

FUJITSU Network SR-M

機能説明書

V03

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。

無線LANを使用した安全なネットワークを構築するために、本装置をご利用ください。

2016年 6月初版

2017年 7月第2版

本ドキュメントには「外国為替及び外国貿易管理法」に基づく特定技術が含まれています。

従って本ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。

Microsoft Corporationのガイドラインに従って画面写真を使用しています。

Copyright FUJITSU LIMITED 2016 - 2017

目次

はじめに	2
本書の構成と使いかた	5
本書の読者と前提知識	5
本書の構成	5
本書における商標の表記について	6
本装置のマニュアルの構成	6
使用許諾条件	7

第 1 章 ネットワーク設計概念..... 13

1.1 レイヤ 2 ネットワーク設計概念	14
1.1.1 VLAN	14
1.2 本装置の設定の概要	15

第 2 章 機能概要..... 17

2.1 無線 LAN 機能	19
2.1.1 無線 LAN 通信規格	20
2.1.2 認証・暗号化機能	20
2.1.3 SSID 非通知（ステルス機能）	21
2.1.4 ANY 接続拒否（ANY キープロテクション）	22
2.1.5 MAC アドレスフィルタ	22
2.1.6 端末台数制限／端末台数最低保証	22
2.1.7 WDS ブリッジ機能	24
2.1.8 プライバシープロテクション機能（AP ブリッジ）	25
2.1.9 仮想アクセスポイント機能（VAP）	25
2.1.10 WMM 機能（IEEE802.11e）	26
2.1.11 PMK キャッシュ機能	27
2.1.12 周辺アクセスポイント検出機能	27
2.1.13 11g プロテクション機能	28
2.1.14 HT プロテクション機能	29
2.1.15 ショートガードインターバル	30
2.1.16 チャンネルボンディング機能	30
2.1.17 MIMO Power Save 機能	30
2.1.18 認証自動切替機能	31
2.1.19 ノイズ回避機能	31
2.2 オートネゴシエーション機能	32
2.3 AutoMDI/MDI-X 機能	33
2.4 フロー制御機能	34
2.5 VLAN 機能	36
2.6 ポート閉塞機能	38
2.7 バックアップポート機能	40
2.8 リンクインテグリティ機能	41
2.9 フィルタリング機能	42
2.9.1 動的フィルタリング（SPI）	43
2.10 IEEE802.1X 認証機能	44
2.11 MAC アドレス認証機能	48
2.12 DHCP 機能	49
2.12.1 IPv4 DHCP 機能	49

2.13	RADIUS 機能	50
2.14	DNS サーバ機能	52
2.14.1	DNS サーバ (スタティック) 機能	52
2.14.2	ProxyDNS (DNS 振り分け) 機能	52
2.15	SNMP 機能	54
2.16	SSH サーバ機能	56
2.17	USB メモリ機能	58
2.17.1	構成定義の転送と保存	59
2.18	アプリケーションフィルタ機能	60
2.19	IDS 機能	61
2.20	ProxyARP 機能	62
2.21	POE 機能	63
2.22	高速転送モード	64
2.23	無線 LAN 管理機能	65
索引		66

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利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

Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標です。

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。

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
SR-M50AP1 ご利用にあたって	SR-M50AP1 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。
コマンドユーザズガイド	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。
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。
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。
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。
Web リファレンス	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 MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

本製品には、スタンフォード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 mrouted の一部が含まれています。

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

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

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

Copyright (c) 1998-2001

University of Southern California/Information Sciences Institute. All rights reserved.

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

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

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

\$Id: LICENSE,v 1.5 2001/09/10 20:31:36 pavlin Exp \$

Part of this program has been derived from mrouted.

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

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

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

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

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

THE UNIVERSITY OF OREGON DOES NOT MAKE ANY REPRESENTATIONS ABOUT THE SUITABILITY OF THIS SOFTWARE FOR ANY PURPOSE. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING,

WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

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

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

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

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

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

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

Part of this program has been derived from mrouted.

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

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

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

Permission to use, copy, modify, and distribute this software and its documentation in source and binary forms for lawful purposes and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that any documentation, advertising materials,and other materials related to such distribution and use acknowledge that the software was developed by the University of Southern California and/or Information Sciences Institute.

The name of the University of Southern California may not be used to endorse or promote products derived from this software without specific prior written permission.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This library is free for commercial and non-commercial use as long as the following conditions are adhered 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 routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

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

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

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

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

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

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

本製品には、Atsushi Onoe 氏、Video54 Technologies 社、Sam Leffler 氏および Errno Consulting 社によって記述された、以下の使用許諾に基づくソフトウェアが含まれています。

Copyright (c) 2001 Atsushi Onoe
Copyright (c) 2002-2008 Sam Leffler, Errno Consulting
All rights reserved.

Copyright (c) 2001 Atsushi Onoe
Copyright (c) 2002-2009 Sam Leffler, Errno Consulting
All rights reserved.

Copyright (c) 2003-2008 Sam Leffler, Errno Consulting
All rights reserved.

Copyright (c) 2005-2008 Sam Leffler, Errno Consulting
All rights reserved.

Copyright (c) 2005-2009 Sam Leffler, Errno Consulting
All rights reserved.

Copyright (c) 2007-2008 Sam Leffler, Errno Consulting
All rights reserved.

Copyright (c) 2007-2009 Sam Leffler, Errno Consulting
All rights reserved.

Copyright (c) 2004 Video54 Technologies, Inc.
Copyright (c) 2004-2008 Sam Leffler, Errno Consulting
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.

本製品には、Damien Bergamini 氏によって記述された、以下の使用許諾に基づくソフトウェアが含まれています。

Copyright (c) 2006
Damien Bergamini <damien.bergamini@free.fr>

Copyright (c) 2007,2008
Damien Bergamini <damien.bergamini@free.fr>

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

本製品には、David Young 氏によって記述された、以下の使用許諾に基づくソフトウェアが含まれています。

Copyright (c) 2003, 2004 David Young. All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of David Young may not be used to endorse or promote products derived from this software without specific prior written permission.

本製品には、Jouni Malinen 氏、Sam Leffler 氏、Instant802 Networks 社および Devicescape Software 社によって記述された、以下の使用許諾に基づくソフトウェアが含まれています。

Copyright (c) 2002-2004, Jouni Malinen <jkmaline@cc.hut.fi>

Copyright (c) 2002-2005, Jouni Malinen <jkmaline@cc.hut.fi>

Copyright (c) 2002-2006, Jouni Malinen <jkmaline@cc.hut.fi>

Copyright (c) 2003-2005, Jouni Malinen <jkmaline@cc.hut.fi>

Copyright (c) 2004-2005, Jouni Malinen <jkmaline@cc.hut.fi>

Copyright (c) 2004-2006, Jouni Malinen <jkmaline@cc.hut.fi>

Copyright (c) 2005, Jouni Malinen <jkmaline@cc.hut.fi>

Copyright (c) 2005-2006, Jouni Malinen <jkmaline@cc.hut.fi>

Copyright (c) 2006, Jouni Malinen <jkmaline@cc.hut.fi>

Copyright (c) 2004, Sam Leffler <sam@errno.com>

Copyright 2002-2003, Instant802 Networks, Inc.

Copyright 2005-2006, Devicescape Software, Inc.

Copyright 2002-2003, Jouni Malinen <jkmaline@cc.hut.fi>

Copyright 2003-2004, Instant802 Networks, Inc.

Copyright 2006, Devicescape Software, Inc.

Copyright 2003, Jouni Malinen <jkmaline@cc.hut.fi>

Copyright 2003-2004, Instant802 Networks, Inc.

Copyright 2005-2006, Devicescape Software, Inc.

Copyright 2003-2006, Jouni Malinen <jkmaline@cc.hut.fi>

Copyright 2003-2004, Instant802 Networks, Inc.

Copyright 2005-2006, Devicescape Software, Inc.

Copyright (c) 2003-2006, Jouni Malinen <jkmaline@cc.hut.fi>

Copyright (c) 2004, Instant802 Networks, Inc.

Copyright (c) 2005-2006, Devicescape Software, Inc.

Copyright (c) 2002-2004, Instant802 Networks, Inc.

Copyright (c) 2005-2006, Devicescape Software, Inc.

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(s) of the above-listed copyright holder(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

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.....	14
1.1.1	VLAN.....	14
1.2	本装置の設定の概要.....	15

1.1 レイヤ2 ネットワーク設計概念

適用機種 SR-M50AP1

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2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。

この2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。

1.2 本装置の設定の概要

適用機種 SR-M50AP1

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。
- ieee80211 定義
本装置の無線 LAN に関する物理的な情報を定義する命令群です。無線 LAN の通信モード (IEEE802.11a/b/g/n/ac) やチャネルなどに関する情報を定義します。
- wlan 定義
本装置の無線 LAN インタフェースに関する情報を定義する命令群です。無線 LAN インタフェースごとに動作タイプ (アクセスポイント、WDS、スキャン専用)、SSID、認証・暗号化方式などに関する情報を定義します。
- vlan 定義
VLAN に関する情報を定義する命令群です。静的な学習テーブルの情報などを定義します。
- 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。また、DHCP などの LAN に固有のサービスに関しても lan 定義によって定義します。
- 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
IP インタフェース
IP 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。

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, ...

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。

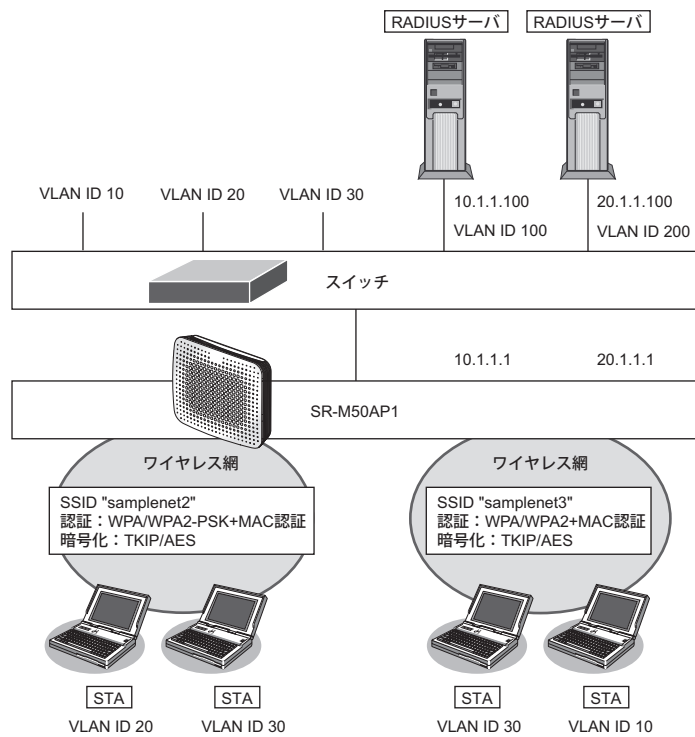
2.1	無線 LAN 機能	19
2.1.1	無線 LAN 通信規格	20
2.1.2	認証・暗号化機能	20
2.1.3	SSID 非通知（ステルス機能）	21
2.1.4	ANY 接続拒否（ANY キープロテクション）	22
2.1.5	MAC アドレスフィルタ	22
2.1.6	端末台数制限／端末台数最低保証	22
2.1.7	WDS ブリッジ機能	24
2.1.8	プライバシープロテクション機能（AP ブリッジ）	25
2.1.9	仮想アクセスポイント機能（VAP）	25
2.1.10	WMM 機能（IEEE802.11e）	26
2.1.11	PMK キャッシュ機能	27
2.1.12	周辺アクセスポイント検出機能	27
2.1.13	11g プロテクション機能	28
2.1.14	HT プロテクション機能	29
2.1.15	ショートガードインターバル	30
2.1.16	チャンネルボンディング機能	30
2.1.17	MIMO Power Save 機能	30
2.1.18	認証自動切替機能	31
2.1.19	ノイズ回避機能	31
2.2	オートネゴシエーション機能	32
2.3	AutoMDI/MDI-X 機能	33
2.4	フロー制御機能	34
2.5	VLAN 機能	36
2.6	ポート閉塞機能	38
2.7	バックアップポート機能	40
2.8	リンクインテグリティ機能	41
2.9	フィルタリング機能	42
2.9.1	動的フィルタリング（SPI）	43
2.10	IEEE802.1X 認証機能	44
2.11	MAC アドレス認証機能	48

2.12	DHCP 機能	49
2.12.1	IPv4 DHCP 機能	49
2.13	RADIUS 機能	50
2.14	DNS サーバ機能	52
2.14.1	DNS サーバ (スタティック) 機能	52
2.14.2	ProxyDNS (DNS 振り分け) 機能	52
2.15	SNMP 機能	54
2.16	SSH サーバ機能	56
2.17	USB メモリ機能	58
2.17.1	構成定義の転送と保存	59
2.18	アプリケーションフィルタ機能	60
2.19	IDS 機能	61
2.20	ProxyARP 機能	62
2.21	POE 機能	63
2.22	高速転送モード	64
2.23	無線 LAN 管理機能	65

2.1 無線LAN機能

適用機種 SR-M50AP1

IEEE802.11 に準拠した無線LANアクセスポイント動作を行うことができます。



2.1.1 無線 LAN 通信規格

SR-M50AP1

IEEE802.11 準拠する以下の無線 LAN 通信規格をサポートします。

本装置は各規格での Wi-Fi 認定を取得しています。本装置に接続する機器は、相互接続性を確保するため Wi-Fi 認定を取得済みの機器とすることを推奨します。

- IEEE802.11b (1-14ch)
- IEEE802.11g (1-13ch)
- IEEE802.11a (W52 : 36/40/44/48ch)
- IEEE802.11a (W53 : 52/56/60/64ch)
- IEEE802.11a (W56 : 100/104/108/112/116/120/124/128/132/136/140ch)
- IEEE802.11n (2.4GHz) (1-13ch)
- IEEE802.11n (5GHz) (W52 : 36/40/44/48ch)
- IEEE802.11n (5GHz) (W53 : 52/56/60/64ch)
- IEEE802.11n (5GHz) (W56 : 100/104/108/112/116/120/124/128/132/136/140ch)
- IEEE802.11ac (W52 : 36/40/44/48ch)
- IEEE802.11ac (W53 : 52/56/60/64ch)
- IEEE802.11ac (W56 : 100/104/108/112/116/120/124/128/132/136/140ch)

 参照 マニュアル「コマンド設定事例集」の無線 LAN の構築に関する記述

2.1.2 認証・暗号化機能

SR-M50AP1

無線 LAN 機能として IEEE802.11 標準の以下の認証・暗号化方式をサポートします。

 補足 AES 暗号化は、ハードウェアによる暗号化を行います。

認証種別	認証方式	EAP プロトコル	暗号化方式
OPEN 認証	-	-	
	IEEE802.1X 連携	MD5	WEP64, WEP128, なし
		TLS	
		TTLS	
		PEAP0	
		PEAP1	
		SIM	
		AKA	
		FAST	
		AKA-PRIME	
SHARED 認証	共通鍵認証	-	
	IEEE802.1X 連携	MD5	

認証種別	認証方式	EAP プロトコル	暗号化方式
		TLS	WEP64, WEP128
		TTLS	(静的 WEP のみ)
		PEAP0	
		PEAP1	
		SIM	
		AKA	
		FAST	
		AKA-PRIME	
WPA 認証	事前共有キー認証	-	
	IEEE802.1X 連携	TLS	
		TTLS	TKIP, AES
		PEAP0	
		PEAP1	
		SIM	
		AKA	
		FAST	
		AKA-PRIME	
WPA2 認証	事前共有キー認証	-	
	IEEE802.1X 連携	TLS	
		TTLS	TKIP, AES
		PEAP0	
		PEAP1	
		SIM	
		AKA	
		FAST	
		AKA-PRIME	

こんな事に気をつけて

IEEE802.11n/ac 通信を行うときは、暗号化方式として WEP および TKIP は使用できません。定義した場合は無効な設定として無線 LAN インタフェースが使用できません。

☞ 参照 マニュアル「コマンド設定事例集」

2.1.3 SSID 非通知（ステルス機能）

適用機種 SR-M50AP1

SSID 非通知は、無線 LAN の不正利用を防ぐための処置の 1 つで、ステルス機能と呼ばれます。

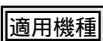
無線 LAN アクセスポイントから送信されるビーコンの中には SSID が含まれているため、電波が届く範囲にある無線 LAN 端末がビーコンを受信することで、無線 LAN アクセスポイントの存在と SSID を知ることができます。

第三者が無断で SSID を設定して使用してしまう危険性を少なくするため、ビーコンに SSID を含めないようにすることで無線 LAN アクセスポイントの存在を隠蔽することができます。



SSID 非通知を有効にすると ANY 接続拒否が同時に動作します。

2.1.4 ANY 接続拒否 (ANY キープロテクション)



SR-M50AP1

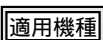
任意の無線 LAN アクセスポイントにも接続できる「ANY」接続という SSID を指定しない接続方法があり、無線 LAN 端末が SSID を指定しないで「ANY」とすることで周辺の無線 LAN アクセスポイントに接続できます。

このようなしくみを逆にとり悪意のある第三者が無線 LAN を不正利用する危険性を少なくするため、「ANY」で接続を行おうとする無線 LAN 端末を接続拒否することができます。



SSID 非通知を有効にすると同時に動作します。

2.1.5 MAC アドレスフィルタ



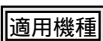
SR-M50AP1

MAC アドレスフィルタリング機能は、無線 LAN 端末の MAC アドレスを判別し、無線 LAN アクセスポイントへの接続を制御することでセキュリティを向上させることができます。

SR-M50AP1 では、送信元 MAC アドレス（無線 LAN 端末の MAC アドレス）のみをフィルタリングの対象とします。

参照 マニュアル「コマンド設定事例集」

2.1.6 端末台数制限／端末台数最低保証



SR-M50AP1

無線 LAN 端末の接続台数過多により発生する通信品質の低下などを防止するため、無線 LAN モジュールごとに無線 LAN 端末の接続台数を制限することができます。

また、仮想アクセスポイントを構築する場合に、接続台数の制限により保守用などの端末が接続不可となることがないように、仮想アクセスポイントごとに接続可能な無線 LAN 端末の台数を保証することができます。

こんな事に気をつけて

- 端末台数最低保証機能の最低保証台数が設定されていた場合、最低保証台数分は本機能の接続可能台数の中から確保されます。そのため、接続可能台数に到達する前に無線 LAN 端末が接続できなくなることがあります。
最低保証されていない接続可能な無線 LAN 端末台数を増やすには、本機能の接続可能台数を増やしてください。
- 無線 LAN 端末が端末台数制限により接続に失敗し、接続先をほかの無線 LAN アクセスポイントへ変更する動作については、SR-M50AP1 は失敗理由を伝えて変更を促すだけとなります。実際に接続先が変更されるには、無線 LAN 端末が接続先を切り替える動作をサポートする必要があります。
- ある無線 LAN モジュールの仮想アクセスポイントすべてに設定されている最低保証台数の合計が、同無線 LAN モジュールの端末台数制限機能による接続可能台数を超えないように設定してください。
- 最低保証する台数は、端末台数制限機能の接続可能台数の中から確保されます。そのため、接続可能台数に到達する前に無線 LAN 端末が接続できなくなることがあります。

- 2.4GHz 帯で TKIP 認証端末を複数台接続する場合、認証キーの割り当て数上限超過により、端末可能台数に到達する前に無線 LAN 端末が接続できなくなることがあります。

無線LANモジュール 接続可能台数		
仮想アクセスポイント1 最低保証台数	仮想アクセスポイント2 最低保証台数	最低保証されていない 接続可能台数

 参照 「2.1.9 仮想アクセスポイント機能 (VAP)」(P25)、
マニュアル「コマンド設定事例集」の「端末台数制限機能を使う」および「端末台数最低保証機能を使う」に関する記述

2.1.7 WDSブリッジ機能

適用機種 SR-M50AP1

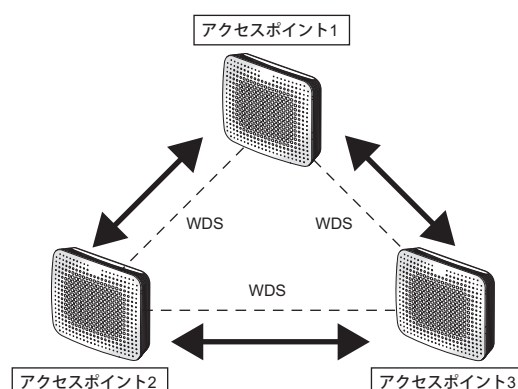
WDS (Wireless Distribution System) ブリッジは、無線 LAN アクセスポイントどうしの通信を可能にする機能です。

ある無線 LAN アクセスポイントを中継して別の無線 LAN アクセスポイントとデータの送受信を行うことができるため、単一の無線 LAN アクセスポイントを使用した場合に比べて広い範囲での通信が可能となります。

SR-M50AP1 では WDS ブリッジのみで無線 LAN ネットワークを構築することができます。

こんな事に気をつけて

- 相手無線 LAN アクセスポイントと同じチャンネル、通信モードで動作させてください。また、WDS のみで運用する場合、any 以外のチャンネルを設定してください。
- WDS ブリッジの相手側無線 LAN インタフェースの MAC アドレスは正確に設定してください。
 なお、SR-M50AP1 の無線 LAN の MAC アドレスは、show system information コマンドで確認することができます。wlan コマンドで定義した無線 LAN インタフェースについて、インタフェース番号が小さいものから順に連続した値の MAC アドレスが割り当てられます。
 動作中の無線 LAN インタフェースの MAC アドレスは、show wlan status コマンドで確認することができます。
- 参照 マニュアル「コマンドリファレンス」の「show system information」、「show wlan status」
- 本機能のブリッジ処理は、同一の VLAN に割り当てられたインタフェース間でのみ行われます。WDS ブリッジ機能を使用する場合は、WDS 用のインタフェースを含み、対象のインタフェース (ether、wlan など) が同一の VLAN となるように設定してください。
- 他社の無線 LAN アクセスポイントとの接続はできません。
- WDS ブリッジを行う無線 LAN アクセスポイント間では、接続認証、接続要求などの手順は行いません。また、利用できる暗号化方式は WEP 暗号化のみです。
- 無線 LAN アクセスポイント 1 台との WDS ブリッジには、無線 LAN インタフェース 1 つを WDS 用のインタフェースとして使用します。そのため、WDS 用のインタフェースを生成した数だけ、仮想アクセスポイントとして利用できる無線 LAN インタフェースが減少することになります。
- 無線 LAN チャンネルが W53/W56 で動作している場合、レーダを検出することがあります。レーダを検出した場合、チャンネルが自動的に切り替わり、一時的に通信ができなくなることがあります。WDS のみで運用している場合は、チャンネルの切り替えは行われません。レーダを検出したチャンネルは 30 分間使用することができないため、WDS のみで運用している場合は、レーダ検出後 30 分間動作を停止します。
- WDS を利用した以下の図のような冗長なネットワーク構成では、無線 LAN 上でのパケットのループが発生するため、このようなネットワーク構成は取らないでください。



- WDS ブリッジを行う無線 LAN アクセスポイント間では、IEEE802.11n/ac を使用することはできません。
 無線通信モードに 11n および 11ac を含む設定をされた場合、2.4G 帯では 11g で、5G 帯の場合は 11a で動作します。

■ 参照 マニュアル「コマンド設定事例集」

2.1.8 プライバシープロテクション機能 (AP ブリッジ)

適用機種 SR-M50AP1

プライバシープロテクションは、無線 LAN アクセスポイント内部でブリッジ（無線 LAN 端末間）を無効にする機能です。

同じ無線 LAN アクセスポイントに接続している無線 LAN 端末はお互いに通信できますが、プライバシープロテクション機能を利用する場合は、無線 LAN 端末間の通信をフィルタリングすることができます。

ほかの無線 LAN 端末からの個人情報の盗み見や共有フォルダへのアクセスを防御でき、ホットスポットサービスなどの不特定多数の利用者が存在する環境で各利用者のプライバシーを保護します。

本機能は仮想アクセスポイント利用時にも動作可能です。

こんな事に気をつけて

プライバシープロテクション機能は、同一仮想アクセスポイント内の端末どうしの通信を防止するものであり、同一の VLAN ID を指定した複数の無線 LAN インタフェース間の通信については可能です。

2.1.9 仮想アクセスポイント機能 (VAP)

適用機種 SR-M50AP1

本装置では、1つの無線 LAN モジュールで複数の無線 LAN ネットワークを構築することができ、無線 LAN インタフェースおよび有線 LAN インタフェースに対し、VLAN 機能を使うことによって、無線 LAN 端末のパケットを、有線 LAN 側に中継することができます。

無線 LAN ネットワークは無線 LAN インタフェースごとに定義でき、各無線 LAN インタフェースは仮想アクセスポイント (VAP) として使用することができます。仮想アクセスポイントには、同一または異なる SSID を割り当てることができ、また、異なるセキュリティポリシーを設定することができます。

仮想アクセスポイントに無線 LAN 端末が接続された際、パケットの中継に必須となる VLAN ID を割り当てる方式として、SR-M50AP1 では固定 VLAN 割り当て方式および認証 VLAN 割り当て方式をサポートします。また、複数の仮想アクセスポイントに対する同一 VLAN の固定割り当ても可能です。

- 固定 VLAN 割り当て方式
VAP に対してあらかじめ固定の VLAN ID を設定しておくことで、端末が接続された場合にその VLAN を固定的に割り当てる方式です。
同一の VLAN が設定されたインタフェースに対してのみブリッジ中継が行われるため、無線 LAN に接続された端末を、仮想アクセスポイント (VAP) 単位に VLAN を振り分けることができます。
- 認証 VLAN 割り当て方式
IEEE802.1X や MAC アドレス認証を経て接続された端末に対して、RADIUS サーバから払い出された VLANID を割り当てる方式で、無線 LAN 端末単位に VLAN を振り分けることができます。
VLANID は認証ごとに更新可能であり、払い出しがない場合は認証機能に設定された初期 ID を割り当てます。

こんな事に気をつけて

同一の SSID かつ同一の認証・暗号化方式の仮想アクセスポイントを設定した場合、どちらの仮想アクセスポイントに接続されるかは不定となります。

 参照 マニュアル「コマンド設定事例集」

2.1.10 WMM機能 (IEEE802.11e)

適用機種 SR-M50AP1

WMMは、無線LANインタフェースに送出するパケットの優先制御を行う機能です。

本機能を利用することで、トラフィックが多い場合でも、音声やビデオなどのパケットを優先的に送出することができます。

無線に送出するパケットはIPパケットのDSCP値を元に4種類の優先クラス Access Category (AC) に分類し、優先度が高い方からAC_VO (音声)、AC_VI (ビデオ)、AC_BE (ベストエフォート)、AC_BK (バックグラウンド) であり、無線LANモジュールではACごとに送信キューを持ち、送信キューにパケットが溜まっている場合は、優先度が高いACの送信キューから優先的にパケットが送信されます。

こんな事に気をつけて

- 以下のパケットは常に同じACに分類されます。

種別	AC
EAPOL パケット	AC_VO
ARP パケット	AC_VO
IP ヘッダを含まないパケット	AC_BE
WMMに対応していない端末あてのパケット	AC_BE

- 本機能は無線LANモジュール単位で制御するため、本機能の有効化／無効化を仮想アクセスポイントごとに設定することはできません。同一の無線LANモジュールを使用しているほかの仮想アクセスポイントのトラフィックの状況によっては、優先度の高いパケットでも送出が遅れる場合があります。
- WMM機能を使うためには、無線LANアクセスポイントのWMM機能も有効にする必要があります。

本装置では振り分けに利用するDSCP値は6bitのうち先頭3bitを参照し、以下の表に従って分類します。

また、ACLを利用することで特定パケットに対する優先クラスを任意に変更することもできます。

ただし、ACLによる変更は2.4G帯の無線LANインタフェースでのみ動作し、5G帯では動作しません。

DSCP 値			AC 分類
	10 進数の値	先頭 3bit の値	
0x38 ～ 0x3f 0x30 ～ 0x37	56 ～ 63 48 ～ 55	7 6	AC_VO
0x28 ～ 0x2f 0x20 ～ 0x27	40 ～ 47 32 ～ 39	5 4	
0x18 ～ 0x1f 0x00 ～ 0x07	24 ～ 31 0 ～ 7	3 0	AC_BE
0x10 ～ 0x17 0x08 ～ 0x0f	16 ～ 23 8 ～ 15	2 1	AC_BK

 参照 マニュアル「コマンド設定事例集」

2.1.11 PMK キャッシュ機能

適用機種 SR-M50AP1

PMK キャッシュ機能は、無線 LAN 接続時に利用される PMK（暗号鍵のマスタ）を、無線 LAN アクセスポイント、無線 LAN 端末双方がキャッシュしておき、接続の際にキャッシュが一致した場合に IEEE802.1X 認証を省略とすることで、無線 LAN 端末の「再接続」に要する接続時間の短縮を可能とする機能です。

2.1.12 周辺アクセスポイント検出機能

適用機種 SR-M50AP1

無線電波をスキャンすることにより、周辺の無線 LAN アクセスポイントを検出することができます。

ネットワークに不正（想定外）なアクセスポイントが存在すると通信に異常が起こることがあり、定期的に周辺アクセスポイントの状況を把握することで未然に問題を防ぐことができます。

- SR-M50AP1
手動スキャン、および自動スキャンによる周辺アクセスポイント検出が行えます。
手動スキャンを実施することで最新の周辺アクセスポイントを検出することができます。
自動スキャンには、運用中スキャンモード、スキャン専用モードがあります。
各モードについて以下に説明します。

運用中スキャンモード

無線 LAN アクセスポイントの運用をしながら無線電波をスキャンすることで、周辺の無線 LAN アクセスポイントを検出することができます。検出は現在運用中のチャンネルだけで行います。
無線 LAN アクセスポイントの運用では、スループットが低下することがあります。
また、電波干渉により近隣チャンネルで動作している無線 LAN アクセスポイントも検出されることがあります。

スキャン専用モード

無線 LAN アクセスポイントの運用をしないでスキャン動作だけを行います。周辺の無線 LAN アクセスポイント無線 LAN モジュールで利用可能なすべてのチャンネルで検出することができます。
レーダ検出などにより利用不可中のチャンネルは検出の対象外となります。

こんな事に気をつけて

- 無線 LAN アクセスポイントの運用では、スループットが低下することがあります。
- 電波干渉により近隣チャンネルで動作している無線 LAN アクセスポイントも検出されることがあります。
- スキャン専用モードで使用する場合、無線 LAN 端末との接続はできません。
- レーダ検出などにより利用不可中のチャンネルは検出の対象外となります。

 参照 マニュアル「コマンド設定事例集」

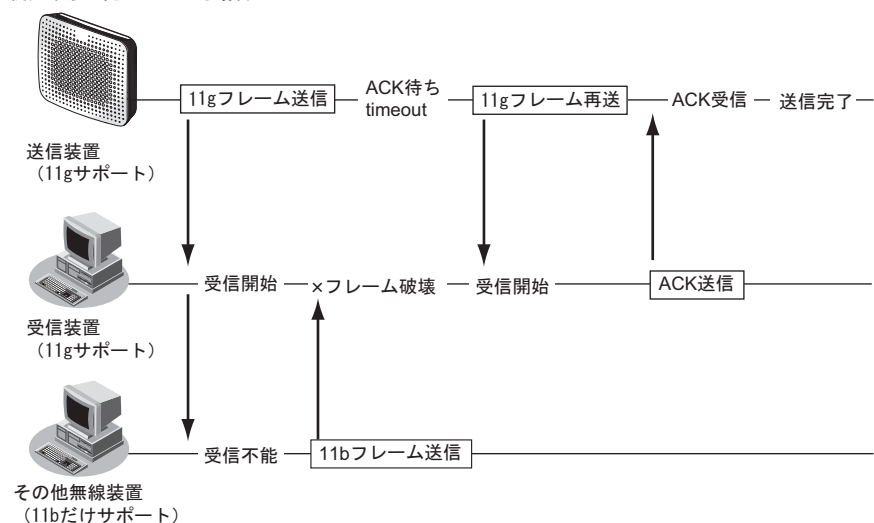
2.1.13 11g プロテクション機能

適用機種 SR-M50AP1

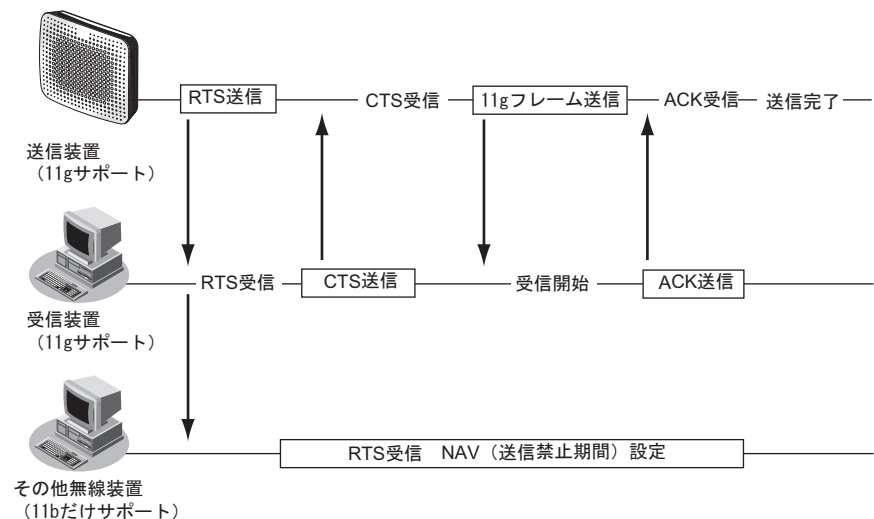
11g プロテクションとは、11b と 11g の装置が混在する環境で通信した場合に発生する、スループットの低下を抑止する機能です。

11b の装置は 11g での通信を理解できないため、11g の通信中に通信フレームを送信してしまう場合があります。この場合、フレーム破壊により通信がエラーとなり、再送が発生して結果 11g の装置のスループットが低下します。これを防ぐため、11g での通信に先立って、11b の装置が理解できる RTS または CTS-to-self のフレームを送信する機能が 11g プロテクションです。11b の装置に対し、RTS および CTS-to-self によってキャリアの占有時間を通知し、11g の通信が行われる間 11b の通信を抑止することで、11g の通信を保護することができます。

例) 干渉が発生している場合



例) RTS/CTSでプロテクションを動作させた場合



こんな事に気をつけて

本機能は常に有効です。

2.1.14 HT プロテクション機能

適用機種 SR-M50AP1

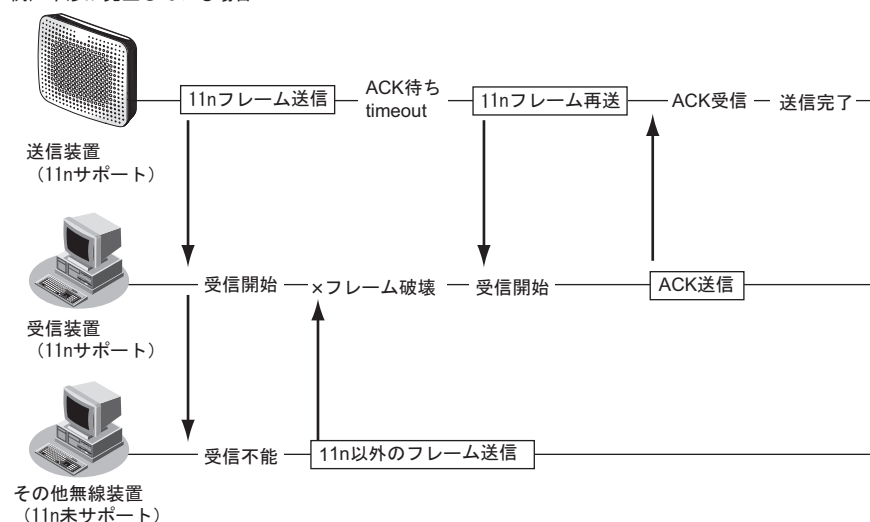
HT プロテクションとは、11n と 11a/11b/11g の装置およびチャネルボンディング機能の使用・未使用の装置が混在する環境で通信した場合に発生する、スループットの低下を抑止する機能です。

11a/11b/11g の装置は 11n での通信を理解できないため、11n の通信中に通信フレームを送信してしまう場合があります。この場合、フレーム破壊により通信がエラーとなり、再送が発生して結果 11n の装置のスループットが低下します。これを防ぐため、11n での通信に先立って、11a/11b/11g の装置が理解できる RTS のフレームを送信する機能が HT プロテクションです。11a/11b/11g の装置に対し、RTS によってキャリアの占有時間を通知し、11n の通信が行われる間 11a/11b/11g の通信を抑止することで、11n の通信を保護することができます。

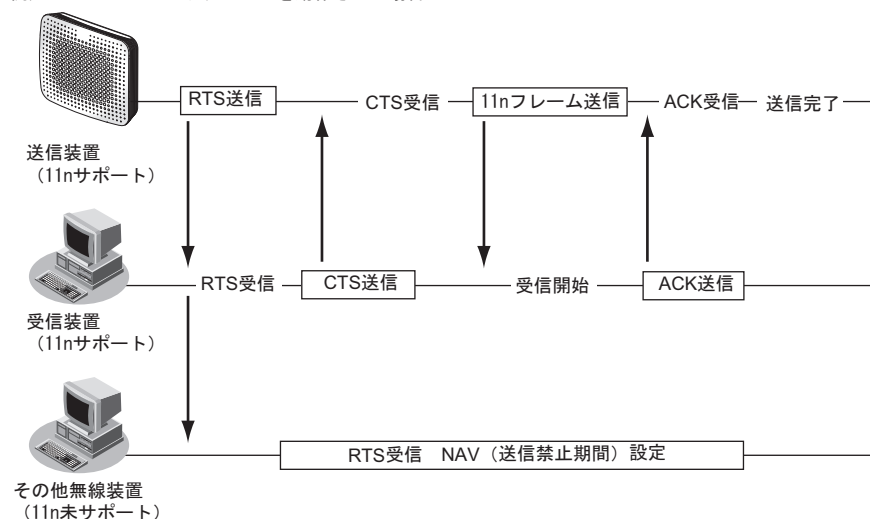
チャネルボンディング機能の使用・未使用の混在時も、未使用の装置は 40MHz 幅での通信を理解できないため、同様のことが起こります。

この場合も HT プロテクションを利用することで、40MHz 幅での通信を保護することができます。

例) 干渉が発生している場合



例) RTS/CTSでプロテクションを動作させた場合



こんな事に気をつけて

- 本機能は 11n 使用時に常に有効です。
- 本装置では HT プロテクションのモードは RTS 固定となり、モード変更は動作しません。

2.1.15 ショートガードインターバル

適用機種 SR-M50AP1

ショートガードインターバルとは、IEEE802.11n および IEEE802.11ac 規格のオプション機能で、11a/11g で 800 ナノ秒であったガードインターバルを 400 ナノ秒で使用するものです。

ショートガードインターバルを使用することで、800 ナノ秒のガードインターバルと比較して通信速度が約 1.1 倍に向上します。

こんな事に気をつけて

- ・ ショートガードインターバルは、無線 LAN アクセスポイントおよび無線 LAN クライアントの両方で有効である場合にだけ動作します。
- ・ ショートガードインターバルは反射波の影響を受けやすいため、オフィスや家庭など無線 LAN アクセスポイントおよび無線 LAN クライアントの距離が近い環境での使用を推奨します。

2.1.16 チャネルボンディング機能

適用機種 SR-M50AP1

チャネルボンディングとは、IEEE802.11n および IEEE802.11ac 規格のオプション機能で、複数のチャネルを束ねて通信する機能です。

40MHz または 80MHz の帯域幅を使用するため、通信速度が 2 倍または 4 倍に向上します。

こんな事に気をつけて

- ・ チャネルボンディングを使用する場合、無線 LAN アクセスポイントおよび無線 LAN クライアントの両方でチャネルボンディングを有効にする必要があります。
- ・ 2.4GHz 帯では、セカンダリチャネルに他 BSS のプライマリチャネルが存在する場合は自動的に 20MHz 幅の BSS を開始します。
- ・ 5GHz 帯では無線 LAN アクセスポイントが運用を開始したあと、他無線 LAN 装置と電波干渉が発生しても、帯域幅を 20MHz に縮退動作することはありません。
- ・ 2.4GHz 帯では重なり合わない 40MHz チャネルが 1 つしか確保できないことに加え、ほかのチャネルとの干渉が発生しやすいため、チャネルボンディングは 5GHz 帯での使用を推奨します。

 参照 マニュアル「コマンド設定事例集」

2.1.17 MIMO Power Save 機能

適用機種 SR-M50AP1

MIMO Power Save とは、無線ネットワークのスループットと通信品質を向上する MIMO (Multiple Input Multiple Output) の電力消費を抑えるための IEEE802.11n および IEEE802.11ac 規格の機能です。

MIMO は複数のアンテナを利用するため、搭載するアンテナの数が多いほど、1 本のアンテナしか利用しない旧規格の無線 LAN クライアントと比べ多くの電力を消費します。この電力消費を抑える機能として、無通信時に 1 つのアンテナを残して、ほかのアンテナの電源を切る MIMO Power Save 機能があります。

本装置は、MIMO Power Save 機能の Dynamic モードまたは Static モードで動作する無線 LAN クライアントとの接続をサポートすることにより、無線 LAN クライアントの電力を削減することができます。

こんな事に気をつけて

MIMO Power Save 機能は本装置に接続する無線 LAN クライアントの電力消費を削減します。
本装置の電力消費を削減することはできません。

2.1.18 認証自動切替機能

適用機種 SR-M50AP1

認証自動切替機能は、IEEE802.1X 認証が定義された無線 LAN インタフェースが利用する RADIUS サーバの監視を行い、RADIUS サーバと通信ができなくなった場合に事前共有キー (PSK) 認証へ認証を切り替えることで、無線 LAN 端末が接続できなくなることを回避し、無線 LAN 通信を継続することができます。

RADIUS サーバの定期監視に限らず、実際の認証要求で応答がない場合もバックアップへの切り替えが行われます。また、バックアップ側インタフェースは PSK 認証に限らず、OPEN / SHARED 認証と MAC アドレス認証との組み合わせも可能です。

 参照 [「2.13 RADIUS 機能」\(P.50\)](#)、
マニュアル「コマンド設定事例集」

2.1.19 ノイズ回避機能

適用機種 SR-M50AP1

ノイズ回避機能は、運用チャンネルに影響する一部のノイズを検出した場合に、チャンネルを変更する機能です。
本機能により、ノイズによる通信影響を緩和できる場合があります。

こんな事に気をつけて

レーダの検出状況により無線 LAN と干渉する電波を検出した場合であってもチャンネルが切り替わらない場合があります。

2.2 オートネゴシエーション機能

適用機種 SR-M50AP1

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ETHERNET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。

接続相手 自装置		Auto-Nego	10M 固定		100M 固定		1000M 固定
			FULL	HALF	FULL	HALF	FULL
Auto-Nego		○ 10M/FULL、10M/HALF 100M/FULL、100M/HALF、 1000M/FULL	× 10M/HALF	○ 10M/HALF	× 100M/HALF	○ 100M/HALF	○ 1000M/FULL
10M 固定	FULL	× 10M/HALF	○ 10M/FULL	×	×	×	×
	HALF	○ 10M/HALF	×	○ 10M/HALF	×	×	×
100M 固定	FULL	× 100M/HALF	×	×	○ 100M/FULL	×	×
	HALF	○ 100M/HALF	×	×	×	○ 100M/HALF	×
1000M 固定	FULL	○ 1000M/FULL	×	×	×	×	○ 1000M/FULL

○：接続可能、×：接続不能（リンク確立するが、通信が異常の場合も含む）

2.3 AutoMDI/MDI-X 機能

適用機種 *SR-M50AP1*

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 ETHERNET 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 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、1000M/FULL 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 として動作します。

MDI/MDI-X の指定 (※)	auto	mdi	mdix
通信モードの指定			
Auto	auto	mdi	mdix
固定	mdi	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

2.4 フロー制御機能

適用機種 SR-M50AP1

本装置では、全二重通信時は 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)。 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)。 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)。 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= 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)。 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。

フロー制御設定が、送信、受信共に on 設定の場合、送受信方向は対称となります。

※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、以下の表のとおり設定されます。

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	D.C.	N	N
		あり	対称	Y	Y
		あり	非対称	Y	Y

※) オートネゴシエーションの結果、送信 Pause=Y となるが、自設定に従って、送信 Pause=N とする。

- 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)

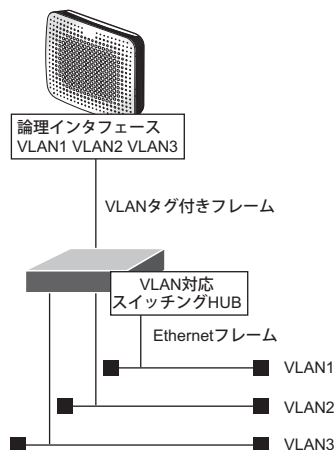
※1) Pause フレーム受信時は無視する。

※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ない。

2.5 VLAN 機能

適用機種 SR-M50AP1

VLAN 機能とは、物理的な LAN を仮想的な複数の LAN に分割する機能です。



SR-M50AP1 でサポートする VLAN 機能は、IEEE802.1q に準拠しています。

SR-M50AP1 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。

VLAN 種別

以下の単位で 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。
- タグ VLAN
フレームに VLAN 番号を記したタグ情報を挿入し、フレーム単位で VLAN の区別を行う機能です。
- 認証 VLAN
認証成功となった端末ごとに、RADIUS サーバから割り当てられた VLAN によって区別を行う機能です。

無線 LAN における VLAN

無線 LAN では SSID と VLAN を対応付け、有線 LAN ポートの VLAN とマッピングして、無線 LAN と有線 LAN ポート間の通信を実現します。認証 VLAN は端末ごとに VLAN を割り当てるため、認証に成功した端末は SSID に関係なく有線 LAN ポートの同一 VLAN へ通信が可能となります。

同一ポート上での VLAN の混在

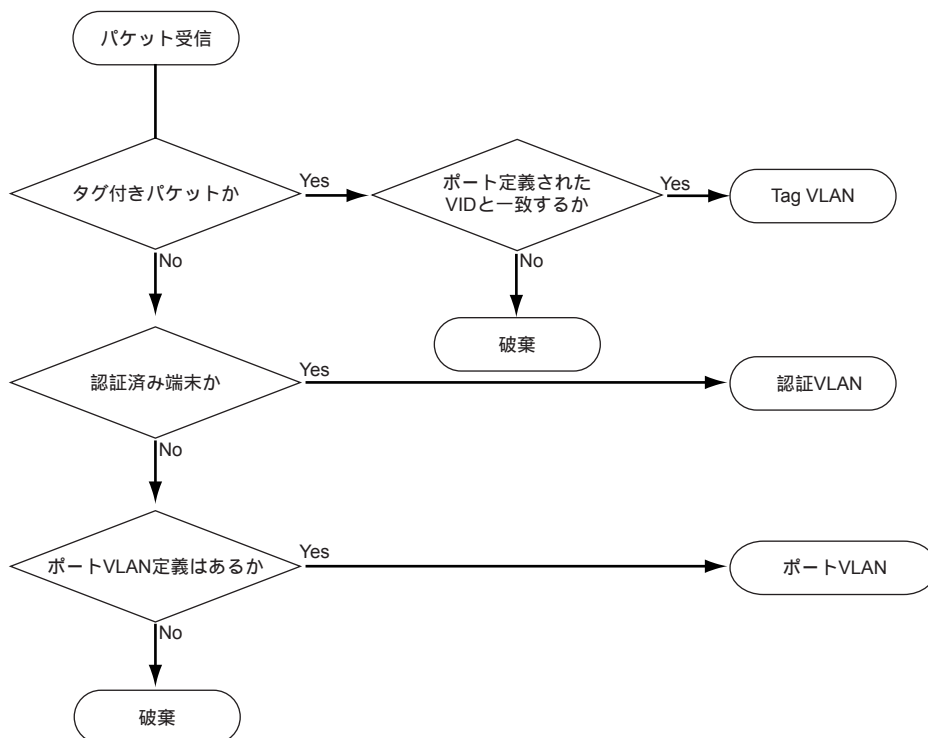
同一ポート上で使用できる VLAN の組み合わせを以下に示します。

○：混在できる、×：混在できない

VLAN 種別	ポート VLAN (untagged)	Tag VLAN (Tagged)
ポート 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。



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。

2.6 ポート閉塞機能

適用機種 SR-M50AP1

ポート閉塞機能とは、物理ポート（Ethernet）または論理インタフェース（無線 LAN インタフェース）のダウン状態（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（Ethernet）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や、論理インタフェース（無線 LAN インタフェース）が通信できない状態になる可能性があります。そのような場合、本装置は意図的にダウン状態（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
- 認証自動切替機能による自動閉塞

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。
- 認証自動切替機能の対象である無線 LAN インタフェースに対して閉塞が行われた場合、認証自動切替機能の対象であるすべての無線 LAN インタフェースが対象となります。

offline コマンド発行による手動閉塞

offline コマンドは、以下を対象に閉塞状態に遷移することができます。

- 物理ポート（Ethernet）
offline ether を発行することにより、対象ポートを閉塞状態とします。
- 論理インタフェース（無線 LAN インタフェース）
offline wlan を発行することにより、対象無線 LAN インタフェース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

バックアップポート機能を使用した場合に、ポート閉塞状態への遷移指定が可能です。

☞ 参照 「2.7 バックアップポート機能」(P.40)

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。

- リンクダウンを契機にした無線 LAN インタフェースの連携閉塞（リンクダウンリレー閉塞（リンクインテグリティ））
リンクダウン時に、構成定義で指定した連携無線 LAN インタフェース番号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、連携無線 LAN インタフェースを同時に閉塞解除することも可能です。

 参照 [「2.8 リンクインテグリティ機能」\(P41\)](#)

認証自動切替による自動閉塞

認証自動切替機能を使用した場合、以下を契機に無線 LAN インタフェースを閉塞状態にします。

- RADIUS サーバからの応答を検出した場合、構成定義で backup 指定した無線 LAN インタフェースを閉塞状態とします。
- RADIUS サーバからの応答が検出できなかった場合、構成定義で master 指定した無線 LAN インタフェースを閉塞状態とし、backup 指定した無線 LAN インタフェースを閉塞解除します。

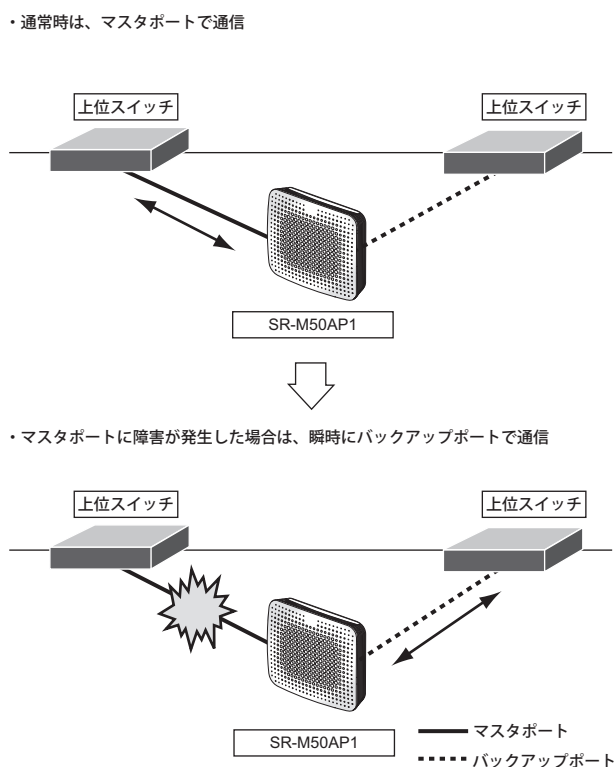
2.7 バックアップポート機能

適用機種 SR-M50AP1

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働させる機能です。

稼働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働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可能です。

グループポートが共にリンクアップしている状態で、マスタポートを必ず優先使用するモードと、先にリンクアップしたポートを使用するモードの選択が可能です。



こんな事に気をつけて

- バックアップポート機能では、障害発生時に稼働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。
- 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。

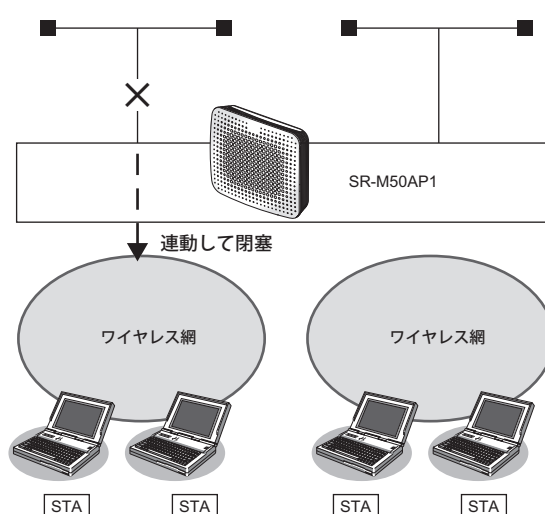
2.8 リンクインテグリティ機能

適用機種 SR-M50AP1

リンクインテグリティ（リンクダウンリレー）機能とは、指定したETHERポートがリンクダウンしたときに、連動して無線LAN インタフェースを閉塞状態に遷移させ、強制的に無線LAN 端末をほかのアクセスポイントにローミングさせる機能です。

リンクダウンしたETHERポートがリンクアップした場合、本機能で閉塞状態にした無線LAN インタフェースを自動的に閉塞解除することができます。また、バックアップポート機能との併用により、指定したバックアップグループの優先／待機ポートの両方がダウン状態となったときに、連動して指定した無線LAN インタフェースを閉塞状態にできます。

☛ 参照 「2.7 バックアップポート機能」(P40)



こんな事に気をつけて

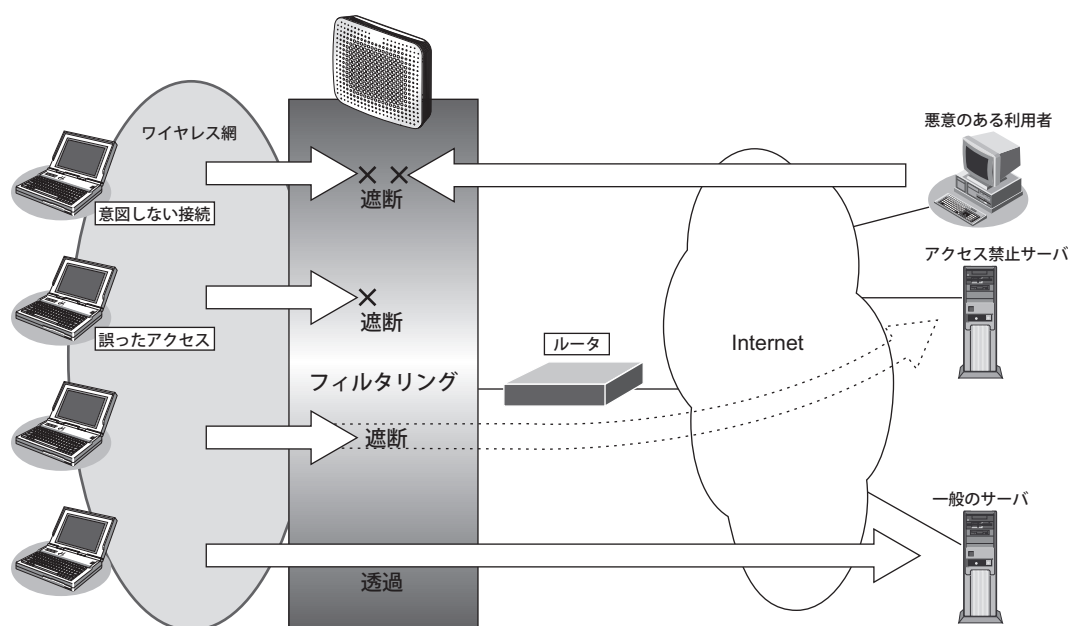
- 指定した無線LAN インタフェースが使用されていない、または、すでに offline 状態のときは、自動的に閉塞解除することはできません。
- 閉塞解除動作がコマンドによる閉塞解除の場合、閉塞された無線LAN インタフェースは online コマンドで閉塞解除してください。
- ETHER ポートの種別がバックアップポート指定、かつ、ether 定義および backup 定義でリンクダウンリレーの設定が行われている場合、ETHER ポートに対する設定は無効となります。

2.9 フィルタリング機能

適用機種 SR-M50AP1

フィルタリング機能では、本装置を経由するパケットをMACアドレス、VLAN ID、IPアドレスや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の向上や、ネットワークへの負荷を軽減することができます。

本装置では、Ethernet フレームに対する MAC アドレスフィルタリング機能および IP パケットに対する IP フィルタリング機能をサポートし、本装置に入力されたパケットが指定された ACL 定義の “acl mac” 定義、“acl ip” 定義、“acl tcp” 定義、“acl udp” 定義または “acl icmp” 定義に該当した場合、同一 VLAN に属する ETHER ポートおよび無線 LAN インタフェースに対して、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
- 本装置以外の要素（ファイアーウォール、ユーザ認証など）

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。

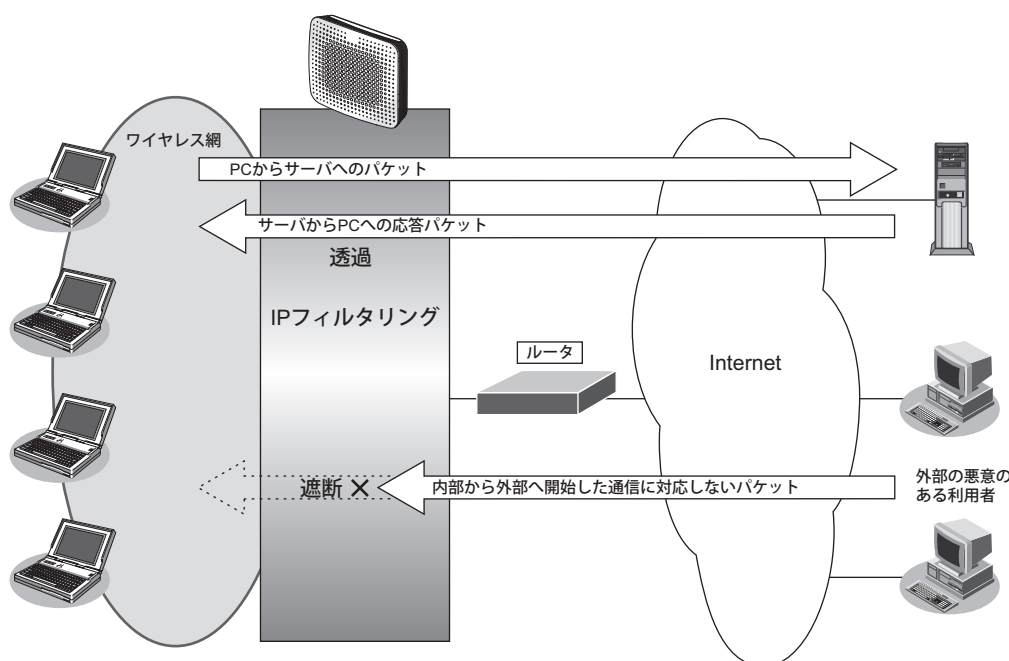
内部ユーザによる不要なアクセスを防ぐ。

● 「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

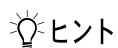
アクセス禁止サーバなどへのアクセスを制限する。

2.9.1 動的フィルタリング (SPI)

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



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



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

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。
- 本装置で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。
- 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。本装置より出力されるパケットは対象となりません。
- SPI対象となるのは本装置に入力されたパケットです。そのため、本装置自身より送出されるパケットは対象となりませんので、本装置から外部側へ通信する場合は、必要な通信を透過させるフィルタリングルールを設定する必要があります。
- “vlan filter”、“serverinfo filter”、“wlan macfilter” コマンドなどのACLを参照する定義は、参照可能上限数を超えた場合、適用されません。
- プライバシープロテクション機能が無効であり、同一仮想アクセスポイント内の端末どうしの通信が可能な場合、端末どうしの通信に対するVLANのフィルタ設定は無効となります。
- 高速転送モードが有効の場合、フィルタ設定は無効となります。

2.10 IEEE802.1X 認証機能

適用機種 SR-M50AP1

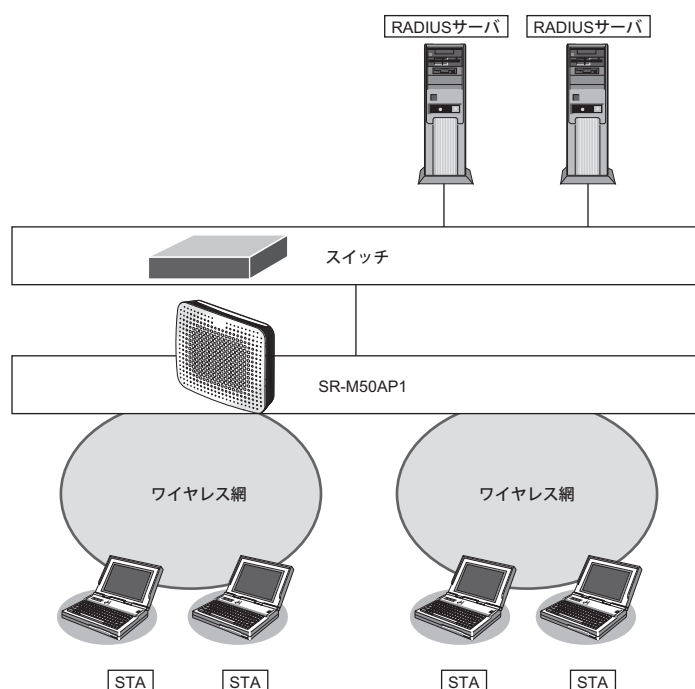
IEEE802.1X 認証機能とは、接続される端末の認証を行いアクセス制御を実施する機能です。

本機能を利用することで、認証許可のないユーザ端末の通信（認証要求を除く）をすべて遮断し、認証されたユーザ端末以外からのネットワークへの不当アクセスを防止します。

本装置では、IEEE802.1Xに準拠した認証機能（802.1X認証）をサポートしています（無線LANインタフェースのみ）。

認証機能は、認証方式「EAP-MD5」、「EAP-TLS」、「EAP-TTLS」、「PEAP」、「SIM」、「AKA」、「FAST」、「AKA-PRIME」での動作を確認しています。認証を行うための認証データベースとして、自装置内のAAA機能を用いたローカル認証と、外部にRADIUSサーバを設置したリモート認証が利用できます。ローカル認証を利用する場合は「EAP-MD5」のみ対応しています。リモート認証を利用する場合は、ローカル認証に比べてより安全な「EAP-TLS」および「EAP-TTLS」などで認証を行います。

RADIUSサーバに属性を設定することによって、認証時、ユーザ端末をVLANに対応付けます。RADIUSサーバからVLAN IDが通知されなかった場合、“wlan dot1x vid”コマンドで設定されたVIDを割り当てます。



こんな事に気をつけて

- 本機能を利用するポートでは、事前にVLANを設定できません。認証成功端末が認証成功時に割り当てられたVLANで通信します。
- AAA機能の課金情報としては通信累計時間のみサポートし、統計値（パケット数、データ量）は、常に0が通知されます。
- 1つの無線LANインターフェースでMACアドレス認証と併用した場合、両方の認証に成功した端末のみ接続できます。その場合、両方の認証で同じVLANを割り当てるようにしてください。

VLAN ID 通知のための属性

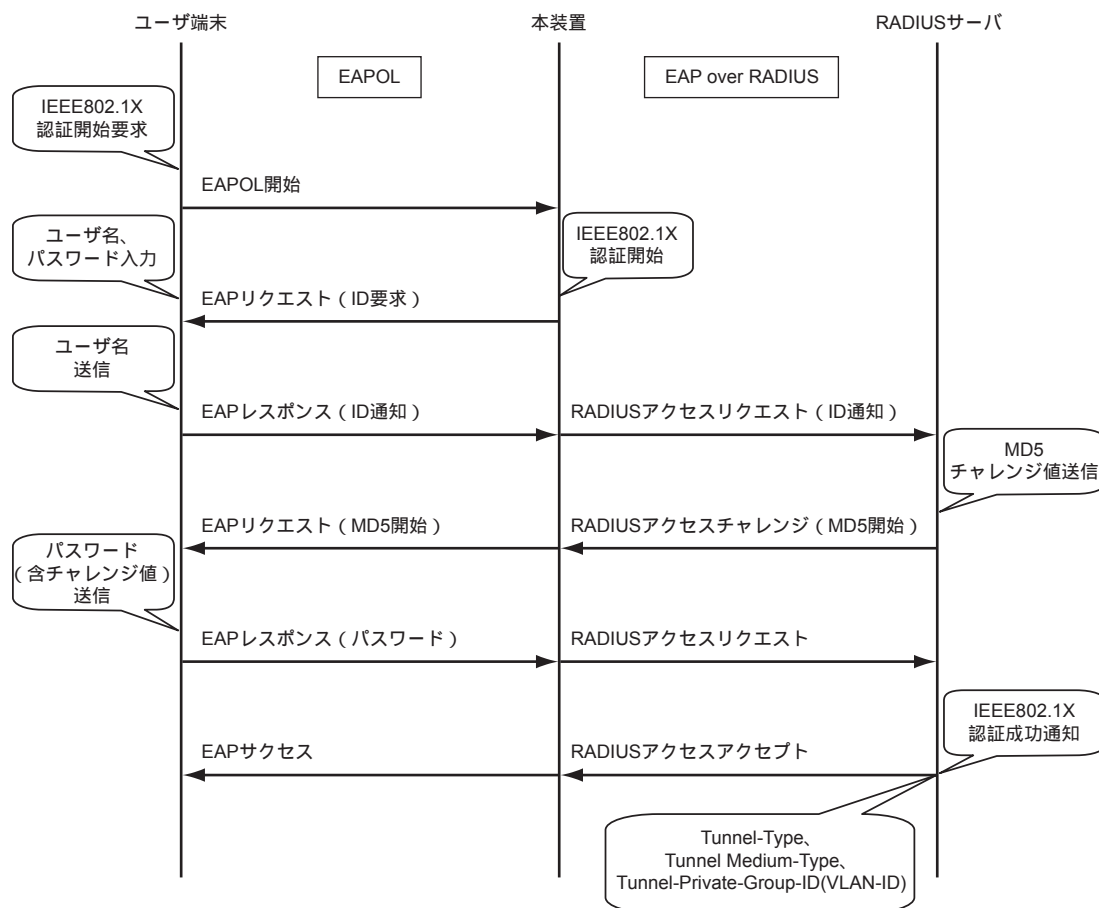
リモート認証時に Supplicant へ割り当てる VLAN ID を RADIUS サーバへ設定する際の属性情報を以下に示します。

名前	番号	属性値 (※)
Tunnel-Type	64	VLAN (13)
Tunnel-Media-Type	65	802 (6)
Tunnel-Private-Group-ID	81	VLAN ID (10 進数表記を ASCII コードでコーディング)

※) () 内の数字は属性として設定される 10 進数の値

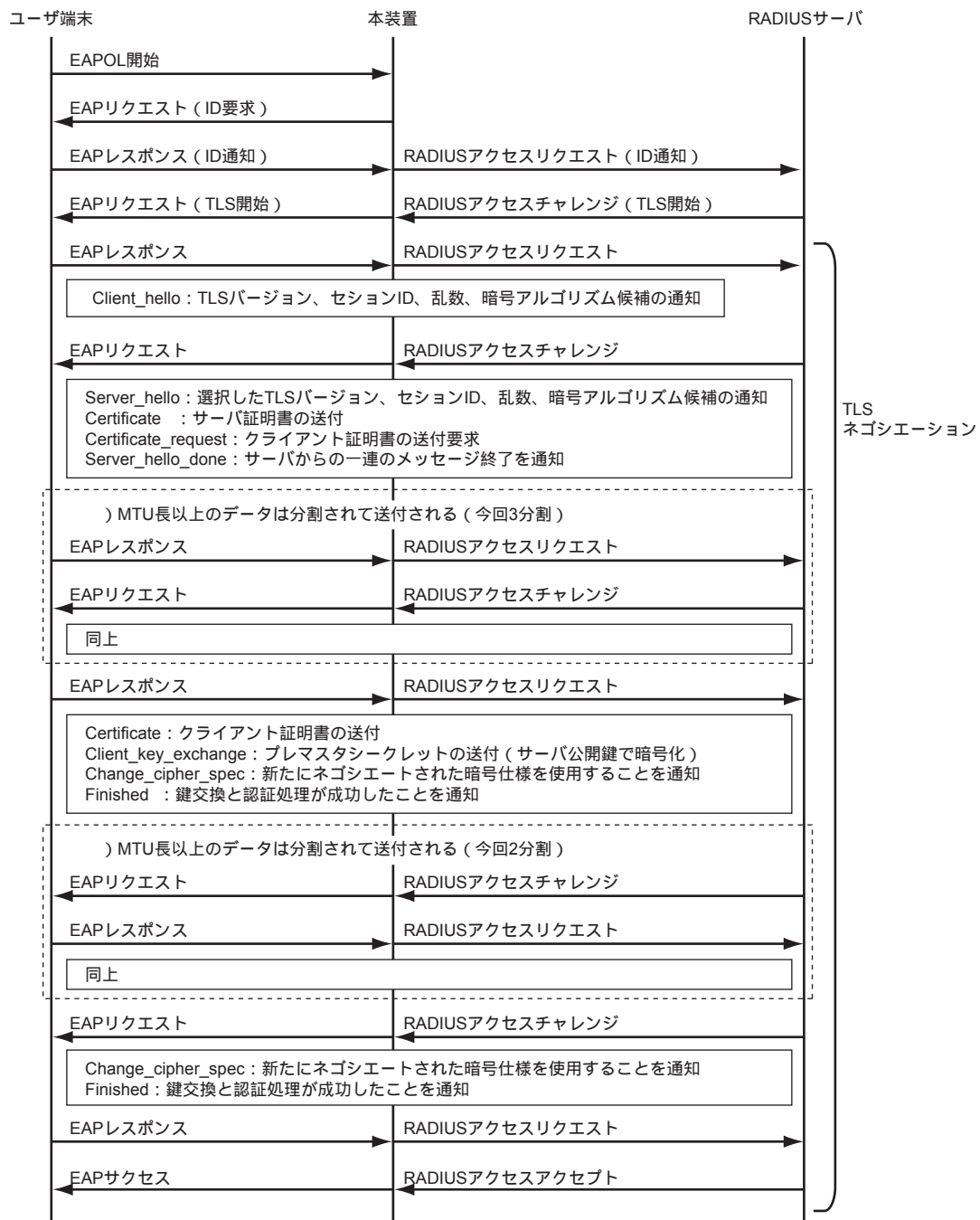
EAP-MD5 認証

EAP-MD5 認証とは、ユーザ端末と RADIUS サーバ間で共通のパスワードを持つことによって、認証する方式です。チャレンジ・レスポンスをやり取りし、MD5 ハッシュ関数によって暗号化して、RADIUS サーバがユーザの認証を行います。ローカル認証時は「RADIUS サーバ」の代わりに本装置内の「AAA 機能」が利用されます。IEEE802.1X 機能の EAP-MD5 認証のシーケンスを以下に示します。



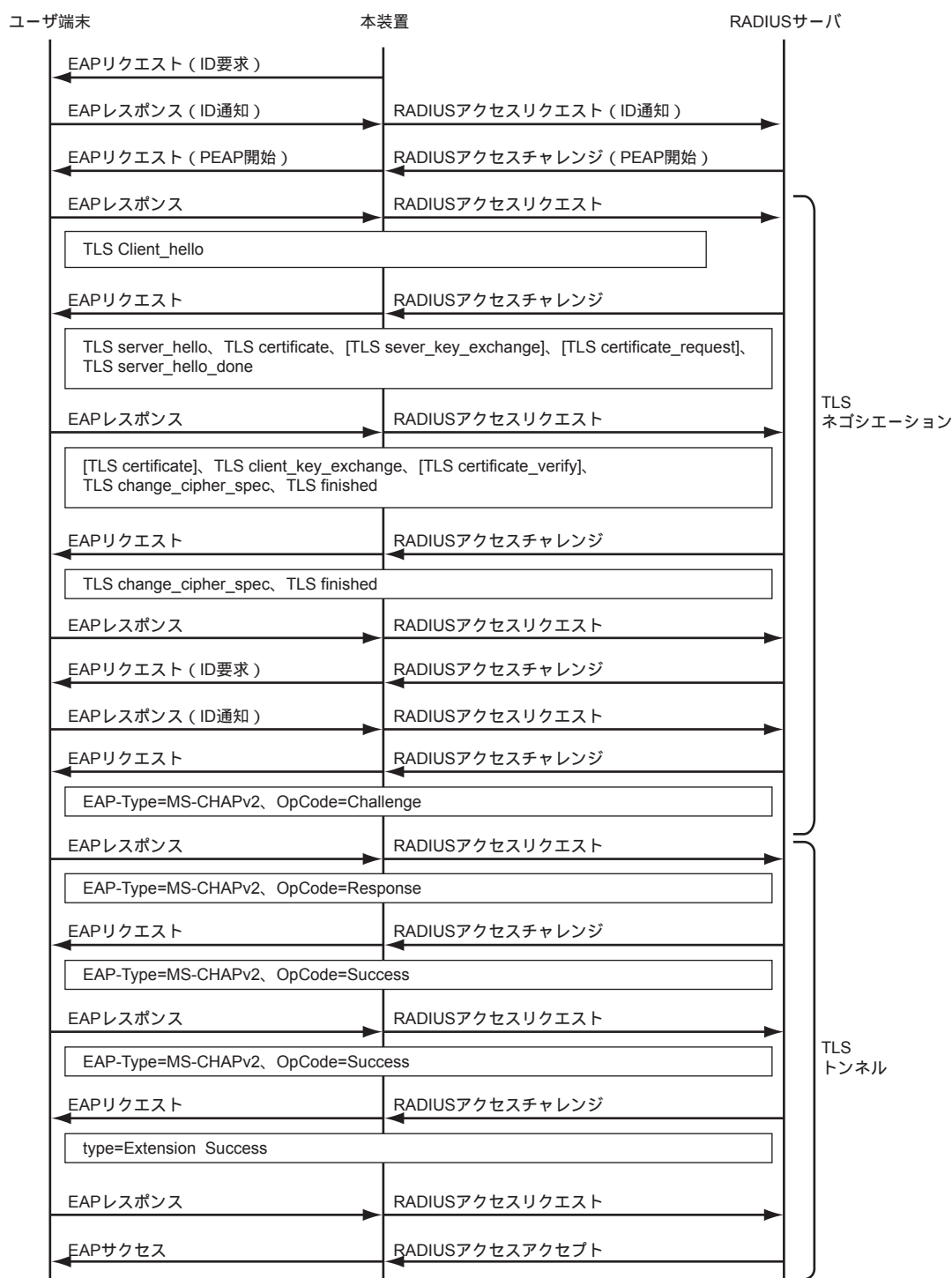
EAP-TLS 認証

EAP-TLS 認証とは、ユーザ端末と RADIUS サーバの双方に証明書を持つことによって、認証する方式です。IEEE802.1X 機能の EAP-TLS 認証のシーケンスを以下に示します。



PEAP 認証 (EAP-TTLS 認証も同様)

PEAP 認証とは、RADIUS サーバのみに証明書を持つことによって、認証する方式です。IEEE802.1X 機能の PEAP 認証のシーケンスを以下に示します。



2.11 MACアドレス認証機能

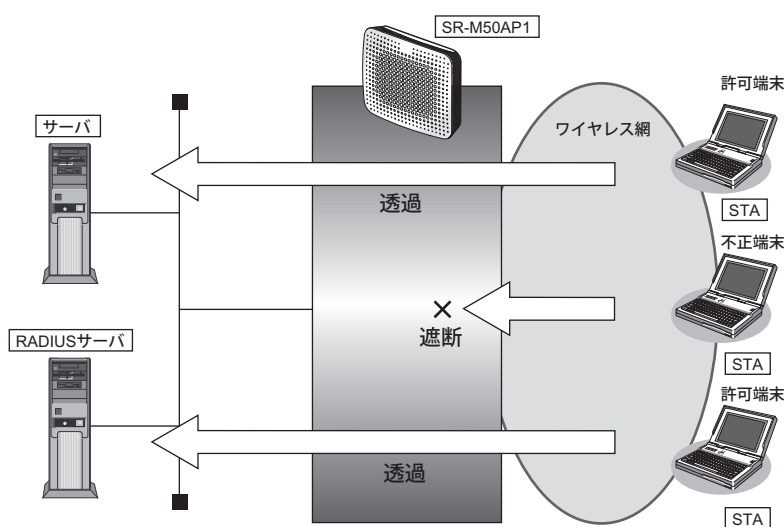
適用機種 SR-M50AP1

MACアドレス認証機能とは、受信パケットの送信元MACアドレスで認証を行い、送信元の端末が接続を許可された端末であるか認証する機能です（無線LANインタフェースのみ）。

本機能を利用することで認証許可のない不正端末を検知し、ネットワークへの不正アクセスを防止します。

認証方式は「CHAP/PAP」に対応し、認証を行うための認証データベースとして、自装置内のAAA機能を用いたローカル認証と、外部にRADIUSサーバを設置したリモート認証が利用できます。

無線LAN側で受信したAUTHENTICATIONフレームの送信元MACアドレスの認証を行い、成功した端末は認証で取得したVLAN IDのVLANに収容されます。

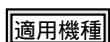


SR-M50AP1のMACアドレス認証

こんな事に気をつけて

- 本機能を利用する無線LANインタフェースでは、事前にVLANを設定できません。認証成功端末が認証成功時に割り当てられたVLANで通信します。
- 本機能では、RADIUSアカウント機能は使用できません。
- 1つの無線LANインターフェースでIEEE802.1X認証と併用した場合、両方の認証に成功した端末のみ接続できます。その場合、両方の認証で同じVLANを割り当てるようにしてください。

2.12 DHCP 機能

 **SR-M50AP1**

2.12.1 IPv4 DHCP 機能

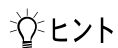
IPv4 DHCP 機能は、DHCP サーバから IP アドレスなどの情報を取得する機能（クライアント機能）です。

DHCP クライアント機能

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

本装置の DHCP クライアント機能は、以下の情報を受け取って動作します。

- IP アドレス
- ネットマスク
- リース期間
- デフォルトルータの IP アドレス
- DNS サーバの IP アドレス
- TIME サーバの IP アドレス
- NTP サーバの IP アドレス
- ドメイン名
- リース更新時間



ヒント

本装置でデフォルトルータの IP アドレスを受け取ると、自動的に優先度 1 のデフォルトルートがスタティック経路として生成されます。このスタティック経路は、スタティック経路情報の設定を行うことにより、デフォルトルート以外の任意のあて先や、優先度 1 以外に変更することができます。このスタティック経路と、ほかの同じあて先への経路情報で冗長構成を行う場合は、それぞれの経路情報に 1 以外の値で優先度を設定してください。



参照 スタティック経路情報の設定については、マニュアル「コマンドリファレンス」の「lan ip route」を参照してください。

2.13 RADIUS 機能

適用機種 SR-M50AP1

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)	アカウントिंग (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
IEEE802.1X 認証	EAP-MD5 認証、EAP-TLS 認証 EAP-TTLS 認証、PEAP 認証 EAP-SIM 認証、EAP-FAST 認証 EAP-AKA 認証、EAP-AKA Prime 認証	使用しません	接続時間
MAC アドレス認証	PAP 認証 / CHAP 認証 (※)	使用しません	使用しません

※) ユーザ名は MAC アドレス (区切り文字なし HEX12 文字)、パスワードは MAC アドレスまたは MAC アドレス認証情報で設定されたパスワードを使った認証となります。

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トिंग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
サーバへ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トングを行う場合、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トングが行える数は 256 です。同時に 257 以上の認証とアカウント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。

RADIUS サーバの監視

RADIUS サーバの監視は、以下のどちらかの方法で行うことができます。

- ICMPを使う方法
RADIUS サーバが動作しているホストに対して、ICMP ECHO パケットを送受信することにより、そのホストの生存確認を行います。
- 認証を使う方法
RADIUS サーバに対する定期的な認証要求を行うことにより、RADIUS サーバの生存確認を行います。監視はCHAP方式を用いた認証で行いますが、認証結果にかかわらず、その応答による生存確認を行います。

2.14 DNSサーバ機能

適用機種 SR-M50AP1

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。

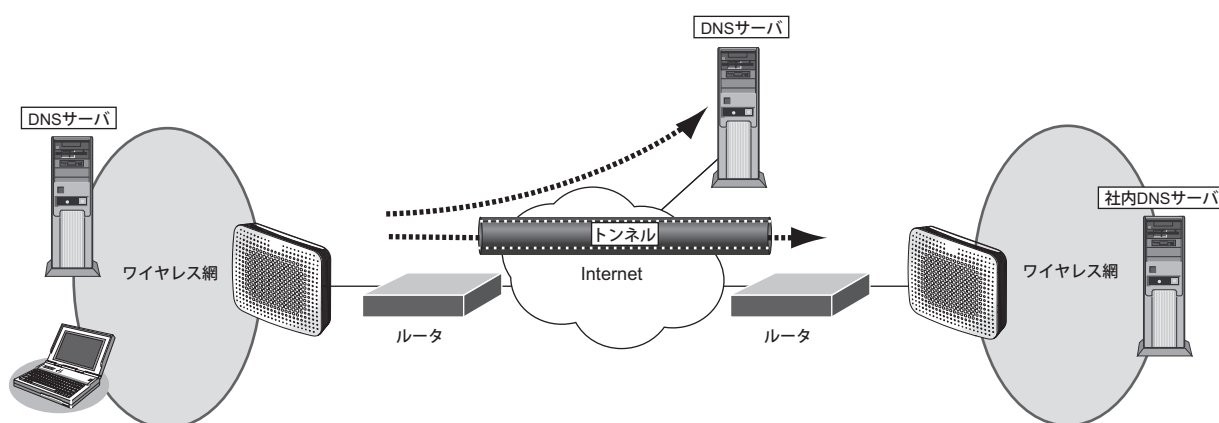
- DNSサーバ（スタティック）機能
- ProxyDNS（DNS振り分け）機能

2.14.1 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）、CLASSをIN（1 the Internet）とします。

2.14.2 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** マニュアル「コマンド設定事例集」

2.15 SNMP 機能

適用機種 SR-M50AP1

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

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

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

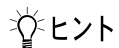
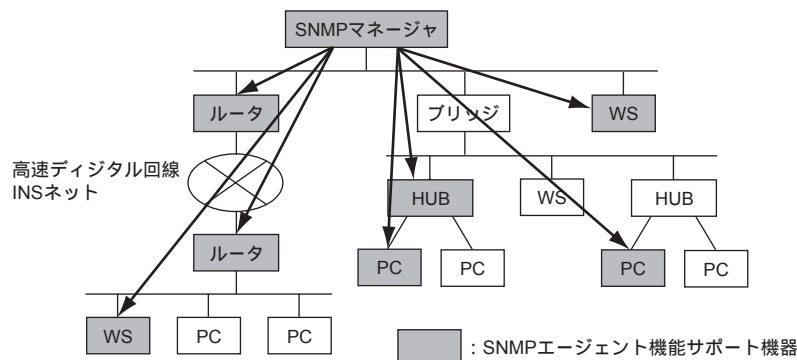
SNMP マネージャ機能は、ネットワーク上の端末の稼働状態や障害状態を一元管理します。SNMP エージェント機能は、SNMP マネージャの要求に対して MIB (Management Information Base : 管理情報ベース) という管理情報を返します。

SNMP 機能は、この2つの機能を使用して、SNMP マネージャと SNMP エージェントとの間で MIB に定義されたパラメー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 マニュアル「仕様一覧」

SNMP 機能による管理



◆ 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 マニュアル「コマンド設定事例集」

ifIndex の割り当て

本装置の 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 ～	ether ポート (ether ポート番号)
101 ～	無線 LAN モジュール (100 + 無線 LAN モジュール定義番号)
10000 ～	wlan 定義 (10000 + 無線 LAN インタフェース定義番号)
19000	loopback インタフェース
20000 ～	lan 定義 (20000 + lan 定義番号)

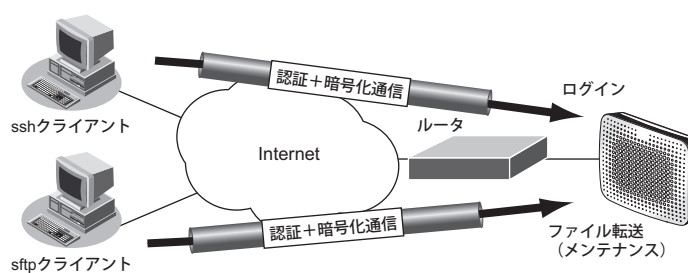
2.16 SSHサーバ機能

適用機種 SR-M50AP1

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 (ログイン中はtelnetinfoの設定に従う)	telnetinfoの設定に従う
シスログメッセージ (一部分抜粋)	login ユーザ名	logon telnet

以下に、sftp接続とftp接続の相違点を示します。

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

本装置でサポートする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
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

2.17 USB メモリ機能

SR-M50AP1

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/>

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、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 メモリからのソフトウェアの更新
- USB メモリへのソフトウェアの保存
- 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）
- PC レスでのソフトウェアと構成定義情報のインストール

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。
- 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。

2.17.1 構成定義の転送と保存

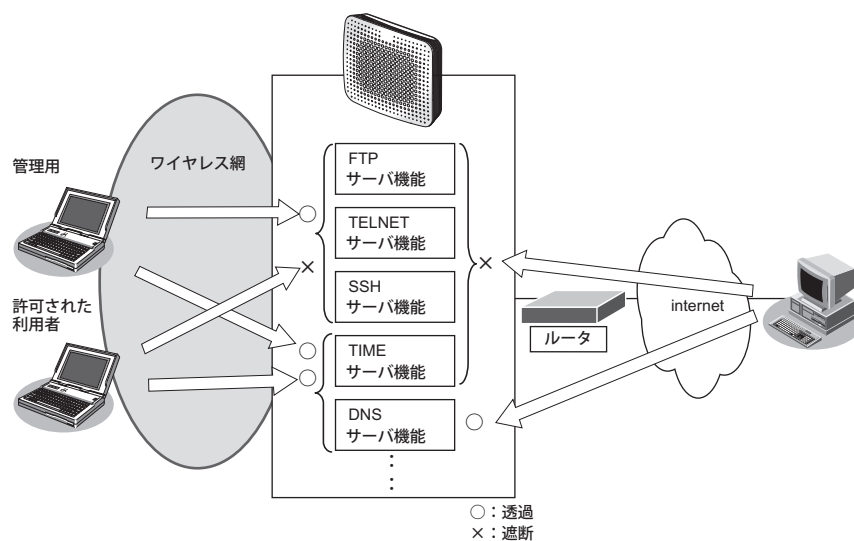
構成定義の転送および保存は、以下の方法で行います。

- 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。
同様にしてソフト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、マニュアル「Web ユーザーズガイド」を参照してください。
- PC レスで転送する場合
PC を使用しないで行う方法は、マニュアル「コマンドユーザーズガイド」の「外部メディア」に関する記述を参照してください。

2.18 アプリケーションフィルタ機能

適用機種 SR-M50AP1

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。



2.19 IDS 機能

適用機種 SR-M50AP1

IDS（IPv4 不正パケット検知）は、侵入などの不正アクセスによりセキュリティに影響を与えるパケットを検知する機能です。

本装置では、同一 VLAN に属する ETHER ポートおよび無線 LAN インタフェースに対して不正アクセスを検知した場合、システムログとして通知します。

検知対象一覧を以下に示します。

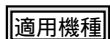
機能分類	検知内容
IP ヘッダ関連	Protocol フィールドが 134 以上のとき
	始点 IP アドレスと終点 IP アドレスが同じとき
	IP ヘッダの長さが length フィールドの長さよりも短いとき
	length フィールドと実際のパケットの長さが違うとき
IP オプションヘッダ関連	オプションヘッダの構造が不正であるとき
	Security and handling restriction header を受信したとき
	Loose source routing header を受信したとき
	Record route header を受信したとき
	Stream identifier header を受信したとき
	Strict source routing header を受信したとき
ICMP 関連	Internet timestamp header を受信したとき
	source quench を受信したとき
	timestamp request を受信したとき
	timestamp reply を受信したとき
	information request を受信したとき
	information reply を受信したとき
	address mask request を受信したとき
UDP 関連	address mask reply を受信したとき
	length フィールドの値が 8 よりも小さいとき
TCP 関連	UDP ヘッダの length フィールドの値が大き過ぎるとき
	フラグに何もセットされていないとき
	SYN と FIN が同時にセットされているとき
FTP 関連	ACK のない FIN を受信したとき
	PORT や PASV コマンドで指定されるポート番号が 1024 ～ 65535 の範囲でないとき

 参照 マニュアル「メッセージ集」の「IDS のメッセージ」

こんな事に気をつけて

- システムログとして通知するためには、syslog pri コマンドでプライオリティ LOG_NOTICE を追加する必要があります。
- プライバシープロテクション機能が無効であり、同一仮想アクセスポイント内の端末どうしの通信が可能な場合、端末どうしの通信に対する VLAN の IDS 設定は無効となります。
- 高速転送モードが有効の場合、IDS 設定は無効となります。

2.20 ProxyARP 機能

**SR-M50AP1**

ProxyARP は、通信相手あての ARP 要求に対して本装置が代理で ARP 要求に応答する機能です。

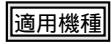
ARP 要求パケットはネットワーク上にブロードキャストされるために、無線 LAN ネットワーク全体に負荷がかかることになります。ProxyARP 機能が有効な場合は、接続されている無線 LAN 端末の IP アドレスと MAC アドレス情報を管理し、ETHER ポート側から受信した無線 LAN 端末への ARP 要求パケットを無線 LAN ネットワーク側へ転送することはせず、本装置が該当する無線 LAN 端末の MAC アドレスを ARP 応答することで、ネットワーク負荷を軽減することができます。

本装置では、ARP 応答パケットの送信元 MAC アドレスに無線 LAN 端末の MAC アドレスを設定して代理応答する機能をサポートします。

こんな事に気をつけて

本装置に接続してからまったく通信していない無線 LAN 端末が存在する場合や、無線 LAN 端末に対するブリッジの学習テーブルエントリの生存時間が経過してエントリが削除された場合は、この無線 LAN 端末に対する ARP 要求は無線 LAN 端末側へ転送されます。

2.21 POE 機能

**SR-M50AP1**

IEEE802.3af/at に準拠した POE (Power over Ethernet) による給電で動作可能です。
2 ポートから受電している場合は、1 ポートからの給電が停止しても動作を継続します。

2.22 高速転送モード

適用機種 *SR-M50AP1*

ハードウェアアクセラレーションにより、高速にパケット転送できる機能です。

こんな事に気をつけて

- 高速転送モードを使用する場合、以下に示す機能は設定があっても無効となります。
 - MAC アドレスフィルタ（転送時フィルタ）
 - IPv4 フィルタ
 - SPI
 - IDS
 - WDS
- 本機能の設定を変更した場合は、装置再起動が必要です。

2.23 無線 LAN 管理機能



SR-M50AP1

無線 LAN 管理機能サポート装置により、管理対象として登録することができます。

SR-M50AP1 を管理対象として登録できる装置は SR-S シリーズです。

無線 LAN 管理機能については、それぞれのマニュアルを参照してください。

索引

記号

11g プロテクション機能 28

A

ANY 接続拒否 22

AutoMDI/MDI-X 33

D

DHCP 機能 49

DHCP クライアント機能 49

DNS サーバ機能 52

DNS 振り分け機能 52

E

EAP-MD5 認証 45

EAP-TLS 認証 46

EAP-TTLS 認証 47

ether 定義 15

F

FTP サーバ機能 56

H

HT プロテクション機能 29

I

IDS 機能 61

IEEE802.1X 認証機能 44

ieee80211 定義 15

IPv4 DHCP 機能 49

L

lan 定義 15

M

MAC アドレス認証機能 48

MAC アドレスフィルタ 22

MIB 54

MIMO Power Save 機能 30

P

PEAP 認証 47

PMK キャッシュ機能 27

POE 機能 63

ProxyARP 機能 62

ProxyDNS 機能 52

R

RADIUS 機能 50

S

sftp サーバ 56

SNMP エージェント 54

SNMP 機能 54

SNMP マネージャ 54

SPI 43

SSH サーバ機能 56

SSID 非通知 21

T

TELNET サーバ機能 56

U

USB メモリ機能 58

V

VLAN 14

VLAN ID 14

VLAN 機能 36

VLAN 種別 36

vlan 定義 15

VLAN の種類 14

W

WDS ブリッジ機能 24

wlan 定義 15

WMM 機能 26

あ

アプリケーションフィルタ機能 60

い

インタフェース 15

え

エントリ 52

お

オートネゴシエーション 32

か

仮想アクセスポイント機能 25

こ

高速転送モード 64

固定 32

し

周辺アクセスポイント検出機能 27

ショートガードインターバル 30

す

スタティック機能 52

ステルス機能 21

せ

セキュリティ 42

セキュリティ方針 42

た

タグ VLAN 14, 36

端末台数最低保証 22

端末台数制限 22

ち

チャンネルボンディング機能 30

つ

通信モード 32

と

動的フィルタリング 43

ドメイン名 52

に

認証・暗号化機能 20

認証 VLAN 36

認証自動切替機能 31

の

ノイズ回避 31

は

バックアップポート 40

バックアップポート機能 40

ふ

ファイアーウォール 42

フィルタリング機能 42

フィルタリングルール 43

プライバシープロテクション機能 25

ほ

ポート VLAN 14, 36

ポート閉塞機能 38

ま

マスタポート 40

マニュアル構成 6

む

無線 LAN 管理機能 65

無線 LAN 機能 19

無線 LAN 通信規格 20

ゆ

ユーザ認証 42

り

リモートファイル転送機能 56

リモートログイン機能 56

リンクインテグリティ機能 41

SR-M 機能説明書

P3NK-5542-02Z0

発行日 2017 年 7 月

発行責任 富士通株式会社

- 本書の一部または全部を無断で他に転載しないよう、お願いいたします。
- 本書は、改善のために予告なしに変更することがあります。
- 本書に記載されたデータの使用に起因する第三者の特許権、その他の権利、損害については、 弊社は
その責を負いません。