サービスカテゴリパターン gfr2s 以外は使用しないでください。

収容できる VC 数は最大 128 本です。128 本を超える場合は回線の増設 (NIF の増設) が必要です。

メガデータネッツの一部速度保証タイプ (GFR) の保証速度 (MCR) 設定については，本装置での最優先度キュー内ピークセルレートの設定値とメガデータネッツと契約する保証速度との大小関係によって 2 種類の使い方があります。

- メガデータネッツの保証速度以下の帯域を priority4_pcr に設定した場合 (帯域制御モード)
  本装置は，最優先度キューに割り当てたパケットを CLP=0 で priority4_pcr (= 保証速度以下の帯域) で送信します (最優先度キュー以外 CLP=1)。一方，メガデータネッツは，端末から受信した CLP=0 のパケットが保証速度を超えないかぎり，網の輻輳状態に関係なく該当 CLP=0 のパケットを廃棄しないという機能を提供します。このため，この方法では，本装置の最優先度キューを通過させた CLP=0 のパケットは，網の輻輳状態に関係なく網内で廃棄されません。したがって，本装置の最優先度キューに入ったパケットは，常に保証速度以下で網内を転送できます。
  メガデータネッツのサービスメニューについて，本設定が一部分サポートされていません。詳細は「表 10-22 各サービスメニューの本装置の設定情報 (一部速度保証タイプ)」を参照してください。
  なお，priority4_pcr は最優先度キュー内ピークセルレート，CLP は Cell Loss Priority(セル損失優先表示) ビット (0：廃棄非優先，1：廃棄優先) を示します。
- メガデータネッツの保証速度を超えた帯域を priority4_pcr に設定した場合 (優先制御モード)
  本装置は，最優先度キューに割り当てたパケットを CLP=0 で priority4_pcr (= 保証速度を超える帯域) で送信します (最優先度キュー以外 CLP=1)。一方，メガデータネッツは，網輻輳時に CLP=0 のパケットに比べて CLP=1 のパケットを優先して廃棄する特性を持っています。このため，この方法では，本装置の最優先度キューを通過させた CLP=0 のパケットが網内で転送されるかどうかは，網の輻輳状

況に依存します。したがって，本装置の最優先度キューに入ったパケットは，網内でベストエフォート的に動作します。
なお，priority4_pcr は最優先度キュー内ピークセルレート，CLP は Cell Loss Priority(セル損失優先表示) ビット (0：廃棄非優先，1：廃棄優先) を示します。

メガデータネッツ仕様の推奨値である最大フレームサイズ (MFS：1 フレームの最大セル数)32 に合わせ，MTU 長を 1520 バイト以下に設定することをお勧めします。

また，同一 VP 内で VC のミニマムセルレート合計が VP のピークセルレート－ 250kbit/s 以下となるように設定してください。

そのほかの構成定義設定値については，「表 10-21　各サービスメニューの本装置の設定情報 (速度保証タイプ)」および「表 10-22　各サービスメニューの本装置の設定情報 (一部速度保証タイプ)」を参照してください。

最優先度キューだけを使用しているときは，VC 帯域が有効活用できません。有効活用したいときは高優先度 / 中優先度 / 低優先度キューも同時に使用してください。

(2) F5-OAM Loopback セルによる VC 状態監視機能との同時使用について

F5-OAM Loopback セルによる VC 状態監視機能は，メガデータネッツの速度保証タイプだけ使用してください。一部速度保証タイプの使用は，網内が輻輳していると F5-OAM セルが廃棄される可能性があるためお勧めしません。なお，VC 監視数の最大は 64 です。VC 状態監視機能については，「解説書 Vol.1 6.3.3(3) Loopback セルによる VC 状態監視機能」を参照してください。

VC 状態監視機能を使用するとき，本装置の ATM インタフェースより F5-OAM Loopback セルと一緒に制御用パケットが同時に送信されます。接続相手装置によっては，接続相手装置側で制御用パケット受信によってエラーカウントアップするケースがあります。

(3) サービスカテゴリの設定

各サービスメニューの本装置の設定情報を，速度保証タイプで契約した VC に対するトラフィックパターンと一部速度保証タイプで契約した VC に対するトラフィックパターンに分けて，「表 10-21　各サービスメニューの本装置の設定情報 (速度保証タイプ)」および「表 10-22　各サービスメニューの本装置の設定情報 (一部速度保証タイプ)」に示します。なお，サービスカテゴリ GFR2 では，一部速度保証タイプの保証速度 (MCR) で重要なフレームを CLP=0 で送信できます (非重要パケットは CLP=1 で送信)。

表 10-21　各サービスメニューの本装置の設定情報 (速度保証タイプ)

サービスメニュー 速度保証タイプ (単位：bit/s)	サービスカテゴリパターン =gfr2s(単位：bit/s)		
	構成定義情報パラメータ設定値 (VC への設定) ※1		
品目	pcr	mcr	priority4_pcr
64k	64k ※2	64k ※2	64k ※2
128k	128k ※2	128k ※2	128k ※2
192k	192k ※2	192k ※2	192k ※2
256k	256k	256k	250k 以上
384k	384k	384k	250k 以上
0.5M	0.5M	0.5M	250k 以上

サービスメニュー 速度保証タイプ (単位：bit/s)	サービスカテゴリパターン =gfr2s(単位：bit/s)		
	構成定義情報パラメータ設定値 (VC への設定) ※1		
1M	1M	1M	500k 以上
2M	2M	2M	500k 以上

注※ 1　pcr は VC のピークセルレート，mcr はミニマムセルレート，priority4_pcr は最優先度キュー内ピークセルレートを示します。
注※ 2　該当する VC を収容する VP 内には一部速度保証タイプの VC を混在させることができません。

表 10-22　各サービスメニューの本装置の設定情報 (一部速度保証タイプ)

サービスメニュー (単位：bit/s)		サービスカテゴリパターン (単位：bit/s)				
		構成定義情報パラメータ設定値 (VC への設定) ※1				
一部速度保証タイプ		pcr	mcr	本装置仕様	priority4_pcr ※2	
最高速度	保証速度			保証速度で CLP=0 送信できる最小値	優先制御モード	帯域制御モード (保証速度で CLP=0 送信)
0.5M	0.1M	500k	500k	250k 以上	500k	未サポート
0.5M	0.3M	500k	500k	250k 以上	500k	300k
1M	0.1M	1000k	1000k	500k 以上	1000k	未サポート
1M	0.5M	1000k	1000k	500k 以上	1000k	500k
2M	0.2M	2000k	2000k	500k 以上	2000k	未サポート
2M	1.0M	2000k	2000k	500k 以上	2000k	1000k
3M	0.3M	3000k	3000k	500k 以上	3000k	未サポート
3M	1.5M	3000k	3000k	500k 以上	3000k	1500k
4M	0.4M	4000k	4000k	500k 以上	4000k	未サポート
4M	2.0M	4000k	4000k	500k 以上	4000k	2000k
5M	0.5M	5000k	5000k	500k 以上	5000k	500k
5M	2.5M	5000k	5000k	500k 以上	5000k	2500k
6M	0.6M	6000k	6000k	500k 以上	6000k	600k
6M	3.0M	6000k	6000k	500k 以上	6000k	3000k
7M	0.7M	7000k	7000k	500k 以上	7000k	700k
7M	3.5M	7000k	7000k	500k 以上	7000k	3500k
8M	0.8M	8000k	8000k	500k 以上	8000k	800k
8M	4.0M	8000k	8000k	500k 以上	8000k	4000k
9M	0.9M	9000k	9000k	500k 以上	9000k	900k
9M	4.5M	9000k	9000k	500k 以上	9000k	4500k
10M	1.0M	10000k	10000k	500k 以上	10000k	1000k
10M	5.0M	10000k	10000k	500k 以上	10000k	5000k

注※１　pcr は VC のピークセルレート，mcr はミニマムセルレート，priority4_pcr は最優先度キュー内ピークセルレートを示します。
注※２　優先制御モード，帯域制御モードについては，「(1) 構成定義条件」を参照してください。

付録

付録 A　準拠規格

付録 B　謝辞 (Acknowledgments)

付録 C　用語解説

付録 A　準拠規格

付録 A.1　イーサネット

表 A-1　イーサネットインタフェースの準拠規格

種別	規格	名称
共通	ISO/IEC 8802.3 [ANSI/IEEE Std 802.3]	CSMA/CD Access Method and Physical Layer Specifications
共通	ISO 8802-2 [ANSI/IEEE Std 802.2]	Logical Link Control (LLC)
Ethernet	IEEE 802.3u	MAC Parameters, Physical Layer, Medium Attachment Units and Repeater for 100Mb/s Operation
Gigabit Ethernet	IEEE 802.3z	Media Access Control(MAC) Parameters, Physical Layer, Repeater and Management Parameters for 1000Mb/s Operation
共通	RFC 894	Standard for the Transmission of IP Datagrams over Ethernet Networks.
共通	RFC1042	Standard for the Transmission of IP Datagrams over IEEE802 Networks.
共通	RFC1398	Definitions of Managed Objects for the Ethernet-like Interface Types.
共通	RFC1757	Remote Network Monitoring Management Information Base.
共通	Ethernet V 2.0	The Ethernet-A Local Area Network:Data Link Layer and Physical Layer Specifications
共通	RFC2464	Transmission of IPv6 Packets over Ethernet Networks
共通	IEEE 802.1Q	IEEE Standards for Local and Metropolitan Networks：Virtual Bridged local Area Networks ※

注※　GVRP/GMRP はサポートしていません。

表 A-2　PPP over Ethernet クライアント機能の準拠規格

規格番号 (発行年月)	準拠規格
RFC2516(1999 年 2 月)	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC1661(1994 年 7 月)	The Point-to-Point Protocol (PPP)
RFC1332(1992 年 5 月)	The PPP Internet Protocol Control Protocol (IPCP)
RFC1877(1995 年 12 月)	PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
RFC1334(1992 年 10 月)	PPP Authentication Protocols
RFC1994(1996 年 8 月)	PPP Challenge Handshake Authentication Protocol (CHAP)
RFC1471(1993 年 6 月)	The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol
RFC1472(1993 年 6 月)	The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol
RFC1473(1993 年 6 月)	The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol

表 A-3　PPP over Ethernet クライアント機能の技術参考資料

技術参考資料	備考
IP 通信網サービスのインタフェース －フレッツシリーズ－ 第 2 版	東日本電信電話株式会社
光・IP 通信網サービスインタフェース 第 1 版	西日本電信電話株式会社
IP 接続サービスのインタフェース 第 2 版	西日本電信電話株式会社

付録 A.2　WAN

表 A-4　WAN 物理インタフェースの準拠規格

規格	名称
ITU-T V.24	List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)
ITU-T V.35	Data transmission at 48 kilobits per second using 60-108 kHz group band circuits
ITU-T X.21	Interface between data terminal equipment and data circuit-terminating equipment for synchronous operation on public data networks
ANSI/EIA RS-232	Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange
JT-I430-a	専用線基本ユーザ・網インタフェース　レイヤ 1 仕様
JT-I430	ISDN 基本ユーザ・網インタフェース　レイヤ 1 仕様
JT-I431-a	専用線一次群速度　ユーザ・網インタフェース　レイヤ 1 仕様
JT-I431	ISDN 一次群速度　ユーザ・網インタフェース　レイヤ 1 仕様
JT-G703-a	専用線二次群速度　ユーザ・網インタフェース　レイヤ 1 仕様
JT-G783　付属資料 B	SDH 多重変換装置の警報系・切替系の動作 付属資料 B　予備切替 (1 ＋ 1) のプロトコル，コマンド，操作
ITU-T G.703	専用線一次群速度 (2M)　ユーザ・網インタフェース　レイヤ 1 仕様
ITU-T G.703	専用線三次群速度 (2M)　ユーザ・網インタフェース　レイヤ 1 仕様
ITU-T I.431	Primary rate user-network interface - Layer 1 specification
ITU-T G.707	Network node interface for the synchronous digital hierarchy (SDH)
ITU-T G.751	Digital multiplex equipments operating at the third order digital multiplex equipments operating at the bit rate of 34,368 kbit/s and the fourth order bit rate of third order 139,264 kbit/s and using posilive justification.
ITU-T G.957	Optical interfaces for equipments and systems relating to the synchronous digital hierarchy
ITU-T G.958	Digital line systems based on the synchronous digital hierarchy for use on optical fiber cables
Bellcore TR-NWT-000253	Synchronous Optical Network (SONET) Transport Systems：Common Generic Criteria
ANSI/EIA T1.105	Telecommunications - Synchronous Optical Network (SONET) - Basic Description Including Multiplex Structures, Rates, and Formats
ANSI/EIA T1.403	Network-to-Customer Installation DSI Metaric Interface
ANSI T1.107	Digital Hierarchy Formats Specifications

表 A-5　PPP プロトコルの準拠規格

規格	名称
RFC1171	The Point-to-Point Protocol for the Transmission of Multi-Protocol Datagrams Over Point-to-Point Links
RFC1172	The Point-To-Point Protocol Initial Configuration Options
RFC1220	Point-to-Point Protocol Extensions for Bridging
RFC1331	The Point-to-Point Protocol (PPP) for the Transmission of Multi-Protocol Datagrams over Point-to Point Links
RFC1332	PPP Internet Protocol Control Protocol
RFC1334	PPP Authentication Protocols
RFC1548	The Point-to-Point-Protocol(PPP)
RFC1552	The PPP Internetwork Packet Exchange Control Protocol(IPXCP)
RFC1618	PPP over ISDN
RFC1619	PPP over SONET/SDH
RFC1661	The Point-To-Point Protocol(PPP)
RFC1662	PPP in HDLC-like Framing
RFC1717	The PPP Multilink Protocol(MP)
RFC1990	The PPP Multilink Protocol(MP)
RFC1994	PPP Challenge Handshake Authentication Protocol(CHAP)
RFC2125	The PPP Bandwidth Allocation Protocol(BAP) The PPP Bandwidth Allocation Control Protocol(BACP)
RFC2472	IP Version 6 over PPP

表 A-6　フレームリレープロトコルの準拠規格

規格	名称
ITU-T Recommendation Q.922 ※1	ISDN data link layer specification for frame mode bearer services
ITU-T Recommendation Q.933 ※2※3	Digital subscriber signalling system no. 1 (DSS 1) - signalling specifications for frame mode switched and permanent virtual connection control and status monitoring
ITU-T Recommendation I.370 ※4	Congestion management for the ISDN frame relaying bearer service
RFC2427 ※5	Multiprotocol Interconnect over Frame Relay
RFC2390 ※6	Inverse Address Resolution Protocol
RFC2115 ※7	Management Information Base for Frame Relay DTEs Using SMIv2
ANSI T1.617a ※8	ISDN- signalling specification for Frame Relay Bearer Service for Digital Subscriber
ANSI T1.606a	Supplement Congestion Management and Frame Size
ANSI T1.618	Digital subscriber signalling system no. 1 (DSS 1)- Core Aspects of Frame Relay Protocol for Use with Frame Relay Bearer Service

注※ 1　JT-Q922 はこの規格に準拠しています。
注※ 2　Annex A だけに準拠しています。
注※ 3　JT-Q933 はこの規格に準拠しています。
注※ 4　JT-I370 はこの規格に準拠しています。
注※ 5　旧規格 (RFC1490) 仕様の製品と接続できます。

注※ 6　旧規格 (RFC1293) 仕様の製品と接続できます。
注※ 7　RFC1315 の改訂規格です。
注※ 8　Annex D だけに準拠しています。

付録 A.3　ATM

表 A-7　ATM の準拠規格および勧告

レイヤ	規格または勧告番号	規格または勧告名称
物理層	I.432	B-ISDN User-Network Interface-Physical Layer Specification
	ATM Forum UNI	V3.0 ／ V3.1
	I.432.5	B-ISDN user-network interface-Physical layer specification：25600 kbit/s operation
	I.432.2	B-ISDN user-network interface-Physical layer specification：155.820 kbit/s and 622080 kbit/s
	ATM Forum PHY	622.08Mbit/s Physical layer specifications af-phy-0046.000
ATM 層	I.150	B-ISDN Asynchronous Transfer Mode Functional Characteristics
	I.361	B-ISDN ATM Layer Specification
	I.371	Traffic Control and Congestion Control in B-ISDN
	I.610	B-ISDN Operation and Maintenance Principles and Functions
	ATM Forum UNI	V3.0 ／ V3.1
	ATM Forum TM	Traffic Management Specification V4.0,Addendum to Traffic Management V4.0 for ABR parameter negotiation
	ATM Forum TM	Traffic Management Specification V4.1 af-tm-0121.000
AAL 層	I.362	B-ISDN ATM Adaptation Layer(AAL) Functional Description
	I.363.5	B-ISDN ATM Adaptation Layer(AAL) Specification:Type 5
LLC/ データリンク層	RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
	RFC 2225	Classical IP and ARP over ATM
	RFC 2492	IPv6 Over ATM Networks

付録 A.4　IPv4 ネットワーク

表 A-8　IP バージョン 4 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC791(1981 年 9 月)	Internet Protocol
RFC792(1981 年 9 月)	Internet Control Message Protocol
RFC826(1982 年 11 月)	An Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware
RFC922(1984 年 10 月)	Broadcasting Internet datagrams in the presence of subnets
RFC950(1985 年 8 月)	Internet Standard Subnetting Procedure
RFC1027(1987 年 10 月)	Using ARP to implement transparent subnet gateways
RFC1122(1989 年 10 月)	Requirements for Internet hosts-communication layers

規格番号 (発行年月)	規格名
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing (CIDR):an Address Assignment and Aggregation Strategy
RFC1812(1995 年 6 月)	Requirements for IP Version 4 Routers
RFC1933(1996 年 4 月)	Transition Mechanisms for IPv6 Hosts and Routers

表 A-9　DHCP/BOOTP リレーエージェントの準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1542(1993 年 10 月)	Clarifications and Extensions for the Bootstrap Protocol
RFC1812(1995 年 6 月)	Requirements for IP Version 4 Routers
RFC2131(1997 年 3 月)	Dynamic Host Configuration Protocol

表 A-10　DHCP サーバ機能の準拠規格

規格番号 (発行年月)	規格名
RFC2131(1997 年 3 月)	Dynamic Host Configuration Protocol
RFC2132(1997 年 3 月)	DHCP Options and BOOTP Vendor Extensions

表 A-11　DHCP クライアント機能の準拠規格

規格番号 (発行年月)	規格名
RFC2131(1997 年 3 月)	Dynamic Host Configuration Protocol
RFC2132(1997 年 3 月)	DHCP Options and BOOTP Vendor Extensions

表 A-12　DNS リレー機能の準拠規格

規格番号 (発行年月)	規格名
RFC1034(1987 年 3 月)	Domain names - concepts and facilities
RFC1035(1987 年 3 月)	Domain names - implementation and specification

表 A-13　NAT，NAPT 機能の準拠規格

規格番号 (発行年月)	規格名
RFC3022(2001 年 1 月)	Traditional IP Network Address Translator (Traditional NAT)
RFC2663(1999 年 8 月)	IP Network Address Translator (NAT) Terminology and Considerations

付録 A.5　RIP/OSPF

表 A-14　RIP/OSPF の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1058(1988 年 6 月)	Routing Information Protocol
RFC2453(1998 年 11 月)	RIP Version 2
RFC2328(1998 年 4 月)	OSPF Version 2

規格番号 (発行年月)	規格名
RFC1587(1994 年 3 月)	The OSPF NSSA Option
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing(CIDR): an Address Assignment and Aggregation Strategy

付録 A.6　BGP4

表 A-15　BGP4 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1771(1995 年 3 月)	A Border Gateway Protocol 4 (BGP-4)
RFC2796(2000 年 4 月)	BGP Route Reflection An alternative to full mesh IBGP
RFC1997(1996 年 8 月)	BGP Communities Attribute
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing(CIDR): an Address Assignment and Aggregation Strategy
RFC1965(1996 年 6 月)	Autonomous System Confederation for BGP
RFC2842(2000 年 5 月)	Capabilities Advertisement with BGP-4
RFC2918(2000 年 9 月)	Route Refresh Capability for BGP-4
RFC3056(1998 年 8 月)	Protection of BGP Sessions via the TCP MD5 Signature Option
draft-ietf-idr-restart-06.txt (2003 年 1 月)	Graceful Restart Mechanism for BGP ※

注※　Receiving Speaker の機能だけをサポートしています。

付録 A.7　IS-IS

表 A-16　IS-IS の準拠規格および勧告

規格番号	規格名
ISO 9542:1988	Information processing systems - Telecommunications and information exchange between systems - End system to Intermediate system routing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)
ISO/IEC 10589:1992	Information technology - Telecommunications and information exchange between system - Intermediate system to Intermediate system intra-domain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473)
RFC1195 (1990 年 12 月)	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
RFC2763 (2000 年 2 月)	Dynamic Hostname Exchange Mechanism for IS-IS
RFC2966 (2000 年 10 月)	Domain-wide Prefix Distribution with Two-Level IS-IS
RFC3373 (2002 年 9 月)	Three-Way Handshake for IS-IS Point-to-Point Adjacencies

規格番号	規格名
draft-ietf-isis-ipv6-03.txt (2001 年 4 月)	Routing IPv6 with IS-IS
draft-ietf-isis-hmac-03.txt (2001 年 7 月)	IS-IS Cryptographic Authentication
draft-ietf-isis-traffic-04.txt (2001 年 8 月)	IS-IS extensions for Traffic Engineering

付録 A.8　IPv4 マルチキャスト

表 A-17　IP マルチキャストの準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2236	Internet Group Management Protocol,Version2
Internet - Draft draft-ietf-idmr-dvmrp-v3-06.txt (1998 年 3 月)	Distance Vector Multicast Routing Protocol
Internet - Draft draft-ietf-pim-v2-dm-03.txt (1999 年 6 月)	Protocol Independent Multicast Version2 Dense Mode Specification
RFC2362	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Specification
Internet-Draft draft-ietf-pim-sm-v2-new-05.txt (2002 年 3 月) ※	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Specification(revised)

注※　この規格は PIM-SSM 関連部だけ準拠しています。

付録 A.9　IPv6 ネットワーク

表 A-18　IPv6 ネットワークの準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2373(1998 年 7 月)	IP Version 6 Addressing Architecture
RFC2460(1998 年 12 月)	Internet Protocol, Version 6 (IPv6) Specification
RFC2461(1998 年 12 月)	Neighbor Discovery for IP Version 6 (IPv6)
RFC2462(1998 年 12 月)	Ipv6 Stateless Address Autoconfiguration
RFC2463(1998 年 12 月)	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (Ipv6) Specification
RFC2473(1998 年 12 月)	Generic Packet Tunneling in IPv6 Specification
RFC2710(1999 年 10 月)	Multicast Listener Discovery for IPv6
RFC3056(2001 年 2 月)	Connectioin of IPv6 Domains via IPv4 Clouds

表 A-19　IPv6 DHCP サーバ機能の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC3315 (2003 年 7 月)	Dynamic Host Configuration Protocol for IPv6(DHCPv6)
draft-ietf-dhcpv6-opt-prefix-delegation-05.txt (2003 年 10 月)	IPv6 Prefix Options for DHCPv6
draft-ietf-dhc-dhcpv6-opt-dnsconfig-05.txt (2003 年 8 月)	DNS Configuration Options for DHCPv6
draft-ietf-dhc-dhcpv6-opt-timeconfig-03.txt (2003 年 10 月)	Time Configuration Options for DHCPv6
draft-ietf-dhc-dhcpv6-interop-01.txt (2003 年 4 月)	Results from Interoperability Tests of DHCPv6 Implementations

表 A-20　NAT-PT 機能の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2766(2000 年 2 月)	Network Address Translation-Protocol Translation (NAT-PT)

付録 A.10　RIPng/OSPFv3

表 A-21　RIPng/OSPFv3 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2080(1997 年 1 月)	RIPng for IPv6
RFC2740(1999 年 12 月)	OSPF for IPv6

付録 A.11　BGP4+

表 A-22　BGP4+ の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1771(1995 年 3 月)	A Border Gateway Protocol 4 (BGP-4)
RFC2545(1999 年 3 月)	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
RFC2858(2000 年 6 月)	Multiprotocol Extensions for BGP-4
RFC2842(2000 年 5 月)	Capabilities Advertisement with BGP-4
RFC2796(2000 年 4 月)	BGP Route Reflection An alternative to full mesh IBGP
RFC1965(1996 年 6 月)	Autonomous System Confederation for BGP
RFC2918(2000 年 9 月)	Route Refresh Capability for BGP-4
RFC1997(1996 年 8 月)	BGP Communities Attribute
RFC2385(1998 年 8 月)	Protection of BGP Sessions via the TCP MD5 Signature Option
draft-ietf-idr-restart-06.txt (2003 年 1 月)	Graceful Restart Mechanism for BGP ※

注※　Receiving Speaker の機能だけをサポートしています。

付録 A.12　IPv6 マルチキャスト

表 A-23　IPv6 マルチキャストの準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2710(1999 年 10 月)	Multicast Listener Discovery (MLD) for IPv6
RFC2362(1998 年 6 月)	Protocol Independent Multicast-Sparse Mode (PIM-SM): Specification
draft-ietf-pim-sm-v2-new-03.txt(2001 年 7 月) ※ 1	Protocol Independent Multicast-Sparse Mode (PIM-SM): Specification (revised)
draft-ietf-pim-sm-v2-new-05.txt(2002 年 3 月) ※ 2	Protocol Independent Multicast-Sparse Mode (PIM-SM): Specification (revised)

注※　この規格は IPv6 関連部だけ準拠しています。
注※　この規格は PIM-SSM 関連部だけ準拠しています。

付録 A.13　Diff-serv

表 A-24　Diff-serv の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2474(1998 年 12 月)	Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers
RFC2475(1998 年 12 月)	An Architecture for Differentiated Services
RFC2597(1999 年 6 月)	Assured Forwarding PHB Group
RFC2598(1999 年 6 月)	An Expedited Forwarding PHB

付録 A.14　ブリッジ

表 A-25　ブリッジの準拠規格および勧告

規格番号 (発行年月)	規格名
ANSI/IEEE Std 802.1D-1990 (1991 年 5 月)	Media Access Control(MAC) Bridges
IEEE 802.1I/D3-1992 (1992 年 8 月)	Supplement to Media Access Control (MAC) Bridges Fibre Distributed Data Interface (FDDI)
IEEE P802.1H/D3 (1992 年 6 月)	Draft Recommended Practice 802.1H:MEDIA ACCESS CONTROL (MAC) BRIDGEING OF ETHERNET V2.0 IN 802 LOCAL AREA NETWORKS

付録 A.15　SNMP

表 A-26　SNMP の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC 1155(1990 年 5 月)	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1157(1990 年 5 月)	A Simple Network Management Protocol(SNMP)
RFC 1213(1991 年 3 月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II

規格番号 (発行年月)	規格名
RFC 1354(1992 年 7 月)	IP Forwarding Table MIB
RFC 1471(1993 年 6 月)	The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol
RFC 1473(1993 年 6 月)	The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol
RFC 1474(1993 年 6 月)	The Definitions of Managed Objects for the Bridge Network Control Protocol of the Point-to-Point Protocol
RFC 1643(1994 年 7 月)	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 1657(1994 年 7 月)	Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2
RFC 1659(1994 年 7 月)	Definitions of Managed Objects for RS-232-like Hardware Devices using SMIv2
RFC 1757(1995 年 2 月)	Remote Network Monitoring Management Information Base
RFC 1850 (1995 年 11 月)	OSPF Version2 Management Information Base
RFC 1901(1996 年 1 月)	Introduction to Community-based SNMPv2
RFC 1902(1996 年 1 月)	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1903(1996 年 1 月)	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1904(1996 年 1 月)	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1905(1996 年 1 月)	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1906(1996 年 1 月)	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1907(1996 年 1 月)	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1908(1996 年 1 月)	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC 2115(1997 年 9 月)	Management Information Base for Frame Relay DTEs Using SMIv2
RFC 2233 (1997 年 11 月)	The Interfaces Group MIB using SMIv2
RFC 2452 (1998 年 12 月)	IP Version 6 Management Information Base for the Transmission Control Protocol
RFC 2454 (1998 年 12 月)	IP Version 6 Management Information Base for the User Datagram Protocol
RFC 2465 (1998 年 12 月)	Management Information Base for IP Version 6: Textual Conventions and General Group
RFC 2466 (1998 年 12 月)	Management Information Base for IP Version 6: ICMPv6 Group
RFC2495(1999 年 1 月)	Definitions of Managed Objects for the DS1,E1,DS2 and E2 Interface Types
RFC2496(1999 年 1 月)	Definitions of Managed Objects for the DS3/E3 Interface Type
RFC 2787(2000 年 3 月)	Definitions of Managed Objects for the Virtual Router Redundancy Protocol

付録 A.16　RADIUS

表 A-27　RADIUS の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service(RADIUS)

付録 A.17　VRRP

表 A-28　VRRP の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2338(1998 年 4 月)	Virtual Router Redundancy Protocol
draft-ietf-vrrp-ipv6-spec-02.txt (2002 年 2 月)	Virtual Router Redundancy Protocol for IPv6

付録 B　謝辞 (Acknowledgments)

[GateD]

Copyright notice:
(C) 1995, 1996, 1997, 1998 The Regents of the University of Michigan
All rights reserved.
Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators.
GateD Release 9.3.1
Copyright (C) 2001 by NextHop Technologies, Inc. and its licensors.
All rights reserved.
GateD Release 9.3.3
Copyright (C) 2003 NextHop Technologies, Inc.
All rights reserved.
Copyright (C) 2001 by NextHop Technologies, Inc. and its licensors.
All rights reserved.
Except as stated herein, none of the software and accompanying documentation "materials") provided by NextHop may be copied, reproduced, distributed, republished, downloaded, displayed, posted or transmitted in any form or by any means, including, but not limited to, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of NextHop. All copyright and other proprietary notices contained within NextHop materials must be retained unless otherwise stated. Permission terminates automatically if any of these terms or conditions is breached. Upon termination, all applicable NextHop materials must be immediately destroyed. Any unauthorized use of any NextHop materials may violate copyright laws, trademark laws, the laws of privacy and publicity, and communications regulations and statutes.
Notice: Acceptance of Terms of Use Use of NextHop material is subject to certain Terms of Use, which constitute a legal agreement between you and NextHop. By using this material, you acknowledge that you have read, understood, and agree to be bound by the Terms of Use. Please review the Terms of Use. A copy of NextHop's Terms of Use is available upon request or on the web at http://www.nexthop.com. If you do not agree to the terms, do not use these materials.
Restricted Rights Legend
This software and any associated documentation are provided with RESTRICTED RIGHTS. The Government's rights to use, modify, reproduce, release, perform, display or disclose are restricted by paragraph (b)(3) of the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation clause at DFAR 252.227-7014 (Jun 95), and the other restrictions and terms in paragraph (g)(3)(i) of Rights in Data-General clause at FAR 52.227-14, Alternative III (Jun 87) and paragraph (c)(2) of the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19 (Jun 87), contained in the above identified contract. Any reproduction of computer software or portions thereof marked with this legend must also reproduce the markings. Any person, other than the Government, who has been provided access to such software must promptly identify the Contractor. The Contractor/Licensor is NextHop Technologies, Inc. located at 517 West William Street, Ann Arbor, MI 48103.

[SNMP]

****

Copyright 1988-1996 by Carnegie Mellon University
All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose

and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
****

Some of this software has been modified by BBN Corporation and is a derivative of software developed by Carnegie Mellon University. Use of the software remains subject to the original conditions set forth above.
****

Some of this software is Copyright 1989 by TGV, Incorporated but subject to the original conditions set forth above.
****

Some of this software is Copyright (C) 1983,1988 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of California at Berkeley. 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'' without express or implied warranty.
****

* Primary Author:
Steve Waldbusser

* Additional Contributors:
Erik Schoenfelder (schoenfr@ibr.cs.tu-bs.de): additions, fixes and enhancements for Linux by 1994/1995.
David Waitzman: Reorganization in 1996.

Wes Hardaker <hardaker@ece.ucdavis.edu>: Some bug fixes in his UC Davis CMU SNMP distribution were adopted by David Waitzman

David Thaler <thalerd@eecs.umich.edu>: Some of the code for making the agent embeddable into another application were adopted by David Waitzman

Many more over the years...

[BSDI Internet Server]

BERKELEY SOFTWARE DESIGN, INC.

Copyright (C) 1992, 1993, 1994, 1995, 1996, 1997 Berkeley Software Design, Inc.
This product includes BSDI Internet Server developed by Berkeley Software Design, Inc.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in thedocumentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association

(CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

Contributors
Sun Microsystems, Inc.
Keith Muller
Mark Nudelman
Jan-Simon Pendry

AT&T (DAVID M. GAY)

Copyright (C) 1991 by AT&T.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHOR NOR AT&T MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

INFO-ZIP GROUP

This product includes Info-ZIP's software which is used for a part of the boot program. Info-ZIP's software (ZIP, UnZip and related utilities) is free and can be obtained as source code or executables from various bulletin board services and anonymous-ftp sites, including CompuServe's IBMPRO forum and ftp.uu.net:/pub/archiving/zip/*.

INTERNET SOFTWARE CONSORTIUM

Copyright (C) 1996 by Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

SIGMASOFT, TH. LOCKERT

Copyright (C) 1994 SigmaSoft, Th. Lockert <tholo@sigmasoft.com>
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SUN MICROSYSTEMS, INC.

Copyright (C) 1984, 1985, 1986, 1987, 1988, 1993 Sun Microsystems, Inc.

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.
2550 Garcia Avenue
Mountain View, California 94043

UNIVERSITY OF TORONTO

Copyright (C) 1986 by University of Toronto.
Written by Henry Spencer. Not derived from licensed software.

Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely,
subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from defects in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.

WASHINGTON UNIVERSITY IN SAINT LOUIS

Copyright (C) 1993, 1994 Washington University in Saint Louis
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the Washington University in Saint Louis and its contributors. 4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY WASHINGTON UNIVERSITY AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL WASHINGTON UNIVERSITY OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

WILDBOAR

Portions or all of this file are Copyright (C) 1994,1995,1996
Yoichi Shinoda, Yoshitaka Tokugawa, WIDE Project, Wildboar Project and Foretune. All rights reserved.

This code has been contributed to Berkeley Software Design, Inc. by the Wildboar Project and its contributors.

The Berkeley Software Design Inc. software License Agreement specifies the terms and conditions

for redistribution.

THIS SOFTWARE IS PROVIDED BY THE WILDBOAR PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE WILDBOAR PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

MARTIN BIRGMEIER

Copyright (C) 1993 Martin Birgmeier
All rights reserved.

You may redistribute unmodified or modified versions of this source code provided that the above copyright notice and this and the following conditions are retained.

This software is provided ``as is'', and comes with no warranties of any kind. I shall in no event be liable for anything that happens to anyone/anything when using this software.

CHRISTOPHER G. DEMETRIOU

Copyright (C) 1993, 1994 Christopher G. Demetriou
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Christopher G. Demetriou.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

DAVID HOVEMEYER

Copyright (C) 1995 David Hovemeyer <daveho@infocom.com>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE DEVELOPERS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE DEVELOPERS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

FRANK VAN DER LINDEN

Copyright (C) 1995 Frank van der Linden
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed for the NetBSD Project by Frank van der Linden
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS

SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THEO DE RAADT

Copyright (C) 1992/3 Theo de Raadt <deraadt@fsa.ca>
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

HENRY SPENCER

Copyright 1992, 1993, 1994 Henry Spencer. All rights reserved.
This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

[diff, grep]

Copyright (C) 1988, 1989, 1992, 1993, 1994 Free Software Foundation, Inc.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY;

without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

[less]

Copyright (C) 1984,1985,1989,1994,1995,1996 Mark Nudelman
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[tcpd]

Copyright 1995 by Wietse Venema. All rights reserved. Some individual files may be covered by other copyrights.

This material was originally written and compiled by Wietse Venema at Eindhoven University of Technology, The Netherlands, in 1990, 1991, 1992, 1993, 1994 and 1995.

Redistribution and use in source and binary forms are permitted provided that this entire copyright notice is duplicated in all such copies.

This software is provided "as is" and without any expressed or implied warranties, including, without limitation, the implied warranties of merchantibility and fitness for any particular purpose.

[tcpdump]

Copyright (C) 1989 Carnegie Mellon 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 Carnegie Mellon University. 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 MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright (C) 1990, 1991, 1993, 1994
John Robert LoVerso. 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 John Robert LoVerso.
THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This implementation has been influenced by the CMU SNMP release, by Steve Waldbusser. However, this shares no code with that system. Additional ASN.1 insight gained from Marshall T. Rose's _The_Open_Book_. Earlier forms of this implementation were derived and/or inspired by an awk script originally written by C. Philip Wood of LANL (but later heavily modified by John Robert LoVerso). The copyright notice for that work is preserved below, even though it may not rightly apply to this file.

This started out as a very simple program, but the incremental decoding (into the BE structure) complicated things.

Los Alamos National Laboratory

Copyright, 1990. The Regents of the University of California.This software was produced under a U.S. Government contract (W-7405-ENG-36) by Los Alamos National Laboratory, which is operated by the University of California for the U.S. Department of Energy. The U.S. Government is licensed to use, reproduce, and distribute this software. Permission is granted to the public to copy and use this software without charge, provided that this Notice and any statement of authorship are reproduced on all copies. Neither the Government nor the University makes any warranty, express or implied, or assumes any liability or responsibility for the use of this software.

[traceroute]

Copyright (C) 1988, 1989, 1991, 1994, 1995, 1996
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution, and (3) all advertising materials mentioning features or use of this software display the following acknowledgement: ``This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.'' Neither the name of the University nor the names of its contributors may 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.

[zlib]

Copyright notice:

(C) 1995-1996 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly　　Mark Adler
gzip@prep.ai.mit.edu　madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.

[Apache HTTP server]

Copyright (C) 2000 The Apache Software Foundation. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)."
Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.
THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL

THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[Xntp Program]

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

Copyright (C) David L. Mills 1992, 1993, 1994, 1995, 1996 Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

[MD5 Program]

Adapted from the RSA Data Security, Inc.
MD5 Message-Digest Algorithm.

[pimdd]

Copyright (C) 1998 by the University of Oregon.
All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation in source and binary forms for lawful purposes and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of Oregon. The name of the University of Oregon may not be used to endorse or promote products derived from this software without specific prior written permission.

THE UNIVERSITY OF OREGON DOES NOT MAKE ANY REPRESENTATIONS ABOUT THE SUITABILITY OF THIS SOFTWARE FOR ANY PURPOSE. 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, TITLE, AND NON-INFRINGEMENT.

IN NO EVENT SHALL UO, OR ANY OTHER CONTRIBUTOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, WHETHER IN CONTRACT, TORT, OR OTHER FORM OF ACTION, ARISING OUT OF OR IN CONNECTION WITH, THE USE OR PERFORMANCE OF THIS SOFTWARE.

Other copyrights might apply to parts of this software and are so noted when applicable.

Questions concerning this software should be directed to Kurt Windisch (kurtw@antc.uoregon.edu)

$Id: LICENSE,v 1.2 1998/05/29 21:58:19 kurtw Exp $

Part of this program has been derived from PIM sparse-mode pimd. The pimd program is covered by the license in the accompanying file named "LICENSE.pimd".

The pimd program is COPYRIGHT 1998 by University of Southern California.

Part of this program has been derived from mrouted. The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

[mrouted]

The mrouted program is covered by the following license. Use of the mrouted program represents acceptance of these terms and conditions.

1. STANFORD grants to LICENSEE a nonexclusive and nontransferable license to use, copy and modify the computer software ``mrouted'' (hereinafter called the ``Program''), upon the terms and conditions hereinafter set out and until Licensee discontinues use of the Licensed Program.

2. LICENSEE acknowledges that the Program is a research tool still in the development state, that it is being supplied ``as is,'' without any accompanying services from STANFORD, and that this license is entered into in order to encourage scientific collaboration aimed at further development and application of the Program.

3. LICENSEE may copy the Program and may sublicense others to use object code copies of the Program or any derivative version of the Program. All copies must contain all copyright and other proprietary notices found
in the Program as provided by STANFORD. Title to copyright to the Program remains with STANFORD.

4. LICENSEE may create derivative versions of the Program. LICENSEE hereby grants STANFORD a royalty-free license to use, copy, modify, distribute and sublicense any such derivative works. At the time LICENSEE provides a copy of a derivative version of the Program to a third party, LICENSEE shall provide STANFORD with one copy of the source code of the derivative version at no charge to STANFORD.

5. STANFORD MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. By way of example, but not limitation, STANFORD MAKES NO REPRESENTATION OR WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED PROGRAM WILL NOT INFRINGE ANY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. STANFORD shall not be held liable for any liability nor for any direct, indirect or consequential damages with respect to any claim by LICENSEE or any third party on account of or arising from this Agreement or use of the Program.

6. This agreement shall be construed, interpreted and applied in accordance with the State of California and any legal action arising out of this Agreement or use of the Program shall be filed in

a court in the State of California.

7. Nothing in this Agreement shall be construed as conferring rights to use in advertising, publicity or otherwise any trademark or the name of ``Stanford".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

[PIM sparse-mode pimd]

Copyright (C) 1998 by the University of Southern California.
All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation in source and binary forms for lawful purposes and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of Southern California and/or Information Sciences Institute. The name of the University of Southern California may not be used to endorse or promote products derived from this software without specific prior written permission.

THE UNIVERSITY OF SOUTHERN CALIFORNIA DOES NOT MAKE ANY REPRESENTATIONS ABOUT THE SUITABILITY OF THIS SOFTWARE FOR ANY PURPOSE. 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, TITLE, AND NON-INFRINGEMENT.

IN NO EVENT SHALL USC, OR ANY OTHER CONTRIBUTOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, WHETHER IN CONTRACT, TORT, OR OTHER FORM OF ACTION, ARISING OUT OF OR IN CONNECTION WITH, THE USE OR PERFORMANCE OF THIS SOFTWARE.

Other copyrights might apply to parts of this software and are so noted when applicable.

Questions concerning this software should be directed to Pavlin Ivanov Radoslavov (pavlin@catarina.usc.edu)

$Id: LICENSE.pimd,v 1.1 1998/05/29 21:58:20 kurtw Exp $

Part of this program has been derived from mrouted.
The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

[LTCS (Label Traffic Control System)]

Copyright (C) 1999 Harris and Jefferies Inc. All rights reserved.
Copyright (C) 2000 NetPlane Systems Inc. All rights reserved.

[KAME IPv6 STACK]

[CRUNCH]

[RADIUS]

and permission notice appear on all copies and supporting documentation,
the name of Livingston Enterprises, Inc. not be used in advertising or
publicity pertaining to distribution of the program without specific
prior permission, and notice be given in supporting documentation that
copying and distribution is by permission of Livingston Enterprises, Inc.

Livingston Enterprises, Inc. makes no representations about the suitability
of this software for any purpose. It is provided "as is" without express
or implied warranty

[totd]

WIDE

Copyright (C) 1998 WIDE Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted
provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and
the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions
and the following disclaimer in the documentation and/or other materials provided with the
distribution.
3. All advertising materials mentioning features or use of this software must display the following
acknowledgement:
This product includes software developed by WIDE Project and and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or
promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.

University of Tromso

Copyright (C) 1999,2000,2001,2002 University of Tromso, Norway. All rights reserved.

Author: Feike W. Dillema, The Pasta Lab, Institutt for Informatikk University of Tromso, Norway

Permission to use, copy, modify and distribute this software and its documentation is hereby
granted, provided that both the copyright notice and this permission notice appear in all copies of
the software, derivative works or modified versions, and any portions thereof, and that both notices
appear in supporting documentation.
THE UNIVERSITY OF TROMSO ALLOWS FREE USE OF THIS SOFTWARE IN ITS "AS IS"

CONDITION. THE UNIVERSITY OF TROMSO DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.
The author requests users of this software to send back any improvements or extensions that they make and grant him and/or the University the rights to redistribute these changes without restrictions.

Invenia Innovation A.S.

Copyright (C) Invenia Innovation A.S., Norway. All rights reserved.

Author: Feike W. Dillema, Invenia Innovation A.S., Norway.

Permission to use, copy, modify and distribute this software and its documentation is hereby granted, provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.
INVENIA INNOVATION A.S. ALLOWS FREE USE OF THIS SOFTWARE IN ITS "AS IS" CONDITION. INVENIA INNOVATION A.S. DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.
The author requests users of this software to send back any improvements or extensions that they make and grant him and/or the Invenia Innovation the rights to redistribute these changes without restrictions.

Todd C. Miller

Copyright (C) 1998 Todd C. Miller <Todd.Miller@courtesan.com> All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author 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 ANY EXPRESS OR IMPLIED WARRANTIES,INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

付録 C　用語解説

（英字）

ARP（Address Resolution Protocol）
IPv4 ネットワークで使用する通信プロトコルです。

AS（Autonomous System）
単一の管理権限で運用している独立したネットワークシステムのことを指します。

AS **境界ルータ**
OSPF を使用して，AS 外経路を OSPF 内に導入するルータです。

ATM（Asynchronous Transfer Mode）
非同期通信モードです。

BGP4（Border Gateway Protocol - version 4）
IPv4 ネットワークで使用する経路制御プロトコルです。

BGP4+（Multiprotocol Extensions for Border Gateway Protocol - version 4）
IPv6 ネットワークで使用する経路制御プロトコルです。

BGP **スピーカ**
BGP が動作するルータのことです。

BGP4+ **スピーカ**
BGP4+ が動作するルータのことです。

BOD（Bandwidth on Demand）**機能**
常用回線の帯域が不足した場合に ISDN 回線で回線の帯域を追加して，トラフィックを分散させる機能です。オーバーロード機能ともいいます。

BPDU（Bridge Protocol Data Unit）
ブリッジ間でやり取りされるフレームです。

DHCP（Dynamic Host Configuration Protocol）
ネットワーク接続時に IP アドレスを自動設定するプロトコルです。リレーエージェント機能，サーバ機能およびクライアント機能があります。

DHCP/BOOTP **リレーエージェント機能**
DHCP/BOOTP サーバと DHCP/BOOTP クライアントが異なるサブネットにあるとき，構成定義情報で設定したサーバの IP アドレスを DHCP/BOOTP パケットの宛先 IP アドレスに設定して，パケットをサブネット間中継する機能です。

Diff-serv（Differentiated services）**機能**
IP パケットのヘッダ情報から優先度を決定して，その優先度に従ってルータが処理する機能です。

DNS **リレー**
DNS(Domain Name System) システムの異なるサブネットワークに存在するサーバとクライアント間で，クライアントからのパケットをドメインネームサーバのアドレスに中継する機能です。

DSCP（Differentiated Services Code Point）

IP フローの IP ヘッダ内 DS Field の上位 6 ビットです。

DS ドメイン

Diff-serv 機能を提供するネットワークです。

DVMRP（Distance Vector Multicast Routing Protocol）

IPv4 マルチキャストで使用する距離ベクトル型の経路制御プロトコルです。

FDB（Filtering Data Base）

トランスペアレント・ブリッジで使用されるテーブルです。FDB にはフレームの送信元 MAC アドレス，フレームを受信したポートおよび監視時刻が記録されます。

ICMP（Internet Control Message Protocol）

IPv4 ネットワークで使用する通信プロトコルです。

ICMPv6（Internet Control Message Protocol version 6）

IPv6 ネットワークで使用する通信プロトコルです。

IGMP（Internet Group Management Protocol）

IPv4 ネットワークで使用するホスト－ルータ間のマルチキャストグループ管理プロトコルです。

IPv4（Internet Protocol version 4）

32 ビットの IP アドレスを持つインターネットプロトコルです。

IPv6（Internet Protocol version 6）

128 ビットの IP アドレスを持つインターネットプロトコルです。

IPv6 グローバルアドレス

アドレスプレフィックスの上位 3 ビットが 001 で始まるアドレスです。経路情報の集約を目的とした階層形式になっています。IPv6 グローバルアドレスは世界で一意なアドレスで，インターネットを使用した通信に使用されます。

IPv6 DHCP サーバ機能

IPv6 DHCP クライアントに対して，プレフィクス，DNS サーバアドレスなどの環境情報（構成情報）を動的に割り当てるための機能です。

IPv6 サイトローカルアドレス

アドレスプレフィックスの上位 10 ビットが 1111 1110 11 で，64 ビットのインタフェース ID 部を含むアドレスです。同一サイト内だけで有効なアドレスで，インターネットに接続されていないネットワークで自由に IPv6 アドレスを付ける場合に使用されます。

IPv6 リンクローカルアドレス

アドレスプレフィックスの上位 64 ビットが fe80:: で，64 ビットのインタフェース ID 部を含むアドレスです。同一リンク内だけで有効なアドレスで，自動アドレス設定，近隣探索，またはルータがないときに使用されます。

IPX（Internetwork Packet Exchange）

米国 Novell 社の Netware がネットワーク層で使用しているプロトコルです。

IS-IS

IS-IS は，ルータ間の接続の状態から構成されるトポロジに基づき最短経路を計算するリンクステートプロトコルです。

MIB（Management Information Base）

機器についての情報を表現するオブジェクトです。SNMP プロトコルで使用します。

MLD（Multicast Listener Discovery）
ルーターホスト間で使用される IPv6 マルチキャストグループ管理プロトコルです。

NAT(Network Address Translation)
ローカルネットワークのプライベートアドレスをインターネットなどで使用するグローバルアドレスに変換する機能です。

NAPT(Network Address Port Translation)
ローカルネットワークのプライベートアドレスとポート番号を，インターネットなどで使用するグローバルアドレスとポート番号に変換する機能です。

NDP（Neighbor Discovery Protocol）
IPv6 ネットワークで使用する通信プロトコルです。

NIF（Network Interface board）
接続する各メディアに対応したインタフェースを持つコンポーネントです。物理レイヤを処理します。

OSPF（Open Shortest Path First）
IPv4 ネットワークで使用する経路制御プロトコルです。

OSPFv3
IPv6 ネットワークで使用する経路制御プロトコルです。

OSPF **ドメイン**
本装置と接続している独立した各 OSPF ネットワークのことです。

OSPF **マルチバックボーン**
本装置で 1 台のルータ上で複数の OSPF ネットワークと接続して，OSPF ネットワークごとに個別に経路の交換，生成などを行う機能です。

PHB（Per Hop Behavior）
インテリアリードで DSCP に基づいた優先転送動作のことをいいます。

PIM-DM（Protocol Independent Multicast-Dense Mode）
DVMRP のように基盤になっているユニキャスト IPv4 の経路機構に依存しないでマルチキャストの経路制御ができるプロトコルです。パケットの送信後，不要な経路を除外します。

PIM-SM（Protocol Independent Multicast-Sparse Mode）
DVMRP のように基盤になっているユニキャスト IPv4 の経路機構に依存しないでマルチキャストの経路制御ができるプロトコルです。ランデブーポイントへのパケット送信後，Shortest path で通信します。

PIM-SSM (Protocol Independent Multicast-Source Specific Multicast)
PIM-SM の拡張機能で，ランデブーポイントを使用しないで最短パスで通信する経路制御プロトコルです。

PPP（Point-to-Point Protocol）
シリアル回線用の通信プロトコルです。非同期接続ができます。

PPP over Ethernet **クライアント機能** (PPPoE)
イーサネット上で PPP を利用した接続をするための機能です。PPPoE を使用すると日本電信電話株式会社の B フレッツやフレッツ・ADSL のサービスに接続できます。

PVC（Permanent Virtual Channel （Connection）/Permanent Virtual Circuit）
物理回線内の通信パスです。

QoS（Quality of Service）制御

実時間型・帯域保証型トラフィックに対して，通信の遅延やスループットなどの通信品質を制御する機能です。

RFC（Request For Comments）

TCP/IP に関する仕様を記述している公開文書です。

RIP（Routing Information Protocol）

IPv4 ネットワークで使用する経路制御プロトコルです。

RIPng（Routing Information Protocol next generation）

IPv6 ネットワークで使用する経路制御プロトコルです。

RM（Routing Manager）

ルーティングマネージャです。装置全体の管理およびルーティングプロトコル処理を行います。また，ルーティング・テーブルを作成・更新して RP に配布します。

RMON(Remote Network Monitoring)

イーサネット統計情報を提供する機能です。

RP（Routing Processor）

ルーティング処理機構です。パケット転送エンジンとルーティング・QoS テーブル検索エンジンを持ち，ルーティング・テーブル，フィルタリング・テーブル，QoS テーブルを検索して，IP パケットを送受信します。

SNMP（Simple Network Management Protocol）

ネットワーク管理プロトコルです。

Tag-VLAN

IEEE が標準化した VLAN の一つで，イーサネットフレームに Tag と呼ばれる識別子を埋め込むことで VLAN 情報を離れたセグメントに伝えることができる VLAN です。

UDP（User Datagram Protocol）

トランスポート層の通信プロトコルです。

VBR キュー

サービスカテゴリが VBR のトラフィックを専用に処理するキューです。

VLL（Virtual Leased Line）

仮想専用線のことです。AX2000R では，イーサネット上で複数の宛先ごとに帯域を割り当てることを指します。

VRRP（Virtual Router Redundancy Protocol）

ルータに障害が発生した場合でも，同一イーサネット上の別ルータを経由して通信経路を確保する，ホットスタンバイ機能です。この機能を使用すると，同一イーサネット上の複数ルータから構成される仮想ルータを定義できます。エンドホスト側はデフォルトとして仮想ルータを設定しておけば，ルータに障害が発生した場合でも別ルータの切り替えを意識する必要がありません。

（ア行）

イコールコストマルチパス

ある 2 点間にコストが同じ経路が複数ある場合に，この複数の経路のことをイコールコストマルチパスといいます。

インターナルピア

同じ AS 内に属し，物理的に直接接続された BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスは直接接続されたインタフェースのインタフェースアドレスを使用します。

インタフェース
本装置で IP アドレスを付与する単位です。

インタフェースバックアップ
回線バックアップで，バックアップ元回線のインタフェースのダウンを契機に，バックアップ先 ISDN 回線を接続する方式です。

インデックス
MIB を限定するための情報です。

インテリアノード
DS ドメインで，DSCP に基づいた転送動作だけを行うノードです。

インポート・フィルタ
指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。

運用端末
本装置の運用管理に使用するコンソールまたはリモート端末のことを運用端末と呼びます。

エキスターナルピア
異なる AS に属する BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスは直接接続されたインタフェースのインタフェースアドレスを使用します。

エキスポート・フィルタ
ルータ上で同時に動作しているルーティングプロトコル間での経路情報の再配布を制御します。エキスポート・フィルタでは配布先プロトコルのフィルタリング条件と学習元プロトコルのフィルタリング条件によって，特定の宛先に特定の経路情報を送出します。

エリアボーダルータ
複数のエリアに所属するルータです。所属するすべてのエリアについて，個別に経路選択を行います。

オブジェクト ID
MIB を特定するための識別 ID です。root から各ノードの数値をならべて番号をつけることで，MIB を一意に識別できます。

（カ行）

仮想リンク
仮想の回線のことです。仮想リンクの実際の経路があるエリアのことを仮想リンクの通過エリアといいます。

均等最低帯域保証
送信帯域の均等最低保証を行う機能です。キューごとに割り当てられた帯域分だけを送信します。ただし，回線の帯域が空いていれば，空いている帯域も使用して送信します。

均等保証
出力キューからパケットを送信するときの送信順を，1 キュー当たり 1 パケットにして各キューから順番に送信する機能です。

クラシファイア
TCP/IP ヘッダからフローを識別して，個々のユーザとの契約に基づいて DSCP に分類・集約する機能です。バウンダリノードが持っている機能です。

グループマネージメント機能

ホストールータ間でのグループメンバーシップ情報の送受信によって，ルータが直接接続したネットワーク上のマルチキャストグループメンバーの存在を学習する機能です。

構成定義情報ファイル

ネットワークの運用環境に合わせて構成および動作条件を設定するファイルです。このファイルはテキストファイル形式で MC に格納します。構成定義情報ファイルには次に示す種類があります。

- 現用構成定義情報ファイル
  本装置の立ち上げに使用します。この構成定義情報に従って運用されます。
- 予備構成定義情報ファイル
  現用構成定義ファイルのコピー，または将来のネットワークの変更に備えた編集用として使用します。
- 一時保存構成定義情報ファイル
  運用中に構成定義を変更して MC に格納した場合に，編集前の現用構成定義情報ファイルを一時保存したものです。

（サ行）

最低帯域保証

送信帯域の最低保証を行う機能です。キューごとに指定された帯域分だけを送信します。ただし，回線の帯域が空いていれば，空いている帯域も使用して送信します。

シェーパ

バウンダリノードで送信帯域を制御する機能です。

重要パケット保護機能

保証帯域内で，重要なパケットは優先的に保証帯域内パケットとして転送し，通常のパケットは重要なパケットが全保証帯域を使用して転送していない場合に保証帯域内パケットとして転送する機能です。

出力優先制御

出力優先度に従って優先パケットの追い越しを行う制御です。出力優先度の高いキューに積まれたパケットをすべて送信したあとで，より低いキューに積まれたパケットを送信します。

スタティックルーティング

ユーザが構成定義によって経路情報を設定するルーティング方法です。

ステートレスアドレス自動設定機能

IPv6 リンクローカルアドレスを装置内で自動生成する機能，ホストが IPv6 アドレスを自動生成するときに必要な情報を通知する機能です。

スパニングツリー・アルゴリズム

ブリッジによるルーティングで使用されるアルゴリズムで，論理的木構造を形成します。このアルゴリズムによって任意の二つの ES 間で単一の経路を決定でき，フレームのループ周回を防ぐことができます。

（タ行）

帯域制御

インタフェース単位の最大帯域制限，およびキューごとの最低保証，最大帯域制限，余剰帯域分配を行う機能です。

ダイナミックルーティング

ルーティングプロトコルによってネットワーク内の他ルータと経路情報を交換して経路を選択するルーティング方法です。

タイムスロット

多重アクセスで時分割された各回線。

多重アクセス
1 本の物理回線を時分割多重によって複数の回線に多重した通信形態。

トラップ
SNMP エージェントから SNMP マネージャに非同期に通知されるイベント通知です。

トラフィックエンシニアリング
多量のトラフィックによって特定経路が輻輳するような場合に，該当するトラフィックを迂回させて輻輳を回避するようにトラフィックを分散させる技術のことです。

トラフィッククラス
トラフィック制御の内容を決定する，CBR，VBR，ABR，UBR，GFR，GFR2 のサービスカテゴリおよびトラフィックパラメータのセットのことです。

トランスペアレント・ブリッジ
MAC 副層によって中継を行う中継装置です。

（ハ行）

パーシャルメッシュ構成
フレームリレーで使用するネットワーク構成です。センターと各拠点間の通信などに適用され，通信パスがない拠点間通信の場合は，センター経由の折り返しで通信します。通信パス数を削減できるので，公衆フレームサービスなどを利用した場合に料金が節約できます。

ハードウェアキュー長
1 回の送信処理で回線ハードウェアに与える送信データ長。

バウンダリノード
DS ドメインで，フローを識別して DSCP へ集約して DSCP に基づいて転送動作を行うノードです。

パラレル PVC
相手装置との間に複数の PVC を割り当てて通信するとき，この複数の PVC をパラレル PVC といいます。

標準 MIB
RFC で規定された MIB です。

フィルタリング
受信したある特定の IP パケットを中継または廃棄する機能です。

物理ポートバックアップ
回線バックアップで，バックアップ元物理ポートのダウンを契機に，同一インタフェース配下のバックアップ先 ISDN 回線を接続する方式です。

プライベート MIB
装置の開発ベンダーが独自に提供する MIB です。

フラッディング
トランスペアレント・ブリッジで，フィルタリング・データベース (FDB) と呼ばれるテーブル内の MAC アドレスと受信したフレームの宛先 MAC アドレスを比較して，一致するエントリがない場合に，フレームを受信したインタフェース以外のすべてのインタフェースにフレームを送信する機能です。

フルメッシュ構成
フレームリレーで使用する，通信先と 1 対 1 で通信パスを持つネットワーク構成です。拠点間で相互に通信する場合な

どに適用します。通信パス数は増えますが，直結パスのために通信遅延を低減できます。

フレームリレー網
プロトコルを簡素化して高速データ伝送を実現したパケット交換型の通信方式です。

ポリシー
どの業務データを優先的に配信するかという方針を指します。

ポリシーインタフェース情報
ポリシールーティングに従ってパケットを転送するときの，構成定義情報で定義したインタフェース情報です。単一または複数のポリシーインタフェース情報をグループ化してポリシーグループ情報を定義します。

ポリシールーティング
ルーティングプロトコルで登録された経路情報に従わないで，ユーザが設定したポリシーをベースにして特定のインタフェースにパケットを転送するルーティング方法です。

（マ行）

マーカ
IP ヘッダの DS フィールドに DSCP 値を書き込む機能です。バウンダリノードが持っている機能です。

マルチキャスト
ネットワーク内で選択されたグループに属している通信先に対して同一の情報を送信する機能です。

マルチキャストトンネル機能
二つのマルチキャストルータがユニキャストルータを経由して接続されている場合に，マルチキャストパケットをカプセル化してデータを送受信して，二つのマルチキャストネットワークを接続する機能です。

マルチパス
宛先のネットワークアドレスに対して複数の経路を構築する接続方式です。

未指定アドレス
すべてのビットが 0 のアドレス 0:0:0:0:0:0:0:0(0::0，または ::) は未指定アドレスと定義されます。未指定アドレスはインタフェースにアドレスがないことを表します。

（ヤ行）

優先 MC スロット指定機能
装置を起動するための優先カードスロットを指定する機能です。

（ラ行）

ルーティングピア
同じ AS 内に属し，物理的に直接接続されない BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスはそのルータの装置アドレス，またはルータ内のインタフェースのインタフェースアドレスのどちらかです。

ルート・フラップ・ダンピング
経路情報が頻発してフラップするような場合に，一時的に該当する経路の使用を抑制して，ネットワークの不安定さを最小限にする機能です。

ルート・リフレクション
AS 内でピアを形成する内部ピアの数を減らすための方法です。内部ピアで配布された経路情報をそのほかの内部ピア

に再配布して，AS 内の内部ピアの数を減らします。

ルート・リフレッシュ

変化が発生した経路だけを広告する BGP4+ で，すでに広告された経路を強制的に再広告させる機能です。

ループバックアドレス

アドレス 0:0:0:0:0:0:0:1(0::1，または ::1) はループバックアドレスと定義されています。ループバックアドレスは自ノード宛てに通信するときに，パケットの送信先アドレスとして使用されます。ループバックアドレスをインタフェースに割り当てることはできません。

ロードバランス機能

マルチパスを使用して既存回線を集合して高帯域を供給するための機能です。

論理回線

多重された一次群回線です。

索引

数字

1000BASE-SX/1000BASE-LX/1000BASE-LH 接続 176
10BASE-T/100BASE-TX 接続 176

A

ADVERTISEMENT パケットの送出 109
alarm グループ 134
ARP〔用語解説〕 245
AS〔用語解説〕 245
AS 境界ルータ〔用語解説〕 245
ATM〔用語解説〕 245
ATM インタフェース 180
ATM サービス 204
ATM の準拠規格および勧告 219
ATM メガリンクサービス 204

B

BA Classifier 52
BGP-4 を使用するときの注意事項 182
BGP4+〔用語解説〕 245
BGP4+ スピーカ〔用語解説〕 245
BGP4+ の準拠規格および勧告 223
BGP4〔用語解説〕 245
BGP4 の準拠規格および勧告 221
BGP スピーカ〔用語解説〕 245
BOD〔用語解説〕 245
BPDU〔用語解説〕 245

C

Cisco 社製ルータ接続 180

D

DHCP/BOOTP リレーエージェント機能〔用語解説〕 245
DHCP/BOOTP リレーエージェントの準拠規格および勧告 220
DHCP〔用語解説〕 245
DHCP クライアント機能の準拠規格 220
DHCP サーバ機能の準拠規格 220
Diff-serv〔用語解説〕 245
Diff-serv 概説 46
Diff-serv 機能 45
Diff-serv 機能の概要 47
Diff-serv の QoS サービス 49
Diff-serv の機能 46
Diff-serv の機能ブロック 51
Diff-serv の準拠規格および勧告 224
Diff-serv の制御仕様 50
Diff-serv の導入手順 49
Diff-serv のネットワークモデル 46
DLCI グループを使用した他社接続 179
DNS リレー機能の準拠規格 220
DNS リレー〔用語解説〕 245
DSCP〔用語解説〕 246
DSCP 書き換え 9
DSCP 値と各クラスのマッピング例 54
DS ドメイン 46
DS ドメイン〔用語解説〕 246
DS フィールドと DSCP 48
DVMRP〔用語解説〕 246

E

event グループ 134

F

FAULT CODE 166
FDB〔用語解説〕 246
frping コマンド 179

G

GetBulkRequest オペレーション 124
GetNextRequest オペレーション 123
GetRequest オペレーション 122
Group 化されたインタフェース 80

H

HDLC パススルーと優先度制御 96
history グループ 134

I

ICMP〔用語解説〕 246
ICMPv6〔用語解説〕 246
IGMP〔用語解説〕 246
IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例 119
IPv4〔用語解説〕 246
IPv6〔用語解説〕 246

IPv6 DHCP サーバ機能〔用語解説〕 246
IPv6 DHCP サーバ機能の準拠規格および勧告 223
IPv6 グローバルアドレス〔用語解説〕 246
IPv6 サイトローカルアドレス〔用語解説〕 246
IPv6 ネットワークの準拠規格および勧告 222
IPv6 マルチキャストの準拠規格および勧告 224
IPv6 リンクローカルアドレス〔用語解説〕 246
IPv6 ルータとの接続 185
IPX〔用語解説〕 246
IPX パケットのヘッダフォーマット 62
IPX パケットヘッダ有効性チェック 62
IPX ルーティング 59
IPX ルーティングエントリ数 68
IPX ルーティング概説 60
IPX ルーティングの機能 61
IP アドレスによるオペレーション制限 127
IP バージョン 4 の準拠規格および勧告 219
IP フロー検出 5
IP フロー識別条件と指定方法 5
IP マルチキャストの準拠規格および勧告 222
IP ルータとの接続 181
IS-IS〔用語解説〕 246
ISDN 一次群回線の契約条件・付加サービス 198
ISDN 回線契約条件 196
ISDN 回線契約条件〔インバースマックス　ターミナルアダプタ接続条件〕 202
ISDN 基本回線の契約条件・付加サービス 197
ISDN 接続〔IPX ルーティング〕 80

L

LED 166
LED および FAULT CODE の表示 166
LED の表示内容 166

M

Marker 52
MC 162
MC 保守コマンド 162
MF Classifier 52
MIB〔用語解説〕 246
MIB オブジェクトの表し方 120
MIB 概説 120
MIB 構造 120
MIB 取得の例 118
MIB 情報収集周期のチューニング 187
MIB を設定できない場合の応答 125
MLD〔用語解説〕 247

N

NAPT〔用語解説〕 247
NAT，NAPT 機能の準拠規格 220
NAT-PT 機能の準拠規格および勧告 223
NAT〔用語解説〕 247
NDP〔用語解説〕 247
NETBIOS パケット 79
NetWare4.1J 使用時の注意 78
Next_Hop 解決 182
nexthopself パラメータ指定の例〔BGP4+〕 186
NIF〔用語解説〕 247
NIF 種別ごとのサポート仕様 29
noinstall オプションが必要な構成例 184

O

OSPF〔用語解説〕 247
OSPFv3〔用語解説〕 247
OSPF ドメイン〔用語解説〕 247
OSPF マルチバックボーン〔用語解説〕 247
OSPF を使用するときの注意事項 182

P

PDU タイプコード 128
PHB〔用語解説〕 247
PIM-DM〔用語解説〕 247
PIM-SM〔用語解説〕 247
PIM-SSM〔用語解説〕 247
ping atm コマンド 168
ping frame-relay コマンド 168
ping ipv6 コマンド 168
ping ipx コマンド 168
Ping 機能 75
ping コマンド 167
PPP〔用語解説〕 247
PPP over Ethernetクライアント機能の技術参考資料 217
PPP over Ethernet クライアント機能の準拠規格 216
PPP over Ethernet クライアント機能〔用語解説〕 247
PPP プロトコルの準拠規格 218
PVC〔用語解説〕 247
PVC Trap 130

Q

QoS〔用語解説〕 248
QoS 制御概説 2
QoS 制御機能 1
QoS 制御機能とプロトコル種別とのサポート仕様 38

QoS 制御機能とメディア種別との対応 37
QoS 制御機能の仕様一覧 37
QoS 制御機能の適用例 31
QoS 制御構造 4
QoS 制御使用時の注意事項 42
QoS 制御の必要性 2
QoS 制御のメリット 3
QoS ネットワーク構成例 31
QoS ネットワークの運用 35

R

RADIUS 136
RADIUS 概説 136
RADIUS サーバ選択のシーケンス 140
RADIUS サーバでの本装置の識別 189
RADIUS サーバとの接続 189
RADIUS サーバの設定 189
RADIUS サーバのポート番号 189
RADIUS サーバのメッセージ 189
RADIUS による認証 135
RADIUS 認証でのログインユーザの扱い 141
RADIUS のサポート範囲 137
RADIUS の準拠する規格および勧告 226
RADIUS の適用機能および範囲 137
RADIUS を使用した認証 139
RFC〔用語解説〕 248
RFC1583 に準拠していない装置と OSPF で接続するときの注意事項 183
RIP/OSPF の準拠規格および勧告 220
RIP〔用語解説〕 248
RIPng/OSPFv3 の準拠規格および勧告 223
RIPng〔用語解説〕 248
RIP 情報 77
RIP パケット送信 / 受信の制御 67
RIP パケットの種類 67
RIP フィルタリング 75
RIP プロトコル 67
RM〔用語解説〕 248
RMON 248
RMON MIB 134
RP〔用語解説〕 248
RP 処理負荷と QoS 制御の関係 42

S

SAP エントリ数 71
SAP 情報 78
SAP テーブルエントリのエージング 71
SAP テーブルエントリの登録と経路 70
SAP テーブルエントリを使用したネットワーク構成 72
SAP テーブルのスタティック設定 71
SAP パケット処理 69
SAP パケット送信の制御 70
SAP フィルタリング 74
SetRequest オペレーション 124
SNMP〔用語解説〕 248
SNMP オペレーション 122
SNMP オペレーションの制限事項 126
SNMP オペレーションのメッセージフォーマット 127
SNMP 概説 118
SNMP の準拠規格および勧告 224
SNMP マネージャ側の応答監視タイマ値の考慮 187
SNMP マネージャとの接続 187
SNMP マネージャによる MIB 情報の収集周期の見直し 188
SNMP を使用したネットワーク管理 117
statistics グループ 134

T

Tag-VLAN〔用語解説〕 248
Tag-VLAN 連携設定 177
Tag-VLAN 連携の LAN スイッチ接続 176
Tag-VLAN 連携の PC 接続 178
Tag-VLAN 連携のヘッダフォーマット 9
TA 間の発着信衝突 203
TA の基本設定内容 200
TA の設定内容 200
TCP パケットに対する帯域監視機能の使用 43
TOS フィールドと DS フィールド 48
traceroute6 コマンド 167
traceroute コマンド 167
Traffic Conditioner 52
Trap 129

U

UDP〔用語解説〕 248

V

VBR キュー〔用語解説〕 248
VLAN ID 177
VLAN 種別 176
VLL〔用語解説〕 248
VP 単位に帯域を確保する場合 206
VRRP 99
VRRP〔用語解説〕 248

VRRP 概説 100
VRRP 使用時の注意事項 114
VRRP でサポートしている項目 100
VRRP による構成例 112
VRRP の準拠規格および勧告 226
VRRP ポーリング 104
VRRP ポーリング使用時の注意事項 105
VRRP ポーリングの概要 104
VRRP ポーリングの障害検出の仕組み 107

W

WAN インタフェース 179
WAN のサービス 194
WAN 物理インタフェースの準拠規格 217
WAN または ATM 接続〔IPX ルーティング〕 79
WAN または ATM 接続〔ブリッジ〕 96

い

イーサネット，ギガビット・イーサネット 192
イーサネットインタフェース 176
イーサネットインタフェースの準拠規格 216
イコールコストマルチパス〔用語解説〕 248
インターナルピア〔用語解説〕 248
インタフェース〔IPX ルーティングの概要〕 61
インタフェース〔用語解説〕 249
インタフェース種別の設定 176
インタフェースのブリッジ動作モード 90
インタフェースバックアップ〔用語解説〕 249
インデックス 121
インデックス〔用語解説〕 249
インテリアノード 46
インテリアノード〔用語解説〕 249
インテリアノードの機能 47
インバースマックス　ターミナルアダプタ接続条件 199
インポート・フィルタ〔用語解説〕 249

う

ウォッチドッグ・パケットの制御 72
ウォッチドッグ・プロトコルのシーケンス 73
ウォッチドッグ・プロトコルのパラメータ値 73
ウォッチドッグ代理応答 73
ウォッチドッグ代理応答機能 73
ウォッチドックパケット 78
運用管理 144
運用機能 143
運用形態ごとの QoS 機能の適用（企業ネットワーク） 36
運用形態ごとの QoS 機能の適用（プロバイダ網） 36
運用形態ごとの QoS 制御範囲 36
運用コマンド 152
運用コマンドとその用途 152
運用端末 144
運用端末〔用語解説〕 249
運用端末の条件 145
運用端末の接続形態 144
運用メッセージおよび運用ログ 165

え

エキスターナルピア〔用語解説〕 249
エキスポート・フィルタ〔用語解説〕 249
エラーステータスコード 128
エリアボーダルータ〔用語解説〕 249

お

オートネゴシエーション接続（10BASE-T, 100BASE-TX, 1000BASE-SX, 1000BASE-LX, 1000BASE-LH） 176
オブジェクト ID〔用語解説〕 249

か

回線テスト 169
各 VC の設定内容（フローごとに固定の帯域を割り当てる場合） 207
各 VC の設定内容（フローのトラフィック特性に応じた優先制御を行う場合） 208
各 VC の設定内容（優先度によるフロー分けを使ったエクストラクラス利用） 208
各機能ブロックの説明 51
拡張フィルタリング 93
拡張フィルタリングの設定例 93
仮想 MAC 宛てフレームの受信 101
仮想 MAC アドレスによる ARP 応答および NDP 応答 102
仮想リンク〔用語解説〕 249
仮想ルータの MAC アドレスと IP アドレス 101
可変帯域制御 21
簡易的 QoS 制御 35
完全優先〔シェーパ〕 18
管理情報の収集 163
管理情報表示コマンド 163
管理情報表示コマンドと表示する管理情報 163

き

企業ネットワークへの適用例 31
機能ブロックと構成定義コマンドの対応 52

機能ブロックに対応する構成定義コマンド 53
機能ブロックの概要 4
キューイング制御の概念 17
キュー仕様 39
禁止トポロジ〔ブリッジ〕 95
均等最低帯域保証 19
均等最低帯域保証〔用語解説〕 249
均等保証〔用語解説〕 249

く

クライアントのサーバログイン条件 72
クラシファイア〔用語解説〕 249
グループ帯域制御 28
グループマネージメント機能〔用語解説〕 250
クロスケーブルの結線仕様 145

け

経路確認 167
経路制御機能〔IPX ルーティング〕 67
経路の決定 68
ケーブルおよびコネクタの設定 205

こ

広域イーサネット 192
広域イーサネットを使用したネットワーク構成例 192
構成定義 149
構成定義作成時の注意事項 55
構成定義条件〔ATM メガリンクサービス〕 205
構成定義条件〔セルリレーサービス〕 209
構成定義条件〔メガデータネッツ〕 210
構成定義情報 149
構成定義情報の運用方法 150
構成定義情報の表示と編集 151
構成定義情報ファイル〔用語解説〕 250
構成定義情報ファイルの種類 150
呼接続時間短縮の注意事項 201
固定帯域制御 21
コミュニティによるオペレーション 127
コンソール 145
コンソールからのソフトウェアのアップデート 173

さ

サービスカテゴリ GFR/GFR2 設定時の制約条件 205
サービスカテゴリごとの接続性 209
サービスカテゴリの設定〔ATM メガリンクサービス〕 205
サービスカテゴリの設定〔セルリレーサービス〕 209
サービスカテゴリの設定〔メガデータネッツ〕 211
再起動 146
最低帯域保証 19
最低帯域保証 (kbit/s 指定) 19
最低帯域保証〔用語解説〕 250
最適経路の決定とルーティングテーブルへの登録 68
サポート仕様〔ブリッジ〕 82
サポートトラップ 129

し

シェーパ 18
シェーパ〔用語解説〕 250
シェーパの位置づけ 18
識別着信の注意事項 202
自己診断テスト 146
指定ブリッジ 85
指定ポート 85
自動切り戻し 111
周期 RIP のトラフィック 77
周期 SAP のトラフィック 78
重要パケット保護機能 7
重要パケット保護機能〔用語解説〕 250
受信した RP と送信した RP の組み合わせごとの優先度指定方式 12
出力優先制御〔用語解説〕 250
障害監視インタフェース 103
障害検出の仕組み 109
障害時の復旧および情報収集 171
障害部位と復旧内容 171
使用条件によって異なる設定 201
使用する RADIUS 属性の内容 137
シリアライゼーションパケット 79

す

推奨 RADIUS サーバ 189
推奨 SNMP マネージャ 187
スイッチ 172
スタティックルーティング〔IPX ルーティング〕 68
スタティックルーティング〔用語解説〕 250
ステートレスアドレス自動設定機能〔用語解説〕 250
スパニングツリー・アルゴリズム 84
スパニングツリー・アルゴリズム〔用語解説〕 250
スパニングツリー・トポロジ管理 90
スパニングツリーの論理トポロジ 86

せ

制御パケットのトラフィック 77
接続できる ATM サービス 204

接続できるサービス品目(ATM メガリンクサービス) 204
接続できるサービス品目(セルリレーサービス) 209
接続できるサービス品目(メガデータネッツ) 210
専用線・フレームリレー・ISDN 194

そ

装置およびインタフェース状態表示 163
装置の状態情報 163
装置の部位ごとの状態情報 163
疎通テスト 167
そのほかの制御パケット 78
ソフトウェアアップデート時の注意事項 173
ソフトウェアのアップデート 173

た

ダイアグノスティックパケット 79
帯域監視 7
帯域制御(トラフィック指定) 20
帯域制御〔用語解説〕 250
帯域保証型ネットワークの概念 2
ダイナミックルーティング〔用語解説〕 250
タイムスロット〔用語解説〕 250
他機種との接続 175
他機種との接続〔IP ルーティングで接続する場合〕 181
タグによる仮想 LAN および優先制御 176
多重アクセス〔用語解説〕 251
他装置との置き換え 183
立ち上げ 146
立ち上げおよび再起動 146

ち

着信タイミングの注意事項 201
中継機能〔IPX ルーティング〕 64
中継性能 77，96
中継できるパケット 177

つ

通信相手との接続時間 202
通信処理機能 62

と

統計情報 164
特殊制御パケット処理機能 69
時計および時刻情報 163
トラップ 129
トラップ〔用語解説〕 251
トラップ概説 129
トラップの例 119
トラップフォーマット 129
トラフィックエンシニアリング〔用語解説〕 251
トラフィッククラス〔用語解説〕 251
トラフィック種別と要求される通信品質 3
トラフィック種別と要求品質 2
トランスペアレント・ブリッジ 83
トランスペアレント・ブリッジ〔用語解説〕 251
トランスレーション 87
トランスレーション適用構成 87
トレース 169

に

認証方式シーケンス 139

ね

ネットワークアドレス 61
ネットワーク管理 118
ネットワーク構成例〔VRRP〕 112
ネットワーク障害切り分け機能 167
ネットワーク設計の考え方〔IPX ルーティング〕 77
ネットワーク設計の考え方〔ブリッジ〕 95
ネットワークマーキング 46

の

ノードアドレス〔IPX ルーティング〕 60

は

パーシャルメッシュ構成〔用語解説〕 251
ハードウェアキュー長〔用語解説〕 251
ハードウェア中継機能使用時の注意事項〔QoS 制御機能〕 6
廃棄制御〔QoS 制御〕 16
バウンダリノード 46
バウンダリノード〔用語解説〕 251
バウンダリノードおよびインテリアノードの機能 47
バウンダリノードの機能 47
パケット長〔IPX ルーティング〕 62
パケット長〔WAN インタフェース〕 179
パケットの認証 110
バックアップ MC の運用 162
発着信中の別の通信相手からの着信 203
発着信についての注意事項 203
パラレル PVC〔用語解説〕 251
バルク伝送方式モード A/ モード B の注意事項 201

ひ

標準 MIB 120
標準 MIB〔用語解説〕 251

ふ

ファイル属性 174
フィルタリング 92
フィルタリング〔用語解説〕 251
負荷分散の例〔VRRP〕 112
二つの VLAN を LAN スイッチ経由で本装置に設定する例 178
物理ポートバックアップ〔用語解説〕 251
プライベート MIB 120
プライベート MIB〔用語解説〕 251
フラッディング 83
フラッディング〔用語解説〕 251
ブリッジ 81
ブリッジ機能 90
ブリッジの準拠規格および勧告 224
フルメッシュ構成〔用語解説〕 251
フレーム・フォーマット 82
フレーム・フォーマットのトランスレーション 88
フレームタイプ 60
フレームタイプの設定 79
フレームトレース 169
フレームリレー /ATM 上で RIP-1 を使用する場合の設定 181
フレームリレー /ATM 上で RIP-2 を使用する場合の設定 181
フレームリレー〔WAN(他機種とのインタフェース)〕 179
フレームリレー接続でのパケットフォーマット 179
フレームリレープロトコルの準拠規格 218
フレームリレー網〔用語解説〕 252
フレームリレー網の加入条件 194
フレームリレー網の加入条件と本装置の構成定義情報 194
フレームリレー網またはATMネットワークへの接続 79
フレッツ・ADSL および B フレッツ接続 (PPPoE での接続) 192
フロー検出〔QoS 制御機能〕 5
フローごとに固定の帯域を割り当てる場合 206
フローコントロール〔インタフェース種別の設定〕 176
フロー制御〔Diff-serv 機能〕 51
フローのトラフィック特性に応じた優先制御を行う場合 207
プロバイダ網への適用例 (DSCP 値を使用した QoS 制御) 32
プロバイダ網への適用例 (最低帯域保証 (kbit/s 指定) を使用した QoS 制御) 34

へ

並列ブリッジ・トポロジ 84
ベストエフォート型ネットワークの概念 2

ほ

ポイントーポイント回線上で RIP-1 を使用する場合の設定 182
ポイントーポイント型回線による BGP4+ 接続での注意事項 185
ポイントーポイント型回線のインタフェースアドレス 185
ポイントーポイント型回線のインタフェースアドレス〔IP ルータとの接続〕 181
ポリシー〔用語解説〕 252
ポリシーインタフェース情報〔用語解説〕 252
ポリシールーティング〔用語解説〕 252
本装置が生成する主な IPv4 パケット 12
本装置でサポートする ISDN 回線 196
本装置の Diff-serv 機能ブロック 51
本装置の構成定義情報 199
本装置のサポート MIB 121
本装置の設定項目 (VP 単位に帯域を確保する場合) 206
本装置の設定項目 (フローごとに固定の帯域を割り当てる場合) 207
本装置の設定項目 (フローのトラフィック特性に応じた優先制御を行う場合) 207
本装置の設定項目 (優先度によるフロー分けを使ったエクストラクラス利用) 208

ま

マーカ〔用語解説〕 252
マーカー 9
マーカーの位置づけ 9
マスタルータの選出方法 111
マルチキャスト〔用語解説〕 252
マルチキャストトンネル機能〔用語解説〕 252
マルチパス〔用語解説〕 252

み

未指定アドレス〔用語解説〕 252

め

メガデータネッツ 210
メモリダンプ 172

も

網・各種専用線サービスとの接続 191
網レベル QoS 制御 35
モデルおよび RM 実装メモリサイズごとに定義できる最大エントリ数 38

ゆ

ユーザマーキング 46
ユーザ優先度書き換え 9
優先 MC スロット指定機能〔用語解説〕 252
優先度 111
優先度指定 10
優先度によるフロー分けを使ったエクストラクラス利用 208

ら

ラウンドロビン 19

り

リスト当たりに使用するエントリ数 38
リモート運用端末からのソフトウェアのアップデート 173
隣接ネットワーク連携 QoS 制御 35

る

ルーティングエントリのエージング 68
ルーティングテーブルの検索とパケット中継 65
ルーティングテーブルの内容〔IPX ルーティング〕 64
ルーティングテーブルの例 64
ルーティングピア〔用語解説〕 252
ルート・フラップ・ダンピング〔用語解説〕 252
ルート・リフレクション〔用語解説〕 252
ルート・リフレッシュ〔用語解説〕 253
ループバックアドレス〔用語解説〕 253

れ

レイヤ 2 連携機能 41

ろ

ロードバランス機能〔用語解説〕 253
ログ 172
ログイン制御 147
ログインセキュリティ制御 147
論理回線〔用語解説〕 253