P3NK-5162-01Z0

# FUJITSU Network SR-X
# 機能説明書

V02

FUJITSU

# 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。
サーバとの共存性を高めた、省スペース・省電力の本製品はサーバ間接続に最適です。

2014 年 10 月初版

# 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。

## 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。

ネットワーク設定を初めて行う方でも「機能説明書」に分かりやすく記載していますので、安心してお読みいただけます。

## 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 IP 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。

| | |
|---|---|
| ヒント | 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。 |
| 補足 | 操作手順で説明しているもののほかに、補足情報を説明しています。 |
| 参照 | 操作方法など関連事項を説明している箇所を示します。 |
| 適用機種 | 本装置の機能を使用する際に、対象となる機種名を示します。 |
| ⚠警告 | 製造物責任法（PL）関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。 |
| ⚠注意 | 製造物責任法（PL）関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。 |

# 本書における商標の表記について

Microsoft、MS-DOS、Windows、Windows NTおよびWindows Vista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。

Adobeおよび Readerは、Adobe Systems Incorporated（アドビシステムズ社）の米国ならびに他の国における商標または登録商標です。

Netscapeは、米国Netscape Communications Corporationの商標です。

UNIXは、米国およびその他の国におけるオープン・グループの登録商標です。

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。

## 製品名の略称について

本書で使用している製品名は、以下のように略して表記します。

なお、本文中では®を省略しています。

| 製品名称 | 本文中の表記 |
|---|---|
| Microsoft® Windows® XP Professional operating system | Windows XP |
| Microsoft® Windows® XP Home Edition operating system | |
| Microsoft® Windows® 2000 Server Network operating system | Windows 2000 |
| Microsoft® Windows® 2000 Professional operating system | |
| Microsoft® Windows NT® Server network operating system Version 4.0 | Windows NT 4.0 |
| Microsoft® Windows NT® Workstation operating system Version 4.0 | |
| Microsoft® Windows Server® 2003, Standard Edition | Windows Server 2003 |
| Microsoft® Windows Server® 2003 R2, Standard Edition | |
| Microsoft® Windows Server® 2003, Enterprise Edition | |
| Microsoft® Windows Server® 2003 R2, Enterprise Edition | |
| Microsoft® Windows Server® 2003, Datacenter Edition | |
| Microsoft® Windows Server® 2003 R2, Datacenter Edition | |
| Microsoft® Windows Server® 2003, Web Edition | |
| Microsoft® Windows Server® 2003, Standard x64 Edition | |
| Microsoft® Windows Server® 2003 R2, Standard Edition | |
| Microsoft® Windows Server® 2003, Enterprise x64 Edition | |
| Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition | |
| Microsoft® Windows Server® 2003, Enterprise Edition for Itanium-based systems | |
| Microsoft® Windows Server® 2003, Datacenter x64 Edition | |
| Microsoft® Windows Server® 2003 R2, Datacenter x64 Edition | |
| Microsoft® Windows Vista® Ultimate operating system | Windows Vista |
| Microsoft® Windows Vista® Business operating system | |
| Microsoft® Windows Vista® Home Premium operating system | |
| Microsoft® Windows Vista® Home Basic operating system | |
| Microsoft® Windows Vista® Enterprise operating system | |
| Microsoft® Windows® 7 64bit Home Premium | Windows 7 |
| Microsoft® Windows® 7 32bit Professional | |

# 本装置のマニュアルの構成

本装置の取扱説明書は、以下のとおり構成されています。使用する目的に応じて、お使いください。

| マニュアル名称 | 内容 |
|---|---|
| ご利用にあたって | 本装置の設置方法やソフトウェアのインストール方法を説明しています。 |
| 機能説明書（本書） | 本装置の便利な機能について説明しています。 |
| トラブルシューティング | トラブルが起きたときの原因と対処方法を説明しています。 |
| メッセージ集 | システムログ情報などのメッセージの詳細な情報を説明しています。 |
| 仕様一覧 | 本装置のハード／ソフトウェア仕様とMIB/Trap一覧を説明しています。 |
| コマンドユーザーズガイド | コマンドを使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。 |
| コマンド設定事例集 | コマンドを使用した、基本的な接続形態または機能の活用方法を説明しています。 |
| コマンドリファレンス | コマンドの項目やパラメタの詳細な情報を説明しています。 |
| Webユーザーズガイド | Web画面を使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。また、Web画面の項目の詳細な情報を説明しています。 |

# 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、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。



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。



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IPネットワークの設計概念について説明します。

# 1.1　レイヤ 2 ネットワーク設計概念

**適用機種**　全機種

## 1.1.1　VLAN

レイヤ 2 のネットワークは、MAC アドレスをもとに到達する先を制御します。レイヤ 2 のネットワークでは、VLAN と呼ばれる論理的なネットワークから構成されます。VLAN を使って複数の物理的な LAN から 1 つの論理的な LAN に構成したり、物理的に 1 つの LAN を複数の論理的な LAN に分けたりします。各 VLAN には VLAN ID（VID）をつけて管理します。

### VLAN ID

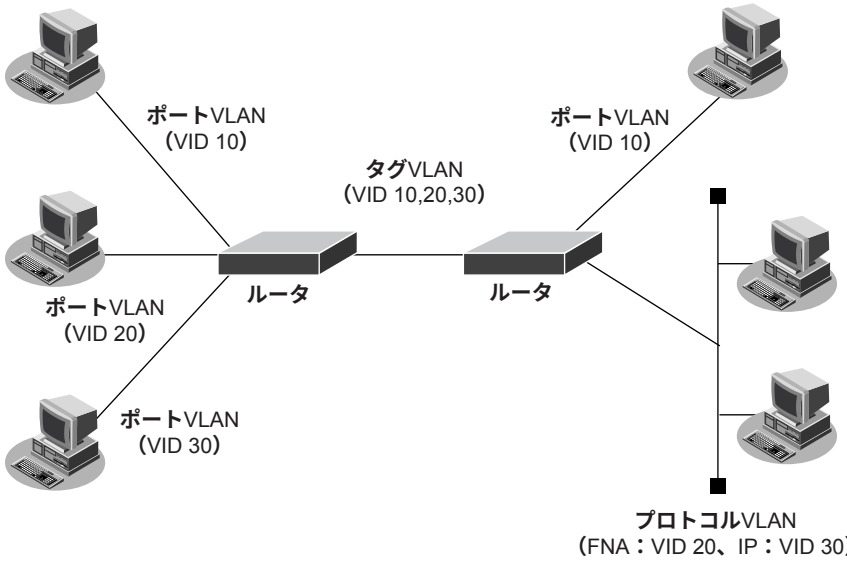
各 VLAN には 10 進数で 1 から 4094 までの番号をつけて管理します。これを VLAN ID と言います。同じ VLAN ID を持つ VLAN に属している装置間では通信可能ですが、異なる VLAN ID を持つ VLAN に属している装置間では通信はできません。

### VLAN の種類

VLAN には以下の 3 つの種類があります。

- ポート VLAN
  ETHER ポートごとに「どの VLAN に所属するか」を設定するものです。
  その ETHER ポートのデータは、すべて指定された VLAN に属します。
- タグ VLAN
  1 つの物理回線上に複数の VLAN を設定する場合に使用します。IEEE802.1Q で標準化された方式で、VLAN ヘッダを Ethernet のフレームヘッダに挿入することによって、1 つの物理回線上に複数の VLAN を実現します。
- プロトコル VLAN
  Ethernet のフレームヘッダには、フレームタイプという 16 ビットのフィールドがあり、そのフレームに格納されている上位プロトコルが識別できるようになっています。たとえば、IP、FNA、IPX といった異なるネットワークプロトコルの通信を Ethernet フレームのレベルで識別することができます。プロトコル VLAN はこの情報を使い、ネットワークプロトコルごとに異なる VLAN を定義できるようにしたものです。たとえば、IP ではサブネットワークごとに VLAN を分けてルーティングを行うが、FNA プロトコルでは分割しないで全体を 1 つのネットワークとして扱う、といった設定が行えます。

この3つの種類はETHERポートごとに設定を変えることができます。つまり、VLAN IDが10のVLANを、ETHERポート1ではポートVLAN、ETHERポート2ではタグVLANにするといったことができます。この場合、VLAN IDが10のVLANのデータは、ETHERポート1とETHERポート2で送受信され、ETHERポート1ではタグのない通常のフレーム、ETHERポート2ではタグ付きのフレームとして送受信されます。




## 1.1.2　リンクアグリゲーション

リンクアグリゲーションとは、複数の物理回線をまとめて1本の論理回線として扱う技術です。1本の物理回線では帯域が足りない場合、複数の物理回線をまとめて広い帯域を確保します。また、リンクアグリゲーションを構成している物理回線のうち、1本の回線が故障などの原因により通信できなくなった場合、ほかの物理回線で通信は継続できるので、冗長構成の機能もあります。

複数のVLANが含まれている場合も物理回線が1本の場合と同様に、リンクアグリゲーションで構成された論理的に1本の回線に複数のVLANが含まれる構造になります。また、STPでも1本の回線として扱い、ポートの制御などはリンクアグリゲーションの論理的な回線に対して行われます。

# 1.2　本装置の設定の概要

**適用機種**　全機種

## ネットワークと設定の関係

本装置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。

- ether 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。回線の種類や速度などに関する情報を定義します。
- vlan 定義
  本装置の VLAN に関する情報を定義する命令群です。プロトコル VLAN の情報や静的な学習テーブルの情報を定義します。
- 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 IP アドレスやネットワークの情報などを定義します。
- 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。

## 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。
- 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。
- oob
  Ethernet インタフェース（マネージメントポート用）
  Ethernet（マネージメントポート）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。oob 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,oob0,...

lan のネットワークインタフェースは lan 定義によって設定されます。lan 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。

## 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、lan1 から出力するための経路情報は lan1 内の定義に分けて設定します。

# 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。

# 2.1　オートネゴシエーション機能

**適用機種**　全機種

オートネゴシエーション機能とは、IEEE802.3u に規定された 2 装置間のプロトコルであり、優先順位に従い通信速度、通信モード（全二重／半二重）の設定を自動的に行う機能です。

本装置が使用している 10/100BASE-T（SR-X526R1 マネージメントポート）、10/100/1000BASE-T ポート、および 10GBASE-R（SFP+）ポートの相互接続について以下に示します。

なお、表中の「100M/FULL」などの記述は、自装置と接続相手の通信モードの組み合わせの結果、リンク確立する接続モードを示します。記述がない場合は、リンク確立しません。

- オートネゴシエーション（Auto-Nego）どうしの接続は、相互に通信できるモードの中から、決められたアルゴリズムにより通信モードが設定されます。
- 固定どうしの接続は、同じ通信モードのときだけ正常に通信できます。

**こんな事に気をつけて**

- **一方がオートネゴシエーションで、他方が FULL（全二重）の固定で接続すると、通信モードは HALF（半二重）と認識されます。この場合、エラー率が高いなど正常な通信ができないことがありますので、通信モードを正しく設定してください。**
- **一方または両方の通信モードがオートネゴシエーションで、お互いが認識できない場合は、両方の通信モードを固定に設定してください。**
- **一方が 10M 固定、他方を 100M 固定で誤接続すると、片方の装置だけがリンク確立したり、通信状態によってはリンクが確立と切断を繰り返したりする場合があります。この場合は通信モードを正しく設定してください。**
- 10GBASE-R（SFP+）**ポートには、オートネゴシエーション機能はありません。**

### ● 10/100/1000BASE-T ポートの場合

○：接続可能、×：接続不能

| 自装置＼接続相手 | | Auto-Nego | 10M 固定 | | 100M 固定 | | 1000M 固定 |
|---|---|---|---|---|---|---|---|
| | | | FULL | HALF | FULL | HALF | FULL |
| Auto-Nego | | ○<br>10M/FULL、10M/HALF<br>100M/FULL、100M/HALF、1000M/FULL | ×（※）<br>10M/HALF | ○<br>10M/HALF | ×（※）<br>100M/HALF | ○<br>100M/HALF | ○<br>1000M/FULL |
| 10M 固定 | FULL | ×（※）<br>10M/HALF | ○<br>10M/FULL | × | × | × | × |
| | HALF | ○<br>10M/HALF | × | ○<br>10M/HALF | × | × | × |
| 100M 固定 | FULL | ×（※）<br>100M/HALF | × | × | ○<br>100M/FULL | × | × |
| | HALF | ○<br>100M/HALF | × | × | × | ○<br>100M/HALF | × |
| 1000M 固定 | FULL | ○<br>1000M/FULL | × | × | × | × | ○<br>1000M/FULL |

※）リンク確立するが、通信設定が異常

## ● マネージメントポートの場合

○：接続可能、×：接続不能

| 接続相手 / 自装置 | Auto-Nego | 10M 固定 | | 100M 固定 | |
|---|---|---|---|---|---|
| | | FULL | HALF | FULL | HALF |
| Auto-Nego | ○<br>100M/FULL、100M/HALF、10M/FULL、10M/HALF | ×（※）<br>10M/HALF | ○<br>10M/HALF | ×（※）<br>100M/HALF | ○<br>100M/HALF |

※）リンク確立するが、通信設定が異常

## ● 10GBASE-R（SFP+）ポートの場合

10G/FULL 固定設定どうしのみ接続可能。

# 2.2　AutoMDI/MDI-X 機能

**適用機種**　***SR-X316T2, 324T2, 340TR1***

AutoMDI/MDI-X 機能とは、接続相手のポートが MDI か MDI-X かを自動的に判断して接続する機能です。

本装置の 10/100/1000BASE-T ポートでは、AutoMDI/MDI-X 機能をサポートしています。

MDI の自動検出は、通信モードが Auto および 1000M/FULL の場合のみ有効であり、10M/FULL 固定、10M/HALF 固定、100M/FULL 固定、100M/HALF 固定の場合は、MDI の自動検出を指定しても、システムログを出力して MDI-X として動作します。

また、MDI の指定は、通信モードが 10M/FULL 固定、10M/HALF 固定、100M/FULL 固定、100M/HALF 固定の場合のみ有効であり、10/100/1000BASE-T ポートの Auto および 1000M/FULL 固定の場合は、MDI を指定してもシステムログを出力して MDI-X として動作します。

| MDI/MDI-X の指定（※）<br>通信モードの指定 | | auto | mdi | mdix |
|---|---|---|---|---|
| Auto | | auto | mdix | mdix |
| 固定 | 1000M/FULL | auto | mdix | mdix |
| | 100M/FULL、100M/HALF、10M/FULL、10M/HALF | mdix | mdi | mdix |

※）　MDI/MDI-X では、以下の動作を指定できます。
auto　：MDI を自動検出
mdi　：MDI として動作
mdix　：MDI-X として動作

# 2.3　フロー制御機能

適用機種　全機種

本装置では、IEEE802.3x に基づく Pause フレーム、半二重通信時はバックプレッシャ機能によるフロー制御機能をサポートしています。
フロー制御の設定による各ポートの動作を以下に示します。

### こんな事に気をつけて

**フロー制御を適用した場合、接続相手が本装置の該当ポートにフレーム送信できなくなることがあります。この場合、接続相手のバッファ容量によって、本装置に設定している優先機能の優先度に関係なくフレーム廃棄されることがあります。このため、音声や画像などを使用するネットワークの場合は、フロー制御を無効にしてください。**
**また、接続相手によっては、データフレームの転送性能が劣化することがあります。**

＜ Auto-nego モードの場合＞

| フロー制御設定 | | システム動作 |
|---|---|---|
| 送信 | 受信 | |
| off 設定 | off 設定 | IEEE802.3x に示されるフロー制御設定を、Pause= なし、送受信方向 = 対称（※1）としてオートネゴシエーションし、全二重モードでリンク確立した場合は、接続相手のフロー制御設定により処理を実行する（※2）。<br>半二重モードでリンク確立した場合は、半二重固定モードと同じ動作となる。 |
| on 設定 | off 設定 | IEEE802.3x に示されるフロー制御設定を、Pause= なし、送受信方向 = 非対称（※1）としてオートネゴシエーションし、全二重モードでリンク確立した場合は、接続相手のフロー制御設定により処理を実行する（※2）。<br>半二重モードでリンク確立した場合は、半二重固定モードと同じ動作となる。 |
| off 設定 | on 設定 | IEEE802.3x に示されるフロー制御設定を、Pause= あり、送受信方向 = 非対称（※1）としてオートネゴシエーションし、全二重モードでリンク確立した場合は、接続相手のフロー制御設定により処理を実行する（※2）。<br>半二重モードでリンク確立した場合は、半二重固定モードと同じ動作となる。 |
| on 設定 | on 設定 | IEEE802.3x に示されるフロー制御設定を、Pause= あり、送受信方向 = 非対称（※1）としてオートネゴシエーションし、全二重モードでリンク確立した場合は、接続相手のフロー制御設定により処理を実行する（※2）。<br>半二重モードでリンク確立した場合は、半二重固定モードと同じ動作となる。 |

※1）"Pause" は、Pause オペレーション能力のあり／なしを示し、" 送受信方向 " は、Pause オペレーション能力が送受信対称か、非対称かを示します。

※2）Auto-nego モード時のフロー制御設定は、接続相手のフロー制御設定により、以下の表のとおりに設定されます。

SR-X316T2/324T2 の場合

| 自装置のフロー制御設定 | | 接続相手のフロー制御設定 | | Auto-Nego 結果 | |
|---|---|---|---|---|---|
| 送信 | 受信 | Pause | 送受信方向 | pause 送信 | pause 受信 |
| off 設定 | off 設定 | D.C. | D.C. | N | N |
| on 設定 | off 設定 | なし | D.C. | N | N |
| | | あり | 対称 | N | N |
| | | あり | 非対称 | Y | N |
| off 設定 | on 設定 | なし | 対称 | N | N |
| | | なし | 非対称 | N | Y |
| | | あり | D.C. | Y | Y |
| on 設定 | on 設定 | なし | 対称 | N | N |
| | | なし | 非対称 | N | Y |
| | | あり | D.C. | Y | Y |

SR-X340TR1 の場合

| 自装置のフロー制御設定 | | 接続相手のフロー制御設定 | | Auto-Nego 結果 | |
|---|---|---|---|---|---|
| 送信 | 受信 | Pause | 送受信方向 | pause 送信 | pause 受信 |
| off 設定 | off 設定 | D.C. | D.C. | N | N |
| on 設定 | off 設定 | なし | D.C. | N | N |
| | | あり | 対称 | N | N |
| | | あり | 非対称 | Y | N |
| off 設定 | on 設定 | なし | 対称 | N | N |
| | | なし | 非対称 | N | Y |
| | | あり | D.C. | N（※） | Y |
| on 設定 | on 設定 | なし | 対称 | N | N |
| | | なし | 非対称 | N | Y |
| | | あり | D.C. | Y | Y |

※）オートネゴシエーションの結果、送信 Pause=Y になりますが、自設定に従って送信 Pause=N になります。

- D.C. ：Don't Care
- Pause フレーム送信時
  Y　：フロー制御のために Pause フレームを送出する
  N　：Pause フレームを送出しない
- Pause フレーム受信時
  Y　：Pause フレームを受信することがあるため、その場合は受信処理（フロー制御）を行う
  N　：Pause フレームを受信しない（受信した場合は、Pause フレームを廃棄し、何も処理しない）

＜固定モードの場合＞

| フロー制御設定 | | 通信モード | システム動作 | |
|---|---|---|---|---|
| 送信 | 受信 | | 送信方向 | 受信方向 |
| off 設定 | off 設定 | 全二重固定 | Pause フレーム送出なし | Pause フレーム受信時は、フロー制御を実行しない（※1） |
| | | 半二重固定 | バックプレッシャ送出なし | バックプレッシャ受信時は、データ送信停止（※2） |
| on 設定 | off 設定 | 全二重固定 | フロー制御のため Pause フレームを送出する | Pause フレーム受信時は、フロー制御を実行しない（※1） |
| | | 半二重固定 | フロー制御のためバックプレッシャを送出する | バックプレッシャ受信時は、データ送信停止（※2） |
| off 設定 | on 設定 | 全二重固定 | Pause フレーム送出なし | Pause フレーム受信時は、フロー制御を実行する |
| | | 半二重固定 | バックプレッシャ送出なし | バックプレッシャ受信時は、データ送信停止（※2） |
| on 設定 | on 設定 | 全二重固定 | フロー制御のため Pause フレームを送出する | Pause フレーム受信時は、フロー制御を実行する |
| | | 半二重固定 | フロー制御のためバックプレッシャを送出する | バックプレッシャ受信時は、データ送信停止（※2） |

ただし、SR-X316T2/324T2 の 1000M 固定モードの場合は、＜ Auto-nego モード＞に従って設定されます。

※1）Pause フレーム受信時は無視します。

※2）バックプレッシャとして送信停止するわけではなく、半二重動作としてデータ送信できません。

# 2.4　EEE 機能

適用機種　***SR-X316T2, 324T2***

IEEE802.3az に準拠した EEE（Energy Efficient Ethernet）機能による省電力モードをサポートします。
ether ポートで通信データが送受信されていない状態のときに、消費電力を削減することができます。

### こんな事に気をつけて

**以下の場合は、省電力モードは有効となりません。**

- **通信速度設定がオートネゴシエーションでない、または 1000Mbps 固定でない場合**
- **オートネゴシエーションの結果、10Mbps または半二重モードでリンクアップした場合**
- **接続された相手装置が同機能に対応していない場合**

# 2.5　フォワーディングモード機能

適用機種　***SR-X526R1***

本装置では、スイッチングの方式として、カットスルーモードとストアアンドフォワードモードを選択することができます。

- カットスルーモード
  本装置にパケットの先頭部分が入力したあとに転送先のポートからパケットを送出します。パケットの全体が入力するのを待たずに転送が行われるため、転送にともなうパケットの遅延（レイテンシ）を最小限に抑えることができます。
- ストアアンドフォワードモード
  本装置にパケットの全体が入力したあとに転送先のポートからパケットを送出します。

こんな事に気をつけて

**カットスルーモードを選択した場合は、レイテンシが短縮できますが、エラーパケットを中継してしまいます。**
**ストアアンドフォワードモードの場合は、エラーパケットが入力されても中継しませんが、レイテンシはパケットデータを蓄積する分だけカットスルーモードより長くなります。**

# 2.6　MACアドレス学習／MACフォワーディング機能

**適用機種**　全機種

本装置では、MACアドレス学習機能として以下の機能をサポートしています。

- MACアドレス学習基本機能

  受信パケットの送信元MACアドレスをダイナミックに学習して、FDB（Filtering Data Base）に登録する機能です。

  登録したMACアドレスは、エージングアウト時間まで保持し続けます。エージングアウト時間は構成定義コマンドで変更できます（初期値は300秒）。

  ポートがリンクダウンした場合は、FDB上の該当ポートから学習したエントリを削除します。

- MACアドレス自動学習停止機能

  構成定義によって、装置単位でダイナミックなMACアドレスの学習を停止する機能です。

- FDBクリア機能

  ダイナミックに学習したFDBエントリを削除する機能です。ポート単位、MACアドレス単位など条件指定することもできます。

- スタティックMACフォワーディング機能

  特定のあて先アドレスを持つフレームをVLANごとに指定したポートへ中継できる機能です。

  あて先アドレスにはユニキャストアドレスが指定できます。

- MACテーブルフラッシュ機能

  指定したMACアドレスの学習ポートの監視を行い、学習ポートの移動を検出した場合に、移動する前のポートに関連したMACアドレス学習テーブルのエントリ情報をクリアする機能です。

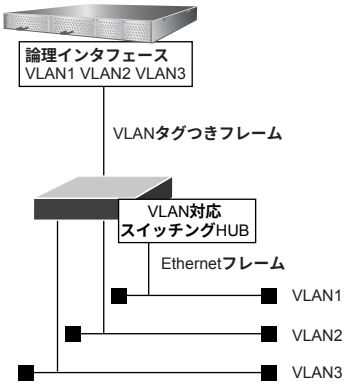
### こんな事に気をつけて

- **SR-X340TR1でMLAG機能を使用する場合、本機能は使用できません。**
- **SR-X526R1では、MACテーブルフラッシュ機能の動作契機が最大で20秒程度遅延することがあります。**

# 2.7　VLAN 機能

**適用機種**　全機種

VLAN 機能とは、物理的な LAN を仮想的な複数の LAN に分割し、ポート、MAC アドレス、プロトコルなどでグループ化を行う機能です。




## 装置内 VLAN

VLAN は、タギング方式と呼ばれる VLAN グループ識別方法を用いた通信方式を規定しています。タギング方式とは、フレームに VLAN タグを付与することでそのフレームがどの VLAN に属するのかを識別する方法です。識別子として定義されたものを VLAN ID と言い、VLAN を 1 つ定義した場合、それに対応する VLAN ID も 1 つ割り当てます。

本装置でサポートする VLAN 機能は、IEEE802.1q に準拠しています。

本装置は、VID=1 に、すべてのポートが VLAN1 のタグなしとして初期設定されていますが、各ポートを特定の VLAN のタグ付きまたはタグなしに設定を変更することができます。

### VLAN とネットワークアドレス

VLAN 機能を使用した場合、ブリッジング通信はその VLAN 内に閉じたものになります。したがって、VLAN を定義するということは、MAC アドレスのレベルでブロードキャストフレームが届く範囲（ブロードキャストドメイン）を制限する、ということになります。

また、これをネットワーク層の位置から考えると、以下の 2 つのことができます。

- 各物理ポートに、VLAN タグを使用して複数のネットワークアドレスを対応させる。
- 複数の物理ポートを束ねたものに、1 つのネットワークアドレスを割り当てる。

## VLAN 種別

本装置がサポートする VLAN 機能では、以下の 2 つの単位で VLAN を分けることができます。

- ポート VLAN
  ポート単位でグループ化を行う機能です。すべてのネットワークプロトコルのアドレスを付与することができます。
- プロトコル VLAN
  特定のプロトコルに基づいてポートをグループ化する機能です。
  プロトコル VLAN で指定可能なプロトコルの種類は以下のとおりです。
  - IPv4
  - IPv6
  - FNA

  また、フレームタイプを直接指定することによって、任意プロトコルのプロトコル VLAN を作成することができます。

## VLAN タグとポートの関係

VLAN 機能を使用する場合、あらかじめ VLAN 内のポートに、フレームを送信するときに VLAN タグを付与するか定義しておきます。付与するかどうかは、各ポートの先にあるノードが VLAN タグを識別できるかどうかによって決まります。

VLAN 機能を使用している場合、本装置の各ポートの先に接続されたセグメントは、以下の 3 つのどれかに属しています。

- アクセスリンク
  VLAN タグなしのフレームだけが流れる区間です。VLAN タグを理解できないエンドノードが接続されます。
- トランクリンク
  VLAN タグ付きフレームだけが流れる区間です。タグ付き VLAN 機能をサポートしている装置どうしは、通常トランクリンクで接続します。VLAN タグを理解できないエンドノードは接続されません。
- ハイブリッドリンク
  VLAN タグ付きのフレームと VLAN タグなしのフレームの両方が流れる区間です。ここには、複数の VLAN が存在し、それぞれの VLAN にとってアクセスリンクまたはトランクリンクとなります。ただし、特定のプロトコルに注目した場合、ハイブリッドリンクをアクセスリンクとして運用できる VLAN は 1 つだけです。たとえば、1 つのハイブリッドリンク上に 2 つの VLAN がアクセスリンクとして運用している場合に、IP プロトコルに注目すると、そのうちの 1 つしか認識することができません。

### こんな事に気をつけて

- **特定のプロトコルに対して、2 つ以上の VLAN をアクセスリンクとして運用する場合、それぞれの VLAN から送信されるフレームには VLAN タグが付与されていないため、属する VLAN を識別することができません。**
- **スパニングツリー機能と併用する場合、ブリッジフレームおよびルーティングフレームはスパニングツリーの制限に従います。**

## 同一ポート上での VLAN の混在

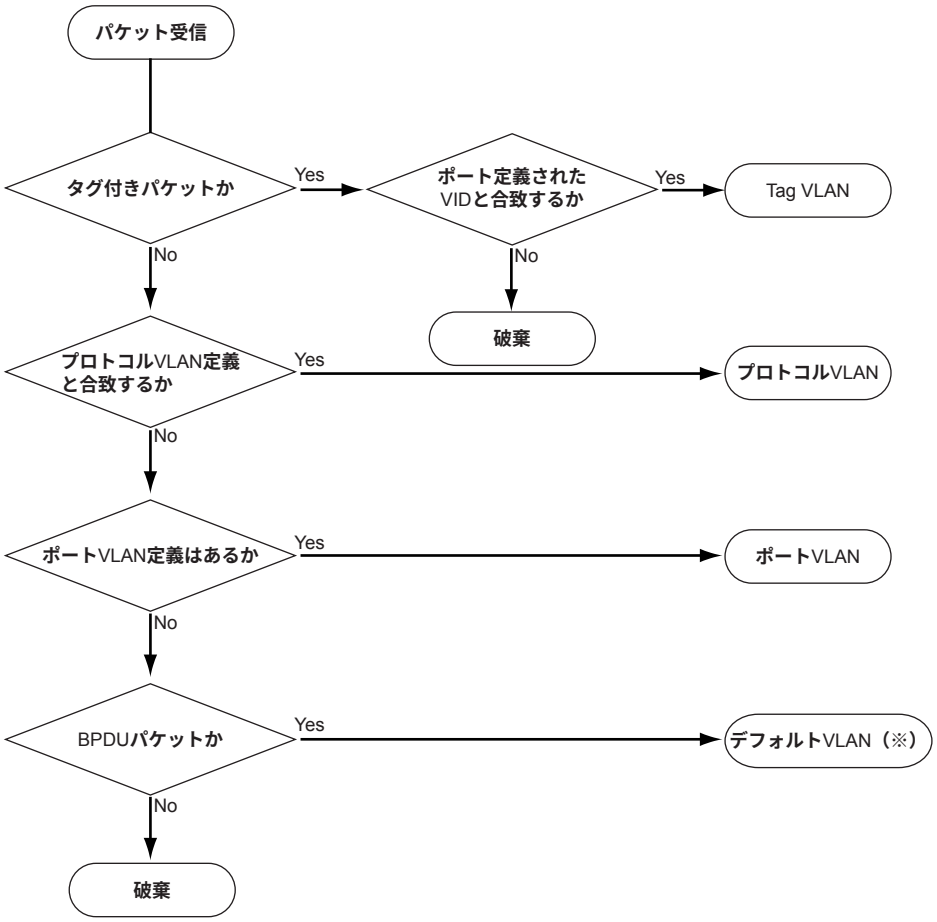
同一ポート上で使用できる VLAN の組み合わせを以下に示します。

○：混在できる、×：混在できない

| VLAN 種別 | ポート VLAN（untagged） | プロトコル VLAN（untagged） | Tag VLAN（Tagged） |
|---|---|---|---|
| ポート VLAN（untagged） | × | ○ | ○ |
| プロトコル VLAN（untagged） | ○ | ○ | ○ |
| Tag VLAN（Tagged） | ○ | ○ | ○ |

### パケット受信時の VLAN 判定

VLAN を設定したポートでパケットを受信した場合、受信したパケットの所属する VLAN の判定を以下の順序で行います。




※）本装置では、構成定義で Tag VLAN ／プロトコル VLAN が定義され、かつ、ポート VLAN（untagged）が未設定のポートに対しては、BPDU パケットを受信するために装置内でデフォルト VLAN を作成します。

### パケット送信時の VLAN タグ

パケット送信時の VLAN タグの扱いは、送信するポートの Tagged ／ Untagged 設定に従って、Tagged ポートの場合は VLAN タグを付与し、Untagged ポートの場合は VLAN タグを付与しないで送信します。

## VLAN トランク機能

VLAN トランク機能とは、VLAN タグの付与および削除が可能なスイッチが VLAN 間の通信を行う際に使用する機能です。複数の VLAN に属するポートからルーティングするために、ほかのレイヤ 3 スイッチへ中継します。ポートでは、どの VLAN に属しているかを認識するために VLAN タグを付け、レイヤ 3 スイッチで VLAN タグ付きフレームを受け取り、ルーティングして中継します。

# 装置間 VLAN

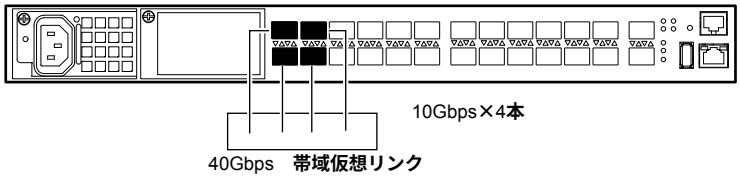
VLAN が装置間をまたぐ場合、フレームに VLAN タグを付けてどの VLAN からきたフレームかを区別します。これによって、たとえば VLAN A どうし、VLAN B どうしは、それぞれ同じスイッチング HUB に接続されているように通信することができます。また、VLAN トランク機能を使用することによって、通常 2 本必要な伝送路が本装置間を 1 本で接続することができます。

参照 仕様一覧「2.3 システム最大値一覧」（P.24）
コマンド設定事例集「1 VLAN 機能を使う」（P.8）
Web ユーザーズガイド「2.5 VLAN 設定」（P.27）

# 2.8　リンクアグリゲーション機能

**適用機種**　全機種

リンクアグリゲーション機能とは、複数のポートを多重化し、1本の高速リンク（トランク・グループ）として扱うための機能です。この機能を使用すると、多重化されたリンク（メンバポート）の1本が故障した場合に、そのトラフィックをほかのメンバポートに分散することによって、リンクの冗長性を高めることができます。
リンクアグリゲーション機能は、マルチリンクイーサまたはポート・トランキングとも呼ばれます。
また、すべてのメンバポートが同じVLAN構成となるように設定してください。




トランク・グループへのトラフィックは、送信パケットのMACアドレスまたは、IPアドレスで判断し、負荷分散されます。
以下の方式から選択して指定することができます。

- 送信先MACアドレスと送信元MACアドレスを元にした負荷分散
- 送信先MACアドレスを元にした負荷分散
- 送信元MACアドレスを元にした負荷分散
- 送信先IPアドレスと送信元IP アドレスを元にした負荷分散
- 送信先IPアドレスを元にした負荷分散
- 送信元IPアドレスを元にした負荷分散

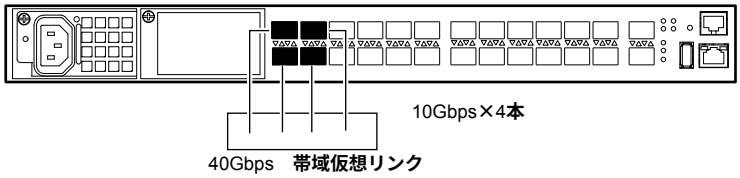
トランク・グループを通信可能とさせるまでの最小メンバポート数を指定することができます。
トランク・グループのメンバポートが指定した数だけ有効となるまでトランク・グループの通信を抑止します。
たとえば、リンクダウンしたメンバポートなどは有効なポートに含まれません。
冗長構成などでトランク・グループを必要な帯域が確保できるまで通信させたくない場合に使用します。
なお、この機能はLACPと併用することができます。

### こんな事に気をつけて

- **多重化されたポートは、論理的な1本のポートとして扱われます。STPやVLAN機能を併用した場合も同じです。**
- **多重化するポートは、必ず連続するポートで構成してください。**
- **ポートをオートネゴシエーションモードで使用した場合に、実際のリンク状態が半二重モードであったり、メンバポートの通信速度が異なるものが混在するときには、リンクアグリゲーションとして正常な動作を行いません。メンバポートが同一の速度で全二重モードとなるように、対向する装置の設定を変更してください。**
- **STPのコスト値は、メンバポートの帯域およびメンバー数より算出し、コスト値を割り当てます。縮退／復旧によってコストが変わることはありません。**
- **SR-X316T2/324T2/340TR1の場合は、MACアドレスを元にした負荷分散の場合、MACアドレスに加えてVLAN ID、イーサタイプの値も元にして負荷分散しています。**

# 2.8.1　LACP 機能

LACP 機能とは、IEEE802.3 準拠の LACP を利用したリンクアグリゲーションです。LACP を取り付けたシステム間で実現可能な最大レベルのリンクアグリゲーションを継続的に提供します。
LACP の利用によってリンクアグリゲーションの整合性確認や、リンクの正常性確認、障害検知の確度を向上できます。




## 導入のメリット

- 隣接装置と整合性を確認するので、たとえば、ポートを差し間違えていたといったようなミスがあった場合でも、プロトコルレベルで一本一本正しいリンク先に接続されていることを確認しながら通信を開始します。そのため誤った接続先へ通信してしまうことがありません。
- 隣接装置からの LACP パケットが一定時間受信されない場合は、リンク異常と判断するので、装置ポートの異常検出範囲を超えたリンクの障害検知が可能です。
- ポートがオートネゴシエーションに設定された場合であっても、接続が半二重であったり回線速度が異なるリンクをリンクアグリゲーションのトランク・グループに含めません。

☛ 参照 「2.8 リンクアグリゲーション機能」（P.32）

### こんな事に気をつけて

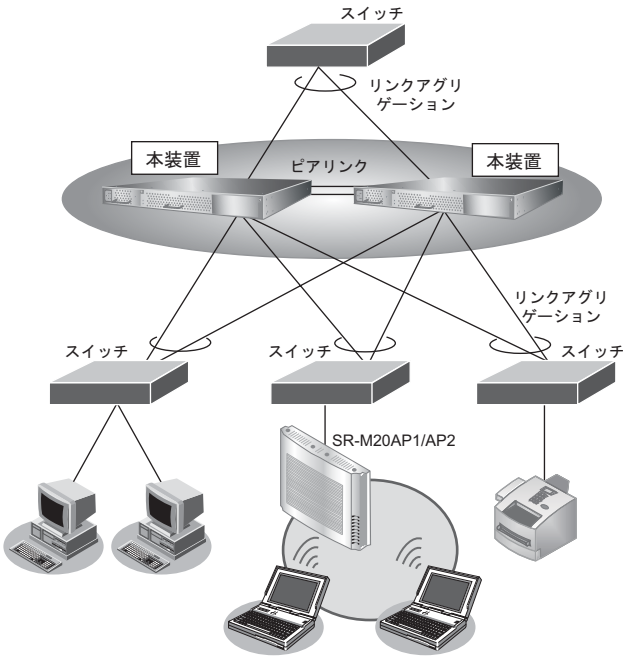
- **LACP を利用したリンクアグリゲーションは、接続先も LACP を有効にする必要があります。**
  **接続先のリンクアグリゲーション動作モードに、static が指定されている場合などの LACP 以外のリンクアグリゲーションとは接続できません。**
- **リンクアグリゲーション動作モードに passive を指定して、接続先も同様に passive とするとリンクアグリゲーションは構成されません。どちらか一方は active と指定してください。**
  **双方を active と指定してもかまいません。**
  **その他の注意事項については、「2.8 リンクアグリゲーション機能」（P.32）を参照してください。**

# 2.9　MLAG 機能

適用機種　***SR-X340TR1***

MLAG（Multi-Chassis Link Aggregation）とは、2 台の装置をまたいだリンクアグリゲーションを実現する機能です。

ループフリーなネットワーク冗長化が可能となり、帯域もフルに有効使用できます。




こんな事に気をつけて

- MLAG 機能を有効にするには、save コマンドによる構成定義の保存と装置の再起動が必要です。
- MLAG を構成する 2 台の装置は、同一機種間のみ接続可能です。異なる機種間での接続はできません。
- MLAG を構成する装置間を接続するピアリンクポートには以下の条件があります。
  - 10Gbps ポートのみ最大 2 ポートまで使用可能です。両装置で同一の設定としてください。
  - SR-X340TR1 では、ether41 と 42、または ether43 と 44 の組み合わせから選択してください。
- ピアリンクポートは 2 ポート設定することでリンクアグリゲーションとして動作します。冗長化および通信帯域の確保のため 2 ポート設定することを推奨します。
- ピアリンクポートに設定された構成定義はすべて無効となります。ピアリンクポートの動作に必要な VLAN などの設定はすべて自動設定されます。
- MLAG を構成する装置間の MLAG 構成定義は、以下の内容で設定してください。
  定義に不備がある場合、MLAG 接続に失敗します。復旧には構成定義の変更と装置再起動が必要となります。
  - 同一ドメイン ID を設定
  - 異なる装置 ID をそれぞれ設定
  - 装置間を接続するピアリンクポートを最大 2 ポートまでで設定
- MLAG を構成する装置の構成定義情報は、装置ごとに設定を行う必要があります。そのため、MLAG 構成装置で IP ホスト機能を利用する場合は、管理用 IP アドレスをそれぞれに設定します。
- MLAG を利用するリンクアグリゲーションは両装置で同一のグループ番号を設定してください。
  また、以下の条件で設定してください。定義に不備がある場合、MLAG インタフェースはアップしません。
  - 動作モード（Static/LACP）を同一に設定
  - 負荷分散アルゴリズムを同一に設定
  - グループメンバポートは両装置の合計で 8 ポートまでとなるように設定
  - グループメンバポートの通信速度および VLAN を同一に設定
- ピアリンクポートがリンクアップしていない、または MLAG 接続に異常があるなどの理由で、MLAG 装置間の通信が不可能となった場合でもそれぞれのリンクアグリゲーションは動作継続されます。ただし、本装置へのアクセスなどでピアリンクを経由している通信は停止となる場合があります。

- **本装置の MLAG ではピアリンクのトラフィックを最小限に抑制するため、自装置の MLAG 構成ポートがすべて通信不可能な状態となった場合のみ、ピアリンクを介したパケット転送を実施します。**
- **MLAG を構成する装置間で MAC 学習エントリの同期処理は実施しないため、MAC 学習エントリの状態が装置間で異なる場合があります。**

## 他機能との併用について

MLAG 機能と併用できない、または制限事項がある機能があります。

以下に併用に制限のあるものを示します。

○：使用できる、×：使用できない

| 機能 | MLAG ポート | 通常ポート | 制限事項 |
|---|---|---|---|
| STP 機能 | × | × | |
| バックアップポート機能 | × | × | 装置で同時に使用できません。 |
| IGMP スヌープ機能 | × | × | |
| MAC テーブルフラッシュ機能 | × | × | |
| etherL3 監視機能 | × | ○ | MLAG 構成ポートで使用できません。 |
| MAC フィルタ／IP フィルタ／優先制御情報書き換え機能 | ○ | ○ | MLAG 使用時は両装置に同一定義を設定してください。なお、ピアリンクポートへの設定は無効となります。 |
| ポート・ミラーリング機能 | ○ | ○ | ピアリンクポートのソースポート設定は無効となります。 |
| スタティック MAC フォワーディング機能 | ○ | ○ | ピアリンクポートへは適用されません。 |

# 2.10 バックアップポート機能

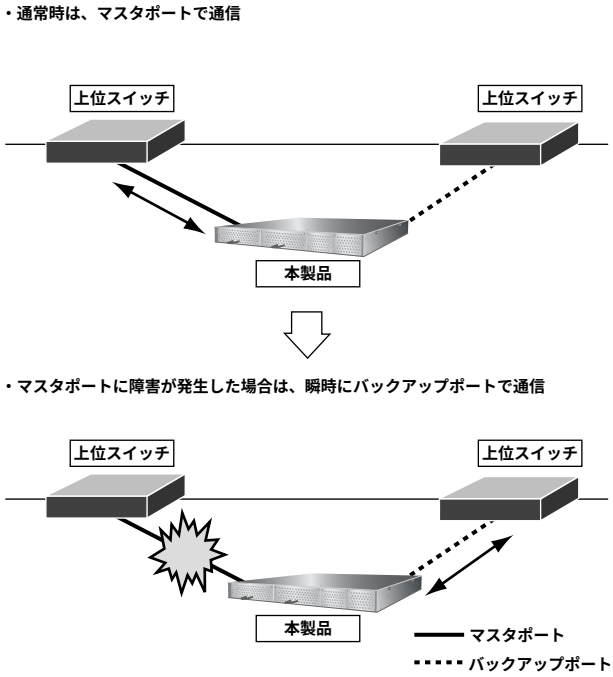
**適用機種**　全機種

バックアップポート機能とは、2つのポートをグループ化し、片方のポートをマスタポート（優先ポート）、もう一方のポートをバックアップポート（待機ポート）として管理し、常にどちらか一方のポートだけを稼動させる機能です。

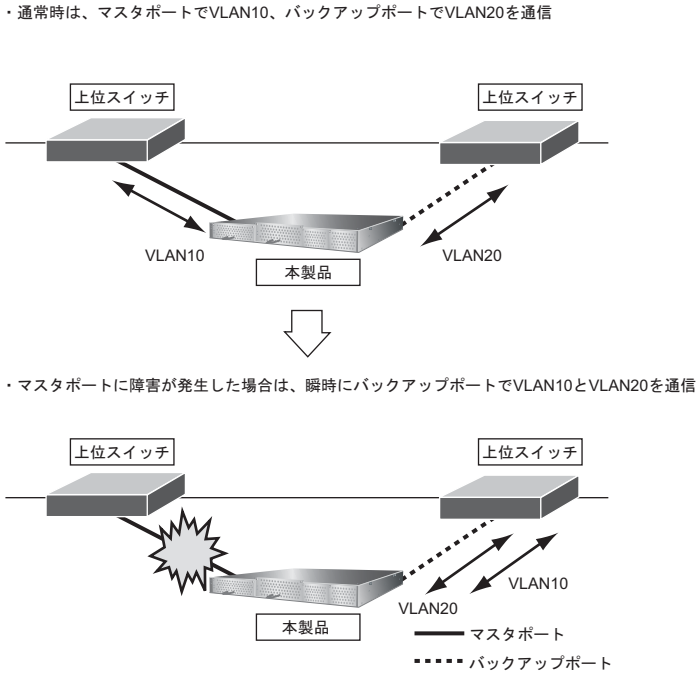
稼動中のポートになんらかの障害が発生した場合に、もう一方の待機ポートを瞬時に稼動ポートに切り替えることで、ネットワーク障害の影響を最小限に抑えることができます。

本機能では以下の3つの動作モードが選択できます。

- master モード
  マスタポートとバックアップポートの両方が使用可能な場合にマスタポートを優先使用します。
- earlier モード
  マスタポートとバックアップポートの両方が使用可能な場合に先に使用可能となったポートを使用します。



- vlan-based モード
  マスタポートとバックアップポートにそれぞれ異なる VLAN を設定し、VLAN ごとに両方のポートを同時に使用します。なお、どちらか一方のポートに障害が発生した場合は、もう一方のポートが両方の VLAN 通信を実施します。




## こんな事に気をつけて

- **バックアップポート機能では、障害発生時に稼動ポートを瞬時に切り替えることが可能ですが、各種プロトコルを使用した場合、通信が復旧するまでに各プロトコルでの復旧時間が必要となります。**
- **切替通知フレームを受信する上位スイッチが正しく MAC アドレスを再学習するために最適な切替通知フレームの送信条件は、上位スイッチの仕様に依存します。本機能を利用する際は、必ず実機確認を行い最適な送信条件を事前に確認してください。**
- **ループ検出などのポートを閉塞する機能と併用した場合に、稼動ポートが閉塞されれば切り替わりが発生します。**
- **リンクアグリゲーションと併用した場合で、そのリンクアグリゲーションがバックアップ構成として不整合な設定であった場合は、リンクアグリゲーションとしても無効となります。**
- **待機ポートの待機状態を offline と設定した場合、待機ポートはリンクダウンしているため、回線抜けなどの異常が発生しても検出はできません。切り替わり動作後に異常検出となります。**
- **vlan-based モードでは STP 機能と同時に使用できません。**
- **SR-X340TR1 で MLAG 機能を使用する場合、本機能は使用できません。**
- **vlan-based モードではマスタポートとバックアップポートに異なる Tagged VLAN だけを設定できます。**
  **Tagged VLAN が未設定、または Untagged VLAN が設定された場合はバックアップポートは使用できません。**

# 稼動ポートの切替通知

バックアップポートの稼動ポートに切り替えが発生した際に、接続装置の MAC アドレス学習テーブルの情報を更新させるための切替通知フレームを送信できます。

切替通知フレームの送信レートなどは上位スイッチの学習性能に合わせて調整できます。

切替通知は以下の 2 つの動作モードから選択できます。

- FDB-table モード
  本装置の MAC アドレス学習テーブル情報より以下の条件に合致するエントリを検索し、該当 MAC アドレスを送信元 MAC アドレスに設定した切替通知フレームを送信します。
  - 切り替えが発生した稼動ポートの VLAN で、当該バックアップグループ以外のポートで学習されているエントリ
- MAC-flush モード
  構成定義された任意の MAC アドレス（省略時は自装置 MAC アドレス）を送信元 MAC アドレスに設定した切替通知フレームを、切り替えが発生した稼動ポートの VLAN ごとに送信します。

補足 バックアップポート接続された上位装置が MAC テーブルフラッシュ機能を有効とした SR-X シリーズであることを想定した動作モードです。ただし、上位装置が SR-X526R1 の場合は、MAC テーブルフラッシュ機能の動作契機が最大で 20 秒程度遅延することがあるため、注意してください。

MAC テーブルフラッシュ機能については、「2.6 MAC アドレス学習／MAC フォワーディング機能」（P.27）を参照してください。

## こんな事に気をつけて

**切替通知フレームは、送出先となる稼動ポートの VLAN 設定が、タグなしの場合は Untagged フレーム、タグありの場合は Tagged フレームで送信します。ただしプロトコル VLAN の場合は送出しません。**

# 2.11 STP 機能

**適用機種**　全機種

STP 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。

**こんな事に気をつけて**

**SR-X340TR1 で MLAG 機能を使用する場合、本機能は使用できません。**

本装置では、以下の機能をサポートしています。

## 2.11.1 STP

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持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持つブリッジ（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**

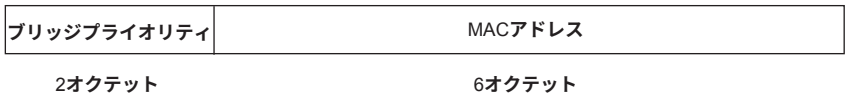
- **ルートポート**
  **フォワーディング状態のポートであり、各ブリッジで最小のルートパスコストのポートがルートポートとなります。ルートポートは、それぞれのブリッジに必ず 1 つ存在します。**
- **代表ポート**
  **フォワーディング状態のポートです。1 つの LAN 上に複数接続したポートの中に 1 つだけ存在します。ルートブリッジのすべてのポートは、接続された LAN 上の代表ポート（代表ブリッジ）となります。**
- **ブロッキングポート**
  **ブロッキング状態のポートであり、MAC フレームは中継しません。ルートポートでも代表ポートでもないポートがブロッキング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

  **＜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持つ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持ちます。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。

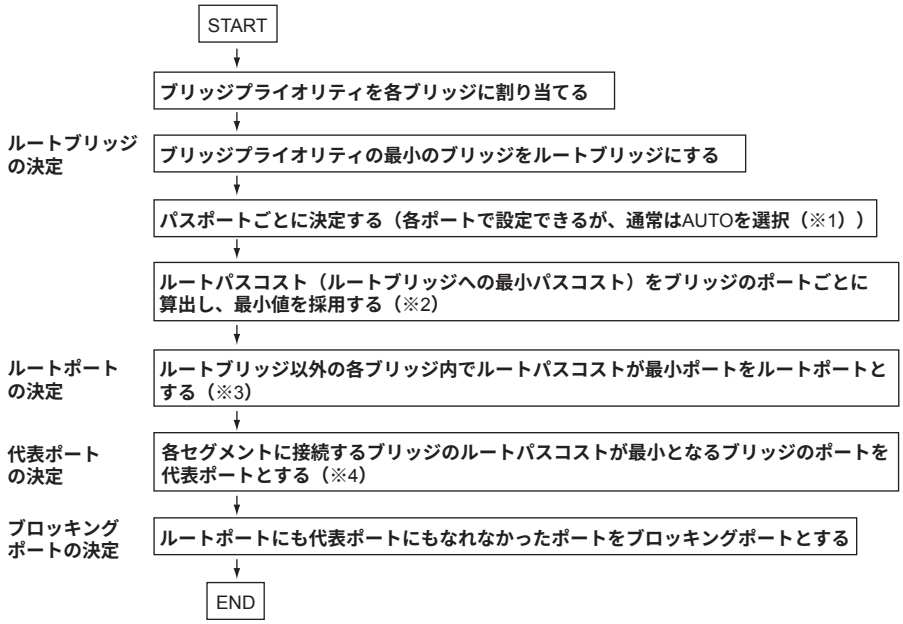
参照「＜ルートパスコストの算出＞」（P.47）

- 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はSTP動作を行わず、ツリーを構成しません。
  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<br>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<br>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<br>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<br>送信する | |
| | ラーニング状態 | しない | する | 受信する<br>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）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 |
|---|---|
| 10M | 2000000 |
| 100M | 200000 |
| 1G | 20000 |
| 10G | 2000 |

リンクアグリゲーションの場合は、伝送速度が 10M の場合は 200000 に、100M の場合は 20000 に、1G の場合は 2000 に、10G の場合は 200 になります。

※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、ブリッジごとに 1 つ存在します。

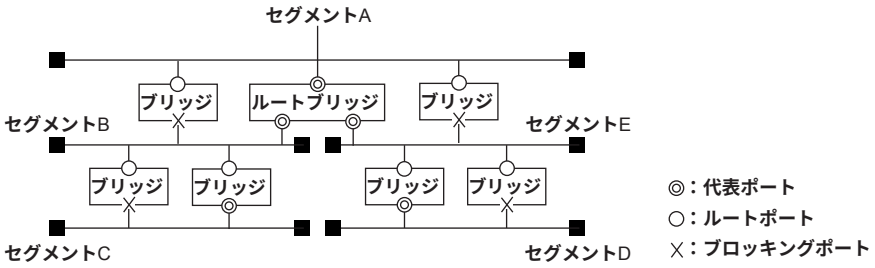
・ルートパスコストが同じ場合、ポート識別子が小さいポートを採用します。

※4）・代表ポートは、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。

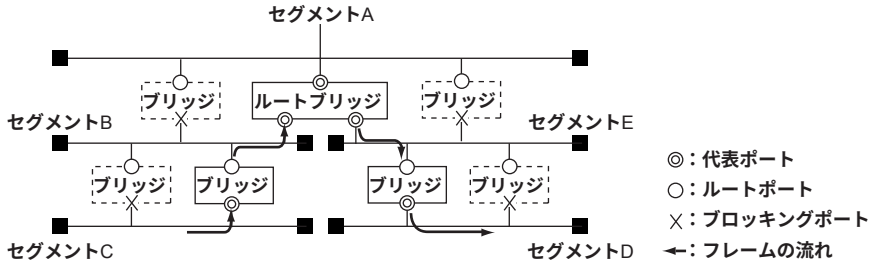



## スパニングツリーでのフレームの流れ

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持つブリッジ（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。ルートポートを持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。

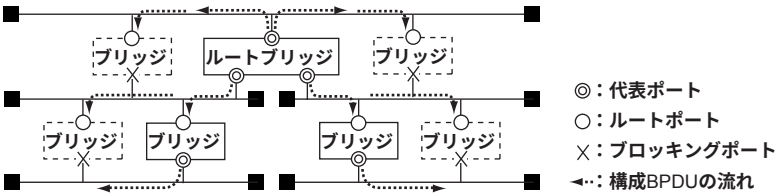



※）[ ] のブリッジは通信経路として使用されません

### 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 を持っており、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

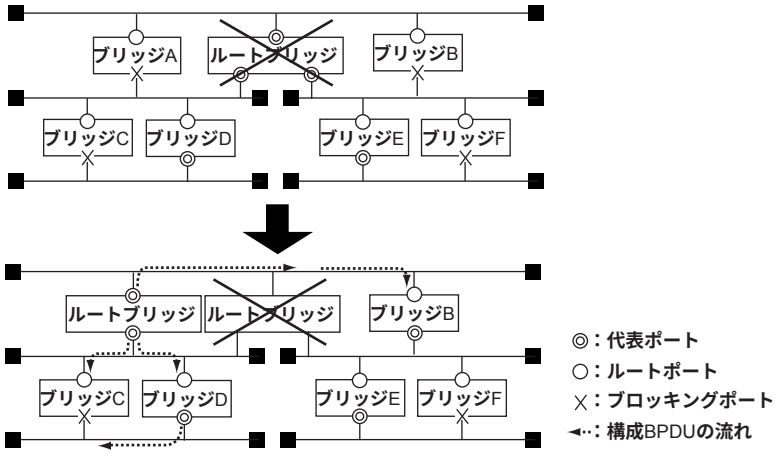
スパニングツリーのツリー構造は、構成 BPDU で維持します。以下のような原因により、タイマ値 STP bridge Max age（推奨値 20 秒）以内に、この構成 BPDU が下流のブリッジに届かなかった場合、ブリッジは障害と判断し、ツリー構造を再構成します。

- 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持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

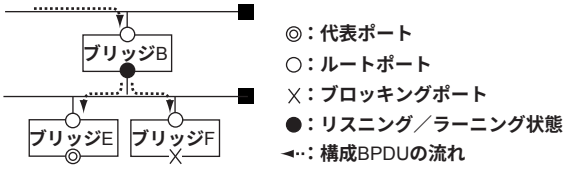
ツリー構造の再構成にともない、ブロッキングしているポートが中継できる状態に変化します。しかし、すべてのブリッジに新しい構成 BPDU が届いていない状態で、1 部のブリッジのポート状態が変化すると、ループ状態となることがあります。そのため、ポートがブロッキング状態からフォワーディング状態に切り替わる間、中間的なポート状態を置き、すべてのブリッジのツリー構成情報を更新し、ツリー構造が確立するのを待ちます。

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＞

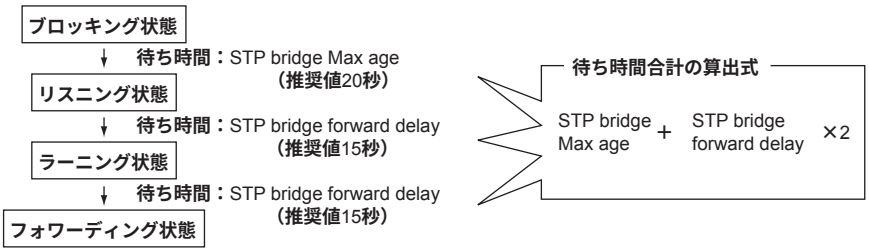
- リスニング状態
  MAC フレームを中継しません。また、MAC アドレス情報の学習を行いません。構成 BPDU を受信します。必要であれば送信します。
- ラーニング状態
  MAC フレームを中継しませんが、MAC アドレス情報の学習は行います。構成 BPDU を受信します。必要であれば送信します。

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 priority） | 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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>STP ドメインを分離すると、そのポートから構成 BPDU の送信を停止します。<br>STP ドメインを分離する設定にしたポートは STP ツリーを構成しません。<br>ただし、構成 BPDU 以外のフレームは中継します。<br>ON ：STP ドメインを分離しない、<br>OFF：STP ドメインを分離する、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。

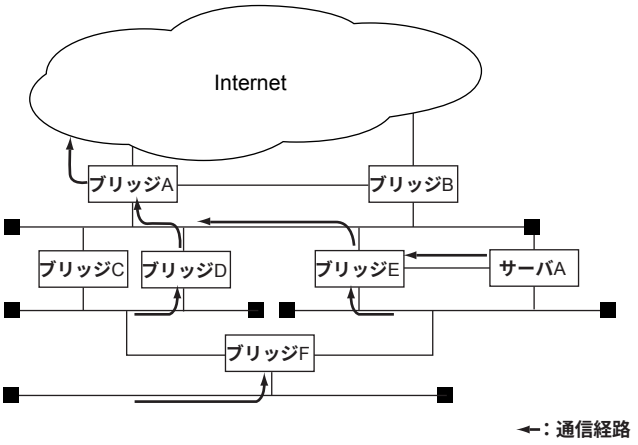
- 各セグメントのトラフィックが均一になるようにバックボーン（FDDI など）に近いブリッジをルートブリッジとします。
- むだなトラフィックがルートブリッジを経由しないようにエンドノートの配置に注意します。たとえば、常に通信しているような端末や大量のトラフィックを通信する端末はルートブリッジを経由しないように配置します。

＜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 に接続しているサーバ A は、ツリー構成に含む必要もなく、STP 動作を行う必要はないため、ブリッジ E のサーバ側のポートで STP 動作を無効にします。なお、Internet 側はツリー構成に入るブリッジが存在しないで、IP ルーティングによる L3 動作を行うため、ブリッジ A、ブリッジ B の Internet 側も STP 動作を無効にします。

＜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 Internet 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。

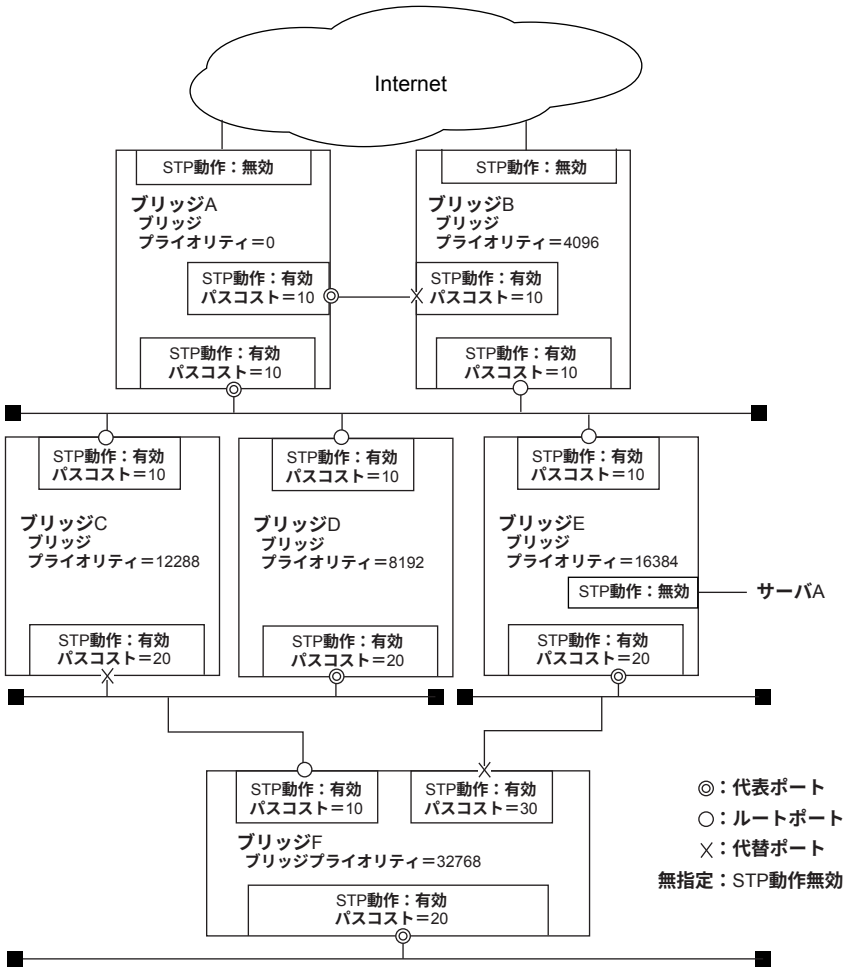
- 代表コスト
  そのポートが接続しているLAN上の代表ブリッジのルートパスコストです。構成BPDUの受信により、各ポートに自動的に設定されます。

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しないで、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。

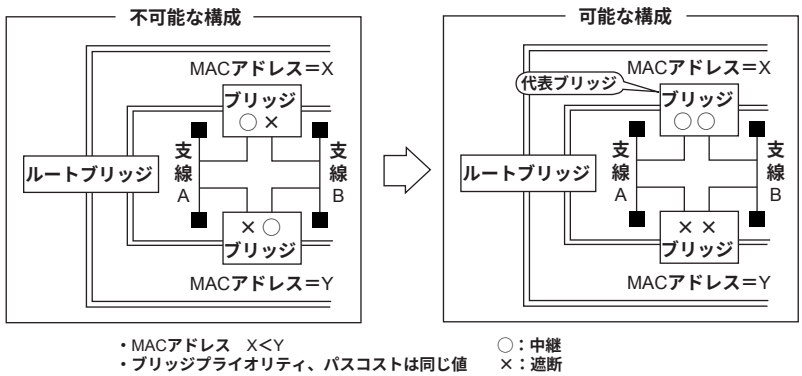
ブリッジFの左ポートのパスコストが10 + 10 = 20、右ポートのパスコストが10 + 30 = 40により、ブリッジFの左ポートがルートポートとなります。



## こんな事に気をつけて

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。

- 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 アドレスを持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。

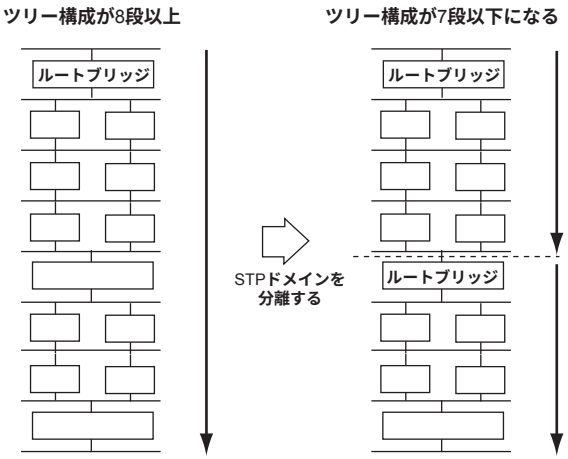



- 国際標準からのツリー構成
  国際標準では、ツリー構成の段数は最大 7 段をお勧めしています。これは、各性能に関するパラメタを推奨値（デフォルト値）で運用した場合にシステムがどのような条件で運用しても、スパニングツリー機能が正常に動作することを保証できる値です。
  推奨値の最大 7 段は、以下の式より算出できます。

| |
|---|
| 最大寿命÷（Hello タイム＋構成メッセージの最大遅延時間）＋ 1<br>＝ 20÷（2 ＋ 1）＋ 1<br>≒ 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　コマンド設定事例集「8 STP 機能を使う」（P.32）

## 2.11.2　RSTP

STP の問題点として、最大で 50 秒の通信断が発生してしまう場合があります。その問題点を克服するために開発されたプロトコルが RSTP（ラピッドスパニングツリープロトコル）です。RSTP を使用するとスパニングツリーの再計算は 1 秒程度となり、瞬断レベルでの切り替えが可能になります。

また、RSTP は IEEE802.1w として標準化されており、従来の STP（IEEE802.1d）とは互換性があります。そのため STP との混在環境でも問題なく動作します。

### RSTP でのポートの役割

STP では各ポートの役割が以下のようになっています。

- 指定ポート
- ルートポート
- ブロッキングポート

RSTP では指定ポートおよびルートポートは、STP の場合と同じ役割として使われます。ブロッキングポートは、以下の 2 つの役割に分けて使われます。

- 代替ポート
  代替パスを提供するポート。ルートポートの次にコストが小さいポートで、ルートブリッジへの代替パスのポートになります。
- バックアップポート
  指定ポートが指定している経路の代替パスのポートです。1 つのスイッチで同一セグメントに対して 2 つ以上の接続を持つ場合に、その代替パスとして提供されます。

代替ポートおよびバックアップポートは、通常ブロッキング状態となります。

### RSTP でのポートの状態

STP では、ブロッキング状態、リスニング状態、ラーニング状態およびフォワーディング状態という 4 つのポート状態があります。ブロッキング状態とリスニング状態ではどちらも MAC フレームの中継は行いません。両者の違いは、ブロッキング状態では BPDU の送信を行わないの対して、リスニング状態では BPDU の送信を行うという点のみです。

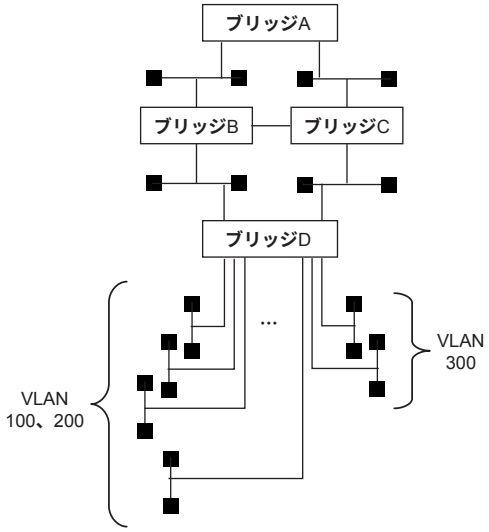
RSTP では、ブロッキング状態とリスニング状態をまとめてディスカーディング状態としています。

## 2.11.3　MSTP

物理的にループしているネットワークでも、VLANの構成によっては、論理的にループしない場合があります。STPではループと判断して、一方のLANを通信に使わないで動作しますが、MSTPではVLAN単位に扱うことができるため、STPよりも効率的にネットワーク内のデータを流すことができます。

以下のようなVLAN環境下でVLAN単位でフレームの制御を行う場合を考えます。

- ブリッジA～C
  すべての接続ポートでVLAN100および200、またはVLAN300をタグVLANとしている。
- ブリッジD
  ブリッジB、Cに接続しているポートは、VLAN100および200、またはVLAN300をタグVLANとしている。
  端末側は、ポートごとにVLAN設定が異なる場合に、MSTPを使用してVLAN単位でロードバランシング（ブリッジA-ブリッジB間は1Gで、ブリッジA-ブリッジC間は100Mのような場合）を行う。




インスタンス0

- ブリッジの優先順位　　：A→B→C→D

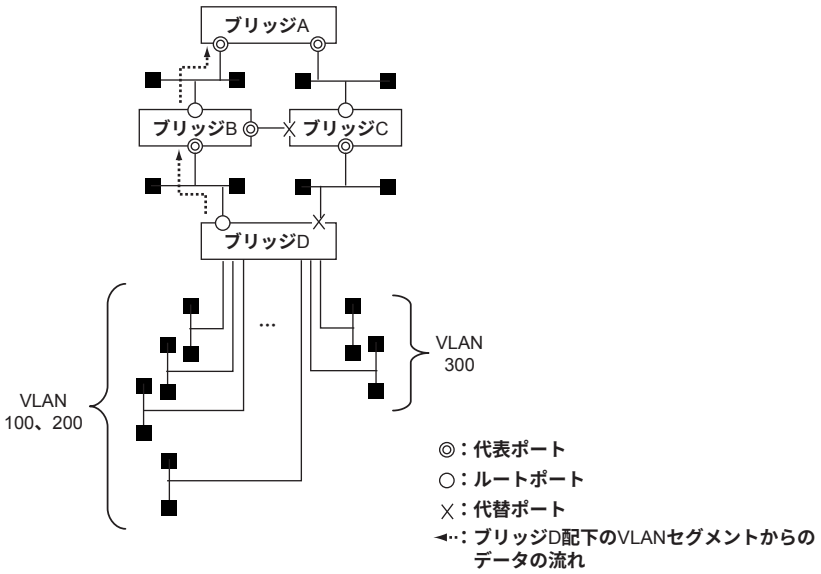
インスタンス1

- ブリッジの優先順位　　：A→B→C→D
- VLAN割り当て　　：100、200

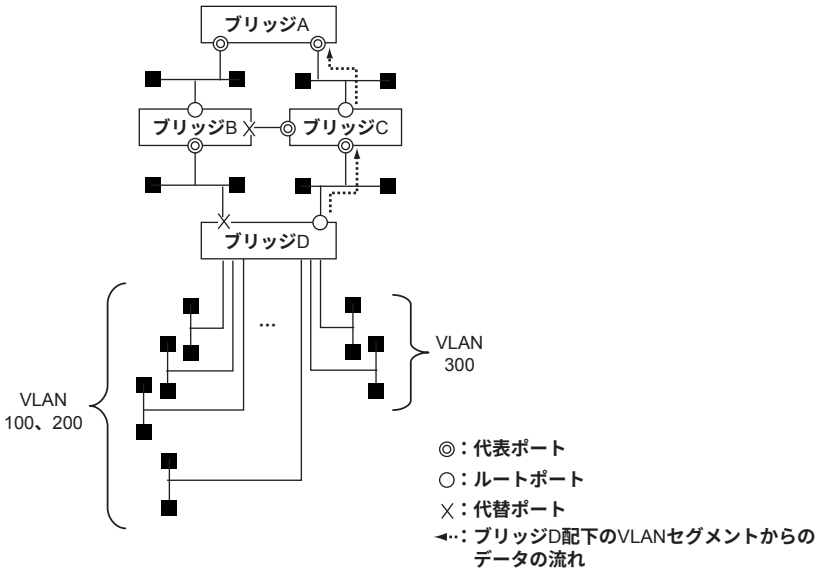
インスタンス2

- ブリッジの優先順位　　：A→C→B→D
- VLAN割り当て　　：300

## インスタンス 1 でのスパンニングツリーと VLAN100、200 のデータの流れ

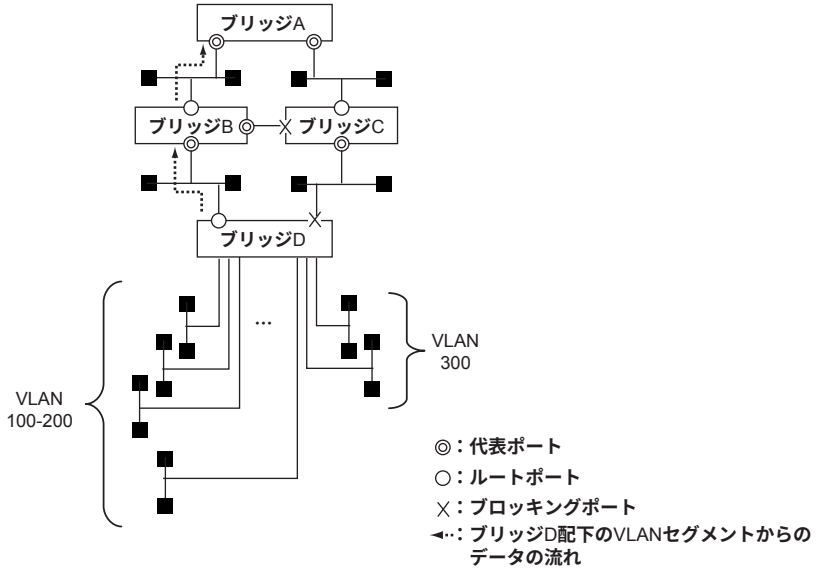



## インスタンス 2 でのスパンニングツリーと VLAN300 のデータの流れ



MSTP を使用すると、「インスタンス 1 でのスパンニングツリーと VLAN100、200 のデータの流れ」、「インスタンス 2 でのスパンニングツリーと VLAN300 のデータの流れ」のように VLAN 単位でのロードバランシングか可能ですが、STP のみの場合は、以下のように VLAN に関係なくスパニングツリーが作成されるためデータが偏ります。

## STP を使った場合の VLAN100 および 200、または VLAN300 を使用したフレームの流れ



# 2.12 LLDP機能

**適用機種**　全機種

LLDP（Link Layer Discovery Protocol）とは、自装置情報を広報することにより隣接装置の把握や接続状態の確認などを目的とした隣接探索プロトコルです。
LLDP情報は、同一物理LANに接続された装置にだけ届き、ルータを超えた先には届きません。

本装置のLLDP機能はIEEE802.1ABに準拠し、以下に示す機能を提供します。

- 自装置情報をLLDPで送信
- LLDPで受信した隣接装置情報を保持
- LLDPに関する情報をMIBとして管理し、SNMP機能でMIBを取得
- 隣接情報が更新されたことをSNMPトラップで通知
- LLDP設定情報、自装置情報、隣接装置情報、統計情報を表示

本装置から送信するLLDP情報には以下に示す情報を含めます。オプション情報は、送信しないように指示することができます。実際に送信される内容は、コマンドやWeb画面で確認できます。

- 装置識別情報（代表MACアドレス）　（必須）
- 物理ポート識別情報（ifIndex MIB）　（必須）
- 保持時間情報（TTL）　（必須）
- 物理ポート解説情報（ifDescr MIB）　（オプション）
- 装置名称情報（sysName MIB）　（オプション）
- 装置解説情報（sysDescr MIB）　（オプション）
- 装置主要機能情報（スイッチ／ルータ）　（オプション）
- 物理ポート管理アドレス情報（MAC/IPv4/IPv6）（オプション）
- ポートVLAN ID情報　（オプション）
- プロトコルVLAN ID情報　（オプション）
- VLAN名称情報　（オプション）
- プロトコルVLAN種別情報　（オプション）
- 物理ポート設定情報　（オプション）
- 物理ポート電源供給情報　（オプション）
- リンクアグリゲーション情報　（オプション）
- 最大フレームサイズ情報　（オプション）

隣接装置から受信したLLDP情報は、LLDP情報に含まれている保持時間が経過するまで保持します。保持している隣接情報は、コマンドやWeb画面で確認できます。

本装置で保持できる隣接情報の最大数を以下に示します。最大保持数を超えたために保持できなかった情報は破棄し、統計情報に破棄したことを計数します。

| 条件 | 保持数 | SR-X 316T2 | SR-X 324T2 | SR-X 340TR1 | SR-X 526R1 |
|---|---|---|---|---|---|
| 装置全体での最大保持数 | 物理ポート数＋装置全体での共用保持数 | 16+224 | 24+336 | 44+616 | 26+364 |
| 1 ポートでの最低保証保持数 | 1 台分 | 1 | 1 | 1 | 1 |
| 装置全体での共用保持数 | 物理ポート数 ×14 台分 | 224 | 336 | 616 | 364 |
| 1 ポートでの最大保持数（※） | 1 台分＋物理ポート数 ×14 台分 | 225 | 337 | 617 | 365 |

※）1 ポートで共用分をすべて保持した場合（ほかのポートでは 1 台分しか保持できない）

# 2.13 MACフィルタ機能

**適用機種**　全機種

MAC フィルタ機能では、本装置を経由するパケットを MAC アドレス、パケット形式、VLAN ID、COS 値、IP アドレス、ポート番号など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、ネットワークへの負荷を軽減することができます。

本装置を通過したパケットが ACL 内の "acl mac" 定義、"acl vlan" 定義、"acl ip" 定義、"acl tcp" 定義、"acl udp" 定義、および "acl icmp" 定義に該当した場合に MAC フィルタ処理が動作します。

## MAC フィルタの条件

以下の条件を指定することによって、パケットデータの流れを制御できます。

- パケット入力ポート
  フィルタ処理の対象となるパケット入力 ETHER ポート
- 動作
  フィルタ処理の対象となるパケットが入力 ETHER ポートに入力された場合の動作（遮断または透過）
- ACL 番号
  MAC フィルタの条件となるパケットパターンを定義した ACL 番号

## MAC フィルタ機能の適用範囲

MAC フィルタ機能では、ACL で指定したパケットパターンのフィルタを以下の単位で適用指定できます。

- ETHER ポート
  ether コマンドで設定します。ETHER ポートに対して、指定した ACL のパケットパターンに一致した入力パケットに対して、フィルタ処理を実施します。
- VLAN
  vlan コマンドで設定します。VLAN に属する ETHER ポートに対して、指定した ACL のパケットパターンに一致した入力パケットに対して、フィルタ処理を実施します。同一 VLAN 内のすべての ETHER ポートに適用する場合に使用します。

**こんな事に気をつけて**

**SR-X526R1 では以下のフレームは ACL 対象となりません。**

- **"acl mac llc" 定義を適用した場合の VLAN タグ付きの llc フレーム**
- **プロトコル VLAN が適用されたフレーム**

# 装置に設定可能な上限

**適用機種**　***SR-X316T2, 324T2, 340TR1***

装置に設定可能な上限を以下に示します。

- ACL による上限：128 個
  "ether macfilter"、"vlan macfilter"、および "lan ip filter" コマンド合わせて装置全体で 128 個まで設定可能です。
  コマンドの適用優先順は、"ether macfilter"、"vlan macfilter"、"lan ip filter" コマンドの順番です。
  また、ether ポート間の優先順位は ether ポート番号が小さいほうが高くなり、VLAN 間の優先順位は VLAN ID が小さいほうが高くなります。
  したがって、ETHER1 ポートに "ether macfilter" コマンドが 128 個まで設定されていた場合、以降の "vlan macfilter"、"lan ip filter" コマンドは適用されません。
- rule による上限：128 個
  "ether macfilter"、"vlan macfilter"、および "lan ip filter" コマンド合わせて装置全体で 128 個まで設定可能です。
  それぞれの ACL のルール数は、以下の計算式によって求められます。
  - TCP または UDP を設定する ACL の場合：TCP または UDP の送信元ポート数とあて先ポート数の掛算の結果
  - ICMP を設定する ACL の場合：ICMP の ICMP TYPE と ICMP CODE のそれぞれの個数の掛算の結果
  - TCP/UDP/ICMP を設定しない ACL の場合：1

### こんな事に気をつけて

- **MAC フィルタの対象となるのは本装置に入力されたパケットです。本装置より出力されるパケットは対象となりません。**
- **装置の設定可能上限を超えた場合は適用されません。**
- **SR-X340TR1 では、**"ether macfilter"、"ether qos aclmap"、"vlan macfilter"、"vlan qos aclmap"、"lan ip filter"、"lan ip dscp"、"serverinfo filter" **コマンドなどの** ACL **を参照する定義は装置全体で** 400 **個まで設定可能です。**
- **SR-X316T2/324T2 では、**"ether macfilter"、"vlan macfilter"、"lan ip filter"、"serverinfo filter" **コマンドなどの** ACL **を参照する定義は装置全体で** 200 **個まで設定可能です。**

**適用機種**　***SR-X526R1***

装置に設定可能な上限を以下に示します。

- 設定コマンドによる上限：装置全体で 64 個
  "ether macfilter"、"vlan macfilter"、"lan ip filter"、"ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp" コマンド合わせて装置全体で 64 個まで設定可能です。
  優先順位は、それぞれ以下のようになります。
  - コマンドの適用優先順は、"ether macfilter"、"vlan macfilter"、"lan ip filter"、"ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp" コマンドの順番です。
  - ether ポート間の優先順位は、ether ポート番号が小さいほうが高くなります。
  - VLAN 間の優先順位は、VLAN ID が小さいほうが高くなります。
  - lan 間の優先順位は、lan 定義番号が小さいほうが高くなります。

- マスク数による上限：装置全体で 64 個
  "ether macfilter"、"vlan macfilter"、"lan ip filter"、"ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp"、"vlan protocol" コマンド合わせて装置全体で 64 マスクまで設定可能です。
  優先順位は、それぞれ以下のようになります。
  - コマンドの適用優先順は、"vlan protocol"、"ether macfilter"、"vlan macfilter"、"lan ip filter"、"ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp" コマンドの順番です。
  - ether ポート間の優先順位は、ether ポート番号が小さいほうが高くなります。

- VLAN 間の優先順位は、VLAN ID が小さいほうが高くなります。
- lan 間の優先順位は lan 定義番号が小さいほうが高くなります。

"ether macfilter"、"vlan macfilter"、"lan ip filter"、"ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp" コマンドが消費するマスク数は、適用する acl によって以下のようになります。

複数の acl を適用する場合はそれぞれの合計となりますが、組み合わせによりそれぞれの合計以下となることがあります。

| 適用する acl の条件 | マスク数 |
|---|---|
| acl mac 定義の場合 | |
| 　llc の LSAP を指定する場合 | 3 |
| 　llc の LSAP を指定しない場合 | 1 |
| acl vlan 定義の場合 | 1 |
| acl ip 定義の場合 | |
| 　srcIP アドレスを指定しない場合 | |
| 　　tos 値 /dscp 値を指定しない場合 | 1 |
| 　　tos 値 /dscp 値を指定する場合 | 3 |
| 　srcIP アドレスを指定する場合 | |
| 　　dstIP アドレスを指定しない場合 | 1 |
| 　　dstIP アドレスを指定する場合 | |
| 　　　srcIP と dstIP のマスク値が同じ場合 | |
| 　　　　tos 値 /dscp 値を指定しない場合 | 1 |
| 　　　　tos 値 /dscp 値を指定する場合 | 3 |
| 　　　srcIP と dstIP のマスク値が異なる場合 | 3 |

"vlan protocol" コマンドが消費するマスク数は、以下のようになります。

| 適用する acl の条件 | マスク数 |
|---|---|
| プロトコル VLAN 定義の場合 | |
| 　vlan protocol ipv4 を指定する場合 | 3 |
| 　vlan protocol ipv6 を指定する場合 | 1 |
| 　vlan protocol <count> ether を指定する場合 | 1 |
| 　vlan protocol <count> llc を指定する場合 | 1 |

- アクション数による上限：装置全体で 16 個
  "ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp"、"vlan protocol" コマンド合わせて装置全体で 16 アクションまで設定可能です。
  優先順位は、それぞれ以下のようになります。
  - コマンドの適用優先順は、"vlan protocol"、"ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp" コマンドの順番です。
  - ether ポート間の優先順位は、ether ポート番号が小さいほうが高くなります。
  - VLAN 間の優先順位は、VLAN ID が小さいほうが高くなります。
  - lan 間の優先順位は、lan 定義番号が小さいほうが高くなります。

以下のコマンドが設定されている場合に 1 アクションが消費されますが、コマンドの指定数にかかわらず 1 アクションのみ消費されます。

- vlan <vid> protocol ipv4
- vlan <vid> protocol ipv6

以下のコマンドが設定されている場合に 1 アクションが消費されます。
<tos_value>、<dscp_value>、<queue_value> が同じ場合は、コマンドの指定数にかかわらず 1 アクションのみ消費されます。

- ether <number> qos aclmap <count> tos <tos_value> <acl>
- ether <number >qos aclmap <count> dscp <dscp_value> <acl>
- ether <number> qos aclmap <count> queue <queue_value> <acl>
- vlan <vid> qos aclmap <count> tos <tos_value> <acl>
- vlan <vid> qos aclmap <count> dscp <dscp_value> <acl>
- vlan <vid> qos aclmap <count> queue <queue_value> <acl>
- lan <number> ip dscp <count> acl <acl_count> <dscp_value>

以下のコマンドが設定されている場合に 1 アクションが消費されます。
<vid> が同じ場合は、コマンドの指定数にかかわらず 1 アクションのみ消費されます。

- vlan <vid> protocol <count> ether
- vlan <vid> protocol <count> llc

### こんな事に気をつけて

**MAC フィルタの対象となるのは本装置に入力されたパケットです。本装置から出力されるパケットは対象となりません。**

# 2.14 QoS 機能

**適用機種**　全機種

Qos 機能とは、優先制御や優先制御の書き換えを行って、通信の品質を確保する機能です。

以下に、優先制御機能と優先制御書き換え機能について説明します。

## 2.14.1 優先制御機能

優先制御機能とは、パケットをキューイングし、対応付けされたキューの優先度に従って出力する機能です。

優先制御機能は、VLAN 機能のユーザプライオリティ値と本装置内部のキューを対応付けることで処理されます。

パケットは一度、出力ポート（自装置あてポート含む）の複数のキューにキューイングされ、優先制御方式に従って出力されます。キューはそれぞれ 0 ～ 7 の優先度を持っており、数字が大きくなるに従って優先度が上がります。優先制御方式は SR-X316T2/324T2/340TR1 では、Strict Priority Queuing（Strict）または Weighted Round Robin（WRR）、SR-X526R1 では、Strict Priority Queuing（Strict）または Deficit Round Robin（DRR）の 2 つから選択します。

また、本装置では、ユーザプライオリティ値と本装置内部のキューの対応付けを変更することもできます。

キューの数は SR-X316T2/324T2 の場合 4 個、SR-X340TR1/526R1 の場合 8 個です。

本装置でサポートする優先制御機能には、以下の種類があります。

**SR-X316T2/324T2 の場合**

- IEEE802.1p に準拠した CoS による優先制御
- タグなし受信パケットに対するデフォルトプライオリティによる優先制御

**SR-X340TR1 の場合**

- IEEE802.1p に準拠した CoS による優先制御
- タグなし受信パケットに対するデフォルトプライオリティによる優先制御
- ACL による出力キュー変更
- ACL による CoS 値の変更（変更後の CoS 値による優先制御が実行されます）
- ACL による IPv4 DSCP 値の変更
- ACL による TOS（IP Precedence）の変更

**SR-X526R1 の場合**

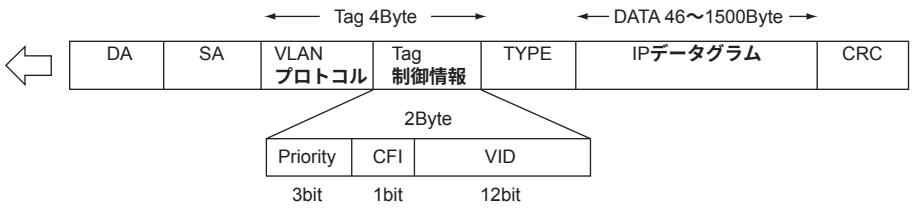
- IEEE802.1p に準拠した CoS による優先制御
- タグなし受信パケットに対するデフォルトプライオリティによる優先制御
- ACL による出力キュー変更
- ACL による IPv4 DSCP 値の変更
- ACL による TOS（IP Precedence）の変更

複数の種類の優先制御を同時に有効にした場合は、ACL による優先制御がもっとも優先され、次に CoS による優先制御、最後にタグなし受信パケットに対するデフォルトプライオリティによる優先制御の順に優先制御がなされます。

以下に、CoS 制御の場合に参照するフレーム内のフィールドを示します。

**CoS 制御**

VLAN タグ付きフレームフォーマット（IEEE802.1q）




【CoS制御】

## ユーザプライオリティ値と優先度の関係

本装置の初期設定および優先制御を行う場合のユーザプライオリティ値と装置内部のキューの推奨設定を、以下に示します。

### ● SR-X316T2/324T2 の場合

| ユーザプライオリティ値（Traffic type） | 本装置内部のキューの初期設定 | 優先制御を行う場合のキュー設定（推奨） |
|---|---|---|
| 0（Best Effort） | 1 | 1 |
| 1（Background） | 0 | 0 |
| 2（予備） | 0 | 0 |
| 3（Excellent effort） | 1 | 1 |
| 4（Controlled Load） | 2 | 2 |
| 5（Video） | 2 | 2 |
| 6（Voice） | 3 | 3 |
| 7（Network Control） | 3 | 3 |

### ● SR-X340TR1/526R1 の場合

| ユーザプライオリティ値（Traffic type） | 本装置内部のキューの初期設定 | 優先制御を行う場合のキュー設定（推奨） | |
|---|---|---|---|
| | | キュー 8 使用 | キュー 4 使用 |
| 0（Best Effort） | 2 | 2 | 1 |
| 1（Background） | 0 | 0 | 0 |
| 2（予備） | 1 | 1 | 0 |
| 3（Excellent effort） | 3 | 3 | 1 |
| 4（Controlled Load） | 4 | 4 | 2 |
| 5（Video） | 5 | 5 | 2 |
| 6（Voice） | 6 | 6 | 3 |
| 7（Network Control） | 7 | 7 | 3 |

# 優先制御の処理方法

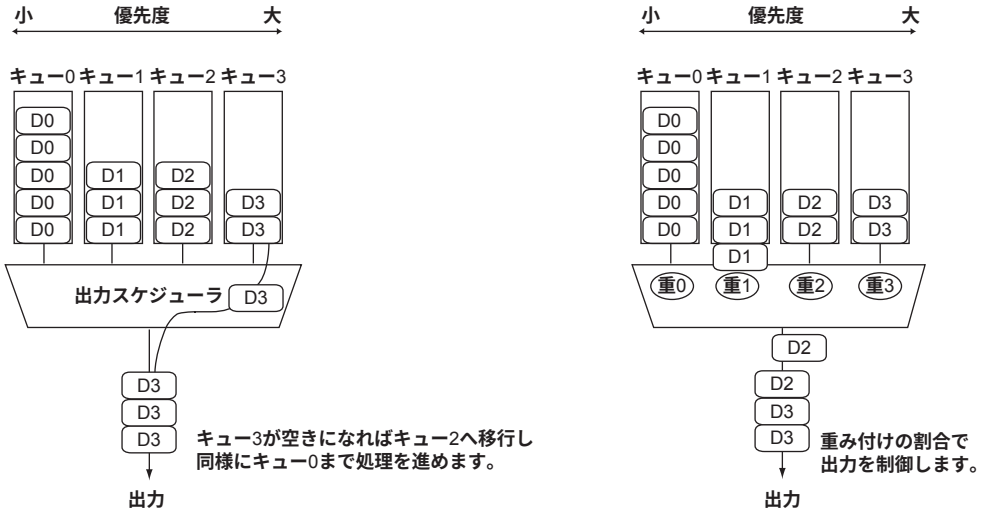
**適用機種**　***SR-X316T2, 324T2, 340TR1***

優先制御の処理には、StrictまたはWRRのどちらかを設定します。

- Strict　：優先度の高いキューのフレームを最優先に処理します。
- WRR　：キューごとに一定の数値（出力比）を設定し、相対的な優先制御を行います。たとえば、キュー7に10を、キュー0に1を設定した場合、キュー7とキュー0は10：1の割合で処理が行われます。

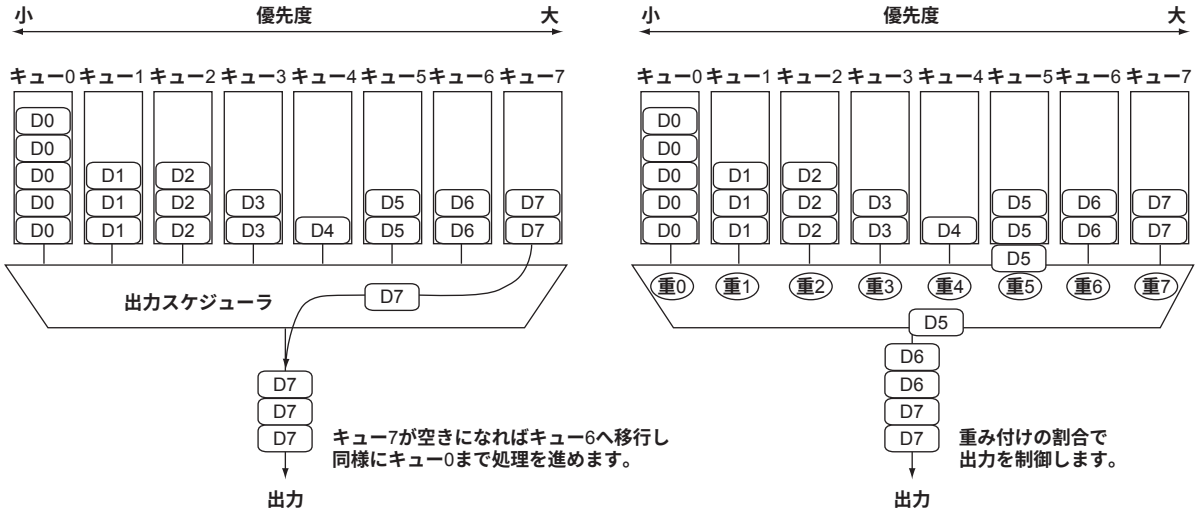
以下に、StrictとWRRの処理例を示します。

### ● SR-X316T2/324T2（キュー 4 使用）の場合




【Strict Priority Queuing】　【Weighted Round Robin】

### ● SR-X340TR1（キュー 8 使用）の場合



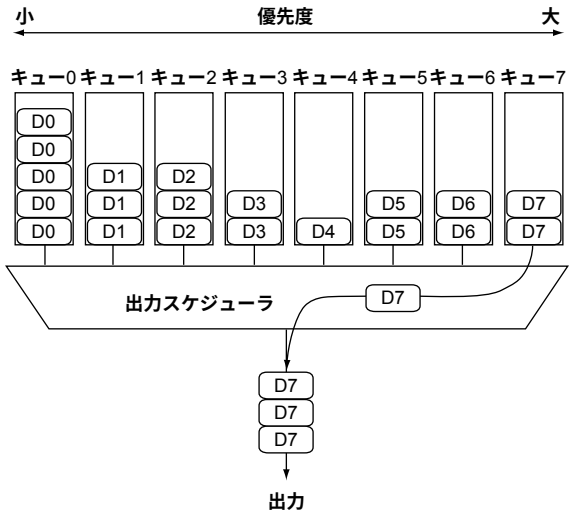

【Strict Priority Queuing】　【Weighted Round Robin】

**適用機種**　***SR-X526R1***

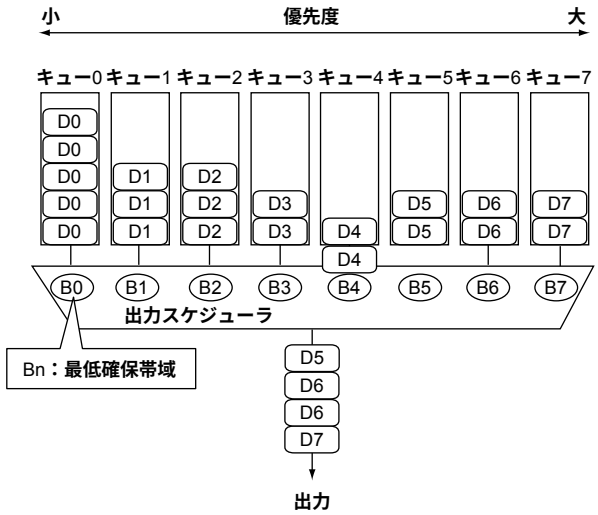
優先制御の処理には、StrictまたはDRRのどちらかを設定します。

- Strict　：優先度の高いキューのフレームを最優先に処理します。
- DRR　：キューごとに、最低限確保したい帯域幅を指定します。この指定に基づいて、装置内部で出力キューごとに出力を継続できるデータ量を決定します。その量以上となるパケットが出力されたらそのキューに出力待ちパケットがあっても次のキューの処理に移るようにします。各キューの帯域の合計は、ポートの最大帯域（10Gbps）になるように指定してください。

以下に、StrictとDRRの処理例を示します。




【Strict Priority Queuing】




【Deficit Round Robin】

# 2.14.2　優先制御情報書き換え機能

適用機種　***SR-X340TR1, 526R1***

優先制御情報書き換え機能では、本装置を経由するパケットのMACアドレス、パケット形式、VLAN ID、COS値、IPアドレス、ポート番号などの組み合わせに基づいて優先制御情報書き換えることができます。
本装置を通過したパケットがACL 内の"acl mac"定義、"acl vlan"定義、"acl ip"定義、"acl tcp"定義、"acl udp"定義、および"acl icmp"定義に該当した場合に優先制御情報が書き換えられます。

## 優先制御情報書き換え条件

以下の条件を指定することによって、優先制御情報の書き換えを制御できます。

- パケット入力ポート
  フィルタ処理の対象となるパケット入力ETHER ポート
- 書き換え優先制御情報
  - COS 値（VLAN 機能のユーザプライオリティ値）※SR-X340TR1 のIPv4 のみ
  - DSCP 値（IPパケットヘッダのTOS フィールドの上位6ビット）※IPv4 のみ
  - IP Precedence 値（IPヘッダのTOS フィールドの上位3ビット）※IPv4 のみ
  - 入力パケットが出力される際に使用される出力ポートのキュー（パケットは書き換えられません）
- ACL 番号
  優先制御情報書き換えの条件となるパケットパターンを定義したACL 番号

## 優先制御情報書き換え機能の適用範囲

優先制御情報書き換え機能では、ACL で指定したパケットパターンで優先制御情報を以下の単位で書き換え指定することができます。

- ETHER ポート
  ether コマンドで設定します。ETHER ポートに対して、指定したACL のパケットパターンに一致した入力パケットに対して、優先制御情報書き換え処理を実施します。
- VLAN
  vlan コマンドで設定します。VLAN に属するETHER ポートに対して、指定したACL のパケットパターンに一致した入力パケットに対して、優先制御情報書き換え処理を実施します。
  同一VLAN 内のすべてのETHER ポートに適用する場合に使用します。

**こんな事に気をつけて**

**SR-X526R1 では、以下のフレームはACL 対象になりません。**

- **"acl mac llc"定義を適用した場合のVLAN タグ付きのllc フレーム**
- **プロトコルVLAN が適用されたフレーム**
- **MAC フィルタ機能が適用されたフレーム**
- **IP フィルタリング機能が適用されたフレーム**
- **優先度の高い優先制御情報書き換え機能が適用されたフレーム**

# 装置に設定可能な上限

**適用機種**　***SR-X340TR1***

装置に設定可能な上限を以下に示します。

- ACL による上限：128 個
  "ether qos aclmap"、"vlan qos aclmap"、および "lan ip dscp" コマンド合わせて装置全体で 128 個まで設定可能です。
  コマンドの適用優先順は、"ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp" コマンドの順番です。
  また、ether ポート間の優先順位は ether ポート番号が小さいほうが高くなり、VLAN 間の優先順位は VLAN ID が　小さいほうが高くなります。
  したがって、ETHER1 ポートに "ether qos aclmap" コマンドが 128 個まで設定されていた場合、以降の "vlan qos aclmap"、"lan ip dscp" コマンドは適用されません。
- rule による上限：128 個
  "ether qos aclmap"、"vlan qos aclmap"、および "lan ip dscp" コマンド合わせて装置全体で 128 個まで設定可能です。
  それぞれの ACL のルール数は、以下の計算式によって求められます。
  - TCP または UDP を設定する ACL の場合：TCP または UDP の送信元ポート数とあて先ポート数の掛算の結果
  - ICMP を設定する ACL の場合：ICMP の ICMP TYPE と ICMP CODE のそれぞれの個数の掛算の結果
  - TCP/UDP/ICMP を設定しない ACL の場合：1

### こんな事に気をつけて

- **優先制御情報書き換えの対象となるのは本装置に入力されたパケットです。本装置より出力されるパケットは対象となりません。**
- **装置の設定可能上限を超えた場合は適用されません。**
- **ether macfilter"、"ether qos aclmap"、"vlan macfilter"、"vlan qos aclmap"、"lan ip filter"、"lan ip dscp"、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 400 個まで設定可能です。**

**適用機種**　***SR-X526R1***

装置に設定可能な上限を以下に示します。

- 設定コマンドによる上限：装置全体で 64 個
  "ether macfilter"、"vlan macfilter"、"lan ip filter"、"ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp" コマンド合わせて装置全体で 64 個まで設定可能です。
  優先順位は、それぞれ以下のようになります。
  - コマンドの適用優先順は、"ether macfilter"、"vlan macfilter"、"lan ip filter"、"ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp" コマンドの順番です。
  - ether ポート間の優先順位は、ether ポート番号が小さいほうが高くなります。
  - VLAN 間の優先順位は、VLAN ID が小さいほうが高くなります。
  - lan 間の優先順位は、lan 定義番号が小さいほうが高くなります。

- マスク数による上限：装置全体で 64 個
  "ether macfilter"、"vlan macfilter"、"lan ip filter"、"ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp"、"vlan protocol" コマンド合わせて装置全体で 64 マスクまで設定可能です。
  優先順位は、それぞれ以下のようになります。
  - コマンドの適用優先順は、"vlan protocol"、"ether macfilter"、"vlan macfilter"、"lan ip filter"、"ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp" コマンドの順番です。
  - ether ポート間の優先順位は、ether ポート番号が小さいほうが高くなります。

- VLAN 間の優先順位は、VLAN ID が小さいほうが高くなります。
- lan 間の優先順位は lan 定義番号が小さいほうが高くなります。

"ether macfilter"、"vlan macfilter"、"lan ip filter"、"ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp" コマンドが消費するマスク数は、適用する acl によって以下のようになります。

複数の acl を適用する場合はそれぞれの合計となりますが、組み合わせによりそれぞれの合計以下となることがあります。

| 適用する acl の条件 | マスク数 |
|---|---|
| acl mac 定義の場合 | |
| llc の LSAP を指定する場合 | 3 |
| llc の LSAP を指定しない場合 | 1 |
| acl vlan 定義の場合 | 1 |
| acl ip 定義の場合 | |
| srcIP アドレスを指定しない場合 | |
| tos 値 /dscp 値を指定しない場合 | 1 |
| tos 値 /dscp 値を指定する場合 | 3 |
| srcIP アドレスを指定する場合 | |
| dstIP アドレスを指定しない場合 | 1 |
| dstIP アドレスを指定する場合 | |
| srcIP と dstIP のマスク値が同じ場合 | |
| tos 値 /dscp 値を指定しない場合 | 1 |
| tos 値 /dscp 値を指定する場合 | 3 |
| srcIP と dstIP のマスク値が異なる場合 | 3 |

"vlan protocol" コマンドが消費するマスク数は、以下のようになります。

| 適用する acl の条件 | マスク数 |
|---|---|
| プロトコル VLAN 定義の場合 | |
| vlan protocol ipv4 を指定する場合 | 3 |
| vlan protocol ipv6 を指定する場合 | 1 |
| vlan protocol <count> ether を指定する場合 | 1 |
| vlan protocol <count> llc を指定する場合 | 1 |

- アクション数による上限：装置全体で 16 個

  "ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp"、"vlan protocol" コマンド合わせて装置全体で 16 アクションまで設定可能です。
  優先順位は、それぞれ以下のようになります。
  - コマンドの適用優先順は、"vlan protocol"、"ether qos aclmap"、"vlan qos aclmap"、"lan ip dscp" コマンドの順番です。
  - ether ポート間の優先順位は、ether ポート番号が小さいほうが高くなります。
  - VLAN 間の優先順位は、VLAN ID が小さいほうが高くなります。
  - lan 間の優先順位は、lan 定義番号が小さいほうが高くなります。

以下のコマンドが設定されている場合に 1 アクションが消費されますが、コマンドの指定数にかかわらず 1 アクションのみ消費されます。

- vlan <vid> protocol ipv4
- vlan <vid> protocol ipv6

以下のコマンドが設定されている場合に 1 アクションが消費されます。
<tos_value>、<dscp_value>、<queue_value> が同じ場合は、コマンドの指定数にかかわらず 1 アクションのみ消費されます。

- ether <number> qos aclmap <count> tos <tos_value> <acl>
- ether <number >qos aclmap <count> dscp <dscp_value> <acl>
- ether <number> qos aclmap <count> queue <queue_value> <acl>
- vlan <vid> qos aclmap <count> tos <tos_value> <acl>
- vlan <vid> qos aclmap <count> dscp <dscp_value> <acl>
- vlan <vid> qos aclmap <count> queue <queue_value> <acl>
- lan <number> ip dscp <count> acl <acl_count> <dscp_value>

以下のコマンドが設定されている場合に 1 アクションが消費されます。
<vid> が同じ場合は、コマンドの指定数にかかわらず 1 アクションのみ消費されます。

- vlan <vid> protocol <count> ether
- vlan <vid> protocol <count> llc

### こんな事に気をつけて

**優先制御情報書き換えの対象となるのは本装置に入力されたパケットです。本装置から出力されるパケットは対象となりません。**

# 2.15 IGMP スヌープ機能

**適用機種**　全機種

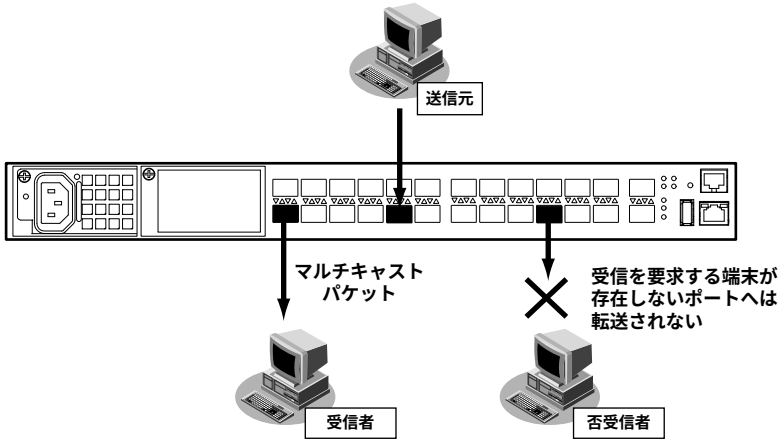
IGMP スヌープ機能とは、送信元が送出した IGMP パケットを確認して、受信者の存在するポートへマルチキャストパケットを転送する機能です。

- 送信元
  本装置に接続している端末またはマルチキャストルータ
- 受信者が存在するポート
  マルチキャストグループアドレスのリスナが存在しているポートまたはマルチキャストルータが接続されたポート

本機能を利用することによって、期待しないマルチキャストパケットを端末が受信しなくなり、端末の負荷を低減することができます。

本装置の IGMP スヌープ機能では、IGMP プロトコルのバージョン 1 と 2 をサポートしています。

以下に、IGMP スヌープ機能の動作について示します。




本装置のポートで、マルチキャストルータが接続されたマルチキャストルータポートまたはリスナが存在するポートとして認識される条件を、以下に示します。

| ポート | 認識される条件 |
|---|---|
| マルチキャストルータポート | マルチキャストルータポートの設定（vlan <vlan_id> igmpsnoop router）によって、以下の条件で認識されます。<br>• auto を指定した場合<br>IGMP Query パケットを受信した場合、そのポートがマルチキャストルータポートと認識されます。<br>• yes <port_no> を指定した場合<br>設定により指定されたポートは起動時にマルチキャストルータポートとして認識されます。さらに、auto を指定した場合と同様に、IGMP Query packet を受信したポートもマルチキャストルータポートとして認識されます。 |
| リスナポート | IGMP Membership Report パケットを受信したポートがリスナポートとして認識されます。 |

マルチキャストグループアドレスをあて先に持つパケットを受信した場合、本装置はマルチキャストルータポートおよびリスナポートにのみ、そのパケットを転送します。

### こんな事に気をつけて

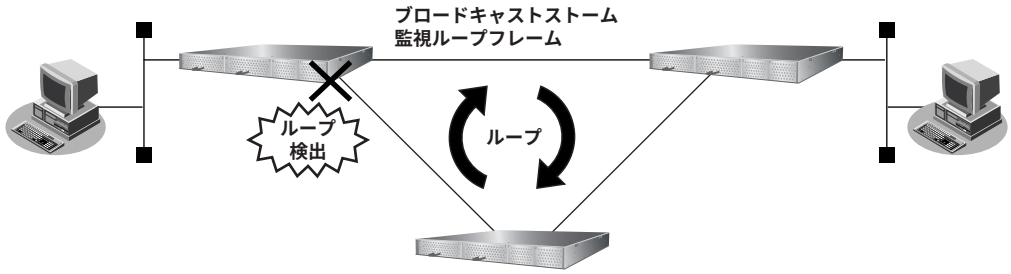
- IGMP を利用しないでマルチキャスト通信を行っている場合は、通信ができなくなる可能性があります。
- IGMP スヌープが有効である装置と接続するポートは、構成定義でマルチキャストルータポートとして設定してください。
- マルチキャストルータが 2 台以上接続される場合は、マルチキャストルータポートを構成定義で設定してください。マルチキャストルータポートが正しく認識されなくなり、マルチキャストルータの先に接続される端末がマルチキャストパケットを受信できなくなる場合があります。
- 本装置では、一度登録されたグループアドレスはリスナ端末が存在しなくなった場合でもエントリ自体を消去しないで、出力ポートの情報のみを消去します。不要なグループアドレスが登録されている場合は、clear igmpsnoop group コマンドで消去することができます。詳細は、「コマンドリファレンス」を参照してください。
- 最大登録可能なマルチキャストグループアドレス数を超えた場合、超えたアドレスはすべて同一 VLAN 内に flooding されます。扱われるグループアドレスが最大登録可能数を超える場合は、IGMP スヌープ機能は利用しないでください。
- 本装置では 224.1.1.1 と 225.1.1.1 や 224.1.1.1 と 225.129.1.1 のように、IP アドレスの下位 23 ビットが同じアドレスについては、同一アドレスとして認識されます。そのため、これらのアドレスで待ち合わせする異なるリスナ端末が存在した場合でも両方のアドレスあてのパケットが転送されます。
- IGMP スヌープの送信元アドレスは通常設定する必要はありません。送信元アドレスが 0.0.0.0 である IGMP パケットを認識できない装置が存在する場合のみ設定してください。なお、IGMP スヌープ装置を複数台接続する場合、IGMP スヌープの送信元アドレスは同一 VLAN 内で 2 台以上設定しないでください。
- マルチキャストルータが接続されないネットワークでは、vlan igmpsnoop querier コマンドで Querier 動作を無効としないでください。

# 2.16 ループ検出機能

**適用機種**　全機種

本装置では、ネットワーク上でのパケットのループを防止するためにループ検出およびループしているポートを閉鎖または論理的に遮断することができます。各ポートから送信するループ監視フレームによって、本装置のMACアドレスを持つパケットを受信することでパケットのループを検出し、該当するポートを閉鎖または論理的に遮断してループを防止します。

ループ検出した際には、システムログの出力およびSNMPマネージャに対してTrap（srxLoopDetect）の送信が可能です。




こんな事に気をつけて

- **ループ時、トラフィックの負荷が帯域100%を占領した場合は、ループを検出することはできません。ブロードキャスト／マルチキャスト制御機能を併用してください。**
- **ループ検出時にポートを閉塞する指定を行っていた場合は、onlineコマンドの閉塞解除指定でポート閉塞を解除してください。**
- **STP機能が有効なポートでは、ループ検出時にポートを論理的に遮断する指定はできません。**

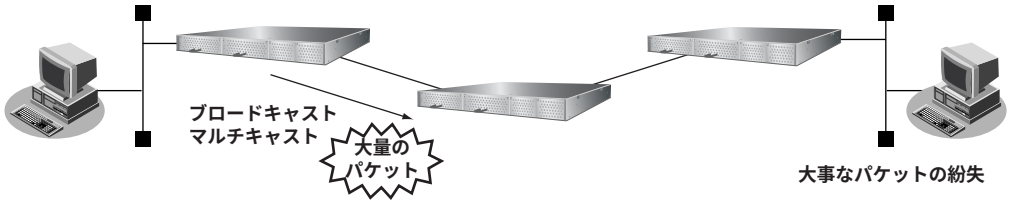
# 2.17　ブロードキャスト／マルチキャストストーム制御機能

**適用機種**　全機種

ブロードキャスト／マルチキャストストーム制御機能とは、障害によってブロードキャスト／マルチキャストのパケットがネットワークを大量に流れ、それ以外のパケットの通信を阻害しないように、パケットを制御する機能です。

本装置は、しきい値を設定し、パケットをポート単位で制御します。パケットの流量がしきい値を超えた場合は、パケットを破棄またはポートを閉塞し、流量を制限します。

しきい値を超えた際には、システムログの出力および SNMP マネージャに対して Trap（srxBroadcastStormDetect/srxMulticastStormDetect）の送信が可能です。




**こんな事に気をつけて**

**パケットの流量がしきい値を超えポート閉塞した場合、ポート閉塞を解除するには、online コマンドによる閉塞解除の指定が必要となります。**

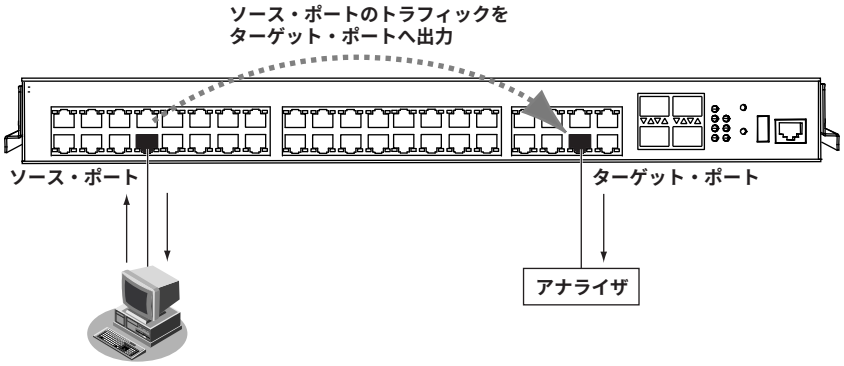
# 2.18 ポート・ミラーリング機能

適用機種　全機種

## SR-X316T2/324T2/340TR1 の場合

ポート・ミラーリング機能とは、指定したターゲット・ポートから、指定したソース・ポートの受信／送信／送受信トラフィックを監視する機能です。

ポート・ミラーリング機能を使用する場合は、まず、ターゲット・ポートに、LAN アナライザなどトラフィックの状況を監視するプローブ装置を接続し、接続したターゲット・ポートと監視するソース・ポートを指定します。また、本装置では複数のソース・ポートを指定することができます。ただし、複数ポートを指定する際には、対象となるソース・ポートのトラフィックの合計が、ターゲット・ポートの帯域を超えないようにしてください。




### こんな事に気をつけて

- ターゲット・ポートに出力されるパケットのあて先 MAC アドレス、送信元 MAC アドレス、VLAN タグの有無とその内容については、実際にソース・ポートで送受信されたパケットと異なる場合があります。
- ターゲット・ポートに出力されるパケットは以下のようになります。
  - ブリッジ転送するパケットをミラーリングした場合
    受信／送信パケットをミラーリングした場合、ミラーパケットの VLAN ID は、ソース・ポート、ターゲット・ポートの VLAN タグ付与の設定や、受信するパケットの VLAN ID により異なります。
  - ルーティング転送するパケットをミラーリングした場合
    ユニキャストパケットをルーティングする場合と、マルチキャストパケットをルーティングする場合では、送信元 MAC アドレスとあて先 MAC アドレスの内容は、以下のように異なる場合があります。

受信パケットをミラーリングする場合

| ミラーされるパケット種別 | ミラーパケットの内容 |
|---|---|
| ユニキャストパケット | ミラーされるパケットが転送先から送信される際に書き換えられるアドレスが付与されるので、ミラーパケットはソース・ポートの受信パケットと異なっている場合があります。 |
| マルチキャストパケット | ミラーパケットはソース・ポートの受信パケットと同じに見えます。 |

送信パケットをミラーリングする場合

| ミラーされるパケット種別 | ミラーパケットの内容 |
|---|---|
| ユニキャストパケット | ミラーパケットはソース・ポートの送信パケットと同じに見えます。 |
| マルチキャストパケット | ルーティング前の受信パケットと同じアドレスが付与されるので、ミラーパケットとソース・ポートの送信パケットは異なっているように見える場合があります。 |

ユニキャストパケットをルーティングする場合と、マルチキャストパケットをルーティングする場合では、VLAN タグの内容は、以下のように異なります。

受信パケットをミラーリングする場合

| ミラーされるパケット種別 | 受信パケットのタグの有無 | ミラーパケットの内容 |
|---|---|---|
| ユニキャストパケット | タグ付き | 送信先に付けられるべきタグが付与されるのでミラーパケットとソース・ポートの受信パケットは異なって見える場合があります。 |
| | タグなし | タグが付与されません。 |
| マルチキャストパケット | タグ付き | ミラーパケットとソース・ポートの受信パケットは同じに見えます。 |
| | タグなし | タグが付与されません。 |

送信パケットをミラーリングする場合

| ミラーされるパケット種別 | ルーティング前パケットのタグの有無 | ミラーパケットの内容 |
|---|---|---|
| ユニキャストパケット | タグ付き | ソース・ポートのタグ付与の設定にかかわらず送信先に付けられることになるタグが必ず付与されます。 |
| | タグなし | ソース・ポートのタグ付与の設定にかかわらずタグが付与されません。 |
| マルチキャストパケット | タグ付き | ソース・ポートのタグ付与の設定にかかわらずルーティング前の受信パケットのタグが付与されます。 |
| | タグなし | ソース・ポートのタグ付与の設定にかかわらずタグが付与されません。 |

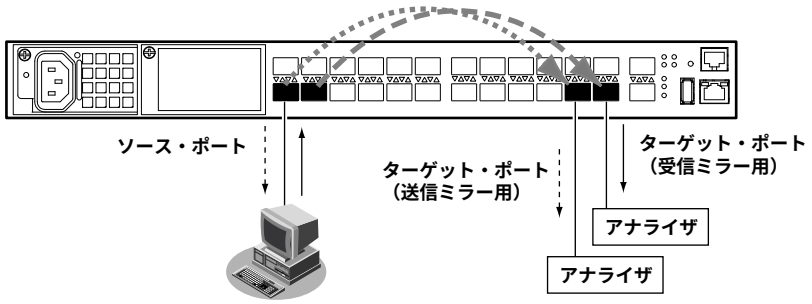
- SR-X340TR1 では、自装置が送信したフレームは VLAN タグが付与されずにターゲット・ポートから送信されます。それ以外の機種では自装置が送信したフレームは、VLAN タグが付与された形式となってターゲット・ポートから送信されます。
- ソース・ポートのフロー制御を有効に設定していて、かつ、ソース・ポートの通信帯域がターゲット・ポートの通信帯域を超えた場合は、ソース・ポートのフロー制御が動作します。
- SR-X316T2/324T2/340TR1 では、ソース・ポートの STP 機能でのポート状態がフォワーディング以外の場合も、ターゲット・ポートにパケットがミラーリングされます。
- SR-X316T2/324T2 では、送信パケットをミラーリングする場合、VLAN タグが付与された形式となってターゲット・ポートから送信されます。
- SR-X316T2/324T2 では、自装置が送信したフレームは、ソース・ポートとターゲット・ポートの VLAN が同一の場合だけターゲット・ポートから送信されます。

## SR-X526R1 の場合

ポート・ミラーリング機能とは、指定したターゲット・ポートから、指定したソース・ポートの受信トラフィック、または、送信トラフィックを監視する機能です。ターゲット・ポートとして、ソース・ポートの受信トラフィックを監視する受信ミラー用ターゲット・ポートと、ソース・ポートの送信トラフィックを監視する送信ミラー用ターゲット・ポートを指定できます。

ポート・ミラーリング機能を使用する場合は、まず、ターゲット・ポートに、LAN アナライザなどトラフィックの状況を監視するプローブ装置を接続し、接続したターゲット・ポートと監視するソース・ポートを指定します。

本装置では複数のソース・ポートを指定することができます。ただし、複数ポートを指定する際には、対象となるソース・ポートのトラフィックの合計が、ターゲット・ポートの帯域を超えないようにしてください。




### こんな事に気をつけて

- ミラーのターゲット・ポートは、装置で送信用と受信用のそれぞれ 1 ポートしか設定できません。
- ミラーのターゲット・ポートの送信用ポートと受信用ポートを同一ポートに設定することはできません。
- ミラーのターゲット・ポートは、ソース・ポートのミラー専用となります。
- ミラーのターゲットで指定したポートをソースとして指定することはできません。
- ミラーのソース・ポートがターゲット・ポートに対して複数ある場合、ターゲット・ポートの帯域を超えた分のパケットは廃棄されます。
- ソース・ポートの STP 機能でのポート状態がフォワーディング以外の場合も、ターゲット・ポートにパケットがミラーリングされます。STP、RSTP、MSTP 状態とミラーされるフレームの関係は以下のようになります。複数のソースのミラーが可能な場合は、それぞれの状態に応じたトラフィックがミラーされます。

| ソース・ポート（MSTP の場合対象 VLAN 内）の状態 | フレーム種類 | ターゲット・ポート転送 |
|---|---|---|
| ディセーブル | BPDU 以外 | 転送されない |
| | BPDU | 転送されない |
| ブロッキング、リスニング | BPDU 以外 | 転送されない |
| （RSTP/MSTP ではディスカーディング） | BPDU | 転送される |
| ラーニング | BPDU 以外 | 転送されない |
| | BPDU | 転送される |
| フォワーディング | BPDU 以外 | 転送される |
| | BPDU | 転送される |

- ターゲット・ポートに出力されるパケットの VLAN タグの有無とその内容については、実際にソース・ポートで送受信されたパケットと異なる場合があります。

- ターゲット・ポートに出力されるパケットは以下のようになります。
  - 送信パケットをミラーリングする場合
    以下のようになります。

| パケットのあて先ソース・ポートのタグ設定 | ミラーパケットの内容 |
|---|---|
| タグ付き設定時<br>（マルチキャスト、ブロードキャスト、フラッディングのパケットで、複数のあて先ソース・ポートがある場合は、その複数のソース・ポートの中にタグ付き設定のものが存在するとき） | タグが付きます。<br>タグの内容は 送信ソース・ポートに付けられるべきタグになります。 |
| タグなし設定時<br>（マルチキャスト、ブロードキャスト、フラッディングのパケットで、複数のあて先ソース・ポートがある場合は、その複数のソース・ポートがすべてタグなし設定のとき） | タグは付きません。 |

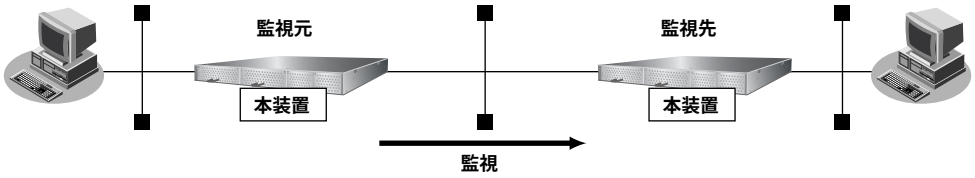
  - 受信パケットをミラーリングする場合
    ターゲット・ポートに出力されるパケットの VLAN タグの有無と内容は、入力時のパケットと一致します。
- DSCP や ip precedence の書き換えを行いながら受信フレームミラーリングを行う場合、受信フレームではなく変更後のフレームがミラーされます。

# 2.19 ether L3 監視機能

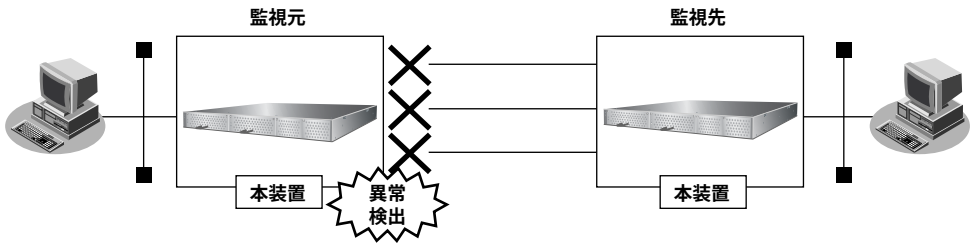
**適用機種**　全機種

ether L3 監視機能とは、ある特定のノード（装置）に対して、ICMP ECHO パケットを送受信することによりそのノードの生存を確認する機能です。監視相手装置が自装置と複数の装置を経由して繋がっている場合などでは、その経路上での障害を検出および監視しているポートを閉塞することができます。また、リンクアグリゲーション機能や、バックアップポート機能と併用することがきます。

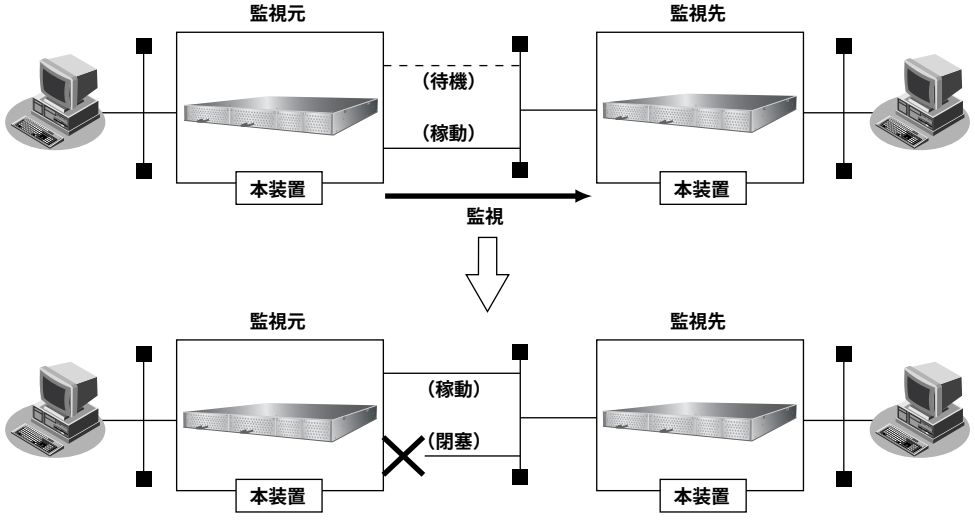
定義反映時、監視ポートが リンクダウン状態だった場合でも、監視を開始します。




- リンクアグリゲーション機能を使用して ether L3 監視
  リンクアグリゲーション機能を使って監視をしている状態で、異常を検出してポートを閉塞させる場合、メンバポートすべてが閉塞されます。




- バックアップポート機能を使用して ether L3 監視
  バックアップポート機能を使って監視を行う場合、稼動ポートで監視を行うように設定してください。
  待機ポートで ether L3 監視機能を設定した場合は、監視を行いません。待機ポートが稼動ポートに切り替わったときに監視を開始します。
  また、異常を検出したとき、監視しているポートを閉塞させる場合、待機ポートが稼動ポートに切り替わることで、ネットワーク障害の影響を最小限に抑えることができます。
  定義反映時、監視ポートが リンクダウン状態だった場合、マスタポートを必ず優先使用するモードになっていれば、マスタポートが監視を開始します。先にリンクアップしたポートを使用するモードになっていれば、監視を設定したポートが監視を開始します。



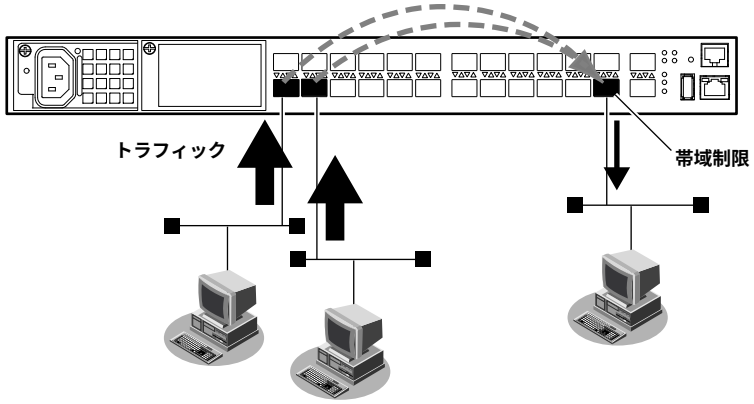
### こんな事に気をつけて

- STP 機能と併用する際には、監視タイムアウトを長めに設定してください。
- 閉塞状態になったポートは、online コマンドの閉塞解除指定でポート閉塞を解除してください。
- 監視対象ポートが認証ポートの場合、監視は行いません。

# 2.20 出力レート制限機能

適用機種　***SR-X526R1***

出力レート制御機能とは、大量のトラフィックが出力先ポートに流れないように、出力ポートの流量を制限する機能です。




本装置は、出力の制限値を設定し、帯域幅をポート単位で制御します。トラフィックの帯域幅がしきい値を超えた場合は、帯域幅を超えるトラフィックが破棄されます。

こんな事に気をつけて

**DRR を用いた優先制御機能と出力レート制御機能を併用することはできません。**

# 2.21 ポート閉塞機能

適用機種　全機種

ポート閉塞機能とは、物理ポートのリンクダウン状態（ポート閉塞状態）を online コマンド発行によるオペレータ指示があるまで保持する機能です。

障害要因によって、物理ポートのリンクアップ、リンクダウンが繰り返し発生する可能性があります。そのような場合、本装置は意図的にリンクダウン状態（ポート閉塞状態）を継続させることで、冗長経路が存在する場合は、安定した通信を保つことができます。

ポート閉塞状態への遷移は、以下で制御します。

- offline コマンド発行による手動閉塞
- 通信制御機能の連携動作による自動閉塞
- 接続ポートのリンク状態変化による自動閉塞

**こんな事に気をつけて**

- **offline コマンドは、管理者クラスだけ発行可能です。**
- **閉塞状態となったポートは、online コマンドの閉塞解除指定でポート閉塞を解除してください。**

## offline コマンド発行による手動閉塞

Ethernet ポート制御コマンドである offline コマンドを発行することによってポートを閉塞状態とします。

## 通信制御機能の連携動作による自動閉塞

ループ検出機能やブロードキャスト／マルチキャストストーム制御機能などを使用した場合に、ポート閉塞状態への遷移指定が可能です。本装置でポート閉塞状態への遷移をサポートしている通信制御機能は以下のとおりです。

- バックアップポート機能
- ループ検出機能
- ブロードキャスト／マルチキャストストーム制御機能
- ether L3 監視機能

参照 「2.10 バックアップポート機能」（P.36）、「2.16 ループ検出機能」（P.69）、
「2.17 ブロードキャスト／マルチキャストストーム制御機能」（P.70）、「2.19 ether L3 監視機能」（P.75）

## 接続ポートのリンク状態変化による自動閉塞

接続ポートのリンク状態の変化を契機にポートを閉塞状態にすることを可能にします。

本装置でポート閉塞状態への遷移が可能なリンク状態変化は以下のとおりです。

- 起動時閉塞
  装置起動時および動的定義反映時にポートを閉塞状態とします。
- リンクダウン回数による閉塞
  構成定義で指定した回数分リンクダウンを検出した場合に、ポートを閉塞状態とします。
- リンクダウンを契機にしたほかのポートの連携閉塞（リンクダウンリレー閉塞）
  リンクダウン時に、構成定義で指定した連携ポートを同時に閉塞状態とします。
  また、リンクアップ状態へ復旧した場合に、連携ポートを同時に閉塞解除することも可能です。

# 2.22 IP 経路制御機能

適用機種　全機種

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

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。

## 2.22.1 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）
  インタフェースに割り当てた IPv4 ネットワークまたは IPv4 アドレスを示します。
- インタフェース経路（IPv6）
  インタフェースに割り当てた IPv6 プレフィックスを示します。構成定義として IPv6 プレフィックスを設定したときや、Router Advertisement Message で IPv6 プレフィックス情報を受信したときに生成されます。
  ループバックインタフェースに割り当てた IPv6 アドレスは、ホストルート（128 ビットネットワークマスク）として管理されます。
- RA 経路（IPv6）
  受信した Router Advertisement（RA）Message の情報に基づき、生成されるデフォルトルートを示します。
- スタティック経路（IPv4/IPv6）
  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。

IP 経路情報は、以下に示す優先度値で管理されます。

### ● IPv4

| 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 | 1（変更可） |

### ● IPv6

| 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 | 1（変更可） |
| RA 経路 | 12（固定） |

## 2.22.2　IP 経路情報の管理

IP 経路情報は、ルーティングテーブルで管理されます。

以下に、ルーティングテーブルについて説明します。

### 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 仕様一覧「2.3 システム最大値一覧」（P.24）

## 2.22.3　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。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。

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の中で経路切り替えを行うことができます。

## 2.22.4　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。

- 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。

# 2.23 IPv6 機能

**適用機種**　全機種

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、IPv6 パケットでのホスト機能動作を行うことができます。

本装置がサポートしている IPv6 ホスト機能は、以下のとおりです。

- 静的な経路設定
- Router Advertisement Message 受信によるアドレスの自動設定
- Router Advertisement Message 受信によるデフォルト経路の自動設定
- Router Advertisement Message 受信による ND 情報の自動設定
- ソースアドレスの自動選択

また本装置では、以下の機能もサポートしています。

- パケットフィルタリング

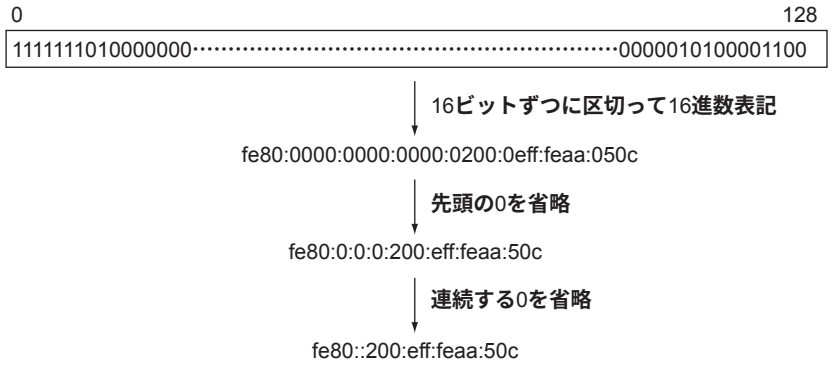
**こんな事に気をつけて**

**IPv6 ホスト機能時は、ICMPv6 リダイレクトメッセージは送信しません。**

## 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。

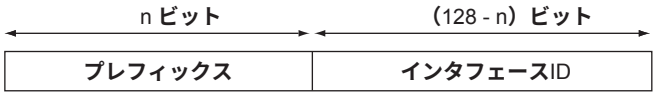
例を以下に示します。



## 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 から割り当てられたアドレスや、IPv6 ルータから受信した Router Advertisement Message 情報を元に自動生成されたアドレスとなります。
- 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。本装置はダイナミックルーティングをサポートしません。

## Router Advertisement Message 受信によるアドレスの自動設定

本装置では、Router Advertisement Messageの受信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情報が含まれています。プレフィックス情報を受信した場合、有効期限を管理するためのプレフィックスリストを生成し、インタフェースIDを付加したIPv6アドレスを自動設定します。

受信したプレフィックス情報は、show ipv6 ra prefix-listコマンドで参照できます。また、自動設定したIPv6アドレスは、show ipv6 routeまたはshow interfaceコマンドで参照できます。

### こんな事に気をつけて

- **1つのインタフェースで複数のプレフィックス情報を受信する場合は、自動生成の設定を必要な数だけ追加してください。**
- **有効期限が365日を超えたプレフィックス情報（無期限は除く）を受信した場合、365日の有効期限として動作します。**
- **プレフィックス情報のプレフィックス長が64以外の場合、そのプレフィックス情報は破棄されます。**
- **プレフィックス情報のオンリンクフラグと自動アドレス生成フラグが設定されている場合、IPv6アドレスをインタフェースに設定します。**

## Router Advertisement Message受信によるデフォルト経路の自動設定

Router Advertisement Messageを受信した場合、送信ルータのリンクローカルアドレスを中継ゲートウェイとするデフォルト経路を設定します。

複数のルータよりRouter Advertisement Messageを受信した場合、デフォルトルータとして利用できるデフォルトルータリストを生成し、この一覧の中でパケットが到達可能なルータをデフォルトルータとして設定します。

生成したデフォルトルータリストは、show ipv6 ra default-router-listコマンドで参照できます。また、show ipv6 routeコマンドで、設定されたデフォルトルータを参照できます。

### こんな事に気をつけて

- **複数ルータからRouter Advertisement Messageを受信した場合、ルータプレファレンスによる優先制御は動作しません。この場合、最初に受信したルータをデフォルトルータとします。**
- **Router Advertisement Messageによるデフォルト経路の優先度値は12で設定します。スタティックのデフォルト経路と混在運用する場合、スタティック経路の優先度値を変更してください。**

## Router Advertisement Message受信によるND情報の自動設定

Router Advertisement Messageには、通信時に使用する隣接情報（ND情報）が含まれています。Router Advertisement Messageを受信し、受信メッセージに含まれているND情報と本装置で保持しているND情報が異なる場合は、ND情報の更新が行われます。

以下に、本装置で保持しているND情報とその初期値を示します。

- 隣接装置の到達性についての有効期間（初期値は30秒）
- 隣接装置の到達性確認を行うNeighbor Solicitation（NS）Messageの送信間隔（初期値は1秒）
- 最大ホップ数（初期値は64）
- 受信ネットワーク上で推奨するMTU長（初期値は1500バイト）

## ソースアドレスの自動選択

IPv6 では、インタフェースに複数の IPv6 アドレスが割り当てられることが一般的です。本装置から通信を始め、アプリケーションによって明示的にソースアドレスを指定しない場合は、複数の IPv6 アドレスの中から一定のルールに基づいてアドレスの選択を行います。

本装置がサポートするソースアドレスの選択ルールは、以下の RFC およびドラフトに準拠します。

- RFC3484：Default Address Selection for Internet Protocol version 6 （IPv6）

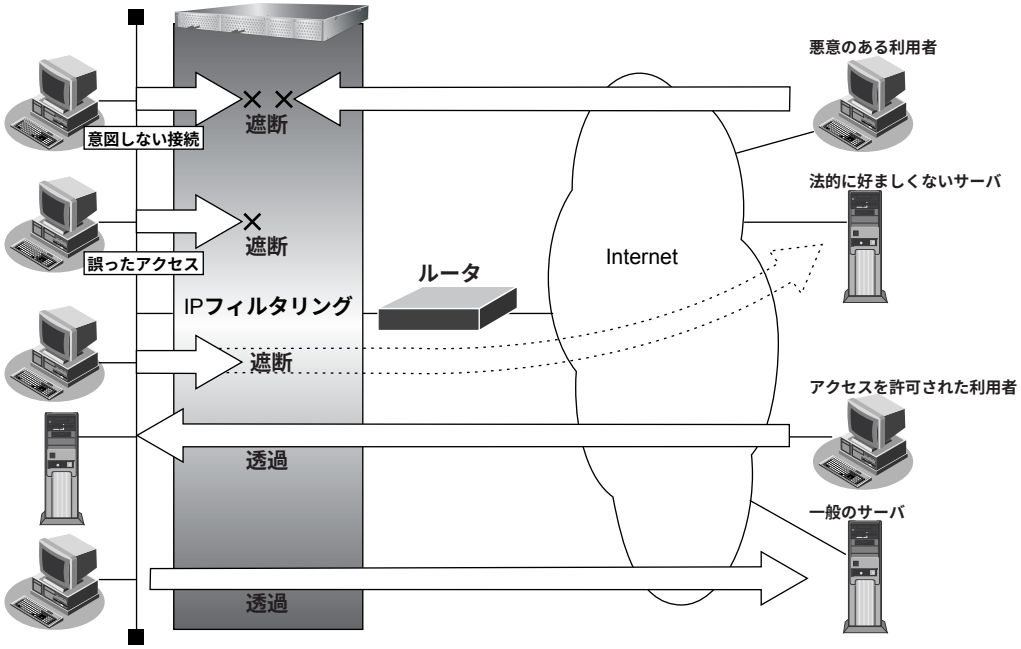
# 2.24 IP フィルタリング機能

**適用機種**　全機種

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、本装置を経由して送受信するパケットを IP アドレスやポート番号など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ることができます。

本装置では、本装置に入力されたパケットが指定された ACL 定義の "acl ip" 定義および、"acl tcp" 定義または "acl udp" または "acl icmp" 定義に該当した場合に IP フィルタリング処理を行います。




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
- スイッチ以外の要素（ファイアーウォール、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。**
- **本装置などのスイッチでは、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。**
- **IP フィルタリングの対象となるのは本装置に入力されたパケットです。本装置から出力されるパケットは対象となりません。**
- **SR-X526R1 では、プロトコル VLAN が適用されたフレームは ACL 対象になりません。**

## 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**

  特定のパケットを受け取らないようにする。

  非公開ホストへのアクセスを拒否する。

  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**

  法的に問題のあるサイトなどへのアクセスを制限する。

  内部ユーザによる不要なアクセスを防ぐ。

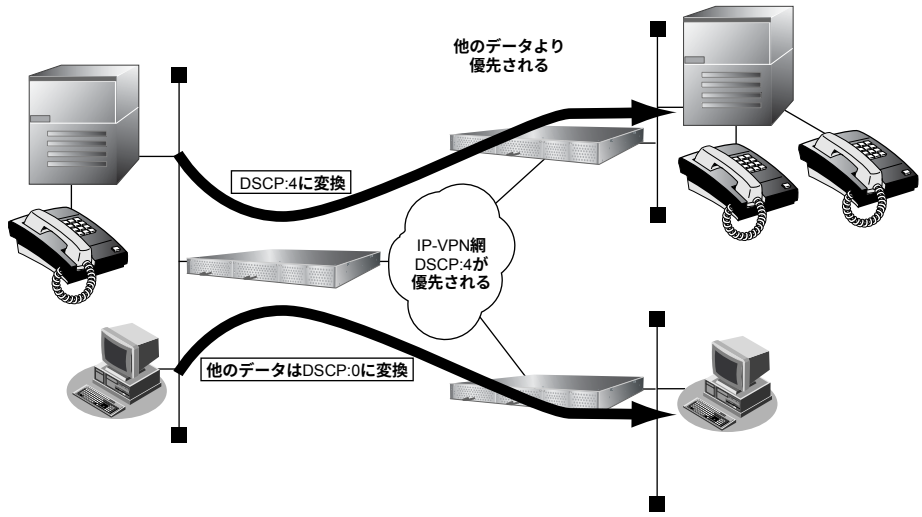
# 2.25 DSCP 値書き換え機能

**適用機種**　***SR-X340TR1, 526R1***

DSCP 値書き換え機能とは、指定する IP パケットの DSCP 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 DSCP 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。DSCP 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。

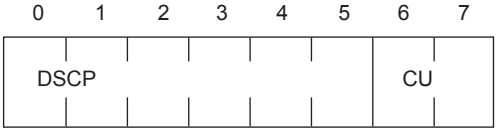
本装置でサポートしている DSCP 値書き換え機能は、以下の RFC（Request For Comments）に準拠しています。

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




DSCP 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）フィールドおよび IPv6 パケットヘッダにある 8 ビットの Traffic Class フィールドのうち、DSCP フィールドを制御することができます。

- RFC791 Internet Protocol
- RFC2460 Internet Protocol,Version 6 （IPv6）Specification




Bits 0-5:　DSCP

Bits 6-7:　Currently unused

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 DSCP 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 DSCP 値は書き換えられません。

本装置では、本装置に入力されたパケットが、指定された ACL 定義の "acl ip" 定義、および、"acl tcp"、"acl udp" または "acl icmp" 定義に該当した場合に DSCP 値書き換え処理を行います。

## こんな事に気をつけて

SR-X526R1 では、以下のフレームは ACL 対象となりません。

- プロトコル VLAN が適用されたフレーム
- MAC フィルタ機能が適用されたフレーム
- IP フィルタリング機能が適用されたフレーム
- QoS 優先制御情報書き換え機能が適用されたフレーム
- 優先度の高い DSCP 値書き換え機能が適用されたフレーム

☛ 参照　コマンド設定事例集「15 DSCP 値書き換え機能を使う」（P.53）

# 2.26 RADIUS機能

適用機種　全機種

RADIUS 機能は、AAA（Authentication, Authorization, Accounting）情報の管理を外部サーバ（RADIUS サーバ）を利用して行う機能です。複数の装置で同じ AAA 情報が必要な場合や、大量のユーザ情報を管理する場合など、ユーザの認証情報や設定情報、ユーザごとの接続時間を集約して管理することができます。

本装置では、RADIUS クライアント機能をサポートしています。

RADIUS クライアント機能は、以下の RADIUS サポート機能から AAA を経由して利用されます。

以下に、それぞれの機能で利用可能な AAA 情報を示します。

| RADIUS サポート機能 | 認証方式（authentication） | ユーザ情報（authorization） | アカウンティング（accounting） |
|---|---|---|---|
| ログインユーザ認証 | PAP 認証／CHAP 認証 | 使用しません | 使用しません |

本装置の RADIUS クライアント機能は、複数台の RADIUS サーバを使用したバックアップ構成または負荷分散構成が可能です。

RADIUS サーバとして定義された認証サーバおよびアカウンティングサーバは、alive 状態と dead 状態を持ちます。

それぞれの状態の意味は以下のとおりです。

- alive 状態
  サーバが使用可能である状態です。
  優先度が高い（定義上の数値が小さい）サーバから優先して使用されます。
  同じ優先度のサーバが複数存在する場合は、ランダムにサーバが選択されます。
- dead 状態
  サーバあてのリクエストがタイムアウトしたことにより、そのサーバの使用を一時的に停止している状態です。ほかに alive 状態のサーバが存在する場合、定義した優先度の値は使用されません。
  復旧待機時間で指定した時間が経過すると、自動的に alive 状態に復旧します。
  認証またはアカウンティングを行う場合、すべてのサーバが dead 状態になると、ランダムに 1 つのサーバで試行し、応答の得られたサーバは alive 状態に復旧します。

### こんな事に気をつけて

- **RADIUS プロトコルの制約で、同時に認証およびアカウンティングが行える数は 256 です。同時に 257 以上の認証とアカウンティングを行った場合は、両方とも失敗します。**
- **RADIUS クライアント機能を定義しても、同じグループのユーザ情報は利用されます。AAA グループに RADIUS クライアント機能（aaa radius）とユーザ情報（aaa user）の両方を定義した場合、RADIUS クライアント機能で認証が行われます。RADIUS クライアント機能で認証が成功した場合はユーザ情報は利用されませんが、認証に失敗した場合は、次にユーザ情報で認証を行います。**

# 2.27 TACACS+ 機能

**適用機種**　全機種

TACACS+ 機能は、AAA（Authentication, Authorization, Accounting）情報の管理を外部サーバ（TACACS+ サーバ）を利用して行う機能です。複数の装置で同じ AAA 情報が必要な場合や、大量のユーザ情報を管理する場合など、認証（Authentication）、認可（Authorization）およびアカウンティング（Accounting）情報を集約して管理することができます。

本装置では、TACACS+ クライアント機能のユーザ認証機能とコマンド認可機能をサポートしています。

ユーザ認証機能とは、アクセスユーザが本装置にログイン時に認証処理を行います。

コマンド認可機能とは、アクセスユーザが本装置の提供するコマンド実行時に認可処理を行います。

TACACS+ クライアント機能は、複数台の TACACS+ サーバを使用したバックアップ構成または負荷分散構成が可能です。

TACACS+ サーバとして定義された認証 / 認可サーバは、alive 状態と dead 状態を持ちます。

それぞれの状態の意味は以下のとおりです。

- alive 状態
  サーバが使用可能である状態です。
  優先度が高い（定義上の数値が小さい）サーバから優先して使用されます。
  同じ優先度のサーバが複数存在する場合は、ランダムにサーバが選択されます。
- dead 状態
  サーバとの TCP 接続失敗やサーバあてのリクエストがタイムアウトしたことにより、そのサーバの使用を一時的に停止している状態です。ほかに alive 状態のサーバが存在する場合、定義した優先度の値は使用されません。
  復旧待機時間で指定した時間が経過すると、自動的に alive 状態に復旧します。
  認証または認可を行う場合、すべてのサーバが dead 状態になると、ランダムに 1 つのサーバで試行し、応答の得られたサーバは alive 状態に復旧します。

### こんな事に気をつけて

- **TACACS+ クライアント機能のアカウンティング機能はサポートしていません。**
- **RADIUS クライアント機能との併用はできません。**AAA グループに RADIUS クライアント機能（aaa radius）と TACACS+ クライアント機能（aaa tacacsp）の両方を定義した場合、TACACS+ クライアント機能は無効となります。AAA グループに TACACS+ クライアント機能とユーザ情報（aaa user）の両方を定義した場合は、TACACS+ クライアント機能で認証が行われます。TACACS+ クライアント機能で認証が失敗しても、ユーザ情報での認証は行われません。
- **TACACS+ サーバ用共有鍵の定義を省略した場合、認証や認可データは暗号化されません。認証や認可データを暗号化する場合は、共有鍵を定義してください。**
- **TACACS+ コマンド認可機能は、TACACS+ ユーザ認証機能を使用してログインした場合のみ有効となります。**
- **TACACS+ ユーザ認証時の権限クラスは、管理者パスワード（password admin set）設定の有無に依存します。**
- **TACACS+ コマンド認可機能は、Web 設定および FTP/SFTP では動作しません。**
- **TACACS+ コマンド認可機能で、実際に実行するコマンドとは別のコマンドに対する認可の設定が必要なものは、以下になります。**

| 実行するコマンド | 認可設定が必要なコマンド |
|---|---|
| diff | show running-config（running-config に対して diff を実行する場合） |
| show tech-support | show（show コマンド全体） |
| save | show（show コマンド全体） |
| load | 構成定義コマンド全体 |

以下に管理者パスワードの有無による認証時の権限クラスを示します。

- 管理者パスワードなしの場合
  一般ユーザクラスでの認証のみ行います。
- 管理者パスワードありの場合
  管理者クラスでの認証を行い、認証が失敗した場合に一般ユーザクラスでの認証を行います。

# 2.28 DNS サーバ機能

**適用機種**　全機種

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。

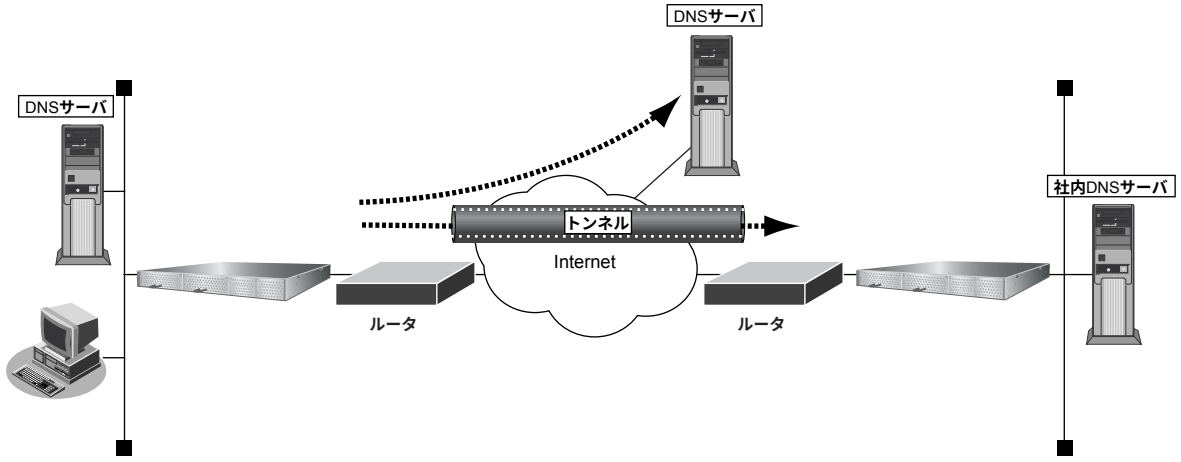
- DNS サーバ（スタティック）機能
- ProxyDNS（DNS 振り分け）機能

## 2.28.1 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 を A（1 a host address）または AAAA（28 a host IPv6 address）、CLASS を IN（1the Internet）とします。

## 2.28.2 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.fujitsu.co.jp　：1.1.1.1
- ftp.fujitsu.co.jp　：2.2.2.2
- *.is.fuku.fujitsu.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。

☛ 参照 コマンド設定事例集「16 DNS サーバ機能を使う（ProxyDNS）」（P.55）

# 2.29 SNMP 機能

適用機種　全機種

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。

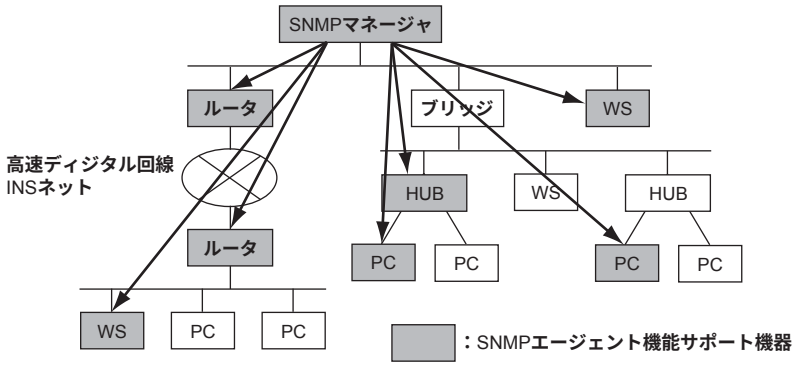
SNMP マネージャ機能は、ネットワーク上の端末の稼動状態や障害状態を一元管理します。SNMP エージェント機能は、SNMP マネージャの要求に対して MIB（Management Information Base：管理情報ベース）という管理情報を返します。

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。

本装置では、SNMPv1、SNMPv2c および SNMPv3 をサポートします。また、標準 MIB および富士通拡張 MIB をサポートしています。

参照　仕様一覧「3.1 標準 MIB」（P.28）、「3.2 富士通拡張 MIB」（P.44）

## 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 エージェントが取り付ける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　コマンド設定事例集「18 SNMP エージェント機能を使う」（P.63）
Web ユーザーズガイド「2.3.1 SNMP の設定」（P.22）

## ifIndex の割り当て

本装置での ifIndex の割り当てを以下に示します。

| ifIndex | インタフェース／定義との対応 |
|---|---|
| 1～ | lan 定義 （1 ＋ lan 定義番号） |
| 100 | マネージメントポート（SR-X526R1 のみ） |
| 5001 | loopback インタフェース |
| 6001～ | リンクアグリゲーション（6000 ＋ <リンクアグリゲーショングループ番号>） |
| 7001～ | ether ポート （7000 ＋ <ether ポート番号>） |

# 2.29.1　RMON 機能

RMON（Remote Network Monitoring）とは、ネットワーク監視のための標準規格であり、遠隔地にある LAN のトラフィックやエラーなどの通信状況を監視する機能です。

RMON 機能は SNMP 機能を拡張したものであり、SNMP エージェント側で LAN の統計情報を蓄積しておき、SNMP マネージャ（または RMON マネージャ）からの要求に応じて蓄積したデータを SNMP の応答として返します。

本装置では以下の RMON グループをサポートします。

- statistics グループ
  監視対象 ETHER ポート上のパケット数やエラー数などの基本的な統計情報を収集します。
- history グループ
  statistics グループで収集する情報とほぼ同じ統計情報を履歴情報として保持します。履歴情報は一定期間の統計情報として装置内で保持されますので、SNMP マネージャ（または RMON マネージャ）は一連の統計情報をまとめて取得することができます。

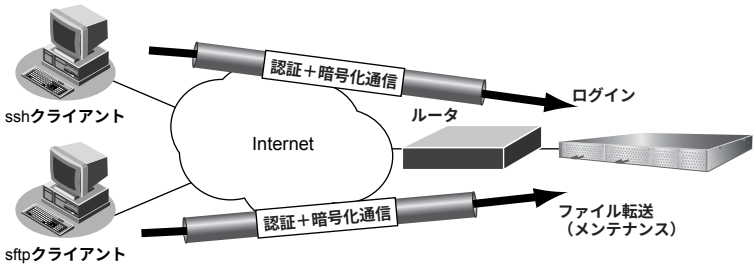
# 2.30 SSH サーバ機能

**適用機種**　全機種

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、公式サイト（http://www.openssh.com/）を参照してください。




**※一時点ではどちらか一方の接続のみ**

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 show ssh server key dsa コマンドまたは show ssh server key rsa 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。

そのあと、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のままであるため、off に設定した方はパスワード入力まで行われたあとに接続拒否されます。

### 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設定を反映した場合、SSH ホスト認証鍵の生成に時間がかかります。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。
- 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、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<br>（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<br>（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<br>（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 SSH サーバ機能

| 項目 | サポート内容 |
|---|---|
| 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、IPv6 |
| 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 |

# 2.31 USB メモリ機能

適用機種　全機種

USB メモリ機能とは、USB メモリに構成定義情報を保存したり、USB メモリから構成定義情報を転送するための機能です。

参照　動作検証済みの USB メモリ（富士通ホームページ）
http://fenics.fujitsu.com/products/manual/usb/

本装置では以下のファイルシステムをサポートしています。

- FAT12（VFAT）
- FAT16（VFAT）
- FAT32（VFAT）

また、本装置では以下の作業を行うことができます。

- USB メモリのフォーマット
- USB メモリからの構成定義の転送
- USB メモリへの構成定義の保存
- USB メモリからのファームウェアの更新
- USB メモリへのファームウェアの保存
- USB メモリへの tech-support の保存
- ファイル操作（ファイル一覧の表示、ファイルの削除、ファイルのコピー、ファイル名変更）

### こんな事に気をつけて

- **本装置は VFAT をサポートしているため、ロングファイル名を指定できます。ただし、日本語のファイル名は指定できません。**
- **USB メモリは、複数のパーティションに分割されたものを利用できますが、MS-DOS® の拡張パーティションは利用できません。**
- **ショートカットを利用することはできません。**
- **アクセス中に本装置から USB メモリを抜いたり、電源切断やリセットを行うと、ファイルシステムが破壊されることがあります。この場合、ERROR ランプが橙色で点滅します。**
- **ファイルシステムの不整合を検出すると、ERROR ランプが橙色で点滅します。この場合は、USB メモリをフォーマットしてください。**
- **他社製品でフォーマットした USB メモリを利用して不都合が発生した場合は、本装置でフォーマットし直してください。**
- **論理フォーマット時の FAT 種別（FAT12、FAT16、FAT32）は、USB メモリの容量に応じて自動的に判断されます。**
- **本装置で USB メモリをフォーマットすると、保存されていた内容はすべて消去され、パーティションは単一になります。フォーマットするときは必要なファイルが残っていないか、十分に注意してください。**
- **USB ポートに、動作保証済み USB メモリ以外の媒体を挿入しないでください。**

## 2.31.1　構成定義の転送と保存

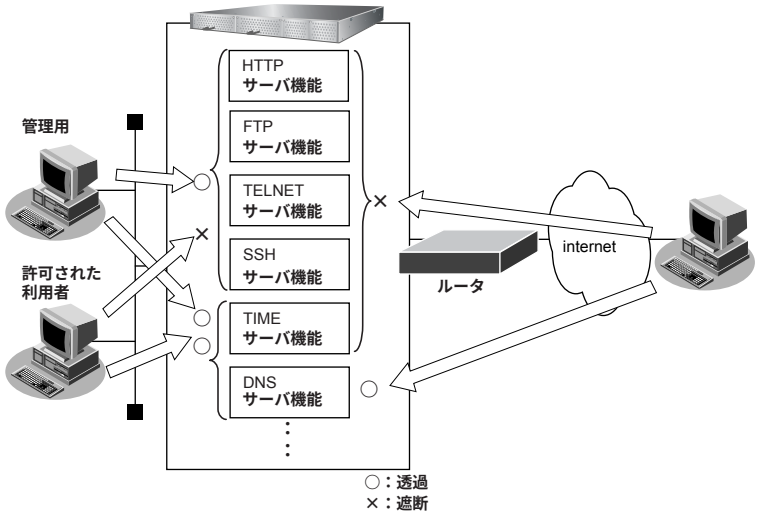
構成定義の転送および保存は、以下の方法で行います。

- copy コマンドで行う場合
  USB メモリのファイルは、/um0/<filename> でアクセスできます。たとえば、USB メモリに格納されている "config.txt" というファイルは、copy コマンドで /um0/config.txt のように指定します。
  USB メモリが複数パーティションに分割されている場合は、先頭のパーティションが利用されます。
  ディレクトリの区切り記号は / です。たとえば、USB メモリの "dir" というディレクトリに格納されている "config.txt" というファイルは、/um0/dir/config.txt のように指定します。
  同様にしてファームウェアの更新および保存ができます。
- Web で行う場合
  Web で行う場合の方法は、Web ユーザーズガイドの「4.2 USB メモリ」（P.45）を参照してください。
  Web で行う場合はディレクトリ配下のファイルは Web の構成定義情報の復元で復元元ファイル名の候補として表示されません。
  退避先ファイル名にディレクトリ配下のファイル（たとえば dir/config.txt）を指定する場合はご注意ください。
- PC レスで転送する場合
  PC を使用しないで行う方法は、コマンドユーザーズガイドの「2.7 外部メディアを使用し PC レスでファームウェアと構成定義をインストールする（外部メディアスタート）」（P.42）を参照してください。

# 2.32 アプリケーションフィルタ機能

**適用機種**　全機種

アプリケーションフィルタ機能では、本装置で動作する各サーバ機能に対してアクセスを制限することができます。これにより、本装置のメンテナンスまたは本装置のサーバ機能を使用する端末を限定し、セキュリティを向上することができます。



# 2.33 縮退機能

**適用機種**　全機種

本装置では、ハード障害を検出した際、装置をシステムダウンさせたあとに縮退モードに遷移します。
縮退モードでは、すべての通信機能を停止しますが、障害情報収集のためにコンソールポートおよび外部メディアのみ使用可能となります。

縮退機能へ遷移させるハード障害は以下のとおりです。

- 冷却ファン異常
- 温度異常
- その他のハード異常（ただし電源異常は除く）
  - Flash メモリ故障
  - スイッチ LSI 故障

# 索引

## あ



## い



## え



## お



## か



## け



## こ



## し



## す



## せ



## そ



## た



## つ



## と



## は



## ふ



## ほ



## ま

## め



## ゆ



## ら



## り



## る

**SR-X　機能説明書**

P3NK-5162-01Z0

発行日　　2014年10月

発行責任　　富士通株式会社