MR1000

取扱説明書

機能説明書

OMRON

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
インターネットやLANをさらに活用するために、本装置をご利用ください。

2005年1月

目次

本書の構成と使いかた

本書では、一般的なネットワークの概要や本装置で使用できる便利な機能について説明しています。
また、CD-ROMの中のREADMEファイルには大切な情報が記載されていますので、併せてお読みください。

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。
本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

本書の構成

以下に、本書の構成と各章の内容を示します。

章タイトル	内　容
第1章　ネットワーク設計概念	この章では、一般的なネットワークの設計概念について説明します。
第2章　機能概要	この章では、本装置の主な機能の概要を説明します。

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。

本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。

こんな事に気をつけて　**本装置をご使用になる際に、注意していただきたいことを説明しています。**

操作手順で説明しているものの他に、補足情報を説明しています。

操作方法など関連事項を説明している箇所を示します。

本書における商標の表記について

RSAおよびMD5は、RSA Security Inc.が開発した暗号およびハッシュアルゴリズムです。
Windowsは、米国Microsoft Corporationの米国およびその他の国における登録商標です。
Hi/fnおよびLZSは、Hi/fn,inc.の登録商標です。
本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

使用許諾条件

本製品には、カリフォルニア大学およびそのコントリビュータによって開発され、下記の使用条件とともに配付されている FreeBSDの一部が含まれています。
@(#)COPYRIGHT 8.2 (Berkeley) 3/21/94

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase "this text" refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase "This material" refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

本製品には、カリフォルニア大学バークレイ校において開発されたソフトウェアが含まれています。

Copyright © 1989 Regents of the University of California. All rights reserved.

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

本製品には、WIDEの KAMEプロジェクトによって開発され、下記の使用条件とともに配付されているソフトウェアが含まれています。

Copyright © 1995,1996,1997,and 1998 WIDE Project.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

本製品には、スタンフォード大学よって開発され、下記の使用条件とともに配布されている mrouted の一部が含まれています。

The mrouted program is covered by the following license. Use of the mrouted program represents acceptance of these terms and conditions.

1. STANFORD grants to LICENSEE a nonexclusive and nontransferable license to use, copy and modify the computer software ''mrouted'' (hereinafter called the ''Program''), upon the terms and conditions hereinafter set out and until Licensee discontinues use of the Licensed Program.
2. LICENSEE acknowledges that the Program is a research tool still in the development state, that it is being supplied ''as is,'' without any accompanying services from STANFORD, and that this license is entered into in order to encourage scientific collaboration aimed at further development and application of the Program.
3. LICENSEE may copy the Program and may sublicense others to use object code copies of the Program or any derivative version of the Program. All copies must contain all copyright and other proprietary notices found in the Program as provided by STANFORD. Title to copyright to the Program remains with STANFORD.
4. LICENSEE may create derivative versions of the Program. LICENSEE hereby grants STANFORD a royalty-free license to use, copy, modify, distribute and sublicense any such derivative works. At the time LICENSEE provides a copy of a derivative version of the Program to a third party, LICENSEE shall provide STANFORD with one copy of the source code of the derivative version at no charge to STANFORD.
5. STANFORD MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED.By way of example, but not limitation, STANFORD MAKES NO REPRESENTATION OR WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED PROGRAM WILL NOT INFRINGE ANY PATENTS,COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. STANFORD shall not be held liable for any liability nor for any direct, indirect or consequential damages with respect to any claim by LICENSEE or any third party on account of or arising from this Agreement or use of the Program.
6. This agreement shall be construed, interpreted and applied in accordance with the State of California and any legal action arising out of this Agreement or use of the Program shall be filed in a court in the State of California.
7. Nothing in this Agreement shall be construed as conferring rights to use in advertising, publicity or otherwise any trademark or the name of ''Stanford''.
The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

本製品には、南カリフォルニア大学およびそのコントリビュータによって開発され、下記の使用条件とともに配布されている pimd の一部が含まれています。

Copyright (c) 1998-2001
University of Southern California/Information Sciences Institute.All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

$Id: LICENSE,v 1.5 2001/09/10 20:31:36 pavlin Exp $
Part of this program has been derived from mrouted.
The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

本製品には、オレゴン大学によって開発され、下記の使用条件とともに配布されている pimdd の一部が含まれています。

Copyright (c) 1998 by the University of Oregon.All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation in source and binary forms for lawful purposes and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that any documentation, advertising materials,and other materials related to such distribution and use acknowledge that the software was developed by the University of Oregon.The name of the University of Oregon may not be used to endorse or promote products derived from this software without specific prior written permission.

THE UNIVERSITY OF OREGON DOES NOT MAKE ANY REPRESENTATIONS ABOUT THE SUITABILITY OF THIS SOFTWARE FOR ANY PURPOSE. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES,INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

IN NO EVENT SHALL UO, OR ANY OTHER CONTRIBUTOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, WHETHER IN CONTRACT,TORT, OR OTHER FORM OF ACTION, ARISING OUT OF OR IN CONNECTION WITH,THE USE OR PERFORMANCE OF THIS SOFTWARE.

Other copyrights might apply to parts of this software and are so noted when applicable.

Questions concerning this software should be directed to Kurt Windisch (kurtw@antc.uoregon.edu)

$Id: LICENSE,v 1.2 1998/05/29 21:58:19 kurtw Exp $

Part of this program has been derived from PIM sparse-mode pimd.
The pimd program is covered by the license in the accompanying file named "LICENSE.pimd".

The pimd program is COPYRIGHT 1998 by University of Southern California.

Part of this program has been derived from mrouted.

The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

Copyright (c) 1998 by the University of Southern California.All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation in source and binary forms for lawful purposes and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that any documentation, advertising materials,and other materials related to such distribution and use acknowledge that the software was developed by the University of Southern California and/or Information Sciences Institute.
The name of the University of Southern California may not be used to endorse or promote products derived from this software without specific prior written permission.

THE UNIVERSITY OF SOUTHERN CALIFORNIA DOES NOT MAKE ANY REPRESENTATIONS ABOUT THE SUITABILITY OF THIS SOFTWARE FOR ANY PURPOSE. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES,INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

IN NO EVENT SHALL USC, OR ANY OTHER CONTRIBUTOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, WHETHER IN CONTRACT,TORT, OR OTHER FORM OF ACTION, ARISING OUT OF OR IN CONNECTION WITH,THE USE OR PERFORMANCE OF THIS SOFTWARE.

Other copyrights might apply to parts of this software and are so noted when applicable.

Questions concerning this software should be directed to Pavlin Ivanov Radoslavov (pavlin@catarina.usc.edu)

$Id: LICENSE.pimd,v 1.1 1998/05/29 21:58:20 kurtw Exp $

Part of this program has been derived from mrouted.
The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

本製品には、RSA Data Security 社が著作権を有している MD5 Message-Digest Algorithm が含まれています。

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

本製品には、Eric Young 氏 (eay@cryptsoft.com) によって記述された暗号ソフトウェアが含まれています。

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

本製品には、OpenSSL ツールキットを使用するために OpenSSL Project (http://www.OpenSSL.org/) によって開発されたソフトウェアが含まれています。

Copyright (c) 1999 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project
for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact licensing@OpenSSL.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

第1章
ネットワーク設計概念

この章では、一般的なネットワークの設計概念について説明します。

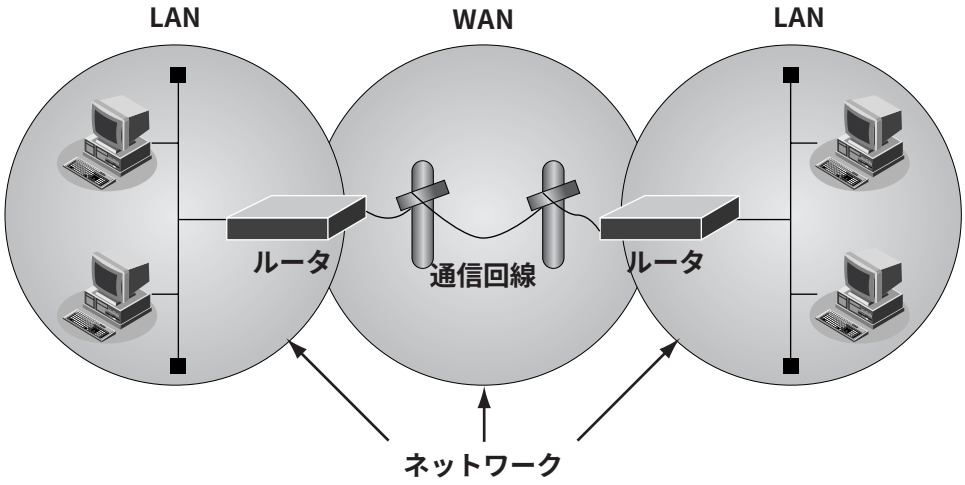
1.1　ネットワーク設計概念

ここでは、本装置を利用してネットワークを設計する際に留意しなくてはならないネットワークの概念と、本装置のネットワーク定義の考え方について説明します。

1.1.1　ネットワークの概念とルーティング

ネットワークの考え方

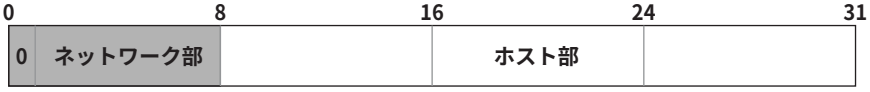
ネットワークとは、通信手段を備えたコンピュータどうしがなんらかの伝送媒体を介して接続した集合体のことです。たとえば、構築された1つのLANは、HUBやスイッチなどの装置によって1つのネットワークとなります。一般加入線や専用回線などを利用して遠隔地を接続しているWANと呼ばれる部分についても、同様に1つのネットワークとなります。また、広義の意味で、これら1つ1つのネットワークが接続された全体もネットワークとなります。



IPネットワーク

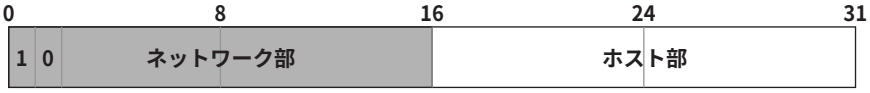
IPネットワークでは、接続されるすべてのコンピュータ（ホスト）やルータなどのネットワーク機器にそれぞれ唯一なIPアドレスを割り当てる必要があります。このIPアドレスは「ネットワーク部」と「ホスト部」から構成されます。

クラスA 各ネットワークにホストが多く存在し、ネットワーク数が少ない場合



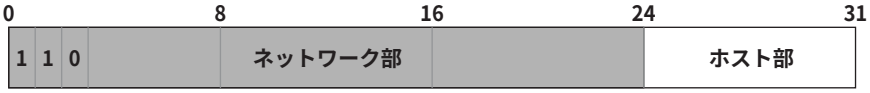
プライベートアドレス: 10.0.0.0～10.255.255.255

クラスB ネットワーク、ホストともに多い場合



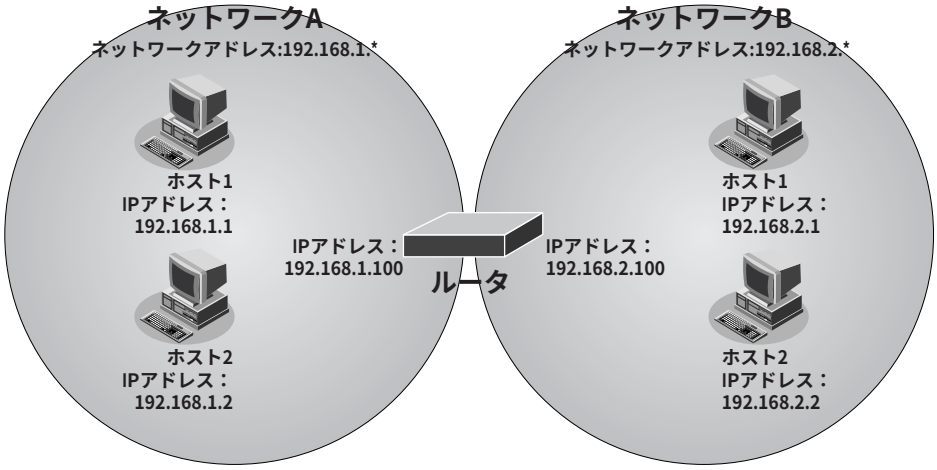
プライベートアドレス: 172.16.0.0～172.31.255.255

クラスC ネットワークごとのホストが少なく、ネットワーク数が多い場合



プライベートアドレス: 192.168.0.0～192.168.255.255

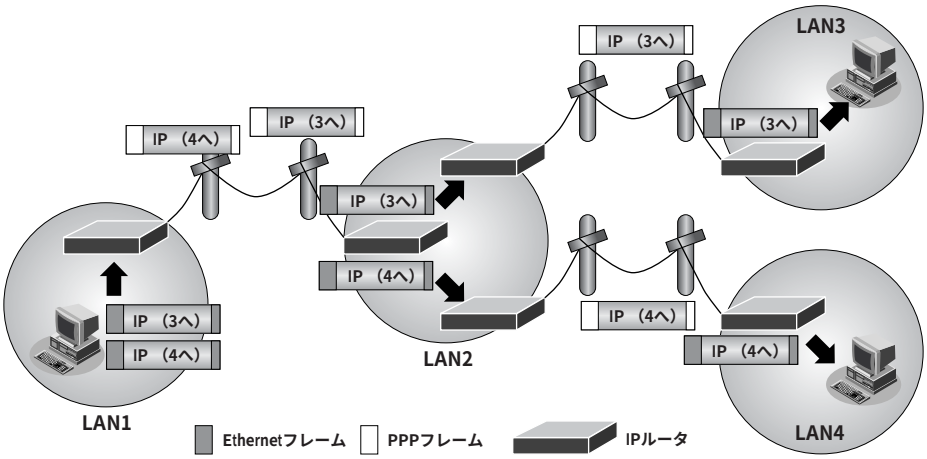
IPネットワークでの1つのネットワークとは、IPアドレスのネットワーク部が同じアドレスを持つ機器の集まりです。つまり、同じデータリンクに接続される機器にはすべて同じネットワークアドレスを設定しなければなりません。さらに、ほかのデータリンクとネットワークアドレスが重ならないように割り当てる必要があります。



以降、本書では、IPの同じネットワーク群のことを「ネットワーク」と言います。また、広義のネットワークについては「ネットワーク全体」と言います。

ネットワークとルータ

本装置は、ネットワークとネットワークを相互に接続するルータと呼ばれる装置です。ルータは、IPパケットと呼ばれる転送単位ごとにパケットに付加されているIPアドレスのネットワーク部の情報に従って通信します。ほかのネットワークあてのデータはデータを転送することにより、ネットワーク間での通信を実現しています。この動作をルーティング（経路制御）と言い、このときにどのネットワークがどこにあるのかを知るために必要な情報を経路情報と言います。ルータはあらかじめ作成された経路情報の集まりであるルーティングテーブル（経路制御表）によって動作します。ルーティングテーブルの作成方法には、2種類の方法があります。管理者があらかじめ装置ごとに設定しておくスタティックルーティングと、接続されているルータどうしで情報を交換しあって自動的に作成するダイナミックルーティングです。



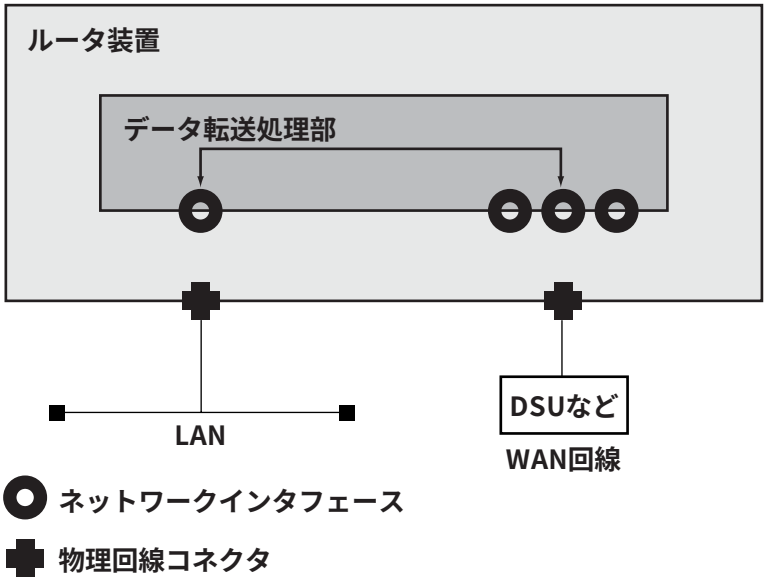
なお、本装置ではIP以外のパケットを転送する機能であるブリッジについてもサポートしています。IPアドレスを持たないIP以外のパケットは、Ethernetフレームの情報に従って適切な相手にデータを転送することができます。

ネットワークインタフェースの概念

ルータがデータを送信または受信する場合は、論理的な出入り口が必要となります。

この出入り口をネットワークインタフェースと言い、すべてのデータの送受信はネットワークインタフェースを通じて行われます。

基本的には、ネットワークインタフェースは物理回線と１対１に対応します。ただし、PPP通信やトンネル通信などのように物理回線と等価に見える論理的な通信路もあるため、ネットワークインタフェースはパケット転送処理のための論理的な出入り口と考える必要があります。



ルーティングによる転送

ルーティングはネットワーク層プロトコルの情報によってデータの転送先を決定します。データ転送はパケットと呼ばれる通信単位ごとに転送先を選択し、転送先に対してデータを転送します。このとき、転送先を選択するための情報としてルーティングテーブル（経路制御表）を利用します。ルーティングテーブルとは「そのネットワークにデータを転送するためには、次にどの装置に対して転送したらよいか」を管理するテーブルです。ルーティングによる転送は、個々のパケットに含まれるあて先IPアドレスを元に経路情報を検索し、その経路に従って送出先を決定します。決定される情報は、出口となるネットワークインタフェースと、経由すべき次装置のアドレス（これは存在しない場合もあります）となります。

例：192.168.2.1 あてのパケットを転送する場合

経路情報

あて先ネットワーク	次装置アドレス	出口インタフェース
192.168.1.0/24	—	lan0
192.168.2.0/24	192.168.1.2	lan0
:	:	:

この経路情報から、192.168.2.1 に到達するために出口となるネットワークインタフェースはlan0であり、次装置は 192.168.1.2 であると判定されます。

この経路選択による出力先の選定は受信したデータに対してだけではなく、本装置が生成するデータについても同様に適用されます。つまり、経路情報が存在しないと装置からデータを送信することができません。このため、最低でも１つの経路情報を設定する必要があります。

ブリッジによる転送

もっとも簡単なブリッジによる転送の構造は、受信したデータをほかのすべてのネットワークインタフェースに対して送信するものです。しかし、これではトラフィックが膨大になるため、学習機能や制御プロトコルによって適切なネットワークインタフェースだけに転送することが一般的です。ルーティングと同じく、ここでもその出口ネットワークインタフェースの選定処理が行われます。

1.1.2　ルータ設定の概要

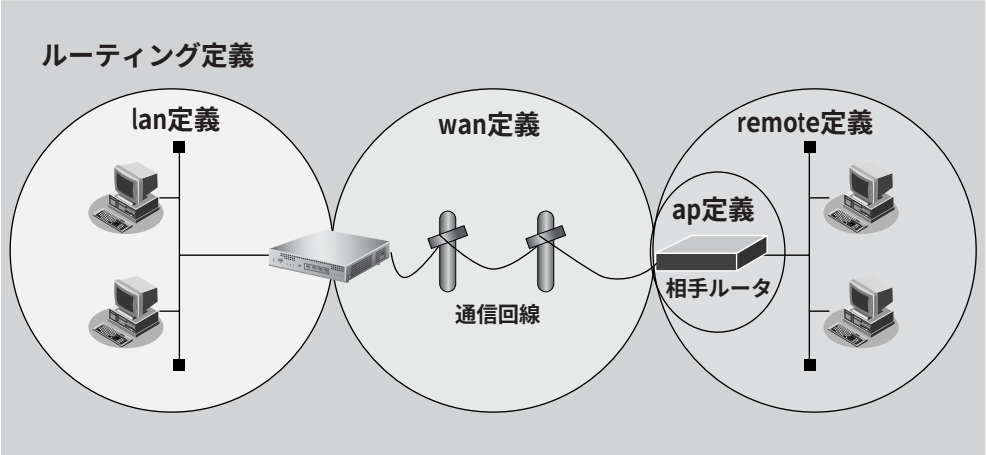
ネットワークと設定の関係

ルータに設定すべき情報としては、接続する回線に関する物理的な情報、接続するネットワークに関する論理的な情報、およびデータの振り分け条件である経路情報が必ず必要となります。また、ほかに装置固有の情報や、付加的なサービスの設定を必要に応じて行います。

本装置では、これらの情報の設定に関して、大きく以下のように分類しています。

- wan定義
  本装置に接続する回線に関する物理的な情報を定義する命令群です。回線の種類や電話番号などの契約に関する情報を定義します。
- lan定義
  本装置に接続するLANに関する論理的な情報を定義する命令群です。LANのアドレスやネットワークの情報などを定義します。また、DHCPなどのLANに固有のサービスに関してもlan定義によって定義します。
- remote定義
  本装置がwan回線を通じて通信を行う相手に関する論理的なネットワーク情報を定義する命令群です。PPPに関する情報や相手ネットワークの接続先に関する情報などを定義します。
- answer定義
  本装置が発信者番号で特定できない相手から接続される場合の情報を定義する命令群です。発信者番号チェックを行わないremote定義の中からPPP認証が一致するremote定義を検索して着信を行います。アナログモデムで着信を行う場合など必要に応じて定義します。
- template定義
  本装置がremote定義やanswer定義を使わずに、着信情報のひな形であるtemplate定義と認証情報などの個別情報をもつAAA定義とを用いて、不特定相手着信や多数の接続相手を受け付けるなど、リモートアクセスサーバを実現する場合に定義します。
- その他の定義
  装置固有の情報や付加サービスの情報を必要に応じて定義する命令群です。ネットワーク管理に関する情報や時刻情報などの定義があります。

各定義の分類と、実際のネットワークの対応を以下に示します。



ネットワークインタフェースの定義

データ転送時の出口となるネットワークインタフェースには、その特性や接続されている回線によっていくつかの種別があります。

以下に、ネットワークインタフェースの種別について説明します。

- lo
  ループバックインタフェース
  装置の内部プログラムで折り返し通信を行う場合に利用されます。外部から利用することはありません。
- lan
  Ethernetインタフェース
  Ethernetを利用して通信する場合に利用するネットワークインタフェースです。lan定義によって設定されます。
- rmt
  設定済み相手用通信インタフェース
  ISDN／専用線／フレームリレー／PPPoEなどの回線を利用して通信する場合、またはIPトンネルやIPsecトンネルを利用して通信する場合に、定義された相手システムとの通信に利用されるネットワークインタフェースです。remote定義によって設定されます。

これらのインタフェース種別にインタフェース番号を付与したものがネットワークインタフェース名となります。

例：lo0,lan0,lan1,rmt0,rmt1,...

lanおよびrmtのネットワークインタフェースはそれぞれlan定義、remote定義によって設定されます。lan定義、remote定義の定義番号とネットワークインタフェースのインタフェース番号は1対1に対応します。loは装置が自動設定するので、設定項目はありません。

経路情報の定義

経路情報は最終的に出口となるネットワークインタフェースを決定するために必要な情報を定義するものです。本装置では出口インタフェースに対応する定義内で経路情報を設定します。たとえば、lan0から出力するための経路情報はlan0内の定義に、rmt0から出力するための経路情報はremote0内の定義に分けて設定します。

高度な転送先選定定義

本来のIPルーティングでの送信先選定のルールでは、出力先インタフェースまでしか選定されません。このため、通常のIPルーティングでは、1つの経路によって決定される接続先は1つしか利用することができません。しかし、本装置では相手ネットワークの定義であるremote定義の配下に、実際の接続先設定となるap定義を複数定義することができます。

これは、経路情報によって決定された出力先のremote定義の範囲で、送信データ内のあて先IPアドレス以外の情報を経路情報の代わりに利用して、さらに送信先を分別するマルチルーティングという機能を利用して実現しています。たとえば、インターネットと通信するためにはデフォルトルートという経路情報が必要ですが、1つのremote定義でデフォルトルートを設定した場合、ほかのremote定義はデフォルトルートを設定できません。このため、通常のIPルーティングの機構では、必要に応じて、remote定義だけでISPを切り替えるということはできません。本装置のマルチルーティングは、ルーティング機構では参照されない情報を利用して、決定されたremote定義の範囲内で、さらに細分化された送信先を選定します。

本装置のマルチルーティング機能については、以下を参照してください。

☛参照「2.12 マルチルーティング（ポリシールーティング）機能」（P.52）

第２章　機能概要

この章では、本装置の主な機能の概要を説明します。

2.1　IPv6機能

IPv6とは、現在、主に利用されているIP（IPv4）を置き換えるための次世代インターネットプロトコルです。本装置では、IPv4パケットだけでなくIPv6パケットも転送することができます。

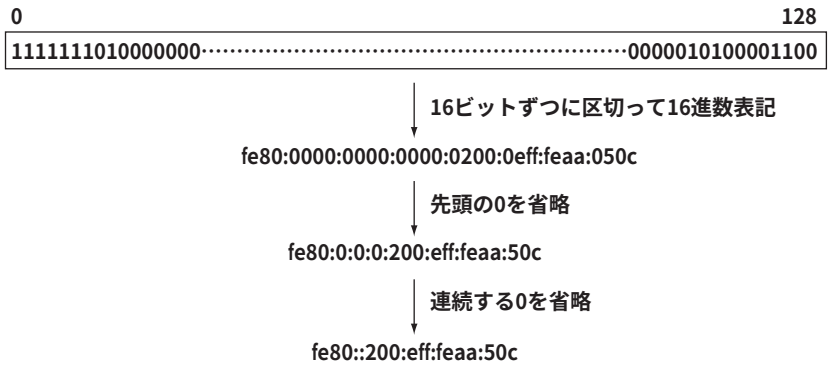
本装置がサポートしているIPv6機能は、以下のとおりです。

- 静的または動的な経路設定
- Router Advertisement Messageによるホストのアドレスの自動設定
- パケットフィルタリング
- IPv6 over IPv4 トンネル

IPv6アドレスの表記方法

128ビットのIPv6アドレスを表記する場合は、そのアドレスを「:」（コロン）で16ビットずつに区切って、その内容を16進数で記述します。個々の16進数の値について先頭の0は省略することができます。連続して0が続く場合は、1つのIPv6アドレスの表記で1回限り「::」で省略することができます。

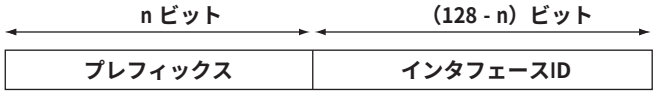
例を以下に示します。



IPv6アドレス体系

IPv6アドレスは、IPv4アドレスがネットワーク部とホスト部に分離することができるように、プレフィックスとインタフェースIDに分離することができます。一般的には、プレフィックスのビット長（プレフィックス長）は64ビットで利用されます。

プレフィックス長を含めてアドレス表記をする場合は、プレフィックス長はアドレスの後ろに「/」で区切って付与します。



IPv6で利用することができるアドレスは、IPv4と同様に、先頭のビット数によって利用方法が決められています。本装置で利用できるアドレスは以下のようなものがあります。

- Global Unicast Addresses
  通常利用するアドレスです。一般的には、契約したISPから割り当てられます。

- Link-Local Unicast Addresses（fe80::/64）
  link内（ルータを介さないで通信できる範囲）だけで有効な特別なアドレスです。このアドレスは先頭の10ビットが1111 1110 10で始まります。通常は11ビット目から64ビット目まではすべて0となります。
- Multicast Addresses
  マルチキャストアドレスです。先頭の8ビットが1111 1111となります。

静的または動的な経路設定

IPv6のネットワークとルーティングの概念は、IPv4の場合とほぼ同じです。装置が持つ経路情報に従って転送先を決定します。この経路情報を装置に持たせる方法として、静的な経路設定（スタティックルーティング）と動的な経路設定（ダイナミックルーティング）があります。

スタティックルーティングとは、経路情報を構成定義として設定し、利用します。この経路情報は構成定義を変更しない限り変更されることはありません。

ダイナミックルーティングとは、ルーティングプロトコルを利用する通信によって、ネットワーク上のほかのノードから経路情報を学習して利用します。本装置ではルーティングプロトコルとしてIPv6 RIPをサポートしています。

Router Advertisement Messageによるホストのアドレスの自動設定

本装置では、Router Advertisement Messageの機能をサポートしています。Router Advertisement Messageには、そのネットワークで利用するプレフィックスの情報が含まれています。このメッセージを受信したホストは、その情報を利用して、自身のIPv6アドレスを自動的に設定します。

パケットフィルタリング

本装置では、特定のIPv6パケットの通過を許可／禁止するためのパケットフィルタリング機能があります。

IPv6 over IPv4 トンネル

IPv6 over IPv4 トンネルとは、IPv6パケットをIPv4パケットでカプセル化して通信する方法です。これにより、IPv4だけを中継することができるルータ／ネットワークを経由してIPv6通信を行うことができます。

IPv6 over IPv4 トンネルを利用する場合は、カプセル化されたIPv4パケットのフラグメントを防ぐため、トンネルに利用する相手情報のMTUに1280を設定してください。

こんな事に気をつけて

本装置では、ファームウェアの更新やSNMPでの監視などの目的でIPv4のアドレスを使用します。そのため、IPv4のアドレスを設定しないで運用することはできません。IPv6およびブリッジだけを使用しているネットワークで運用する場合でも、どれかのインタフェースに必ずIPv4のアドレスを設定してください。

2.2 IP経路制御機能

IP経路情報は、ルーティングテーブルで管理され、IPパケットの転送先の判断に使用します。

IP経路情報は、以下の機能で制御します。

- インタフェースの障害検出による経路制御機能
- スタティックルーティング機能
- ダイナミックルーティング機能

ここでは、IP経路情報の種類、管理方法およびIP経路情報を制御する機能について説明します。

2.2.1 IP経路情報の種類

IP経路情報は、以下に示す情報で分類されます。

- インタフェース経路（IPv4）
  ネットワークインタフェース（lan、lo、rmt）に割り当てたIPv4ネットワークまたはIPv4アドレスを示します。loとrmtに割り当てたIPv4アドレスは、ホストルート（32ビットネットワークマスク）として管理されます。また、rmtは、自側と相手側の2つのホストルートとして管理されます。
- インタフェース経路（IPv6）
  ネットワークインタフェース（lan、rmt）に割り当てたIPv6プレフィックスを示します。
- スタティック経路
  構成定義として設定し、装置に保持される経路情報を示します。
- RIP経路
  RIPv1およびv2によって受信した経路情報を示します。
- BGP4経路
  BGP4によって受信した経路情報を示します。
- OSPF経路
  OSPFv2によって受信したリンク情報をもとに作成する最短経路（ショートパス）を示します。
- DNS経路（IPv4/IPv6）
  DNSサーバにより解決したホストルートを示します。
- RIP経路（IPv6）
  RIP（IPv6）によって受信した経路情報を示します。
- DHCP経路（IPv6）
  DHCPv6サーバ機能を使用し、クライアントにプレフィックスを配布する場合、クライアント側ネットワークと通信するために自動生成する経路情報を示します。

IP経路情報は、次に示す優先度値で管理されます。

IP経路情報	優先度値
インタフェース経路	0（固定）
スタティック経路	0（変更可）
RIP経路（IPv4/IPv6）	120（変更可）
BGP4経路（EBGP）	20（変更可）
BGP4経路（IBGP）	200（変更可）
OSPF経路	110（変更可）
DNS経路（IPv4/IPv6）	15（変更可）
DHCP経路（IPv6）	10（変更可）

2.2.2　IP経路情報の管理

IP経路情報は、ルーティングプロトコルの経路テーブルとルーティングテーブルで管理されます。
以下に、2つのテーブルについて説明します。

ルーティングプロトコルの経路テーブル

ルーティングプロトコルでは、以下のテーブルでIP経路情報を管理します。各テーブルには、最大エントリ数を規定しています。最大エントリ数を超えたIP経路情報は破棄されます。

☛参照　MR1000　仕様一覧「2.3 システム最大値一覧」（P.19）

- RIPテーブル
  RIPで使用する経路テーブルを示し、以下のものを含みます。
  - RIPで受信した経路情報
  - RIPに再配布した経路情報

  インタフェース経路を除いた経路情報をエントリ数として管理します。
- BGP4テーブル
  BGP4で使用する経路テーブルを示し、以下のものを含みます。
  - EBGP/IBGPで受信した経路情報
  - BGPに再配布した経路情報

  BGPネットワーク経路、BGP集約機能で生成された経路情報、およびBGP/MPLS VPNのIBGP受信経路を除いた経路情報をエントリ数として管理します。

こんな事に気をつけて

BGPテーブルの最大値は、接続数によって変わります。以下の条件で使用してください。
最大エントリ数＝（6000-（4000×（接続数-10））/190）

- VRFテーブル
  BGP/MPLS VPNで使用する経路テーブルを示し、以下のものを含みます。
  - IBGPで受信した経路情報（VPNv4）
  - IBGPに再配布したVPN用スタティック経路
- OSPFリンクステートデータベース（LSDB）
  OSPFで使用するリンク情報を保存するデータベースを示し、以下のものを含みます。
  - OSPFで受信したLSA情報
  - OSPFに再配布した経路情報

  再配布した経路情報もLSAで管理され、LSA数として最大保有数を規定します。
- RIP（IPv6）テーブル
  RIP（IPv6）で使用する経路テーブルを示し、以下のものを含みます。
  - RIP（IPv6）で受信した経路情報
  - RIP（IPv6）に再配布した経路情報

  RIP集約経路およびインタフェース経路を除いた経路情報をエントリ数として管理します。

ルーティングテーブル

ルーティングテーブルは、IP経路情報の中から選択した優先経路（ベストパス）で構成されます。また、ルーティングテーブルで管理するIP経路情報の中で、インタフェース経路を除いたものをルーティングエントリ数として管理します。

ルーティングエントリは、装置ごとに最大エントリ数を規定し、最大エントリ数を超えた経路情報は破棄されます。

なお、IPv4とIPv6では別々に管理されます。

☛参照　MR1000　仕様一覧「2.3 システム最大値一覧」（P.19）

こんな事に気をつけて

ルーティングプロトコルの経路テーブルで、最大エントリ数を超えた経路情報は破棄され、エントリ数を超えたことを示すシステムログ情報が記録されます。このとき、装置の再起動を行わないと反映されないことがあります。必要な経路情報の有無を確認のうえ、装置の再起動などの対処を行ってください。
たとえば、スタティック経路を追加設定した際に経路テーブルオーバが発生した場合は、装置の再起動を行ってください。

2.2.3　インタフェースの障害検出による経路制御機能

インタフェースの障害検出（ハードウェアによる異常検出など）により、インタフェース経路情報をルーティングテーブルから削除することができます（インタフェース経路のフローティング機能）。このインタフェース経路の削除により、スタティックルーティング機能やダイナミックルーティング機能で作成されるIP経路情報（同じあて先の経路情報）への切り替えを行うことができます。インタフェース経路のフローティング機能が無効の場合、インタフェースの通信状態に関係なく、インタフェース経路はルーティングテーブルで常に有効なIP経路情報と扱われます。

また、インタフェースの障害検出は、スタティックルーティング機能およびダイナミックルーティング機能で使用するインタフェースの異常として通知され、スタティックルーティング機能およびダイナミックルーティング機能の中で経路切り替えを行うことができます。

こんな事に気をつけて

本装置の初期設定では、インタフェース経路のフローティング機能は無効となっています。

2.2.4　スタティックルーティング機能

スタティック経路を使用し、以下の機能と組み合わせることにより、IP経路情報を制御します。

また、優先度が同一値のスタティック経路を使用することにより、ECMP機能で使用するIP経路情報を作成できます。

☛参照 「2.23 ECMP機能」（P.83）

- インタフェースの障害検出による経路制御機能
  インタフェースの障害検出により、該当インタフェースを出口とする優先度1以上のスタティック経路をルーティングテーブルから削除することができます。ただし、優先度0のスタティック経路を使用した場合は、インタフェースの障害に関係なく、常に有効なIP経路情報として扱われ、ルーティングテーブルから削除されません。インタフェースの障害検出に連動して、優先度0のスタティック経路を削除する場合は、インタフェース経路のフローティング機能を有効に設定してください。
- 優先経路制御機能
  同じあて先の経路に対して、優先度（distance）によって、ルーティングテーブルに追加するIP経路情報を選択することができます。優先度が小さいほど優先経路と扱われ、優先経路だけをルーティングテーブルに反映します。また、この優先経路が無効となった場合、次の優先経路に切り替えることができます。

こんな事に気をつけて

スタティック経路の設定で、優先度を省略時、優先度に0が設定されるため、優先経路として扱われます。

2.2.5　ダイナミックルーティング機能

ルーティングプロトコルが経路情報の送受信を行うことにより、IP経路情報を制御します。
本装置のルーティングプロトコルとして RIP、BGP4、OSPFおよびIPv6 RIPをサポートします。

なお、OSPFでは、ECMP機能で使用するIP経路情報を作成できます。

☛参照 「2.3 RIP機能」（P.28）、「2.4 BGP4機能」（P.30）、「2.5 OSPF機能」（P.33）、「2.6 IPv6 RIP機能」（P.35）、「2.23 ECMP機能」（P.83）

また、以下のIP経路制御機能をサポートしています。

- 経路再配布機能
  ルーティングテーブルに登録されたIP経路情報をルーティングプロトコルに取り込むことができます。本機能を使用することでルーティングプロトコルで受信した経路やスタティック経路などを異なるルーティングプロトコルで広報することができます。IPv4経路情報からIPv6経路情報、また、IPv6経路情報からIPv4経路情報への経路再配布はできません。
- インタフェースの障害検出による経路制御機能
  インタフェースの障害検出により、該当インタフェースを介して受信した経路情報をルーティングテーブルから削除できます。また、該当インタフェースを出口とする経路情報を再配布している場合、それらの経路情報が無効になったことを即座に広報することができます。
- 優先経路制御機能
  同じあて先の経路に対して、優先度（distance）によって経路を選択することができます。優先度が小さいほど優先経路として扱われ、優先経路だけをルーティングテーブルに反映します。また、この優先経路が無効となった場合、次の優先経路に切り替えることができます。IPv4経路情報とIPv6経路情報との間で、優先経路制御はできません。
- 経路フィルタリング機能
  RIPとBGP4では、送受信するIP経路情報に対してフィルタリングすることができます。
- 再配布フィルタリング
  IPv4ルーティングでは、RIP、OSPFおよびBGP4に取り込むIP経路情報に対してフィルタリングすることができます。また、IPv6ルーティングでは、IPv6 RIPに取り込むIP経路情報に対してフィルタリングすることができます。このフィルタリングは、条件に一致した場合の動作として、“透過”または“遮断”を指定することができます。

⚠注意

ダイナミックルーティングで、WAN側のホストルート（インタフェース経路）を広報する設定を行ったとき、経路情報の交換が正しく行われず、接続できない場合があります。特に、IP-VPN網などに接続する場合は、接続・切断を繰り返すことがあります。このような環境では、インタフェース経路を広報しない設定を行うか、またはWAN側のホストルートに対し、経路フィルタリングを使用してください。

こんな事に気をつけて

- **IPv4セカンダリアドレスが属するネットワーク上では、ルーティングプロトコルによる経路交換を行うことはできません。**
- **ダイナミックルーティングで利用するインタフェースは RIPv1/v2を除き、IPアドレスを設定する必要があります。**
- **経路情報を多く保持している状態や多くのインタフェースを定義してある状態で、定義の設定（enable allコマンドの実行など）を行った場合、経路情報のすべての変更が行われるため、enableコマンドの完了までに5分程度がかかることがあります。この完了時間は、経路数や定義数に比例します。**

2.3 RIP機能

RIP（Routing Information Protocol）は、ルータ間で使用するダイナミックルーティングプロトコルです。RIPプロトコルを使用するルータ間で経路情報の交換を行い、パケットを転送する経路を制御します。各ルータは、あて先のネットワークに到達するために、いくつのルータを経由する（ホップ数）かという情報を保持します。また、該当するあて先に対してホップ数が一番少ない経路を使用してパケットを転送するという動作を行います。

RIP機能を使用した場合、直接接続しているネットワークの各ルータに対して、定期的に自装置が保持している経路情報を広報します。起動直後は直接接続しているインタフェースの経路情報だけを広報しますが、ほかのルータから経路情報の通知を受けると、以降はその経路情報もあわせて広報するようになります。

本装置では定期的に経路情報を広報する時間間隔にゆらぎを持たせています。ルータが一斉に立ち上がった場合に、同じ時間間隔で経路情報を広報するとタイミングが集中し、ネットワークのトラフィックが圧迫されるためです。ゆらぎがあるとこのような事態を避けることができます。

初期値では、定期広報タイマ設定値の50～150%の範囲でゆらぎます。このゆらぎの範囲は設定することができます。

RIPプロトコルを使用する場合は、ホップ数は15までに制限されます。そのため、この数を超えるような大規模なネットワークは構築することができません。また、短い間隔（初期値では30秒）ですべての経路情報を再広報するため、ネットワークが大規模になるほど広報処理によってネットワークのトラフィックが圧迫されます。したがって、RIP機能は小規模なネットワークを構築する場合に使用してください。

本装置でサポートするRIP機能は、以下のRFC（Request For Comments）に準拠しています。

- RFC1058：Routing Information Protocol （RIP）
- RFC2453：RIP Version 2

本装置でサポートするRIP機能

項目	サポート内容
RIPバージョン	バージョン1、バージョン2
unnumberedインタフェース	サポート
トリガードアップデート	サポート
スプリットホライズン	サポート（シンプルのみ）
認証	テキスト認証をサポート
RIPタイマ設定	以下のタイマ変更をサポート ・定期広報タイマ ・有効期限タイマ ・ガーベージタイマ
RIPへの再配布	以下の経路情報の再配布をサポート ・インタフェース経路情報（ループバックインタフェースアドレスを含む） ・スタティック経路情報 ・BGP経路情報 ・OSPF経路情報 ・DNS経路情報 経路情報種別ごとに、再配布するかどうかを指定できます。
RIP経路の他プロトコルへの広報	BGP、OSPFでの広報をサポート
マルチパス	同じあて先への経路情報最大2エントリまでの保持をサポート
フィルタリング	以下をサポート ・経路情報単位での透過／遮断／メトリックの変更 ・特定の隣接ルータからの経路情報の透過／遮断
再配布フィルタリング	経路情報単位での透過／遮断をサポート

⚠注意

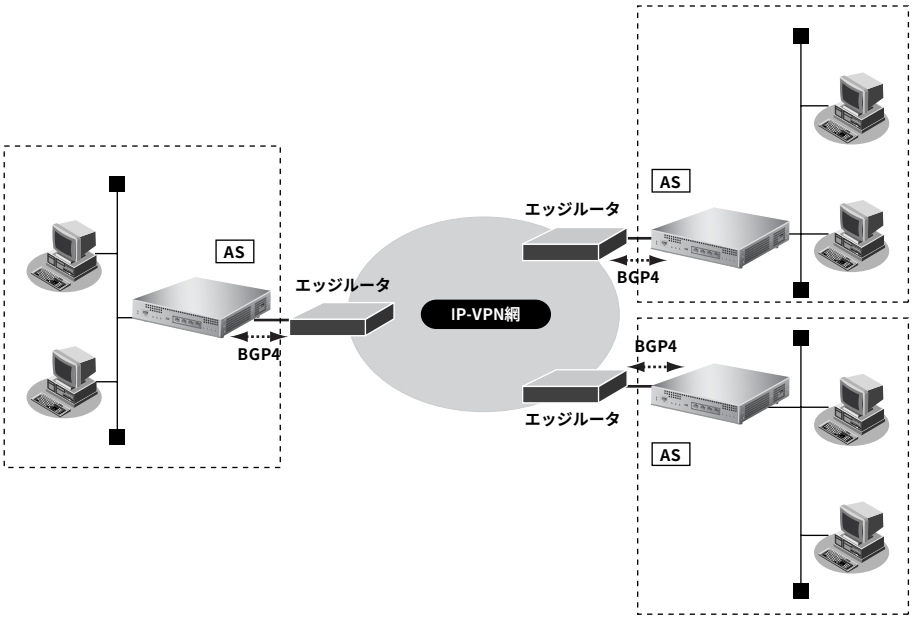
RIP機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境ではRIP機能は使用しないでください。

こんな事に気をつけて

- remoteインタフェースでRIP機能を使用した場合、自側と相手側に割り当てられたアIPドレスを、ホスト経路として広報します。
- 本装置の初期設定では、インタフェース経路とスタティック経路をRIP機能を使用して広報します。RIP機能は定期的に保有するすべての経路情報を広報します。このため、大量のインタフェースが設定されていると、RIPは定期的に大量のRIP広報パケットを送信し、通信トラフィックを圧迫する場合があります。インタフェース経路やスタティック経路がRIPで広報不要な場合は、インタフェース経路とスタティック経路のRIPへの再配布を行わない設定に変更してください。なお、RIP機能を使用するインタフェースに関しては、再配布の設定に関係なく必ずRIPで広報します。
- RIPv2の経路集約は未サポートです。

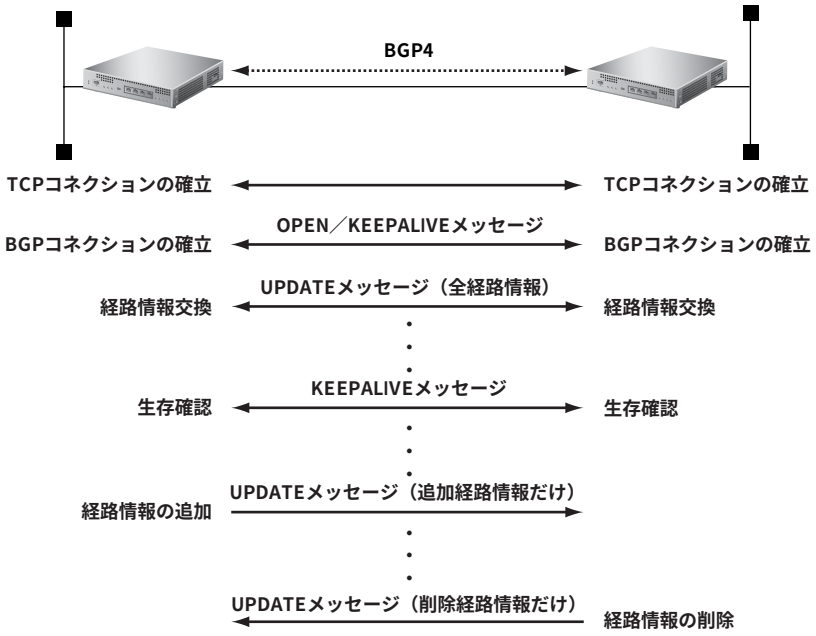
2.4　BGP4機能

BGP4（Border Gateway Protocol version4）機能とは、AS（自律システム：同じポリシに従って運用されているネットワークの単位）間で経路情報を交換するためのルーティングプロトコル機能です。BGP4機能は、IP-VPNサービスで、信頼性の高いネットワーク構成を構築するために必要な機能です。



BGP4のセッションには、EBGP（External BGP）とIBGP（Internal BGP）の2種類があります。
EBGPはAS間で使用するBGPセッションで、IBGPは同じAS内で使用するBGPセッションです。

BGP4は、TCPコネクションを確立し、TCPコネクション上にBGPコネクションを構築します。BGPコネクションはOPEN／KEEPALIVEメッセージを交換することにより確立します。BGPコネクションが確立すると、お互いの装置がすべての経路情報をUPDATEメッセージで交換し合います。そのあとで、経路情報に変更がない場合は、定期的にKEEPALIVEパケットで生存確認を行います。経路情報に追加がある場合は、UPDATEパケットで追加された経路情報だけを広報します。経路情報の削除がある場合は、UPDATEパケットで削除された経路情報だけを広報します。



本装置でサポートしているBGP4機能は、以下のRFC（Request For Comments）に準拠しています。

- RFC1771：A Border Gateway Protocol 4（BGP-4）

本装置でサポートするBGP機能

項目	サポート内容
BGPバージョン	バージョン4だけをサポート
BGPセッション	EBGP、IBGP
EBGPマルチホップ	サポート
ルートリフレッシュ	受信だけをサポート
デフォルトルート広報	サポート
BGPへの再配布	以下の経路情報の再配布をサポート ・インタフェース経路情報（ループバックインタフェースを含む） ・スタティック経路情報 ・RIP経路情報 ・OSPF経路情報 ・DNS経路情報 経路情報種別ごとに、再配布するかどうかを指定できます。
BGP経路の他プロトコルへの広報	RIP、OSPFでの広報をサポート
フィルタリング	以下をサポート ・経路情報単位での透過／遮断 ・特定のASからの経路情報の透過／遮断 ・経路情報単位での属性設定（MEDメトリック値、ASパスプリペンド、 ローカル優先度）
再配布フィルタリング	以下をサポート ・経路情報単位での透過／遮断
経路集約	サポート

⚠注意

- **BGP4 機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、BGP4 機能を使用しないでください。**
- **BGP セッションで使用する WAN インタフェースのインタフェース経路（ホストルート）を BGP で広報した場合、BGP セッションの接続・切断を繰り返す場合があります。該当するインタフェース経路は BGP で広報しないように設定してください。該当しないインタフェース経路を BGP で広報する場合は、以下のどちらかを設定してください。**
  - **BGP にインタフェース経路を再配布しないで、広報するインタフェース経路を BGP ネットワークとして設定します。**
  - **BGP にインタフェース経路を再配布し、該当するインタフェース経路を BGP フィルタリングで送信を破棄するように設定します。**

こんな事に気をつけて

- BGP4 機能は IPv4 の場合だけ利用できます。IPv6 では使用できません。
- NAT 機能と併用することはできません。

☛参照　MR1000　コマンド設定事例集「2.5 BGP の経路を制御する（IPv4）」（P.95）
MR1000　Web 設定事例集「2.5 BGP の経路を制御する（IPv4）」（P.233）

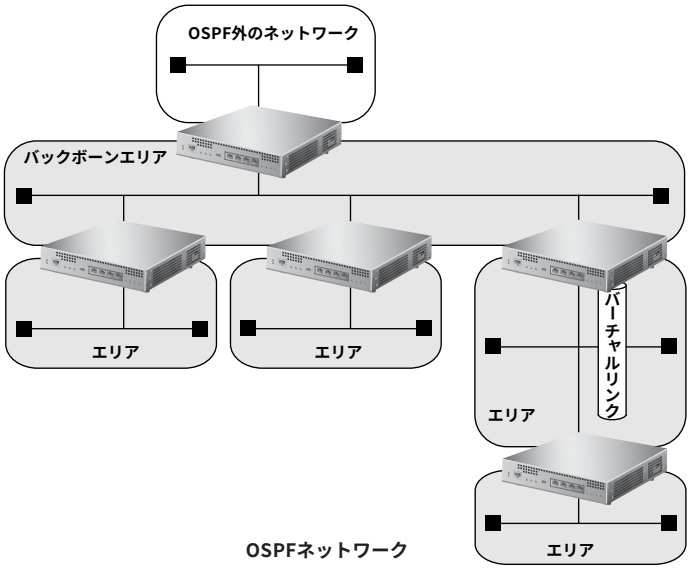
2.5　OSPF機能

OSPF（Open Shortest Path Fast）は、大規模ネットワークに適したルーティングプロトコルです。

OSPFはリンクステート方式を使用して、各ルータが自装置に接続されているリンクの状態やコストなどの情報をLSA（Link State Advertisement）として広報します。また、各ルータは、受信したLSAでネットワーク構成の情報をもつLSDB（Link State Data Base）を作成することにより最適な経路を決定します。

OSPFでは、ネットワーク全体をエリアという単位で分割して管理します。OSPFネットワークは、1つのバックボーンエリアとその他のエリアから構成されます。バックボーンエリアにその他のエリアを接続し、各エリア間のLSAの交換は、バックボーンエリアを経由して行われます。ただし、バックボーンエリアに直接接続できないエリアは、バーチャルリンクを使用することにより、ほかのエリアを経由して、バックボーンエリアに仮想的に接続することができます。

OSPFネットワークは、OSPF以外の経路情報を取り入れることができます。また、スタブエリア、準スタブエリアを設定して、OSPF以外の経路情報数を削減することができます。



OSPFを使用するルータは、運用により以下のルータとして動作します。

- エリア境界ルータ（Area Border Router）
  エリア間に設置されたルータです。エリア間でのLSAの交換を行います。エリア内のLSAは集約して広報することができます。
- AS境界ルータ（AS Border Router）
  OSPF以外の経路情報をエリア内に取り入れるルータです。OSPF以外の経路情報をLSAに変換し、エリア内に広報します。OSPF以外の経路情報を集約して広報することや、デフォルトルートを広報することができます。
- 内部ルータ（Internal Router）
  エリア内のルータです。自装置のOSPFを使用するインタフェースやコストの情報を広報します。
  マルチアクセスネットワーク（ポイント・ツー・ポイント以外のネットワーク）では、内部ルータを指定ルータ（Designated Router）として動作させる必要があります。指定ルータは、ほかのルータの代表としてLSAの交換を行います。また、指定ルータのバックアップとして副指定ルータを動作させておくことができます。
- バックボーンルータ（Backbone Router）
  バックボーンエリアのルータです。機能は内部ルータと同じです。

本装置でサポートしているOSPF機能は、以下のRFC（Request For Comments）に準拠しています。

- RFC1587：The OSPF NSSA Option
- RFC2328：OSPF Version 2

本装置でサポートするOSPF機能

項目	サポート内容
OSPFバージョン	バージョン2だけサポート
ルータ種別	バックボーンルータ、エリア境界ルータ、AS境界ルータ、内部ルータをサポート
エリアタイプ	スタブエリア、準スタブエリアをサポート
バーチャルリンク	サポート
エリア境界ルータでの経路集約	サポート
AS境界ルータでの経路集約	サポート
AS境界ルータでのデフォルトルート広報	サポート（NSSA内部のAS境界ルータを除く）
Passive-Interface	サポート
認証	テキスト認証、MD5認証をサポート
OSPFへの再配布	以下の経路情報の再配布をサポート ・インタフェース経路情報（ループバックインタフェースを含む） ・スタティック経路情報 ・RIP経路情報 ・BGP経路情報 ・DNS経路情報 経路情報種別ごとに、再配布するかどうかを指定できます。
OSPF経路の他プロトコルへの広報	BGP、RIPでの広報をサポート
ECMP機能	サポート
再配布フィルタリング	以下のフィルタリングをサポート ・AS境界ルータでのAS外部経路に対する経路情報単位の透過／遮断 ・透過経路のメトリック値／メトリックタイプの変更

⚠注意

OSPF機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、OSPF機能は使用しないでください。

こんな事に気をつけて

- OSPF機能はIPv4の場合だけ利用できます。IPv6では使用できません。
- NAT機能と併用することはできません。
- OSPFを使用できるインタフェースには上限があります。OSPFを使用するインタフェースの合計が本装置の上限を超えないように設定する必要があります。

2.6　IPv6 RIP機能

IPv6 RIP（Routing Information Protocol）機能は、ダイナミックルーティングプロトコルの1つで、インテリアゲートウェイプロトコルとして、自律システム内でのIPv6経路情報を隣接ルータと交換する機能です。

本機能では、経路情報ごとにあて先へ到達するためのルータ経由数（ホップ数）をメトリックとして管理します。メトリックは、同じあて先への経路情報が複数ある場合に、どの経路情報を使用するかの判断で使用され、もっとも小さいメトリックの経路情報が使用されます。有効なメトリックの最大は15です。このため、15台以上のルータを経由するような大規模ネットワークでは、IPv6 RIP機能を使用できません。

本機能では、RIPテーブルに登録されている経路情報を定期的に広報します。定期的な広報は、定期広報タイマ30秒に±50%のゆらぎを加えた時間ごとに行われます。隣接ルータから受信した経路情報は、有効期限タイマ180秒の間、有効な経路情報として扱われ、ほかのネットワークにも広報されます。有効期限を過ぎた経路情報は、ガーベージ状態となり無効な経路情報として扱われ、ガーベージタイマ120秒の間、ほかのネットワークに無効を示すメトリック16の値で広報されます。

本装置でサポートしているIPv6 RIP機能は、以下のRFC（Request For Comments）に準拠しています。

- RFC2080 : RIPng for IPv6

本装置でサポートするIPv6 RIP機能

項目	サポート内容
RIPバージョン	バージョン1をサポート
トリガードアップデート	サポート ただし、使用しないようにすることはできません。
スプリットホライズン	サポート（シンプルのみ） ただし、使用しないようにすることはできません。
RIPタイマ変更	以下のタイマ変更をサポート ・定期広報タイマ ・有効期限タイマ ・ガーベージタイマ 定期広報で使用するゆらぎ幅は変更できません。
RIPへの再配布	以下の経路情報の再配布をサポート ・インタフェース経路情報 ・スタティック経路情報 ・DNS経路情報 ・DHCP経路情報 経路情報種別ごとに、再配布するかどうかを指定できます。
マルチパス	同じあて先への経路情報最大2エントリまでの保持をサポート
フィルタリング	以下のフィルタリングをサポート ・RIP経路情報ごとの透過／遮断 ・透過となった経路情報のメトリックの変更
再配布フィルタリング	再配布経路情報ごとの透過／遮断をサポート
経路集約広報	サポート

⚠注意

IPv6 RIP機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、IPv6 RIP機能を使用しないでください。

こんな事に気をつけて

RIPへの再配布機能で、インタフェース経路情報をRIPに再配布しないように設定してもRIPを使用するインタフェースのインタフェース経路情報は再配布されます。RIPを使用するインタフェースのインタフェース経路情報をRIPに再配布しない場合は、再配布フィルタで遮断するように設定してください。

2.7 MPLS機能

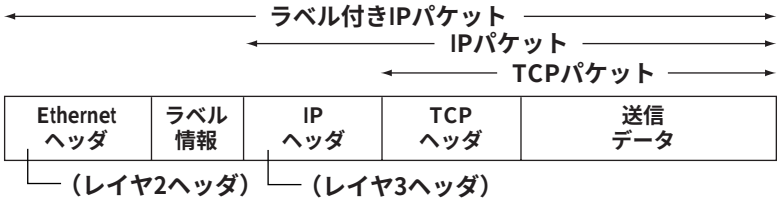
MPLS（Multiprotocol Label Switching）機能とは、パケット転送技術の1つです。パケットにラベルを付加し、ラベルに基づいてスイッチングを行うことができます。MPLSを構成するルータは、MPLS網の端でラベルを抜き差しするLER（Label Edge Router：MPLSエッジルータ）と、MPLS網の中でラベルだけを用いて転送するLSR（Label Switching Router：MPLSコアルータ）の2種類に大きく分けられます。本装置ではLERだけをサポートしています。

MPLS機能の特徴は、以下のとおりです。

- MPLSプロトコルの位置付け
  MPLSは、レイヤ3（ネットワーク層）とレイヤ2（データリンク層）の間に位置します。
- ラベル付けによる通信分離
  パケットにラベルを付加するため、1本の回線をラベルを識別子として多重化できます。異なるラベル値でカプセル化することにより、異なるネットワーク間で通信されるトラフィックが、通過途中に存在するほかのネットワークの影響を受けずに元のパケットを転送することが可能です。
- 固定長ラベル
  パケットをルーティングする場合は、経路を探索する際にプレフィックスの最長一致などの処理に時間がかかるが、MPLSでの転送の場合は、固定長のラベルだけを参照して転送先を決定するため、一般的にIPルーティングの場合よって高速に転送することができます。

ラベルなしのパケットに対して、適切なラベルを挿入してLSRに転送し、出口のLERでは、ラベルを取り除き、通常のパケットとして転送します。

ラベル付きEthernetフレームの例



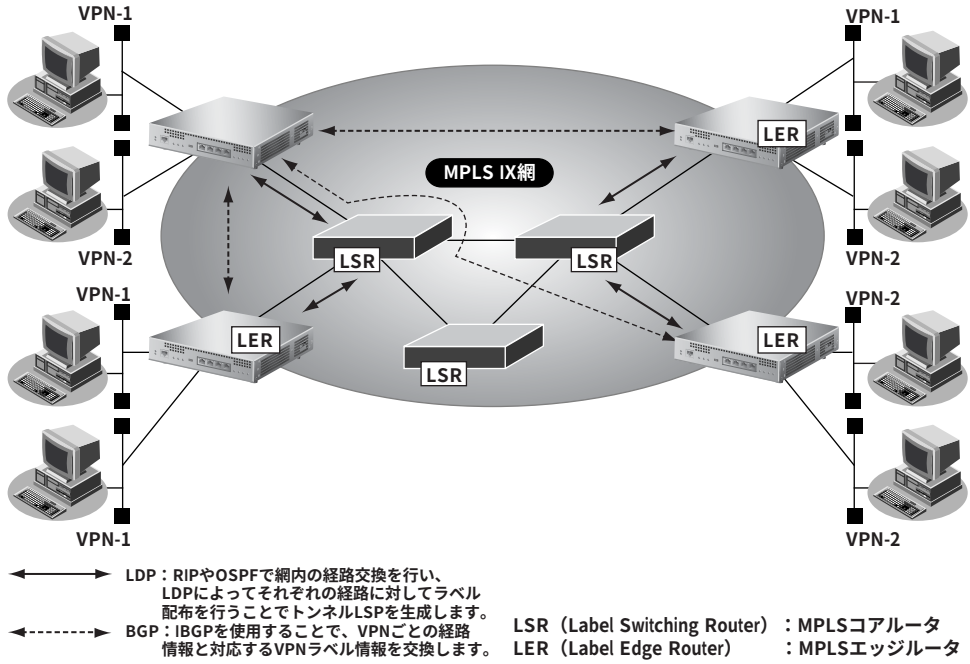
本装置では、MPLSのラベル配布プロトコルとしてLDP（Label Distribution Protocol）をサポートしています。LDPは、隣接LSRとLDPセッションを確立し、OSPFやRIPなどでやりとりされる経路情報を元にラベル生成を行い、メッセージ交換によりラベル配布を行うことでLSP（label Switching Path：トンネルラベルスイッチングパス）を構築するプロトコルです。

本装置のLDPでは、以下の動作モードに対応します。

- LDP配布制御方式
  - Independent Label Distribution Control
  - Ordered Label Distribution Control
- ラベル保持方式
  - Conservative Label Retention Mode
  - Liberal Label Retention Mode
- ラベル広報方式
  - Downstream Unsolicited
  - Downstream on Demand

MPLSを使用した広域分散網（MPLS IX）

本装置は、MPLSをユーザインタフェースとするデータ伝送サービスとの接続に対応します。



本装置では、ここで作成したLSPを仮想トンネルインタフェース（MPLS LSPトンネル）として利用することができます。MPLS網内では、OSPFやRIPなどのダイナミックルーティングプロトコルで経路情報が交換されます。MPLS制御ルータ（LSRとLER）は、LDPを用いて、それぞれの経路情報にラベルを対応付けることで、ラベルで転送可能なLSPを構築します。

LERは各拠点のLERへのスタティックルートを設定するだけでよく、各拠点どうしの経路情報はBGP（Border Gateway Protocol）で交換されます。BGPのメッセージ交換は、TTLを1として通信することで、LSPが切れたときBGPセッションも切断されるため、LSPの接続、切断と連動して経路情報の追加と削除ができます。

こんな事に気をつけて

- **隣接LSRは、ダイナミックルーティングを用いて最適経路から決定することはできません。MPLS LSPの送出先の設定とMPLS LSPでの次ホップのラベルスイッチルータの設定で静的に指定する必要があります。**
- **MPLS LSPトンネルでは、IPv4、IPv6のプロトコルだけをサポートしています。ブリッジは使用できません。MPLS LSPトンネル上にさらにラベルをスタックできるのは、BGP/MPLS VPN機能だけです。LDP over LDPの形態はサポートしていません。MPLS LSPトンネルを使用するインタフェースでは、MPLSを利用しない設定にしてください。**
- **MPLS LSPトンネルでIPv6通信を行う場合、2層目のラベルスタックにIPv6 Explicit NULLラベルを用いた多重スタックとなります。また、MPLS TTL伝達の設定で指定した値に関係なく、TTLの継承は行われません。**
- **MPLS通信で、優先制御機能、EXP値書き換え機能、およびシェーピング機能を利用する場合は、MPLS LSPトンネルを使用してください。**

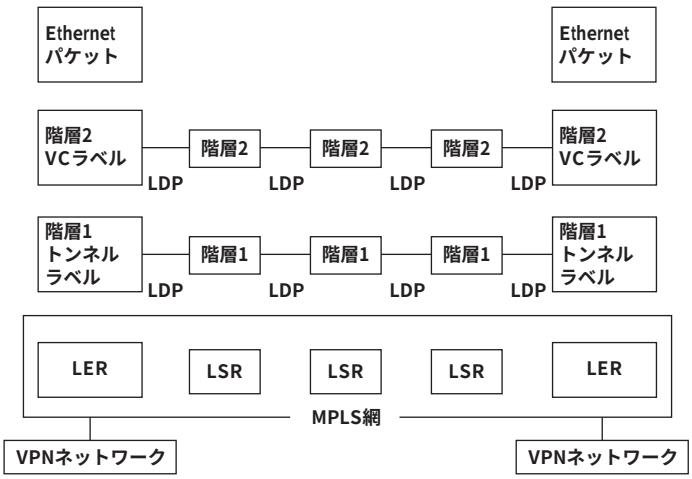
2.7.1　MPLSを使用したレイヤ2VPN（EoMPLS）

EoMPLS（Ethernet over MPLS）とは、MPLSを使用したネットワーク上で、エンドユーザごとに1対1のレイヤ2VPNを構築し、Ethernetフレームを転送することができます。VPN（Virtual Private Network）は、公衆ネットワーク上に仮想的なプライベートネットワーク（閉域網）を構築する技術です。

EoMPLSでは、VC（Virtual Circuit）IDと呼ばれる識別子を使用してVPNごとに区別されたレイヤ2ネットワークを構築します。EoMPLSは2階層ラベルを使用したMPLS制御によって実現します。1層目のラベル（トンネルラベル）はMPLS網内のラベル転送時に使用します。2階層目のラベル（VCラベル）は、LDPによって交換され、同じVPNの出口への転送時に使用します。

以下にEoMPLSの構成を示します。

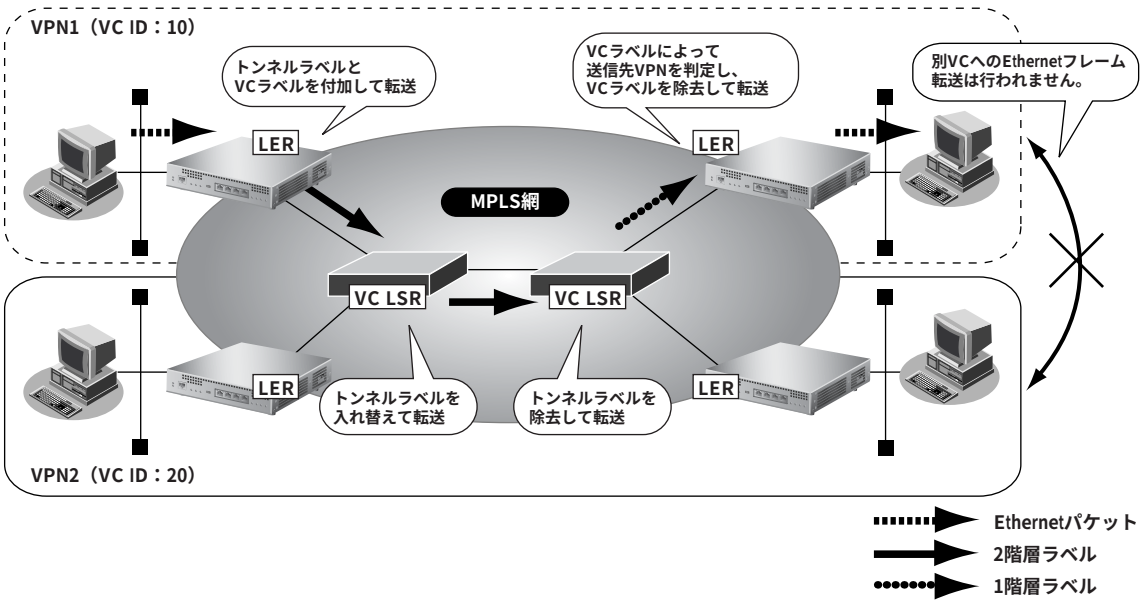
EoMPLSの構成



また、EoMPLSでは、VC IDによってレイヤ2ネットワークを確立します。

VC IDに対してVCラベルを割り当てることにより、同一VC ID間をL2転送を開始することができます。異なるVC ID間は、L2転送を行うことはできません。

EoMPLSネットワークでは、以下のようにEthernetフレームの転送が行われます。



VPNサイトから送信されたEthernetフレームは、入口のLERで、あて先をVCラベルを付加します。次に、MPLS網内をラベル転送するためのトンネルラベルを付加し、VC LSRへ転送します。MPLS網内ではトンネルラベルだけを参照して、トンネルラベルを入れ替え（スワップ）ながら、ラベル転送を行います。PHP（Penultimate Hop Popping）機能によって、出口の1つ手前のMPLS制御ルータでトンネルラベルを除去し、VCラベル付きのEthernetフレームが出口のLERに到着します。出口のLERでは、LANインタフェースに設定されたVC IDとあて先のアドレスでVCインタフェースが決定され、VCラベルを削除したあと、VPNサイトへ転送します。

こんな事に気をつけて

- **複数のインタフェースを同一のVCに含めることはできません。**
- **VCインタフェースでは、シェーピング機能、LANポートバックアップ機能およびVLAN機能を併用して動作させることができます。IP機能、IPv6機能、ブリッジ機能（MACフィルタ機能を含む）、VRRP機能は動作できません。**
- **EoMPLS通信を行う場合は、MAC学習やSTPのサポートを行わないため、パケットのループが発生しないように構成してください。Ethernetフレームがループし続けて通信できなくなります。また、EoMPLS通信を用いて冗長構成を行う場合も、LANインタフェース側に、STPなどを使用できるスイッチ装置を設置し、Ethernetフレームがループしないように設定してください。**
- **VLAN Tagが異なるVLANインタフェースどうしでVCを構成し、LAN側でSTPを使用する場合は、VLAN Tagの値をそろえてください。**

☛参照 MR1000　コマンド設定事例集「2.7 MPLSを使用したレイヤ2VPN（EoMPLS）を構築する」（P.107）
MR1000　Web設定事例集「2.7 MPLSを使用したレイヤ2VPN（EoMPLS）を構築する」（P.263）

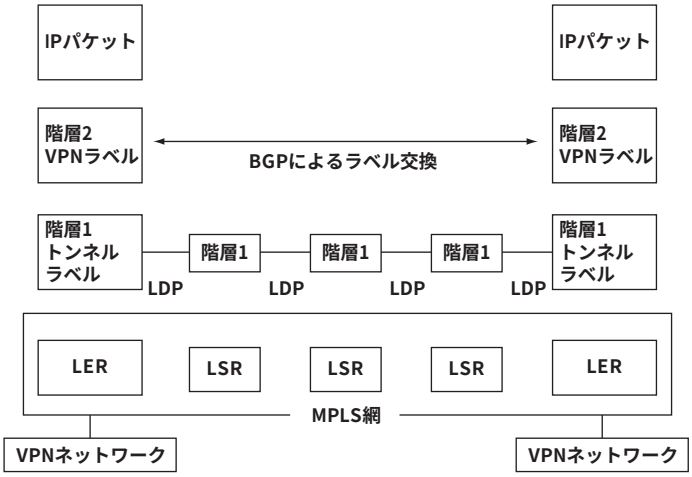
2.7.2　MPLSを使用したレイヤ3VPN（BGP/MPLS VPN）

BGP/MPLS VPNは、本装置で、MPLSのしくみを応用して、IPネットワーク上に仮想的なネットワークを構成することができます。

BGP/MPLS VPNは、RFC2547bisで定義され、2階層ラベルを使用したMPLS制御によって実現します。1階層目のラベル（トンネルラベル）はLDPで交換され、MPLS網内のラベル転送時に使用します。2階層目のラベル（VPNラベル）は、BGPによって交換され、同じVPNグループの出口への転送時に使用します。

以下にBGP/MPLS VPNの構成とフレーム構成を示します。

BGP/MPLS VPNの構成



BGP/MPLS VPNのフレーム構成

トンネル ラベル	VPNラベル	IPv4パケット

また、BGP/MPLS VPNでは、VPNを識別するRD（Route Distinguisher）とIPv4アドレスを組み合わせたVPN-IPv4アドレスを使用して、VPNごとに区別されたネットワークを構築します。

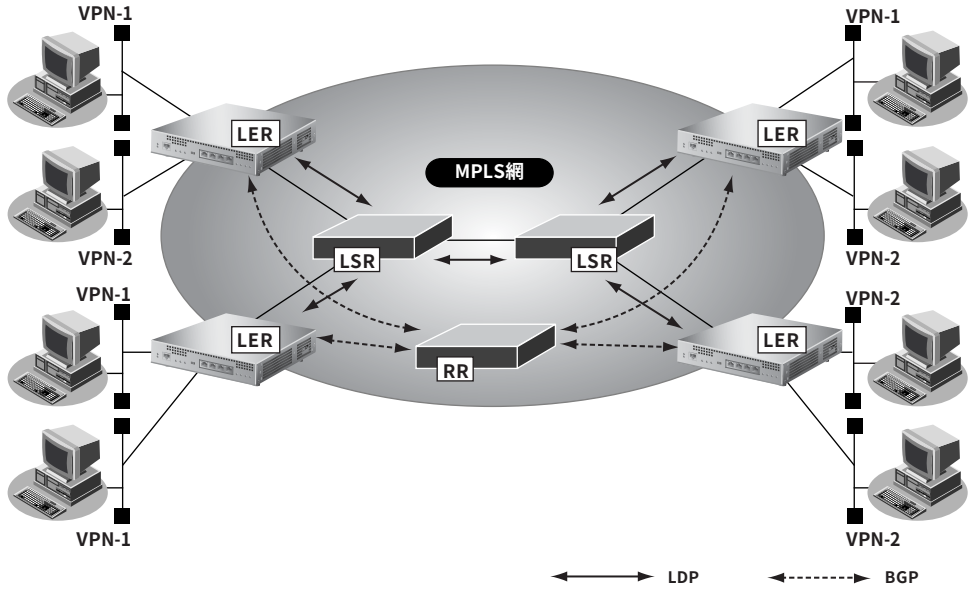
このVPN-IPv4アドレスは、異なるルーティングテーブル（VRF：Virtual Routing Forwarding）で管理され、BGPによって経路情報が交換されます。

以下にVPN-IPv4アドレスを示します。

TYPE値 （2バイト）	AS番号 （2バイト）	任意の番号 （4バイト）	IPv4アドレス

RD

BGP/MPLS VPN ネットワークで、それぞれのルータは、以下のように経路情報とラベル情報を交換します。



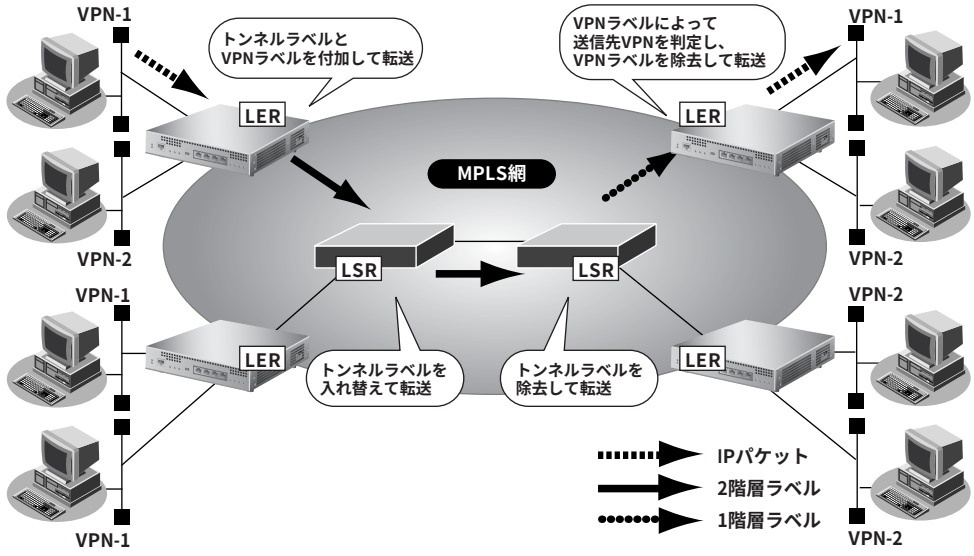
MPLS網内では、OSPFやRIPなどのダイナミックルーティングプロトコルで経路情報が交換されます。MPLS制御ルータ（LSRとLER）は、LDPを用いて、それぞれの経路情報にラベルを対応付けることで、ラベルで転送可能なLSPを構築します。

それぞれのLERは、BGPを使用して、VPN内の経路情報（VPN-1およびVPN-2）とその経路に対応するVPNラベルを交換します。それによって、すべてのLERでVPN情報が交換されます。

なお、このBGPを使用した通信では、それぞれのLERがフルメッシュで経路情報を交換しないで、代表となるRR（ルートリフレクタ）とだけ経路情報を交換する方法が一般に使用されます。RRは、MPLS網内に設置され、必要なVPNグループの情報だけを管理するBGPルータです。RRを設置することで、それぞのLERが保有する経路情報を最小限に抑えることができます。

本装置は、RRに接続することでBGP/MPLS VPNをサポートします。

このように経路情報が交換されたネットワークでは、以下のようにパケット転送が行われます。



VPNサイトから送信されたパケットは、入口のLERで、あて先をVPN経路から検索して、VPNラベルを付加します。次に、MPLS網内をラベル転送するためのトンネルラベルを付加し、LSRへ転送します。MPLS網内ではトンネルラベルだけを参照して、トンネルラベルを入れ替え（スワップ）ながら、ラベル転送を行います。PHP（Penultimate Hop Popping）機能によって、出口の1つ手前のMPLS制御ルータでトンネルラベルを除去し、VPNラベル付きのパケットが出口のLERに到着します。出口のLERでは、VPNラベルによって出力先インタフェースが決定され、VPNラベルを削除したあと、VPNサイトへ転送します。

本装置でサポートしているMPLS-VPN機能は、以下のRFC（Request For Comments）およびInternet-Draftに準拠しています。

- RFC 1771 Border Gateway Protocol version 4（BGP-4）
- RFC 2796 BGP Route Reflection -An Alternative to Full Mesh IBGP
- RFC 2842 Capabilities Advertisement with BGP-4
- RFC 2858 Multiprotocol Extensions for BGP-4（MP-BGP）
- Internet-Draft:Draft-ietf-ppvpn-rfc2547bis-00.txt
- RFC3031 Multiprotocol Label Switching Architecture
- RFC3032 MPLS Label Stack Encoding
- RFC3036 LDP Specification

⚠注意

MPLS、BGP、OSPFおよびRIPを使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、BGP/MPLS VPN機能は使用しないでください。

こんな事に気をつけて

- **BGP/MPLS VPN機能はIPv4の場合だけ利用できます。IPv6では使用できません。**
- **BGPで接続できる相手は1セッションだけです。このため、ルートリフレクタと接続する必要があります。**
- **IP-VPN接続と併用することはできません。**
- **BGPネットワーク、BGP集約経路およびBGPフィルタリングの機能は使用できません。**
- **BGP/MPLS VPN機能とNAT機能を併用することはできません。**
- **サポートインタフェースはPRI（ISDN、HSD）、BRI（ISDN、HSD）、およびLANです。モデムやフレームリレーには対応していません。**
- **BGP/MPLS VPNで構成されたVPNネットワーク内では、EBGP、OSPFおよびRIPは使用できません。**
- **異なるVPNを収容する場合、VPNのインタフェースに設定したIPアドレスおよび属するネットワークアドレスを他VPNインタフェースに設定できません。必ず異なるネットワークアドレスを設定してください。**
- **MPLS網と接続するインタフェースでRIPを使用する場合、VPNで使用するインタフェース経路をRIPで広報します。MPLSへの広報に対してフィルタリングを行ってください。**
- **LERでは、受信したIPパケットをIP処理層を通さずにラベルを付加します。IPフィルタリング機能、TOS値書き換え機能およびソートフラグメント機能は、VPNに設定したインタフェースへの入力に限り動作します。ただし、VPNからの入力をIPsecによって暗号化し、対向ルータに送信する運用や帯域制御（WFQ）機能、イコールコストマルチパスなどの他IP機能を使用した運用は行うことはできません。**
- **VRRPと併用する場合は、トリガとしてインタフェースダウントリガまたはルートダウントリガ（VPN内経路は対象外）が利用できます。ノードダウントリガは利用できません。**
- **BGP/MPLS VPN構成では、LERはMTU長の設定にかかわらず、IPパケットのフラグメント処理を行いません。受信したパケットはそのままラベルを付加して送信します。このため、MTU長を調整する必要がある運用（VoIP通信でのインターリーブなど）はできません。**

☛参照　MR1000　コマンド設定事例集「2.8 MPLSを使用したレイヤ3VPN（BGP/MPLS VPN）を構築する」（P.111）
MR1000　Web設定事例集「2.8 MPLSを使用したレイヤ3VPN（BGP/MPLS VPN）を構築する」（P.271）

2.8　マルチリンク機能

マルチリンク機能とは、複数の物理回線／論理回線を1本のデータリンク・コネクションとして扱うための機能です。この機能を使用することにより、バルク転送することができます。

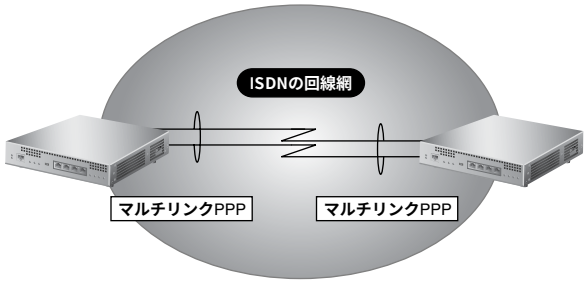
本装置でサポートするマルチリンク機能は、以下のRFC（Request For Comments）に準拠しています。

- RFC1990：The PPP Multilink Protocol（MP）
- RFC2125：The PPP Bandwidth Allocation Protocol（BAP）
  The PPP Bandwidth Allocation Control Protocol（BACP）

マルチリンク機能は、ISDN回線での接続でだけ利用することができます。また、バルクとしてまとめることができるチャネル数は2チャネルまでです。

マルチリンク機能の運用形態

ISDN回線を使用して、複数のチャネルを論理的な一本のリンクとして通信します。あるチャネルで障害が発生した場合、残ったチャネルで通信を続けます。



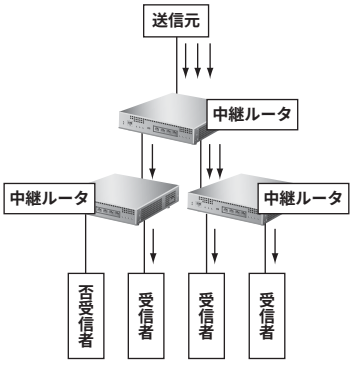
参照　MR1000　コマンド設定事例集「2.9 マルチリンク機能を使う」（P.120）
MR1000　Web設定事例集「2.9 マルチリンク機能を使う」（P.294）

2.9　マルチキャスト機能

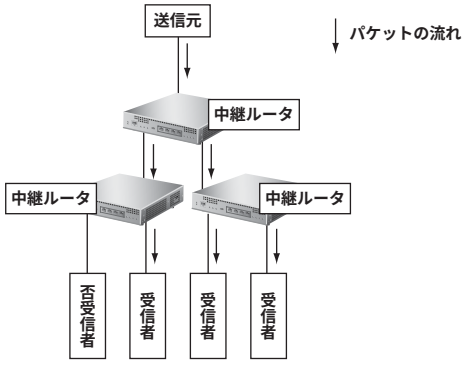
マルチキャスト機能とは、異なるネットワーク上に複数の受信者がいる場合に、動画や音声データなどを効率よく配送することができる機能です。

配送される受信者が存在するインタフェースにだけパケットを複製して転送することで、通常のユニキャストによるパケットの配送に比べて、ネットワークのトラフィックを削減することができます。

以下の図のように、ユニキャストによる配送では、送信元から受信者の数だけパケットが送出されるため、送信元のトラフィックが受信者数に比例して増大してしまいます。マルチキャストによる配送では、1つのパケットを必要な数だけ中継ルータでコピーして配送するため、ネットワークの負荷を軽減できます。



ユニキャストによる配送



マルチキャストによる配送

本装置には、マルチキャスト機能を動作させるマルチキャストルーティングプロトコルとして、以下の2種類のプロトコルがあります。

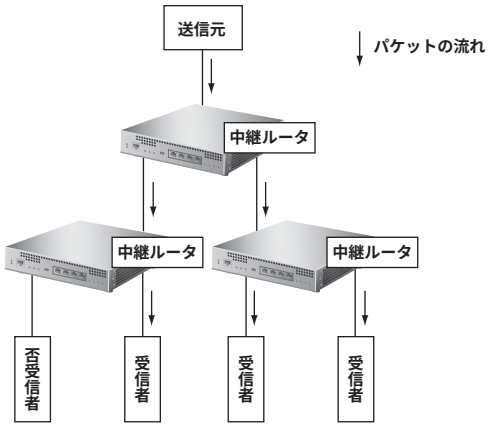
- PIM-DM
- PIM-SM

また、本装置では、ルーティングプロトコルは使用しないで、スタティックにマルチキャスト経路を設定することもできます。

以下に、それぞれのルーティングプロトコルについて説明します。

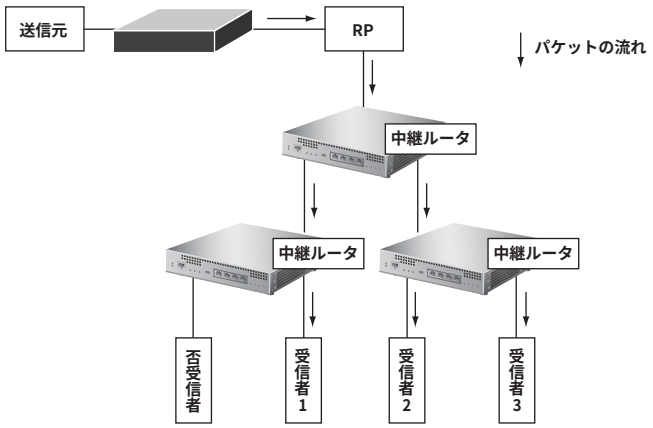
2.9.1　PIM-DM

PIM-DMは、会社のLANなど、十分な帯域と信頼性のあるネットワーク上で利用するプロトコルです。パケットの配送は、送信元が配送樹の頂点となります。



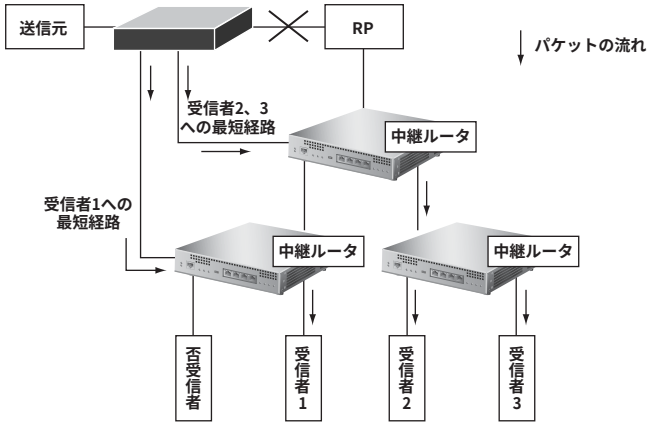
2.9.2 PIM-SM

PIM-SMは、インターネットなど、十分な帯域を保証されないネットワーク上で利用するプロトコルです。パケットは、送信元からRP（ランデブーポイント）に一度送られ、RPが配送樹の頂点となります。



RPの情報は、BSR（ブートストラップ・ルータ）によって広報されます。PIM-SMを利用する場合、ネットワーク上で1つ以上のRPとBSRを動作させる必要があります。

マルチキャスト・パケットは、最初はRPを経由して転送されますが、その後最短経路（SPT：Shortest Path Tree）を経由して転送する経路に切り替わります。



こんな事に気をつけて

- マルチキャスト機能での配送は信頼性を持たないため、パケットの消失や重複などが起こる可能性があります。これらの信頼性の確保は、アプリケーション側での責任になります。
- マルチキャストを利用する場合は、隣接するすべてのルータ上でマルチキャスト機能を有効にしておく必要があります。
- 隣接するすべてのルータ上で、同じプロトコルを選択する必要があります（本装置ではPIM-DMとPIM-SMは併用できません）。
- マルチキャストをスタティック経路で転送する場合は、PIM-DM、PIM-SMを併用することはできません。
- PIM-DM、PIM-SMは、動作する際、ユニキャストのルーティングテーブルを参照するため、ユニキャストの経路を正しく設定してください。このとき、RIPやOSPFなどのユニキャスト・ルーティングプロトコルと併用することができます。
- マルチキャスト・プロトコルにPIM-SMを利用する場合、ネットワーク上で1つ以上のRPとBSRを動作させる必要があります。RPまたはBSRが消失した場合、既存の通信を含め、通信できなくなります。これを防止するためには、RPおよびBSRを複数動作させます。
- マルチキャスト機能は、マルチNAT機能と併用することができません。
- IPアドレスが設定されていないインタフェースではマルチキャスト機能を使用することはできません。また、リモートインタフェース上でマルチキャスト機能を動作させる場合は、自側IPアドレスと相手側IPアドレスの両方を正しく設定する必要があります。
- 本装置で実装されているPIM-SMのバージョンはPIM-SMv2です。PIM-SMv1の装置との接続は保証されません。
- PIM-SMでは、送信元とRPの間をPIM Registerパケットによって通信します。
  PIM Registerパケットのチェックサムの計算範囲は、RFC2362ではヘッダ部だけで計算するように定義されていますが、一部のルータはパケット全体で計算します。このようなルータがRPを行う場合は、チェックサムの計算範囲を「パケット全体」に変更する必要があります。本装置はPIM Registerパケットの受信時には、ヘッダ部（RC2362準拠）とパケット全体の2つの方法で計算するため、本装置がRPを行う場合は、どちらの計算方法のパケットを受信しても問題はありません。
- 転送経路をSPTに切り替える場合は、一時的に複数のマルチキャスト・ルーティングテーブルを作成します。このため、マルチキャスト・ルーティングテーブルの上限数の通信ができなくなる可能性があります。
- SPTへの切り替えは、パケットの転送開始直後に行われます。パケット受信者の直前のルータでSPT切り替えを無効に設定することによって、SPTへの切り替えを無効にすることができます。
- インタフェースごとにパケットのTTL（Time To Live）しきい値を設定することによって、特定のTTLのパケットを遮断することができます。
- マルチキャスト・パケットは、パケット送信者側のルータとRP間をPIM Registerパケットによってカプセル化され、ユニキャスト転送されます。このとき、トンネル用の仮想的なインタフェースとして、registerインタフェースを使用します。registerインタフェースには通常のマルチキャスト・インタフェースの設定は適用されません。このため、PIM Registerによってカプセル化されたパケットには、インタフェースのTTLしきい値の設定は適用されません。
- パケット送信者側のルータとRP間は、転送開始時にPIM Registerによってカプセル化され、ユニキャスト通信されますが、転送開始直後にはマルチキャスト・パケットによる通信に切り替わります。

☛ 参照　MR1000　コマンド設定事例集「2.10 マルチキャスト機能を使う」（P.121）
MR1000　Web設定事例集「2.10 マルチキャスト機能を使う」（P.296）

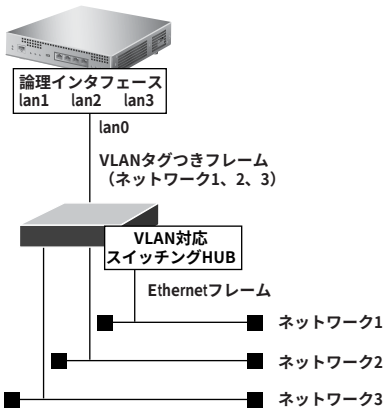
2.10　VLAN機能

VLAN（Virtual LAN）機能とは、1つのLANインタフェース上に複数のLANセグメントを仮想的に構築する機能です。

VLAN機能を利用することで、論理的にLANインタフェースを管理することができ、物理的なポートの数以上に、論理的なLANセグメントを構築することができます。

VLAN機能には、VLANタグ付きフレームを使用します。通常のEthernetフレームに4バイトのヘッダ情報を付加することで、VLANインタフェースを識別することができます。

以下に、VLANの基本動作について説明します。



VLAN対応機器どうしでVLANインタフェース間の通信を行う場合は、Ethernetフレームの送信時にVLANタグをフレームに付加して送出します。VLANタグには、VLAN IDが格納されています。受信側ではVLANタグ中のVLAN IDを見て、フレームを受けとるインタフェースを決定します。

本装置では、VLANインタフェースを設定して、VLAN間のルーティングも可能です。

こんな事に気をつけて

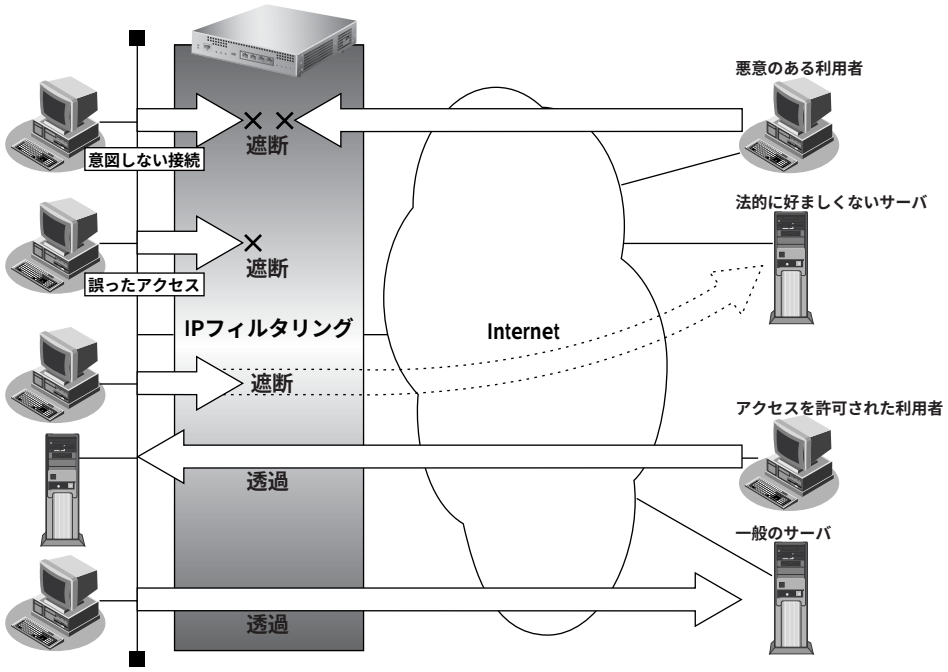
- **VLANインタフェース上では、シェーピング、帯域制御（WFQ）、ホットスタンバイの機能を利用することはできません。**
- **VLANの物理インタフェースに、VLANインタフェースを使用することはできません。**
- **同じ物理インタフェースを使用する複数のVLANインタフェース上で、重複するVLAN IDを使用することはできません。**
- **本装置のVLAN機能は、VLANタグの有無やVLAN IDの違いによって、1つの物理ポートを論理的に複数のLANセグメントに分割することができます。本装置のVLAN機能を利用する場合は、それぞれの論理LANセグメントが明確に分割されているかどうか、十分に確認してください。正しく分割されていない場合は、正常に通信できない場合があります。**

参照　MR1000　仕様一覧「2.3 システム最大値一覧」（P.19）
MR1000　コマンド設定事例集「2.11 VLAN機能を使う」（P.131）
MR1000　Web設定事例集「2.11 VLAN機能を使う」（P.305）

2.11　IPフィルタリング機能

本装置は、IPフィルタリング機能やパスワードの設定などを使って、ネットワークのセキュリティを向上させることができます。

IPフィルタリング機能とは、本装置を経由してインターネットに送出されるパケット、またはインターネットから受信したパケットをIPアドレスとポート番号の組み合わせで制御することによって、ネットワークのセキュリティを向上させたり、回線への超過課金を防止することができます。



ネットワークのセキュリティを向上させるには、以下の要素について考える必要があります。

- ネットワークのセキュリティ方針
- ルータ以外の要素（ファイアウォール、ユーザ認証など）

こんな事に気をつけて

- **ProxyDNSを設定している場合、ProxyDNSに対してのIPフィルタリングを設定しても効果はありません。**
- **本装置などのルータでは、コンピュータウィルスの感染を防ぐことはできません。パソコン側でウィルス対策ソフトを使用するなど、別の手段が必要です。**

補足　NAT機能にも、セキュリティを向上させる効果があります。

接続形態に応じてセキュリティ方針を決める

インターネットに接続する場合でもLANどうしを接続する場合でも、データの流れには「外部から内部へ」、「内部から外部へ」という2つの方向があります。セキュリティ方針を決める場合は、2つの方向について考慮する必要があります。

● 「外部から内部へ」流れるデータに対するセキュリティ方針の例

- インターネット（ネットワーク型接続）の場合
  特定のパケットを受け取らないようにする
- インターネットの場合
  非公開ホストへのアクセスを拒否する
- LANどうしを接続する（ISDN回線を使用）場合
  接続先電話番号が外部に知られたときの対策を立てる
- LANどうしを接続する場合
  内部ユーザによる不要なアクセスを防ぐ

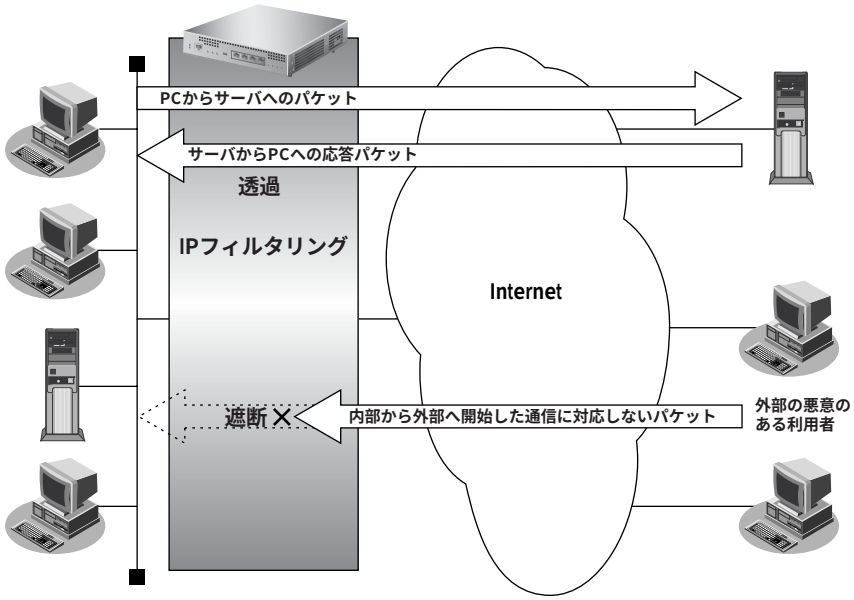
● 「内部から外部へ」流れるデータに対するセキュリティ方針の例

- インターネットの場合
  法的に問題のあるサイトなどへのアクセスを制限する
- LANどうしを接続する場合
  内部ユーザによる不要なアクセスを防ぐ

補足 IPフィルタリングは、「外部から内部へ」流れるデータと「内部から外部へ」流れるデータに対して機能します。内部にあるパソコン間のデータ（LAN内のデータ）に対しては機能しません。

2.11.1　動的フィルタリング（SPI）

SPIは内部から外部へ通信を開始すると、これに対応するフィルタリングルールを自動的に作成し、外部からの応答パケットを透過させます。また、フィルタリングルールに対応しない外部から内部への通信を開始したパケットを遮断することができます。



補足　ブロードキャストアドレスやマルチキャストアドレスあてにSPIでフィルタリングを行うことはできません。DHCP、RIPおよびRIPv2などブロードキャストアドレスを用いる通信をSPIと併用する場合は、これらの通信を透過させるフィルタリングルールを設定してください。

ヒント

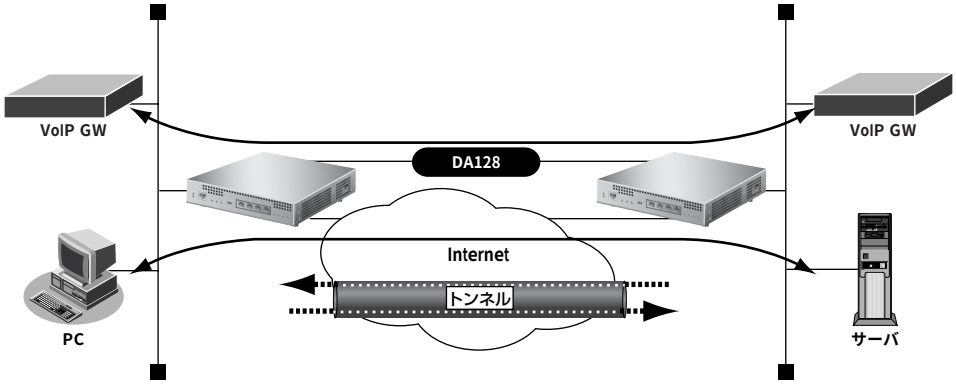
SPIによるフィルタリング対象は、構成定義で設定されたIPフィルタリングを透過したパケットです。

参照　MR1000　Web設定事例集「2.15 マルチNAT機能（アドレス変換機能）を使う」（P.473）、
MR1000　コマンド設定事例集「2.15 マルチNAT機能（アドレス変換機能）を使う」（P.198）

2.12　マルチルーティング（ポリシールーティング）機能

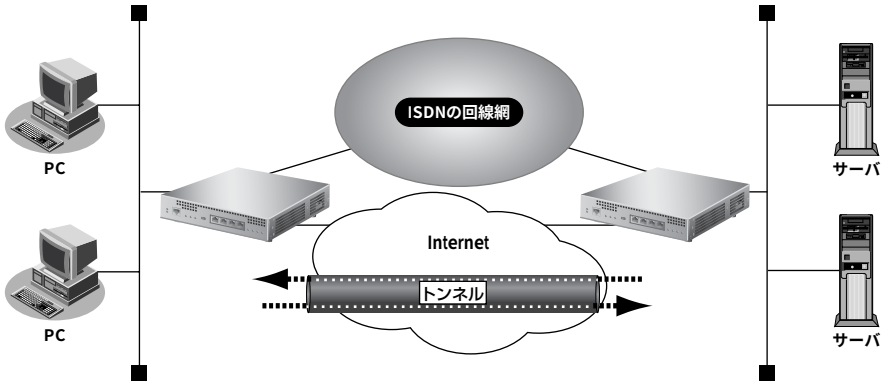
マルチルーティング機能とは、転送パケットのあて先IPアドレスだけではなく、送信元IPアドレスやポート番号などの情報も利用して、通信パスを選定する機能です。この機能を利用することによって、それぞれの通信内容に通信パスを分離することができます。

例）VoIP通信を専用線で、ほかの通信をインターネットVPNで、通信する



また、この機能は、それぞれの通信パスの障害発生時に、通信バックアップとしても利用することができます。

例）インターネットVPNをISDNで通信バックアップする



ここでは、ネットワーク設計概念で紹介したマルチルーティング機能の詳細を説明します。

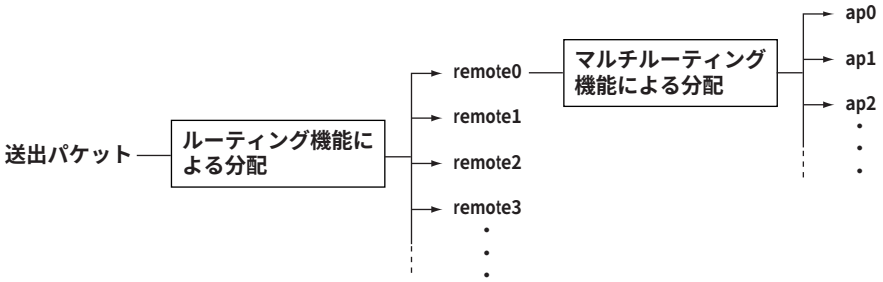
参照 「1.1 ネットワーク設計概念」（P.12）

2.12.1　通常のIPルーティングとマルチルーティングの関係

IPルーティングでの送信先選定では、出力先インタフェースを選定します。マルチルーティング機能は、IPルーティングで選定された出力先インタフェースの構成を定義するremote定義の配下に、実際の接続先設定（通信パス設定）となるap定義を複数定義して、さらに通信パスを選定することができます。

マルチルーティングは、同じremote定義内での送信先選定動作であるため、remote定義によるデータ送信先の分離と、ap定義によるデータ送信先の分離は、以下のように使い分けます。

- remote定義による分離
  経路情報として分離できる接続先（つまり、独立したネットワークとして識別できる接続先）は、それぞれ別のremote定義として定義し、ルーティング機能を用いて分配します。
- ap定義（マルチルーティング）による分離
  経路情報では分離できない接続先（つまり、独立したネットワークとして識別できない接続先）は、同じremote定義内にそれぞれ別のap定義として定義し、マルチルーティング機能を用いて分配します。



2.12.2　利用するap定義の選定方法

ここでは、それぞれの送信データに対して、利用するap定義の選定方法を説明します。remote定義内に設定されている複数のap定義は、表示される順に優先度が高いものとして扱われ、優先度の高いものから順に利用するかどうかを判断します。送出できるap定義がない場合は、データは送信されません。

通信内容に従った選定

通信内容ごとに通信パスを分離する場合は、remote ap multiroute pattern定義によって、ap定義を利用する通信内容を設定し、通信内容に従った選定を行います。

通信内容の選定条件として、以下の条件が利用できます。

- 送信元IPアドレス
- 送信元ポート番号（送信データがTCPまたはUDPの場合のみ）
- あて先IPアドレス
- あて先ポート番号（送信データがTCPまたはUDPの場合のみ）
- 上位プロトコル
- TOS値

こんな事に気をつけて

選定条件は、IPv4の場合だけ利用されます。IPv6およびブリッジ通信の場合は選定条件がないものとして扱われます。

また、上記条件に一致した場合の動作を、以下から選択します。

- use　このap定義で送信する
- unuse　このap定義で送信しない
- backup　優先度の低いap定義で送信できるものがない場合にだけ送信する

この条件によって、ap定義は、以下のどれかに送信データごと分類されます。

- 設定条件に一致
- 条件設定なし
- 利用不可

接続状態に従った選定

通信バックアップとして利用する場合は、接続状態に従った選定を行います。この場合、ap定義ごとの接続状態は、以下の3つに分類されます。

- 接続中
- 接続可能（ISDNおよびPPPoEの場合だけ：接続済みではないが接続可能）
- 利用不可

以下に、利用不可と判定する条件を示します。

専用線

- 利用回線が同期はずれ状態であるとき
- 接続先が閉塞状態であるとき
- 接続先監視が失敗状態であるとき

フレームリレー

- 利用回線が同期はずれ状態であるとき
- 接続先が閉塞状態であるとき
- 接続先監視が失敗状態であるとき
- PVC状態確認手順（ITU-T Q.933 Annex A）によって障害検出状態であるとき

ISDN

- 利用回線が同期はずれ状態であるとき
- 接続先が閉塞状態であるとき（常時接続機能利用時のみ）
- 接続先監視が失敗状態であるとき（常時接続機能利用時のみ）
- 未接続状態であるとき（常時接続機能利用時または自動発信禁止設定時）

PPPoE

- 利用回線が同期はずれ状態であるとき
- 接続先が閉塞状態であるとき（常時接続機能利用時のみ）
- 接続先監視が失敗状態であるとき（常時接続機能利用時のみ）

IPsec

- 接続先が閉塞状態であるとき
- 接続先監視が失敗状態であるとき

オーバーラップ

- 接続先が閉塞状態であるとき
- 接続先監視が失敗状態であるとき
- 送出先インタフェースがダウン状態であるとき

MODEM

- モデムと通信不可能な状態であるとき
- 未接続状態であるとき（自動発信禁止設定時）

MPLS トンネル接続

- 接続先が閉塞状態であるとき
- 接続先監視が失敗状態であるとき
- LSPが未確立状態であるとき

☛ 参照 「2.12.3 マルチルーティング機能の応用」（P.56）

最終的な送出先判断

最終的な送出先判断は、通信内容に従った選定の結果と、接続状態に従った選定の結果を組み合わせて判断します。この組み合わせ条件は、それぞれのap定義に以下のように判断されます。

ap0（優先度高） / ap1（優先度低）		設定条件に一致		設定条件なし	
		接続中	接続可能	接続中	接続可能
設定条件に一致	接続中	ap0	ap1	ap0	ap1
	接続可能	ap0	ap0	ap0	ap0
設定条件なし	接続中	ap0	ap0	ap0	ap1
	接続可能	ap0	ap0	ap0	ap0

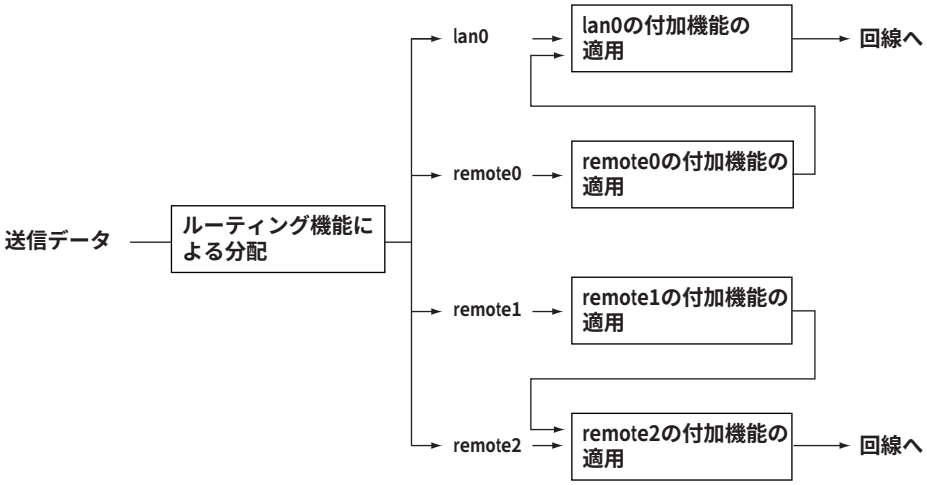
2.12.3　マルチルーティング機能の応用

IPルーティングでの送信先選定ルールでは、出力先インタフェースを選定します。シェーピング、帯域制御およびMSS書き換えなどの付加機能は、インタフェース単位での適用となります。そのため、同じインタフェースから出力される送信データは、すべて同じ付加機能が適用されます。

マルチルーティング機能の応用として、本装置は、IPルーティングによって選定された出力先インタフェースからの送信データを、さらに別インタフェースへの出力として重ね合わせる（オーバーラップする）機能をサポートしています。この機能を利用すると、同じインタフェースから出力される送信データにも、異なる付加機能を適用することができます。

この機能を利用する場合は、相手ネットワーク設定であるremote定義の配下に、最終出力先となるインタフェースを指定する特別な接続先（ap定義）を設定します。

以下に、内部的な送信データの流れを示します。remote0はlan0を利用して送信するように、またremote1はremote2を利用して送信するように設定されているものとします。



以下に、この機能を利用する場合にオーバーラップ元インタフェースで利用できる付加機能を示します。

- MTU分割機能
- マルチルーティング機能
- IPフィルタリング機能
- MSS書き換え機能
- TOS/Traffic Class値書き換え機能
- シェーピング機能
- 帯域制御（WFQ）機能

こんな事に気をつけて

- **オーバーラップ元インタフェースでは、マルチNAT機能は利用できません。**
- **オーバーラップ元インタフェースでは、ダイナミックルーティングは利用できません。**

また、オーバーラップ先インタフェースでは、以下の付加機能を利用することができます。

- マルチルーティング機能（remote定義を利用して送出する場合のみ）
- IPフィルタリング機能
- MSS書き換え機能（remote定義を利用して送出する場合のみ）
- マルチNAT機能
- TOS/Traffic Class値書き換え機能
- シェーピング機能
- 帯域制御（WFQ）機能

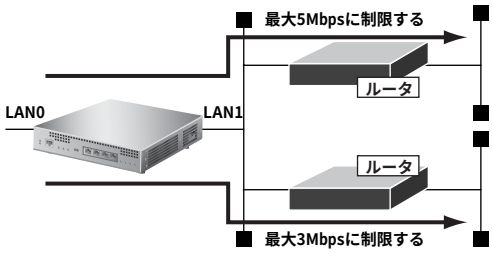
オーバーラップ先インタフェースとして lan を指定した場合は、次ホップルータアドレスを設定する必要があります。次ホップルータアドレスは、隣接ルータのアドレスでなければいけません。この設定がない場合、または次ホップルータアドレスが隣接ルータのアドレスでない場合は、データは送信されません。

こんな事に気をつけて

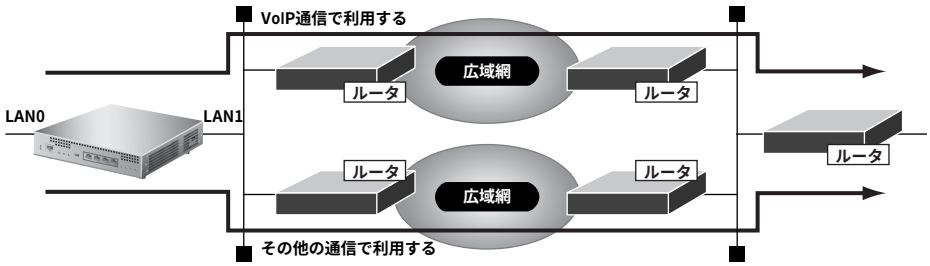
- **オーバーラップ機能は、IPv4 および IPv6 の場合に利用できます。**
- **オーバーラップ先インタフェースの MTU は、オーバーラップ元インタフェースの MTU より大きい値を設定してください。正常に通信することができなくなることがあります。**

この機能を利用した例を以下に示します。

例 1）対地シェーピングを行う



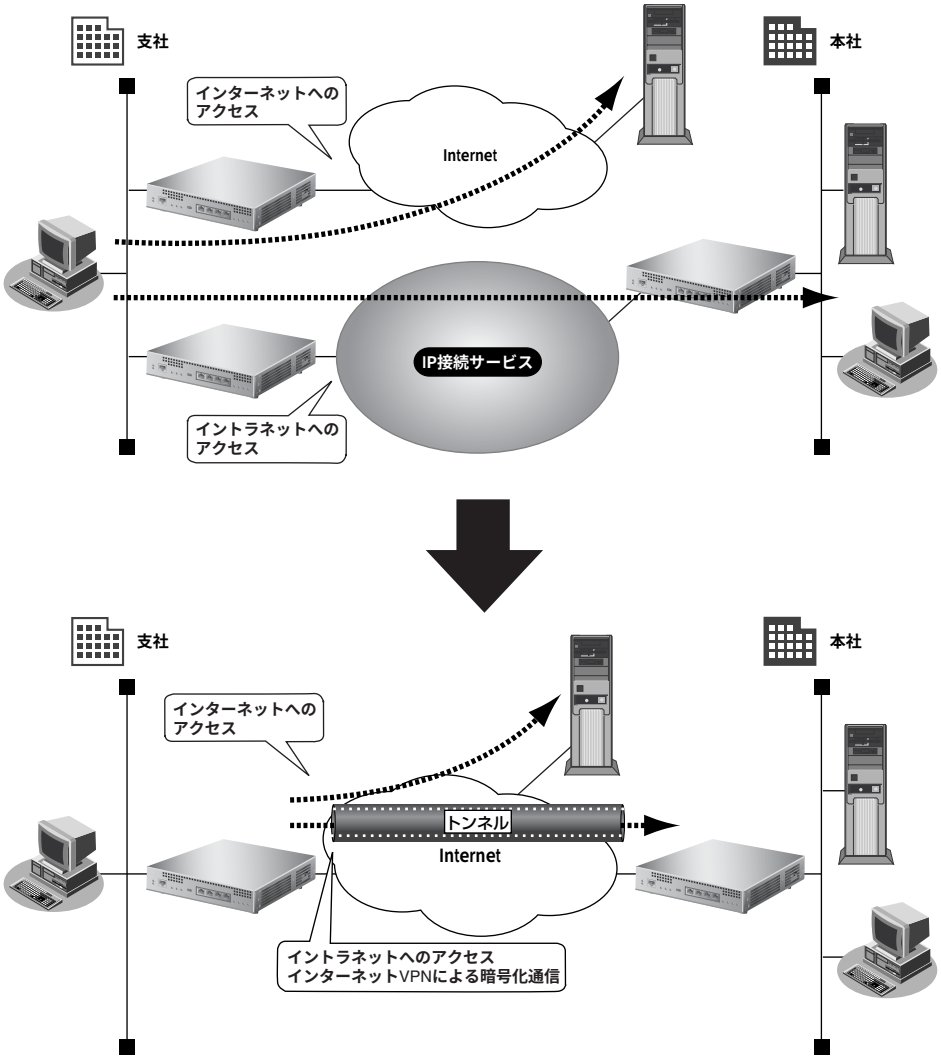
例 2）特定の通信データを分離する



2.13　IPsec機能

VPN（Virtual Private Network）とは、インターネットのように公衆で利用されているネットワークに、通信パスを仮想的に設定することによって専用線のように使用することができます。最近ではインターネットを利用してVPNを構築する、インターネットVPNのこと自体をVPNと言うこともあります。

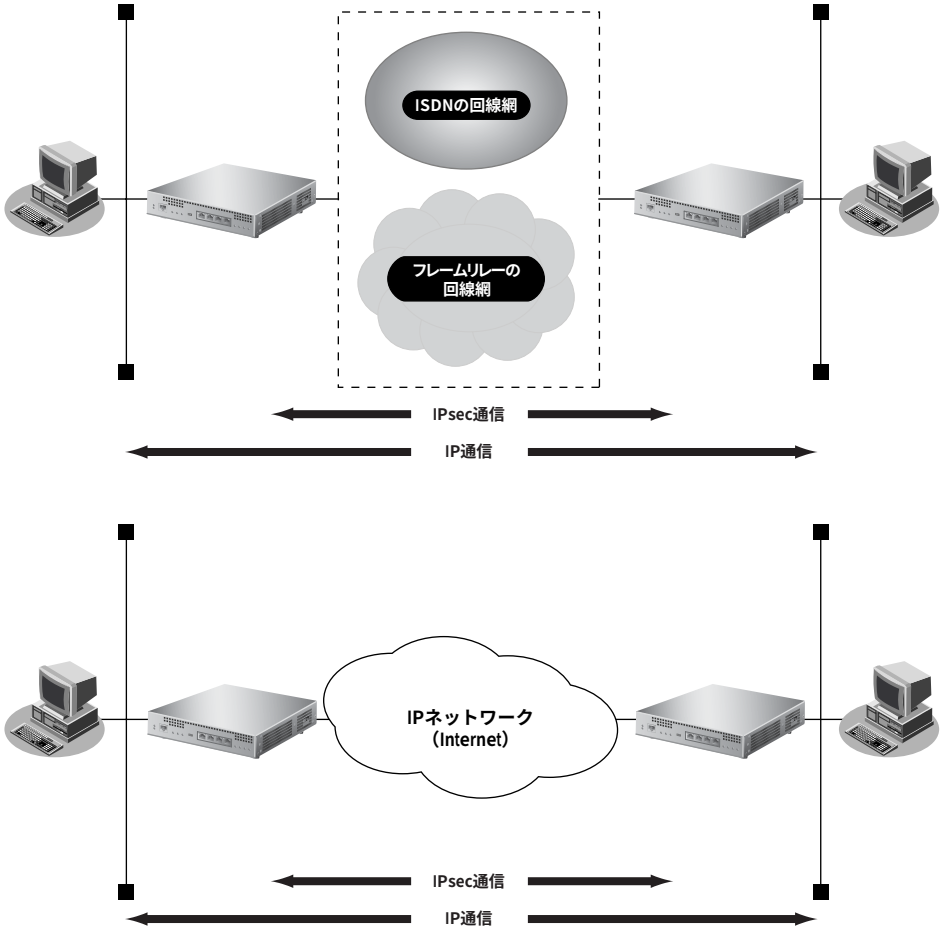
VPNではVPN装置間でデータをカプセリングし、相手のVPN装置に送信します。その際、データの盗聴、改ざんを防止するために、認証や暗号化などのセキュリティ機能によりデータを保護します。これにより、簡単に機密性の高いシステムが構築できます。



本装置ではVPNを実現するためにIPsecというプロトコルを使用します。

IPsecで使用できる機能は2つあります。IPパケットに認証用のヘッダをつけて認証する機能AHと、暗号化したあとに認証してカプセル化する機能ESPです。

IPsecには、IPヘッダを認証／暗号化しないトランスポートモードとIPヘッダを認証／暗号化するトンネルモードの2つのモードがあります。本装置はトンネルモードだけをサポートしているため、ここではトンネルモードだけを説明します。



本装置でサポートするIPsecの範囲

本装置がサポートするIPsecの範囲は、以下のとおりです。

項目	IPsecの範囲
IPsec適用範囲	AH、ESP、認証付ESP
鍵設定／鍵交換方式	手動鍵設定、自動鍵設定（Main Mode、Aggressive Mode）
セキュリティパケット送信方法	トンネルモード（IPv4 over IPv4、IPv4 over IPv6、IPv6 over IPv4、IPv6 over IPv6）
暗号アルゴリズム	DES-CBC、3DES-CBC、AES-CBC
認証アルゴリズム	HMAC-MD5、HMAC-SHA1 認証アルゴリズムと認証アルゴリズムモードの主な特徴 MD5：シンプルで認証が早い SHA1：セキュリティが強いが、認証が遅い

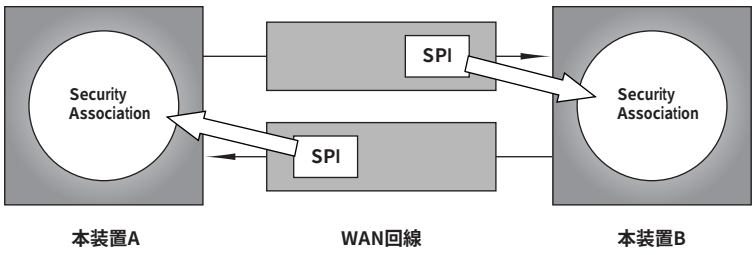
本装置でサポートするIPsec機能は、以下の新プロトコルのRFCに準拠します。

- RFC2401: "Security Architecture for the Internet Protocol"
- RFC2402: "IP Authentication Header"
- RFC2403: "The Use of HMAC-MD5-96 within ESP and AH"
- RFC2404: "The Use of HMAC-SHA1-96 within ESP and AH"
- RFC2104: "HMAC: Keyed-Hashing for Message Authentication"
- RFC2406: "IP Encapsulating Security Payload （ESP）"
- RFC2405: "The ESP DES-CBC Cipher Algorithm With Explicit IV"
- RFC2410: "The NULL Encryption Algorithm and Its Use With IPsec"
- RFC2411: "IPsecurity Document Roadmap"
- RFC3394: "Advanced Encryption Standard（AES）Key Wrap Algorithm"

Security AssociationとSecurity Parameters Index

IPsecの特徴は、認証・暗号化のアルゴリズムや鍵管理のしくみをIPsecのプロトコル自体から切り離したことです。IPsecで通信するホストどうしは、通信する前になんらかの方法で認証・暗号化のアルゴリズムや使用する鍵を決定して、その情報を共有する必要があります。この関係をSA（Security Association）と言います。

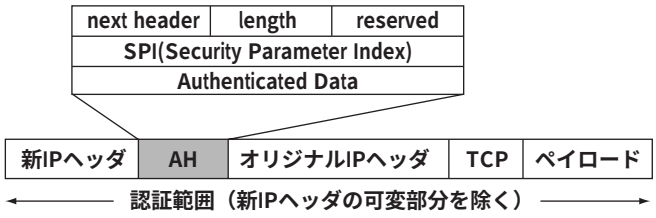
1つのホストは複数の通信に対応するための複数のSAを持っています。そのため、受け取ったIPsecのパケットが、どのSAに対応するものなのかを識別する必要があります。識別するためのパラメタとして、あとに説明するAHやESPのヘッダ中に含まれるSPI（Security Parameter Index）を使用します。



AHヘッダとESPヘッダ

IPsecでは、IPパケットのオプションヘッダに、認証にはAH（Authentication Header）ヘッダを、暗号化および認証にはESP（Encapsulating Security Payload）ヘッダを使用しています。

IPパケット認証（AH:Authentication Header）



AHはIPパケットを認証するためにIPヘッダに拡張されるものです。元々あるIPパケットの前にIPsecゲートウェイのアドレスと上記の構成からなるAHヘッダを挿入します。

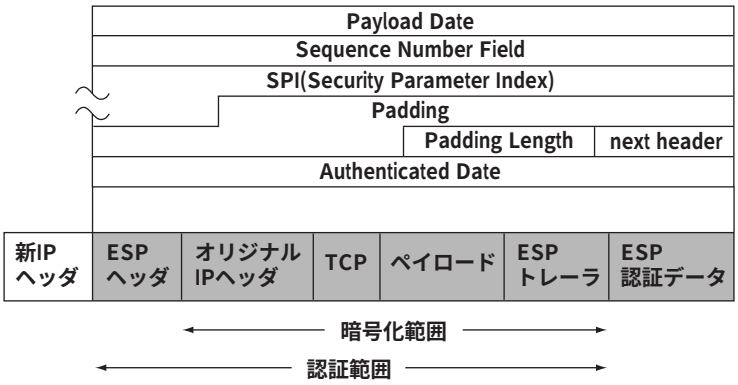
AHは認証アルゴリズム・認証キー・暗号アルゴリズム・暗号キー・キー寿命・キー配送方法などを決めるSPI値と、認証アルゴリズムで使用するデータ・フィールドAuthenticated Dataから成り立っています。

送信する側は、オリジナルのIPパケットと認証鍵からハッシュ関数を使って圧縮したものをAuthenticated Dataに書き込んで送信します。

受信する側は、SPIの情報で相手先を特定します。その相手先と同じ暗号鍵および認証アルゴリズムを使用して送信する側と同様の計算を行います。AHヘッダ内のAuthenticated Dataと一致した場合に、相手を認証したと判断します。

認証に使用する認証鍵およびハッシュ関数などは、SAデータベースにあらかじめ登録しておきます。SAとは、暗号に必要な認証方式や認証鍵などのデータが入っているデータ構造のことです。

IPパケット暗号化（ESP:Encapsulating Security Payload）

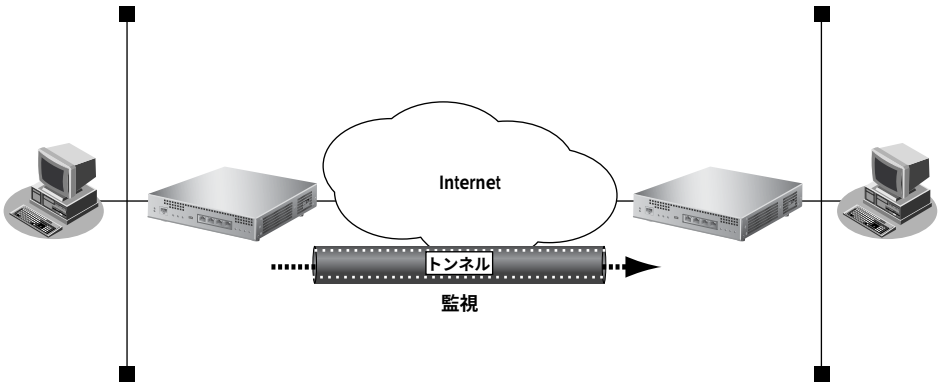


ESPはIPパケットを認証（IPパケットの改ざんチェック）だけではなく、IPパケットを暗号化します。

接続先監視

IPsec通信の場合、回線の切断や相手装置の再起動によって相手装置のSAが削除されることがあります。このとき、相手装置のSAが削除されたことを検出することができないため、通信できない状態になります。

接続先監視を使用することにより、IPsecトンネルを経由して相手装置のSAが削除されていることを検出します。IPsec通信できない場合は、SAを再作成することによって、通信を復旧させることができます。



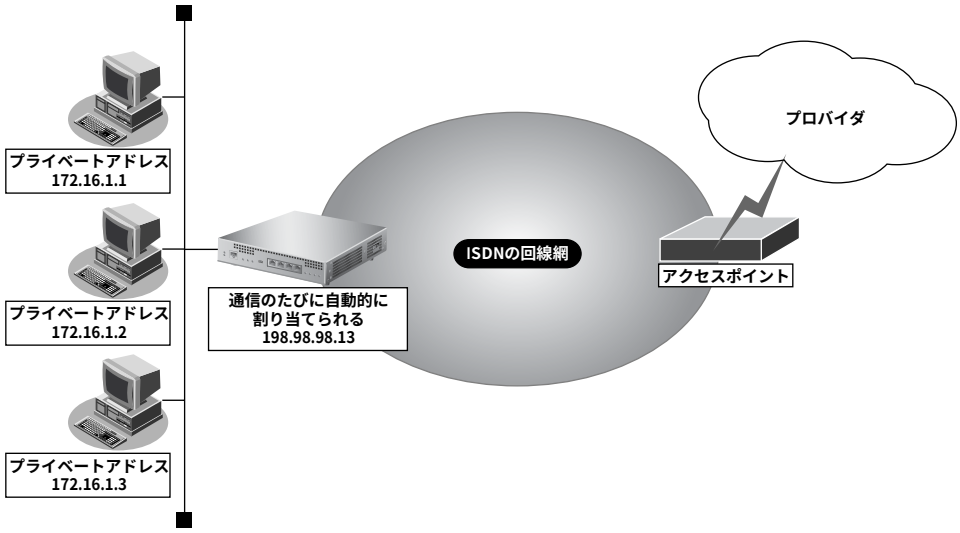
こんな事に気をつけて

- **接続先監視を使用すると、相手ノードにICMP ECHOパケットを定期的に送信します。そのため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、接続先監視を使用しないでください。**
- **接続先監視を使用する場合は、監視対象となる相手ノードおよび自装置のアドレスがIPsec対象範囲に含まれる必要があります。IPsec対象範囲に含まれない場合は、接続先監視のパケットが破棄され、IPsec通信ができません。**
- **IKEセッション監視の設定が同時に設定されている場合は、IKEセッション監視は動作しないで、接続先監視だけが動作します。**

☛参照　MR1000　コマンド設定事例集「2.13 IPsec機能を使う」（P.159）
MR1000　Web設定事例集「2.13 IPsec機能を使う」（P.373）

2.14　マルチNAT機能

マルチNAT機能（アドレス変換機能）とは、LAN内に接続された複数台のパソコンで使用するプライベートアドレスを、本装置に割り当てたグローバルアドレスに変換する機能です。マルチNAT機能を使用すると、限られた数のグローバルアドレスでそれ以上の数のパソコンを接続できます。たとえば、端末型接続でプロバイダからもらえる1台分のグローバルアドレスを使って、複数台のパソコンからインターネットに接続できます。また、LAN内に接続されたパソコンのプライベートアドレスは外部からわからないため、外部からの不正なアクセスを遮断できます。



補足
- プライベートアドレスとグローバルアドレスについて
  プライベートアドレスとは、ユーザが自由に割り当てることができるIPアドレスです。
  グローバルアドレスとは、インターネット上のホストを識別するために、InterNICなどのアドレス管理機構から割り当てられる世界で唯一のIPアドレスです。プロバイダ接続の場合はプロバイダからもらえます。
- LANどうしを接続する場合（事業所間など）、両方プライベートアドレスとなることがあります。本装置では、WAN側のアドレスをグローバルアドレス、LAN側のアドレスをプライベートアドレスとしています。
- 「端末型接続」と「ネットワーク型接続」はインターネットに接続する際のIPアドレスの割り当て方が異なります。
  端末型接続は、接続先に接続するごとにグローバルアドレスがプロバイダから動的に割り当てられます。
  ネットワーク型接続は、LANを単位として接続する形態で、あらかじめプロバイダからグローバルアドレスが割り当てられます。プロバイダ接続の場合は契約時の申し込み台数に応じてグローバルアドレスが割り当てられます。

マルチNAT機能を使用すると、すでにLANを構築している場合も、プライベートアドレスを変更することなくインターネットに接続できるようになります。しかし、同時に接続できる台数は、割り当てられたグローバルアドレスの個数に限られます。これを解決するために、マルチNAT機能があります。マルチNAT機能を使用すると、ポート番号を使って、割り当てられたグローバルアドレスの個数以上のパソコンを接続できます。

マルチNAT機能とは、以下の2つの機能で構成されます。

- 動的NAT
- 静的NAT

補足　カタログなどで説明するマルチNAT機能は、基本NAT、動的NAT、静的NATの総称です。

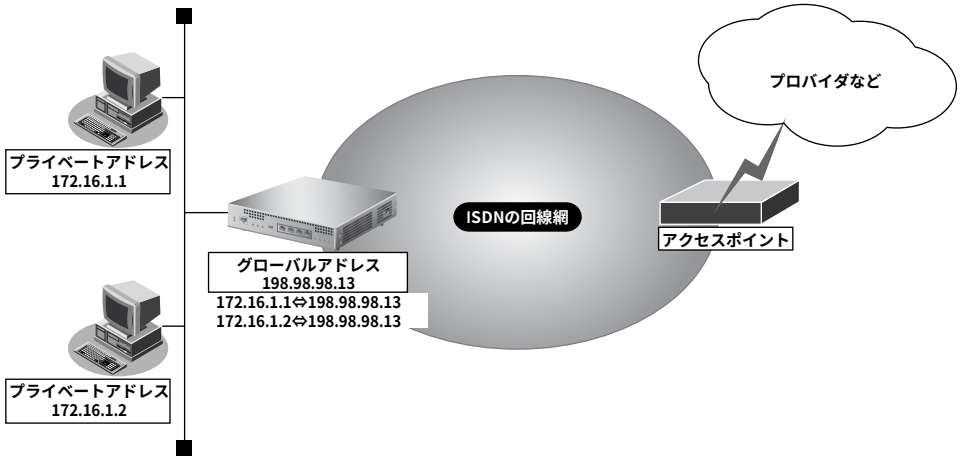
こんな事に気をつけて

IPパケットのフラグメントが発生する環境の場合は、フラグメントされた先頭パケットより前に後続パケットを受信すると、そのフラグメントパケットは破棄され、正常に通信できない場合があります。

ヒント

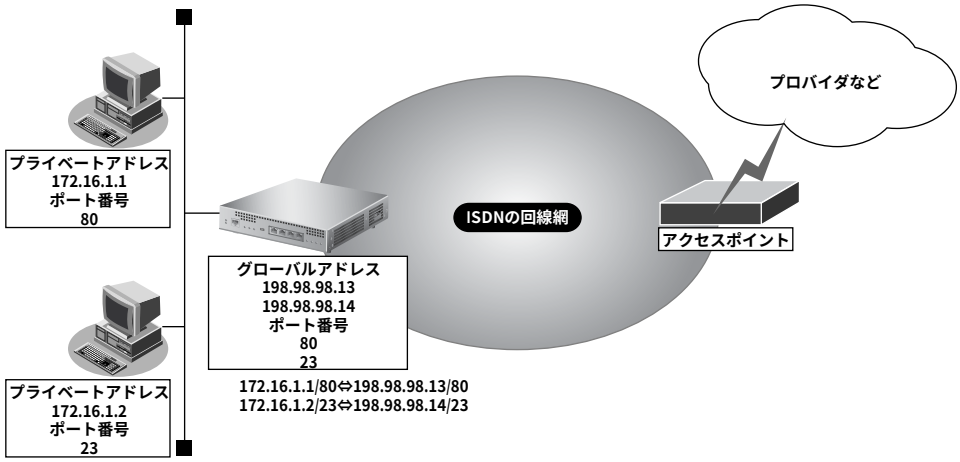
◆ 動的NATとは

基本NATは、プライベートアドレスとグローバルアドレスを1対1に対応付けます。インターネットに同時に接続できるパソコンの台数は、プロバイダと契約したグローバルアドレスの個数です。「動的NAT」を使用すると、使用可能なグローバルアドレスの個数以上のパソコンが同時に接続できます。



◆ 静的NATとは

基本NATは、通信発生のたびに空いているグローバルアドレスを割り当てます。そのため、LAN上のWebサーバを公開するような場合は適していません。「静的NAT」を使用すると、特定のパソコンやアプリケーションに同じIPアドレス、ポート番号を割り当てるので、この問題を解決できます。



2.14.1　NAT機能の選択基準

ネットワーク環境および使用目的によって、適切なマルチNAT機能を設定する必要があります。選択基準を以下に示します。

NAT機能が必要な場合

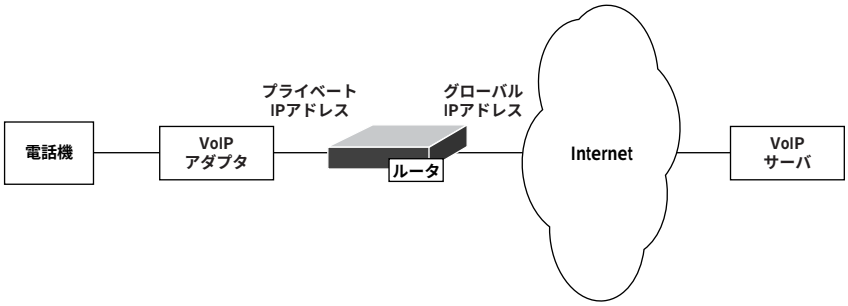
- 端末型ダイヤルアップ接続する場合
- プロバイダから割り当てられたグローバルアドレスより多くのパソコン（端末）を接続する場合（ここでいう端末には本装置も含まれます）
- 既存のネットワークのアドレスをそのまま使用する場合
- 自側のネットワークのアドレスを隠す場合
  - 基本NATで十分な場合
    - 端末型ダイヤルアップ接続で、同時に接続するパソコン台数が1台の場合
    - ネットワーク型接続で、同時に接続するパソコン台数がグローバルアドレス数以下の場合
  - 動的NATが必要な場合
    - 端末型ダイヤルアップ接続で、同時に複数のパソコンから接続する場合
    - 同時に接続するパソコンの台数がグローバルアドレス数を超える場合
  - 静的NATが必要な場合
    - 外部にサービスを公開する場合（WWWサーバ、FTPサーバなど）
    - IPアドレスを意識して動作するアプリケーションを使用する場合
- インターネットVPNなどで、IPsec通信のほかにインターネット上のサーバなどとの通信がある場合、マルチNAT機能を使用する必要があります。このとき、VPNで使用するアドレスがNATのアドレスプールに含まれる場合は、静的NATを指定してください。これはIPsec通信に用いられるアドレスが正しく変換されるように、関係するプロトコルやポート番号ごとに設定します（ESP（プロトコル番号：50）やIKE（ポート番号UDP：500）など）。
- IPsecがAggressive Modeの場合、Initiatorだけがマルチ NAT機能を使用しているときはIPsec SA自体を確立できますが、その後ResponderからIPsecパケットを送信しなければNATテーブルが作成されず、通信できません。Responderでマルチ NAT機能だけを使用しているとIPsec SAも確立されません。Main Modeの場合は、IKEのネゴシエーションを双方から開始するので、マルチ NAT機能だけを使用していてもIPsec SAは確立されます。ただし、IPsec通信はNATテーブルが双方に作成されるまで不可能となります。

☛参照　MR1000　コマンド設定事例集「2.15 マルチNAT機能（アドレス変換機能）を使う」（P.198）
MR1000　Web設定事例集「2.15 マルチNAT機能（アドレス変換機能）を使う」（P.473）

2.15　VoIP NAT トラバーサル機能

VoIP NAT トラバーサル機能とは、マルチ NAT 機能を使用すると動作しない VoIP アダプタを動作できるようにする機能です。ただし、UPnP（Universal Plug and Play）に対応した VoIP アダプタでなければ動作しません。同様に、UPnP に対応した装置やアプリケーションプログラムもマルチ NAT 機能を使用しても動作できるようになることがあります。

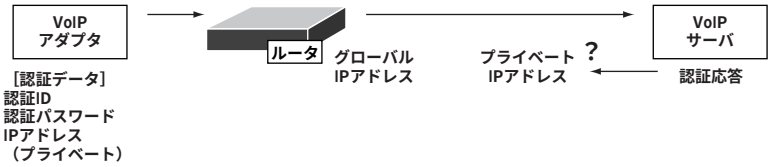
マルチ NAT 機能を使用することによって通信ができない場合



上図で、通信ができない要因には、以下のようなことが考えられます。

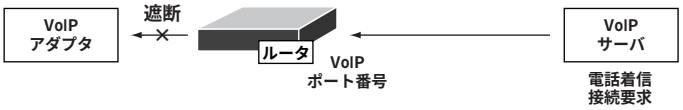
要因 1

VoIP アダプタから VoIP サーバへ接続するとき、認証データに VoIP アダプタの IP アドレス（プライベート IP アドレス）を含めるため、VoIP サーバからの認証応答が VoIP アダプタに届きません。

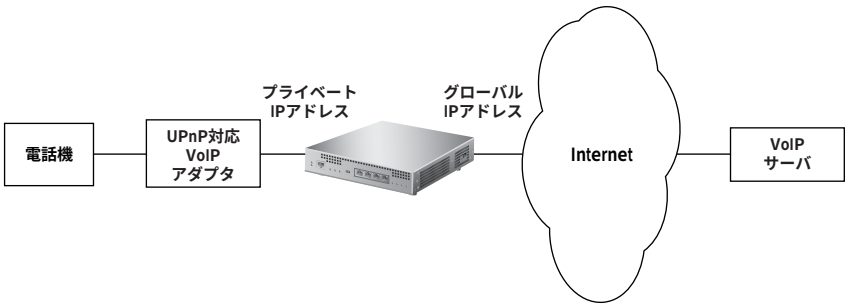


要因 2

VoIP サーバから電話着信接続要求があるとき、ルータの VoIP ポート番号との通信が遮断されているため、VoIP アダプタに届きません。



VoIP NAT トラバーサル機能によって通信ができる場合



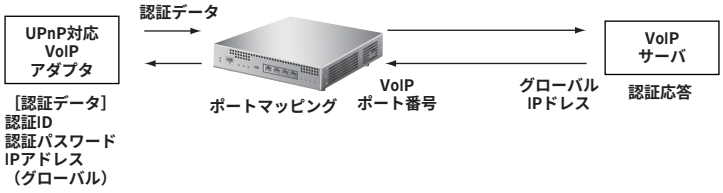
ここでは、VoIP NAT トラバーサル機能によって通信できるときの、動作の概要について説明します。

（1） UPnP 対応VoIP アダプタは、ルータにグローバル IP アドレスを問い合わせます。

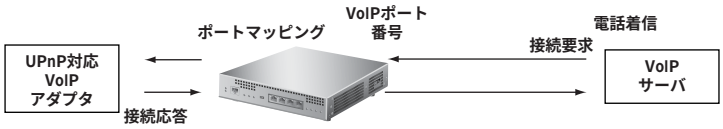
（2） UPnP 対応VoIP アダプタは、ルータのVoIP ポート番号に届いたデータをVoIP アダプタへ届けるようにルータにポートマッピングを設定します。

（3） Volpアダプタは、認証データにルータの IP アドレス（グローバル IP アドレス）を含めて VoIP サーバに接続します。

VoIP サーバからルータに届いた認証応答は、ポートマッピングの設定によって VoIP アダプタに届きます。



（4） VoIP サーバからルータに届いた電話着信接続要求もポートマッピングの設定によってVoIP アダプタに届きます。



こんな事に気をつけて

- VoIPアダプタのマニュアルを参照して、UPnP機能が使用できるように設定されていることを確認してください。
- VoIPアダプタは、マルチNAT機能を使用しないlanインタフェースのどれかに接続してください。
- VoIPサーバは、マルチNAT機能を使用するもっとも小さい定義番号のlanインタフェースに接続されているものとして動作します。マルチNAT機能を使用するlanインタフェースがない場合は、マルチNAT機能を使用するもっとも小さい定義番号のremoteインタフェースのもっとも優先度の高いアクセスポイントに接続されているものとして動作します。
- VoIP NATトラバーサル機能は、マルチNAT機能を使用するインタフェースへの通信に対して動作します。
- VoIP NATトラバーサル機能では、以下のポート番号を使用します。そのため、これらのポートをIPフィルタリングで遮断しないでください。

プロトコル	ポート番号
UDP	1900
TCP	5432

- ポートマッピング情報は、装置全体で（NATテーブル総数-消費NATテーブル数）個まで設定できます。

☛参照 MR1000　仕様一覧「2.3 システム最大値一覧」（P.19）

- ポートマッピング情報は、UPnP対応装置が設定する際に有効期限を設定するか削除要求するまで残ったままになります。
- VoIPアダプタによっては、NATを併用する場合があります。NATの割り当て時間が短いと通信が切断されますので、NATの定義で必要な割り当て時間を設定してください。
- NATの定義では、グローバルIPアドレスの個数に、必ず1を設定してください。2以上を設定した場合、UPnPが正しく動作しないことがあります。

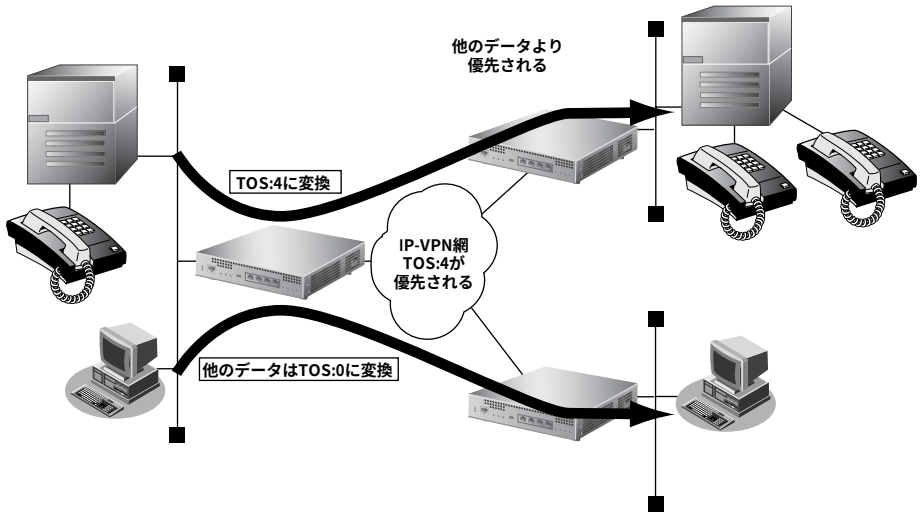
☛参照 MR1000　コマンド設定事例集「2.16 VoIP NATトラバーサル機能を使う」（P.206）
MR1000　Web設定事例集「2.16 VoIP NATトラバーサル機能を使う」（P.486）

2.16　TOS/Traffic Class値書き換え機能

TOS/Traffic Class値書き換え機能とは、指定するIPパケットのTOS値またはIPv6パケットのTraffic Class値を書き換える機能です。IP-VPN網を使って音声やレスポンスが要求されるデータのTOS/Traffic Class値を変更して送信することにより、IP-VPN網内の遅延を減らすことができます。TOS/Traffic Class値でパケット優先制御を行うキャリアVPNサービス（スーパーVPNなど）と接続する場合に有効な機能です。

本装置でサポートしているTOS/Traffic Class値書き換え機能は、以下のRFC（Request For Comments）に準拠しています。

- RFC2474：Definition of the Differentiated Services Field（DS Field）in the IPv4 and IPv6 Headers



TOS値書き換え機能は、IPv4[RFC791]で定義されている、IPパケットヘッダにある8ビットのType Of Service（TOS）フィールドを制御することができます。一般的にはこの中のPrecedenceフィールドをTOSフィールドと言いますが、本装置ではPrecedenceを含む8ビット全体を書き換えることができます。

- RFC791 Internet Protocol

0	1	2	3	4	5	6	7
Precedence			D	T	R	0	0

Bits 0-2:　Precedence.
　111 - Network Control
　110 - Internetwork Control
　101 - CRITIC/ECP
　100 - Flash Override
　011 - Flash
　010 - Immediate
　001 - Priority
　000 - Routine

Bit　3:　0 = Normal Delay,　　1 = Low Delay.

Bits　4:　0 = Normal Throughput,　1 = High Throughput.

Bits　5:　0 = Normal Relibility,　　1 = High Relibility.

Bit 6-7:　Reserved for Future Use.

RFC791のPrecedenceにより指定する場合は、以下の表を参照してください。

TOS:5（CRITIC/ECP）に変換する場合は、0xA0を指定します。

	Precedence	bit	HEX
111 -	Network Control	→ 11100000	→ 0xE0
110 -	Internetwork Control	→ 11000000	→ 0xC0
101 -	CRITIC/ECP	→ 10100000	→ 0xA0
100 -	Flash Override	→ 10000000	→ 0x80
011 -	Flash	→ 01100000	→ 0x60
010 -	Immediate	→ 01000000	→ 0x40
001 -	Priority	→ 00100000	→ 0x20
000 -	Routine	→ 00000000	→ 0x00

書き換え条件では、送信先IPアドレス、あて先ポート番号、送信元IPアドレス、送信元ポート番号、およびプロトコル番号を指定できます。この条件に一致するパケットのTOS/Traffic Class値を書き換えて送信します。複数の条件と一致する場合は、定義番号が小さい方の条件を使用します。

書き換えの対象とならなかったパケットのTOS/Traffic Class値は書き換えられません。

参照　MR1000　コマンド設定事例集「2.17 TOS/Traffic Class値書き換え機能を使う」（P.208）
MR1000　Web設定事例集「2.17 TOS/Traffic Class値書き換え機能を使う」（P.488）

2.17　VLANプライオリティマッピング機能

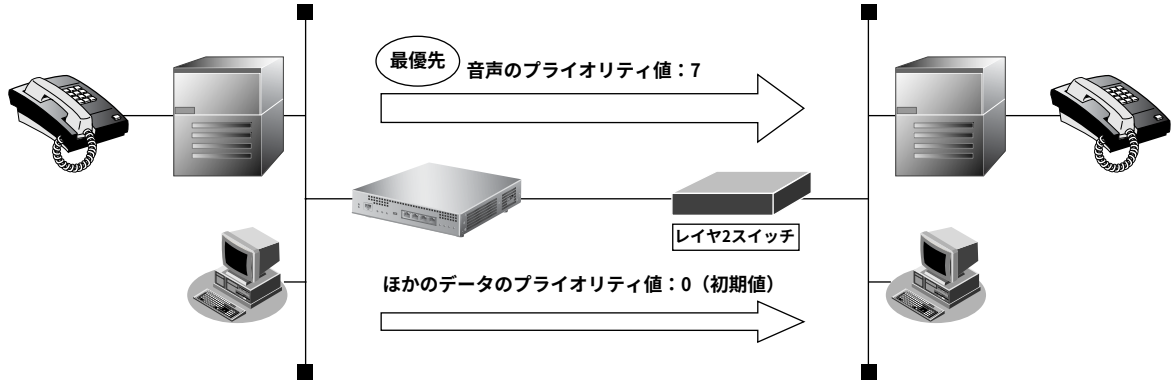
VLANプライオリティマッピング機能とは、本装置から送信するVLANパケットのプライオリティを設定する機能です。

プライオリティを設定することにより、プライオリティフィールドに対してQoS機能をサポートしているレイヤ2スイッチなどと接続することができます。

本装置では、IPパケットのTOSフィールドおよびIPv6パケットのTraffic Classフィールドの値から、VLANパケットのプライオリティ値を設定します。

プライオリティフィールドの値は0～7で、優先順位は以下のとおりです。

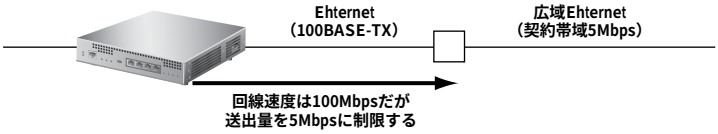
高い：7→6→5→4→3→0（初期値）→2→1：低い



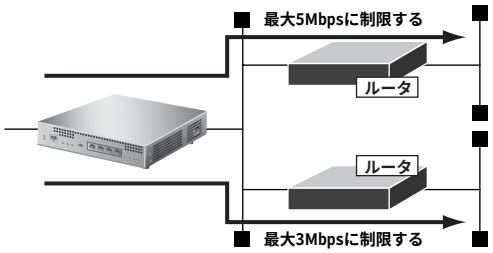
参照 MR1000　コマンド設定事例集「2.18 VLANプライオリティマッピング機能を使う」（P.210）
MR1000　Web設定事例集「2.18 VLANプライオリティマッピング機能を使う」（P.491）

2.18　シェーピング機能

シェーピング機能とは、LANおよびWAN回線に送出するデータ量（帯域）を制限する機能です。この機能を利用することで、実際の回線の帯域ではなく、指定した帯域でデータを送信することができます。



また、マルチルーティング機能と併用することによって、あて先ネットワークごとに送出帯域を制限することができます（対地シェーピング）。



こんな事に気をつけて

シェーピング機能は、以下の接続先種別では動作しません。

- ISDN
- フレームリレー
- モデム
- IPトンネル

参照　MR1000　コマンド設定事例集「2.19 シェーピング機能を使う」（P.211）
MR1000　Web設定事例集「2.19 シェーピング機能を使う」（P.493）

2.19　帯域制御（WFQ）機能

WFQ機能とは、LANおよびWAN回線上に流れる特定のデータの帯域を予約する機能です。

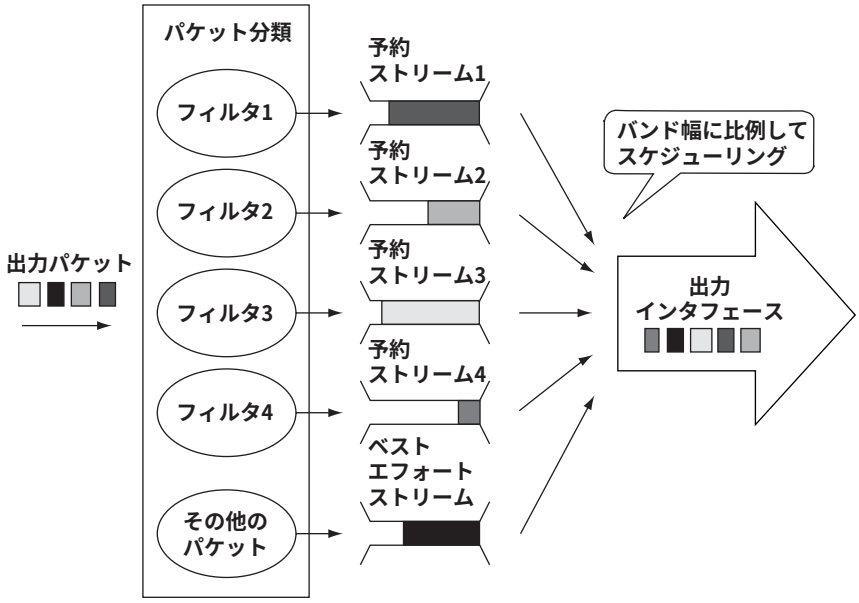
WFQ機能は予約したバンド幅の比率に応じて、出力パケットをスケジューリングします。

データストリームには、以下の2種類があります。

- 予約ストリーム
  帯域を予約したデータストリームを予約ストリームと言います。バンド幅（帯域幅）は、1Kbps単位または%で指定します。
- ベストエフォートストリーム
  予約ストリーム以外のデータフローをベストエフォートストリームと言います。ベストエフォートストリームに割り当てられるバンド幅は、「予約ストリームのバンド幅の合計」を差し引いた帯域です。

ベストエフォートストリームのバンド幅が0の場合は、予約ストリームのデータがすべての予約バンド幅を使用していないときだけ、残りのバンド幅にデータを流すことができます。

予約ストリームと予約フィルタ



予約フィルタの条件

予約フィルタとは、出力パケットがどの予約ストリームに属するのかを判別する場合に使用します。予約フィルタのIPパケットは、以下の条件で指定します。

- あて先情報（IPアドレス／アドレスマスク／ポート番号（TCP/UDP））
- 送信元情報（IPアドレス／アドレスマスク／ポート番号（TCP/UDP））
- IPパケットのTOS値またはIPv6パケットのTraffic Class値
- プロトコル番号

補足　本装置ではTOSフィールド全体を0x00～0xffで指定できますが、RFC791ではTOSを規定しています。
「• RFC791 Internet Protocol」（P.69）を参照してください。

ヒント

◆ 予約フィルタの優先順位

予約フィルタは、1つのパケットが複数のフィルタリング条件に一致する場合があります。その場合、定義番号の小さいものが優先されます。

こんな事に気をつけて

予約フィルタは、ルーティングパケットだけチェックします。これらのパケットが「ブリッジ機能」により回線上に出力していた場合は、予約帯域を使用できません。

2.19.1　トラフィックがあるストリーム数によるバンド幅の変動

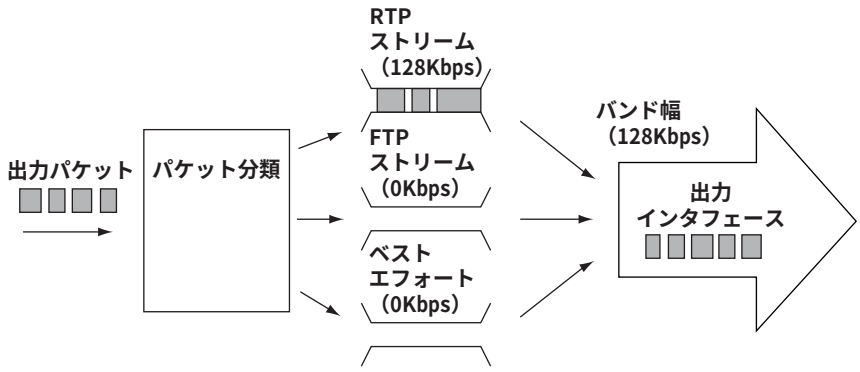
各ストリームが利用できるバンド幅は、トラフィックがあるストリーム数により変動します。
以下の条件を設定している場合を例に説明します。

● WFQの設定

- インタフェース：バンド幅＝128Kbps
- RTPストリーム：バンド幅＝32Kbps
- FTPストリーム：バンド幅＝16Kbps
- ベストエフォートストリーム：バンド幅＝80Kbps

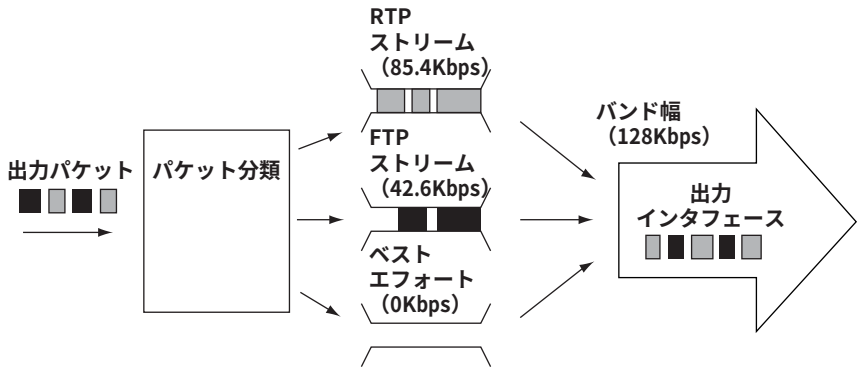
1つのストリームにトラフィックがある場合

3つのストリームのうち、1つのストリームにだけトラフィックがある場合、その1つのストリームがインタフェースのすべての帯域を使用します。
以下のようにRTPストリームにだけトラフィックがある場合、128Kbpsのすべて帯域を使用することができます。



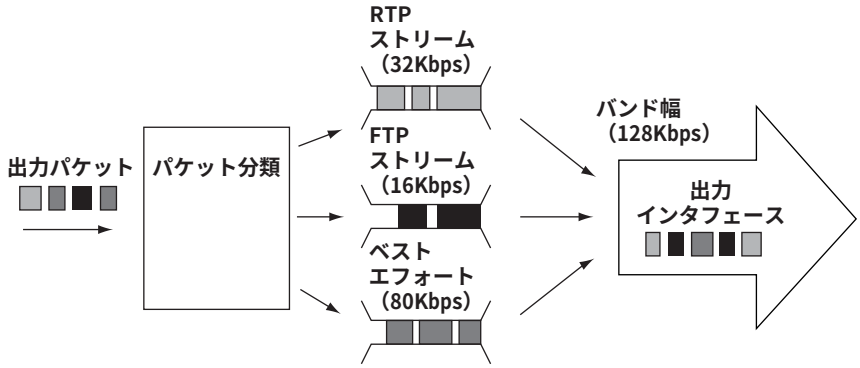
2つのストリームにトラフィックがある場合

以下のようにRTPストリームとFTPストリームにトラフィックがあります。ベストエフォートストリームにトラフィックがない場合、トラフィックがあるストリームの予約バンド幅の比率でパケットをスケジューリングします。RTPストリームとFTPストリームの予約バンド幅の比率が32：16の場合、この比率で128Kbpsの帯域を分割します。RTPストリームは85.4Kbps、FTPストリームは42.6Kbpsの帯域を使用することができます。



3つのストリームすべてにトラフィックがある場合

すべてのストリームにトラフィックがある場合は空いている帯域はありません。予約したバンド幅に従ってパケットをスケジューリングします。



こんな事に気をつけて

予約ストリームに設定するバンド幅は100%以上の負荷がかかったときの最大帯域であり、ほかのストリームが使用していない場合は空いている帯域を使って通信できます。

参照　MR1000　コマンド設定事例集「2.21 帯域制御（WFQ）機能を使う」（P.215）
MR1000　Web設定事例集「2.21 帯域制御（WFQ）機能を使う」（P.500）

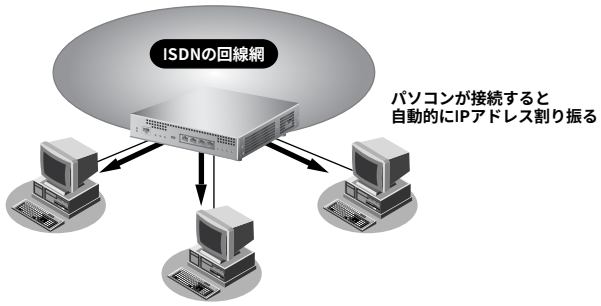
2.20　DHCP機能

2.20.1　IPv4 DHCP機能

IPv4 DHCP機能は、IPアドレスなどの情報を端末に割り振ったり（サーバ機能）、DHCPサーバからIPアドレスなどの情報を取得したり（クライアント機能）、DHCPサーバから配布される情報を遠隔地のDHCPクライアントに中継する（リレーエージェント機能）機能です。

簡易DHCPサーバ機能

簡易DHCPサーバ機能とは、IPアドレスなどの情報を端末に動的に割り振る機能です。この機能を使用して、DHCPクライアント機能を持っている端末にIPアドレスを自動的に割り当てます。割り当てたIPアドレスは、クライアントのMACアドレスと対応付けして管理します。したがって、本装置配下のLANにDHCPクライアント機能を持つ端末を接続する場合は、端末側にIPアドレスを設定する必要はありません。Windows® ではDHCPクライアント機能をサポートしています。

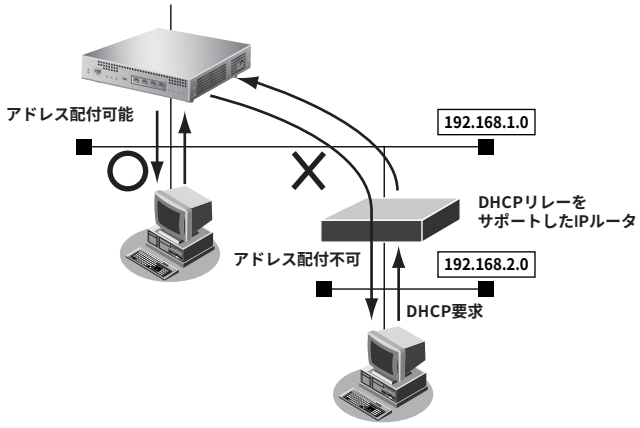


本装置はクライアントにIPアドレスを割り振る場合、ICMP ECHOパケットにより、すでに特定のIPアドレスを割り当てられているホストが存在しないかどうかをチェックします。これにより、IPアドレスが重複する危険性を取り除くことができます。

実際の設定では、割り当てるIPアドレスの開始IPアドレスと割り振ることができるIPアドレスの最大個数を設定します。本装置のIPアドレスの割り当て個数は、MR1000　仕様一覧「2.3 システム最大値一覧」（P.19）を参照してください。

こんな事に気をつけて

本装置の簡易DHCPサーバ機能は、本装置のLAN側ネットワークだけにIPアドレスを配布することができます。DHCPリレーをサポートしたIPルータを中継して、IPアドレスを配布することはできません。



以下に、本装置の簡易DHCPサーバ機能の設定内容を示します。

オプションの種類	設定範囲	初期値	意味
Subnet Mask	設定項目はない	ルータのLANのインターフェイスのサブネットマスク	
Router Option	0.0.0.0～255.255.255.255	192.168.1.1	デフォルトゲートウェイ
Domain Name Server Option	0.0.0.0～255.255.255.255	192.168.1.1	DNSサーバアドレス、セカンダリDNSサーバアドレス
Domain Name	最大80文字の英数字	なし	ドメイン名
割り当てIPアドレス数	1～253	32	
割り当て開始アドレス	0.0.0.0～255.255.255.255	192.168.1.2	
割り当て時間	0秒～1年	1日	

DHCPクライアント機能

DHCPクライアント機能は、DHCPサーバからIPアドレスなどの情報を取得する機能です。使用する場合は、DHCPサーバが動作しているLANに接続する必要があります。利用者は、IPアドレスを意識することなくネットワークを利用できます。

本装置のDHCPクライアント機能は、以下の情報を受け取って動作します。

- IPアドレス
- ネットマスク
- リース期間
- デフォルトルータのIPアドレス
- DNSサーバのIPアドレス
- TIMEサーバのIPアドレス
- NTPサーバのIPアドレス

DHCPリレーエージェント機能

DHCPクライアントは、同じネットワーク上にあるサーバから、IPアドレスなどの情報を獲得することができます。

DHCPリレーエージェントは、遠隔地にあるDHCPクライアントの要求をDHCPサーバが配布する情報を中継する機能です。この機能を利用することで、遠隔地の別のネットワークにDHCPサーバが存在する場合も同様に情報を獲得することができます。

☛参照 MR1000　コマンド設定事例集「2.22.1 DHCPサーバ機能を使う」（P.218）、
「2.22.2 DHCPスタティック機能を使う」（P.220）、「2.22.3 DHCPクライアント機能を使う」（P.222）、
「2.22.4 DHCPリレーエージェント機能を使う」（P.223）

MR1000　Web設定事例集「2.22.1 DHCPサーバ機能を使う」（P.505）、
「2.22.2 DHCPスタティック機能を使う」（P.508）、「2.22.3 DHCPクライアント機能を使う」（P.510）、
「2.22.4 DHCPリレーエージェント機能を使う」（P.512）

2.20.2　IPv6 DHCP機能

IPv6 DHCP 機能は、IPv6プレフィックスなどの情報をIPv6 DHCP クライアントに配布したり（サーバ機能）、プロバイダのIPv6 DHCP サーバからIPv6プレフィックスなどの情報を取得する（クライアント機能）機能です。
IPv6 DHCP 機能は、rmtインタフェースで利用することができます。

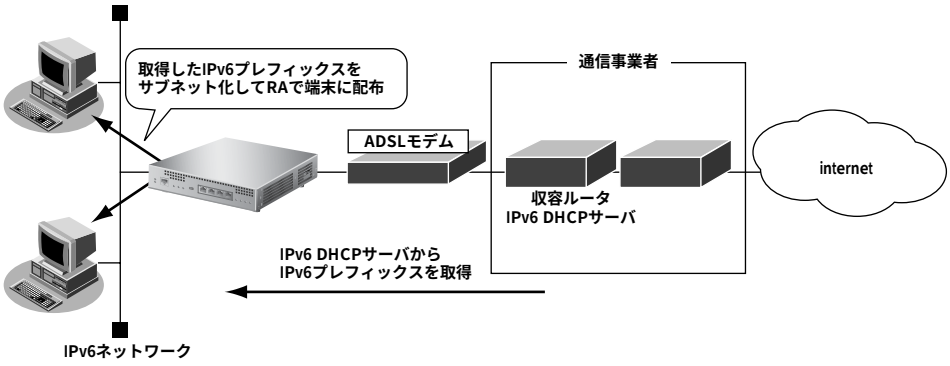
IPv6 DHCP サーバ機能

本装置では、IPv6 DHCP サーバ機能を使用して、IPv6プレフィックスとパラメタの配布をサポートしています。
以下に、IPv6 DHCP サーバ機能で設定できる項目および設定範囲を示します。

項目	設定範囲
クライアントへの割り当てIPv6プレフィックス数	1
クライアントに割り当てるプレフィックス長	48～64ビット
割り当てDNSサーバアドレス数	2

IPv6 DHCP クライアント機能

本装置では、IPv6 DHCP クライアント機能を使用して、IPv6プレフィックスとパラメタの取得をサポートしています。
本機能を利用すると、プロバイダから取得したIPv6プレフィックスをサブネット化して、Router Advertisement Message（RA）で下流ネットワークに64ビットのIPv6プレフィックスを配布することができます。



以下に、IPv6 DHCP クライアント機能で設定できる項目および設定範囲を示します。

項目	設定範囲
本装置で同時に利用できるクライアント数	4
取得できるIPv6プレフィックス数	1
取得できるプレフィックス長	48～64ビット
取得できるDNSサーバアドレス数	2

本装置でサポートするIPv6 DHCP機能は、以下のRFC（Request For Comments）およびInternet-Draftに準拠しています。

- RFC3315：Dynamic Host Configuration Protocol for IPv6（DHCPv6）
- RFC3633：IPv6 Prefix Options for Dynamic Host Configuration Protocol（DHCP）version 6
- RFC3646：DNS Configuration options for Dynamic Host Configuration Protocol for IPv6（DHCPv6）
- draft-troan-dhcpv6-opt-prefix-delegation-01.txt

以下に、本機能でサポートするIPv6 DHCPメッセージとIPv6 DHCPオプションを示します。

○：サポートする ×：サポートしない

IPv6 DHCP メッセージ	サーバ機能	クライアント機能
Solicit	○	○
Advertise	○	○
Request	○	○
Renew	○	○
Rebind	○	○
Reply	○	○
Release	○	○
Information-Request	○	×

○：サポートする ×：サポートしない

IPv6 DHCP オプション	サーバ機能	クライアント機能
OPTION_CLIENTID	○	○
OPTION_SERVERID	○	○
OPTION_ORO	○	○
OPTION_PREFERENCE	○	○
OPTION_ELAPSED_TIME	○	○
OPTION_STATUS_CODE	○	○
OPTION_DNS_SERVERS	○	○
OPTION_IA_PD	○	○
OPTION_IAPREFIX	○	○
OPTION_PREFIXDEL	×	○
OPTION_PREFIX_INFO	×	○

参照　MR1000　コマンド設定事例集「2.22.5 IPv6 DHCPクライアント機能を使う」（P.226）
MR1000　Web設定事例集「2.22.5 IPv6 DHCPクライアント機能を使う」（P.516）

2.21　DNSサーバ機能

DNSサーバ機能とは、LANインタフェース内の端末へのDNS要求に対して、上位DNSサーバ（たとえば、プロバイダのDNSサーバ）を中継しないで、本装置が持っている情報を返すことができる機能です。

DNSサーバ機能を使用する場合、端末はDNSアドレスとしてルータのIPアドレスを設定します。端末がDHCPクライアントの場合は、DHCPサーバが通知するDNSアドレスとしてルータのLANポートのIPアドレスを通知する必要があります。

本装置には、以下の2種類のDNSサーバ機能があります。

- DNSサーバ（スタティック）機能
- ProxyDNS（DNS振り分け）機能

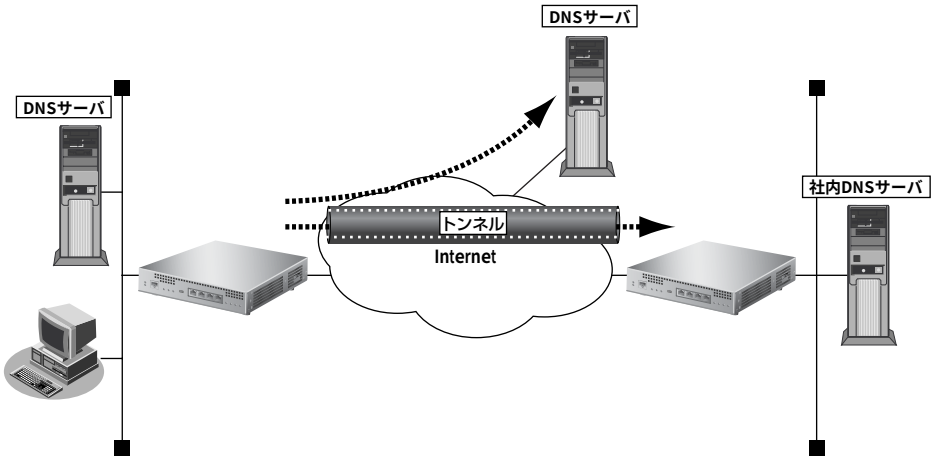
2.21.1　DNSサーバ（スタティック）機能

ドメイン名（FQDN：Fully Qualified Domain Name）とIPアドレスの組を静的に設定します。DNSクライアントからの問い合わせ（順引き、逆引き）に対し、設定したエントリを検索し、該当エントリが見つかった場合は応答します。見つからなかった場合は、上位DNSサーバに問い合わせます。逆引き（IPアドレスから名前を応答）する場合は、応答パケット内に含まれるTYPEとCLASSを、TYPE=A（1 a host address）、CLASS IN（1 the Internet）固定とします。

スタティックテーブルは最大で64エントリです。

2.21.2　ProxyDNS（DNS振り分け）機能

ProxyDNS（DNS振り分け）機能は、DNS機能を使用した場合に問い合わせられたURL（順引き）またはIPアドレス（逆引き）により、本装置が問い合わせ先のDNSサーバを自動的に割り振ることができます。そのため、DNSを使用しないで、以下のような環境をリモートサイト側に実現できます。



本装置が端末からDNSのQueryメッセージを受信した場合、DNS振り分けテーブル内に、問い合わせ先のドメイン名と一致するエントリが存在するかどうかをチェックします。一致するエントリが存在する場合は、その一致したエントリのDNSアドレスにメッセージを転送します。一致するエントリが存在しない場合は、デフォルトDNSアドレスにメッセージを転送します。

文字列の後ろから順に設定された文字列長を比較し、すべての文字列が一致している場合に、エントリと一致したと判断します。また、"＊"は特別な文字として、"＊"以降の比較は行わずに該当エントリを一致したと判断します。

設定例）

ドメイン名	DNSサーバアドレス
www.omron.co.jp	1.1.1.1
ftp.omron.co.jp	2.2.2.2
*.is.fuku.omron.co.jp	3.3.3.3

デフォルトDNSサーバの設定ができ、上記でエントリを検索できなかった場合は、デフォルトサーバに問い合わせます。

DNS振り分けテーブルは最大32エントリです。

参照　MR1000　コマンド設定事例集「2.23 DNSサーバ機能を使う（ProxyDNS）」（P.228）
MR1000　Web設定事例集「2.23 DNSサーバ機能を使う（ProxyDNS）」（P.520）

2.22　SNMP機能

SNMP（Simple Network Management Protocol）とは、IP層およびTCP層レベルの情報を収集、管理するためのIP管理用のプロトコルです。

SNMP機能では、管理する装置をSNMPマネージャ、管理される装置をSNMPエージェントと言います。

SNMP機能でネットワークを管理する場合、管理する側はSNMPマネージャ機能を、管理される側はSNMPエージェント機能をサポートしている必要があります。

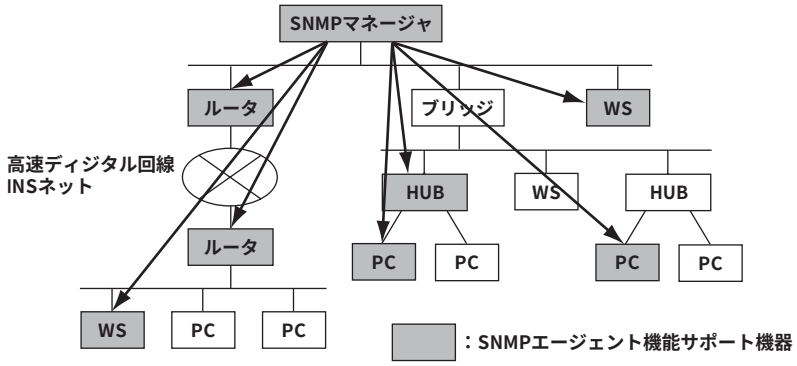
SNMPマネージャ機能は、ネットワーク上の端末の稼働状態や障害状態を一元管理します。SNMPエージェント機能は、SNMPマネージャの要求に対してMIB（Management Information Base：管理情報ベース）という管理情報を返します。

SNMP機能は、この2つの機能を使用して、SNMPマネージャとSNMPエージェントとの間でMIBに定義されたパラメタを送受信してネットワークを管理します。

本装置で使用するMIBは、標準MIBをサポートしています。

参照　MR1000　仕様一覧「3.1 標準MIB定義」（P.23）

SNMP機能による管理



ヒント

◆ MIBとは

MIBには、装置のベンダに関係ない標準MIBと装置ベンダ固有の拡張MIBがあります。RFC1213などで定義される標準MIBは、管理ノードのそれぞれの管理対象（オブジェクト）にアクセスするための仮想の情報領域です。RFCでは、SNMPエージェントが実装すべき管理情報を定義しています。管理情報には、SNMPノードとしてのシステム情報（システム名や管理者名など）やTCP/IPに関連する統計情報があります。しかし、RFCで定義されている項目では伝送路やHUBなどを十分に管理できません。そのため、各種プロトコルの情報や各社の装置ごとのベンダ固有に合わせてMIBを拡張します。これを拡張MIBと言います。

MIBはASN.1（Abstract Syntax Notation 1）という形式で定義します。SNMPマネージャが拡張MIBを管理するためには、SNMPエージェント側でその拡張MIBを公開して、SNMPマネージャがその拡張MIBの情報を収集するように定義する必要があります。

参照　MR1000　コマンド設定事例集「2.25 SNMPエージェント機能を使う」（P.237）
MR1000　Web設定事例集「2.25 SNMPエージェント機能を使う」（P.532）

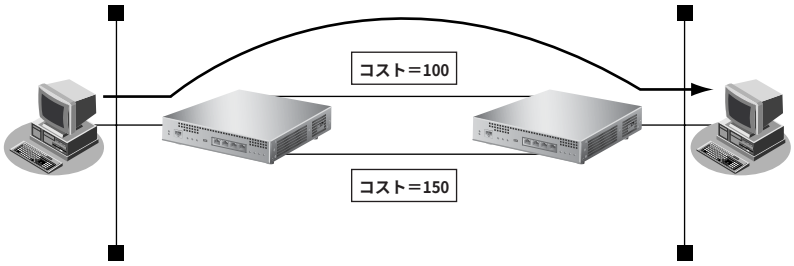
2.23　ECMP機能

一般的に、ルーティングによる転送先は、経路として設定された1つのネットワークに対して到達可能な通信パスが複数ある場合、その通信コストを考慮して、もっとも通信コストの小さい通信パスを唯一に決定します。

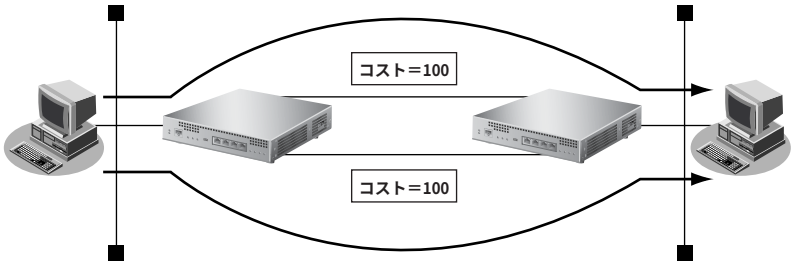
ECMP（Equal Cost Multi Path）機能は、同じあて先ネットワークにパケットを送信する場合に、同じ通信コストのパスを併用することによって、通信パスの負荷を分散することができる機能です。

通信パスは、最大4つまで同時に利用することができます。

- 一般的なルーティング：通信コストが最小の通信パスだけを利用する場合



- ECMP機能によるルーティング：同じ通信コストの通信パスを同時利用する場合



ECMP機能では、スタティックルーティングによる経路設定またはOSPFを利用して経路学習を行った場合に、複数の通信パスを同時に利用することができます。

スタティックルートとOSPFを併用した複数パスは構成できません。スタティックルートの範囲で構成される複数の通信パスとOSPFの範囲で構成される複数の通信パスとは独立して設定されます。同じ経路に対してスタティックルートとOSPFの両方の通信パスが存在した場合は、優先度設定に基づいて、どちらかの通信パスが決定されます。

- スタティックルーティングの場合
  経路優先度およびメトリック値が同じスタティックルートはECMPとして同時に利用されます。
- OSPFを利用する場合
  通信パスの経路計算によって同じ通信コストとなった場合に、ECMPとして同時利用されます。

こんな事に気をつけて

- **ECMP機能はIPv4の場合だけ利用できます。**
- **特定の通信セッションを特定の通信パスに意図的に通すことはできません。利用する通信パスは、パケット転送時に決定されます。ハッシュ方式を使用した場合も、通信パス数が変化すると、利用される通信パスが変更されることがあります。**
- **NAT機能と併用することはできません。また、ECMP機能によって負荷を分散した通信パスの途中経路で、NAT機能によってアドレス変換を動作させることはできません。NAT機能を利用する場合は、それぞれの通信セッションが同じ通信パスを利用し続けることが必要ですが、ECMP機能を利用して負荷を分散した場合、同じ通信パスを利用し続けることができなくなることがあります。**
- **通信パス選択方式でラウンドロビン方式を選択した場合は、ECMP機能によって負荷分散する通信パスの途中経路で、パケットの内容を参照して処理を行う機能（IPフィルタリングやTOS書き換え機能など）を使用しないでください。IPフラグメントされたそれぞれのパケットも別々の通信パスを使用するため、正しく処理できない場合があります。**
- **MPLS機能と併用した場合、経路として複数通信パスが構成されていても、負荷を分散することはできません。**
- **ISDN通信またはPPPoE通信で常時接続機能を利用しない接続先との通信パスは、認証失敗などの理由で通信できない場合でも通信パスの異常が検出できないため、ECMP機能の通信パスに利用しないでください。正常に通信することができなくなることがあります。**

2.23.1　通信パス選択方法

ECMP機能では、どの複数の通信パスでパケットを転送するのかを決定するのに、以下の方式があります。

- ラウンドロビン方式
  それぞれの送出パケットに、利用する通信パスを切り替えることができます。通信パスの負荷はほぼ均等に分散しますが、パケットの転送順は保証されません。
- ハッシュ方式
  送出パケットの内容によって、利用する通信パスを選択します。この方法を利用した場合、同じホスト間の通信は同じ通信パスを利用します。そのため、パケットの転送順は保証されますが、通信パスの負荷は偏る場合があります。

本装置では、以下の順序で通信パスを選択します。

（1）　転送パケットの送信元IPアドレスとあて先IPアドレスを、32ビットの値として加算します。

（2）　（1）の結果の上位16ビットの値と下位16ビットの値を加算し、桁上がりを無視して16ビットの値を算出します。

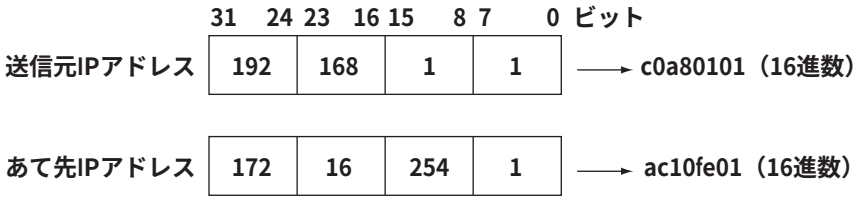
（3）　(2)の結果の上位8ビットの値と下位8ビットの値を加算し、桁上がりを無視して8ビットの値を算出します。

（4）　（3）の結果を利用可能な通信パス数で割った余りを求めます。

（5）　（4）の余りを、以下に当てはめて、通信パスを決定します。
・余りが0の場合 ： 通信パス1を利用
・余りが1の場合 ： 通信パス2を利用
・余りが2の場合 ： 通信パス3を利用
・余りが3の場合 ： 通信パス4を利用

例）送信元IPアドレスが192.168.1.1、あて先IPアドレスが172.16.254.1であるパケットについて、192.168.2.0/24に到達する通信パス1、通信パス2、通信パス3、通信パス4が存在する場合

（1）



それぞれを加算します。
c0a80101 + ac10fe01 = 16cb8ff02（16進数）
桁上がりを無視して32ビットの値にすると6cb8ff02（16進数）となります。

（2）（1）の結果の上位16ビットと下位16ビットを加算します。
6cb8 + ff02 = 16bba（16進数）
桁上がりを無視して16ビットの値にすると6bba（16進数）となります。

（3）（2）の結果の上位8ビットと下位8ビットを加算します。
6b + ba = 125（16進数）
桁上がりを無視して8ビットの値にすると25（16進数）となります。この値を10進数で表すと37になります。

（4）（3）の結果の37を4で割った余りを求めると1となります。

（5）（4）の結果により、通信パス2の利用が決定されます。

2.23.2　通信バックアップ機能

通信バックアップ機能と併用することによって、通信パスの一部に障害が発生した場合、正常な通信パスを利用して通信を継続することができます。これによって、正常時には複数通信パスを利用して負荷を分散し、通信障害発生時には利用可能な通信パスを利用して通信を継続することができます。

参照　MR1000　コマンド設定事例集「2.26 ECMP機能を使う」（P.239）
MR1000　Web設定事例集「2.26 ECMP機能を使う」（P.534）

2.24　VRRP機能

VRRP機能とは、動的に経路制御（RIPなど）できない端末から、別のネットワークへの通信に使用しているルータがなんらかの理由で中継できなくなった場合、自動でほかのルータが通信をバックアップする機能（簡易ホットスタンバイ機能）です。また、VRRPのグループを複数設定することで、通信の負荷分散と冗長構成を実現する機能（クラスタリング機能）もサポートしています。

VRRP機能は2つ以上のルータがグループを形成し、1台のルータ（仮想ルータ）のように動作します。グループ内の各ルータには優先度が設定されており、その優先度に従ってマスタルータ（実際にルーティングを行う装置）とバックアップルータ（マスタルータで異常を検出したときにルーティング処理を引き継ぐ装置）を決定します。また、グループごとに仮想IPアドレスを設定し、マスタルータがグループあてのパケットを処理します。

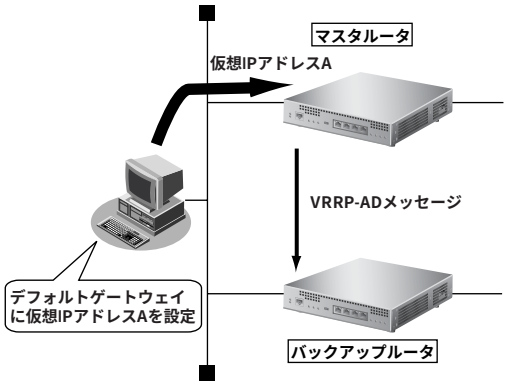
動的な経路制御をサポートしていない端末では、静的経路のデフォルトルータとして仮想IPアドレスを設定することで、仮想ルータを使用した信頼性の高い通信を実現できます。

さらに、2つ以上のルータで複数のグループをマスタルータが分散するように設定し、端末ごとにデフォルトルートの仮想ルータを分けて設定することで、負荷分散と冗長構成のクラスタリング機能も実現できます。

VRRP機能を使用するときのルータの動作を以下に説明します。

2.24.1　簡易ホットスタンバイ機能

- 通常時の動作
  VRRP機能を使用している場合、マスタルータは、定期的にバックアップルータにVRRP-ADメッセージ（VRRP Advertisement message:VRRP広報メッセージ）を送信します。バックアップルータは、マスタルータからのVRRP-ADメッセージを受信することで、マスタルータが正常に動作していると判断します。
  マスタルータでは、仮想IP／MACアドレスあてのパケットは処理されますが、バックアップルータではすべて破棄されます。

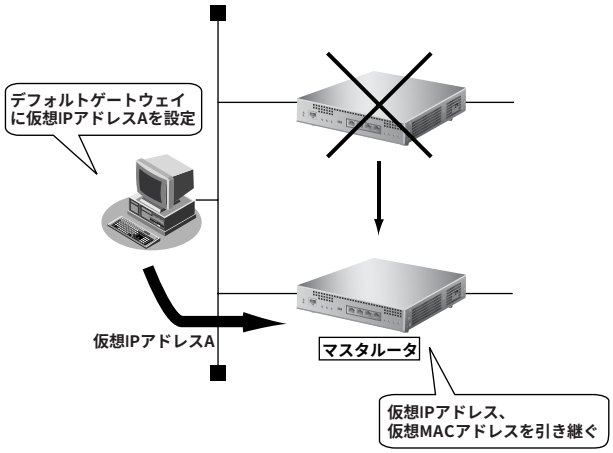


- 障害発生時の動作
  マスタルータがダウンすると、VRRP-ADメッセージは送信されません。よって、バックアップルータでは、最後にVRRP-ADメッセージを受信してからマスタルータのダウン検出時間までに次のVRRP-ADメッセージが受信できなかった場合、マスタルータがダウンしたと判断します。バックアップルータは、仮想IPアドレスと仮想MACアドレスを引き継いで、マスタルータとして動作します。マスタルータのダウン時間は、以下の計算式で計算されます。

  VRRP-ADメッセージ送信間隔 × 3 ＋ Skew_Time［秒］

  Skew_Time　：マスタルータがダウンした際に、より優先度の高いバックアップルータがスムーズに切り替われるようにするための誤差であり、以下の計算式で計算されます。

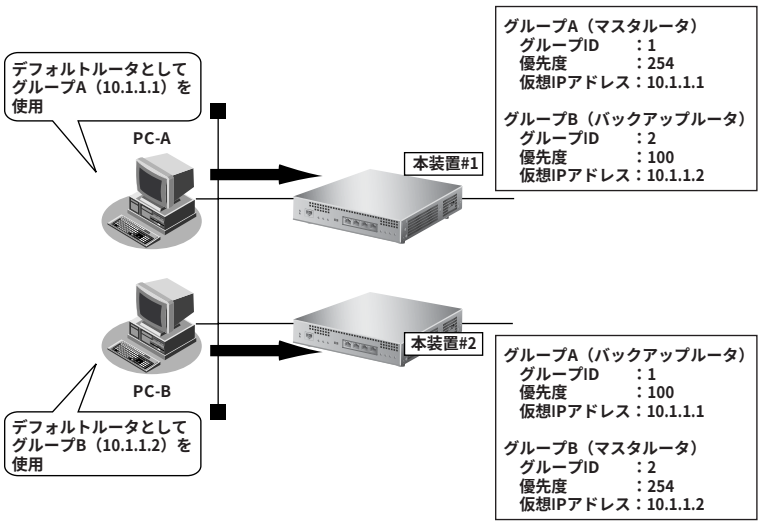
  Skew_Time =（256 - VRRP優先度）/ 256［秒］



- ダウントリガ
  ダウントリガが適用された場合、VRRP グループの現在の優先度から指定した値を減算した優先度のVRRP ルータとして動作します。
  - インタフェースダウントリガ
    ケーブル抜け、同期はずれ、またはPVC 状態確認手順によって通信不可と判断された該当インタフェースに設定されたダウントリガを適用します。
  - ルートダウントリガ
    指定したあて先経路が、指定したインタフェースのルーティングテーブルに存在しない場合、ダウントリガを適用します。
  - ノードダウントリガ
    指定したインタフェースから指定したあて先にICMP ECHO パケットを送出し応答がない場合、ダウントリガを適用します。
- 障害復旧時の動作
  グループ内でもっとも優先度の高いルータが復旧した場合、同じグループ内のマスタルータはマスタルータを放棄し、バックアップルータとなります。
  自動復旧を望まない環境ではプリエンプトモードをoff にすることで、自動復旧を禁止することができます。その場合は、保守作業完了後に「操作メニュー」の「VRRP 手動切り戻し」またはvrrpctl コマンドを実行することでマスタルータの切り替え（切り戻し）ができます。

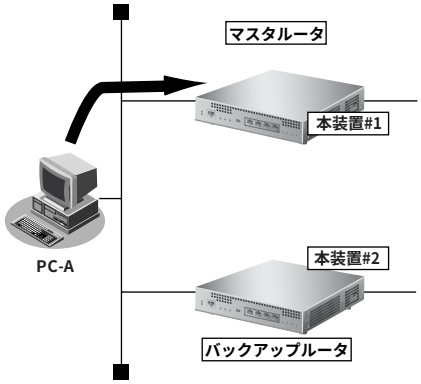
2.24.2　クラスタリング機能

- 通常時の動作
  PC-A グループはVRRP グループA を、PC-B グループはVRRP グループB をデフォルトルータとして設定することで、負荷分散を実現できます。また、グループごとにバックアップルータが存在して、ルータを相互にバックアップしているので、グループAのマスタルータがダウンした場合でもバックアップルータが処理を引き継ぐことができます。

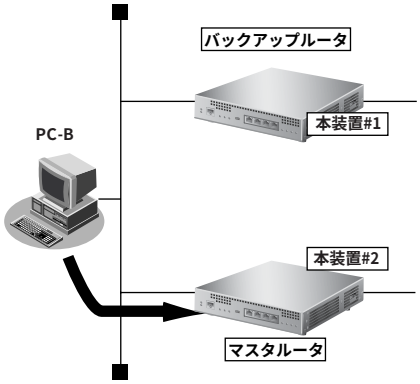


上の図をPC-A グループ、PC-B グループから見たときの構成は以下のようになります。

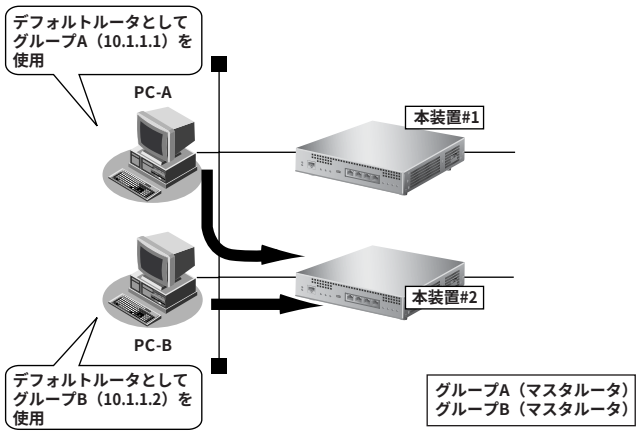
PC-A グループから見たときの構成



PC-B グループから見たときの構成



- 障害発生時の動作
  本装置 #1 がダウンしたとき、グループ A に対するマスタルータは本装置 #2 に引き継がれます。切り替え動作については、「2.24.1 簡易ホットスタンバイ機能」（P.86）を参照してください。



- ダウントリガ
  ダウントリガが適用された場合、VRRP グループの現在の優先度から指定した値を減算した優先度の VRRP ルータとして動作します。
  トリガの種類については、「2.24.1 簡易ホットスタンバイ機能」（P.86）を参照してください。
- 障害復旧時の動作
  「2.24.1 簡易ホットスタンバイ機能」（P.86）と同様の手順で切り替えが発生します。

こんな事に気をつけて

- VRRP 機能は IPv4 だけサポートしています。
- 同一のインタフェースに定義可能な VRRP グループは最大 2 つまでです。
- VRRP グループのグループ ID は、同一装置内で重複しないように設定してください。
- VRRP グループに割り当てる仮想 IP アドレスと実 IP アドレスは、必ず同じサブネットになるよう設定することをお勧めします。
- 同一グループには最大 2 台まで属することができます。
- 同一グループとして使用できるルータは VRRP をサポートする本装置だけです。
- 本装置の電源の投入、マスタルータでの設定反映、または装置リセットを実行した場合、バックアップルータがマスタルータとなることがあります。
- VRRP 機能によって切り替えが発生したあと、通信可能となるまでの時間は使用している経路制御プロトコルに依存します。
- VRRP 機能を使用している場合、マスタルータは、VRRP-AD（VRRP Advertisement message：VRRP 広報メッセージ）をバックアップルータに定期的に送信します。バックアップルータは、マスタルータからの VRRP-AD メッセージを受信することで、マスタルータが正常に動作していると判断します。バックアップルータは VRRP-AD メッセージを最後に受信してから一定時間内に次の VRRP-AD メッセージを受信できなかった場合、マスタルータがダウンしたと判断し、新たなマスタルータとして動作します。
- ノードダウントリガを使用する場合、相手ノードに ICMP ECHO パケットを定期的に送信します。そのため、定額制ではない回線を使用している場合は、超過課金の原因になることがあります。このような環境ではノードダウントリガを使わないでください。ルートダウントリガで指定したあて先経路に対してスタティックルートが存在する場合、ルートダウントリガは発生しません。また、ルートダウントリガで指定したあて先経路とすべて同じ経路情報ではない場合でも、デフォルトルートまたはネットワークマスクがより小さい同じネットワークの経路情報が存在したときは、ルートダウントリガは発生しません。
- 簡易ホットスタンバイ機能を使用する場合、ブリッジ機能と併用することはできません。また、ルータと接続する HUB は、STP 機能を無効にしてください。STP 機能を有効にすると、簡易ホットスタンバイで連携している装置と無関係なケーブルの抜き差しによって、故障を検出することがあります。
- VRRP 機能と併用して、以下の機能を使用する場合は注意が必要です。
  マルチ NAT 機能　：切り替え発生時に端末からの通信が途切れることがあります。
  簡易 DHCP サーバ機能　：DHCP スタティック機能を使用しない場合、IP アドレスを更新すると別の IP アドレスが割り当てられることがあります。
  IP フィルタリング機能　：切り替え発生時に端末からの ftp が途切れることがあります。

課金制御機能	：切り替え発生時に課金情報は引き継がれません。課金情報の累計は0から再スタートとなります。
Proxy DNS	：仮想ルータのIPアドレスをDNSサーバのアドレスとして使用することはできません。
VPN機能	：マスタルータとバックアップルータは同じIPsecトンネル（対象パケットとトンネル出口のIPアドレスが同じ）を設定しないでください。同じIPsecトンネルを設定した場合、相手装置からの送信パケットを正しいルータで受信することができません。また、自動鍵交換は、仮想IPアドレスを使用することはできません。

参照　MR1000　コマンド設定事例集「2.27 VRRP機能を使う」（P.244）
MR1000　Web設定事例集「2.27 VRRP機能を使う」（P.573）

2.25　ブリッジ機能

ブリッジ機能とは、異なるLANを接続し、MACフレームを中継する機能です。接続形態には、LAN-LAN接続とLAN-WAN接続の2つがあります。

LAN-WAN接続でブリッジ接続可能な接続先種別は、以下のとおりです。

- ISDN
- 専用線
- フレームリレー
- IPトンネル（Ethernet over IPブリッジ）
- アナログモデム

本装置では、以下の3つの機能をサポートしています。

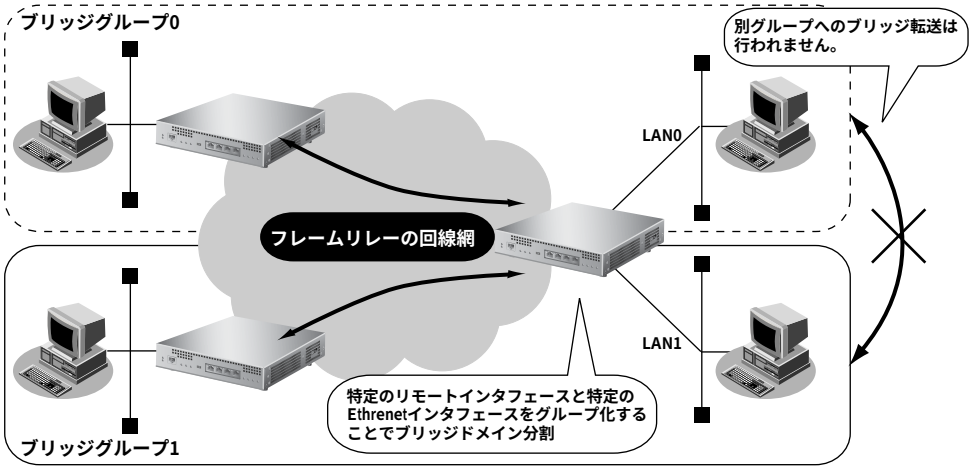
- ブリッジドメインを分割するためのブリッジグルーピング機能
- IPフレームの転送方式（ルーティング／ブリッジ）の選択機能
- 物理的にループ形態になっているネットワークで、MACフレームの中継が無限にループするのを回避するスパニングツリー機能

それぞれの機能に対応している機種は、以下を参照してください。

参照　MR1000　仕様一覧「2.1 ソフトウェア仕様」（P.15）

2.25.1　ブリッジグルーピング機能

ブリッジグルーピング機能とは、各インタフェースにグループ識別子を設定し、それぞれのインタフェースにグループを割り当てることによって、ブリッジ転送が、そのグループ内に閉じた形で行われるようにする機能です。グループを分けることで、以下の図のように、ブリッジ通信を各グループに分離することができます。

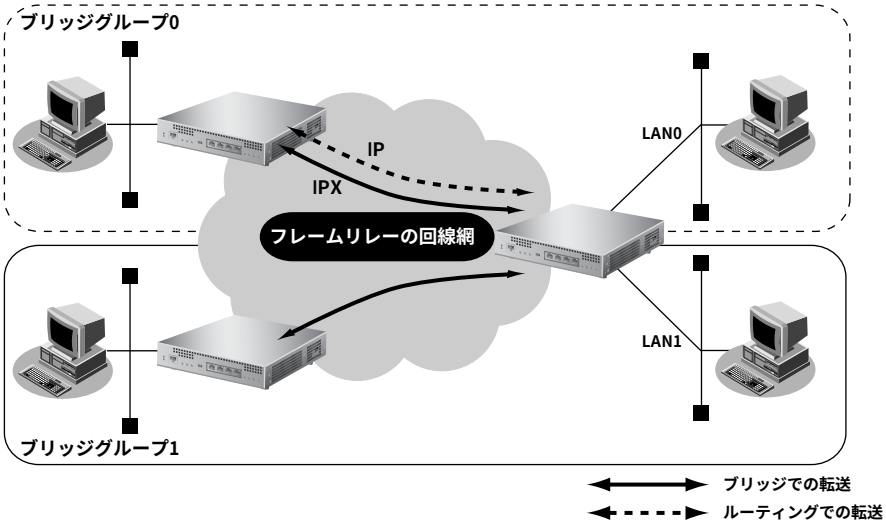


2.25.2　IPフレームの転送方式の選択機能

ブリッジグループ単位で受信したIPv4またはIPv6のフレームを、ブリッジ対象とするかどうかを選択することができます。通常、受信したIPフレームは、ルーティングで転送されます。しかし、ブリッジグループ内でルーティングを無効にした場合、IPフレームはブリッジで転送されます。

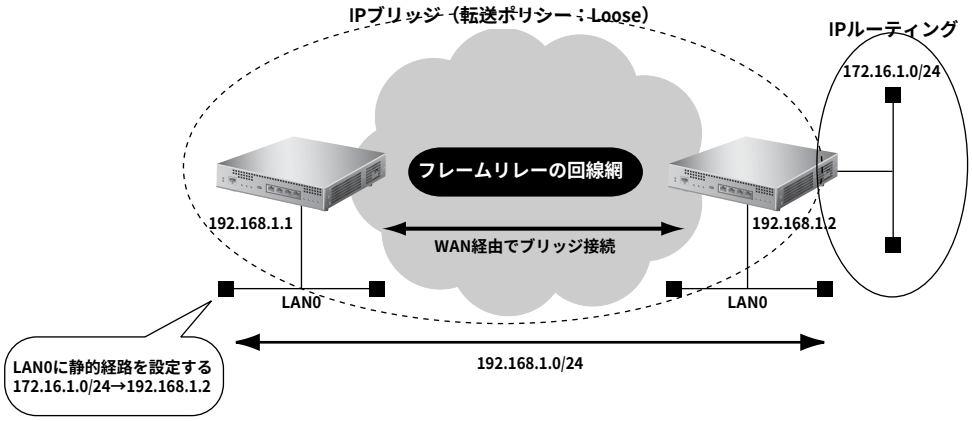
以下に例を示します。

ここでは、グループ0では、IPがルーティングで転送され、IP以外（IPXなど）はブリッジで転送されます。グループ1では、IPおよびIP以外もブリッジで転送されます。



IPフレームをブリッジ対象とした場合、WANインタフェース上ではブリッジで中継されるEthernetフレームだけが送受信され、直接WAN側にEthernetフレームではないIPパケットを送受信することはできません。

よって、IPフレームをブリッジする運用形態では、IPフレームに関する定義はすべてLANインタフェース側で行い、リモートインタフェースではIPフレームに関する定義は行わないでください。WANを経由して相手装置とブリッジで接続されているため、IPフレームをブリッジ対象として運用する場合は、以下の図のようにLAN側に静的経路の設定を行います。その経路に該当するIPパケットは、LAN側に送出される過程でブリッジによってWAN側にも転送されます。そのため、WANの先に存在するネットワークであっても、LAN側に静的経路を設定することで、そのネットワークにブリッジ経由で到達することができます。



転送ポリシ

IPv4またはIPv6のフレームをブリッジで処理する場合、受信したIPフレームのあて先MACアドレスが本装置あてでないとき、そのIPフレームはそのままブリッジで転送されます。

受信したIPフレームのあて先MACアドレスが受信インタフェースあてで、あて先IPアドレスも受信インタフェースあての場合は、本装置あてのIPフレームとして処理します（これによってPingの応答やファームウェアの更新などがIPフレームをブリッジで転送するインタフェース上でも可能になります）。

しかし、あて先MACアドレスが受信インタフェースあての場合でも、あて先IPアドレスが受信インタフェースあてではないことがあります。あて先IPアドレスが受信インタフェースあてでなかった場合は、転送ポリシを設定することによって、そのIPパケットを転送するかどうかを選択することができます。

また、IPフレームをルーティングで処理するインタフェースからIPフレームをブリッジで転送するインタフェースへ、ルーティング処理によって受信したパケットを出力する場合も、転送ポリシによって、そのパケットがブロックされるか転送されるかが決まります。

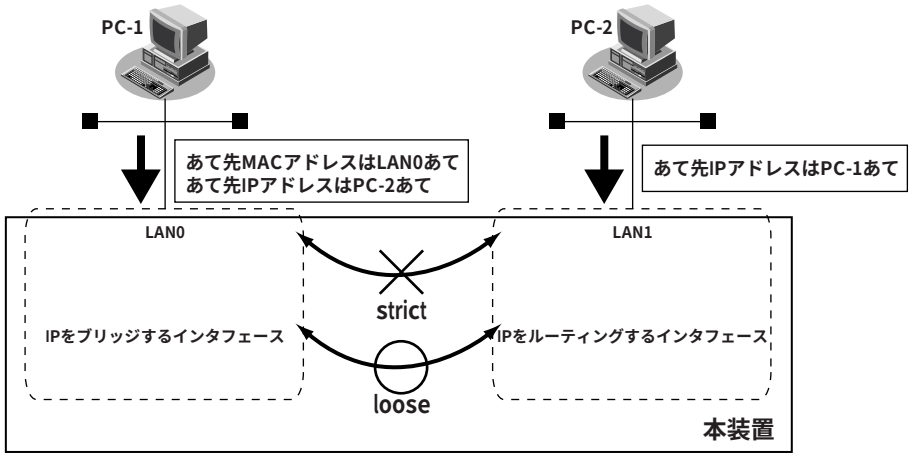
転送ポリシには、以下の2つがあります。

- strict
  IPv4ブリッジを行う場合は、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行いません。
- loose
  IPv4ブリッジを行う場合は、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行います。

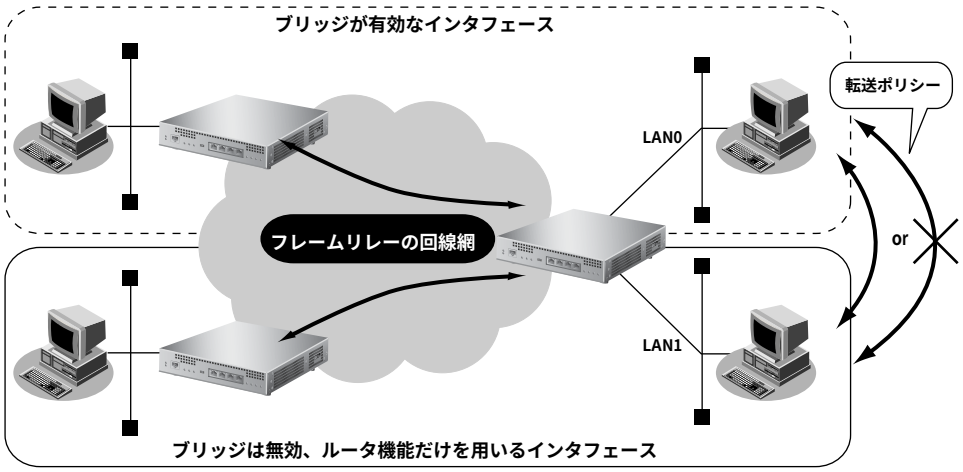
IPv4ブリッジ動作時にグループ内からグループ外へのルーティングによる転送が行われるのは、受信フレームのあて先MACアドレスが受信インタフェースあてであるが、あて先IPアドレスが受信インタフェースあてでない場合です。

また、IPv4ブリッジ動作時にグループ外からグループ内へのルーティングによる転送が行われるのは、IPv4をルーティングするインタフェースで受信したパケットが、ルーティングによって、IPv4をブリッジするインタフェースへ出力される場合です。

strictの場合、これらの転送をブロックすることで、ブリッジ転送対象外のパケットに対してもグループ内に閉じた通信を行うことができます。



また、以下の図のように、ルータ機能を使用するインタフェースと、ブリッジ機能を使用するインタフェースを同時に動作させることができます。ブリッジが有効なインタフェース上で、IPもブリッジ対象としている場合は、転送ポリシを選択することによって、ルータ機能を用いているインタフェースとIPをブリッジするインタフェースとの間の転送をブロックするかどうかを決めることができます。



複数 LAN を同じグループに設定して IPv4 や IPv6 をブリッジする場合、そのグループ内で定義番号がもっとも小さい LAN インタフェースがレイヤ 3 代表インタフェースとなります。

本装置あての IP 通信や IP 関連の機能は、そのブリッジグループ内ではレイヤ 3 代表インタフェースでだけ使用することができます。上記の運用形態でファームウェアの更新や Web 画面設定などを行う場合は、本装置のレイヤ 3 代表インタフェースに割り当てられた IP アドレスをあて先として作業してください。

また、VLAN インタフェースをブリッジグループに含める場合は、1 つの VLAN インタフェースと、1 つまたは複数のリモートインタフェースのグルーピングだけを行うことができます。複数の VLAN インタフェースのグルーピングや VLAN インタフェースと通常の LAN インタフェースのグルーピングは行うことができません。

2.25.3　スパニングツリー機能

スパニングツリー機能とは、物理的にループを構成するブリッジ構成で、複数ある経路のうちの 1 つだけを通信経路とし、論理的にツリー構造のネットワークを構成する機能です。この機能を使用することによって、システムダウンにつながるようなフレームのループは発生しません。また、使用している経路上になんらかの障害が発生した場合は、自動的にほかの経路を用いてツリー構造を再構成するため、障害に強いネットワークが構築できます。

ヒント

以下にスパニングツリーを構成するうえで重要な語句を説明します。

◆ スパニングツリーを構成するブリッジ

- **ルートブリッジ**
  システム中で最小のブリッジ識別子をもつブリッジをルートブリッジと言います。ルートブリッジはツリー構造の頂点に位置し、システム中に 1 台だけ存在します。
- **代表ブリッジ**
  1 つの LAN に接続された複数のブリッジの中で、最小のルートパスコストをもつブリッジ（ルートブリッジに近い）をその LAN の代表ブリッジと言います。ルートブリッジは接続されているすべての LAN 上で代表ブリッジとなります。

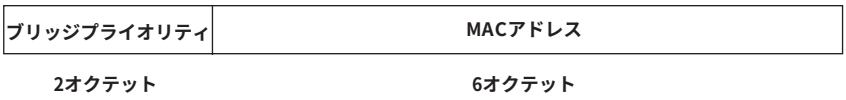
◆ スパニングツリーを構成するブリッジのポート

- **ルートポート**
  フォワーディング状態のポートであり、各ブリッジで最小のルートパスコストのポートがルートポートとなります。ルートポートは、それぞれのブリッジに必ず 1 つ存在します。
- **代表ポート**
  フォワーディング状態のポートです。1 つの LAN 上に複数接続したポートの中に 1 つだけ存在します。ルートブリッジのすべてのポートは、接続された LAN 上の代表ポート（代表ブリッジ）となります。

- ブロッキングポート
  ブロッキング状態のポートであり、MACフレームは中継しません。ルートポートでも代表ポートでもないポートがブロッキングポートとなります。
  ＜フレームの中継動作＞
  - フォワーディング
    MACフレームを中継します。また、MACアドレス情報の学習を行います。
  - ブロッキング
    MACフレームは中継しません。また、MACアドレス情報の学習を行いません。

◆ ツリー構造を構成するための要素

- ブリッジ識別子
  ブリッジ識別子は、最小のブリッジプライオリティ（任意に指定）とポート番号のポートがもつMACアドレスの2つのフィールドから構成されます。ブリッジ識別子とルートパスコストにより、構成するツリー構造の各ブリッジの優先度を決めます。同じ値のブリッジプライオリティが設定されたブリッジは、MACアドレスにより識別されますが、通常はブリッジプライオリティ＝ブリッジ識別子となります。



- ルートパスコスト
  各経路にコストが割り当てられると、各ブリッジはそのブリッジからルートブリッジへ達するいくつかの経路にそれぞれ対応して、1つまたは複数のコストをもちます。この中で最小のコストをブリッジでのルートパスコストと言います。

☛参照「＜ルートパスコストの算出＞」(P.102)

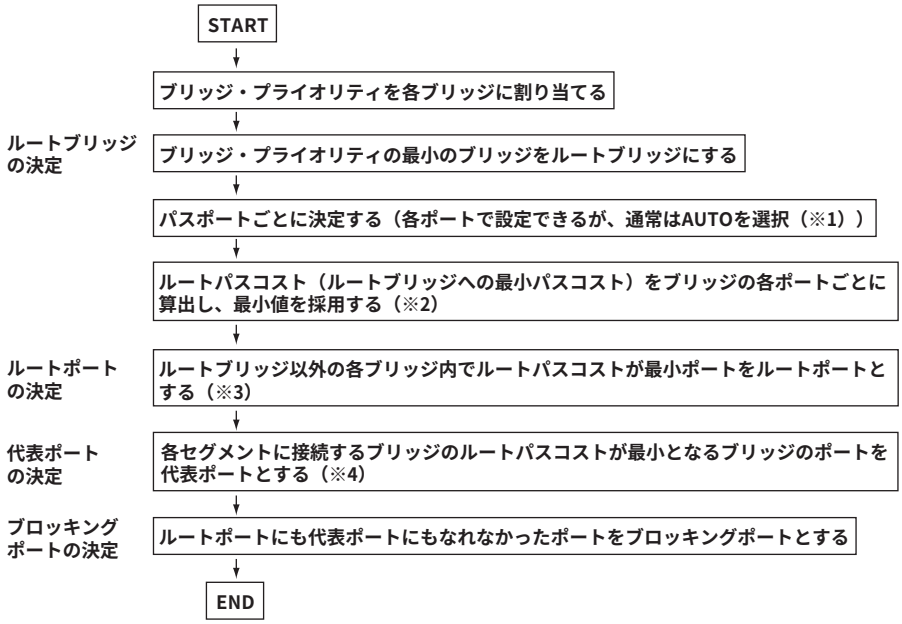
- 構成BPDU
  論理的なツリー構造を構成するためにブリッジ間でやり取りされるブリッジ・プロトコル・データ・ユニット（Bridge Protocol Data Unit）です。ルートブリッジに接続しているすべてのネットワークに、構成BPDUを定期的に送出します。
  ＜ポートによる構成BPDUの制御＞
  - 代表ポート
    構成BPDUを定期的に送信します。
  - ルートポート
    構成BPDUを受信しますが、送信しません。
  - ブロッキングポート
    構成BPDUを受信しますが、送信しません。
- STPドメイン
  1台のルートブリッジを頂点として、スパニングツリーが動作しているエリアをSTPドメインと言います。構成BPDUの送受信をポートごとに停止できるブリッジは、構成BPDUの送受信を停止することにより、そのポートを境界にSTPドメインを分離することができます。ドメインを分離する設定にしたポートとSTPドメイン内のポートでのブリッジは正常に中継しますが、ツリー構造は分離されたことになります。

ポートの種類と状態を以下に示します。

	ポート状態	MACフレームの中継	MACアドレスの学習	構成BPDUの送受信	備考
代表ポート	フォワーディング状態	する	する	定期的に送信する	LAN上に1つ存在 ルートブリッジはすべてのポート
ルートポート	フォワーディング状態	する	する	受信する 送信しない	ルートブリッジ以外のブリッジに必ず1つ存在
ブロッキングポート	ブロッキング状態	しない	しない	受信する 送信しない	代表ポート、ルートポート以外のポート
	リスニング状態	しない	しない	受信する 送信する	
	ラーニング状態	しない	する	受信する 送信する	

ルートポート・代表ポート・ブロッキングポートの決定手順

各種ポートの決定手順を以下に示します。



※1）本装置は伝送路タイプではなく、伝送速度でポートのデフォルトコストが決まります。
フレームリレーの場合、ポートのCIR値が伝送速度となります。
AUTO選択時のデフォルトコスト値を以下に示します。

伝送速度	デフォルトコスト値
1M≧速度	1000
1.5M≧速度＞1M	667
4M≧速度＞1.5M	250
6M≧速度＞4M	167
10M≧速度＞6M	100
16M≧速度＞10M	62
20M≧速度＞16M	50
25M≧速度＞20M	40
40M≧速度＞25M	25
80M≧速度＞40M	12
速度＞80M	10

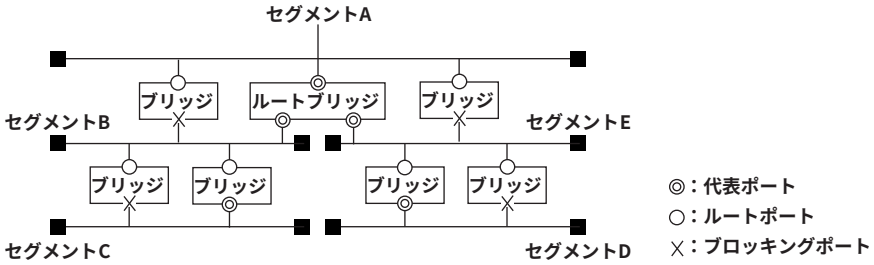
※2）・ルートパスコストは、ルートブリッジからの経路で構成BPDUパケットが入力するポートのパスコストの合計であり、最小値を採用します。
・ルートブリッジのパスコストは0です。

※3）・ルートポートは、各ブリッジごとに1つ存在します。
・ルートパスコストが同じ場合、ポート識別子が小さいポートを採用します。

※4）・代表ポートは、各セグメントごとに1つ存在します。
・最小値となるポートが2ポート以上ある場合、ブリッジプライオリティが小さいブリッジのポートを採用します。

スパニングツリーでのフレームと構成BPDUの流れ

以下のような構成（ポート状態）になるように、各ブリッジのブリッジプライオリティ、パスコストを設定した場合のフレームと構成BPDUの流れについて説明します。

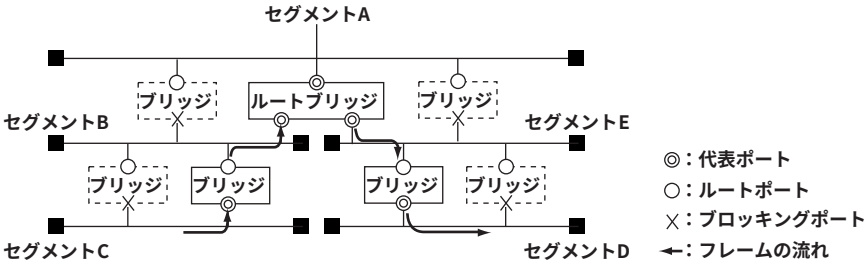


スパニングツリーでのフレームの流れ

ノードから発信したフレームは、そのセグメント上の代表ポートをもつブリッジ（代表ブリッジ）が中継します。フレームを受け取った代表ブリッジは、あて先MACアドレスにより、どのセグメントに中継するかを判断し（MACアドレス学習機能）、該当するセグメントにルートポートを介してフレームを中継します。ブロッキングポートを介してフレームは中継しません。

その先のブリッジでも同様に中継しますが、ルートブリッジがフレームを受け取った場合、代表ポートを介して次のセグメントにフレームを中継します（ルートブリッジのポートはすべてのLANに対して代表ポートです）。そのため、その先でフレームを中継するブリッジはルートポートでデータを受け取り、代表ポートを介して次のセグメントにフレームを中継します。ルートポートをもつブリッジがセグメント上に複数存在する場合、経路をブロッキングポートで1つに制限し、ルートブリッジ方向またはほかの経路に再びフレームは中継しません。

上の図のセグメントCからセグメントDへの通信のフレームの流れを以下の図に示します。セグメント上は、図のような通信経路だけとなり、フレームはループしないであて先に中継します。

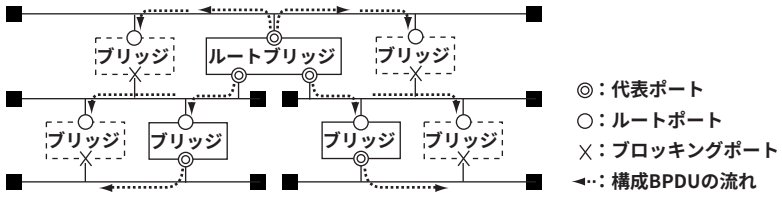


※) [ ] のブリッジは通信経路として使用されません

スパニングツリーでの構成BPDUの流れ

ルートブリッジは、Helloタイム（1～10秒（推奨値2秒））間隔で接続しているすべてのネットワークに構成BPDUを送出します。構成BPDUは、グループMACアドレス800143000000をもっており、それぞれのブリッジはこのグループMACアドレスを認識します。このとき、代表ブリッジはパスコストとタイミング情報を更新し、構成BPDUを下流へ転送します。

構成BPDUはルートブリッジから発信され、ツリー構造に沿ってすべてのネットワークに行き渡ります。スパニングツリー構成は、構成BPDUの代表ブリッジからの定期的な送信により維持されます。



※) [ ] のブリッジは通信経路として使用されません

ツリー構造の再構成

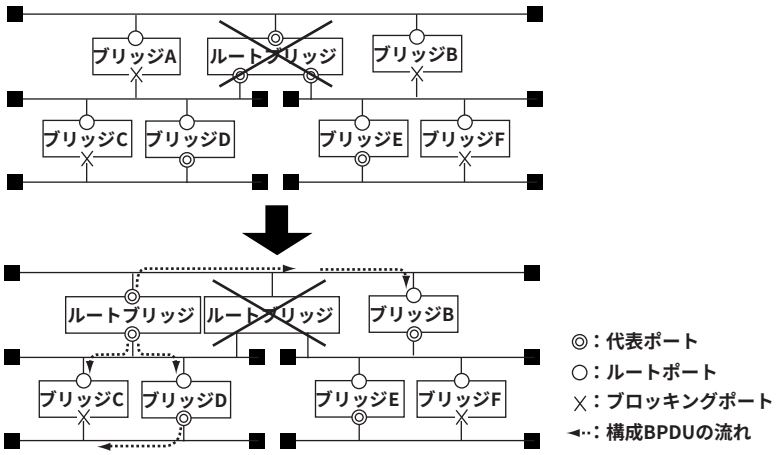
スパニングツリーのツリー構造は、構成BPDUで維持します。以下のような原因により、タイマ値STP bridge Max age（推奨値20秒）以内に、この構成BPDUが下流のブリッジに届かなかった場合、ブリッジは障害と判断し、ツリー構造を再構成します。

- ルートブリッジがダウンし、システム全体で構成BPDUの受信が停止
- ツリー構造の上流に位置するブリッジがダウンし、その下流で構成BPDUの受信が停止

以下の図でルートブリッジがダウンした場合のツリー構造の再構成について説明します。

新ルートブリッジの決定

ルートブリッジがダウンした場合、システム中でルートブリッジの次に小さいブリッジプライオリティをもつブリッジが新ルートブリッジとなります。新ルートブリッジは、接続した各LANに構成BPDUを送信し、それを受け取った各ブリッジにより、ツリー構造を再構成します。以下の図では、ブリッジAが新ルートブリッジに切り替わることを示しています。



ブロッキングポートの中継可能状態への変化

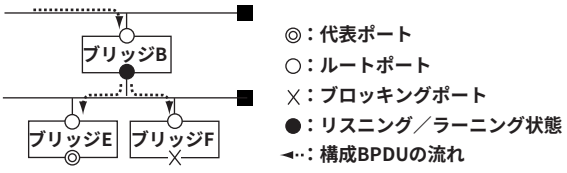
ツリー構造の再構成にともない、ブロッキングしているポートが中継できる状態に変化します。しかし、すべてのブリッジに新しい構成BPDUが届いていない状態で、1部のブリッジのポート状態が変化すると、ループ状態となることがあります。そのため、ポートがブロッキング状態からフォワーディング状態に切り替わる間、中間的なポート状態を置き、すべてのブリッジのツリー構成情報を更新し、ツリー構造が確立するのを待ちます。

ブロッキング状態からフォワーディング状態に切り替わるまで以下の2つの中間状態があります。それぞれの中間状態の待ち時間STP bridge forward delay（推奨値15秒）でポート状態が変化します。

＜中間状態＞

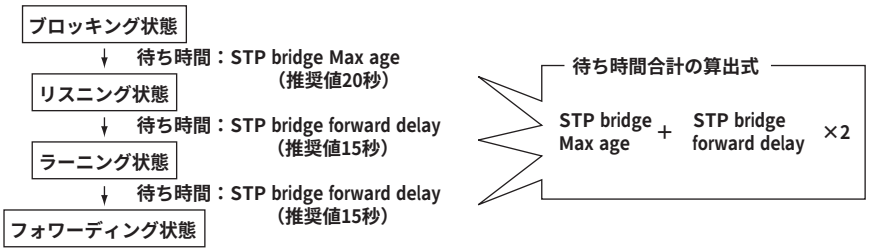
- リスニング状態
  MACフレームを中継しません。また、MACアドレス情報の学習を行いません。構成BPDUを受信します。必要であれば送信します。
- ラーニング状態
  MACフレームを中継しませんが、MACアドレス情報の学習は行います。構成BPDUを受信します。必要であれば送信します。

したがって、以下のブリッジBのブロッキングポートは、フォワーディング状態になる前に、リスニング、ラーニング状態で構成BPDUを下流へ送信します。



ポート状態変化の待ち時間

ポートがブロッキング状態からフォワーディング状態に切り替わる待ち時間の合計は、以下の式により算出できます。待ち時間のパラメタに、推奨値を採用する場合は、約50秒（20＋15×2）でフォワーディング状態に切り替わります。



ツリー構造の確立

ツリー構造の再構成によって、ポート状態が変化したブリッジは、構成変更を通知する構成BPDUを、ルートポートを介して上流ブリッジに送信します。構成変更通知BPDUはツリー構造に沿って上流ブリッジに中継され、最終的にルートブリッジまで中継されます。

構成変更通知BPDUを受信したルートブリッジは、定期的に送信している構成BPDUの中の構成変更フラグをONにして各ブリッジに送信します。構成変更フラグがONとなった構成BPDUを受信したブリッジは、MACアドレス学習テーブルのエントリ（通常は5分でタイムアウト）を早めに削除するために、各エントリのタイムアウト値をSTP bridge forward delay（転送遅延）に変更し、学習テーブルを短時間で更新します。以上の動作でツリー構造は動的に再構成します。

スパニングツリー機能を利用したネットワーク設計

スパニングツリーでのパラメタ

スパニングツリーでは、設計したツリー構成やツリー性能を実現させるために、いくつかのパラメタをブリッジに設定します。このパラメタにより、ツリー構成とツリー性能を決定します。

＜ツリー構成を決定するパラメタ＞

以下のパラメタにより、ツリー構成を決定します。

パラメタ	設定対象	備考
ブリッジプライオリティ（STP bridge priorty）	ブリッジごと	ブリッジごとに設定し、小さい値を設定したブリッジを優先経路として使用します。ルートブリッジとなるブリッジには、システムの中での最小値を設定します。
ポート識別子（STP port identifier）	ポートごと	ルートパスコストとブリッジ識別子の判断がつかない場合は、ポート識別子の小さいポートが代表ポートとなります。ただし、ブリッジ識別子には、MACアドレスが含まれているため、ポート識別子で代表ポートが決定することはほとんどありません。
パスコスト（STP port path cost）	ポートごと	ルートポート（上流ブリッジへの経路）を決めます。パスコストとブリッジプライオリティにより代表ポート（代表ブリッジ）を決めます。ブリッジでポートごとに設定し、小さい値のルートが選択されます。伝送速度の遅いルートは高いコストを設定し、バックアップ用にします。 パスコストは、デフォルト値（1000÷伝送速度Mbps）を用いることをお勧めします。

＜ツリー性能を決定するパラメタ＞

以下のパラメタにより、ツリー性能（障害時のルート変更時間など）を決定します。

パラメタ	設定対象	備考
Hello タイム （STP bridge hello time）	ブリッジごと	ルートブリッジがツリー構成を確認するために発信する構成 BPDU の送出間隔です。 推奨値は 2 秒です。
最大寿命 （STP bridge Max age）	ブリッジごと	構成 BPDU が届かなくなったためにツリーの再構成を始めるタイマ値です。 ツリー構成の末端のブリッジに届くまでの遅延時間により異なりますが、推奨値は 20 秒です。 同じタイミングで再構成するために、同じネットワーク内のブリッジは同じパラメタで設定します。
転送遅延 （STP bridge forward delay）	ブリッジごと	ブロッキング状態からフォワーディング状態に切り替わるまでの中間状態での待ち時間です。 この時間が短い場合、リスニング状態でツリー構成全体の同期がとれなくなります。ラーニング状態では、MAC アドレス学習テーブルの学習が不十分なために、すべてのポートに中継してしまう場合やループ状態になる場合があります。また、時間が長い場合は、ツリーの再構成に必要とする時間が長くなります。 推奨値は 15 秒です。

＜その他のパラメタ＞

パラメタ	設定対象	備考
STP ドメインの分離 （STP domainSeparation）	ポートごと	ブリッジの各ポートに、STP ドメインを分離するかどうかを設定します。 STP ドメインを分離すると、そのポートから構成 BPDU の送信を停止し、そのポートを境界にツリー構成は分離されます。ただし、構成 BPDU 以外のフレームは中継します。 本装置では、WAN 側は STP ドメインを分離し、LAN 側は STP ドメインを分離しません。ON：分離する、OFF：分離しない、で設定します。

スパニングツリーでのネットワーク設計のポイント

スパニングツリー機能を使用して、ツリー構成を設計するポイントを以下に説明します。

＜ルートブリッジの決定のポイント＞

まず、ルートブリッジを決め、システム内で最小のブリッジプライオリティを設定します。ルートブリッジはツリー構造の頂点に位置し、トラフィックが集中する傾向にあるため、ルートブリッジを決める場合は以下の点に注意してください。

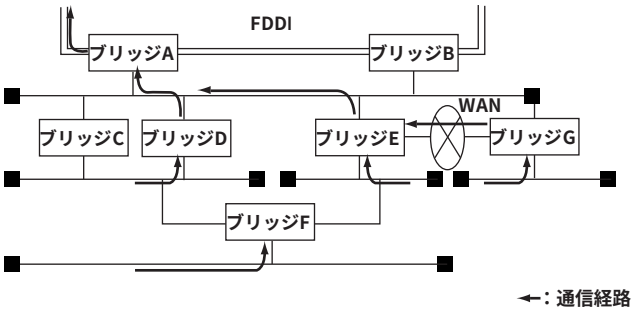
- 各セグメントのトラフィックが均一になるようにバックボーン（FDDI など）に近いブリッジをルートブリッジとします。
- むだなトラフィックがルートブリッジを経由しないようにエンドノートの配置に注意します。たとえば、常に通信しているような端末や大量のトラフィックを通信する端末はルートブリッジを経由しないように配置します。

＜ルートブリッジの障害時の対応＞

障害が起き、ルートブリッジがダウンすると、ツリーは新ルートブリッジで再構成します。ただし、新ルートブリッジの位置により、ツリー構成がすべて変わる場合があります。そのため、ルートブリッジの障害を想定し、ツリー構成の変更が小さい新ルートブリッジを決め、システム中で 2 番目に小さいブリッジプライオリティを設定します。

スパニングツリーでのツリー構成の設計

スパニングツリー機能を使用するツリー構成の設計について、以下の構成例を用いて説明します。



＜ツリー構成範囲の決め方＞

ブリッジの中でツリー構成（スパニングツリー動作範囲）に組み込むブリッジを決めます。まず、ブリッジEからWANの先に位置するブリッジGは、ツリー構成に含む必要もなく、WAN回線上に余計なトラフィック（構成BPDU）を流さないために、ブリッジEのWAN側のポートでSTPドメインを切り離します。なお、FDDIの先にはツリー構成に入るブリッジが存在しないため、ブリッジA、ブリッジBのFDDIポートもSTPドメインを切り離します。

＜ルートブリッジの決定（ブリッジプライオリティの設定）＞

ツリー構成を設計する場合は、まずルートブリッジを決める必要があります。上の図のネットワーク構成では、ブリッジAとブリッジBがバックボーンとなるFDDIに接続しており、ブリッジAをルートブリッジに、ブリッジBをルートブリッジ障害時の新ルートブリッジになるように設計します。よって、ブリッジAに1番小さなブリッジプライオリティを、ブリッジBに2番目に小さいブリッジプライオリティを設定します。

その他のブリッジは実現する通信経路を考慮し、ルートブリッジに近い上流ブリッジより、小さな値を設定します。

＜ポートの設計（パスコストの設定）＞

各ブリッジのポートごとにパスコストを設定し、ブリッジのポート状態を設計します。ルートパスコストがポート状態を確立します。ルートパスコストは以下の計算により算出できます。

＜ルートパスコストの算出＞

各ブリッジのポートごとに「代表コスト＋パスコスト」を算出し、各ブリッジ中で最小の値をそのブリッジのルートパスコストとします。

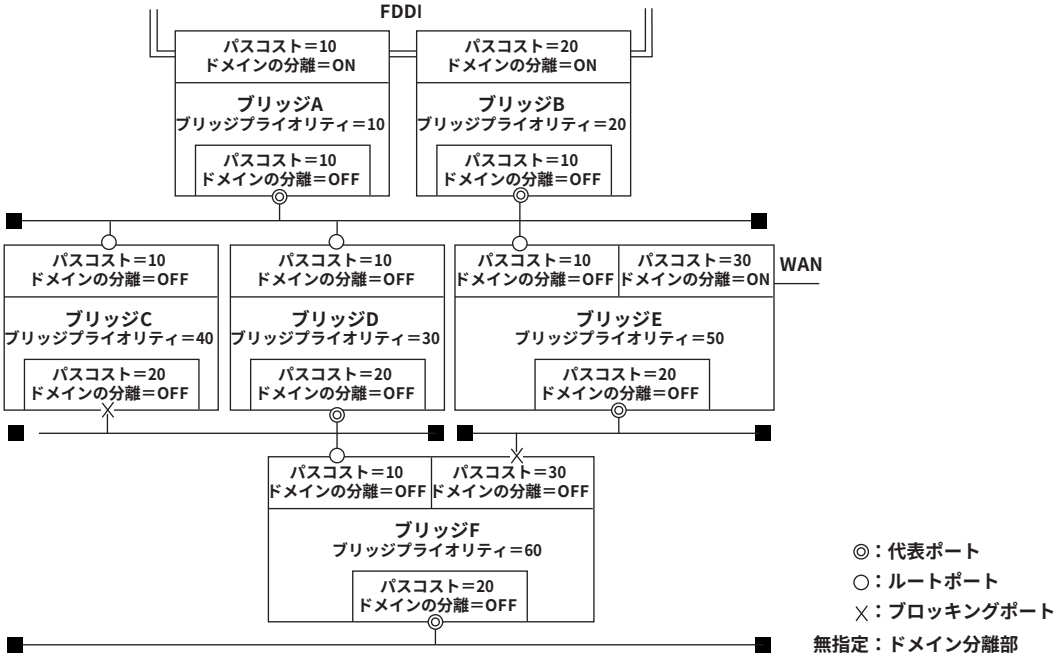
- 代表コスト
  そのポートが接続しているLAN上の代表ブリッジのルートパスコストです。構成BPDUの受信により、各ポートに自動的に設定されます。

設計上でルートパスコストを意識することは困難です。そのため、設計段階ではルートパスコストを使用せず、ブリッジプライオリティとパスコストでポート状態を設計します。たとえば、LAN上に2台のブリッジが存在した場合、経路とするブリッジの方を他方のブリッジよりブリッジプライオリティを低く設定します。ブリッジの中で経路となるポートには、そのブリッジの中で低いパスコストを設定します。

＜各ブリッジの設定状態＞

以下に、実際にブリッジに設定した各パラメタの値を示します。

ブリッジFの左ポートのパスコストが10＋10＝20、右ポートのパスコストが10＋30＝40により、ブリッジFの左ポートがルートポートとなります。



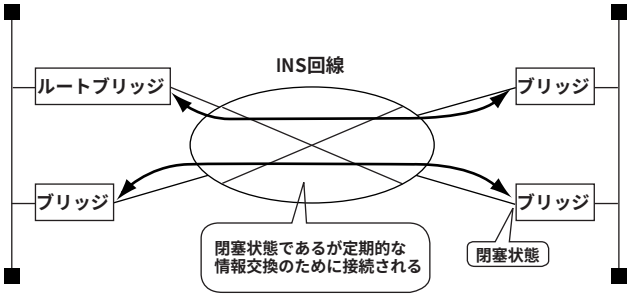
こんな事に気をつけて

- 本装置では、ファームウェアの更新やSNMPでの監視などの目的でIPv4のIPアドレスを使用します。そのため、IPv4のIPアドレスを設定しないで運用することはできません。IPv6およびブリッジだけを使用しているネットワークで運用する場合でも、どれかのLANインタフェースに必ずIPv4のIPアドレスを設定してください。
- ブリッジ学習テーブル生存時間は、グループ0に設定した値がすべてのグループで使用されます。
- VLANでバインドされたインタフェースでブリッジを行うことはできません。
- VLANインタフェースをブリッジグループに含める場合は、1つまたは複数のリモートインタフェースとVLANインタフェースでだけグルーピングできます。
- 本装置のブリッジMAC学習は、異なるVLAN上で同一のMACアドレスを学習することはできません。本装置は、唯一装置がもつ学習テーブルを各VLANが共有するSVL（Shared VLAN Learning）と呼ばれる方式で学習を行っています。VLANインタフェースでブリッジを行う場合は、異なるVLAN上に同一のMACアドレスを持つネットワークと接続しないでください。
- IPフレームをブリッジする場合、そのブリッジグループに属するインタフェース上では、以下の機能を利用することができます。それ以外の機能は、IPフレームをブリッジするインタフェース上では利用できません。また、複数のLANインタフェースを同じグループに含めてIPブリッジをする場合は、同じグループ内で定義番号がもっとも小さいLANインタフェースでだけ以下の機能を利用できます。
  - FTP（ファームアップデートなど）
  - telnet
  - Webブラウザによる設定
  - syslogの送信
  - SNMPエージェント、Trap送信
  - ダイナミックルーティング

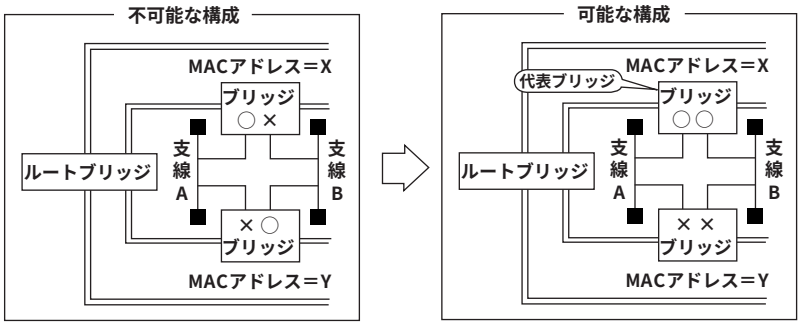
  IPフレームをブリッジする場合に、転送ポリシをlooseに設定したときだけ、ブリッジグループ外とルーティングが行われます。また、ブリッジドメイン内は唯一のIPセグメントであることに注意してダイナミックルーティングを使用してください。

スパニングツリー機能を使用する場合は、以下の点に注意してください。

- スパニングツリー機能は、グループ0でだけ動作します。
- VLANインタフェースでは、STPを使用できません。
- 従量課金回線を使用時の留意点
  LAN-WAN-LANの接続形態でスパニングツリー機能を使用する場合は、LANの接続形態と同様にブリッジ間で構成BPDUを定期的に送受信します。そのため、通常回線にINS回線などの従量課金回線を使用する場合、構成BPDUの送信により発呼したり、回線がつながったままになる場合があります。



- 複数支線の構成時の留意点
  以下のように2台のブリッジ間に複数の支線が接続する構成の場合は、支線ごとに中継するブリッジを選択することはできません。
  代表ポート（各支線に中継するポート）は、以下の順序で決めます。
  (1)ルートパスコストの低いブリッジ
  (2)ブリッジ識別子（ブリッジプライオリティ＋MACアドレス）
  　ただし、複数のMACアドレスをもつ場合は装置の代表MACアドレスを使用します。
  (3)ポート識別子（ポートプライオリティ＋ポート番号）
  したがって、以下のように2台のブリッジ間に複数の支線が接続する構成の場合は、2台のブリッジに同じブリッジプライオリティ／パスコストを設定できます。しかし、同じMACアドレスは使用できないため、同じブリッジ識別子は設定できません。どちらかが代表ブリッジになり、すべての支線を中継します。

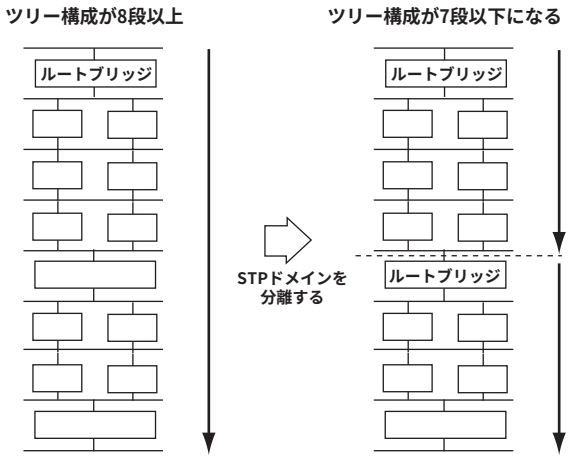


- **国際標準からのツリー構成**
  国際標準では、ツリー構成の段数は最大7段をお勧めしています。これは、各性能に関するパラメタを推奨値（デフォルト値）で運用した場合にシステムがどのような条件で運用しても、スパニングツリー機能が正常に動作することを保証できる値です。
  推奨値の最大7段は、以下の式より算出できます。

  ```
  最大寿命÷（Helloタイム＋構成メッセージの最大遅延時間）＋1
  ＝20÷（2＋1）＋1
  ≒7
  ```

  ツリー構成の段数が7段を超える場合は、以下の2つの対応方法があります。
  - 構成するすべてブリッジの最大寿命を長くします。
  - STPドメインを分離します。

  前者は変更規模が大きくなり構成を変更する時間が長くなるため、後者での対応をお勧めします。



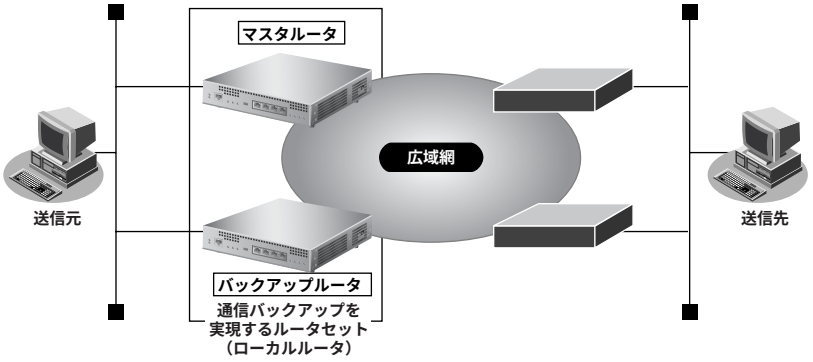
参照　MR1000　コマンド設定事例集「2.32 ブリッジ／STP機能を使う」（P.260）
MR1000　Web設定事例集「2.32 ブリッジ／STP機能を使う」（P.597）

2.26　通信バックアップ機能

通信バックアップ機能とは、通信障害が発生した通信パスを検出した場合に、迂回通信パスを利用することで、エンドツーエンドの通信を維持する機能です。通信バックアップ機能は、以下の2つの機能の組み合わせで実現されます。

- 通信障害の検出機能
- 検出された通信障害に対する通信パス迂回機能

ここでは、以下の図のネットワーク例に基づいて説明します。



こんな事に気をつけて

ここでは片方向通信について説明していますが、一般的なクライアントーサーバモデルの通信は、「クライアントからサーバへの通信（主に要求）と「サーバからクライアントへの通信（主に応答）」が成立して初めて成立します。このため、実際に利用する場合は、本書を参考にして、双方向の通信が成立するようにネットワーク設計を行ってください。

2.26.1　通信障害の検出機能

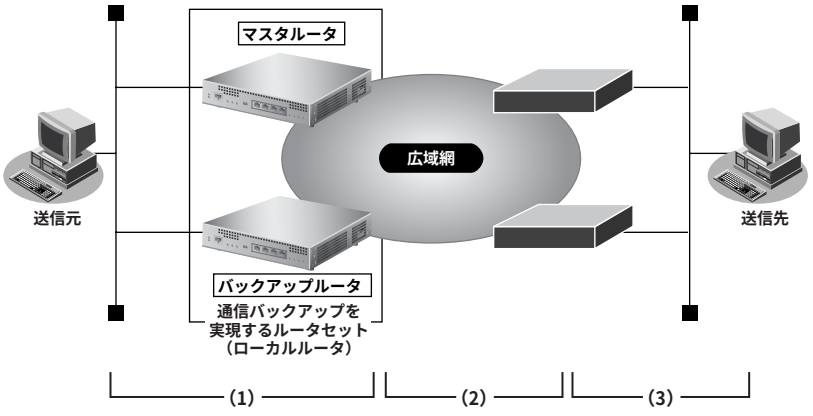
通信障害はさまざまな要因で発生します。その要因は、主に、以下の3つに分類することができます。

（1）　送信元とローカルルータとの間の到達性喪失を要因とする通信障害

（2）　ローカルルータと隣接ルータとの間の到達性喪失を要因とする通信障害

（3）　隣接ルータと送信先との間の到達性喪失を要因とする通信障害

それぞれ障害が発生する箇所について、以下に示します。



ここでは、それぞれの要因ごとに、本装置の障害検出機能について説明します。

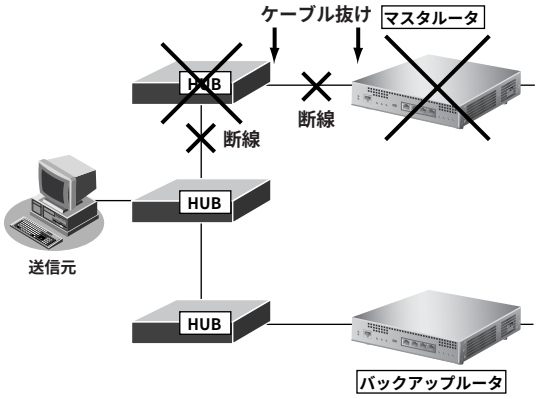
（1） 送信元とローカルルータとの間の通信障害

送信元とローカルルータとの間の通信障害には、以下の要因が考えられます。

- マスタルータとローカルネットワークとの間の障害（ケーブル断線、ケーブル抜け、HUB の故障など）
- マスタルータの故障

これらの障害に対する本装置の検出方法と障害検出可能な箇所は、以下のとおりです。

- VRRP 機能を利用した障害検出（IPv4）
- ダイナミックルーティング機能を利用した障害検出



以下に、それぞれの検出方法について説明します。

VRRP 機能を利用した障害検出（IPv4）

本装置では、VRRP（Virtual Router Redumdancy Protocol）をサポートしています。この障害検出方法は、送信元でダイナミックルーティングプロトコルが利用できない（しない）場合に利用します。

マスタルータとバックアップルータ間で VRRP を利用する場合、ローカルネットワーク上では 1 台のルータ（仮想ルータ）だけ動作しているように見えます。そのため、マスタルータが故障した場合も、Ethernet 上のほかのノードはその故障を検出する必要はありません。

マスタルータは、定期的にバックアップルータに VRRP-AD パケットを送信します。バックアップルータは、VRRP-AD パケットを一定時間受信できなかった場合に、VRRP でマスタルータの障害を検出します。障害復旧は、バックアップルータが VRRP-AD パケットを受信することによって検出されます。

ダイナミックルーティング機能を利用した障害検出

本装置では、いくつかのダイナミックルーティングプロトコルをサポートしています。この障害検出方法は、送信元でダイナミックルーティングプロトコルを使用する場合に利用します。

どのダイナミックルーティングプロトコルも、定期的に制御データが送信されています。制御データを一定時間受信できなかった場合に、バックアップルータは経路喪失としてマスタルータの障害を検出します。障害復旧は、バックアップルータが制御データを受信することによって検出されます。

（2） ローカルルータと隣接ルータとの間の通信障害

ローカルルータと隣接ルータとの間の通信障害には、以下の要因が考えられます。

- ローカルルータと隣接ルータとの間の障害（ケーブル断線、ケーブル抜け、広域網障害など）
- 隣接ルータの故障

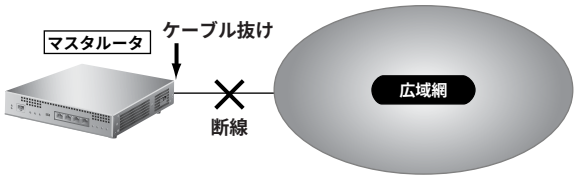
これらの障害に対する本装置の検出方法と障害検出可能な箇所は、以下のとおりです。

- ハードウェアによる障害検出
- データリンクプロトコルを利用した障害検出
- 接続先監視機能を利用した障害検出
- ダイナミックルーティング機能を利用した障害検出

以下に、それぞれの検出方法について説明します。

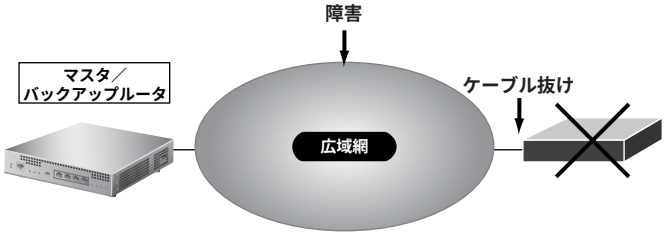
ハードウェアによる障害検出

この障害検出は、物理回線を直接利用して隣接ルータと通信する場合に利用できます。IPsecおよびIPトンネルでは利用できません。この方法で検出された障害は、物理回線を直接利用して通信できない障害と判断されます。



データリンクプロトコルを利用した障害検出

この障害検出方法は、ローカルルータと隣接ルータとの間で以下の接続先種別を利用している場合に利用できます。この方法で検出された障害は、この接続先が利用できないと判断されます。



- フレームリレーを利用する場合
  PVC状態確認手順（ITU-T Q.933 Annex A）を利用した場合、本装置および相手装置は周期的にリンク状態を問い合わせるメッセージを送出します。それに対して網からリンクの状態を表示するメッセージを受信します。本装置では10秒ごとに「状態問い合わせ」メッセージを送信します。最新の4回の「状態問い合わせ」メッセージの送信に対して、「状態表示」メッセージの未受信または無効メッセージ受信のエラーを3回以上検出した場合に、本装置と網間の通信障害が検出されます。検出復旧は、3回連続して正しい「状態表示」メッセージを受信することによって検出されます。
  また、6回の「状態問い合わせ」メッセージを送出するごとに完全な状態表示を要求することになり、本装置と相手装置間のPVC状態を把握することができます。
- ISDNを利用する場合（常時接続機能利用時のみ）
  ISDNで常時接続機能を利用した場合は、回線切断の発生が通信障害として検出されます。また、障害復旧は回線接続によって検出されます。

- PPPoEを利用する場合（常時接続機能利用時のみ）
  PPPoEで常時接続機能を利用した場合は、PPPoEセッション切断の発生が通信障害として検出されます。また、障害復旧はPPPoEセッション接続によって検出されます。

接続先監視機能を利用した障害検出

本装置は、確認先装置に対して定期的にICMP echo requestを送信して、その応答を受信することによって到達性を確認するL3監視機能をサポートしています。

以下の機能で、通信バックアップのための通信障害を検出することができます。

- VRRPノードダウントリガ機能（IPv4）
  VRRPノードダウントリガ機能は、IPv4通信が利用できる任意の接続先種別で利用できます。この方法で検出された障害は、VRRP機能の中で判断されます。また、障害復旧はICMP echo replyの受信によって検出します。
- 接続先監視機能
  接続先監視機能は、以下の接続先種別でIPv4通信が可能な場合に利用できます。この方法で検出された障害は、この接続先が利用できないものとして判断されます。また、障害復旧は、ICMP echo replyの受信によって検出されます。
  - 専用線
  - フレームリレー
  - ISDN（常時接続機能利用時のみ）
  - PPPoE（常時接続機能利用時のみ）
  - IPトンネル
  - IPsec
  - overlap

こんな事に気をつけて

装置起動や設定反映によって本装置が動作を開始した直後は、障害が発生していなくてもL3監視機能が障害と検出する場合があります。これは、監視タイムアウトが発生するまでに周辺ネットワークが通信可能状態まで達することができない場合に発生します。これは、監視タイムアウト時間を十分に長くすることにより回避することができます。

ダイナミックルーティングを利用した障害検出

「送信元とローカルルータとの間の通信障害」（P.107）の方法と同様です。

（3） 隣接ルータと送信先との間の通信障害

隣接ルータと送信先との間の通信障害には、以下の要因が考えられます。

- 隣接ルータから送信先までの経路制御障害

この障害に対する本装置の検出方法は、以下のとおりです。

- 接続先監視機能を利用した障害検出
- ダイナミックルーティング機能を利用した障害検出

以下に、それぞれの検出方法について説明します。

接続先監視機能を利用した障害検出

「ローカルルータと隣接ルータとの間の通信障害」（P.108）の方法と同様です。

監視先を送信先に設定することによって、隣接ルータの先の通信障害まで検出できます。

こんな事に気をつけて

L3監視機能を利用して双方向通信の相互監視を行う場合は、互いに隣接ルータを監視するように設定してください。隣接ルータより先の装置を監視した場合、ICMP echo replyは、迂回経路を利用して監視元に転送されます。迂回経路でも通信障害が発生した場合、障害が復旧してもICMP echo replyが監視元に到達できなくなるため、復旧検出が行うことができなくなります。

ダイナミックルーティングを利用した障害検出

ダイナミックルーティングを利用した場合、隣接ルータからの経路喪失の通知によって検出されます。障害復旧は、隣接ルータからの経路通知により検出されます。

接続先閉塞機能

本装置は定義された接続先ごとに通信障害を検出する機能をサポートしています。障害の復旧検出も自動で行うことができます。ここで、障害要因によって、障害検出と復旧検出が頻繁に連続して発生することで安定した通信が保てなくなる場合もあります。これに対し、本装置は意図的に通信不能状態を継続させる接続先閉塞機能で対応しています。

接続先閉塞機能を利用した場合、その接続先はconnectコマンド発行によるオペレータ指示があるまで通信不能状態のまま保持されます。これにより、間欠障害発生時にも安定した通信を保つことができます。

閉塞状態への遷移は、disconnectコマンド発行による手動閉塞と、通信障害検出時による自動閉塞を行うことができます。自動閉塞の有無はremote ap recovery定義で決定されます。

2.26.2　検出された通信障害に対する通信パス迂回機能

通信障害の検出方法によって、本装置での通信パス迂回機能による利用方法が異なります。
ここでは、それぞれの検出方法による利用方法と本装置での通信パス迂回機能について説明します。

検出された通信障害の利用

「2.26.1 通信障害の検出機能」（P.106）によって検出された通信障害は、以下のように利用されます。

- VRRP 機能を利用した障害検出
  VRRP 機能で、マスタルータ切り替え要因として利用されます。
- ダイナミックルーティング機能を利用した障害検出
  経路制御機能で、経路切り替え要因として利用されます。
- ハードウェアによる障害検出
  Ethernet回線で、lan インタフェースのダウン要因として利用されます。
  BRI 回線と PRI 回線では、その回線を利用する接続先の利用不能状態への遷移要因として利用されます。相手定義内のすべての接続先が利用不能状態となる場合は、該当するrmt インタフェースのダウン要因として利用されます。
- データリンクプロトコルを利用した障害検出
  接続先の利用不能状態への遷移要因として利用されます。相手定義内のすべての接続先が利用不能状態となる場合は、該当するrmt インタフェースのダウン要因として利用されます。
- 接続先監視機能を利用した障害検出
  接続先の利用不能状態への遷移要因として利用されます。相手定義内のすべての接続先が利用不能状態となる場合は、該当するrmt インタフェースのダウン要因として利用されます。

通信パス迂回機能

本装置の通信パス迂回機能は、以下のとおりです。

- VRRP 機能を利用した迂回機能
- 経路制御機能を利用した迂回機能
- マルチルーティング機能を利用した迂回機能
- LAN ポートバックアップ機能を利用した迂回機能

以下に、それぞれの通信パス迂回機能の詳細を説明します。

VRRP 機能を利用した迂回機能

VRRP機能を利用した場合、VRRPルータは、自身より優先度の高い装置が存在すると判断されているときは、仮想ルータの MAC アドレスあてに送信されたパケットを受信しません。LAN 内のもっとも優先度が高いVRRPルータ（マスタルータ）がパケットを受信し、転送します。ほかの VRRP ルータ（バックアップルータ）は転送しません。

マスタルータは、障害検出を契機に自身の優先度の変更を LAN 上に広報します。マスタルータが優先度を下げる契機として、以下の契機があります。

- インタフェースダウントリガ
  インタフェースダウントリガは、インタフェースのダウンを契機として利用します。この機能は lan vrrp group trigger ifdown 定義によって設定されます。
- ルートダウントリガ
  ルートダウントリガは、設定された経路が装置から喪失したことを契機として利用します。この機能は lan vrrp group trigger route 定義によって設定されます。

- ノードダウントリガ
  ノードダウントリガは、VRRP ノードダウントリガ機能を利用して監視先装置への到達性がなくなったことを契機として利用します。この機能はlan vrrp group trigger node 定義によって設定されます。

バックアップルータは、VRRP-AD パケットによってマスタルータ喪失の検出またはマスタルータの優先度変更通知によって、自身が新しくマスタルータになるべきかを判断します。その結果、自身がマスタルータとなった場合、仮想ルータ MAC アドレスあてパケットを受信し、転送します。これによって、通信パスが迂回されます。

経路制御機能を利用した迂回機能

本装置は、受信したパケットをどのインタフェースから転送するかを、自身が持つ経路情報によって判断します。経路制御機能を利用することにより、障害検出時に経路情報を迂回経路側に変更し、通信パスが迂回されます。また、ダイナミックルーティング機能を利用している場合は、経路情報の変更をダイナミックルーティングプロトコルを利用して隣接ルータに通知することによって、本装置に到達する前に、迂回するように指示することもできます。これら経路制御機能は、利用するプロトコルによって異なります。

IPv4 を利用する場合

ダイナミックルーティング機能を利用して障害検出された場合、まず、そのダイナミックルーティングプロトコルの範囲で経路変更が行われます。RIPv1/RIPv2、OSPF およびBGP4 の場合、代替経路を学習しているときは、代替経路に変更されます。代替経路がないときは、削除されます。

インタフェースダウンによって障害検出された場合は、以下の動作となります。

- スタティックルート（distanceが1以上に設定されたもの）
  経路情報が削除されます。
- ダイナミックルーティングによって学習された経路
  ダウンしたインタフェースを利用する経路に対して、ダイナミックルーティングを利用した障害検出時の処理と同じです。

これらの処理を行ったあと、スタティックルートおよびそれぞれのダイナミックルーティングの中で最適な経路が選択され、最終的な新経路が決定されます。また、ダイナミックルーティング機能を利用している場合は、最終的な新経路の決定結果を隣接ルータに対して通知します。異なるダイナミックルーティングプロトコル間の経路通知は、routemanage ip redist定義によって決定されます。

こんな事に気をつけて

本装置の初期設定では、インタフェースに設定したアドレスに付随する経路（connected route）は、インタフェースダウンが起きても経路情報から削除されません。そのため、自身から直接到達できる装置に対する通信データが本装置まで到達してしまった場合は迂回させることができません。このような場合、インタフェース経路のフローティング機能（routemanage interface floating 定義）を使用することで、インタフェースダウンが起きても、経路情報から削除することができます。

IPv6 を利用する場合

IPv6 RIP を利用して障害検出された場合、代替経路を学習しているときは、代替経路に変更されます。代替経路がないときは、削除されます。

インタフェースダウンによって障害検出された場合は、以下の動作となります。

- スタティックルート（distanceが1以上に設定されたもの）
  経路情報が削除されます。
- IPv6 RIP によって学習された経路
  ダウンしたインタフェースを利用する経路に対して、ダイナミックルーティングを利用した障害検出時の処理と同じです。

マルチルーティング機能を利用した迂回機能

本装置には、相手情報定義（remote）の配下に複数の接続先定義（ap）を定義した場合、どの接続先を利用して送信データを転送するかを選択するマルチルーティング機能があります。相手情報定義は経路制御機能によって選択されますが、マルチルーティング機能はここで選択された相手情報の配下のどの接続先を利用するかを選択するため、経路情報を変更しないで通信パスを迂回させることができます。

マルチルーティングは、もっとも優先度が高く、通信可能状態となっている接続先に対して通信データを送信します。優先度の高い接続先が利用できないと判断されている場合は、利用できる別の接続先を利用して送信することによって、通信パスが迂回されます。

こんな事に気をつけて

マルチルーティング機能を利用する際に、rmtインタフェースのLinkUp trapおよびLinkDown trapは、以下の場合に送出されます。

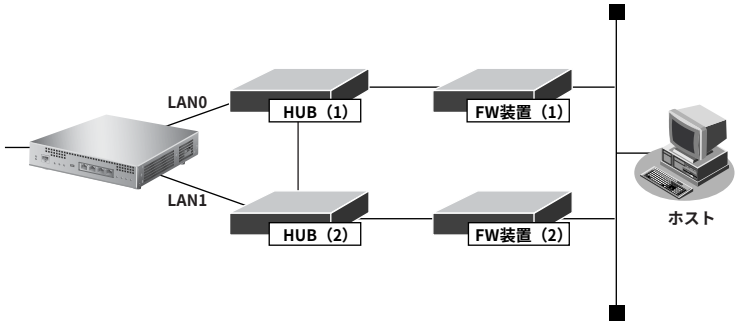
- **LinkUp trapは、rmtインタフェースに対応する相手情報定義（remote）の配下の接続先定義（ap）がすべて利用できない状態から、1つでも利用できる状態になった場合に送出されます。**
- **LinkDown trapは、rmtインタフェースに対応する相手情報定義（remote）の配下の接続先定義（ap）がすべて利用できない状態になった場合に送出されます。**

それぞれの接続先の状態の変化では、rmtインタフェースのLinkUp trapおよびLinkDown trapは送出されません。

LAN ポートバックアップ機能を利用した迂回機能

LANポートバックアップ機能を利用した場合、同じセグメントに対して2つのLANポートを接続できます。これによって、一方のLANポートで障害が発生したときも、他方の障害の発生していないLANポートを利用して通信を継続することができます。

以下に、LANポートバックアップ機能を利用する場合の構成例を示します。



● 運用前提

- 本装置は、LAN0を通信ポート、LAN1をバックアップポートとして定義されている
- FW装置（1）とFW装置（2）は、お互いをバックアップする構成となっている（HUBとFW装置との間の通信障害を検出し、系切り替えを行うことができる）

● 通信動作

通常状態

本装置は、LAN0を通信ポート、LAN1をバックアップポートで定義され、LAN0を利用して通信しています。この状態の通信経路を、以下に示します。

本装置［LAN0］←→HUB（1）←→FW装置（1）←→ホスト

「通常状態」の［LAN0］でケーブル抜け、断線などが発生した場合

本装置は、LAN0ポートの通信障害を検出し、通信ポートをLAN1に切り替えます。この場合、FW装置は障害に気付くことはありません。この状態の通信経路を、以下に示します。

本装置［LAN1］←→HUB（2）←→HUB（1）←→FW装置（1）←→ホスト

「通常状態」のHUB（1）の故障が発生した場合

本装置は、LAN0ポートでの通信障害を検出し、通信ポートをLAN1に切り替えます。この場合、FW装置（1）も障害を検出し、FW装置（2）を経由した通信に切り替わったことを前提とします。この状態の通信経路を、以下に示します。

本装置［LAN1］←→HUB（2）←→FW装置（2）←→ホスト

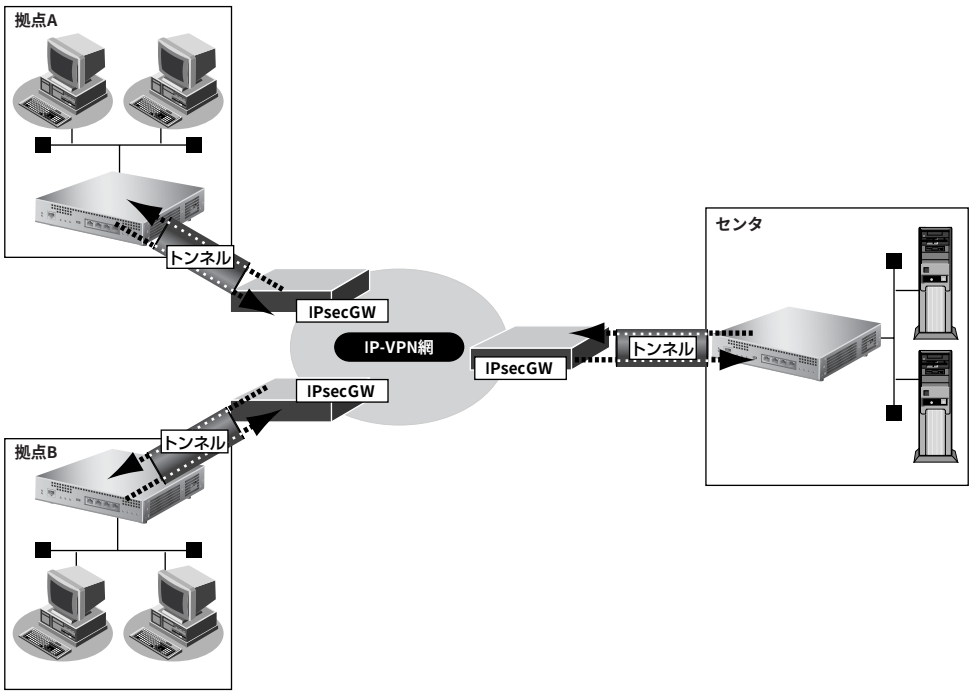
こんな事に気をつけて

- **LANポートバックアップ機能を利用する際に、lanインタフェースのLinkUp trapおよびLinkDown trapは、以下の場合に送出されます。**
  - **LinkUp trapは、両LANポートが利用できない態から、どちらか一方が利用できる状態になった場合に送出されます。**
  - **LinkDown trapは、両LANポートが利用できない状態になった場合に送出されます。**

  それぞれのLANポートの状態の変化では、lanインタフェースのLinkUp trapおよびLinkDown trapは送出されません。
- **バックアップポートでの通信中に通信ポートが復旧した場合、バックアップポートがポート切り替えのために一時的に停止状態になります。このため、バックアップポート側ではキャリア喪失のsyslogが出力されますが、これは異常ではありません。**

2.26.3　ISDN接続を契機とした通信バックアップ

これまで説明した方法の通信バックアップ機能は、通信する装置どうしで障害を検出できることが前提となります。しかし、ネットワーク形態によっては、一方の装置で通信障害を検出できない場合もあります。以下のネットワーク構成は、通信障害を検出できない場合の例です。

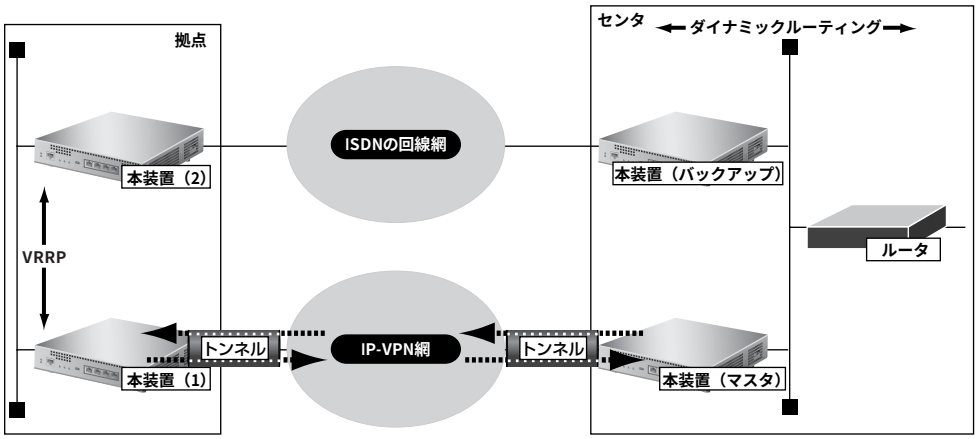


この構成では、拠点側本装置は接続先監視機能などを利用してIPsec区間およびIP-VPN網の障害検出を行うことができます。しかし、センタ側IPsec区間はすべての拠点からの通信で共用することになり、センタ側本装置は拠点ごとの個別の障害検出を行うことができません。このため、センタ側は、これまでに説明した方法ではバックアップ経路への迂回を行うことができません。

本装置では、以下の機能を利用することによって、バックアップ経路となるISDN回線の接続を契機とした経路切り替えを行い、このような場合の通信バックアップを実現することができます。

- 無通信監視の方向性機能（拠点側本装置で利用）
- 着信時経路UP機能（センタ側本装置で利用）

ここでは、無通信監視の方向性機能と着信時経路UP機能を利用した通信バックアップについて説明します。
以下にネットワーク構成の例を示します。



● 運用前提

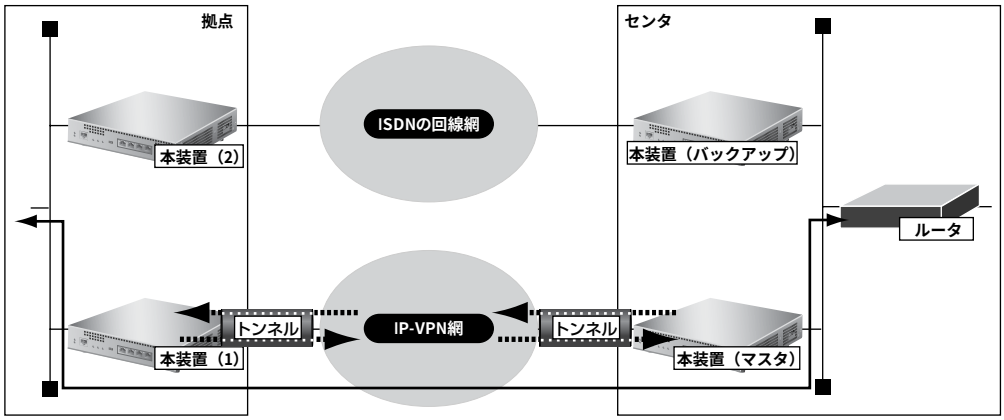
- 本装置（バックアップ）は、着信時経路UP機能を利用して、バックアップ回線となるISDN接続時だけセンタ側ネットワークに経路情報を広報するように構成する
- 本装置（2）は送出パケットだけに着目した無通信監視の方向性機能を利用する

● 通信動作

通常運用時

拠点側　：本装置（1）がマスタルータとなり、センタへのパケットは本装置（1）から送信されます。

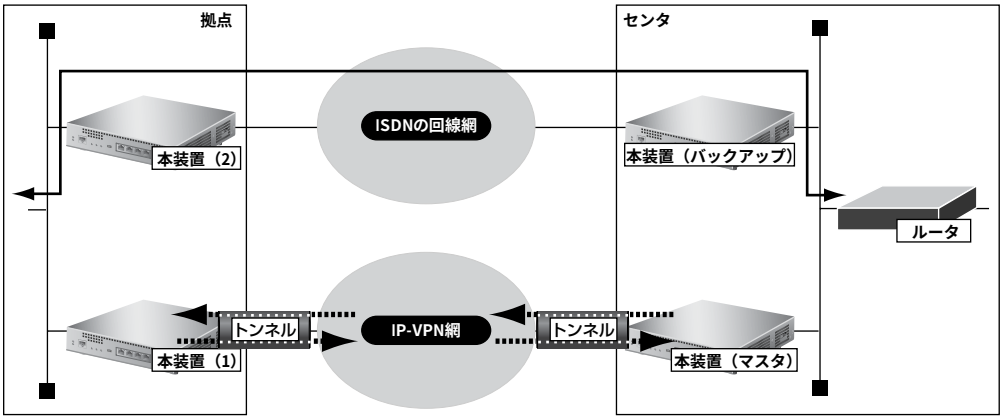
センタ側：本装置（マスタ）は拠点への経路を広報していますが、本装置（バックアップ）は経路を広報しません。その結果、拠点への通信は本装置（マスタ）から送信されます。



IP-VPN網障害発生時

拠点側　：本装置（2）がマスタルータとなります。センタへのパケットは本装置（2）から送信され、ISDN回線が接続されます。

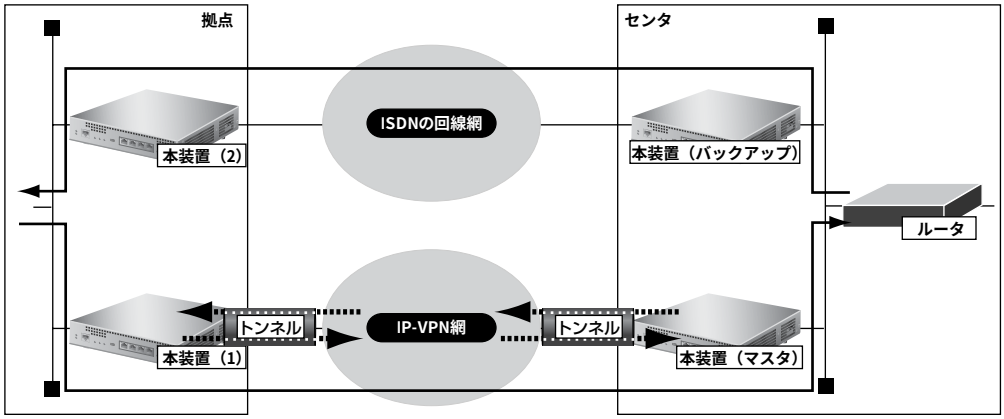
センタ側：本装置（バックアップ）はISDN回線の接続によって拠点への経路広報を開始します。この広報情報の優先度（メトリックなど）を、本装置（マスタ）の広報情報より高くすることで、拠点への通信は本装置（バックアップ）から送信されます。



（3）IP-VPN網復旧時

拠点側　：本装置（1）がマスタルータに戻り、センタへのパケットは本装置（1）から送信されます。

センタ側：ISDN回線が接続されている間、拠点への通信は本装置（バックアップ）から送信されます。



ISDN回線切断前は、本装置（2）はセンタからの受信だけを受け持つことになります。しかし、無通信監視の方向性機能を利用して送信だけを監視することによって、設定した時間になると回線が自動的に切断されます。

ISDN回線切断後は、「通常運用時」の状態に戻ります。

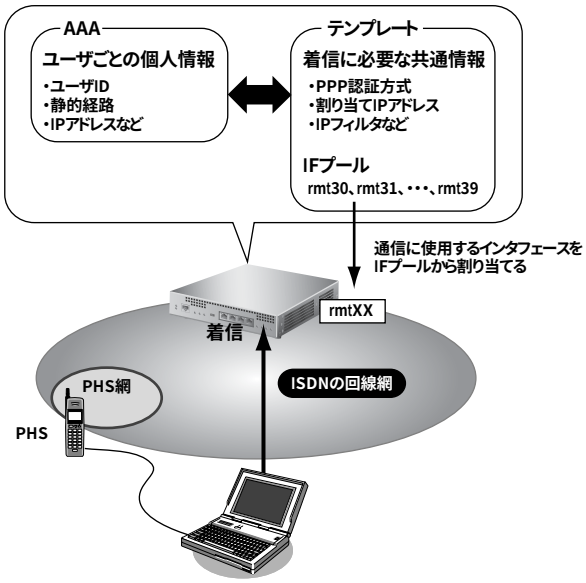
参照　MR1000　コマンド設定事例集
「1.13 NATと併用しない固定IPアドレスでのVPN（自動鍵交換）」（P.41）、
「1.14 NATと併用した固定IPアドレスでのVPN（自動鍵交換）」（P.47）、「2.26 ECMP機能を使う」（P.239）
MR1000　Web設定事例集
「1.13 NATを併用しない固定IPアドレスでのVPN（自動鍵交換）」（P.127）、
「1.14 NATと併用した固定IPアドレスでのVPN（自動鍵交換）」（P.138）、「2.26 ECMP機能を使う」（P.534）

2.27　テンプレート着信機能

テンプレート着信機能とは、あらかじめ着信接続時に共通する情報をテンプレートに定義しておき、そのテンプレートを使って着信を行う機能です。テンプレート着信は、接続するたびに、設定したプール情報の中から使用していない情報を接続相手に動的に割り当てるため、不特定相手着信を実現することができます。

また、同一の相手には、AAA（Authentication、Authorization、Accounting）から個別情報を取得することより、同一の情報を静的に割り当てることができます。さらに、AAAから情報を取得することにより、接続先を相手ネットワーク情報に設定したときに比べて、より多くの接続相手を登録することができます。

本装置のAAA情報では、テンプレート着信で接続するユーザの認証情報など通信接続に関する情報を登録しておくことができます。



テンプレート着信時に使用するインタフェースは、テンプレート用に予約されたIFプールから、空いているインタフェースを自動的に検索して通信します。

また、着信時の認証は、AAA情報に登録されたユーザ情報で行われます。

接続相手の登録を追加する場合は、AAA情報に接続相手のユーザ情報を登録するだけで追加することができます。

こんな事に気をつけて

- テンプレート着信機能をサポートする回線はISDNです（MP接続はできません）。
- テンプレート着信で使用するインタフェースはテンプレート専用になります。テンプレート用に予約されたrmtインタフェースには、remote定義を設定しないでください。
  たとえば、rmt30～47インタフェースをテンプレート用に予約した場合、remote 30～47までのremote定義を設定しないでください。
- テンプレート情報を定義する場合（IPフィルタリングなど）、定義数は「テンプレート情報で設定した定義数×テンプレートで使用するrmtインタフェース数」で計算されるため、それを含めて装置最大定義数の範囲に収まるように定義してください。装置最大定義数を超えたときは、資源不足により該当機能が動作しない場合があります。
- 接続先情報を設定する場合、テンプレート用のインタフェースの個数分は設定しないでください。
  たとえば、接続先定義を最大48定義可能な装置で、10インタフェースをテンプレート用に使用する場合、接続先定義の定義数は38となります。
- テンプレート情報とAAA情報のユーザ側の設定に同じ項目がある場合は、個人情報であるAAA情報が適用されます。
- 発信者番号による識別（CLID相手判定）をAAA情報に設定していない場合は、発信者番号による相手判定は行いません（PPPのユーザ認証の結果だけで接続できるかどうかが決まります）。
- AAA情報に同一ユーザ（パスワードも同一）が存在するときには、定義番号が小さいAAAユーザ情報が優先されます。定義番号が大きいユーザ情報に発信者番号が一致する定義があり、定義番号が小さいユーザ情報に発信番号で識別を行わない定義がある場合も、定義番号の小さいユーザで着信が行われます。
- 共通IDで複数の着信を行う場合は、AAA情報のユーザ定義に、IDとパスワードだけを定義してください（個別情報を定義しないで、IDとパスワードだけのユーザ情報を定義すると共有IDとして扱われます）。

☛参照 MR1000　コマンド設定事例集「2.37 外部のパソコンから着信接続する（リモートアクセスサーバ）」（P.282）
MR1000　Web設定事例集「2.37 外部のパソコンから着信接続する（リモートアクセスサーバ）」（P.639）

2.28　SSHサーバ機能

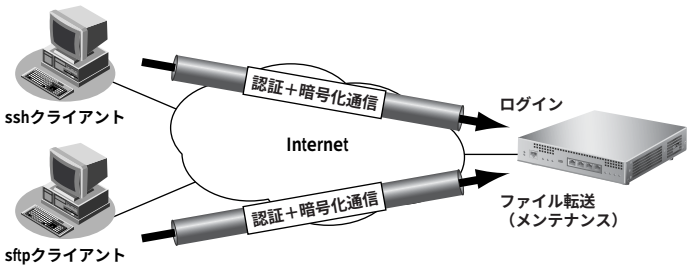
SSHサーバ機能とは、TELNETサーバ機能と同じリモートログイン機能（sshサーバ）とFTPサーバ機能と同じリモートファイル転送機能（sftpサーバ）をサポートしています。

TELNETサーバ機能およびFTPサーバ機能では、平文テキストデータのまま通信するため、通信内容を傍受されたり、改ざんされる危険性があります。SSHサーバ機能では、ホスト認証および暗号化通信により、安全で信頼できるログイン機能およびファイル転送機能を利用することができます。

参照　本装置のSSHサーバ機能は、BSDライセンスに基づいて公開されているフリーソフトウェアのOpenSSHを利用しています。詳しくは、以下のURLを参照してください。

英語版　：http://www.openssh.com/

日本語版：http://www.openssh.com/ja/



本装置の電源投入時およびリセット時に本装置のSSHホスト認証鍵が生成されます。生成時間は、数十秒から数分です。SSHホスト認証鍵生成開始時と完了時にシスログが出力され、生成完了した時点から本装置にSSH接続することができます。

SSHクライアントソフトウェアにあらかじめ接続相手のSSHホスト認証鍵を設定しておく必要がある場合は、本装置でsshkeyコマンドを実行して表示されるSSHホスト認証鍵を設定します。

本装置にSSH接続した際に、本装置のSSHホスト認証鍵がSSHクライアント側に送信されて、設定または保存されている鍵と異なる場合は、SSH接続が拒否されます。したがって、装置交換などにより、SSHホスト認証鍵が変更された場合は、SSHクライアントソフトウェアに設定または保存されているSSHホスト認証鍵を再設定するか削除してからSSH接続します。

その後、パスワード入力プロンプトが表示されますが、SSHホスト認証などの処理により、表示されるまで多少時間がかかります。

本装置へのSSH接続は、同時に1接続しかできないため、SSH接続中に新たなSSH接続要求があった場合は、SSHホスト認証をする前に切断されます。

また、serverinfo ssh/serverinfo sftpコマンドをoffに設定することにより、SSHサーバ機能を完全に停止させることができます。

sshクライアントとsftpクライアントはSSHポートに接続するため、serverinfoコマンドのsshまたはsftpのどちらかがonの場合、本装置のSSHポートは接続できる状態で、serverinfoコマンドでoffになっていてもパスワード入力まで行われたあとに、接続が切断されます。

こんな事に気をつけて

SSHサーバ機能が完全に停止している状態で本装置を起動し、serverinfoコマンドでSSH機能のどちらかを有効にして定義設定（enable allコマンドの実行など）した場合、SSHホスト認証鍵が生成され、数十秒から数分間の時間がかかります。このとき、セッション監視タイムアウトが発生するなど、ほかの処理に影響する可能性があります。

以下に、ssh 接続と telnet 接続の相違点を示します。

項目	ssh 接続	telnet接続
パスワード入力時無入力自動切断時間	2 分 （ログイン中は telnetinfo の設定に従う）	telnetinfo の設定に従う
シスログメッセージ（一部分抜粋）	login ユーザ名	logon telnet

以下に、sftp 接続と ftp 接続の相違点を示します。

項目	sftp 接続	ftp接続
ユーザ ID 指定	接続前に指定 （一部の sftp クライアントは接続開始時に指定する）	接続後に指定 （一部の ftp クライアントは接続前に指定する）
バイナリモード指定	なし	あり
パッシブモード指定	なし	あり

本装置でサポートする SHH サーバ機能

項目	サポート内容
SSH サーババージョン	OpenSSH 3.9p1
SSH プロトコルバージョン	SSH プロトコルバージョン 2だけをサポート
SSH ポート番号／プロトコル	22／ TCP
IP プロトコルバージョン	IPv4 および IPv6 をサポート
ホスト認証プロトコル	RSA
ホスト認証アルゴリズムの種類	ssh-rsa, ssh-dss
暗号方式の種類	aes128-cbc、3des-cbc、blowfish-cbc、cast128-cbc、arcfour、aes192-cbc、aes256-cbc、rijndael-cbc@lysator.liu.se、aes128-ctr、aes192-ctr、aes256-ctr
メッセージ認証コードの種類	hmac-md5、hmac-sha1、hmac-ripemd160、hmac-ripemd160@openssh.com、hmac-sha1-96、hmac-md5-96
同時接続数	1

2.28.1　SSHクライアントソフトウェア

本装置にSSH接続するには、SSHクライアントソフトウェアが別途必要です。

本装置のSSHサーバ機能では、SSHプロトコルバージョン2だけをサポートしているため、SSHプロトコルバージョン2に対応したSSHクライアントソフトウェア（sshクライアントソフトウェアおよびsftpクライアントソフトウェア）を使用してください。

以下に、使用できるクライアントソフトウェア一覧を示します。

補足　以下の表は、使用可能なソフトウェア一覧であり、すべての動作について保証するものではありません。

sshクライアント（ログインクライアント）ソフトウェア

OS名	sshクライアント名	IPv4接続	IPv6接続
Windows® XP／2000／Me／98（SE）	PuTTY 0.55	可能	可能
FreeBSD	ssh（OpenSSH 3.9p1）	可能	可能
Linux	ssh（OpenSSH 3.9p1）	可能	可能

sftpクライアント（ファイル転送クライアント）ソフトウェア

OS名	sftpクライアント名	IPv4接続	IPv6接続
Windows® XP／2000／Me／98（SE）	FileZilla 2.2.8d	可能	不可
	psftp（PuTTY 0.55）	可能	可能（※）
FreeBSD	sftp（OpenSSH 3.9p1）	可能	不可
	cftp 0.12	可能	可能
Linux	sftp（OpenSSH 3.9p1）	可能	不可
	cftp 0.12	可能	可能

※）IPv6アドレス指定は接続できず、ホスト名指定でのみ接続できます。

索引

N

O

P

R

S

T

U

V

W

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

な

に

ね

の

は

ふ

へ

ほ

ま

む

ゆ

よ

ら

り

る

れ

ろ

MR1000　機能説明書

発行日　　2005年1月

第1版　　K1N-D-04167A

発行責任　　オムロン株式会社

Printed in Japan