AX2000R ソフトウェアマニュアル

# 運用ガイド

Ver. 8.4 対応

AX-10-161-10

## ■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（ＡＸ２００１Ｒ）
ＡＸ－６５３１－２Ｒ（ＡＸ２００２Ｒ）
ＡＸ－６５３１－２ＲＸ（ＡＸ２００２ＲＸ）

■発行

２００５年　１２月 （第２版） ＡＸ－１０－１６１－１０

## 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 |
|---|---|
| 5.8.1　QoS 制御機能を確認する | • B モデル用新規 NIF である NEB100-1TC サポートに伴い，「(3) Tag-VLAN 連携回線毎の帯域制御によるパケット廃棄の確認」を追記しました。 |

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

このマニュアルは，次に示す九つの章と付録から構成されています。

**第1章　運用開始前に**

運用管理の概要，および運用開始前に準備するものについて説明しています。

**第 2 章　装置起動**

本装置の起動と停止について説明しています。

**第 3 章　コマンド操作**

本装置でのコマンドの指定方法について説明しています。

**第 4 章　初期導入時の作業**

本装置を導入したときに必要な作業について説明しています。

**第 5 章　インタフェース状態・ルーティング状態の確認**

構成定義コマンドでネットワーク状態を設定したあとや運用中のトラブル発生時に行う，インタフェース状態およびルーティング状態の確認方法について説明しています。

**第 6 章　運用中の作業**

本装置がネットワーク上で運用されている間に行う作業について説明しています。

**第 7 章　トラブル発生時の対応**

本装置が正常に動作しない，通信ができないといったトラブルが発生した場合の対処方法について説明しています。

**第 8 章　保守作業**

保守関連の作業について説明しています。

**第 9 章　ソフトウェアアップデート**

ソフトウェアのアップデートやインストールの概念，代表的なトラブルについて説明しています。

**付録 A　用語解説**

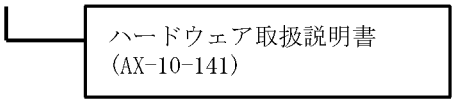
このマニュアルで使用している用語の意味を説明しています。

## ■このマニュアルの URL

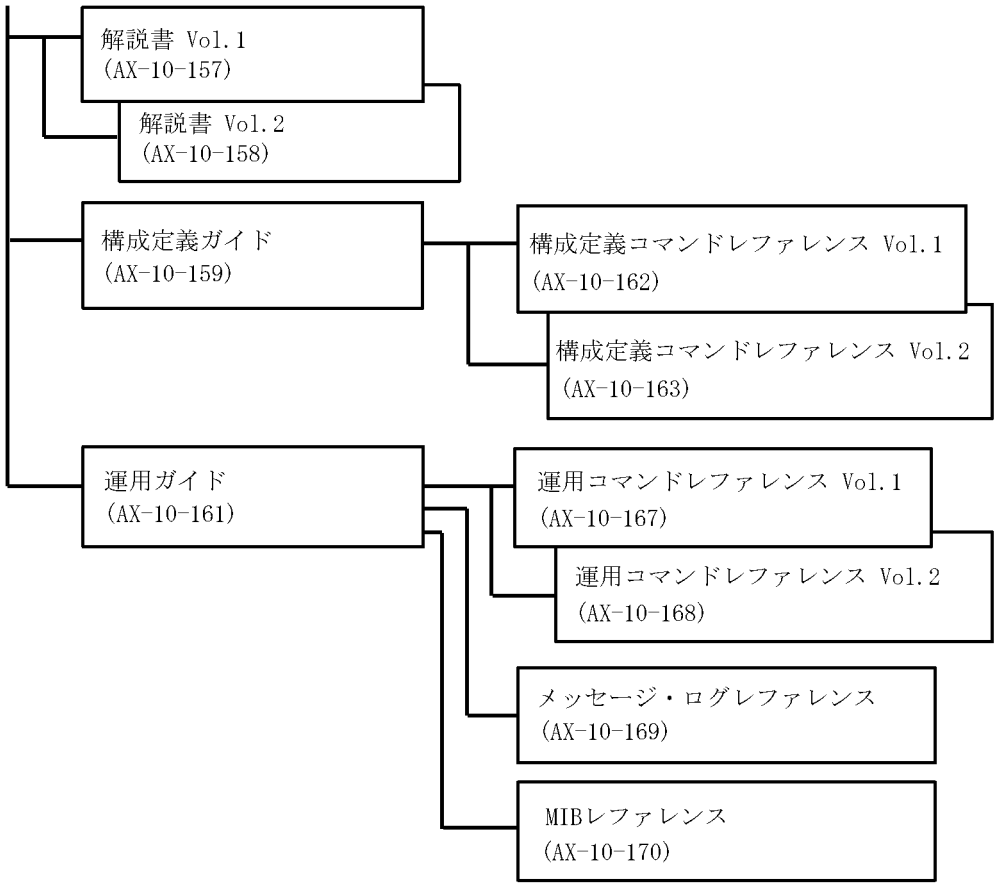
このマニュアルの内容は下記 URL に掲載しております。
http://www.alaxala.com

## ■ 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 |

## ■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

# 1 運用開始前に

この章では，運用管理の概要，および運用を開始する前に準備するものについて説明します。

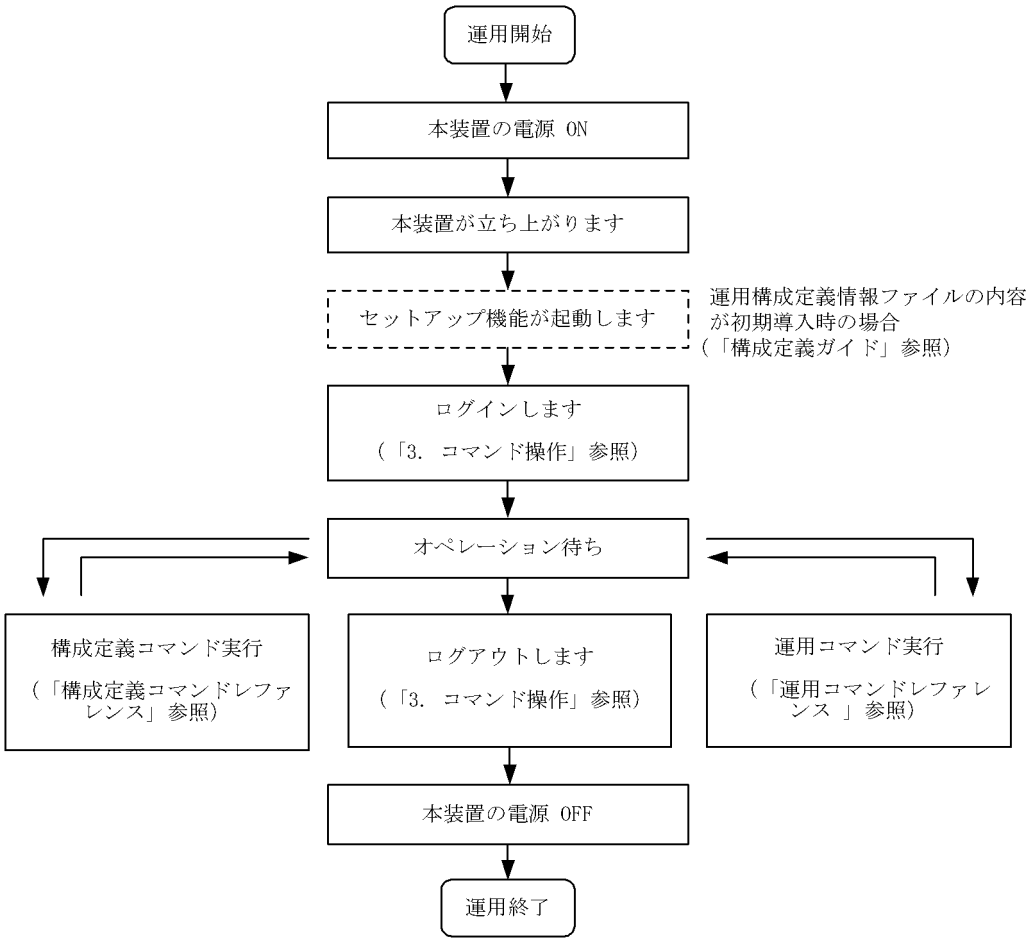
# 1.1 運用管理の概要

本装置はセットアップ作業が終了し，装置の電源 ON で運用に入ります。本装置と接続した運用端末では，運用コマンドや構成定義コマンドを実行し，装置の状態を調べたり，接続ネットワークの変更に伴う構成定義情報の変更を実施したりできます。運用端末の種類を「表 1-1　運用端末の種類」に，運用管理の概略を「図 1-1　運用管理の概略」に示します。

**表 1-1　運用端末の種類**

| 項番 | 種類 | 概要 |
|---|---|---|
| 1 | コンソール | 本装置と RS232C ケーブルで接続する端末 |
| 2 | リモート運用端末（リモートログイン） | 本装置と TCP／IP で通信できる端末で，telnet などでリモートログインする端末 |

**図 1-1　運用管理の概略**



# 1.2 本装置を運用する上での準備品

## 1.2.1 コンソール

本装置の初期導入時に運用端末として必要になるのがコンソールです。コンソールは RS-232C に接続する端末で，一般的な通信端末，通信ソフトウェアが使用可能です。

### (1) 通信ソフトウェア

コンソールで使用する通信ソフトウェアの一部を次に示します。

● Microsoft Windows 95 ／ Windows 98 ／ Windows 2000 ／ Windows NT 付属のハイパーターミナル

● Microsoft Windows 3.1 付属の Terminal

● Tera Term Pro(Version 2.3)

### (2) 通信ソフトウェアの設定値確認

コンソールが本装置と通信できるように，次の標準 VT-100 設定値（本装置のデフォルト設定値）が通信ソフトウェアに設定されていることを確認してください。

● 通信速度：9600bps

● データ長：8 ビット

● パリティビット：なし

● ストップビット：1 ビット

● フロー制御：なし

なお，通信速度に 9600bps 以外（1200 ／ 2400 ／ 4800 ／ 19200bps）を設定して使用したい場合は，構成定義コマンド router で本装置側の通信速度設定を変更してください。ただし，実際に設定が反映されるのはコンソールからいったんログアウトしたあとです。

### (3) 通信ソフトウェア使用上の注意

「(1) 通信ソフトウェア」であげた通信ソフトウェアは，それぞれ次に示す注意事項があります。

#### (a) ハイパーターミナル

接続中に通信速度を変更しても実際の通信速度は変更されません。ただし，ステータスバーの表示は変更後の値になります。ツールバーから切断，接続を行って通信速度を変更してください。

#### (b) Windows 3.1 付属の Terminal

［Ctrl］＋［C］によるコマンドの中断機能が使用できません。一般的に通信ソフトによって［ESC］，［Ctrl］との組み合わせ，ファンクションキー，特殊記号との組み合わせによる動作が異なります。

#### (c) Tera Term Pro(Version 2.3)

本装置立ち上げ後にコンソールを接続し，通信ソフトとして Tera Term Pro を立ち上げた場合，通信速度の不一致により文字化けを起こすことがあります。本現象となった場合は Tera Term Pro からブレーク信号を発行することで通信速度を一致させることができます（Tera Term Pro では［Alt］＋［B］によってブレーク信号を発行することができます）。通信速度が一致するまでに必要なブレーク信号の発行回数は，Tera Term Pro の設定内容と，本装置がそれ以前に認識していた通信速度によって異なります。また，表

示される内容が長い場合，1 行に表示可能な文字数が少ないと画面端で表示が折り返され，項目名と内容の表示がずれることがあります。通信ソフトの設定で画面サイズを変更し，1 行で表示可能な文字数を多くしてください。

### (4) RS-232C

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 1-2　クロスケーブルの結線仕様**

| 項番 | 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 |
| 1 | 5 | SG | ——— | 5 | GND |
| 2 | 3 | SD | ——— | 2 | RX |
| 3 | 2 | RD | ——— | 3 | TX |
| 4 | 7 | RS | ———┐ | 1 | DCD |
| 5 | 8 | CS | ———┘ ┌——— | 8 | CTS |
| 6 | 1 | CD | ———┐ └——— | 7 | RTS |
| 7 | 6 | DR | ——— | 4 | DTR |
| 8 | 4 | ER | ——— | 6 | DSR |

### (5) モデム

RM シリアル接続を行う場合，モデムやモデムと AT 互換機を接続するためのストレートケーブルを用意してください。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。

また，モデムに付属の説明書を参照し，AT コマンドを使用して次の表に示す設定を行ってください。拡張 AT コマンドを持つモデムでは，例で示したコマンドと異なるコマンドを使用する場合があります。

**表 1-2　モデムの設定**

| 設定項目 | 設定内容 | 指定例（Hayes 互換 AT コマンドの場合） |
|---|---|---|
| CD 信号状態 | CD 信号は通常オフで，相手モデムのキャリアを受信するとオンにします。 | AT&C1 |
| DTR 信号状態 | DTR 信号がオンからオフに変るとモデムを初期化します。 | AT&D3 |
| コマンドエコー | 入力したコマンドを DTE に出力しません。 | ATE0 |
| フロー制御 | DTE と DCE 間のフロー制御を設定します。<br>• RTS/CTS フロー制御有効<br>• XON/XOFF フロー制御無効 | AT&K3 |
| リザルトコード | リザルトコードを DTE に出力しません。 | ATQ1 |
| 自動着信 | 自動着信するまでの呼出し回数を設定します。 | ATS0=2 |
| リセット時の設定 | モデム内の不揮発性メモリから設定を読み出します。 | AT&Y0 |
| 設定の保存 | 設定をモデム内の不揮発性メモリに保存します。 | AT&W0 |

コマンドを DTE に出力しないようにコマンドエコーを設定すると，コマンドを入力しても文字は表示されません。設定が完了したらモデムに設定内容を保存します。設定保存後に設定内容を表示して確認します。

（例）Hayes 互換 AT コマンドでモデムを自動着信に設定する場合
AT&F&C1&D3E0&K3Q1S0=2&W0&Y0&V

RM シリアル接続（モデム）の場合は，通信ソフトウェアのダイアル機能を使用してダイアルします。ダイアルの設定は通信ソフトウェアの説明を参照してください。端末から AT コマンドを使用してダイアル接続できます。ダイアル機能を持たない通信ソフトウェアを使用する場合などは AT コマンドでダイアルしてください。AT コマンドのダイアル方法についてはモデムのマニュアルを参照してください。

（例）Hayes 互換 AT コマンドでダイアルする場合

- 公衆回線を使用してトーンで 123-4567 へダイアルする
  AT&FE0&S1S0=0S2=255TD123-4567
- 構内交換機を使用してトーンで 123-4567 へダイアルする
  AT&FX3E0&S1S0=0S2=255TD123-4567
- 構内交換機を使用してトーンで 0 をダイアルして，数秒待ってから 123-4567 へダイアルする
  AT&FX3E0&S1S0=0S2=255TD0,123-4567

## 1.2.2 リモート運用端末

本装置に，IP ネットワーク経由で接続してコマンド操作を行う端末が，リモート運用端末です。telnet，rlogin，および ftp プロトコルのクライアント機能がある端末はすべてリモート運用端末として使用することができます。

### (a) Windows2000 Telnet をリモート運用端末として使用する場合

Windows2000 Telnet を使用して本装置に Telnet ログインする場合，Windows2000 Telnet 改行コードの設定を画面上で変更する必要があります。次に示す手順で設定をしてください。一度設定すれば Windows 2000 端末の電源を OFF/ON しても設定内容は保存されます。

1. コマンドプロンプトから Windows 2000 付属の Telnet をオプションなしで起動します。
   ```
   C:¥Windows>telnet
   ```
2. Windows 2000 Telnet の画面がプロンプト付きで表示されるので，unset CRLF を実行します。
   ```
   Microsoft Telnet> unset CRLF
   ```

## 1.2.3 バックアップ用 MC

MC には，本装置の制御プログラムや構成定義情報などが格納されます。そのため，MC が故障すると本装置の立ち上げができなくなります。MC 故障時に迅速な復旧（故障 MC の交換）をするため，ご発注時に MC を 2 枚購入されていない場合は，別途バックアップ用 MC として MC をもう 1 枚追加購入されることをお勧めします。

また，MC が 2 枚あれば次の表に示す運用も可能です。

**表 1-3　2 枚の MC による運用方法**

| 運用方法 | 詳細 |
|---|---|
| 予備 MC によるバックアップ運用 | 予備の MC は，MC または MC スロットの障害時のバックアップとして使用します。<br>この場合，構成定義情報の変更は常に反映して同一内容にする必要があります。 |

| 運用方法 | 詳細 |
| --- | --- |
| 構成定義情報の 2 世代管理運用 | 2 種類の構成定義情報を切り替えて使用します。スロット 0 とスロット 1 の MC に異なる構成定義情報を入れておき，優先 MC スロットの設定を変更して起動することで構成定義情報を切り替えます。この場合，MC はバックアップとして使用できません。本運用は，優先 MC スロット指定機能がサポートされたバージョン以降で運用できます。 |
| ソフトウェアバージョンの 2 世代管理運用 | 2 種類のソフトウェアバージョンを切り替えて使用します。スロット 0 とスロット 1 の MC に異なるソフトウェアバージョンを入れておき，優先 MC スロットの設定を変更して起動することで，ソフトウェアバージョンを切り替えます。この場合，MC はバックアップとして使用できません。本運用は，優先 MC スロット指定機能がサポートされたバージョン以降で運用できます。 |

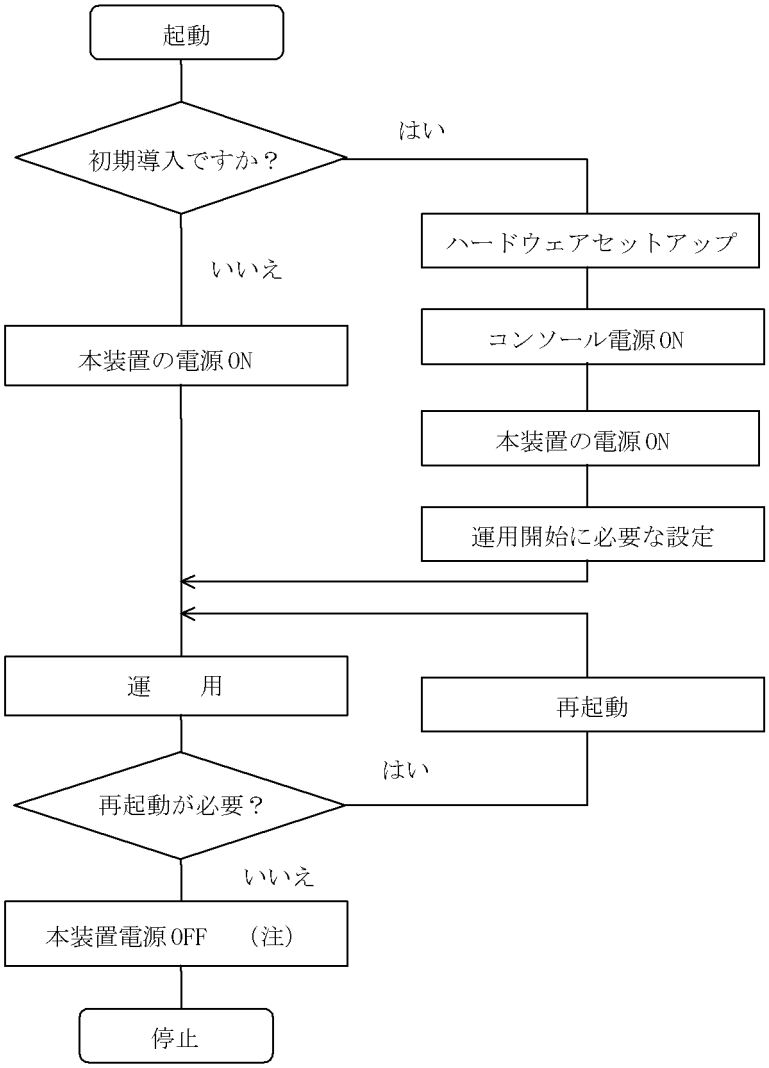
# 2 装置起動

この章では，装置の起動と停止について説明します。

# 2.1 起動から停止までの概略

本装置の起動から停止までの概略フローを次の図に示します。ハードウェアセットアップの内容については「ハードウェア取扱説明書」を参照してください。

**図 2-1 起動から停止までの概略フロー**




注

MC にアクセスしているときに電源 OFF すると，MC を破損する場合があります。

# 2.2　装置を起動する

本装置の起動，再起動の方法を，次の表に示します。

**表 2-1　起動，再起動の方法**

| 項番 | 起動の種類 | 内容 | 操作方法 |
|---|---|---|---|
| 1 | 電源 ON による起動 | 本装置の電源 OFF からの立ち上げです。 | 本体の電源スイッチを ON にします。 |
| 2 | リセットによる再起動 | 障害発生などにより，本装置をリセットしたい場合に行います。 | 本体のリセットスイッチを押します。 |
| 3 | コマンドによる再起動 | 障害発生などにより，本装置をリセットしたい場合に行います。 | reload コマンドを実行します。 |
| 4 | デフォルトリスタート | パスワードを忘れた場合に行います。パスワードによるセキュリティチェックを行いませんのでデフォルトリスタートによる起動を行う場合は十分に注意してください。なお，アカウント，構成定義情報はデフォルトリスタート前のものが使用されます。 | リセットスイッチを 3 秒以上押したあとに解除します。 |

本装置を起動，再起動した場合に STATUS ランプが赤点灯となった場合は，「7.1.2　STATUS ランプが緑点灯以外の状態である」を参照してください。また LED ランプ表示内容の詳細は，「ハードウェア取扱説明書」を参照してください。

# 2.3 装置を停止する

本装置の電源を OFF する場合は，MC にアクセスしていないことを確認して行ってください。MC のスロットごとに MC アクセスを示す LED があります。電源を OFF するときは，LED が消灯している（MC にアクセスしていない）ことを確認してください。LED が点灯している（MC にアクセスしている）ときに電源を OFF すると，MC を破損する場合があります。

また，運用コマンドまたは構成定義コマンドを実行したあと，すぐに電源を OFF する必要がある場合は，しばらく時間（約 10 秒）をおいたあと電源 OFF するか，reload stop コマンドで装置を停止させたあとに電源を OFF してください。

# 2.4 コンソールからログインする

装置起動後，コンソールには次の図に示すメッセージが表示されます。最後にログインプロンプトが表示されますので，そこで本装置にログインしてください。ログインの実行例については，「3.1 CLI での操作 （1）ログイン」を参照してください。

**図 2-2 装置起動時のメッセージ**

```
08/18 11:17:30 Starting 1st loader

ROM 03-02 Rev6 Wed Mar  6 13:05:59 2002 JST
BIOS Rev.:R1.02.E4 (990129)

08/18 11:17:33 Loading from MC slot 0

08/18 11:17:33 Starting 2nd loader
08/18 11:17:33 Loading /boot ... done.


08/18 11:17:34 Starting 3rd loader
08/18 11:17:35 Loading /bsd.0000.gz ... done.
08/18 11:17:37 Loading rdimage.gz ... done.(08/18 11:17:42 )
08/18 11:17:42 Loading rdimage2.gz ... done.(08/18 11:17:43 )

BSDI BSD/OS 3.1

login:
```

## 2.4.1 初期導入時のログイン

初期導入時にログインする場合，次のアカウント名を使用してください。

アカウント名：operator

パスワード：なし

# 3 コマンド操作

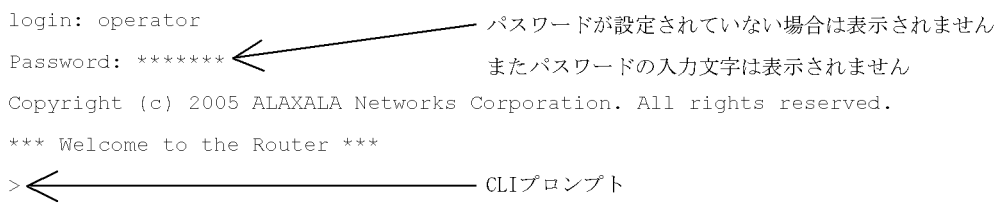
この章では，本装置でのコマンドの指定方法について説明します。

# 3.1 CLI での操作

## (1) ログイン

ログイン画面を次の図に示します。この画面でユーザ名とパスワードを入力してください。正しく認証された場合は，CLI プロンプトが表示されます。また，認証に失敗した場合は ” Login incorrect ” のメッセージが表示されます。

**図 3-1 ログイン画面**




## (2) ログアウト

CLI での操作を終了してログアウトしたい場合には logout コマンドまたは exit コマンドを実行してください。

**図 3-2 ログアウト**

```
> logout
login:
```

## (3) プロンプト

初期導入時の CLI プロンプトはユーザレベルとコマンド入力モードを識別しています。CLI プロンプト一覧を次の表に示します。

**表 3-1 CLI プロンプト一覧**

| ユーザレベル | コマンド入力モード | 実行するコマンド | プロンプト |
|---|---|---|---|
| 一般ユーザ | 運用コマンド | 新シンタックス運用コマンド | > |
| ルータ管理者※1 | 運用コマンド | 新シンタックス運用コマンド | # |
| | 構成定義コマンド※2 | 構成定義コマンド | (config)#※3 |

注※ 1

一般ユーザからルータ管理者になる場合は enable コマンドを実行してください。

注※ 2

構成定義コマンドモードになる場合は，ルータ管理者になってから configure コマンドを実行してください。

また，以下の場合においても，その状態を意味する文字が上記プロンプトの先頭に表示されます。

1. 本装置の識別名称を設定している（「構成定義コマンドレファレンス Vol.1　router」参照）場合，プロンプトに識別名称が反映されます。
2. 運用構成定義情報を編集し，その内容を構成定義情報ファイルに上書き保存（「構成定義コマンドレ

ファレンス Vol.1　save（write）」参照）していない場合，プロンプトの先頭に ”！” が付きます。

3. IPv4 ルーティングプロトコル情報，IPv4 マルチキャストルーティングプロトコル情報，IPv6 ルーティングプロトコル情報，IPv6 マルチキャストルーティングプロトコル情報および DHCP サーバ情報を編集し，構成定義コマンド apply でその内容を運用構成定義情報に反映していない場合は，プロンプトの先頭に ”!!” が付きます。

次の図に 1. ～ 3. の表示例を示します。

**図 3-3　プロンプト表示例**

```
> enable
# configure
(config)# router name "Router name"
!Router name(config)# save
Router name(config)# static 192.168.201.0 masklen 24 gateway 172.16.178.2
!!Router name(config)# apply
!Router name(config)# save
Router name(config)# quit
Router name# quit
Router name>
```

## (4) 補完機能

コマンドライン上で［Tab］を入力することで，コマンド入力時のコマンド名称やファイル名の入力を少なくすることができ，コマンド入力が簡単になります。次の図に補完機能を使用したコマンド入力の簡略化を示します。

**図 3-4　補完機能を使用したコマンド入力の簡略化**

```
(config)# li[Tab]
line        line-group
(config)# lin
```

［Tab］押下で使用することができるパラメータやファイル名の一覧が表示されます。

```
(config)# line line0 [Tab]
25atm             ct3               j2                oc48pos           t3
aps_protection    e1                oc12atm           pri
bri               e3                oc12pos           priisdn
briisdn           ethernet          oc3atm            serial
ce3               gigabit_ethernet  oc3pos            t1
(config)# line line0 [Tab]
```

## (5) ヘルプ機能

コマンドライン上で［?］を入力することで，指定できるコマンドまたはパラメータを検索できます。またコマンドやパラメータの意味を知ることができます。次の図に［?］入力時の表示例を示します。

**図 3-5 ［?］入力時の表示例**

```
> show ip ?
  bgp         Display BGP information
  cache       Display the conditions of policy route group information
  cpu-load    Display CPU load of the IP routing program
  dvmrp       Display DVMRP protocol information
  entry       Display a detail information of a particular route
  igmp        Display IGMP protocol information
  interface   Display the information of interface
  local       Display summarized policy routing information
  mcache      Displays multicast routing information
  memory      Display memory usage status by the IP routing program
  mroute      Display all PIM-SM routing information
  mstatic     Displays information about joining statically a multicast group
  ospf        Display OSPF protocol information
  pim         Display PIM protocol information
  policy      Display Policy Routing Information
  rip         Display RIP information
  route       Display all route
  rpf         Display RPF information for multicast source address
  task        Display the task information of the IP routing program
  timer       Display the timer information of the IP routing program
>
```

なお，パラメータの入力途中でスペース文字を入れずに［?］を入力した場合は，補完機能が実行されます。

また，コマンドパラメータで？文字を使用する場合は，［Ctrl］＋［V］を入力後，［?］を入力してください。

## (6) 入力エラー位置指摘機能

コマンドまたはパラメータを不正に入力した際，エラー位置を ”＾” で指摘し，次行にエラーメッセージ（「運用コマンドレファレンス Vol.1　1.2 入力エラー位置指摘で表示するメッセージ」を参照）を表示します。［Tab］入力時と［?］入力時も同様となります。

”＾” の指摘個所とエラーメッセージの説明により，コマンドまたはパラメータを修正し再度入力してください。入力エラー位置指摘の表示例を「図 3-6　スペルミス時の表示例」～「図 3-8　パラメータ入力途中の表示例」に示します。

**図 3-6　スペルミス時の表示例**

```
(config)# line line0 ehternet 1/0
line line0 ehternet 1/0
           ^
% illegal parameter at '^' marker
(config)#
```

**図 3-7　同じパラメータを 2 回入力したときの表示例**

```
(config)# line line0 ethernet 0/0
[line line0]
(config)# type 10m_full_duplex type auto_negotiation
type 10m_full_duplex type auto_negotiation
                     ^
% illegal combination or already appeared at '^' marker
[line line0]
(config)#
```

**図** 3-8　**パラメータ入力途中の表示例**

```
(config)# line line0 ethernet 0/0
[line line0]
(config)# type
type
      ^
% Incomplete commnad at '^' marker
[line line0]
(config)#
```

## （7） コマンド短縮実行

コマンドまたはパラメータを短縮して入力し，入力された文字が一意のコマンドまたはパラメータとして認識できる場合，コマンドを実行します。次の図に短縮入力のコマンド実行例を示します。

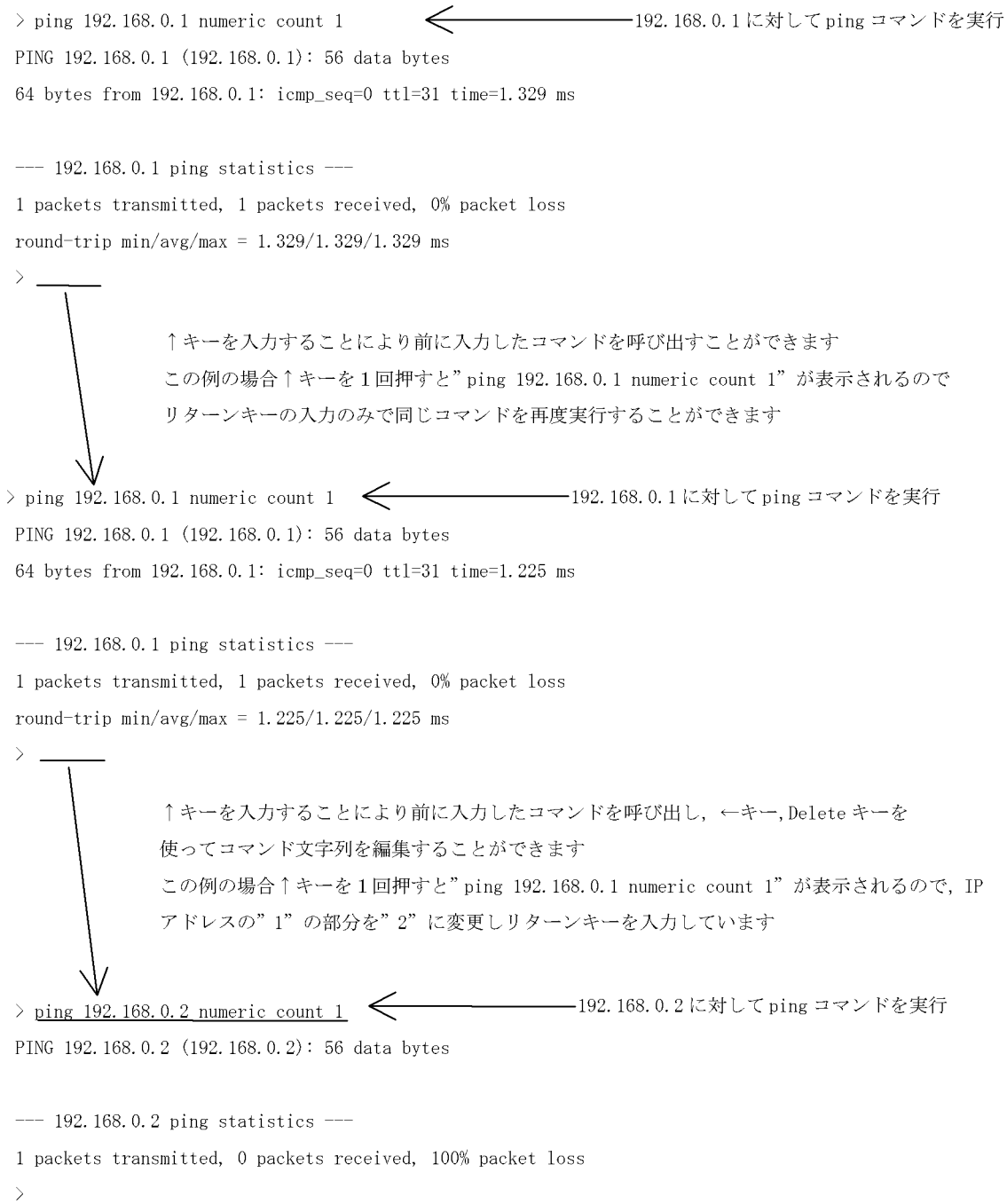
**図** 3-9　**短縮入力のコマンド実行例**（show ip route **の短縮入力**）

```
> sh ip ro[Enter]
Total: 6 routes
Destination       Next Hop       Interface     Metric    Protocol  Age
127/8             ----           localhost     0/0     Direct     4h 59m
127.0.0.1/32      127.0.0.1      localhost     0/0     Direct     4h 59m
172.16.250/24     192.168.11.101 rmEthernet    0/0     Static     4h 49m
172.16.251.64/26  192.168.11.101 rmEthernet    0/0     Static     4h 49m
192.168.11/24     192.168.11.14  rmEthernet    0/0     Direct     4h 49m
192.168.11.14/32  192.168.11.14  rmEthernet    0/0     Direct     4h 49m
>
```

## （8） ヒストリ機能

ヒストリ機能を使用すると，過去に入力したコマンドを簡単な操作で再実行したり，過去に入力したコマンドの一部を変更して再実行したりできます。次の図にヒストリ機能を使用した例を示します。

**図 3-10 ヒストリ機能を使用したコマンド入力の簡略化**




ヒストリ機能に次の表に示す文字列を使用した場合には，コマンド実行前に過去に実行したコマンド文字列に変換したあとにコマンドを実行します。

**表 3-2 ヒストリのコマンド文字列変換で使用できる文字一覧**

| 項番 | 指定 | 説明 |
|---|---|---|
| 1 | !! | 直前に実行したコマンドへ変換して実行します。 |
| 2 | !n | ヒストリ番号 n※のコマンドへ変換して実行します。 |
| 3 | !-n | n 回前のコマンドへ変換して実行します。 |

| 項番 | 指定 | 説明 |
|---|---|---|
| 4 | !str | 文字列 str で始まる過去に実行した最新のコマンドへ変換して実行します。 |
| 5 | ^str1^str2 | 直前に実行したコマンドの文字列 str1 を str2 に置換して実行します。 |

注※
show history コマンドで表示される配列番号のこと

注意事項
通信ソフトウェアによって方向キー（[↑]，[↓]，[←]，[→]）を入力してもコマンドが呼び出されない場合があります。その場合は通信ソフトウェアのマニュアルなどにより設定を確認してください。

## (9) パイプ機能

パイプ機能を利用することにより，コマンドの実行結果を別のコマンドに引き継ぐことができます。実行結果を引き継ぐコマンドに grep コマンドや sort コマンドを使うことにより，コマンドの実行結果をよりわかりやすくすることができます。「図 3-11　show sessions コマンド実行結果」に show sessions コマンドの実行結果を，「図 3-12　show sessions コマンド実行結果を grep コマンドでフィルタリング」に show sessions コマンドの実行結果を grep コマンドでフィルタリングした結果を示します。また，「図 3-13　show ip interface コマンド実行結果」に show ip interface コマンドの実行結果を，「図 3-14　show ip interface コマンド実行結果を sort コマンドでフィルタリング」に show ip interface コマンドの実行結果を sort コマンドでフィルタリングした結果を示します。

**図 3-11　show sessions コマンド実行結果**

```
> show sessions
operator         console  -----  0  Jul  7 10:57:30
operator         ttyp0    -----  1  Jul  7 10:13:01 (192.168.3.7)
operator         ttyp1    -----  2  Jul  7 10:49:49 (192.168.3.7)
operator         ttyp2    admin  3  Jul  7 11:06:41 (192.168.3.7)
>
```

**図 3-12　show sessions コマンド実行結果を grep コマンドでフィルタリング**

```
> show sessions | grep admin
operator         ttyp2    admin  3  Jul  7 11:06:41 (192.168.3.7)
>
```

**図 3-13　show ip interface コマンド実行結果**

```
> show ip interface summary
tokyo: UP  192.168.0.1  255.255.255.0
nagoya: UP  192.168.1.1  255.255.255.0
osaka: DOWN  192.168.2.1  255.255.255.0
fukuoka: UP  192.168.3.1  255.255.255.0
sapporo: DOWN  192.168.4.1  255.255.255.0
>
```

**図 3-14　show ip interface コマンド実行結果を sort コマンドでフィルタリング**

```
> show ip interface summary | sort
fukuoka: UP  192.168.3.1  255.255.255.0
nagoya: UP  192.168.1.1  255.255.255.0
osaka: DOWN  192.168.2.1  255.255.255.0
sapporo: DOWN  192.168.4.1  255.255.255.0
tokyo: UP  192.168.0.1  255.255.255.0
>
```

## (10) リダイレクト

リダイレクト機能を利用することにより，コマンドの実行結果をファイルに格納できます。次の図に show interfaces コマンドの実行結果をファイルに格納する例を示します。

**図 3-15 show interfaces コマンド実行結果をファイルに出力**

```
> show interfaces nif 0 line 0 > show_interface.log
>
```

## (11) ページング

コマンドの実行により出力される表示について，表示すべき情報が一画面にすべて表示しきれない場合には，ユーザのキー入力を契機に一画面ごとに区切って表示します。ただし，リダイレクトのあるときにはページングを行いません。なお，ページングは set terminal pager コマンドでその機能を有効にしたり無効にしたりできます。

## (12) 警告メッセージ

装置の状態を変更して，その状態のままにしておくと運用に差し障りがある場合があります。例えば，回線テストコマンドを実行すると該当回線は回線テスト状態のままになり，運用状態にはならないため該当回線を使用した通信が行えません。このように運用に差し障りがある状態にした場合には，警告メッセージがある旨のメッセージ「You have warning messages. Use ”show warning ”to see them.」を表示しますので，show warning コマンドを用いて警告メッセージを確認してください。また，set terminal warning-level コマンドによりその表示レベルを変更できます。警告メッセージの内容を次の表に示します。

**表 3-3 警告メッセージ一覧**

| メッセージ | 内容 |
|---|---|
| mc0 is disable | MC0 が使用禁止状態になっています。MC へのアクセスができないため，正常なオペレーションができない可能性があります。 |
| mc1 is disable | MC1 が使用禁止状態になっています。MC へのアクセスができないため，正常なオペレーションができない可能性があります。 |
| This Router is restarted by pressing default-restart-switch | デフォルトリスタートによって装置が起動されています。パスワードによるセキュリティチェックが動作していないので注意してください。 |
| Version mismatch between active and standbysoftware detected. | 運用系と待機系でソフトウェアのバージョンが異なっています。二重化運用をしていませんので注意してください。 |
| Date mismatch between active and standby configuration files detected. | 運用系と待機系で構成定義情報が異なっています。二重化運用をしていませんので注意してください。二重化にて運用している装置で運用系現用 MC に構成定義をコピーする場合，一時的に運用系と待機系の構成定義情報に差分が生じるため表示されている場合があります。 |
| NIF <NIF No.> Line <Line No.> is under line-test | 該当回線が回線テスト中になっています。該当回線は運用していません。<br><NIF No.>：NIF 番号<br><Line No.>：Line 番号<br><Subline No.>：Subline 番号 |
| NIF <NIF No.> Line <Line No.> subline <Subline No.> is under line-test | |

## (13) 運用メッセージ

装置の状態が変化した場合は運用メッセージをコンソールやリモート運用端末に表示します。例えば，回線が障害状態から回復した場合は回線が回復したメッセージを，回線が障害になり運用を停止した場合は回線が障害になったメッセージを表示します。運用メッセージの詳細については「メッセージ・ログレファレンス　2. ルーティングプロトコルのイベント情報」を参照してください。なおシェルプログラム実

行時や高負荷時には運用メッセージが表示されない場合がありますが，ログ情報にすべての運用メッセージが記録されていますので，ログ情報で確認してください。

## （14）自動ログアウト

CLI 起動中，一定時間（デフォルト：60 分）内にキー入力がなかった場合には自動的にログアウトします。なお自動ログアウト時間は set exec-timeout コマンドで変更できます。

# 3.2 CLI タイプ 1 の注意事項

## 3.2.1 自動ログアウト時の注意

自動ログアウトした場合は，再度ログインして CLI タイプ 1 を起動し直してください。なお，構成定義情報を編集中のまま自動ログアウトした場合は，構成定義情報ファイルはオープンしたままの状態になります。再度 CLI タイプ 1 を起動し，構成定義コマンド close で構成定義情報ファイルをクローズしてください。

## 3.2.2 ログイン後に運用端末がダウンした場合

ログイン後，運用端末がダウンした場合，本装置内ではログインしたままの状態になっている場合があります。この場合，自動ログアウトを待つか，再度ログインし直してログインしたままの状態になっているユーザを killuser コマンドで削除してください。また，構成定義編集中の場合は，「3.2.1　自動ログアウト時の注意」と同じように構成定義情報ファイルはオープンしたままの状態になっていますので，構成定義コマンド close で構成定義情報ファイルをクローズしてください。

# 4 初期導入時の作業

この章では，本装置を導入したときに必要な作業について説明しています。

# 4.1 ソフトウェアバージョンを確認する

運用開始後に，show version コマンドで本装置に組み込まれているソフトウェアの情報を確認してください。次の図に例を示します。

**図 4-1 ソフトウェア情報の確認**

```
> show version software
Model: AX2002RX  Serial No.: 0L HBY41C00026E801
S/W: AX-P6531-8B Ver.8.3.R [ROUTE-OS8B, Routing software]
>
```

# 4.2 ログインセキュリティを設定する

## 4.2.1 ルータ管理者のパスワードを設定する

構成定義コマンドを実行するためには enable コマンドでルータ管理者になる必要があります。初期導入時に enable コマンドを実行した場合，ルータ管理者のパスワードは設定されていませんので認証なしでルータ管理者になれます。ただし，通常運用中にすべての一般ユーザがパスワード認証なしでルータ管理者になれるのはセキュリティ上危険ですので，初期導入時にルータ管理者のパスワードを設定しておいてください。次の図に実行例を示します。

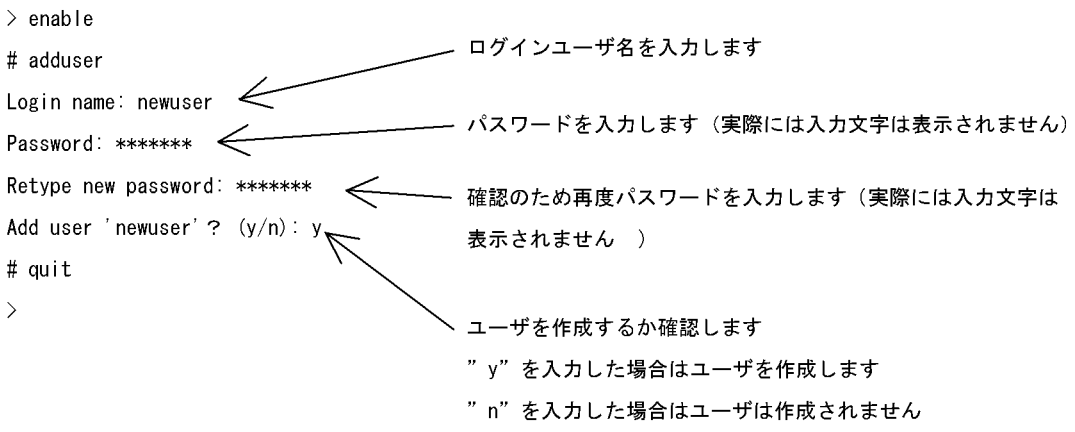
**図 4-2 初期導入直後のルータ管理者のパスワード設定**

```
> enable
# password
Changing local password for admin.
New password:
New password:
>
```

## 4.2.2 ログインユーザを作成する

adduser コマンドを用いて本装置にログインできるユーザを作成してください。次の図にログインユーザの作成例を示します。

**図 4-3 ユーザ newuser を作成**




また，RADIUS 認証を行う場合，RADIUS サーバに登録するユーザは本装置にも登録することをお勧めします。ただし，RADIUS サーバへの登録だけでもログインはできます。

## 4.2.3 初期導入時のログインユーザを削除する

初期導入時に設定されているログインユーザ ”operator ”を運用中のログインユーザとして使用しない場合は，セキュリティの低下を防ぐため，新しいログインユーザを作成したあとに rmuser コマンドで削除することをお勧めします。

## 4.2.4 同時にログインできるユーザ数を設定する

本装置に同時にログインできるユーザ数は，構成定義コマンド router（「構成定義コマンドレファレンス Vol.1 router」を参照）で変更できます。次の図に設定例を示します。

**図 4-4 同時にログインできるユーザ数の設定例**

```
(config)# router login_user 5
(config)#
```

**表 4-1 同時にログインできるユーザ数**

| 時期 | コンソール／リモート運用端末（telnet，rlogin） |
|---|---|
| 初期導入時 | 4 |
| 構成定義設定時 | 1 ～ 5 |

同時ログインに関する動作概要を次に示します

- 複数ユーザが同時ログインを行うと，ログインしているユーザ数が制限数以下でもログインできない場合があります。
- 同時にログインできるユーザ数を変更しても，すでにログインしているユーザのセッションが切れることはありません。

## 4.2.5 リモート運用端末からのログインを制限する

リモート運用端末から本装置へのログインについて，次に示す設定でログインを制限できます。なお，設定後はリモート運用端末から本装置へのログインの可否について確認してください。

### (1) ログインを許可する IP アドレスを設定する

リモート運用端末から本装置にアクセスするには，構成定義コマンド router（「構成定義コマンドレファレンス Vol.1 router」を参照）であらかじめアクセスを許可する端末の IP アドレスを登録しておく必要があります。アクセスを許可する IPv4 アドレスとサブネットマスク，または IPv6 アドレスとプレフィックスは，合わせて最大 128 個の登録ができます。なお，アクセスを許可していない（構成定義情報で登録していない）端末からのアクセスがあった場合，すでにログインしているその他の端末には，アクセスがあったことを示す ” Unknown host address <IP アドレス > ” のメッセージを表示します。

### (2) プロトコル単位でログイン停止を設定する

本装置は，構成定義コマンド router で，リモート運用端末からのログインをプロトコル単位で停止できます。指定できるプロトコルは telnet，rlogin，および ftp です。

### (3) RADIUS を使用して認証する

リモート運用端末から本装置へのログイン時，RADIUS を使用した認証が可能です。

# 4.3 時刻を設定する

## 4.3.1 概要

時刻は，本装置のログ情報や各種ファイルの作成時刻などに付与される情報です。運用開始時には正確な時刻を本装置に設定してください。時刻は，set calendar コマンドで設定します。

また，このほかに時刻情報に関連する設定には次の表に示すコマンドや機能があります。

**表 4-2 時刻情報に関連する設定**

| 項番 | コマンド／機能 | 設定内容 | 参照先 |
|---|---|---|---|
| 1 | config router コマンドの timezone パラメータ | 装置のタイムゾーンを設定します。 | 「構成定義コマンドレファレンス Vol.1 router」 |
| 2 | NTP 機能 | NTP プロトコルにより時刻情報を NTP サーバに同期させます。 | 「構成定義コマンドレファレンス Vol.2 ntp（NTP 情報）」 |
| 3 | rdate コマンド | リモートから日付・時刻情報を取得し設定します。 | 「運用コマンドレファレンス Vol.1 rdate」 |

## 4.3.2 時刻変更に関する注意事項

- 本装置で収集している統計情報の RM および RP の CPU 使用率と RP のバッファ使用率は，時刻が変更された時点で 0 クリアされます。
- OSPF または OSPFv3 使用時，10 秒以上の時刻変更を連続して実行した場合，OSPF の隣接関係が切断される場合があります。切断条件は，HelloInterval 時間（デフォルト 10 秒）内に RouterDeadInterval 時間 /10 回以上（デフォルトは 40/10 = 4 回以上）実施した場合です。
- 本装置において DVMRP による IP マルチキャスト通信を行う際に，時刻変更コマンド／機能により 10 秒以上の時刻変更を連続して実施した場合，DVMRP の隣接関係が切断され，一時的にマルチキャストパケット中継が停止することがあります。10 秒間に 10 秒以上の補正を連続して 2 回以上行った場合に発生します。

# 4.4 ボードの実装状態を確認する

装置起動後は，実装した RM/RP/NIF ボードの動作状態や搭載メモリ量などを確認してください。また，本装置はボードの種類が限定される機能もあります（詳細は「解説書 Vol.1　3. 収容条件」を参照）ので，現用構成定義情報を設定する前には，ボードの種類も確認してください。

## (1) RM/RP ボード

RM/RP ボードの状態や種類は show router コマンドで確認してください。

**図 4-5　RM/RP ボードの確認**

```
> show router
2005/04/25 17:40:52
router: AX2002RX, AX-P6531-8B Ver.8.3.R [ROUTE-OS8B]
node  : name=
        contact=
        locate=
     node info: simplex mode
     tunnel optimize: off
     ipv4 routing entry: current number=4 , max number=250000
     ipv6 routing entry: current number=7 , max number=25000
     main fan : active no=MFAN0, MFAN1, MFAN2
     power fan : active no=PFAN0
     power0 : active
     STATUS(RMP) LED : green
   rm0 : active
     rm   : INTERNAL 0000
     boot : 04/25 17:39:46 , power on , 0 times restart
     lamp : READY LED=green ,
            ALARM LED=light off , ERROR LED=light off , STATUS CODE=light off
     board: CPU=Intel Celeron 566MHz , memory=524,288kB(512MB)
     temperature : RM-CPU board=normal(30degree)
     MC0  : primary slot , mc-enabled
            AX-F6531-MC64 [BMC64] , AX2000R format , 001c0001
            37,808kB used (user Area: 37,808kB , dump Area: 0kB)
            19,152kB free (user Area: 13,050kB , dump Area: 6,102kB)
            56,960kB total(user Area: 50,858kB , dump Area: 6,102kB)
     MC1  : secondary slot , mc-disconnect
   rp0   :active INTERNAL
     memory : size = 131,072kB(128MB),18,432KB(18.0MB) used
              Fixed area used = 14,848KB(14.5MB)
              WAN used = 0KB(0.0MB)
              Ether used = 512KB(0.5MB)
              ATM used = 0KB(0.0MB)
              IP(unicast) used = 1,024KB(1.0MB)
              IP(multicast) used = 1,024KB(1.0MB)
              IPv6(unicast) used = 512KB(0.5MB)
              IPv6(multicast) used = 512KB(0.5MB)
```

## (2) NIF ボード

NIF ボードの状態や種類は show nif コマンドで確認してください。なお，show nif コマンドで表示される NIF 番号と対応する RP 番号は次の表に示すとおり，装置モデル別に異なりますのでご注意ください。

**図 4-6　NIF ボードの確認**

```
> show nif
2002/08/28 14:20:08
NIF0: unused  4-port PRI(leased line/dial up)  retry:0
NIF1: unused  2-port OC-3c/STM-1 POS(single-mode MPLS)  retry:0
>
```

表 4-3 NIF と RP の実装関係

| モデル | NIF 番号 | RP 番号 |
|---|---|---|
| AX2001R | 0，2 | 0 |
| AX2002R，AX2002RX | 0 ～ 2 | 0 |

# 4.5 構成定義情報を設定する

## 4.5.1 概要

運用開始時，本装置に接続するネットワークのメディアの種類や使用するルーティングプロトコルなど，本装置の動作環境を構成定義情報に定義してください。構成定義情報は，構成定義コマンドで定義できます。個々の構成定義情報の説明やコマンド，パラメータの仕様については「構成定義コマンドレファレンス Vol.1」「構成定義コマンドレファレンス Vol.2」を参照してください。また「構成定義ガイド」に，現用／予備構成定義情報ファイルの運用方法や構成定義情報の設定操作例を掲載していますので，併せて参照してください。

# 4.6 セキュリティへの配慮

## 4.6.1 ネットワークサービス機能を停止する

次の表で示すネットワークサービス機能は，ネットワーク上の装置に対して IP 通信ができれば使用可能になりますが，使用しない機能についてはセキュリティをより向上させるため停止することをお勧めします。

**表 4-4 初期導入時に使用可能なネットワークサービス機能**

| 項番 | 機能 | 停止方法 |
|---|---|---|
| 1 | リモート運用端末からの telnet プロトコルによるログイン | 構成定義コマンド router telnet disable を実行する。 |
| 2 | リモート運用端末からの rlogin プロトコルによるログイン | 構成定義コマンド router rlogin disable を実行する。 |
| 3 | リモート運用端末からの ftp プロトコルによるログイン | 構成定義コマンド router ftp disable を実行する。 |
| 4 | リモート運用端末からの time プロトコルによる時刻応答 | 構成定義コマンド router time disable を実行する。 |

# 5 インタフェース状態・ルーティング状態の確認

この章では，構成定義コマンドでネットワーク構成を設定したあとや運用中のトラブル発生時に行う，インタフェース状態およびルーティング状態の確認方法について説明します。

# 5.1 ネットワークインタフェース状態の確認

## 5.1.1 イーサネット／ギガビット・イーサネット回線の動作状態を確認する

イーサネット／ギガビット・イーサネット回線の動作状態確認方法は，次に示すとおりです。

### (1) 物理インタフェース

本装置からネットワークへの回線接続を行う上でイーサネットおよびギガビット・イーサネット回線を使用している場合，show interfaces コマンドを実行し，表示項目 <NIF 状態 > の表示が ” active ”（正常動作中），<Line 状態 > の表示が ” active up ”（正常動作中）であることを確認してください。

**図 5-1 「ギガビット・イーサネット回線接続状態」表示例**

```
> show interfaces nif 0 line 0
2000/04/02 12:00:00
NIF0: active  1-port 1000BASE-SX  retry:2
        Average:700/2000Mbps  Peak:750Mbps at 08:10:30
Line0: active up  1000BASE-SX full  00:00:87:40:0a:01
(以下省略)
>
```

なお，動作状態が正常でない場合の対応は「7.4.1　イーサネット回線の接続ができない」を参照してください。

### (2) Tag-VLAN 連携通信

本装置のイーサネットおよびギガビット・イーサネット回線で Tag-VLAN 連携通信機能を設定した場合，次の確認をしてください。

#### (a) 動作状態の確認

show interfaces コマンドで Tag-VLAN 連携を設定しているイーサネットおよびギガビット・イーサネット回線を指定して，表示項目 <NIF 状態 > の表示が ” active ”（正常動作中），<Line 状態 > の表示が ” active up ”（正常動作中）であることを確認してください。また，構成定義コマンド vlan で設定した Tag-vlan 連携回線情報が表示されていることも確認してください。

**図 5-2　Tag-VLAN 連携回線 summary 情報表示例**

```
> show interfaces nif 0 line 0
2000/04/02 12:00:00
NIF0: active  1-port 1000BASE-SX  retry:2
        Average:700/2000Mbps  Peak:750Mbps at 08:10:30
Line0: active up  1000BASE-SX full  00:00:87:40:0a:01
        Time-since-last-status-change:10:30:30
(以下途中省略)
VLAN:1 Interface name: TokyoOffice1 description: Network1
VLAN:2 Interface name: TokyoOffice2 description: Network2
>
```

#### (b) 統計情報の確認

show vlans コマンドまたは show vlan コマンドを実行し，Tag-VLAN 連携通信が実際運用されていること（送受信パケット数が 0 でないこと）を確認してください。

**図 5-3 Tag-VLAN 連携回線統計情報表示例**

```
> show vlans
2000/04/02 12:00:00
NIF1/LINE0: vlan statistics on
VLAN:1 Interface name: TokyoOffice1 description: Network1
<Out packets counter>                <In packets counter>
Out packets            :       120  In packets            :       130
Out Discard packets    :         5  In Discard packets    :         5
(以下省略)
>
```

### (3) PPPoE クライアント

本装置のイーサネット回線で PPPoE（PPP over Ethernet）クライアント機能を使用した場合，次の確認をしてください。

#### (a) セッション状態の確認

show interfaces コマンドを実行し，PPPoE セッション状態が ” connected ” であることを確認してください。” connected ” 状態以外のときの対応は，「7.5.3 PPPoE 通信ができない」を参照してください。

```
> show interfaces OsakaISP2
2002/04/05 10:56:30
NIF2: active  4-port 10BASE-T/100BASE-TX  retry:0
        Average:0/800Mbps  Peak:150Mbps at 13:53:03
Line0: active up  100BASE-TX full(auto)  00:00:87:a8:c5:1c
        Average out:20Mbps  Average in:10Mbps
PPPoE:OsakaISP2 connected  Session ID:e714  retry:0
        Connected time 02/13 00:00:00  Connecting time 1234:56:30
    Auto connection timer(past/setting):---/10(sec)
        Service Name:OsakaISPservice1
    AC Name:OsakaISP01server
    Destination MAC address  00:00:87:a8:fe:2c
    Source IP address:192.168.100.1  Destination IP address:192.168.35.2
    Primary DNS server IP address:128.10.10.1
    Secondary DNS server IP address:128.10.10.10
                                    ⎩
    CHAP Challenge timeout  :
>
```

Connected になっていること

MAC アドレスが取得できていること

## 5.1.2 WAN 回線の動作状態を確認する

WAN 回線の動作状態確認方法は，次に示すとおり回線種別やレイヤ 2 プロトコルの種別によって異なります。なお，動作状態が正常でない場合の対応は「7.4.2 WAN 回線の接続ができない」を参照してください。

### (1) 物理インタフェース

本装置からネットワークへの回線接続を行う上で WAN 回線を使用している場合，show interfaces コマンドを実行し，<NIF 状態 > の表示が ” active ”（正常動作中），<Line 状態 > の表示が ” active up ”（正常動作中）であることを確認してください。また，WAN T3 多重／ E3 多重回線については <Subline 状態 > の表示が ” active up ”（正常動作中）であることを，WAN BRI ／ PRI ／ 6.3M interface ／ T1 ／ T3 ／

E1 ／ E3 回線については <Timeslot 状態 > の表示が ” active up ”（正常動作中）であることを確認してください。

**図 5-4 「WAN 物理インタフェース接続状態」表示例**

```
> show interfaces nif 0 line 0 ts 1
2000/04/02 12:00:00
NIF0: active  8-port BRI(leased line/dial up)  retry:1
Line0: active up  BRI(leased line/dial up)  retry:1
Timeslot: 1-2 active up
(以下省略)
>
```

## (2) PPP

任意の物理インタフェースのレイヤ 2 プロトコルに PPP を指定している場合は，show interfaces コマンドを実行し，Line または Timeslot の detail 情報の，表示項目 LCP の表示が ” up ”（確立）であることを確認してください。また，次の表にあるネットワークプロトコルを使用している場合，それぞれの NCP の状態表示が ” up ”（確立）であることを確認してください。

**表 5-1 PPP NCP 対象のネットワークプロトコル**

| 項番 | ネットワークレイヤプロトコル | NCP |
|---|---|---|
| 1 | IP | IPCP |
| 2 | IPv6 | IPv6CP |
| 3 | IPX | IPXCP |
| 4 | Bridge | BridgeCP |

**図 5-5 「WAN PPP 状態」表示例**

```
> show interfaces nif 0 line 0
2000/04/02 12:00:00
NIF0: active  4-port serial(V.24/V.35/X.21)  retry:2
Line0: active up  serial(V.24)  speed:28.8kbps
       Protocol:PPP  MRU:4500 Bytes MTU:4500 Bytes
       LCP:up IPCP:up IPXCP:down BridgeNCP:down MPLSCP:down IPV6CP:down
(以下省略)
>
```

## (3) フレームリレー

任意の物理インタフェースのレイヤ 2 プロトコルにフレームリレーを指定している場合，次に示す手順で動作状態を確認してください。

1. show interfaces コマンドを実行し，Line または Timeslot の detail 情報の項目 local management（PVC 状態確認手順）の状態表示が ” up ” であることを確認してください。

**図 5-6 「WAN PVC 状態確認手順」表示例**

```
> show interfaces nif 0 line 0 ts 1
2000/04/02 12:00:00
NIF0: active  8-port BRI(leased line/dial up)  retry:1
Line0: active up  BRI(leased line/dial up)  retry:1
Timeslot: 1-2  active up
       Protocol:Frame Relay  local management:Q933 bidirectional up
(以下省略)
>
```

2. show frame-relay コマンドを実行し，<DLCI 状態 > の表示が ” active ”（正常動作中）であることを確認してください。

**図 5-7 「DLCI 状態」表示例**

```
> show frame-relay nif 0 line 0 ts 1 dlci 16
2000/04/02 12:00:00
NIF0: active  2-port PRI(leased line/dial up)  retry:2
Line0: active up  PRI(leased line/dial up)  retry:1
       description: Kansai local area communication line
Timeslot: 1-2 active
       Protocol:Frame Relay
       description: Kyoto area network
DLCI16 active forward static MTU:4096 Bytes no congestion
（以下省略）
>
```

3. 本装置を対向接続している場合，ping frame-relay コマンドを実行し，PVC(DLCI) の接続が確立（" Received " を表示）しているかどうかを確認してください。

**図 5-8 「Inverse ARP 応答」の表示例**

```
> ping frame-relay nif 0 line 1 dlci 16
Data Received InARP-seq=0
Data Received InARP-seq=1
Data Received InARP-seq=2
Data Received InARP-seq=3
Data Received InARP-seq=4
>
```

### （4） ISDN PPP

BRI 回線や PRI 回線のレイヤ 2 プロトコルに ISDN-PPP を指定している場合，show peer コマンドを実行し，通信相手情報の通信相手状態が " active "（運用中）であることを確認してください。

**図 5-9 「通信相手状態」表示例**

```
> show peer peer1
2000/04/02  12:00:00
peer1: active  ID:user1
        Phone Number1:0457743333
        Phone Number2:0457744444/1234
(以下省略)
>
```

## 5.1.3 ATM 回線の動作状態を確認する

本装置からネットワークへの回線接続を行う上で ATM 回線を使用した場合，次に示す手順で動作状態を確認してください。なお，動作状態が正常でない場合の対応は「7.4.3 ATM 回線の接続ができない」を参照してください。

1. show interfaces コマンドを実行し，<NIF 状態 > の表示が " active "（正常動作中），<Line 状態 > の表示が " active up "（正常動作中）であることを確認してください。

**図 5-10 「NIF/Line 状態」表示例**

```
> show interfaces nif 0 line 0
 2000/04/02 12:00:00
 NIF0: active  1-port OC-3c/STM-1 ATM(multi-mode)  retry:0
 Line0: active up  OC-3c/STM-1 ATM(multi-mode)
   Time-since-last-status-change:1:30:30
(以下省略)
>
```

2. show atm コマンドを実行し，<VC 状態 > の表示が " up "（正常動作中）であることを確認してください。

**図 5-11 「VC 状態」表示例**

```
> show atm nif 0 line 0 vpi 0 vci 32
 2000/04/02 12:00:00
 NIF0: active  1-port OC-3c/STM-1 ATM(multi-mode)  retry:0
 Line0: active up  OC-3c/STM-1 ATM(multi-mode)
(途中省略)
 VPI0:   PCR(VP Shaper)  10000kbps
VPI0/VCI32:     up  PVC ALARM
(以下省略)
>
```

3. VC の相手装置が F5 OAM Loopback セルをサポートしている場合，ping atm コマンドを実行し，当該 VC 間の通信が可能（”Received ”を表示している）かどうかを確認してください。

**図 5-12 「OAM F5 loopback cell 応答」表示例**

```
> ping atm nif 0 line 0 vpivci 0 32
Data Received OAM-seq=0
Data Received OAM-seq=1
Data Received OAM-seq=2
Data Received OAM-seq=3
Data Received OAM-seq=4
>
```

# 5.2 IPv4 ネットワーク状態の確認

本節では，構成定義コマンド ip で IPv4 アドレスを指定しているインタフェースの確認について説明します。

## 5.2.1 インタフェースの up/down を確認する

IPv4 ネットワークに接続する本装置の回線や回線内のポートに IPv4 アドレスを設定したあとに，show ip interface コマンドを実行し，IPv4 インタフェースの up/down 状態が ” UP ” であることを確認してください。

**図 5-13 「IPv4 インタフェース状態」の表示例**

```
> show ip interface summary
nagoya(0/0): UP  158.214.179.30/25
osaka(0/1): DOWN  158.214.180.30/25
fukuoka(0/2): UP  158.214.181.30/25
sapporo(0/3): DOWN  158.214.182.30/25
>
```

インタフェースが DOWN 状態の場合は，「7.5.1　通信ができない，または切断されている」を参照してください。

## 5.2.2 当該宛先アドレスとの通信可否を確認する

IPv4 ネットワークに接続している本装置のインタフェースについて，通信相手となる装置に対して通信できるかどうかを，ping コマンドを実行して確認してください。

**図 5-14　ping コマンドの実行結果（通信可の場合）**

```
> ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.1.51: icmp_seq=0 ttl=255 time=0.286 ms
64 bytes from 192.168.1.51: icmp_seq=1 ttl=255 time=0.271 ms
64 bytes from 192.168.1.51: icmp_seq=2 ttl=255 time=0.266 ms
^C
--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.266/0.274/0.286 ms
>
```

**図 5-15　ping コマンドの実行結果（通信不可の場合）**

```
> ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
ping: sendto: エラー要因
ping: wrote 192.168.0.1 64 chars, ret=-1
ping: sendto: エラー要因
ping: wrote 192.168.0.1 64 chars, ret=-1
ping: sendto: エラー要因
ping: wrote 192.168.0.1 64 chars, ret=-1
^C
--- 192.168.0.1 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
>
```

## 5.2.3 当該宛先アドレスまでの経路を確認する

traceroute コマンドを実行して，IPv4 ネットワークに接続している本装置のインタフェースから通信相手となる装置までの中継装置を確認してください。

**図 5-16 traceroute コマンドの実行結果**

```
> traceroute 192.168.0.1 numeric
traceroute to 192.168.0.1 (192.168.0.1), 30 hops max, 40 byte packets
1  192.168.2.101  0.612 ms  0.541 ms  0.532 ms
2  192.168.1.51  0.905 ms  0.816 ms  0.807 ms
3  192.168.0.1  1.325 ms  1.236 ms  1.227 ms
>
```

## 5.2.4 隣接装置との ARP 解決情報を確認する

IPv4 ネットワークに接続する本装置の回線や回線内のポートに IPv4 アドレスを設定したあとに，show ip arp コマンドを実行し，本装置と隣接装置間のアドレス解決をしているか（ARP エントリ情報があるか）どうかを確認してください。アドレス解決をしていない場合は，「7.5.1 通信ができない，または切断されている」を参照してください。

## 5.2.5 フィルタリング機能を確認する

本装置でフィルタリング機能を使用した場合の確認内容には次のものがあります。

### (1) 運用中の確認

#### (a) 統計情報の確認

show filter-flow コマンドを実行して IP フロー統計情報を表示し，廃棄されているパケット数を確認してください。廃棄パケット数が多い場合，本来はパケット廃棄をしてはいけない通信部位かもしれません。現在のネットワークの運用状況を確認してください。

**図 5-17 フィルタリングによるパケット廃棄数表示**

```
> show filter-flow interface tokyo detail
<Filter List No.>:    1
      Using Interface:tokyo1/in
      source ip :170.10.11.21 -170.10.11.30
      forward packets                                          :       461
<Filter List No.>:    2
      Using Interface:tokyo1/in
      drop packets                                             :     50121
<Filter List No.>:    1
      Using Interface:tokyo4/out
      source ip :170.10.12.1 -170.10.12.254
      forward packets                                          :         3
(以下省略)
>
```

## 5.2.6 ポリシールーティング機能を確認する

本装置でポリシールーティング機能を使用した場合の確認内容には次のものがあります。

### (1) 構成定義設定後の確認

#### (a) 入力先インタフェースの設定確認

show ip local policy コマンドを実行し，入力先インタフェースの現在のポリシールーティング条件が構成定義コマンド flow filter で設定されている内容であることを確認してください。

**図 5-18 入力先インタフェースの動作状態表示**

```
> show ip local policy interface tokyo
<Interface Name>:   tokyo    <Filter List No.>:    1
 ip source:                  200.1.4.0 - 200.1.4.255
 ip destination:             200.1.7.0 - 200.1.8.255
 current policy route
     Policy Group Name       route1
     Output Interface        tokyo3
     Next Hop IP address     200. 1. 10. 1
<Interface Name>:   tokyo    <Filter List No.>:    2
 ip source:                  200.1.5.0 - 200.1.5.255
 ip destination:             200.1.19.0 - 200.1.20.255
 current policy route
     Policy Group Name       route2
     Output Interface        yokohama
     Next Hop IP address     200. 1. 50. 2
(以下省略)
>
```

### (2) 運用中の確認

#### (a) 出力先インタフェースの状態確認

show ip cache policy コマンドを実行し，出力先インタフェースの動作状態が UP であることを確認してください。

**図 5-19 出力先インタフェースの動作状態表示**

```
> show ip cache policy route1
<Policy Group Name>:     route1
       priority  Interface Name  status   Nexthop
   *>      1     tokyo1            Up     200. 1. 1.  2
           2     tokyo1            Up     200. 1. 2.  2
           3     tokyo2            Down   200. 1. 8.  3
           4     tokyo3            Down   200. 1. 10. 1    default
>
```

## 5.2.7 Null インタフェースを確認する

本装置で Null インタフェースの機能を使用した場合の確認内容には次のものがあります。

### (1) 構成定義設定後の確認

#### (a) 経路情報の確認

show ip route コマンドを実行し，構成定義コマンド static で定義した経路情報の設定内容が正しく反映されているかどうかを確認してください。

**図 5-20 Null インタフェース経路情報表示**

```
> show ip route static
Total: 3 routes
Destination        Next Hop        Interface     Metric  Protocol  Age
172.16.250/24      192.168.11.101  rmEthernet    0/0     Static     1h  8m
172.16.251.89/32   ----            null          0/0     Static     1m  9s
(以下省略)
>
```

### (2) 運用中の確認

#### (a) パケット廃棄数の確認

show ip interface コマンドを実行し，Null インタフェースでパケットが廃棄されているかどうかを確認してください。

**図 5-21 Null インタフェースパケット廃棄数表示例**

```
> show ip interface delete-packets null-interface
Interface Name:null
Discard Packets(IPv4) :92(pkts)
>
```

## 5.2.8 ロードバランスで使用する選択パスを確認する

### (1) 構成定義設定後の確認

#### (a) 経路情報の確認

show ip route コマンドを実行し，定義したマルチパス経路の設定内容が正しく反映されているかどうかを確認してください。

**図 5-22 マルチパスの経路情報表示**

```
> show ip route
Total: 4 routes
Destination        Next Hop        Interface      Metric   Protocol  Age
172.16.10/24       172.16.10.1     LAN01          0/0      Direct    29s
172.16.10.1/32     172.16.10.1     LAN01          0/0      Direct     1h 12m
172.16.20.2/24     192.168.10.1    LAN10          0/0      Static     1h 10m
                   192.168.20.1    LAN20          -        -          -
                   192.168.30.1    LAN30          -        -          -
                   192.168.40.1    LAN40          -        -          -
172.16.100.2/24    172.16.10.2     LAN01          2/0      RIP       29s
>
```

#### (b) 当該宛先アドレスとの通信可否を確認する

ロードバランスで使用する本装置のインタフェースについて，通信相手となる装置に対して通信できるかどうかを，ping <IPv4 Address> specific-route source <Source Address> コマンドを実行して確認してください。ping コマンドの <Source Address> にはロードバランスで使用するインタフェースの本装置の自 IPv4 アドレスを指定してください。

## 5.2.9 マルチホーム接続を確認する

### (1) 構成定義設定後の確認

#### (a) 経路情報の確認

show ip interface コマンドを実行し，該当インタフェースに構成定義コマンド ip-address でマルチホーム

接続として定義した IPv4 アドレスが正しく反映されているかどうかを確認してください。

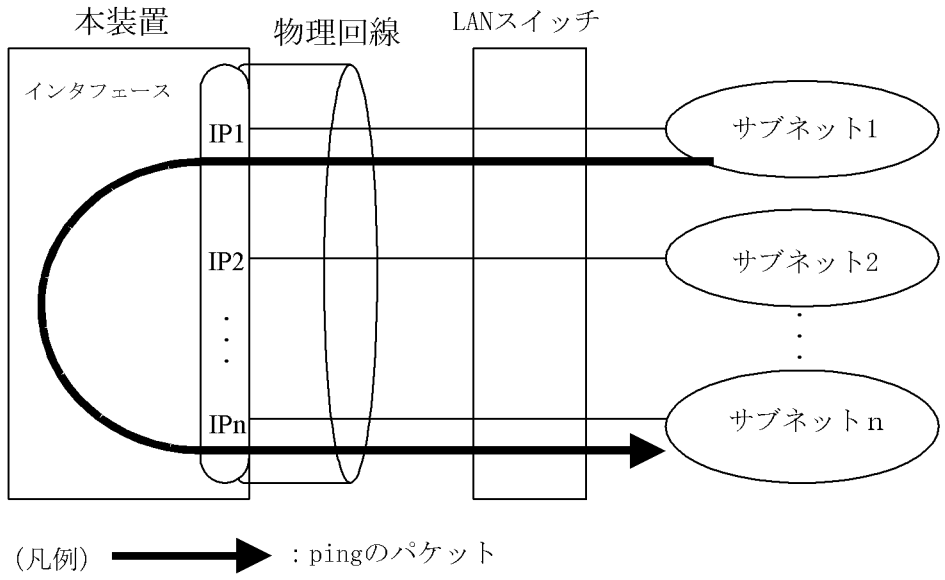
**図 5-23 マルチホーム接続時の IPv4 アドレス表示**

```
> show ip interface
tokyo1:  flags=80e3<UP,BROADCAST,NOTRAILERS,RUNNING,NOARP,MULTICAST>
         mtu 1500
         inet 172.16.10.1/24 broadcast 172.16.10.255
         inet 172.16.20.1/24 broadcast 172.16.20.255
         inet 172.16.30.1/24 broadcast 172.16.30.255
         NIF0/Line0: UP media 100BASE-TX full(auto) 00:00:87:d0:97:d8
         Time-since-last-status-change: 00:00:30
         Last down at: 08/21 16:21:01
>
```

#### (b) 当該宛先アドレスとの通信可否を確認する

本装置からマルチホーム接続の通信相手となる装置に対して通信できるかどうかを，ping コマンドを実行して確認してください。さらに，本装置とマルチホーム接続であり，同じインタフェースを使用している装置同士で通信できるかどうかを，ping コマンドを実行して確認してください。

**図 5-24 マルチホーム接続を確認する ping の流れ**




## 5.2.10 DHCP ／ BOOTP リレーエージェント機能を確認する

本装置で DHCP ／ BOOTP リレーエージェント機能を設定した場合の確認内容には次のものがあります。

### (1) 構成定義設定後の確認

#### (a) DHCP ／ BOOTP サーバへの通信確認

本装置から構成定義コマンド relay-list で設定した DHCP ／ BOOTP サーバまたは DHCP ／ BOOTP サーバが存在しているネットワークまでの，中継可能なルータの IP アドレスに対して通信ができるかどうかを，ping コマンドを実行して確認してください。

#### (b) リレーエージェントアドレスの確認

show dhcp giaddr コマンドを実行し，出力された IP アドレスが構成定義コマンド relay-interface で設定

したインタフェースの IP アドレスであることを確認してください。

**図 5-25　DHCP ／ BOOTP giaddr 表示**

```
> show dhcp giaddr interface Department1
DHCP GIADDR < Department1> : 130.3.3.1
>
```

show dhcp giaddr コマンドを実行し，出力された IP アドレスが「DHCP ／ BOOTP クライアントが接続されている本装置設定 IP アドレス」と一致していることを確認してください。特に，クライアント接続インタフェースにマルチホームの設定がある場合，そのインタフェースに最後に定義した IP アドレスをリレーエージェントアドレスとして設定していますのでご注意ください。次に構成例および実行例を示します。

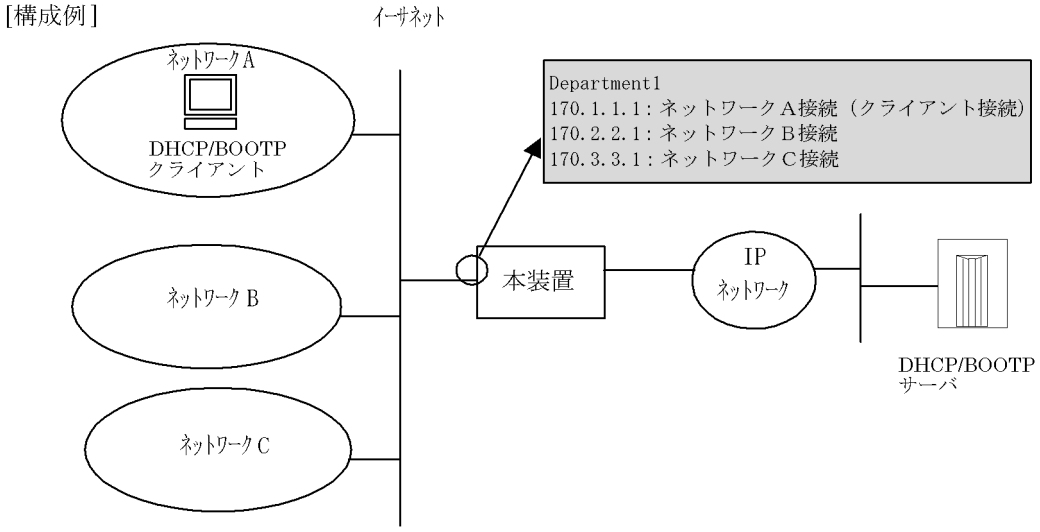



**図 5-26　DHCP ／ BOOTP giaddr 表示**

```
> show dhcp giaddr interface Department1
DHCP GIADDR < Department1> : 170.1.1.1
>
```

なお，出力された IP アドレスが，DHCP ／ BOOT クライアントが接続されている本装置 IP アドレスと一致していない場合の対応は，「7.5.2　DHCP 機能にて IP アドレスが割り振られない」を参照してください。

## 5.2.11　DHCP サーバ機能を確認する

本装置で DHCP サーバ機能を設定した場合の確認内容には次のものがあります。

### (1) 構成定義設定時の確認

#### (a) DHCP リレーエージェント装置との通信確認

DHCP リレーエージェントを経由して DHCP クライアントに IP アドレスを割り当てる場合，DHCP リレーエージェント装置に対して通信できるかどうかを，ping コマンドを実行して確認してください。

#### (b) 割り当て IP アドレスプール数の確認

本装置で接続できるクライアントの台数（IP アドレスプールの数）は 2000 台です。show ip dhcp server statistics コマンドを実行し，構成定義コマンド dhcp subnet や dhcp host で設定した，クライアントに割り当てる IP アドレスの数を確認してください。

**図 5-27 割り当て IP アドレスプール数表示例**

```
> show ip dhcp server statistics
   < DHCP Server use statistics >
     address pools           :10
     automatic bindings      :0
(以下省略)
>
```

### (2) 運用中の確認

#### (a) 割り当て済み IP アドレス数の確認

実際に DHCP クライアントへ割り当てられた IP アドレスについては，show ip dhcp binding コマンドを実行して確認してください。リースを満了していない IP アドレスが表示されます。

**図 5-28 割り当て済み IP アドレス数表示例**

```
> show ip dhcp binding
<IP address>    <MAC address>       <Lease expiration>   <Type>
192.168.200.9   00:80:98:48:e9:2d   01/12/06 19:59:40    Automatic
192.168.200.99  00:60:97:92:f7:b9                        Manual
>
```

## 5.2.12 DHCP クライアント機能を確認する

本装置で DHCP クライアント機能を設定した場合の確認内容には次のものがあります。

### (1) 構成定義設定後の確認

#### (a) IP アドレス取得の可否の確認

DHCP クライアント機能を設定したあと，構成定義コマンド dhcp-client で指定した本装置のインタフェースと同一ネットワーク上に DHCP サーバが存在すれば，IP アドレスが取得できます。show dhcp lease コマンドを実行し，実際に IP アドレスが取得できているかどうかを確認してください。また，DHCP サーバからデフォルトルータアドレスや DNS サーバアドレスを取得できるように構成定義コマンド dhcp-client でオプション指定している場合は，実際にそれらを取得できているかも確認してください

**図 5-29　show dhcp lease コマンド実行結果**

```
> show dhcp lease Site1
<Site1> ← インタフェース名
  IP-address  210.141.119.162    ← 表示が-.-.-.-の場合 IP アドレスが取得できていません。
  subnet-mask 255.255.255.0
  routers     210.141.119.1      ← デフォルトルータ，DNS サーバアドレス
  DNS         210.226.1.90, 210.226.1.20
  host-name   my_hostname
  domain-name foo.ne.jp
  lease-time  43200
  server-ID   210.226.1.41
  lease start 8/18 13:12:11
  T1 (renew)  8/18 19:12:11
  T2 (rebind) 8/18 23:42:11
  lease end   8/19 01:12:11
>
```

### (2) 運用中の確認

#### (a) 動作状態の確認

show ip dhcp client statistics コマンドを実行し，DHCP クライアントの動作状態を確認してください。
なお，確認内容は「7.5.2　DHCP 機能にて IP アドレスが割り振られない」を参照してください。

## 5.2.13　NAT，NAPT 機能を確認する

本装置で NAT，NAPT 機能を使用した場合の確認内容には次のものがあります。

### (1) 構成定義設定後の確認

#### (a) NAT，NAPT ルール情報の確認

show ip nat translations コマンドを実行し，構成定義コマンド nat で設定した NAT，NAPT 変換ルールが表示されることを確認してください。

**図 5-30　NAT，NAPT 変換ルール表示例**

```
> show ip nat translations
List of active rules:
isp01 static_nat 192.168.1.5-    200.200.1.15-
                 192.168.1.14/32 200.200.1.24/32
isp01 nat 192.168.2.0/24 200.200.2.0/28
isp01 static_napt auto 192.168.3.1/32 port 80 8080
isp01 napt 192.168.4.0/24 auto port_range 2000 3000
(以下省略)
>
```

### (2) 運用中の確認

#### (a) NAT，NAPT 変換情報の確認

show ip nat statistics コマンドを実行し，NAT，NAPT 変換の失敗がないことを確認してください。失敗

している場合は，show ip nat translations コマンドを実行し，表示項目 ” Reason ” でその要因を確認して対応してください。

**図 5-31 NAT，NAPT 変換情報表示例**

```
> show ip nat statistics
Translations Packet Count
    In       :          0    Out        :           0
Binding Table Information
    Added    :          0    Time-Out   :           0
    In Use   :          0    Max Use    :           0
    Rules    :          0
Misses
    Bad Translations :          2
>
```

**図 5-32 NAT，NAPT 変換失敗情報表示例**

```
> show ip nat translations
(途中省略)
List of bad translations:
                       Original              Outside             Reason
06/12 15:29:07 TCP  Out 192.168.0.42:1066     200.200.1.211:80    No Rules
06/12 15:33:17 UDP  Out 192.168.0.42:49188    200.200.1.211:7     No Port
06/12 15:33:18 TCP  Out 192.168.4.1:1053      203.203.3.3:80      No Port
>
```

## 5.2.14 DNS リレー機能を確認する

本装置で DNS リレー機能を使用した場合の確認内容には次のものがあります。

### (1) 構成定義設定後の確認

#### (a) ネームサーバの設定確認

show dns-relay コマンドを実行し，構成定義コマンド dns-resolver で設定したネームサーバの IP アドレスが表示されることを確認してください。

**図 5-33 ネームサーバ IP アドレス表示例**

```
> show dns-relay
Primary   NameServer: 192.168.253.177
Secondary NameServer: 192.168.253.178
Thirdary  NameServer: -
(以下省略)
>
```

なお，ネームサーバを PPPoE セッションで自動取得するように設定している場合は，PPPoE セッション情報で DNS アドレスが取得されているか確認してください。取得されていない場合は，相手サーバ（接続プロバイダ）側で DNS サーバアドレスを通知しないように設定されています。この場合は，接続プロバイダなどにご確認のうえ，手動でネームサーバを設定するようにしてください。

```
> show interfaces OsakaISP2
2002/04/05 10:56:30
NIF2: active  4 -port 10BASE -T/100BASE -TX  retry:0
       Average:0/800Mbps  Peak:150Mbps at 13:53:03
Line0: active up  100BASE  -TX full(auto)  00:00:87:a8:c5:1c
        Average out:20Mbps  Average in:10Mbps
PPPoE:Os akaISP2 connected  Session ID:e714  retry:0
       Connected time 02/13 00:00:00  Connecting time 1234:56:30
        Auto connection timer(past/setting):  ---/10(sec)
       Service Name:OsakaISPservice1
        AC Name:OsakaISP01server
        Destination MAC address 00:00:87:a8:fe:2c
        Source IP address:192.168.100.1  Destination IP address:192.168.35.2
        Primary DNS server IP address: 128.10.10.1
        Secondary DNS server IP address: 128.10.10.10
                      ⎩
        CHAP Challenge timeout  :
>
```

両方または,どちらかのアドレスが取得されていること

#### (b) ネームサーバへの通信確認

構成定義コマンド dns-resolver で設定した IP アドレス，または DHCP クライアント機能や PPPoE 機能で自動取得した IP アドレスについて，本装置と疎通できることを，ping コマンドを実行して確認してください。

### (2) 運用中の確認

#### (a) 動作状態確認

show dns-relay コマンドを実行し，DNS リレーの動作状態を確認してください。

なお，確認内容の詳細は「7.5.5　DNS リレー通信にてドメイン解決ができない」を参照してください。

## 5.2.15　VRRP の同期を確認する

本装置で VRRP の機能を使用した場合の確認内容には次のものがあります。

### (1) 構成定義設定後の確認

#### (a) 経路情報の確認

show vrrpstatus detail コマンドを実行し，構成定義コマンド virtual-router で定義した VRRP 情報の設定内容が正しく反映されているかどうかを確認してください。

**図 5-34 VRRP 運用状態表示**

```
> show vrrpstatus detail
Department1: VRID 1
   Virtual Router IP Address : 170.10.10.2
   Virtual MAC Address : 00-00-5e-00-01-01
   Current State : MASTER
   Admin State : enable
   Priority : 100/100
   IP Address Count : 1
   Master Router's IP Address : 170.10.10.2
   Primary IP Address : 170.10.10.1
   Authentication Type : SIMPLE TEXT PASSWORD
   Authentication Key : ABCDEFG
   Advertisement Interval : 1
   Preempt Mode : ON
   Virtual Router Up Time : Tue Feb 22 13:05:53 2000
   Critical Interface1 : Department2  Status : (IF UP)  DownPriority : 50
   VRRP Polling Status : (reachable)
   Target Address : 170.10.10.10
   Master Transition Delay : 60
```

## (2) 運用中の確認

### (a) 仮想ルータ状態の確認

本装置および本装置と同一仮想ルータを構成する相手装置において，仮想ルータの状態が MASTER または BACKUP になっていること，および同一仮想ルータで複数のマスタルータが存在しないことを確認してください。本装置での仮想ルータの状態確認には show vrrpstatus コマンドを使用してください。

**図 5-35 仮想ルータの状態表示例**

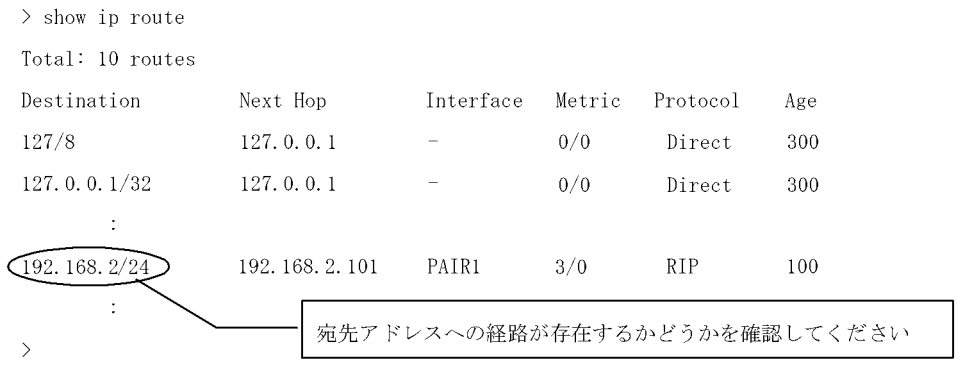
```
> show vrrpstatus
Department1:VRID 1 MASTER virtual-ip 170.10.10.2 priority 150
>
```

# 5.3 IPv4 ユニキャストルーティング情報の確認

## 5.3.1 宛先アドレスへの経路を確認する

本装置で IPv4 ユニキャストルーティング情報を設定した場合は，show ip route コマンドを実行して宛先アドレスへの経路が存在していることを確認してください。存在しない場合は，「5.3.2 RIP のゲートウェイ情報を確認する」～「5.3.4 BGP4 のピアリング情報を確認する」について確認してください。

**図 5-36 show ip route コマンドの実行結果**




## 5.3.2 RIP のゲートウェイ情報を確認する

本装置の IPv4 ユニキャストルーティング情報で RIP 機能を設定した場合は，show ip rip gateway を実行して，次のことを確認してください。

- Gateway Address 内に当該経路を広告すべき隣接ルータが存在するか確認してください。存在しない場合，隣接ルータから RIP パケットを受信していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- Age が 30 秒以内になっていることを確認してください。30 秒以上になっている場合，隣接ルータから周期的に RIP パケットが到達していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- Flags に Format，AuthFail が表示されていないか確認してください。Format，AuthFail が表示されている場合，隣接ルータから不正な RIP パケットを受信しています。隣接ルータを調査してください。
- Flags に Reject 表示がされていないか確認してください。Reject 表示がされている場合，当該ルータからの RIP パケットの受信が拒否状態となっています。構成定義情報の rip コマンド（interface 指定）で当該インタフェースに ripin オプションを指定してください。
- Flags に ImportRestrict 表示がされていないか確認してください。ImportRestrict がされている場合，インポートフィルタにより当該経路の取込みがフィルタリングされている可能性があります。構成定義情報のインポートフィルタを調査してください。
- その他の場合，隣接ルータが当該経路を広告していない可能性があります。隣接ルータを調査してください。

**図 5-37 show ip rip gateway コマンドの実行結果**

```
> show ip rip gateway
Gateway Address Age        Flags
192.168.50.185   1s      <Accept>
192.168.60.30   14s      <Accept>
192.168.70.30    9s      <Accept>
     :
>
```

## 5.3.3 OSPF のインタフェース情報を確認する

本装置の IPv4 ユニキャストルーティング情報で OSPF 機能を設定した場合は，show ip ospf interface <IP Address> または show ip ospf interface detail を実行して，次のことを確認してください。

- Neighbors 内に当該経路を広告すべき隣接ルータが存在するか確認してください。存在しない場合，隣接ルータから Hello パケットを受信していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- State が Two Ways 状態でないことを確認してください。Two Ways 状態の場合，自装置および隣接ルータの priority が設定されていない可能性があります。自装置および隣接ルータの priority を設定してください。
- State が Full 状態となっていることを確認してください。Full 状態以外の場合，隣接ルータとの隣接関係が確立していません。隣接ルータを調査してください。
- State が Full 状態の場合，隣接ルータが当該経路を広告していない可能性があります。隣接ルータを調査してください（隣接ルータが当該経路情報を広告しているかどうかは，show ip ospf database <LS-Type> コマンドで確認できます）。

**図 5-38 show ip ospf interface コマンドの実行結果**

```
> show ip ospf interface 192.168.50.1
Domain: 1
Index: 2, Name: Office1, Address: 192.168.50.1, State: BackupDR
Auth Type: Simple
MTU: 1436, DDinPacket: 70, LSRinPacket: 117, ACKinPacket: 70
Router ID: 172.168.50.1, Network Type: Broadcast
Area: 0.0.0.0, DR: 192.168.50.2, Backup DR: 192.168.50.1
Priority: 1, Cost: 1
Intervals:
Hello: 10s, Dead Router: 40s, Retransmission: 5s, Delay: 1s

Neighbor List (1):
Address         State      RouterID     Priority DR              Backup DR
192.168.50.2    Full       192.168.50.2    1     192.168.50.2    192.168.50.1
    :
>
```

## 5.3.4 BGP4 のピアリング情報を確認する

本装置の IPv4 ユニキャストルーティング情報で BGP4 機能を設定した場合は，show ip bgp neighbors を実行して，次のことを確認してください。

- BGP Status が Established 状態となっていることを確認してください。Established 状態以外の場合，相手 BGP4 スピーカとのピアリングが確立していません。相手 BGP4 スピーカとの通信が可能か ping コマンドなどで調査してください。不可能な場合，自装置と相手 BGP4 スピーカ間のインタフェースま

たはルータが障害となっている可能性があります。traceroute コマンドなどで障害部位を特定し，障害部位を調査してください。可能な場合，相手 BGP4 スピーカを調査してください。

- BGP Status が Established 状態の場合，相手 BGP4 スピーカが当該経路を広告していない可能性があります。相手 BGP4 スピーカを調査してください（相手 BGP4 スピーカが当該経路情報を広告しているかどうかは，show ip bgp route コマンドで確認できます）。

**図 5-39　show ip bgp neighbors コマンドの実行結果**

```
> show ip bgp neighbors 192.168.50.2
BGP Peer: 192.168.50.2, Remote AS: 1810
    BGP Status: Established         HoldTime: 90
    Established Transitions: 1      Established Time: 16:25:34
    BGP Version: 4                  Type: External
    Local Address: 192.168.50.1     Local AS: 2735
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 18:42:20  Last Keep Alive Receive: 18:42:20
    BGP Messages UpdateIn UpdateOut TotalIn TotalOut
                      12        14      36       42
    BGP Capability negotiation: <IPv4-Uni>
      Send   : <IPv4-Uni>
      Receive: <IPv4-Uni>
    Authentication : TCP MD5
   :
>
```

## 5.3.5　IS-IS の隣接情報を確認する

本装置の IPv4 ユニキャストルーティング情報で IS-IS 機能を設定した場合は，show isis adjacency を実行し，次のことを確認してください。

- Adjacencies 内に当該経路を広告すべき隣接ルータが存在するか確認してください。存在しない場合，隣接ルータから Hello パケットを受信していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- State が Up 状態となっていることを確認してください。Up 状態以外の場合，隣接ルータが本装置を認識していません。隣接ルータを調査してください。
- State が Up 状態の場合，隣接ルータが当該経路を広告していない可能性があります。隣接ルータを調査してください（隣接ルータが当該経路情報を広告しているかどうかは，show isis database コマンドで確認できます）。

**図 5-40　show isis adjacency コマンドの実行結果**

```
> show isis adjacency detail
Level-1 adjacencies
Interface: Office1, Interface Type: Broadcast
    System ID: 0000.87c0.3655, Type: IS, State: Up
    Speaks: IP
    Circuit ID: 0x04, SNPA: 00.00.87.c0.36.55
    Priority : 64, Hold Timer: 9s, Established Time: 2003/07/01 15:30:00
    Interface Address: 192.168.7.2
>
```

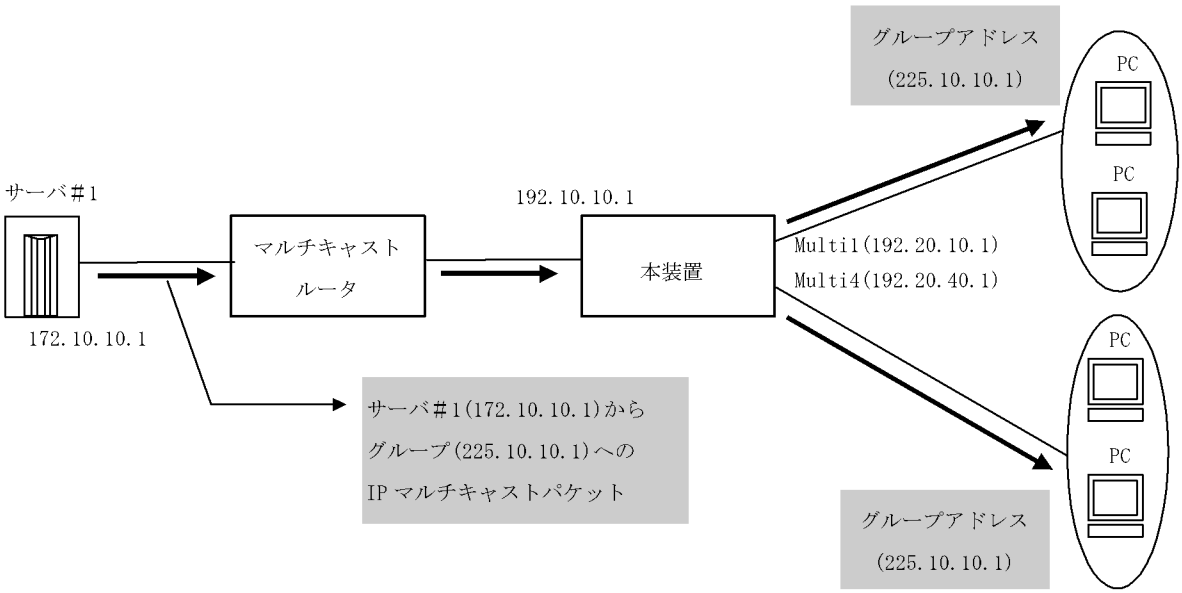
# 5.4　IPv4 マルチキャストルーティング情報の確認

## 5.4.1　宛先グループアドレスへの経路を確認する

本装置で IPv4 マルチキャストルーティング情報の設定を行った場合は，show ip mcache コマンドを実行して宛先アドレスへの経路が存在していることを確認してください。存在しない場合，および downstream が正しくない場合は，「5.4.2　PIM-DM，PIM-SM 情報を確認する」～「5.4.4　IGMP 情報を確認する」について確認してください。

**図 5-41　show ip mcache コマンドの実行結果**

```
> show ip mcache
Total: 1 routes
Group               Source              Uptime    Expires   Interface
225.10.10.1         172.10.10.1         01:00     02:00     192.10.10.1
      downstream:
          Multi1(192.20.10.1)
          Multi4(192.20.40.1)

>
```




## 5.4.2　PIM-DM，PIM-SM 情報を確認する

本装置の IPv4 マルチキャストルーティング情報で，PIM-DM 機能または PIM-SM 機能を設定した場合の確認内容には次のものがあります。

### (1) インタフェース情報

show ip pim interface を実行して，次のことを確認してください。

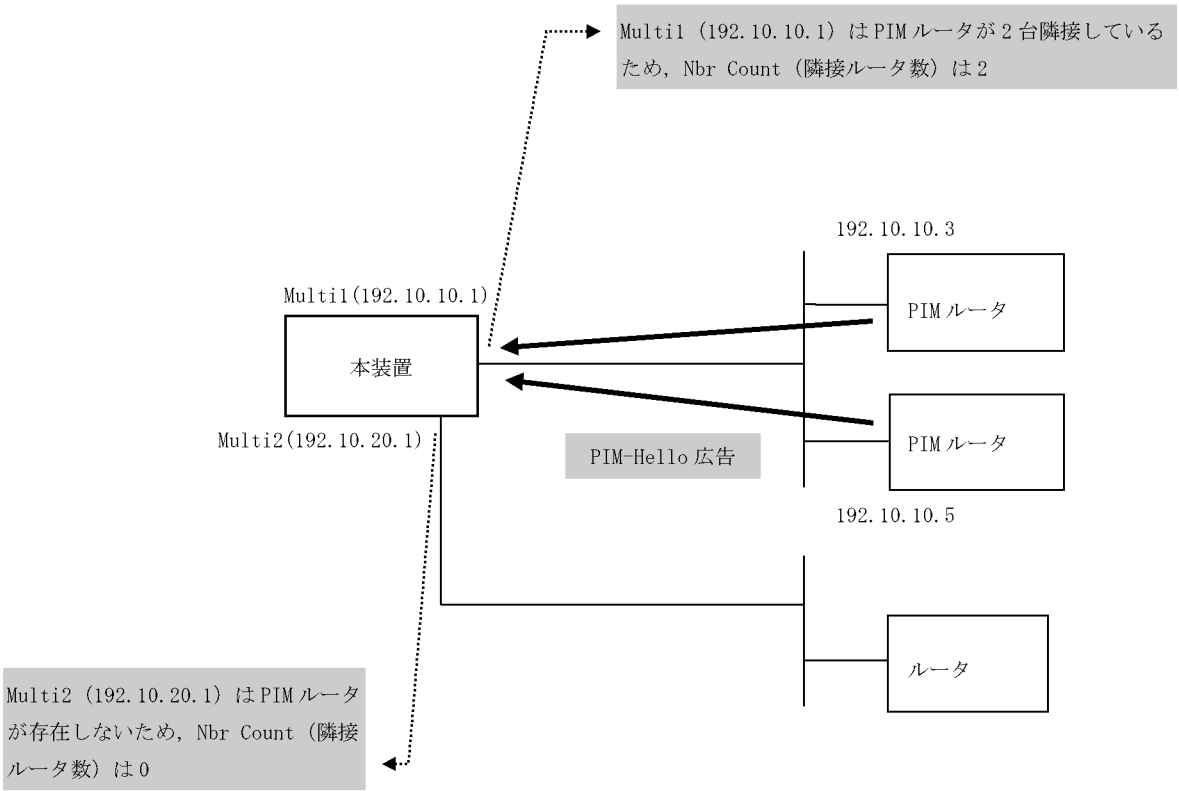
● Address 内のインタフェースを確認してください。存在しない場合，そのインタフェースで PIM-DM

および PIM-SM は動作していません。構成定義情報で当該インタフェースで PIM が enable になっているか確認してください。また，そのインタフェースに障害が発生していないか確認してください。

● 該当インタフェースの Nbr Count（PIM 隣接ルータ数）を確認してください。0 の場合は隣接ルータが存在しないか，隣接ルータが PIM-Hello を広告していない可能性があります。隣接ルータを調査してください。

**図 5-42　show ip pim interface コマンドの実行結果**

```
[PIM-DMの場合の表示]

> show ip pim interface
Address       Interface   Component  Vif  Nbr     Query   JP      C-RP      DR
                                            Count   Intvl   Intvl
192.10.10.1   Multi1      PIM-DM     1    2       30      -       -         -
192.10.20.1   Multi2      PIM-DM     2    0       30      -       -         -
>

[PIM-SMの場合の表示]

> show ip pim interface
Address           Interface   Component  Vif   Nbr       Hello   DR
                                                Count     Intvl
192.10.10.1       Multi1      PIM-SM     1     2         30      192.10.10.5
192.10.20.1       Multi2      PIM-SM     2     0         30      192.10.20.1
>
```



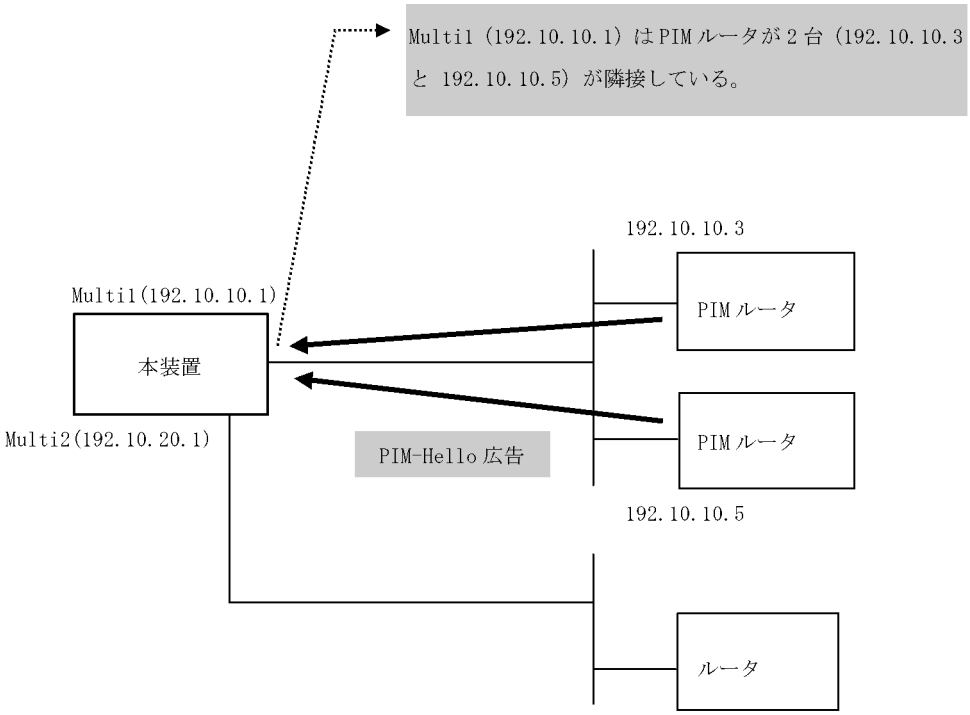

## （2） 隣接情報

show ip pim neighbor を実行し，当該インタフェースの NeighborAddress 内の IP アドレスで隣接相手を

確認してください。ある特定の隣接が存在しない場合，隣接ルータが PIM-Hello を広告していない可能性があります。隣接ルータを調査してください。

**図 5-43 show ip pim neighbor コマンドの実行結果**

```
> show ip pim neighbor
Address             Interface           NeighborAddress     Uptime    Expires
192.10.10.1         Multi1              192.10.10.3         00:05     01:40
                                        192.10.10.5         00:10     01:35
>
```

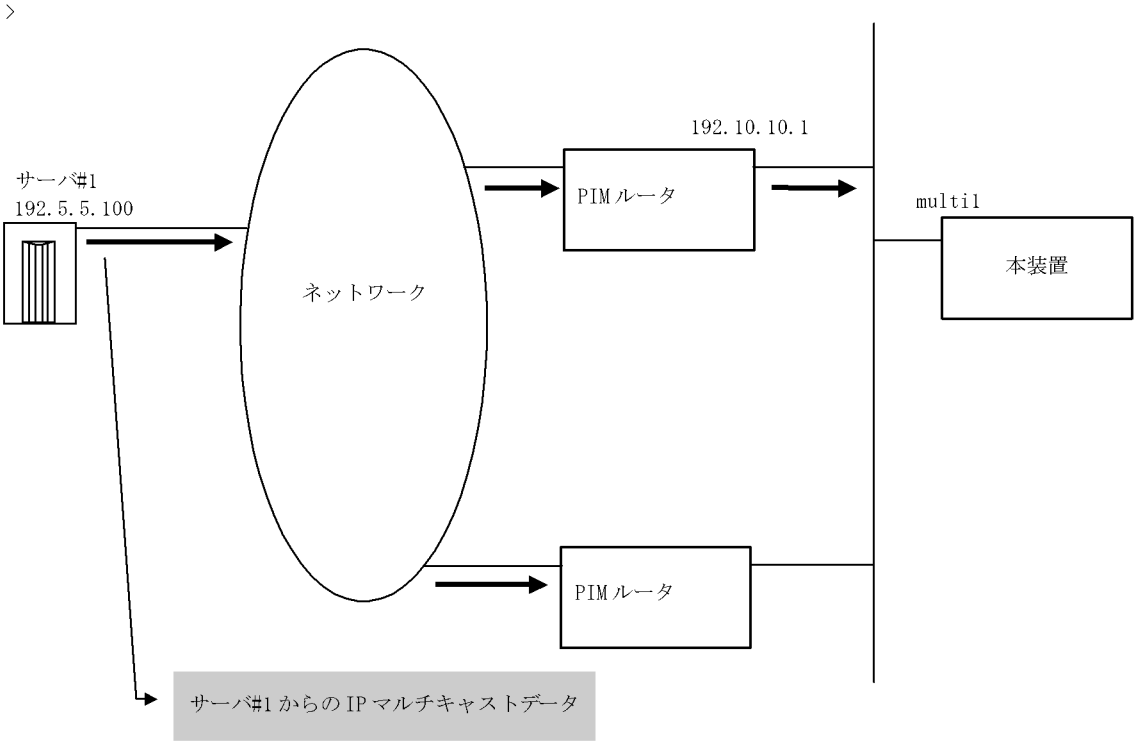



## （3） 送信元ルート情報

show ip rpf コマンドを実行し，送信元のルート情報を確認してください。

**図 5-44 show ip rpf コマンドの実行結果**

```
> show ip rpf 192.5.5.100
RPF Information for ? (192.5.5.100):
If multi1 NextHop 192.10.10.1 proto 103

>
```




## (4) PIM-SM BSR 情報

show ip pim bsr を実行し，BSR アドレスが表示されていることを確認してください。”----”表示の場合，BSR が Bootstrap メッセージを広告していないか，BSR が存在していない可能性があります。BSR を調査してください。なお，PIM-SSM では BSR は使用しませんのでご注意ください。

**図 5-45 show ip pim bsr コマンドの実行結果**

```
> show ip pim bsr
Status: Not Candidate Bootstrap Router
BSR Address:192.10.10.10
    Priority:100,Hash Mask length:30
    Uptime:03:00
    Bootstrap Timeout:130 seconds
>
```

## (5) PIM-SM ランデブーポイント情報

show ip pim rendezvous-point mapping を実行し，該当の IPv4 マルチキャストグループアドレスに対する C-RP Address が表示されていることを確認してください。表示のない場合，BSR が Bootstrap メッセージを広告していないか，ランデブーポイントまたは BSR が存在していない可能性があります。ランデブーポイントおよび BSR を調査してください。なお，PIM-SSM ではランデブーポイントは使用しませんのでご注意ください。

**図 5-46 show ip pim rendezvous-point mapping コマンドの実行結果**

```
> show ip pim rendezvous-point mapping
Status: Not Candidate Rendezvous Point
Total: 2 routes, 2 group, 1 RPs
Group/masklen         C-RP Address        pri   Uptime  Expires
224.100.100.0/24      192.1.1.1           100   02:00   02:30
224.100.200.0/24      192.1.1.1           100   02:00   02:30
>
```

### (6) PIM-SM ルーティング情報

show ip mroute コマンドを実行し，当該宛先アドレスへの経路が存在するかどうかを確認してください。(S,G) エントリが存在しない場合は，(*,G) エントリが存在しているかを確認してください。(*,G) が存在しない場合，および in-coming.downstream が正しくない場合は隣接ルータを調査してください。なお，PIM-SSM では (*,G) は使用しません (存在しません)。

**図 5-47 PIM-SM マルチキャストルート情報の表示**

```
> show ip mroute
Total: 5 routes, 3 groups, 2 RPs
(S,G) 2 routes ------------------------------------------------------------
Group Address      Source Address  Protocol Flags  Uptime  Expires  Assert
224.100.100.10     192.1.1.1       SM       F      02:00   02:30    01:00
    in-coming : Multi1(192.1.1.3)               upstream: Direct, Reg-Sup: 60s
    downstream: Multi2(192.1.2.3)               uptime 02:30, expires 00:40
224.100.100.20     192.1.1.1       SM       F      02:00   02:30    01:00
    in-coming : Multi1(192.1.1.3)               upstream: Direct
    downstream: Localhost(127.0.0.1) <Register to 192.1.5.1>
224.100.100.30     192.1.4.1       SM       F      02:00   02:30    01:00
    in-coming : Multi1(192.1.1.3)               upstream: 192.1.1.5
    downstream: Multi2(192.1.2.3)               uptime 02:30, expires 00:40

(*,G) 2 routes ------------------------------------------------------------
Group Address      RP Address      Protocol Flags  Uptime  Expires  Assert
225.100.100.10     192.1.5.1       SM       R      02:00   02:30    01:00
    in-coming : Localhost(127.0.0.1)            upstream: This Router
    downstream: Multi2(192.1.2.3)               uptime 02:30, expires 00:40
225.100.100.10     192.1.5.1       SM       R      02:00   02:30    01:00
    in-coming : Multi1(192.1.1.3)               upstream: 192.1.1.2
    downstream: Multi3(192.1.3.3)               uptime 02:30, expires 00:40
>
```

## 5.4.3 DVMRP 情報を確認する

本装置の IPv4 マルチキャストルーティング情報で DVMRP 機能を設定した場合の確認内容には次のものがあります。

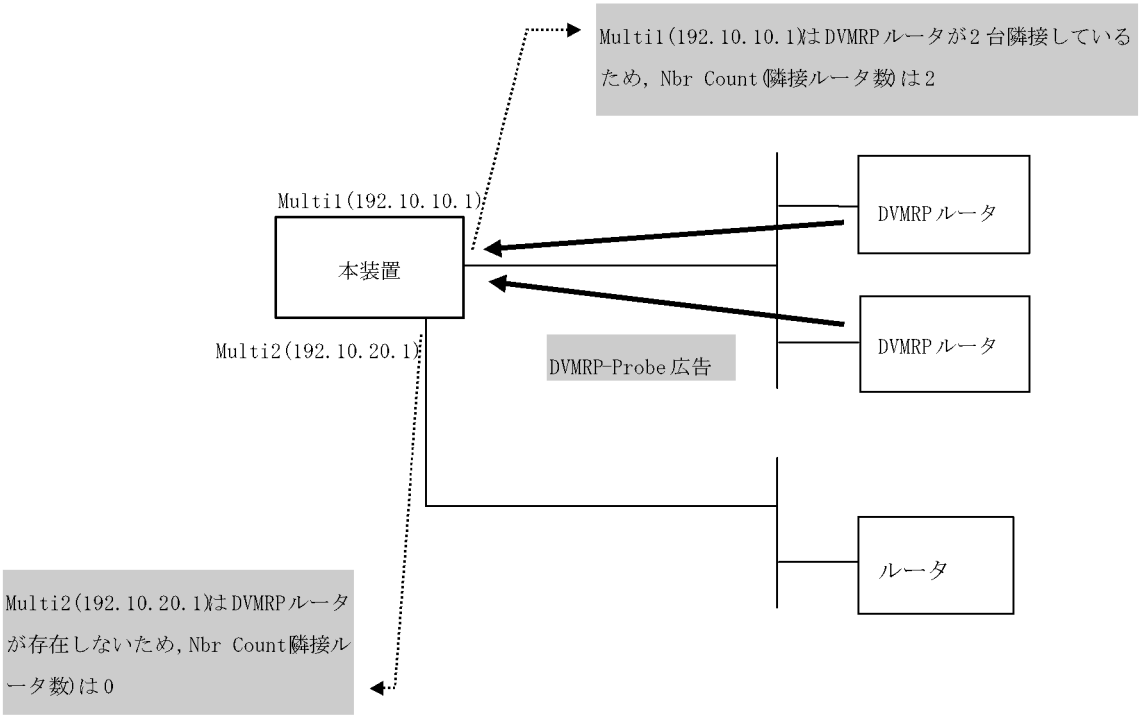
### (1) インタフェース情報

show ip dvmrp interface を実行し，次のことを確認してください。

- Address 内のインタフェースを確認してください。存在しない場合，そのインタフェースで DVMRP は動作していません。構成定義情報で当該インタフェースで DVMRP が enable になっているか確認してください。また，そのインタフェースに障害が発生していないか確認してください。
- 該当インタフェースの Nbr Count (DVMRP 隣接ルータ数) を確認してください。0 の場合は隣接ルータが存在しないか，隣接ルータが DVMRP-Probe を広告していない可能性があります。隣接ルータを調査してください。

**図 5-48 show ip dvmrp interface コマンドの実行結果**

```
> show ip dvmrp interface
Address            Interface    Component  Vif    Nbr       #Bad      #Bad      Kind
                                                   Count     Pkts      Pkts
192.10.10.1        Multi1       DVMRP       1        2        0         0       -
192.10.20.1        Multi2       DVMRP       2        0        0         0       -
>
```

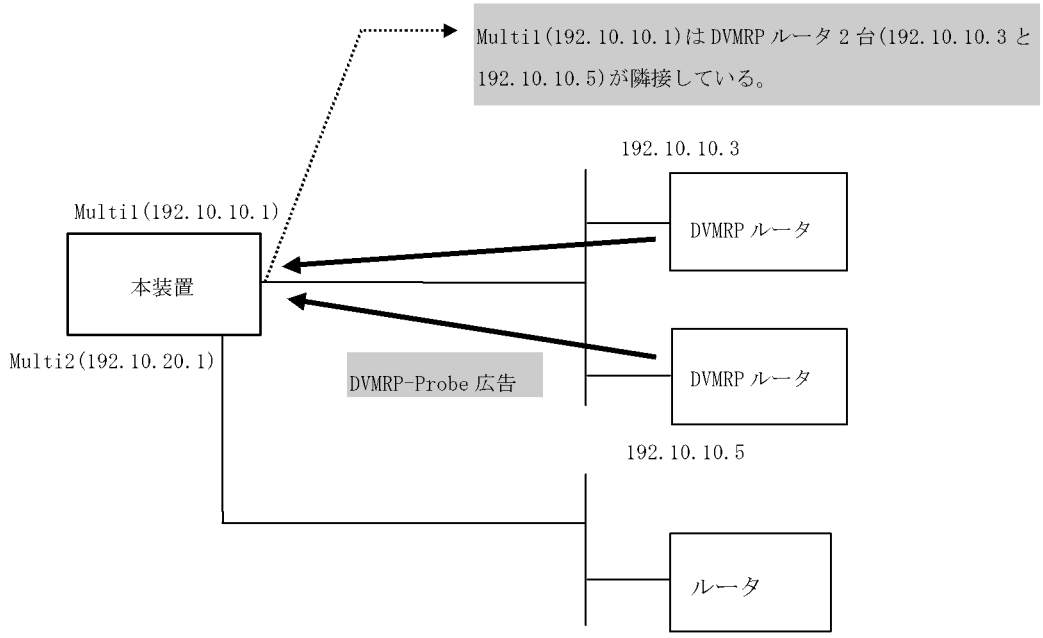



## (2) 隣接情報

show ip dvmrp neighbor を実行し，当該インタフェースの NeighborAddress 内の IP アドレスで隣接相手を確認してください。ある特定の隣接が存在しない場合，隣接ルータが DVMRP-Probe を広告していない可能性があります。隣接ルータを調査してください。

**図 5-49 show ip dvmrp neighbor コマンドの実行結果**

```
> show ip dvmrp neighbor
Address             Interface           NeighborAddress     Uptime    Expires   GenID
192.10.10.1         Multi1              192.10.10.3         00:05     01:40     898492808
                                        192.10.10.5         00:10     01:35     747551062
>
```

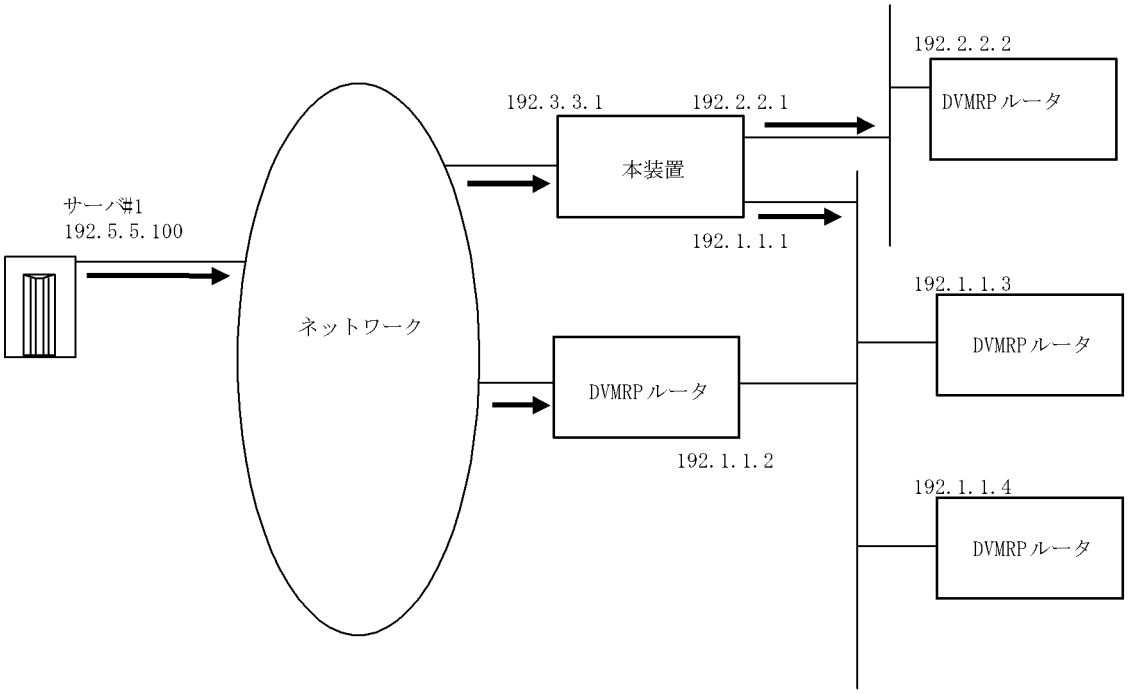



## (3) 送信元ルート情報

show ip dvmrp route を実行し，送信元のルート情報を確認してください。

**図 5-50 show ip dvmrp route コマンドの実行結果**

```
> show ip dvmrp route 192.5.5.100
RPF Information for ? (192.5.5.100):Iif multi1 (192.3.3.1)
DownstreamIface     Forwarder           Depnbrs
192.1.1.1           192.1.1.1           2
                                        DepNbr     192.1.1.3
                                        DepNbr     192.1.1.4
192.2.2.1           192.2.2.1           1
                                        DepNbr     192.2.2.2

>
```




：マルチキャストデータパケット

## 5.4.4 IGMP 情報を確認する

本装置の IPv4 マルチキャストルーティング情報で IGMP 機能を設定した場合の確認内容には次のものがあります。

### (1) インタフェース情報

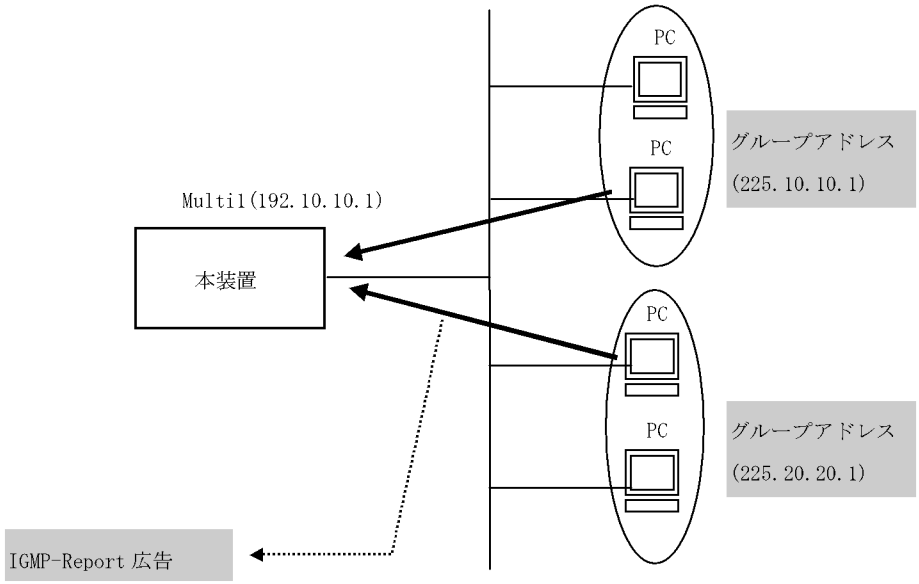
show ip igmp interface を実行し，次のことを確認してください。

- Address 内のインタフェースを確認してください。存在しない場合，そのインタフェースで IGMP は動作していません。PIM が動作している場合，構成定義情報の当該インタフェースで PIM が enable，DVMRP が動作している場合，構成定義情報の当該インタフェースで IGMP が enable かつ DVMRP が enable になっているか確認してください。また，そのインタフェースに障害が発生していないか確認してください。

● 該当インタフェースの Group Count（加入グループ数）を確認してください。0 の場合は加入グループが存在しないかグループ加入ホスト（PC）が IGMP-Report を広告していない可能性があります。ホストを調査してください。

**図 5-51　show ip igmp interface コマンドの実行結果**

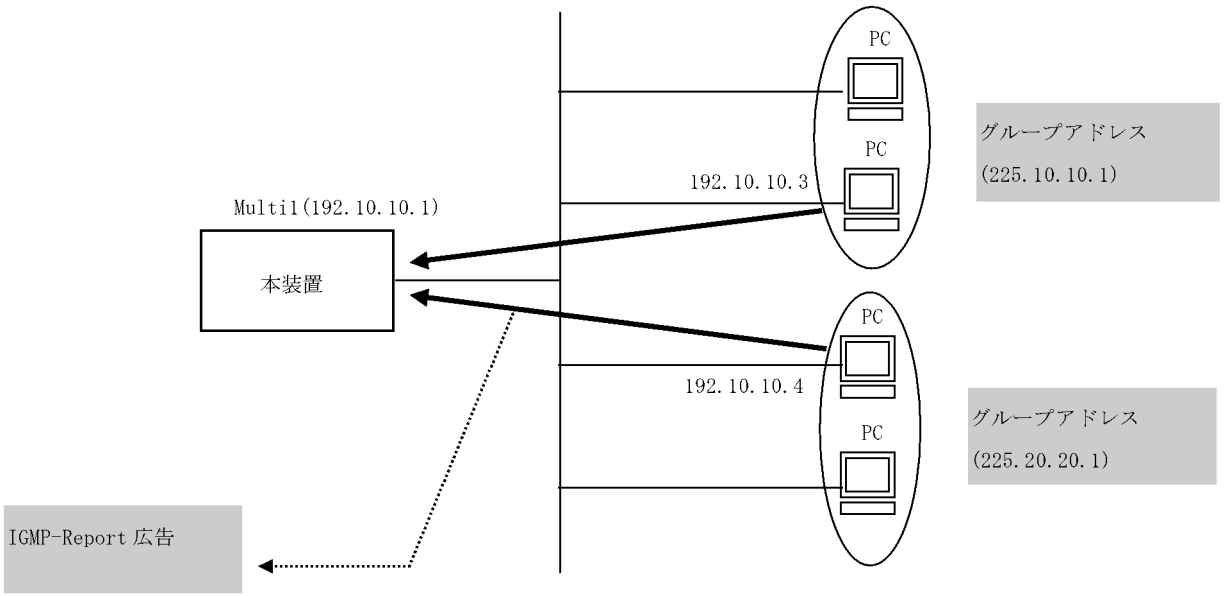
```
> show ip igmp interface
Address             Interface           Querier             Group Count
192.10.10.1         Multi1              192.10.10.1                   2


>
```




## (2) グループ情報

show ip igmp groups を実行し，Group Address 内のグループを確認してください。存在しない場合，そのグループメンバ（ホスト）が IGMP-Report を広告していない可能性があります。ホスト（PC）を調査してください。

**図 5-52　show ip igmp groups コマンドの実行結果**



# 5.5 IPv6 ネットワーク状態の確認

本節では，構成定義コマンド ip で IPv6 アドレスを指定しているインタフェースの確認について説明します。

## 5.5.1 インタフェースの up/down を確認する

IPv6 ネットワークに接続する本装置の回線や回線内のポートに IPv6 アドレスを設定したあとに，show ipv6 interface コマンドを実行し，IPv6 インタフェースの up/down 状態が ” UP ” であることを確認してください。

**図 5-53 「IPv6 インタフェース状態」の表示例**

```
> show ipv6 interface summary
tokyo: UP  3ffe::1:1/64
nagoya: UP  3ffe:1::1/64
osaka: DOWN  3ffe:2::1/64
fukuoka: UP  3ffe:3::1/64
sapporo: DOWN  3ffe:4::1/64
>
```

インタフェースが DOWN 状態の場合は，「7.8.1　通信ができない，または切断されている」を参照してください。

## 5.5.2 当該宛先アドレスとの通信可否を確認する

IPv6 ネットワークに接続している本装置のインタフェースについて，通信相手となる装置に対して通信できるかどうかを，ping ipv6 コマンドを実行して確認してください。

**図 5-54　ping ipv6 コマンドの実行結果（通信可の場合）**

```
> ping ipv6 3ffe:501:811:ff01::1
PING6 (56=40+8+8 Bytes) 3ffe:501:811:ff01::10 -->3ffe:501:811:ff01::1
16 bytes from 3ffe:501:811:ff01::1, icmp_seq=0 ttl=255 time=0.286 ms
16 bytes from 3ffe:501:811:ff01::1, icmp_seq=1 ttl=255 time=0.271 ms
16 bytes from 3ffe:501:811:ff01::1, icmp_seq=2 ttl=255 time=0.266 ms
^C
--- 3ffe:501:811:ff01::1 ping6 statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.266/0.274/0.286 ms
>
```

**図 5-55　ping ipv6 コマンドの実行結果（通信不可（経路あり）の場合）**

```
> ping ipv6 3ffe:501:811:ff01::1
PING6 (56=40+8+8 bytes) 3ffe:501:811:ff01::10 --> 3ffe:501:811:ff01::1
^C
--- 3ffe:501:811:ff01::1 ping6 statistics ---
12 packets transmitted, 0 packets received, 100% packet loss
>
```

**図 5-56　ping ipv6 コマンドの実行結果（通信不可（経路なし）の場合）**

```
> ping ipv6 3ffe:501:811:ff01::1
PING6 (56=40+8+8 bytes) 3ffe:501:811:ff01::10 --> 3ffe:501:811:ff01::1
ping6: UDP connect: No route to host
>
```

## 5.5.3 当該宛先アドレスまでの経路を確認する

traceroute ipv6 コマンドを実行して，IPv6 ネットワークに接続している本装置のインタフェースから通信相手となる装置までの中継装置を確認してください。

**図 5-57 traceroute ipv6 コマンドの実行結果**

```
> traceroute ipv6 3ffe:501:811:ff01::1 numeric
traceroute6 to 3ffe:501:811:ff01::1 (3ffe:501:811:ff01::1), 30 hops max, 40 byte
packets
1  3ffe:501:811:ff03::10  0.612 ms  0.541 ms  0.532 ms
2  3ffe:501:811:ff02::5  0.905 ms  0.816 ms  0.807 ms
3  3ffe:501:811:ff01::1  1.325 ms  1.236 ms  1.227 ms
>
```

## 5.5.4 隣接装置との NDP 解決情報を確認する

IPv6 ネットワークに接続する本装置の回線や回線内のポートに IPv6 アドレスを設定したあとに，show ipv6 neighbors コマンドを実行し，本装置と隣接装置間のアドレス解決をしているか（NDP エントリ情報があるか）どうかを確認してください。アドレス解決をしていない場合は，「7.8.1 通信ができない，または切断されている」を参照してください。

## 5.5.5 フィルタリング機能を確認する

本装置でフィルタリング機能を使用した場合の確認内容には次のものがあります。

### (1) 運用中の確認

#### (a) 統計情報の確認

show filter-flow コマンドを実行して IP フロー統計情報を表示し，廃棄されているパケット数を確認してください。廃棄パケット数が多い場合，本来はパケット廃棄をしてはいけない通信かもしれません。現在のネットワークの運用状況を確認してください。

**図 5-58 フィルタリングによるパケット廃棄数表示**

```
> show filter-flow interface tokyo1 detail
<Filter IPv6 List No.>: 40010
      Using Interface:tokyo1/in
      protocol:6
      ip destination:3ffe:501:811:ff00::0 - 3ffe:501:811:fffe::ffff
      port source:80
      forward packets                                          :   7469982
<Filter IPv6 List No.>: 41000
      Using Interface:tokyo1/in
      drop packets                                             : 327032706
 (以下省略)
>
```

## 5.5.6 Null インタフェースを確認する

本装置で Null インタフェースの機能を使用した場合の確認内容には次のものがあります。

### (1) 構成定義設定後の確認

#### (a) 経路情報の確認

show ipv6 route コマンドを実行し，構成定義コマンド static で定義した経路情報の設定内容が正しく反映されているかどうかを確認してください。

**図 5-59 NULL インタフェース経路情報表示**

```
> show ipv6 route static
Total: 1 routes
Destination                                 Next Hop
      Interface      Metric   Protocol  Age
3ffe:501:811:ffcc::/64                     *----
      null           0/0      Static    16s
>
```

### (2) 運用中の確認

#### (a) パケット廃棄数の確認

show ipv6 interface コマンドを実行し，Null インタフェースでパケットが廃棄されているかどうかを確認してください。

**図 5-60 Null インタフェースパケット廃棄数表示例**

```
> show ipv6 interface delete-packets null-interface
Interface Name:null
Discard Packets(IPv6) :92(pkts)
>
```

## 5.5.7 ロードバランスで使用する選択パスを確認する

### (1) 構成定義設定後の確認

#### (a) 経路情報の確認

show ipv6 route コマンドを実行し，定義したマルチパス経路の設定内容が正しく反映されているかどうかを確認してください。

**図 5-61 マルチパスの経路情報表示**

```
> show ipv6 route
Total: 4 routes
Destination                                 Next Hop
      Interface      Metric   Protocol  Age
::1/128                                     ::1
      localhost      0/0      Direct    51m 45s
3ffe::/64                                   fe80:11::1
      Office1        0/0      Static    50m 30s
                                            fe80:12::1
      Office2         -        -         -
                                            fe80:13::1
      Office3         -        -         -
                                            fe80:14::1
      Office4         -        -         -
fe80::/64                                   fe80:20::1
      Office5           0/0      Direct    51m 27s
fe80:20::1/128                              ::1
      localhost      0/0      Direct    50m 30s 29s
>
```

#### (b) 当該宛先アドレスとの通信可否を確認する

ロードバランスで使用する本装置のインタフェースについて，通信相手となる装置に対して通信できるかどうかを，ping ipv6 <IPv6 Address> specific-route source <Source Address> コマンドを実行して確認してください。ping ipv6 コマンドの <Source Address> にはロードバランスで使用する本装置の IPv6 アドレスを指定してください。

## 5.5.8 IPv6 DHCP サーバ機能を確認する

本装置で，DHCP サーバ機能を設定した場合の確認内容には次のものがあります。

### (1) 構成定義設定時の確認

#### (a) ネットワーク確認

本装置の DHCP サーバ機能は，IPv6 DHCP クライアント直結の構成のみをサポートします。IPv6 DHCP リレーエージェントを経由する構成はサポートしていません。ネットワークの構成で，そのような構成となっている場合は，直結の構成に変更してください。

#### (b) 設定した配布プレフィックス数の確認

本装置で配布・管理可能なプレフィックス数は 200 です。show ipv6 dhcp server statistics コマンドを実行し，構成定義コマンド dhcp6-server host の prefix で設定した配布プレフィックス数を確認してください。

**図 5-62 設定配布プレフィックス数表示例（100 個設定の場合）**

```
> show ipv6 dhcp server statistics
   < DHCP Server use statistics >
     prefix pools           :100
     automatic bindings     :0
     manual    bindings     :0
(以下省略)
>
```

### (2) 運用中の確認

#### (a) 配布済みプレフィックス数の確認

実際にクライアントへ配布したプレフィックス数については，show ipv6 dhcp statistics コマンドを実行し，下線部の数を加算することで確認してください。

**図 5-63 配布済みプレフィックス数表示例**

```
> show ipv6 dhcp server statistics
   < DHCP Server use statistics >
     prefix pools           :40
     automatic bindings     :50
     manual bindings        :10
(以下省略)
>
```

#### (b) 配布済みプレフィックスの確認

配布したプレフィックスは，show ipv6 dhcp binding コマンドにより確認できます。

**図 5-64 配布済みプレフィックスの表示例**

```
> show ipv6 dhcp binding
<Prefix>             <Lease expiration>  <Type>
3ffe:1234:5678::/48      infinity            Automatic
3ffe:aaaa:1234::/48      03/04/01 11:29:00   Automatic
>
```

**図 5-65 配布済みプレフィックスの表示例 ( 詳細 )**

```
> show ipv6 dhcp binding detail
<Prefix>              <Lease expiration>  <Type>
  <DUID>
3ffe:1234:5678::/48       infinity            Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48       03/04/01 11:29:00   Automatic
  00:01:00:01:aa:bb:cc:dd:ee:66:77:88:99:aa
>
```

#### (c) プレフィックスを配布したクライアントへの経路情報の確認

本装置 DHCP サーバは，構成定義コマンドによって ” dhcp6-server static-route-setting ” を定義することで，プレフィックスを配布したクライアントへの経路をスタティック経路として自動的に設定します。

**図 5-66 クライアントへの経路情報の確認**

```
> show ipv6 route -s
Total: 10routes
Destination             Next Hop      Interface        Metric  Protocol  Age
3ffe:1234:5678::/48     ::1           tokyo            0/0      Static   45m
        <Active Gateway Dhcp>
3ffe:aaaa:1234::/48     ::1           osaka            0/0      Static   23m
        <Active Gateway Dhcp>
:
>
```

プレフィックスを配布したクライアントへ経路情報を自動設定させる場合は，構成定義に ” dhcp6-server static-route-setting ” を設定してください (「構成定義コマンドレファレンス Vol.1　21. IPv6 DHCP サーバ情報」参照 )。なお，本装置 DHCP サーバで自動設定した経路情報は，下記の手順で削除してください。

(1) 運用コマンド clear ipv6 dhcp6 binding によって配布情報を削除する。

(2) 構成定義から対象のプレフィクスの配布定義を削除する。

(3) 構成定義から dhcp6-server static-route-setting を削除する。

(4) クライアントが配布をうけたプレフィクスを開放する。

### (3) 構成定義変更時の対応

本装置 DHCP サーバでは，構成定義を変更した場合に送信するよう定義されている DHCP メッセージタイプ ” Reconfigure ” をサポートしていません。したがって本装置の構成定義を変更し適用するためには，接続されるクライアント装置のクライアント機能のリセット，またはクライアント装置の再起動が明示的に必要となります。ただし，これらを実施しなかった場合でも，初期設定（新たにプレフィックスを要求してくる）を試みます。これにより，構成定義変更内容がクライアントに反映されます。

### (4) DUID(DHCP Unique Identifier) について

本装置 DHCP サーバは，初回導入時に自装置の DUID を自動生成します。DUID は装置で静的に保持しなければならないため，本装置は生成した DUID を MC 内に保存します。

#### (a) DUID 保存場所

本装置 DHCP サーバは，生成した DUID を PrimaryMC 上の ” /primaryMC/usr/var/dhcp6/dhcp6s_duid ” に保存します。

#### (b) DUID 確認方法

本装置 DHCP サーバの自装置の DUID は，運用コマンド show ipv6 dhcp server statistics で確認できます。

**図 5-67 自装置 DUID の確認**

```
> show ipv6 dhcp server statistics
   < Server Duid >
     00:01:00:01:3e:00:2e:5e:11:22:33:44:55:66
>
```

### (5) DUID の性質に伴う導入に際しての注意

#### (a) 初期導入時

DHCP では DUID を装置ごとにユニークな値に設定しなければならない点に注意してください。ただし，本装置 DHCP サーバは初期導入時にだけ，インタフェースの MAC アドレスと時刻（時，分，秒）を使用して DUID を自動生成します。そのため本装置間または他社製品間で同一になることはほとんどありません。ただし，同一ネットワークで併用する他装置で DUID を本装置の DUID と同じ値に設定しないでください。

#### (b) copy mc による運用

DUID の保存ファイルは，copy mc によってバックアップ MC へコピーされます。この場合，作成されたバックアップ MC を使って，現在サービス中の本装置と同一ネットワーク上に，別の本装置を IPv6 DHCP サーバとして設置する場合は，DUID 保存ファイルを削除してから実施してください。削除は運用コマンド ”rm ” を使用します。

**図 5-68 DUID 保存ファイルの削除**

```
> rm /primaryMC/usr/var/dhcp6/dhcp6s_duid
>
```

#### (c) 他社製品とのリプレース

本装置 DHCP サーバは他社製品とのリプレースを行うに際して，DUID を他社製品で使用していた値に再設定することはできません。リプレースによるネットワーク構築の際は，必ずクライアント装置を再起動，またはクライアント機能を再起動してください。

### (6) 本装置を同時に 2 台以上使用する場合の注意

本装置を 2 台以上使用する場合，それぞれに同じプレフィクスの配布設定をすると，配布先のインタフェースに接続した，2 台以上の異なるクライアントに対して，装置ごとに同じプレフィクスを配布することがあります。これは構成定義において，dhcp6-server interface に対し，preference パラメタに優先度を設定することで，回避可能です。ただし，構成定義コマンドで dhcp6-server option rapid-commit を定義した場合，またはクライアントの実装が以下のどれかに該当する場合は，本値を無視することがあります。

1. クライアントによる最初の SOLICIT メッセージ送信後のサーバ応答メッセージ監視時間が，本装置がクライアントを探すために実施する NDP の応答時間よりも短く設定されている。
2. preference を無視する実装である。

現象の発生を確認した場合や，上記条件に一致する場合は，2 台以上の装置を同時に運用する構成を止めるか，または，それぞれに異なるプレフィクスの配布設定をしてください。

## 5.5.9 VRRP の同期を確認する

本装置で VRRP の機能を使用した場合の確認内容には次のものがあります。

### (1) 構成定義設定後の確認

#### (a) 経路情報の確認

show vrrpstatus detail コマンドを実行し，構成定義コマンド virtual-router で定義した VRRP 情報の設定内容が正しく反映されているかどうかを確認してください。

**図 5-69 VRRP 運用状態表示**

```
> show vrrpstatus detail
Department1: VRID 1
   Virtual Router IP Address : fe80::1234
   Virtual MAC Address : 00-00-5e-00-01-01
   Current State : MASTER
   Admin State : enable
   Priority : 100
   IP Address Count : 1
   Master Router's IP Address : fe80::abcd
   Primary IP Address : fe80::abcd
   Authentication Type : SIMPLE TEXT PASSWORD
   Authentication Key : ABCDEFG
   Advertisement Interval : 1
   Preempt Mode : ON
   Virtual Router Up Time : Tue Feb 22 13:05:53 2000
   Critical Interface : Department2
   Critical Interface Status : (IF UP)
>
```

### (2) 運用中の確認

#### (a) 仮想ルータ状態の確認

本装置および本装置と同一仮想ルータを構成する相手装置において，仮想ルータの状態が MASTER または BACKUP になっていること，および同一仮想ルータで複数のマスタルータが存在しないことを確認してください。本装置における仮想ルータの状態確認には show vrrpstatus コマンドを使用してください。

**図 5-70 仮想ルータの状態表示例**

```
> show vrrpstatus
Department1:VRID 1 MASTER virtual-ip fe80::1234 priority 150
>
```

## 5.5.10 トンネルインタフェース情報を確認する

本装置でトンネルインタフェースを使用した場合の確認内容には次のものがあります。

### (1) 動作状態の確認

show ipv6 interface コマンドを実行し，次の観点でトンネルインタフェースの状態を確認してください。

- 表示結果の physical address で示すアドレスが，本装置のトンネルインタフェース以外のインタフェースに設定されているアドレスであることを確認してください。アドレスが間違っている場合には，正しいアドレスに変更してください。
- 表示結果の physical address で示すアドレスが設定されているインタフェースの状態が UP していることを確認してください。

**図 5-71 トンネルインタフェース状態表示**

```
> show ipv6 interface TokyoOsakaT
TokyoOsakaT: flags=80b1<UP,POINTtoPOINT,NOTRAILERS,NOARP,MULTICAST>
        mtu 1280
        inet6 3ffe:1234:5678:9abc::64 --> fec0:1234:5678:9abc::64
        physical address inet 192.168.100.1/24 --> 192.168.100.2
>
```

### (2) 通信の確認

トンネル情報で設定した自アドレス・宛先アドレスに対して，本装置および接続先装置から ping，ping ipv6 コマンドを実行し，到達性を確認してください。もし，到達性がない場合は次の対応を行ってください。

● どちらの装置からも到達性がない場合
経路情報に問題があると考えられます。「7.8.1 通信ができない，または切断されている」を参照してください。

● 一方の装置から到達性がない場合
中継経路間にアドレス変換装置がないかネットワーク構成を確認してください。アドレス変換装置を使用している場合は禁止構成に該当しますので，トンネルを設定する中継経路間にアドレス変換装置を設置しないようにネットワーク構成を変更してください（禁止構成については「解説書 Vol.1 14.11.4 トンネル機能使用時の注意事項」を参照してください）。

### (3) 到達経路の確認

トンネルインタフェースに設定した接続先アドレスの到達経路を，show netstat routing-table numeric，show ipv6 interface，および show ip interface を実行して確認してください。経路の中継先が，本装置の別のトンネルインタフェースであった場合，禁止構成である多重トンネルとなっていることが考えられます。経路制御の設定を変更して，トンネルインタフェース以外が中継先となるように変更してください。

**図 5-72 トンネルインタフェース状態表示**

```
> show ipv6 interface TokyoOsakaT
TokyoOsakaT: flags=80b1<UP,POINTtoPOINT,NOTRAILERS,NOARP,MULTICAST>
        mtu 1280
        inet6 3ffe:1234:5678:9abc::64 --> fec0:1234:5678:9abc::64
        physical address inet 192.168.100.1/24 --> 192.168.100.2
> show netstat routing-table numeric
Routing tables
Internet:
Destination        Gateway          Flags    Refs    Use  Interface
 (途中省略)
192.168.100/24     link#3           UC/DMA      0      0  TokyoNagoyaT
 (途中省略)
> show ip interface TokyoNagoyaT
TokyoOsakaT: flags=80b1<UP,POINTtoPOINT,NOTRAILERS,NOARP,MULTICAST>
        mtu 1280
        inet 192.168.100.1 --> 192.168.100.2
        physical address inet6 fe80::1/64 --> fe80::2
>
```

## 5.5.11 NAT-PT 機能を確認する

### (1) 運用中の確認

#### (a) 統計情報の確認

show ipv6 natpt statistics コマンドを実行すると，NAT-PT に関する統計情報が表示されます。NAT-PT

による変換が成功している場合には，変換パケット数が増加します。NAT-PT による変換が失敗している場合には，変換しなかったパケット数や廃棄したパケット数が増加，またはどのカウンタも増加しません。変換に失敗している場合には NAT-PT の設定か，パケットに問題があると考えられます。問題の切り分けについては「7.8.5　NAT-PT 通信ができない」を参照してください。

**図 5-73　NAT-PT 統計情報表示**

```
> show ipv6 natpt statistics
                                          6->4         4->6        Total
  NAT-PT packet counter:                   440          279          719
    Translated packet:                     432          274          706
    Not translated packet:                   0            1            3
    Discarded packet:                        8            4           12
>
```

また，NAT-PT 機能使用時に show dns-relay コマンドを実行すると，DNS-ALG による DNS クエリーや DNS レスポンスの変換に関する統計情報が表示されます。本装置の DNS-ALG を使用した名前解決が成功している場合には変換回数が増加します。

**図 5-74　DNS-ALG 統計情報表示**

```
> show dns-relay
(途中省略)
DNS-ALG Statistics:
  AAAA -> A           : 10
  A    -> AAAA        : 10
>
```

### (b) バインディングエントリの確認

show ipv6 natpt translation コマンドを実行すると，バインディングエントリが表示されます。バインディングエントリより，通信を行っている端末間のアドレス，ポート番号，レイヤ４プロトコル，また TCP の場合 TCP ステータスを確認することができます。通信ができない場合には，バインディングエントリを表示して，通信を行おうとしている端末間のバインディングエントリが作成されているかどうかを確認してください。

**図 5-75　バインディングエントリ表示**

```
>show ipv6 natpt translation 2000::1
 Total Entry: 6/1000
 No.   IPv6 Address                                    IPv4 Address
 1     2000::1 1000                                ---> 10.20.30.40 80
> show ipv6 natpt translation 2000::1 detail
 Total Entry: 6/1000
 No.   Protocol           Timeout   Expire
       IPv6 Address                                    IPv4 Address
       Translation Address              6->4 Packets      4->6 Packets
 1     TCP ESTABLISHED  00:10:00  00:08:42
       2000::1 1000                                ---> 10.20.30.40 80
       10.20.30.100 1                              149               836
>
```

### (c) ログの確認

show ipv6 natpt log コマンドを実行すると，変換失敗や，バインディングエントリの変更履歴などのログが表示されます。統計情報や，バインディングエントリを確認した結果，正常に変換できていないと思われるときには，ログから詳細な情報を得ることができます。

**図** 5-76 **ログ表示**

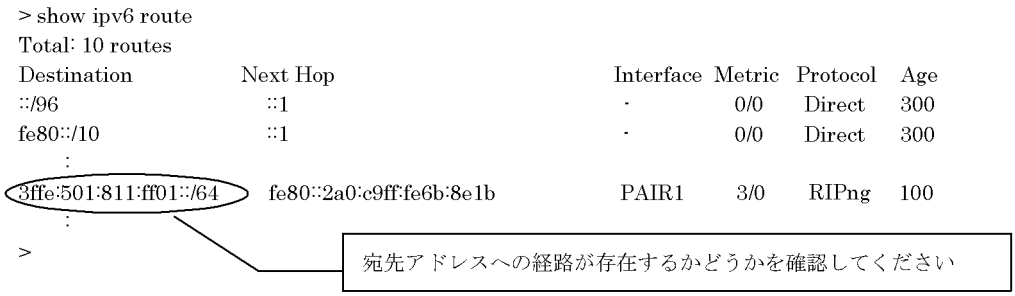
```
> show ipv6 natpt log
Date   Time      Log       Detail                        Protocol
       IPv6 Address                                      IPv4 Address
05/31  13:30:35  Add       -                             TCP CLOSED
       2000::1 1000                                ---> 10.20.30.40 80
>
```

# 5.6 IPv6 ユニキャストルーティング情報の確認

## 5.6.1 宛先アドレスへの経路を確認する

本装置で IPv6 ユニキャストルーティング情報を設定した場合は，show ipv6 route コマンドを実行して宛先アドレスへの経路が存在していることを確認してください。存在しない場合は，「5.6.2 RIPng のゲートウェイ情報を確認する」～「5.6.6 IPv6 アドレス情報が正しく配布されているかを確認する」について確認してください。

**図 5-77 show ipv6 route コマンドの実行結果**




## 5.6.2 RIPng のゲートウェイ情報を確認する

本装置の IPv6 ユニキャストルーティング情報で RIPng 機能を設定した場合は，show ipv6 rip gateway を実行して，次のことを確認してください。

- Gateway Address 内に当該経路を広告すべき隣接ルータが存在するか確認してください。存在しない場合，隣接ルータから RIPng パケットを受信していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- Age が 30 秒以内になっていることを確認してください。30 秒以上になっている場合，隣接ルータから周期的に RIPng パケットが到達していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- Flags に Format が表示されていないか確認してください。Format が表示されている場合，隣接ルータから不正な RIPng パケットを受信しています。隣接ルータを調査してください。
- Flags に Reject 表示がされていないか確認してください。Reject 表示がされている場合，当該ルータからの RIPng パケットの受信が拒否状態となっています。構成定義情報の ripng コマンド（interface 指定）で当該インタフェースに ripin オプションを指定してください。
- Flags に ImportRestrict 表示がされていないか確認してください。ImportRestrict 表示がされている場合，インポートフィルタにより当該経路の取込みがフィルタリングされている可能性があります。構成定義情報のインポートフィルタを調査してください。
- その他の場合，隣接ルータが当該経路を広告していない可能性があります。隣接ルータを調査してください。

**図 5-78　show ipv6 rip gateway コマンドの実行結果**

```
> show ipv6 rip gateway
Gateway Address                 Age        Flags
fe80::2a0:c9ff:fe6b:8e1b%eth00   5s        <Accept>
fe80::200:87ff:fed0:e261%Depart  8s        <Accept>
fe80::260:8ff:fe8e:3090%TestPC  12s        <Accept>
     :
>
```

## 5.6.3　OSPFv3 のインタフェース情報を確認する

本装置の IPv6 ユニキャストルーティング情報で OSPFv3 機能を設定した場合は，show ipv6 ospf interface <Interface Name> または show ipv6 ospf interface detail を実行して，次のことを確認してください。

- Neighbor List 内に当該経路を広告すべき隣接ルータが存在するか確認してください。存在しない場合，隣接ルータから Hello パケットを受信していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。
- State が Two Ways 状態でないことを確認してください。Two Ways 状態の場合，自装置および隣接ルータの priority が設定されていない可能性があります。自装置および隣接ルータの priority を設定してください。
- State が Full 状態となっていることを確認してください。Full 状態以外の場合，隣接ルータとの隣接関係が確立していません。隣接ルータを調査してください。
- State が Full 状態の場合，隣接ルータが当該経路を広告していない可能性があります。隣接ルータを調査してください（隣接ルータが当該経路情報を広告しているかどうかは，show ipv6 ospf database <LS-Type> コマンドで確認できます）。

**図 5-79　show ipv6 ospf interface コマンドの実行結果**

```
> show ipv6 ospf interface Ether00
Domain: 1
Area: 0.0.0.0
Interface ID: 2, Link Local Address: fe80::1000:00ff:fe00:0001%Office00
    IPv6 Address: 3ffe:501:ffff::1/64
    MTU: 1460, DDinPacket: 70, LSRinPacket: 117, ACKinPacket:70
    Router ID: 172.16.1.1, Network Type: Broadcast, State: Backup DR
    DR: 172.17.1.1, Backup DR: 172.16.1.1
    Priority: 1, Cost: 1, Instance: 0
    Intervals:
        Hello: 10s, Dead Router: 40s, Retransmission: 5s, Delay: 1s

   Neighbor List (1):
    Address                     State        Router ID         Priority
    fe80::1000:00ff:fe00:2002   Full         172.16.10.11         1
    Priority
    fe80::1000:00ff:fe00:2002   Full         172.16.10.11         1
>
```

## 5.6.4　BGP4+ のピアリング情報を確認する

本装置の IPv6 ユニキャストルーティング情報で BGP4+ 機能を設定した場合は，show ipv6 bgp neighbors を実行して，次のことを確認してください。

● BGP Status が Established 状態となっていることを確認してください。Established 状態以外の場合，相手 BGP4+ スピーカとのピアリングが確立していません。相手 BGP4+ スピーカとの通信が可能か ping ipv6 コマンドなどで調査してください。不可能な場合，自装置と相手 BGP4+ スピーカ間のインタフェースまたはルータが障害となっている可能性があります。traceroute コマンドなどで障害部位を特定し，障害部位を調査してください。可能な場合，相手 BGP4+ スピーカを調査してください。

● BGP Status が Established 状態の場合，相手 BGP4+ スピーカが当該経路を広告していない可能性があります。相手 BGP4+ スピーカを調査してください（相手 BGP4+ スピーカが当該経路情報を広告しているかどうかは，show ipv6 bgp コマンドで確認できます）。

**図** 5-80　show ipv6 bgp neighbors **コマンドの実行結果**

```
> show ipv6 bgp neighbors 3ffe:501:ffff:5::2
BGP4+ Peer: 3ffe:501:ffff:5::2, Remote AS: 300, Policy Group: 1
Description: Tokyo-Center IPv6
BGP4+ Status: Established         HoldTime: 90
    Established Transitions: 1      Established Date: 2001/08/21 19:41:01
    BGP4+ Version: 4                Type: External
    Local Address: 3ffe:501:ffff:5::1
    Local AS: 500
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 10:39:30  Last Keep Alive Received: 10:40:01
    BGP4+ Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                   1          7          61         68
    BGP4+ Capability negotiation: <>
      Send   : <IPv6-uni>
      Receive: <>
    Authentication: TCP MD5
>
```

## 5.6.5　IS-IS の隣接情報を確認する

本装置の IPv6 ユニキャストルーティング情報で IS-IS 機能を設定した場合は，show isis adjacency を実行し，次のことを確認してください。

● Adjacencies 内に当該経路を広告すべき隣接ルータが存在するか確認してください。存在しない場合，隣接ルータから Hello パケットを受信していません。隣接ルータまたは隣接ルータと接続されたインタフェースを調査してください。

● State が Up 状態となっていることを確認してください。Up 状態以外の場合，隣接ルータが本装置を認識していません。隣接ルータを調査してください。

● State が Up 状態の場合，隣接ルータが当該経路を広告していない可能性があります。隣接ルータを調査してください（隣接ルータが当該経路情報を広告しているかどうかは，show isis database コマンドで確認できます）。

**図** 5-81　show isis adjacency **コマンドの実行結果**

```
> show isis adjacency detail
Level-1 adjacencies
Interface: Office1, Interface Type: Broadcast
    System ID: 0000.87c0.3655, Type: IS, State: Up
    Speaks: IPv6
    Circuit ID: 0x04, SNPA: 00.00.87.c0.36.55
    Priority : 64, Hold Timer: 9s, Established Time: 2003/07/01 15:30:00
    Interface Address: 192:168:7::2
>
```

## 5.6.6 IPv6 アドレス情報が正しく配布されているかを確認する

本装置から端末へ IPv6 アドレス情報が RA によって配布されているかどうかを確認します。

### (1) 端末へアドレス情報を正しく配布しているか確認する

show ipv6 routers interface を実行して，次のことを確認してください。

- 配布すべきプレフィックスが出力されていることを確認してください。
- インタフェースが存在していることを確認してください。存在しない場合，RA の設定またはインタフェースに配布すべきプレフィックスが設定されていない可能性があります。RA またはインタフェースの IPv6 アドレスの構成定義情報を確認してください。

**図 5-82 show ipv6 routers interface コマンドの実行結果**

```
> show ipv6 routers interface Office01
Office01 Index: 2
Line: 0/1
Change: <>      State: <Up Broadcast>
Refcount: 6     Up-down Transitions: 1
INET6 3ffe:500:811:ff00::1  Metric: 0      MTU: 1460
    Refcount: 2  Preference: 0   Down: 120
    Change: <>   State: <>
    Remote Address:
    Address: 3ffe:500:811:ff00::1
    Subnet Masklen: 64
    Route: 3ffe:500:811:ff00::/64
    Autonomous System: 0
    Routing Protocol Active:
>
```

### (2) 本装置－端末間の疎通を確認する

端末側から本装置へ ping ipv6 コマンドを実行して，到達性のあることを確認してください。もし通信不可（到達経路無）の場合，配布されたプレフィックスが端末に設定されていない可能性がありますので端末を調査してください。

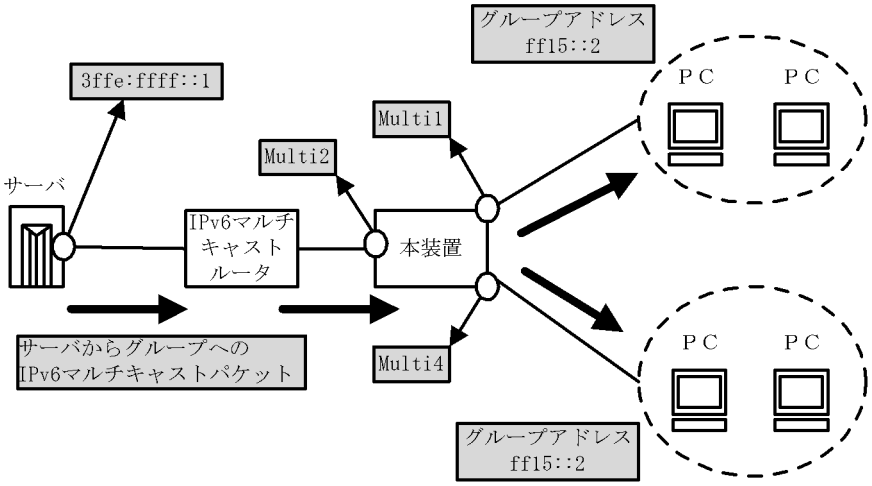
# 5.7 IPv6 マルチキャストルーティング情報の確認

## 5.7.1 宛先グループアドレスへの経路を確認する

本装置で IPv6 マルチキャストルーティング情報の設定を行った場合は，show ipv6 mcache コマンドを実行して宛先アドレスへの経路が存在していることを確認してください。存在しない場合，および downstream が正しくない場合は，「5.7.2 PIM-SM 情報を確認する」と「5.7.3 MLD 情報を確認する」について確認してください。

**図 5-83 show ipv6 mcache コマンドの実行結果**

```
> show ipv6 mcache

Group                                   Source
ff15::2                                 2001:100::1
    upstream:
        Multi2
    downstream:
        Multi1
        Multi4
    Uptime 00:20  Expires 02:40
```




## 5.7.2 PIM-SM 情報を確認する

本装置の IPv6 マルチキャストルーティング情報で，PIM-SM 機能を設定した場合の確認内容には次のものがあります。

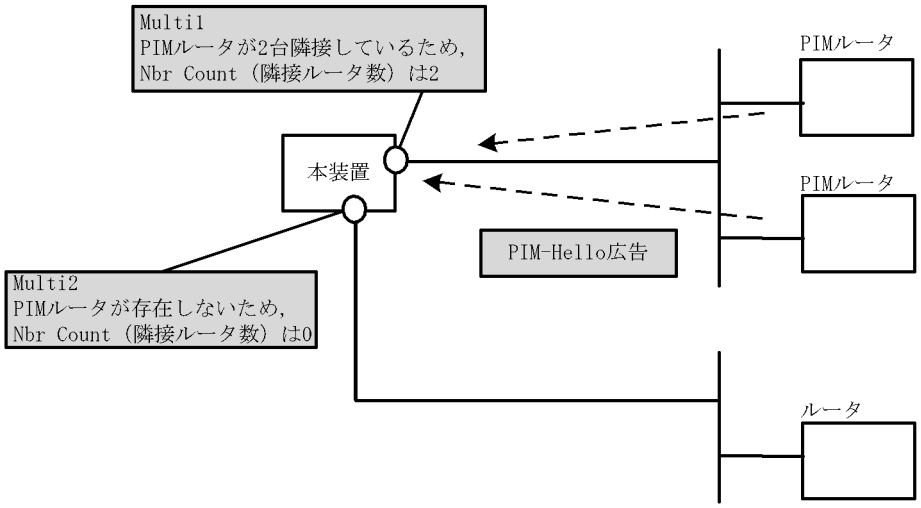
### (1) インタフェース情報

show ipv6 pim interface を実行して，次のことを確認してください。

**図 5-84 show ipv6 pim interface コマンドの実行結果**

```
> show ipv6 pim interface
Interface   Component  Vif   Nbr    Hello   DR                       This
                              Count  Intvl   Address                  Router
Multi1      PIM-SM     1     2      30      fe80::200:87ff:fe10:a95a Y
(以下省略)
>
```

- 当該インタフェース名称が含まれていることを確認してください。当該インタフェース名称が含まれていない場合，そのインタフェースで IPv6 PIM-SM は動作していません。構成定義情報で当該インタフェースで IPv6 PIM が enable になっているか確認してください。また，そのインタフェースに障害が発生していないか確認してください。
- 該当インタフェースの Nbr Count（PIM 隣接ルータ数）を確認してください。0 の場合は隣接ルータが存在しないか，隣接ルータが PIM-Hello を広告していない可能性があります。隣接ルータを調査してください。

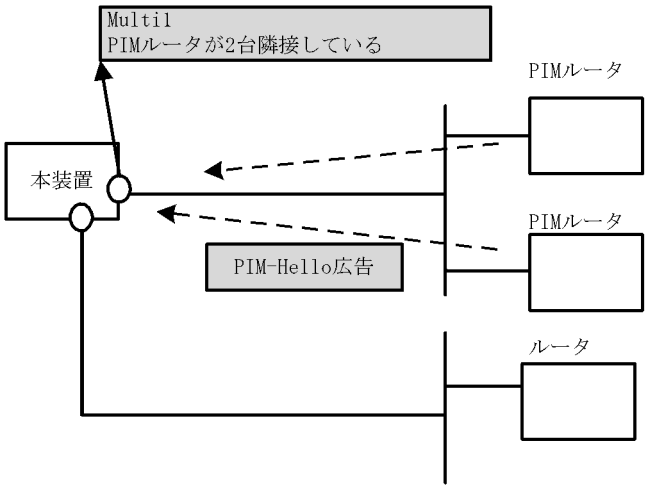



## (2) 隣接情報

show ipv6 pim neighbor を実行して，当該インタフェースに関する隣接相手を確認してください。ある特定の隣接が存在しない場合，隣接ルータが PIM-Hello を広告していない可能性があります。隣接ルータを調査してください。

**図 5-85　show ipv6 pim neighbor コマンドの実行結果**

```
> show ipv6 pim neighbor
NeighborAddress          Interface Uptime Expires
fe80::200:87ff:fea0:abcd Multi1    00:05  01:40
fe80::200:87ff:feb0:1234 Multi1    00:05  01:40
(以下省略)
>
```

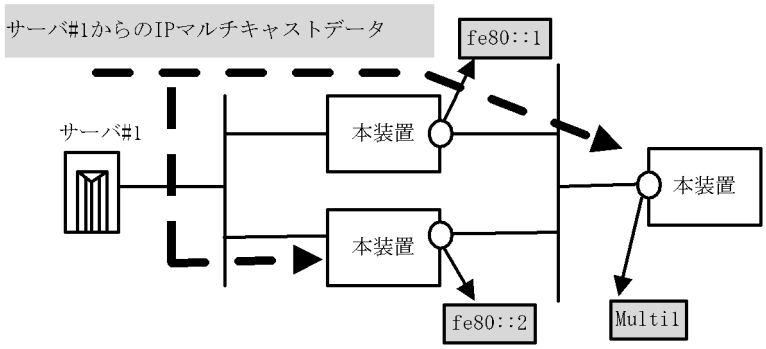


### (3) 送信元ルート情報

show ipv6 rpf コマンドを実行して，送信元のルート情報を確認してください。

**図 5-86 show ipv6 rpf コマンドの実行結果**

```
> show ipv6 rpf
RPF Information for ? (2001:100::1):
If multi1 NextHop fe80::1
(以下省略)
>
```




### (4) PIM-SM BSR 情報

show ipv6 pim bsr を実行して，BSR アドレスが表示されていることを確認してください。”----”表示の場合，BSR が Bootstrap メッセージを広告していないか，BSR が存在していない可能性があります。BSR を調査してください。なお，PIM-SSM では BSR は使用しませんのでご注意ください。

**図 5-87 show ipv6 pim bsr コマンドの実行結果**

```
> show ipv6 pim bsr
Status: Not Candidate Bootstrap Router
BSR Address:2001::1
    Priority:100,Hash Mask length:30
    Uptime:03:00
    Bootstrap Timeout:130 seconds
>
```

### (5) PIM-SM ランデブーポイント情報

show ipv6 pim rendezvous-point mapping を実行して，該当の IPv6 マルチキャストグループアドレスに対する C-RP Address が表示されていることを確認してください。表示のない場合，BSR が Bootstrap メッセージを広告していないか，ランデブーポイントまたは BSR が存在していない可能性があります。ランデブーポイントおよび BSR を調査してください。なお，PIM-SSM ではランデブーポイントは使用しませんのでご注意ください。

**図 5-88 show ipv6 pim rendezvous-point mapping コマンドの実行結果**

```
> show ipv6 pim rendezvous-point mapping brief
Status: Not Candidate Rendezvous Point
Total: 2 routes, 2 group, 1 RPs
Group/masklen                          C-RP Address
ff15:100::/32                          2001::1
ff15:200::/32                          2001::2
>
```

### (6) PIM-SM ルーティング情報

show ipv6 mroute コマンドを実行し，当該宛先アドレスへの経路が存在するかどうかを確認してください。(S,G) エントリが存在しない場合は，(*,G) エントリが存在しているかを確認してください。(*,G) が存在しない場合，および in-coming.downstream が正しくない場合は隣接ルータを調査してください。なお，PIM-SSM では (*,G) は使用しません（存在しません)。

**図 5-89 PIM-SM マルチキャストルート情報の表示**

```
> show ipv6 mroute
Total: 4 routes, 3 groups, 2 RPs
(S,G) 2 routes ------------------------------------------------------
Group Address                              Source Address
ff15:100::50 2001:100::1
    Uptime 02:00  Expires 02:30  Assert 01:00  Flags F  Protocol SM
    in-coming : Multicast01234 upstream: Direct Reg-Sup: 60s
    downstream: Multi2         uptime 02:30 expires 00:40
ff15:200::1 2001:200::10
    Uptime 02:00  Expires 02:30  Assert 01:00  Flags F  Protocol SM
    in-coming : Multi1         upstream: Direct Reg-sup：60s
    downstream: localhost      uptime 02:30 expires--:--

(*,G) 2 routes ------------------------------------------------------
Group Address                              RP Address
ff15:100::50 2001::1
    Uptime 02:00  Expires 02:30  Assert 01:00  Flags R  Protocol SM
    in-coming : Multi1         upstream: This Router
    downstream: Multi2         uptime 02:30 expires 00:40
ff15:200::1 2001::2
    Uptime 02:00  Expires 02:30  Assert 01:00  Flags R  Protocol SM
    in-coming : Multi1         upstream: fe80::1200:87ff:fe10:1234
    downstream: Multi2         uptime 02:30 expires 00:40
    downstream: Multi3         uptime 02:30 expires 00:41
```

## 5.7.3 MLD 情報を確認する

本装置の IPv6 マルチキャストルーティング情報で MLD 機能を設定した場合の確認内容には次のものがあります。

### (1) インタフェース情報

show ipv6 mld interface を実行して，次のことを確認してください。

- Interface 内のインタフェースを確認してください。存在しない場合，そのインタフェースで MLD は動作していません。PIM が動作している場合，構成定義情報の当該インタフェースで PIM が enable になっているか確認してください。また，そのインタフェースに障害が発生していないか確認してください。
- 該当インタフェースの Group Count（加入グループ数）を確認してください。0 の場合は加入グループが存在しないかグループ加入ホスト（PC）が MLD-Report を広告していない可能性があります。ホストを調査してください。

**図** 5-90　show ipv6 mld interface **コマンドの実行結果**

```
> show ipv6 mld interface
Interface     Querier                    Group Count  This Router
Multi1        fe80::1200:87ff:fe10:2959  4            N
Multi3        fe80::1                    2            N
Multi5        fe80::200:87ff:fe10:1959   5            Y
Multicast0123 fe80::1234                 3            N
Multi7        fe80::2592                 6            N
(以下省略)
>
```

## （2）グループ情報

show ipv6 mld group を実行し，Group Address 内のグループを確認してください。存在しない場合，そのグループメンバ（ホスト）が MLD-Report を広告していない可能性があります。ホスト（PC）を調査してください。

**図** 5-91　show ipv6 mld group **コマンドの実行結果**

```
> show ipv6 mld group brief
Group Address               Last Reporter            Interface
ff15:100::50                fe80::3                  Multi1
ff15:100::60                fe80::200:87ff:fe7a:baaa Multi2
ff15:200::1                 fe80::1                  Multi2
ff15:200::2                 fe80::5                  Multi3
```

# 5.8 QoS 機能の確認

## 5.8.1 QoS 制御機能を確認する

本装置で QoS 制御機能を使用した場合，運用中の確認内容には次のものがあります。

### (1) 帯域制御によるパケット廃棄の確認

show qos ip-flow コマンドを実行して IP フロー統計情報を表示し，QoS 機能の帯域制御によって廃棄されているパケット数を確認してください。廃棄パケット数が多い場合，本来はパケット廃棄をしてはいけない通信部位の可能性があります。現在のネットワークの運用状況を確認してください。

**図 5-92 QoS IP フロー統計情報表示**

```
> show qos ip-flow detail
<QoS IP List No.>:    1
      Using Interface:tokyo1/in
      source ip :170.10.11.21 -170.10.11.30
      packets of    1000000bps and under(priority3  discard4) :     7021
      packets of    1000000bps over     (drop)                 :      729
      forward packets                                          :      461
<QoS IP List No.>:    2
      Using Interface:tokyo2/out
      protocol :6  destination port :20 -21
      hit packets                     (priority8  discard4) : 11568793
(以下省略)
>
```

### (2) キュー制御によるパケット廃棄の確認

show qos queueing コマンドを実行して出力優先度キュー情報を表示し，QoS 機能のキュー制御によって廃棄されているパケット数を確認してください。廃棄パケット数が多い場合，本来はパケット廃棄をしてはいけない通信部位の可能性があります。現在のネットワークの運用状況を確認してください。

なお，NEB100-1TC では，show qos queueing コマンドでキューの詳細情報を確認することはできません。NEB100-1TC でキュー毎の情報を確認する場合は，「(3) Tag-VLAN 連携毎の帯域制御によるパケット廃棄の確認」を参照してください。

**図 5-93 出力優先度キュー情報表示**

```
> show qos queueing nif 1 line 3 output
NIF1 Line3: 10BASE-T half TX
Interface name: tokyo1
    Limit Qlen               :  255
    Priority1  Qlen          :   87  Priority2  Qlen         :       112
    Priority3  Qlen          :  215  Priority4  Qlen         :        58
    Priority5  Qlen          :   66  Priority6  Qlen         :        32
    Priority7  Qlen          :  147  Priority8  Qlen         :       178
    Priority1  maximum Qlen  :  148  Priority2  maximum Qlen :       139
    Priority3  maximum Qlen  :  227  Priority4  maximum Qlen :        89
    Priority5  maximum Qlen  :  129  Priority6  maximum Qlen :        78
    Priority7  maximum Qlen  :  194  Priority8  maximum Qlen :       233
    Total out frames                                         :   2784609
    Total out bytes                                          : 178214976
    Total discarded frames due to queue overflow             :      2375
>
```

### （3） Tag-VLAN 連携毎の帯域制御によるパケット廃棄の確認

show vll コマンドを実行して出力優先度キュー情報を表示し，QoS 機能の Tag-VLAN 連携回線毎の帯域制御によって廃棄されているパケット数を確認してください。廃棄パケット数が多い場合，本来はパケットを廃棄してはいけない通信部位の可能性があります。現在のネットワーク運用状態を確認してください。本機能は NEB100-1TC で使用します。

**図 5-94　優先度キュー情報表示**

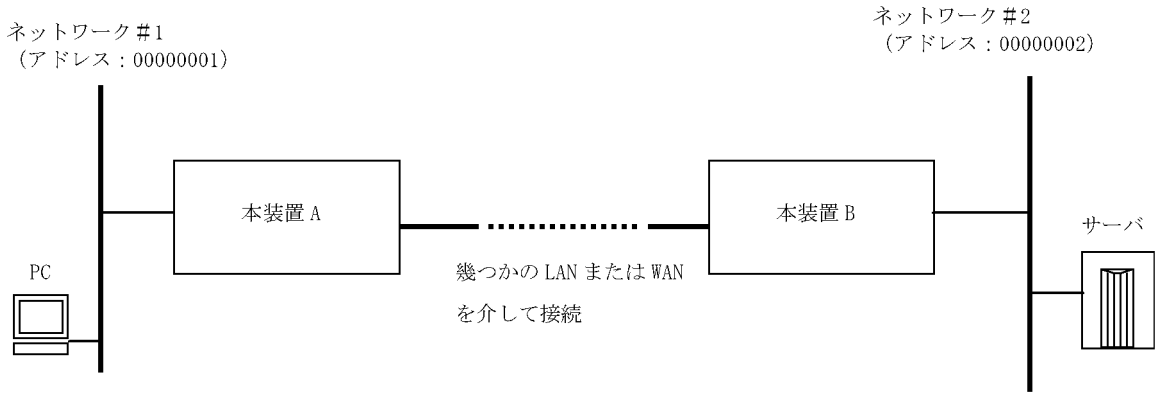
```
> show vll nif 0 line vlan 10
NIF/Line=0/0
 Interface=office-vlan1, Qmode=4WFQ, Peak_rate=2000kbps
  Queue    send_pkt   discard_pkt   send_byte    discard_byte
  1               0             0           0               0
  2            6831       4782607      23314k      685562231k
  3              11             0          3k               0
  4        14530338      33261538   14846684k     7202566486k
  total    14537180      38044145   14870001k     7888152034k
>
```

# 5.9 マルチプロトコル通信の確認

## 5.9.1 IPX 通信機能を確認する

本装置で IPX 通信を使用した場合の確認内容には次のものがあります。

例となる構成を次に示します。




### (1) 構成定義情報の確認

以下の観点で，運用中の構成定義情報を確認してください

● ipx 情報の「プロトコル使用スイッチ」が ” no ” であると，ほかのインタフェース情報が正しく設定されていても ipx ルーティング機能はまったく動作しないので注意してください。

実行例）

```
(config)# show ipx
ipx yes    ← ここが yes になっていること
!
   :
   :
(config)#
```

● ネットワークアドレス，ホストアドレスが重複していないことを確認してください。

実行例 )

```
(config)# show ipx-interface
ipx_interface Department1 ethernet802_3_network_address 00000001
ipx_interface Department1 ethernet2_network_address 22222222
ipx_interface Department1 llc_network_address 33333333
ipx_interface Department1 snap_network_address 44444444  ↑
ipx_interface Department1 watchdog_spoofing proxy        フレームタイプに
ipx_interface Department1 serialization_filtering        合わせてどれか一
ipx_interface Department1 diagnostic_packet_forwarding   つ以上が設定され
ipx_interface Department1 non_periodic_rip_send          ていること。サー
ipx_interface Department1 non_periodic_sap_send          バルータ，クライ
ipx_interface Department1 periodic_rip_interval 1        アントで合わせて
ipx_interface Department1 periodic_sap_interval 1        ください。
ipx_interface Department1 nearest_sap_reply
(config)#
```

### (2) インタフェース情報の確認

show ipx interface コマンドを実行し，インタフェースが up していること，期待しているフレームフォー

マットのインタフェースが設定されていることを確認してください。期待どおりでない場合は構成定義情報を見直して修正してください。

**図 5-95 IPX インタフェース情報表示**

```
> show ipx interface
watchdog spoofing interval : 30        watchdog forwarding interval : 30
#Index Name       NIF/LINE    Type      Status
#000   Department1  01/02     EtherNet   up
#001   TokyoNagoya  02/04     WAN        down
>
```

## (3) ルーティング情報の確認

show ipx route コマンドを実行し，サーバの存在するネットワークがクライアント側のルータ（本装置 A）からルーティング可能であるか確認してください。なお，ルーティング情報はルータ同士の RIP 情報交換でダイナミックに構築させる方法と，WAN 経由で接続する場合など，RIP 情報の周期送信を止めスタティックにルーティングエントリを設定しておく方法とがあります。どちらも相手ネットワークへのルーティング情報が構築されていないと通信ができませんので確認してください。

**図 5-96 IPX ルーティング情報表示**

```
> show ipx route
total: 3 routes
Dest.Net  NextHopNet  NextHopHost        I/F Name       hops/ticks    flags
00000001  00000001    00:00:87:c0:e2:45  Department1      01/00001    static
00000002  00000002    00:00:87:c0:22:45  TokyoNagoya      02/00002    rip
00000003  00000003    00:00:87:c0:e2:47  TokyoNagoya      01/00001    static
>
```

ルーティング情報が構築されていない場合，以下の原因が考えられます。

- インタフェース情報の設定で RIP の送信を off にしている（この場合，相手ルータが RIP 学習できません）。
- 必要な RIP スタティック情報が設定されていない（学習 RIP を使用する場合は不要です）。
- ルータ間で動作の認識が合っていない（片側は RIP 送信し，相手側は RIP 送信しないように定義しているなど）。
- インタフェースに設定したネットワークアドレスがルータ間で不一致になっている。

## (4) 疎通確認

ping ipx コマンドを実行し，本装置 A から本装置 B に対して IPX レベルの経路疎通ができるか確認してください。

**図 5-97 IPX 経路疎通確認（応答あり）**

```
> ping ipx 00000002.00:00:87:e2:68:59 32
Reply from 00000002.00:00:87:e2:68:59  bytes=32 time[ms]=10
>
```

コマンドを実行して応答が帰ればルーティングは正しく設定されています。応答がない場合，またはコマンド実行直後にエラー終了する場合は，ルーティング情報の設定を再度確認してください。ただし，ping は echo パケットを使用していますので，本装置 A ／ B の間に echo パケットを中継できないルータ装置が介入している場合は ping がタイムアウトになります。

## (5) サーバ情報の確認

show ipx servers コマンドを実行し，RIP と同様に SAP 情報（サーバ情報）がクライアント側のルータ

（本装置 A）に登録されているか確認してください。なお，SAP 情報はルータ同士の SAP 情報交換でダイナミックに構築させる方法と，WAN 経由で接続する場合など，SAP 情報の周期送信を止めスタティックにルーティングエントリを設定しておく方法とがあります。どちらにしても目的のサーバの SAP 情報が構築されていないと通信（サーバへのログイン）ができませんので確認してください。

**図 5-98　IPX サーバ情報表示**

```
> show ipx servers
total: 2 servers
NetAddress type Socket Nodeaddress      NextHopNet NextHopHost     hops  Flags
    ServerName           I/F Name
46024316   4    451    00:00:00:00:00:01  00000003 00:00:00:00:00:03 2 sap
    Server1              Department1
46024317   4    451    00:00:00:00:00:01  00000003 00:00:00:00:00:04 3 sap
    ALAXALA-File-Server2 Department6
>
```

SAP 情報が構築されていない場合，次の要因が考えられます。

- インタフェース情報の設定で SAP の送信を off にしている（この場合，相手ルータが SAP 学習できません）。
- 必要な SAP スタティック情報が設定されていない（学習 SAP を使用する場合は不要です）。
- ルータ間で動作の認識が合っていない（片側は SAP 送信し，相手側は SAP 送信しないように定義しているなど）。
- 必要な RIP 情報が設定されていない（該当 SAP に対応してルーティング可能でないと SAP 情報は活性化しません）。
- ネットワーク内に同じサーバ名称のサーバ装置を複数接続している（サーバ名称はサーバ装置ごとに一意な名称を付与してください）。

## 5.9.2　ブリッジ中継を確認する

本装置でブリッジ中継を使用した場合の確認内容には次のものがあります。

### (1) ブリッジインタフェース状態の確認

show bridge interface コマンドを実行し，インタフェース状態が Forwarding（フレーム中継に参加している状態）になっているか確認してください。

**図 5-99　ブリッジインタフェース状態表示**

```
> show bridge interface
Interface Name    Spt-port No.  NifNo./LineNo.   SPT       status
Department1              1         01/01         Enable    Forwarding
Department2              2         01/02         Enable    Disabled
Department3             --         01/03         Disable   Forwarding
TokyoNagoya              3         05/00         Enable    Forwarding
TokyoSendai              4         02/01         Enable    Learning
TokyoOsakaV             --         03/00         Disable   Forwarding
>
```

### (2) フィルタリングデータベースの確認

show bridge fdb コマンドを実行し，フィルタリングデータベースのスタティックエントリが正しいことを確認してください。

**図** 5-100 **フィルタリングデータベース表示**

```
> show bridge fdb
MAC Address        Interface Name   Action    Status(count)     Age
00:00:87:c0:11:92  Department1      forward   learned(    321)   20
00:00:87:c0:11:93  Department2      drop      learned(   4321)   20
00:00:87:c0:11:94  Department3      forward   learned(  54321)   20
00:00:87:c0:11:95  TokyoNagoya      drop      learned( 654321)   20
>
```

# 5.10 SNMP エージェント通信の確認

## 5.10.1 SNMP マネージャとの通信を確認する

本装置に SNMP エージェント機能を設定して SNMP プロトコルによるネットワーク管理を行う場合，次のことを確認してください。

● ネットワーク上の SNMP マネージャから本装置に対して MIB を取得できること

● 本装置からネットワーク上の SNMP マネージャへ SNMP のトラップが送信されていること

確認手順を次に示します。なお，本装置から取得できる MIB については「MIB レファレンス　1. サポート MIB の概要」を，本装置から送信されるトラップについては「MIB レファレンス　4.2 サポートトラップ -UDP 内パラメータ」を，それぞれ参照してください。

1. ping コマンドを SNMP マネージャの IP アドレスを指定して実行し，本装置から SNMP マネージャに対して IP 通信ができることを確認してください。通信ができない場合は「7.5.1　通信ができない，または切断されている」を参照してください。
2. SNMP マネージャから本装置に対して MIB の取得ができることを確認してください。取得できない場合の対応は「7.12　SNMP の通信障害」を参照してください。

# 6 運用中の作業

この章では，装置がネットワーク上で運用されている間に行う作業について説明します。

# 6.1 ログインユーザを追加・削除する

運用中，本装置に対して運用端末を利用するユーザが新規で発生した場合は，adduser コマンドでログインユーザを追加してください。また，利用されてないログインユーザは rmuser コマンドで削除するようにしてください。なお，登録中のログインユーザを確認する場合は，次の図に示す操作でパスワードファイル（/etc/passwd）を参照してください。

**図 6-1 登録済みログインユーザの表示例**

```
> cat /etc/passwd | grep tcsh
operator:*:100:100::/usr/home/operator:/bin/tcsh
user1:*:101:100::/usr/home/user1:/bin/tcsh
user2:*:102:100::/usr/home/user2:/bin/tcsh
>
```

# 6.2 ログインユーザのパスワードを変更する

本装置の運用中，セキュリティ強化のため定期的にログインユーザのパスワードを変更することをお勧めします。特にお勧めする契機を次に示します。

- ネットワーク構成を大幅に変更したとき
- 構成定義コマンド router で本装置にログインできる運用端末 IP アドレスを新たに追加したとき
- 運用ログや運用メッセージで，不正なログインを意味するログメッセージ（「6.3.1　ログインの履歴を確認する」を参照）があったとき

なお，パスワードの変更は password コマンドを使用してください。

# 6.3 運用ログを確認する

## 6.3.1 ログインの履歴を確認する

セキュリティ強化のため，定期的に本装置へのログインの履歴を確認することをお勧めします。

### (1) ログイン認証に成功したユーザを確認する

本装置へのログイン認証に成功していたユーザの履歴は ” show logging | grep Login ” の実行でまとめて表示することができます。次の図に実行例を示します。

**図 6-2 ログイン履歴の表示**

```
> show logging | grep Login
EVT 07/25 12:11:20 E3 RM 00005002 1001:000000000000 Login operator from
172.16.251.69(ttyp3).
EVT 07/25 11:23:56 E3 RM 00005002 1001:000000000000 Login operator from
172.16.251.106 (ttyp2).
EVT 07/25 11:17:10 E3 RM 00005002 1001:000000000000 Login operator from
172.16.251.67(ttyp1).
(以下省略).
>
```

表示結果を元に次の観点で確認してください（ただし，” Login incorrect ” が含まれているログはログイン認証失敗時に採取されるものですので，ここではチェックの対象外です)。

1. 運用端末（IP アドレス）の利用者とログインユーザ名の利用者は一致しているか。もし，一致していない場合は，運用端末の利用者にその経緯を確認してください。

### (2) リモート認証に失敗したユーザを確認する

ログインを許可していないリモート運用端末からのログイン認証に失敗しているユーザの履歴は ” show logging | grep ” Unknown host address ”” の実行でまとめて表示することができます。次の図に実行例を示します。

**図 6-3 ログイン履歴の表示**

```
> show logging | grep "Unknown host address"
EVT 08/19 10:41:52 E3 ACCESS 00000001 0201:000000000000 Unknown host address 172
.16.251.69.
>
```

### (3) ログイン認証に失敗したユーザを確認する

本装置へのログイン認証に失敗しているユーザの履歴は ” show logging | grep ” Login incorrect ”” の実行でまとめて表示することができます。次の図に実行例を示します。

**図 6-4 ログイン履歴の表示**

```
> show logging | grep "Login incorrect"
(途中省略)
EVT 08/01 10:38:40 E3 ACCESS 00000002 0201:000000000000 Login incorrect user2.
(以下省略)
>
```

もし履歴が多い場合，入力ミス以外の要因で採取されているのかもしれません。次のチェックを原因がわかるまで順に行ってください。

1.「パスワードを忘れているのか」をログインユーザ名利用者全員に確認してください。忘れている利用

者が存在する場合は，「7.2.3　ログインパスワードを忘れてしまった」を参照の上，対応してください。

2. ルータ管理者や同じログインユーザ名を使用するほかの利用者のパスワードが変更されていないかを show logging コマンドで確認の上，ログインユーザ名利用者全員にパスワードの認識を徹底させてください。

**図 6-5　パスワード変更履歴の検索**

```
> ll /PrimaryMC/etc/passwd
-rw-r--r--  1 root  wheel  342 Aug  1 10:34 /primaryMC/etc/passwd
> show logging | grep KEY
KEY 08/01 10:35:05 user1:> show logging | grep KEY
(途中省略)
KEY 08/01 10:34:38 user2:> passwd
(以下省略)
>
```

## 6.3.2　障害に関するログがないかを確認する

運用中，障害に関するログが採取されていないことを定期的に確認することをお勧めします。運用中の機能すべてに影響するわけではないため発生時点では見逃される可能性のある（回線障害などのイベントレベルが低い）障害に関するログについては，特に注意してください。障害に関するログは ” show logging | grep EVT ” や ” show logging | grep ERR ” の実行でまとめて表示することができます。

**図 6-6　障害に関するログ表示**

```
> show logging | grep EVT
(途中省略)
EVT 08/03 08:34:51 E4 LINELAN NIF:2 LINE:0 41000101 1350:02ff00000038 Error
detected on the line.
EVT 08/03 08:34:37 E4 LINELAN NIF:2 LINE:0 41000001 1350:03030000003b Line status
is up.
(以下省略)
>
```

障害に関するログの内容については「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。もし，show logging コマンドを実行した時点で障害が回復していない場合や頻繁に起こる障害については，「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」の［対応］や「7　トラブル発生時の対応」を参照の上，即時対応を行ってください。

# 6.4 SNMP トラップ情報を確認する

本装置で SNMP エージェント機能を使用した場合，主に障害などが発生した場合にトラップと呼ばれるイベント通知が SNMP マネージャに送信されます。このトラップ情報によって装置の状態変化を知ることができますので，運用中は定期的に確認してください。なお，本装置固有のトラップ情報には次に示すものがあります。

**表 6-1 本装置特有のトラップ情報**

| 項番 | トラップの種類 | 意味 | 発行契機 |
|---|---|---|---|
| 1 | ax2000rSystemMsgTrap | システムメッセージ出力 | システムメッセージを出力したとき。 |
| 2 | ax2000rStandbySystemUpTrap | 予備系 RM 正常再起動 | RM 二重化装置で，Cold Start 以降に予備系 RM が正常動作中であると判断したとき。 |
| 3 | ax2000rStandbySystemDownTrap | 予備系 RM 異常検出 | RM 二重化装置で，Cold Start 以降に予備系 RM が障害であると判断したとき。 |
| 4 | ax2000rTemperatureTrap | 温度状態の遷移 | RM の監視している温度が，正常，注意，警告，異常の各状態に遷移したとき。 |
| 5 | ax2000rAtmPvcTrap | PVC 障害を通知 | ATM インタフェース上の PVC が，新たに一つ以上通信不可状態となったとき。 |

その他のトラップ情報については，「MIB レファレンス　4.2 サポートトラップ -UDP 内パラメータ」を参照してください。

# 6.5 MC 容量を確認する

運用中，MC 上のファイルシステムの使用状況を show mc コマンドを用いて確認することをお勧めします。もし使用量が限りなく 100%に近い場合は，「7.1.4 MC の容量が不足している」を参照の上，対応してください。

**図 6-7 MC 容量の確認**

```
> show mc
Slot0  : primary Slot , mc-enabled
         AX-F6531-MC64 [BMC64] , AX2000R format , 00070000
         29,034KB used (user Area: 29,034KB , dump Area: 0KB)
         27,926KB free (user Area: 21,824KB , dump Area: 6,102KB)
         56,960KB total(user Area: 50,858KB , dump Area: 6,102KB)
Slot1  : secondary Slot , mc-disabled
>
```

# 6.6 ネットワーク構成を変更する

運用中にネットワークの構成を変更する場合，本装置では「6.6.1 ボードを追加する」～「6.6.4 構成定義情報を入れ替える」の作業を行ってください。

## 6.6.1 ボードを追加する

ネットワーク構成に収容条件がある機能を追加する場合は，RP ／ NIF ボードの入れ替えや追加が必要になる場合があります（収容条件がある機能については「解説書 Vol.1 3.2 収容条件」を参照してください）。RP ／ NIF ボードの入れ替えや追加の操作手順は「8.4 ボード，メモリの取り外し／増設」を参照してください。

## 6.6.2 運用構成定義情報をバックアップする

ネットワーク構成の変更により運用構成定義の内容を大幅に変更する場合は，変更前と変更後の運用構成定義情報をそれぞれバックアップすることをお勧めします。操作方法については「構成定義ガイド 4.1 構成定義情報のバックアップ」を参照してください。

## 6.6.3 予備構成定義情報ファイルを作成する

ネットワーク構成の変更により運用構成定義の内容を大幅に変更する場合は，事前に予備構成定義情報ファイルを作成することをお勧めします。操作方法については「構成定義ガイド 3.2 予備構成定義情報ファイルの編集」を参照してください。

## 6.6.4 構成定義情報を入れ替える

構成定義コマンドを用いて，バックアップした構成定義情報ファイルを運用に使用したり，新しいネットワーク構成の構成定義情報ファイルを運用に使用したりします。

### (1) 予備構成定義情報ファイルを運用に使用する

copy backup-config コマンドを用いて構成定義情報ファイルの入れ替えを運用系に対して行うと，MC の現用構成定義情報ファイルを書き替えます。書き替え後，変更後の内容で運用を開始します。なおこの時運用中のポートを再起動するため，ネットワーク経由でログインしている場合は通信が切断されますのでご注意ください。

**図 6-8 予備構成定義情報ファイルの使用**

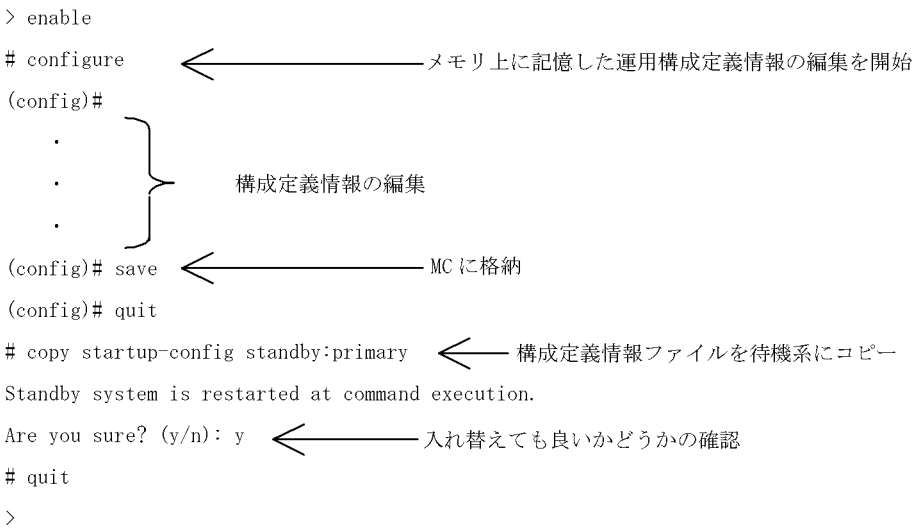
### (2) メモリ上に記憶した運用構成定義情報を待機系の運用に使用する

メモリ上に記憶した運用構成定義情報を変更した場合，変更した内容はすぐに運用に反映されますが，待機系へ構成定義情報を反映させる契機は構成定義情報保存（save）を行った時点で行われます。そのため，運用系および定期系の構成定義情報に不一致が起こっている状態で，運用系に致命的な障害が発生，運用系で swap rm コマンドを実行しますと，運用している構成定義情報から入れ替わるため，系交替後に RP の最起動を行い，一次的に通信ができなくなります。

また，set mode コマンドで二重化固定モード（duplex）を設定している状態で，運用系と待機系の構成定義情報に差分がある場合，運用系での swap rm コマンドの実行による系交替は抑止されます。また，運用系に致命的障害が発生した場合には，系交替を行わずに装置の再起動が発生します。

運用系の系交替による通信段避け，また運用系の系交替を実行可能にするには，運用構成定義情報を変更した後，構成定義コマンド save または copy startup-config コマンドを実行し，運用系と待機系の構成定義情報ファイルを一致させてください。

**図 6-9　待機系へのコピー**



# 6.7 ソフトウェア／構成定義情報を MC にバックアップする

運用中，構成定義情報の変更やソフトウェアのアップデートを行った場合には，その情報をバックアップ MC にコピーすることをお勧めします。次の表に，バックアップ MC にコピーするコマンドと情報を示します。

**表 6-2 バックアップ MC にコピーするコマンドと情報**

| 項番 | コマンド名 | バックアップ MC にコピーする情報 | 実行契機 |
|---|---|---|---|
| 1 | copy mc | 全情報 | 運用中の MC に対してソフトウェアのアップデートを行った場合 |
| 2 | synchronize | 次に示す情報<br>• ログインユーザ情報（ホームディレクトリ配下のファイル，パスワードファイル）<br>• 冗長構成設定情報（電源機構，基本制御機構）<br>• 運用構成定義情報 | 運用中の MC に対して次の操作を行った場合<br>• ログインユーザの追加・削除<br>• ログインユーザやルータ管理者のパスワード変更<br>• 冗長構成設定変更<br>• 運用構成定義情報変更 |
| 3 | 運用コマンド<br>copy startup-config<br>copy backup-config | 現用または予備の構成定義ファイル | 運用中の MC に左記のファイルが新規で作成されたとき |

# 7 トラブル発生時の対応

本章では装置が正常に動作しない，または通信ができないといったトラブルが発生した場合の対処方法を説明します。

# 7.1 装置または装置の一部の障害

## 7.1.1 FAULT CODE が表示された

運用中，FAULT CODE が表示されたままの場合，発生した障害が回復していない状態です。この場合，以下の順で対応してください。

1.「メッセージ・ログレファレンス　1.2 FAULT CODE の確認」を参照して障害部位を特定させてください。
2. show logging コマンドを実行して，特定した障害部位に関するログの内容を確認してください。
3.「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 2. で検知したログの内容を確認し，［対応］欄に明記されている対応を行ってください。

## 7.1.2 STATUS ランプが緑点灯以外の状態である

運用中，基本制御機構（BCU）の STATUS ランプが緑点灯以外の状態である場合，本装置は動作可能状態ではありません。次の表に示すとおり，STATUS ランプの状態別に対応をしてください。

**表 7-1　STATUS ランプの状態と対応**

| STATUS ランプの状態 | 対応 |
|---|---|
| 緑点滅 | 本装置は起動中です。時間をおいて STATUS ランプが緑点灯になることを確認してください。 |
| 黄色点灯 | 内蔵 RP が一時的に閉塞されている状態です。close rp コマンドで閉塞している場合は，free rp コマンドを実行することで運用が再開されます。また，構成定義情報で閉塞している場合は，disable 情報の削除によって運用が再開されます。 |
| － | 本装置は二重化運用で待機系が一時的に閉塞されている状態です。待機系を運用する場合は，運用系から free standby コマンドを実行してください。 |
| 赤点灯 | 本装置に障害が発生して動作が停止しています。直ちに保守員に連絡してください。 |
| 消灯 | 電源を OFF していないでほかの LED が動作している場合，STATUS ランプの動作が不可の状態です。直ちに保守員に連絡し，その指示にしたがってください。 |

注

AX2000R モデルは，基本制御機構（BCU），ルーティング処理機構（RP）などが一体化されて，装置本体に内蔵されています。

## 7.1.3 MC にアクセスできない

MC へのアクセスにトラブルが発生した場合は，次の表に従い確認をしてください。

| 項番 | 障害内容 | 確認内容 |
|---|---|---|
| 1 | MC への書き込みができない。 | • 書き込みを行う MC が操作対象の MC スロットに正しく挿入されていること。show mc コマンドを実行して操作対象となる MC の実装状態が mc-connect であることを確認してください。<br>• MC の型番が正しいこと。show mc コマンドを実行して操作対象の MC の型名を確認してください。<br>• MC に空き容量があること。show mc コマンドを実行して操作対象の MC に空き容量が十分にあることを確認してください。 |
| 2 | MC のフォーマットができない | • MC が予備側の MC スロットに正しく挿入されていること。show mc コマンドを実行して予備スロットの MC の実装状態が mc-connect であることを確認してください。<br>• MC の型番が正しいこと。show mc コマンドを実行して MC の型名を確認してください。 |

## 7.1.4 MC の容量が不足している

MC 上のファイルシステムの使用率が 100% を超えた場合に，ファイルの削除を実施して空き領域を確保した場合でもファイルシステム使用率 100% の状態が継続し，構成定義のセーブやファイルのコピーなどが実行できない状態となる場合があります。この状態のとき，装置を停止または再起動すると MC 上のファイルシステムが破壊され，MC が復旧できなくなる場合があります。ファイルシステムの使用率が 100% の場合または MC の容量不足が原因でコマンドが実行できない場合は，以下の手順を実施してください。

1. 「6.5　MC 容量を確認する」を参照して MC のファイルシステムの空き領域を確認してください。ファイルシステムに空き領域がない場合には，不要なファイルを削除して空き領域を確保してください。
2. ファイルの削除を実施し，空きエリアを確保してもファイルシステムの使用率が 100% の状態となっている場合は，du -s /primaryMC コマンドを実行してください。本コマンドの実行により，ファイルシステム情報が更新され，MC へ書き込みができるようになります。

# 7.2 運用端末のトラブル

## 7.2.1 コンソールからの入力，表示がうまくできない

コンソールとの接続トラブルが発生した場合は，「表 7-2 コンソールとの接続トラブルおよび対応」に従い確認をしてください。

モデムとの接続トラブルが発生した場合には，「表 7-3 モデムとの接続トラブルおよび対応」に従い確認をしてください。また，モデムに付属の取扱説明書を参照してください。

**表 7-2 コンソールとの接続トラブルおよび対応**

| 項番 | 障害内容 | 確認内容 |
|---|---|---|
| 1 | 画面に何も表示されない | 次の手順で確認してください。<br>1. 装置の Status ランプが緑点灯になっているかを確認してください。緑点灯していない場合は，「7.1.2 STATUS ランプが緑点灯以外の状態である」を参照してください。<br>2. ケーブルの接続が正しいか確認してください。<br>3. RS232C クロスケーブルを用いていることを確認してください。<br>4. ポート番号，通信速度，データ長，パリティビット，ストップビット，フロー制御などの通信ソフトウェアの設定が以下のとおりになっているか確認してください。<br>通信速度：9600bps（変更している場合は設定値）<br>データ長：8bit<br>パリティビット：なし<br>ストップビット：1bit<br>フロー制御：なし |
| 2 | キー入力を受け付けない | 次の手順で確認してください。<br>1. XON ／ XOFF によるフロー制御でデータの送受信を中断している可能性があります。データ送受信の中断を解除してください（［Ctrl］＋［Q］をキー入力してください）。それでもキー入力ができない場合は 2. 以降の確認をしてください。<br>2. 通信ソフトウェアの設定が正しいか確認してください。<br>3. ［Ctrl］＋［S］により画面が停止している可能性があります。何かキーを入力してください。 |
| 3 | ログイン時に異常な文字が表示される | 通信ソフトウェアとのネゴシエーションが正しくできていない可能性があります。通信ソフトウェアの通信速度を次の手順で確認してください。<br>1. 構成定義コマンド router にて CONSOLE(RS232C) の通信速度を設定していない場合は，通信ソフトウェアの通信速度が 9600bps に設定されているか確認してください。<br>2. 構成定義コマンド router にて CONSOLE(RS232C) の通信速度を 1200，2400，4800，9600，または 19200bps に設定している場合は，通信ソフトウェアの通信速度が正しく設定されているか確認してください。<br>3. 構成定義コマンド router にて CONSOLE(RS232C) の通信速度を auto に設定している場合は，通信ソフトウェアの通信速度が 1200，2400，4800，9600，または 19200bps に設定されているか確認してください。通信ソフトウェアからブレーク信号を発行しログイン画面が表示されるか確認してください。なお，通信ソフトウェアの通信速度により複数回ブレーク信号を発行しないとログイン画面が表示されない場合があります。ブレーク信号の発行方法については通信ソフトウェアのマニュアルをご参照ください。<br>4. 運用端末を AUX ポートに接続している場合は，通信ソフトウェアの通信速度が 9600bps に設定されているか確認してください。 |
| 4 | ユーザ名入力中に異常な文字が表示された | CONSOLE(RS232C) の通信速度を変更された可能性があります。項番 3 を参照してください。 |

| 項番 | 障害内容 | 確認内容 |
|---|---|---|
| 5 | ログインできない | 次のことを確認してください。<br>• 画面にログインプロンプトが出ていますか？ 出ていなければ，装置を起動中なので，しばらくお待ちください。<br>• ログインできる最大アカウント数を超えていませんか？ （詳細は「4.2.4 同時にログインできるユーザ数を設定する」を参照してください） |
| 6 | ログイン後に通信ソフトウェアの通信速度を変更したら異常な文字が表示され，コマンド入力ができない | ログイン後に通信ソフトウェアの通信速度を変更しても正常な表示はできません。通信ソフトウェアの通信速度を元に戻してください。 |
| 7 | Microsoft Windows 95, Microsoft Windows 98 付属のハイパーターミナルで通信速度を変更したが通信速度が変わらない | Microsoft Windows 95，Microsoft Windows 98 付属ハイパーターミナルでは，接続中に通信速度を変更しても実際の通信速度は変更されません（ステータスバーの表示は変更後の値になります）。ツールバーから切断，接続を行って通信速度を変更してください。 |
| 8 | Microsoft Windows 3.1 付属のターミナルで［Ctrl］＋［C］によるコマンドの中断機能が使用できない | Microsoft Windows 3.1 付属のターミナルでは［Ctrl］＋［C］による中断機能は使用できません。 |
| 9 | Tera Term Pro を使用してログインしたいがログイン時に異常な文字が表示される | 通信ソフトウェアとのネゴシエーションが正しくできていない可能性があります。項番 3 を参照してください。［Alt］＋［B］でブレーク信号を発行します。なお Tera Term Pro の通信速度により複数回ブレーク信号を発行しないとログイン画面が表示されない場合があります。 |
| 10 | 項目名と内容がずれて表示される | 1 行で表示可能な文字数を超える情報を表示している可能性があります。通信ソフトウェアの設定で画面サイズを変更し，1 行で表示可能な文字数を多くしてください。 |

**表 7-3 モデムとの接続トラブルおよび対応**

| 項番 | 障害内容 | 確認内容 |
|---|---|---|
| 1 | モデムが自動着信しない | 次のことを確認してください。<br>• ケーブルの接続が正しいこと。<br>• モデムの電源が ON になっていること。<br>• 電話番号が正しいこと。<br>• モデムの設定内容が正しいこと。<br>• 2 台の端末にモデムを接続し，ダイアルすることで回線接続できること。 |
| 2 | ログイン時に異常な文字が表示される | 次の手順で確認してください。<br>1. 構成定義コマンド router にて CONSOLE(RS232C) の通信速度を 1200, 2400，4800，または 19200bps に設定している場合は，9600bps または auto に設定してください。<br>2. 本装置とモデムとのネゴシエーションが正しくできていない可能性があります。構成定義にて CONSOLE(RS232C) の通信速度を auto に設定している場合は，通信ソフトウェアからブレーク信号を発行しログイン画面が表示されるか確認してください。なお，複数回ブレーク信号を発行しないとログイン画面が表示されない場合があります。ブレーク信号の発行方法については通信ソフトウェアのマニュアルを参照してください。<br>3. モデムが V.90, K56flex, x2 またはそれ以降の通信規格に対応している場合は，V.34 通信方式以下で接続するように設定してください。 |
| 3 | 何度ブレーク信号を送信しても表示が正しく行われない | ユーザがコンソールからログインしたままの状態では本装置側の接続速度を変更できません。ユーザのオートログアウトを待つか，運用端末からユーザをログアウトさせてください。 |
| 4 | 回線切断後，再ダイアルしても通話中でつながらない | 回線切断が行われてから数秒間は着信しない場合があります。モデムのマニュアルを参照してください。 |

## 7.2.2 リモート運用端末からログインできない

リモート運用端末との接続トラブルが発生した場合は，「表 7-4　リモート運用端末との接続トラブルおよび対応」に従い確認をしてください。

**表 7-4　リモート運用端末との接続トラブルおよび対応**

| 項番 | 現象 | 対処方法，または参照個所 |
|---|---|---|
| 1 | リモート接続ができない。 | 次の手順で確認してください。<br>1. リモート接続のための経路は確立されていますか？　PC や WS から ping コマンドを使用して経路が確立されているかを確認してください。<br>2. コネクション確立のメッセージ表示後プロンプトが表示されるまで時間がかかる場合は，DNS サーバとの通信ができなくなっている可能性があります（DNS サーバとの通信ができない場合プロンプトが表示されるまで約 5 分かかります。なおこの時間は目安でありネットワークの状態によって変化します）。 |
| 2 | ログインができない。 | 次の手順で確認してください。<br>1. 構成定義コマンド router で許可された IP または IPv6 アドレスを持つ端末を使用していますか？　また，構成定義コマンド router で設定した IP または IPv6 アドレスに restrict を指定していませんか？（詳細は「4.2.5　リモート運用端末からのログインを制限する」を参照してください）<br>2. ログインできる最大アカウント数を超えていませんか？（詳細は「4.2.4　同時にログインできるユーザ数を設定する」を参照してください）<br>3. 構成定義コマンド router で，本装置へのアクセスを禁止しているプロトコルを使用していませんか？（詳細は「4.2.5　リモート運用端末からのログインを制限する」を参照してください） |
| 3 | キー入力を受け付けない。 | 次の手順で確認してください。<br>1. XON ／ XOFF によるフロー制御でデータの送受信を中断している可能性があります。データ送受信の中断を解除してください（［Ctrl］＋［Q］をキー入力してください）。それでもキー入力できない場合は，項番 2 以降の確認をしてください。<br>2. 通信ソフトウェアの設定が正しいか確認してください。<br>3. ［Ctrl］＋［S］により画面が停止している可能性があります。何かキーを入力してください。 |
| 4 | ログインしたままの状態になっているユーザがある。 | 自動ログアウトするのを待つか，再度ログインしてログインしたままの状態になっているユーザを killuser コマンドで削除します。また，構成定義情報を編集中の場合はファイルがオープンしたままの状態になっていますので，再度ログインしてクローズしてください。 |

## 7.2.3 ログインパスワードを忘れてしまった

### (1) ログインユーザのパスワード

運用中，ログインユーザのパスワードを忘れてしまい本装置にログインできない場合は，以下の手順で対応してください。

1. ルータ管理者への通知
   まずはルータ管理者に連絡してください。ただし，（ほかのログインユーザ利用者がいない場合などの理由で）ルータ管理者になれるログインユーザ利用者がいない場合は，デフォルトリスタートをして再度パスワード設定を行ってください（デフォルトリスタートについての詳細は「2.2　装置を起動する」を参照してください）。
2. パスワードの変更
   パスワード変更の連絡を受けたルータ管理者は，パスワードを変更して対象ログインユーザの利用者全員に通知してください（なお，パスワードを変更する場合は password コマンドを，パスワードの削除だけ行う場合は clear password コマンドを実行してください）。

**図 7-1 ルータ管理者によるログインユーザパスワード変更**

```
# password user1
Changing local password for user1.
New password:
New password:
#
```

### (2) ルータ管理者のパスワード

運用中，ルータ管理者の権限を持っているログインユーザ利用者全員が，ルータ管理者のパスワードを忘れてしまいルータ管理者モードになれない場合は，デフォルトリスタートをして再度パスワード設定を行ってください（デフォルトリスタートの操作方法については「2.2 装置を起動する」を参照してください)。

## 7.2.4 RADIUS を利用したログイン認証ができない

RADIUS を利用したログイン認証ができない場合，以下の確認を行ってください。

1. RADIUS サーバへの通信
   ping コマンドで，本装置から RADIUS サーバに対して疎通ができているかを確認してください。疎通ができない場合は，「7.5.1 通信ができない，または切断されている」を参照してください。また，構成定義情報でローカルアドレスを定義している場合は，RADIUS サーバに本装置のローカルアドレスに対する経路が存在するかを確認してください。
2. タイムアウト値およびリトライ回数設定
   構成定義コマンド radius の設定により，本装置が RADIUS サーバとの通信が不能と判断する時間は最大で＜設定したタイムアウト値（秒）＞×＜設定したリトライ回数＞×＜設定した RADIUS サーバ数＞となります。この時間が極端に大きくなると，リモート運用端末の telnet などのアプリケーションがタイムアウトによって終了する可能性があります。この場合，RADIUS 構成定義の設定かリモート運用端末で使用するアプリケーションのタイムアウトの設定を変更してください。また，運用ログに RADIUS 認証が成功したメッセージが出力されているにもかかわらず，telnet や ftp が失敗する場合は，構成定義で指定した複数の RADIUS サーバの中で，稼動中の RADIUS サーバに接続するまでに，リモート運用端末側のアプリケーションがタイムアウトしていることが考えられますので，稼動中の RADIUS サーバを優先するように設定するか，＜タイムアウト値（秒）＞×＜リトライ回数＞の値を小さくしてください。

# 7.3 障害情報検出

## 7.3.1 運用ログの中に障害に関するログが記録されている

運用ログで障害に関するログが記録されている場合,「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」を参照しながらログメッセージの内容を確認してください。

## 7.3.2 ダンプファイルが作成されている

ダンプファイル格納ディレクトリ（/primaryMC/var/dump）に，RM，RP，NIF のどれかのダンプファイルが採取されている場合は，次の作業を行ってください。なお，ダンプファイルの詳細を「表 7-5 ダンプ情報一覧」に示します。

1. ファイル作成時刻を確認します
   ”ls -l ”を実行して，ファイルが作成された時刻を確認してください。

**図 7-2 ダンプファイル作成時刻の確認**

```
> ls -l /primaryMC/var/dump/
total 2536
-rwxr-xr-x  1 root  wheel  2596411 Aug 19 16:04 rmdump
>
```

2. ファイルが作成された要因を調査します
   show logging コマンドを実行して，ファイルが作成された時刻のログメッセージの内容を「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」を参照しながら確認してください。

**図 7-3 ダンプファイル作成時のログメッセージ確認**

```
> show logging
(途中省略)
EVT 08/19 16:04:04 E3 RM 00003004 1000:000000000111 RM restarted due to user
operation.
EVT 08/19 16:03:57 E3 RM 01910202 1001:000000000000 System restarted by user
operation.
(以下省略)
>
```

3. 障害情報を採取します
   ダンプファイルが障害により作成されている場合は，show tech-support コマンド実行して障害情報を採取してください（詳細は「8.1 障害情報の取得」を参照してください）。
4. ファイルを保存します
   障害解析などで必要な場合は，ダンプファイルを保存してください。なお，ダンプファイルをコンソールやリモート運用端末に保存する場合は「8.2 保守情報のファイル転送」を参照してください。また，予備 MC に保存する場合は cp コマンドを実行してください。
5. ファイルを削除します
   障害解析の終了などでダンプファイルが不要になった場合は，erase dumpfile コマンドを実行して削除してください。

**表 7-5 ダンプ情報一覧**

| 保守関連情報 | 内容 | 格納してあるディレクトリ |
|---|---|---|
| RP/NIF の dump コマンドによるダンプ情報 | RP/NIF のダンプ情報です。<br>ファイルは dump rp，dump nif コマンドで格納します。 | dump rp，dump nif コマンドで指定したディレクトリにあります。 |
| NIF 部障害※1 時自動収集によるダンプ情報 | NIF のダンプ情報です。<br>ファイルは NIF 部障害時に自動で収集されます。 | 標準のダンプ情報ファイルは，/var/dump/nif<NIF 番号 >.< 収集番号 > です。( 予備 MC の場合は，/secondaryMC/var/dump/nif<NIF 番号 >.< 収集番号 > です。)<br><NIF 番号 >：NIF スロット番号 (2 桁 )<br>< 収集番号 >：収集番号 (3 桁 ) |
| RP 重度障害※2 時自動収集によるダンプ情報 | RP のダンプ情報です。<br>ファイルは RP 重度障害時に自動で収集されます。 | ダンプ情報ファイルは，/var/dump/rp<RP 番号 >.< 収集番号 > です。( 予備 MC の場合は，/secondaryMC/var/dump/rp<RP 番号 >.< 収集番号 > です。) また，拡張の RP メモリダンプ・ファイルは／ secondary MC ／ var ／ dump ／ rpe1 ＜ RP 番号＞＜収集番号＞です。<br><RP 番号 >：RP スロット番号 (2 桁 )<br>< 収集番号 >：収集番号 (3 桁 ) |
| 致命的障害※3 時自動収集によるダンプ情報 | RM のダンプ情報です。<br>ファイルは致命的障害時に自動で収集されます。 | ダンプ情報ファイルは，/var/dump/rmdump です。( 予備 MC の場合は，/secondaryMC/var/dump/rmdump です。) |

注※ 1　NIF 部障害は種別ログのイベントレベルが E6（詳細は「メッセージ・ログレファレンス　1.4 ログの確認」を参照）を示しています。
注※ 2　RP 重度障害は種別ログのイベントレベルが E8（詳細は「メッセージ・ログレファレンス　1.4 ログの確認」を参照）を示しています。
注※ 3　致命的障害は種別ログのイベントレベルが E9（詳細は「メッセージ・ログレファレンス　1.4 ログの確認」を参照）を示しています。

## 7.3.3 コアファイルが作成されている

コアファイル格納ディレクトリ（/primaryMC/var/core）にコアファイルが作成されている場合は，次の作業を行ってください。

1. ファイル作成時刻を確認します
   ”ls -l ”を実行して，ファイルが作成された時刻を確認してください。

**図 7-4 コアファイル作成時刻の確認**

```
> ls -l /primaryMC/var/core
-rwxrwxrwx  1 root  wheel  1153219 Jun 21 16:35 rtm.core
>
```

2. ファイルが作成された要因を調査する
   show logging コマンドを実行して，ファイルが作成された時刻のログメッセージの内容を「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」を参照しながら確認してください。

**図 7-5 コアファイル作成時のログメッセージ確認**

```
> show logging
(途中省略)
EVT 06/21 16:36:27 R7 RM 05001001 1001:000000000000 rtm restarted.
(以下省略)
>
```

3. 障害情報を採取する
   コアファイルが障害により作成されている場合は，show tech-support コマンドを実行して障害情報を採取してください（詳細は「8.1　障害情報の取得」を参照してください)。

4. ファイルを保存する
   障害解析などで必要な場合は，コアファイルを保存してください。なお，コアファイルをコンソールやリモート運用端末に保存する場合は「8.2　保守情報のファイル転送」を参照してください。また，予備 MC に保存する場合は cp コマンドを実行してください。
5. ファイルを削除する
   障害解析の終了などでコアファイルが不要になった場合は，rm コマンドを実行して削除してください。

# 7.4　ネットワークインタフェースの通信障害

## 7.4.1　イーサネット回線の接続ができない

通信障害の原因がイーサネット回線にあると考えられる場合は，NIF，Line の各状態を以下に従い確認してください。

### (a) NIF の状態確認

show interfaces コマンドにより NIF の状態確認してください。次の表に NIF 状態に対する対応を示します。

**表 7-6　NIF 状態の確認／対応**

| 項番 | NIF 状態 | 原因 | 対応 |
|---|---|---|---|
| 1 | active | 当該 NIF は正常に動作中です。 | 「表 7-7　Line 状態の確認／対応」により Line の状態を確認してください。 |
| 2 | mismatch | 実装している NIF では，当該 NIF 配下に構成定義されている Line を使用することはできません（実装されている NIF と Line の構成定義情報が不一致です）。 | 実装している NIF が間違っていないか，または Line の構成定義情報が間違っていないか確認してください。 |
| 3 | unused | 当該 NIF 配下に Line の構成定義情報が設定されていません。 | 使用する Line の構成定義情報を設定してください。 |
| 4 | closed | close コマンドにより当該 NIF の運用が停止されています。 | 使用する NIF ボードが実装されていることを確認の上，free コマンドにより当該 NIF を運用状態にしてください。 |
| 5 | fault | 当該 NIF が障害となっています。 | show logging コマンドにより表示される当該 Line のログ情報より，「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」の該当個所を参照し，記載されている［対応］にしたがって対応してください。 |
| 6 | initialize | 当該 NIF が障害検出後の再起動中です。 | 同上 |
| 7 | locked | 構成定義情報により当該 NIF の運用が停止されています。 | 使用する NIF ボードが実装されていることを確認の上，構成定義情報を設定して当該 NIF を運用状態にしてください。 |

### (b) Line の状態確認

show interfaces コマンドにより Line 状態を確認してください。次の表に Line 状態に対する対応を示します。

**表 7-7　Line 状態の確認／対応**

| 項番 | Line 状態 | 原因 | 対応 |
|---|---|---|---|
| 1 | active up | 当該 Line は正常に動作中です。※ | なし |
| 2 | active down | 当該 Line に回線障害が発生しています。 | show logging コマンドにより表示される当該 Line のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |

| 項番 | Line 状態 | 原因 | 対応 |
|---|---|---|---|
| 3 | mismatch | 実装している Line では，当該 Line 配下に設定されている Line を使用することはできません（実装 NIF と Line の構成定義情報が不一致です）。 | 実装している Line が正しいか，または Line の構成定義情報が正しいか確認してください。 |
| 4 | unused | 当該 Line 配下に Line の構成定義情報が設定されていません。 | 使用する Line の構成定義情報を設定してください。 |
| 5 | closed | close コマンドにより当該 Line の運用が停止されています。 | 使用する Line にケーブルが接続されていることを確認の上，free コマンドにより当該 Line を運用状態にしてください。 |
| 6 | test | test interfaces コマンドにより，当該 Line は回線テスト中です。 | 通信を再開する場合は，no test interfaces コマンドにより回線テストを停止してください。 |
| 7 | fault | 当該 Line の回線部分のハードウェアが障害となっています。 | show logging コマンドにより表示される当該 Line のログより，「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」の該当個所を参照し，記載されている［対応］にしたがって対応してください。 |
| 8 | initialize | 当該 Line が障害検出後の再起動中です。 | 同上 |
| 9 | locked | 構成定義情報により当該 Line の運用が停止されています。 | 使用する Line にケーブルが接続されていることを確認の上，構成定義情報を設定して当該 Line を運用状態にしてください。 |

注※

接続相手が AX2000R の場合，接続相手が RP，NIF，LINE の CLOSE を行ってもリンクダウンせず，”active up” 状態となる場合があります。

## 7.4.2 WAN 回線の接続ができない

通信障害の原因が WAN 回線にあると考えられる場合は以下に従い確認してください。

### (1) 状態確認

#### (a) NIF の状態確認

show interfaces コマンドにより NIF 状態を確認してください。次の表に NIF 状態に対する対応を示します。

**表 7-8　NIF 状態の確認／対応**

| 項番 | NIF 状態 | 原因 | 対応 |
|---|---|---|---|
| 1 | active | 当該 NIF は正常に動作中です。 | 「表 7-9　Line 状態の確認／対応」により Line の状態を確認してください。 |
| 2 | mismatch | 実装している NIF では，当該 NIF 配下に構成定義されている Line を使用することはできません（実装されている NIF と Line の構成定義情報が不一致です）。 | 実装している NIF が間違っていないか，または Line の構成定義情報が間違っていないか確認してください。 |
| 3 | unused | 当該 NIF 配下に Line の構成定義情報が設定されていません。 | 使用する Line の構成定義情報を設定してください。 |
| 4 | closed | close コマンドにより当該 NIF の運用が停止されています。 | 使用する NIF ボードが実装されていることを確認の上，free コマンドにより当該 NIF を運用状態にしてください。 |

| 項番 | NIF 状態 | 原因 | 対応 |
|---|---|---|---|
| 5 | fault | 当該 NIF が障害となっています。 | show logging コマンドにより表示される当該 Line のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |
| 6 | initialize | 当該 NIF が障害検出後の再起動中です。 | 同上 |
| 7 | locked | 構成定義により当該 NIF の運用が停止されています。 | 使用する NIF ボードが実装されていることを確認の上，構成定義情報を設定して当該 NIF を運用状態にしてください。 |

### (b) Line の状態確認

show interfaces コマンドにより Line 状態を確認してください。次の表に Line 状態に対する対応を示します。

**表 7-9　Line 状態の確認／対応**

| 項番 | Line 状態 | 原因 | 対応 |
|---|---|---|---|
| 1 | active up | 当該 Line は正常に動作中です。 | 当該 Line の Line 種別が Subline を待つ回線※1 の場合は，「表 7-10　Subline 状態の確認／対応」により Subline の状態を確認してください。<br>当該 Line の Line 種別が Timeslot を持つ回線※2 の場合は，「表 7-11　Timeslot 状態の確認／対応」により Timeslot の状態を確認してください。<br>当該 Line の Line 種別が Timeslot を持たない回線の場合は，「表 7-12　PPP 状態の確認／対応」～「表 7-14　DLCI 状態の確認／対応」により当該 Line のリンクレイヤプロトコルの状態を確認してください。 |
| 2 | active down | 当該 Line に回線障害が発生しています。 | show logging コマンドにより表示される当該 Line のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |
| 3 | mismatch | 実装している Line では，当該 Line 配下に構成定義されている Line を使用することはできません（実装されている Line と Line の構成定義情報が不一致です）。 | 実装している Line が正しいか，または Line の構成定義情報が正しいか確認してください。 |
| 4 | unused | 当該 Line 配下に Line の構成定義情報が設定されていません。 | 使用する Line の構成定義情報を設定してください。 |
| 5 | closed | close コマンドにより当該 Line の運用が停止されています。 | 使用する Line にケーブルが実装されていることを確認の上，free コマンドにより当該 Line を運用状態にしてください。 |
| 6 | test | test interfaces コマンドまたは bert コマンドにより，当該 timeslot を含む Line は回線テスト中です。 | 通信を再開する場合は，no test interfaces コマンドまたは no bert コマンドにより回線テストを停止してください。 |
| 7 | looped by remote | 当該 Line と網を経由して接続するピアルータによる remote loopback テスト中です。 | 通信を再開する場合は，ピアルータの remote loopback テストを停止してください。 |

| 項番 | Line 状態 | 原因 | 対応 |
|---|---|---|---|
| 8 | fault | 当該 Line の回線部分のハードウェアが障害となっています。 | show logging コマンドにより表示される当該 Line のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |
| 9 | initialize | 当該 Line が障害検出後の再起動中，または未起動。※3 | 同上 |
| 10 | locked | 構成定義により当該 Line の運用が停止されています。 | 使用する Line にケーブルが接続されていることを確認の上，構成定義情報を設定して当該 Line を運用状態にしてください。 |
| 11 | auto locked | APS 回線のペアの回線で回線テストを実行しているため自動で運用停止しています。 | APS 回線のペアの回線で実行している回線テストを終了することで運用を開始します。 |

注※ 1

BRI(leased line)，PRI(leased line)，T1(leased line)，E1(leased line)，6.3M interface(leased line) を指します。

注※ 2

CE3(leased line)，CT3（leased line）を指します。

注※ 3

serial 回線で，かつインタフェースバックアップを定義している場合，現在使用していないインタフェースは起動しません（バックアップ先回線が ISDN で，かつ自動切戻しの場合を除く）。このとき本状態となります。

### (c) Subline（論理 Line）の状態確認

show interfaces コマンドにより Subline 状態を確認してください。次の表に Subline 状態に対する対応を示します。

**表 7-10　Subline 状態の確認／対応**

| 項番 | Line 状態 | 原因 | 対応 |
|---|---|---|---|
| 1 | active up | 当該 Subline は正常に動作中です。 | 当該 Subline の Line 種別が Timeslot を持つ回線※の場合は，「表 7-11　Timeslot 状態の確認／対応」により Timeslot の状態を確認してください。 |
| 2 | active down | 当該 Subline に回線障害が発生しています。 | show logging コマンドにより表示される当該 Subline のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |
| 3 | mismatch | 実装している Line ／ Subline では，当該 Subline 配下に構成定義されている Subline を使用することはできません。 | 実装している Line ／ Subline が正しいか，または Subline の構成定義情報が正しいか確認してください。 |
| 4 | unused | 当該 Subline 配下に Subline の構成定義情報が設定されていません。 | 使用する SubLine の構成定義情報を設定してください。 |
| 5 | closed | close コマンドにより当該 Subline の運用が停止されています。 | 使用する Line にケーブルが実装されていることを確認の上，free コマンドにより当該 Line，Subline を運用状態にしてください。 |
| 6 | test | test interfaces コマンドまたは bert コマンドにより，当該 timeslot を含む Subline は回線テスト中です。 | 通信を再開する場合は，no test interfaces コマンドまたは no bert コマンドにより回線テストを停止してください。 |

| 項番 | Line 状態 | 原因 | 対応 |
|---|---|---|---|
| 7 | initialize | 当該 Subline が障害検出後の再起動中です。 | 同上 |
| 8 | locked | 構成定義により当該 Subline の運用が停止されています。 | 使用する Line にケーブルが実装されていることを確認の上，構成定義情報を設定して当該 Line，Subline を運用状態にしてください。 |

注※

E1(CE3 leased line)，T1(CT3 leased line) を指します。

### (d) Timeslot の状態確認

show interfaces コマンドにより Timeslot 状態を確認してください。次の表に Timeslot 状態に対する対応を示します。

**表 7-11 Timeslot 状態の確認／対応**

| 項番 | timeslot 状態 | 原因 | 対応 |
|---|---|---|---|
| 1 | active up | 当該 Timeslot は正常に動作中です。 | 「表 7-12 PPP 状態の確認／対応」～「表 7-14 DLCI 状態の確認／対応」により当該 Timeslot のリンクレイヤプロトコルの状態を確認してください。 |
| 2 | active down | 当該 Timeslot に回線障害が発生しています。 | show logging コマンドにより表示される当該 Line のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |
| 3 | unused | 当該 Timeslot 配下に Timeslot の構成定義情報が設定されていません。 | 使用する Line，Subline，Timeslot の構成定義情報を設定してください。 |
| 4 | closed | close コマンドにより当該 Timeslot の運用が停止されています。 | free コマンドにより当該 Timeslot を運用状態にしてください。 |
| 5 | test | test interfaces コマンドまたは bert コマンドにより，当該 Timeslot を含む Line は回線テスト中です。 | 通信を再開する場合は no test interfaces コマンドまたは no bert コマンドにより回線テストを停止してください。 |
| 6 | initialize | 当該 Timeslot が障害検出後の再起動中，または未起動。※ | 同上 |
| 7 | locked | 構成定義により当該 Timeslot の運用が停止されています。 | 使用する Line ケーブルが実装されていることを確認の上，構成定義情報を設定して当該 Line，Subline，Timeslot を運用状態にしてください。 |

注※

BRI（leased line），PRI（leased line），6.3M interface（leased line）にてインタフェースバックアップを定義している場合，現在使用していないインタフェースは起動しません（バックアップ先回線が ISDN で，かつ自動切戻しの場合を除く）。このとき本状態となります。

### (e) リンクレイヤプロトコルの状態確認

該当する Line または Timeslot のリンクレイヤプロトコル状態を以下のとおり確認します。

**● リンクレイヤプロトコルが PPP の場合**

show interfaces コマンドにより PPP の LCP の状態，NCP（IPCP ／ IPv6CP ／ IPXCP ／ BridgeNCP ／ MPLSCP）の状態を確認してください。次の表に LCP の状態，NCP の状態に対する対

応を示します。

**表 7-12 PPP 状態の確認／対応**

| 項番 | PPP の各状態 | 原因 | 対応 |
|---|---|---|---|
| 1 | LCP の状態が up である | 相手局との間で LCP は確立しています。 | 項番 3，4 により NCP（IPCP ／ IPv6CP ／ IPXCP ／ BridgeNCP ／ MPLSCP）の状態を確認してください。 |
| 2 | LCP の状態が down である | 相手局との間で LCP が確立していません。 | show logging コマンドにより表示される当該 Line または Timeslot のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |
| 3 | IPCP ／ IPv6CP ／ IPXCP ／ BridgeNCP ／ MPLSCP の状態が up である | 相手局との間で IPCP ／ IPv6CP ／ IPXCP ／ BridgeNCP ／ MPLSCP は確立しています。 | show logging コマンドにより表示されるのログ情報を確認してください。また，ログ情報が採取されていない場合は，「(2) 統計情報の確認」により統計情報を確認してください。 |
| 4 | IPCP ／ IPv6CP ／ IPXCP ／ BridgeNCP ／ MPLSCP の状態が down である | 相手局との間で IPCP ／ IPv6CP ／ IPXCP ／ BridgeNCP ／ MPLSCP が確立していません。なお，使用するネットワークレイヤプロトコルの NCP だけ確立していればよく，それ以外の NCP 状態は up となる必要はありません。例えば，ネットワークレイヤプロトコルに IP だけ使用し，IPv6CP，IPX，Bridge ／ MPLSCP を使用しない場合は，IPCP だけ up となっていればよく，IPv6CP ／ IPXCP ／ BridgeNCP ／ MPLSCP は up となる必要はありません。 | show logging コマンドにより表示される当該 Line のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |

### ● リンクレイヤプロトコルがフレームリレーの場合

- **PVC 状態確認手順の確認**

  show interfaces コマンドにより PVC 状態確認手順の状態を確認してください。次の表に PVC 状態確認手順の状態に対する対応を示します。

**表 7-13 PVC 状態確認手順状態の確認／対応**

| 項番 | PVC 状態確認手順の状態 | 原因 | 対応 |
|---|---|---|---|
| 1 | up | PVC 状態確認手順は確立しています。 | 「表 7-14 DLCI 状態の確認／対応」により，DLCI の状態を確認してください。 |
| 2 | down | PVC 状態確認手順が確立していません。 | show logging コマンドにより表示される当該 Line または timeslot のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |

- **DLCI 状態の確認**

  show frame-relay コマンドにより DLCI 状態を確認してください。次の表に DLCI 状態に対する対応を示します。

**表 7-14 DLCI 状態の確認／対応**

| 項番 | DLCI 状態 | 原因 | 対応 |
|---|---|---|---|
| 1 | active | 次のことが考えられます。<br>1. 相手装置上で，カプセル化フォーマットの設定が誤っている可能性があります。この場合，show interfaces コマンドの line または timeslot 指定で表示する統計情報 "In unknown protos" をカウントアップします。<br>2. 本装置のフレームリレー構成定義情報の max_packet_size が，相手装置が送信するパケット長未満となっている可能性があります。この場合，show frame-relay コマンドで表示する統計情報 "In over maximum length frames" をカウントアップします。<br>3. 相手装置が，本装置へ接続している DLCI を正常に認識していないか，相手装置の DLCI の設定が誤っている可能性があります。 | それぞれの原因に対して，次にように対応してください。<br>1. 相手装置のカプセル化フォーマットの設定を「IETF(RFC1940 または RFC2427)」に設定してください。<br>2. 本装置のフレームリレー構成定義情報の max_packet_size ≧相手装置が送信するパケット長，となるよう設定してください。<br>3. 相手装置の設定が誤っていないか確認してください。本装置を対向で接続している場合は，ping frame-relay により PVC(DLCI) の接続を確認してください。 |
| 2 | inactive | 相手装置，またはフレームリレー網での障害検出がフレームリレー網から本装置へ通知されています。<br>1. 相手装置の PVC 状態確認手順の状態が down となっている可能性があります。<br>2. フレームリレー網と相手装置間の回線で障害が発生している可能性があります。<br>3. フレームリレー網内で障害が発生している可能性があります。 | それぞれの原因に対して，次にように対応してください。<br>1. 相手装置の設定が誤っていないか確認してください。<br>2. 相手装置のフレームリレー網への接続状態に異常がないか確認してください。運用による装置の電源断，または回線の閉塞を行っている場合もあります。<br>3. フレームリレー網事業者に網の状態に異常はないか確認してください。 |
| 3 | invalid | 当該 DLCI がフレームリレー網に認識されていません。 | フレームリレー網と契約している接続条件に誤りがないか，また当該 DLCI が使用可能となるようフレームリレー網側での設定が完了しているかフレームリレー網事業者に確認してください。 |

### (f) 通信相手の状態確認

show peer コマンドにより該当する通信相手の状態を確認してください。次の表に通信相手の状態に対する対応を示します。

**表 7-15 通信相手状態の確認**

| 項番 | 確認項目 | 原因 | 対応 |
|---|---|---|---|
| 1 | 通信相手状態が closed | 当該通信相手が close コマンドにより閉塞されているため，接続できません。 | 当該通信相手を free コマンドにより閉塞解除してください。 |
| 2 | 通信相手状態が disabled | 当該通信相手が構成定義により disable 設定になっているため，接続できません。 | 当該通信相手を enable 設定になるように構成定義変更してください。 |
| 3 | 通信相手状態が restricted | 当該通信相手への発信が規制中になっているため，接続できません。 | 当該通信相手を enable 設定になるように構成定義変更してください。 |
| 4 | Phone Number が不正 | 当該通信相手の電話番号／サブアドレスが実際と異なるため，接続できません。 | 当該通信相手の電話番号／サブアドレスを正しい設定に変更してください。 |
| 5 | ID が不正 | 認証 ID が実際と異なるため，接続できません。 | 当該通信相手の認証 ID を正しい設定に変更してください。 |

### (g) ISDN POOL の状態確認

show isdn-pool コマンドにより該当する通信相手が使用している ISDN POOL の状態を確認してくださ

い。次の表に ISDN POOL の状態に対する対応を示します。

**表 7-16 ISDN POOL の確認**

| 項番 | 確認項目 | 原因 | 対応 |
|---|---|---|---|
| 1 | channel use rate | 本項目により空きチャネルがない場合，通信に使うチャネルを割り当てることができません。 | ISDN POOL 内で使用可能なチャネル数と通信相手数との関連を見直してください。 |
| 2 | Lost calls(originate) | 本項目がカウントアップされる場合，空きチャネルがないため発信できない現象が発生しています。 | 同上 |
| 3 | Lost calls(answer) | 本項目がカウントアップされる場合，空きチャネルがないため着信できない現象が発生しています。 | 同上 |

### (2) 統計情報の確認

show interfaces コマンドにより，当該 Line または Timeslot の以下の統計情報（フレーム受信・送信失敗）を確認してください。フレーム受信・送信失敗が発生している場合は，回線テストを実行し NIF ボード／ケーブル／モデムが故障していないか確認してください※。

また，シリアル回線を使用している場合は，show interfaces コマンドにより未サポートの回線速度になっていないか確認してください。なお，NWVX-4，NWVX-8，NWBMX2-4 ではサポートする回線速度に違いがありますので，ご注意ください。それぞれの NIF でサポートする回線速度については，「構成定義コマンドレファレンス Vol.1　4. ライン情報　line_speed」を参照してください。

注※

回線テストの方法は以下を参照してください。

- 「運用コマンドレファレンス Vol.1　test interfaces(WAN)」
- 「8.7　回線をテストする」

[ フレーム受信失敗に関する統計情報 ]

In fcs errors
In overrun errors
In aborted frames
In not octed aligned frames
In short frames
In overflow frames
In error discarded frames

[ フレーム送信に関する統計情報 ]

Out underrun errors
Send complete supervising timeout
out error discarded frames

NIF ボード／ケーブル／モデムの故障ではない場合は，回線業者に対して回線の状態が正常か問い合わせてください。

### (3) フレームリレーの PVC（DLCI）接続の確認

リンクレイヤプロトコルがフレームリレーで，本装置を対向接続している場合，ping frame-relay コマンドにより PVC(DLCI) の接続を確認してください。

「図 7-6　ping frame-relay コマンドの実行例（PVC が確立している場合）」は相手装置との間で PVC 接続

が確立している場合の実行例,「図 7-7　ping frame-relay コマンドの実行例（PVC が確立していない場合)」は PVC 接続が確立していない場合の実行例です。

**図 7-6　ping frame-relay コマンドの実行例（PVC が確立している場合）**

```
> ping frame-relay nif 1 line 0 dlci 31
Data Received InARP-seq=0
Data Received InARP-seq=1
Data Received InARP-seq=2
Data Received InARP-seq=3
Data Received InARP-seq=4
>
```

**図 7-7　ping frame-relay コマンドの実行例（PVC が確立していない場合）**

```
> ping frame-relay nif 1 line 0 dlci 31
Timeout InARP-seq=0
Timeout InARP-seq=1
Timeout InARP-seq=2
Timeout InARP-seq=3
Timeout InARP-seq=4
>
```

実行結果が「図 7-7　ping frame-relay コマンドの実行例（PVC が確立していない場合)」のようになった場合は，相手装置が本装置へ接続している DLCI を正常に認識していないか，相手装置の DLCI の設定が誤っている可能性があります。相手装置での DLCI の状態，および設定を確認してください。実行結果が「図 7-6　ping frame-relay コマンドの実行例（PVC が確立している場合)」のようになった場合は，PVC(DLCI) の接続は正常ですので，ネットワークレイヤ（IP など）の確認を行ってください。

## 7.4.3　ATM 回線の接続ができない

通信障害の原因が ATM 回線にあると考えられる場合は ATM の NIF，Line などの状態を以下に従い確認してください。

### (1) 状態確認

#### (a) NIF の状態確認

show interfaces コマンドにより NIF 状態を確認してください。次の表に NIF 状態に対する対応を示します。

**表 7-17　NIF 状態の確認／対応**

| 項番 | NIF 状態 | 原因 | 対応 |
|---|---|---|---|
| 1 | active | 当該 NIF は正常に動作中です。 | show interfaces コマンドにより Line の状態を確認し，「表 7-18　Line 状態の確認／対応」の対応にしたがってください。 |
| 2 | mismatch | 実装している NIF では，当該 NIF 配下に構成定義されている Line を使用することはできません（実装されている NIF と Line の構成定義情報が不一致です)。 | 実装している NIF が間違っていないか，または Line の構成定義情報が間違っていないか確認してください。 |
| 3 | unused | 当該 NIF 配下に Line の構成定義情報が設定されていません。 | 使用する Line の構成定義情報を設定してください。 |
| 4 | closed | close nif コマンドにより当該 NIF の運用が停止されています。 | 使用する NIF ボードが実装されていることを確認の上，free コマンドにより当該 NIF を運用状態にしてください。 |

| 項番 | NIF 状態 | 原因 | 対応 |
|---|---|---|---|
| 5 | fault | 当該 NIF が障害となっています。 | show logging コマンドにより表示される当該 Line のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |
| 6 | initialize | 当該 NIF が障害検出後の再起動中です。 | 同上 |
| 7 | locked | 構成定義により当該 NIF の運用が停止されています。 | 使用する NIF ボードが実装されていることを確認の上，構成定義情報を設定して当該 NIF を運用状態にしてください。 |

### (b) Line の状態確認

show interfaces コマンドにより Line 状態を確認してください。次の表に Line 状態に対する対応を示します。

**表 7-18　Line 状態の確認／対応**

| 項番 | Line 状態 | 原因 | 対応 |
|---|---|---|---|
| 1 | active up | 当該 Line は正常に動作中です。 | show atm コマンドにより VC の状態を確認し，「表 7-19　VC 状態の確認／対応」の対応にしたがってください。 |
| 2 | active down | 当該 Line に回線障害が発生しています。 | show logging コマンドにより表示される当該 Line のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |
| 3 | mismatch | 実装している Line では，当該 Line 配下に構成定義されている Line を使用することはできません。 | 実装している Line が正しいか，または Line の構成定義情報が正しいか確認してください。 |
| 4 | unused | 当該 Line 配下に Line の構成定義情報が設定されていません。 | 使用する Line の構成定義情報を設定してください。 |
| 5 | closed | close コマンドにより当該 Line の運用が停止されています。または，未サポートサービスカテゴリパターンが指定されています。 | 使用する Line にケーブルが実装されていることを確認の上，free コマンドにより当該 Line を運用状態にしてください。未サポートサービスカテゴリパターンを指定している場合，サポートパターンに変更してください。 |
| 6 | test | test interfaces コマンドにより，当該 Line は回線テスト中です。 | 通信を再開する場合は，no test interfaces コマンドにより回線テストを停止してください。 |
| 7 | fault | 当該 Line の回線部分のハードウェアが障害となっています。 | show logging コマンドにより表示される当該 Line のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |
| 8 | initialize | 当該 Line が障害検出後の再起動中です。 | 同上 |
| 9 | locked | 構成定義により当該 Line の運用が停止されています。 | 使用する Line にケーブルが接続されていることを確認の上，構成定義情報を設定して当該 Line を運用状態にしてください。 |

### (c) VC の状態確認

show atm コマンドにより VC 状態を確認してください。次の表に VC 状態に対する対応を示します。

表 7-19 VC 状態の確認／対応

| 項番 | VC 状態 | 原因 | 対応 |
|---|---|---|---|
| 1 | up | 当該 VC は正常に動作中です。 | ping atm コマンドで相手装置との接続を確認してください。 |
| 2 | locked | 当該 VC は構成定義情報により非運用状態です。 | 運用を開始する場合は，構成定義コマンド vc により当該 VC を運用状態にしてください。 |
| 3 | closed | 次のことが考えられます。<br>1. close コマンドにより当該 VC の運用が停止されています。<br>2. test interfaces コマンドにより，当該 VC を含む Line は回線テスト中です。<br>3. 当該 VC は IP インタフェースとして構成定義されていません。 | それぞれの原因に対して，次にように対応してください。<br>1. free コマンドにより VC を運用状態にしてください。<br>2. 通信を再開する場合は，no test interfaces コマンドにより回線テストを停止してください。<br>3. 構成定義コマンド ip によりインタフェースを定義してください。 |
| 4 | fault | 次のことが考えられます。<br>1. NIF 状態が ” active ” で Line 状態が ” active up ” の場合，ATM ネットワーク内での障害，または相手装置が電源 OFF または障害が発生している可能性があります。<br>2. NIF 状態または Line 状態が ” fault ” の場合，NIF 状態または Line 状態が fault になったことによるものです。 | それぞれの原因に対して，次にように対応してください。<br>1. ATM ネットワークの状態および相手装置の動作状態を確認してください。<br>2. show logging コマンドにより表示される当該 Line のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |
| 5 | initialize | 当該 VC が障害検出後の再起動中です。 | 同上 |

## (2) VC 接続の確認

ping atm コマンドにより VC の疎通を確認することができます。本コマンドは F5 OAM Loopback セルをサポートしている装置との間で実行可能です。

「図 7-8 ping atm コマンドの実行結果（疎通可能な状態）」に相手装置との間で当該 VC が通信可能な状態である場合の実行結果を，また「図 7-9 ping atm コマンドの実行結果（疎通不可な状態）」に通信ができない場合の実行結果を示します。

図 7-8 ping atm コマンドの実行結果（疎通可能な状態）

```
> ping atm nif 0 line 0 vpivci 0 32
Data Received OAM-seq=0
Data Received OAM-seq=1
Data Received OAM-seq=2
Data Received OAM-seq=3
Data Received OAM-seq=4
>
```

図 7-9 ping atm コマンドの実行結果（疎通不可な状態）

```
> ping atm nif 0 line 0 vpivci 0 32
Timeout OAM-seq=0
Timeout OAM-seq=1
Timeout OAM-seq=2
Timeout OAM-seq=3
Timeout OAM-seq=4
>
```

表 7-20 VC 状態の確認／対応

| 項番 | ping atm コマンド結果 | 原因 | 対応 |
|---|---|---|---|
| 1 | 疎通可 | 次のことが考えられます。<br>1. ATM 上のカプセル化方式が一致していない可能性があります。<br>2. ダイナミックなアドレス解決が失敗している可能性があります。<br>3. IP レイヤ以上で通信不可となっている可能性があります。 | それぞれの原因に対して，次にように対応してください。<br>1. 本装置と相手装置の間でカプセル化方式が一致するよう，構成定義情報の設定を合わせてください。<br>2. show ip arp コマンドで対応するエントリがあることを確認してください。エントリがなければ，構成定義コマンド arp でアドレス解決情報を構成定義してください。<br>3.「7.5.1 通信ができない，または切断されている」を参照してください。 |
| 2 | 疎通不可 | 本装置，ATM ネットワーク内の中継装置，または相手装置で VPI/VCI の設定が誤っている可能性があります。 | 本装置および相手装置の VPI/VCI の設定が誤っていないか確認してください。また，キャリアのサービスに接続する場合，契約した VPI/VCI の範囲を確認してください。 |

# 7.5 IPv4 ネットワークの通信障害

## 7.5.1 通信ができない，または切断されている

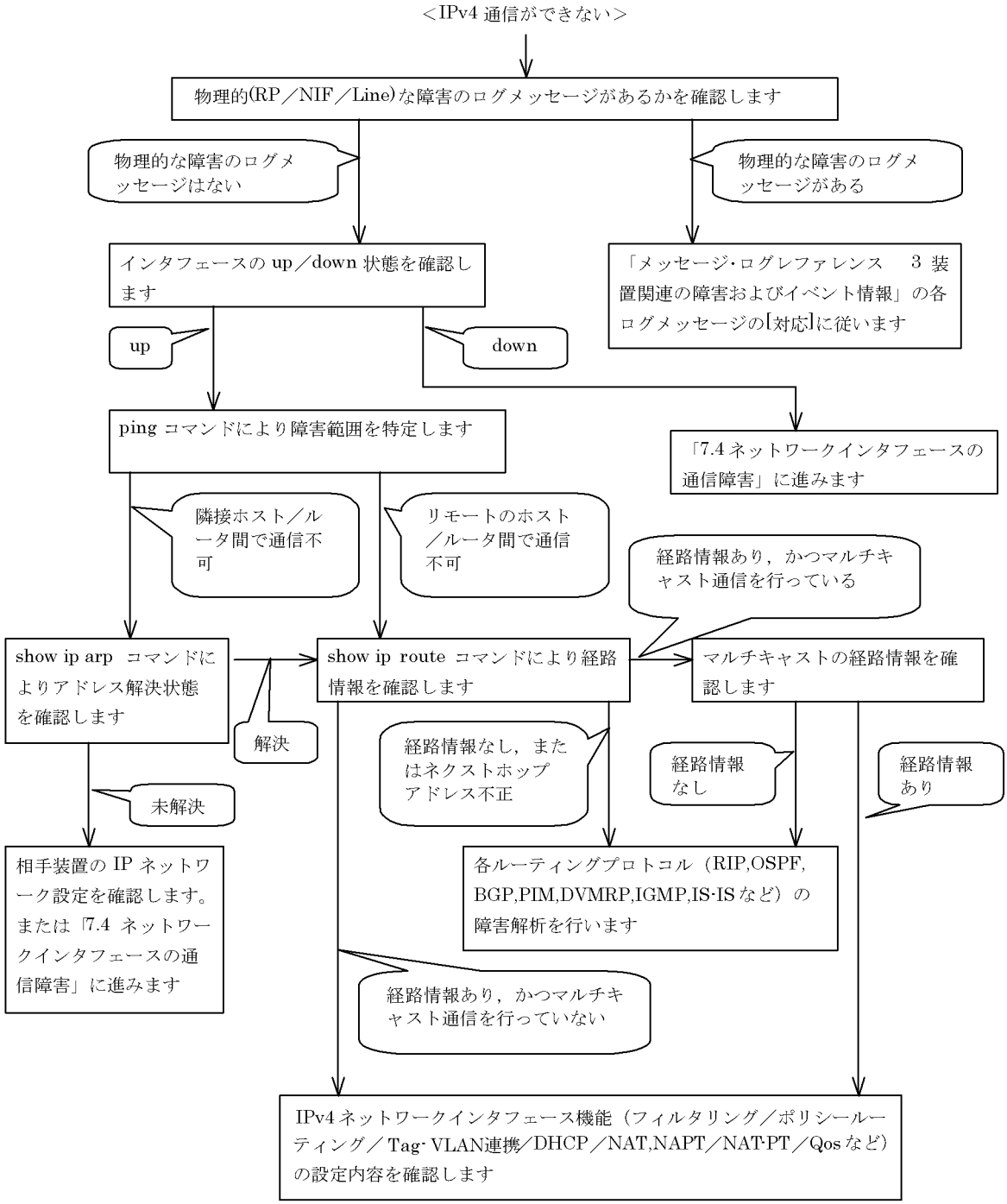
本装置を使用している IPv4 ネットワーク上で，通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. IP 通信に関係する構成定義情報の変更
2. ネットワークの構成変更
3. ネットワークを構成する機器の障害

上記 1. および 2. については，構成定義情報およびネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。

ここでは，3. に示すように「構成定義情報およびネットワーク構成は正しいのに IP 通信ができない」，「これまで正常に動いていたのに IP 通信ができなくなった」というケースを中心に，障害部位および原因の切り分け手順を説明いたします。

障害部位および原因の切り分け方法は，次のフローにしたがってください。




## (1) ログメッセージの確認

通信ができなくなる原因の一つには，ハードウェア（RP ／ NIF ／ Line）の障害（または壊れ）が考えられます。本装置が表示するログメッセージで，ハードウェアの障害を示すメッセージの表示手順を示します。

なお，ログメッセージの内容については，「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。

1. 本装置にログインします。
2. show logging コマンドを使ってログメッセージを表示させます。
3. ログメッセージには各々発生した日時が表示されます。通信ができなくなった日時にログメッセージが表示されていないか確認してください。
4. 通信ができなくなった日時に表示されているログメッセージの障害の内容および障害への対応は「メッセージ・ログレファレンス」に記載しています。その指示にしたがってください。
5. 通信ができなくなった日時にログメッセージの表示がないときは,「(2) インタフェース状態の確認」に進んでください。

### (2) インタフェース状態の確認

本装置のハードウェアは正常に動作している場合でも，本装置と接続している隣接の装置のハードウェアに障害が発生していることも考えられます。

本装置と隣接の装置間の，インタフェースの状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ip interface コマンドを使って該当装置間のインタフェースの Up ／ Down 状態を確認してください。
3. 該当インタフェースが ” Down ” 状態のときは,「7.4　ネットワークインタフェースの通信障害」を参照してください。
4. 該当インタフェースとの間のインタフェースが ” Up ” 状態のときは,「(3) 障害範囲の特定（本装置から実施する場合)」に進んでください。

### (3) 障害範囲の特定（本装置から実施する場合）

本装置に障害がない場合は，通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか，障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. ping コマンドを使って通信できない両方の相手との疎通を確認してください。ping コマンドの操作例および実行結果の見方は,「5.2.2　当該宛先アドレスとの通信可否を確認する」を参照してください。
3. ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使って本装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping コマンド実行の結果，障害範囲が隣接装置の場合は「(5) 隣接装置との ARP 解決情報の確認」に，リモート先の装置の場合は「(6) ユニキャストルーティング情報の確認」に進んでください。

### (4) 障害範囲の特定（お客様の端末装置から実施する場合）

本装置にログインすることができない環境にある場合に，お客様の端末装置から通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. お客様の端末装置に ping 機能があることを確認してください。
2. ping 機能をお使いになり，お客様の端末装置と通信相手との疎通ができるか確認してください。
3. ping 機能で通信相手との疎通が確認できなかったときは，さらに ping コマンドを使ってお客様の端末装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping 機能による障害範囲が特定できましたら，障害と考えられる装置が本装置である場合は本装置にログインしていただき，障害解析フローにしたがって障害原因の調査を行ってください。

### (5) 隣接装置との ARP 解決情報の確認

ping コマンドの実行結果によって隣接装置との疎通が不可の場合は，ARP によるアドレスが解決していないことが考えられます。本装置と隣接装置間のアドレス解決状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ip arp コマンドを使って隣接装置間とのアドレス解決状態（ARP エントリ情報の有無）を確認してください。
3. 隣接装置間とのアドレスが解決している（ARP エントリ情報有り）場合は，「(6) ユニキャストルーティング情報の確認」に進んでください。
4. 隣接装置間とのアドレスが解決していない（ARP エントリ情報無し）場合は，隣接装置と本装置の IP ネットワーク設定が一致しているかを確認してください。

## (6) ユニキャストルーティング情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない場合や，IPv4 ユニキャスト通信で通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ip route コマンドを実行して，本装置が取得した経路情報を確認してください。
3. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がない場合やネクストホップアドレスが不正の場合は「7.6　IPv4 ユニキャストルーティングの通信障害」に進んでください。
4. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。
   - マルチキャストルーティング通信
     「(7) マルチキャストルーティング情報の確認」に進んでください
   - フィルタリング／ QoS 機能
     「(8) フィルタリング／ QoS 設定情報の確認」に進んでください。
   - ポリシールーティング機能
     「(10) ポリシールーティング設定情報の確認」に進んでください。
   - Tag-VLAN 連携機能
     「(11) Tag-VLAN 連携設定情報の確認」に進んでください。
   - NAT，NAPT 機能
     「7.5.4　NAT，NAPT 通信ができない」に進んでください。
   - NAT-PT 機能
     「7.8.5　NAT-PT 通信ができない」に進んでください。

## (7) マルチキャストルーティング情報の確認

マルチキャストパケットを受信しているにもかかわらず経路情報が存在しない場合は，本装置が取得している隣接情報や IGMP グループ情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. 次の表に示すコマンドを使って本装置が取得している隣接情報および IGMP グループ情報を確認してください。これらのコマンドの詳細は「運用コマンドレファレンス Vol.2　4. IP マルチキャストルーティングプロトコル情報」を参照してください。また，マルチキャストルーティングのプロトコル別の確認方法は，「7.7　IPv4 マルチキャストルーティングの通信障害」を参照してください。

**表 7-21 PIM 動作時のコマンド**

| 項番 | コマンド | 確認内容 |
|---|---|---|
| 1 | show ip pim interface | PIM インタフェースが動作していること |
| 2 | show ip pim neighbor | 近隣の PIM ルータが存在していること |
| 3 | show ip rpf xxx.xxx.xxx.xxx | マルチキャストデータ送信元に対する RPF が存在していること |
| 4 | show ip igmp interface | IGMP インタフェースが動作していること |
| 5 | show ip igmp groups | 参加している IGMP グループが認識されていること |
| 6 | show ip pim bsr | PIM-SM の BSR 情報を保持していること |
| 7 | show ip pim rendezvous-point mapping | PIM-SM のランデブーポイント情報を保持していること |
| 8 | show ip pim rendezvous-point-hash XXX.XXX.XXX.XXX | 当該アドレス（グループアドレス）に対するランデブーポイントが存在していること |
| 9 | show ip mroute | PIM-SM のルート情報を保持していること |

注

項番 6 ～ 9 は PIM-SM だけ

**表 7-22 DVMRP 動作時のコマンド**

| 項番 | コマンド | 確認内容 |
|---|---|---|
| 1 | show ip dvmrp interface | DVMRP インタフェースが動作していること |
| 2 | show ip dvmrp neighbor | 近隣の DVMRP ルータが存在していること |
| 3 | show ip dvmrp route xxx.xxx.xxx.xxx | マルチキャストデータ送信元に対する経路が存在していること |
| 4 | show ip igmp interface | IGMP インタフェースが動作していること |
| 5 | show ip igmp groups | 参加している IGMP グループが認識されていること |

3. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。
   - フィルタリング／ QoS 機能

   「(8) フィルタリング／ QoS 設定情報の確認」に進んでください。

## (8) フィルタリング／ QoS 設定情報の確認

本装置において，インタフェースが up 状態で，かつ経路情報も正しく設定されているにもかかわらず通信ができない場合は，フィルタリング機能により特定のパケットが廃棄されているか，あるいは QoS 機能の帯域制御，出力優先制御，または廃棄制御によりパケットが廃棄されている可能性があります。

したがって，現用構成定義情報のフィルタリング機能および QoS 機能の設定条件が正しいか，システム構築において帯域制御ならびに優先・廃棄制御がシステム運用において適切であるか見直してください。また，フィルタリング機能および QoS 機能によって本装置内でパケットが廃棄されている場合の，廃棄個所の特定方法の手順を次に示します。

### (a) フィルタリング機能によるパケット廃棄の確認方法

1. 本装置にログインします。
2. show filter-flow コマンドを使って入出力インタフェースでパケットが廃棄されていないか確認してく

ださい。

**[確認例]**

通信できないパケットの入力インタフェース名称が tokyo1，送信元 IP アドレスが 170.10.11.10 の場合，フィルタリング機能で廃棄されているかどうかを確認します。

1. 本装置にログインします。
2.「show filter-flow detail」と入力します。

```
> show filter-flow detail
<Filter List No.>:    1
      Using Interface:tokyo1/in
      source ip :170.10.11.21 -170.10.11.30
      forward packets                                          :       461
<Filter List No.>:    2
      Using Interface:tokyo1/in
      drop packets                                             :     50121
<Filter List No.>:    1
      Using Interface:tokyo4/out
      source ip :170.10.12.1 -170.10.12.254
      forward packets                                          :         3
>
```

3. 入力インタフェース名称が tokyo1 の <Filter List No> を確認します。
   上記例では，<Filter List No.>:1,2 が該当します。
4. 3. で確認したフロー条件と通信できないパケットの内容を比較して，一致する <Filter List No.> の動作が廃棄になっていないか確認します。
   本例ではパケットの送信元 IP アドレスが 170.10.11.10 なので <Filter List No.>:2 と一致します。
   <Filter List No.>:2 の動作は廃棄なので，入力インタフェースのフィルタリング機能で廃棄されている可能性があります。

### (b) QoS 機能の帯域制御によるパケット廃棄の確認方法

1. 本装置にログインします。
2. show qos ip-flow コマンドを使って入出力インタフェースでパケットが QoS 機能の帯域制御によって廃棄されていないか確認してください。

**[確認例]**

通信できないパケットの入力インタフェース名称が tokyo1，送信元 IP アドレスが 170.10.11.21 の場合，QoS 機能の帯域制御によって廃棄されているかどうかを確認します。

1. 本装置にログインします。
2.「show qos ip-flow detail」と入力します。

```
> show qos ip-flow detail
<QoS IP List No.>:    1
      Using Interface:tokyo1/in
      source ip :170.10.11.21 -170.10.11.30
      packets of    1000000bps and under(priority3  discard4) :     7021
      packets of    1000000bps over     (drop)                :      729
      forward packets                                         :      461
<QoS IP List No.>:    2
      Using Interface:tokyo2/out
      protocol :6  destination port :20 -21
      hit packets                     (priority8  discard4) : 11568793
>
```

3. 入力インタフェース名称が tokyo1 の <QoS IP List No.> を確認します。
   上記例では <QoS IP List No.>:1 が該当します。

4. 3. で確認したフロー条件と通信できないパケットの内容を比較して，一致する <QoS IP List No.> の動作が廃棄になっていないか確認します。
   本例ではパケットの送信元 IP アドレスが 170.10.11.21 なので，<QoS IP List No.>:1 と一致します。
   <QoS IP List No.>:1 の契約帯域違反時（packets of 1000000bps over (drop)）の動作は廃棄なので，入力インタフェースの QoS 機能の帯域制御で廃棄されている可能性があります。

#### (c) QoS 機能のキュー制御によるパケット廃棄の確認方法

1. 本装置にログインします。
2. show qos queueing コマンドを使って出力インタフェースでパケットが QoS 機能のキュー制御によって廃棄されていないか確認してください。

**[確認例]**

通信できないパケットの出力インタフェースが NIF 番号 1，Line 番号 3 の場合，QoS 機能のキュー制御によって廃棄されているかどうかを確認します。

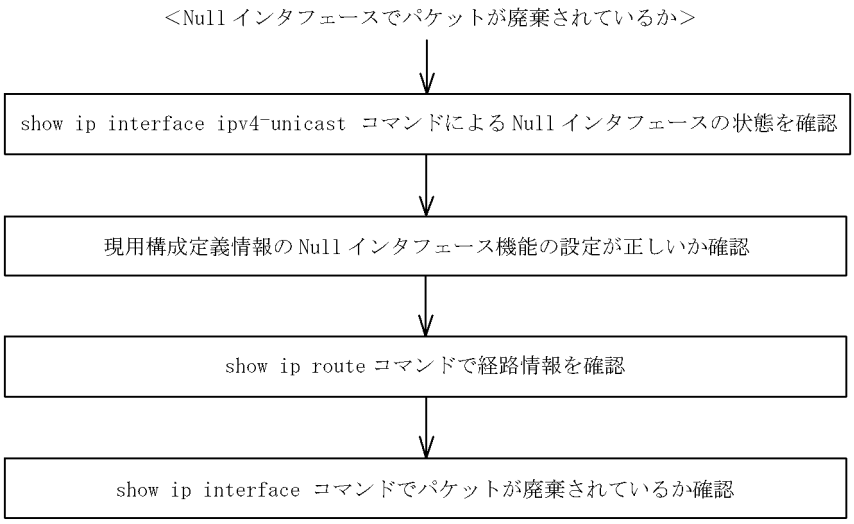
1. 本装置にログインします。
2.「show qos queueing nif 1 line 3 input」と入力します。

```
> show qos queueing nif 1 line 3 input
NIF1 Line3: 10BASE-T half TX
Interface name: tokyo1
    Limit Qlen              :  255
    Priority1  Qlen         :   87  Priority2  Qlen         :       112
    Priority3  Qlen         :  215  Priority4  Qlen         :        58
    Priority5  Qlen         :   66  Priority6  Qlen         :        32
    Priority7  Qlen         :  147  Priority8  Qlen         :       178
    Priority1  maximum Qlen :  148  Priority2  maximum Qlen :       139
    Priority3  maximum Qlen :  227  Priority4  maximum Qlen :        89
    Priority5  maximum Qlen :  129  Priority6  maximum Qlen :        78
    Priority7  maximum Qlen :  194  Priority8  maximum Qlen :       233
    Total out frames                                        :   2784609
    Total out bytes                                         : 178214976
    Total discarded frames due to queue overflow            :      2375
>
```

3. 総廃棄フレーム数（Total discarded frames due to queue overflow）が 1 以上の場合，キュー制御によってパケットが廃棄されています。
   本例では総廃棄フレーム数が 2375 なので，キュー制御によってパケットが廃棄されています。

### (9) Null インタフェース設定情報の確認

特定のネットワーク宛または特定の端末宛の通信を Null インタフェースに向けて制限しているにもかかわらず，パケットが廃棄されない場合は，Null インタフェースの設定内容に誤りがある可能性があります。次の手順で Null インタフェースの設定内容が正しいか確認してください。




1. show ip interface ipv4-unicast コマンドを使い Null インタフェースの状態を確認します。Null インタフェースが UP しているか確認してください。
2. 現用構成定義情報で Null インタフェースが定義されているか確認します。
3. show ip route コマンドで経路情報を確認します。
   構成定義コマンド static で定義した経路情報の設定内容が正しいかどうかを確認してください。
4. パケットが廃棄されているか確認します。
   show ip interface コマンドを使って Null インタフェースでパケットが廃棄されているか確認してください。

## (10) ポリシールーティング設定情報の確認

本装置において物理的障害は発生してなく，経路情報も正しく設定されているにもかかわらず通信ができない場合は，ポリシールーティング機能の出力先インタフェースに障害が発生しているためにパケットが廃棄されている可能性が考えられます。

したがって，次の手順でポリシールーティングの現在使用されている出力先インタフェースの状態を確認してください。

### (a) ポリシールーティング機能による出力先インタフェースの確認方法

1. 本装置にログインします。
2. show ip policy コマンドを使って入力インタフェースのポリシールーティング設定内容と，現在使用されている出力先インタフェースの状態を確認します。

**[確認例]**

通信できないパケットの入力インタフェースが tokyo，送信元 IP アドレスが 200.1.4.5 の場合，ポリシールーティング機能で使用されている出力先を確認します。

1. 本装置にログインします。
2.「show ip policy interface tokyo」と入力します。

```
> show ip policy interface tokyo
<Interface Name>            <Filter List No>
  tokyo                      1,2
```

```
>
```

3. 入力インタフェース tokyo で使用されている条件番号を確認します。
   上記例では，＜ Filter List No. ＞:1,2 が該当します。
4. 3. で確認した条件の詳細を表示します。「show ip local policy interface tokyo 1 2」と入力します。

```
> show ip local policy interface tokyo 1 2
<Interface Name>:   tokyo    <Filter List No.>:    1
 ip source:                  200.1.4.0 - 200.1.4.255
 ip destination:             200.1.7.0 - 200.1.8.255
 current policy route
     Policy Group Name       route1
     Output Interface        tokyo3
     Next Hop IP address     200. 1. 10. 1
<Interface Name>:   tokyo    <Filter List No.>:    2
 ip source:                  200.1.5.0 - 200.1.5.255
 ip destination:             200.1.19.0 - 200.1.20.255
 current policy route
     Policy Group Name       route2
     Output Interface        yokohama
     Next Hop IP address     200. 1. 50. 2
>
```

5. 各条件の内容と条件とその際の出力先を確認します。
   通信できないパケットの内容を比較して，一致する条件のポリシールーティンググループ名称を確認します。
6. 採用されているポリシーグループの状態を確認します。「show ip cache policy route1」と入力します。

```
> show ip cache policy route1
<Policy Group Name>:     route1
       priority  Interface Name  status   Nexthop
           1     tokyo1           Down   200. 1. 1.  2
           2     tokyo1           Down   200. 1. 2.  2
           3     tokyo2           Down   200. 1. 8.  3
   *>      4     tokyo3           Down   200. 1. 10. 1    default
>
```

7. 出力先インタフェースが障害により出力できないためパケットが廃棄されています。現用構成定義情報のポリシー情報の設定を見直すと共に，「7.4　ネットワークインタフェースの通信障害」にしたがってください。
   なお，show ip cache policy コマンド実行時，使用中の経路がない（経路の先頭に *> の表示がない）場合も，出力先インタフェースの障害によりパケットが廃棄されていることを表します。

### （11）Tag-VLAN 連携設定情報の確認

本装置に，IP インタフェース情報，経路情報が正しく設定されているにもかかわらず通信ができない場合は，Tag-VLAN 連携情報の設定が誤っている（またはされていない）ために，パケットが廃棄されている可能性が考えられます。本装置の Tag-VLAN 連携設定情報を確認する手順を次に示します。

1. 本装置にログインします。
2. show interfaces コマンドを使用して Tag-VLAN 連携設定情報（Tag-VLAN 連携機能の使用の有無，Tag-VLAN 連携回線情報および VLAN ID）を確認してください。
3. スタティック ARP の設定をした場合は，show ip arp コマンドを使用して ARP エントリに関する Tag-VLAN 連携設定情報（VLAN ID）を確認してください。

上記コマンドで Tag-VLAN 連携の設定が正しいと確認できた場合は，本装置に関する Tag-VLAN 連携の設定に問題はありません。接続装置（LAN Switch など）の設定に問題（VLAN 設定をしていない，VLAN ID が一致していない）がある可能性がありますので，接続装置の設定情報を確認してください。

## 7.5.2 DHCP 機能にて IP アドレスが割り振られない

### (1) DHCP ／ BOOTP リレーの通信トラブル

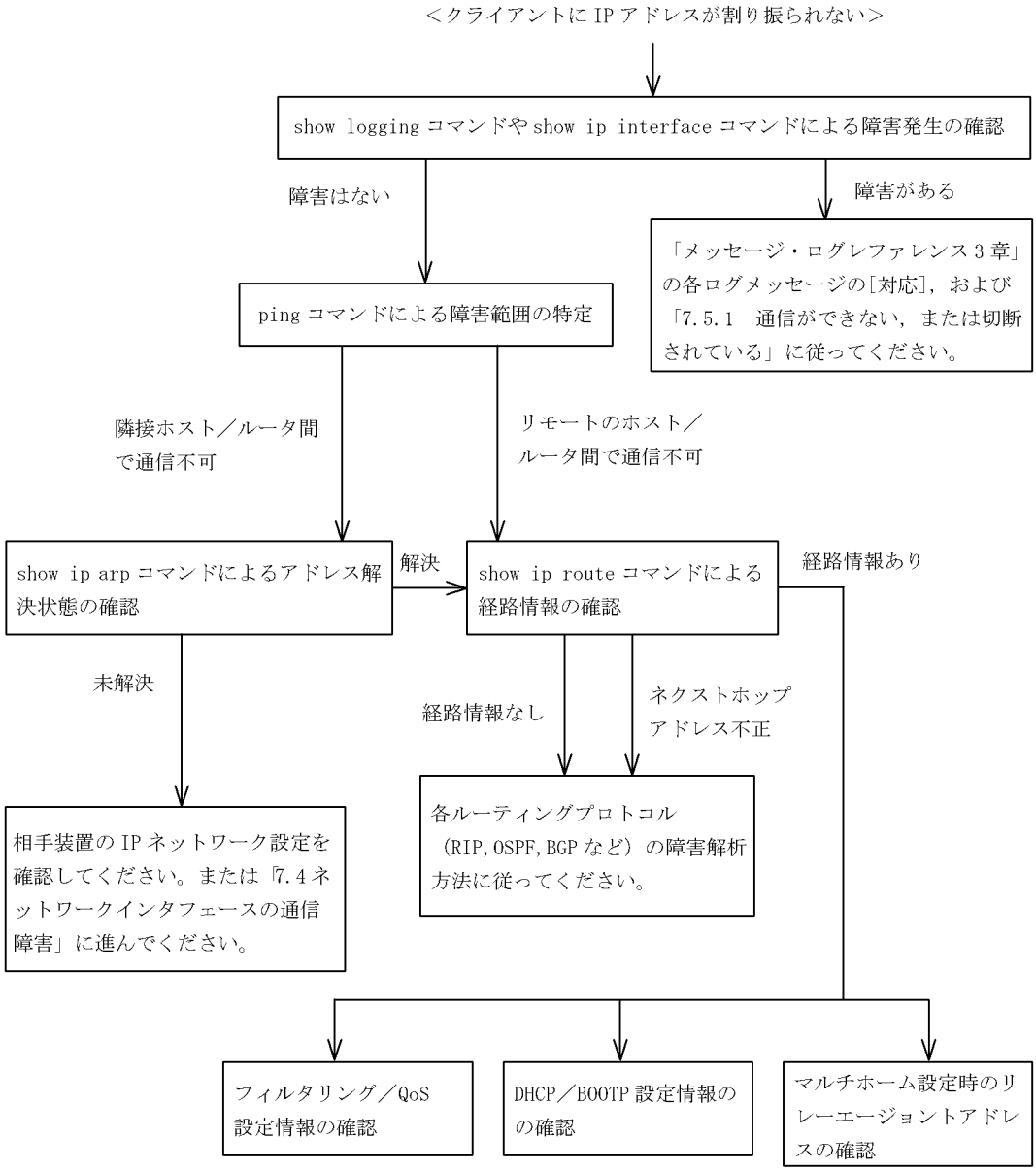
DHCP ／ BOOTP リレーの通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. DHCP ／ BOOTP リレー通信に関係する構成定義情報の変更
2. ネットワークの構成変更
3. DHCP ／ BOOTP サーバの障害

上記 2. については，ネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。

ここでは，クライアントの設定（ネットワークカードの設定，ケーブルの接続など）は確認されているものとし，上記 1. および 3. に示すような「構成定義情報の変更を行ったら，DHCP ／ BOOTP サーバから IP アドレスが割り振られなくなった」,「構成定義情報およびネットワーク構成は正しいのにクライアントに IP アドレスが割り振られず，IP 通信できない」，というケースについて，障害部位および原因の切り分け手順を説明いたします。

障害部位および原因の切り分け方法は，次のフローにしたがってください。




### (a) ログメッセージおよびインタフェースの確認

クライアントにIPアドレスが割り振られなくなる原因の一つにクライアントーサーバ間で通信ができなくなっていることが考えられます。本装置が表示するログメッセージやshow ip interfaceコマンドによるインタフェースのup／down状態を確認してください。手順については「7.5.1　通信ができない，または切断されている」を参照してください。

### (b) 障害範囲の特定（本装置から実施する場合）

本装置に障害がないときは通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. pingコマンドを使って通信できない両方の相手との疎通を確認してください pingコマンドの操作例お

よび実行結果の見方は，「5.2.2　当該宛先アドレスとの通信可否を確認する」を参照してください。
3. ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使って本装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping コマンド実行の結果，障害範囲が隣接装置の場合は「(d) 隣接装置との ARP 解決情報の確認」に，リモート先の装置の場合は「(e) 経路情報の確認」に進んでください。

#### (c) 障害範囲の特定（お客様の端末装置から実施する場合）

本装置にログインすることができない環境にある場合に，お客様の端末装置から通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. お客様の端末装置に ping 機能があることを確認してください。
2. ping 機能をお使いになり，お客様の端末装置と通信相手との疎通ができるか確認してください。
3. ping 機能で通信相手との疎通が確認できなかったときは，さらに ping コマンドを使ってお客様の端末装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping 機能による障害範囲の特定ができましたら，障害と考えられる装置が本装置である場合は本装置にログインしていただき，障害解析フローにしたがって障害原因の調査を行ってください。

#### (d) 隣接装置との ARP 解決情報の確認

ping コマンドによって隣接装置との疎通が不可のときは，ARP によるアドレスが解決していないことが考えられます。本装置と隣接装置間のアドレス解決状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ip arp コマンドを使って隣接装置間とのアドレス解決状態（ARP エントリ情報の有無）を確認してください。
3. 隣接装置間とのアドレスが解決している（ARP エントリ情報有り）場合は，「(e) 経路情報の確認」に進んでください。
4. 隣接装置間とのアドレスが解決していない（ARP エントリ情報無し）場合は，隣接装置と本装置の IP ネットワーク設定が疎通できる設定になっているかを確認してください。

#### (e) 経路情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない，通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ip route コマンドを使って本装置が取得した経路情報を確認してください。
3. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がない場合やネクストホップアドレスが不正の場合は「7.6　IPv4 ユニキャストルーティングの通信障害」に進んでください。
4. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。
   - フィルタリング／ QoS 機能
     「(f) フィルタリング／ QoS 設定情報の確認」に進んでください。
   - DHCP ／ BOOTP 機能
     「(g) DHCP ／ BOOTP 設定情報の確認」に進んでください。
   - マルチホーム機能
     「(h) マルチホーム設定時の DHCP ／ BOOTP リレーエージェント機能情報の確認」に進んでください。

### (f) フィルタリング／QoS 設定情報の確認

本装置において，物理的障害がなく，経路情報も正しく設定されているにもかかわらず通信ができない場合は，フィルタリング機能により特定のパケットだけを廃棄する設定になっているか，QoS 機能の帯域制御，出力優先制御または廃棄制御によりパケットが廃棄されている可能性があります。

したがって，構成定義情報のフィルタリング機能および QoS 機能の設定条件が正しいか，システム構築において帯域制御，出力優先制御，または廃棄制御がシステム運用において適切であるかを確認してください。

### (g) DHCP ／ BOOTP 設定情報の確認

DHCP ／ BOOTP サーバに貸し出し用 IP アドレスが十分に残っている場合，DHCP ／ BOOTP リレーの構成定義設定ミスによりクライアントに IP アドレスが割り振られないという原因が考えられます。次に構成定義情報の確認手順を示します。

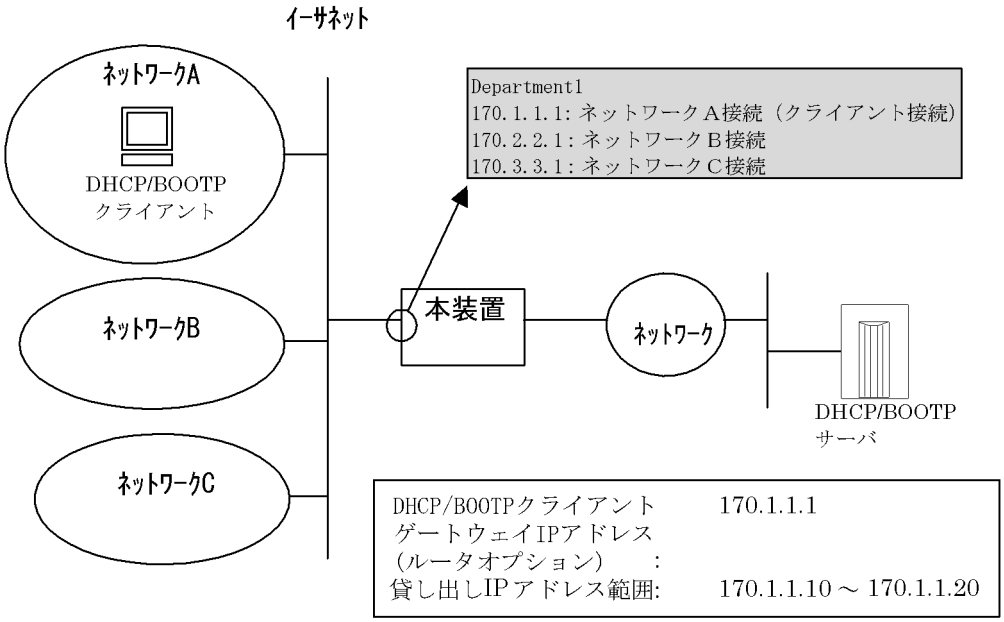
1. relay list は DHCP ／ BOOTP サーバの IP アドレス，または DHCP ／ BOOTP リレーエージェント機能付き次ルータの IP アドレスが指定されているか確認してください。
2. クライアント側のインタフェースに relay interface が設定されているか確認してください。
3. 該当クライアントへ IP アドレスを貸与させたい DHCP ／ BOOTP サーバの IP アドレスが，relay list へ登録されており，かつそのリレーリストの登録された relay group が，リレーインタフェースに設定されているかを確認してください。
4. relay interface の bootp hops 値がクライアントから見て正しい bootp hops 値となっているか確認してください。

### (h) マルチホーム設定時の DHCP ／ BOOTP リレーエージェント機能情報の確認

DHCP ／ BOOTP サーバでは，DHCP ／ BOOTP REQUEST パケット内 giaddr の IP アドレスから貸し出し IP アドレスを選択しています。

本装置において，DHCP ／ BOOTP クライアント接続インタフェースにマルチホームの設定がある場合，インタフェースに最後に IP 定義した IP アドレスを，リレーエージェントアドレスとして DHCP ／ BOOTP REQUEST パケット内 giaddr に設定しています。

DHCP ／ BOOTP クライアントが接続されているインタフェースにマルチホームが設定されている場合において，「リレーエージェントアドレス」と「DHCP ／ BOOTP クライアントが接続されている本装置設定 IP アドレス」が一致していない場合，DHCP ／ BOOTP サーバで対象貸し出し IP アドレスが識別できず，DHCP ／ BOOTP クライアントに IP アドレスの貸し出しが行われない可能性があります。この場合，show dhcp giaddr コマンドを実行し，出力された IP アドレスが，DHCP ／ BOOTP クライアントが接続されている本装置設定 IP アドレスと一致しているか確認してください。




上記構成において，show dhcp giaddr コマンドを入力した時以下のように出力された場合，リレーエージェントアドレスと DHCP ／ BOOTP クライアントが接続されている IP アドレスとが一致していないため，IP アドレスの貸し出しが行われません。

```
> show dhcp giaddr interface Department1
DHCP GIADDR < Department1> : 170.2.2.1
>
```

一致していない場合，次の手順にしたがって DHCP ／ BOOTP リレーエージェント機能で適用するリレーエージェントアドレスの変更を行ってください。なお，DHCP ／ BOOTP クライアント接続インタフェースの IP 構成定義情報を再設定するため，DHCP ／ BOOTP クライアント接続セグメントの運用を一時的に停止することになります。

**[IP 構成定義再設定方法]**

1. インタフェースの IP 定義からクライアントが接続されている IP アドレスを削除してください（IP 定義内の IP アドレスがすべて削除されてしまう場合は relay-interface を先に削除してください）。

```
(config)# show
line Department1 ethernet 0/0
  ip 170.2.2.1/24
  ip-address 170.1.1.1/24
  ip-address 170.3.3.1/24
!
relay_list 1 170.10.10.10
relay_group BlueGroup 1
relay-interface Department1 relay_group BlueGroup
!
(config)# line Department1 ethernet 0/0
[line Department1]
(config)# delete ip-address 170.1.1.1/24
Are you sure? (y/n): y
[line Department1]
(config)# show ip
ip 170.2.2.1/24
  ip-address 170.3.3.1/24
!
```

```
(config)#
```

2. インタフェースにクライアントが接続されている IP アドレスを再設定します。
   構成定義コマンド show で変更した IP 定義を表示したとき，クライアントが接続されている IP アドレスが一番下に表示されていることを確認してください。

```
[line Department1]
(config)# show ip
ip 170.2.2.1/24
  ip-address 170.3.3.1/24
!
[line Department1]
(config)# ip-address 170.1.1.1/24
[line Department1]
(config)# show ip
ip 170.2.2.1/24
ip-address 170.3.3.1/24
ip-address 170.1.1.1/24
!
[line Department1]
(config)#
```

3. 構成定義コマンドモードを quit で終了し，show dhcp giaddr を実行してください。出力結果が 2. で入力した IP アドレスとなっていることを確認してください。

```
(config)# quit
# show dhcp giaddr interface Department1
DHCP GIADDR < Department1 >： 170.1.1.1
#
```

   出力結果が 2. で入力した IP アドレスとなっていない場合は，次の手順にしたがって IP 定義と relay-interface の再設定を行ってください。なお，IP 構成定義情報の再設定を行うため，該当インタフェースの運用を一時的に停止することになります。

   (3-1)

   インタフェースに設定してある relay-interface 定義を削除後，インタフェースの IP 定義をすべて削除してください。

```
(config)# delete relay-interface Department1
Are you sure? (y/n): y
(config)# line Department1 ethernet 0/0
[line Department1]
(config)# delete ip
Are you sure? (y/n): y
[line Department1]
(config)# exit
(config)# show
line Department1 ethernet 0/0
!
relay_list 1 170.10.10.10
relay_group BlueGroup 1
!
(config)#
```

   (3-2)

   インタフェースにクライアントが接続されている IP アドレス以外の IP アドレスを IP 登録します。

```
(config)# line Department1 ethernet 0/0
[line Department1]
(config)# ip 170.2.2.1/24
```

```
[line Department1]
(config)# ip-address 170.3.3.1/24
[line Department1]
(config)# exit
(config)# show
line Department1 ethernet 0/0
  ip 170.2.2.1/24
  ip-address 170.3.3.1/24
!
relay_list 1 170.10.10.10
relay_group BlueGroup 1
!
(config)#
```

(3-3) 最後にクライアントが接続されている IP アドレスを IP 登録してください。

```
(config)# line Department1 ethernet 0/0
[line Department1]
(config)# ip-address 170.1.1.1/24
[line Department1]
(config)# exit
(config)# show
line Department1 ethernet 0/0
  ip 170.2.2.1/24
  ip-address 170.3.3.1/24
  ip-address 170.1.1.1/24
!
relay_list 1 170.10.10.10
relay_group BlueGroup 1
!
(config)#
```

(3-4) インタフェースに relay-interface の設定を行ってください。

```
(config)# relay-interface Department1 relay_group BlueGroup
(config)# show
line Department1 ethernet 0/0
  ip 170.2.2.1/24
  ip-address 170.3.3.1/24
  ip-address 170.1.1.1/24
!
relay_list 1 170.10.10.10
relay_group BlueGroup 1
relay-interface Department1 relay_group BlueGroup
!
(config)#
```

(3-5)

show dhcp giaddr 運用コマンドを実行し，(3-3) で入力した IP アドレスが表示されることを確認してください。

```
(config)# quit
# show dhcp giaddr interface Department1
DHCP GIADDR < Department1 >： 170.1.1.1
#
```

#### (i) DHCP リレーと VRRP が同一インタフェースで運用されている場合の確認

DHCP ／ BOOTP リレーと VRRP が同一インタフェースで運用されている場合，DHCP ／ BOOTP サーバにおいて，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 VRRP 構成定義で設定した仮想ルータアドレスに設定しなければなりません。設定しなかった場合，VRRP によるマ

スタ・スタンバイルータ切り替え後，DHCP ／ BOOTP クライアントが通信できなくなる可能性があります。確認方法については各 DHCP ／ BOOTP サーバの確認方法にしたがってください。

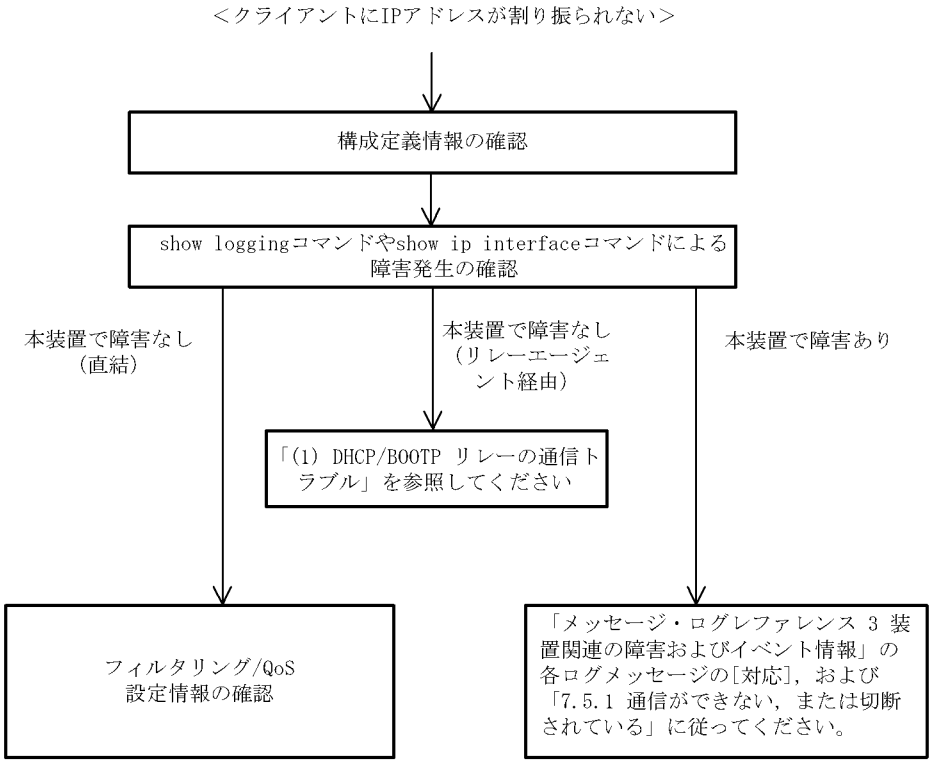
## (2) DHCP サーバの通信トラブル

DHCP サーバの通信トラブル（クライアントにアドレス配信できない）が発生する要因として考えられるのは，次の 3 種類があります。

1. 構成定義情報の設定ミス
2. ネットワークの構成変更
3. DHCP サーバの障害

障害部位および原因の切り分け手順を次のフローに示します。

まず上記 1. の確認を行ってください。構成定義情報の設定で間違えやすいものを例にとり説明します。上記 2. については，ネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。クライアント／サーバの設定（ネットワークカードの設定，ケーブルの接続など）は確認されている場合，上記 3. に示すような「構成定義情報およびネットワーク構成は正しいのにクライアントに IP アドレスが割り振られず，IP 通信できない」，というケースについては，詳細を「(b) ログメッセージおよびインタフェースの確認」～「(e) フィルタリング／ QoS 設定情報の確認」に示します。




### (a) 構成定義情報の確認

DHCP サーバ上のリソース類の構成定義設定ミスによりクライアントに IP アドレスが割り振られないという原因が考えられます。構成定義情報の確認手順を次に示します。

1. DHCP クライアントに割り付ける IP アドレスの範囲指定（range パラメータ）が同時使用するクライアントの台数分確保してあるかを，構成定義情報で確認してください。

2. 固定 IP アドレスを割り付ける PC に IP アドレス配信ができない場合，構成定義情報の動的に割り付ける IP アドレスの範囲指定の中に構成定義コマンド dhcp host で指定した固定 IP アドレス（fixed-address パラメータ）が含まれていないかを確認してください。アドレスが競合している可能性があります。
   例えば下記の例では，動的に割り当てるアドレスを 192.168.10.100 から 192.168.10.120 で定義していますが，この範囲内に固定に割り付けるアドレス（192.168.10.110）が含まれています。
   192.168.10.110 のアドレスを動的に割り当てるアドレスとして先に使用した場合，アドレスを固定に割り付けたいホストには 192.168.10.110 を割り当てることができません。

   ＜固定割り付けアドレスと動的割り付けアドレスの競合例＞

   ```
   dhcp subnet 192.168.10.0/24 range 192.168.10.100 192.168.10.120
   dhcp host manager hardware 00:11:11:ef:ff:11 fixed-address 192.168.10.110
   ```

3. クライアントが本装置からアドレスを割り振られたあと，クライアントと他装置との通信ができない場合は，デフォルトルータの設定がされていない場合があります。dhcp option routers でクライアントが接続されているネットワークのルータアドレス（デフォルトルータ）が設定されているか確認してください（「構成定義コマンドレファレンス Vol.1　19. DHCP サーバ情報」を参考にしてください）。
4. DHCP リレーエージェントとなる装置の設定を確認してください。DHCP リレーエージェントも本装置を使用している場合，「(1) DHCP ／ BOOTP リレーの通信トラブル」を参照してください。
5. DHCP サーバデーモンの起動がうまくできていない場合もあります。DHCP サーバに関する構成定義情報設定時は再起動操作が必要になります。これらの起動方法の手順は，「構成定義コマンドレファレンス Vol.1　dhcp（dhcp サーバ情報）」を参照してください。

#### (b) ログメッセージおよびインタフェースの確認

クライアントに IP アドレスが割り振られなくなる原因の一つにクライアントーサーバ間で通信ができなくなっていることが考えられます。本装置が表示するログメッセージや show ip interface コマンドによるインタフェースの up ／ down 状態を確認してください。手順については「7.5.1　通信ができない，または切断されている」を参照してください。

#### (c) 障害範囲の特定（本装置から実施する場合）

本装置に障害がないときは通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. クライアントとサーバ間にルータなどがある場合，ping コマンドを使って通信できない相手（DHCP クライアント）との間にある装置（ルータ）の疎通を確認してください。ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使って本装置からクライアント側に向けて近い装置から順に通信相手に向けて疎通を確認してください。ping コマンドの操作例および実行結果の見方は，「5.2.2　当該宛先アドレスとの通信可否を確認する」を参照してください。
3. サーバとクライアントが直結の場合，HUB やケーブルの接続を確認してください。
4. ping コマンドによる障害範囲が隣接装置かリモートの装置かによって，障害解析フローの次のステップに進んでください。

#### (d) 経路情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない，通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ip route コマンドを使って本装置が取得した経路情報を確認してください。

#### (e) フィルタリング／ QoS 設定情報の確認

本装置において物理的障害がなく，経路情報も正しく設定されているにもかかわらず通信ができない場合は，フィルタリング機能により特定のパケットだけが廃棄されているか，あるいは QoS 機能の帯域制御，出力優先制御または廃棄制御によりパケットが廃棄されている可能性があります。したがって，構成定義情報のフィルタリング機能および QoS 機能の設定条件が正しいか，システム構築において帯域制御，出力優先制御または廃棄制御がシステム運用において適切であるか，本装置およびクライアント・サーバ間にある中継装置でも見直しを行ってください。

### (3) DHCP クライアントの通信トラブル

DHCP クライアントの通信トラブル（本装置の DHCP クライアントインタフェースに IP アドレスが割り当てられない）が発生する要因として考えられるのは，次の 4 種類があります。

なお，IP アドレス割り当て後の通信トラブルについては，「7.5.1　通信ができない，または切断されている」を参照してください。

1. 構成定義情報の設定誤り
2. DHCP クライアントの障害
3. ネットワーク構成上の問題
4. DHCP サーバ装置間の障害

始めに，DHCP サーバから IP アドレスが取得できているかを確認してください。

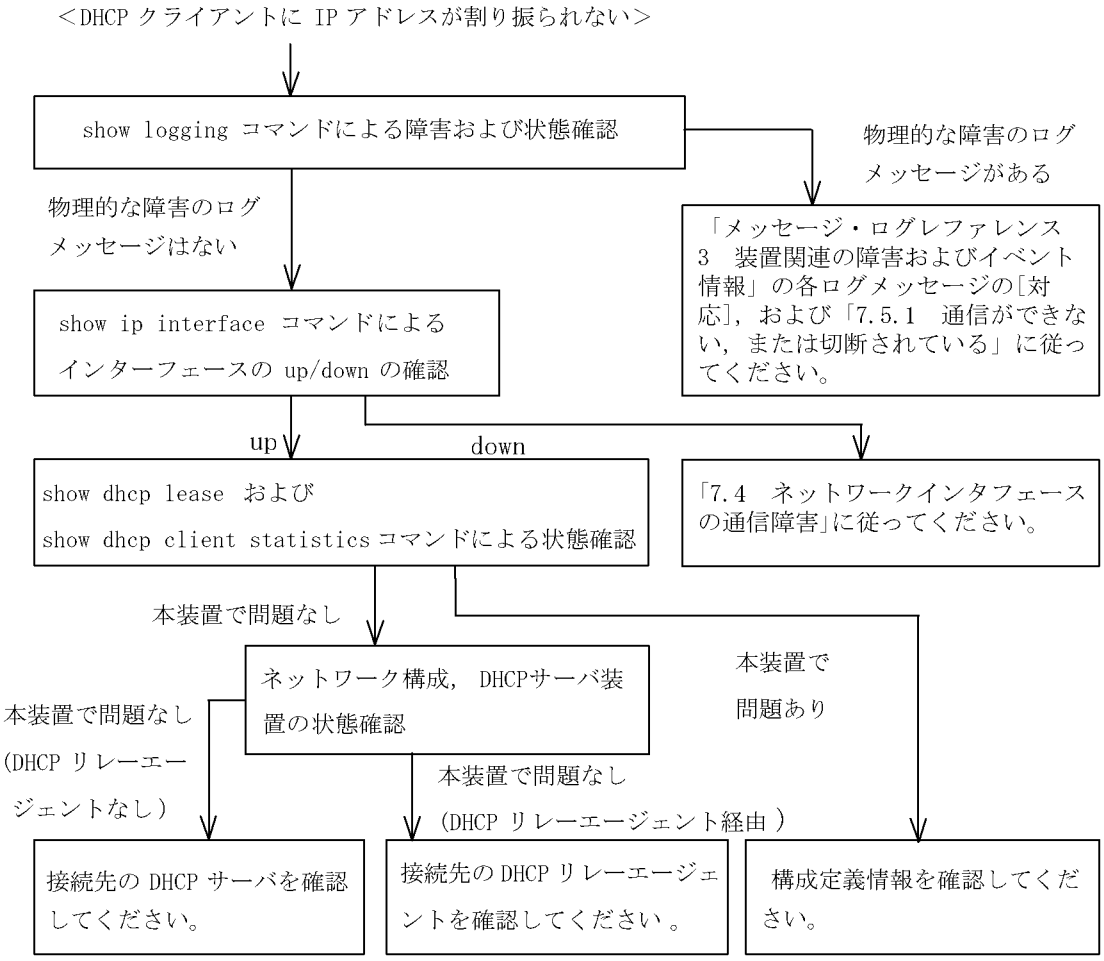
IP アドレスが取得できていない場合，原因の切り分けを次のフローの手順で行います。

まず，show logging で種別ログ，show ip interface でインタフェースの状態を確認してください。

問題がなければ次に 2. に関する本装置の DHCP クライアントの状態を確認してください。

本装置に問題があるようなら 1. に関する構成定義情報を確認してください。

問題がないようなら 3. や 4. の問題が考えられます。HUB やケーブルなどのネットワーク機器の接続や DHCP サーバ，リレーエージェントの設定内容などを確認してください。




### (a) ログメッセージおよびインタフェースの確認

本装置の DHCP クライアントインタフェースに IP アドレスが割り振られない原因の一つに，DHCP クライアントー DHCP サーバ間で通信ができないことが考えられます。本装置が表示するログメッセージや show ip interface コマンドによるインタフェースの up ／ down 状態を確認してください。手順については「7.5.1 通信ができない，または切断されている」を参照してください。

### (b) 本装置の DHCP クライアント状態確認

本装置の DHCP クライアントの障害により DHCP サーバから IP アドレスが割り振られないということが考えられます。次に確認事項を示します。

- **show dhcp lease（DHCP クライアントリース情報表示）コマンドで，構成定義で指定したインタフェース名が存在することを確認してください。**

なお，本コマンドが実行できない（コマンド応答メッセージが ” No such dhcp sub_command. ”）場合は，本装置の DHCP クライアントデーモンが起動されていません。起動方法の手順は，「構成定義コマンドレファレンス Vol.1 dhcp-client（DHCP クライアント情報)」を参照してください。

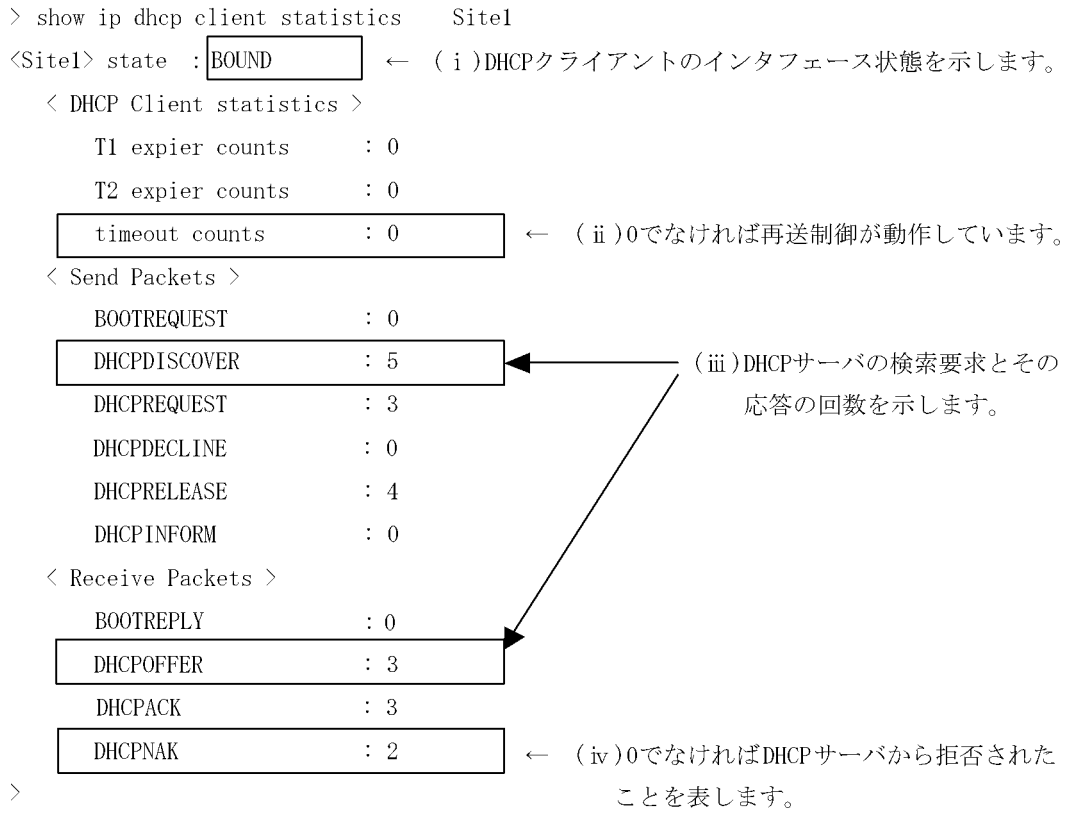
```
> show dhcp lease Site1
<Site1> ← インタフェース名
  IP-address  210.141.119.162     ← 表示が-.-.-.-の場合 IP アドレスが取得できていません。
  subnet-mask 255.255.255.0
  routers     210.141.119.1       ← デフォルトルータ，DNS サーバアドレス
  DNS         210.226.1.90, 210.226.1.20
  host-name   my_hostname
  domain-name foo.ne.jp
  lease-time  43200
  server-ID   210.226.1.41
  lease start 8/18 13:12:11
  T1 (renew)  8/18 19:12:11
  T2 (rebind) 8/18 23:42:11
  lease end   8/19 01:12:11
>
```

● **show dhcp client statistics（DHCP クライアント統計情報表示）コマンドで統計情報を確認してください。**

インタフェース状態（state），送信パケット（Send Packet），受信パケット（Receive Packet）の数を確認してください。

なお，本コマンドが実行できない場合は，本装置の DHCP クライアントデーモンが起動されていません。

起動方法の手順は，「構成定義コマンドレファレンス Vol.1　dhcp（dhcp サーバ情報）」を参照してください。




(i) インタフェース状態が "REBOOTING","INIT","SELECTING","REQUESTING" の場合は，IP アドレス取得中です。しばらく待ち，再度確認してください。

(ii) 応答待ちタイムアウト (timeout counts) がカウントアップされている場合は，DHCP サーバとの通信が正常に行われていません。DHCP サーバとなる装置の設定が正しいか確認，および「(d) 障害範囲の特定」をしてください。

(iii) 送信パケット数 (DHCPDISCOVER) がカウントアップされ，受信パケット数 (DHCPOFFER) がカウントアップされていない場合は，DHCP サーバとの通信が正常に行われていません。DHCP サーバとなる装置の設定が正しいか確認，および「(d) 障害範囲の特定」をしてください。

(iv) 受信パケットの DHCPNAK パケット数がカウントされている場合は，DHCP サーバ装置からの IP アドレス割付が拒否されています。DHCP サーバとなる装置の設定が正しいか確認，および「(d) 障害範囲の特定」をしてください。

**(c) 構成定義情報の確認**

本装置（DHCP クライアント）上の構成定義設定誤りにより DHCP サーバから IP アドレスが割り振られないという原因が考えられます。次に確認事項を示します。

- **構成定義情報を確認し，インタフェース定義，および指定したオプションが適切であるか確認してください。**

DHCP サーバへの要求オプション (require) については，指定したオプションがすべて DHCP サーバから通知されなければなりません。DHCP サーバ装置でのサポートオプションを確認してください。

DNS サーバアドレスやデフォルトルータのアドレスをサーバより取得する必要がある場合は，構成定義情報 dhcp-client コマンドでデフォルトルータのアドレス取得をサーバに要求するよう，require オプション

で指定する必要があります。デフォルトルータや DNS サーバのアドレスが正常に取得できているかは，dhcp show lease コマンドで確認できます（「(b) 本装置の DHCP クライアント状態確認」を参照)。

**(d) 障害範囲の特定**

本装置の DHCP クライアントインタフェースに対し IP アドレスが割り当てられてなく，本装置にも障害がない場合は，本装置と DHCP サーバ装置間に障害が発生している可能性があります。本装置の HUB やケーブルなどのネットワーク機器の接続の確認（可能なら DHCP サーバ側から ping コマンドを使って障害部位を特定）を実施してください。

### 7.5.3 PPPoE 通信ができない

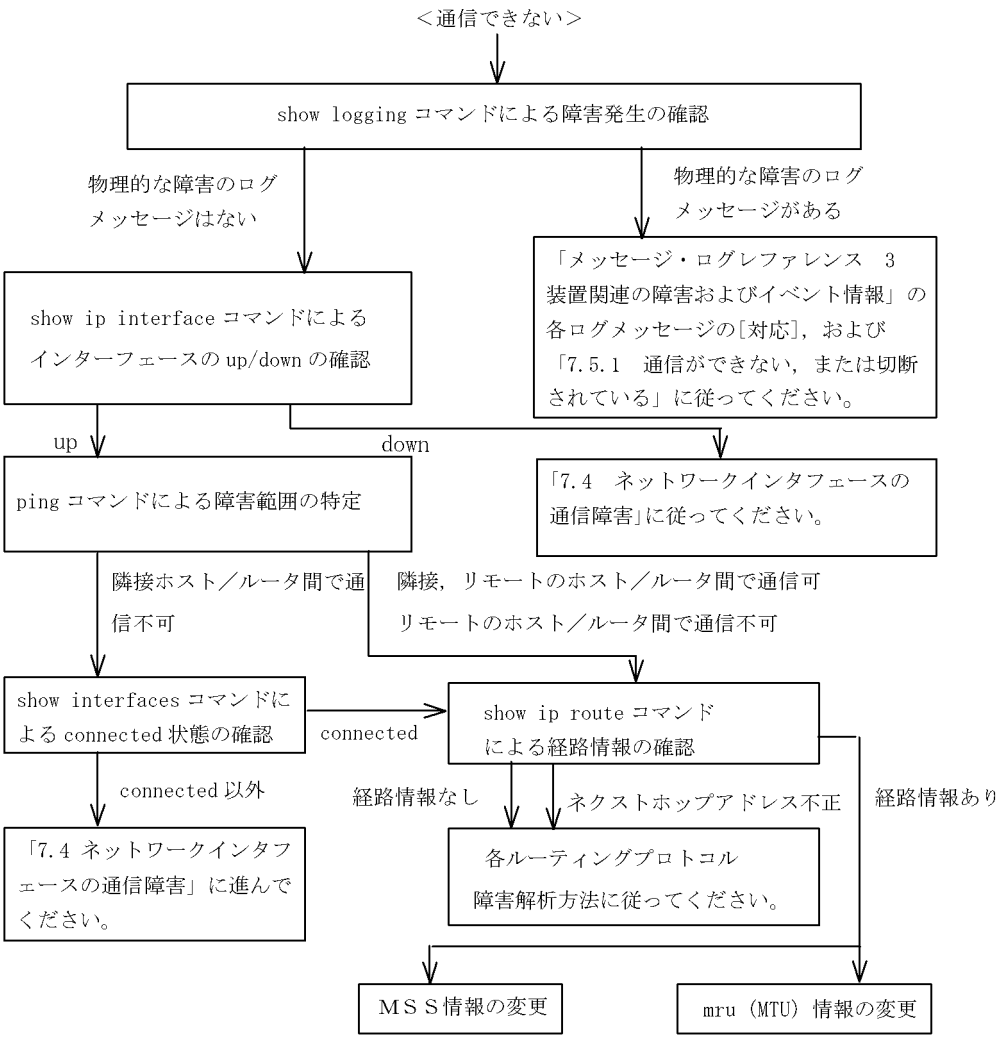
PPPoE の通信トラブルが発生する要因として考えられるのは，主に次の 4 種類があります。

1. ネットワークの構成変更
2. PPPoE に関係する構成定義情報の変更
3. mru（MTU）の設定値
4. mss 情報の設定値

上記 1，2 については，構成定義情報およびネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。

ここでは，クライアントの設定（ネットワークカードの設定，ケーブルの接続など）は確認されているものとし，上記 3，4 の設定値により「通信できない（ある特定の HP にアクセスできなくなる)」というケースについて「mru，mss の設定値が原因となる」障害部位および原因の切り分け手順を説明いたします。

障害部位および原因の切り分け方法は，次のフローにしたがってください。




## (1) ログメッセージおよびインタフェース状態の確認

通信ができなくなる原因として，ハードウェア（RP ／ NIF ／ Line）の障害（または壊れ）や，隣接装置の障害が考えられます。本装置が表示するログメッセージや show ip interface コマンドによるインタフェースの up/down 状態を確認してください。手順については「7.5.1 通信ができない，または切断されている」を参照してください。

注 RP 輻輳発生時の PPPoE セッション切断

RP 輻輳が発生している状態において，PPPoE セッション接続監視用のパケットが廃棄されセッションが切断される場合があります（ただし，構成定義コマンド PPPoE の自動再接続時間（auto_connection）で再接続を行うように設定している場合は，自動で再接続を行います)。この場合，下記のログメッセージが収集されていますのでご注意ください。

＜ログメッセージ＞

```
E4 PPPoE NIF:x LINE:x 00020008 0850 :000000000000 <セッション名>:
Disconnection of PPP session detected via Link Status Monitoring. Check
the line cable connection with modem/ONU and the peer router's status.
```

### (2) 障害範囲の特定（本装置から実施する場合）

本装置に障害がない場合は，通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. ping コマンドを使って通信できない両方の相手との疎通を確認してください。ping コマンドの操作例および実行結果の見方は，「5.2.2　当該宛先アドレスとの通信可否を確認する」を参照してください)。
3. ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使って本装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping コマンド実行の結果，障害範囲が隣接装置の場合は「(4) PPPoE セッション状態の確認」に，リモート先の装置の場合は「(5) 経路情報の確認」に進んでください。

### (3) 障害範囲の特定（お客様の端末装置から実施する場合）

本装置にログインすることができない環境にある場合に，お客様の端末装置から通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. お客様の端末装置に ping 機能があることを確認してください。
2. ping 機能をお使いになり，お客様の端末装置と通信相手との疎通ができるか確認してください。
3. ping 機能で通信相手との疎通が確認できなかったときは，さらに ping コマンドを使ってお客様の端末装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping 機能による障害範囲が特定できましたら，障害と考えられる装置が本装置である場合は本装置にログインしていただき，障害解析フローにしたがって障害原因の調査を行ってください。

### (4) PPPoE セッション状態の確認

本装置のハードウェアは正常に動作している場合でも，本装置と接続している隣接の装置のハードウェアに障害が発生していることも考えられます。

本装置と隣接の装置間の PPPoE セッション状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show interfaces コマンドを使って PPPoE セッション状態を確認してください。該当セッション状態が“ connected ”状態以外のときは，「7.4　ネットワークインタフェースの通信障害」に進んでください。該当セッション状態が“ connected ”状態のときは，「(5) 経路情報の確認」に進んでください。

```
> show interfaces OsakaISP2
2002/04/05 10:56:30
NIF2: active  4-port 10BASE-T/100BASE-TX  retry:0
        Average:0/800Mbps  Peak:150Mbps at 13:53:03
Line0: active up  100BASE-TX full(auto)  00:00:87:a8:c5:1c
        Average out:20Mbps  Average in:10Mbps
PPPoE:OsakaISP2 connected  Session ID:e714  retry:0
        Connected time 02/13 00:00:00  Connecting time 1234:56:30
    Auto connection timer(past/setting):---/10(sec)
        Service Name:OsakaISPservice1
    AC Name:OsakaISP01server
    Destination MAC address  00:00:87:a8:fe:2c
    Source IP address:192.168.100.1  Destination IP address:192.168.35.2
    Primary DNS server IP address:128.10.10.1
    Secondary DNS server IP address:128.10.10.10
                                    ⟩
    CHAP Challenge timeout ：
>
```

Connected になっていること

MACアドレスが取得できていること

## (5) 経路情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない，通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ip route コマンドを使って本装置が取得した経路情報を確認してください。
3. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がない場合やネクストホップアドレスが不正の場合は「7.6　IPv4 ユニキャストルーティングの通信障害」に進んでください。
4. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する項目の調査を行ってください。
   - mru（MTU）
     「(6) mru（MTU）の設定値」に進んでください。
   - MSS
     「(7) mss 情報の設定値」に進んでください。

## (6) mru（MTU）の設定値

PPPoE の構成定義（mru 値）を変更していないにもかかわらず，特定の HP にアクセスできない場合があります。その解決方法として mru（MTU）のサイズ変更をする必要があります。下記にフレッツ・ADSL，B フレッツサービスの通信障害時の例，および mru（MTU）のサイズ変更手順を示します。

例）フレッツ・ADSL ／ B フレッツを含む PPPoE では，MTU が 1454 バイトに，また，一般のイーサネットで使用する MTU は 1500 となっています。

このパケットサイズが整合せずエラーとなり，そのサーバとの間ではコネクションが確立するのに，データは流れないという状況が発生してしまいますので，本装置の mru（MTU）値を調整してお試しください。

mru（MTU）変更の手順

構成定義 show pppoe コマンドで PPPoE 情報の mru の設定値を確認してください。

［実行結果］

```
(config)# show pppoe OsakaISP1
pppoe OsakaISP1
  user_name "user2@osakaisp2"
  password "osakaisp2password"
  authentication_protocol chap
  echo_interval 3600
  mru 1492 ◀── 現状の mru 値
  mss 1414
        :
(config)# pppoe  OsakaISP1
[pppoe OsakaISP1]
(config)# mss 1454 ◀──── 現状設定値より小さい値 を設定する。
[pppoe OsakaISP1]
(config)# exit
[line Department2]
(config)# exit
(config)# exit
# free OsakaISP1 ◀──── 設定情報を有効にするために次のコマンドを入力します。
```

## （7） mss 情報の設定値

PPPoE の構成定義（MSS 値）を変更していないにもかかわらず，特定の HP にアクセスできない場合があります。その理由は，データのサイズが一度に受信できるサイズの上限を上回るために起きる現象です。その解決方法として MSS のサイズ変更をする必要があります。下記に MSS サイズ変更についてと変更手順を示します。

**MSS のサイズ変更について**

イーサネットの MTU は通常 1500 バイトであり，通信（TCP/IP）ヘッダサイズ（40 バイト）＋データサイズ（MSS）になることで MSS は 1460 バイトが要求されます。

[ MSS(1460) = MTU(1500) － 40(TCP/IP ヘッダサイズ ) ]

ところが，WAN 側の PPPoE 回線では PPPoE ヘッダ（8 バイト）が追加されるため，このヘッダデータ分が溢れてしまいフラグメントが発生します。その結果，性能低下や通信経路中に存在するブラックホール・ルータによりパケットが廃棄され，特定のホームページが見られないと言った現象が発生します。これらの問題を解決するために，本装置では上り下りパケットについて MSS のサイズ変更を行わなければなりません。

**MSS 情報の変更手順**

構成定義コマンド show pppoe にて PPPoE 情報の mss の設定値を確認してください。

[ 実行結果 ]

```
(config)# show pppoe OsakaISP1
pppoe OsakaISP1
  user_name  "user2@osakaisp2"
  password  "osakaisp2password"
  authentication_protocol chap
  echo_interval 3600
  mru  1492
  mss  1414  ← 現状の mss 値
       :
(config)# pppoe  OsakaISP1
[pppoe OsakaISP1]
(config)# mss 1408
[pppoe OsakaISP1]
(config)# mss 1
[pppoe OsakaISP1]
(config)# exit
[line Department2]
(config)# exit
(config)# exit
# free OsakaISP1
```

現状設定値より小さい値を設定する。
または auto の設定（1）にする。

設定情報を有効にするために次のコマンドを入力します。

## 7.5.4 NAT，NAPT 通信ができない

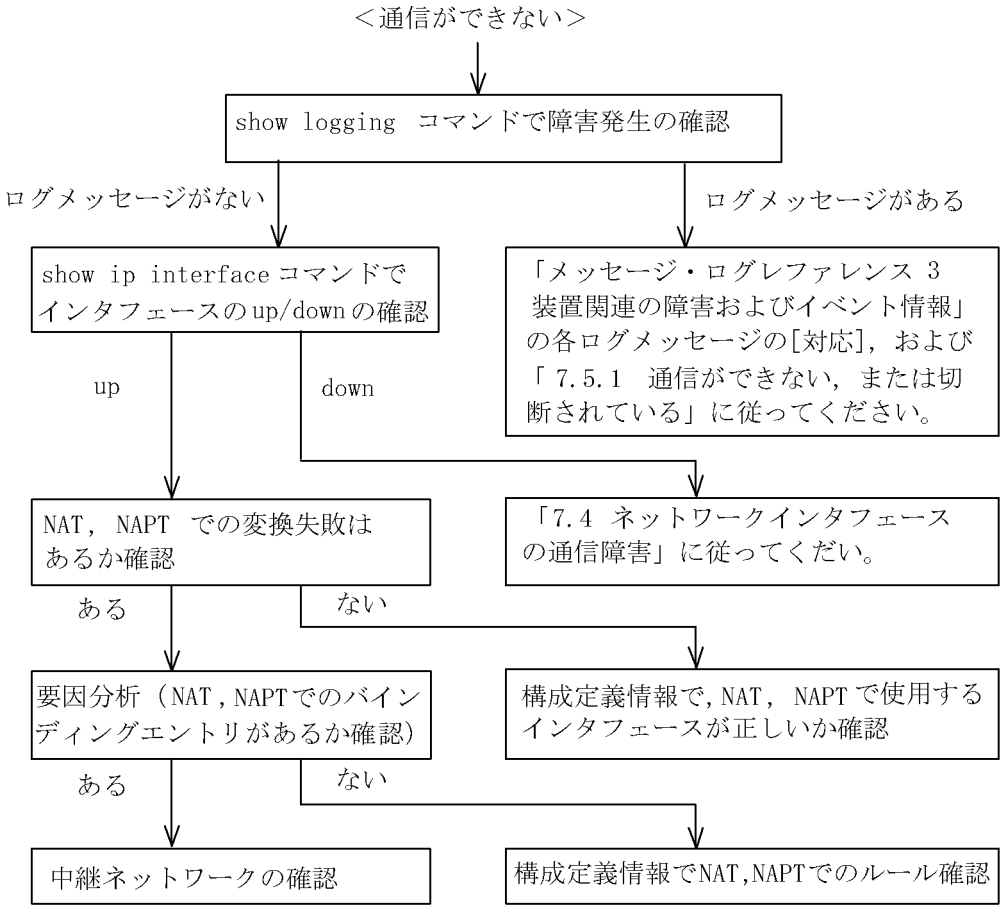
NAT，NAPT の通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. NAT，NAPT に関係する構成定義情報の誤り
2. ネットワークの構成変更
3. 中継ネットワークの障害

上記 2. については，ネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。

本章では，プライベートネットワーク側の設定（ネットワークカードの設定，ケーブルの接続など）は確認されているものとし，上記 1. および 3. に示すような「構成定義情報およびネットワーク構成は正しいのに，IP 通信できない。」，「構成定義情報の変更を行ったら，IP 通信できなくなった。または，IP アドレスおよびポート番号の変換がされなくなった。」，というケースについて，障害部位および原因の切り分け手順を説明いたします。

障害部位および原因の切り分け方法は，次のフローにしたがって行ってください。




## （1） ログメッセージおよびインタフェースの確認

通信ができなくなる原因として，ハードウェア（RP ／ NIF ／ Line）の障害（または壊れ）や，隣接装置の障害が考えられます。本装置が表示するログメッセージや show ip interface コマンドによるインタフェースの up/down 状態を確認してください。手順については「7.5.1 通信ができない，または切断されている」を参照してください。

## （2） NAT，NAPT 変換失敗有無の確認

NAT，NAPT で IP アドレスおよびポートの変換に失敗している可能性があります。show ip nat statistics コマンドで Misses の NAT，NAPT 変換失敗の発生有無を確認してください。カウンタが 0 以外（NAT 変換が失敗）の場合，「(3) NAT，NAPT 変換失敗情報の確認（要因分析)」で原因を調査してください。

```
>show  ip nat statistics
 Translations Packet Count
     In       :       0    Out      :          0
 Binding Table Information
     Added    :       0    Time-Out :          0
     In Use   :       0    Max Use  :          0
     Rules    :       0
 Misses
  Bad Translations :    0   ←0 以外であればNAT，NAPT変換失敗が発生しています。
```

### (3) NAT，NAPT 変換失敗情報の確認（要因分析）

show ip nat translations コマンドで NAT，NAPT 変換失敗情報を確認してください。

```
> show ip nat translations
List of active rules:
isp01 nat 192.168.2.0/24 200.200.2.0/28

List of active sessions:

List of bad translations:
                        Original            Outside             Reason
03/27 18:18:45 TCP  Out  192.168.2.4:1053     203.203.2.2:80      No Pool
```

List of bad translations に NAT，NAPT 変換失敗した情報を表示します。失敗した理由は Reason に表示します。

### (4) 構成定義 NAT，NAPT 使用回線の確認

構成定義コマンドの nat outside_interface や nat inside_interface で設定したインタフェース名に誤りがあると，IP アドレスおよびポート番号の変換ができません。構成定義コマンド show nat で構成定義の内容を確認してください。

```
(config)# show nat
nat outside_interface isp01 nat 192.168.1.0/24 auto   ← この内容をご確認ください。
nat inside_interface local01
```

### (5) バインディングエントリ有無の確認

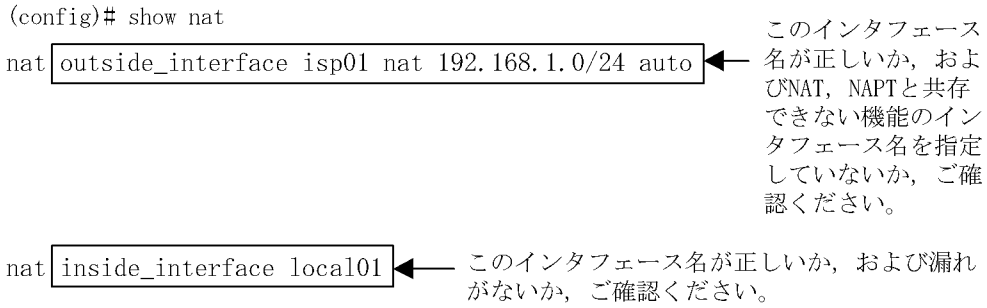
構成定義コマンド nat outside_interface で設定した定義に誤りがあるとバインディングできません。
show ip nat translations コマンドで List of active sessions のバインディングエントリ情報を確認してください。バインディングエントリ情報が表示されない場合，「(6) 構成定義 NAT，NAPT ルールの確認」を参照し，構成定義情報を修正してください。

```
>show ip nat translations
 List of active rules:
 isp01 nat 192.168.2.0/24 200.200.2.0/28

 List of active sessions:
           Original              Translation           Outside
 TCP  Out  192.168.2.1:1053      200.200.2.1:1553      203.203.2.2:80
   Create[ 7m 15s] T.O.[ 2m 45s] Packet[       227,        312] [ESTABLISHED]

 List of bad translations:
```

何も表示されない場合，バインディングエントリが存在しません。

### (6) 構成定義 NAT，NAPT ルールの確認

構成定義 show nat コマンドで構成定義の内容を確認してください。




### (7) 中継ネットワークの確認

中継ネットワークの障害により通信ができなくなっていることが考えられます。手順については「7.5.1 通信ができない，または切断されている」を参照してください。

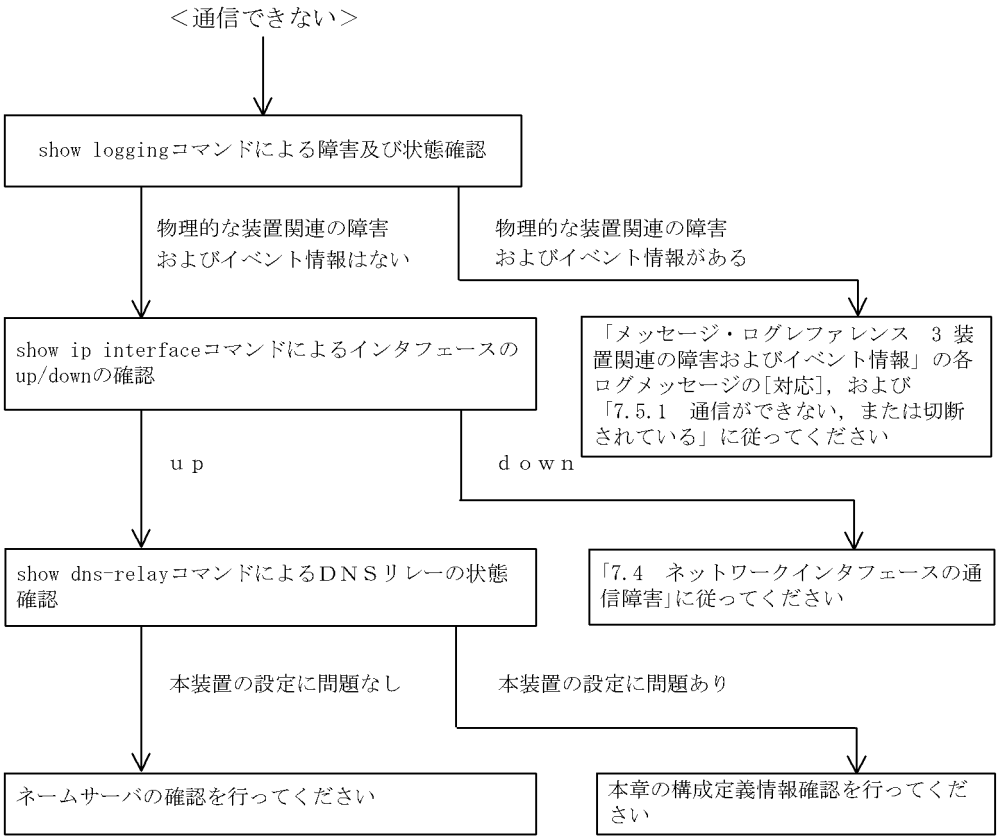
また，PPPoE を使用している場合は「7.5.3　PPPoE 通信ができない」を，DHCP クライアントを使用している場合は「7.5.2　DHCP 機能にて IP アドレスが割り振られない　(3) DHCP クライアントの通信トラブル」を参照してください。

## 7.5.5　DNS リレー通信にてドメイン解決ができない

DNS リレーの通信トラブル（ドメイン解決ができない）の発生要因として考えられるのは，次の 3 種類があります。

1. 構成定義情報の設定誤り
2. 本装置内の障害
3. ネームサーバの障害・設定誤り

本節では，障害部位および原因の切り分け手順を説明いたします。障害部位および原因の切り分け方法は，次のフローにしたがってください。




## (1) ログメッセージおよびインタフェースの確認

通信ができなくなる原因として，ハードウェア（RP ／ NIF ／ Line）の障害（または壊れ）や，隣接装置の障害が考えられます。本装置が表示するログメッセージや show ip interface コマンドによるインタフェースの up/down 状態を確認してください。手順については「7.5.1 通信ができない，または切断されている」を参照してください。

## (2) 本装置の DNS リレー状態確認

### (a) DNS リレーデーモンの起動確認

show dns-relay コマンドにて DNS リレーデーモンから情報が取得できるか確認してください。show dns-relay コマンドの実行結果が次の場合は，構成定義コマンド dns-resolver にてリレー機能を再設定してください。

[実行結果]

```
> show dns-relay
 Can not execute this command.
 No DNS relay configuration.
```

### (b) ネームサーバの設定確認

show dns-relay コマンドにて DNS リレーデーモンが使用しているネームサーバ情報を確認してください。ネームサーバが設定されていない場合は，構成定義情報の確認を参照してください。

```
>show dns-relay
Primary   NameServer: 192.168.0.1
Secondary NameServer: 192.168.0.2
Thirdary  NameServer:  -
 Error Statistics:
 Over max capacity   : 0
 Lack of memory      : 0
 Communication error : 0
 Communication status:
  <source IP address>   <destination IP address>   <status>
```

← ネームサーバのIPアドレス表示を確認してください

なお，ネームサーバを PPPoE セッションで自動取得するように設定している場合は，PPPoE セッション情報で DNS アドレスが取得されているか確認してください。取得されていない場合は，相手サーバ（接続プロバイダ）側で DNS サーバアドレスを通知しないように設定されています。この場合は，接続プロバイダなどにご確認のうえ手動でネームサーバを設定するようにしてください。

```
> show interfaces OsakaISP2
2002/04/05 10:56:30
NIF2: active  4-port 10BASE-T/100BASE-TX  retry:0
        Average:0/800Mbps  Peak:150Mbps at 13:53:03
Line0: active up  100BASE-TX full(auto)  00:00:87:a8:c5:1c
        Average out:20Mbps  Average in:10Mbps
PPPoE:OsakaISP2 connected  Session ID:e714  retry:0
        Connected time 02/13 00:00:00  Connecting time 1234:56:30
        Auto connection timer(past/setting):---/10(sec)
        Service Name:OsakaISPservice1
        AC Name:OsakaISP01server
        Destination MAC address 00:00:87:a8:fe:2c
        Source IP address:192.168.100.1  Destination IP address:192.168.35.2
        Primary DNS server IP address:128.10.10.1
        Secondary DNS server IP address:128.10.10.10
                                ⟆
        CHAP Challenge timeout  :        0
>
```

両方，またはどちらかのアドレスが取得されていること

### (c) DNS リレーの輻輳状態確認

DNS リレーは最大で 2000 個の要求を処理することができます。しかし，その収容条件を超えてしまった場合は DNS リレーにてクライアントへエラー応答を送信してしまいます。この状態に陥った要因を調査する場合は運用コマンドを使用して確認してください。

- 通信異常が発生している場合は，本装置からクライアント，およびネームサーバへのルーティングを確認してください。ネームサーバの確認は本項のネームサーバの確認にしたがってください。
- 最大収容数オーバやメモリ不足が発生している場合は，クライアントからの要求が大量に発生していないか確認してください。
- 通信異常のリトライ処理により最大収容数オーバやメモリ不足が発生する場合もあります。最大収容数オーバやメモリ不足発生時は通信異常時の確認も実施してください。

```
>show dns-relay
 Primary   NameServer: 192.168.0.1
 Secondary NameServer: 192.168.0.2
 Thirdary  NameServer: -
 Error Statistics:
  Over max capacity   : 235   ← 0以外は最大収容数オーバが発生しています。
  Lack of memory      : 125   ← 0以外はメモリー不足が発生しています。
  Communication error : 374   ← 0以外は通信エラーが発生しています。
Communication status:
  <source IP address>   <destination IP address>   <status>
  192.168.253.9         192.168.0.1                inquiry
  192.168.253.9         192.168.0.1                inquiry
  192.168.253.9         192.168.0.1                inquiry
  192.168.253.9         192.168.0.2                retry-inquiry(1)
  192.168.253.9         192.168.0.2                retry-inquiry(1)
        :                     :                          :
        :                     :                          :
```

同一のIPアドレスからの大量アクセスがないかご確認ください。

## (3) 構成定義情報の確認

構成定義情報の誤りによって DNS リレーが通信を行えない可能性があります。次に構成定義情報の確認手順を示します。

### (a) DNS リレー機能の有効設定確認

構成定義コマンド show dns-resolver にて DNS リレー機能が有効になっているか確認してください。

```
>show  dns-resolver
  dns_resolver yes {
   hostname router.mydomain.com;
   nameserver 192.168.0.1  ;
   nameserver 192.168.0.2  ;
   relay yes;   ← yesに設定されていることを確認してください。
  };
```

### (b) ネームサーバの設定確認

ネームサーバが設定されているか確認してください。

```
  >show dns-resolver
   dns_resolver yes {
    hostname router.mydomain.com ;
    nameserver 192.168.0.1;   ← ネームサーバのIPアドレスが設定されていることを
    nameserver 192.168.0.2;      確認してください。
  relay yes;
  };
```

ただし，PPPoE 機能や DHCP クライアント機能を有効に設定してネームサーバの自動取得機能を使用する場合，この限りではありません。その場合，ネームサーバを設定した状態のままにしておくと，自動取

得した情報が DNS リレーに反映されないという問題が発生します。ですので，自動取得したネームサーバ情報を有効にする場合は，構成定義情報のネームサーバ情報を削除してください。

```
>show dns-resolver
 dns_resolver yes {                  ネームサーバのIPアドレスが設定されて
   hostname router.mydomain.com;       いないことを確認
   relay yes;
 };
```

### (4) ネームサーバの確認

本装置に異常が発生していなくても，ネームサーバがダウンしていたり，ルーティングできない IP アドレスが設定されている場合には通信を行うことはできません。ネームサーバに関連する情報の正常性や状態を確認してください。

#### (a) IP アドレスの正常性確認

構成定義コマンド dns-resolver で設定した IP アドレスに間違いがないか再度確認してください。自動取得した IP アドレスの場合は，配布先（PPPoE，DHCP サーバ）の管理者にお問い合わせの上，正常性を確認してください。

#### (b) ネームサーバへのルーティング確認

構成定義コマンド dns-resolver で設定した IP アドレスまたは自動取得した IP アドレスと本装置の間で ping コマンドによる疎通試験を実施して，問題ないことを確認してください。

#### (c) ネームサーバの起動確認

ネームサーバ管理者にお問い合わせください。

## 7.5.6 VRRP 構成にて通信ができない

VRRP 構成にて通信ができない場合は，次の表に示す障害解析方法にしたがって原因の切り分けを行ってください。

**表 7-23 VRRP の障害解析方法**

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| 1 | 同一仮想ルータを構成する相手装置と本装置において仮想ルータの状態を確認し，マスタルータとなっている装置が 1 台でありほかの装置はバックアップになっていることを確認してください。 | 同一仮想ルータを構成する装置間で，マスタ状態となっている装置が 1 台だけであり，そのほかはバックアップとなっている場合には，本装置を含めた通信経路上の装置での経路情報を確認してください。 |
| | | 仮想ルータの状態が正しい場合は項番 2 へ。 |
| 2 | 同一仮想ルータを構成する相手装置と本装置の仮想ルータの状態が，お互いにマスタ状態となっていないことを確認してください。 | 複数の仮想ルータがマスタ状態となっている場合は項番 3 へ。 |
| | | 複数の仮想ルータがマスタ状態となっていない場合は項番 5 へ。 |
| 3 | ping コマンドで，マスタルータ間の通信を実 IPv4 アドレスで確認してください。 | マスタルータ間の実 IPv4 アドレスによる通信ができない場合，仮想ルータを構成するルータ間の物理的なネットワーク構成を確認してください。 |

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| | | マスタルータ間の実 IPv4 アドレスを用いた ping コマンドによる確認ができた場合は項番 4 へ。 |
| 4 | show vrrpstatus detail コマンドにより VRRP の統計情報を確認してください。 | VRRP の受信パケットにエラーが発生している場合は，本装置と相手装置の構成定義情報を再確認してください。 |
| | | VRRP のパケットが正常に受信されている場合は，相手装置を確認してください。受信されていない場合には，ネットワークの物理構成を確認してください。 |
| 5 | 障害監視インタフェース定義がある場合，障害監視インタフェースの状態を確認してください。 | 障害監視インタフェースを定義したインタフェースに別の仮想ルータの定義があり，その仮想ルータの障害監視インタフェースが該当仮想ルータのインタフェースになっていないことを確認してください。なっている場合は，どちらかの障害インタフェースの定義を削除してください。 |
| | | 上記の障害監視インタフェースの定義がない場合は項番 6 へ。 |
| 6 | フィルタの定義で VRRP の Advertisement パケットを廃棄する設定がないことを確認してください。 | 該当するフィルタの定義がある場合，VRRP の Advertisement を廃棄しないようにフィルタの定義を変更してください。 |
| | | フィルタの定義がない場合，同一の仮想ルータを構成する相手装置の動作を確認してください。 |

# 7.6 IPv4 ユニキャストルーティングの通信障害

## 7.6.1 RIP 経路情報がない

本装置が取得した経路情報の表示に，RIP の経路情報が存在しない場合は，次の表に示す障害解析方法にしたがって原因の切り分けを行ってください。

**表 7-24 RIP の障害解析方法**

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| 1 | RIP の隣接情報を表示します。<br>show ip rip gateway | 隣接ルータのインタフェースが表示されていない場合は項番 2 へ。 |
| | | 隣接ルータのインタフェースが表示されている場合は項番 3 へ。 |
| 2 | 構成定義情報で RIP 定義が正しいか確認してください。 | 構成定義情報が正しい場合は項番 3 へ。 |
| | | 構成定義情報が正しくない場合は構成定義情報を修正してください。 |
| 3 | 構成定義情報で経路フィルタリングが正しいか確認してください。 | 構成定義情報が正しい場合は項番 4 へ。 |
| | | 構成定義情報が正しくない場合は構成定義情報を修正してください。 |
| 4 | 隣接ルータが RIP 経路を広告しているか確認してください。 | 広告している場合は該当ルータで障害情報を収集してください。<br>dump protocols ipv4-unicast all ※ |
| | | 広告していない場合は隣接ルータを確認してください。 |

注※

障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。
格納エリア：/primaryMC/usr/var/rtm
ファイル名：rt_trace と rt_dump.gz

## 7.6.2 OSPF 経路情報がない

本装置が取得した経路情報の表示に，OSPF の経路情報が存在しない場合は，次の表に示す障害解析方法にしたがって原因の切り分けを行ってください。

**表 7-25 OSPF の障害解析方法**

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| 1 | OSPF のピア状態を確認します。<br>show ip ospf interface <IP Address> | 隣接ルータの状態が Full 以外の場合は項番 2 へ。 |
| | | 隣接ルータの状態が Full の場合は項番 3 へ。 |
| 2 | 構成定義情報で OSPF の定義が正しいか確認してください。 | 構成定義情報が正しい場合は項番 3 へ。 |
| | | 構成定義情報が正しくない場合は構成定義情報を修正してください。 |
| 3 | OSPF 経路を学習している経路を確認してください。<br>show ip route all-routes | 経路が InActive または存在しない場合には項番 4 へ。 |
| | | 経路が Active の場合は障害情報を収集してください。<br>dump protocols ipv4-unicast all ※ |

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| 4 | 構成定義情報でフィルタリングしていないか確認してください。 | 構成定義情報が正しい場合は項番 5 へ。 |
| | | 構成定義情報が正しくない場合は構成定義情報を修正してください。 |
| 5 | 隣接ルータが OSPF 経路を広告しているか確認してください。 | 広告している場合は該当ルータで障害情報を収集してください。<br>dump protocols ipv4-unicast all ※ |
| | | 広告していない場合は隣接ルータを確認してください。 |

注※

障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。
格納エリア：/primaryMC/usr/var/rtm
ファイル名：rt_trace と rt_dump.gz

## 7.6.3 BGP4 経路情報がない

本装置が取得した経路情報の表示に，BGP4 の経路情報が存在しない場合は，次の表に示す障害解析方法にしたがって原因の切り分けを行ってください。

**表 7-26 BGP4 の障害解析方法**

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| 1 | BGP4 のピア状態を確認します。<br>show ip bgp neighbor | ピア状態が Established 以外の場合は項番 2 へ。 |
| | | ピア状態が Established の場合は項番 3 へ。 |
| 2 | 構成定義情報で BGP4 の定義が正しいか確認してください。 | 構成定義情報が正しい場合は項番 3 へ。 |
| | | 構成定義情報が正しくない場合は構成定義情報を修正してください。 |
| 3 | BGP4 経路を学習しているか確認してください。<br>show ip bgp received-routes | 経路が存在しない場合には項番 4 へ。 |
| | | 経路が存在する場合は障害情報を収集してください。<br>dump protocols ipv4-unicast all ※ |
| 4 | 構成定義情報でフィルタリングしていないか確認してください。 | 構成定義情報が正しい場合は項番 5 へ。 |
| | | 構成定義情報が正しくない場合は構成定義情報を修正してください。 |
| 5 | 隣接ルータが BGP4 経路を広告しているか確認してください。 | 広告している場合は該当ルータで障害情報を収集してください。<br>dump protocols ipv4-unicast all ※ |
| | | 広告していない場合は隣接ルータを確認してください。 |

注※

障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。
格納エリア：/primaryMC/usr/var/rtm
ファイル名：rt_trace と rt_dump.gz

## 7.6.4 IS-IS 経路情報がない

本装置が取得した経路情報の表示に，IS-IS の経路情報が存在しない場合は，次の表に示す障害解析方法にしたがって原因の切り分けを行ってください。

**表 7-27 IS-IS の障害解析方法**

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| 1 | IS-IS の隣接状態を確認します。show isis adjacency | 隣接状態が Up 以外の場合は項番 2 へ。 |
| | | 隣接状態が Up の場合は項番 4 へ。 |
| 2 | 構成定義情報で IS-IS の定義が正しいか確認してください。 | 構成定義情報が正しい場合は項番 3 へ。 |
| | | 構成定義情報が正しくない場合は構成定義を修正してください。 |
| 3 | IS-IS のインタフェース状態を確認します。<br>show isis interface | インタフェース状態が Active の場合は項番 4 へ。 |
| | | インタフェース状態が Passive の場合は IS-IS 未サポートのインタフェースです。 |
| 4 | IS-IS 経路を学習しているか確認してください。<br>show ip route all-routes | 経路が InActive または存在しない場合には項番 5 へ。 |
| | | 経路が Active の場合は障害情報を収集してください。<br>dump protocols unicast all ※ |
| 5 | 構成定義情報でフィルタリングしていないか確認してください。 | 構成定義情報が正しい場合は項番 6 へ。 |
| | | 構成定義情報が正しくない場合は構成定義を修正してください。 |
| 6 | 隣接ルータが IS-IS 経路を広告しているか確認してください。 | 広告している場合は該当ルータで障害情報を収集してください。<br>dump protocols unicast all ※ |
| | | 広告していない場合は隣接ルータを確認してください。 |

注※

障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。

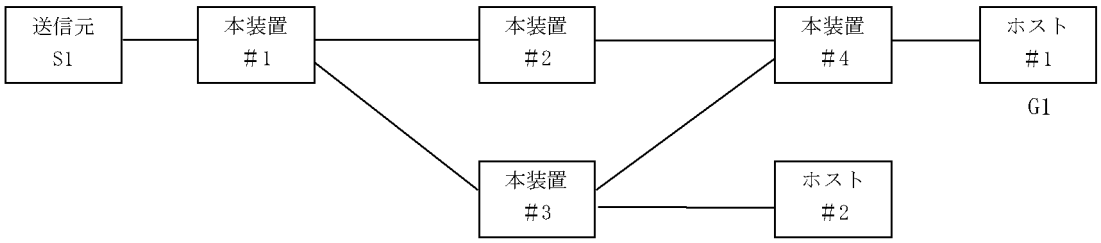
格納エリア：/primaryMC/usr/var/rtm

ファイル名：rt_trace と rt_dump.gz

# 7.7 IPv4 マルチキャストルーティングの通信障害

本装置で IPv4 マルチキャスト通信ができない場合の対処について説明します。

## 7.7.1 PIM-DM ネットワークで通信ができない



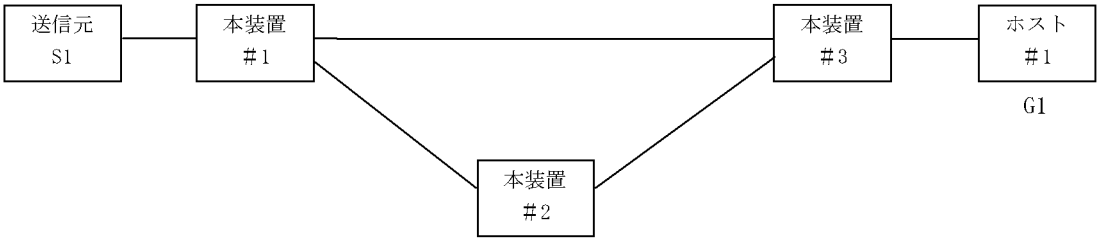

本装置 #2 上の本装置 #4 との IP アドレス < 本装置 #3 上の本装置 #4 との IP アドレス

図に示す IPv4 PIM-DM ネットワークの構成にて，送信元 S1 から G1 宛のパケットがホスト #1 で受信できない場合，次の手順にしたがって対処してください。

1. 本装置 #4 で show ip igmp interface コマンドを実行し，ホスト #1 とのインタフェースが enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
2. 本装置 #4 で show ip igmp groups コマンドを実行し，G1 グループにホスト #1 が参加していることを確認してください。
3. 本装置 #4 で show ip mcache コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，本装置 #3 との PIM-DM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
4. 本装置 #1 で show ip mcache コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，S1 との PIM-DM のインタフェース定義が enable であり，フィルタなどによる抑止定義がないことを確認してください。
5. ルーティングキャッシュの下流が存在しない場合，show ip pim neighbor で本装置 #2 と本装置 #3 が表示されていることを確認してください。
6. 本装置 #3 で show ip mcache コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，本装置 #1 との PIM-DM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
7. ルーティングキャッシュの下流が存在しない場合，show ip pim neighbor で本装置 #1 と本装置 #4 が表示されていることを確認してください。
8. 本装置 #3 で show ip rpf [S1] コマンドを実行し，上流が本装置 #1 へのインタフェース，下流が本装置 #4 へのインタフェースを表示することを確認してください。

## 7.7.2 PIM-SM ネットワークで通信ができない

### (1) PIM-SM ネットワーク

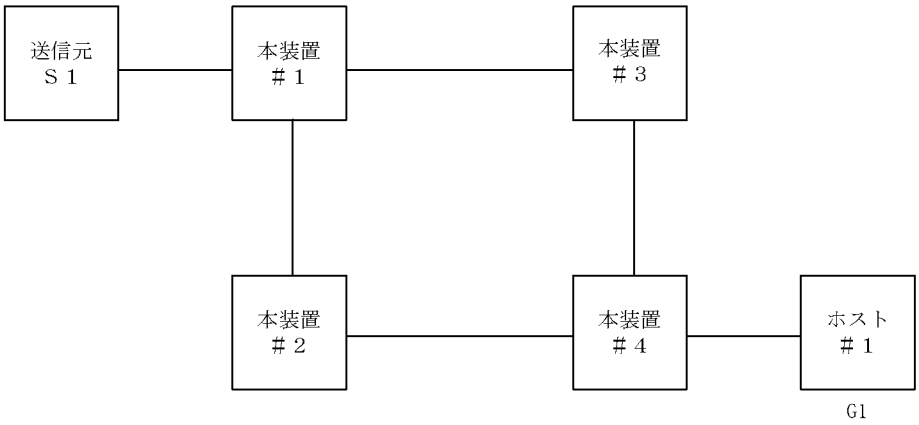



本装置#2 はランデブーポイント及び BSR

図に示す IPv4 PIM-SM ネットワークの構成にて，IPv4 PIM-SM ネットワークで送信元 S1 から G1 宛のパケットがホスト #1 で受信できない場合，次の手順にしたがって対処してください。

1. すべての本装置の構成定義情報に SSM が定義されている場合は，G1 が SSM アドレスでないことを確認してください。
2. 本装置 #3 で show ip igmp interface コマンドを実行し，ホスト #1 とのインタフェースが enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
3. 本装置 #3 で show ip igmp groups コマンドを実行し，G1 グループにホスト #1 が参加していることを確認してください。
4. 本装置 #3 で show ip mroute コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュ（S,G）および G1 へのマルチキャストルーティングキャッシュ（*,G）が存在していることを確認してください。存在しない場合は，本装置と #1 および #2 との PIM-SM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
5. 本装置 #1 で show ip mroute コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，S1 との PIM-SM のインタフェース定義が enable であり，フィルタなどによる抑止定義がないことを確認してください。
6. ルーティングキャッシュの下流が存在しない場合，show ip pim neighbor で本装置 #2 と本装置 #3 が表示されていることを確認してください。また，ルーティングキャッシュが存在しない場合は，show ip pim bsr および show ip pim rendezvous-point mapping を実行し，BSR およびランデブーポイント（RP）が本装置 #2 であることを確認してください。
7. BSR およびランデブーポイント（RP）が存在しないか本装置 #2 でない場合，本装置 #2 で show ip pim bsr および show ip pim rendezvous-point mapping コマンドを実行し，本装置が BSR およびランデブーポイント（RP）であることを確認してください。本装置が BSR およびランデブーポイントでない場合，構成定義情報で BSR およびランデブーポイントの定義が正しいか確認してください。
8. 本装置 #2 で show ip mroute コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュ（S,G）および G1 へのマルチキャストルーティングキャッシュ（*,G）が存在していることを確認してください。存在しない場合は，本装置 #1 および本装置 #3 との PIM-SM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
9. ルーティングキャッシュの下流が存在しない場合，show ip pim neighbor で本装置 #1 と本装置 #3 が表示されていることを確認してください。
10. ルーティングキャッシュが存在しない場合は，本装置 #3 で show ip pim bsr および show ip pim rendezvous-point mapping を実行し，BSR およびランデブーポイント（RP）が本装置 #2 であることを確認してください。

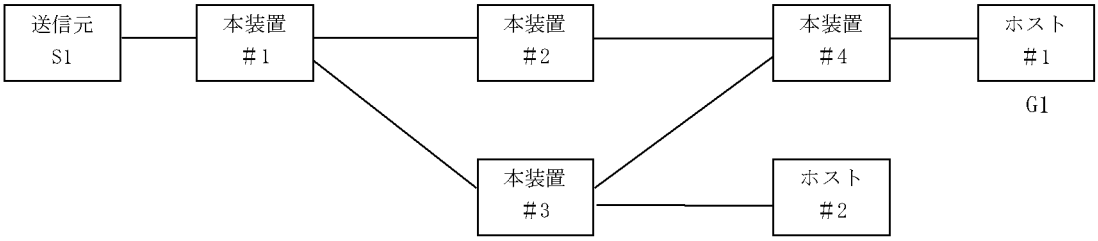
## (2) PIM-SSM ネットワーク




図に示す IPv4 PIM-SSM ネットワークの構成にて，IPv4 PIM-SSM ネットワークで送信元 S1 から G1 宛のパケットがホスト #1 で受信できない場合，次の手順にしたがって対処してください。

1. すべての本装置の構成定義情報に SSM が定義され，G1 が SSM アドレスであることを確認してください。
2. 本装置 #4 で show ip igmp interface コマンドを実行し，ホスト #1 とのインタフェースが enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
3. 本装置 #4 で show ip igmp groups コマンドを実行し，G1 グループにホスト #1 が参加していることを確認してください。
4. 本装置 #4 で ssm-join の構成定義情報に（G1,S1）が定義されていることを確認してください。
5. 本装置 #4 で show ip rpf コマンドを実行し，S1 への経路を認識していることを確認してください（ここでは本装置 # 2 側を上流とします）。
6. 本装置 #4 で show ip mroute コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュ（S1,G1）が存在していることを確認してください。存在する場合は，iif が装置 #2 側のインタフェースで，oif がホスト #1 側のインタフェースである SSM エントリであることを確認してください。存在しない場合は，本装置 #2 との PIM-SM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
7. 本装置 #4 で show ip pim neighbor コマンドを実行し，本装置 #4 が本装置 #2 を認識できていることを確認してください。
8. 本装置 #2 で show ip mroute コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュ（S1,G1）が存在していることを確認してください。存在する場合は，iif が装置 #1 側のインタフェースで，oif が装置 #4 側のインタフェースである SSM エントリであることを確認してください。存在しない場合は，本装置 #4 および本装置 #1 との PIM-SM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
9. 本装置 #2 で show ip pim neighbor コマンドを実行し，本装置 #2 が本装置 #4 および本装置 #1 を認識できていることを確認してください。
10. 本装置 #1 で show ip mroute コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在する場合は，iif が S1 のインタフェースで，oif が装置 #2 側のインタフェースである SSM エントリであることを確認してください。存在しない場合は，S1 との PIM-SM のインタフェース定義が enable であり，フィルタなどによる抑止定義がないことを確認してください。
11. 本装置 #1 で show ip pim neighbor コマンドを実行し，本装置 #1 が本装置 #2 を認識できていることを確認してください。

## 7.7.3 DVMRP ネットワークで通信ができない




本装置 #2 上の本装置 #4 との IP アドレス < 本装置 #3 上の本装置 #4 との IP アドレス

図に示す IPv4 DVMRP ネットワークの構成にて，送信元 S1 から G1 宛のパケットがホスト #1 で受信できない場合，次の手順にしたがって対処してください。

1. 本装置 #4 で show ip igmp interface コマンドを実行し，ホスト #1 とのインタフェースで IGMP と DVMRP のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。IGMP だけの定義では動作しません。
2. 本装置 #4 で show ip igmp groups コマンドを実行し，G1 グループにホスト #1 が参加していることを確認してください。
3. 本装置 #4 で show ip mcache コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，本装置 #2 との DVMRP のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
4. 本装置 #1 で show ip mcache コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，S1 との DVMRP のインタフェース定義が enable であり，フィルタなどによる抑止定義がないことを確認してください。
5. ルーティングキャッシュの下流が存在しない場合，ip show dvmrp neighbor で本装置 #2 と本装置 #3 が表示されていることを確認してください。
6. show ip dvmrp route [S1] コマンドを実行し，本装置 #2 か本装置 #3 へのルートが存在することを確認してください。ここで，本装置 #3 だけが表示された場合は本装置 #2 と本装置 #4 のインタフェースが障害でないか確認してください。
7. 本装置 #2 で show ip mcache コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，本装置 #1 との DVMRP のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
8. ルーティングキャッシュの下流が存在しない場合，show ip dvmrp neighbor で本装置 #1 と本装置 #4 が表示されていることを確認してください。
9. 本装置 #2 で show ip dvmrp route [S1] コマンドを実行し，上流が本装置 #1 へのインタフェース，下流が本装置 #4 へのインタフェースを表示することを確認してください。

# 7.8 IPv6 ネットワークの通信障害

## 7.8.1 通信ができない，または切断されている

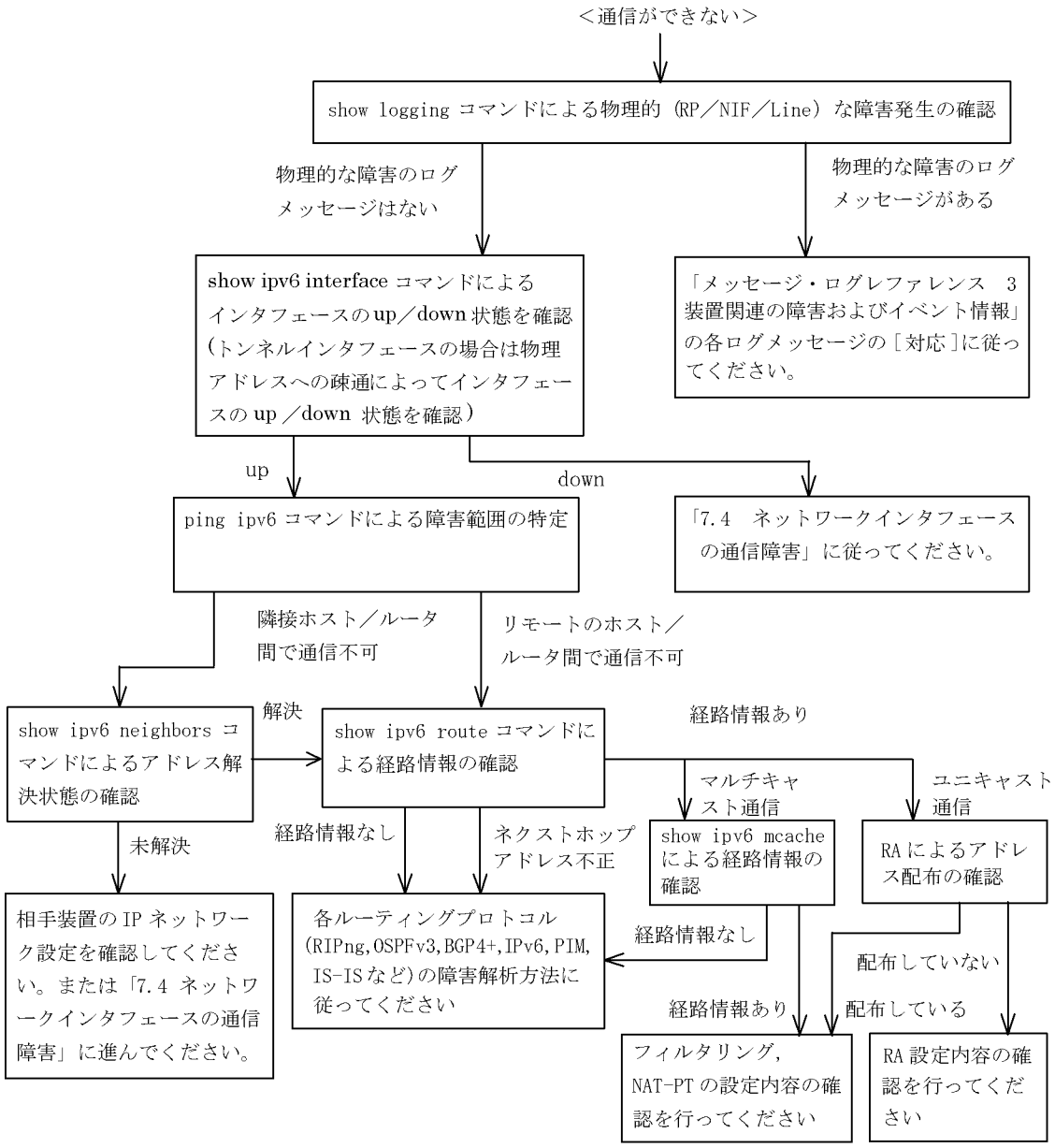
本装置を使用している IPv6 ネットワーク上で，通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. IPv6 通信に関係する構成定義情報の変更
2. ネットワークの構成変更
3. ネットワークを構成する機器の障害

上記 1. および 2. については，構成定義情報およびネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないかご確認ください。

ここでは，3. に示すように「構成定義情報およびネットワーク構成は正しいのに IPv6 通信ができない」，「これまで正常に動いていたのに IPv6 通信ができなくなった」というケースを中心に，障害部位および原因の切り分け手順を説明いたします。

障害部位および原因の切り分け方法は，次のフローにしたがってください。




## (1) ログメッセージおよびインタフェースの確認

通信ができなくなる原因として，ハードウェア（RP ／ NIF ／ Line）の障害（または壊れ）や，隣接装置の障害が考えられます。本装置が表示するログメッセージや show ipv6 interface コマンドによるインタフェースの up/down 状態を確認してください。手順については，「7.5.1 通信ができない，または切断されている」を参照してください。

## (2) 障害範囲の特定（本装置から実施する場合）

本装置に障害がない場合は，通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. 本装置にログインします。

2. ping ipv6 コマンドを使って通信できない両方の相手との疎通を確認してください。ping ipv6 コマンドの操作例および実行結果の見方は，「5.5.2　当該宛先アドレスとの通信可否を確認する」を参照してください)。
3. ping ipv6 コマンドで通信相手との疎通が確認できなかった場合は，さらに ping ipv6 コマンドを使って本装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping ipv6 コマンド実行の結果，障害範囲が隣接装置の場合は「(4) 隣接装置との NDP 解決情報の確認」に，リモート先の装置の場合は「(5) ユニキャストインタフェース情報の確認」に進んでください。

### (3) 障害範囲の特定（お客様の端末装置から実施する場合）

本装置にログインすることができない環境にある場合に，お客様の端末装置から通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. お客様の端末装置に ping ipv6 機能があることをご確認ください。
2. ping ipv6 機能をお使いになり，お客様の端末装置と通信相手との疎通ができるか確認してください。
3. ping ipv6 機能で通信相手との疎通が確認できなかった場合は，さらに ping ipv6 コマンドを使ってお客様の端末装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping ipv6 機能による障害範囲が特定できましたら，障害と考えられる装置が本装置である場合は本装置にログインしていただき，障害解析フローにしたがって障害原因の調査を行ってください。

### (4) 隣接装置との NDP 解決情報の確認

ping ipv6 コマンドの実行結果によって隣接装置との疎通が不可の場合は，NDP によるアドレスが解決していないことが考えられます。本装置と隣接装置間のアドレス解決状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ipv6 neighbors コマンドを使って隣接装置間とのアドレス解決状態（NDP エントリ情報の有無）を確認してください。
3. 隣接装置間とのアドレスが解決している（NDP エントリ情報有り）場合は，「(5) ユニキャストインタフェース情報の確認」に進んでください。
4. 隣接装置間とのアドレスが解決していない（NDP エントリ情報無し）場合は，隣接装置と本装置の IP ネットワーク設定が一致しているかを確認してください。

### (5) ユニキャストインタフェース情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない場合や，IPv6 ユニキャスト通信で通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ipv6 route コマンドを実行して，本装置が取得した経路情報を確認してください。
3. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がない場合やネクストホップアドレスが不正の場合は「7.9　IPv6 ユニキャストルーティングの通信障害」に進んでください。
4. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。
   - マルチキャスト通信
     「(6) マルチキャストインタフェース情報の確認」に進んでください。
   - RA 機能
     「(8) RA 設定情報の確認」に進んでください。

- トンネルインタフェース
  「(11) トンネルインタフェース設定情報の確認」に進んでください
- NAT-PT
  「7.8.5 NAT-PT 通信ができない」に進んでください。

## (6) マルチキャストインタフェース情報の確認

IPv6 マルチキャストパケットを受信しているにもかかわらず経路情報が存在しない場合は，本装置が取得している隣接情報や MLD グループ情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. 次の表に示すコマンドを使って本装置が取得している隣接情報および MLD グループ情報を確認してください。これらのコマンドの詳細は「運用コマンドレファレンス Vol.2 6. IPv6 マルチキャストルーティングプロトコル情報」を参照してください。また，マルチキャストルーティングのプロトコル別の確認方法は，「7.10 IPv6 マルチキャストルーティングの通信障害」を参照してください。

**表 7-28 IPv6 PIM 動作時のコマンド**

| 項番 | コマンド | 確認内容 |
|---|---|---|
| 1 | show ipv6 pim interface | IPv6 PIM インタフェースが動作していること |
| 2 | show ipv6 pim neighbor | 近隣の IPv6 PIM ルータが存在していること |
| 3 | show ipv6 rpf <IPv6 Address> | IPv6 マルチキャストデータ送信元に対する RPF が存在していること |
| 4 | show ipv6 mld interface | MLD インタフェースが動作していること |
| 5 | show ipv6 mld group | 参加している MLD グループが認識されていること |
| 6 | show ipv6 pim bsr | IPv6 PIM-SM の BSR 情報を保持していること |
| 7 | show ipv6 pim rendezvous-point mapping | IPv6 PIM-SM のランデブーポイント情報を保持していること |
| 8 | show ipv6 pim rendezvous-point-hash<IPv6 Address> | 当該 IPv6 アドレス（グループアドレス）に対するランデブーポイントが存在していること |
| 9 | show ipv6 mroute | IPv6 PIM-SM のルート情報を保持していること |

3. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。
   - フィルタリング／ QoS 機能
     「(7) フィルタリング／ QoS 設定情報の確認」に進んでください。

## (7) フィルタリング／ QoS 設定情報の確認

本装置において，物理的障害がなく，経路情報も正しく設定されているにもかかわらず通信ができない場合は，フィルタリング機能により特定のパケットだけを廃棄する設定になっているか，QoS 機能の帯域制御または優先廃棄制御によりパケットが廃棄されている可能性があります。

したがって，構成定義情報のフィルタリング機能および QoS 機能の設定条件が正しいか，システムの構築において帯域制御ならびに優先廃棄制御がシステム運用において適切であるか見直してください。手順については，「7.5.1 通信ができない，または切断されている (8) フィルタリング／ QoS 設定情報の確認」を参照してください。

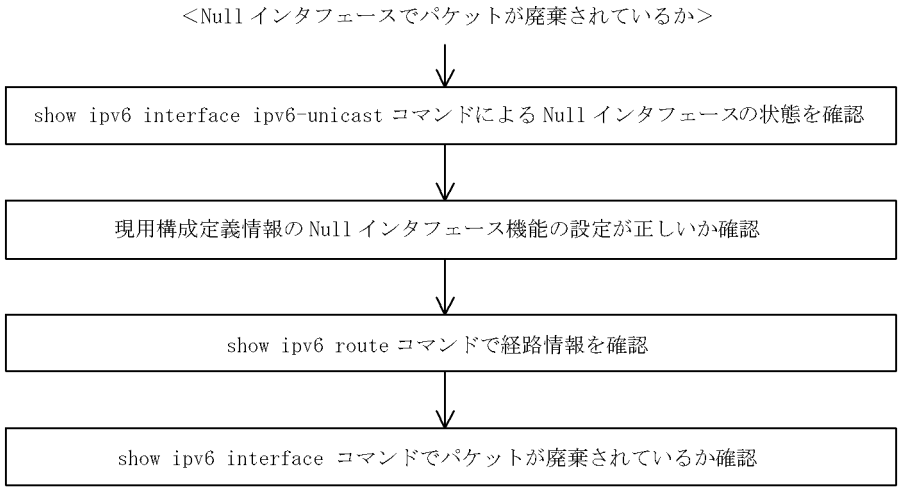
### (8) RA 設定情報の確認

本装置と本装置に直接接続されている端末との間で通信ができない場合は，RA によるアドレス情報配布が正常に行われていない可能性が考えられます。したがって，構成定義情報の RA 機能の設定が正しいか確認してください。手順については「5.6.6　IPv6 アドレス情報が正しく配布されているかを確認する」を参照してください。IPv6 アドレス情報が正しく配布されていた場合，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。

- フィルタリング／ QoS 機能
  「(7) フィルタリング／ QoS 設定情報の確認」を参照してください。
- Tag-VLAN 連携機能
  「(10) Tag-VLAN 連携設定情報の確認」に進んでください。

### (9) Null インタフェース設定情報の確認

特定のネットワーク宛または特定の端末宛の通信を Null インタフェースに向けて制限しているにもかかわらず，パケットが廃棄されない場合は，Null インタフェースの設定内容に誤りがある可能性があります。次の手順で Null インタフェースの設定内容が正しいか確認してください。




1. show ipv6 interface ipv6-unicast コマンドを使い Null インタフェースの状態を確認します。Null インタフェースが UP しているか確認してください。
2. 現用構成定義情報で Null インタフェースが定義されているか確認します。
3. show ipv6 route コマンドで経路情報を確認します。
   static コマンドで定義した経路情報の設定内容が正しいか確認してください。
4. パケットが廃棄されているか確認します。
   show ip interface コマンドを使って Null インタフェースでパケットが廃棄されているか確認してください。

### (10) Tag-VLAN 連携設定情報の確認

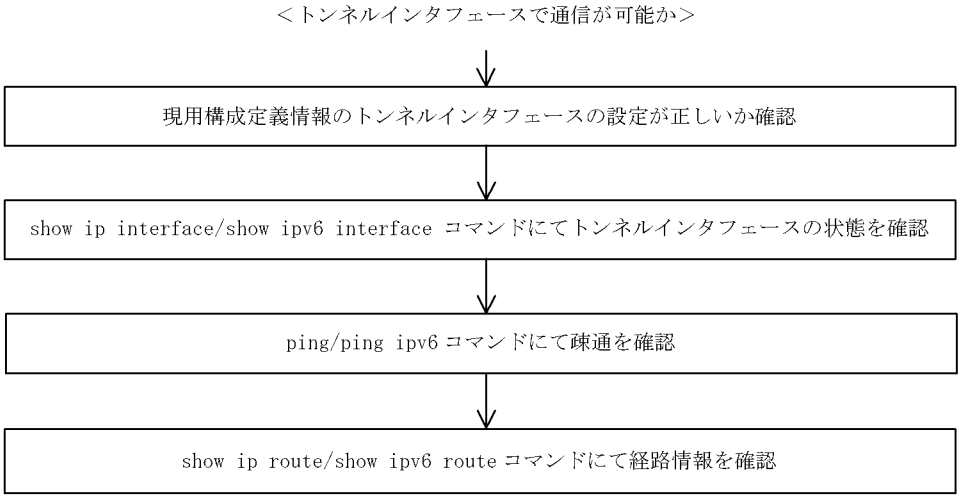
本装置に，IP インタフェース情報，経路情報が正しく設定されているにもかかわらず通信ができない場合は，Tag-VLAN 連携情報の設定が誤っている（またはされていない）ために，パケットが廃棄されている可能性が考えられます。本装置の Tag-VLAN 連携設定情報を確認する手順を次に示します。

1. 本装置にログインします。
2. show interfaces コマンドを使用して Tag-VLAN 連携設定情報（VLAN エントリ情報の有無，VLAN ID）を確認してください。
3. Tag-VLAN 連携設定情報が正しい（VLAN エントリ情報有り，正しい VLAN ID）場合は，show interfaces コマンドを使用して Tag-VLAN 連携設定情報（VLAN 設定の有無）を確認してください。
4. スタティック NDP の設定をした場合は，show ipv6 neighbors コマンドを使用して NDP エントリに関する Tag-VLAN 連携設定情報（VLAN ID）を確認してください。

上記コマンドで Tag-VLAN 連携の設定が正しいと確認できた場合は，本装置に関する Tag-VLAN 連携の設定に問題はありません。接続装置（LAN Switch など）の設定に問題（VLAN 設定をしていない，VLAN ID が一致していない）がある可能性がありますので，接続装置の設定情報を確認してください。

## （11）トンネルインタフェース設定情報の確認

本装置にトンネルインタフェースを設定している状態で，特定のネットワーク宛または特定の端末宛の通信ができない場合，トンネルインタフェースの設定内容／ネットワーク構成に誤りがある可能性があります。次の手順でトンネルインタフェースの設定内容／ネットワーク構成が正しいか確認してください。




1. 構成定義情報でトンネルインタフェースの定義を確認します。
   - 構成定義コマンド tunnel（「構成定義コマンドレファレンス Vol.1　tunnel（トンネル情報）」を参照）で設定したトンネル情報のアドレスが，本装置のトンネルインタフェース以外のインタフェースに設定されていることを確認してください。アドレスが間違っている場合，正しいアドレスに変更してください。
   - トンネル情報に設定したアドレスと，構成定義コマンド ip でトンネルインタフェースに設定したアドレスのプロトコルが同一でないことを確認してください。同一の場合は，正しいアドレスに変更してください。
2. show ipv6 interface コマンドを使用して，トンネルインタフェースの状態を確認します。
   - 表示結果の physical address で示すアドレスが，本装置のトンネルインタフェース以外のインタフェースに設定されているアドレスであることを確認してください。アドレスが間違っている場合には，正しいアドレスに変更してください。
   - 表示結果の physical address で示すアドレスが設定されているインタフェースの状態が，UP しているか確認してください。状態が UP となっていない場合は，当該インタフェースの障害と考えられま

す。「7.5.1　通信ができない，または切断されている」または「7.8.1　通信ができない，または切断されている」を参照してください。

3. トンネル情報で設定した自アドレス・宛先アドレスに対して，本装置および接続先装置より ping，ping ipv6 コマンドを使用して到達性を確認します。
   - どちらの装置からも到達性がない場合は，経路情報に問題があると考えられます。「7.5.1　通信ができない，または切断されている」または「7.8.1　通信ができない，または切断されている」を参照してください。
   - 一方の装置から到達性がない場合は，中継経路間にアドレス変換装置がないかネットワーク構成を確認してください。アドレス変換装置を使用している場合は禁止構成に該当しますので，トンネルを設定する中継経路間にアドレス変換装置を設置しないようにネットワーク構成を変更してください（禁止構成については「解説書 Vol.1　14.11.4 トンネル機能使用時の注意事項」を参照してください）。
4. ネットワーク構成を確認します。
   - トンネルインタフェースに設定した接続先アドレスの到達経路を，show netstat routing-table numeric コマンドを使用して確認してください。経路の中継先が，本装置の別のトンネルインタフェースであった場合，禁止構成である多重トンネルとなっていることが考えられます。経路制御の設定を変更して，トンネルインタフェース以外が中継先となるように変更してください（禁止構成については「解説書 Vol.1　14.11.4 トンネル機能使用時の注意事項」を参照してください）。

## 7.8.2　IPv6 DHCP に関するトラブルシューティング

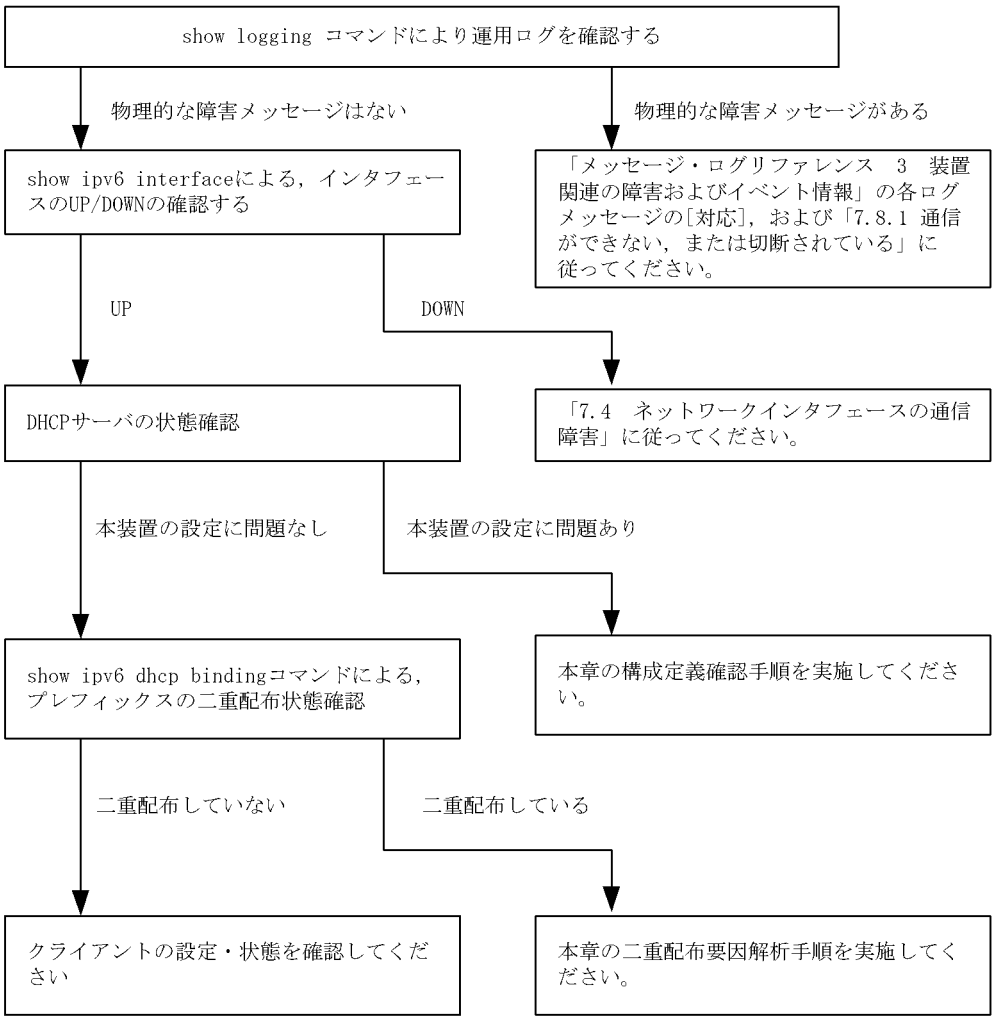
### (1) コンフィグレーション情報が配布されない

本装置 DHCP サーバのプレフィックス配布機能を使用するにあたり，サービスが正常に動作しない原因としては，以下の 5 点が考えられます。

1. プレフィックス配布定義数に対して，クライアント数が多い。
2. クライアント DUID（DHCP Unique Identifier）の指定を誤っている。
3. dhcp6-server interface 定義を誤っている。
4. DHCP 運用中の障害
5. その他の障害

上記は，以下の手順をもって障害個所を切り分け，確認することができます。

**図 7-10　DHCP サーバの障害解析手順**




### (a) ログメッセージおよびインタフェースの確認

通信ができなくなる原因として，ハードウェア (RP ／ NIF ／ Line) の障害 ( または壊れ ) や，隣接装置の障害が考えられます。本装置が表示するログメッセージや，show ipv6 interface コマンドによるインタフェースの up/down 状態を確認してください。手順については「7.5.1　通信ができない，または切断されている」を参照してください。

### (b) 本装置の DHCP サーバ状態確認

1. DHCP サーバサービスの起動確認
   show ipv6 dhcp server statistics コマンドで，DHCP サーバデーモンから情報が取得できるか確認してください。show ipv6 dhcp server statistics コマンドの実行結果が下記の場合は，構成定義コマンド dhcp6-server にて DHCP サーバ機能を再設定してください。

   [ 実行結果 ]

   ```
   > show ipv6 dhcp server statistics
   > < show binding>: dhcp6_server doesn't seem to be running.
   ```

2. 配布可能なプレフィックスの残数を確認する
   show ipv6 dhcp server statistics コマンドで，DHCP サーバがあといくつプレフィックスを配布できる

かを確認してください。確認手順は「5.5.8　IPv6 DHCP サーバ機能を確認する（2）運用中の確認」を実施してください。確認の結果，配布可能なプレフィックス数が 0 である場合は配布するプレフィックス数を増やしてください。なお，配布可能なプレフィックス数の上限は 200 です。

**(c) 構成定義確認手順**

1. DHCP サーバ機能の有効設定の確認
   構成定義コマンド show dhcp6-server コマンドで，DHCP サーバ定義が有効になっているかを確認してください。実行結果で示す下線部が，no ではなく yes であれば，定義は有効です。

   [ 実行結果 ]

```
(config)# show dhcp6-server
dhcp6-server yes
!
(config)#
```

2. インタフェース (dhcp6-server interface) 定義を確認する
   構成定義コマンド show dhcp6-server interface コマンドで，DHCP サーバインタフェース定義の有無を確認してください。定義が無い場合は追加してください。定義がある場合は，定義しているインタフェースが，クライアント接続ネットワーク向けの定義であるかを確認してください。

   [ 実行結果 ]

```
(config)# show dhcp6-server interface
dhcp6-server yes
dhcp6-server interface TokyoOsaka preference 100
!
(config)#
```

3. ホスト (dhcp6-server host) 定義を確認する
   構成定義コマンド show dhcp6-server host コマンドにて，DHCP サーバで配布しようとしているプレフィックス配布定義の有無を確認してください。定義が無い場合は追加してください。定義がある場合は，配布するプレフィックスを指定する prefix ／ range の設定値，配布クライアントを決める duid の定義有無，ならびに duid に指定したクライアント DUID の値が正しいかを確認してください。

   [ 実行結果 ]

```
(config)# show dhcp6-server host Tokyo1
dhcp6-server yes
dhcp6-server host Tokyo1 duid any
   range 3ffe:ffff:1111::/48 3ffe:ffff:1112::/48;
!
(config)#
```

4. ホストターゲット (dhcp6-server host-target) の確認
   本装置 DHCP サーバは，構成定義コマンド dhcp6-server interface の host-target にホスト定義名を指定することで，クライアントが接続されるネットワークを制限することができます。そのため，host-target を指定するインタフェースを誤ると，その他のインタフェースで目的のクライアントから要求を受信した場合に，要求を廃棄します。DHCP サーバの構成定義を見直し，host-target を指定しているインタフェースや，指定しているホスト定義名の指定が正しいかどうかの確認を行ってください。

   [ 実行結果 ]

```
(config)# show dhcp6-server interface
dhcp6-server yes
dhcp6-server interface TokyoOsaka preference 100 host-target tokyo
host-target osaka
!
(config)#
```

**(d) クライアントによる二重取得**

1. binding 情報の確認

show ipv6 dhcp binding detail コマンドにより，同一 DUID に対してプレフィックスが二重で配布されていないかを確認します。以下に表示例を示します。

[ 実行結果 ]

```
> show ipv6 dhcp binding detail
<Prefix>             <Lease expiration>  <Type>
  <DUID>
3ffe:1234:5678::/48      03/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48      03/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
>
```

下線で示すように，同一 DUID が 2 個以上存在する場合は，プレフィックス情報を不当に取得しているクライアントである可能性があります。各クライアントを確認し，配布を受けたプレフィックス値を確認してください。

2. 配布済みプレフィックスとクライアントの対応を取る
   show ipv6 dhcp binding detail の結果において，プレフィックスを二重取得しているクライアントが見つからない場合は，表示される DUID とクライアント装置の対応を取る手順が必要となります。対応付けは，binding 情報に示される「配布済みプレフィックスの値」と「クライアント装置が配布を受けたプレフィックスの情報」を比較することで確認してください。

#### (e) クライアントの設定状態を確認する

クライアントの設定状態を確認する場合は，クライアント付属のマニュアルにしたがってください。

#### (f) 二重配布からの回復手順

本装置 DHCP サーバで，同一クライアントへプレフィックスを二重配布したことを確認した場合は，表示される DUID とクライアントの対応から，現在未使用のプレフィックスを調査してください。現在未使用のプレフィックスについては，運用コマンド clear ipv6 dhcp binding < 未使用プレフィックス > によって，binding 情報を削除してください。

[ 実行結果 ]

```
> show ipv6 dhcp binding detail
<Prefix>             <Lease expiration>  <Type>
  <DUID>
3ffe:1234:5678::/48      03/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48      03/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
> clear ipv6 dhcp binding detail 3ffe:1234:5678::/48
> show ipv6 dhcp binding detail
<Prefix>             <Lease expiration>  <Type>
  <DUID>
3ffe:aaaa:1234::/48      03/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
>
```

### (2) プレフィックス配布先への通信ができない

本装置 DHCP サーバのプレフィックス配布先への自動経路情報設定機能を利用する場合，経路情報が設定されない要因は以下の三つがあります。

1. 構成定義済みだが，未配布である。
2. 自動経路情報設定に関連する機能に影響がある操作，またはイベントが発生した。
3. 本装置 DHCP サーバ機能が再起動した。

上記は経路情報を確認する運用コマンド show ipv6 route -s の結果と show ipv6 dhcp server binding での配布済みプレフィックス情報を比較することで切り分けることができます。

**表 7-29 プレフィックス配布先への経路情報関連障害切り分け**

| 条件 | | 発生要因 |
|---|---|---|
| binding 情報 | 経路情報 | |
| 有 | 経路有 | 該当なし。正常運用状態。 |
| 有 | 経路無 | 要因 4 |
| 無 | 経路有 | 要因 3 |
| 無 | 経路無 | 要因 1，2 |

プレフィックス配布先への経路情報の保有性については，次の表に示す制限があります。

**表 7-30 プレフィックス配布先への経路情報の保有性**

| 保有情報 | 発生イベントと保有性 | | | |
|---|---|---|---|---|
| | サーバ機能<br>再起動 | ルーティングマネージャ<br>再起動 | 本装置<br>再起動 | RM 二重化<br>切り替え |
| クライアントへの<br>経路情報 | ○ | ○ | × | × |

（凡例）
○：保護される
×：削除される（再設定要）

注
プレフィックス配布先への経路情報設定を行う際に必要な経路管理機能

なお，その他の障害については，「7.8.1 通信ができない，または切断されている」を参照してください。

#### (a) 経路情報の確認

本装置 DHCP サーバのプレフィックス配布先への自動経路設定機能を利用する場合，プレフィックス配布後の経路情報は，経路情報を確認する運用コマンド show ipv6 route -s で確認できます。

**図 7-11 運用コマンドによる経路情報の確認**

```
> show ipv6 route -s
Total: 10routes
Destination             Next Hop      Interface        Metric  Protocol  Age
3ffe:1234:5678::/48     ::1           tokyo            0/0      Static   45m
        <Active Gateway Dhcp>
3ffe:aaaa:1234::/48     ::1           osaka            0/0      Static   23m
        <Active Gateway Dhcp>
:
>
```

#### (b) 経路情報の再設定を行う

本装置 DHCP サーバのプレフィックス配布先への自動経路設定機能を利用する場合，障害等で経路情報がクリアされるイベントが発生したとき，その復旧にはプレフィックスの再配布が必要です。クライアント装置で，プレフィックス情報を再取得する操作を行ってください。

### (3) 本装置 DUID が他装置と重複した場合

本装置を含む DHCP サーバを同一ネットワーク上で 2 台以上運用する構成で，DUID が重複する場合は，下記手順にて本装置の DUID を再設定してください。

#### (a) DUID 情報保存ファイルを削除する

本装置 DUID は /primaryMC/usr/var/dhcp6/dhcp6s_duid に保存されています。運用コマンドラインより，rm コマンドを使用し，明示的に削除願います。

#### (b) DUID を再生成させる

DUID ファイルを削除後は，運用コマンド restart ipv6 dhcp server によって再起動させるか，構成定義へ DHCPv6 サーバ定義を追加してください。本装置 DHCP サーバは起動時に DHCP インタフェースとして使用する ipv6 インタフェースの MAC アドレスを取得し，これと時刻情報を基に新たに生成します。

#### (c) DUID の確認

運用コマンド show ipv6 dhcp server statistics によって確認できます。詳細は「5.5.8　IPv6 DHCP サーバ機能を確認する　(4) DUID(DHCP Unique Identifier) について」を参照してください。

## 7.8.3　VRRP 構成にて通信ができない

VRRP 構成にて通信ができない場合は，次の表に示す障害解析方法にしたがって原因の切り分けを行ってください。

**表 7-31　VRRP の障害解析方法**

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| 1 | 同一仮想ルータを構成する相手装置と本装置において仮想ルータの状態を確認し，マスタルータとなっている装置が 1 台でありほかの装置はバックアップになっていることを確認してください。 | 同一仮想ルータを構成する装置間で，マスタ状態となっている装置が 1 台だけであり，そのほかはバックアップとなっている場合には，本装置を含めた通信経路上の装置での経路情報を確認してください。 |
| | | 仮想ルータの状態が正しい場合は項番 2 へ。 |
| 2 | 同一仮想ルータを構成する相手装置と本装置の仮想ルータの状態が，お互いにマスタ状態となっていないことを確認してください。 | 複数の仮想ルータがマスタ状態となっている場合は項番 3 へ。 |
| | | 複数の仮想ルータがマスタ状態となっていない場合は項番 5 へ。 |
| 3 | ping ipv6 コマンドで，マスタルータ間の通信を実 IPv6 アドレスで確認してください。 | マスタルータ間の実 IPv6 アドレスによる通信ができない場合，仮想ルータを構成するルータ間の物理的なネットワーク構成を確認してください。 |
| | | マスタルータ間の実 IPv6 アドレスを用いた ping ipv6 コマンドによる確認ができた場合は項番 4 へ。 |
| 4 | show vrrpstatus detail コマンドにより VRRP の統計情報を確認してください。 | VRRP の受信パケットにエラーが発生している場合は，本装置と相手装置の構成定義情報を再確認してください。 |
| | | VRRP のパケットが正常に受信されている場合は，相手装置を確認してください。受信されていない場合には，ネットワークの物理構成を確認してください。 |
| 5 | 障害監視インタフェース定義がある場合，障害監視インタフェースの状態を確認してください。 | 障害監視インタフェースを定義したインタフェースに別の仮想ルータの定義があり，その仮想ルータの障害監視インタフェースが該当仮想ルータのインタフェースになっていないことを確認してください。なっている場合は，どちらかの障害インタフェースの定義を削除してください。 |
| | | 上記の障害監視インタフェースの定義がない場合は項番 6 へ。 |

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| 6 | フィルタの定義で VRRP の Advertisement パケットを廃棄する設定がないことを確認してください。 | 該当するフィルタの定義がある場合，VRRP の Advertisement を廃棄しないようにフィルタの定義を変更してください。 |
| | | フィルタの定義がない場合，同一の仮想ルータを構成する相手装置の動作を確認してください。 |

## 7.8.4 トンネルインタフェース上で通信ができない

通信障害の原因がトンネル回線にあると考えられる場合は，以下に従い確認をしてください。

### (1) 状態確認

show interfaces コマンドにより，該当するトンネル回線状態を確認します。表示されるトンネル回線状態を次の表のとおり確認します。

表 5-25 トンネル回線状態の確認／対応

| 項番 | Line 状態 | 原因 | 対応 |
|---|---|---|---|
| 1 | active up | 当該トンネル回線は正常に動作中です。 | なし。 |
| 2 | active down | 当該トンネル回線に回線障害が発生しています。 | 当該トンネル回線が 6to4 トンネルの場合だけ発生する状態です。show logging コマンドにより表示される当該 6to4 トンネル回線に対応する回線のログ情報より，「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」の該当ログ情報を参照し，記載されている［対応］にしたがって対応してください。 |
| 3 | locked | 構成定義により当該トンネルの運用が停止されています。 | 構成定義情報を設定して当該トンネルを運用状態にしてください。 |

### (2) 統計情報の確認

show interfaces コマンドにより，当該トンネル回線の統計情報（パケット受信・送信失敗）を確認してください。パケット受信・送信失敗が発生している場合は，「7.8.1　通信ができない，または切断されている （11）トンネルインタフェース設定情報の確認」にしたがって設定情報の確認をしてください。

## 7.8.5 NAT-PT 通信ができない

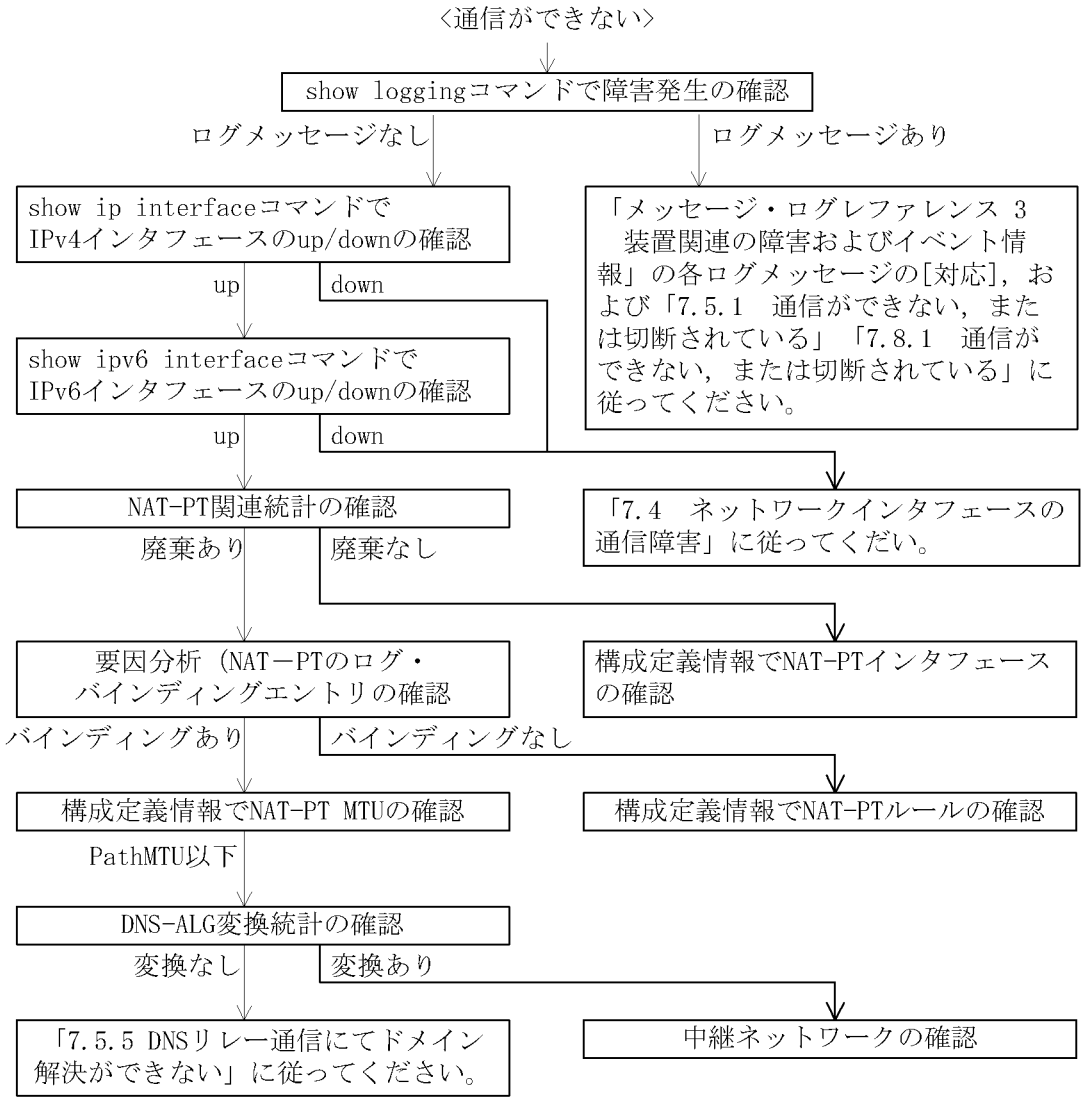
NAT-PT の通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. NAT-PT に関係する構成定義情報の誤り
2. ネットワークの構成変更
3. 中継ネットワークの障害

上記 2. については，ネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。

ここでは，IPv6 ネットワーク，IPv4 ネットワークそれぞれの設定（ネットワークカードの設定，ケーブルの接続など）は確認されているものとし，上記 1. および 3. に示すような「構成定義情報およびネットワーク構成は正しいのに，通信できない。」，「構成定義情報の変更を行ったら，通信できなくなった。」というケースについて，障害部位および原因の切り分け手順を説明いたします。

障害部位および原因の切り分け方法は，次のフローにしたがってください。




## (1) ログメッセージおよびインタフェースの確認

通信ができなくなる原因として，ハードウェア（RP ／ NIF ／ Line）の障害（または壊れ）や，隣接装置の障害が考えられます。本装置が表示するログメッセージや show ip interface コマンド，show ipv6 interface コマンドによるインタフェースの up/down 状態を確認してください。手順については「7.5.1 通信ができない，または切断されている」(IPv4 ネットワーク)，「7.8.1 通信ができない，または切断されている」(IPv6 ネットワーク)を参照してください。

## (2) NAT-PT 関連統計の確認

show ipv6 natpt statistics コマンドで Not translated packet，Discarded packet のカウンタが増加している場合，NAT-PT での変換に失敗している可能性があります。「(4) ログ情報の確認（要因分析)」「(5) バインディングエントリの確認（要因分析)」で原因を調査してください。どのカウンタも増加していない場合，NAT-PT インタフェースの設定に間違いがある可能性があります。「(3) 構成定義 NAT-PT インタフェースの確認」で設定内容を確認してください。

```
> show ipv6 natpt statistics
                                    6->4          4->6          Total
  NAT-PT packet counter:             440           279            721
    Translated packet:               432           274            706
    Not translated packet:             0             1              3
    Discarded packet:                  8             4             12
>
```

0以外であれば変換失敗が発生しています。

### (3) 構成定義 NAT-PT インタフェースの確認

構成定義コマンド natpt interface で設定したインタフェース名に誤りがあると，NAT-PT は変換を行いません。構成定義コマンド show natpt interface で構成定義の内容を確認してください。

```
(config)# show natpt interface
natpt yes

natpt  interface IPv6-net
natpt  interface IPv4-net
```

この内容を確認してください。

### (4) ログ情報の確認（要因分析）

show ipv6 natpt log コマンドでログ情報を確認してください。

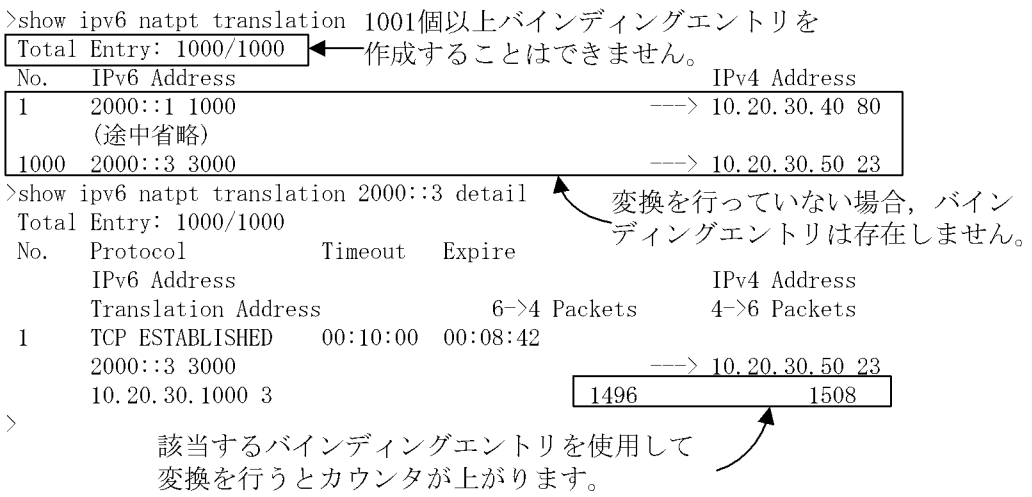
```
> show ipv6 natpt log
Date   Time      Log       Detail                        Protocol
       IPv6 Address                                      IPv4 Address
05/31  14:17:01  Fail4->6  FAIL_NOT_FOUND_RULE           ICMP
       10.20.30.100                                <--- 10.20.30.40
05/31  14:16:32  Fail6->4  FAIL_LACK_TSLOT               TCP CLOSED
       2000::1 1024                                ---> 10.20.30.50 80
>
```

IPv6 パケットから IPv4 パケットへの変換に失敗すると，Log は Fail6->4 となります。逆に IPv4 パケットから IPv6 パケットへの変換に失敗すると，Log は Fail4->6 となります。それぞれ失敗した理由を Detail に表示します。

### (5) バインディングエントリの確認（要因分析）

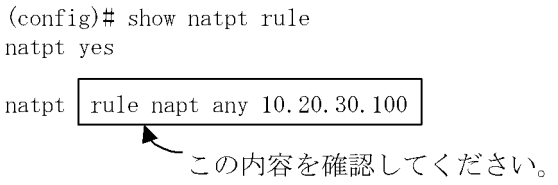
show ipv6 natpt translation コマンドでバインディングエントリ情報を確認してください。該当するバインディングエントリ情報がない場合，まず Total Entry が 1000/1000 と表示されているかどうかを確認してください。表示されている場合，新規にバインディングエントリを作成することができないため，通信を行うことができません。ほかの通信の終了を待つか，clear ipv6 natpt translation コマンドで，不要なバインディングエントリを削除してください。Total Entry が 1000/1000 と表示されていない場合，「(6) 構成定義 NAT-PT ルールの確認」で設定内容を確認してください。該当するバインディングエントリ情報がある場合，show ipv6 natpt translation に detail オプションをつけて実行し，バインディングエントリごとの統計を表示してください。統計数が上がっていれば NAT-PT による変換を行っています。統計数が上がっていない場合，「(9) 中継ネットワークの確認」で IPv4 と IPv6 ネットワークの状態を確認してください。統計数が上がっている場合，「(7) 構成定義 NAT-PT MTU の確認」で設定内容を確認してくださ

い。



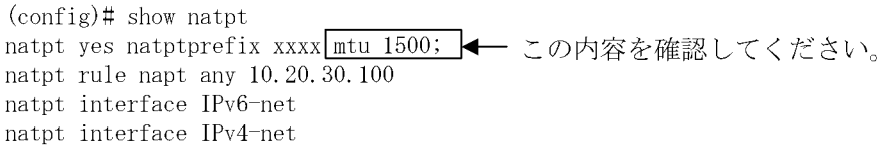

## (6) 構成定義 NAT-PT ルールの確認

構成定義コマンド show natpt rule で変換ルールの内容を確認してください。




## (7) 構成定義 NAT-PT MTU の確認

IPv6 変換後のパケットサイズが PathMTU よりも大きいと，IPv6 ネットワーク内でパケットが廃棄されます。構成定義コマンド show natpt で MTU サイズを確認し，PathMTU よりも小さな値に設定してください。PathMTU が分からない場合には MTU 設定を削除し，default 値 (1280byte) に戻してください。MTU を正しく設定しても通信できない場合は「(8) DNS-ALG 関連統計の確認」,「(9) 中継ネットワークの確認」を参照してください。




## (8) DNS-ALG 関連統計の確認

IPv6 から IPv4 への通信で，名前解決できない場合には，show dns-relay コマンドで，DNS-ALG 統計情報を表示してください。AAAA->A，A->AAAA 共に増加しない場合，DNS-ALG による DNS クエリーや DNS レスポンスの変換を行っていません。このような場合には DNS リレーに問題がある可能性があります。DNS リレーの問題解決については「7.5.5　DNS リレー通信にてドメイン解決ができない」を参照し

てください。

```
> show dns-relay
(途中省略)
DNS-ALG Statistics:
  AAAA -> A           : 0
  A    -> AAAA        : 0
>
```

変換を行っていない場合，増加しません。

### (9) 中継ネットワークの確認

中継ネットワークの障害により通信ができなくなっていることが考えられます。手順については「7.5.1 通信ができない，または切断されている」(IPv4 ネットワーク)，「7.8.1　通信ができない，または切断されている」(IPv6 ネットワーク) を参照してください。

また，IPv4 ネットワークと接しているインタフェースにて，PPPoE を使用している場合は「7.5.3 PPPoE 通信ができない」を，DHCP クライアントを使用している場合は「7.5.2　DHCP 機能にて IP アドレスが割り振られない　(3) DHCP クライアントの通信トラブル」を参照してください。

# 7.9 IPv6 ユニキャストルーティングの通信障害

## 7.9.1 RIPng 経路情報がない

本装置が取得した経路情報の表示に，RIPng の経路情報が存在しない場合は，次の表に示す障害解析方法にしたがって原因の切り分けを行ってください。

**表 7-32 RIPng の障害解析方法**

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| 1 | RIPng の隣接情報を表示します。<br>show ipv6 rip gateway | 隣接ルータのインタフェースが表示されていない場合は項番 2 へ。 |
| | | 隣接ルータのインタフェースが表示されている場合は項番 3 へ。 |
| 2 | 構成定義情報で RIPng 定義が正しいか確認してください。 | 構成定義情報が正しい場合は項番 3 へ。 |
| | | 構成定義情報が正しくない場合は構成定義情報を修正してください。 |
| 3 | 構成定義情報で経路フィルタリングが正しいか確認してください。 | 構成定義情報が正しい場合は項番 4 へ。 |
| | | 構成定義情報が正しくない場合は構成定義情報を修正してください。 |
| 4 | 隣接ルータが RIPng 経路を広告しているか確認してください。 | 広告している場合は該当ルータで障害情報を収集してください。<br>dump protocols unicast all ※ |
| | | 広告していない場合は隣接ルータを確認してください。 |

注※

障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。

格納エリア：/primaryMC/usr/var/rtm

ファイル名：rt_trace と rt_dump.gz

## 7.9.2 OSPFv3 経路情報がない

本装置が取得した経路情報の表示に，OSPFv3 の経路情報が存在しない場合は，次の表に示す障害解析方法にしたがって原因の切り分けを行ってください。

**表 7-33 OSPFv3 の障害解析方法**

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| 1 | OSPFv3 のピア状態を確認します。<br>show ipv6 ospf interface <Interface Name> | 隣接ルータの状態が Full 以外の場合は項番 2 へ。 |
| | | 隣接ルータの状態が Full の場合は項番 3 へ。 |
| 2 | 構成定義情報で OSPFv3 の定義が正しいか確認してください。 | 構成定義情報が正しい場合は項番 3 へ。 |
| | | 構成定義情報が正しくない場合は構成定義情報を修正してください。 |
| 3 | OSPFv3 経路を学習している経路を確認してください。<br>show ipv6 route -r | 経路が InActive または存在しない場合には項番 4 へ。 |

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| | | 経路が存在する場合は障害情報を収集してください。<br>dump protocols unicast all ※ |
| 4 | 構成定義情報でフィルタリングしていないか確認してください。 | 構成定義情報が正しい場合は項番 5 へ。 |
| | | 構成定義情報が正しくない場合は構成定義情報を修正してください。 |
| 5 | 隣接ルータが OSPFv3 経路を広告しているか確認してください。 | 広告している場合は該当ルータで障害情報を収集してください。<br>dump protocols unicast all ※ |
| | | 広告していない場合は隣接ルータを確認してください。 |

注※

障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。

格納エリア：/primaryMC/usr/var/rtm

ファイル名：rt_trace と rt_dump.gz

## 7.9.3 BGP4+ 経路情報がない

本装置が取得した経路情報の表示に，BGP4+ の経路情報が存在しない場合は，次の表に示す障害解析方法にしたがって原因の切り分けを行ってください。

**表 7-34 BGP4+ の障害解析方法**

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| 1 | BGP4+ のピア状態を確認します。<br>show ipv6 bgp neighbor | ピア状態が Established 以外の場合は項番 2 へ。 |
| | | ピア状態が Established の場合は項番 3 へ。 |
| 2 | 構成定義情報で BGP4+ の定義が正しいか確認してください。 | 構成定義情報が正しい場合は項番 3 へ。 |
| | | 構成定義情報が正しくない場合は構成定義情報を修正してください。 |
| 3 | BGP4+ 経路を学習しているか確認してください。<br>show ipv6 bgp received-routes | 経路が存在しない場合には項番 4 へ。 |
| | | 経路が存在する場合は障害情報を収集してください。<br>dump protocols unicast all ※ |
| 4 | 構成定義情報でフィルタリングしていないか確認してください。 | 構成定義情報が正しい場合は項番 5 へ。 |
| | | 構成定義情報が正しくない場合は構成定義情報を修正してください。 |
| 5 | 隣接ルータが BGP4+ 経路を広告しているか確認してください。 | 広告している場合は該当ルータで障害情報を収集してください。<br>dump protocols unicast all ※ |
| | | 広告していない場合は隣接ルータを確認してください。 |

注※

障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。

格納エリア：/primaryMC/usr/var/rtm

ファイル名：rt_trace と rt_dump.gz

## 7.9.4 IS-IS 経路情報がない

本装置が取得した経路情報の表示に，IS-IS の経路情報が存在しない場合は，次の表に示す障害解析方法にしたがって原因の切り分けを行ってください。

**表 7-35 IS-IS の障害解析方法**

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| 1 | IS-IS の隣接状態を確認します。<br>show isis adjacency | 隣接状態が Up 以外の場合は項番 2 へ。 |
| | | 隣接状態が Up の場合は項番 4 へ。 |
| 2 | 構成定義情報で IS-IS の定義が正しいか確認してください。 | 構成定義情報が正しい場合は項番 3 へ。 |
| | | 構成定義情報が正しくない場合は構成定義を修正してください。 |
| 3 | IS-IS のインタフェース状態を確認します。<br>show isis interface | インタフェース状態が Active の場合は項番 4 へ。 |
| | | インタフェース状態が Passive の場合は IS-IS 未サポートのインタフェースです。 |
| 4 | IS-IS 経路を学習しているか確認してください。<br>show ipv6 route all-routes | 経路が InActive または存在しない場合には項番 5 へ。 |
| | | 経路が Active の場合は障害情報を収集してください。<br>dump protocols unicast all ※ |
| 5 | 構成定義情報でフィルタリングしていないか確認してください。 | 構成定義情報が正しい場合は項番 6 へ。 |
| | | 構成定義情報が正しくない場合は構成定義を修正してください。 |
| 6 | 隣接ルータが IS-IS 経路を広告しているか確認してください。 | 広告している場合は該当ルータで障害情報を収集してください。<br>dump protocols unicast all ※ |
| | | 広告していない場合は隣接ルータを確認してください。 |

注※

障害情報収集コマンドを実行すると，次に示すエリアにファイルが作成されます。

格納エリア：/primaryMC/usr/var/rtm

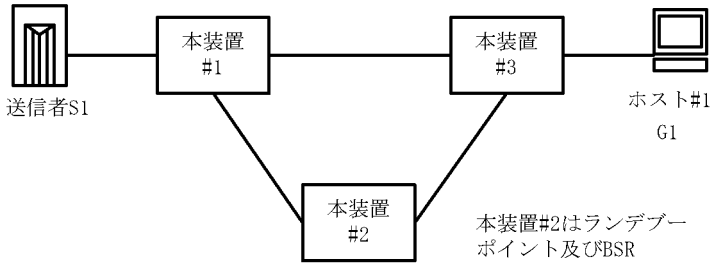
ファイル名：rt_trace と rt_dump.gz

# 7.10 IPv6 マルチキャストルーティングの通信障害

本装置で IPv6 マルチキャスト通信ができない場合の対処について説明します。

## 7.10.1 PIM-SM ネットワークで通信ができない

### (1) PIM-SM ネットワーク

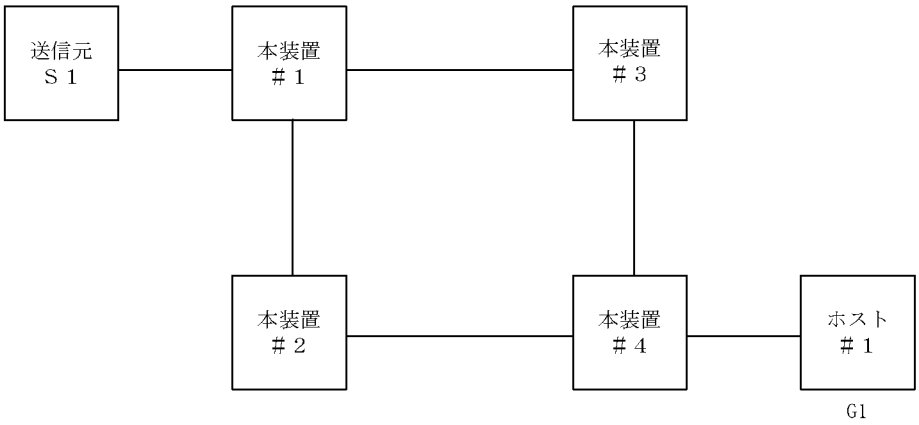



図に示す IPv6 PIM-SM ネットワークの構成にて，送信元 S1 から G1 宛のパケットがホスト #1 で受信できない場合，次の手順にしたがって対処してください。

1. 本装置 #3 で show ipv6 mld interface コマンドを実行し，ホスト #1 とのインタフェースが表示されること，フィルタなどによる中継抑止定義がないことを確認してください。
2. 本装置 #3 で show ipv6 mld group コマンドを実行し，G1 グループにホスト #1 が参加していることを確認してください。
3. 本装置 #3 で show ipv6 mroute コマンドを実行し，送信元 S1 から G1 への IPv6 マルチキャストルーティングキャッシュ（S,G）および G1 への IPv6 マルチキャストルーティングキャッシュ（*,G）が存在していることを確認してください。存在しない場合は，本装置と #1 および #2 との IPv6 PIM-SM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
4. 本装置 #1 で show ipv6 mroute コマンドを実行し，送信元 S1 から G1 への IPv6 マルチキャストルーティングキャッシュが存在していることを確認してください。存在しない場合は，S1 との IPv6 PIM-SM のインタフェース定義が enable であり，フィルタなどによる抑止定義がないことを確認してください。
5. IPv6 ルーティングキャッシュの下流が存在しない場合，show ipv6 pim neighbor で本装置 #2 と本装置 #3 が表示されていることを確認してください。また，IPv6 ルーティングキャッシュが存在しない場合は，show ipv6 pim bsr および show ipv6 pim rendezvous-point mapping を実行し，BSR およびランデブーポイント（RP）が本装置 #2 であることを確認してください。
6. BSR およびランデブーポイント（RP）が存在しないか本装置 #2 でない場合，本装置 #2 で show ipv6 pim bsr および show ipv6 pim rendezvous-point mapping コマンドを実行し，本装置が BSR およびランデブーポイント（RP）であることを確認してください。本装置が BSR およびランデブーポイントでない場合，構成定義情報で BSR およびランデブーポイントの定義が正しいか確認してください。
7. 本装置 #2 で show ipv6 mroute コマンドを実行し，送信元 S1 から G1 への IPv6 マルチキャストルーティングキャッシュ（S,G）および G1 への IPv6 マルチキャストルーティングキャッシュ（*,G）が存在していることを確認してください。存在しない場合は，本装置 #1 および本装置 #3 との IPv6 PIM-SM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
8. IPv6 ルーティングキャッシュの下流が存在しない場合，show ipv6 pim neighbor で本装置 #1 と本装置 #3 が表示されていることを確認してください。

9. ルーティングキャッシュが存在しない場合は，本装置 #3 で show ipv6 pim bsr および show ipv6 pim rendezvous-point mapping を実行し，BSR およびランデブーポイント（RP）が本装置 #2 であることを確認してください。

### （2） PIM-SSM ネットワーク




図に示す IPv6 PIM-SSM ネットワークの構成にて，送信元 S1 から G1 宛のパケットがホスト #1 で受信できない場合，次の手順にしたがって対処してください。

1. すべての本装置の構成定義情報に SSM が定義され，G1 が SSM アドレスであることを確認してください。
2. 本装置 #4 で show ipv6 mld interface コマンドを実行し，ホスト #1 とのインタフェースが表示されること，フィルタなどによる中継抑止定義がないことを確認してください。
3. 本装置 #4 で show ipv6 mld group コマンドを実行し，G1 グループにホスト #1 が参加していることを確認してください。
4. 本装置 #4 で ssm-join の構成定義情報に（G1,S1）が定義されていることを確認してください。
5. 送信元 S1 のデータ送信を行うインタフェースに S1 が定義されていることを確認してください。複数個の IPv6 アドレスが設定されている場合（アドレスの自動設定機能が有効になっている場合など）には，送信されるデータの送信元アドレスが S1 であることを確認してください。
6. 本装置 #4 で show ipv6 rpf コマンドを実行し，S 1 への経路を認識していることを確認してください（ここでは本装置 #2 側を上流とします）。
7. 本装置 #4 で show ipv6 mroute コマンドを実行し，送信元 S1 から G1 への IPv6 マルチキャストルーティングキャッシュ（S,G）が存在していることを確認してください。存在する場合は，iif が #2 側のインタフェースで，oif がホスト #1 側のインタフェースである SSM エントリであることを確認してください。存在しない場合は，本装置と #2 の IPv6 PIM-SM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
8. 本装置 #4 で show ipv6 pim neighbor コマンドを実行し，本装置 #4 が本装置 #2 を認識できていることを確認してください。
9. 本装置 #2 で show ipv6 mroute コマンドを実行し，送信元 S1 から G1 へのマルチキャストルーティングキャッシュ（S1,G1）が存在していることを確認してください。存在する場合は，iif が装置 #1 側のインタフェースで，oif が装置 #4 側のインタフェースである SSM エントリであることを確認してください。存在しない場合は，本装置 #4 および本装置 #1 との PIM-SM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
10. 本装置 #2 で show ipv6 pim neighbor コマンドを実行し，本装置 #2 で本装置 #4 および本装置 #1 が表示されていることを確認してください。

11. 本装置 #1 で show ipv6 mroute コマンドを実行し，送信元 S1 から G1 への IPv6 マルチキャストルーティングキャッシュ（S,G）が存在していることを確認してください。存在する場合は，iif が S1 のインタフェースで，oif が装置 #2 側のインタフェースである SSM エントリであることを確認してください。存在しない場合は，本装置 #1 および本装置 #3 との IPv6 PIM-SM のインタフェース定義が enable であり，フィルタなどによる中継抑止定義がないことを確認してください。
12. IPv6 ルーティングキャッシュの下流が存在しない場合，show ipv6 pim neighbor コマンドを実行し，本装置 #2 が表示されていることを確認してください。

# 7.11　マルチプロトコルの通信障害

## 7.11.1　IPX 通信で NetWare サーバにログインできない

次に示す手順で確認してください。

1. 装置／回線状態の確認
   「4.4　ボードの実装状態を確認する」「5.1　ネットワークインタフェース状態の確認」を参照の上，装置や回線が障害となっていないか確認してください。障害となっている場合は「7.1　装置または装置の一部の障害」「7.4　ネットワークインタフェースの通信障害」を参照の上，対応してください。
2. 運用構成定義情報の確認
   「5.9.1　IPX 通信機能を確認する」を参照してください。
3. インタフェース情報の確認
   「5.9.1　IPX 通信機能を確認する」を参照してください。
4. ルーティング情報の確認
   「5.9.1　IPX 通信機能を確認する」を参照してください。
5. サーバ情報の確認
   「5.9.1　IPX 通信機能を確認する」を参照してください。

## 7.11.2　ブリッジ通信でフレームが中継されない

### (1) ブリッジインタフェース定義の確認

構成定義コマンド show bridge で，各インタフェースに定義したブリッジインタフェースが正しく定義されているか確認してください。また，show bridge interface コマンドおよび show spanning-tree summary コマンドを実行し，インタフェースが障害（Down）となっていないか，また定義したとおりのインタフェース種別で動作しているか確認してください。

### (2) フィルタリングデータベースの確認

フィルタリングデータベースのスタティックエントリが誤って設定されていると，期待したフレーム中継がされなかったり，誤った LAN に中継されたりすることがあります。構成定義コマンド show bridge でスタティックエントリが正しく設定されているか確認してください。さらに，show bridge fdb コマンドで現在のフィルタリングデータベースの内容を表示し，これと合わせて確認してください。また，特に定義で設定する MAC アドレスはキャノニカル表現で設定することにご注意ください。

# 7.12 SNMP の通信障害

## 7.12.1 SNMP マネージャから MIB の取得ができない

次に示す手順で確認してください。

1. 構成定義コマンド show snmp（「構成定義コマンドレファレンス Vol.2 snmp（SNMP マネージャの登録）」を参照）を実行し，本装置の構成定義情報に SNMP マネージャに関する情報が登録されているかどうかを確認してください。
   登録されていない場合は，構成定義コマンド snmp を実行して，SNMP マネージャに関する情報を定義してください。

```
(config)#  show snmp
snmp  "public" 20.1.1.1 read_write none
snmp  "public" 10.1.1.1 read ex_trap level 7
snmp  "event-monitor"  30.1.1.1 read trap
!
(config)#
```

登録されている SNMP マネージャのコミュニティ名称を示します。

登録されている SNMP マネージャの IP アドレスを示します。

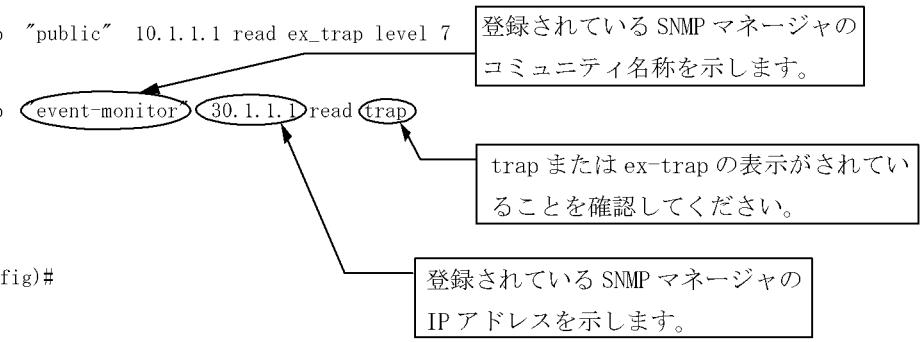
2. 構成定義情報は正しく登録されているが，SNMP マネージャからの要求に対して応答タイムアウトする場合，SNMP マネージャ側の応答タイムアウト値を少なくとも 5 秒以上に設定してください。
   なお，ネットワークのレスポンスが悪い（SNMP マネージャと本装置間の回線速度が低い，SNMP マネージャと本装置の間に多数の接続装置（ブリッジ，ルータ，スイッチなど）がある）場合は，応答タイム値をさらに延ばす必要があります。
3. SNMP マネージャ側の応答タイムアウト値を変更しても，MIB の取得ができない場合，SNMP マネージャと本装置との間で SNMP フレームのフィルタリング（廃棄）がされている可能性があります。
   ネットワーク管理者に SNMP フレームのフィルタリングがされていないか確認してください（SNMP フレームは，ポート番号 161 の UDP フレームを使って通信しています）。

## 7.12.2 SNMP マネージャでトラップが受信できない

次に示す手順で確認してください。

1. 構成定義コマンド show snmp（「構成定義コマンドレファレンス Vol.2 snmp（SNMP マネージャの登録）」を参照）を実行し，本装置の構成定義情報に SNMP マネージャおよびトラップに関する情報が登録されているかどうかを確認してください。
   登録されていない場合は，構成定義コマンド snmp を実行して，SNMP マネージャおよびトラップに関する情報を定義してください。

```
(config)# show snmp

snmp  "public"  20.1.1.1 read_write none

snmp  "public"  10.1.1.1 read ex_trap level 7

snmp  "event-monitor"  30.1.1.1 read trap

!

(config)#
```




2. 構成定義情報は正しく定義されているがトラップを受信しない場合，SNMP マネージャと本装置との間で SNMP フレームのフィルタリング（廃棄）がされている可能性があります。ネットワーク管理者に SNMP フレームのフィルタリングがされていないか確認してください（SNMP のトラップは，ポート番号 162 の UDP フレームを使って通信しています）。

# 7.13 NTP の通信障害

## 7.13.1 NTP による時刻同期ができない

NTP による時刻同期ができない場合は，次の表に示す障害解析方法にしたがって原因の切り分けを行ってください。

**表 7-36 NTP の障害解析方法**

| 項番 | 確認内容・コマンド | 対応 |
|---|---|---|
| 1 | 構成定義情報でタイムゾーンの定義があることを確認してください。 | 構成定義情報にタイムゾーンが定義されている場合は項番 2 へ。 |
| | | 構成定義情報にタイムゾーンが定義されていない場合はタイムゾーンの定義をしてください。 |
| 2 | タイムゾーン構成定義が反映されているか date コマンドで確認してください。 | コマンドの表示結果にタイムゾーンの情報が含まれている場合は項番 3 へ。 |
| | | コマンドの表示結果にタイムゾーンの情報が含まれていない場合は，装置を再起動してタイムゾーンの情報を反映させてください。 |
| 3 | 本装置と NTP サーバとの時刻差を確認してください。 | 本装置と NTP サーバとの時刻差が 1000 秒以内の場合は項番 4 へ。 |
| | | 本装置と NTP サーバとの時刻差が 1000 秒以上ある場合には，date コマンドを使用して本装置の時刻を NTP サーバと合わせてください。 |
| 4 | NTP サーバとの IPv4 による通信を確認してください。 | NTP サーバと本装置間で IPv4 の通信が可能か，ping コマンドで確認してください。 |
| | | NTP サーバの設定で，UDP ポート番号 123 のパケットを廃棄する設定がないことを確認してください。 |

# 8 保守作業

この章では，主に保守関連作業を行うときの作業手順について説明しています。

# 8.1 障害情報の取得

show tech-support コマンドを使用して，障害発生時の情報採取を一括して採取することができます。また，本コマンドでは，採取した障害情報を指定した ftp サーバに転送することができます（「8.2.3 show tech-support コマンドを使用した保守情報のファイル転送」を参照）。本コマンドで採取する情報を次の表に示します。

**表 8-1 show tech-support コマンドの情報採取内容**

| 情報採取レベル※ | 採取内容 |
|---|---|
| 基本情報 | ソフトウェアバージョン情報 |
| | ハードウェア実装情報 |
| | 運用系，待機系のログ情報，ダンプ情報 |
| | インタフェース情報 |
| | 統計情報 |
| | MC 情報 |
| | 構成定義情報（コマンドオプションで採取しないことも可能です） |
| | プロセス情報 |
| | バッファ情報 |
| 詳細情報 | インタフェース詳細情報 |
| | ハードウェアバッファ情報 |
| | トンネルハードウェア情報 |
| | ARP 情報 |
| | 経路情報統計 |
| | フィルタ情報 |
| | QoS 情報 |
| | DHCP，SNMP，VRRP，IPX，ISDN，ブリッジのソフトウェア動作情報 |
| | その他，ソフトウェア，ハードウェアの障害トレース情報 |

注※

show tech-support コマンドに detail パラメータを付けて実行した場合は「基本情報」と「詳細情報」を採取し，detail パラメータを付けないで実行した場合は「基本情報」だけを採取します。

# 8.2 保守情報のファイル転送

装置運用中に障害発生により自動的に採取されたログ情報やダンプ情報，またはコマンドを用いることで採取したダンプ情報をコンソールまたはリモート運用端末にファイル転送する方法を示します。ファイル転送を行うには ftp コマンド，zmodem コマンド，および show tech-support コマンドの三つの方法があります。なお，保守情報には次の表に示すものがあります。

**表 8-2 保守情報**

| 項番 | 項目 | 格納場所およびファイル名 |
|---|---|---|
| 1 | 装置再起動時のダンプ情報ファイル | /primaryMC/var/dump/rmdump |
| 2 | RP および NIF のダンプ情報ファイル | /primaryMC/var/dump/rp**.*** ... 標準の RP ダンプ<br>/secondaryMC/var/dump/rp**e1.*** ... 拡張の RP ダンプ（拡張の RP ダンプ採取指定時だけ）および<br>/primaryMC/var/dump/nif**.*** ...NIF ダンプ (** はスロット番号，*** はシーケンス番号または " cmd ") |
| 3 | ログ情報 | 採取したディレクトリ（「図 8-2 ログ情報のリモート運用端末へのファイル転送」を参照）から次の名前で格納する<br>運用ログ :log.txt<br>種別ログ：log_ref.txt |
| 4 | 構成定義情報ファイル | /config/router.cnf |
| 5 | 障害待避情報 | /primaryMC/var/core/*.core |

注 1

項番 1，2 および 5 のファイルを ftp コマンドで転送する場合はバイナリモードで転送してください。

注 2

項番 2 の拡張の RP ダンプ指定は「運用コマンドレファレンス Vol.1 dump rp」を参照してください。拡張の RP ダンプを指定した場合，標準の RP ダンプと拡張の RP ダンプの，二つのダンプファイルを出力します。

## 8.2.1 ftp コマンドを使用したファイル転送

リモート運用端末との間でファイル転送を行う場合は ftp コマンドを使用します。

## (1) ダンプファイルをリモート運用端末に転送する

**図 8-1 ダンプファイルのリモート運用端末へのファイル転送**

```
> cd /var/dump/
> ftp 192.168.0.1                    <-- 転送先端末のアドレスを指定
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Fri Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp>prompt                          <-- 対話モードを変更
Interactive mode off.
ftp>bin                             <-- バイナリモードに設定※1
200 Type set to I.
ftp>cd 転送先ディレクトリ             <-- 転送先ディレクトリの指定
250 CMD command successful.
ftp> mput *                         <-- ダンプファイルの転送
local: rmdump remote: rmdump
200 PORT command successful.
150 Opening BINARY mode data connection for rmdump (2,312,345 bytes)
226 Transfer complete.
local: rp00.000 remote: rp00.000
200 PORT command successful.
150 Opening BINARY mode data connection for rp00.000 (512,322 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
>
```

注※ 1

ダンプファイルは必ずバイナリモードで転送してください。ダンプファイルをアスキーモードで転送すると，正確なダンプ情報が取得できなくなります。

## (2) ログ情報をリモート運用端末に転送する

**図 8-2 ログ情報のリモート運用端末へのファイル転送**

```
> show logging > log.txt
> show logging reference > log_ref.txt
> ftp 192.168.0.1                    <-- 転送先端末のアドレスを指定
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Fri Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp>ascii                          <-- アスキーモードに設定
200 Type set to A.
ftp>cd 転送先ディレクトリ           <-- 転送先ディレクトリの指定
250 CMD command successful.
ftp> put log.txt                   <-- ログ情報の転送
local: log.txt remote: log.txt
200 PORT command successful.
150 Opening ASCII mode data connection for log.txt (1,345 bytes)
226 Transfer complete.
ftp>put log_ref.txt
local: log_ref.txt remote: log_ref.txt
200 PORT command successful.
150 Opening ASCII mode data connection for log_ref.txt (846 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
>
```

### (3) 障害退避情報ファイルをリモート運用端末に転送する

**図 8-3 障害退避情報ファイルのリモート運用端末へのファイル転送**

```
> cd /primaryMC/var/core/
> ls                                  <---- 障害退避情報ファイルが存在することを確認。
interfaceControl.core    nodeInit.core      ファイルが存在しない場合は、何もせずに終了。
>
> ftp 192.168.0.1                     <---- 転送先端末のアドレスを指定
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Fri Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp>prompt                           <---- 対話モードを変更
Interactive mode off.
ftp>bin                              <---- バイナリモードに設定※1
200 Type set to I.
ftp>cd 転送先ディレクトリ             <---- 転送先ディレクトリの指定
250 CMD command successful.
ftp> mput *.core                     <---- 障害退避情報ファイルの転送
local: interfaceControl.core remote: interfaceControl.core
200 PORT command successful.
150 Opening BINARY mode data connection for interfaceControl.core (16,363 bytes)
226 Transfer complete.
local: nodeInit.core remote: nodeInit.core
200 PORT command successful.
150 Opening BINARY mode data connection for nodeInit.core (29,322 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
```

注※ 1

障害退避情報ファイルは必ずバイナリモードで転送してください。障害退避情報ファイルをアスキーモードで転送すると，正確な障害退避情報が取得できなくなります。

## 8.2.2 zmodem コマンドを使用したファイル転送

本装置と RS232C ケーブルで接続されているコンソールとの間でファイル転送を行う場合は zmodem コマンドを使用します。なお，通信を始めるにあたり，あらかじめコンソール側通信プログラムの受信操作を行ってください。

### (1) ダンプファイルをコンソールに転送する

**図 8-4 ダンプファイルのコンソールへのファイル転送**

```
> cd /var/dump/
> zmodem put rmdump          <---------- ダンプファイルの転送
**000000000000
>
```

### (2) ログ情報をコンソールに転送する

**図 8-5 ログファイルのコンソールへのファイル転送**

```
> show logging > log.txt
> show logging reference > log_ref.txt
> zmodem put log.txt         <---------- ログファイルの転送
**000000000000
> zmodem put log_ref.txt
**000000000000
>
```

### (3) 障害退避情報ファイルをコンソールに転送する

**図 8-6 障害退避情報ファイルのコンソールへのファイル転送**

```
> cd /primaryMC/var/core
> ls                         <---------- 障害退避情報ファイルが存在することを確認。
                                         ファイルが存在しない場合は、何もせずに終了。
interfaceControl.core   nodeInit.core
> zmodem put interfaceControl.core   <---------- ログファイルの転送
**000000000000
> zmodem put nodeInit.core
**000000000000
```

## 8.2.3 show tech-support コマンドを使用した保守情報のファイル転送

リモート運用端末またはリモートホストに対して保守情報のファイル転送を行う場合は show tech-support コマンドを使用します。

## (1) 保守情報をリモート運用端末またはリモートホストに転送する

**図 8-7 保守情報のリモート運用端末またはリモートホストへのファイル転送**

```
> show tech-support ftp                                          <—  ※1
Specify Host Name of FTP Server.       : ftpserver.example.com   <—  ※2
Specify User ID for FTP connections.   : user1                   <—  ※3
Specify Password for FTP connections.  : xxxxxx                  <—  ※4
Specify Path Name on FTP Server.       : /usr/home/user1         <—  ※5
Specify File Name of log and Dump files: support                 <—  ※6
Transfer Text file
file name      support.txt
Executing . . . . . .
Operation normal end.
########## Dump files' Information ##########
***** ls -l /dump0 *****
total 1368
-rwxr-xr-x  1 root  wheel  1316167 Apr 23 21:14 rmdump
-rwxr-xr-x  1 root  wheel    52077 Apr 23 21:14 dpdump
***** ls -l /standby/dump0 *****
total 1368
-rwxr-xr-x  1 root  wheel  1316167 Apr 23 21:14 rmdump
-rwxr-xr-x  1 root  wheel    52077 Apr 23 21:14 dpdump
########## End of Dump files' Information ##########
########## Core files' Information ##########
***** ls -l /primaryMC/usr/var/core *****
***** ls -l /standby/primaryMC/usr/var/core *****
No Core Files
########## End of Core files' Information ##########
Transfer binary file
file name      support.tgz
Executing . . . . . .
Operation normal end.
>
```

注※1 コマンドの実行
注※2 リモートホスト名を指定
注※3 ユーザ名を指定
注※4 パスワードを入力
注※5 転送先ディレクトリの指定
注※6 ファイル名を指定

# 8.3 障害が発生したボードの交換

## 8.3.1 障害が発生したボードの交換（電源 OFF したあと）

ここでは保守点検などでいったん電源 OFF（電源スイッチの搭載位置は，「ハードウェア取扱説明書」を参照）して，ボードを交換したい場合の手順を記載しています。

### (1) NIF の交換

「ハードウェア取扱説明書」を参照してください。

# 8.4 ボード，メモリの取り外し／増設

## 8.4.1 ボードの取り外し ( 電源 OFF したあと )

### (1) NIF の取り外し

「ハードウェア取扱説明書」を参照してください。

## 8.4.2 ボードの増設

### (1) NIF の取り外し

「ハードウェア取扱説明書」を参照してください。

## 8.4.3 メモリの増設 ( 電源 OFF したあと )

「ハードウェア取扱説明書」を参照してください。

# 8.5 MC の取り外し／取り付け

本装置の MC は，予備 MC だけ装置の動作中に抜き差しができます。本装置の動作中に予備 MC の抜き差しを行う場合は次の点にご注意ください。

また，誤って本装置の動作中に現用 MC の抜き差しを行ってしまった場合は，電源 OFF ／ ON を実行して本装置を再起動してください。

### (1) MC アクセス中の LED が消灯していること

カードスロットごとに MC アクセスを示す LED があります。MC を抜き差しする場合は，LED が消灯している（MC にアクセスしていない）ことを確認してください。LED が点灯しているとき（MC アクセス中）に抜き差しを行うと MC を破損する恐れがあります。

### (2) より安全に MC の抜き差しを行うためには

本装置には MC のアクセスを禁止するコマンドがあります。MC アクセス禁止コマンドを実行すると，MC アクセス禁止解除コマンドを実行するまでは，本装置は MC にはアクセスしません（MC アクセス禁止コマンド実行後は，いったん LED が消灯していることを確認してください）。コマンドの詳細は，「運用コマンドレファレンス Vol.1　set mc disable」の解説を参照してください。

### (3) MC 抜き差し後に注意すること

コマンド操作を行っているディレクトリが予備 MC 上（例：/secondaryMC/usr/home/operator）の場合，コマンドが実行できなくなる場合があります。cd コマンドでホームディレクトリ（例：/primaryMC/usr/home/operator）に移動してからコマンドを再実行してください。

### (4) MC 挿入時の注意事項

MC を予備スロットへ挿入したあと，show mc コマンドを使用して，挿入した MC が認識されていることを確認してください。show mc コマンドを実行し，該当する予備 MC のサイズが 0 バイトと表示されている場合は予備 MC が正常にマウントされていません。この場合は，10 秒ほど経過した後に再度確認してください。再度確認しても挿入した MC が認識されていない場合には set mc disable コマンド実行後，MC を抜き，再挿入してください。

# 8.6 装置／回線の状態を確認する

## 8.6.1 交換／増設した NIF の状態確認

ここでは通常運用時や本装置の NIF の交換，増設を行ったあとなどの状態を確認するときの手順を記載しています。また，障害のログメッセージが出ているときの対応作業の一つとしても参照してください。

### (1) イーサネット／ギガビット・イーサネットの場合

**[実行例]**

本装置の NIF 番号 2 に Line 番号 0 のセグメント規格をオートネゴシエーションに設定し，オートネゴシエーションで動作している HUB に接続したあとの回線状態の確認。

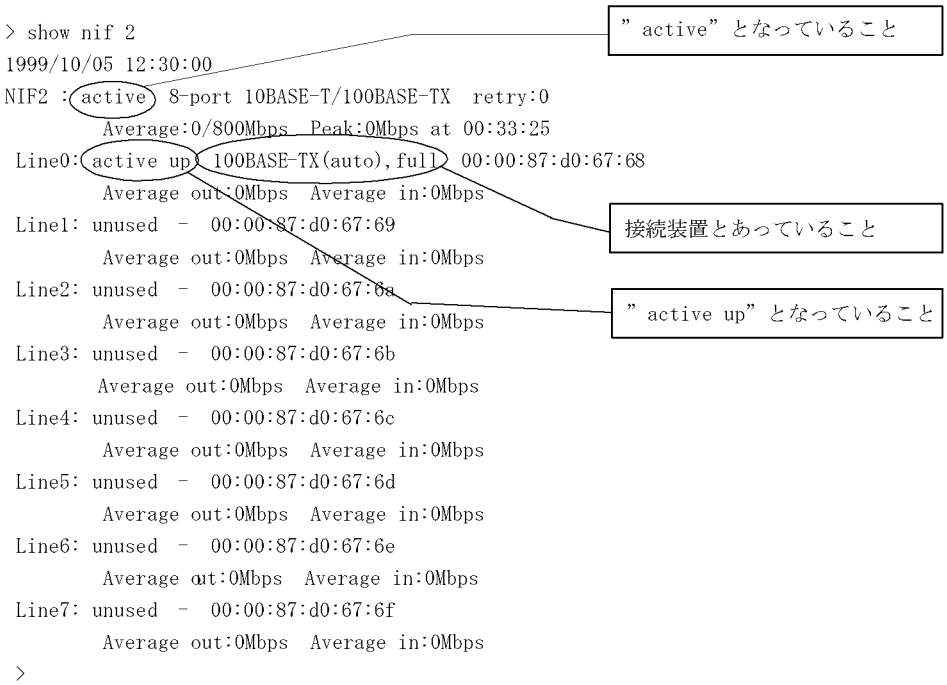
運用端末から次に示す show nif コマンドを実行します。

```
> show nif 2[Enter]
```

コマンド実行結果として，「図 8-8　イーサネット NIF の show nif コマンド実行による確認結果」に示す画面を表示しますので，次のことを確認してください。

- 該当する NIF が正常に運用（本例では ” NIF2: active ”）であること
- 該当する回線が正常に運用（本例では ” Line0: active up ”）であること
- 回線タイプが接続している装置と合っている（本例では，” 100BASE-TX(auto),full ”）こと
- 注：確認時，期待値にならないときは次の確認を行ってください。
- 回線が正常動作しない ( ” Line0: active up ” にならない）場合
  1. ケーブルが抜けていたり半挿し状態でないか。
  2. クロスケーブル／ストレートケーブルを間違えていないか。
  3. 接続している装置の立ち上げが完了しているか。
- 回線タイプが接続している装置と合っていない場合
  1. 接続している装置の通信速度およびセグメント規格（全二重／半二重）と構成定義が合っているか。
  2. 全二重固定の装置と接続するときに本装置の構成定義をオートネゴシエーションにしていないか。

**図 8-8 イーサネット NIF の show nif コマンド実行による確認結果**




## (2) WAN 回線の場合

**[実行例]**

本装置の NIF 番号 1 の LINE 番号 0 に V.24 回線が接続されている場合の回線状態の確認。

運用端末から次に示す show nif コマンドを実行します。

```
> show nif 1[Enter]
```

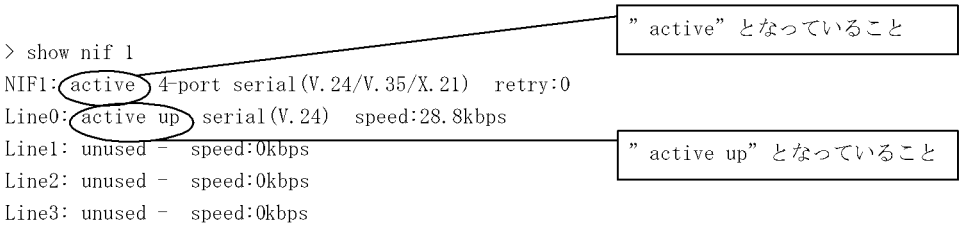
コマンド実行結果として,「図 8-9 WAN の NIF の show nif コマンド実行による確認結果」に示す画面を表示しますので,次のことを確認してください。

- 該当する NIF が正常に運用状態(本例では ” NIF1: active ”)であること
- 該当する LINE が正常に運用状態(本例では ” Line0: active up ”)であること

注:

” NIF1: active ” でない,または ” Line0: active up ” でない場合は,「7.4.2 WAN 回線の接続ができない」を参照してください。

**図 8-9 WAN の NIF の show nif コマンド実行による確認結果**



## (3) ATM の場合

### [実行例]

本装置の NIF 番号 0 の位置に，OC-3c/STM-1 ATM(multi-mode) の NIF を実装し，Line 番号 0 の回線を DSU，ATM スイッチなどの隣接装置に接続します。Line 番号 0 が構成定義された状態で回線状態を確認する例を示します。

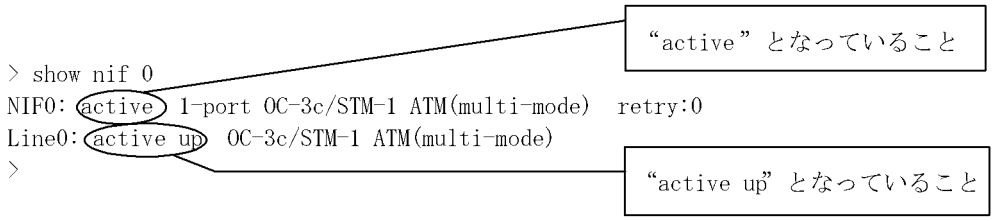
運用端末から次に示す show nif コマンドを実行します。

```
> show nif 0[Enter]
```

コマンド実行結果として，「図 8-10　ATM の NIF の show nif コマンド実行による確認」に示す画面を表示しますので，次のことを確認してください。

- 該当する NIF が運用中（正常動作中）（本例では ” NIF0: active ”）であること
- 該当する Line が運用中（正常動作中）（本例では ” Line0: active up ”）であること
- 注：Line が運用中（正常動作中）にならない（ ” Line0: active up ” にならない）場合は，次の確認を行ってください。
- ケーブルが抜けていたり半挿し状態でないか。
- マルチモードファイバを使用しているか（シングルモードファイバを間違えて使用していないか)。
- 接続している装置の立ち上げが完了しているか。

**図 8-10　ATM の NIF の show nif コマンド実行による確認**



# 8.7 回線をテストする

## 8.7.1 イーサネット

NIF 番号 2 の Line 番号 0 のケーブルを抜いてイーサネット用のループコネクタを接続します。

運用端末から test interfaces コマンド，no test interfaces コマンドの順でコマンドを実行します。

```
> test interfaces nif 2 line 0 connector [Enter]
```

（約1分待つ）

```
> no test interfaces nif 2 line 0 [Enter]
```

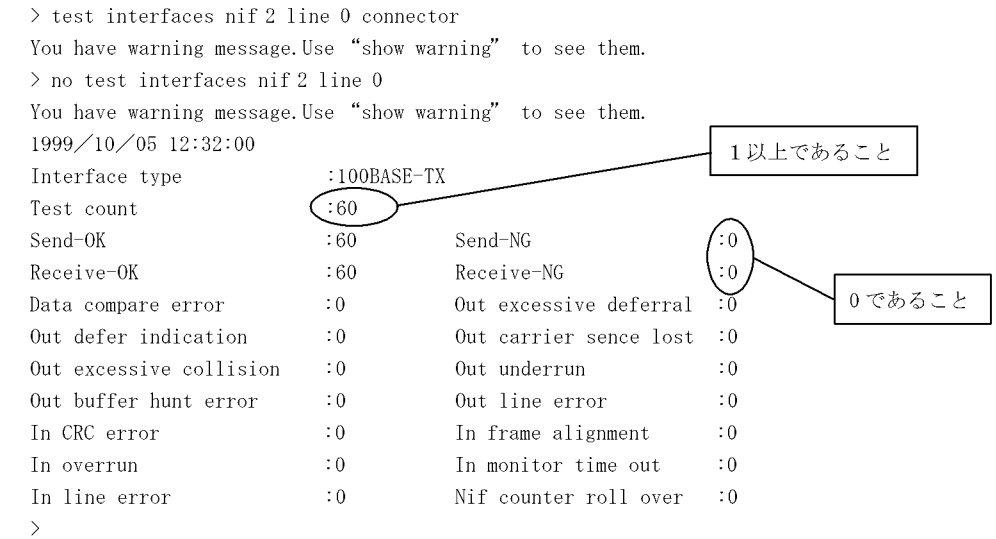
コマンド実行結果として，「図 8-11　イーサネット回線での test interfaces，no test interfaces コマンド実行による確認例」に示す画面を表示しますので，次のことを確認してください。

- ”Send-NG”および”Receive-NG”が 0 であること。
  ”Send-NG”および”Receive-NG”が 0 の場合，回線テスト結果は正常です。

  注 1：
  ”Send-NG”および”Receive-NG”が 0 でない場合は，何らかの異常がありますので「運用コマンドレファレンス Vol.1　no test interfaces（LAN）」の回線テスト実行結果の表示内容を参照してください。
  ループコネクタがない場合は内部ループテストを実施してください。

  注 2：
  ギガビット・イーサネットの NIF ボードについては，モジュール内部ループバックテストを行う場合もループコネクタが必要です。また，NE100-4FS4，NE1G-1LHA，NE1G-1LHA8 または NE1G-1LHBA でループコネクタループバックテストを行う場合には光アッテネータ（光減衰器）が必要です。

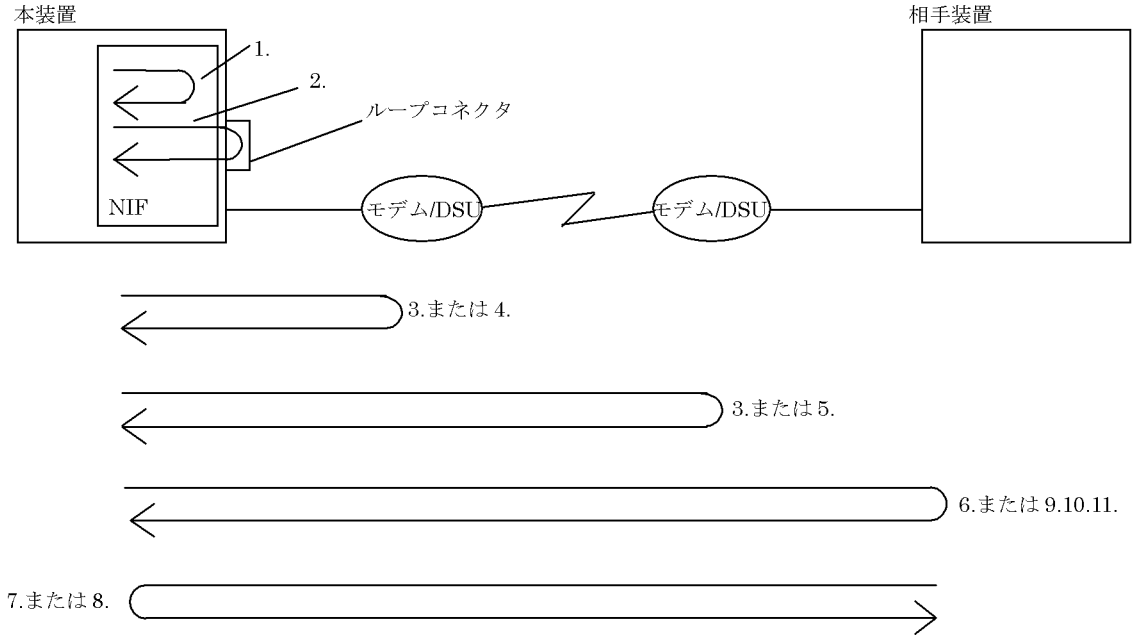
**図 8-11　イーサネット回線での test interfaces，no test interfaces コマンド実行による確認例**



## 8.7.2 WAN 回線

WAN 回線の回線テストまたは BERT（bit err rate test）では，指定するテスト種別により，テスト用に送出するフレームまたはデータの折り返し位置が異なります。テスト種別によるフレームの折り返し位置を次の図に示します。

**図 8-12 WAN 回線での回線テストのテスト種別によるフレームの折り返し位置**




1.モジュール内部ループバックテスト
2.ループコネクタループバックテスト
3.モデム手動ループバックテスト※1
4.ローカルモデムループバックテスト※2
5.リモートモデムループバックテスト※2
6.リモートラインループバックテスト※3
7.ネットワークラインループバックテスト※4
8.ネットワークペイロードループバックテスト※5
9.BERT※7
10.リモートペイロードループバックテスト※6
11.リモートラインインバンドループバックテスト※6
注※1 serial 回線(V.24／V.35／X.21)で，かつモデムを接続している場合だけ実行可能。
注※2 V.24 回線で，かつモデムを接続している場合だけ実行可能。
注※3 T1，T3 非多重回線の場合だけ実行可能。
注※4 T1，E1，T3 非多重，E3 非多重，E3 多重，T3 多重回線 POS の OC-3c（8 ポート），OC-12c（4 ポート），OC-48c の場合だけ実行可能。
注※5 T1，E1 回線の場合だけ実行可能。
注※6 T1 回線の場合だけ実行可能。
注※7 T1，E1，T3 非多重、E3 非多重回線の場合だけ実行可能。

また，回線種別により，実行可能なテスト種別が異なります（回線種別と実行可能なテスト種別は，「運用コマンドレファレンス Vol.1 test interfaces(WAN)」を参照してください）。

次にテスト種別ごとのテスト方法を説明します。

### (1) モジュール内部ループバックテスト

本テストは全回線種別で実行可能です。

本テストでは，テスト用フレームは本装置の NIF ボード内で折り返します。

テスト例として，NIF 番号 1 の LINE 番号 0 にテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> test interfaces nif 1 line 0 internal[Enter]
```

（約1分間待つ）

```
> no test interfaces nif 1 line 0[Enter]
```

コマンド実行結果として，「図 8-13　WAN 回線での test interfaces，no test interfaces コマンド実行結果例」に示す画面を表示しますので，次のことを確認してください。

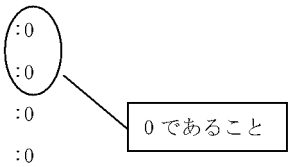
- ”Send-NG ”および ”Receive-NG ”が 0 であること。
  ”Send-NG ”および ”Receive-NG ”が 0 の場合，回線テスト結果は正常です。

  注 1：
  ”Send-NG ”および ”Receive-NG ”が 0 でない場合は，何らかの異常がありますので「運用コマンドレファレンス Vol.1　no test interfaces（WAN）」の回線テスト実行結果の表示内容を参照してください。

  注 2：
  NIF ボード OC-3c（8 ポート），OC-12c（4 ポート），OC-48c は構成定義情報 line の clock ＝ independent 設定のときだけテスト実行可能で，clock ＝ external に設定した場合，回線障害になる可能性があります。

**図 8-13　WAN 回線での test interfaces，no test interfaces コマンド実行結果例**

```
> test interfaces nif 1 line 0 internal
You have warning messages. Use "information -w" to see them.
> no test interfaces nif 1 line 0
1999/04/19 17:30:36
Interface type            :serial(----)
Test count                :40
Send-OK                   :40          Send-NG                :0
Receive-OK                :40          Receive-NG             :0
Data compare error        :0           Out timeout            :0
In timeout                :0           Underrun               :0
CRC error                 :0           Overrun                :0
Short frame               :0           Abort                  :0
Bit error                 :0           Error receive frame    :0
Physical down error       :none
Out buffer error          :none        H/W error              :none
Last signal status        :00000304
>
```




## (2) ループコネクタループバックテスト

本テストは全回線種別で実行可能です。

本テストでは，テスト用フレームは本装置の NIF ボードに接続したループコネクタ内で折り返します。

回線種別ごとにテストする対象の LINE 番号のケーブルを抜いて各回線種別ごとのループコネクタを接続しテストを実施します。ループコネクタ未接続，またはその回線に対応するループコネクタを接続しない場合，正しくテストが実施できませんので注意してください。テスト例として，NIF 番号 1 の LINE 番号 0 のケーブルを抜いて各回線種別ごとのループコネクタを接続しテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> test interfaces nif 1 line 0 connector[Enter]
```

（約1分間待つ）

```
> no test interfaces nif 1 line 0[Enter]
```

なお，テスト実行結果の確認は「(1) モジュール内部ループバックテスト」のテスト実行結果と同様に行ってください。

注：

NIF ボード OC-3c（8 ポート），OC-12c（4 ポート），OC-48c は構成定義情報 line の clock ＝ independent 設定のときだけテスト実行可能で，clock ＝ external に設定した場合，回線障害になる可能性があります。

## (3) モデム手動ループバックテスト

本テストは serial 回線（V.24 ／ V.35 ／ X.21）で，かつモデムを接続している場合にだけ実行可能です。また，モデムは折り返しモードが設定可能であることが必要です。

本テストでは，テスト用フレームは折り返しモードに設定したモデムで折り返します。

テスト例として，NIF 番号 1 の LINE 番号 0 にテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> test interfaces nif 1 line 0 manual[Enter]
```

（約1分間待つ）

```
> no test interfaces nif 1 line 0[Enter]
```

注：

テスト実行結果の画面で ” Test Count ” が 0 の場合は，show interfaces コマンドで回線状態を確認してください。

上記以外のテスト実行結果の確認は「(1) モジュール内部ループバックテスト」のテスト実行結果と同様に行ってください。

### (4) ローカルモデムループバックテスト（LLB）

本テストは serial 回線（V.24）で，かつモデムを接続している場合にだけ実行可能です（V.35，X.21 では使用できません)。また，モデムはローカルモデムループバックテストに対応している必要があります。

本テストでは，テスト用フレームはローカル（自局側）モデムで折り返します。

テスト例として，NIF 番号 1 の LINE 番号 0 にテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> test interfaces nif 1 line 0 local[Enter]
```

（約1分間待つ）

```
> no test interfaces nif 1 line 0[Enter]
```

注：

テスト実行結果の画面で ” Test Count ” が 0 の場合は，show interfaces コマンドで回線状態を確認してください。

上記以外のテスト実行結果の確認は「(1) モジュール内部ループバックテスト」のテスト実行結果と同様に行ってください。

### (5) リモートモデムループバックテスト（RLB）

本テストは serial 回線（V.24）で，かつモデムを接続している場合にだけ実行可能です（V.35，X.21 では使用できません)。また，モデムはリモートモデムループバックテストに対応している必要があります。

本テストでは，テスト用フレームはリモート（相手局側）モデムで折り返します。

テスト例として，NIF 番号 1 の LINE 番号 0 にテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> test interfaces nif 1 line 0 remote[Enter]
```

（約1分間待つ）

```
> no test interfaces nif 1 line 0[Enter]
```

注：

テスト実行結果の画面で ” Test Count ” が 0 の場合は，show interfaces コマンドで回線状態を確認してください。

上記以外のテスト実行結果の確認は「(1) モジュール内部ループバックテスト」のテスト実行結果と同様に行ってください。

## (6) リモートラインループバックテスト

本テストは本装置と相手装置の当該 Line 上で異常が発生した場合，フレーム単位のテスト用データにより障害発生部位切り分けや，障害部品交換後の動作確認時に使用します。テスト用データは，相手装置にて物理層フレームごとに折り返されます。T1 回線※および T3 非多重回線だけ実行可能です。また，相手装置はリモートラインループバックテストに対応している必要があります。ただし，T3 非多重回線の場合，リモートループバックテスト要求には，ループバック種別の指定がありません。このため，リモートループバックテスト実行時のループバック種別は，接続装置の設定によりラインループバックかペイロードループバックのどちらかとなります。本装置のリモートラインループバックテストは，接続装置のループバック種別設定によらずテストが実行可能です。なお，本装置でのループバック種別の指定は「構成定義コマンドレファレンス Vol.1　line（Line 情報）(-remote_loopback)」を参照してください。

注※

フレームフォーマットが ESF の場合だけ実行可能です。
ただし，次の場合は，テスト実行できませんのでリモートラインインバンドループバックテストを実行してください。

- フレームフォーマット＝ SF
- フレームフォーマット＝ ESF かつデータリンク＝ AT & T

なお，T3 多重回線内の T1 回線では未サポートです。

テスト例として，NIF 番号 1 の LINE 番号 0 にテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> test interfaces nif 1 line 0 remote-line[Enter]
```

（約1分間待つ）

```
> no test interfaces nif 1 line 0[Enter]
```

注：

テスト実行結果の画面で ” Test Count ” が 0 の場合は，show interfaces コマンドで回線状態を確認してください。
上記以外のテスト実行結果の確認は「(1) モジュール内部ループバックテスト」のテスト実行結果と同様に行ってください。

## (7) ネットワークラインループバックテスト

本テストは受信したデータの折り返し設定だけ行います。T1 回線，E1 回線，T3 非多重，E3 非多重，E3 多重回線，T3 多重回線，OC-3c（8 ポート），OC-12c（4 ポート），および OC-48c だけ実行可能です。

相手装置から受信したデータは，物理層フレームごとに折り返します。

テスト例として，NIF 番号 1 の LINE 番号 0 にテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> test interfaces nif 1 line 0 local network-line[Enter]
```

（約1分間待つ）

```
> no test interfaces nif 1 line 0[Enter]
```

注：

本テストは，受信データの折り返し設定だけを行うため，テスト結果表示はありません。このため，テスト間隔，テストパターン番号，テストデータ長は，指定不可となります。

## (8) ネットワークペイロードループバックテスト

本テストは受信したデータの折り返し設定だけ行います。T1 回線※および E1 回線だけ実行可能です。

注※　T3 多重回線内の T1 回線では未サポートです。

相手装置から受信したデータは，物理層フレーム内のデータ部分だけ折り返します。

テスト例として，NIF 番号 1 の LINE 番号 0 にテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> test interfaces nif 1 line 0 network-payload[Enter]
```

（約1分間待つ）

```
> no test interfaces nif 1 line 0[Enter]
```

注：

本テストは，受信データの折り返し設定だけを行うため，テスト結果表示はありません。このため，テスト間隔，テストパターン番号，テストデータ長は，指定不可となります。

## (9) リモートペイロードループバックテスト

本テストは本装置と相手装置の当該 Line 上で異常が発生した場合，フレーム単位のテスト用データにより障害発生部位切り分けや，障害部品交換後の動作確認時に使用します。テスト用データは，相手装置にて物理層フレーム内のデータ部分だけ折り返されます。T1 回線※だけ実行可能です。また，相手装置はリモートペイロードループバックテストに対応している必要があります。

注※　T3 多重回線内の T1 回線では未サポートです。

テスト例として，NIF 番号 1 の LINE 番号 0 にテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> test interfaces nif 1 line 0 remote-payload[Enter]
```

（約1分間待つ）

```
> no test interfaces nif 1 line 0[Enter]
```

注：

テスト実行結果の画面で ” Test Count ” が 0 の場合は，show interfaces コマンドで回線状態を確認してください。
上記以外のテスト実行結果の確認は「(1) モジュール内部ループバックテスト」のテスト実行結果と同様に行ってください。

### (10) リモートラインインバンドループバックテスト

本テストは本装置と相手装置の当該 Line 上で異常が発生した場合，フレーム単位のテスト用データにより障害発生部位切り分けや，障害部品交換後の動作確認時に使用します。テスト用データは，相手装置にて物理層フレームごとに折り返されます。T1 回線だけ実行可能です。また，相手装置はリモートラインインバンドループバックテストに対応している必要があります。

テスト例として，NIF 番号 1 の LINE 番号 0 にテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> test interfaces nif 1 line 0 remote-line-inband[Enter]
```

（約1分間待つ）

```
> no test interfaces nif 1 line 0[Enter]
```

注 1：
テスト実行結果の画面で ” Test Count ” が 0 の場合は，show interfaces コマンドで回線状態を確認してください。
上記以外のテスト実行結果の確認は「(1) モジュール内部ループバックテスト」のテスト実行結果と同様に行ってください。

注 2：
フレームフォーマットが SF，かつリモートラインループバックテストを実行する場合，本テストを実行してください。

## 8.7.3 ATM 回線

ATM の回線テストでは，モジュール内部ループバックテストおよびループコネクタループバックテストができます。コマンドの詳細は「運用コマンドレファレンス Vol.1　test interfaces（ATM）」および「運用コマンドレファレンス Vol.1　no test interfaces（ATM）」を参照してください。

### (1) モジュール内部ループバックテスト

本テストでは，本装置はテスト用フレームを送信し，NIF ボード内で折り返して受信します。

次に，NIF 番号 0 の Line 番号 0 をテストした例を示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> test interfaces nif 0 line 0 internal[Enter]
```

（約1分間待つ）

```
> no test interfaces nif 0 line 0[Enter]
```

コマンド実行結果として，「図 8-14　ATM の test interfaces，no test interfaces コマンド実行結果例」に示す画面を表示しますので，” Send-NG ” および ” Receive-NG ” が 0 であることを確認してください。”

Send-NG ”および ” Receive-NG ” が 0 の場合，回線テスト結果は正常です。

注：

” Send-NG ”および ” Receive-NG ” が 0 でない場合は，何らかの異常がありますので「運用コマンドレファレンス Vol.1　no test interfaces（ATM）」の回線テスト実行結果の表示内容を参照してください。

**図 8-14　ATM の test interfaces，no test interfaces コマンド実行結果例**

```
> test interfaces nif 1 line 0 internal
You have warning message. Use “show warning” to see them.
>
08/02 10:36:18 E4 LINEATM NIF:1 LINE:0 32020000 1550:700000000000 Line status
become up.
> no test interfaces nif 1 line 0
1999/08/02 10:37:13
Interface type              :OC-3c/STM-1 ATM(multi-mode)
Test Count                  :48
Send-OK                     :48             Send-NG                 :0
Receive-OK                  :48             Receive-NG              :0
Timeout                     :0              Data compare error      :0
<AAL layer>
NIF buffer busy             :0              RP buffer busy          :0
Overrun                     :0              T1 timeout              :0
CRC32 error                 :0              AAL5 length mismatch    :0
Long pkts                   :0              Short pkts              :0
<ATM layer>
Overrun                     :0              Invalid VPI/VCI         :0
Uncorrectable HEC error     :0
<PHY layer>
PHY layer status :up
LOS             :0          LOF             :0          OOF         :0
LOP             :0          LOC             :0          OOCD        :0
L-RDI           :0          P-RDI           :0          L-AIS       :0
P-AIS           :0          L-FEBE          :0          P-FEBE      :0
L-BIP24         :0          P-BIP8          :0          S-BIP8      :0
Symbol error    :0
>
08/02 10:37:18 E4 LINEATM NIF:1 LINE:0 32020000 1550:700000000000 Line status
become up.
>
```



## (2) ループコネクタループバックテスト

本テストでは，本装置はテスト用フレームを送信し，NIF ボードに接続したループコネクタ内で折り返し

て受信します。テスト対象の Line 位置のコネクタにループコネクタを接続したあと，テストを行います。ループコネクタ未接続の場合，および回線種別に対応するループコネクタを接続しない場合，正しくテストができませんのでご注意ください。

次に NIF 番号 0 の Line 番号 0 をテストした例を示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> test interfaces nif 0 line 0 connector[Enter]
```

（約1分間待つ）

```
> no test interfaces nif 0 line 0[Enter]
```

テスト実行結果の確認は「(1) モジュール内部ループバックテスト」のテスト実行結果と同様に行ってください。

注：

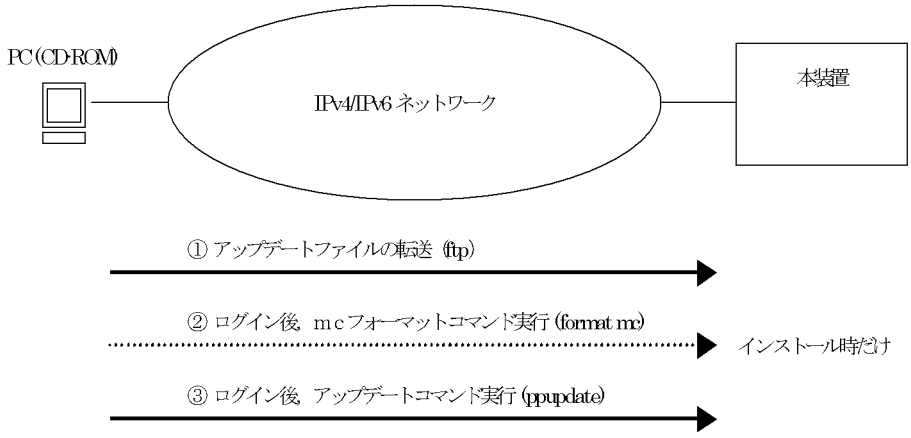
構成定義情報 line の clock=external（デフォルト）設定の場合，ケーブルを抜いた状態あるいはループコネクタを接続した状態では回線からのクロック供給が無いため，NIF ボード上の ACT ランプが消灯し，LINE ERR ランプが点灯します。これは問題ありませんので，テストを継続実施してください。テスト時は内蔵クロックに切り替わり，送受信動作します。なお，clock=independent 設定の場合は上記のような ACT ランプ消灯および LINE ERR ランプ点灯状態にはなりません。

# 9 ソフトウェアアップデート

この章では，ソフトウェアのアップデートやインストールの概念，代表的なトラブルについて説明します。実際のアップデート，インストール手順については，ソフトウェア添付資料「インストールガイド」を参照してください。

# 9.1 概要

ソフトウェアのアップデートは，PC などのリモート運用端末からアップデートファイルを装置に転送し，アップデートコマンド（ppupdate）を実行することによって行います。なお，インストール時にはフォーマットコマンド（format mc）の実行が別途必要となります。




アップデートとは

アップデートとは，旧バージョンのソフトウェアから新バージョンのソフトウェアにバージョンアップを行うことをいいます。

アップデートは，アップデート用のファイルを本装置に転送し，ppupdate コマンドを実行することにより行います。アップデートの場合，装置構成定義情報およびユーザ情報（ログインアカウント，パスワードなど）はそのまま引き継がれます。

インストールとは

インストールとは，予備 MC スロット（secondary）の MC に対して新規にソフトウェアをインストールすることをいいます。

インストールは，アップデート用のファイルを本装置に転送し，予備 MC スロットの MC を format mc コマンドでフォーマットして ppupdate コマンドを予備 MC に対して実行することにより行います。インストールの場合，装置構成定義情報およびユーザ情報は初期状態（工場出荷時の状態）となります。インストールは予備 MC に対してだけ実行可能です。

アップデートおよびインストールはどちらの場合も，CD-ROM 内のアップデート用ファイルを装置に転送後，ppupdate コマンドを実行することにより行います。

# 9.2 アップデート後の作業

本装置のソフトウェアアップデート時に発生する代表的なトラブルについて，対処方法を次に示します。その他のトラブルと対処方法については，ソフトウェア添付資料「インストールガイド」を参照してください。

### (1) 装置が立ち上がらない

1. ソフトウェアアップデートが正常に終了しなかった可能性があります。ソフトウェアを再インストールしてください。
2. アップデート前の構成定義情報をバックアップしてある場合，構成定義情報をバックアップからコピーしてください。アップデート前の構成定義情報をバックアップしていない場合は，装置を起動後，再作成してください。
3. 装置を再立ち上げしてください。

### (2) 装置は立ち上がるが正常に動作しない

1. 構成定義情報が機器構成と合っていない可能性があります。ソフトウェアアップデートと合わせて構成定義情報の変更や機器の増移設を行った場合は，変更内容および増移設した機器を再確認してください。

新ソフトウェアでは，旧ソフトウェアと構成定義パラメータのデフォルト値が異なっていることがあります。ソフトウェア添付資料を参照のうえ，構成定義情報・機器構成を再確認してください。

# 付録

付録 A　用語解説

# 付録 A　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。

### 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－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

## N



## O



## P



## Q



## R



## S



## T



## U



## V



## W



## Z



## い

## う



## え



## お



## か



## き



## く



## け



## こ



## さ



## し



## す



## そ



## た



## つ

## と



## に



## ね



## は



## ひ



## ふ



## へ



## ほ



## ま



## み



## め



## も



## ゆ



## り



## る

## ろ