P3NK-3852-06Z0

SR-Sシリーズ セキュアスイッチ

Web設定事例集 V13



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。 認証機能などによりセキュリティを強化して、安全なネットワークを提供するために、本装置をご利用ください。

> 2009年11月初版 2010年7月第2版 2010年10月第3版 2012年7月第4版

> 2012 年 9月第5版

2013 年 1月第6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 2009 - 2013

目次

はじる	めに	2
本書(の使いかた	6
	本書の読者と前提知識	6
	本書における商標の表記について	7
	本装置のマニュアルの構成	8
1	VLAN 機能を使う	9
	1.1 ポート VLAN 機能を使う	9
	1.2 タグ VLAN 機能を使う	12
	1.3 プロトコル VLAN 機能を使う	14
2	リンクアグリゲーション機能を使う	17
	2.1 LACP 機能を使う	21
3	バックアップポート機能を使う	25
4	MAC フィルタリング機能を使う	27
	4.1 特定 MAC アドレスからのパケットだけを許可する	29
	4.2 特定 MAC アドレスへのパケットだけを許可する	32
	4.3 特定パケット形式のパケットだけを禁止する	35
	4.4 ETHERBLOCK 単位で特定 MAC アドレスからのパケットだけを許可する	
	4.5 ETHERBLOCK 単位で特定 MAC アドレスへのパケットだけを許可する	41
	4.6 ETHERBLOCK 単位で特定パケット形式のパケットだけを禁止する	
	4.7 VLAN 単位で特定 MAC アドレス間の通信だけを遮断する	
-	4.8 VLAN 単位で特定ハケット形式のハケットにけを計可する	
5	スタナイック MAC フォワーナイノク機能を使う	
6		60
	6.1 優先制御機能を使う	60
7	6.2 愛先制御情報書さ探え機能を使う	
/	SIP	
	7.1 SIP を使う	
0	7.2 MSTP を使う	100
0		108
9		
10	IEEE802.1X 認証機能を使う	115
11	Web 認証機能を使う	122
	11.1 AAA でローカル認証を行う	
	11.2 AAA でリモート認証を行う	
12	MAC アドレス認証機能を使う	143
13	接続端末数制限機能を使う	149
14	ARP 認証機能を使う	151
15	ループ検出機能を使う	155
16	ポート・ミラーリング機能を使う	157
17	ether L3 監視機能を使う	159
	17.1 リンクアグリゲーション機能を使用した ether L3 監視機能を使う	
18	ポート閉塞機能を使う	166
19	LAN をネットワーク間接続する	
20	IPv4 のネットワークに IPv6 ネットワークを追加する	
21	RIP を使用したネットワークを構築する(IPv4)	
22	BIPの経路を制御する(IPv4)	185
~~	 シュニュロ Cipper 2 0 (1・1) 221 特定の経路情報の送信を許可する 	197
	22.1 「17.2.0/1241111111100011101110100011001100000000	189

	22.3	特定の経路情報の受信を許可する	191
	22.4	特定の経路情報のメトリック値を変更して受信する	
	22.5	特定の経路情報の送信を禁止する	196
	22.6	特定の経路情報の受信を禁止する	198
23	RIP の紙	圣路を制御する(IPv6)	200
	23.1	特定の経路情報の送信を許可する	202
	23.2	特定の経路情報のメトリック値を変更して送信する	204
	23.3	特定の経路情報の受信を許可する	206
	23.4	特定の経路情報のメトリック値を変更して受信する	208
	23.5	特定の経路情報の送信を禁止する	211
	23.6	特定の経路情報の受信を禁止する	213
24	OSPF を	を使用したネットワークを構築する(IPv4)	215
	24.1	バーチャルリンクを使う	221
	24.2	スタブエリアを使う	228
25	OSPF 0	D経路を制御する(IPv4)	235
	25.1	OSPF ネットワークでエリアの経路情報(LSA)を集約する	235
	25.2	AS 外部経路を集約して OSPF ネットワークに広報する	238
	25.3	エリア境界ルータで不要な経路情報(LSA)を遮断する	242
26	OSPF 榜	幾能を使う(IPv6)	245
	26.1	OSPF ネットワークを構築する	245
	26.2	エリア境界ルータでエリア内部経路を集約する	249
	26.3	エリア境界ルータで不要な経路情報を遮断する	251
27	マルチ=	キャスト機能を使う	253
	27.1	マルチキャスト機能(PIM-DM)を使う	
	27.2	マルチキャスト機能 (PIM-SM) を使う	
	27.3	マルチキャスト機能(スタティックルーティング)を使う	261
28	IPフィ	レタリング機能を使う	
28	IP フィル 28.1	レタリング機能を使う 外部の特定サービスへのアクセスだけを許可する	265 267
28	IP フィ, 28.1 28.2	レタリンク機能を使う 外部の特定サービスへのアクセスだけを許可する 外部の特定サービスへのアクセスだけを許可する(IPv6 フィルタリング)	265 267 273
28	IP フィル 28.1 28.2 28.3	レタリンク機能を使う	265 267 273 279
28	IP フィル 28.1 28.2 28.3 28.4	レタリンク機能を使う	265 267 273 279 279
28	IP フィ, 28.1 28.2 28.3 28.4 28.5	レタリング機能を使う	
28	IP フィ, 28.1 28.2 28.3 28.4 28.5 DSCP fi	レタリンク機能を使う 外部の特定サービスへのアクセスだけを許可する 外部の特定サービスへのアクセスだけを許可する(IPv6 フィルタリング) 外部から特定サーバへのアクセスだけを許可する 外部の特定サーバへのアクセスだけを禁止する 外部から特定サーバへの ping だけを禁止する 	
28 29 30	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP 値 VBRP 様	レタリンク機能を使う	
28 29 30	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP 値 VRRP 様 30.1	レタリンク機能を使う 外部の特定サービスへのアクセスだけを許可する 外部の特定サービスへのアクセスだけを許可する(IPv6 フィルタリング) 外部から特定サーバへのアクセスだけを許可する 外部の特定サーバへのアクセスだけを禁止する 外部から特定サーバへの ping だけを禁止する 動都から特定サーバへの ping だけを禁止する 働書き換え機能を使う	
28 29 30	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP 値 VRRP 様 30.1 30.2	レタリンク機能を使う	
28 29 30	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP 値 VRRP 様 30.1 30.2 ECMP#	レタリンク機能を使う	
28 29 30 31	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP 値 VRRP 様 30.1 30.2 ECMP 様	レタリンク機能を使う	
28 29 30 31 32	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP 値 VRRP 様 30.1 30.2 ECMP 様 22.1	レタリンク機能を使う	
29 30 31 32	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP 値 VRRP 様 30.1 30.2 ECMP 様 32.1 22.2	レタリンク機能を使う	
28 29 30 31 32	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP 値 VRRP 様 30.1 30.2 ECMP 様 32.1 32.2 23.2	 レタリンク機能を使う 外部の特定サービスへのアクセスだけを許可する 外部の特定サービスへのアクセスだけを許可する ハ部から特定サーバへのアクセスだけを許可する 外部の特定サーバへのアクセスだけを許可する 外部から特定サーバへのアクセスだけを禁止する 外部から特定サーバへの ping だけを禁止する 	
28 29 30 31 32	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP 値 VRRP 様 30.1 30.2 ECMP 様 32.1 32.2 32.3 22.4	レタリンク機能を使う	
29 30 31 32	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP 値 VRRP 様 30.1 30.2 ECMP 様 32.1 32.2 32.3 32.4 22.5	レタリンク機能を使う	
28 29 30 31 32	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP 値 VRRP 様 30.1 30.2 ECMP 様 32.1 32.2 32.3 32.4 32.5 DNS ##	レタリング機能を使う 外部の特定サービスへのアクセスだけを許可する 外部の特定サービスへのアクセスだけを許可する(IPv6 フィルタリング) 外部から特定サーバへのアクセスだけを許可する 外部から特定サーバへのアクセスだけを禁止する 外部から特定サーバへの ping だけを禁止する 動都から特定サーバへの ping だけを禁止する 参能を使う 簡易ホットスタンバイ機能を使う	
28 29 30 31 32 33	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP fl VRRP 様 30.1 30.2 ECMP 様 30.1 30.2 ECMP 様 32.1 32.2 32.3 32.4 32.5 DNS サ	レタリング機能を使う 外部の特定サービスへのアクセスだけを許可する 外部の特定サービスへのアクセスだけを許可する(IPv6 フィルタリング) 外部から特定サーバへのアクセスだけを許可する 外部から特定サーバへのアクセスだけを禁止する 外部から特定サーバへの ping だけを禁止する	
28 29 30 31 32 33	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP 値 VRRP 様 30.1 30.2 ECMP 様 32.1 32.2 32.3 32.4 32.5 DNS サ 33.1 22.2	レタリング機能を使う 外部の特定サービスへのアクセスだけを許可する 外部の特定サービスへのアクセスだけを許可する(IPv6 フィルタリング) 外部から特定サーバへのアクセスだけを許可する 外部から特定サーバへのアクセスだけを禁止する 外部から特定サーバへの ping だけを禁止する 直書き換え機能を使う 簡易ホットスタンバイ機能を使う クラスタリング機能を使う 機能を使う DHCP サーバ機能を使う DHCP サーバ機能を使う DHCP サーバ機能を使う DHCP リレーエージェント機能を使う IPv6 DHCP リレーエージェント機能を使う IPv6 DHCP リレーエージェント機能を使う 	
28 29 30 31 32 33	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP 们 VRRP 様 30.1 30.2 ECMP 様 30.1 30.2 ECMP 様 32.1 32.2 32.3 32.4 32.5 DNS サ 33.1 33.2	レタリンク機能を使う 外部の特定サービスへのアクセスだけを許可する 外部の特定サービスへのアクセスだけを許可する 外部から特定サーバへのアクセスだけを許可する 外部から特定サーバへのアクセスだけを許可する 外部から特定サーバへのアクセスだけを禁止する 直書き換え機能を使う 整能を使う 巻能を使う 機能を使う DHCP サーバ機能を使う DHCP サーバ機能を使う DHCP サーバ機能を使う DHCP サーバ機能を使う DHCP サーバ機能を使う DHCP サーバ機能を使う IPv6 DHCP サーバ機能を使う IPv6 DHCP サーバ機能を使う IPv6 DHCP サーバ機能を使う IPv6 DHCP リレーエージェント機能を使う IPv6 DHCP リレーエージェント機能を使う DNS サーバの自動切り替え機能(逆引き)を使う DNS 切ーバの自動切り替え機能(逆引き)を使う	
28 29 30 31 32 33	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP ff VRRP 様 30.1 30.2 ECMP 様 30.1 30.2 ECMP 様 32.1 32.2 32.3 32.4 32.5 DNS サ 33.1 33.2 33.4	レタリンク機能を使う 外部の特定サービスへのアクセスだけを許可する 外部の特定サービスへのアクセスだけを許可する 外部から特定サーバへのアクセスだけを許可する 外部から特定サーバへのアクセスだけを禁止する 外部から特定サーバへの ping だけを禁止する 動から特定サーバへの ping だけを禁止する 動まから特定サーバへの ping だけを禁止する	
28 29 30 31 32 33	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP ft VRRP 様 30.1 30.2 ECMP 様 30.1 30.2 ECMP 様 32.1 32.2 32.3 32.4 32.5 DNS サ 33.1 33.2 33.3 33.4 特定の	レタリンク機能を使う 外部の特定サービスへのアクセスだけを許可する	
28 29 30 31 32 33 33	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP ft VRRP 様 30.1 30.2 ECMP 様 30.1 30.2 ECMP 様 32.1 32.2 32.3 32.4 32.5 DNS サ 33.1 33.2 33.3 33.4 特定の	レタリンク機能を使う 外部の特定サービスへのアクセスだけを許可する 外部の特定サービスへのアクセスだけを許可する(IPv6 フィルタリング) 外部から特定サーバへのアクセスだけを許可する 外部から特定サーバへのアクセスだけを禁止する 外部から特定サーバへの ping だけを禁止する 外部から特定サーバへの ping だけを禁止する 着書き換え機能を使う 箇易ホットスタンバイ機能を使う クラスタリング機能を使う かいたなりが機能を使う DHCP サーバ機能を使う DHCP サーバ機能を使う DHCP サーバ機能を使う IPv6 DHCP サーバ機能を使う IPv6 DHCP サーバ機能を使う IPv6 DHCP リレーエージェント機能を使う IPv6 DHCP リレーエージェント機能を使う IPv6 DHCP リレーエージェント機能を使う DNS サーバの自動切り替え機能(順引き)を使う DNS サーバの自動切り替え機能(逆引き)を使う DNS サーバ機能を使う DNS サーバ機能を使う URL へのアクセスを禁止する(URL フィルタ機能)	
 28 29 30 31 32 33 34 35 32 	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP ff VRRP 様 30.1 30.2 ECMP 様 30.1 30.2 ECMP 様 30.1 30.2 ECMP 様 32.1 32.2 32.3 32.4 32.5 DNS サ 33.1 33.2 33.4 特定の SNMP	レタリンク機能を使う 外部の特定サービスへのアクセスだけを許可する	
28 29 30 31 32 33 33 34 35 36	IP フィル 28.1 28.2 28.3 28.4 28.5 DSCP ft VRRP 構 30.1 30.2 ECMP 構 30.1 30.2 ECMP 構 32.1 32.2 32.4 32.5 DNS サ 33.1 33.2 33.3 33.4 特定の SNMP	レタリンク機能を使う 外部の特定サービスへのアクセスだけを許可する	

	37.1	構成定義情報の切り替えを予約する	350
38	アプリ	ケーションフィルタ機能を使う	351
39	IEEE80	02.1ad 機能を使う	
	39.1	IEEE802.1ad 機能をポートベースサービスインタフェースとして使う	
	39.2	IEEE802.1ad 機能を C-TAG サービスインタフェースとして使う	358
40	IEEE80	02.1ah 機能を使う	
	40.1	IEEE802.1ah 機能をポートベースサービスインタフェースとして使う	
	40.2	IEEE802.1ah 機能を S-TAG サービスインタフェースとして使う	
	40.3	IEEE802.1ah 機能で L2 トンネリング動作を使う	
41	L2 暗号	号機能を使う	
42	無線 L	AN 管理機能を使う	
	42.1	無線 LAN 管理機能の環境を設定する	
	42.2	アクセスポイントモニタリングを行う	401
	42.3	クライアントモニタリングを行う	403
	42.4	無線 LAN アクセスポイントに MAC アドレスフィルタを配布する	
		(MAC アドレスフィルタ配布)	405
	42.5	無線 LAN アクセスポイントの電波出力を調整する(電波出力自動調整)	407
	42.6	無線 LAN アクセスポイントの無線 LAN チャネルを調整する	
索引			411

本書の使いかた

本書では、ネットワークを構築するために、代表的な接続形態や本装置の機能を活用した接続形態について説明しています。

また、CD-ROMの中のREADMEファイルには大切な情報が記載されていますので、併せてお読みください。

本書の読者と前提知識

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

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。

▲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、Windows Server 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。

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	
${\sf Microsoft}^{{\rm I\!C}}{\sf Windows}$ Vista $^{\rm I\!C}{\sf Home}$ 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 - 構成定義編 -	構成定義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。
コマンドリファレンス - 運用管理編 -	運用管理コマンド、その他の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。
Web 設定事例集(本書)	Web画面を使用した、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。
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。

1 VLAN 機能を使う

適用機種 全機種

1.1 ポート VLAN 機能を使う

適用機種 全機種

ここでは、ポート単位でグループ化したタグなしパケットをポート VLAN で送受信する場合の設定方法を説明します。

SR-S316C2/716C2の場合を例にします。



● 設定条件

- ETHER1、5 ポートを使用する
- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける VLAN ID: 10 ネットワークアドレス: 192.168.10.0/24 VLAN ID: 20 ネットワークアドレス: 192.168.20.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

ETHER1ポートのメディア種別および VLAN を設定する

- **1. 設定メニューの詳細設定で「ether情報」をクリックします**。 「ether情報」ページが表示されます。
- **2.** 「ether 情報」でポート番号が1の [修正] ボタンをクリックします。 ether 1 情報の設定項目と「基本情報」が表示されます。

• メディア種別

Untagged

→通常ポート (RJ45)

• VLAN

→ 10

■基本	「情報	3
ボート	使用	⊙使用する○使用しない
<mark>説明文</mark>	ξ	
メディ	P種別	○自動 ③通常ボート(RJ45) ○ SFPボート
通信递	通信速度	
<mark>全二重/半二重</mark>		◎全二重◎半二重
MDI		●自動 ○ MDI ○ MDI-X
フロー制	送信	●したい ○する
御	受信	⊙する ○しない
	Tagged	
V L/UN	Untagged	10

機種によりメディア種別に対応しているポート番号は異なります。

- 4. [保存] ボタンをクリックします。
- 5. 手順1.~4.を参考に、ETHER5ポートを設定します。
 - メディア種別 →通常ポート(RJ45)
 - VLAN
 Untagged → 20

VLAN10のネットワークを設定する

- 6. 設定メニューの詳細設定で「LAN 情報」をクリックします。 「LAN 情報」ページが表示されます。
- 7. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 8. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

9. 以下の項目を指定します。



- 10. 【保存】ボタンをクリックします。
- 11. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

• IPアドレス

- →192.168.10.1
- ネットマスク →24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報	3
IPアドレス	192.168.10.1
ネットマスク	24 (255.255.255.0)
フロートキャストアトレス	ネットワークアドレス+オール1 🔽

- 13. [保存] ボタンをクリックします。
- **14. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 15. 以下の項目を指定します。
 - VLAN ID →20

	<lan情報追加フィールド></lan情報追加フィールド>
VLAN ID	20

16. [追加] ボタンをクリックします。

「LAN1 情報」ページが表示されます。

- 17.
 「IP 関連」をクリックします。

 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 18. 手順 12.~13.を参考に、以下の項目を設定します。
 - IPアドレス → 192.168.20.1
 - ネットマスク →24 (255.255.255.0)
 - ブロードキャストアドレス →ネットワークアドレス+オール1
- 19. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

1.2 タグ VLAN 機能を使う

適用機種 全機種

ここでは、1つのポートで、2つのVLANからのタグ付きパケットを、それぞれのVLANで送受信する場合の設定方法を説明します。

SR-S316C2/716C2の場合を例にします。



● 設定条件

- ETHER1、5 ポートを使用する
- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける VLAN ID: 10 ネットワークアドレス: 192.168.10.0/24 VLAN ID: 20 ネットワークアドレス: 192.168.20.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

ETHER1、ETHER5ポートのメディア種別および VLAN を設定する

- **1. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - ポートリスト → 1,5
 ポート リスト 1.5
 修正 初期化
- 3. [修正] ボタンをクリックします。

ether 1,5情報の設定項目と「基本情報」が表示されます。

• メディア種別

→通常ポート (RJ45)

 VLAN Tagged

→ 10,20

■基本	情報	3	
ボート	使用	●使用する●使用しない	
<mark>説明文</mark>	τ		
メディ	P種別	○自動 ④通常ボート(RJ45) ○ SFPボート	
通信递	<mark>信速度</mark>		
全二重	[/半二重	◎全二重◎半二重	
MDI		●自動 ○ MDI ○ MDI-X	
フロ	送信	⊙し/むヽ ○する	
御	受信	⊙する ○しない	
	Tagged	10.20	
V L MIN	Untagged		

機種によりメディア種別に対応しているポート番号は異なります。

5. [保存] ボタンをクリックします。

VLAN10、VLAN20のネットワークを設定する

- 6. 「1.1 ポート VLAN 機能を使う」(P.9)の手順6.~18.を参考に、VLANのネットワークを設定します。
 「LAN0 情報」-「共通情報」-「基本情報」
 - VLAN ID → 10

「LAN0情報」-「IP関連」-「IPアドレス情報」

- IPアドレス → 192.168.10.1
- ネットマスク → 24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

「LAN情報」

• VLAN ID →20

「LAN1情報」-「IP 関連」-「IP アドレス情報」

- IPアドレス → 192.168.20.1
- ネットマスク →24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

7. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

1.3 プロトコル VLAN 機能を使う

SR-S224PS1, 224CP1, 248TC1, 308TL1, 310TL2, 316TL1, 318TL2, 324TL2, 316C2, 324TC1, 328TR1, 348TC1, 716C2, 724TC1, 748TC1

ここでは、IPプロトコルのパケットをそれぞれのポートでVLAN10およびVLAN20として送受信し、IPプロトコル以外のパケットについてはVLAN100として送受信する場合の設定方法を説明します。 SR-S316C2/716C2の場合を例にします。



VLAN ID 100 (IP以外)

● 設定条件

- ETHER1、5 ポートを使用する
- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける VLAN ID: 10 ネットワークアドレス: 192.168.10.0/24 VLAN ID: 20 ネットワークアドレス: 192.168.20.0/24 VLAN ID: 100

上記の設定条件に従って設定を行う場合の設定例を示します。

ETHER1ポートのメディア種別および VLAN を設定する

- **1. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- **2.** 「ether 情報」でポート番号が1の [修正] ボタンをクリックします。 ether 1 情報の設定項目と「基本情報」が表示されます。

適用機種

メディア種別

Untagged

→通常ポート (RJ45)

• VLAN

→ 10,100

■基本	「情報	3	
ボート	使用	●使用する●使用しない	
<mark>説明文</mark>	τ		
メディ	P種別	○自動 ③通常ボート(RJ45) ○ SFPボート	
通信递	<mark>通信速度</mark>		
全二重	全二重/半二重 ◎全二重 ○半二重		
MDI		●自動 ○ MDI ○ MDI-X	
フロ	送信	⊙しない○する	
御	受信	⊙する ○しない	
	Tagged		
VEAN	Untagged	10,100	

機種によりメディア種別に対応しているポート番号は異なります。

- 4. [保存] ボタンをクリックします。
- 5. 手順1.~4.を参考に、ETHER5ポートを設定します。
 - メディア種別 →通常ポート(RJ45)
 - VLAN
 Untagged → 20,100

VLAN10をプロトコルVLANに設定する

6. 設定メニューの詳細設定で「VLAN 情報」をクリックします。

「VLAN情報」ページが表示されます。

- 7. 以下の項目を指定します。
 - VLAN ID

→ 10

<vlan情報追加フィールド></vlan情報追加フィールド>	
VLAN ID	10

- 【追加】ボタンをクリックします。
 「VLAN10 情報」ページが表示されます。
- 「基本情報」をクリックします。
 「基本情報」が表示されます。

• プロトコル定義 →システム定義プロトコルから指定

"システム定義プロトコルから指定"を選択すると、「プロトコル種別」の設定項目が表示されます。

プロトコル種別 → IPv4

ブロトコル定義	 ○ 指定しない ● システム定義プロトコルから指定 ○ プロトコルをユーザ定義指定
ブロトコル種別	 ● IPv4 ○ IPv6 ○ FNA

- 11. [保存] ボタンをクリックします。
- 12. 手順6.~11.を参考に、以下の項目を設定します。

「VLAN情報」

VLAN ID →20
 「VLAN20情報」-「基本情報」
 ・ プロトコル定義 →システム定義プロトコルから指定
 ・ プロトコル種別 → IPv4

VLAN10、VLAN20のネットワークを設定する

13. 「1.1 ポート VLAN 機能を使う」(P.9)の手順6.~18.を参考に、VLANのネットワークを設定します。

「LAN0情報」-「共通情報」-「基本情報」

• VLAN ID → 10

「LAN0 情報」-「IP 関連」-「IP アドレス情報」

- IPアドレス → 192.168.10.1
- ネットマスク → 24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

「LAN情報」

• VLAN ID →20

「LAN1情報」-「IP関連」-「IPアドレス情報」

- IPアドレス → 192.168.20.1
- ネットマスク → 24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

14. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2 リンクアグリゲーション機能を使う

適用機種 全機種

ここでは、4 ポートの 1000M 回線をリンクアグリゲーションとする場合の設定方法を説明します。 SR-S316C2/716C2の場合を例にします。



● 設定条件

- ETHER1~4ポートを使用する
- メディア種別を 10/100/1000BASE-T ポートに変更する
- 通信速度を 1000 Mbps 固定に変更する
- VLAN ID とネットワークアドレスを以下のように対応付ける
 VLAN ID: 10
 ネットワークアドレス: 192.168.10.0/24
 VLAN ID: 20
 ネットワークアドレス: 192.168.20.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

- 設定メニューの詳細設定で「ether 情報」をクリックします。
 「ether 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - ポートリスト → 1-4



3. [修正] ボタンをクリックします。

ether 1-4 情報の設定項目と「基本情報」が表示されます。

- メディア種別 →通常ポート(RJ45)
- 通信速度 → 1000Mbps
- VLAN Tagged

→ 10,20

■基本	5情報	3	
<mark>ボート使用</mark> ⊙使用する ○使用しない		●使用する●使用しない	
<mark>説明文</mark>	τ		
メディブ	ア種別	○自動 ④通常ボート(RJ45) ○ SFPボート	
<mark>通信速度</mark> ○自動 ○10Mbps ○100Mbps ⊙1000Mbps		〇自動 ◯ 10Mbps ◯ 100Mbps ⊙ 1000Mbps	
全二重/半二重		◎全二重○半二重	
MDI ◎自動 ○ MDI ○ MDI-X		●自動 ○ MDI ○ MDI-X	
フロ 一知	送信	⊙しばい ○する	
御	受信	⊙する○しばい	
	Tagged	10,20	
VEAN	Untagged		

機種によりメディア種別に対応しているポート番号は異なります。

5. [保存] ボタンをクリックします。

6. 「ポート種別情報」をクリックします。

「ポート種別情報」が表示されます。

7. 以下の項目を指定します。

- ポート種別 →リンクアグリゲーション
 "リンクアグリゲーション"を選択すると、「リンクアグリゲーショングループ情報」の設定項目が表示されます。
- リンクアグリゲーショングループ情報
 グループ番号 →1
 アンカポート番号 →1

■ポート種別情報 []		
ボート種別	 ○通常 ●リンクアグリゲーション ○バックアップ ○ミラー 	
リンクアグ リケーショ ン グルーブ 情報	グループ番号 <u>1 ×</u> アンカボート番号 <u>1 ×</u>	

- 8. [保存] ボタンをクリックします。
- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **10.** 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- **11. 「共通情報」をクリックします。** 共通情報の設定項目と「基本情報」が表示されます。

- VLAN ID → 10
 基本情報
 VLAN ID 10
- 13. [保存] ボタンをクリックします。
- 14. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

15. 以下の項目を指定します。

• IPアドレス

- → 192.168.10.1
- ネットマスク → 24 (255.255.255.0)

■IPアドレス情報	3
IP アド レス	192.168.10.1
ネットマスク	24 (255.255.255.0)

- 16. [保存] ボタンをクリックします。
- **17. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 18. 以下の項目を指定します。
 - VLAN ID

→20

<lan情報追加フィールド></lan情報追加フィールド>		
VLAN ID	20	

- **19. [追加] ボタンをクリックします**。 「LAN1情報」ページが表示されます。
- **20. 「IP 関連」をクリックします。** IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 21. 手順 15.~16.を参考に、以下の項目を設定します。
 - IPアドレス → 192.168.20.1
 - ネットマスク →24 (255.255.255.0)
- **22. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する | を参考に、本装置2を設定します。 「ether情報」 • ポートリスト → 1-4 [ether 1-4 情報] - 「基本情報」 • メディア種別 →通常ポート (RJ45) 通信速度 → 1000Mbps • VLAN Tagged → 10,20 「ether 1-4 情報」-「ポート種別情報」 ポート種別 →リンクアグリゲーション 「LAN情報」 「LAN0情報」-「共通情報」-「基本情報」 VLAN ID **→**10 「LAN0情報」-「IP関連」-「IPアドレス情報」 • IPアドレス → 192.168.10.2 ネットマスク →24 (255.255.255.0) 「LAN情報」 • VLAN ID →20 「LAN1情報」-「IP関連」-「IPアドレス情報」 • IPアドレス → 192.168.20.2 ネットマスク →24 (255.255.255.0)

☞ 参照 機能説明書「2.7 リンクアグリゲーション機能」(P.36)

2.1 LACP機能を使う

適用機種 全機種

ここでは、4 ポートの 1000M 回線を LACP を利用したリンクアグリゲーションとする場合の設定方法を説明します。 SR-S316C2/716C2 の場合を例にします。



● 設定条件

- ETHER1~4ポートを使用する
- メディア種別を 10/100/1000BASE-T ポートに変更する
- 通信速度を 1000 Mbps 固定に変更する
- VLAN IDとネットワークアドレスを以下のように対応付ける VLAN ID: 10 ネットワークアドレス: 192.168.10.0/24 VLAN ID: 20 ネットワークアドレス: 192.168.20.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

- 設定メニューの詳細設定で「ether 情報」をクリックします。
 「ether 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - ポートリスト → 1-4



3. [修正] ボタンをクリックします。

ether 1-4情報の設定項目と「基本情報」が表示されます。

- メディア種別 →通常ポート(RJ45)
- 通信速度 → 1000Mbps
- VLAN Tagged

→ 10,20

■基本情報		
ボート使用		●使用する●使用しない
<mark>説明文</mark>	τ	
メディス	P種別	○自動 ④通常ボート(RJ45) ○ SFPボート
通信速度 ○自動 ○10Mbps ○100		〇自動 ◯10Mbps ◯100Mbps ⊙1000Mbps
全二重/半二重		◎全二重◎半二重
MDI		●自動 ○ MDI ○ MDI-X
フロー当日	送信	⊙しない○する
御	受信	⊙する ○しばい
	Tagged	10,20
V L MIN	Untagged	

機種によりメディア種別に対応しているポート番号は異なります。

5. [保存] ボタンをクリックします。

6. 「ポート種別情報」をクリックします。

「ポート種別情報」が表示されます。

- 7. 以下の項目を指定します。
 - ポート種別

→リンクアグリゲーション

■ポート種別情報	
ボート種別	 ○通常 ●リンクアグリゲーション ○バックアップ ○ミラー

- 8. [保存] ボタンをクリックします。
- **9. 設定メニューの詳細設定で「リンクアグリゲーショングループ情報」をクリックします**。 「リンクアグリゲーショングループ情報」ページが表示されます。
- **10.** 「リンクアグリゲーショングループ情報」でリンクアグリゲーショングループ番号が1の [修正] ボ タンをクリックします。

リンクアグリゲーショングループ1情報の設定項目と「基本情報」が表示されます。

- 11. 以下の項目を指定します。
 - 動作モード → active
 基本情報 ②
 動作モード active ▼
- 12. [保存] ボタンをクリックします。
- **13. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。

14. 「LAN 情報」でインタフェースがLAN0の [修正] ボタンをクリックします。

「LAN0 情報」ページが表示されます。

- **15. 「共通情報」をクリックします。** 共通情報の設定項目と「基本情報」が表示されます。
- 16. 以下の項目を指定します。

VLAN ID	→ 10	
■基本情報		3
VLAN ID	10	

- 17. [保存] ボタンをクリックします。
- **18.** 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 19. 以下の項目を指定します。
 - IPアドレス → 192.168.10.1
 - ネットマスク →24 (255.255.255.0)
 - ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報	3
IPアドレス	192.168.10.1
ネットマスク	24 (255.255.255.0)
フロートキャストアトレス	ネットワークアドレス+オール1 🔽

- 20. [保存] ボタンをクリックします。
- **21. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 22. 以下の項目を指定します。
 - VLAN ID

→20

<lan情報追加フィールド></lan情報追加フィールド>			
VLAN ID		20	

23. [追加] ボタンをクリックします。

「LAN1 情報」ページが表示されます。

24. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 25. 手順 19.~20.を参考に、以下の項目を設定します。
 - IPアドレス → 192.168.20.1
 - ネットマスク →24 (255.255.255.0)
 - ブロードキャストアドレス →ネットワークアドレス+オール1

26. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。 「ether情報」 • ポートリスト → 1-4 「ether 1-4 情報」-「基本情報」 メディア種別 →通常ポート (RJ45) 通信速度 → 1000Mbps • VLAN → 10,20 Tagged 「ether 1-4 情報」- 「ポート種別情報」 ポート種別 →リンクアグリゲーション 「リンクアグリゲーショングループ情報」 「リンクアグリゲーショングループ1情報」-「基本情報」 動作モード → active 「LAN情報」 「LAN0情報」-「共通情報」-「基本情報」 VLAN ID **→**10 「LAN0情報」-「IP関連」-「IPアドレス情報」 • IPアドレス → 192.168.10.2 • ネットマスク →24 (255.255.255.0) • ブロードキャストアドレス →ネットワークアドレス+オール1 「LAN情報」 • VLAN ID →20 「LAN1情報」-「IP関連」-「IPアドレス情報」 • IPアドレス → 192.168.20.2

- ネットマスク →24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1
- 参照 機能説明書「2.7 リンクアグリゲーション機能」(P36)、「2.7.1 LACP機能」(P37)

バックアップポート機能を使う 3

適用機種 全機種

ここでは、アップリンクポートをバックアップポートとして利用する場合の設定方法について説明します。 アップリンクポートをそれぞれ異なるスイッチに接続することで、冗長アップリンクの形態にできます。 SR-S224TC2の場合を例にします。



● 設定条件

- ETHER25、26 ポートをバックアップポートとして使用する (ETHER25をマスタポート、ETHER26をバックアップポートとする)
- マスタポートを優先的に使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

- 1. 設定メニューの詳細設定で「ether情報」をクリックします。 「ether 情報」ページが表示されます。
- 2. 「ether情報」でポート番号が25の[修正] ボタンをクリックします。 ether 25 情報の設定項目と「基本情報」が表示されます。
- 3. 「ポート種別情報」をクリックします。 「ポート種別情報」が表示されます。
- 以下の項目を指定します。 4.
 - ポート種別 →バックアップ

"バックアップ"を選択すると、「バックアップグループ情報」の設定項目が表示されます。

- バックアップグループ情報 優先度 →優先ポート ■ポート種別情報 ○通常 ○リンクアグリゲーション ボート種別 ・
 バックアップ 0ミラー
- 3 バックアッ グループ番号 1 🔽 グループ 優先度 ●優先ボート●待機ボート 情報
- [保存] ボタンをクリックします。 5.

- 6. 手順1.~5.を参考に、ETHER26ポートを設定します。
 - ポート種別 →バックアップ
 バックアップグループ情報
 - 優先度 →待機ポート
- 7. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

4 MACフィルタリング機能を使う

```
適用機種 全機種
```

本装置を経由するパケットを、MACアドレス、パケット形式、ETHERNETタイプ、VLAN ID、COS 値などの組 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。

● 参照 機能説明書 [2.11 MAC フィルタ機能」(P.55)

こんな事に気をつけて

SR-S308TL1/310TL2/316TL1/318TL2/324TL2では、以下の機能を同時に使用することができません。 MACフィルタ情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ/QoS資源の配分」の機能を"フィ ルタのみ"、プロトコルを"IPv4のみ"に設定する必要があります。

- MACフィルタ機能(IPv4) / IPフィルタリング機能(IPv4)
- MAC フィルタ機能(IPv6 フィルタ) / IP フィルタリング機能(IPv6)
- ・ 優先制御情報書き換え機能(IPv4) / DSCP 値書き換え機能(IPv4)
- ・ 優先制御情報書き換え機能(IPv6) / DSCP 値書き換え機能(IPv6)



フィルタリング条件

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。

- ACLのMAC定義およびVLAN定義で指定した以下の情報
 - 送信元 MAC 情報(MAC アドレス/パケット形式/ETHERNET タイプ/LSAP)
 - あて先MAC情報(MACアドレス/パケット形式/ETHERNETタイプ/LSAP)
 - VLAN ID
 - COS値
 - 送信元 IP 情報 (IP アドレス/アドレスマスク)
 - あて先IP情報(IPアドレス/アドレスマスク)
 - プロトコル
 - TCP・UDPのポート番号
 - ICMP TYPE、ICMP CODE
 - IPパケットのTOS値、DSCP値
- フィルタ処理の対象となるパケット入力 ETHER ポート
- 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)

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の2つがあります。

- A. 特定の条件のパケットだけを透過させ、その他はすべて遮断する
- B. 特定の条件のパケットだけを遮断し、その他はすべて透過させる

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 特定 MAC アドレスからのパケットだけを許可する
- 特定 MAC アドレスへのパケットだけを許可する

また、設計方針 Bの例として、以下の設定例について説明します。

• 特定パケット形式のパケットだけを禁止する

4.1 特定 MAC アドレスからのパケットだけを許可する

適用機種 全機種

ここでは、VLAN内の特定ポートで特定のMACアドレスを持つホストからの入力パケットだけを許可し、その他のホストからの入力パケットを禁止する場合の設定方法を説明します。

こんな事に気をつけて

SR-S308TL1/310TL2/316TL1/318TL2/324TL2では、以下の機能を同時に使用することができません。 MAC フィルタ情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ/QoS 資源の配分」の機能を"フィ ルタのみ"、プロトコルを"IPv4のみ"に設定する必要があります。

- MAC フィルタ機能(IPv4) / IP フィルタリング機能(IPv4)
- MACフィルタ機能(IPv6フィルタ) / IPフィルタリング機能(IPv6)
- ・ 優先制御情報書き換え機能(IPv4)/DSCP値書き換え機能(IPv4)
- ・ 優先制御情報書き換え機能(IPv6)/DSCP値書き換え機能(IPv6)

● フィルタリング設計

- VLAN 10はETHER1~8ポートで構成されるポートVLANで、それぞれのポートでタグなしである
- VLAN 20はETHER1~4ポートおよびETHER9~12ポートで構成されるポートVLANで、ETHER1~4ポートでタグ付き、ETHER9~12ポートでタグなしである
- ETHER2 ポートの VLAN 10 では MAC アドレス 00:0b:01:02:03:04 のホストからの入力パケットだけを許可し、その他はすべて禁止する

上記のフィルタリング設計に従って設定を行う場合の設定例を示します。

(1) VLAN ID が 10 で送信元 MAC アドレスが 00:0b:01:02:03:04 であるパケットの形式を ACL で設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

→ acl0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	aciO	

- **3. [追加] ボタンをクリックします**。 「ACL定義情報(acl0)」ページが表示されます。
- **4. 「MAC 定義情報」をクリックします**。 「MAC 定義情報」が表示されます。

٠	送信元MACアドレス	→指定する
	アドレス指定	→00:0b:01:02:03:04
•	あて先 MAC アドレス	→すべて

フォーマット種別 →すべて

■MAC定義情報		
送信元MACアドレス	指定する ▼ アドレス指定(″指定する″を選択時のみ有効です) 00:0b:01:02:03:04	
あて先MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)	
フォーマット種別	 ● すべて ● LLC形式 ■ LSAP ● Ethernet形式 ■ type値 	

- 6. [保存] ボタンをクリックします。
- 7. 「VLAN定義情報」をクリックします。

「VLAN定義情報」が表示されます。

8. 以下の項目を指定します。

- VLAN ID → 10
- COS値
 →指定しない

	3
10	
	10

- 9. [保存] ボタンをクリックします。
- (2) VLAN IDが10のすべてのパケットの形式をACLで設定する
- 10. 手順1.~3.および手順7.~9.を参考に、以下の項目を設定します。

「ACL情報」

•	定義名	→ acl1
ΓA	CL定義情報	(acl1)」-「VLAN定義情報」
•	VLAN ID	→ 10
•	COS值	→指定しない

(3) ETHER2ポートで(1) で設定した形式のパケットを透過させる

11. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether 情報」ページが表示されます。

- **12.** 「ether 情報」でポート番号が2の [修正] ボタンをクリックします。 ether 2 情報の設定項目と「基本情報」が表示されます。
- 13. 「フィルタ情報」をクリックします。

「フィルタ情報」が表示されます。

- 14. 以下の項目を指定します。
 - 動作 →透過
 - ACL定義番号 →0

▲ 「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の [選択] ボタンをクリックして設定します。

<フィルタ情報入力フィールド>	
動作	◎透過○遮断
ACL定義番号	0 参照

- 15. [追加] ボタンをクリックします。
- (4) ETHER2 ポートで(2) で設定した形式のパケットを遮断する
- 16. 手順 14.~15を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL定義番号 →1
- **17. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

4.2 特定 MAC アドレスへのパケットだけを許可する

適用機種 全機種

ここでは、VLAN内の特定ポートで特定のMACアドレスを持つホストへの送信パケットだけを許可し、その他のホストへの送信パケットを禁止する場合の設定方法を説明します。

こんな事に気をつけて

SR-S308TL1/310TL2/316TL1/318TL2/324TL2では、以下の機能を同時に使用することができません。 MAC フィルタ情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ/QoS 資源の配分」の機能を"フィ ルタのみ"、プロトコルを"IPv4のみ"に設定する必要があります。

- MAC フィルタ機能(IPv4) / IP フィルタリング機能(IPv4)
- MACフィルタ機能(IPv6フィルタ) / IPフィルタリング機能(IPv6)
- ・ 優先制御情報書き換え機能(IPv4)/DSCP値書き換え機能(IPv4)
- ・ 優先制御情報書き換え機能(IPv6) / DSCP 値書き換え機能(IPv6)

● フィルタリング設計

- VLAN 10はETHER1~8ポートで構成されるポートVLANで、それぞれのポートでタグなしである
- VLAN 20はETHER1~4ポートおよびETHER9~12ポートで構成されるポートVLANで、ETHER1~4ポートでタグ付き、ETHER9~12ポートでタグなしである
- ETHER4~8ポートのVLAN 10では MAC アドレス 00:0b:01:02:03:04 のホストへの送信パケットだけを許可し、その他はすべて禁止する

上記のフィルタリング設計に従って設定を行う場合の設定例を示します。

(1) VLAN ID が10であて先MACアドレスが00:0b:01:02:03:04であるパケットの形式を ACLで設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

→ acl0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	aciO	

- **3. [追加] ボタンをクリックします**。 「ACL定義情報(acl0)」ページが表示されます。
- **4. 「MAC 定義情報」をクリックします**。 「MAC 定義情報」が表示されます。

- ・ 送信元 MAC アドレス →すべて
 ・ あて先 MAC アドレス →指定する アドレス指定 →00:0b:01:02:03:04
- フォーマット種別 →すべて

MAC定義情報	3
送信元MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
あて先MACアドレス	指定する ▼ アドレス指定(″指定する″を選択時のみ有効です) 00:0b:01:02:03:04
フォーマット種別	 すべて LLC形式 LSAP Ethernet形式 type値

- 6. [保存] ボタンをクリックします。
- 7. 「VLAN定義情報」をクリックします。

「VLAN定義情報」が表示されます。

8. 以下の項目を指定します。

- VLAN ID → 10
- COS 値 →指定しない

VLAN定義情報		3
VLAN ID	10	
COS値		

- 9. [保存] ボタンをクリックします。
- (2) VLAN IDが10のすべてのパケットの形式をACLで設定する
- 10. 手順1.~3.および手順7.~9.を参考に、以下の項目を設定します。

「ACL情報」

- 定義名 → acl1
- 「ACL定義情報(acl1)」-「VLAN定義情報」
- VLAN ID → 10
- COS値
 →指定しない
 →

 →

- (3) ETHER4~8ポートで(1) で設定した形式のパケットを透過させる
- 11. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether 情報」ページが表示されます。

- 12. 以下の項目を指定します。
 - ポートリスト → 4-8



- **13.** [修正] ボタンをクリックします。 ether 4-8 情報の設定項目と「基本情報」が表示されます。
- **14. 「フィルタ情報」をクリックします。** 「フィルタ情報」が表示されます。
- 15. 以下の項目を指定します。
 - 動作 →透過
 - ACL定義番号 →0

fACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択]
 ボタンをクリックして設定します。

<フィルタ情報入力フィールド>		
動作	◎ 透過 ○ 遮断	
ACL定義番号	0 参照	

- 16. [追加] ボタンをクリックします。
- (4) ETHER4~8ポートで(2) で設定した形式のパケットを遮断する
- 17. 手順 15.~16.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL定義番号 →1
- 18. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

4.3 特定パケット形式のパケットだけを禁止する

適用機種 全機種

ここでは、VLAN内の特定ポートで特定のパケット形式を持つ入力パケットだけを禁止し、その他の入力パケットを許可する場合の設定方法を説明します。

こんな事に気をつけて

SR-S308TL1/310TL2/316TL1/318TL2/324TL2では、以下の機能を同時に使用することができません。 MAC フィルタ情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ/QoS 資源の配分」の機能を"フィ ルタのみ"、プロトコルを"IPv4のみ"に設定する必要があります。

- MACフィルタ機能(IPv4) / IPフィルタリング機能(IPv4)
- MACフィルタ機能(IPv6フィルタ) / IPフィルタリング機能(IPv6)
- ・ 優先制御情報書き換え機能(IPv4) / DSCP 値書き換え機能(IPv4)
- ・ 優先制御情報書き換え機能(IPv6)/DSCP値書き換え機能(IPv6)

● フィルタリング設計

- VLAN 10は ETHER1 ~ 8 ポートで構成されるポート VLAN で、それぞれのポートでタグなしである
- VLAN 20は ETHER1~4ポートおよび ETHER9~12ポートで構成されるポート VLAN で、ETHER1~4ポートでタグ付き、ETHER9~12ポートでタグなしである
- ETHER1~4ポートではIPプロトコルの入力パケットだけを禁止し、その他はすべて許可する

上記のフィルタリング設計に従って設定を行う場合の設定例をSR-S316C2を例にして示します。

(1) IP プロトコルのパケット (IP, ARP, Reverse ARP) の形式を ACL で設定する

- 設定メニューの詳細設定で「ACL情報」をクリックします。
 「ACL情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 定義名

→acl0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	ac IO	

3. [追加] ボタンをクリックします。

「ACL定義情報 (acl0)」ページが表示されます。

4. 「MAC 定義情報」をクリックします。 「MAC 定義情報」が表示されます。

- ・ 送信元 MAC アドレス →すべて
- あて先MACアドレス →すべて
- フォーマット種別 → Ethernet形式
 type値 → 0800

■MAC定義情報	[3
送信元MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
あて先MACアドレス	すべて アドレス指定("指定する"を選択時のみ有効です)
フォーマット種別	 すべて LLC形式 LSAP Ethernet形式 type値 0800

6. [保存] ボタンをクリックします。

7. 手順1.~6.を参考に、以下の項目を設定します。

「ACL情報」

定義名

→acl1

「ACL定義情報 (acl1)」-「MAC 定義情報」

- ・ 送信元 MAC アドレス →すべて
- あて先MACアドレス →すべて
- フォーマット種別 → Ethernet形式 type値 → 0806

「ACL情報」

• 定義名 → acl2

「ACL定義情報 (acl2)」-「MAC 定義情報」

- ・ 送信元 MAC アドレス →すべて
 ・ あて先 MAC アドレス →すべて
- フォーマット種別 → Ethernet形式
 type値 → 8035

(2) ETHER1~4ポートで(1) で作成したパケットのパターンを遮断する

8. 設定メニューの詳細設定で「ether 情報」をクリックします。 「ether 情報」ページが表示されます。

9. 以下の項目を指定します。

 ポートリスト → 1-4
 ポート リスト
 1-4
 修正 初期化
10. [修正] ボタンをクリックします。

ether 1-4 情報の設定項目と「基本情報」が表示されます。

11. 「フィルタ情報」をクリックします。

「フィルタ情報」が表示されます。

- 12. 以下の項目を指定します。
 - 動作

- →遮断
- ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<フィルタ情報入力フィールド>		
動作	○透過 ⊙遮断	
ACL定義番号	0 参照	

- 13. [追加] ボタンをクリックします。
- 14. 手順 12.~13.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL定義番号 →1
- 15. 手順 12.~13.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL定義番号 →2
- 16. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

4.4 ETHERBLOCK 単位で特定 MAC アドレスからのパケットだけを 許可する

適用機種 SR-S208TC2, 224TC2, 208PD1, 224PS1, 224CP1, 248TC1

ここでは、ETHERBLOCK内のポートで特定のVLANおよびMACアドレスを持つホストからの入力パケットだけ を許可し、その他のホストからの入力パケットを禁止する場合の設定方法を説明します。 「ether 情報」-「フィルタ情報」で設定した場合、ETHER1~8ポートで同一のフィルタを設定する場合も、 ETHERBLOCK1で使用する acl 数は8個となりますが、「etherblock 情報」でETHER1~8ポートで同一のフィル タを設定する場合は ETHERBLOCK1で使用する acl 数は1個となるため、acl 数による制限の緩和に有効です。

● フィルタリング設計

- VLAN 10は ETHER1 ~ 8 ポートで構成されるポート VLAN で、それぞれのポートでタグなしである
- VLAN 20はETHER1~4ポートおよびETHER9~12ポートで構成されるポートVLANで、ETHER1~4ポートでタグ付き、ETHER9~12ポートでタグなしである
- ETHERBLOCK1 (ETHER1~8ポート)のVLAN 10では MAC アドレス 00:0b:01:02:03:04のホストからの入 カパケットだけを許可し、その他はすべて禁止する

上記のフィルタリング設計に従って設定を行う場合の設定例を示します。

(1) VLAN ID が 10 で送信元 MAC アドレスが 00:0b:01:02:03:04 であるパケットの形式を ACL で設定する

- 設定メニューの詳細設定で「ACL 情報」をクリックします。
 「ACL 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 定義名

→acl0



3. [追加] ボタンをクリックします。

「ACL定義情報(acl0)」ページが表示されます。

4. 「MAC定義情報」をクリックします。

「MAC定義情報」が表示されます。

٠	送信元 MAC アドレス	→指定する
	アドレス指定	→00:0b:01:02:03:04
•	あて先 MAC アドレス	→すべて

フォーマット種別 →すべて

■MAC定義情報	
送信元MACアドレス	指定する アドレス指定("指定する"を選択時のみ有効です) 00:0b:01:02:03:04
あて先MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
フォーマット種別	 ● すべて ● LLC形式 ■ LSAP ● Ethernet形式 ■ type値

- 6. [保存] ボタンをクリックします。
- 7. 「VLAN定義情報」をクリックします。

「VLAN定義情報」が表示されます。

8. 以下の項目を指定します。

- VLAN ID → 10
- COS 値 →指定しない

VLAN定義情報		3
VLAN ID	10	
COS値		

- 9. [保存] ボタンをクリックします。
- (2) VLAN IDが10のすべてのパケットの形式をACLで設定する
- 10. 手順1.~3.および手順7.~9.を参考に、以下の項目を設定します。

「ACL情報」

- 定義名 →acl1
- 「ACL定義情報(acl1)」-「VLAN定義情報」
- VLAN ID → 10
- COS値
 →指定しない
 →

 →

 →

(3) ETHERBLOCK1 (ETHER1~8ポート)で(1)で設定した形式のパケットを透過させる

11. 設定メニューの詳細設定で「etherblock 情報」をクリックします。

「etherblock 情報」ページが表示されます。

12. 「etherblock 情報」で etherblock 番号が1の [修正] ボタンをクリックします。

etherblock 1 情報の設定項目と「フィルタ情報」が表示されます。

- 13. 以下の項目を指定します。
 - 動作 →透過
 - ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<フィルタ情報入力フィールド>		
動作	◎透過 ○遮断	
ACL定義番号	0 参照	

- 14. [追加] ボタンをクリックします。
- (4) ETHERBLOCK1 (ETHER1~8ポート)で(2)で設定した形式のパケットを遮断する
- 15. 手順13.~14.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL定義番号 →1
- **16. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

4.5 ETHERBLOCK 単位で特定 MAC アドレスへのパケットだけを 許可する

適用機種 SR-S208TC2, 224TC2, 208PD1, 224PS1, 224CP1, 248TC1

ここでは、ETHERBLOCK内のポートで特定のVLANおよびMACアドレスを持つホストへの送信パケットだけを 許可し、その他のホストへの送信パケットを禁止する場合の設定方法を説明します。 「ether 情報」-「フィルタ情報」で設定した場合、ETHER1~8ポートで同一のフィルタを設定する場合も、 ETHERBLOCK1で使用する acl 数は8個となりますが、「etherblock 情報」でETHER1~8ポートで同一のフィル

タを設定する場合は ETHERBLOCK1 で使用する acl 数は1 個となるため、acl 数による制限の緩和に有効です。

● フィルタリング設計

- VLAN 10は ETHER1 ~8ポートで構成されるポート VLAN で、それぞれのポートでタグなしである
- VLAN 20はETHER1~4ポートおよびETHER9~12 ポートで構成されるポートVLANで、ETHER1~4ポートでタグ付き、ETHER9~12 ポートでタグなしである
- ETHERBLOCK1 (ETHER1~8ポート)のVLAN 10 では MAC アドレス 00:0b:01:02:03:04 のホストへの送信 パケットだけを許可し、その他はすべて禁止する

上記のフィルタリング設計に従って設定を行う場合の設定例を示します。

(1) VLAN ID が 10 であて先 MAC アドレスが 00:0b:01:02:03:04 であるパケットの形式を ACL で設定する

- 設定メニューの詳細設定で「ACL情報」をクリックします。
 「ACL情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 定義名

→acl0



3. [追加] ボタンをクリックします。

「ACL定義情報(acl0)」ページが表示されます。

4. 「MAC定義情報」をクリックします。

「MAC定義情報」が表示されます。

- ・ 送信元 MAC アドレス →すべて
 ・ あて先 MAC アドレス →指定する アドレス指定 →00:0b:01:02:03:04
- フォーマット種別 →すべて

MAC定義情報	3
送信元MACアドレス	すべて アドレス指定("指定する"を選択時のみ有効です)
あて先MACアドレス	指定する ● アドレス指定(‴指定する″を選択時のみ有効です) 00:0b:01:02:03:04
フォーマット種別	 ● すべて ● LLC形式 ■ LSAP ● Ethernet形式 ■ type値

- 6. [保存] ボタンをクリックします。
- 7. 「VLAN定義情報」をクリックします。

「VLAN定義情報」が表示されます。

8. 以下の項目を指定します。

- VLAN ID
- COS値
 →指定しない

5
10

→10

- 9. [保存] ボタンをクリックします。
- (2) VLAN IDが10のすべてのパケットの形式をACLで設定する
- 10. 手順1.~3.および手順7.~9.を参考に、以下の項目を設定します。

「ACL情報」

•	定義名	→acl1
ΓA	CL定義情報	(acl1)」-「VLAN定義情報」
•	VLAN ID	→ 10
•	COS值	→指定しない

(3) ETHERBLOCK1 (ETHER1~8ポート)で(1)で設定した形式のパケットを透過させる

11. 設定メニューの詳細設定で「etherblock 情報」をクリックします。

「etherblock 情報」ページが表示されます。

12. 「etherblock 情報」で etherblock 番号が1の [修正] ボタンをクリックします。

etherblock 1 情報の設定項目と「フィルタ情報」が表示されます。

- 13. 以下の項目を指定します。
 - 動作 →透過
 - ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<フィルタ情報入力フィールド>		
動作	◎透過 ○遮断	
ACL定義番号	0 参照	

- 14. [追加] ボタンをクリックします。
- (4) ETHERBLOCK1 (ETHER1~8ポート)で(2)で設定した形式のパケットを遮断する
- 15. 手順13.~14.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL定義番号 →1
- **16. 画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

4.6 ETHERBLOCK 単位で特定パケット形式のパケットだけを禁止 する

適用機種 SR-S208TC2, 224TC2, 208PD1, 224PS1, 224CP1, 248TC1

ここでは、ETHERBLOCK内のポートで特定のパケット形式を持つ入力パケットだけを禁止し、その他の入力パケットを許可する場合の設定方法を説明します。

「ether 情報」-「フィルタ情報」で設定した場合、ETHER1~8ポートで同一のフィルタを設定する場合も、 ETHERBLOCK1で使用する acl 数は8個となりますが、「etherblock 情報」で ETHER1~8ポートで同一のフィル タを設定する場合は ETHERBLOCK1で使用する acl 数は1個となるため、acl 数による制限の緩和に有効です。

● フィルタリング設計

- VLAN 10は ETHER1 ~ 8 ポートで構成されるポート VLAN で、それぞれのポートでタグなしである
- VLAN 20は ETHER1~4ポートおよび ETHER9~12ポートで構成されるポート VLAN で、ETHER1~4ポートでタグ付き、ETHER9~12ポートでタグなしである
- ETHERBLOCK1 (ETHER1~8ポート)ではIPプロトコルの入力パケットだけを禁止し、その他はすべて許可する

上記のフィルタリング設計に従って設定を行う場合の設定例を示します。

(1) IP プロトコルのパケット (IP, ARP, Reverse ARP) の形式を ACL で設定する

→ acl0

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名



- 【追加】ボタンをクリックします。
 「ACL定義情報(acl0)」ページが表示されます。
- **4. 「MAC 定義情報」をクリックします**。 「MAC 定義情報」が表示されます。

- ・ 送信元 MAC アドレス →すべて
- あて先MACアドレス →すべて
- フォーマット種別 → Ethernet形式
 type値 → 0800

■MAC定義情報	3
送信元MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
あて先MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
フォーマット種別	 すべて LLC形式 LSAP Ethernet形式 type値 0800

6. [保存] ボタンをクリックします。

7. 手順1.~6.を参考に、以下の項目を設定します。

「ACL情報」

• 定義名 → acl1

「ACL定義情報 (acl1)」-「MAC 定義情報」

- 送信元 MAC アドレス →すべて
- あて先MACアドレス →すべて
- フォーマット種別 → Ethernet形式
 type値 → 0806

「ACL情報」

• 定義名 → acl2

「ACL定義情報(acl2)」-「MAC定義情報」

- 送信元 MAC アドレス →すべて
- あて先 MAC アドレス →すべて
- フォーマット種別 → Ethernet形式 type値 → 8035

(2) ETHERBLOCK1 (ETHER1~8ポート)で(1)で作成したパケットのパターンを遮断 する

8. 設定メニューの詳細設定で「etherblock 情報」をクリックします。

「etherblock 情報」ページが表示されます。

9. 「etherblock 情報」でetherblock 番号が1の [修正] ボタンをクリックします。

etherblock 1 情報の設定項目と「フィルタ情報」が表示されます。

10. 以下の項目を指定します。

- 動作 →遮断
- ACL定義番号 →0

<フィルタ情報入力フィールド>		
動作	○透過 ⊙ 遮断	
ACL定義番号	0 参照	

- 11. [追加] ボタンをクリックします。
- 12. 手順10.~11.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL定義番号 → 1
- 13. 手順 10.~11.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL定義番号 →2
- 14. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

4.7 VLAN 単位で特定 MAC アドレス間の通信だけを遮断する

適用機種 全機種

ここでは、VLAN内のポートで特定のMACアドレスを持つホスト間の通信だけを遮断する場合の設定方法を説明します。

こんな事に気をつけて

SR-S308TL1/310TL2/316TL1/318TL2/324TL2 では、以下の機能を同時に使用することができません。 MAC フィルタ情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ/QoS 資源の配分」の機能を"フィ ルタのみ"、プロトコルを"IPv4のみ"に設定する必要があります。

- MACフィルタ機能(IPv4) / IPフィルタリング機能(IPv4)
- MACフィルタ機能(IPv6フィルタ) / IPフィルタリング機能(IPv6)
- ・ 優先制御情報書き換え機能(IPv4)/DSCP値書き換え機能(IPv4)
- ・ 優先制御情報書き換え機能(IPv6) / DSCP 値書き換え機能(IPv6)

● フィルタリング設計

- VLAN10はETHER1~4ポートでタグなし、ETHER5~8ポートでタグ付きで構成されるポートVLANである
- VLAN20はETHER1~4ポートでタグ付き、ETHER5~8ポートでタグなしで構成されるポートVLANである
- VLAN10ではMACアドレス00:0b:01:02:03:04のホストからMACアドレス00:0b:11:12:13:14間のTCP通信だけを禁止し、VLAN 20ではMACアドレス00:0b:21:22:23:24のホストからMACアドレス00:0b:31:32:33:34 間のUDP通信だけを禁止する

上記のフィルタリング設計に従って設定を行う場合の設定例を示します。

(1)送信元 MAC アドレスが 00:0b:01:02:03:04、あて先 MAC アドレスが 00:0b:11:12:13:14 である TCP パケットの形式を ACL で設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

定

<acl情報追加フィールド></acl情報追加フィールド>			
義名	ac IO		

→acl0

3. [追加] ボタンをクリックします。

「ACL定義情報 (acl0)」ページが表示されます。

4. 「MAC 定義情報」をクリックします。 「MAC 定義情報」が表示されます。

- 送信元 MAC アドレス →指定する アドレス指定
- あて先 MAC アドレス アドレス指定
- →00:0b:01:02:03:04 →指定する
- →00:0b:11:12:13:14
- フォーマット種別

フォーマット種別	→すべて
MAC定義情報	3
送信元MACアドレス	指定する ▼ アドレス指定(″指定する″を選択時のみ有効です) 00:0b:01:02:03:04
あて先MACアドレス	指定する ▼ アドレス指定(″指定する″を選択時のみ有効です) 00:0b:11:12:13:14
フォーマット種別	 ● すべて ● LLC形式 ● LSAP ● Ethernet形式 type値

- 6. [保存] ボタンをクリックします。
- 7. 「IP定義情報」をクリックします。

「IP定義情報」が表示されます。

8. 以下の項目を指定します。

•	プロトコル	→tcp
•	送信元情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0.0)
•	あて先情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0)

• QoS

→指定なし

ブロトコル		tcp (番号指定: ************************************
送信元情	IPアドレス	
報	アトレスマ スク	0 (0.0.0)
あて失情	IPアドレス	
報	アトレスマ スク	0 (0.0.0)
QoS		^{指定なし} TOS、または、DSCPを選択時に値を入力してく ださい

[保存] ボタンをクリックします。 9.

(2)送信元 MAC アドレスが 00:0b:11:12:13:14、あて先 MAC アドレスが 00:0b:01:02:03:04 である TCP パケットの形式を ACL で設定する

10. 手順1.~9.を参考に、以下の項目を設定します。

「ACL情報」

定義名

→acl1

「ACL定義情報 (acl1)」-「MAC 定義情報」

- ・ 送信元 MAC アドレス →指定する
 アドレス指定 → 00:0b:11:12:13:14
- あて先MACアドレス →指定する
 アドレス指定 →00:0b:01:02:03:04
- フォーマット種別 →すべて

「ACL定義情報 (acl1)」-「IP 定義情報」

- プロトコル → tcp
 送信元情報
 iPアドレス →指定しない
 アドレスマスク → 0 (0.0.0.0)

 あて先情報
 iPアドレス →指定しない
 アドレスマスク → 0 (0.0.0.0)
- QoS →指定なし
- (3)送信元 MAC アドレスが 00:0b:21:22:23:24、あて先 MAC アドレスが 00:0b:31:32:33:34 である UDP パケットの形式を ACL で設定する

11. 手順1.~9.を参考に、以下の項目を設定します。

「ACL情報」

 定義名 →acl2 「ACL定義情報(acl2)」-「MAC定義情報」 • 送信元 MAC アドレス →指定する アドレス指定 →00:0b:21:22:23:24 • あて先 MAC アドレス →指定する アドレス指定 →00:0b:31:32:33:34 フォーマット種別 →すべて 「ACL定義情報(acl2)」-「IP定義情報」 • プロトコル →udp 送信元情報 IPアドレス →指定しない アドレスマスク →0 (0.0.0.0) あて先情報 IPアドレス →指定しない

- アドレスマスク →0 (0.0.0.0)
- QoS →指定なし

- (4)送信元 MAC アドレスが 00:0b:31:32:33:34、あて先 MAC アドレスが 00:0b:21:22:23:24 である UDP パケットの形式を ACL で設定する
- 12. 手順1.~9.を参考に、以下の項目を設定します。

「ACL **情報」** • 定義名

→ acl3

「ACL定義情報 (acl3)」-「MAC 定義情報」

- ・ 送信元 MAC アドレス →指定する
 アドレス指定 → 00:0b:31:32:33:34
- あて先MACアドレス →指定する
 アドレス指定 →00:0b:21:22:23:24
- フォーマット種別 →すべて

「ACL定義情報 (acl3)」-「IP 定義情報」

- プロトコル → udp
 送信元情報
 IPアドレス →指定しない
 アドレスマスク → 0 (0.0.00)
- あて先情報
 IPアドレス →指定しない
 アドレスマスク → 0 (0.0.00)
 QoS →指定なし
- (5) VLAN10で(1)、(2) で設定した形式のパケットを遮断する

13. 設定メニューの詳細設定で「VLAN情報」をクリックします。

「VLAN情報」ページが表示されます。

- 14. 以下の項目を指定します。
 - VLAN ID

→ 10

<vlan情報追加フィールド></vlan情報追加フィールド>		
VLAN ID	10	

15. [追加] ボタンをクリックします。

「VLAN10情報」ページが表示されます。

16. 「フィルタ情報」をクリックします。 「フィルタ情報」が表示されます。

• 動作

• ACL定義番号 →0

▲ 「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<フィルタ情報入力フィールド>			
動作 ②透過 ③遮断			
ACL定義番号 0 参照			

→遮断

- 18. [追加] ボタンをクリックします。
- 19. 手順 17.~18.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL定義番号 →1
- (6) VLAN20で(3)、(4) で設定した形式のパケットを遮断する
- 20. 手順13.~18.を参考に、以下の項目を設定します。

「VLAN情報」

• VLAN ID →20

- 「VLAN20 情報」-「フィルタ情報」
- 動作 →遮断
- ACL定義番号 →2
- 21. 手順 17.~18.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL定義番号 →3
- **22. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

4.8 VLAN 単位で特定パケット形式のパケットだけを許可する

適用機種 全機種

ここでは、VLAN内のポートで特定のパケット形式を持つ入力パケットだけを許可し、その他の入力パケットを 遮断する場合の設定方法を説明します。

こんな事に気をつけて SR-S308TL1/310TL2/316TL1/318TL2/324TL2では、以下の機能を同時に使用することができません。 MAC フィルタ情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ/QoS資源の配分」の機能を"フィ ルタのみ"、プロトコルを"IPv4のみ"に設定する必要があります。

- MAC フィルタ機能(IPv4) / IP フィルタリング機能(IPv4)
- MACフィルタ機能(IPv6フィルタ) / IPフィルタリング機能(IPv6)
- 優先制御情報書き換え機能(IPv4) / DSCP 値書き換え機能(IPv4)
- ・ 優先制御情報書き換え機能(IPv6) / DSCP 値書き換え機能(IPv6)

● フィルタリング設計

- VLAN10はETHER1~4ポートでタグなし、ETHER5~8ポートでタグ付きで構成されるポートVLANである
- VLAN20はETHER1~4ポートでタグ付き、ETHER5~8ポートでタグなしで構成されるポートVLANである
- VLAN10ではIPプロトコルの入力パケットだけを許可する
- VLAN 20では FNA プロトコルの入力パケットだけを許可する

上記のフィルタリング設計に従って設定を行う場合の設定例を示します。

(1) IP プロトコルのパケット (IP, ARP, Reverse ARP)の形式をACL で設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。 「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

→acl0



- **3. [追加] ボタンをクリックします**。 「ACL 定義情報 (acl0) | ページが表示されます。
- **4. 「MAC 定義情報」をクリックします**。 「MAC 定義情報」が表示されます。

- ・ 送信元 MAC アドレス →すべて
- あて先MACアドレス →すべて
- フォーマット種別 → Ethernet形式
 type値 → 0800

MAC定義情報	
送信元MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
あて先MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
フォーマット種別	 すべて LLC形式 LSAP Ethernet形式 type値 0800

6. [保存] ボタンをクリックします。

7. 手順1.~6.を参考に、以下の項目を設定します。

「ACL情報」

• 定義名 → acl1

「ACL定義情報 (acl1)」-「MAC 定義情報」

- 送信元 MAC アドレス →すべて
- あて先MACアドレス →すべて
- フォーマット種別 → Ethernet形式
 type値 → 0806

「ACL情報」

• 定義名 → acl2

「ACL定義情報(acl2)」-「MAC定義情報」

- 送信元 MAC アドレス →すべて
- あて先 MAC アドレス →すべて
- フォーマット種別 → Ethernet形式 type値 → 8035

(2) FNA プロトコルのパケットの形式を ACL で設定する

8. 手順1.~6.を参考に、以下の項目を設定します。

「ACL情報」

• 定義名 → acl3

「ACL定義情報 (acl3)」-「MAC 定義情報」

- 送信元 MAC アドレス →すべて
- あて先MACアドレス →すべて
- フォーマット種別 → LLC形式 LSAP → 8080

「ACL情報」

• 定義名 → acl4

「ACL定義情報	(acl4)] -	「MAC定義情報」
----------	-----------	-----------

- 送信元 MAC アドレス →すべて
- あて先 MAC アドレス →すべて
- フォーマット種別 → LLC形式
 LSAP → 0000

「ACL情報」

• 定義名 → acl5

「ACL定義情報 (acl5)」-「MAC 定義情報」

- ・ 送信元 MAC アドレス →すべて
- あて先 MAC アドレス →すべて
- フォーマット種別 → LLC形式
 LSAP → 0001
- (3) 全プロトコルのパケットの形式をACLで設定する

9. 手順1.~6を参考に、以下の項目を設定します。

「ACL情報」

- • 定義名 → acl6

 「ACL定義情報 (acl6)」 「MAC 定義情報」
- ・ 送信元 MAC アドレス →すべて
- あて先MACアドレス →すべて
- フォーマット種別 →すべて

(4) VLAN10で(1) で作成したパケットのパターン以外を遮断する

設定メニューの詳細設定で「VLAN 情報」をクリックします。 10.

「VLAN情報」ページが表示されます。

11. 以下の項目を指定します。

 VLAN ID **→**10



12. [追加] ボタンをクリックします。

「VLAN10情報」ページが表示されます。

- 13. 「フィルタ情報」をクリックします。 「フィルタ情報」が表示されます。
- 14. 以下の項目を指定します。
 - 動作 →透過
 - ACL定義番号 **→**0

「ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の [選択] ボタンをクリックして設定します。

<フィルタ情報入力フィールド>		
動作		
ACL定義番号	0 参照	

- 15. [追加] ボタンをクリックします。
- 手順14.~15.を参考に、以下の項目を設定します。 16.
 - 動作 →透過
 - ACL定義番号 **→**1
- 17. 手順14.~15.を参考に、以下の項目を設定します。
 - 動作 →透過
 - ACL 定義番号 →2
- 18. 手順14.~15.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL 定義番号 →6

(5) VLAN20で(2) で作成したパケットのパターン以外を遮断する

19. 手順 10.~15.を参考に、以下の項目を設定します。

「VLAN情報」 • VLAN ID →20 「VLAN20情報」-「フィルタ情報」 動作 →透過 ACL定義番号 →3 20. 手順14.~15.を参考に、以下の項目を設定します。 動作 →透過 ACL定義番号 →4 21. 手順14.~15.を参考に、以下の項目を設定します。 動作 →透過 ACL 定義番号 →5

- 22. 手順14.~15.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL定義番号 →6
- 23. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

5 スタティック MAC フォワーディング機能を使う



スタティックMACフォワーディング機能を利用すると、構成定義によって、MACアドレスをスタティックにFDB に登録することができ、フラッディングによる余分なフレームがネットワーク上を流れることを防止できます。 ここでは、各ETHERポートに接続されるサーバのMACアドレスをスタティックエントリとして設定する方法を 説明します。

SR-S316C2/716C2の場合を例にします。



● 設定条件

- ETHER2、5ポートにサーバ1、2を接続し、VLANを10とする
- ETHER10ポートにサーバ3を接続し、VLANを20とする
- サーバ1のMACアドレス : 00:00:00:00:011
- サーバ2のMACアドレス : 00:00:00:00:22
- サーバ3のMACアドレス : 00:00:00:00:033

上記の設定条件に従って設定を行う場合の設定例を示します。

ETHER ポートに VLAN を設定する

- 設定メニューの詳細設定で「ether 情報」をクリックします。
 「ether 情報」ページが表示されます。
- [ether 情報] でポート番号が2の [修正] ボタンをクリックします。
 ether 2 情報の設定項目と「基本情報」が表示されます。
- 3. 以下の項目を指定します。
 - VLAN
 Untagged

→10

VLAN	Tagged	
V L/UV	Untagged	10

4. [保存] ボタンをクリックします。

5. 手順1.~4.を参考に、以下の項目を設定します。

[ether 5]	
• VLAN	
Untagged	→ 10
[ether 10]	
[ether 10] • VLAN	

VLAN にスタティック MAC フォワーディングを設定する

6. 設定メニューの詳細設定で「VLAN 情報」をクリックします。

「VLAN 情報」ページが表示されます。

- 7. 以下の項目を指定します。
 - VLAN ID

<vlan情報追加フィールド></vlan情報追加フィールド>		
VLAN ID	10	

→10

- **8. [追加] ボタンをクリックします**。 「VLAN10 情報」ページが表示されます。
- **9.** 「静的 MAC 学習テーブル情報」をクリックします。 「静的 MAC 学習テーブル情報」が表示されます。
- 10. 以下の項目を指定します。
 - MACアドレス → 00:00:00:00:00:11
 - ポート番号 →2

<静的MAC学習テーブル情報入力フィールド>		
MACアドレス	00:00:00:00:11	
ポート番号	2 🗸	

- 11. [追加] ボタンをクリックします。
- **12.** 静的MAC学習テーブルが追加されたことを確認し、画面左側の[設定反映]ボタンをクリックします。 設定した内容が有効になります。

13. 手順6.~12.を参考に、以下の項目を設定します。

[サーバ2]

「VLAN 情報」 • VLAN ID

- **→**10
- 「VLAN10情報」-「静的MAC学習テーブル情報」
- MACアドレス →00:00:00:00:22
- ポート番号 →5

[サーバ3]

「VLAN情報」

• VLAN ID →20

「VLAN20情報」-「静的MAC学習テーブル情報」

- MACアドレス →00:00:00:00:33
- ポート番号 → 10
- 14. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

6 QoS 機能を使う

適用機種 全機種

● 参照 機能説明書「2.12 QoS機能」(P.63)

6.1 優先制御機能を使う

適用機種 全機種

本装置では、VLAN機能のユーザプライオリティ値に出力ポート(自装置あてポート含む)の複数の優先度の異なるキューを対応付けることで、パケットの優先制御を行うことができます。

こんな事に気をつけて

- ・ 本装置の初期設定は、機能説明書「2.12.1 優先制御機能」(P.63)を参照してください。
- SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1/308TL1/310TL2/316TL1/318TL2/324TL2の場合のキュー は4個、SR-S316C2/324TC1/328TR1/348TC1/716C2/724TC1/748TC1の場合のキューは8個となります。

SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1/308TL1/ 310TL2/ 316TL1/318TL2/324TL2の場合

● 優先制御設計

パケットのタイプ	CoS值	装置内部のキュークラス
管理パケット	7	3
	6	
音声	5	
FAX/呼制御	4	2
映像	3	
	2	1
その他	1	
	0	0

上記の優先制御設定に従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「QoS 情報」をクリックします。

「QoS情報」ページが表示されます。

2. 「COSキュー情報」をクリックします。

「COSキュー情報」が表示されます。

- パケットのCOS値
 - 0→0
 - 1→1
 - 2→1
 - 3→2
 - 4→2
 - 5→3
 - 6→3
 - 7→3

■COSキュー情報	3
パケットのCOS値	格納キュー
0	0 💌
1	1 💌
2	1 💌
3	2 🗸
4	2 💌
5	3 🗸
6	3 🗸
7	3 💌

- 4. [保存] ボタンをクリックします。
- 5. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

SR-S316C2/324TC1/328TR1/348TC1/716C2/724TC1/748TC1の場合

パケットのタイプ	CoS值	装置内部のキュークラス
管理パケット	7	4
	6	
音声	5	3
FAX/呼制御	4	2
映像	3	1
	2	
その他	1	0
	0	

● 優先制御設計

上記の優先制御設定に従って設定を行う場合の設定例を示します。

- **1. 設定メニューの詳細設定で「QoS 情報」をクリックします**。 「QoS 情報」ページが表示されます。
- **2. 「COSキュー情報」をクリックします**。 「COSキュー情報」が表示されます。

- パケットのCOS値
 - 0→0
 - 1→0
 - 2→1
 - 3→1
 - 4→2
 - 5→3
 - 6→4
 - 7→4

■COSキュー情報	3
バケットのCOS値	格納キュー
0	0 🗸
1	0 🗸
2	1 🗸
3	1 🕶
4	2 🗸
5	3 🗸
6	4 🗸
7	4 💌

- 4. [保存] ボタンをクリックします。
- 5. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

6.2 優先制御情報書き換え機能を使う

適用機種 全機種

本装置を経由して送出されるパケットをMACアドレス、パケット形式、ETHERNETタイプ、VLAN ID、COS 値などの組み合わせで指定し、ETHER ポートへの入力時に優先制御情報を書き換えることができます。

こんな事に気をつけて

SR-S308TL1/310TL2/316TL1/318TL2/324TL2では、以下の機能を同時に使用することができません。 優先制御情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ/QoS 資源の配分」の機能を"QoSのみ"、 プロトコルを"IPv4のみ"に設定する必要があります。

- MACフィルタ機能(IPv4) / IPフィルタリング機能(IPv4)
- MACフィルタ機能(IPv6フィルタ) / IPフィルタリング機能(IPv6)
- 優先制御情報書き換え機能(IPv4) / DSCP 値書き換え機能(IPv4)
- 優先制御情報書き換え機能(IPv6) / DSCP 値書き換え機能(IPv6)

書き換え条件

以下の条件を指定することによって、優先制御情報を書き換えることができます。

- ACLのMAC定義およびVLAN定義で指定した以下の情報
 - 送信元 MAC 情報(MAC アドレス/パケット形式/ ETHERNET タイプ/ LSAP)
 - あて先 MAC 情報(MAC アドレス/パケット形式/ ETHERNET タイプ/ LSAP)
 - VLAN ID
 - COS値
 - 送信元 IP 情報 (IP アドレス/アドレスマスク)
 - あて先IP情報(IPアドレス/アドレスマスク)
 - TCP・UDPのポート番号
 - ICMP TYPE、ICMP CODE
 - IPパケットのTOS値、DSCP値
- 優先制御情報書き換えの対象となるパケット入力 ETHER ポート
- 優先制御情報書き換え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以下の動作
 - パケットのCOS値を指定した値で書き換える
 - パケットの COS 値をパケットの ip precedence 値で書き換える
 - パケットのDSCP値を指定した値で書き換える
 - パケットの ip precedence 値を指定した値で書き換える
 - パケットのip precedence 値をパケットの COS 値で書き換える
 - 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を指定したキューに変更する

以下に設定例を示します。

パケットの COS 値を指定した値で書き換える

適用機種 全機種

ここでは、VLAN内の特定ポートで特定のMACアドレスを持つホストからの入力パケットのCOS値を指定した 値に書き換える方法を説明します。

● 書き換え要求

- VLAN 20はETHER1~5ポートで構成されるポートVLANで、ETHER1~4ポートでタグ付き、ETHER5 ポートでタグなしである
- ETHER5ポートのVLAN 20では MAC アドレス 00:0b:01:02:03:04のホストからの入力パケットの COS 値を5 に変更する

上記の書き換え要求に従って設定を行う場合の設定例を示します。

 (1) VLAN ID が 20 で送信元 MAC アドレスが 00:0b:01:02:03:04 であるパケットの形式を ACL で設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL 情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - ・ 定義名
 → acl0

<acl情報追加フィールド></acl情報追加フィールド>			
定義名 acl0 acl0 acl0 acl0 acl0 acl0 acl0 acl0			

3. [追加] ボタンをクリックします。

「ACL 定義情報(acl0)」ページが表示されます。

4. 「MAC定義情報」をクリックします。

「MAC 定義情報」が表示されます。

5. 以下の項目を指定します。

- ・ 送信元 MAC アドレス →指定する アドレス指定 → 00:0b:01:02:03:04
- あて先MACアドレス →すべて
- フォーマット種別 →すべて

MAC定義情報	3
送信元MACアドレス	指定する ▼ アドレス指定(″指定する″を選択時のみ有効です) 00:0b:01:02:03:04
あて先MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
フォーマット種別	 ● すべて ● LLC形式 ■ LSAP ● Ethernet形式 ■ type値

- 6. [保存] ボタンをクリックします。
- **7. 「VLAN 定義情報」をクリックします**。 「VLAN 定義情報」が表示されます。
- 8. 以下の項目を指定します。
 - VLAN ID → 20

•	COS值	→指定しない

■VLAN定義情報	3
VLAN ID	20
COS値	

- 9. [保存] ボタンをクリックします。
- (2) ETHER5ポートで(1) で設定した形式のパケットのCOS値を5に書き換える
- **10. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- **11.** 「ether 情報」でポート番号が5の [修正] ボタンをクリックします。 ether 5 情報の設定項目と「基本情報」が表示されます。
- 12. 「QoS関連」をクリックします。

QoS関連の設定項目と「基本情報」が表示されます。

13. QoS 関連の設定項目の「QoS 情報」をクリックします。

「QoS情報」が表示されます。

- 14. 以下の項目を指定します。
 - 動作 → cos 値書き換え
 書き換え値 → cos 値指定 5
 - ACL定義番号 →0

1
1 HB

ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<qos情報入力フィールド></qos情報入力フィールド>			
	 ⊙ cos値書き換え 		
		書き換え 値	●cos値指定 5 ○ip precedence値
	○ ip precedence値書き換え		
動作		書き換え 値	 ● ip precedence値指定 ○ cos値
	0		
		書き換え 値	
	0	出力キュー	
ACL定義番号	0	参照	

15. [追加] ボタンをクリックします。

16. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

パケットのCOS 値をパケットの ip precedence 値で書き換える

適用機種 全機種

ここでは、VLAN内の特定ポートで特定のMACアドレスを持つホストへの送信パケットのCOS値をパケットの ip precedence 値で書き換える方法を説明します。

● 書き換え要求

- VLAN 10は ETHER1 ~8ポートで構成されるポート VLAN で、すべてタグ付きである
- ETHER1 ポートの VLAN 10 では MAC アドレス 00:0b:01:02:03:04 のホストへの送信パケットの COS 値をパ ケットの ip precedence 値で書き換える

上記の書き換え要求に従って設定を行う場合の設定例を示します。

- (1) VLAN ID が10であて先MACアドレスが00:0b:01:02:03:04であるパケットの形式を ACLで設定する
- 1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL 情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名 → acl0



- **3. [追加] ボタンをクリックします**。 「ACL 定義情報(acl0)」ページが表示されます。
- **4.** 「MAC定義情報」をクリックします。

「MAC定義情報」が表示されます。

- ・ 送信元 MAC アドレス →すべて
 ・ あて先 MAC アドレス →指定する アドレス指定 →00:0b:01:02:03:04
- フォーマット種別 →すべて

■MAC定義情報		
送信元MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)	
あて先MACアドレス	指定する ▼ アドレス指定("指定する"を選択時のみ有効です) 00:0b:01:02:03:04	
フォーマット種別	 すべて LLC形式 LSAP Ethernet形式 type値 	

- 6. [保存] ボタンをクリックします。
- 7. 「VLAN定義情報」をクリックします。

「VLAN定義情報」が表示されます。

8. 以下の項目を指定します。

- VLAN ID → 10
- COS値
 →指定しない

■VLAN定義情報	3
VLAN ID	10
COS値	

- 9. [保存] ボタンをクリックします。
- (2) ETHER1 ポートで(1) で設定した形式のパケットのCOS 値をパケットの ip precedence 値で書き換える
- **10. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- **11.** 「ether 情報」でポート番号が1の [修正] ボタンをクリックします。 ether 1 情報の設定項目と「基本情報」が表示されます。
- 12.
 「QoS 関連」をクリックします。

 QoS 関連の設定項目と「基本情報」が表示されます。
- **13.** QoS **関連の設定項目の「QoS 情報」をクリックします**。 「QoS 情報」が表示されます。

- 動作 → cos 値書き換え 書き換え値 →ip precedence 値 **→**0
- ACL 定義番号

「ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の [選択] ボタンをクリックして設定します。

<qos情報入力フィールド></qos情報入力フィールド>			
	 ⊙ cos値書き換え 		
		書き換え 値	○cos値指定 ⊙ip precedence値
	○ ip precedence値書き換え		ce値書き換え
動作	書き換え 値 dscp値書き 書き換え 値	書き換え 値	⊙ip precedence値指定 ○cos値
		dscp値書き換え	
	○ 出力キュー指定		
ACL定義番号	0	参照	

- [追加] ボタンをクリックします。 15.
- 画面左側の [設定反映] ボタンをクリックします。 16. 設定した内容が有効になります。

パケットの DSCP 値を指定した値で書き換える

適用機種 全機種

ここでは、VLAN内の特定ポートですべての入力パケットのDSCP値を指定した値で書き換える方法を説明します。

● 書き換え要求

- VLAN 10はETHER1~8ポートで構成されるポートVLANで、すべてタグ付きである
- ETHER1 ポートでは全入力パケットの DSCP 値を40 に書き換える

上記の書き換え要求に従って設定を行う場合の設定例を示します。

(1) すべてのパケットの形式をACLで設定する

- 設定メニューの詳細設定で「ACL情報」をクリックします。 1. 「ACL 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 定義名 → acl0

<acl情報追加フィールド></acl情報追加フィールド>			
定義名	acl0		

- 【追加】ボタンをクリックします。
 「ACL 定義情報(acl0)」ページが表示されます。
- **4.** 「MAC定義情報」をクリックします。

「MAC定義情報」が表示されます。

- 5. 以下の項目を指定します。
 - ・ 送信元 MAC アドレス →すべて
 - あて先MACアドレス →すべて
 - フォーマット種別 →すべて

MAC定義情報	3
送信元MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
あて先MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
フォーマット種別	 ● すべて ● LLC形式 ■ LSAP ● Ethernet形式 ■ type値

- 6. [保存] ボタンをクリックします。
- (2) ETHER1ポートで(1) で設定した形式のパケットのDSCP 値を40 に書き換える
- 設定メニューの詳細設定で「ether 情報」をクリックします。
 「ether 情報」ページが表示されます。
- Fether 情報」でポート番号が1の[修正]ボタンをクリックします。
 ether 1 情報の設定項目と「基本情報」が表示されます。
- 「QoS 関連」をクリックします。
 QoS 関連の設定項目と「基本情報」が表示されます。
- **10.** QoS 関連の設定項目の「QoS 情報」をクリックします。 「QoS 情報」が表示されます。

٠	動作	→dscp 値書き換え
	書き換え値	→ 40
•	ACL定義番号	→ 0

「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<qos情報入力フィールド></qos情報入力フィールド>			
	○ cos値書き換え		
		書き換え 値	⊙cos值指定 ○ip precedence值
	○ ip precedence値書き換え		ce値書き換え
動作		書き換え 値	⊙ip precedence值指定 ○cos値
	 ● dscp値書き 書き換え 値 	dscp値書き換え	
		40	
	\circ	出力キュー打	
ACL定義番号	0	参照	

- 12. [追加] ボタンをクリックします。
- **13. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

パケットの ip precedence 値を指定した値で書き換える

適用機種 全機種

ここでは、VLAN内の特定ポートで特定のCOS値の入力パケットのip precedence値を指定した値に書き換える方法を説明します。

● 書き換え要求

- VLAN 10は ETHER1~8ポートで構成されるポート VLAN で、すべてタグ付きである
- VLAN 10 では COS 値5のパケットが入力された場合に、入力パケットの ip precedence 値を6 に書き換える

上記の書き換え要求に従って設定を行う場合の設定例を示します。

(1) VLAN ID が 10 で COS 値が5のパケットの形式を ACL で設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL 情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

→acl0

<acl情報追加フィールド></acl情報追加フィールド>				
定義名	ac IO			

- 【追加】ボタンをクリックします。
 「ACL 定義情報 (acl0)」ページが表示されます。
- **4. 「VLAN 定義情報」をクリックします**。 「VLAN 定義情報」が表示されます。

|VLAN に我 同報」 が 衣小 C 1 は 9。

- 5. 以下の項目を指定します。
 - VLAN ID → 10
 - COS値 →5

VLAN定義情報	3
VLAN ID	10
COS値	5

- 6. [保存] ボタンをクリックします。
- (2) VLAN10に属するETHER1~8ポートで(1)で設定した形式のパケットのip precedence 値を6に書き換える
- 7. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether 情報」ページが表示されます。

- 8. 以下の項目を指定します。
 - ポートリスト → 1-8
 ポート リスト 1-8
 修正 初期化
- [修正] ボタンをクリックします。
 ether 1-8 情報の設定項目と「基本情報」が表示されます。
- **10.** 「QoS 関連」をクリックします。 QoS 関連の設定項目と「基本情報」が表示されます。
- 11. QoS 関連の設定項目の「QoS 情報」をクリックします。

「QoS情報」が表示されます。

- 動作 → ip precedence 値書き換え 書き換え値 → ip precedence 值指定 6 →0
- ACL定義番号

「ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の [選択] ボタンをクリックして設定します。

<qos情報入力フィールド></qos情報入力フィールド>			
	○ cos値書き換え		
		書き換え 値	⊙cos値指定 ○ip precedence値
	۲	ip precedence値書き換え	
動作		書き換え 値	 ⊙ ip precedence値指定 ○ cos値
	 ○ dscp値書ぎ 書き換え 値 		
	0	出力キュー	
ACL定義番号	0	参照	

- 13. [追加] ボタンをクリックします。
- 14. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

パケットの ip precedence 値をパケットの COS 値で書き換える

適用機種 全機種

ここでは、VLAN内の特定ポートで特定のVLANからの入力パケットのip precedence 値をパケットのCOS 値で 書き換える方法を説明します。

● 書き換え要求

ETHER10ポートはVLAN10、VLAN20、VLAN30にタグ付き、VLAN100にタグなしで属する ETHER10 ポートからのVLAN 20、VLAN30、VLAN100からの入力パケットの ip precedence 値をパケットの COS値に書き換える

上記の書き換え要求に従って設定を行う場合の設定例を示します。
(1) VLAN IDが20、30、100のパケットの形式をそれぞれACLで設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL 情報」ページが表示されます。

2. 以下の項目を指定します。



- **3. [追加] ボタンをクリックします**。 「ACL 定義情報(acl0)」ページが表示されます。
- **fvlan定義情報」をクリックします。** 「vlan定義情報」が表示されます。
- 5. 以下の項目を指定します。
 - VLAN ID →20
 - COS値
 →指定しない

■VLAN定義情報	3
VLAN ID	20
COS值	

- 6. [保存] ボタンをクリックします。
- 7. 手順1.~6.を参考に、以下の項目を設定します。

「ACL情報」

- 定義名 → acl1
- 「ACL定義情報 (acl1)」-「VLAN 定義情報」
- VLAN ID → 30
- COS値
 →指定しない

「ACL情報」

- 定義名 → acl2
- 「ACL定義情報 (acl2)」-「VLAN 定義情報」
- VLAN ID → 100
- COS値
 →指定しない
- (2) ETHER10 ポートで(1) で作成した形式のパケットの ip precedence 値をパケットの COS 値に書き換える
- 8. 設定メニューの詳細設定で「ether情報」をクリックします。 「ether情報」ページが表示されます。
- **9.** 「ether 情報」でポート番号が10の [修正] ボタンをクリックします。
 ether 10 情報の設定項目と「基本情報」が表示されます。

「QoS関連」をクリックします。 10.

QoS関連の設定項目と「基本情報」が表示されます。

- 11. QoS関連の設定項目の「QoS情報」をクリックします。 「QoS情報」が表示されます。
- 12. 以下の項目を指定します。
 - 動作 → ip precedence 値書き換え
 - →cos値 書き換え値
 - ACL 定義番号 →0



▲ 「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の [選択] ボタンをクリックして設定します。

<qos情報入力フィールド></qos情報入力フィールド>				
	0	cos値書き換え		
		書き換え 値	⊙cos値指定 ○ip precedence値	
	۲	ip preceden	ce値書き換え	
動作		書き換え 値	○ip precedence値指定 ⑨cos値	
	0	dscp値書ぎ	換え	
		書き換え 値		
	0	出力キュー		
ACL定義番号	0	参照		

[追加] ボタンをクリックします。 13.

14. 手順12.~13.を参考に、以下の項目を設定します。

- 動作 → ip precedence 値書き換え 書き換え値 →cos値
- ACL定義番号 **→**1
- 手順12.~13.を参考に、以下の項目を設定します。 15.
 - 動作 → ip precedence 値書き換え 書き換え値 →cos値 • ACL 定義番号 **→**2

画面左側の〔設定反映〕ボタンをクリックします。 16.

設定した内容が有効になります。

ETHERBLOCK単位でパケットの COS 値を指定した値で書き換える

適用機種 SR-S208TC2, 224TC2, 208PD1, 224PS1, 224CP1, 248TC1

ここでは、ETHERBLOCK内のポートで特定のVLANおよび特定のMACアドレスを持つホストからの入力パケットのCOS値を指定した値に書き換える方法を説明します。

「ether 情報」-「QoS 関連」で設定した場合、ETHER1~8ポートで同一の優先制御情報書き換えを設定する場合 も、ETHERBLOCK1で使用する acl 数は8個となりますが、「etherblock 情報」でETHER1~8ポートで同一の優 先制御情報書き換えを設定する場合はETHERBLOCK1で使用する acl 数は1個となるため、acl 数による制限の緩 和に有効です。

● 書き換え要求

- VLAN 20はETHER1~5ポートで構成されるポートVLANで、ETHER1~4ポートでタグ付き、ETHER5 ポートでタグなしである
- ETHERBLOCK1(ETHER1~8ポート)のVLAN 20ではMACアドレス00:0b:01:02:03:04のホストからの入 カパケットのCOS値を5に変更する

上記の書き換え要求に従って設定を行う場合の設定例を示します。

(1) VLAN ID が 20 で送信元 MAC アドレスが 00:0b:01:02:03:04 であるパケットの形式を ACL で設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL 情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

→acl0

	<acl情報追加フィールド></acl情報追加フィールド>
定義名	ac IO

- **3. [追加] ボタンをクリックします。** 「ACL 定義情報(acl0)」ページが表示されます。
- **4. 「MAC 定義情報」をクリックします**。 「MAC 定義情報」が表示されます。

•	送信元MACアドレス	→指定する
	アドレス指定	→00:0b:01:02:03:04
•	あて先 MAC アドレス	→すべて

フォーマット種別 →すべて

■MAC定義情報	
送信元MACアドレス	指定する アドレス指定(‴指定する″を選択時のみ有効です) 00:0b:01:02:03:04
あて先MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
フォーマット種別	 ● すべて ● LLC形式 ■ LSAP ● Ethernet形式 ■ type値

- 6. [保存] ボタンをクリックします。
- **7. 「VLAN 定義情報」をクリックします**。 「VLAN 定義情報」が表示されます。

8. 以下の項目を指定します。

- VLAN ID →20
- COS値
 →指定しない

■VLAN定義情報	3
VLAN ID	20
COS値	

- 9. [保存] ボタンをクリックします。
- (2) ETHERBLOCK1 (ETHER1~8ポート)で(1)で設定した形式のパケットのCOS値を 5に書き換える
- **10. 設定メニューの詳細設定で「etherblock 情報」をクリックします。** 「etherblock 情報」ページが表示されます。
- **11.** 「etherblock 情報」で etherblock 番号が1の [修正] ボタンをクリックします。 etherblock 1 情報の設定項目と「フィルタ情報」が表示されます。
- **12.** 「QoS 情報」をクリックします。 「QoS 情報」が表示されます。

٠	● 動作 →cos値書き打	
	書き換え値	→cos値指定 5
•	ACL定義番号	→0

「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

		<mark><qos情報< mark=""></qos情報<></mark>	入力フィールド>
	 ⊙ cos値書き換え 		
		書き換え 値	⊙cos値指定 5 ○ip precedence値
	0	ip preceden	ce値書き換え
動作		書き換え 値	 ⊙ ip precedence値指定 ○ cos値
	0	dscp値書ぎ	換え
		書き換え 値	
	0	出力キュー	
ACL定義番号	0	参照	

14. [追加] ボタンをクリックします。

15. 画面左側の[設定反映]ボタンをクリックします。 設定した内容が有効になります。

ETHERBLOCK単位でパケットの COS 値をパケットの ip precedence 値で書き換える

適用機種 SR-S208TC2, 224TC2, 208PD1, 224PS1, 224CP1, 248TC1

ここでは、ETHERBLOCK内のポートで特定のVLANおよび特定のMACアドレスを持つホストへの送信パケットのCOS値パケットのip precedence値で書き換える方法を説明します。

「ether 情報」-「QoS 関連」で設定した場合、ETHER1~8ポートで同一の優先制御情報書き換えを設定する場合 も、ETHERBLOCK1で使用する acl 数は8個となりますが、「etherblock 情報」でETHER1~8ポートで同一の優 先制御情報書き換えを設定する場合はETHERBLOCK1で使用する acl 数は1個となるため、acl 数による制限の緩 和に有効です。

● 書き換え要求

- VLAN 10は ETHER1 ~8ポートで構成されるポート VLAN で、すべてタグ付きである
- ETHERBLOCK1(ETHER1~8ポート)のVLAN 10ではMACアドレス00:0b:01:02:03:04のホストへの送信 パケットのCOS値をパケットのip precedence値で書き換える

上記の書き換え要求に従って設定を行う場合の設定例を示します。

(1) VLAN ID が 10 であて先 MAC アドレスが 00:0b:01:02:03:04 であるパケットの形式を ACL で設定する

1. 設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2. 以下の項目を指定します。

3.

- ・ 定義名
 →acl0
- **[追加]ボタンをクリックします。** 「ACL 定義情報(acl0)」ページが表示されます。
- **4.** 「MAC定義情報」をクリックします。

「MAC 定義情報」が表示されます。

5. 以下の項目を指定します。

- 送信元 MAC アドレス →すべて
- あて先 MAC アドレス →指定する
 アドレス指定 → 00:0b:01:02:03:04
- フォーマット種別 →すべて

MAC定義情報	3
送信元MACアドレス	すべて ▼ アドレス指定(″指定する″を選択時のみ有効です)
あて先MACアドレス	指定する ▼ アドレス指定(″指定する″を選択時のみ有効です) 00:0b:01:02:03:04
フォーマット種別	 ● すべて ● LLC形式 ■ LSAP ● Ethernet形式 ■ type値

- 6. [保存] ボタンをクリックします。
- **7. 「VLAN 定義情報」をクリックします**。 「VLAN 定義情報」が表示されます。
- 8. 以下の項目を指定します。

• VLAN ID

- COS 値 →指定しない

VLAN定義情報	3
VLAN ID	10
COS値	

→10

9. [保存] ボタンをクリックします。

- (2) ETHERBLOCK1 (ETHER1~8ポート)で(1)で設定した形式のパケットのCOS値を パケットのip precedence値で書き換える
- **10. 設定メニューの詳細設定で「etherblock 情報」をクリックします**。 「etherblock 情報」ページが表示されます。
- **11.** 「etherblock 情報」で etherblock 番号が1の [修正] ボタンをクリックします。 etherblock 1 情報の設定項目と「フィルタ情報」が表示されます。
- **12.** 「QoS情報」をクリックします。

「QoS情報」が表示されます。

13. 以下の項目を指定します。

動作 → cos 値書き換え
 書き換え値 → ip precedence 値
 ACL 定義番号 → 0

▲ 「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<qos情報入力フィールド></qos情報入力フィールド>			
	 ⊙ cos値書き換え 		
	書き換え 値 ・ ip precedence値		
	○ ip precedence値書き換え		
動作	書き換え 値 ・ cos値		
	dscp値書き換え		
	書き換え 値		
	○ 出力キュー指定		
ACL定義番号	0 参照		

- 14. [追加] ボタンをクリックします。
- **15. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

ETHERBLOCK 単位でパケットの DSCP 値を指定した値で書き換える

適用機種 SR-S208TC2, 224TC2, 208PD1, 224PS1, 224CP1, 248TC1

ここでは、ETHERBLOCK内のポートですべての入力パケットのDSCP 値を指定した値で書き換える方法を説明 します。

「ether 情報」-「QoS 関連」で設定した場合、ETHER1~8ポートで同一の優先制御情報書き換えを設定する場合 も、ETHERBLOCK1で使用する acl 数は8個となりますが、「etherblock 情報」でETHER1~8ポートで同一の優 先制御情報書き換えを設定する場合はETHERBLOCK1で使用する acl 数は1個となるため、acl 数による制限の緩 和に有効です。

● 書き換え要求

- VLAN 10は ETHER1 ~8ポートで構成されるポート VLAN で、すべてタグ付きである
- ETHERBLOCK1(ETHER1~8ポート)では全入カパケットのDSCP値を40に書き換える

上記の書き換え要求に従って設定を行う場合の設定例を示します。

(1) すべてのパケットの形式をACLで設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL 情報」ページが表示されます。

2. 以下の項目を指定します。

• 定義名 → acl0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	ac IO	

3. [追加] ボタンをクリックします。

「ACL 定義情報(acl0)」ページが表示されます。

4. 「MAC定義情報」をクリックします。

「MAC定義情報」が表示されます。

- ・ 送信元 MAC アドレス →すべて
- あて先 MAC アドレス →すべて
- フォーマット種別 →すべて

MAC定義情報	3
送信元MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
あて先MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
フォーマット種別	 ● すべて ● LLC形式 ■ LSAP ● Ethernet形式 ■ type値

- 6. [保存] ボタンをクリックします。
- (2) ETHERBLOCK1 (ETHER1~8ポート)で(1)で設定した形式のパケットのDSCP値を 40に書き換える
- 設定メニューの詳細設定で「etherblock 情報」をクリックします。
 「etherblock 情報」ページが表示されます。
- 8. 「etherblock 情報」で etherblock 番号が1の [修正] ボタンをクリックします。 etherblock 1 情報の設定項目と「フィルタ情報」が表示されます。
- 「QoS 情報」をクリックします。
 「QoS 情報」が表示されます。

٠	動作	→dscp 値書き換え
	書き換え値	→ 40
•	ACL定義番号	→ 0

「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<qos情報入力フィールド></qos情報入力フィールド>			
○ cos値書き換え			
		書き換え 値	⊙cos値指定 ○ip precedence値
	○ ip precedence値書き換え		ce値書き換え
動作		書き換え 値	⊙ip precedence値指定 ○cos値
	● dscp値書 書き換え 値	dscp値書き換え	
		書き換え 値	40
	0	出力キュー	
ACL定義番号	0	参照	

- 11. [追加] ボタンをクリックします。
- **12. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

ETHERBLOCK 単位でパケットの ip precedence 値を指定した値で書き換える

適用機種 SR-S208TC2, 224TC2, 208PD1, 224PS1, 224CP1, 248TC1

ここでは、ETHERBLOCK内のポートで特定のVLANおよび特定のCOS値の入力パケットのip precedence値を指定した値に書き換える方法を説明します。

「ether 情報」-「QoS 関連」で設定した場合、ETHER1~8ポートで同一の優先制御情報書き換えを設定する場合 も、ETHERBLOCK1で使用する acl 数は8個となりますが、「etherblock 情報」でETHER1~8ポートで同一の優 先制御情報書き換えを設定する場合はETHERBLOCK1で使用する acl 数は1個となるため、acl 数による制限の緩 和に有効です。

● 書き換え要求

- VLAN 10は ETHER1~8ポートで構成されるポート VLANで、すべてタグ付きである
- VLAN 10 では COS 値5のパケットが入力された場合に、入力パケットの ip precedence 値を6 に書き換える

上記の書き換え要求に従って設定を行う場合の設定例を示します。

(1) VLAN IDが10でCOS値が5のパケットの形式をACLで設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL 情報」ページが表示されます。

2. 以下の項目を指定します。

- 定義名 → acl0
 <ACL情報追加フィールド>
 定義名 acl0
- **3. [追加] ボタンをクリックします**。 「ACL 定義情報(acl0)」ページが表示されます。
- **fvlan定義情報」をクリックします**。
 「vlan定義情報」が表示されます。
- 5. 以下の項目を指定します。
 - VLAN ID → 10
 - COS値 →5

■VLAN定義情報	3
VLAN ID	10
COS値	5

- 6. [保存] ボタンをクリックします。
- (2) VLAN10 に属する ETHERBLOCK1 (ETHER1~8ポート)で(1)で設定した形式のパ ケットの ip precedence 値を6 に書き換える
- 7. 設定メニューの詳細設定で「etherblock 情報」をクリックします。

「etherblock 情報」ページが表示されます。

- **8.** 「etherblock 情報」で etherblock 番号が1の [修正] ボタンをクリックします。 etherblock 1 情報の設定項目と「フィルタ情報」が表示されます。
- 9. 「QoS情報」をクリックします。

「QoS 情報」が表示されます。

 動作 → ip precedence 値書き換え 書き換え値 → ip precedence 値指定 6
 ACL定義番号 → 0

▲ 「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の [選択] ボタンをクリックして設定します。

<qos情報入力フィールド></qos情報入力フィールド>			
○ cos値書き換え			
	書 き換え 値	●cos值指定 ○ip precedence値	
	⊙ ip preceder	nce値書き換え	
動作	書き換え 値	●ip precedence値指定 6 ○cos値	
	◯ dscp値書き	dscp値書き換え	
	書き換え 値		
	○ 出力キュー	指定	
ACL定義番号	0 参照		

- 11. [追加] ボタンをクリックします。
- **12. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

ETHERBLOCK 単位でパケットの ip precedence 値をパケットの COS 値で書き換える

適用機種 SR-S208TC2, 224TC2, 208PD1, 224PS1, 224CP1, 248TC1

ここでは、ETHERBLOCK内のポートで特定のVLANからの入力パケットのip precedence 値をパケットのCOS 値で書き換える方法を説明します。

「ether 情報」-「QoS 関連」で設定した場合、ETHER1~8ポートで同一の優先制御情報書き換えを設定する場合 も、ETHERBLOCK1で使用する acl 数は8個となりますが、「etherblock 情報」でETHER1~8ポートで同一の優 先制御情報書き換えを設定する場合はETHERBLOCK1で使用する acl 数は1個となるため、acl 数による制限の緩 和に有効です。

● 書き換え要求

- ETHER1~8ポートはVLAN10、VLAN20、VLAN30にタグ付き、VLAN100にタグなしで属する
- ETHER1~6ポートからのVLAN 20、VLAN30、VLAN100からの入力パケットのip precedence 値をパケットのCOS 値に書き換える

上記の書き換え要求に従って設定を行う場合の設定例を示します。

(1) VLAN IDが20、30、100のパケットの形式をそれぞれACLで設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL 情報」ページが表示されます。

2. 以下の項目を指定します。

定義名 → acl0
 <ACL情報追加フィールド>
 定義名 acl0

3. [追加] ボタンをクリックします。 「ACL 定義情報(acl0)」ページが表示されます。

fvlan定義情報」をクリックします。 「vlan定義情報」が表示されます。

5. 以下の項目を指定します。

- VLAN ID → 20
- COS値
 →指定しない

■VLAN定義情報	2
VLAN ID	20
COS値	

- 6. [保存] ボタンをクリックします。
- 7. 手順1.~6.を参考に、以下の項目を設定します。

「ACL情報」

定義名

- →acl1
- 「ACL定義情報 (acl1)」-「VLAN 定義情報」
- VLAN ID → 30
- COS値 →指定しない

「ACL情報」

• 定義名 →acl2

「ACL定義情報 (acl2)」-「VLAN 定義情報」

- VLAN ID → 100
- COS値
 →指定しない

(2) ETHERBLOCK1 (ETHER1~8ポート)で(1)で作成した形式のパケットのip precedence 値をパケットのCOS 値に書き換える

8. 設定メニューの詳細設定で「etherblock 情報」をクリックします。

「etherblock 情報」ページが表示されます。

- **9.** 「etherblock 情報」で etherblock 番号が1の [修正] ボタンをクリックします。 etherblock 1 情報の設定項目と「フィルタ情報」が表示されます。
- **10.** 「QoS情報」をクリックします。

「QoS 情報」が表示されます。

11. 以下の項目を指定します。

- 動作 → ip precedence 値書き換え
- 書き換え値 → cos 値
- ACL定義番号 →0

ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の「選択」 ボタンをクリックして設定します。

<qos情報入力フィールド></qos情報入力フィールド>			
 ○ cos値書き換え 			
	書 き換え 値	⊙cos値指定 ○ip precedence値	
	⊙ ip preceden	ip precedence値書き換え	
動作	書 き換え 値	 ○ ip precedence値指定 ◎ cos値 	
	◯ dscp値書き		
	書 き換え 値		
	○ 出力キュー	指定	
ACL定義番号	0 参照		

- 12. [追加] ボタンをクリックします。
- 13. 手順 11.~12.を参考に、以下の項目を設定します。
 - 動作 → ip precedence 値書き換え 書き換え値 → cos 値
 ACL 定義番号 → 1
- 14. 手順 11.~ 12.を参考に、以下の項目を設定します。
 - 動作 → ip precedence 値書き換え 書き換え値 → cos 値
 ACL定義番号 →2
- **15. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

VLAN 単位でパケットの出力キューを変更する

適用機種 全機種

ここでは、VLAN内のポートで特定のMACアドレスを持つホストからの入力パケットが出力ポートから出力される際に使用されるキューを変更する方法を説明します。

● 書き換え要求

- VLAN20はETHER1~5ポートで構成されるポートVLANで、ETHER1~4ポートでタグ付き、ETHER5ポートでタグなしである
- VLAN20ではMACアドレス00:0b:01:02:03:04のホストからの入力パケットが出力される際に使用される出 カポートのキューを3に変更する

上記の書き換え要求に従って設定を行う場合の設定例を示します。

(1) 送信元 MAC アドレスが 00:0b:01:02:03:04 であるパケットの形式を ACL で設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL 情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

→acl0

<acl情報追加フィールド></acl情報追加フィールド>			
定義名	ac ID		

3. [追加] ボタンをクリックします。

「ACL 定義情報(acl0)」ページが表示されます。

4. 「MAC定義情報」をクリックします。

「MAC定義情報」が表示されます。

5. 以下の項目を指定します。

● 送信元 MAC アドレス	→指定する
アドレス指定	→00:0b:01:02:03:04
● あて先 MAC アドレス	→すべて

フォーマット種別 →すべて

- 6. [保存] ボタンをクリックします。
- (2) VLAN20 で(1) で設定した形式のパケットが出力ポートから出力される際に使用される キューを3 に変更する
- 7. 設定メニューの詳細設定で「VLAN情報」をクリックします。

「VLAN情報」ページが表示されます。

- 8. 以下の項目を指定します。
 - VLAN ID →20

	<vlan情報追加フィールド></vlan情報追加フィールド>	
VLAN ID	20	

9. [追加] ボタンをクリックします。

「VLAN20情報」ページが表示されます。

10. 「QoS情報」をクリックします。

「QoS情報」が表示されます。

- 11. 以下の項目を指定します。
 - 動作 →出力キュー指定 3
 - ACL定義番号 →0

<qos情報入力フィールド></qos情報入力フィールド>				
	○ cos値書き換え			
		書き換え 値	⊙cos値指定 ○ip precedence値	
○ ip precedence値書き換え				
動作		書き換え 値	⊙ip precedence值指定 ○cos值	
	0	dscp値書き換え		
		書き換え 値		
	<u>ا</u> ا	出力キュー打	管定 3	
ACL定義番号	0	参照		

- 12. [追加] ボタンをクリックします。
- **13. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

[「]ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

7 STP 機能を使う

適用機種 全機種

ここでは、STP 機能を使用する場合の設定方法を説明します。

7.1 STP を使う

適用機種 全機種

STPを使用すると、物理的にループしているネットワークでも、論理的にループしないようにすることができます。これによって、ネットワーク内のデータを円滑に流すことができます。

● 参照 機能説明書「2.9.1 STP」(P.39)

SR-S316C2/716C2の場合を例にします。



● 設定条件

- STP を使用する
- ETHER1、2ポートをVID 10のポートVLANとする

上記の設定条件に従って設定を行う場合の設定例を示します。

メディア種別および VLAN を設定する

- **1. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - ポートリスト

ボート リスト [1-2	修正	初期化

→ 1-2

【修正】ボタンをクリックします。
 ether 1-2 情報の設定項目と「基本情報」が表示されます。

• メディア種別

Untagged

→通常ポート (RJ45)

• VLAN

→ 10

■基本	情報	3	
ボート	使用	●使用する●使用しない	
<mark>説明文</mark>	τ		
メディブ	P種別	○自動 ③ 通常ボート(RJ45) ○ SFPボート	
通信速度		●自動 ○10Mbps ○100Mbps ○1000Mbps	
全二重/半二重		◎全二重 ○半二重	
MDI		●自動 ○ MDI ○ MDI-X	
フロ	送信	⊙しない○する	
 御 受信 ●する ○しない 			
	Tagged		
V L J U V	<mark>Untagged</mark>	10	

機種によりメディア種別に対応しているポート番号は異なります。

5. [保存] ボタンをクリックします。

STP を設定する

6. 「STP 関連」をクリックします。

STP関連の設定項目と「基本情報」が表示されます。

- 7. 以下の項目を指定します。
 - STP機能 →使用する

■基本情報	ł		3
	 ○ 使用しない ● 使用する 		
OTD HE AL	STP動作バージョン	指定なし 🔽	
る「尸物或用店	バスコスト	 ●自動決定 ●指定する 	
	インタフェース優先度	128 🛩	

- 8. [保存] ボタンをクリックします。
- 9. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

7.2 MSTPを使う

適用機種 全機種

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。

● 参照 機能説明書「2.9.3 MSTP」(P.50)

SR-S316C2/716C2の場合を例にします。

- 設定条件
- 以下のような VLAN 環境下で MSTPを併用した VLAN 単位でフレームの制御を行う
- 本装置1-本装置2間は1Gとする
- 本装置1-本装置3間は100Mとし、トラフィック量が多いものは本装置1-2間に流す
- 装置間の回線はクロスケーブルを使用する



[インスタンス 0]

• ブリッジの優先順位 :本装置1→本装置2→本装置3→本装置4

[インスタンス1]

- :本装置1→本装置2→本装置3→本装置4
- VLAN割り当て : 100、200

[インスタンス2]

• ブリッジの優先順位

• ブリッジの優先順位

- :本装置1→本装置3→本装置2→本装置4
- VLAN割り当て

[本装置1]

- ETHER1ポートで本装置2と接続し、回線速度は1Gとする
- ETHER2ポートで本装置3と接続し、回線速度は100Mとする
- ETHER1、2ポートのSTPパスコストは、全インスタンス20000とする

: 300

[本装置2]

- ETHER1ポートで本装置1と接続し、回線速度は1Gとする
- ETHER2ポートで本装置3と接続し、回線速度は100Mとする
- ETHER3ポートで本装置4と接続し、回線速度は1Gとする
- ETHER1~3ポートのSTPパスコストは、全インスタンス20000とする

[本装置3]

- ETHER1ポートで本装置1と接続し、回線速度は100Mとする
- ETHER2ポートで本装置2と接続し、回線速度は100Mとする
- ETHER3ポートで本装置4と接続し、回線速度は100Mとする
- ETHER1~3ポートのSTPパスコストは、全インスタンス20000とする

[本装置4]

- ETHER1ポートで本装置2と接続し、回線速度は1Gとする
- ETHER2ポートで本装置3と接続し、回線速度は100Mとする
- ETHER1、2ポートのSTPパスコストは、全インスタンス20000とする
- ETHER3~9ポートでVID100の端末と接続し、回線速度は100Mとする
- ETHER10~14ポートでVID200の端末と接続し、回線速度は100Mとする
- ETHER15、16ポートでVID300の端末と接続し、回線速度は100Mとする

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

メディア種別、MDIおよび VLANを設定する

- 設定メニューの詳細設定で「ether 情報」をクリックします。
 「ether 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - ポートリスト → 1-2



3. 【修正】ボタンをクリックします。 ether 1-2 情報の設定項目と「基本情報」が表示されます。

- メディア種別 →通常ポート(RJ45)
- MDI → MDI-X
- VLAN Tagged

→ 100,200,300

■基本	5情報	3	
ボート	使用	●使用する●使用しない	
<mark>説明文</mark>	τ		
メディ	ア種別	○自動 ●通常ボート(RJ45) ● SFPボート	
通信速度		●自動 ○10Mbps ○100Mbps ○1000Mbps	
全二重/半二重		◎全二重○半二重	
MDI		○自動 ○ MDI ⊙ MDI-X	
フロー当日	送信	⊙しない ○する	
御 受信 ●する ○しない			
	Tagged	100,200,300	
VLAN	Untagged		

機種によりメディア種別に対応しているポート番号は異なります。

5. [保存] ボタンをクリックします。

ETHER1、2ポートを設定する

- 6. 設定メニューの詳細設定で「ether 情報」をクリックします。 「ether 情報」ページが表示されます。
- **7.** 「ether 情報」でポート番号が1の [修正] ボタンをクリックします。 ether 1 情報の設定項目と「基本情報」が表示されます。
- 8. 以下の項目を指定します。
 - 通信速度 → 1000Mbps

■基本情報		3
ポート使用	⊙使用する○使用しない	
メディア種別	○自動 ●通常ボート(RJ45) ● SFPボート	
通信速度	〇自動 ◯ 10Mbps ◯ 100Mbps ⊙ 1000Mbps	

- 9. [保存] ボタンをクリックします。
- **10.** 手順6.~9.を参考に、ETHER2ポートを設定します。
 - 通信速度 → 100Mbps

ETHER1、2ポートのSTPパスコストを設定する

11. 設定メニューの詳細設定で「ether 情報」をクリックします。 「ether 情報」ページが表示されます。

• ポートリスト	→ 1-2
ポート リスト 1-2	修正 初期化

13. [修正] ボタンをクリックします。

ether 1-2 情報の設定項目と「基本情報」が表示されます。

14. 「STP 関連」をクリックします。

STP関連の設定項目と「基本情報」が表示されます。

15. 以下の項目を指定します。

•	STP機能	→使用する
	パスコスト	→指定する
		→20000

■基本情報	Ř	3
	 ○ 使用しばい ③ 使用する 	
OT D HE AL	STP動作バージョン 指定なし 💌	
STPHOGHE	バスコスト ○自動決定 ○指定する ²⁰⁰⁰⁰	
	インタフェース優先度 128 💌	

- 16. [保存] ボタンをクリックします。
- **17.** 「MSTP インスタンス情報」をクリックします。 「MSTP インスタンス情報」が表示されます。
- 18. 「MSTPインスタンス情報」でインスタンスIDが1の[修正]ボタンをクリックします。

インスタンス ID 1の「MSTPインスタンス情報入力フィールド」が表示されます。

- 19. 以下の項目を指定します。
 - パスコスト

→指定する →20000

	<mstpインスタンス情報入力フィールド></mstpインスタンス情報入力フィールド>	
1	バスコスト	 ○自動決定 ○指定する20000
	インタフェース優先度	128 🗸

- 20. [保存] ボタンをクリックします。
- 21. 手順 18.~20.を参考に、インスタンス ID 2を設定します。
 - パスコスト →指定する →20000

STP を設定する

22. 設定メニューの詳細設定で「STP情報」をクリックします。 STP情報の設定項目と「基本情報」が表示されます。

STP 機能

→使用する

"使用する"を選択すると、「ブリッジの優先度」および「STP動作モード」の設定項目が表示されます。

- ブリッジの優先度 →4096
- STP動作モード → MSTP

■基本情報	3	
STP機能	○使用しない ⊙使用する	
ブリッジのハロ ー待ち時間	20 秋少	
フォワーディング 遅延時間	15 秒	
ブリッジのハロ ー送出間隔	2_秒	
ブリッジの優先 度	4096 🗸	
STP動作モード	 STP RSTP MSTP 最大ホッブカウント 20 銀大ホッブカウント 20 加ST構成 20 ロージョン region1 空素 リビジョン 0 	

24. [保存] ボタンをクリックします。

25. 「MSTPインスタンス情報」をクリックします。

「MSTPインスタンス情報」が表示されます。

- **26.** 「MSTP インスタンス情報」でインスタンス ID が 1 の [修正] ボタンをクリックします。 インスタンス ID 1 の「MSTP インスタンス情報入力フィールド」が表示されます。
- 27. 以下の項目を指定します。
 - ブリッジの優先度 →4096
 - MSTPインスタンスへのVLAN割り当て(VLAN ID) → 100,200

	<mstpインスタンス情報入力フィールド></mstpインスタンス情報入力フィールド>		
	ブリッジの優先度	4096 🗸	
1	MSTPインスタンスへ のVLAN割り当て		
		100,200	
	(VLAN ID)		

- 28. [保存] ボタンをクリックします。
- 29. 手順26.~28.を参考に、インスタンスID2を設定します。
 - ブリッジの優先度 → 4096
 - MSTPインスタンスへのVLAN割り当て(VLAN ID)

→300

30. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

本装置2を設定する

1.

2.

3.

4.

5.

メディア種別、MDIおよび VLANを設定する 設定メニューの詳細設定で「ether情報」をクリックします。 「ether 情報」ページが表示されます。 以下の項目を指定します。 • ポートリスト → 1-3 ポート リスト 1-3 修正初期化 [修正] ボタンをクリックします。 ether 1-3 情報の設定項目と「基本情報」が表示されます。 以下の項目を指定します。 メディア種別 →通常ポート(RJ45) • MDI → MDI-X VLAN Tagged → 100,200,300 ■基本情報 ボート使用 ⊙使用する○使用しない 説明文 メティア種別 ○自動 ③ 通常ボート(RJ45) ○ SFPボート 通信速度 ●自動 ○10Mbps ○100Mbps ○1000Mbps 全二重/半二重 ◎全二重 ◎半二重 MDI ○自動 ○ MDI ⊙ MDI-X 70 送信 ⊙しない ○する -制 受信 ⊙する ○しない 御 100,200,300 Tagged VLAN Untagged 機種によりメディア種別に対応しているポート番号は異なります。 [保存] ボタンをクリックします。

3

ETHER1~3ポートを設定する

設定メニューの詳細設定で「ether情報」をクリックします。 6.

「ether 情報」ページが表示されます。

- 以下の項目を指定します。 7.
 - ポートリスト



→1,3

[修正] ボタンをクリックします。 8.

ether 1,3 情報の設定項目と「基本情報」が表示されます。

通信速度

→ 1000Mbps

■基本情報	2	J
ポート使用 ●使用する ○使用しない		
説明文		
メディア種別 ○自動 ●通常ボート(RJ45) ○ SFPボート		
通信速度	○自動 ○ 10Mbps ○ 100Mbps ③ 1000Mbps	

機種によりメディア種別に対応しているポート番号は異なります。

- 10. [保存] ボタンをクリックします。
- 11. 画面上部の「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

- **12.** 「ether 情報」でポート番号が2の [修正] ボタンをクリックします。 ether 2 情報の設定項目と「基本情報」が表示されます。
- 13. 手順9.~10.を参考に、以下の項目を設定します。
 - 通信速度 → 100Mbps

ETHER1~3ポートのSTPパスコストを設定する

- **14. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- 15. 以下の項目を指定します。
 - ポートリスト

ポート リスト 1-3 (修正) (初期化)

→ 1-3

16. [修正]ボタンをクリックします。

ether 1-3 情報の設定項目と「基本情報」が表示されます。

17. 「STP 関連」をクリックします。

STP関連の設定項目と「基本情報」が表示されます。

18. 以下の項目を指定します。

•	STP機能	→使用する
	パスコスト	→指定する
		→20000

基本情報		3
STP機能	 ● 使用しない ● 使用する STP動作バージョン 指定なし ● パスコスト ○ 自動決定 ○ 指定する 20000 	
	インタフェース優先度 128 🖌	

19. [保存] ボタンをクリックします。

20. 「MSTPインスタンス情報」をクリックします。

「MSTPインスタンス情報」が表示されます。

21. 「MSTPインスタンス情報」でインスタンスIDが1の[修正]ボタンをクリックします。

インスタンスID1の「MSTPインスタンス情報入力フィールド」が表示されます。

- 22. 以下の項目を指定します。
 - パスコスト

→指定する →20000

<mstpインスタンス情報入力フィールド></mstpインスタンス情報入力フィールド>		情報入力フィールド>
1	バスコスト	 ○自動決定 ○指定する20000
	インタフェース優先度	128 🗸

- 23. [保存] ボタンをクリックします。
- 24. 手順21.~23.を参考に、インスタンスID2を設定します。
 - パスコスト →指定する →20000

STP を設定する

25. 設定メニューの詳細設定で「STP 情報」をクリックします。

STP情報の設定項目と「基本情報」が表示されます。

- 26. 以下の項目を指定します。
 - STP機能 →使用する

"使用する"を選択すると、「ブリッジの優先度」および「STP動作モード」の設定項目が表示されます。

- ブリッジの優先度 →8192
- STP動作モード → MSTP

■基本情報	基本情報	
STP機能	○使用しない ⊙使用する	
ブリッジのハロ 一待ち時間	20承少	
フォワーティング 遅延時間	15 和少	
ブリッジのハロ ー送出間隔	2 秒	
ブリッジの優先 度	8192 🗸	
STP動作モート	 STP RSTP MSTP 最大ホップカウント 20 MST構成 名 region1 要素 リビジョン レベル 0 	

27. [保存] ボタンをクリックします。

28. 「MSTPインスタンス情報」をクリックします。

「MSTPインスタンス情報」が表示されます。

29. 「MSTPインスタンス情報」でインスタンスIDが1の[修正]ボタンをクリックします。

インスタンス ID 1の「MSTP インスタンス情報入力フィールド」が表示されます。

30. 以下の項目を指定します。

- ブリッジの優先度 →8192
- MSTPインスタンスへのVLAN割り当て(VLAN ID)

→ 100,200

	<mstpインスタンス情報入力フィールド></mstpインスタンス情報入力フィールド>	
	ブリッジの優先度	8192 🗸
1	MSTPインスタンスへ	
	のVLAN語の当て (VLAN ID)	100,200

- 31. [保存] ボタンをクリックします。
- 32. 手順29.~31.を参考に、インスタンスID2を設定します。
 - ブリッジの優先度 →12288
 - MSTPインスタンスへのVLAN割り当て(VLAN ID) →300
- **33. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置3を設定する

メディア種別、MDIおよび VLAN を設定する

- **1. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - ポートリスト

ポート リスト 1-3 修正 初期化

→ 1-3

3. [修正] ボタンをクリックします。

ether 1-3 情報の設定項目と「基本情報」が表示されます。

- ・ メディア種別 →通常ポート(RJ45)
- 通信速度 → 100Mbps
- MDI → MDI-X
- VLAN

Tagged

→ 100,200,300

■基本	■基本情報	
ボート	使用	●使用する●使用しない
説明文	ξ	
メディン	P種別	○自動 ● 通常ボート(RJ45) ● SFPボート
通信进	度	〇自動 ◯ 10Mbps ⊙ 100Mbps ◯ 1000Mbps
全二重/半二重 ◎全二重 ○半二重		◎全二重 ○半二重
MDI ○自動 ○ MDI ⊙ MDI-X		○自動 ○ MDI ⊙ MDI-X
7日 送信 ●しない ○する		⊙しない○する
御 受信 ●する ○したい		⊙する ○しだい
VLAN Tagged 100,200,300 Untagged		100,200,300

機種によりメディア種別に対応しているポート番号は異なります。

5. [保存] ボタンをクリックします。

ETHER1~3ポートのSTPパスコストを設定する

- **6. 設定メニューの詳細設定で「ether情報」をクリックします**。 「ether情報」ページが表示されます。
- 7. 以下の項目を指定します。
 - ポートリスト

→1-3

修正	初期化

8. [修正] ボタンをクリックします。

ether 1-3 情報の設定項目と「基本情報」が表示されます。

9. 「STP 関連」をクリックします。

STP関連の設定項目と「基本情報」が表示されます。

10. 以下の項目を指定します。

•	STP機能	→使用する
	パスコスト	→指定する
		→20000

基本情報		3
	 ○ 使用しない ● 使用する 	
OT D HE AL	STP動作バージョン 指定なし 💌	
る「尸骸尾	バスコスト ○自動決定 ●指定する20000	
	インタフェース優先度 128 💌	

- 11. [保存] ボタンをクリックします。
- **12.** 「MSTP インスタンス情報」をクリックします。 「MSTP インスタンス情報」が表示されます。
- **13.** 「MSTPインスタンス情報」でインスタンスIDが1の[修正]ボタンをクリックします。

インスタンスID1の「MSTPインスタンス情報入力フィールド」が表示されます。

- 14. 以下の項目を指定します。
 - パスコスト

→指定する →20000

	<mstpインスタンス情報入力フィールド></mstpインスタンス情報入力フィールド>	
1	バスコスト	 ●自動決定 ●指定する20000
	インタフェース優先度	128 🗸

- 15. [保存] ボタンをクリックします。
- 16. 手順13.~15.を参考に、インスタンスID2を設定します。
 - パスコスト →指定する →20000

STP を設定する

- **17. 設定メニューの詳細設定で「STP情報」をクリックします**。 STP情報の設定項目と「基本情報」が表示されます。
- 18. 以下の項目を指定します。
 - STP機能 →使用する

"使用する"を選択すると、「ブリッジの優先度」および「STP動作モード」の設定項目が表示されます。

- ブリッジの優先度 →12288
- STP動作モード → MSTP

■基本情報	基本情報	
STP機能	○使用しない ⊙使用する	
ブリッジのハロ 一待ち時間	20 利少	
フォワーディング 遅延時間	15 和少	
ブリッジのハロ ー送出間隔	2 秒	
ブリッジの優先 度	12288 💌	
STP動作モート	 STP RSTP MSTP 	

19. [保存] ボタンをクリックします。

20. 「MSTPインスタンス情報」をクリックします。

「MSTPインスタンス情報」が表示されます。

21. 「MSTPインスタンス情報」でインスタンスIDが1の[修正]ボタンをクリックします。

インスタンスID1の「MSTPインスタンス情報入力フィールド」が表示されます。

22. 以下の項目を指定します。

- ブリッジの優先度 →12288
- MSTPインスタンスへのVLAN割り当て(VLAN ID)

→100,200

	<mstpインスタンス情報入力フィールド></mstpインスタンス情報入力フィールド>	
	ブリッジの優先度	12288 🗸
1	MSTPインスタンスへ	
		100,200
	(VEAN ID)	

- 23. [保存] ボタンをクリックします。
- 24. 手順21.~23.を参考に、インスタンスID2を設定します。
 - ブリッジの優先度 →8192
 - MSTPインスタンスへのVLAN割り当て(VLAN ID) →300
- **25. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置4を設定する

メディア種別、MDIおよび VLAN を設定する

- **1. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - ポートリスト → 1-16
 ポート
 リスト
 1-16
 修正 初期化
- 3. [修正] ボタンをクリックします。

ether 1-16情報の設定項目と「基本情報」が表示されます。

- メディア種別 →通常ポート(RJ45)
- MDI → MDI-X

■基本情報		
ボート使用	●使用する●使用しない	
説明文		
メディア種別	○自動 ●通常ボート(RJ45) ● SFPボート	
通信速度		
全二重/半二重	●全二重○半二重	
MDI	○自動 ○ MDI ⊙ MDI-X	

機種によりメディア種別に対応しているポート番号は異なります。

5. [保存] ボタンをクリックします。

ETHER1~16ポートを設定する

- **6. 設定メニューの詳細設定で「ether情報」をクリックします**。 「ether情報」ページが表示されます。
- **7. 「**ether **情報」でポート番号が1の [修正] ボタンをクリックします**。 ether 1 情報の設定項目と「基本情報」が表示されます。

8. 以下の項目を指定します。

● 通信速度

→ 1000Mbps

■基本情報		
ポート使用	●使用する●使用しない	
<mark>説明文</mark>		
メディア種別	ディア種別 ○自動 ③通常ボート(RJ45) ○ SFPボート	
通信速度	〇自動 ◯10Mbps ◯100Mbps ⊙1000Mbps	

機種によりメディア種別に対応しているポート番号は異なります。

9. [保存] ボタンをクリックします。

10. 画面上部の「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

- 11. 以下の項目を指定します。
 - ポートリスト

```
→2-16
```

```
ポート
リスト
2-16
(修正) 初期化
```

12. [修正] ボタンをクリックします。

ether 2-16 情報の設定項目と「基本情報」が表示されます。

- 13. 手順8.~9.を参考に、以下の項目を設定します。
 - 通信速度 →100Mbps

VLAN を設定する

14. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether 情報」ページが表示されます。

- 15. 「ether情報」でポート番号が1の[修正]ボタンをクリックします。 ether 1 情報の設定項目と「基本情報」が表示されます。
- 以下の項目を指定します。 16.
 - VLAN

Tagged

→ 100,200,300

→ 100,200,300

	Tagged	100,200,300
VLAN	Untagged	

- 17. [保存] ボタンをクリックします。
- 18. 手順14.~17.を参考に、ETHER2ポートを設定します。 「ether 2 情報」-「基本情報」
 - VLAN tagged
- 19. 画面上部の「ether情報」をクリックします。 「ether 情報」ページが表示されます。
- 20. 以下の項目を指定します。
 - ポートリスト

++:			
$\gamma \gamma = \Gamma$	3-9	修正	初期化
リスト	<u> </u>		
22.00			

[修正] ボタンをクリックします。 21. ether 3-9情報の設定項目と「基本情報」が表示されます。

22.

以下の項目を指定します。 • VLAN

ボー

Untagged

→ 100

→ 3-9

VI AN	Tagged	
V L Hart	Untagged	100

- 23. [保存] ボタンをクリックします。
- 24. 手順19.~23.を参考に、ETHER10~14ポートを設定します。 「ether 10-14 情報」-「基本情報」
 - VLAN Untagged

→200

- 25. 手順19.~23.を参考に、ETHER15、16ポートを設定します。 「ether 15-16 情報」-「基本情報」
 - VLAN →300 Untagged

ETHER1、2ポートのSTPパスコストを設定する

26. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether 情報」ページが表示されます。

- 27. 以下の項目を指定します。
 - ポートリスト → 1-2



- 28. [修正] ボタンをクリックします。 ether 1-2 情報の設定項目と「基本情報」が表示されます。
- 29. 「STP関連」をクリックします。

STP関連の設定項目と「基本情報」が表示されます。

- 以下の項目を指定します。 30.
 - STP 機能 →使用する パスコスト →指定する →20000

■基本情報	l	3
	 ○ 使用しない ● 使用する 	
പെങ്കുക	STP動作バージョン 指定なし	· 🛩
STPHNGHE	バスコスト ○自動 ⊙指定	決定 する <mark>20000</mark>
	インタフェース優先度 128 🗸	

- 31. [保存] ボタンをクリックします。
- 「MSTP インスタンス情報」をクリックします。 32. 「MSTPインスタンス情報」が表示されます。
- 33. 「MSTPインスタンス情報」でインスタンスIDが1の[修正] ボタンをクリックします。

インスタンス ID 1の「MSTP インスタンス情報入力フィールド」が表示されます。

- 34. 以下の項目を指定します。
 - パスコスト

→指定する →20000

	<mstpインスタンス情報入力フィールド></mstpインスタンス情報入力フィールド>	
1	バスコスト	 ●自動決定 ●指定する20000
	インタフェース優先度	128 🗸

- 35. [保存] ボタンをクリックします。
- 手順33.~35.を参考に、インスタンスID2を設定します。 36.
 - パスコスト →指定する

STP を設定する

37. 設定メニューの詳細設定で「STP 情報」をクリックします。

STP情報の設定項目と「基本情報」が表示されます。

38. 以下の項目を指定します。

STP機能 →使用する

"使用する"を選択すると、「ブリッジの優先度」および「STP動作モード」の設定項目が表示されます。

- ブリッジの優先度 → 32768
- STP動作モード → MSTP

■基本情報	■基本情報 []		
STP機能	○使用しない ⊙使用する		
ブリッジのハロ 一待ち時間	20 承少		
フォワーディング 遅延時間	15 承少		
ブリッジのハロ ー送出間隔	2 秒		
ブリッジの優先 度	32768 🗸		
STP動作モート	 ○ STP ○ RSTP ○ MSTP 显大ホッブカウント 20 最大ホッブカウント 20 風大ホッブカウント 20 レージョン region1 リージョン 10 		

- 39. [保存] ボタンをクリックします。
- 40. 「MSTP インスタンス情報」をクリックします。

「MSTPインスタンス情報」が表示されます。

41. 「MSTPインスタンス情報」でインスタンスIDが1の[修正]ボタンをクリックします。

インスタンス ID 1の「MSTP インスタンス情報入力フィールド」が表示されます。

- 42. 以下の項目を指定します。
 - ブリッジの優先度 → 32768
 - MSTPインスタンスへのVLAN割り当て(VLAN ID)

→ 100,200

	<mstpインスタンス情報入力フィールド></mstpインスタンス情報入力フィールド>	
	ブリッジの優先度	32768 🗸
1	MSTPインスタンスへ のVLAN書り当て (VLAN ID)	100.200

43. 【保存】ボタンをクリックします。

- 44. 手順41.~43.を参考に、インスタンスID2を設定します。
 - ブリッジの優先度 → 32768
 - MSTPインスタンスへのVLAN割り当て(VLAN ID)

→300

45. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

8 DHCPスヌープ機能を使う

適用機種 全機種

DHCPスヌープ機能を使用すると、DHCPでIPアドレスが割り当てられた端末だけ通信を許可することができ、 管理外の不正端末によるネットワークへの不正アクセスを防止することができます。

● 参照 機能説明書「2.13 DHCPスヌープ機能」(P.74)

- こんな事に気をつけて
 - ・ 本機能は IPv4 の場合に使用できます。
 - DHCPサーバは通信許可を"すべての端末"に設定されたポートに接続してください。
 - 同一 VLAN 内で IPv4 DHCP 機能を有効に設定した場合、この VLAN では本機能が無効になり、すべての端末が通信可能となります。
 - 通信許可が "DHCPでIPアドレスを割り当てられた端末のみ"に設定されたポートで以下の条件に一致する場合、このポートでは本機能が無効になり、すべての端末が通信可能となります。
 - IEEE802.1X 認証、Web 認証および MAC アドレス認証のどれかが有効に設定されている場合
 - リンクアグリゲーションとして設定されている場合
 - タグ VLAN が設定されている場合
 - SR-S224PS1/224CP1/248TC1/308TL1/310TL2/316TL1/318TL2/324TL2/316C2/324TC1/328TR1/348TC1/ 716C2/724TC1/748TC1で、プロトコルVLANが設定されている場合
 - SR-S208TC2/224TC2/208PD1では、転送許可ポートを設定したポートが存在した場合、本機能は無効となり、すべての端末が通信可能となります。
 - 本装置では、一度登録された許可端末が存在しなくなってもエントリ自体はリース期間の満了まで消去しません。 DHCPサーバでリース期間を適切に設定してください。
 また、不要なエントリが登録されている場合は、「表示メニュー」-「DHCPスヌープ関連」-「エントリ情報」で消去 することができます。
 - ・ 監視可能な DHCP クライアント数を超えた場合、受信した DHCPパケットは破棄されエントリ登録されません。
 また、最大エントリ数に満たない場合でも登録できないことがあります。エントリ登録に失敗した場合は、登録に失敗したことを示すシステムログが記録されます。
 - 本機能は DHCP パケットの往復を監視して動作します。DHCP クライアントとサーバ間の通信は必ず本装置を経由す るようなネットワーク構成にしてください。
 - ・ 設定反映、または装置リセットを実行した場合、エントリが破棄される場合があります。この場合、端末がDHCPで IPアドレスを再取得するまで通信できなくなります。


● 設定条件

• VLAN10でDHCPスヌープ機能を使用する

٠	ETHER ポートの通信許可	
	ETHER1 ポート	:DHCPでIPアドレスを割り当てられた端末のみ
	ETHER5ポート	:すべての端末
	ETHER11 ポート	:DHCPでIPアドレスを割り当てられた端末のみ

上記の設定条件に従って設定を行う場合の設定例を示します。

DHCP スヌープ機能を使用する

- **1. 設定メニューの詳細設定で「VLAN 情報」をクリックします**。 「VLAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - VLAN ID



→10

- **3. [追加] ボタンをクリックします**。 「VLAN10 情報」ページが表示されます。
- **「DHCP スヌープ情報」をクリックします**。
 「DHCP スヌープ情報」が表示されます。
- 5. 以下の項目を指定します。
 - DHCPスヌープ機能 →使用する

■DHCPスヌープ情報		3
DHCPスヌーブ機能	●使用しない ●使用する	

6. [保存] ボタンをクリックします。

DHCPスヌープのETHERポートの通信許可を設定する

- 設定メニューの詳細設定で「ether情報」をクリックします。
 「ether情報」ページが表示されます。
- 8. 「ether 情報」でポート番号が1の「修正」ボタンをクリックします。 ether1 情報の設定項目と「基本情報」が表示されます。
- **9.** 「DHCPスヌープ情報」をクリックします。 「DHCPスヌープ情報」が表示されます。
- 10. 以下の項目を設定します。
 - ポートの通信許可 →DHCPでIPアドレスを割り当てられた端末のみ

■DHCPスヌープ情報		3
ポートの通信許可	 ● DHCPでIPアドレスを割り当てられた端末のみ ● すべての端末 	

11. 【保存】ボタンをクリックします。

12. 「基本情報」をクリックします。

「基本情報」が表示されます。

VLAN
 untagged

→10

V/LAN	Tagged	
VLAN	Untagged	10

- 13. 【保存】ボタンをクリックします。
- 14. 手順6.~12.を参考にETHERポート5を設定します。
 「ether5情報」-「DHCPスヌープ情報」

 ポートの通信許可 →すべての端末
 「ether5情報」-「基本情報」
 VLAN
 <untagged →10

 15. 手順6.~12.を参考にETHERポート11を設定します。
 「ether11情報」-「DHCPスヌープ情報」

 ポートの通信許可 →DHCPでIPアドレスを割り当てられた端末のみ
 「ether11情報」-「基本情報」
 - VLAN untagged → 10
- 16. 【保存】ボタンをクリックします。
- **17. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

9 IGMPスヌープ機能を使う

適用機種 全機種

IGMPスヌープ機能を使用すると、マルチキャストパケットを必要としているポートをIGMPパケットから検出 し、そのポート以外へはマルチキャストパケットを転送しません。これにより、無用なトラフィックを端末や サーバに送出することが防止でき、マルチキャストを利用しているネットワークで端末やサーバの負荷を軽減す ることができます。

● 参照 機能説明書「2.14 IGMPスヌープ機能」(P.75)

こんな事に気をつけて

- マルチキャストルーティング機能が有効である lan 定義が存在する場合、IGMP スヌープ機能は無効となり、動作しません。
- 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、「表示メニュー」「IGMPスヌープ関連」-「リスナ情報」で消去することができます。
- 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破棄されます。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。
- IGMPスヌープ機能を有効にした場合、「VLAN 情報」-「IGMPスヌープ情報」の「IGMP 送信元アドレス」に定義がないと送信元アドレスとして0.0.0.0を使用します。送信元アドレスが0.0.0.0である IGMP Query パケットを扱えない装置が接続されている場合、「VLAN 情報」-「IGMPスヌープ情報」の「IGMP 送信元アドレス」を設定してください。なお、マルチキャストルータが接続されているネットワークでは、マルチキャストルータのアドレスより大きな値となるアドレスを送信元アドレスとして指定してください。
- IGMP V1/V2 が混在する環境では、「VLAN 情報」-「IGMP スヌープ情報」でIGMP 代理応答モードを"代理応答しない"と選択してください。
- IPv4 マルチキャスト以外の通信(例: IPv6 通信)を利用するネットワークでは利用できません。IGMP スヌープ機能は有効にしないでください。
- 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 情報」-「IGMP スヌープ情報」でQuerier モードを 動作可能としてください。



● 設定条件

• IGMPスヌープ機能を利用する

リスナ端末はそれぞれ以下に属す	6	
リスナ端末1	ポート	:ETHER1、2ポート
	VLAN	: 10
リスナ端末2	ポート	:ETHER3、4ポート
	VLAN	: 11
リスナ端末3	ポート	:ETHER5、6ポート
	VLAN	: 12

- マルチキャストルータ1はタグVLANを使用し、VLAN10~12を設定する ポートは ETHER15に接続する
- マルチキャストルータ2はVLAN10に属し、ポートはETHER16に接続する

上記の設定条件に従って設定を行う場合の設定例を示します。

IGMPスヌープ機能を使用する

- **1. 設定メニューの詳細設定で「IGMPスヌープ情報」をクリックします**。 「IGMPスヌープ情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - IGMPスヌープ機能 →使用する

■基本情報	3	1
IGMPスヌーブ機能	○使用しない ●使用する	-

3. [保存] ボタンをクリックします。

メディア種別および VLAN を設定する

4. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether 情報」ページが表示されます。

5. 以下の項目を指定します。

ポートリスト → 1-2

ポート 1-2	修正初期化

6. [修正] ボタンをクリックします。

ether 1-2 情報の設定項目と「基本情報」が表示されます。

7. 以下の項目を指定します。

- メディア種別 →通常ポート(RJ45)
- VLAN

Untagged

→ 10

■基本情報			3
ボート使用		⊙使用する○使用しない	
メティア	重別	○自動 ⊙通常ポート(RJ45) ○ SFPポート	
通信速度		●自動 ○ 10Mbps ○ 100Mbps ○ 1000Mbps	
全二重/半二重		●全二重○半二重	
MDI		●自動 ○ MDI ○ MDI-X	
70-	送信	⊙しない○する	
制御受信		⊙する ○しない	
	Tagged		
V L PUL	Untagged	10	

機種によりメディア種別に対応しているポート番号は異なります。

8. [保存] ボタンをクリックします。

9. 手順4.~8.を参考に、ETHER3~6、15、16を設定します。

「ether 3 情報」-「基本情報」

VLAN Untagged	→ 11
「ether 4 情報」-「基本情報」	
 VLAN Untagged 	→ 11
「ether 5 情報」-「基本情報」	
• VLAN	
Untagged	→ 12
「ether 6 情報」-「基本情報」	
• VLAN	
Untagged	→ 12
「ether 15 情報」-「基本情報」	
• VLAN	
Tagged	→10-12

「ether 16 情報」-「基本情報」

VLAN
 Untagged → 10

複数のマルチキャストルータが接続される VLAN10 にマルチキャストルータポートを設定する

10. 設定メニューの詳細設定で「VLAN情報」をクリックします。

「VLAN情報」ページが表示されます。

11. 以下の項目を指定します。

VLAN ID

→10

</th <th>/LAN情報追加フィールド></th>	/LAN情報追加フィールド>
VLAN ID	10

12. [追加]ボタンをクリックします。

「VLAN10情報」ページが表示されます。

- **13. 「IGMPスヌープ情報」をクリックします**。 「IGMPスヌープ情報」が表示されます。
- 14. 以下の項目を指定します。
 - 静的ルータポート →設定する ルータポート → 15,16

■IGMPスヌープ情報	3
静的ルータボート	 ○ 自動認識 ● 設定する
	ルータポート 15.16

- 15. 【保存】ボタンをクリックします。
- **16. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

10 IEEE802.1X 認証機能を使う

適用機種 全機種

IEEE802.1X 認証を使用すると、本装置に接続する端末ユーザがネットワークへのアクセス権限を持っているか を認証することができます。また、認証データベースで、ユーザごとに所属する VLAN ID を設定すると、認証さ れたユーザが所属するネットワークも同時に管理できます。これらの機能によりネットワークへのアクセスを ユーザ単位で制御でき、ネットワークのセキュリティを向上することができます。

● 参照 機能説明書「2.15 IEEE802.1X 認証機能」(P.77)

- こんな事に気をつけて
 - IEEE802.1X 認証を利用するポートでは、事前に VLAN を設定できません。ただし、SR-S308TL1/310TL2/316TL1/ 318TL2/324TL2/316C2/324TC1/328TR1/348TC1/716C2/724TC1/748TC1 で、以下の場合はその限りではありません。
 - Web認証機能が併用されている場合の、Web認証用のタグなしのポートVLAN設定
 - VLAN タグ付きフレームを認証しないで透過する場合の、タグ VLAN 設定
 - ・ IEEE802.1X 認証で利用する AAA のグループ ID を正しく設定してください。
 - ローカル認証で利用できる認証方式はEAP-MD5のみです。
 - マルチサプリカント環境で確認済みのサプリカントソフトは富士通製「Systemwalker Desktop Inspection 802.1X サプリカント」です。
 - ・ マルチサプリカント環境では課金情報のうち以下の項目が正しく採取できません。
 - 送信パケット数
 - 受信パケット数
 - 送信バイト数
 - 受信バイト数

SR-S316C2/716C2の場合を例にします。



● 設定条件

- ETHER10~12ポートでIEEE802.1X認証を使用する
- ETHER10~12ポートで利用する認証データベース
 ETHER10、11ポート : RADIUSサーバ
 ETHER12ポート : ローカルで設定した認証情報

- AAA グループID
 ETHER10、11 ポート : 0
 ETHER12 ポート : 1
- SupplicantのMACアドレスごとに認証を行う
- ETHER12ポートで利用可能なユーザは以下のとおり

ユーザID	パスワード	割り当てる VLAN ID
Supp1	Supp1-pass	VLAN123
Supp2	Supp2-pass	VLAN100

- RADIUSサーバのIPアドレス : 172.16.1.100
- RADIUS サーバは VLAN13 に接続されている
- RADIUSサーバのシークレット : radius-secret
- ETHER10、11 ポートで利用する RADIUS サーバで、認証処理と課金情報(※)の収集を行う
- ※)本装置がサポートする課金情報と対応する属性を以下に示します。
 - 接続時間 : Acct-Session-Time
 - 送信パケット数 : Acct-Output-Packets
 - 受信パケット数 : Acct-Input-Packets
 - 送信バイト数 :Acct-Output-Octets
 - 受信バイト数 : Acct-Input-Packets

こんな事に気をつけて

 RADIUS サーバにはユーザに VLAN ID を割り当てるために以下の属性を設定してください。設定方法については RADIUS サーバのマニュアルを参照してください。

名前	番号	属性值(※)
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

• タグにより複数のトンネル属性が設定されている場合は、利用可能な値が指定されているもっとも小さなタグの情報 がユーザに割り当てる VLAN 情報として選択されます。

上記の設定条件に従って設定を行う場合の設定例を示します。

IEEE802.1X 認証を使用する

- 設定メニューの詳細設定で「認証情報」をクリックします。
 「認証情報」ページが表示されます。
- **2.** 「IEEE802.1X 認証情報」をクリックします。 「IEEE802.1X 認証情報」が表示されます。
- 3. 以下の項目を指定します。
 - IEEE802.1X認証 →使用する

■IEEE802.1X認証情報		3
IEEE802.1X認証	●使用しない●使用する	

4. [保存] ボタンをクリックします。

RADIUS サーバの VLAN を設定する

- **5. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 6. 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 7. 「共通情報」をクリックします。 共通情報の設定項目と「基本情報」が表示されます。
- 8. 以下の項目を指定します。
 - VLAN ID → 13



- 9. [保存] ボタンをクリックします。
- **10.** 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 11. 以下の項目を指定します。
 - IPアドレス → 172.16.1.101
 - ネットマスク → 16 (255.255.0.0)

■IPアドレス 情報	3
IPアドレス	172.16.1.101
ネットマスク	16 (255.255.0.0)

12. [保存] ボタンをクリックします。

RADIUSサーバを接続するポートを設定する

- **13. 設定メニューの詳細設定で「ether情報」をクリックします**。 「ether情報」ページが表示されます。
- **14.** 「ether 情報」でポート番号が1の [修正] ボタンをクリックします。 ether 1 情報の設定項目と「基本情報」が表示されます。

VLAN を設定する

- 15. 以下の項目を指定します。
 - VLAN
 Untagged

→13

	Tagged	
VLAN	Untagged	13

16. 【保存】ボタンをクリックします。

IEEE802.1X により認証された Supplicant が接続される VLAN 情報を設定する

- **17.** 手順13.~16.を参考に、ETHER2~5ポートを設定します。
 - 「ether 2 情報」-「基本情報」

VLAN Untagged	→ 10
「ether 3 情報」-「基本情報」	
• VLAN	
Untagged	→ 11
「ether 4 情報」-「基本情報」	
• VLAN	
Untagged	→ 100
「ether 5 情報」-「基本情報」	
• VLAN	
Untagged	→123

IEEE802.1X 認証ポートを設定する

- **18. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- 19. 以下の項目を指定します。
 - ポートリスト → 10-11



- **20.** 【修正】ボタンをクリックします。 ether 10-11 情報の設定項目と「基本情報」が表示されます。
- **21.** 「IEEE802.1X 認証情報」をクリックします。

「IEEE802.1X認証情報」が表示されます。

- 22. 以下の項目を指定します。
 - 認証動作モード →使用する
 - "使用する"を選択すると、「参照する AAA 情報」の設定項目が表示されます。
 - 参照する AAA 情報 →0

■IEEE802.1X認証情報		3
認証動作モート	○使用しない ⊙使用する	
認証方式	●デフォルト ● MACアドレスごと ●ボートごと	
ボート認証制御	●自動○認証拒否○認証許容	
認証失敗時再認証 抑止時間	1 分 🗸	
認証開始送信間隔	30 秒 🕶	
EAP応答待ち時間	30 秒 🗸	
EAP再送回数	2 0	
再認証間隔	 ●時間指定 1 時間 ▼ ● 再認証しない 	
参照するAAA情報	0	

- 23. [保存] ボタンをクリックします。
- **24. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- **25.** 「ether 情報」でポート番号が 12 の [修正] ボタンをクリックします。 ether 12 情報の設定項目と「基本情報」が表示されます。
- 26. 手順21.~23.を参考に、以下の項目を設定します。
 - 認証動作モード →使用する
 - 参照する AAA 情報 →1

RADIUS サーバを利用する AAA グループ情報を設定する

- **27. 設定メニューの詳細設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- 28. 以下の項目を指定します。
 - グループ名

	<グループID情報追加フィールド>	
ループ名	rmtauth	

→ rmtauth

29. [追加] ボタンをクリックします。

「グループID 情報(0)」ページが表示されます。

30. 「RADIUS 関連」をクリックします。

RADIUS 関連の設定項目と「基本情報」が表示されます。

31. 以下の情報を指定します。

 RADIUSサービス 	→クライアント機能
認証	→チェックする
アカウンティング	→チェックする

- 自側認証 IP アドレス → 172.16.1.101
- 自側アカウンティングIPアドレス →172.16.1.100

■基本情報	3
RADIUSサービス	クライアント機能 ✓ ✓ 認証 ✓ アカウンティング (クライアント機能を選択した場合にのみ有効 となります)
自側認証IPアトレス	172.16.1.101
自側アカウンティングIP アドレス	172.16.1.100

- 32. [保存] ボタンをクリックします。
- **33.** RADIUS 関連の設定項目の「サーバ情報」をクリックします。 「サーバ情報(クライアント機能)」が表示されます。
- 34. 「認証情報1」の[修正] ボタンをクリックします。

	共有鍵	••••••
	サーバIPア ドレス	172.16.1.100
	サーバ UDPポート	⊙ 1812 ◯ 1645
認証情報 1	復旧待機 時間	0 秒 🗸
	優先度	0
	自側認証 IPアドレス	

36. 認証情報1の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

37. 「アカウンティング情報1」の[修正] ボタンをクリックします。

38. 以下の項目を指定します。

 アカウンティング情報1 共有鍵 → radius-secret サーバIPアドレス → 172.16.1.100

	共有鍵	••••••
	サーバIPア ドレス	182.16.1.100
	サーバ UDPポート	⊙ 1813 ◯ 1646
アカウンティング情報 1	復旧待機 時間	0 秒 🗸
	優先度	0
	自側アカウ ンティング	
	IPアドレス	

39. アカウンティング情報1の[保存]ボタンをクリックします。 「サーバ情報(クライアント機能)」に戻ります。

ローカル認証情報を利用する AAA グループ情報を設定する

40. 設定メニューの詳細設定で「AAA 情報」をクリックします。

「AAA 情報」ページが表示されます。

- 41. 以下の項目を指定します。
 - グループ名

→ localauth

</th <th>ブループID情報追加フィールド></th>	ブループID情報追加フィールド>
グループ名	localauth

42. [追加] ボタンをクリックします。

「グループID情報(1)」ページが表示されます。

43. 「AAA ユーザ情報」をクリックします。

AAAユーザ情報の設定項目と「AAAユーザ情報」が表示されます。

- 44. 以下の項目を指定します。
 - ユーザID → Supp1
 <AAAユーザ情報追加フィールド>
 ユーザID [Supp1]
- 45. [追加] ボタンをクリックします。

「AAAユーザ情報(0)」ページが表示されます。

46. 「認証情報」をクリックします。

認証情報の設定項目と「認証情報」が表示されます。

- 47. 以下の項目を指定します。
 - ユーザID → Supp1
 - ● 認証パスワード
 → Supp1-pass

 ●
 コンパスワード

■認証情報	報	3
ユーザID	Supp1	
認証バス ワード	•••••	
権限クラ ス	●指定しない ○管理者クラス ○一般ユーザクラス	

- 48. [保存] ボタンをクリックします。
- **49.** 「サプリカント関連」をクリックします。 サプリカント関連の設定項目と「サプリカント情報」が表示されます。
- 50. 以下の項目を指定します。
 - 割り当てる VLAN ID → 123

■サプリカント情報	3
割り当てるVLAN ID	123

- 51. [保存] ボタンをクリックします。
- **52.** 手順44.~51.を参考に、以下の項目を設定します。

「グループ ID 情報(1)」-「AAA ユーザ情報(1)」-「認証情報」-「認証情報」

- ユーザID → Supp2
- ● 認証パスワード
 → Supp2-pass

 ●
 コンパスワード

「グループID 情報(1)」-「AAA ユーザ情報(1)」-「サプリカント関連」-「サプリカント情報」

- 割り当てる VLAN ID → 100
- 53. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

11 Web 認証機能を使う

適用機種 全機種

Web 認証機能を使用すると、認証が成功した場合のみ外部のネットワークに接続するため、セキュリティを向上 させることができます。

● 参照 機能説明書 [2.16 Web 認証機能」(P.82)

こんな事に気をつけて

- Web認証を利用するポートでは、Web認証機能で用いるためのVLANとして、タグなしのポートVLANだけ指定できます。タグVLANおよびプロトコルVLANは設定しないでください。ただし、SR-S308TL1/310TL2/316TL1/318TL2/324TL2/316C2/324TC1/328TR1/348TC1/716C2/724TC1/748TC1で、以下の場合はその限りではありません。
 VLANタグ付きフレームを認証しないで透過する場合の、タグVLAN設定
- 認証用 VLAN への経路を広報しないように経路フィルタを設定してください。
- ・ 認証用 VLAN から外部へ IP パケットが透過しないように IP フィルタを設定してください。

11.1 AAA でローカル認証を行う

適用機種 全機種

SR-S716C2の場合を例にします。



● 設定条件

• ETHER10、11 ポートでWeb 認証機能を用いて、AAA グループIDは1を使用する

•	ETHER10、11 ポートの認証方法	
	ETHER10ポート	:MACアドレス
	ETHER11 ポート	:ポート

- 認証プロトコルとして MD5-CHAP を使用する
- 認証用 VLAN の VLAN ID : 500
- 認証用 VLAN の LAN0 の IP アドレス : 192.168.1.0/24
- 認証用 VLAN では DHCPで IP アドレスを割り当てる 割り当てる IP アドレス : 192.168.1.2/24 から 100 個 リース期間 : 30 秒

- 認証用 VLANの LAN0で許可する通信
 送信元 IP アドレス : 192.168.1.0/24
 あて先 IP アドレス : 192.168.1.1/32
- VLAN ID 10が割り当てられた場合は、ETHER2ポートと通信する
- VLAN ID 11 が割り当てられた場合は、ETHER3 ポートと通信する
- ユーザuser0とuser1をAAAグループ1に登録する user0で割り当てるVLAN ID 10 user1で割り当てるVLAN ID 11

上記の設定条件に従って設定を行う場合の設定例を示します。

IPフォワーディング機能を有効に設定する

- **1. 設定メニューの詳細設定で「IP 情報」をクリックします**。 「IP 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - IPフォワーディング機能 →使用する

■基本情報	3
ARPエントリ有効時間	20 分
IPフォワーティング機能	○使用しない ⊙使用する

3. [保存] ボタンをクリックします。

Web認証機能を使用する

- **4. 設定メニューの詳細設定で「認証情報」をクリックします**。 「認証情報」ページが表示されます。
- **5.** 「Web 認証情報」をクリックします。 「Web 認証情報」が表示されます。
- 6. 以下の項目を指定します。
 - 認証機能 →使用する
 - 認証プロトコル → CHAP

Web認証情報	3
認証機能	○使用しない ◎使用する
認証ブロトコル	⊙CHAP ○ PAP

7. [保存] ボタンをクリックします。

認証用 VLAN の VID に 500(LAN0)を設定する

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 9. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。

10. 「共通情報」をクリックします。 共通情報の設定項目と「基本情報」が表示されます。

- 11. 以下の項目を指定します。
 - VLAN ID → 500
 基本情報
 VLAN ID 500
- 12. [保存] ボタンをクリックします。

DHCP サーバ機能を設定する

13. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

- 14. 以下の項目を指定します。
 - IPアドレス → 192.168.1.1
 - ネットマスク → 24 (255.255.255.0)
 - ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報	3
IP アド レス	192.168.1.1
ネットマスク	24 (255.255.255.0)
フロートキャストアトレス	ネットワークアドレス+オール1 💌

- 15. [保存] ボタンをクリックします。
- **16.** IP **関連の設定項目の「DHCP 情報」をクリックします**。 「DHCP 情報」が表示されます。
- 17. 以下の項目を指定します。

•	DHCP機能	→サーバ機能を使用する
	割当て先頭IPアドレス	→ 192.168.1.2
	割当てアドレス数	→ 100
	リース期間	→30秒
	DNSサーバ広報	→ 192.168.1.1

	۲	サーバ機能を使用す	-3
DUCD		割当て先頭IPアド レス	192.168.1.2
機能		割当てアドレス数	100
		リース期間	30 秒 💙
		デフォルトルータ広 報	
		DNSサーバ広報	192.168.1.1

18. [保存] ボタンをクリックします。

ETHER10、11 ポートでは STP を使用しない

19. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether 情報」ページが表示されます。

- 20. 以下の項目を設定します。
 - ポートリスト → 10,11



- **21.** 【修正】ボタンをクリックします。 ether 10,11 情報の設定項目と「基本情報」が表示されます。
- **22. 「**STP 関連」をクリックします。

STP 関連の設定項目と「基本情報」が表示されます。

- 23. 以下の項目を指定します。
 - STP 機能

→使用しない

■基本情報	■基本情報 []				
	 ● 使用しばい ○ 使用する 				
പാക്കും	STP動作バージョン 指定なし 🕶				
STPOKEL	バスコスト ●自動決定 ○指定する				
	インタフェース優先度 128 💌				

24. [保存] ボタンをクリックします。

ETHER10、11 ポートで Web 認証機能を使用する

- **25. 画面上部の「ether 10,11 情報」をクリックします**。 ether 10,11 情報の設定項目と「基本情報」が表示されます。
- 26. 以下の項目を指定します。
 - VLAN
 Untagged

→500

	Tagged	
VEFU	Untagged	500

- 27. [保存] ボタンをクリックします。
- 28. 「Web認証関連」をクリックします。

Web 認証関連の設定項目と「基本情報」が表示されます。

認証機能 →使用する
 参照する AAA 情報 →0

■基本情報 []				
	使用しない 使用する			
	参照するAAA情報 0			
	認証方式 ◎ MACアドレスごと ○ボ・	ートごと		
	デフォルト割り当て VLAN			
設計機 能	Web認証有効時間 ・認証を解除しない エージアウト後指定時 時	間経過 経過時		
	WOL転送モード ◎転送しない ○転送する	,		

- 30. [保存] ボタンをクリックします。
- **31. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- **32.** 「ether 情報」でポート番号が 11 の [修正] ボタンをクリックします。 ether 11 情報の設定項目と「基本情報」が表示されます。
- **33.** 「Web 認証関連」をクリックします。 Web 認証関連の設定項目と「基本情報」が表示されます。
- 34. 手順29.~30.を参考に、以下の項目を設定します。
 - 認証機能 →使用する
 認証方式 →ポートごと

Web認証後、VLAN IDが割り当てられたときに通信する ETHER ポートを設定する

- **35. 設定メニューの詳細設定で「ether情報」をクリックします**。 「ether情報」ページが表示されます。
- **36.** 「ether 情報」でポート番号が2の [修正] ボタンをクリックします。 ether 2 情報の設定項目と「基本情報」が表示されます。
- 37. 以下の項目を指定します。
 - VLAN Untagged

→10

VLAN	Tagged	
	Untagged	10

38. [保存] ボタンをクリックします。

39. 手順 35.~38.を参考に、ETHER3 ポートを設定します。

「ether 3 情報」-「基本情報」

VLAN
 Untagged → 11

外部と通信する ETHER ポートを設定する

- **40.** 手順 35. ~ 38. を参考に、ETHER16 ポートを設定します。 「ether 16 情報」-「基本情報」
 - VLAN
 Untagged → 100

IP フィルタリング機能で使用する ACL 情報を設定する

- **41. 設定メニューの詳細設定で「ACL 情報」をクリックします**。 「ACL 情報」ページが表示されます。
- 42. 以下の項目を指定します。
 - 定義名

→acl0



43. [追加] ボタンをクリックします。

「ACL 定義情報(acl0)」ページが表示されます。

44. 「IP 定義情報」をクリックします。

「IP定義情報」が表示されます。

45. 以下の項目を指定します。

- プロトコル →すべて
 送信元情報
 IPアドレス → 192.168.1.0
 アドレスマスク → 24 (255.255.255.0)
- あて先情報
 IPアドレス → 192.168.1.1
 アドレスマスク → 32 (255.255.255)
- QoS →指定なし

■IP定義情報		
ブロトコル		すべて (番号指定:
送信元情	IPアドレス	192.168.1.0
報	アドレスマ スク	24 (255.255.255.0)
あて先情	IPアドレス	192.168.1.1
報	アトレスマ スク	32 (255.255.255.255) 💌
QoS		指定なし ▼ TOS、または、DSCPを選択時に値を入力してく ださい

- 46. [保存] ボタンをクリックします。
- 47. 手順41.~46.を参考に、以下の項目を設定します。

「ACL情報」

• 定義名	→acl1		
「ACL定義情報 (acl1)」-「IP 定義	青報」		
• プロトコル	→すべて		
 送信元情報 IP アドレス 	→指定しない		
アドレスマスク	$\rightarrow 0 \ (0.0.0.0)$		
 あて先情報 IPアドレス アドレスマスク 	→ 255.255.255.255 → 32 (255.255.255.255)		
• QoS	→指定なし		
「ACL情報」			
• 定義名	→acl2		
「ACL定義情報(acl2)」-「IP定義情報」			
• プロトコル	→すべて		
 送信元情報 IPアドレス アドレスマスク 	→指定しない →0 (0000)		
 あて先情報 	0 (0.0.0.0)		
IPアドレス アドレスマスク	→指定しない →0(0.0.0)		
• QoS	→指定なし		

外部と通信する LAN1 を設定する

48. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

49. 以下の項目を指定します。

• VLAN ID → 100

<lan情報追加フィールド></lan情報追加フィールド>		
VLAN ID	100	

- **50. [追加] ボタンをクリックします**。 「LAN1 情報」ページが表示されます。
- **51. 「IP 関連」をクリックします**。 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 52. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IPフィルタリング情報」が表示されます。

53. 以下の項目を指定します。

- 動作 →透過
- ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作 ③透過 ○遮断		
ACL定義番号	0 参照	

54. [追加] ボタンをクリックします。

55. 手順53.~54.を参考に、以下の項目を設定します。

- 動作 →透過
- ACL定義番号 →1
- 56. 手順 53. ~ 54. を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL定義番号 →2

57. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

- IPアドレス
- → 172.16.1.102
- ネットマスク →24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報	3
IPアトレス	172.16.1.102
ネットマスク	24 (255.255.255.0) 💌
フロートキャストアトレス	ネットワークアドレス+オール1 💌

59. [保存] ボタンをクリックします。

外部と通信するLAN1ではRIPを使用してダイナミックルーティングを行う

60. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

61. 以下の項目を指定します。

- RIP送信 → V2 (Multicast) で送信する
- RIP受信 → V2、V2 (Multicast) で受信する
- メトリック値 →0
- 認証パケット →破棄しない
 パスワード →指定しない

RIP情報	3	
RIP送信	●送信しない ●V1で送信する ●V2で送信する ●V2(Multicast)で送信する	
RIP受信	○受信しない ○V1で受信する ⊙V2、V2(Multicast)で受信する	
《 RIP 送信時は加算する	るメトリック値を設定してください。》	
メトリック値	0 💌	
《 RIP V2使用時で認証バケットを破棄しない時はRIP V2バスワードを設定してください。》		
認証バケット	 ○ 破棄する ③ 破棄しない パスワード 	

62. [保存] ボタンをクリックします

RIPを使用するインタフェースでは認証用 VLAN の 192.168.1.0/24 に対する経路を配布しない

- **63. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **64. 「**RIP 関連」をクリックします。

RIP関連の設定項目と「RIPタイマ情報」が表示されます。

65. 「RIP 再配布フィルタリング情報」をクリックします。

「RIP再配布フィルタリング情報」が表示されます。

 動作 →遮断
 フィルタリング条件 →経路情報指定 検索条件 →完全に一致
 IPアドレス → 192.168.1.0
 アドレスマスク → 24 (255.255.255.0)

<rip再配布フィルタリング情報入力フィールド></rip再配布フィルタリング情報入力フィールド>			
動作	○透過 ④遮断		
フィルタリング条件	 すべて デフォルトルート 経路情報指定 検索条件 ・完全に一致 ・マスクした結果が一致 IPアドレス 192.168.1.0 アドレスマスク 24 (255.255.255.0) 		

- 67. [追加] ボタンをクリックします
- 68. 手順66.~67.を参考に、以下の項目を設定します。
 - 動作 →透過
 - フィルタリング条件 →すべて

AAA情報を設定する

- **69. 設定メニューの詳細設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- 70. 以下の項目を指定します。
 - グループ名

→home	
-------	--

<グループID情報追加フィールド>		
グループ名	home	

71. [追加] ボタンをクリックします。

「グループID 情報(0)」ページが表示されます。

72. 「AAA ユーザ情報」をクリックします。

AAAユーザ情報の設定項目と「AAAユーザ情報」が表示されます。

- 73. 以下の項目を指定します。
 - ユーザID

→user0



74. [追加] ボタンをクリックします。

「AAAユーザ情報(0)」ページが表示されます。

75. 「認証情報」をクリックします。 認証情報の設定項目と「認証情報」が表示されます。

- ユーザID
- • 認証パスワード → pass0

 • 認証パスワード

■認証情報	R []
ユーザID	user0
認証バス ワード	•••••
<mark>権限</mark> クラ ス	●指定しない ●管理者クラス ◎一般ユーザクラス

- 77. [保存] ボタンをクリックします。
- 78. 「サプリカント関連」をクリックします。

サプリカント関連の設定項目と「サプリカント情報」が表示されます。

- 79. 以下の項目を指定します。
 - 割り当てる VLAN ID

→ 10

→user0

サプリカントMACアドレスによる識別

→ MAC アドレスをチェックしな	こ
-------------------	---

■サプリカント情報	3
割り当てるVLAN ID	10
サブリカントMACアドレスによる 識別	 MACアドレスをチェックしない MACアドレスをチェックする MACアドレス

- 80. [保存] ボタンをクリックします。
- 81. 手順 73. ~ 80. を参考に、以下の項目を設定します。

「グループID 情報(1)」-「AAA ユーザ情報」-「AAA ユーザ情報」

• ユーザID → user1

「AAA ユーザ情報(1)」-「認証情報」-「認証情報」

- ユーザID →user1
- • 認証パスワード → pass1

 • 認証パスワード

「AAA ユーザ情報(1)」「サプリカント関連」-「サプリカント情報」

- 割り当てる VLAN ID → 11
- サプリカントMACアドレスによる識別 → MACアドレスをチェックしない
- 82. 画面左側の[再起動] ボタンをクリックします。 装置の再起動後、設定した内容が有効になります。

11.2 AAA でリモート認証を行う

適用機種 全機種

SR-S716C2の場合を例にします。



● 設定条件

• ETHER10、11 ポートでWeb 認証機能を用いて、AAA グループIDは1を使用する

•	ETHER10、11 ポートの認証方法	
	ETHER10 ポート	:MACアドレス
	ETHER11 ポート	:ポート
•	RADIUSサーバのIPアドレス	: 172.16.1.100
•	認証プロトコルとして MD5-CHAP を使用する	
•	認証用VLANのLAN0のIPアドレス	: 192.168.1.0/24
•	認証用VLANではDHCPでIPアドレスを割り当る	てる
	割り当てるIPアドレス	:192.168.1.2/24から100個
	リース期間	:30秒
•	認証用 VLAN の LAN0 で許可する通信	
	送信元 IP アドレス	: 192.168.1.0/24
	あて先 IP アドレス	: 192.168.1.1/32

上記の設定条件に従って設定を行う場合の設定例を示します。

IPフォワーディング機能を有効に設定する

1. 設定メニューの詳細設定で「IP 情報」をクリックします。

「IP 情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - IPフォワーディング機能 →使用する

■基本情報	3
ARPエントリ有効時間	20 分
IPフォワーディング機能	○使用しない ◎使用する

3. [保存] ボタンをクリックします。

Web 認証機能を使用する

4. 設定メニューの詳細設定で「認証情報」をクリックします。

「認証情報」ページが表示されます。

5. 「Web認証情報」をクリックします。

「Web 認証情報」が表示されます。

- 6. 以下の項目を指定します。
 - 認証機能 →使用する
 - 認証プロトコル → CHAP

Web認証情報	3
認証機能	○使用しない ⊙使用する
認証ブロトコル	⊙CHAP ○ PAP

7. [保存] ボタンをクリックします。

認証用 VLAN の VID に 500 を設定する

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 9. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 10. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 11. 以下の項目を指定します。
 - VLAN ID

→500

■基本情報		
VLAN ID	500	

12. [保存] ボタンをクリックします。

DHCP サーバ機能を設定する

13. 「IP 関連」をクリックします。

IP 関連の設定項目と「IPアドレス情報」が表示されます。

• IP アドレス

- →192.168.1.1
- ネットマスク →24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報	3
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0)
フロートキャストアトレス	ネットワークアドレス+オール1 💌

15. [保存] ボタンをクリックします。

16. IP 関連の設定項目の「DHCP 情報」をクリックします。 「DHCP 情報」が表示されます。

17. 以下の項目を指定します。

 DHCP機能 →サーバ機能を使用する 割当て先頭IPアドレス → 192.168.1.2
 割当てアドレス数 → 100
 リース期間 → 30秒
 DNSサーバ広報 → 192.168.1.1

	۲	サーバ機能を使用す	-3
		割当て先頭IPアド レス	192.168.1.2
機能		割当てアドレス数	100
		リース期間	30 秒 💙
		デフォルトルータ広 報	
		DNSサーバ広報	192.168.1.1

18. [保存] ボタンをクリックします。

IPフィルタリング機能を設定する

- **19. 設定メニューの詳細設定で「ACL情報」をクリックします**。 「ACL 情報」ページが表示されます。
- 20. 以下の項目を指定します。
 - ・ 定義名
 → acl0
 <ACL情報追加フィールドン</p>
 定義名
 acl0
- **21. [追加] ボタンをクリックします**。 「ACL 定義情報(acl0)」ページが表示されます。
- **22. 「IP 定義情報」をクリックします**。 「IP 定義情報」が表示されます。

• QoS

•	プロトコル	→すべて
•	送信元情報	
	IPアドレス	→ 192.168.1.0
	アドレスマスク	→24 (255.255.255.0)
•	あて先情報	
	IPアドレス	→ 192.168.1.1
	アドレスマスク	→32 (255.255.255.255)

→指定なし

■IP定義情報		
ブロトコル		すべて (番号指定: ″その他″を選択時のみ有効で す)
送信元情	IPアドレス	192.168.1.0
報	アトレスマ スク	24 (255.255.255.0)
あて先情 報	IPアドレス	192.168.1.1
	アドレスマ スク	32 (255.255.255.255) 💌
QoS		指定なし ▼ TOS、または、DSCPを選択時に値を入力してく ださい

- 24. [保存] ボタンをクリックします。
- 25. 手順 19.~24.を参考に、以下の項目を設定します。

「ACL情報」

• 定義名	→acl1
「ACL定義情報(acl1)」-「IP定義	青報」
• プロトコル	→すべて
 送信元情報 IP アドレス アドレスマスク 	→指定しない →0(0.0.0.0)
 あて先情報 IPアドレス アドレスマスク 	→ 255.255.255.255 → 32 (255.255.255.255)
• QoS	→指定なし
「ACL情報」	
• 定義名	→acl2
「ACL定義情報(acl2)」-「IP定義	青報」
 プロトコル 送信元情報 IPアドレス 	→すべて →指定しない)
アドレスマスク	→0 (0.0.00)
 あて先情報 IPアドレス アドレスマスク 	→指定しない →0(0.0.0)
QoS	→指定なし

ETHER10、11 ポートでは STP を使用しない

26. 設定メニューの詳細設定で「ether 情報」をクリックします。 「ether 情報」ページが表示されます。

27. 以下の項目を設定します。

ポートリスト → 10.11



- **28.** 【修正】ボタンをクリックします。 ether 10,11 情報の設定項目と「基本情報」が表示されます。
- **29. 「**STP 関連」をクリックします。

STP 関連の設定項目と「基本情報」が表示されます。

- 30. 以下の項目を指定します。
 - STP機能

■基本情報	ŧ.	3
	 ● 使用しない ● 使用する 	
OT D HE AL	STP動作バージョン 指定なし 🗸	
るIP板成用店	バスコスト ○ 自動決定 ○ 指定する	
	インタフェース優先度 128 💌	

31. 【保存】ボタンをクリックします。

ETHER10、11 ポートで Web 認証機能を使用する

- **32. 画面上部の「ether 10,11 情報」をクリックします**。 ether 10,11 情報の設定項目と「基本情報」が表示されます。
- 33. 以下の項目を指定します。
 - VLAN
 Untagged

→500

	Tagged	
VLAN	Untagged	500

- 34. [保存] ボタンをクリックします。
- 35. 「Web認証関連」をクリックします。

Web 認証関連の設定項目と「基本情報」が表示されます。

認証機能 →使用する
 参照する AAA 情報 → 0

■基本情報 []				
	○ 使用しない ⊙ 使用する			
	参照するAAA情報 0			
	認証方式 🤇)MACアドレスごと ○ボートごと		
==0= . 7+8%	デフォルト割り当て VLAN			
認証機 能	● Web認証有効時間) 認証を解除しない エージアウト後指定時間経過 時 分) 認証完了後指定時間経過時		
	WOL転送モード)転送しない○転送する		

- 37. [保存] ボタンをクリックします。
- **38. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- **39.** 「ether 情報」でポート番号が 11 の [修正] ボタンをクリックします。 ether 11 情報の設定項目と「基本情報」が表示されます。
- **40.** 「Web 認証関連」をクリックします。 Web 認証関連の設定項目と「基本情報」が表示されます。
- 41. 手順36.~37.を参考に、以下の項目を設定します。
 - 認証機能 →使用する
 認証方式 →ポートごと

Web 認証後、VLAN ID が割り当てられたときに通信する ETHER ポートを設定する

- **42. 設定メニューの詳細設定で「ether情報」をクリックします**。 「ether情報」ページが表示されます。
- **43.** 「ether 情報」でポート番号が2の [修正] ボタンをクリックします。 ether 2 情報の設定項目と「基本情報」が表示されます。
- 44. 以下の項目を指定します。
 - VLAN
 Untagged

→10

	Tagged		
VEFU	Untagged	10	

- 45. [保存] ボタンをクリックします。
- **46.** 手順42.~45.を参考に、ETHER3ポートを設定します。
 - VLAN Untagged

LAN1をVLAN ID 100 に割り当てる

47. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

48. 以下の項目を指定します。

• VLAN ID → 100

<lan情報追加フィールド></lan情報追加フィールド>		
VLAN ID	100	

49. [追加] ボタンをクリックします。

「LAN1 情報」ページが表示されます。

50. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

- 51. 以下の項目を指定します。
 - IPアドレス → 172.16.1.102
 - ネットマスク → 24 (255.255.255.0)
 - ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報	3
IPアドレス	172.16.1.102
ネットマスク	24 (255.255.255.0)
フロートキャストアトレス	ネットワークアドレス+オール1 💌

52. [保存] ボタンをクリックします。

フィルタリング動作を定義する

- **53. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **54.** 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。 「LAN1 情報」ページが表示されます。
- **55. 「IP 関連」をクリックします**。 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **56.** IP 関連の設定項目の「IP フィルタリング情報」をクリックします。 「IP フィルタリング情報」が表示されます。

- 動作
- ACL定義番号 →0

▲ 「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作		⊙透過 ○遮断
ACL定義番号		0 参照

→透過

- 58. [追加] ボタンをクリックします。
- 59. 手順57.~58.を参考に、以下の項目を設定します。
 - 動作 →透過
 - ACL定義番号 →1
- 60. 手順57.~58.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - ACL定義番号 →2

外部と通信するLAN1ではRIPを使用してダイナミックルーティングを行う

61. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

62. 以下の項目を指定します。

- RIP送信 → V2 (Multicast) で送信する
- ■ RIP受信
 → V2、V2 (Multicast) で受信する
- メトリック値 →0
- 認証パケット →破棄しない
 パスワード →指定しない

■RIP情報	3	
RIP送信	 ○送信しない ○V1で送信する ○V2で送信する ⊙V2(Multicast)で送信する 	
RIP受信	○受信しない ○V1で受信する ⊙V2、V2(Multicast)で受信する	
メドリタン値		
《 RIP V2使用時で認証/	「ケットを破棄しない時はRIP V2バスワードを設定し	てください。》
認証バケット	 ○ 破棄する ③ 破棄しない バスワード 	

63. [保存] ボタンをクリックします。

RIPを使用するインタフェースでは認証用 VLAN の 192.168.1.0/24 に対する経路を配布しない

- **64. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- 65. 「RIP 関連」をクリックします。

RIP関連の設定項目と「RIPタイマ情報」が表示されます。

66. 「RIP 再配布フィルタリング情報」をクリックします。

「RIP再配布フィルタリング情報」が表示されます。

67. 以下の項目を指定します。

 動作 →遮断
 フィルタリング条件 →経路情報指定 検索条件 →完全に一致
 IPアドレス → 192.168.1.0
 アドレスマスク → 24 (255.255.255.0)

<rip再配布フィルタリング情報入力フィールド></rip再配布フィルタリング情報入力フィールド>				
動作	○透過 ⊙遮断			
フィルタリング条件	 ○ すべて ○ デフォルトルート ③ 経路情報指定 ▲ かまな(#) ③ 完全に一致 			
74702727#H	検索条件 ○ マスクした結果が一致 IPアドレス アドレスマスク 24 (255.255.255.0) ▼			

- 68. [追加] ボタンをクリックします
- 69. 手順67.~68.を参考に、以下の項目を設定します。
 - 動作 →透過
 - フィルタリング条件 →すべて

AAA情報を設定する

70. 設定メニューの詳細設定で「AAA 情報」をクリックします。

「AAA情報」ページが表示されます。

- 71. 以下の項目を指定します。
 - グループ名

→home

<グルーブID情報追加フィールド>		
グループ名	home	

72. [追加] ボタンをクリックします。

「グループ ID 情報 (0)」ページが表示されます。

73. 「RADIUS 関連」をクリックします。

RADIUS 関連の設定項目と「基本情報」が表示されます。

•	RADIUSサービス	→クライアント機能
	認証	→チェックする
	アカウンティング	→チェックする

■基本情報	
RADIUSサービス	クライアント機能 ▼ 図認証 ▼アカウンティング (クライアント機能を選択した場合にのみ有効 となります)

75. [保存] ボタンをクリックします。

76. RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報(クライアント機能)」が表示されます。

77. 「認証情報1」の [修正] ボタンをクリックします。

78. 以下の項目を指定します。

 認証情報1 共有鍵 サーバIPアドレス

→ test → 172.16.1.100

	共有鍵	••••
	サーバIPア ドレス	172.16.1.100
	サーバ UDPポート	⊙ 1812 ◯ 1645
認証情報 1	復旧待機 時間	0 秒 🗸
	優先度	0
	自側認証 IPアドレス	

79. 認証情報1の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

80. 画面左側の[再起動] ボタンをクリックします。 本装置の再起動後、設定した内容が有効になります。

12 MACアドレス認証機能を使う



MACアドレス認証機能を使用すると、本装置に接続する端末がネットワークへのアクセス権限を持っているかを認証することができます。

こんな事に気をつけて

- MACアドレス認証を利用するポートでは、事前に VLAN を設定できません。ただし、SR-S308TL1/310TL2/316TL1/ 318TL2/324TL2/316C2/324TC1/328TR1/348TC1/716C2/724TC1/748TC1で、以下の場合はその限りではありません。
 - Web認証機能が併用されている場合の、Web認証用のタグなしのポートVLAN設定
 - VLAN タグ付きフレームを認証しないで透過する場合の、タグ VLAN 設定
- MACアドレス認証で利用するAAAのグループIDを正しく設定してください。

SR-S316C2/716C2の場合を例にします。



● 設定条件

- ETHER10~12ポートでMACアドレス認証を使用する
- ETHER10~12ポートで利用する認証データベース
 ETHER10、11ポート : RADIUSサーバ
 ETHER12ポート : ローカルで設定した認証情報
- AAA グループID
 ETHER10、11 ポート : 0
 ETHER12 ポート : 1
- SupplicantのMACアドレスごとに認証を行う
- ETHER12ポートで利用可能なユーザは以下のとおり

MACアドレス	割り当てる VLAN ID
00:11:11:00:00:01	VLAN123
00:22:22:00:00:02	VLAN100

- RADIUSサーバのIPアドレス : 172.16.1.100
- RADIUS サーバは VLAN13 に接続されている
- RADIUSサーバのシークレット : radius-secret
- 認証プロトコルとして MD5-CHAP を使用する

- こんな事に気をつけて
 - RADIUS サーバにはユーザに VLAN ID を割り当てるために以下の属性を設定してください。設定方法については RADIUS サーバのマニュアルを参照してください。

名前	番号	属性值(※)
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

• タグにより複数のトンネル属性が設定されている場合は、利用可能な値が指定されているもっとも小さなタグの情報 がユーザに割り当てる VLAN 情報として選択されます。

上記の設定条件に従って設定を行う場合の設定例を示します。

MACアドレス認証を設定する

1. 設定メニューの詳細設定で「認証情報」をクリックします。

「認証情報」ページが表示されます。

2. 「MACアドレス認証情報」をクリックします。

「MAC アドレス認証情報」が表示されます。

3. 以下の項目を指定します。

● 認証機能	→使用する
パスワード	→ macauth-pass
パスワードの確認	→ macauth-pass
認証プロトコル	→ CHAP

MACアドL	レス認証情報	3	
 ○ 使用しない ● 使用する 			
認証機能	バスワード		
	バスワードの確認 •••••		
	認証ブロトコル OCHAP OPAP		

4. [保存] ボタンをクリックします。

RADIUS サーバの VLAN を設定する

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 6. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「共通情報」をクリックします。
 共通情報の設定項目と「基本情報」が表示されます。
• VLAN ID

→ 13

	<lan情報追加フィールド></lan情報追加フィールド>
VLAN ID	13

9. [保存] ボタンをクリックします。

10. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

11. 以下の項目を設定します。

- IPアドレス
- ネットマスク →16 (255.255.0.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

→ 172.16.1.101

■IPアドレス情報	3
IPアドレス	172.16.1.101
ネットマスク	16 (255.255.0.0)
フロートキャストアトレス	ネットワークアドレス+オール1 💌

12. [保存] ボタンをクリックします。

RADIUSサーバを接続するポートを設定する

- **13. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- **14.** 「ether 情報」でポート番号が1の [修正] ボタンをクリックします。 ether 1 情報の設定項目と「基本情報」が表示されます。
- 15. 以下の項目を設定します。
 - VLAN
 Untagged

→13

	Tagged	
VLAN	Untagged	13

16. 【保存】ボタンをクリックします。

MAC アドレス認証で認証された Supplicant が接続される VLAN 情報を設定する

17. 手順 13.~16.を参考に、ETHER2~5ポートを設定します。

「ether 2 情報」-「基本設定」

 VLAN Untagged → 10
 「ether 3 情報」 - 「基本設定」
 VLAN Untagged → 11

「ether 4 情報」-「基本設定」		
• VLAN		
Untagged	→ 100	
「ether 5 情報」-「基本設定」		
• VLAN		
Untagged	→123	

MACアドレス認証ポートを設定する

- **18. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- **19.** 「ether 情報」でポート番号が10の [修正] ボタンをクリックします。 ether 10 情報の設定項目と「基本情報」が表示されます。

20. 「MACアドレス認証関連」をクリックします。

MACアドレス認証関連の設定項目と、「基本情報」が表示されます。

- 21. 以下の項目を設定します。
 - 認証機能 →使用する
 参照する AAA 情報 → 0

基本情報				
	 ○ 使用しない ● 使用する 			
	参照するAAA情報	0		
==0=±±±±	認証方式	⊙MACアドレスごと○ボートごと		
でる証L19% Aと 目と	デフォルト割り当て VLAN	1		
	認証成功保持時間	20 分 💙		
	認証失敗保持時間	5 分 💙		
	WOL転送モード	●転送しない●転送する		

- 22. [保存] ボタンをクリックします。
- 23. 手順 18. ~ 22. を参考に、ETHER11、12 ポートを設定します。
 「ether 11 情報」-「MACアドレス認証関連」-「基本情報」
 - ・認証機能
 →使用する
 参照する AAA 情報
 →0

「ether 12 情報」-「MACアドレス認証関連」-「基本情報」

RADIUS サーバを利用する AAA グループ情報を設定する

24. 設定メニューの詳細設定で「AAA 情報」をクリックします。 「AAA 情報」ページが表示されます。

グループ名

→localAuth

<グループID情報追加フィールド>		
グループ名	localAuth	

- 26. [追加] ボタンをクリックします。
- **27.** 手順24.~25.を参考に、グループ名を設定します。
 - グループ名 → radiusAuth
- **28. [追加] ボタンをクリックします**。 「グループID情報(1)」ページが表示されます。
- **29.** 「RADIUS 関連」をクリックします。 RADIUS 関連の設定項目と「基本情報」が表示されます。
- 30. 以下の情報を指定します。

•	RADIUSサービス	→クライアント機能
	認証	→チェックする
	アカウンティング	→チェックしない
•	自側認証 IP アドレス	→ 172.16.1.101



- 31. [保存] ボタンをクリックします。
- **32.** RADIUS **関連の設定項目の「サーバ情報」をクリックします**。 「サーバ情報(クライアント機能)」が表示されます。
- 33. 「認証情報1」の[修正]ボタンをクリックします。
- 34. 以下の項目を指定します。
 - 認証情報1 共有鍵 サーバIPアドレス

→ radius-secret → 172.16.1.100



35. 認証情報1の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

ローカル認証情報を利用する AAA グループ情報を設定する

36. 「AAA ユーザ情報」をクリックします。

AAAユーザ情報の設定項目と「AAAユーザ情報」が表示されます。

- 37. 以下の項目を指定します。
 - ユーザID

→001111000001

	<aaaユーザ情報追加フィールド></aaaユーザ情報追加フィールド>
ユーザID	001111000001

38. [追加] ボタンをクリックします。

「AAAユーザ情報(0)」ページが表示されます。

39. 「認証情報」をクリックします。

認証情報の設定項目と「認証情報」が表示されます。

- 40. 以下の項目を設定します。
 - ユーザID →001111000001
 - ● 認証パスワード
 → macauth-pass

記証情	R []
ユーザID	001111000001
認証バス ワート	•••••
権限クラ ス	●指定しない ●管理者クラス ◎一般ユーザクラス

- 41. [保存] ボタンをクリックします。
- 42. 「サプリカント関連」をクリックします。

サプリカント関連の設定項目と「サプリカント情報」が表示されます。

- 43. 以下の項目を設定します。
 - 割り当てる VLAN ID → 123

■サプリカント情報	3	
割り当てるVLAN ID	123	

- 44. [保存] ボタンをクリックします。
- **45.** 手順 36. ~ 44. を参考に、以下の項目を設定します。 「AAA ユーザ情報(1)」-「認証情報」-「認証情報」
 - ユーザID →002222000002
 - 認証パスワード → macauth-pass

「AAA ユーザ情報(1)」-「サプリカント関連」-「サプリカント情報」

- 割り当てる VLAN ID → 100
- **46. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

13 接続端末数制限機能を使う

適用機種 全機種

接続端末数制限機能を使用すると、簡易的に本装置への不正接続を検出することができます。

こんな事に気をつけて

- 本機能は、不正接続を検出する機能であり、不正接続とみなした端末に対する通信の遮断は行いません。不正な接続 を検出した際に通信を遮断したい場合はポート閉塞モードを有効にしてください。
- ・ IEEE802.1X認証、Web認証およびMACアドレス認証のどれかを有効にしたポートでは、本機能は無効となります。
- リンクアグリゲーションとして設定されたポートでは、本機能は無効となります。

SR-S316C2/716C2の場合を例にします。



● 設定条件

- ETHER5~7ポートで接続端末数制限機能を使用する
- 接続許容端末数 ETHER5、6 ポート :1 ETHER7 ポート :6
- ポート閉塞モード
 ETHER5、6 ポート
 ETHER7 ポート
 : 閉塞する
 : 閉塞しない

上記の設定条件に従って設定を行う場合の設定例を示します。

- **1. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- **2.** 「ether 情報」でポート番号が5の [修正] ボタンをクリックします。 ether 5 情報の設定項目と「基本情報」が表示されます。
- 「MAC 関連」をクリックします。
 MAC 関連の設定項目と「ストーム制御情報」が表示されます。
- MAC 関連の設定項目の「接続端末数制限情報」をクリックします。
 「接続端末数制限情報」が表示されます。

•	接続端末数制限機能	→使用する
	接続許容最大数	→ 1
	ポート閉塞	→する

■接続端末数制限情報		3
接続端末数制限機能	 ● 使用しばい ● 使用する 接続許容最大数 1 ポート閉塞 ●しばい ●する 	

6. [保存] ボタンをクリックします。

7. 手順1.~6.を参考に、ETHER6、7ポートを設定します。
 「ether 6 情報」-「MAC 関連」-「接続端末数制限」

- 8. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

14 ARP 認証機能を使う

適用機種 全機種

ここでは、既存のネットワークに本装置を追加して、ARP 認証を行う場合の設定方法を説明します。

こんな事に気をつけて ARP認証で利用するAAAのグループIDを正しく設定してください。



SR-S324TC1/724TC1の場合を例にします。

● 設定条件

- VLAN10でARP認証を使用する
- ARP認証で利用する認証データベース : RADIUS サーバ
- AAA グループの ID : 0
- RADIUSサーバのIPアドレス : 172.16.1.100
- RADIUSサーバはVLAN20に接続されている
- RADIUSサーバのシークレット : radius-secret
- 認証失敗時の通信妨害を行う
- 通信妨害のためのARPパケット送信間隔 10秒

上記の設定条件に従って設定を行う場合の設定例を示します。

RADIUS サーバの VLAN を設定する

- **1. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「共通情報」をクリックします。
 共通情報の設定項目と「基本情報」が表示されます。

• VL	AN ID	→ 20
■基本	本情報	3
VLAN	I ID	20

- 5. [保存] ボタンをクリックします。
- 6. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 7. 以下の項目を指定します。
 - IPアドレス
 - ネットマスク → 16 (255.255.0.0)
 - ブロードキャストアドレス →ネットワークアドレス+オール1

→ 172.16.1.200

■IPアドレス情報	3
IPアドレス	172.16.1.200
ネットマスク	16 (255.255.0.0)
フロートキャストアトレス	ネットワークアドレス+オール1 🗸

8. [保存] ボタンをクリックします。

RADIUSサーバを接続するポートを設定する

- 設定メニューの詳細設定で「ether 情報」をクリックします。
 「ether 情報」ページが表示されます。
- **10.** 「ether 情報」でポート番号が21の [修正] ボタンをクリックします。 ether 21 情報の設定項目と「基本情報」が表示されます。
- 11. 以下の項目を指定します。
 - VLAN
 Untagged

→20

	Tagged	
VLAN	Untagged	20

12. [保存] ボタンをクリックします。

ARP 認証が動作する VLAN を設定する

- **13. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- **14.** 「ether 情報」でポート番号が1の [修正] ボタンをクリックします。 ether 1 情報の設定項目と「基本情報」が表示されます。

VLAN		
Untagged		→ 10
VLAN	Tagged State	
VLAN	Untagged	10

16. [保存] ボタンをクリックします。

ARP 認証を設定する

- **17. 設定メニューの詳細設定で「VLAN 情報」をクリックします**。 「VLAN 情報」ページが表示されます。
- 18. 以下の項目を指定します。
 - VLAN ID

	<vlan情報追加フィールド></vlan情報追加フィールド>
VLAN ID	10

→10

19. [追加] ボタンをクリックします。

「VLAN10情報」ページが表示されます。

20. 「ARP認証関連」をクリックします。

ARP認証関連の設定項目と、「ARP認証情報」が表示されます。

- 21. 以下の項目を指定します。
 - ARP認証情報 →使用する

"使用する"を選択すると、「参照する AAA 情報」および「通信妨害」の設定項目が表示されます。

 参照する AAA 情報 → 0
 通信妨害 → する 通信妨害間隔 → 10秒

ARP認証情報		3
ARP認証情報	●使用しない ●使用する	
参照するAAA情報	0	
通信妨害	 ○しない ●する 通信妨害間隔10 秒 	

22. [保存] ボタンをクリックします。

RADIUS サーバを利用する AAA グループ情報を設定する

- **23. 設定メニューの詳細設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- 24. 以下の項目を指定します。
 - グループ名

	ブループID情報追加フィール	۲°>
グループ名	RADIUS	

→ RADIUS

25. [追加] ボタンをクリックします。

「グループID情報(0)」ページが表示されます。

26. 「RADIUS 関連」をクリックします。

RADIUS関連の設定項目と「基本情報」が表示されます。

27. 以下の情報を指定します。

RADIUS	サービス	→クライアント機能
認証		→チェックする
アカウン	ティング	→チェックしない
 自側認証 	IPアドレス	→ 172.16.1.200

■基本情報	3
RADIUSサービス	クライアント機能 ✓ ✓ 認証□アカウンティング (クライアント機能を選択した場合にのみ有効 となります)
自側認証IPアドレス	172.16.1.200

- 28. [保存] ボタンをクリックします。
- **29**. RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報(クライアント機能)」が表示されます。

30. 「認証情報1」の[修正] ボタンをクリックします。

31. 以下の項目を指定します。

 認証情報1 共有鍵 → radius-secret サーバIPアドレス → 172.16.1.100

	共有鍵	••••••
	サーバIPア ドレス	172.16.1.100
	サーバ UDPポート	⊙ 1812 ◯ 1645
認証情報 1	復旧待機 時間	0 秒 🗸
	優先度	0
	自側認証 IPアドレス	

32. 認証情報1の[保存]ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

33. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

15 ループ検出機能を使う

適用機種 全機種

ループ検出機能を利用すると、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。

ここではループ検出機能の設定方法を説明します。



● 設定条件

- ループ検出機能を有効にする
- ポート閉塞を行う
- ループ検出用フレームの送信間隔 :1分

上記の設定条件に従って設定を行う場合の設定例を示します。

- 1. 設定メニューの詳細設定で「ループ検出情報」をクリックします。 「ループ検出情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - ループ検出機能 →使用する ループ検出時の動作 →閉塞する ループ検出用フレームの送信間隔 →1分

■基本情報		3
	 ○ 使用しない ● 使用する 	
ルーブ検出機能	ループ検出時の動作	 ○何もしない ○遮断する ●閉塞する
	ループ検出用フレームの送信間隔	1 分 💌
	復日監視回数	60

- 3. [保存] ボタンをクリックします。
- 画面左側の [設定反映] ボタンをクリックします。 4. 設定した内容が有効になります。

こんな事に気をつけて

- 閉塞されたポートは自動では復旧しません。ポートが閉塞された状態から閉塞を解除させたい場合は、「操作メニュー」の「閉塞/閉塞解除」を使用してポート閉塞を解除してください。
- トラフィックが高負荷状態になった場合、ループを検出することができません。ブロードキャスト/マルチキャスト ストーム制御を併用してください。
- ・ 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。
- SR-S208TC2/224TC2/208PD1では、「ether情報」の転送許可ポートを設定したポートが存在する場合、ポートの遮 断は動作しません。

16 ポート・ミラーリング機能を使う



ポート・ミラーリング機能を利用すると、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ことができます。

ここでは、ETHER1ポートをソースポート、ETHER8ポートをターゲット・ポートとして設定し、ソースポートの受信トラフィックをターゲット・ポートへミラーリングする場合の設定方法を説明します。



● 設定条件

- ETHER1 ポートをソースポートとする(受信フレーム指定)
- ETHER8ポートをターゲット・ポートとする

上記の設定条件に従って設定を行う場合の設定例を示します。

- 設定メニューの詳細設定で「ether情報」をクリックします。
 「ether情報」ページが表示されます。
- **2.** 「ether 情報」でポート番号が8の [修正] ボタンをクリックします。 ether 8 情報の設定項目と「基本情報」が表示されます。
- 「ポート種別情報」をクリックします。
 「ポート種別情報」が表示されます。

- ポート種別 →ミラー
 "ミラー"を選択すると、「ミラー情報」の設定項目が表示されます。
- ミラー情報 ソースポート番号 ミラー動作モード

→1 →受信フレームをミラーする

■ポート	種別情報 []
ポート種 別	 ●通常 ●リンクアグリゲーション ●バックアップ ●ミラー
ミラー情 報	 ※追加・修正情報は一覧の入力フィールドで設定してください。 定義番号 ソースボート番号 ミラー動作モード 操作 全削除 <ミラー条件入力フィールド> ソースボート番号 1 ● ○送受信フレームをミラーする ○受信フレームをミラーする ○送信フレームをミラーする ○送信フレームをミラーする ○送信フレームをミラーする

- 5. [追加] ボタンをクリックします。
- 6. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

17 ether L3 監視機能を使う

適用機種 全機種

ether L3 監視機能を使用すると、指定した ETHER ポートから監視相手装置を監視することによって、経路上の 障害を検出および監視をしているポートを閉塞します。

ここでは、ether L3 監視機能を使用する場合の設定方法を説明します。

こんな事に気をつけて

閉塞されたポートは自動では復旧しません。ポートが閉塞された状態から閉塞を解除させたい場合は、「操作メニュー」 の「閉塞/閉塞解除」を使用してポート閉塞を解除してください。

SR-S316C2/716C2の場合を例にします。



● 設定条件

- ETHER1 ポートを使用する
- VLAN ID とネットワークアドレスを以下のように対応付ける VLAN ID:1 ネットワークアドレス: 192.168.10.0/24
- ether L3 監視機能を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

- 1. 設定メニューの詳細設定で「ether情報」をクリックします。

 「ether情報」ページが表示されます。
- **2.** 「ether 情報」でポート番号が1の [修正] ボタンをクリックします。 ether 1 情報の設定項目と「基本情報」が表示されます。

• メディア種別

Untagged

→通常ポート (RJ45)

• VLAN

→1

■基本情報		3
ボート	使用	●使用する●使用しない
<mark>説明文</mark>	τ	
メディ	ア種別	○自動 ● 通常ボート(RJ45) ● SFPボート
通信速度		⊙自動 ◯ 10Mbps ◯ 100Mbps ◯ 1000Mbps
全二重	1/半二重	◎全二重 ○半二重
MDI		●自動 ○ MDI ○ MDI-X
フロ	送信	⊙しない○する
御	受信	⊙する ○しない
	Tagged	
VEAN	Untagged	1

機種によりメディア種別に対応しているポート番号は異なります。

- 4. 【保存】ボタンをクリックします。
- 5. 「接続先監視情報」をクリックします。

「接続先監視情報」ページが表示されます。

6. 以下の項目を指定します。

•	接続先監視	→使用する
	あて先 IP アドレス	→192.168.10.2
	正常時送信間隔	→15秒
	タイムアウト時間	→40秒
	再送間隔	→5秒



- 7. [保存] ボタンをクリックします。
- **8. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 9. 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 10. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

VLAN ID

基本情報 VLAN ID 1

→1

- 12. [保存] ボタンをクリックします。
- 13. [IP 関連]をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

14. 以下の項目を指定します。

- IPアドレス
- ネットマスク → 24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

→ 192.168.10.1

■IPアドレス情報	3
IPアドレス	192.168.10.1
ネットマスク	24 (255.255.255.0)
フロートキャストアトレス	ネットワークアドレス+オール1 🗸

- 15. 【保存】ボタンをクリックします。
- **16. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

「ether情報」

「ether 1 情報」-「基本情報」

- メディア種別 →通常ポート(RJ45)
- VLAN
 Untagged → 1

「LAN情報」

- 「LAN0情報」-「共通情報」-「基本情報」
- VLAN ID → 1

「LAN0情報」-「IP関連」-「IPアドレス情報」

- IPアドレス → 192.168.10.2
- ネットマスク →24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

17.1 リンクアグリゲーション機能を使用した ether L3 監視機能を使う

適用機種 全機種

ここでは、リンクアグリゲーション機能を利用したポートで ether L3 監視機能を使用する場合の設定方法を説明します。

SR-S316C2/716C2の場合を例にします。

● 設定条件

- ETHER1~4ポートを使用する
- メディア種別を通常ポート(RJ45)に変更する
- 通信速度を 1000 Mbps 固定に変更する
- VLAN IDとネットワークアドレスを以下のように対応付ける VLAN ID: 10 ネットワークアドレス: 192.168.10.0/24
- ether L3 監視機能を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

- **1. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - ポートリスト → 1-4

1-4 修正 初期化	+* L			
	$\gamma \gamma = \rho$	1-4	修正	初期化
	リスト			

3. [修正] ボタンをクリックします。

ether 1-4 情報の設定項目と「基本情報」が表示されます。

- メディア種別 →通常ポート(RJ45)
- 通信速度 → 1000Mbps
- VLAN

Tagged

→ 10

■基本情報		3
ボート	使用	●使用する●使用しない
<mark>説明文</mark>		
メディス	ア種別	○自動 ④通常ボート(RJ45) ○ SFPボート
<mark>通信速度</mark> ○自動 ○10Mbps ○100Mbps ⊙1000Mbps		〇自動 ◯10Mbps ◯100Mbps ⊙1000Mbps
全二重	至/半二重	◎全二重 ○半二重
MDI		●自動 ○ MDI ○ MDI-X
フロー制	送信	⊙しない○する
御	受信	⊙する ○しない
	Tagged	10
VEAN	Untagged	

機種によりメディア種別に対応しているポート番号は異なります。

- 5. [保存] ボタンをクリックします。
- 6. 「ポート種別情報」をクリックします。

「ポート種別情報」が表示されます。

- 7. 以下の項目を指定します。
 - ポート種別 →リンクアグリゲーション

■ポート種別情報	
ボート種別	 ○通常 ●リンクアグリゲーション ○バックアップ ○ミラー

- 8. [保存] ボタンをクリックします。
- **9. 設定メニューの詳細設定で「リンクアグリゲーショングループ情報」をクリックします**。 「リンクアグリゲーショングループ情報」ページが表示されます。
- **10.** 「リンクアグリゲーショングループ情報」でグループ番号が1の [修正] ボタンをクリックします。 リンクアグリゲーショングループ1情報の設定項目と「基本情報」が表示されます。
- **11. リンクアグリゲーショングループ1情報の設定項目の「接続先監視情報」をクリックします**。 「接続先監視情報」が表示されます。

•	接続先監視	→使用する
	あて先IPアドレス	→ 192.168.10.2
	正常時送信間隔	→15秒
	タイムアウト時間	→40秒
	再送間隔	→5秒

・使用しない ・ ・ ・	■接続先監視情	報	3
	接続先監視	 使用しない 使用する あて先IPアドレス 192.168.10.2 正常時送信間隔 15 秒 マ タイムアウト時間 40 秒 マ 再送間隔 5 秒 マ 	

- 13. [保存] ボタンをクリックします。
- **14. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **15.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 16. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 17. 以下の項目を指定します。
 - VLAN ID

3

```
■基本情報
VLAN ID 10
```

- 18. [保存] ボタンをクリックします。
- 19.
 [IP 関連]をクリックします。

 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 20. 以下の項目を指定します。
 - IPアドレス → 192.168.10.1
 - ネットマスク →24 (255.255.255.0)
 - ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報	3
IPアドレス	192.168.10.1
ネットマスク	24 (255.255.255.0)
フロートキャストアトレス	ネットワークアドレス+オール1 💌

- 21. [保存] ボタンをクリックします。
- **22. 画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。 「ether情報」 • ポートリスト →1-4 「ether 1-4 情報」-「基本情報」 • メディア種別 →通常ポート (RJ45) 通信速度 → 1000Mbps • VLAN Tagged **→**10 「ether 1-4 情報」-「ポート種別情報」 ポート種別 →リンクアグリゲーション 「LAN情報」 「LAN0情報」-「共通情報」-「基本情報」 • VLAN ID **→**10 「LAN0情報」-「IP関連」-「IPアドレス情報」 • IPアドレス → 192.168.10.2 • ネットマスク →24 (255.255.255.0) ブロードキャストアドレス →ネットワークアドレス+オール1

18 ポート閉塞機能を使う

適用機種 全機種

ポート閉塞機能を利用すると、間欠障害発生時にも接続ポートが閉塞状態を保持するため、安定した通信を保つ ことができます。

ここでは、バックアップポート機能と併用し、マスタポートの間欠障害発生時にはマスタポートを閉塞し、バックアップポートだけを使用する場合を例に説明します。

こんな事に気をつけて

閉塞されたポートは自動では復旧しません。ポートが閉塞された状態から閉塞を解除させたい場合は、「操作メニュー」 の「閉塞/閉塞解除」を使用してポート閉塞を解除してください。



● 設定条件

[本装置1]

- 各装置でETHER1、16ポートをバックアップポートとして使用する (ETHER1をマスタポート、ETHER16をバックアップポートとし、マスタポートを優先的に使用する)
- リンクダウン回数による閉塞を行う
- リンクダウン回数の上限値の設定

[本装置2]

- 各装置でETHER1、16ポートをバックアップポートとして使用する (ETHER1をマスタポート、ETHER16をバックアップポートとし、マスタポートを優先的に使用する)
- リンクダウン回数による閉塞を行う
- リンクダウン回数の上限値の設定

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

- **1. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- [ether 情報] でポート番号が1の [修正] ボタンをクリックします。
 ether 1 情報の設定項目と「基本情報」が表示されます。
- 3. 以下の項目を指定します。
 - リンクダウン回数の上限値 →5

リンクダウン回数の 上限値	5
------------------	---

- 4. [保存] ボタンをクリックします。
- 5. 「ポート種別情報」をクリックします。

「ポート種別情報」ページが表示されます。

- 6. 以下の項目を指定します。
 - ポート種別

→バックアップ

"バックアップ"を選択すると、「バックアップグループ情報」の設定項目が表示されます。

 バックアップグループ情報 グループ番号 優先度

→1 →優先ポート

■ポート種	別情報	3
ボート種別	 ●通常 ●リンクアグリゲーション ●バックアップ ●ミラー 	
バックアッ ブ グルーブ 情報	グルーブ番号 1 ▼ 優先度 ●優先ボート ○待機ボート	

- 7. [保存] ボタンをクリックします。
- 画面上部の「ether 情報」をクリックします。
 「ether 情報」ページが表示されます。
- **9.** 「ether 情報」でポート番号が 16 の [修正] ボタンをクリックします。 ether 16 情報の設定項目と「基本情報」が表示されます。
- 10. 手順5.~7.を参考に、以下の項目を設定します。
 - ポート種別 →バックアップ
 バックアップグループ情報 グループ番号 →1 優先度 →1
- **11. 設定メニューの詳細設定で「バックアップグループ情報」をクリックします**。 「バックアップグループ情報」ページが表示されます。

12. 「バックアップグループ情報」でバックアップグループ番号が1の [修正] ボタンをクリックします。 「バックアップグループ1情報」が表示されます。

13. 以下の項目を指定します。

優先使用ポート → master

	<バックアップグループ情報入力フィールド>			
	1	優先使用ポート	⊙ master○ 先にリンクアップしたボート	
		待機状態	 ⑦閉塞しない ○閉塞する 	

14. [保存] ボタンをクリックします。

15. 画面左側の[設定反映]ボタンをクリックします。

設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

「ether情報」

「ether 1 情報」-「基本情報」 • リンクダウン回数の上限値 →5 「ether 1 情報」-「ポート種別情報」 ポート種別 →バックアップ • バックアップグループ情報 グループ番号 **→**1 優先度 →優先ポート 「ether 16情報」-「ポート種別情報」 ポート種別 →バックアップ • バックアップグループ情報 グループ番号 **→**1 優先度 →待機ポート

「バックアップグループ情報」 「バックアップグループ1情報」

● 優先使用ポート → master

19 LAN をネットワーク間接続する

適用機種 SR-S716C2, 724TC1, 748TC1

ここでは、既存のLAN-Bに新規のLAN-Aをネットワーク間接続し、静的に経路情報を設定する場合を例に説明します。

こんな事に気をつけて

Webユーザーズガイド「1.2 本装置のトップページを表示させる」(P.9)に従って設定した状態からの設定例です。以前 の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

● 参照 トラブルシューティング「3ご購入時の状態に戻すには」(P.24) Webユーザーズガイド「1.2本装置のトップページを表示させる」(P.9)

SR-S716C2の場合を例にします。



• ルーティングプロトコルとして RIP-V1 を使用する

- インターネットにつながるルータ1と、事業所内のその他のネットワークにつながるルータ2が存在し、静的に経路情報を登録する ルータ1のIPアドレス : 192.168.0.5 ルータ2のIPアドレス : 192.168.0.10
- LAN-Cのネットワークアドレス/ネットマスク : 192.168.2.0/24

[その他の条件]

 自動時刻設定にする タイムサーバ サーバ設定 プロトコル

: 使用する : 設定する : TIME プロトコル : 192.168.0.20

∛∑・ヒント =

◆ TIME プロトコル、SNTP とは?

タイムサーバのアドレス

TIME プロトコル (RFC868) はネットワーク上で時刻情報を配布するプロトコルです。SNTP (Simple Network Time Protocol、RFC1361、RFC1769) はNTP (Network Time Protocol)のサブセットで、パソコンなど末端のクライアントマシンの時刻を同期させるのに適しています。

こんな事に気をつけて

- 本装置のIPアドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。
- 「IP 情報」-「基本情報」の「IP フォワーディング機能」の設定を変更した場合は、装置を再起動してください。

上記の設定条件に従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「IP 情報」をクリックします。

「IP情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - IPフォワーディング機能 →使用する

■基本情報		
ARPエントリ有効時間	20 分	
IPフォワーティング機能	○使用しない ⊙使用する	

3. [保存] ボタンをクリックします。

LAN0 情報を設定する

- **1. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- **2. 「**ether **情報」でポート番号が1の [修正]** ボタンをクリックします。 ether 1 情報の設定項目と「基本情報」が表示されます。
- 3. 以下の項目を指定します。
 - メディア種別 →通常ポート(RJ45)
 - VLAN
 Untagged

→1

■基本	■基本情報		
ボート使用		⊙使用する○使用しない	
<mark>説明文</mark>	τ		
メディ	ア種別	○自動 ● 通常ボート(RJ45) ● SFPボート	
通信递	度		
全二重/半二重		◎全二重 ○半二重	
MDI		●自動 ○ MDI ○ MDI-X	
フロ、送信		⊙したい ○する	
御受信		⊙する ○しない	
	Tagged		
VLAN	Untagged	1	

機種によりメディア種別に対応しているポート番号は異なります。

- 4. 【保存】ボタンをクリックします。
- 5. 「ether 情報」でポート番号が2の [修正] ボタンをクリックします。 ether 2 情報の設定項目と「基本情報」が表示されます。
- 6. 手順3.~4.を参考に、以下の項目を設定します。
 - メディア種別 →通常ポート(RJ45)
 - VLAN
 Untagged →2
- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 8. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。

• IPアドレス

- →192.168.0.1
- ネットマスク →24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報		
IPアドレス	192.168.0.1	
ネットマスク	24 (255.255.255.0)	
フロートキャストアトレス	ネットワークアドレス+オール1 🗸	

11. [保存] ボタンをクリックします。

12. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

13. 以下の項目を指定します。

- RIP送信 → V1 で送信する
- • RIP受信
 → V1 で受信する
- メトリック値 →0

■RIP情報	Į	3
RIP送信	 ○送信しない ○V1で送信する ○V2で送信する ○V2(Multicast)で送信する 	
RIP受信	●受信しない ●V1で受信する ●V2、V2(Multicast)で受信する	
《 RIP 送信時は加算するメトリック値を設定してください。》 メトリック値		

14. 【保存】ボタンをクリックします。

15. IP 関連の設定項目の「スタティック経路情報」をクリックします。

→1

「スタティック経路情報」が表示されます。

- 16. 以下の項目を指定します。
 - ネットワーク →デフォルトルート
 中継ルータアドレス → 192.168.0.5
 - メトリック値 →1
 - 優先度



- 17. [追加] ボタンをクリックします。
- 18. 手順 16.~17.を参考に、以下の項目を設定します。
 - ネットワーク
 ネットワーク指定
 あて先IPアドレス
 → 192.168.2.0
 → 24 (255.255.255.0)
 → 192.168.0.10
 メトリック値
 → 1
 優先度
 → 1
- 19. IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP情報」が表示されます。

20. 以下の項目を指定します。

DHCP機能

→使用しない

■DHCP情報				
	 ● 使用しない ● リレー機能を使用する ■ DHCPサーバIPアドレ ス1 ■ DHCPサーバIPアドレ ス2 			
機能	ロホストデータベース AAA 参照するAAA情報 認証プロトコル ③CHAP ○ PAP			
	○ サーバ機能を使用する			

21. [保存] ボタンをクリックします。

LAN1 情報を設定する

1. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - VLAN ID

<lan情報追加フィールド></lan情報追加フィールド>		
VLAN ID	2	

→2

- 【追加】ボタンをクリックします。
 「LAN1 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 5. 以下の項目を指定します。
 - IPアドレス → 192.168.1.1
 - ネットマスク →24 (255.255.255.0)
 - ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス 情報	3
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0)
フロートキャストアトレス	ネットワークアドレス+オール1 🔽

- 6. [保存] ボタンをクリックします。
- 7. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

- 8. 以下の項目を指定します。
 - RIP送信 → V1 で送信する
 - RIP受信 → V1 で受信する
 - メトリック値 →0

RIP情報		3	
RIP送信	 ○送信しない ○V1で送信する ○V2で送信する ○V2(Multicast)で送信する 		
RIP受信	○受信しない ●V1で受信する ●V2、V2(Multicast)で受信する		
《 RIP 送信時は加算するメトリック値を設定してください。》 <mark>メトリック値</mark>			

9. [保存] ボタンをクリックします。

10. IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP情報」が表示されます。

11. 以下の項目を指定します。

٠	DHCP機能	→サーバ機能を使用する
	割当て先頭IPアドレス	→ 192.168.1.2
	割当てアドレス数	→253
	リース期間	→1日
	デフォルトルータ広報	→192.168.1.1
	DNSサーバ広報	→192.168.1.1
	セカンダリ DNS サーバ広報	→指定しない
	ドメイン名広報	→指定しない
	MACアドレスチェック	→指定しない

	⊙ サーバ機能を使用する			
DUOD	割当て先頭IPアド レス	92.168.1.2		
機能	割当てアドレス数 28	53		
	リース期間 1			
	デフォルトルータ広 報	92.168.1.1		
	DNSサーバ広報 19	92.168.1.1		
	セカンダリDNSサ ーバ広報			
	ドメイン名広報			
	MACアドレスチェッ]ホストデータベース]AAA		
	2	参照するAAA情報		
		認証プロトコル OCHAP OPAP		
	※"割当て先頭アドレス ークアドレス内であるこ	、"が本装置のIPアドレスと同じネットワ とを確認してください。		

12. 【保存】ボタンをクリックします。

自動時刻を設定する

- 設定メニューの基本設定で「装置情報」をクリックします。
 「装置情報」ページが表示されます。
- 「タイムサーバ情報」をクリックします。
 「タイムサーバ情報」が表示されます。
- 3. 以下の項目を指定します。
 - タイムサーバ機能 →使用する
 - サーバ設定 プロトコル → TIME プロトコル
 タイムサーバIPアドレス → 192.168.0.20

■タイムサ・	■タイムサーバ情報		3
タイムサーバ	「機能	●使用しない ●使用する	
サーバ設定	ブロトコル	 ● TIMEプロトコル ● SNTPプロトコル 	
	タイムサーバIPアドレス	192.168.0.20	

- 4. [保存] ボタンをクリックします。
- 5. **画面左側の [再起動] ボタンをクリックします**。 装置の再起動後、設定した内容が有効になります。

20 IPv4のネットワークに IPv6 ネットワークを追加 する



ここでは、IPv4で通信しているネットワーク環境にIPv6ルーティング設定を追加する例について説明します。



● 設定条件

[LAN-A側]

- プレフィックス/プレフィックス長
- RA送信を行う
- VLANはタグなし

[LAN-B側]

プレフィックス/プレフィックス長

: 2001:db8:1111:1000::/64

: 2001:db8:1111:1001::/64

- RA送信を行う
- VLAN はタグなし

こんな事に気をつけて

- IPv4のネットワークをすでに使用している場合の設定例です。新規に IPv6 だけのネットワーク構成を設定する場合は、ether ポートへの VLAN 設定などが必要になります。
- 「IPv6 情報」-「基本情報」の「IPv6 フォワーディング機能」の設定を変更した場合は、装置を再起動してください。

上記の設定条件に従って設定を行う場合の設定例を示します。

IPv6フォワーディング機能を設定する

- 設定メニューの詳細設定で「IPv6 情報」をクリックします。
 「IPv6 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - IPv6 フォワーディング機能 →使用する
 基本情報
- 3. [保存] ボタンをクリックします。

IPv6フォワーディンク機能

LAN0 情報を設定する

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。
 「LAN0 情報」ページが表示されます。

| ○ 使用しない ⊙ 使用する

3

「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

- IPv6
- インタフェースID
 ロのマードレス
- IPv6アドレス アドレスまたはプレフィックス
- ルータ広報 プレフィックス Valid Lifetime Pref. Lifetime フラグ

→使用する
 →自動
 →ユニキャストアドレスを指定する
 → 2001:db8:1111:1000::
 →送信する
 → 2001:db8:1111:1000::
 →期限あり 30日
 →期限あり 7日

フラグ →c0 ■IPv6基本情報 3 IPv6 ○使用しない ⊙使用する ◉自動 インタフェースID ○指定する ○ルータ広報で受信したブレフィックスを使用する ⊙ ユニキャストアドレスを指定する アドレスまたはプ IPv6アドレス 2001:db8:1111:1000:: レフィックス ○ エニキャストアドレスを指定する アドレス

	 ○ 使用しない ○ 受信する ○ 送信する 	
	最大送信間隔 600 秒	
	最小送信間隔 200 秒	
	Router Lifetime 1800 秒	
	MTU	
山、石广却	Reachable Time 0 ミリ秒	
ルーメル報	Retrans Timer 0 ミリ秒	
	Cur Hop Limit 64	
	フラグ 00	
	プレフィックス 2001:db8:1111:1000::	Ī
	●期限なし Valid Lifetime 30 日 ▼	
	●期限なし Pref. Lifetime 7 日 ▼	
	フラグ 0	

5. [保存] ボタンをクリックします。

LAN1情報を設定する

 1. 設定メニューの詳細設定で「LAN 情報」をクリックします。

 「LAN 情報」ページが表示されます。

- **2.** 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。 「LAN1 情報」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
- 4. 以下の項目を指定します。
 - IPv6
 - インタフェースID
 - IPv6アドレス アドレスまたはプレフィックス
 - ルータ広報 プレフィックス Valid Lifetime Pref. Lifetime フラグ

→使用する
→自動
→ユニキャストアドレスを指定する
→ 2001:db8:1111:1001::
→送信する
→ 2001:db8:1111:1001::
→期限あり 30 日
→期限あり 7 日
→ c0





- 5. [保存] ボタンをクリックします。
- 6. **画面左側の【再起動】ボタンをクリックします**。 装置の再起動後、設定した内容が有効になります。
21 RIPを使用したネットワークを構築する(IPv4)

適用機種 SR-S716C2, 724TC1, 748TC1

ここでは、RIPv2を使用したダイナミックルーティングのネットワーク設定について説明します。



● 前提条件

- すべてのインタフェースに IP アドレスの設定がされている
- IP フォワーディング機能を使用する設定がされている

● 設定条件

- LANOのネットワークは、RIPネットワークに広報する
- LAN1でRIPv2を使用する
- LAN2でRIPv2を使用する
- LAN3 でルータ2 を経由するネットワークはスタティック経路で設定し、このスタティック経路を RIP ネット ワークに広報する

上記の設定条件に従って設定を行う場合の設定例を示します。

RIP基本情報を設定する

- **1. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。 「LAN1 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4. IP 関連の設定項目の「RIP 情報」をクリックします**。 「RIP 情報」が表示されます。
- 5. 以下の項目を指定します。
 - ● RIP送信
 → V2 (Multicast) で送信する
 - RIP受信 →V2、V2 (Multicast) で受信する
 - メトリック値 →0
 - 認証パケット →破棄しない
 パスワード →指定しない

RIP情報	3	
RIP送信	 ○送信しない ○V1で送信する ○V2で送信する ⊙V2(Multicast)で送信する 	
RIP受信	○受信しない ○V1で受信する ⊙V2、V2(Multicast)で受信する	
《 RIP 送信時は加算する	5メトリック値を設定してください。》	
メトリック値	0 💌	
《 RIP V2使用時で認証/	「ケットを破棄しない時(まRIP V2バスワードを設定し	てください。》
認証バケット	 ○ 破棄する ③ 破棄しない パスワード 	

6. [保存] ボタンをクリックします。

7. 手順2.~6.を参考に、LAN2情報を設定します。

「LAN2情報」-「IP関連」-「RIP情報」

- RIP送信 → V2 (Multicast) で送信する
 RIP受信 → V2、V2 (Multicast) で受信する
- メトリック値 →0
- 認証パケット →破棄しない
 パスワード →指定しない

ルータ2を経由する経路をスタティック経路で設定する

- **8. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **9.** 「LAN 情報」でインタフェースがLAN3の【修正】ボタンをクリックします。 「LAN3 情報」ページが表示されます。
- **10.** 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- **11.** IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。
- 12. 以下の項目を指定します。
 - ネットワーク
 ネットワーク指定
 あて先IPアドレス
 →10.3.1.0
 →24 (255.255.255.0)
 中継ルータアドレス
 →10.1.3.2
 - メトリック値 →1
 優先度 →1

	<スタティック経路情報入力フィールド>
	 デフォルトルート 中継ルータアドレス
ネットワーク	 ○ ネットワーク指定 あて先IPアドレス 10.3.1.0 あて先マドレフマフク 24 (255 255 2)
	め (元) ドレスマスク 24 066.266.266.07 ▼ 中継ルータアドレス 10.1.3.2
メトリック値	1 🗸
優先度	1

13. [追加] ボタンをクリックします。

RIPへの再配布経路を設定する

- **14. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **15.** 「ルーティングマネージャ情報」をクリックします。 ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。
- 16. 以下の項目を指定します。
 - RIP
 インタフェース経路情報 →再配布する
 スタティック経路情報 →再配布する

■再配布情報		3	
	インタフェース経路情報	○再配布しない ⊙再配布する	
RIP	スタティック経路情報	○再配布しない⊙再配布する	

17. [保存] ボタンをクリックします。

18. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

☆
ヒント

◆ RIP ユニキャスト送信

RIPの経路広報は通常マルチキャスト/ブロードキャストパケットを使用して行われますが、ユニキャストフレームを使用して広報することができます。

ユニキャスト送信は、以下の画面で設定します。

- 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→ [RIP 関連]
 - → [RIPユニキャスト送信情報]
- 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[RIP 情報]

ユニキャスト送信先に対して、加算メトリック、認証機能およびRIP機能を使用する場合は、送信先ネットワークが属するインタフェースの設定を行います。

◆ RIP マルチパス機能

RIPを利用した冗長ネットワークで通信経路に障害が発生した場合は、ルーティングテーブルから障害経路が削除されても、新しい経路情報をRIP定期広報などで受信するまでは経路が切り替わりません。そこで、マルチパス機能を利用し、バックアップ経路として冗長な経路を1つ保持することで、障害経路が削除された直後に経路を切り替えることができます。

マルチパス機能は、以下の画面で設定します。

- 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→ [RIP 関連] → [RIP マルチパス情報]

こんな事に気をつけて

- 本装置の初期設定では、インタフェース経路とスタティック経路をRIPに再配布する設定となっています。再配布が 不要な場合は、再配布しない設定を行ってください。
- メトリック値が同じ冗長経路を受信した場合、先に受信した RIP 経路を優先経路として扱います。 ECMP としては動作しません。
- ・ 複数のインタフェースでRIPを利用する場合、以下の条件式の範囲で広報RIPパケット数を設計してください。 条件式 : 広報RIPパケット数×RIP利用インタフェース数≪243 広報RIPパケット数は、広報RIP経路数を25で割り、小数点以下を切り上げた値です。広報RIP経路数は、経路 フィルタにより減らすことができます。「広報RIPパケット数×RIP利用インタフェース数」の値は、本装置が集中 して受信するRIPパケット数であり、この値が243に近ければRIP受信パケットの破棄など通信に影響が出る場合が あります。このため、243よりも十分小さくなるように設計してください。 なお、破棄されたパケット数は、統計情報表示(show ip traffic udp)の統計値「dropped due to full socket buffers」 で確認できます。

22 RIPの経路を制御する(IPv4)

適用機種 SR-S716C2, 724TC1, 748TC1

本装置を経由して、ほかのルータに送受信する経路情報に対して、IPアドレスや方向を組み合わせて指定するこ とによって、特定のあて先への経路情報だけを広報する、または不要な経路情報を遮断することができます。

経路情報のフィルタリング条件

対象となる経路情報

• RIPによる経路情報

指定条件

本装置では、以下の条件を指定することによって、経路情報を制御することができます。

- 動作
- 方向
- フィルタリング条件(IPアドレス/アドレスマスク)
- メトリック値

メトリック値は指定メトリック値の経路情報をフィルタリングするのではなく、フィルタリング後の経路情報のメト ※トリック値は指定メトリック値の経路時報をフィルフラフラッシンにいる、、、アルンフランクシンでは、

通辺 リック値を変更する場合に指定します。0を指定すると変更は行いません。経路情報のフィルタリング条件にすべて以 外を指定した場合に有効です。送信方向のメトリック値に1~16を指定した場合、インタフェースに設定したRIPの 加算メトリック値は加算されません。

∛♡`**ヒント** =

◆ IP アドレスとアドレスマスクの決め方

フィルタリング条件の要素には、「IPアドレス」と「アドレスマスク」があります。制御対象となる経路情報は、 経路情報のIPアドレスとアドレスマスクが指定したIPアドレスとアドレスマスクと一致したものだけです。

例) 指定値 : 172.21.0.0/16の場合

> 経路情報 : 172.21.0.0/16は制御対象となる

172.21.0.0/24 は制御対象とならない

また、フィルタリング条件のIPアドレスと指定したIPアドレスが、指定したアドレスマスクまで一致した場 合に制御対象とすることもできます。

指定值	:172.21.0.0/16 の場合
経路情報	:172.21.0.0/24は制御対象となる
	172.21.10.0/24は制御対象となる

こんな事に気をつけて

RIPv1を使用している場合もアドレスマスクの設定が必要です。この場合、インタフェースのアドレスマスクを指定して ください。また、アドレスクラスが異なる経路情報を制御する場合は、ナチュラルマスク値を指定してください。 例) 192.168.1.1/24 が設定されているインタフェースで 10.0.0.0の経路情報を制御する場合は、10.0.0.0/8を指定します。

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の2つがあります。

- A.特定の条件の経路情報だけを透過させ、その他はすべて遮断する
- B.特定の条件の経路情報だけを遮断し、その他はすべて透過させる

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する
- また、設計方針 Bの例として、以下の設定例について説明します。
- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

こんな事に気をつけて

- フィルタリング条件には、優先度を示す定義番号があり、小さい値ほど、より高い優先度を示します。
- RIP受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しないRIP経路情報は 遮断されます。
- RIP送信時には、優先順位の高い定義から順に送信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、送信方向のすべての条件に一致しないRIP経路情報は 遮断されます。

22.1 特定の経路情報の送信を許可する

適用機種 SR-S716C2, 724TC1, 748TC1

ここでは、本装置からルータへのデフォルトルートの送信だけを許可し、それ以外の経路情報の送信を禁止する 場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPアドレスとRIPv2を使用する設定がされている
- IP フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置からルータへのデフォルトルートの送信だけを許可
- その他はすべて遮断

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。 「RIP フィルタリング情報」が表示されます。

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →デフォルトルート
- メトリック値 →指定しない



6. [追加] ボタンをクリックします。

方向

- 7. 手順5.~6.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - →送信
 - フィルタリング条件 →すべて
 - メトリック値 →指定しない

8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

22.2 特定の経路情報のメトリック値を変更して送信する

<u>適用機種</u> SR-S716C2, 724TC1, 748TC1

ここでは、本装置がルータ2へ192.168.10.0/24、メトリック値1の経路情報を送信する場合の設定方法を説明します。

なお、本装置は、ルータ1から192.168.10.0/24のメトリック値10と192.168.20.0/24のメトリック値1の経路情報を受信するものとします。



● 前提条件

- すべてのインタフェースに IP アドレスと RIPv2 を使用する設定がされている
- IPフォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置から 192.168.10.0/24 の送信を許可する場合、メトリック値1 に変更
- 192.168.10.0/24 以外の経路情報は、メトリック値を変更しない

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。 「LAN1 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします**。 「RIP フィルタリング情報」が表示されます。

•	動作	→透過
•	方向	→送信
•	フィルタリング条件	→経路情報指定
	検索条件	→完全に一致
	IPアドレス	→ 192.168.10.0
	アドレスマスク	→24 (255.255.255.0)
•	メトリック値	→ 1

<ripフィルタリング情報入力フィールド></ripフィルタリング情報入力フィールド>		
動作	 ●透過 ○遮断 	
方向	○受信⊙送信	
フィルタリング条件	 すべて デフォルトルート 経路情報指定 検索条件 ○完全に一致 マスクした結果が一致 IPアドレス IP2.168.10.0 アドレスマスク 24 (255.255.25.0) 	
メトリック値	1	

6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を設定します。

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →すべて
- メトリック値 →指定しない

8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

- ・ 送信方向でメトリック値が設定されている場合、インタフェースのRIP加算メトリック値の加算は行われません。
- 送信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。

22.3 特定の経路情報の受信を許可する

適用機種 SR-S716C2, 724TC1, 748TC1

ここでは、本装置はルータからデフォルトルートの受信だけを許可し、それ以外の経路情報の受信を禁止する場 合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPアドレスとRIPv2を使用する設定がされている
- IP フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

- **1. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。 「RIP フィルタリング情報」が表示されます。

- 動作 →透過
- 方向 →受信
- フィルタリング条件 →デフォルトルート
- メトリック値 →指定しない

<ripフィルタリング情報入力フィールド></ripフィルタリング情報入力フィールド>		
動作	⊙透過 ○遮断	
方向	⊙受信○送信	
フィルタリング条件	 すべて デフォルトルート 経路情報指定 検索条件 ⑦完全に一致 マスクした結果が一致 IPアドレス アドレスマスク 0 00000 ♥ 	
メトリック値		

- 6. [追加] ボタンをクリックします。
- 7. 手順5.~6.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - 方向 →受信
 - フィルタリング条件 →すべて
 - メトリック値 →指定しない
- 8. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

22.4 特定の経路情報のメトリック値を変更して受信する

<u>適用機種</u> SR-S716C2, 724TC1, 748TC1

ここでは、本装置が、ルータ1とルータ2から同じあて先への経路情報192.168.10.0/24を受信した場合に、ルータ1から受信した経路情報を採用する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースに IP アドレスと RIPv2 を使用する設定がされている
- IP フォワーディング機能を使用する設定がされている

● フィルタリング設計

- ルータ1から、192.168.10.0/24の経路情報を受信した場合、メトリック値1に変更
- ルータ2から、192.168.10.0/24の経路情報を受信した場合、メトリック値5に変更
- 上記以外の経路情報は、メトリック値を変更しない

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。
 「RIP フィルタリング情報」が表示されます。

•	動作	→透過
•	方向	→受信
•	フィルタリング条件	→経路情報指定
	検索条件	→完全に一致
	IPアドレス	→ 192.168.10.0
	アドレスマスク	→24 (255.255.255.0)
•	メトリック値	→ 1

<ripフィルタリング情報入力フィールド></ripフィルタリング情報入力フィールド>		
動作	⊙透過 ○遮断	
方向	⊙受信○送信	
フィルタリング条件	 すべて デフォルトルート 経路情報指定 検索条件 ⑦完全に一致 マスクした結果が一致 IPアドレス 192.168.10.0 アドレスマスク 24 (255.265.265.0) 	
メトリック値	1	

6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を設定します。

- 動作 →透過
- 方向 →受信
- フィルタリング条件 →すべて
- メトリック値 →指定しない
- **8. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **9.** 「LAN 情報」でインタフェースが LAN1 の [修正] ボタンをクリックします。 「LAN1 情報」ページが表示されます。
- **10.** 「IP 関連」をクリックします。 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 11. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIPフィルタリング情報」が表示されます。

- 12. 手順5.~6.を参考に、以下の項目を設定します。
 - 動作 →透過
 - 方向 →受信
 フィルタリング条件 →経路情報指定 検索条件 →完全に一致
 IPアドレス → 192.168.10.0
 アドレスマスク → 24 (255.255.2)
 メトリック値 →5

13. 手順5.~6.を参考に、以下の項目を設定します。

- 動作 →透過
 方向 →受信
 フィルタリング条件 →すべて
- メトリック値 →指定しない

14. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

受信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。

22.5 特定の経路情報の送信を禁止する

<u>適用機種</u> SR-S716C2, 724TC1, 748TC1

ここでは、本装置からルータへの10.20.30.0/24の送信を禁止し、それ以外の経路情報の送信を許可する場合の 設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPアドレスとRIPv2を使用する設定がされている
- IP フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置からルータへの10.20.30.0/24の送信を禁止
- その他はすべて透過

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします**。 「RIP フィルタリング情報」が表示されます。

•	動作	→遮断
•	方向	→送信
•	フィルタリング条件	→経路情報指定
	検索条件	→完全に一致
	IPアドレス	→ 10.20.30.0
	アドレスマスク	→24 (255.255.255.0)
•	メトリック値	→指定しない

→指定しない

<ripフィルタリング情報入力フィールド></ripフィルタリング情報入力フィールド>		
動作	○透過 ◉遮断	
方向	○受信⊙送信	
フィルタリング条件	 すべて デフォルトルート 経路情報指定 検索条件 ○完全に一致 マスクした結果が一致 IPアドレス 10.20.30.0 アドレスマスク 24 (255.255.255.0) 	
メトリック値		

[追加] ボタンをクリックします。 6.

7. 手順5.~6.を参考に、以下の項目を設定します。

- 動作 →透過
- →送信 方向
- →すべて • フィルタリング条件
- メトリック値 →指定しない
- 画面左側の [設定反映] ボタンをクリックします。 8. 設定した内容が有効になります。

22.6 特定の経路情報の受信を禁止する

<u>適用機種</u> SR-S716C2, 724TC1, 748TC1

ここでは、本装置は、ルータから10.20.30.0/24の経路情報の受信を禁止し、それ以外の経路情報の受信を許可 する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPアドレスとRIPv2を使用する設定がされている
- IPフォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置は10.20.30.0/24の受信を禁止
- その他はすべて透過

- 1. 設定メニューの詳細設定で「LAN 情報」をクリックします。

 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします**。 「RIP フィルタリング情報」が表示されます。

٠	動作	→遮断
•	方向	→受信
•	フィルタリング条件	→経路情報指定
	検索条件	→完全に一致
	IPアドレス	→ 10.20.30.0
	アドレスマスク	→24 (255.255.255.0)
•	メトリック値	→指定しない

<ripフィルタリング情報入力フィールド></ripフィルタリング情報入力フィールド>			
動作	○透過 ⊙遮断		
方向	⊙受信○送信		
フィルタリング条件	 すべて デフォルトルート 経路情報指定 検索条件 ⑦完全に一致 マスクレた結果が一致 IPアドレス ID20.30.0 アドレスマスク 24 (255.255.255.0) 		
メトリック値			

6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を設定します。

- 動作 →透過
- 方向 →受信
- フィルタリング条件 →すべて
- メトリック値 →指定しない
- 8. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

RIPの経路を制御する(IPv6) 23

適用機種 SR-S724TC1, 748TC1

本装置を経由して、ほかのルータに送信する経路情報や、ほかのルータから受信する経路情報に対して、経路情 報や方向を組み合わせて指定することによって、特定のあて先への経路情報だけを広報する、または、不要な経 路情報を遮断することができます。

経路情報のフィルタリング条件

対象となる経路情報

RIPによる経路情報(IPv6)

指定条件

本装置では、以下の条件を指定することによって、経路情報を制御することができます。

- 動作
- 方向
- フィルタリング情報(プレフィックス/プレフィックス長)
- メトリック値



メトリック値は指定メトリック値の経路情報をフィルタリングするのではなく、フィルタリング後の経路情報のメト 構図 リック値を変更する場合に指定します。0を指定すると変更は行いません。経路情報のフィルタリング条件にすべて以 外を指定した場合に有効です。送信方向のメトリック値に1~16を指定した場合、インタフェースに設定したRIPの 加算メトリック値は加算されません。

∛♡⁻ヒント =

◆ プレフィックスとプレフィックス長の決め方

経路情報

フィルタリング条件の要素には、「プレフィックス」と「プレフィックス長」があります。制御対象となる経 路情報は、経路情報のプレフィックスとプレフィックス長が指定したプレフィックスとプレフィックス長と一 致したものだけです。

例) 指定値 : 2001:db8:1111::/32の場合

: 2001:db8:1111::/32は制御対象となる

2001:db8:1111::/64は制御対象とはならない

また、経路情報のプレフィックスと指定したプレフィックスが、指定したプレフィックス長まで一致した場合 に制御対象とすることもできます。

指定値	:2001:db8::/16 の場合
経路情報	:2001:db8::/32は制御対象となる
	2001:db8:1111::/32は制御対象となる

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の2つがあります。

- A.特定の条件の経路情報だけを透過させ、その他はすべて遮断する
- B.特定の条件の経路情報だけを遮断し、その他はすべて透過させる

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する
- また、設計方針 Bの例として、以下の設定例について説明します。
- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

こんな事に気をつけて

- フィルタリング条件には、優先度を示す定義番号があり、小さい値ほど、より高い優先度を示します。
- RIP受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しないRIP経路情報は 遮断されます。
- RIP送信時には、優先順位の高い定義から順に送信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、送信方向のすべての条件に一致しないRIP経路情報は 遮断されます。

23.1 特定の経路情報の送信を許可する

適用機種 SR-S724TC1, 748TC1

ここでは、本装置からルータへのデフォルトルートの送信だけを許可し、それ以外の経路情報の送信を禁止する 場合の設定方法を説明しています。



● 前提条件

- すべてのインタフェースに IPv6 機能と RIP (IPv6)を使用する設定がされている
- IPv6 フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置からルータへのデフォルトルートの送信だけを許可
- その他はすべて遮断

- **1. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
- **4.** IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。 「IPv6 RIP フィルタリング情報」が表示されます。

- 動作 →透過
 方向 →送信
- フィルタリング条件 →デフォルトルート
- メトリック値 →指定しない



- 6. [追加] ボタンをクリックします。
- 7. 手順5.~6.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - 方向 →送信
 - フィルタリング条件 →すべて
 - メトリック値 →指定しない
- 8. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

23.2 特定の経路情報のメトリック値を変更して送信する

適用機種 SR-S724TC1, 748TC1

ここでは、本装置がルータ2へ2001:db8:1111::/64、メトリック値1の経路情報を送信する場合の設定方法を説明します。

なお、本装置は、ルータ1から2001:db8:1111::/64のメトリック値10と2001:db8:2222::/64のメトリック値1の 経路情報を受信するものとします。



● 前提条件

- すべてのインタフェースにIPv6機能とRIP(IPv6)を使用する設定がされている
- IPv6フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置から2001:db8:1111::/64の送信を許可する場合、メトリック値1に変更
- 2001:db8:1111::/64以外の経路情報は、メトリック値を変更しない

- **1. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。 「LAN1 情報」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
- **4.** IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。 「IPv6 RIP フィルタリング情報」が表示されます。

- 動作 →透過
 方向 →送信
 フィルタリング条件 →経路情報指定 検索条件 →完全に一致 プレフィックス/プレフィックス長 →2001:db8:1111::/64
- メトリック値



- 6. [追加] ボタンをクリックします。
- 7. 手順5.~6.を参考に、以下の項目を設定します。

•	動作	→透過
•	方向	→送信
•	フィルタリング条件	→すべて
•	メトリック値	→指定しない

8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

- ・ 送信方向でメトリック値が設定されている場合、インタフェースのRIP加算メトリック値の加算は行われません。
- ・ 送信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。

→1

23.3 特定の経路情報の受信を許可する

適用機種 SR-S724TC1, 748TC1

ここでは、本装置はルータからデフォルトルートの受信だけを許可し、それ以外の経路情報の受信を禁止する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースに IPv6 機能と RIP (IPv6)を使用する設定がされている
- IPv6 フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

- **1. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
- **4.** IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。 「IPv6 RIP フィルタリング情報」が表示されます。

- 動作 →透過
 方向 →受信
- フィルタリング条件 →デフォルトルート
- メトリック値 →指定しない



- 6. [追加] ボタンをクリックします。
- 7. 手順5.~6.を参考に、以下の項目を設定します。
 - 動作 →遮断
 - 方向 →受信
 - フィルタリング条件 →すべて
 - メトリック値 →指定しない
- 8. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

23.4 特定の経路情報のメトリック値を変更して受信する

適用機種 SR-S724TC1, 748TC1

ここでは、本装置が、ルータ1とルータ2から同じあて先への経路情報2001:db8:1111::/64を受信した場合に、 ルータ1から受信した経路情報を採用する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPv6機能とRIP(IPv6)を使用する設定がされている
- IPv6フォワーディング機能を使用する設定がされている

● フィルタリング設計

- ルータ1から、2001:db8:1111::/64の経路情報を受信した場合、メトリック値1に変更
- ルータ2から、2001:db8:1111::/64の経路情報を受信した場合、メトリック値5に変更
- 上記以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合の設定例を示します。

1. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

- **2.** 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
- **4.** IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。 「IPv6 RIP フィルタリング情報」が表示されます。

 動作 →透過
 方向 →受信
 フィルタリング条件 →経路情報指定 検索条件 →完全に一致 プレフィックス/プレフィックス長 →2001:db8:1111::/64

→ 1

• メトリック値



- 6. [追加] ボタンをクリックします。
- 7. 手順5.~6.を参考に、以下の項目を設定します。

•	動作	→透過
•	方向	→受信
•	フィルタリング条件	→すべて
•	メトリック値	→指定しない

8. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

- **9.** 「LAN 情報」でインタフェースが LAN1 の [修正] ボタンをクリックします。 「LAN1 情報」ページが表示されます。
- **10.** 「IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

- **11.** IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。 「IPv6 RIP フィルタリング情報」が表示されます。
- 12. 手順5.~6.を参考に、以下の項目を設定します。

•	動作	→透過
•	方向	→受信
•	フィルタリング条件 検索条件 プレフィックス/プレフィックス長	→経路情報指定 →完全に一致 →2001:db8:1111::/64
•	メトリック値	→ 5

13. 手順5.~6.を参考に、以下の項目を指定します。

•	動作	→透過
•	方向	→受信
•	フィルタリング条件	→すべて
•	メトリック値	→指定しない

14. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

受信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。

23.5 特定の経路情報の送信を禁止する

適用機種 SR-S724TC1, 748TC1

ここでは、本装置からルータへの2001:db8:1111::/64の送信を禁止し、それ以外の経路情報の送信を許可する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースに IPv6 機能と RIP (IPv6)を使用する設定がされている
- IPv6フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置からルータへの2001:db8:1111::/64の送信を禁止
- その他はすべて透過

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
- **4. IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします**。 「IPv6 RIP フィルタリング情報」が表示されます。

動作

٠

٠

- →遮断 →送信 方向 フィルタリング条件 検索条件 プレフィックス/プレフィックス長
- メトリック値

→経路情報指定 →完全に一致 →2001:db8:1111::/64 →指定しない



6. [追加] ボタンをクリックします。

手順5.~6.を参考に、以下の項目を設定します。 7.

- 動作 →透過 →送信 方向 →すべて • フィルタリング条件 メトリック値 →指定しない
- 画面左側の [設定反映] ボタンをクリックします。 8.

設定した内容が有効になります。

23.6 特定の経路情報の受信を禁止する

適用機種 SR-S724TC1, 748TC1

ここでは、本装置は、ルータから2001:db8:1111::/64の経路情報の受信を禁止し、それ以外の経路情報の受信を 許可する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースに IPv6 機能と RIP (IPv6)を使用する設定がされている
- IPv6フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置は2001:db8:1111::/64の受信を禁止
- その他はすべて透過

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
- 4. IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。 「IPv6 RIP フィルタリング情報」が表示されます。

- 動作
- 方向
- フィルタリング条件 検索条件 プレフィックス/プレフィックス長
- メトリック値

→受信 →経路情報指定 →完全に一致 →2001:db8:1111::/64 →指定しない

→遮断

<ipv6 ripフィルタリング情報入力フィールド=""></ipv6>			
動作	○透過 ⊙遮断		
方向	⊙受信○送信		
フィルタ リング条 件	 すべて デフォルトルート 経路情報指定 検索条件 ・完全に一致 ・マスクした結果が一致 プレフィックス ノブレフィック ス長 		
メトリック 値			

6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を設定します。

•	動作	→透過
•	方向	→受信
•	フィルタリング条件	→すべて
•	メトリック値	→指定しない

8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

24 OSPFを使用したネットワークを構築する (IPv4)

適用機種 SR-S716C2, 724TC1, 748TC1

ここでは、OSPFv2を使用したダイナミックルーティングのネットワークの設定方法について説明します。 OSPFを使用するネットワークは、バックボーンエリアとその他のエリアに分割して管理します。 エリアには、エリアごとにエリアIDを設定します。バックボーンエリアには必ず0.0.0.0のエリアIDを設定し、 ほかのエリアには重複しないように0.0.0.0以外のエリアIDを設定します。

エリア境界ルータでは、エリア内の経路情報を集約して広報することができます。

● 参照 機能説明書「2.30 OSPF機能」(P.108)

こんな事に気をつけて

- OSPFを使用するインタフェースは、それぞれ異なったネットワークに属するIPアドレスを設定する必要があります。同じネットワークに属するIPアドレスを設定した場合、OSPFを使用しないと判断されます。
- ・ ルータは、各エリアに50台まで設置することができます。ただし、複数のエリアの境界ルータとして使用する場合 は、2つ以上のエリアの指定ルータ(Designated Router)とならないように設定してください。
- ・ 隣接する OSPF ルータどうしは、同じ MTU 値を設定してください。
- 経路情報を最大値まで保持した場合、OSPF以外の経路情報の減少によって経路情報に空きができても、OSPFの経路は、経路情報に反映されません。
- 本装置で保有できるLSA数には上限値があります。この上限値を超えるネットワークで本装置を使用した場合、正しく通信することができません(LSDBオーバフロー)。
 また、LSA生成元のルータの停止などによって、LSA数が本装置の上限値以下まで減少した場合、本装置の電源を再投入したり、または[設定反映]ボタンや[再起動]ボタンをクリックしても、正常に通信ができるまでに最大60分かかることがあります。
- OSPF 使用中に【設定反映】ボタンをクリックした場合、自装置が広報したすべてのLSA に対して MaxAge で再広報 を行ったあとに、OSPF ネットワークへの経路情報が再作成されることがあります。
- ・ OSPFで使用するインタフェースは、以下の条件で使用してください。

本装置が DR を兼務する場合	本装置がDRを兼務しない場合	
(25000÷本装置保有LSA数)未満	(50000÷本装置保有LSA数)未満	



● 前提条件

- すべてのスイッチのすべてのインタフェースに IP アドレスの設定がされている
- すべてのスイッチに IP フォワーディング機能を使用する設定がされている

● 設定条件

[]	スイッチ1でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.0
•	LAN1でのOSPFエリアID	: 0.0.0.1
•	LAN1 でのルータ優先度	: 0
•	エリア 0.0.0.1 への集約経路設定	: 10.20.0.0/16
[]	スイッチ2でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.1
•	LAN1でのOSPFエリアID	: 0.0.0.1
•	LAN0でのルータ優先度	: 1
•	LAN1 での passive-interface 設定	:設定する
[]	スイッチ3でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.1
•	LAN1でのOSPFエリアID	: 0.0.0.1
•	LAN0でのルータ優先度	: 255
•	LAN1 での passive-interface 設定	:設定する
[]	スイッチ4でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.1
•	LAN1でのOSPFエリアID	: 0.0.0.1
•	LAN0でのルータ優先度	: 1
•	LAN1でのpassive-interface設定	:設定する
[]	スイッチ5でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.0
•	LAN1でのOSPFエリアID	: 0.0.0.2
•	エリア 0.0.0.2 への集約経路設定	: 10.30.0.0/16
[スイッチ6でのルーティングプロトコル情報]

•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.2
•	LAN1 でのOSPF エリア ID	: 0.0.0.2
•	LAN1でのpassive-interface 設定	:設定する

上記の設定条件に従って設定を行う場合の設定例を示します。

スイッチ1を設定する

LAN情報を設定する

- **1. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP **関連の設定項目の「OSPF 情報」をクリックします**。 「OSPF 情報」が表示されます。
- 5. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF情報	3
OSPF機能	○使用しない ●使用する
エリア定義番号	0
出力コスト	1
指定ルータ優先度	1

- 6. [保存] ボタンをクリックします。
- 7. 手順2.~6.を参考に、LAN1情報を指定します。

「LAN1情報」-「IP 関連」-「OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 →1
- 指定ルータ優先度 →0

OSPF 関連を設定する

- **8. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- 「OSPF 関連」をクリックします。
 OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。
- **10.** OSPF **関連の設定項目の「OSPF エリア情報」をクリックします**。 「OSPF エリア情報」が表示されます。
- **11.** 【追加】ボタンをクリックします。 OSPFエリア情報(0)の設定項目と「OSPFエリア基本情報」が表示されます。

→0.0.0.0

- 12. 以下の項目を指定します。
 - エリアID



- 13. [保存] ボタンをクリックします。
- **14. 画面上部の「ルーティングプロトコル情報」をクリックします**。 OSPF 関連項目と「OSPF エリア情報」が表示されます。
- 15. 手順 11.~13.を参考に、以下の項目を設定します。
 「OSPFエリア情報(1)」-「OSPFエリア基本情報」
 ・ エリアID → 0.0.0.1
- **16.** OSPF **エリア情報(1)の設定項目の「経路集約情報」をクリックします**。 「経路集約情報」が表示されます。
- 17. 以下の項目を指定します。
 - ネットワークアドレス → 10.20.0.0
 - ネットマスク → 16 (255.255.0.0)

<経路集約情報入力フィールド>		
ネットワークアドレス	10.20.0.0	
ネットマスク	16 (255.255.0.0) 🗸	

- 18. [追加] ボタンをクリックします。
- **19. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

スイッチ2を設定する

「スイッチ1を設定する」を参考に、スイッチ2を設定します。

「LAN情報」

- 「LAN0情報」-「IP 関連」-「OSPF 情報」
- OSPF機能 →使用する
- エリア定義番号 →0
- 指定ルータ優先度 →1

「LAN1情報」-「IP関連」-「OSPF情報」

- OSPF機能 →使用する
- エリア定義番号 →0
- パケット送信 →抑止する

「ルーティングプロトコル情報」 「OSPF 関連」-「OSPF エリア情報(0)」-「OSPF エリア基本情報」

エリアID → 0.0.0.1

スイッチ3を設定する

「スイッチ1を設定する」を参考に、スイッチ3を設定します。

「LAN情報」

「LAN0情報」-「IP 関連」-「OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 →0
- 指定ルータ優先度 →255

「LAN1情報」-「IP 関連」-「OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 →0
- パケット送信 →抑止する

「ルーティングプロトコル情報」 「OSPF 関連」-「OSPF エリア情報 (0)」-「OSPF エリア基本情報」 • エリアID → 0.0.0.1

スイッチ4を設定する

「スイッチ1を設定する」を参考に、スイッチ4を設定します。

「LAN情報」

「LAN0情報」-「IP 関連」-「OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 →0
- 指定ルータ優先度 →1

「LAN1情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 **→**0
- パケット送信 →抑止する

「ルーティングプロトコル情報」 「OSPF 関連」-「OSPF エリア情報(0)」-「OSPF エリア基本情報」 • エリアID →0.0.0.1

スイッチ5を設定する

「スイッチ1を設定する」を参考に、スイッチ5を設定します。

「LAN情報」

「LAN0情報」-「IP 関連」-「OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 **→**0

「LAN1情報」-「IP 関連」-「OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 **→**1

「ルーティングプロトコル情報」 「OSPF 関連」-「OSPF エリア情報(0)」-「OSPF エリア基本情報」 エリアID →0.0.0.0 「OSPF 関連」-「OSPF エリア情報(1)」-「OSPF エリア基本情報」 • エリアID →0.0.0.2 経路集約情報 ネットワークアドレス → 10.30.0.0

→16 (255.0.0.0)

スイッチ6を設定する

ネットマスク

「スイッチ1を設定する」を参考に、スイッチ6を設定します。

「LAN情報」

「LAN0情報」-「IP 関連」-「OSPF 情報」 OSPF機能 →使用する エリア定義番号 **→**0 「LAN1情報」-「IP 関連」-「OSPF 情報」 • OSPF機能 →使用する エリア定義番号 **→**0 パケット送信 →抑止する 「ルーティングプロトコル情報」 「OSPF 関連」-「OSPF エリア情報(0)」-「OSPF エリア基本情報」

• エリアID →0.0.0.2

24.1 バーチャルリンクを使う

<u>適用機種</u> SR-S716C2, 724TC1, 748TC1

バックボーンエリアと直接接続できないエリアを、バーチャルリンクを使用して接続する設定方法について説明 します。

こんな事に気をつけて

- バーチャルリンクは、スタブエリア、準スタブエリアを経由して使用することはできません。
 - ・ バーチャルリンクを使用する場合は、OSPF ルータ ID を設定する必要があります。設定する際は、OSPF ルータ ID が重複しないように設定してください。



● 前提条件

- すべてのスイッチのすべてのインタフェースに IP アドレスの設定がされている
- すべてのスイッチにIPフォワーディング機能を使用する設定がされている

● 設定条件

[スイッチ1でのルーティングプロトコル情報]

•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.0
•	LAN1 でのOSPF エリア ID	: 0.0.0.1
[7	、イッチ2でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.1
•	LAN1 でのOSPF エリア ID	: 0.0.0.1

[スイッチ3でのルーティングプロトコル情報]

•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LAN0でのOSPFエリアID	: 0.0.0.0
•	LAN1でのOSPFエリアID	: 0.0.0.2
•	OSPF ルータ ID	: 10.30.10.1
•	バーチャルリンク接続先 OSPF ルータ ID	: 10.40.10.1
[7	スイッチ4でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LAN0でのOSPFエリアID	: 0.0.0.2
•	LAN1でのOSPFエリアID	: 0.0.0.3
•	OSPF ルータ ID	: 10.40.10.1
•	バーチャルリンク接続先 OSPF ルータ ID	: 10.30.10.1
[7	スイッチ5でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LAN0でのOSPFエリアID	: 0.0.0.3
•	LAN1でのOSPFエリアID	: 0.0.0.3

上記の設定条件に従って設定を行う場合の設定例を示します。

スイッチ1を設定する

LAN0 情報を設定する

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 2. 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4. IP 関連の設定項目の「OSPF 情報」をクリックします**。 「OSPF 情報」が表示されます。
- 5. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

OSPF情報	3
OSPF機能	○使用しない ●使用する
エリア定義番号	0

- 6. [保存] ボタンをクリックします。
- 手順2.~6.を参考に、LAN1情報を設定します。
 「LAN1情報」-「IP関連」-「OSPF情報」
 - OSPF機能 →使用する
 - エリア定義番号 →1

OSPF 関連を設定する

- **8. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- 「OSPF 関連」をクリックします。
 OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。
- **10.** OSPF **関連の設定項目の「OSPF エリア情報」をクリックします**。 「OSPF エリア情報」が表示されます。
- **11.** [追加] ボタンをクリックします。 OSPFエリア情報(0)の設定項目と「OSPFエリア基本情報」が表示されます。
- 12. 以下の項目を指定します。
 - エリアID → 0.0.0.0

■OSPFエリア基本情報		3
エリアID	0.0.0.0	

- 13. [保存] ボタンをクリックします。
- **14. 画面上部の「ルーティングプロトコル情報」をクリックします**。 OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。
- 15. 手順 11. ~ 13. を参考に、以下の項目を設定します。
 「OSPF エリア情報 (1)」 「OSPF エリア基本情報」
 ・ エリアID → 0.0.0.1
- **16. 画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

スイッチ2を設定する

「スイッチ1を設定する」を参考に、スイッチ2を設定します。

 「LAN 情報」
 「IP 関連」 - 「OSPF 情報」

 • OSPF機能
 →使用する

 • エリア定義番号
 →0

 「LAN1 情報」 - 「IP 関連」 - 「OSPF 情報」

 • OSPF機能
 →使用する

 • エリア定義番号
 →0

 「LAN1 情報」 - 「IP 関連」 - 「OSPF 情報」

 • OSPF機能
 →使用する

 • エリア定義番号
 →0

「OSPF関連」-「OSPFエリア情報(0)」-「OSPFエリア基本情報」

エリアID →0.0.0.1

スイッチ3を設定する

LAN0 情報を設定する

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

- 5. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF情報		3
OSPF機能	○使用しない ⊙使用する	
エリア定義番号	0	

- 6. [保存] ボタンをクリックします。
- 手順2.~6.を参考に、以下の項目を設定します。
 「LAN1情報」-「IP関連」-「OSPF情報」
 - OSPF機能 →使用する
 - エリア定義番号 →1

OSPF 関連を設定する

- **8. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- 9. 「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

- 10. 以下の項目を指定します。
 - ルータID

→ 10.30.10.1

■ルータID情報		3
ルータID	10.30.10.1	

- 11. 【保存】ボタンをクリックします。
- **12.** OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。 「OSPF エリア情報」が表示されます。
- 13. [追加]ボタンをクリックします。

OSPFエリア情報(0)の設定項目と「OSPFエリア基本情報」が表示されます。

- 14. 以下の項目を指定します。
 - エリアID

→0.0.0.0

■OSPFエリア基本情報		3
エリアID	0.0.0.0	

- 15. 【保存】ボタンをクリックします。
- **16. 画面上部の「ルーティングプロトコル情報」をクリックします**。 OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。
- 17. 手順 13. ~ 15. を参考に、以下の項目を設定します。
 「OSPF エリア情報(1)」-「OSPF エリア基本情報」
 ・ エリアID → 0.0.0.2
- **18.** OSPF **エリア情報(1)の設定項目の「バーチャルリンク情報」をクリックします**。 「バーチャルリンク情報」が表示されます。
- 19. 以下の項目を指定します。
 - 接続先ルータID → 10.40.10.1

```
<バーチャルリンク情報入力フィールド>
接続先ルータID 10.40.10.1
```

- 20. [追加] ボタンをクリックします。
- **21. 画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

スイッチ4を設定する

LAN0 情報を設定する

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4. IP 関連の設定項目の「OSPF 情報」をクリックします**。 「OSPF 情報」が表示されます。
- 5. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF 情報	3
OSPF機能	○使用しない ●使用する
エリア定義番号	0

- 6. [保存] ボタンをクリックします。
- 手順2.~6.を参考に、以下の項目を設定します。
 「LAN1情報」-「IP関連」-「OSPF情報」
 - OSPF機能 →使用する
 - エリア定義番号 →1

OSPF 関連を設定する

- **8. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- 9. 「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

- 10. 以下の項目を指定します。
 - ルータID → 10.40.10.1

■ルータID情報		3
ルータID	10.40.10.1	

11. 【保存】ボタンをクリックします。

12. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

「OSPFエリア情報」が表示されます。

13. [追加]ボタンをクリックします。

OSPF エリア情報(0)の設定項目と「OSPF エリア基本情報」が表示されます。

- 14. 以下の項目を指定します。
 - エリアID → 0.0.0.2
 OSPFエリア基本情報
 エリアID 0.0.2
- 15. [保存] ボタンをクリックします。
- **16.** OSPF エリア情報(0)の「バーチャルリンク情報」をクリックします。 「バーチャルリンク情報」が表示されます。
- 17. 以下の項目を指定します。
 - 接続先ルータID → 10.30.10.1

<バーチャルリンク情報入力フィールド>	
接続先ルータID	10.30.10.1

- 18. [追加] ボタンをクリックします。
- **19. 画面上部の「ルーティングプロトコル情報」をクリックします**。 OSPF 関連の設定項目と「OSPF エリア基本情報」が表示されます。
- 20. 手順 13. ~ 15. を参考に、以下の項目を設定します。
 「OSPF エリア情報(1)」-「OSPF エリア基本情報」
 ・ エリアID → 0.0.0.3
- **21. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

スイッチ5を設定する

「スイッチ1を設定する」を参考に、スイッチ5を設定します。

「LAN情報」

「LAN0情報」-「IP 関連」-「OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 →0

「LAN1情報」-「IP関連」-「OSPF情報」

- OSPF機能 →使用する
- エリア定義番号 →0

「ルーティングプロトコル情報」

「OSPF 関連」-「OSPF エリア情報(0)」-「OSPF エリア基本情報」

エリアID →0.0.0.3

24.2 スタブエリアを使う

<u>適用機種</u> SR-S716C2, 724TC1, 748TC1

OSPF 以外のルーティングプロトコルを使用したネットワークとの接続の設定について説明します。 OSPF は、RIP で受信した経路情報、スタティック経路情報およびインタフェース経路情報を OSPF ネットワーク に取り入れることができます。また、OSPF の経路情報を RIP で広報することができます。

OSPF以外のネットワークと接続する場合、スタブエリアとして運用すると、OSPFネットワーク外の経路とし てデフォルトルートを使用するため、エリア内の経路情報を少なくすることができます。スタブエリアから OSPF以外のネットワークに直接接続することはできません。直接、接続する場合は、準スタブエリア(NSSA) として運用します。

こんな事に気をつけて

OSPF以外のネットワークと接続する場合、OSPF以外のネットワークで使用するインタフェース経路情報をOSPF ネットワークに取り入れるように設定する必要があります。



● 前提条件

- すべてのスイッチのすべてのインタフェースに IP アドレスの設定がされている
- すべてのスイッチに IP フォワーディング機能を使用する設定がされている

● 設定条件

[スイッチ1でのルーティングプロトコル情報]

•	LAN0でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LAN0でのOSPFエリアID	: 0.0.0.0
•	LAN1でのOSPFエリアID	: 0.0.0.1
•	エリアID 0.0.0.1のエリアタイプ	: stub
[7	スイッチ2でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN0 でのルーティングプロトコル LAN1 でのルーティングプロトコル	: OSPF : OSPF
•	LAN0 でのルーティングプロトコル LAN1 でのルーティングプロトコル LAN0 での OSPF エリア ID	: OSPF : OSPF : 0.0.0.1
•	LAN0 でのルーティングプロトコル LAN1 でのルーティングプロトコル LAN0 での OSPF エリア ID LAN1 での OSPF エリア ID	: OSPF : OSPF : 0.0.0.1 : 0.0.0.1
• • • •	LAN0 でのルーティングプロトコル LAN1 でのルーティングプロトコル LAN0 での OSPF エリア ID LAN1 での OSPF エリア ID エリア ID 0.0.0.1 のエリアタイプ	: OSPF : OSPF : 0.0.0.1 : 0.0.0.1 : stub

[スイッチ3でのルーティングプロトコル情報]

•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.0
•	LAN1 でのOSPF エリア ID	: 0.0.0.2
•	エリア ID 0.0.0.2 のエリアタイプ	: nssa
[7	スイッチ4でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: RIP V2,OSPF
•	LANOでのOSPFエリアID	: 0.0.0.2
•	LAN1 での passive-interface 設定	:設定する
•	エリア ID0.0.0.2 のエリアタイプ	: nssa
•	OSPF 経路の RIP での広報	:再配布する
•	RIP 経路の OSPF での広報	:再配布する

上記の設定条件に従って設定を行う場合の設定例を示します。

スイッチ1を設定する

LAN0 情報を設定する

- **1. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 2. 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- IP 関連の設定項目の「OSPF 情報」をクリックします。
 「OSPF 情報」が表示されます。
- 5. 以下の項目を指定します。
 - OSPF機能
 →使用する
 - エリア定義番号 →0

■OSPF情報	3
OSPF機能	○使用しない ⊙使用する
エリア定義番号	0

6. [保存] ボタンをクリックします。

7. 手順2.~6.を参考に、以下の項目を設定します。

「LAN1情報」-「IP関連」-「OSPF情報」

- OSPF機能 →使用する
- エリア定義番号 →1

OSPF 関連を設定する

- 8. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。 「ルーティングプロトコル情報」ページが表示されます。
- **9.** 「OSPF 関連」をクリックします。
 OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。
- **10.** OSPF **関連の設定項目の「OSPF エリア情報」をクリックします**。 「OSPF エリア情報」が表示されます。
- **11.** 【追加】ボタンをクリックします。 OSPFエリア情報(0)の設定項目と「OSPFエリア基本情報」が表示されます。
- 12. 以下の項目を指定します。
 - エリアID

→0.0.0.0

■OSPFエリア基本情報		3
エリアID	0.0.0.0	
エリア種別	 ●通常エリア ○スタブエリア ○準スタブエリア 	

- 13. [保存] ボタンをクリックします。
- **14. 画面上部の「ルーティングプロトコル情報」をクリックします**。 OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。
- **15.** 手順 11. ~ 13. を参考に、以下の項目を設定します。 「OSPF エリア情報(1)」-「OSPF エリア基本情報」
 - エリアID → 0.0.0.1
 - エリア種別 →スタブエリア
- **16. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

スイッチ2を設定する

「スイッチ1を設定する」を参考に、スイッチ2を設定します。

 「LAN 情報」
 「IP 関連」 - 「OSPF 情報」

 ・ OSPF 機能
 →使用する

 ・ エリア定義番号
 →0

 「LAN1 情報」 - 「IP 関連」 - 「OSPF 情報」

 ・ OSPF 機能
 →使用する

 ・ UPア定義番号
 →0

 「LAN1 情報」 - 「IP 関連」 - 「OSPF 情報」

 ・ OSPF 機能
 →使用する

 ・ UPア定義番号
 →0

 「ルーティングプロトコル情報」

「OSPF 関連」-「OSPF エリア情報(0)」-「OSPF エリア基本情報」

- エリアID →0.0.0.1
- エリア種別 →スタブエリア

スイッチ3を設定する

「スイッチ1を設定する」を参考に、スイッチ3を設定します。

「LAN情報」

「LAN0情報」-「IP関連」-「OSPF情報」

- OSPF機能 →使用する
- エリア定義番号 →0

「LAN1情報」-「IP関連」-「OSPF情報」

- OSPF機能 →使用する
- エリア定義番号 →1

「ルーティングプロトコル情報」

「OSPF 関連」-「OSPF エリア情報(0)」-「OSPF エリア基本情報」

エリアID → 0.0.0.0

「OSPF 関連」-「OSPF エリア情報(1)」-「OSPF エリア基本情報」

- エリアID →0.0.0.2
- エリア種別 →準スタブエリア

スイッチ4を設定する

LAN0 情報を設定する

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP **関連の設定項目の「**OSPF **情報」をクリックします**。 「OSPF 情報」が表示されます。
- 5. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF 情報	3
OSPF機能	○使用しない ●使用する
エリア定義番号	0

6. [保存] ボタンをクリックします。

LAN1情報を設定する

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- FLAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。
 「LAN1 情報」ページが表示されます。
- 9. 「IP 関連」をクリックします。IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 10. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

- 11. 以下の項目を指定します。
 - RIP送信

→V2(Multicast)で送信する

 ● RIP受信 → V2、V2 (Multicast) で受信する

RIP情報	3
RIP送信	●送信しない ●V1で送信する ●V2で送信する ●V2(Multicast)で送信する
RIP受信	○受信しない ○V1で受信する ⊙V2、V2(Multicast)で受信する

- 12. [保存] ボタンをクリックします。
- **13.** IP **関連の設定項目の「OSPF 情報」をクリックします**。 「OSPF 情報」が表示されます。
- 14. 以下の項目を指定します。
 - OSPF機能 →使用する
 エリア定義番号 →0
 - パケット送信 →抑止する

■OSPF情報	3
OSPF機能	○使用しない ◎使用する
エリア定義番号	0
出力コスト	1
指定ルータ優先度	1
Helloバケット送信間隔	10 秒 🗸
隣接ルータ停止確認間隔	40 秒 🗸
バケット再送間隔	5 秒 🗸
LSUバケット送信遅延時間	1 秒 🗸
認証方式	 ● 認証を行わない ● テキスト認証 鍵種別 ● 文字列 ● 16進数 認証鍵 ● MD5認証 MD5認証鏈ID MD5認証鏈
バケット送信	⊙抑止する○抑止しない

15. [保存] ボタンをクリックします。

OSPF 関連を設定する

- **16. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **17.** 「OSPF 関連」をクリックします。 OSPF 関連の設定項目と「ルータID 情報」が表示されます。
- **18.** OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。 「OSPF エリア情報」が表示されます。
- 19.
 【追加】ボタンをクリックします。

 OSPFエリア情報(0)の設定項目と「OSPFエリア基本情報」が表示されます。

20. 以下の項目を指定します。

- エリアID
- エリア種別 →準スタブエリア

■OSPFエリア基本情報		3
エリアID	0.0.0.2	
エリア種別	 ●通常エリア ●スタブエリア ●準スタブエリア 	

21. [保存] ボタンをクリックします。

ルーティングマネージャ情報を設定する

22. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。 「ルーティングプロトコル情報」ページが表示されます。

→0.0.0.2

23. 「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

- 24. 以下の項目を指定します。
 - RIP OSPF経路情報 →再配布する
 • OSPF
 - RIP経路情報 →再配布する

■再配布情報		
	インタフェース経路情報	○再配布しない⊙再配布する
DID	スタティック経路情報	○再配布しない⊙再配布する
КIР	OSPF経路情報	○再配布しない ●再配布する メトリック値: 0 ▼
	インタフェース経路情報	 ● 再配布しない ● 再配布する メトリック値 20 メトリックタイブ type2 マ
OSPF	PF スタティック経路情報	 ● 再配布しばい ● 再配布する メトリック値 20 メトリックタイブ type2 ▼
	RIP経路情報	 再配布しない 再配布する メトリック値 20 メトリックタイプ type2 マ

- 25. [保存] ボタンをクリックします。
- **26. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

25 OSPFの経路を制御する(IPv4)

適用機種 SR-S716C2, 724TC1, 748TC1

本装置で、ほかのルータから受信する経路情報(LSA)に変更を加えることで、本装置で保有する経路情報や広報する経路情報の数を制御することができます。

25.1 OSPF ネットワークでエリアの経路情報(LSA)を集約する

適用機種 SR-S716C2, 724TC1, 748TC1

エリア内のLSAを、本装置(エリア境界ルータ)で集約して、バックボーンエリアへ取り込む場合の設定方法を 説明します。



● 前提条件

- すべてのインタフェースに IP アドレスの設定がされている
- IP フォワーディング機能を使用する設定がされている

● 経路情報の設計

• エリア内のLSAを、本装置(エリア境界ルータ)で集約してバックボーンエリアに取り込む

● 設定条件

- LAN0でのルーティングプロトコル : OSPF
 LAN1でのルーティングプロトコル : OSPF
 LAN0でのエリアID : 0.0.0.0
 LAN1でのエリアID : 0.0.0.1
- バックボーンエリアへの集約経路設定 : 10.20.0.0/16

上記の経路情報に従って設定する場合の設定例を示します。

LAN 情報を設定する

- **1. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「OSPF 情報」をクリックします。 「OSPF 情報」が表示されます。
- 5. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF情報	[3
OSPF機能	○使用しない ⊙使用する	
エリア定義番号	0	

- 6. [保存] ボタンをクリックします。
- 7. 手順1.~6.を参考に、LAN1情報で以下の項目を設定します。
 「LAN1情報」-「IP関連」-「OSPF情報」
 - OSPF機能 →使用する
 - エリア定義番号 →1

OSPF 関連を設定する

- **8. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **9.** 「OSPF 関連」をクリックします。
 OSPF 関連の設定項目と「ルータID 情報」が表示されます。
- **10.** OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。 「OSPF エリア情報」が表示されます。
- **11.** 【追加】ボタンをクリックします。 OSPFエリア情報(0)の設定項目と「OSPFエリア基本情報」が表示されます。
- 12. 以下の項目を指定します。
 - エリアID

→0.0.0.0

■OSPFエリア基本情報		3
エリアID	0.0.0.0	

13. 【保存】ボタンをクリックします。

- **14. 画面上部の「ルーティングプロトコル情報」をクリックします**。 OSPF 関連項目と「OSPF エリア情報」が表示されます。
- 15. 手順 11. ~ 13. を参考に、以下の項目を設定します。
 「OSPF エリア情報(1)」-「OSPF エリア基本情報」
 ・ エリアID → 0.0.0.1
- **16.** OSPF**エリア情報(1)の「経路集約情報」をクリックします。** 「経路集約情報」が表示されます。
- 17. 以下の項目を指定します。
 - ネットワークアドレス → 10.20.0.0
 - ネットマスク → 16 (255.255.0.0)

<経路集約情報入力フィールド>		
ネットワークアドレス	10.20.0.0	
ネットマスク	16 (255.255.0.0) 🔽	

- 18. [追加] ボタンをクリックします。
- 19. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

25.2 AS外部経路を集約してOSPFネットワークに広報する

適用機種 SR-S716C2, 724TC1, 748TC1

AS 外部(OSPF 以外)のネットワークの経路情報を本装置(AS 境界ルータ)で集約して、バックボーンエリア に広報する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースに IP アドレスの設定がされている
- LAN1 インタフェースに RIPv2 を使用する設定がされている
- IPフォワーディング機能を使用する設定がされている

● 経路情報の設計

- AS外部経路情報を本装置(AS境界ルータ)で集約して OSPF ネットワーク(バックボーンエリア)に広報する
- その他のAS外部経路情報はすべて遮断する

● 設定条件

- LANOでのルーティングプロトコル : OSPF
- LANOでのエリアID : 0.0.0.0
- バックボーンエリアへの集約経路設定 : 20.10.0.0/16

上記の経路情報に従って設定する場合の設定例を示します。

LAN情報を設定する

- **1. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- **3.** 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

4. IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

- 5. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF情報	2	3
OSPF機能	○使用しない ⊙使用する	
エリア定義番号	0	

6. [保存] ボタンをクリックします。

OSPF 関連を設定する

- 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。
 「ルーティングプロトコル情報」ページが表示されます。
- **6.** 「OSPF 関連」をクリックします。
 OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。
- OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。
 「OSPF エリア情報」が表示されます。
- **10.** [追加] ボタンをクリックします。 OSPFエリア情報(0)の設定項目と「OSPFエリア基本情報」が表示されます。
- 11. 以下の項目を指定します。
 - エリアID →0.0.0.0

■OSPFエリア基本	≤情報	3
エリアID	0.0.0.0	

12. [保存] ボタンをクリックします。

ルーティングマネージャ情報を設定する

- **13. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **14.** 「ルーティングマネージャ情報」をクリックします。 ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。
- 15. 以下の項目を指定します。
 - OSPF RIP 経路情報

→再配布する

OSPF	○ 再配布しない● 再配布する
RIP轻路頂報	メトリック値 20 メトリックタイブ type2 🖌

16. [保存] ボタンをクリックします。

OSPF 関連を設定する

- **17. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- 18. 「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

- **19.** OSPF **関連の設定項目の「AS 外部経路集約情報」をクリックします**。 「AS 外部経路集約情報」が表示されます。
- 20. 以下の項目を指定します。
 - ネットワークアドレス → 20.10.0.0
 - ネットマスク → 16 (255.255.0.0)

<as外部経路集約情報入力フィールド></as外部経路集約情報入力フィールド>		
ネットワークアドレス	20.10.0.0	
ネットマスク	16 (255.255.0.0) 🗸	

- 21. [追加] ボタンをクリックします。
- **22**. OSPF 関連項目の「OSPF 再配布フィルタリング情報」をクリックします。

「OSPF 再配布フィルタリング情報」が表示されます。

23. 以下の項目を指定します。

動作 →透過
 フィルタリング条件 →経路情報指定
 検索条件 →マスクした結果が一致
 IPアドレス → 20.10.0.0
 アドレスマスク → 16 (255.255.0.0)
 メトリック →指定しない

<0SPF再配布フィルタリング情報入力フィールド>			
動作	⊙透過 ○遮断		
フィルタリング条件	 すべて デフォルトルート 経路情報指定 検索条件 ○ 完全に一致 ○ マスクした結果が一致 IPアドレス 20.10.0 アドレスマスク 16 (255.255.0.0) 		
メトリック	 ● 指定しばい ● 指定する メトリック値 メトリックダイブ type2 ▼ 		

24. [追加] ボタンをクリックします。

25. 手順23.~24.を参考に、以下の項目を設定します。

- 動作 →遮断
- フィルタリング条件 →すべて
- メトリック →指定しない

26. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

25.3 エリア境界ルータで不要な経路情報(LSA)を遮断する

適用機種 SR-S716C2, 724TC1, 748TC1

エリア境界ルータで、通信に使用しないTYPE3サマリLSAの経路情報を遮断する設定方法を説明します。



● 前提条件

- すべてのインタフェースに IP アドレスの設定がされている
- IP フォワーディング機能を使用する設定がされている

● 経路情報の設計

- エリア1の10.0.0/8のネットワークとエリア2のネットワークでは通信を行わないため、10.0.0/8の経路 情報を遮断する
- その他はすべて透過させる

● 設定条件

- LANOでのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LANOでのエリアID : 0.0.0.0
- LAN1でのエリアID : 0.0.0.2
- 10.0.0/8のLSAを遮断

上記の経路情報に従って設定する場合の設定例を示します。

LAN 情報を設定する

- **1. 設定メニューの詳細設定で、「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

- 5. 以下の項目を指定します。
 - OSPF機能
 →使用する
 - エリア定義番号 →0

■OSPF情報	3
OSPF機能	○使用しない ●使用する
エリア定義番号	0

- 6. [保存] ボタンをクリックします。
- 手順2.~6.を参考に、以下の項目を設定します。
 [LAN1情報]-「IP関連」-「OSPF情報」
 - OSPF機能 →使用する
 - エリア定義番号 →1

OSPF 関連を設定する

- 8. 設定メニューの詳細設定で、「ルーティングプロトコル情報」をクリックします。 「ルーティングプロトコル情報」ページが表示されます。
- **9. 「**OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

- **10.** OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。 「OSPF エリア情報」が表示されます。
- **11.** 【追加】ボタンをクリックします。 OSPFエリア情報(0)の設定項目と「OSPFエリア基本情報」が表示されます。
- 12. 以下の項目を指定します。
 - エリアロ

→0.0.0.0

■OSPFエリア基本情報		
エリアID	0.0.0.0	

- 13. [保存] ボタンをクリックします。
- **14. 画面上部の「ルーティングプロトコル情報」をクリックします**。 OSPF 関連項目と「OSPF エリア情報」が表示されます。
- 15. 手順 11. ~ 13. を参考に、以下の項目を設定します。
 「OSPF エリア情報(1)」 「OSPF エリア基本情報」
 ・ エリアID → 0.0.0.2
- **16. 画面上部の「ルーティングプロトコル情報」をクリックします**。 OSPF 関連項目と「OSPF エリア情報」が表示されます。
- **17. エリア定義番号(1)の[修正]ボタンをクリックします**。 OSPFエリア情報(1)の設定項目と「OSPFエリア基本情報」が表示されます。

18. OSPF エリア情報(1)の設定項目の「サマリLSA入出力可否情報」をクリックします。

「サマリ LSA 入出力可否情報」が表示されます。

19. 以下の項目を指定します。

٠	動作	→遮断
•	方向	→入力
•	対象経路情報 検索条件	→経路情報指定 →完全に一致
	IPアドレス	→ 10.0.0.0
	アドレスマスク	→ 8 (255.0.0.0)

<サマリLSA入出力可否情報入力フィールド>			
動作	○透過 ⊙遮断		
方向	◎入力○出力		
対象経路情報	 すべて 経路情報指定 検索条件 ○ 完全に一致 ○ マスクした結果が一致 IPアドレス ID2000 アドレスマスク 8 (255.0.00) 		

- 20. [追加] ボタンをクリックします。
- 21. 手順 19.~20.を参考に、以下の項目を設定します。
 - 動作 →透過
 - 方向 →入力
 - 対象経路情報 → すべて
- **22. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

26 OSPF機能を使う(IPv6)

適用機種 SR-S724TC1, 748TC1

26.1 OSPF ネットワークを構築する

OSPF (IPv6)を使用したネットワークの構築について説明します。

こんな事に気をつけて

- ・ ルータは、各エリアに 30 台まで設置することができます。ただし、複数のエリアの境界ルータとして使用する場合 は、2 つ以上のエリアの指定ルータ(DR: Designated Router)とならないように設定してください。
- ・ LANを使用した隣接OSPFルータとMTU値が一致しない場合は、隣接関係を構築できません。
- 経路情報を最大値まで保持した場合、OSPF以外の経路情報の減少によって経路情報に空きができても、OSPFの経路は、経路情報に反映されません。
- 本装置で保有できるLSA数には上限値があります。この上限値を超えるネットワークで本装置を使用した場合、正しく通信することができません(LSDBオーバフロー)。
 また、LSA生成元のルータの停止などによって、LSA数が本装置の上限値以下まで減少した場合、本装置の電源を再

なん、LSA主成九のルータの停止などによりて、LSA数が本装置の工限値以下よど減少した場合、本装置の電源を再 投入したり、[設定反映] ボタンや [再起動] ボタンをクリックしたりしても、正常に通信できるまでに最大60分か かることがあります。

・ OSPFで使用するインタフェースは、以下の条件で使用してください。

本装置がDRを兼務する場合	本装置がDRを兼務しない場合
(10000÷本装置保有LSA数)未満	(20000÷本装置保有LSA数)未満



● 前提条件

- 本装置1、2のすべてのインタフェースでIPv6機能を利用する設定がされている
- 本装置1、2にIPv6フォワーディング機能を使用する設定がされている
- 本装置1のLAN1には、グローバルアドレスが設定されている
- 本装置1のLAN2には、OSPF外ネットワークへの経路がスタティック設定されている

● 設定条件

- 本装置1はバックボーンエリアと通常エリアのエリア境界ルータであり、かつ、OSPF外ネットワークへ到達 するためのAS境界ルータとして運用する
- 本装置2はバックボーンエリアとスタブエリアのエリア境界ルータとして運用する。また、バックボーンエ リアでは指定ルータとして運用する

 各エリアIDは、以下のとおり バックボーンエリア : 0.0.0.0 通常エリア : 0.0.0.1 スタブエリア : 0.0.0.2

[本装置1]

- LANOはバックボーンエリアに属する
- LAN1 は通常エリアに属し、ほかにルータが接続されていないため、Passive-interface として OSPF パケット を送信しないようにする
- OSPFルータIDは 100.0.0.1 とする
- スタティック経路をOSPFに再配布する

[本装置2]

- LAN0はバックボーンエリアに属し、バックボーンエリアの指定ルータとするため、指定ルータ優先度に255 を設定する
- LAN1はスタブエリアとする
- OSPFルータIDは 100.0.2とする

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

LAN情報を設定する

- **1. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 3. 「IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

- **4. IPv6 関連の設定項目の「IPv6 OSPF 情報」をクリックします**。 「IPv6 OSPF 情報」が表示されます。
- 5. 以下の項目を指定します。
 - OSPF機能
 →使用する
 - エリア定義番号 →0

■IPv6 OSPF情報	3
OSPF機能	●使用しない●使用する
エリア定義番号	0

6. [保存] ボタンをクリックします。

7. 手順1.~6.を参考に、「LAN1情報」で以下の項目を指定します。

「LAN1 情報」-「IPv6 関連」-「IPv6 OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 →1
- パケット送信 →抑止する

IPv6 OSPF 関連を設定する

- **8. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- 9. 「IPv6 OSPF 関連」をクリックします。

IPv6 OSPF 関連の設定項目と「IPv6 ルータ ID 情報」が表示されます。

- 10. 以下の項目を指定します。
 - ルータID → 100.0.0.1

■IPv6 ルータID情報		?
ルータID	100.0.0.1	

- 11. 【保存】ボタンをクリックします。
- **12.** IPv6 OSPF 関連の設定項目の「IPv6 OSPF エリア情報」をクリックします。 「IPv6 OSPF エリア情報」が表示されます。
- 13. [追加] ボタンをクリックします。

IPv6 OSPFエリア情報(0)の「IPv6 OSPFエリア基本情報」が表示されます。

14. 以下の項目を指定します。

- エリアID →0.0.0.0
- エリア種別 →通常エリア

■IPv6 OSPFエリア基本情報	
エリアID	0.0.0.0
エリア種別	 ●通常エリア ●スタブエリア

- 15. [保存] ボタンをクリックします。
- **16. 画面上部のルーティングプロトコル情報をクリックします**。 IPv6 OSPF 関連項目と「IPv6 OSPF エリア情報」が表示されます。
- 17. 手順 13.~15.を参考に、以下の項目を指定します。
 - エリアID → 0.0.0.1
 - エリア種別 →通常エリア

ルーティングマネージャ情報を設定する

18. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。 「ルーティングプロトコル情報」ページが表示されます。

19. 「IPv6 ルーティングマネージャ情報」をクリックします。

IPv6ルーティングマネージャ情報の設定項目と「IPv6再配布情報」が表示されます。

20. 以下の項目を指定します。

OSPF

スタティック経路情報 →再配布する

2.0DF		○ 再配布しない● 再配布する
OSPF	人タティック経路情報	メトリック値 20 メトリックタイプ type2 💌

21. [保存] ボタンをクリックします。

22. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

LAN0情報]- IPv6関連]	
「IPv6 OSPF 情報」	
● OSPF機能	→ 使用する
 エリア定義番号 	→0
• 指定ルータ優先度	→255
「LAN1情報」- 「IPv6関連」	
「IPv6 OSPF 情報」	
● OSPF機能	→ 使用する
 エリア定義番号 	→1
「ルーティングプロトコル情報	暍」- 「IPv6 OSPF 関連」
「ルーティングプロトコル情報 「IPv6 ルータID情報」	暍」- 「IPv6 OSPF 関連」
「 ルーティングプロトコル情報 「IPv6 ルータ ID 情報」 ・ ルータ ID	報 」- 「IPv6 OSPF 関連」 →100.0.0.2
「 ルーティングプロトコル情報 「IPv6 ルータ ID 情報」 ・ ルータ ID 「IPv6 OSPF エリア情報(0)」-	報】- 「IPv6 OSPF 関連」 → 100.0.0.2 「IPv6 OSPF 基本情報」
「 ルーティングプロトコル情報 「IPv6 ルータ ID 情報」 ・ ルータ ID 「IPv6 OSPF エリア情報(0)」 - ・ エリア ID	報】- 「IPv6 OSPF 関連」 → 100.0.0.2 「IPv6 OSPF 基本情報」 → 0.0.0.0
「 ルーティングプロトコル情報 「IPv6 ルータ ID 情報」 ・ ルータ ID 「IPv6 OSPF エリア情報(0)」 - ・ エリア ID ・ エリア種別	報J - 「IPv6 OSPF 関連」 → 100.0.0.2 「IPv6 OSPF 基本情報」 → 0.0.0.0 →通常エリア
「 ルーティングプロトコル情報 「IPv6 ルータ ID 情報」 ・ ルータ ID 「IPv6 OSPF エリア情報(0)」 - ・ エリア ID ・ エリア種別 「IPv6 OSPF エリア情報(1)」 -	報J - 「IPv6 OSPF 関連」 → 100.0.0.2 「IPv6 OSPF 基本情報」 → 0.0.0.0 →通常エリア 「IPv6 OSPF 基本情報」
「ルーティングプロトコル情報」 「IPv6 ルータID情報」 ・ ルータID 「IPv6 OSPF エリア情報 (0)」 - ・ エリアID ・ エリア種別 「IPv6 OSPF エリア情報 (1)」 - ・ エリアID	 ・「IPv6 OSPF 関連」 → 100.0.0.2 「IPv6 OSPF 基本情報」 → 0.0.0.0 →通常エリア 「IPv6 OSPF 基本情報」 → 0.0.0.2

26.2 エリア境界ルータでエリア内部経路を集約する

適用機種 SR-S724TC1, 748TC1

エリア境界ルータで、エリア内経路を集約してほかのエリアに広報する設定について説明します。



● 前提条件

- 本装置のすべてのインタフェースで IPv6 機能を利用する設定がされている
- IPv6 フォワーディング機能を使用する設定がされている
- 本装置はバックボーンエリアとエリア1のエリア境界ルータとして運用し、LAN0、LAN1、LAN2でOSPFを 使用する
- OSPFルータIDは、100.0.0.1

•	各エリアIDは、以下のとおり	
	バックボーンエリア	: 0.0.0.0(エリア定義番号0)
	エリア1	: 0.0.0.1(エリア定義番号1)

 各インタフェースのIPアドレスは、以下のとおり LAN1 : 2001:db8:10::1/64 LAN2 : 2001:db8:20::1/64

● 設定条件

 エリア1のエリア内部経路(2001:db8:10::/64、2001:db8:20::/64)は、集約経路(2001:db8::/32、コスト 100)としてバックボーンエリアに広報する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置を設定する

IPv6 OSPF 関連を設定する

- **1. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- 「IPv6 OSPF 関連」をクリックします。
 IPv6 OSPF 関連の設定項目と「IPv6 ルータ ID 情報」が表示されます。
- **3.** IPv6 OSPF 関連の設定項目の「IPv6 OSPF エリア情報」をクリックします。 「IPv6 OSPF エリア情報」が表示されます。

4. エリア定義番号1の [修正] ボタンをクリックします。

IPv6 OSPF エリア情報(1)の「IPv6 OSPF エリア基本情報」が表示されます。

5. 「IPv6 経路集約情報」をクリックします。

「IPv6 経路集約情報」が表示されます。

- 6. 以下の項目を指定します。
 - プレフィックス/プレフィックス長
- →2001:db8::/32

• コスト

→100

<ipv6 経路集約情報入力フィールド=""></ipv6>		
プレフィックス/プレフィックス長	2001:db8::	32
コスト	100	

- 7. [追加] ボタンをクリックします。
- 8. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

26.3 エリア境界ルータで不要な経路情報を遮断する

適用機種 SR-S724TC1, 748TC1

エリア境界ルータで、ほかのエリアに対し特定のエリア内経路(エリア間プレフィックスLSA)を遮断して広報 する設定について説明します。



● 前提条件

- 本装置のすべてのインタフェースで IPv6 機能を利用する設定がされている
- IPv6フォワーディング機能を使用する設定がされている
- 本装置はバックボーンエリアとエリア1のエリア境界ルータとして運用し、LAN0、LAN1、LAN2でOSPFを 使用する
- OSPFルータIDは、100.0.0.1
- 各エリアIDは、以下のとおり バックボーンエリア : 0.0.0.0 (エリア定義番号0) エリア1 : 0.0.0.1 (エリア定義番号1)
- 各インタフェースのIPアドレスは、以下のとおり LAN1 : 2001:db8:10::1/64 LAN2 : 2001:db8:20::1/64

● 設定条件

• エリア1からバックボーンエリアへの広報で、2001:db8:20::/64は破棄し、その他のエリア内部経路は透過させる

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置を設定する

- **1. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- [IPv6 OSPF 関連]をクリックします。
 IPv6 OSPF 関連の設定項目と「IPv6 ルータ ID 情報」が表示されます。
- **3.** IPv6 OSPF 関連の設定項目の「IPv6 OSPF エリア情報」をクリックします。 「IPv6 OSPF エリア情報」が表示されます。

4. エリア定義番号1の [修正] ボタンをクリックします。

IPv6 OSPF エリア情報(1)の「IPv6 OSPF エリア基本情報」が表示されます。

5. 「IPv6エリア間プレフィックスLSA入出力可否情報」をクリックします。

「IPv6エリア間プレフィックスLSA入出力可否情報」が表示されます。

6. 以下の項目を指定します。

 動作 →遮断
 方向 →出力
 対象経路情報 →経路情報指定 検索条件 →完全に一致 プレフィックス/プレフィックス長 →2001:db8:20::/64

<ipv6 エリア間ブレフィックスlsa入出力可否情報入力フィールド=""></ipv6>		
動作	○透過 ④遮断	
方向	○入力 ⊙出力	
	 ○ すべて ● 経路情報指定 	
対象経 路情報	 ・ 一致 ・ 検索条件 ・ マスクした結果が一致 ・ ・ マスクした結果が一致 ・ ・ ・	
	プレフィックス/ プレフィックス長 2001:db8:20:: 64	

- 7. [追加] ボタンをクリックします。
- **8.** 手順6.~7.を参考に、以下の項目を設定します。
 - 動作 →透過
 - 方向 →出力
 - 対象経路情報 →すべて
- 9. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。
27 マルチキャスト機能を使う

適用機種 SR-S716C2, 724TC1, 748TC1

本装置には、マルチキャスト機能を動作させるために以下の2種類のプロトコルがあります。

- PIM-DMプロトコル
- PIM-SM プロトコル

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

● 参照 機能説明書「2.33 マルチキャスト機能」(P.112)

27.1 マルチキャスト機能 (PIM-DM) を使う

適用機種 SR-S716C2, 724TC1, 748TC1

マルチキャスト機能 (PIM-DM) を使用すると、会社などのLAN内で、動画や音声などを配送することができます。

こんな事に気をつけて

マルチキャストでパケットを配送するルータは、すべて PIM-DM に対応している必要があります。また、ルータ上では ユニキャストのルーティングテーブルが作成されている必要があります。



ここでは、PIM-DMを利用してマルチキャストパケットを転送する場合の設定方法を説明します。 本装置1、本装置2、本装置3が以下のとおり設定されていることを前提とします。

● 前提条件

[本装置1]

- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN0のIPアドレス : 192.168.1.1/24
- LAN1のIPアドレス : 192.168.2.1/24
- LAN2のIPアドレス : 192.168.3.1/24

[本装置2]

- ユニキャストのルーティングテーブルの作成に RIPを使用する
- LAN0のIPアドレス : 192.168.4.1/24
- LAN1のIPアドレス : 192.168.2.2/24

[本装置3]

- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN0のIPアドレス : 192.168.5.1/24
- LAN1のIPアドレス : 192.168.3.2/24

● 設定条件

• マルチキャスト・ルーティングプロトコルには PIM-DM を利用する

[本装置1]

 マルチキャストパケットを転送するインタフェースとしてLAN0、LAN1、LAN2を使用し、それぞれ、 ETHER1、ETHER2、ETHER3に割り当てる

[本装置2]

• マルチキャストパケットを転送するインタフェースとして LAN0、LAN1 を使用し、それぞれ、ETHER1、 ETHER2 に割り当てる

[本装置3]

 マルチキャストパケットを転送するインタフェースとしてLAN0、LAN1を使用し、それぞれ、ETHER1、 ETHER2に割り当てる

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- IP 関連の設定項目の「マルチキャスト情報」をクリックします。
 「マルチキャスト情報」が表示されます。

マルチキャスト機能 → PIM-DM

■マルチキャスト情報 マルチキャスト機能
○使用しない ○ static ⊙ PIM-DM ○ PIM-SM

- 6. [保存] ボタンをクリックします。
- 7. 手順1.~6.を参考に、以下の項目を設定します。
 「LAN1情報」-「IP関連」-「マルチキャスト情報」
 ・マルチキャスト機能 → PIM-DM
 「LAN2情報」-「IP関連」-「マルチキャスト情報」
 ・マルチキャスト機能 → PIM-DM
- 8. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。 **「LAN0情報」-「IP関連」-「マルチキャスト情報」** マルチキャスト機能 → PIM-DM
 「LAN1情報」-「IP関連」-「マルチキャスト情報」 マルチキャスト機能 → PIM-DM

本装置3を設定する

「本装置1を設定する」を参考に、本装置3を設定します。
 「LAN0情報」-「IP関連」-「マルチキャスト情報」
 マルチキャスト機能 → PIM-DM
 「LAN1情報」-「IP関連」-「マルチキャスト情報」
 マルチキャスト機能 → PIM-DM

27.2 マルチキャスト機能 (PIM-SM)を使う

適用機種 SR-S716C2, 724TC1, 748TC1

マルチキャスト機能(PIM-SM)を使用すると、インターネットなど、十分な帯域を保証されないネットワーク 上で、マルチキャストパケットを配送することができます。

こんな事に気をつけて

- マルチキャストパケットを配送するルータは、すべて PIM-SM に対応している必要があります。また、ルータ上ではユニキャストのルーティングテーブルが作成されている必要があります。
- ネットワーク内に BSR(Bootstrap Router:ブートストラップルータ)として動作するルータを1台以上置く必要が あります。BSRは RP(Rendezvous Point:ランデブーポイント)の情報を広報します。
- ネットワーク内に RP として動作するルータを1台以上置く必要があります。パケットの配送は、RP を配送樹の頂点として開始され、その後、最短経路(SPT: Shortest Path Tree)に切り替わります。
- PIM-SMではマルチキャストパケットの配送をRPを配送樹の頂点として開始するため、RPはネットワークの中心付近に置くことをお勧めします。



ここでは、PIM-SMを利用してマルチキャストパケットを転送する場合の設定方法を説明します。

マルチキャストパケットは、はじめは RP である本装置2を経由して、本装置1→本装置2→本装置3→本装置4 の順に配送されます(一度、本装置1から本装置2に送られ、本装置2を配送樹の頂点として配送されます)。本 装置4へのパケット転送開始直後に、本装置4は SPT への切り替えを開始します。切り替えが行われると、本装 置1→本装置3→本装置4のように、最短経路を利用して配送されます(本装置1を配送樹の頂点として配送さ れます)。同様の切り替えが本装置5でも行われます。

ここでは、本装置1、本装置2、本装置3、本装置4、本装置5が以下のとおりに設定されていることを前提とします。

● 前提条件

• ユニキャストのルーティングテーブルの作成に RIP を使用する

[本装置1]

- LANOのIPアドレス : 192.168.10.1/24
- LAN1のIPアドレス : 192.168.11.1/24
- LAN2のIPアドレス : 192.168.12.1/24

[本装置2]

- LANOのIPアドレス : 192.168.12.2/24
- LAN1のIPアドレス : 192.168.13.1/24

[本装置3]

- LAN0のIPアドレス : 192.168.11.2/24
- LAN1のIPアドレス : 192.168.13.2/24
- LAN2のIPアドレス : 192.168.2.1/24
- LAN3のIPアドレス : 192.168.3.1/24

[本装置4]

- LANOのIPアドレス : 192.168.4.1/24
- LAN1のIPアドレス : 192.168.2.2/24

[本装置5]

- LAN0のIPアドレス : 192.168.5.1/24
- LAN1のIPアドレス : 192.168.3.2/24

● 設定条件

- マルチキャスト・ルーティングプロトコルには PIM-SM を利用する RP : 本装置2(192.168.12.2)
 BSR : 本装置2(192.168.12.2)
- SPTへの切り替えを行う(初期値)

[本装置1]

• マルチキャストパケットを転送するインタフェースとして LAN0、LAN1、LAN2 を使用し、それぞれ、 ETHER1、ETHER2、ETHER3 に割り当てる

[本装置2]

- マルチキャストパケットを転送するインタフェースとして LAN0、LAN1 を使用し、それぞれ、ETHER1、 ETHER2 に割り当てる
- RP : 192.168.12.2
- BSR : 192.168.12.2

[本装置3]

マルチキャストパケットを転送するインタフェースとして LAN0、LAN1、LAN2、LAN3を使用し、それぞれ、ETHER1、ETHER2、ETHER3、ETHER4に割り当てる

[本装置4]

 マルチキャストパケットを転送するインタフェースとして LAN0、LAN1を使用し、それぞれ、ETHER1、 ETHER2 に割り当てる

[本装置5]

• マルチキャストパケットを転送するインタフェースとして LAN0、LAN1を使用し、それぞれ、ETHER1、 ETHER2 に割り当てる 上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

- **1. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「マルチキャスト情報」をクリックします。 「マルチキャスト情報」が表示されます。
- 5. 以下の項目を指定します。
 - マルチキャスト機能 → PIM-SM

■マルチキャスト情報 マルチキャスト機能 ○使用しない Ostatic OPIM-DM ⊙PIM-SM

- 6. [保存] ボタンをクリックします。
- 7. 手順1.~6.を参考に、以下の項目を設定します。
 「LAN1情報」-「IP関連」-「マルチキャスト情報」
 ・マルチキャスト機能 → PIM-SM
 「LAN2情報」-「IP関連」-「マルチキャスト情報」
 ・マルチキャスト機能 → PIM-SM
- 8. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

- 「本装置1を設定する」を参考に、以下の項目を設定します。
 「LAN0 情報」-「IP 関連」-「マルチキャスト情報」
 ・マルチキャスト機能 → PIM-SM
 「LAN1 情報」-「IP 関連」-「マルチキャスト情報」
 ・マルチキャスト機能 → PIM-SM
 2. 設定メニューの詳細設定で「マルチキャスト情報」をクリックします。
- 2. 設定メニューの詳細設定で「マルナキャスト情報」をクリックします 「マルチキャスト情報」ページが表示されます。
- 「IPマルチキャスト情報」をクリックします。
 「IPマルチキャスト情報」が表示されます。

→する
→ 192.168.12.2
→する
→ 192.168.12.2

	RP候補	 ● しない ● する IPアドレ ス ブライオ リティ ●
PIM- SM	BSR候補	 ● しない ● する IPアドレ ス 192.168.12.2 ブライオ リティ ●

- 5. [保存] ボタンをクリックします。
- 6. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

本装置3を設定する

「本装置1を設定する」を参考に、本装置3を設定します。
 「LAN0情報」-「IP関連」-「マルチキャスト情報」
 マルチキャスト機能 → PIM-SM
 「LAN1情報」-「IP関連」-「マルチキャスト情報」
 マルチキャスト機能 → PIM-SM
 「LAN2情報」-「IP関連」-「マルチキャスト情報」
 マルチキャスト機能 → PIM-SM
 「LAN3情報」-「IP関連」-「マルチキャスト情報」
 マルチキャスト機能 → PIM-SM

本装置4を設定する

「本装置1を設定する」を参考に、本装置4を設定します。 **「LAN0情報」-「IP関連」-「マルチキャスト情報」** マルチキャスト機能 → PIM-SM
 「LAN1情報」-「IP関連」-「マルチキャスト情報」 マルチキャスト機能 → PIM-SM

本装置5を設定する

「本装置1を設定する」を参考に、本装置5を設定します。 「LAN0 情報」-「IP 関連」-「マルチキャスト情報」 • マルチキャスト機能 → PIM-SM 「LAN1 情報」-「IP 関連」-「マルチキャスト情報」

マルチキャスト機能 → PIM-SM

27.3 マルチキャスト機能(スタティックルーティング)を使う

<u>適用機種</u> SR-S716C2, 724TC1, 748TC1

マルチキャスト機能(スタティックルーティング)を利用すると、マルチキャストパケットが配送される経路を 静的に設定することができます。



ここでは、スタティックルーティングを利用してマルチキャストパケットの転送を行う場合を例に説明します。 本装置1、本装置2、本装置3が以下のとおり設定されていることを前提とします。

: 192.168.1.1/24

● 前提条件

LANOのIPアドレス

[本装置1]

LAN1のIPアドレス : 192.168.2.1/24
LAN2のIPアドレス : 192.168.3.1/24
[本装置 2]
LAN0のIPアドレス : 192.168.4.1/24
LAN1のIPアドレス : 192.168.2.2/24
[本装置 3]
LAN0のIPアドレス : 192.168.5.1/24
LAN1のIPアドレス : 192.168.5.1/24
LAN1のIPアドレス : 192.168.5.1/24

● 設定条件

- マルチキャスト・スタティックルーティングを利用する
- マルチキャストパケットの送信元アドレスは 192.168.1.2 とする
- マルチキャストパケットのグループアドレスは 239.255.1.1 とする

[本装置1]

 マルチキャストパケットを転送するインタフェースとして LAN0、LAN1、LAN2 を 使用し、それぞれ、 ETHER1、ETHER2、ETHER3 に割り当てる

[本装置2]

 マルチキャストパケットを転送するインタフェースとして LAN0、LAN1 を使用し、それぞれ、ETHER1、 ETHER2 に割り当てる

[本装置3]

 マルチキャストパケットを転送するインタフェースとして LAN0, LAN1 を使用し、それぞれ、ETHER1、 ETHER2 に割り当てる

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。
 「LAN0 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「マルチキャスト情報」をクリックします。 「マルチキャスト情報」が表示されます。
- 5. 以下の項目を指定します。
 - マルチキャスト機能 → static

■マルチキャスト情報 マルチキャスト機能
○使用しない ③ static ○ PIM-DM ○ PIM-SM

- 6. [保存] ボタンをクリックします。
- 7. 手順1.~6.を参考に、以下の項目を設定します。
 「LAN1情報」-「IP関連」-「マルチキャスト情報」
 ・マルチキャスト機能 → static
 「LAN2情報」-「IP関連」-「マルチキャスト情報」
 ・マルチキャスト機能 → static
- 8. 設定メニューの詳細設定で「マルチキャスト情報」をクリックします。 「マルチキャスト情報」ページが表示されます。
- **9.** 「IP マルチキャストスタティック経路情報」をクリックします。 「IP マルチキャストスタティック経路情報」が表示されます。

- 配送元ホストアドレス → 指定する
 - → 192.168.1.2
- マルチキャストグループアドレス → 239.255.1.1
- 入力インタフェース → LAN0
- ・ 出力インタフェース → lan1-lan2
- グループ参加 → しない

<ipマルチキャストスタティック経路情報入力フィールド></ipマルチキャストスタティック経路情報入力フィールド>		
配送元ホストアドレス	 すべて 指定する 192.168.1.2 	
マルチキャストグループアドレス	239.255.1.1	
入力インタフェース	LANO 🗸	
出力インタフェース	lan1-lan2	
グループ参加	⊙したい ○する	

- 11. [追加] ボタンをクリックします。
- **12. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

「LAN情報」

「LAN0情報」-「IP関連」-「マルチキャスト情報」

- マルチキャスト機能 → static
- 「LAN1情報」-「IP関連」-「マルチキャスト情報」
- マルチキャスト機能 → static

「マルチキャスト情報」

「IPマルチキャストスタティック経路情報」

- 配送元ホストアドレス → 指定する
- → 192.168.1.2
 マルチキャストグループアドレス → 239.255.1.1
- 入力インタフェース → LAN1
- ・ 出力インタフェース → lan0
- グループ参加 → しない

本装置3を設定する

「本装置1を設定する」を参考に、本装置3を設定します。

「LAN情報」

- 「LAN0情報」-「IP関連」-「マルチキャスト情報」
- マルチキャスト機能 → static
- 「LAN1情報」-「IP関連」-「マルチキャスト情報」
- マルチキャスト機能 → static

「マルチキャスト情報」 「IPマルチキャストスタティック経路情報」

- ・ 配送元ホストアドレス
 → 指定する
 → 192.168.1.2
- マルチキャストグループアドレス → 239.255.1.1
- 入力インタフェース → LAN1
- ・ 出力インタフェース → lan0
- グループ参加 → しない

28 IP フィルタリング機能を使う

適用機種 全機種

本装置を経由してインターネットに送出されるパケット、またはインターネットから受信したパケットをIPアドレスとポート番号の組み合わせで制御することによって、ネットワークのセキュリティを向上させることができます。

● 参照 機能説明書「2.34 IPフィルタリング機能」(P.115)

こんな事に気をつけて

SR-S308TL1/310TL2/316TL1/318TL2/324TL2では、フィルタリング機能(IPv4/IPv6)およびQoS書き換え機能(IPv4/IPv6)を同時に使用することができません。

IP フィルタリングを有効にするためには「装置情報」-「資源情報」で、QoS 機能および IPv4 プロトコルを選択してください。



IP フィルタリングの条件

本装置では、ACL番号で指定したACL定義の中で、以下の条件を指定することによってデータの流れを制御できます。

- プロトコル
- 送信元情報(IPアドレス/アドレスマスク/ポート番号)
- あて先情報(IPアドレス/アドレスマスク/ポート番号)
- IPパケットのTOS値/DSCP値

☆ ヒント

◆ IP アドレスとアドレスマスクの決め方

IPフィルタリング条件の要素には「IPアドレス」と「アドレスマスク」があります。制御対象となるパケットは、本装置に届いたパケットのIPアドレスとアドレスマスクの論理積の結果が、指定したIPアドレスと一致したものに限ります。

IP フィルタリングの設計方針

IP フィルタリングの設計方針には大きく分類して以下の2つがあります。

- A. 基本的にパケットをすべて遮断し、特定の条件のものだけを透過させる
- B. 基本的にパケットをすべて透過させ、特定の条件のものだけを遮断する

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 外部の特定サービスへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけを許可する
- また、設計方針 Bの例として、以下の設定例について説明します。
- 外部の特定サーバへのアクセスだけを禁止する
- 外部から特定サーバへのpingだけを禁止する

こんな事に気をつけて

- IP フィルタリングでDHCP(ポート番号67、68)でのアクセスを制限する設定を行った場合、DHCP機能が使用できなくなる場合があります。
- IP フィルタリング条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用 されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。

28.1 外部の特定サービスへのアクセスだけを許可する

適用機種 全機種

ここでは、一時的にLANを作成し、外部LANのすべてのWebサーバに対してアクセスすることだけを許可し、 ほかのサーバ(FTPサーバなど)へのアクセスを禁止する場合の設定方法を説明します。ただし、Webサーバ名 を解決するために、DNSサーバへのアクセスは許可します。

補足

DNSサーバに問い合わせが発生する場合、DNSサーバへのアクセスを許可する必要があります。 DNSサーバへのアクセスを許可することによって、Webサービス以外でドメイン名を指定した場合もDNSサーバへ の発信が発生します。あらかじめ接続するWebサーバが決まっている場合は、本装置のDNSサーバ機能を利用する ことによって、DNSサーバへの発信を抑止することができます

こんな事に気をつけて

SR-S308TL1/310TL2/316TL1/318TL2/324TL2では、フィルタリング機能(IPv4/IPv6)およびQoS書き換え機能 (IPv4/IPv6)を同時に使用することができません。

IP フィルタリングを有効にするためには「装置情報」-「資源情報」で、QoS 機能および IPv4 プロトコルを選択してください。



● フィルタリング設計

- 内部 LAN のホスト(192.168.1.0/24)から外部 LAN の Web サーバへのアクセスを許可
- 内部LANのホスト(192.168.1.0/24)から外部LANのDNSサーバへのアクセスを許可
- ICMPの通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

● フィルタリングルール

- ICMPの通信を許可するためには (1)ICMPパケットを透過させる
- その他をすべて遮断するには (1)すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合の設定例を示します。

任意のWebサーバのポート80へのTCPパケットを透過させる(内部LAN→外部LAN)

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名 → acl0

	<acl情報追加フィールド></acl情報追加フィールド>
定義名	aci0

3. [追加] ボタンをクリックします。

「ACL定義情報(acl0)」ページが表示されます。

4. 「IP定義情報」をクリックします。

「IP定義情報」が表示されます。

以下の項目を指定します。 5.

•	プロトコル	→tcp
•	送信元情報	
	IP アドレス	→ 192.168.1.0
	アドレスマスク	→24 (255.255.255.0)
•	あて先情報	

- IPアドレス →指定しない アドレスマスク →0 (0.0.0) →指定なし
- QoS

■IP定義	情報	3
ブロトコル		tcp (番号指定: 7その他"を選択時のみ有効で す)
、 _{¥信二桂} IPアドレス		192.168.1.0
報	アトレスマ スク	24 (255.255.255.0)
あて生情	IPアドレス	
報	アトレスマ スク	0 (0.0.0)
QoS		指定なし ✓ TOS、または、DSCPを選択時に値を入力してく ださい

- 6. [保存] ボタンをクリックします。
- 7. 「TCP定義情報」をクリックします。

「TCP定義情報」が表示されます。

- 送信元ポート番号 →指定しない
- あて先ポート番号 →80

■TCP定義情報	3
送信元ボート番号	
あて先ポート番号	80

- 9. [保存] ボタンをクリックします。
- 10. 設定メニューの詳細設定の「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

- **11.** 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。 「LAN1 情報」ページが表示されます。
- **12.** 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

13. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IPフィルタリング情報」が表示されます。

14. 以下の項目を指定します。

- 動作 →透過
- ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作	◎透過 ○遮断	
ACL定義番号	0 参照	

15. [追加] ボタンをクリックします。

Web サーバからの応答パケットを透過させる(外部 LAN →内部 LAN)

16. 手順1.~15を参考に、以下の項目を指定します。

「ACL情報」

定義名

→acl1

「ACL定義情報(acl1)」-「IP定義情報」

「ACL定義情報(acl1)」-「TCP定義情報」

•	送信元ポート番号	→80
•	あて先ポート番号	→指定しない
٢L	AN 情報」-「IP 関連」	
ΓII	^D フィルタリング情報」	
•	動作	→透過
•	ACL定義番号	→ 1

DNS サーバのポート 53 への UDP パケットを透過させる (内部 LAN → 外部 LAN)

17. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→acl2		
٢A	「ACL定義情報(acl2)」-「IP定義情報」			
•	プロトコル	→udp		
•	送信元情報 IPアドレス アドレスマスク	→ 192.168.1.0 → 24 (255.255.255.0)		
•	あて先情報 IPアドレス アドレスマスク	→ 192.168.0.10 → 32 (255.255.255.255)		
	• •			

• QoS →指定なし

18. 「UDP 定義情報」をクリックします。

「UDP定義情報」が表示されます。

19. 以下の項目を指定します。

- 送信元ポート番号 →指定しない
- あて先ポート番号 → 53

UDP定義情報	3
送信元ポート番号	
あて先ボート番号	53

- 20. [保存] ボタンをクリックします。
- 21. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- ACL定義番号 →2

DNS サーバからの応答パケットを透過させる(外部 LAN → 内部 LAN)

22. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」 定義名 →acl3 「ACL定義情報(acl3)」-「IP定義情報」 • プロトコル →udp • 送信元情報 IPアドレス → 192.168.0.10 アドレスマスク → 32 (255.255.255.255) あて先情報 IPアドレス → 192.168.1.0 アドレスマスク →24 (255.255.255.0) • QoS →指定なし

23. 手順18.~20.を参考に、以下の項目を指定します。

「ACL定義情報 (acl3)」-「UDP 定義情報」

- 送信元ポート番号 →53
- あて先ポート番号 →指定しない

24. 手順 10. ~ 15. を参考に、以下の項目を指定します。 「LAN 情報」-「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- ACL定義番号 →3

ICMP のパケットを透過させる

25. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→acl4
ΓA	CL定義情報(acl4)」-「IP定義情	青報」
•	プロトコル	→icmp
•	送信元情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0.0)
•	あて先情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0.0)
•	QoS	→指定なし

26. 「ICMP 定義情報」をクリックします。

「ICMP定義情報」が表示されます。

• IC	MP				
タ	イプ			→指定し	ない
	ード			→指定し	ない
			'n		[]
	ICMP.	正我们	牧		3
IC	MD	タイプ			
10	IVIE	コード			
		- -			

- 28. [保存] ボタンをクリックします。
- 29. 手順 10. ~ 15. を参考に、以下の項目を指定します。
 「LAN 情報」-「IP 関連」
 「IP フィルタリング情報」
 - 動作 →透過
 ACL定義番号 →4
- 残りのパケットをすべて遮断する
- 30. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

• 定義名 → acl5

「ACL定義情報(acl5)」-「IP定義情報」

•	プロトコル	→すべて
•	送信元情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0.0)
•	あて先情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0.)
	0.0	

• QoS →指定なし

31. 手順23.~24.を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」 「IP フィルタリング情報」

- 動作 →遮断
- ACL定義番号 →5
- **32. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

28.2 外部の特定サービスへのアクセスだけを許可する(IPv6フィルタ リング)

適用機種 全機種

ここでは、一時的にLANを作成し、外部LANのすべてのWeb サーバに対してアクセスすることだけを許可し、 ほかのサーバ(ftp サーバなど)へのアクセスを禁止する場合の設定方法を説明します。ただし、Web サーバ名 を解決するために、DNSサーバへのアクセスは許可します。



DNSサーバに問い合わせが発生する場合、DNSサーバへのアクセスを許可する必要があります。 me DNS サーバに回いロクセルチェック物ロ、DNS サーバス以外でドメイン名を指定した場合もDNS サーバへ DNS サーバへのアクセスを許可することによって、Web サービス以外でドメイン名を指定した場合もDNS サーバへ の発信が発生します。あらかじめ接続するWebサーバが決まっている場合は、本装置のDNSサーバ機能を利用する ことによって、DNSサーバへの発信を抑止することができます。

こんな事に気をつけて

SR-S308TL1/310TL2/316TL1/318TL2/324TL2では、フィルタリング機能(IPv4/IPv6)および QoS 書き換え機能 (IPv4/IPv6)を同時に使用することができません。

IPフィルタリングを有効にするためには「装置情報」-「資源情報」で、QoS機能およびIPv4プロトコルを選択してく ださい。



● フィルタリング設計

- 内部 LAN 上のホスト(2001:db8:1::/64)から任意の Web サーバへのアクセスを許可
- 内部 LAN 上のホスト(2001:db8:1::/64)から外部 LAN の DNS サーバへのアクセスを許可
- ICMPv6の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPv6 は、IPv6 通信を行う際にさまざまな制御メッセージを交換します。ICMPv6の通信を遮断すると正常な通信が できなくなる場合がありますので、ICMPv6の通信を透過させる設定を行ってください。

● フィルタリングルール

- ICMPv6の通信を許可するためには (1)ICMPv6パケットを透過させる
- その他をすべて遮断するには

 (1)すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合の設定例を示します。

任意のWebサーバのポート80へのTCPパケットを透過させる(内部LAN→外部LAN)

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

→ acl0

	<acl情報追加フィールド></acl情報追加フィールド>
定義名	ac10

- 【追加】ボタンをクリックします。
 「ACL定義情報(acl0)」ページが表示されます。
- **4.** 「IPv6 定義情報」をクリックします。 「IPv6 定義情報」が表示されます。

5. 以下の項目を指定します。

- プロトコル
- 送信元 IPv6 アドレス/プレフィックス
- あて先IPv6アドレス/プレフィックス

→2001:db8:1::/64 →指定しない

→指定なし

→ tcp

• QoS

■IPv6定義情報	3
プロトコル	tcp ▼ (番号指定: / ~ その他"を選択時のみ有効です)
送信元IPv6アドレス/ ブレフィックス	2001:db8:1::
あて先IPv6アトレス/ ブレフィックス	
QoS	指定なし ♥ Traffic Class、または、DSCPを選択時に値を入 力してください

6. [保存] ボタンをクリックします。

- **7. 「TCP定義情報」をクリックします**。 「TCP定義情報」が表示されます。
- 8. 以下の項目を指定します。
 - ・ 送信元ポート番号 →指定しない
 - あて先ポート番号 →80

TCP定義情報		3
送信元ボート番号		
あて先ボート番号	80	

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューの詳細設定の「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **11.** 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。 「LAN1 情報」ページが表示されます。
- 12. 「IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

- **13.** IPv6 関連の設定項目の「IPv6 フィルタリング情報」をクリックします。 「IPv6 フィルタリング情報」が表示されます。
- 14. 以下の項目を指定します。
 - 動作 →透過
 - ACL定義番号 →0

「ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の「選択」 ボタンをクリックして設定します。

<ipv6フィルタリング情報入力フィールド></ipv6フィルタリング情報入力フィールド>		
動作	⊙透過 ○遮断	
ACL定義番号	0 参照	

- 15. [追加] ボタンをクリックします。
- Web サーバからの応答パケットを透過させる(外部 LAN → 内部 LAN)

16. 手順1.~15を参考に、以下の項目を指定します。

「ACL情報」

- 定義名 → acl1
- 「ACL定義情報(acl1)」-「IPv6定義情報」
- プロトコル
- 送信元 IPv6 アドレス/プレフィックス →指定しない
- あて先IPv6アドレス/プレフィックス →2001:db8:1::/64
- QoS →指定なし

→ tcp

「ACL定義情報(acl1)」-「TCP定	義情報」
• 送信元ポート番号	→指定しない
• あて先ポート番号	→80
「LAN 情報」-「IPv6 関連」	
「IPv6フィルタリング情報」	
 ● 動作 	→透過
• ACL定義番号	→ 1

DNS サーバのポート 53 への UDP パケットを透過させる (内部 LAN → 外部 LAN)

17. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

18.

19.

•	定義名		→acl2
ΓA	CL定義情報(acl2)」-「IPv6定義	青報」	
•	プロトコル		→udp
•	送信元 IPv6 アドレス/プレフィック	ス	→2001:db8:1::/64
•	あて先IPv6アドレス/プレフィック	ス	→指定しない
•	QoS		→指定なし
ΓL	IDP 定義情報」をクリックします。	,	
ΓU	DP定義情報」が表示されます。		
以	下の項目を指定します。		
•	送信元ポート番号 -	◆指定しない	

あて先ポート番号 →53

■UDP定義情報		3
送信元ボート番号		
あて先ポート番号	53	

- 20. [保存] ボタンをクリックします。
- 21. 手順 10.~15.を参考に、以下の項目を指定します。
 「LAN 情報」-「IPv6 関連」
 「IPv6 フィルタリング情報」
 - 動作 →透過
 - ACL定義番号 →2

DNS サーバからの応答パケットを透過させる(外部 LAN → 内部 LAN)

22. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」 定義名 → acl3 「ACL定義情報(acl3)」-「IPv6定義情報」 • プロトコル → udp • 送信元 IPv6 アドレス/プレフィックス →指定しない • あて先IPv6アドレス/プレフィックス → 2001:db8:1::/64 →指定なし • QoS 23. 手順18.~20.を参考に以下の項目を指定します。 「ACL定義情報(acl3)」-「UDP定義情報」 送信元ポート番号 →53 あて先ポート番号 →指定しない 24. 手順10.~15.を参考に、以下の項目を指定します。 「LAN 情報」-「IPv6 関連」 「IPv6フィルタリング情報」 動作 →透渦 • ACL 定義番号 →3

ICMPv6のパケットを透過させる

25. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

• 定義名 → acl4

「ACL定義情報(acl4)」-「IPv6定義情報」

- プロトコル → icmpv6
- 送信元 IPv6 アドレス/プレフィックス →指定しない あて先 IPv6 アドレス/プレフィックス→指定しない
- QoS →指定なし
- **26.** 「ICMP 定義情報」をクリックします。

「ICMP定義情報」が表示されます。

27. 以下の項目を指定します。

ICMP
 タイプ

コード

→指定しない	
→指定しない	

	3	

28. [保存] ボタンをクリックします。

29. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」-「IPv6 関連」 「IPv6 フィルタリング情報」

- 動作 →透過
- ACL定義番号 →4

残りのパケットをすべて遮断する

30. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

- ・ 定義名 → acl5
 「ACL定義情報 (acl5)」-「IPv6定義情報」
 ・ プロトコル → すべて
 ・ 送信元 IPv6 アドレス/プレフィックス →指定しない
 ・ あて先 IPv6 アドレス/プレフィックス →指定しない
 ・ QoS →指定なし
- 31. 手順10.~15.を参考に、以下の項目を指定します。

「LAN情報」-「IPv6 関連」

「IPv6フィルタリング情報」

- 動作 → 遮断
- ACL定義番号 →5
- **32. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

28.3 外部から特定サーバへのアクセスだけを許可する

適用機種 全機種

ここでは、内部LANの特定サーバに対するアクセスを許可し、ほかのサーバに対するアクセスを禁止する場合の 設定方法を説明します。ただし、Webサーバ名を解決するためにDNSサーバへのアクセスは許可します。

DNS サーバに問い合わせが発生する場合、DNS サーバへのアクセスを許可する必要があります。
DNS サーバへのアクセスを許可することによって、Web サービス以外でもドメイン名で指定されるとDNS サーバへの問い合わせが発生します。あらかじめ接続するWeb サーバが決まっている場合は、本装置のDNS サーバ機能を利用することで、DNS サーバへの問い合わせを抑止することができます。

こんな事に気をつけて

SR-S308TL1/310TL2/316TL1/318TL2/324TL2では、フィルタリング機能(IPv4/IPv6)およびQoS書き換え機能(IPv4/IPv6)を同時に使用することができません。

IP フィルタリングを有効にするためには「装置情報」-「資源情報」で、QoS 機能および IPv4 プロトコルを選択してください。



● フィルタリング設計

- 内部 LAN のホスト(192.168.1.5/32)を Web サーバとして利用を許可
- 内部 LAN のネットワークへの DNS サーバへのアクセスを許可
- ICMPの通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

● フィルタリングルール

- 内部 LAN のホストの Web サーバとしての利用を許可するには

 (1) 192.168.1.5/32 のポート 80 (http) への TCP パケットを透過させる
 (2) Web サーバからの応答パケットを透過させる

- ICMPの通信を許可するためには (1)ICMPパケットを透過させる
- その他をすべて遮断するには (1)すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合の設定例を示します。

Webサーバのポート80へのTCPパケットを透過させる(外部LAN→内部LAN)

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名 → acl0

	<acl情報追加フィールド></acl情報追加フィールド>
定義名	ac IO

3. [追加] ボタンをクリックします。

「ACL定義情報(acl0)」ページが表示されます。

4. 「IP定義情報」をクリックします。

「IP定義情報」が表示されます。

以下の項目を指定します。 5.

•	プロトコル	→tcp
•	送信元情報	
	IP アドレス	→ 192.168.0.0
	アドレスマスク	→24 (255.255.255.0)
•	あて先情報	

- IPアドレス → 192.168.1.5 アドレスマスク →32 (255.255.255.255)
- QoS

→指定なし

IP定義	情報	3
ブロトコル		tep (番号指定: 7その他 ″を選択時のみ有効で す)
送信元情	IPアドレス	192.168.0.0
報	アトレスマ スク	24 (255.255.255.0)
あて生情	IPアドレス	
報	アトレスマ スク	0 (0.0.0.0)
QoS		指定なし <mark>→</mark> TOS、または、DSCPを選択時に値を入力してく ださい

- 6. [保存] ボタンをクリックします。
- 7. 「TCP定義情報」をクリックします。

「TCP定義情報」が表示されます。

- 送信元ポート番号 →指定しない
- あて先ポート番号 →80

■TCP定義情報	3
送信元ポート番号	
あて先ボート番号	80

- 9. [保存] ボタンをクリックします。
- **10**. 設定メニューの詳細設定の「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

- **11.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- **12.** 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

13. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IPフィルタリング情報」が表示されます。

14. 以下の項目を指定します。

- 動作 →透過
- ACL定義番号 →0

▲ 「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作		⊙透過 ○遮断
ACL定義番号		0 参照

15. [追加] ボタンをクリックします。

Web サーバからの応答パケットを透過させる(内部 LAN → 外部 LAN)

16. 手順1.~15.を参考に、以下の項目を指定します。

「ACL情報」

定義名

→acl1

「ACL定義情報(acl1)」-「IP定義情報」

•	プロトコル	→tcp
•	送信元情報 IP アドレス アドレスマスク	→指定しない →0(0.0.0.0)
•	あて先情報 IPアドレス アドレスマスク	→ 192.168.0.0 → 24 (255.255.255.0)
	0.0	

• QoS →指定なし

「ACL定義情報(acl1)」-「TCP定義情報」

• 送信元ポート番号	→80
• あて先ポート番号	→指定しない
「LAN情報」-「IP関連」	
「IP フィルタリング情報」	
• 動作	→透過
 ACL定義番号 	→ 1

DNS サーバのポート 53 への UDP パケットを透過させる(外部 LAN → 内部 LAN)

17. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→acl2
ГA	CL定義情報(acl2)」-「IP定義情	青報」
•	プロトコル	→udp
•	送信元情報 IPアドレス アドレスマスク	→ 192.168.0.0 → 24 (255.255.255.0)
•	あて先情報 IPアドレス アドレスマスク	→ 192.168.1.10 → 32 (255.255.255.255)
•	QoS	→指定なし

18. 「UDP 定義情報」をクリックします。

「UDP定義情報」が表示されます。

19. 以下の項目を指定します。

- 送信元ポート番号 →指定しない
- あて先ポート番号 →53

UDP定義情報		3
送信元ポート番号		
あて先ボート番号	53	

- 20. [保存] ボタンをクリックします。
- 21. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- ACL定義番号 →2

DNS サーバからの応答パケットを透過させる(内部 LAN → 外部 LAN)

22. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」 定義名 →acl3 「ACL定義情報(acl3)」-「IP定義情報」 • プロトコル →udp • 送信元情報 IPアドレス → 192.168.1.10 アドレスマスク → 32 (255.255.255.255) あて先情報 IPアドレス → 192.168.0.0 アドレスマスク →24 (255.255.255.0) • QoS →指定なし

23. 手順18.~20.を参考に、以下の項目を指定します。

「ACL定義情報 (acl3)」-「UDP 定義情報」

- 送信元ポート番号 →53
- あて先ポート番号 →指定しない

24. 手順 10. ~ 15. を参考に、以下の項目を指定します。 「LAN 情報」-「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- ACL定義番号 →3

ICMP のパケットを透過させる

25. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→acl4
٢A	CL定義情報(acl4)」-「IP定義情	青報」
•	プロトコル	→icmp
•	送信元情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0.0)
•	あて先情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0.0)
•	QoS	→指定なし

26. 「ICMP 定義情報」をクリックします。

「ICMP定義情報」が表示されます。

• IC	MP				
タ	イプ			→指定し	ない
	ード			→指定し	ない
			'n		[]
	ICMP.	正我们	牧		3
IC	MD	タイプ			
10	IVIE	コード			
		- -			

- 28. [保存] ボタンをクリックします。
- 29. 手順 10. ~ 15. を参考に、以下の項目を指定します。
 「LAN 情報」-「IP 関連」
 「IP フィルタリング情報」
 動作 →透過
 - ACL定義番号 →4
- 残りのパケットをすべて遮断する
- 30. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

• 定義名 → acl5

「ACL定義情報(acl5)」-「IP定義情報」

•	プロトコル	→すべて
•	送信元情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0.0)
•	あて先情報 IPアドレス アドレスマスク	→指定しない →0 (0.0.0.0)
	0.0	

- QoS →指定なし
- 31. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」 「IP フィルタリング情報」

- 動作 →遮断
- ACL定義番号 →5
- **32. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

28.4 外部の特定サーバへのアクセスだけを禁止する

適用機種 全機種

ここでは、外部 LAN の FTP サーバに対するアクセスを禁止する場合の設定方法を説明します。

こんな事に気をつけて

SR-S308TL1/310TL2/316TL1/318TL2/324TL2では、フィルタリング機能(IPv4/IPv6)およびQoS書き換え機能 (IPv4/IPv6)を同時に使用することができません。 IPフィルタリングを有効にするためには「装置情報」-「資源情報」で、QoS機能およびIPv4プロトコルを選択してく

ださい。



● フィルタリング設計

• 内部LANのホスト(192.168.1.0/24)から外部LANのFTPサーバ(192.168.0.5)へのアクセスを禁止

● フィルタリングルール

FTPサーバへのアクセスを禁止するには

 (1)192.168.1.0/24から192.168.0.5のポート21(ftp)へのTCPパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

```
→ ftp_deny
```

<acl情報追加フィールド></acl情報追加フィールド>		
定義名 ftp_deny ftp_den		

3. [追加] ボタンをクリックします。

「ACL定義情報(ftp_deny)」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP定義情報」が表示されます。

• QoS

•	プロトコル	→tcp
•	送信元情報 IP アドレス アドレスマスク	→ 192.168.1.0 → 24 (255.255.255.0)
•	あて先情報 IPアドレス アドレスマスク	→ 192.168.0.5 → 32 (255.255.255.255)

→指	定なし
→指	定なし

■IP定義情報		
ブロトコル		tcp く (番号指定: でその他"を選択時のみ有効です)
送信元情	IPアドレス	192.168.1.0
報	アトレスマ スク	24 (255.255.255.0)
あて先情	IPアドレス	192.168.0.5
報	アトレスマ スク	32 (255.255.255.255) 💌
QoS		指定なし ▼ TOS、または、DSCPを選択時に値を入力してく ださい

- 6. [保存] ボタンをクリックします。
- 7. 「TCP定義情報」をクリックします。

「TCP定義情報」が表示されます。

- 8. 以下の項目を指定します。
 - 送信元ポート番号 →21
 - あて先ポート番号 →指定しない

■TCP定義情報	3
送信元ボート番号	21
あて先ポート番号	

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューの詳細設定の「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **11.** 「LAN 情報」でインタフェースが LAN1 の [修正] ボタンをクリックします。 「LAN1 情報」ページが表示されます。
- **12. 「IP 関連」をクリックします。** IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **13.** IP 関連の設定項目の「IP フィルタリング情報」をクリックします。 「IP フィルタリング情報」が表示されます。

- 動作
- ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択]
 ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作		○透過 ⊙ 遮断
ACL定義番号		0 参照

→遮断

- 15. [追加] ボタンをクリックします。
- **16. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

28.5 外部から特定サーバへの ping だけを禁止する

適用機種 全機種

ここでは、内部LANの特定のサーバに対するping(ICMP ECHO)を禁止し、この特定のサーバに対するほかの ICMPパケット、その他のプロトコルのパケットおよびほかのホストに対するパケットはすべて許可する場合の設 定方法を説明します。

こんな事に気をつけて

SR-S308TL1/310TL2/316TL1/318TL2/324TL2では、フィルタリング機能(IPv4/IPv6)およびQoS書き換え機能(IPv4/IPv6)を同時に使用することができません。

IP フィルタリングを有効にするためには「装置情報」-「資源情報」で、QoS 機能および IPv4 プロトコルを選択してください。



● フィルタリング設計

- 内部 LAN のサーバ(192.168.1.5/32) に対して外部からの ping (ICMP ECHO)を禁止
- その他はすべて通過
- フィルタリングルール
- 内部LANのサーバ(192.168.1.5/32)に対して外部からのping(ICMP ECHO)を禁止するには (1)192.168.1.5/32へのICMP TYPE 8のICMPパケットを遮断する
- その他のパケットを許可する

 (1)すべてのパケットを透過させる

上記のフィルタリングルールに従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

→ ping_deny

<acl情報追加フィールド></acl情報追加フィールド>			
定義名	ping_deny		

3. [追加] ボタンをクリックします。

「ACL定義情報 (ping_deny)」ページが表示されます。
4. 「IP定義情報」をクリックします。

「IP定義情報」が表示されます。

5. 以下の項目を指定します。

• プロトコル	→icmp
 送信元情報 IP アドレス アドレスマスク 	→指定しない →0 (0.0.0.0)
 あて先情報 IPアドレス アドレスマスク 	→ 192.168.1.5 → 32(255.255.255

- → 32 (255.255.255.255)
- QoS

→指定なし

■IP定義情報				
ブロトコル		icmp (番号指定: "その他"を選択時のみ有効で す)		
送信元情	IPアドレス			
報	アトレスマ スク	0 (0.0.0)		
あて生情	IPアドレス	192.168.1.5		
報	アトレスマ スク	32 (255.255.255.255) 💌		
QoS		指定なし ▼ TOS、または、DSCPを選択時に値を入力してく ださい		

- 6. [保存] ボタンをクリックします。
- 7. 「ICMP定義情報」をクリックします。 「ICMP定義情報」が表示されます。

以下の項目を指定します。 8.

• ICMP タイプ コード

→8 →指定しない

	定義情報	k <u>13</u>
	タイプ	8
ICIMP	コード	

- 9. [保存] ボタンをクリックします。
- 設定メニューの詳細設定の「LAN 情報」をクリックします。 10. 「LAN 情報 | ページが表示されます。
- 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 11. 「LAN0情報」ページが表示されます。
- 12. 「IP 関連」をクリックします。 IP関連の設定項目と「IPアドレス情報」が表示されます。

13. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IPフィルタリング情報」が表示されます。

14. 以下の項目を指定します。

- 動作 → 遮断
- ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択]
 ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>			
動作			
ACL定義番号	0 参照		

15. [追加] ボタンをクリックします。

16. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

29 DSCP 値書き換え機能を使う

適用機種 全機種

本装置を経由してネットワークに送信される、またはネットワークから受信したパケットをIPアドレスとポート 番号の組み合わせでDSCP値を変更することにより、ポリシーベースネットワークのポリシーに合わせることが できます。

● 参照 機能説明書「2.35 DSCP 値書き換え機能」(P.117)

こんな事に気をつけて

SR-S308TL1/310TL2/316TL1/318TL2/324TL2では、フィルタリング機能およびQoS書き換え機能を同時に使用することができません。

また、それぞれの機能でIPv4およびIPv6条件を同時に使用することができません。

DSCP 値書き換えを有効にするためには「装置情報」-「資源情報」で、QoS 機能および IPv6 プロトコルを選択してください。

DSCP値書き換え機能の条件

本装置では、ACL番号で指定したACL定義の中で、以下の条件を指定することによってポリシーベースネット ワークのポリシーに合ったDSCP値に書き換えることができます。

- プロトコル
- 送信元情報(IPアドレス/アドレスマスク/ポート番号)
- あて先情報(IPアドレス/アドレスマスク/ポート番号)
- IPパケットのTOS値またはDSCP値(全機種) または、

IPv6パケットのTraffic Class値またはDSCP値(SR-S324TC1/328TR1/348TC1/724TC1/748TC1のみ)

ここではネットワークが以下のポリシーを持つ場合の設定方法を説明します。

- FTP (DSCP 値 10) を最優先とする
- その他はなし



● 設定条件

•	送信元IPアドレス/アドレスマスク	: 192.168.1.0/24
•	送信元ポート番号	:指定しない
•	あて先IPアドレス/アドレスマスク	:指定しない
•	あて先ポート番号	:20(ftp-dataのポート番号)、21(ftpのポート番号)
•	プロトコル	: TCP
•	DSCP值	: 0
•	新DSCP值	: 10

上記の設定条件に従って設定を行う場合の設定例を示します。

FTP サーバのアクセスで DSCP 値を0から10に書き換える

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

2. 以下の項目を指定します。

定義名

	<acl情報追加フィールド></acl情報追加フィールド>
定義名	aci0

→ acl0

3. [追加] ボタンをクリックします。

「ACL定義情報 (acl0)」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP定義情報」が表示されます。

5. 以下の項目を指定します。

- プロトコル → tcp
 送信元情報
 IP アドレス → 192.168.1.0
 アドレスマスク → 24 (255.255.255.0)
- あて先情報
 IPアドレス →指定しない
 アドレスマスク → 0 (0.0.0.0)
 QoS → DSCP

→0



- 6. [保存] ボタンをクリックします。
- 7. 「TCP定義情報」をクリックします。 「TCP定義情報」が表示されます。
- 8. 以下の項目を指定します。
 - 送信元ポート番号 →指定しない
 - あて先ポート番号 → 20 (ftp-data のポート番号)、21 (ftp のポート番号)

■TCP定義情報		3
送信元ポート番号		
あて先ボート番号	20	

- 9. [保存] ボタンをクリックします。
- 設定メニューの詳細設定で「LAN 情報」をクリックします。 10. 「LAN情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN0の[修正] ボタンをクリックします。 11. 「LAN0 情報」ページが表示されます。
- 12. 「IP 関連」をクリックします。 IP関連の設定項目と「IPアドレス情報」が表示されます。
- 「DSCP値書き換え情報」をクリックします。 13. 「DSCP値書き換え情報」が表示されます。
- 14. 以下の項目を指定します。
 - 新DSCP **→**10
 - →0 ACL定義番号

<dscp値書き換え情報入力フィールド></dscp値書き換え情報入力フィールド>			
新DSCP 10			
ACL定義番号	0 参照		

- 15. [追加] ボタンをクリックします。
- 16. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

30 VRRP 機能を使う

適用機種 SR-S716C2, 724TC1, 748TC1

VRRP機能は2つ以上のルータがグループを形成し、1台のルータ(仮想ルータ)のように動作します。グループ 内の各ルータには優先度が設定されており、その優先度に従ってマスタルータ(実際に経路情報を処理する装置) とバックアップルータ(マスタルータで異常を検出したときに経路情報の処理を引き継ぐ装置)を決定します。 本装置には、以下のVRRP機能があります。

- ・ 簡易ホットスタンバイ機能
 動的に経路制御(RIPなど)できない端末から、別のネットワークへの通信に使用しているルータがなんらか
 の理由で中継できなくなった場合、自動でほかのルータが通信をバックアップします。
- クラスタリング機能 VRRPのグループを複数設定することで、通信の負荷分散と冗長構成を実現します。本装置では、2台のルー タを組み合わせることで簡易ホットスタンバイによる信頼性の高い通信を実現できます。

● 参照 機能説明書「2.36 VRRP機能」(P.119)

こんな事に気をつけて

- 本装置の電源の投入、マスタルータでの設定反映、または装置リセットを実行した場合、バックアップルータがマスタルータとなることがあります。プリエンプトモードが on の場合は自動で切り戻りますが、プリエンプトモードが offの場合は、操作メニューの「VRRP 手動切り戻し」で切り戻しを行う必要があります。
- ・ 優先度の値が大きい方が優先的にマスタルータとなります。
- LAN に接続される装置はデフォルトルートとして仮想 IP アドレスを設定してください。
- VRRP機能では、VRRP-ADメッセージに以下のパケットを使用します。IPフィルタ設定時には、このパケットを遮断しないように設定する必要があります。 IPv4-VRRP

あて先IP アドレス: 224.0.0.18 プロトコル番号: 112 IPv6-VRRP あて先IP アドレス: ff02::12 IPv6 Next Header: 112

• IPv6 VRRPは、SR-S724TC1/748TC1の場合に使用できます。

30.1 簡易ホットスタンバイ機能を使う

適用機種 SR-S716C2, 724TC1, 748TC1

本装置では、2台のルータを組み合わせることで簡易ホットスタンバイ機能による信頼性の高い通信を実現する ことができます。

ここでは、インターネット側へはバックボーンルータを経由、ローカル LAN 側を VLAN 構成とする場合の設定方法を説明します。



● 設定条件

- 障害発生後の切り戻しは手動で行う
- マスタルータはインターネット側経路をノードダウントリガによって監視する

[VLAN	100]
-------	------

• グループID	: 10
• 仮想IPアドレス	: 192.168.1.1
[VLAN 200]	
• グループID	: 20
● 仮想IPアドレス	: 192.168.2.1
[マスタルータ]	
• バックボーンルータへの接続ポート	:ETHER1ポート
• VLAN 100への接続ポート	:ETHER2 ポート
• VLAN 200 への接続ポート	:ETHER3 ポート
 本装置のIPアドレス/ネットマスク 	: 192.168.1.10/24
 ノードダウントリガの監視 IP アドレス 	:202.168.2.1(プロバイダ側のDNSサーバアドレスなど)
[バックアップルータ]	
• バックボーンルータへの接続ポート	:ETHER1 ポート
• VLAN 100への接続ポート	:ETHER2 ポート
• VLAN 200 への接続ポート	:ETHER3 ポート
 本装置のIPアドレス/ネットマスク 	: 192.168.1.11/24

上記の設定条件に従って設定を行う場合の設定例を示します。

マスタルータを設定する

- **1. 設定メニューの詳細設定で「ether情報」をクリックします**。 「ether情報」ページが表示されます。
- **2.** 「ether 情報」でポート番号が1の [修正] ボタンをクリックします。 ether 1 情報の設定項目と「基本情報」が表示されます。

3. 以下の項目を指定します。

- メディア種別 →通常ポート(RJ45)
- VLAN
 Untagged

→ 10

■基本	5情報	3	
<mark>ボート使用</mark> ●使用する ○使用しない		●使用する●使用しない	
<mark>説明文</mark>	τ		
メディ	ア種別	○自動 ④通常ボート(RJ45) ○ SFPボート	
通信递	腹	●自動 ○10Mbps ○100Mbps ○1000Mbps	
全二重	<mark>二重/半二重</mark>		
MDI	●自動 ○ MDI ○ MDI-X		
フロー制	送信	⊙しない○する	
御	受信	⊙する ○しばい	
	Tagged		
V L MUN	Untagged	10	

機種によりメディア種別に対応しているポート番号は異なります。

4. [保存] ボタンをクリックします。

5. 手順2.~4.を参考に、ETHER2、3ポートを設定します。

「ether 2 情報」-「基本情報」

- メディア種別 →通常ポート(RJ45)
- VLAN Tagged → 100
 [ether 3 情報] - 「基本情報」
- メディア種別 →通常ポート(RJ45)
- VLAN
 Tagged →200

6. 設定メニューの詳細設定で「STP 情報」をクリックします。

「STP情報」ページが表示されます。

7. 以下の項目を指定します。

STP機能 →使用しない

■基本情報			3
STP機能	●使用しない	○使用する	

8. [保存] ボタンをクリックします。

9. 設定メニューの詳細設定で「IP 情報」をクリックします。

「IP 情報」ページが表示されます。

10. 以下の項目を指定します。

IPフォワーディング機能 →使用する

■基本情報	3
ARPエントリ有効時間	20 分
IPフォワーティング機能	○使用しない⊙使用する

- 11. [保存] ボタンをクリックします。
- **12. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **13.** 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- **14. 「共通情報」をクリックします。** 共通情報の設定項目と「基本情報」が表示されます。
- 15. 以下の項目を指定します。
 - VLAN ID → 100

■基本情報		3
VLAN ID	100	

- 16. [保存] ボタンをクリックします。
- **17.** 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 18. 以下の項目を指定します。
 - IPアドレス → 192.168.1.10
 - ネットマスク →24 (255.255.255.0)
 - ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報	3
IPアドレス	192.168.1.10
ネットマスク	24 (255.255.255.0)
フロートキャストアトレス	ネットワークアドレス+オール1 💌

- 19. [保存] ボタンをクリックします。
- **20. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 21. 以下の項目を指定します。
 - VLAN ID →200

<lan情報追加フィールド></lan情報追加フィールド>			
VLAN ID	200		

- 22. [追加] ボタンをクリックします。
 「LAN1 情報」ページが表示されます。
 23. 手順 17.~19.を参考に、LAN1 情報を設定します。
 ・ IPアドレス → 192.168.2.10
 - ネットマスク →24 (255.255.255.0)
 - ロードキャストアドレス →ネットワークアドレス+オール1
- 24. 手順20.~22.および手順17.~19.を参考に、以下の項目を設定します。

「LAN 情報」 ● VLAN ID

- → 10
- 「LAN2情報」-「IP 関連」-「IP アドレス情報」
- IPアドレス → 192.168.3.10
- ネットマスク → 24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1
- **25. 手順24.で設定したLAN2情報の「IP関連」をクリックします。** IP関連の設定項目と「IPアドレス情報」が表示されます。
- 26. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

27. 以下の項目を指定します。

ネットワーク →デフォルトルート
 中継ルータアドレス → 192.168.3.1

<スタティック経路情報入力フィールド>		
ネットワーク	 ● デフォルトルート 中継ルータアドレス 192.168.3.1 ● ネットワーク指定 あて先IPアドレス あて先アドレスマスク 0 00.0.0) 中継ルータアドレス 	

- 28. [追加] ボタンをクリックします。
- **29. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **30.** 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- **31. 「共通情報」をクリックします**。 共通情報の設定項目と「基本情報」が表示されます。

• VRRP機能

基本情報		3
VLAN ID	10	
VRRP機能	 ● 使用しない ● 使用する パスワード TRAPモード ● 旧仕様 ○ 新仕様 	

SR-S716C2では、表示が上記の画面とは異なります。

- 33. [保存] ボタンをクリックします。
- **34. 共通情報の設定項目の「VRRP グループ情報」をクリックします**。 「VRRP グループ情報」が表示されます。
- **35.** 「VRRP グループ情報」でグループ番号が0の [修正] ボタンをクリックします。 VRRP グループ0 情報の設定項目と「基本情報」が表示されます。

→使用する

36. 以下の項目を指定します。

•	グループID	→ 10
•	プライオリティ	→優先度指定
	優先度	→254
	仮想IPアドレス	→192.168.1.1
•	プリエンプトモード	→OFF

■基本情報		3
グループID	10	
ブライオリティ	 ● 優先度指定 優先度 254 仮想IPアドレ 192.168.1.1 ● 優先度固定(最優先) 優先度 255 仮想IPアドレス インタフェースアドレスを使用 ● IPv4 ● IPv6 	
AD送信間隔	1 秒	
ブリエンブトモード	 ○ ON ⊙ OFF 移行禁止時間 ○ 秒 	

- 37. [保存] ボタンをクリックします。
- **38.** VRRP グループ0 情報の設定項目の「VRRP トリガ情報」をクリックします。 「VRRP トリガ情報」が表示されます。

 減算プライオリティ →254 • トリガ種別 →ノードダウントリガ (node) あて先 IP アドレス →202.168.2.1 送出インタフェース →指定なし 再送間隔 →5 タイムアウト時間 →16 正常時送信間隔 **→**17 異常時送信間隔 →30



SR-S716C2では、表示が上記の画面とは異なります。

- [追加] ボタンをクリックします。 40.
- 41. 手順29.~40.を参考に、以下の項目を設定します。 「LAN1情報」-「共通情報」-「基本情報」
 - VRRP機能
 - →使用する

「LAN1情報」-「共通情報」-「VRRP グループ0情報」-「基本情報」

- グループID **→**20 • プライオリティ →優先度指定 優先度 →254 仮想IPアドレス → 192.168.2.1
- プリエンプトモード → OFF

「LAN1情報」-「共通情報」-「VRRP グループ0情報」-「VRRP トリガ情報」 →254

- 減算プライオリティ
- トリガ種別 →ノードダウントリガ (node) あて先IPアドレス →202.168.2.1 送出インタフェース →指定なし 再送間隔 →5 タイムアウト時間 →16 正常時送信間隔 **→**17 異常時送信間隔 →30

42. 画面左側の[再起動]ボタンをクリックします。

装置の再起動後、設定した内容が有効になります。

バックアップルータを設定する

「マスタルータを設定する」を参考に、バックアップルータを設定します。

「ether情報」			
「ether 1 情報」-「基本情報」			
• メディア種別	→通常ポート(RJ45)		
• VLAN			
Untagged	→ 10		
「ether 2 情報」-「基本情報」			
• メディア種別	→通常ポート(RJ45)		
• VLAN			
Tagged	→ 100		
「ether 3 情報」-「基本情報」			
• メディア種別	→通常ポート(RJ45)		
• VLAN			
Tagged	→200		
「STP情報」 「基本情報」 • STP機能	→使用しない		
「IP 情報」 「基本情報」 ・ IP フォワーディング機能	→使用する		
「LAN 情報」(LAN0)			
VLAN ID	→ 100		
「I ANO 情報」- 「IP 関連」- 「IP アドレス情報」			
 IPアドレス 	→ 192.168.1.11		
 ネットマスク 	→ 24 (255 255 255 0)		
	·唐報1		
	♪ IFJ+KJ → 体田すろ		
	「区川り句		

「LAN0情報」-「共通情報」-「VRRP グループ0情報」-「基本情報」 • グループID **→**10 • プライオリティ →優先度指定 優先度 → 100 仮想IPアドレス → 192.168.1.1 • プリエンプトモード → ON ※ノードダウントリガは設定しません。 「LAN情報」(LAN1) VLAN ID →200 「LAN1情報」-「IP関連」-「IPアドレス情報」 • IPアドレス → 192.168.2.11 ネットマスク →24 (255.255.255.0) 「LAN1情報」-「共通情報」-「基本情報」 →使用する VRRP機能 「LAN1 情報」-「共通情報」-「VRRP グループ0 情報」-「基本情報」 グループID **→**20 • プライオリティ →優先度指定 優先度 → 100 仮想IPアドレス → 192.168.2.1 • プリエンプトモード →ON ※ノードダウントリガは設定しません。 「LAN 情報」(LAN2) VLAN ID **→** 10 「LAN2情報」-「IP関連」-「IPアドレス情報」 • IPアドレス → 192.168.3.11 ネットマスク →24 (255.255.255.0)

「LAN2情報」-「IP関連」-「スタティック経路情報」

- ネットワーク →デフォルトルート
- 中継ルータアドレス → 192.168.3.2

30.2 クラスタリング機能を使う

<u>適用機種</u> SR-S716C2, 724TC1, 748TC1

本装置では、2台のルータに複数のグループIDを設定することで、信頼性を高めると同時に通信の負荷分散を実現できます。

ここでは、インターネット側へはバックボーンルータを経由、ローカル LAN 側を VLAN 構成とする場合の設定方法を説明します(VLAN 100のみクラスタリング機能を使用する)。



● 設定条件

- 故障発生後の切り戻しは手動で行う
- マスタルータはバックボーンルータ側のインタフェースをインタフェースダウントリガにより監視する

[VLAN 100]

● [グループA]	
- グループID	: 10
- 仮想 IP アドレス	: 192.168.1.1
● [グループB]	
- グループID	: 11
- 仮想 IP アドレス	: 192.168.1.2
[VLAN 200]	
• グループID	: 20
• 仮想 IP アドレス	: 192.168.2.1
[マスタルータ]	
• バックボーンルータへの接続ポート	:ETHER1ポート
• VLAN 100への接続ポート	:ETHER2ポート
● VLAN 200への接続ポート	:ETHER3ポート
 本装置のIPアドレス/ネットマスク 	: 192.168.1.10/24

[バックアップルータ]

- バックボーンルータへの接続ポート : ETHER1 ポート
 VLAN 100への接続ポート : ETHER2 ポート
 VLAN 200への接続ポート : ETHER3 ポート
- 本装置のIPアドレス/ネットマスク
- こんな事に気をつけて

クラスタリング機能を有効に利用するには、端末からのトラフィック量に応じて、端末側で設定するデフォルトルート の定義を適切に分散してください。

: 192.168.1.11/24

上記の設定条件に従って設定を行う場合の設定例を示します。

マスタルータを設定する

1. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether 情報」ページが表示されます。

2. 「ether情報」でポート番号が1の[修正]ボタンをクリックします。

ether 1 情報の設定項目と「基本情報」が表示されます。

- 3. 以下の項目を指定します。
 - メディア種別 →通常ポート(RJ45)
 - VLAN
 Untagged

→10

■基本	「情報	3
ボート	使用	●使用する●使用しない
説明文		
メディス	P種別	○自動 ④ 通常ボート(RJ45) ○ SFPボート
通信退	<mark>循速度</mark> ◎自動 ◎ 10Mbps ◎ 100Mbps ◎ 1000Mbps	
全二重	<mark>全二重/半二重</mark> ◎全二重 ○半二重	
MDI ◎自動 ○ MDI ○ MDI-X		●自動 ○ MDI ○ MDI-X
フロ	送信	⊙しばい ○する
御	受信	⊙する ○しない
	Tagged	
VEAN	Untagged	10

機種によりメディア種別に対応しているポート番号は異なります。

- 4. [保存] ボタンをクリックします。
- 5. 手順2.~4.を参考に、ETHER2、3ポートを設定します。

「ether 2 情報」-「基本情報」

- メディア種別 →通常ポート(RJ45)
- VLAN
 Tagged → 100

「ether 3 情報」-「基本情報」

- メディア種別 →通常ポート(RJ45)
- VLAN
 Tagged → 200
- 6. 設定メニューの詳細設定で「STP 情報」をクリックします。

「STP情報」ページが表示されます。

- 7. 以下の項目を指定します。
 - STP機能 →使用しない
 基本情報 ②
 STP機能 ●使用しない ○使用する
- 8. [保存] ボタンをクリックします。
- 設定メニューの詳細設定で「IP 情報」をクリックします。
 「IP 情報」ページが表示されます。
- 10. 以下の項目を指定します。
 - IPフォワーディング機能 →使用する

■基本情報		3
ARPエントリ有効時間	20 分	
IPフォワーディング機能	○使用しない ⊙使用する	

- 11. 【保存】ボタンをクリックします。
- **12. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **13.** 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- **14. 「共通情報」をクリックします**。 共通情報の設定項目と「基本情報」が表示されます。
- 15. 以下の項目を指定します。
 - VLAN ID → 100

■基本情報	3	J
VLAN ID	100	

- 16. 【保存】ボタンをクリックします。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。

• IPアドレス

- →192.168.1.10
- ネットマスク → 24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報	3
IPアドレス	192.168.1.10
ネットマスク	24 (255.255.255.0)
フロートキャストアトレス	ネットワークアドレス+オール1 🗸

- 19. [保存] ボタンをクリックします。
- 20. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

- 21. 以下の項目を指定します。
 - VLAN ID →200

	<lan情報追加t< th=""><th>フィールド></th></lan情報追加t<>	フィールド>
VLAN ID		200

22. [追加] ボタンをクリックします。

「LAN1情報」ページが表示されます。

- 23. 手順 17.~19.を参考に、LAN1 情報を設定します。
 - IPアドレス → 192.168.2.10
 - ネットマスク → 24 (255.255.255.0)
 - ブロードキャストアドレス →ネットワークアドレス+オール1
- 24. 手順20.~22.および手順17.~19.を参考に、以下の項目を設定します。

「LAN 情報」 • VLAN ID

→10

- 「LAN2情報」-「IP関連」-「IPアドレス情報」
- IPアドレス → 192.168.3.10
- ネットマスク →24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1
- **25. 手順24. で設定したLAN2 情報の「IP 関連」をクリックします**。 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **26.** IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。

ネットワーク →デフォルトルート
 中継ルータアドレス → 192.168.3.1
 <スタティック経路情報入力フィールド>
 デフォルトルート
 ・デフォルトルート
 ・中継ルータアドレス 192.168.3.1
 ・ネットワーク
 ・ネットワーク指定
 あて先IPアドレス

あて先アドレスマスク 0 (0.0.0.0)

中継ルータアドレス

- 28. [追加] ボタンをクリックします。
- **29. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **30.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。

→使用する

¥

- **31. 「共通情報」をクリックします。** 共通情報の設定項目と「基本情報」が表示されます。
- 32. 以下の項目を指定します。
 - VRRP機能

基本情報		3
VLAN ID	10	
VRRP機能	 ● 使用しない ● 使用する パスワード TRAPモード ● 旧仕様 ○ 新仕様 	

SR-S716C2では、表示が上記の画面とは異なります。

- 33. [保存] ボタンをクリックします。
- **34. 共通情報の設定項目の「VRRP グループ情報」をクリックします**。 「VRRP グループ情報」が表示されます。
- **35.** 「VRRP グループ情報」でグループ番号が0の [修正] ボタンをクリックします。 VRRP グループ0情報の設定項目と「基本情報」が表示されます。

 グループID → 10
 プライオリティ →優先度指定 優先度 → 254
 仮想IPアドレス → 192.168.1.1
 プリエンプトモード → OFF

■基本情報	基本情報	
グルーブID	10	
	⊙ 優先度指定	
	優先度 254	
-1- /	仮想Pアドレ ス 192.168.1.1	
ノフキオリティ	○ 優先度固定(最優先)	
	優先度 255	
	仮想IPアドレス インタフェースアドレスを使用 ● IPv4 ● IPv6	
AD送信間隔	1 秒	
	O ON	
ブリエンプトモード OFF		
	移行禁止時間 0 秒	

- 37. 【保存】ボタンをクリックします。
- **38.** VRRP グループ 0 情報の設定項目の「VRRP トリガ情報」をクリックします。 「VRRP トリガ情報」が表示されます。

39. 以下の項目を指定します。

- 減算プライオリティ → 254
- トリガ種別 →インタフェースダウントリガ (ifdown)
 インタフェース → lan2



- 40. [追加] ボタンをクリックします。
- **41.** 手順34.~37.を参考に、グループ番号1を設定します。
 - グループID →11
 プライオリティ →優先度指定 優先度 →100 仮想IPアドレス →192.168.1.2
 プリエンプトモード →ON

42. 手順29.~40.を参考に、以下の項目を設定します。

「LAN1情報」-「共通情報」-「基本	「情報」
● VRRP機能	→使用する
「LAN1情報」-「共通情報」-「VR	RPグループ0情報」-「基本情報」
● グループID	→20
 プライオリティ 優先度 	→優先度指定 →254
仮想IPアドレス	→192.168.2.1
• プリエンプトモード	→OFF
「LAN1情報」-「共通情報」-「VR	RP <mark>グループ 0 情報」</mark> -「VRRP トリガ情報」
• 減算プライオリティ	→ 254
 トリガ種別 インタフェーフ 	→インタフェースダウントリガ(ifdown) → lan2
	r Iai Iz

43. 画面左側の [再起動] ボタンをクリックします。

装置の再起動後、設定した内容が有効になります。

バックアップルータを設定する

「マスタルータを設定する」を参考に、バックアップルータを設定します。

「ether**情報」** 「ether1情報」-「基本情報」

• メディア種別		→通常ポート	(RJ45)
• VLAN			
Untagged		→ 10	
「ether 2 情報」-	「基本情報」		
• メディア種別		→通常ポート	(RJ45)
• VLAN			
Tagged		→ 100	
「ether 3 情報」-	「基本情報」		
• メディア種別		→通常ポート	(RJ45)
• VLAN			
Tagged		→200	
「STP情報」			
「基本情報」			
 STP機能 		→使用しない	
「IP情報」			
「基本情報」			
• IPフォワーデ	ィング機能	→使用する	

「LAN 情報」(LAN0) • VLAN ID → 100 「LAN0情報」-「IP関連」-「IPアドレス情報」 • IPアドレス → 192.168.1.11 • ネットマスク →24 (255.255.255.0) 「LAN0情報」-「共通情報」-「基本情報」 VRRP機能 →使用する 「LAN0 情報」-「共通情報」-「VRRP グループ0 情報」-「基本情報」 グループID **→**10 • プライオリティ →優先度指定 → 100 優先度 仮想IPアドレス → 192.168.1.1 • プリエンプトモード →ON ※インタフェースダウントリガは設定しません。 「LAN0 情報」-「共通情報」-「VRRP グループ1 情報」-「基本情報」 グループID → 11 • プライオリティ →優先度指定 優先度 →254 仮想IPアドレス → 192.168.1.2 • プリエンプトモード → OFF 「LAN0 情報」-「共通情報」-「VRRP グループ1 情報」-「VRRP トリガ情報」 減算プライオリティ →254 • トリガ種別 →インタフェースダウントリガ (ifdown) →lan2 インタフェース 「LAN情報」(LAN1) VLAN ID →200 「LAN1情報」-「IP関連」-「IPアドレス情報」 • IPアドレス → 192,168,2,11 ネットマスク →24 (255.255.255.0) 「LAN1情報」-「共通情報」-「基本情報」 • VRRP機能 →使用する 「LAN1 情報」-「共通情報」-「VRRP グループ0 情報」-「基本情報」 グループID →20 • プライオリティ →優先度指定 優先度 → 100 仮想IPアドレス → 192.168.2.1 • プリエンプトモード → ON

※インタフェースダウントリガは設定しません。

「LAN 情報」(LAN2)

VLAN ID → 10
 「LAN2 情報」-「IP 関連」-「IP アドレス情報」
 IP アドレス → 192.168.3.11
 ネットマスク → 24 (255.255.255.0)

「LAN2情報」-「IP関連」-「スタティック経路情報」

- ネットワーク →デフォルトルート
- 中継ルータアドレス → 192.168.3.2

ECMP 機能を使う 31

適用機種 SR-S716C2, 724TC1, 748TC1

ここでは、ECMP 機能を利用した負荷分散通信を行う場合の設定方法を説明します。



● 参照 機能説明書「2.37 ECMP機能」(P.123)

▶ 設定条件

拠点では、センタへの通信は、ルータ1とルータ2を利用して負荷分散して送信します。

上記の設定条件に従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether 情報」ページが表示されます。

2. 以下の項目を指定します。

> • ポートリスト → 1-14



3. [修正] ボタンをクリックします。

ether 1-14 情報の設定項目と「基本情報」が表示されます。

• メディア種別

Untagged

→通常ポート (RJ45)

• VLAN

→ 10

■基本	□情報	3	
ボート	使用	●使用する●使用しない	
<mark>説明</mark> 文	τ		
メディ	P種別	○自動 ③通常ボート(RJ45) ○ SFPボート	
通信递	腹		
全二重	[/半二重	◎全二重 ○半二重	
MDI		●自動 ○ MDI ○ MDI-X	
フロー当日	送信	⊙し/む ○する	
御	受信	⊙する ○しない	
	Tagged		
VEAN	Untagged	10	

機種によりメディア種別に対応しているポート番号は異なります。

- 5. [保存] ボタンをクリックします。
- **6. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- **7.** 「ether 情報」でポート番号が 15の [修正] ボタンをクリックします。 ether 15 情報の設定項目と「基本情報」が表示されます。
- 8. 手順4.~5.を参考に、以下の項目を設定します。
 - メディア種別 →通常ポート(RJ45)
 - VLAN
 Untagged → 11
- 9. 手順6.~8.を参考に、ETHER16ポートを設定します。
 - メディア種別 →通常ポート(RJ45)
 - VLAN
 Untagged → 12
- **10. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 11.
 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。

 「LAN0 情報」ページが表示されます。
- 12. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 13. 以下の項目を指定します。
 - VLAN ID → 10

■基本情報		3
VLAN ID	10	

- 14. [保存] ボタンをクリックします。
- **15.** 「IP 関連」をクリックします。 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 16. 以下の項目を指定します。
 - IPアドレス → 192.168.1.1
 - ネットマスク →24 (255.255.255.0)
 - ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報	3
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0) 🗸
フロートキャストアトレス	ネットワークアドレス+オール1 💌

- 17. [保存] ボタンをクリックします。
- **18. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。

- 19. 以下の項目を指定します。
 - VLAN ID

→ 11

<lan情報追加フィールド></lan情報追加フィールド>	
VLAN ID	11

- **20. [追加] ボタンをクリックします**。 「LAN1情報」ページが表示されます。
- 21. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

22. 以下の項目を指定します。

- IPアドレス →192.168.2.1
- ネットマスク →24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス 情報	3
IPアドレス	192.168.2.1
ネットマスク	24 (255.255.255.0) 🗸
フロートキャストアトレス	ネットワークアドレス+オール1 💌

- 23. [保存] ボタンをクリックします。
- **24. 「スタティック経路情報」をクリックします**。 「スタティック経路情報」が表示されます。

優先度

- ネットワーク あて先IPアドレス あて先アドレスマスク 中継ルータアドレス
 メトリック
- →ネットワーク指定 →202.168.1.0 →24(255.255.255.0) →192.168.2.2 →1

→1

<スタティック経路情報入力フィールド>		
ネットワーク	 デフォルトルート 中継ルータアドレス ネットワーク指定 あて先IPアドレス 202.168.1.0 あて先アドレスマスク 24 (255.255.255.0) 中継ルータアドレス 192.168.2.2 	
メトリック値	1 🗸	
優先度	1	

- 26. [追加] ボタンをクリックします。
- 27. 手順18.~26.を参考に、以下の項目を設定します。

「LAN情報」

- VLAN ID **→**12 「LAN2情報」-「IP関連」-「IPアドレス情報」 • IPアドレス → 192.168.3.1 • ネットマスク →24 (255.255.255.0) • ブロードキャストアドレス →ネットワークアドレス+オール1 「LAN2情報」-「IP関連」-「スタティック経路情報」 ネットワーク →ネットワーク指定 あて先 IP アドレス →202.168.1.0 あて先アドレスマスク →24 (255.255.255.0) 中継ルータアドレス → 192.168.3.2 • メトリック **→**1
- 優先度 →1
- **28. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。

29. 「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

30. [ECMP 情報] をクリックします。

「ECMP情報」が表示されます。

● ECMP機能

→ハッシュ方式

ECMP情報	3
ECMP機能	 ○使用しない ●ハッシュ方式

- 32. [保存] ボタンをクリックします。
- 33. 設定メニューの詳細設定の「IP 情報」をクリックします。

「IP 情報」ページが表示されます。

- 34. 以下の項目を指定します。
 - IPフォワーディング機能 →使用する

■基本情報	3
ARPエントリ有効時間	20 分
IPフォワーティンク機能	○使用しない ⊙使用する

- 35. [保存]ボタンをクリックします。
- **36. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

32 DHCP機能を使う

適用機種 全機種

本装置のDHCPには、以下の機能があります。

- DHCPサーバ機能
- DHCPスタティック機能
- DHCPリレーエージェント機能(IPv4:SR-S716C2/724TC1/748TC1のみ、IPv6:SR-S724TC1/748TC1のみ)

● 参照 機能説明書「2.38 DHCP機能」(P.125)

本装置では、それぞれのインタフェースでDHCP機能が使用できます。

こんな事に気をつけて

- 1つのインタフェースでは、1つの機能だけ動作します。同時に複数の機能を動作することはできません。
 - 本装置のDHCPサーバは、リレーエージェントを経由して運用することはできません。

32.1 DHCP サーバ機能を使う

適用機種 全機種

DHCP サーバ機能は、ネットワークに接続されているパソコンに対して、IP アドレスの自動割り当てを行う機能です。管理者はパソコンが増えるたびにIP アドレスが重複しないように設定する必要があります。

この機能を利用すると、DHCPクライアント機能を持つパソコンはIPアドレスの設定が不要になり、管理者の手間を大幅に省くことができます。

本装置のDHCPサーバ機能は、以下の情報を広報することができます。

- 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
- ドメイン名

こんな事に気をつけて

 ・ 文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白 文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

・ 本装置のDHCPサーバ機能は、DHCPリレーエージェントのサーバにはなれません。

ここでは、SR-S716C2の場合を例にして、DHCPサーバ機能を使用する場合の設定方法を説明します。



● 前提条件

- LANOが設定されている
- LAN1はVLANが設定されている

● 設定条件

- 本装置のIPアドレス
- ブロードキャストアドレス
- パソコンに割り当てる IP アドレス
- パソコンに割り当て可能 IP アドレス数
- ネットワークアドレス/ネットマスク
- DHCPサーバ機能を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

1. 「1.1 ポート VLAN 機能を使う」(P.9)の手順 1.~4.を参考に、ETHER1 ポートを設定します。

• メディア種別

→通常ポート(RJ45)

- VLAN
 Untagged → 10
- **2. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 3. 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。 「LAN1 情報」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。

DHCP 機能を使う

318

: 192.168.2.0/24

: 32

- : 192.168.2.1
- :3(ネットワークアドレス+オール1)
- : 192.168.2.2~192.168.2.33

• IPアドレス

- →192.168.2.1
- ネットマスク →24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報	3
IPアドレス	192.168.2.1
ネットマスク	24 (255.255.255.0)
フロートキャストアトレス	ネットワークアドレス+オール1 🔽

[保存] ボタンをクリックします。 6.

7. IP 関連の設定項目の「DHCP 情報」をクリックします。 「DHCP情報」が表示されます。

8. 以下の項目を指定します。

•	DHCP機能	→サーバ機能を使用する
	割当て先頭IPアドレス	→ 192.168.2.2
	割当てアドレス数	→ 32



補足 DHCPサーバ機能で割り当てることのできる最大数は253です。

	⊙ サーバ機能を使用する	5
DHOD	割当て先頭IPアド レス	92.168.2.2
機能	割当てアドレス数 3	2
	リース期間 1	
	デフォルトルータ広 報	
	DNSサーバ広報	
	セカンダリDNSサ ーバ広報	
	ドメイン名広報	
		コホストデータベース
	MACアドレスチェッ	
	2	参照するAAA情報
		認証ブロトコル OCHAP OPAP
	※"割当て先頭アドレス ークアドレス内であるこ	ス"が本装置のIPアドレスと同じネットワ ことを確認してください。

必要に応じて上記以外の項目を指定します。

- 9. [保存] ボタンをクリックします。
- 10. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

32.2 DHCPスタティック機能を使う

適用機種 全機種

DHCPサーバは、使用していないIPアドレスを一定期間(またはパソコンがIPアドレスを返却するまで)割り当 てます。不要になったIPアドレスは自動的に再利用されるため、パソコンのIPアドレスが変わることがあります。 本装置では、IPアドレスとMACアドレスを対応付けることによって、登録されたパソコンからDHCP要求が発行 されると、常に同じIPアドレスを割り当てることができます。これをDHCPスタティック機能と言います。 DHCPスタティック機能を利用する場合は、ホストデータベース情報にIPアドレスとMACアドレスを設定して ください。



MACアドレスとは、LAN機器に設定されていて世界中で重複されないように管理されている固有のアドレスです。
 本装置がサポートしているIPフィルタリング機能などはパソコンのIPアドレスが固定されていないと使いにくい場

合があります。これらの機能とDHCPサーバ機能の併用を実現するために、本装置では「DHCPスタティック機能」 をサポートしています。

こんな事に気をつけて

文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

● 参照 Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P.21)

ここでは、SR-S716C2の場合を例にして、DHCPスタティック機能を使用する場合の設定方法を説明します。



● 設定条件

- ネットワークアドレス/ネットマスク
 - : 192.168.2.0/24
- IPアドレスを固定するパソコンのMACアドレス:00:00:0e:12:34:56
- 割り当てIPアドレス

- : 192.168.2.2
- DHCPサーバ機能を使用する

こんな事に気をつけて

設定の「LAN0 情報」、「LAN1 情報」でDHCP サーバ機能を使用する設定をしていない場合は、DHCP スタティック機能の設定は有効になりません。

上記の設定条件に従って設定を行う場合の設定例を示します。

- 1. 設定メニューの詳細設定で「ホストデータベース情報」をクリックします。 「ホストデータベース情報」ページが表示されます。
- 2. 未設定の欄の[修正]ボタンをクリックします。 「ホストデータベース情報」が表示されます。
- 3. 以下の項目を指定します。
 - IPv4アドレス → 192.168.2.2
 - MACアドレス →00:00:0e:12:34:56

▲ ホストデータベース情報は「DHCPスタティック機能」、「DNSサーバ機能」で使われており、それぞれ必要な項目だ けを設定します。

ホスト名	
IPv4アドレス	192.168.2.2
IPv6アドレス	
MACアドレス	00:00:0e:12:34:56
DUID	

必要に応じて上記以外の項目を指定します。

- 4. [保存] ボタンをクリックします。
- 5. 画面左側の〔設定反映〕ボタンをクリックします。 設定した内容が有効になります。



補足 DHCPスタティック機能で設定できるホストの最大数は100です。

32.3 DHCP リレーエージェント機能を使う

<u>適用機種</u> SR-S716C2, 724TC1, 748TC1

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

こんな事に気をつけて

文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

● ● ● Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P21)

ここでは、DHCPリレーエージェント機能を使用する場合の設定方法を説明します。



[LAN1]

- 本装置のIPアドレス : 192.168.1.1
- DHCPリレーエージェント機能を使用する

[LAN0]

- 本装置のIPアドレス : 192.168.0.1
- DHCPサーバ : 192.168.0.10

上記の設定条件に従って設定を行う場合の設定例を示します。

ここでは、LAN1を使用した場合を例に説明します。LAN0の場合も同様の手順で設定できます。

1. 「1.1 ポート VLAN 機能を使う」(P.9)の手順 1.~4.を参考に、ETHER1、2 ポートを設定します。

ETHER1ポート

- メディア種別 →通常ポート(RJ45)
- VLAN
 Untagged → 10
- ETHER2ポート
- メディア種別 →通常ポート(RJ45)
- VLAN
 Untagged → 20
- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **3.** 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。 「LAN1 情報」ページが表示されます。
- 4. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- **5.** IP 関連の設定項目の「DHCP 情報」をクリックします。 「DHCP 情報」が表示されます。
- 6. 以下の項目を指定します。
 - DHCP機能
 DHCPサーバIPアドレス1

→リレー機能を使用する
→ 192.168.0.10

DHCP情報			
DHCP 機能	•	使用しない リレー機能を使用する DHCPサーバIPアドレ ス1 DHCPサーバIPアドレ ス2	92.168.0.10
		MACアドレスチェック	□ホストデータベース □AAA 参照するAAA情 報 認証プロトコル ◎CHAP ○PAP
	0	サーハ機能を使用する	

- 7. [保存] ボタンをクリックします。
- 8. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

32.4 IPv6 DHCP サーバ機能を使う

適用機種 全機種

本装置の IPv6 DHCP サーバ機能は、以下の情報を広報することができます。

- IPv6アドレス
- IPv6 プレフィックス
- DNSサーバのIPv6アドレス
- DNS ドメイン名

こんな事に気をつけて 本装置の IPv6 DHCP サーバ機能は、IPv6 DHCP リレーエージェントのサーバにはなれません。

IPv6 DHCPサーバ機能を使用する場合の設定方法を説明します。



● 設定条件

- 本装置の IP アドレス
- パソコンに割り当てる IPv6 アドレス
- パソコンに割り当て可能 IPv6 アドレス数
- ネットワークアドレス/プレフィックス長
- Valid Lifetime
- Preferred Lifetime
- DNSサーバのIPv6アドレス

- : 2001:db8:1::1
- : 2001:db8:1::100~2001:db8:1::163
- : 100
- : 2001:db8:1::/64
- :30日
- :7日
- : 2001:db8:1::53

上記の設定条件に従って設定を行う場合の設定例を示します。
IPv6 DHCP サーバ機能を設定する

- 設定メニューの詳細設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。 「LAN1 情報」ページが表示されます。

3. 「IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

4. 以下の項目を指定します。

- IPv6 →使用する
- IPv6アドレス →ユニキャストアドレスを指定する アドレスまたはプレフィックス →2001:db8:1::1

 ■IPv6基本情報		
IPv6	○使用しない。●使用する	
インタフェースID	 ● 自動 ○ 指定する 	
IPv6アドレス	 ルータ広報で受信したプレフィックスを使用する ユニキャストアドレスを指定する アドレスまたはブレフィックス 2001:db8:1:1 	

- 5. [保存] ボタンをクリックします。
- **6.** IPv6 関連の設定項目の「IPv6 DHCP 情報」をクリックします。 「IPv6 DHCP 情報」が表示されます。

- DHCP機能 →サーバ機能を使用する
 "サーバ機能を使用する"を選択すると、「サーバ機能」の設定項目が表示されます。
- サーバ機能 アドレス配布 →する
 割当て開始アドレス → 2001:db8:1::100
 割当てアドレス数 → 100
 Valid Lifetime →期限あり30日
 Pref. Lifetime →期限あり7日
 DNSサーバアドレス配布 → 2001:db8:1::53

■IPv6 DHCP情報			3
DHCP機能		 ○使用しない ○リレーエージェント機能を使用する ○サーバ機能を使用する 	
	DUID	 ● 自動 ● 指定する 	
	ブリファレンス 値		
	アドレス配布	 しない する 割当て開始アドレス 2001:db8:1::100 割当てアドレス数 100 Valid Lifetime 期限おし の期限なし の期限なし ●期限なし ●期限あり30 日 ▼ ●期限あり7 日 ▼ 	
サーバ機能	ブレフィックス 配布	 ● しない ● する ブレフィックス ✓ ✓	
	DNSサーバア ドレス 配布	ブライマリ 2001:db8:1::53 セカンダリ	

- 8. [保存] ボタンをクリックします。
- 9. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

32.5 IPv6 DHCP リレーエージェント機能を使う

適用機種 SR-S724TC1, 748TC1

ここでは、IPv6 DHCP リレーエージェント機能を使用する場合の設定方法を説明します。



● 設定条件

[内部LAN側]

- 本装置のIPv6アドレス : 2001:db8:1::1
- IPv6 DHCP リレーエージェント機能を使用する

[外部 LAN 側]

本装置のIPv6アドレス : 2001:db8::1

上記の設定条件に従って設定を行う場合の設定例を示します。

IPv6 DHCP リレーエージェント機能を設定する

- **1. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

 IPv6 →使用する
 IPv6アドレス →ユニキャストアドレスを指定する アドレスまたはプレフィックス →2001:db8:1::1
 ルータ広報 →使用しない

■IPv6基本情報			
IPv6	○使用しない ⊙使用する		
インタフェースID	 ● 自動 ○ 指定する 		
	 ○ ルータ広報で受信したブレフィックスを使用する ○ ユニキャストアドレスを指定する 		
IPv6アドレス	アドレスまたはブ レフィックス 2001:db8:1::1		



- 5. [保存] ボタンをクリックします。
- **6. 設定メニューの詳細設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 7. 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。 「LAN1 情報」ページが表示されます。
- **FIPv6 関連」をクリックします。** IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

• IPv6

フラグ

→使用する • IPv6アドレス →ユニキャストアドレスを指定する アドレスまたはプレフィックス →2001:db8::1 ルータ広報 →送信する →c0

■IPv6基本情報			
IPv6	○使用しない ⊙使用する		
インタフェースID	 ● 自動 ○ 指定する 		
IPv6アドレス	 ルータ広報で受信したブレフィックスを使用する ユニキャストアドレスを指定する アドレスまたはブレフィックス 2001:db8:1 		



10. [保存] ボタンをクリックします。

IPv6 関連の設定項目の「IPv6 DHCP 情報」をクリックします。 11. 「IPv6 DHCP 情報」が表示されます。

DHCP 機能を使う

329

DHCP機能

→DHCPリレーエージェント機能を使用する

"DHCPリレーエージェント機能を使用する"を選択すると、「リレーエージェント機能」の設定項目が表示されます。

リレーエージェント機能
 リレー先インタフェース → lanO

IP	v6 DH	CP情報	3
DHCP機能			 ○使用しない ●リレーエージェント機能を使用する ●サーバ機能を使用する
	リレー エージェント 機能	リレー先 インタフェース	lan0 💌
リレンエー		リレー先 サーバアトレス	
7210		送信元アドレ ス	

- 13. [保存] ボタンをクリックします。
- **14. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

33 DNSサーバ機能を使う(ProxyDNS)

適用機種 全機種

本装置の ProxyDNS には、以下の機能があります。

- DNS サーバの自動切り替え機能
- DNS 問い合わせタイプフィルタ機能
- DNS サーバ機能

● 参照 機能説明書「2.40 DNS サーバ機能」(P.130)

33.1 DNS サーバの自動切り替え機能(順引き)を使う

適用機種 全機種

ProxyDNSは、パソコン側で本装置のIPアドレスをDNSサーバのIPアドレスとして登録するだけで、ドメイン ごとに使用するDNSサーバを切り替えて中継できます。ここでは、順引きの場合の設定方法を説明します。



● 設定条件

- 会社のDNSサーバを使用する場合 使用するドメイン : honsya.co.jp DNSサーバのIPアドレス : 192.168.2.2
- インターネット上のDNSサーバを使用する場合 使用するドメイン : honsya.co.jp以外 DNSサーバのIPアドレス : 100.100.100

こんな事に気をつけて

文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白文 字、["」、「<」、「>」、「&」、「%」は入力しないでください。

● 参照 Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P.21)

上記の設定条件に従って設定を行う場合の設定例を示します。

ProxyDNS 情報を設定する

1. 設定メニューの詳細設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

「ProxyDNS 情報/URL フィルタ情報」ページが表示されます。

- **2. 「順引き情報」をクリックします**。 「順引き情報」が表示されます。
- 3. 以下の項目を指定します。
 - ・ドメイン名 →*.honsya.co.jp
 ・動作 →設定したDNSサーバへ問い合わせる DNSサーバアドレス → 192.168.2.2

→ *



- 4. [追加] ボタンをクリックします。
- 5. 手順3.~4.を参考に、以下の項目を設定します。
 - ドメイン名
 - 動作 DNSサーバアドレス

→設定したDNSサーバへ問い合わせる → 100.100.100.100

6. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

パソコン側の設定を確認する

1. パソコン側がDHCP クライアントかどうか確認します。

DHCP クライアントでない場合は設定します。 設定方法は、「33.2 DNS サーバの自動切り替え機能(逆引き)を使う」(P.333)の「パソコン側の設定を行う」 (P.335)を参照してください。

33.2 DNSサーバの自動切り替え機能(逆引き)を使う

適用機種 全機種

ProxyDNSは、先に説明した順引きとは逆に、IPアドレスごとに使用するDNSサーバを切り替えて中継できます。ここでは、逆引きの場合の設定方法を説明します。



● 設定条件

•	会社のDNSサーバを使用する場合		
	逆引き対象のネットワークアドレス	:	192.168.0.0
	DNSサーバのIPアドレス	:	192.168.2.2
•	インターネット上のDNSサーバを使用する場合		
	逆引き対象のネットワークアドレス	:	192.168.0.0以外
	DNSサーバのIPアドレス	:	100.100.100.100

こんな事に気をつけて

文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

● 参照 Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P.21)

上記の設定条件に従って設定を行う場合の設定例を示します。

ProxyDNS情報を設定する

- **1. 設定メニューの詳細設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします**。 「ProxyDNS 情報/URL フィルタ情報」ページが表示されます。
- 2. 「逆引き情報」をクリックします。

「逆引き情報」が表示されます。

- 3. 以下の項目を指定します。
 - ネットワークアドレス

→指定する →192.168.0.0/24

動作
 DNS サーバアドレス

→設定したDNSサーバへ問い合わせる →192.168.2.2

	<逆引き情報入力フィールド>		
ネットワ ークアド レス	指定する ▼ (*指定する*を選択時のみ有効です。) 192.168.0.0 / 24 ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィ ックス長形式で入力してください。		
動作	 ○ 廃棄する ● 設定したDNSサーバへ問い合わせる DNSサーバアドレス 192.168.2.2 		

4. [追加] ボタンをクリックします。

5. 手順3.~4.を参考に、以下の項目を設定します。

- ネットワークアドレス →すべて
- 動作 →設定したDNS サーバへ問い合わせる
- DNSサーバアドレス → 100.100.100.100
- 6. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

パソコン側の設定を行う

ここでは、Windows 2000の場合を例に説明します。

- [コントロールパネル]ウィンドウで [ネットワークとダイヤルアップ接続] アイコンをダブルク リックします。
- **2. [ローカルエリア接続] アイコンを右クリックし、プロパティを選択します**。 [ローカルエリア接続のプロパティ] ダイアログボックスが表示されます。
- 3. 一覧から「インターネットプロトコル (TCP/IP)」をクリックして選択します。
- 4. [プロパティ] ボタンをクリックします。
- 5. 「次のDNSサーバーのアドレスを使う」を選択します。
- 6. 「優先 DNS サーバー」に、本装置の IP アドレスを入力します。
- 7. [OK] ボタンをクリックします。
- 8. [はい] ボタンをクリックし、パソコンを再起動します。

再起動後に、設定した内容が有効になります。

心 ヒントー

◆本装置の「DHCPサーバ機能」を使わない場合の設定は?

パソコン側の「DNS 設定」で本装置の IP アドレスを指定すると、ProxyDNS 機能だけ使用できます。また、 本装置以外の DHCP サーバを使用している場合でも、DHCP サーバで広報する DNS サーバの IP アドレスとし て本装置の IP アドレスを指定すると ProxyDNS 機能を使用できます。

◆ DNS 解決したホストへのホスト経路を自動で作成する設定は?

「ProxyDNS 情報 URL フィルタ情報」-「順引き情報」の動作に"接続先の DNS サーバへ指定ネットワークを 経由して問い合わせる"を指定した場合は、「解決したホストへのホスト経路自動作成」に"する"を指定す ることにより、DNS 解決したホストへのホスト経路を自動で作成することができます。

33.3 DNS 問い合わせタイプフィルタ機能を使う

適用機種 全機種

端末が送信する DNS パケットのうち、特定の問い合わせタイプ (QTYPE) のパケットを破棄することができます。

こんな事に気をつけて

ProxyDNS機能を使用する場合、問い合わせタイプがA(1)のDNS問い合わせパケットを破棄するように指定にする と、正常な通信が行えなくなります。

● 設定条件

- ドメイン名 :*
- 問い合わせタイプ : SOA (6)
- 動作
 : 破棄する

こんな事に気をつけて

文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

● 参照 Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P.21)

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置側を設定する

1. 設定メニューの詳細設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。 「ProxyDNS 情報/URL フィルタ情報」ページが表示されます。

2. 「順引き情報」をクリックします。

「順引き情報」が表示されます。

- 3. 以下の項目を指定します。
 - ・ドメイン名 →*
 - タイプ → SOA
 - 動作 →廃棄する

<順引き情報入力フィールド>				
ドメイン 名	*			
タイプ	SOA (番号指定) (番号指定) (その他"を選択時のみ有効です。) 			
送信元 IPアドレ ス ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフ ス ックス長形式で入力してください。				
動作	 ● 廃棄する ● 設定したDNSサーバへ問い合わせる DNSサーバアドレス 			

4. [追加] ボタンをクリックします。

5. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

パソコン側の設定を行う

パソコン側の設定を行います。

設定方法は、「33.2 DNS サーバの自動切り替え機能(逆引き)を使う」(P.333)の「パソコン側の設定を行う」 (P.335)を参照してください。

再起動後に、設定した内容が有効になります。

33.4 DNS サーバ機能を使う

適用機種 全機種

本装置のホストデータベースにホスト名とIPアドレスを登録します。登録したホストに対してDNS要求があった場合は、ProxyDNSがDNSサーバの代わりに応答します。

● 設定条件

- ホスト名
 host.com
- IPv4アドレス : 192.168.1.2

こんな事に気をつけて

文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白文字、["」、「<」、「>」、「&」、「%」は入力しないでください。

● 参照 Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P.21)

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置側を設定する

- **1. 設定メニューの詳細設定で「ホストデータベース情報」をクリックします**。 「ホストデータベース情報」ページが表示されます。
- 2. 未設定の欄の [修正] ボタンをクリックします。 「ホストデータベース情報」が表示されます。
- 3. 以下の項目を指定します。
 - ホスト名 → host.com (パソコンの名前)
 - IPv4アドレス → 192.168.1.2 (パソコンのIPアドレス)

₩ ホストデータベース情報は「DHCPスタティック機能」、「DNSサーバ機能」で使われており、それぞれ必要な項目だ けを設定します。

ホスト名	host.com	
IPv4アドレス	192.168.1.2	

- 4. [保存] ボタンをクリックします。
- 5. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

パソコン側の設定を行う

パソコン側の設定を行います。

設定方法は、「33.2 DNS サーバの自動切り替え機能(逆引き)を使う」(P.333)の「 パソコン側の設定を行う」 (P.335)を参照してください。

34 特定のURLへのアクセスを禁止する (URLフィルタ機能)

適用機種 全機種

URLフィルタ機能は、特定のURLへのアクセスを禁止することができます。本機能を使用する場合は、 ProxyDNS 情報で設定します。

以下にURLフィルタを行う場合の設定方法を説明します。



● 参照 機能説明書「2.40 DNSサーバ機能」(P.130)

ここでは、会社のネットワークとプロバイダがすでに接続されていることを前提とします。また、ProxyDNS情報は何も設定されていないものとします。

● 設定条件

- アクセスを禁止するドメイン名 :www.danger.com
- DNSサーバのIPアドレス : 100.100.100.100

こんな事に気をつけて

- URL フィルタ機能を使用する場合は、LAN内のパソコンが本装置のIPアドレスをDNSサーバのIPアドレスとして登録する必要があります。
- 文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白 文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

● 参照 Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P.21)

☆ ヒント

◆「*」は使えるの?

たとえば「www.danger.com」と「XXX.danger.com」の両方をURLフィルタの対象とする場合は「*.danger.com」と指定することで両方を対象にできます。

上記の設定条件に従って設定を行う場合の設定例を示します。

- **1. 設定メニューの詳細設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします**。 「ProxyDNS 情報/URL フィルタ情報」ページが表示されます。
- 2. 「順引き情報」をクリックします。

「順引き情報」が表示されます。

3. 以下の項目を指定します

動作

- ・ドメイン名 → www.danger.com
 - →廃棄する



- 4. [追加] ボタンをクリックします。
- 5. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

35 SNMPエージェント機能を使う



本装置は、SNMP(Simple Network Management Protocol)エージェント機能をサポートしています。 ここでは、SNMPホストに対して MIB 情報を通知する場合の設定方法を説明します。



● 参照 機能説明書「2.41 SNMP機能」(P.132)



♦ SNMPとは?

SNMP (Simple Network Management Protocol)は、ネットワーク管理用のプロトコルです。SNMPホストは、ネットワーク上の端末の稼動状態や障害状況を一元管理します。SNMPエージェントは、SNMPホストの要求に対してMIB (Management Information Base)という管理情報を返します。

また、特定の情報についてはトラップという機能を用いて、SNMPエージェントからSNMPホストに対して 非同期通知を行うことができます。

● 参照 仕様一覧「3.1 標準 MIB」(P.75)、「3.2 富士通拡張 MIB」(P.97)、「3.4 Trap 一覧」(P.106)

こんな事に気をつけて

 文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白 文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

● 参照 Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P.21)

- エージェントアドレスには、本装置に設定されたどれかのインタフェースのIPアドレスを設定します。誤ったIPアドレスを設定した場合は、SNMPホストとの通信ができなくなります。
- 認証プロトコルとパスワード、暗号プロトコルとパスワードは、SNMPホストの設定と同じ設定にします。誤ったプロトコルとパスワードを設定した場合は、SNMPホストとの通信ができなくなります。
- SNMPv3で認証/暗号プロトコルを使用する場合、snmp設定反映時の認証/暗号鍵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。
- SNMPv3で使用される snmpEngineBoots 値は、装置再起動時に初期化(初期値:1)されます。そのため、MIB 情報 取得中に装置が再起動されると、SNMP ホストによっては継続した MIB 情報の取得ができないことがあります。

SNMPv1またはSNMPv2cでアクセスする場合の情報を設定する

SNMPv1またはSNMPv2cでのアクセスする場合は、以下の情報を設定します。

● 設定条件

- SNMPエージェント機能を使用する
- 管理者 : suzuki
- 機器名称 :SR-S316C2
- 機器設置場所 : 1F(1階)
- エージェントアドレス : 192.168.1.1 (自装置 IP アドレス)
- SNMPホストアドレス : 192.168.1.100
- コミュニティ名 :public00

上記の設定条件に従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「SNMP情報」をクリックします。

「SNMP情報」ページが表示されます。

2. 以下の項目を指定します。

- SNMPエージェント機能 →使用する
- 機器管理者 → suzuki
 機器名称 →指定する(SR-S316C2)
 機器設置場所 → 1F
- エージェントアドレス → 192.168.1.1

■基本情報	3
SNMPエージェント機能	○使用しない ⊙使用する
機器管理者	suzuki
機器名称	装置名称を使用する (装置名称情報が設定されていないため選択できま せん) ● 指定する 機器名 称 SR-S316C2
機器設置場所	1 F
エージェントアドレス	192.168.1.1

- 3. [保存] ボタンをクリックします。
- **4. 「SNMPv1/v2c情報」をクリックします。** 「SNMPv1/v2c情報」が表示されます。

•	SNMPホスト1	→指定する
	コミュニティ名	→ public00
	IPアドレス	→ 192.168.1.100

SNMPホスト2以降 →指定しない

■SNMPv1/v2c情報		
SNMPホスト1	 publicとする(任意のホストを対象とする) 指定する コミュニティ名 public00 IPアドレス 192.168.1.100 トラップ 送信しない ○V1 ○V2 書ぎ込み要求 ③許可しない ○許可する 	
SNMPホスト2	 ● 指定しない ● 指定する コミュニティ名 □Pアドレス トラップ ●送信しない ○V1 ○V2 書ぎ込み要求 ●許可しない ○許可する 	

6. [保存] ボタンをクリックします。

SNMPv3でアクセスする場合の情報を設定する

SNMPv3でアクセスする場合は、以下の情報を設定します。

● 設定条件

- SNMPエージェント機能を使用する
- 管理者 : suzuki • 機器名称 : SR-S316C2 • 機器設置場所 :1F (1階) • エージェントアドレス : 192.168.1.1 (自装置 IP アドレス) • SNMPホストアドレス : 192.168.1.100 トラップ通知ホストアドレス : 192.168.1.100 • ユーザ名 : user00 認証プロトコル : MD5 認証パスワード : auth_password 暗号プロトコル : DES 暗号パスワード : priv_password MIBビュー :MIB読み出しはsystem、interfacesグループのみ許可。 トラップ通知はlinkDown、linkUpトラップのみ許可。

上記の設定条件に従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「SNMP情報」をクリックします。

「SNMP情報」ページが表示されます。

2. 以下の項目を指定します。

- SNMPエージェント機能 →使用する
- 機器管理者 → suzuki
- 機器名称 →指定する(SR-S316C2)
- 機器設置場所 → 1F
- エージェントアドレス → 192.168.1.1

■基本情報		
SNMPエージェント機能	○使用しない ⊙使用する	
機器管理者	suzuki	
機器名称	装置名称を使用する 装置名称を使用する 装置名称情報が設定されていないため選択できま せん ・ 指定する 機器名 称 SR-S316C2	
機器設置場所	1F	
エージェントアドレス	192.168.1.1	

- 3. [保存] ボタンをクリックします。
- **4. 「SNMPv3情報」をクリックします**。 「SNMPv3情報」ページが表示されます。
- **5.** SNMPv3 **情報の設定項目の「MIB ビュー情報」をクリックします**。 「MIB ビュー情報」が表示されます。

→0

- 6. 以下の項目を指定します。
 - ビュー定義番号



7. [追加] ボタンをクリックします。

- サブツリー名/ビュータイプ → system / 含む
- サブツリー名/ビュータイプ → interfaces / 含む
- サブツリー名/ビュータイプ → linkdown / 含む
- サブツリー名/ビュータイプ → linkup / 含む

	サブツリー名		ビュータイプ
	system	~	⊙含む ○除<
	interfaces	~	⊙含む ○除<
	linkdown	*	⊙含む ○除<
	linkup	*	⊙含む ○除<
		*	○含む ○除<
		*	○含む ○除<
		*	○含む ○除<
0		*	○含む ○除<
0		*	○含む ○除<
		*	○含む ○除<
		*	○含む ○除<
		*	○含む ○除<
		*	○含む ○除<
		*	○含む ○除<
		~	○含む ○除<
		~	○含む ○除<

- 9. [保存] ボタンをクリックします。
- **10.** SNMPv3 **情報の設定項目の「ユーザ情報」をクリックします**。 「ユーザ情報」が表示されます。
- 11. ユーザ情報リストの [修正] ボタンをクリックします。

暗号パスワード

•	ユーザ名	→user00
•	ホストアドレス SNMPホスト トラップ通知ホスト	→ 192.168.1.100 → 192.168.1.100
•	セキュリティプロトコル 認証プロトコル 認証パスワード 暗号プロトコル	→ MD5 → auth_password → DES

- → priv_password
- MIBビュー MIB読み出し/ビュー定義番号 → MIBビュー情報を使用/0

• トラップ通知/ビュー定義番号 → MIBビュー情報を使用/0

	ユーザ 名	user00			
		SNMP木.	スト	トラップ通知ホスト	
		192.168.1.100		192.168.1.100	
	ホ スト				
	アド				
	ž				
1	セ	!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!		MD5 V	
	キ っリ				
	ティブロト	認証ハスワート			
		暗号ブロトコル		DES	
	コ ル	暗号バスワード		••••••	
		MIB書き込み	⊙許可した	ない○許可する	
	MID	MIB読み出し	○許可する	る ○許可しない ⊙ MIBビュー情報を使用	
	Ĕ	ビュー定義		義番号 0 MIBビュー情報参照	
	л —	トラップ通知 〇許可する			
			ヒュー正義		

- [保存] ボタンをクリックします。 13.
- 14. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

36 システムログを採取する

適用機種 全機種

本装置では、各種システムログ(回線の接続/切断など)をネットワーク上の syslog サーバに送信することができます。また、セキュリティログとして以下のログを採取することができます。

- URLフィルタ(遮断したパケット)
- DHCP (配布した IPv4 アドレス)

ここでは、システムログを採取する場合の設定方法を説明します。



● 設定条件

- 以下のセキュリティログを採取する
 - URLフィルタ
 - DHCP
- ログ受信用サーバのIPアドレス : 192.168.1.10

上記の設定条件に従ってシステムログを採取する場合の設定例を示します。

システムログ情報を設定する

- 設定メニューの基本設定で「装置情報」をクリックします。
 「装置情報」ページが表示されます。
- 「システムログ情報」をクリックします。
 「システムログ情報」が表示されます。
- 3. 以下の項目を指定します。
 - システムログ送信 →送信する
 送信先ホスト → 192.168.1.10
 - セキュリティログ → URLフィルタ、DHCP

システムログ情報	■システムログ情報	
	サーバ1	 ○ 送信しない ◎ 送信する 送信先ホスト 192.168.1.10
シフテルログ洋信	サーバ2	 ● 送信しない ● 送信する 送信先ホスト
	サーバ3	 送信しない 送信する 送信先ホスト
	ヘッダ部の追加	 ● しない ● する 送信元IPアドレス
セキュリティログ		♥URLフィルタ ♥DHCP

- 4. [保存] ボタンをクリックします。
- 5. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

採取したシステムログを確認する

採取したシステムログの確認方法は、お使いのサーバによって異なります。 ここでは、本装置で確認する方法を説明します。

1. 表示メニューの「システム関連」の「システムログ情報」をクリックします。

「システムログ情報」ページが表示されます。

【システムログ情報】	
システムログ情報を初期状態に戻す場合は、システムログ情報クリアをクリックしてください。	
システムログ 情報クリア	
Nov 16 18:34:24 10.35.156.172 SR-S718C2: init: system startup now. Nov 16 18:34:24 10.35.156.172 SR-S718C2: l2nsm: lan 1 vlan 20 definition is invalid. vlan 20 is not defined. Nov 16 18:34:24 10.35.156.172 SR-S718C2: protocol: ether 1 link up Nov 16 18:34:24 10.35.156.172 SR-S718C2: protocol: ether 1 link up Nov 16 18:34:24 10.35.156.172 SR-S718C2: protocol: ether 1 link up Nov 16 18:34:24 10.35.156.172 SR-S718C2: protocol: ether 1 link up Nov 16 18:34:24 10.35.156.172 SR-S718C2: protocol: ether 1 link up Nov 16 18:34:50 10.35.156.172 SR-S718C2: protocol: ether 1 link up Nov 17 11:38:40 10.35.156.172 SR-S718C2: logon: failed login b44 on console Nov 17 11:38:42 10.35.156.172 SR-S718C2: logon: login admin on console Nov 17 11:40:09 10.35.156.172 SR-S718C2: logon: login admin on console Nov 17 11:42:37 10.35.156.172 SR-S718C2: logon: exit admin on console Nov 17 11:42:31 10.35.156.172 SR-S718C2: logon: exit admin on console Nov 17 11:43:13 10.35.156.172 SR-S718C2: logon: exit admin on console	

37 スケジュール機能を使う

適用機種 全機種

本装置のスケジュール機能は、以下のとおりです。

- 構成定義情報切り替え予約
 本装置は、内部に2つ構成定義情報を持つことができます。運用構成の変更に備え、あらかじめ構成定義情報を用意し、指定した日時に新しい構成定義に切り替えることができます。
- こんな事に気をつけて 設定前に本装置の内部時刻を正しくセットしてください。

● 参照 Web ユーザーズガイド「1.5 時刻を設定する」(P18)

37.1 構成定義情報の切り替えを予約する

適用機種 全機種

本装置は、内部に構成定義情報を2つ持つことができます。

ここでは、2006年12月1日6時30分に構成定義情報を構成定義情報1から構成定義情報2に切り替える場合の 設定方法を説明します。

● 設定条件

- 実行日時 : 2006年12月1日 6時30分
- 構成定義情報切り替え :構成定義情報1の構成定義情報→構成定義情報2の構成定義情報

上記の設定条件に従って構成定義情報を切り替える場合の設定例を示します。

- **1. 設定メニューの基本設定で「スケジュール情報」をクリックします**。 「スケジュール情報」ページが表示されます。
- **2. 「構成定義切り替え予約情報」をクリックします**。 「構成定義切り替え予約情報」が表示されます。
- 3. 「構成定義切り替え予約情報」で未設定の欄の[修正]ボタンをクリックします。
- 4. 以下の項目を指定します。
 - 実行日時 →2006年12月1日6時30分
 - 動作 →構成定義情報2で再起動

実行日時	20 06 年12 月1 日6 時30 分	
動作	構成定義情報2で再起動 ⊻	

- 5. [保存] ボタンをクリックします。
- 6. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

38 アプリケーションフィルタ機能を使う

適用機種 全機種

本装置上で動作する各サーバ機能に対してアクセス制限を行うことができます。

これにより、装置をメンテナンスまたは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させる ことができます。



ここでは、アプリケーションフィルタを利用して各サーバ機能へのアクセスを制限する場合の設定方法を説明し ます。

● 設定条件

- 管理用のホスト(192.168.1.100)からのみTELNET/FTP/SSHサーバ機能へのアクセスを許可する
- 内部LANのホスト(192.168.1.0/24)からのみTIMEサーバ機能へのアクセスを許可する
- その他のサーバ機能は制限しない

こんな事に気をつけて

IP フィルタリングにより自装置へのパケットを遮断している場合、アプリケーションフィルタで許可する設定を行って いてもアクセスはできません。

上記の設定条件に従ってアプリケーションフィルタを設定する場合の設定例を示します。

メンテナンス用のサーバ機能(TELNET/FTP/SSH)にアクセスできるパソコンを制限する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL 情報」ページが表示されます。

2. 以下の項目を指定します。

定義名

→acl0

	<acl情報追加フィールド></acl情報追加フィールド>
定義名	aciO

3. [追加] ボタンをクリックします。 「ACL 定義情報(acl0)」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP 定義情報」が表示されます。

5. 以下の項目を指定します。

٠	プロトコル	→すべて
•	送信元情報	
	IP アドレス	→ 192.168.1.100
	アドレスマスク	→32 (255.255.255.255)
•	あて先情報	
	IP アドレス	→指定しない

 IP アドレス
 →指定しない

 アドレスマスク
 →0 (0.0.0.0)

 • QoS
 →指定なし

■ PE表	情報	
ブロトコル		オペて (番号指定:
送信元情	IPアドレス	192.168.1.100
報	アトレスマ スク	32 (255.255.255.255)
あて先情	IPアドレス	
報	アドレスマ スク	0 (0.0.0)
QoS		指定なし ▼ TOS、または、DSCPを選択時に値を入力してく ださい

- 6. [保存] ボタンをクリックします。
- 設定メニューの基本設定で「装置情報」をクリックします。
 「装置情報」ページが表示されます。
- **8. 「サーバ機能情報」をクリックします。** 「サーバ機能情報」が表示されます。
- **9.** 「FTP サーバ機能」のアプリケーションフィルタ機能に対する[設定]ボタンをクリックします。 「アプリケーションフィルタ情報 (FTP)」が表示されます。
- 10. 「条件にあてはまらない場合の動作」の [修正] ボタンをクリックします。
- 11. 以下の項目を指定します。

動作

→遮断

<アプリケーションフィルタ情報入力フィールド(条件にあてはまらない場合)>	
動作	 ○ 透過 ○ 遮断

12. [保存] ボタンをクリックします。

「アプリケーションフィルタ情報(FTP)」に戻ります。

- 動作
- ACL定義番号 →0

▲ 「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<アプリケーションフィルタ情報入力フィールド>	
動作 ②透過 〇 遮断	
ACL定義番号	0 参照

14. [追加] ボタンをクリックします。

15. 手順 7. ~ 14. を参考に、TELNET サーバ機能、SSH サーバ機能に対しても同様の設定を行います。

TIME サーバ機能を使用できるパソコンを192.168.1.0/24のネットワークに制限する

16. 手順 1. ~ 14. を参考に、以下の項目を設定します。

「ACL情報」

定義名

→acl1

→透過

「ACL定義情報 (acl1)」-「IP 定義情報」

•	プロトコル	→すべて
•	送信元情報 IP アドレス アドレスマスク	→ 192.168.1.0 → 24 (255.255.255.0)
•	あて先情報 IP アドレス アドレスマスク	→指定しない →0(0.0.0)
•	QoS	→指定なし

「装置情報」

「サーバ機能情報」-「アプリケーションフィルタ情報(TIME)」条件にあてはまらない場合の動作

動作 →遮断

「サーバ機能情報」-「アプリケーションフィルタ情報(TIME)」

- 動作 →透過
- ACL定義番号 → 1
- 17. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

39 IEEE802.1ad 機能を使う



ここでは、IEEE802.1ad機能を使用する場合の設定方法を説明します。

● 参照 機能説明書「2.47 IEEE802.1ad 機能」(P.143)

39.1 IEEE802.1ad 機能をポートベースサービスインタフェースとして 使う

ここでは、IEEE802.1ad機能をポートベースサービスインタフェースとして使用する場合の設定方法を説明します。



● 設定条件

[IEEE802.1ad 共通]

- サービス VLAN のタグプロトコル ID
- : 0x88a8

[VLAN タグマッピング (条件1)]

- カスタマー VLAN
- サービス VLAN

[本装置1]

• カスタマーポート

- :なし
- : 500
- : ether1 VLANタグマッピング(条件1)でカプセル化を行う すべてのフレーム(タグあり/タグなし)にサービス VLAN=500を付与し転送する
- :ether28

[本装置2]

• カスタマーポート

• プロバイダーポート

: ether1 VLANタグマッピング(条件1)でカプセル化を行う すべてのフレーム(タグあり/タグなし)にサービス VLAN=500を付与し転送する

• プロバイダーポート

: ether28

こんな事に気をつけて

VLAN タグマッピングルールで関連付けられるカスタマーポートとプロバイダーポートを、ポート間アクセス制御で互い に転送許可ポートとして設定することで、構成により発生する以下の不要な flooding パケットを抑止することができます。

- ・ カスタマーポートと IEEE802.1ad 未使用ポート間で発生する flooding パケット
- ・ プロバイダーポートと IEEE802.1ad 未使用ポート間、およびプロバイダーポート間で発生する flooding パケット

上記の設定条件に従ってIEEE802.1ad機能をポートベースサービスインタフェースとして使用する場合の設定例を示します。

本装置1を設定する

IEEE802.1ad 情報を設定する

1. 設定メニューの詳細設定で「IEEE802.1ad 情報」をクリックします。

「IEEE802.1ad情報」ページと「基本情報」が表示されます。

- 2. 以下の項目を指定します。
 - IEEE802.1ad機能 →使用する
 - タグプロトコルID →88a8

■基本情報	3
IEEE802.1ad機能	○使用しない ⊙使用する
タグブロトコルID	88a8

- 3. [保存] ボタンをクリックします。
- **4. 「VLAN タグマッピングルール情報」をクリックします**。 「VLAN タグマッピングルール情報」が表示されます。
- 5. 以下の項目を指定します。
 - サービス VLAN ID

<vlanタグマッピングルール情報入力フィールド></vlanタグマッピングルール情報入力フィールド>		
説明文		
カスタマーVLAN ID		
サービスVLAN ID	500	
サ <i>ー</i> ビスVLAN優先 順位	0 🗸	

→500

6. [追加] ボタンをクリックします。

一覧に追加されます。

カスタマーポートのether情報を設定する

- 設定メニューの詳細設定で「ether 情報」をクリックします。
 「ether 情報」ページが表示されます。
- Fether 情報」でポート番号1の[修正]ボタンをクリックします。
 ether1 情報の設定項目と「基本情報」が表示されます。

転送許可ポート

→設定する (28)

転送許可ボート	 ○ 設定しない ◎ 設定する
	28

- 10. [保存] ボタンをクリックします。
- **11.** 「IEEE802.1ad 関連」をクリックします。

「基本情報」が表示されます

12. 以下の項目を指定します。

- IEEE802.1ad 機能 →カスタマーポート
 "カスタマーポート"を選択すると、「VLAN タグマッピングルールデフォルト動作」の設定項目が表示されます。
- VLAN タグマッピングルールデフォルト動作 →転送する
- VLAN タグマッピングルール番号

→0(手順6.で追加された番号)

■基本情報	3
IEEE802.1ad機能	 ● 動作しない ● カスタマーボート ● プロバイダーボート
VLANタグマッピングルールデフォ ルト動作	 ○ 破棄する ● 転送する VLANタグマッピングルール番号 ●

「マッピングルール番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定するマッピング
 ルール番号欄の [選択] ボタンをクリックして設定します。

13. 【保存】ボタンをクリックします。

プロバイダーポートの ether 情報を設定する

14. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether 情報」ページが表示されます。

15. 「ether 情報」でポート番号28の [修正] ボタンをクリックします。 ether28 情報の設定項目と「基本情報」が表示されます。

16. 以下の項目を指定します。

• VLAN

Tagged

→500

転送許可ポート →設定する(1)

VI AN	Tagged	500
VLAN	Untagged	
転送評	F可ボート	 ○ 設定しない ● 設定する
		1

17. 【保存】ボタンをクリックします。

18. 「IEEE802.1ad 関連」をクリックします。

「基本情報」が表示されます。

19. 以下の項目を指定します。

 IEEE802.1ad 機能
 →プロバイダーポート

IEEE802.1ad機能 の かたない の カスタマーボート の プロバイダーボート	報
	lad機能 ○動作しない ○カスタマーボート ○プロバイダーポート

- 20. [保存] ボタンをクリックします。
- **21. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。 「IEEE802.1ad 情報」-「基本情報」 • IEEE802.1ad 機能 →使用する • タグプロトコルID →88a8 「IEEE802.1ad 情報」-「VLAN タグマッピングルール情報」 サービス VLAN ID →500 「ether情報」 「ether1情報」-「基本情報」 転送許可ポート →設定する(28) 「ether1 情報」-「IEEE802.1ad 関連」-「基本情報」 • IEEE802.1ad 機能 →カスタマーポート • VLAN タグマッピングルールデフォルト動作 →転送する • VLAN タグマッピングルール番号 →0 「ether情報」 「ether28情報」-「基本情報」 • VLAN → 500 Tagged 転送許可ポート →設定する(1) 「ether28情報」-「IEEE802.1ad 関連」-「基本情報」 • IEEE802.1ad 機能 →プロバイダーポート

39.2 IEEE802.1ad 機能を C-TAG サービスインタフェースとして使う

ここでは、IEEE802.1ad 機能を C-TAG(カスタマー VLAN タグ)サービスインタフェースとして使用する場合の 設定方法を説明します。



VLAN タグマッピングルールで関連付けられるカスタマーポートとプロバイダーポートを、ポート間アクセス制御で互い に転送許可ポートとして設定することで、構成により発生する以下の不要な flooding パケットを抑止することができます。 ・ カスタマーポートと IEEE802.1ad 未使用ポート間で発生する flooding パケット

・ プロバイダーポートとIEEE802.1ad 未使用ポート間、およびプロバイダーポート間で発生する flooding パケット

上記の設定条件に従ってIEEE802.1ad機能をC-TAGサービスインタフェースとして使用する場合の設定例を示します。

本装置1を設定する

IEEE802.1ad 情報を設定する

- **1. 設定メニューの詳細設定で「IEEE802.1ad 情報」をクリックします**。 「IEEE802.1ad 情報」ページと「基本情報」が表示されます。
- 2. 以下の項目を指定します。
 - IEEE802.1ad 機能
 →使用する
 - タグプロトコルID →8100

■基本情報	[3	J
IEEE802.1ad機能	○使用しない ●使用する	
タグブロトコルID	8100	

- 3. [保存] ボタンをクリックします。
- **4.** 「VLAN タグマッピングルール情報」をクリックします。 「VLAN タグマッピングルール情報」が表示されます。
- 5. 以下の項目を指定します。
 - カスタマー VLAN ID → 10
 - サービス VLAN ID → 1000
 - サービス VLAN 優先順位 →5

<vlanタグマッピングルール情報入力フィールド></vlanタグマッピングルール情報入力フィールド>		
説明文		
カスタマーVLAN ID	10	
サービスVLAN ID	1000	
サ <i>ー</i> ビスVLAN優先 順位	5 🗸	

6. [追加] ボタンをクリックします。

一覧に追加されます。

- 7. 以下の項目を指定します。
 - カスタマー VLAN ID → 20,30
 - サービス VLAN ID → 2000
- 8. [追加] ボタンをクリックします。

一覧に追加されます。

カスタマーポートの ether 情報を設定する

9. 設定メニューの詳細設定で「ether情報」をクリックします

「ether 情報」ページが表示されます。

10. 「ether 情報」でポート番号5の [修正] ボタンをクリックします。 ether5 情報の設定項目と「基本情報」が表示されます。

11. 以下の項目を指定します。

• 転送許可ポート

→設定する (27,28)

転送許可ボート	 ○ 設定しない ③ 設定する
	27,28

12. 【保存】ボタンをクリックします。

13. 「IEEE802.1ad 関連」をクリックします。

「基本情報」が表示されます。

14. 以下の項目を指定します。

- IEEE802.1ad 機能 →カスタマーポート
 "カスタマーポート"を選択すると、「VLAN タグマッピングルールデフォルト動作」の設定項目が表示されます。
- VLAN タグマッピングルールデフォルト動作 →破棄する

■基本情報	3
IEEE802.1ad機能	 ● 動作しない ● カスタマーボート ● プロバイダーボート
VLANタグマッピングルールデフォ ルト動作	 ● 破棄する ● 転送する ▼LANタグマッピングルール番号

15. [保存] ボタンをクリックします。

16. 「VLAN タグマッピングルール情報」をクリックします。

「VLANタグマッピングルール情報」が表示されます。

17. 以下の項目を指定します。

• マッピングルール番号 →0(手順6.で追加された番号)

<vlanタグマッピングルール情報入力フィールド></vlanタグマッピングルール情報入力フィールド>		
マッピングルール番号	0 参照	

「マッピングルール番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定するマッピング
 ルール番号欄の「選択」ボタンをクリックして設定します。

18. [追加] ボタンをクリックします。

一覧に追加されます。

- 19. 以下の項目を指定します。
 - マッピングルール番号 →1 (手順8.で追加された番号)
20. [追加] ボタンをクリックします。 一覧に追加されます。

プロバイダーポートの ether 情報を設定する

- **21. 設定メニューの詳細設定で「ether情報」をクリックします**。 「ether情報」ページが表示されます。
- 22. 以下の項目を指定します。
 - ポートリスト →27-28

1. L			
AD 15	27_20	修正	211世日(ト
ロフト	27-20	[™≊ III]	TURALL
221			

23. [修正] ボタンをクリックします。

ether27-28情報の設定項目と「基本情報」が表示されます。

24. 以下の項目を指定します。

- VLAN Tagged → 1000,2000
- 転送許可ポート →設定する(5)

	Tagged	1000,2000
VLAN	Untagged	
転送評	キ可ボート	 ○ 設定しない ● 設定する
		5

25. [保存] ボタンをクリックします。

26. 「ポート種別情報」をクリックします。

「ポート種別情報」が表示されます。

27. 以下の項目を指定します。

- ポート種別 →リンクアグリゲーション
 "リンクアグリゲーション"を選択すると、「リンクアグリゲーショングループ情報」の設定項目が表示されます。
- リンクアグリゲーショングループ情報 グループ番号 →1 アンカポート番号 →27

■ポート種		
ボート種別	 ○通常 ●リンクアグリゲーション ○バックアップ ○ミラー 	
リンクアグ リゲーショ ン グループ 情報	グループ番号 1 ♥ アンカポート番号 27 ♥	

28. [保存] ボタンをクリックします。

プロバイダーポートのリンクアグリゲーショングループ情報を設定する

- **29. 設定メニューの詳細設定で「リンクアグリゲーショングループ情報」をクリックします**。 「リンクアグリゲーショングループ情報」ページが表示されます。
- 30. 「リンクアグリゲーショングループ情報」でリンクアグリゲーショングループ番号が1の [修正] ボ タンをクリックします。

リンクアグリゲーショングループ1情報の設定項目と「基本情報」が表示されます。

31. 「IEEE802.1ad 関連」をクリックします。

「基本情報」が表示されます。

- 32. 以下の項目を指定します。
 - IEEE802.1ad 機能
 →プロバイダーポート

■基本情報		3
IEEE802.1ad機能	 ●動作しない ●カスタマーボート ●プロバイダーボート 	

- 33. [保存] ボタンをクリックします。
- **34. 画面左側の[設定反映]ボタンをクリックします。**

設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。 「IEEE802.1ad 情報」-「基本情報」 • IEEE802.1ad 機能 →使用する • タグプロトコルID →8100 「IEEE802.1ad 情報」-「VLAN タグマッピングルール情報」 カスタマー VLAN ID **→** 10 サービス VLAN ID → 1000 • サービス VLAN 優先順位 →5 「IEEE802.1ad 情報」-「VLAN タグマッピングルール情報」 カスタマー VLAN ID →20,30 サービス VLAN ID →2000 サービス VLAN 優先順位 →0 「ether 情報」 「ether5 情報」-「基本情報」 転送許可ポート →設定する(27,28) 「ether5 情報」-「IEEE802.1ad 関連」-「基本情報」 • IEEE802.1ad 機能 →カスタマーポート • VLAN タグマッピングルールデフォルト動作 →破棄する 「ether5 情報」-「IEEE802.1ad 関連」「VLAN タグマッピングルール情報」 マッピングルール番号 **→**0

「ether5 情報」-「IEEE802.1ad 関連」「VLAN タグマッピングルール情報」			
• マッピングルール番号	→ 1		
「ether情報」			
• ポートリスト	→27-28		
「ether 27-28 情報」-「基本情報」			
• VLAN			
Tagged	→ 1000,2000		
• 転送許可ポート	→設定する (5)		
「ポート種別情報」			
• ポート種別	→リンクアグリゲーション		
 リンクアグリゲーショングループ情報 			
グループ番号	→ 1		
アンカポート番号	→27		
「リンクアグリゲーショングループ情報」			
「リンクアグリゲーショングループ1情報」-「IEEE802.1ad 関連」-「基本情報」			
• IEEE802.1ad 機能	→プロバイダーポート		

40 IEEE802.1ah 機能を使う



ここでは、IEEE802.1ah機能を使用する場合の設定方法を説明します。

● 参照 機能説明書「2.48 IEEE802.1ah 機能」(P.146)

40.1 IEEE802.1ah 機能をポートベースサービスインタフェースとして 使う

ここでは、IEEE802.1ah機能をポートベースサービスインタフェースとして使用する場合の設定方法を説明します。



[本装置2]

 カスタマーポート 	: ether1 バックボーンサービス(0)でカプセル化を行う すべてのフレーム(タグあり/タグなし)にバックボーン VLAN=300、サービスインスタンスID=0x100を付与し転 送する
 プロバイダーポート 	:ether25 バックボーンサービス(0)でデカプセル化を行う
• 仮想 MAC アドレス	: 00:22:22:00:00:00
[本装置 3]	
 カスタマーポート 	: ether1 バックボーンサービス(0)でカプセル化を行う すべてのフレーム(タグあり/タグなし)にバックボーン VLAN=300、サービスインスタンスID=0x100を付与し転 送する
 プロバイダーポート 	:ether25 バックボーンサービス(0)でデカプセル化を行う
• 仮想 MAC アドレス	: 00:33:33:00:00:00

こんな事に気をつけて

バックボーンサービスで関連付けられるカスタマーポートとプロバイダーポートを、ポート間アクセス制御で互いに転 送許可ポートとして設定することで、構成により発生する以下の不要な flooding パケットを抑止することができます。

- 同一のサービスインスタンス ID が設定されたバックボーンサービスを利用するカスタマーポート間で発生する flooding パケット
- ・ プロバイダーポートとIEEE802.1ah 未使用ポート間、およびプロバイダーポート間で発生する flooding パケット

上記の設定条件に従ってIEEE802.1ah機能をポートベースサービスインタフェースとして使用する場合の設定例を示します。

本装置1を設定する

IEEE802.1ah 情報を設定する

 1.
 設定メニューの詳細設定で「IEEE802.1ah 情報」をクリックします。

 「IEEE802.1ah 情報」ページと「基本情報」が表示されます。

- IEEE802.1ah 機能
- サービス VLAN のタグプロトコル ID
- バックボーン VLAN タグプロトコル ID

→ 8100 → 00:11:11:00:00:00

→使用する

→8100

バックボーン送信元 MAC アドレス

■基本情報	
IEEE802.1ah機能	○使用しない ⊙使用する
MACアトレス自動学 習	⊙有効にする ○無効にする
サービスVLANタグブ ロトコルID	8100
バックボーンVLANタ クブロトコルID	8100
バックホーン送信元 MACアトレス	00:11:11:00:00:00

- 3. [保存] ボタンをクリックします。
- 4. 「バックボーンサービス関連」をクリックします。
- 5. 以下の項目を指定します。
 - インスタンス ID

→ 100

<バックボーンサ <i>ー</i> ビス	情報入力フィールド>
インスタンスID	100

- 6. [追加] ボタンをクリックします。 一覧に追加されます。
- 7. 追加された「サービスID」の [修正] ボタンをクリックします。

バックボーンサービス情報の設定項目と「共通情報」が表示されます。

- 8. 以下の項目を指定します。
 - インスタンスID

- **→** 100
- バックボーン VLAN ID → 300

■共通情報	3
説明文	
インスタンスID	100
サービスVLAN ID	
バックボーンVLAN ID	300
バックボーンVLAN 優先順位	 ●受信フレームのcos値から引き継ぐ ●新規に設定する 優先順位

- 9. [保存] ボタンをクリックします。
- **10**. 「バックボーン MAC アドレス情報」をクリックします。

「バックボーンMACアドレス情報」が表示されます。

- バックボーンあて先 MAC アドレス あて先不明フレーム
- →00:22:22:00:00:00 →マルチキャスト



12. [追加] ボタンをクリックします。

一覧に追加されます。

- 13. 以下の項目を指定します。
 - バックボーンあて先 MAC アドレス → 00:33:33:00:00:00
 あて先不明フレーム →マルチキャスト
- **14. [追加] ボタンをクリックします**。 一覧に追加されます。

カスタマーポートの ether 情報を設定する

- **15. 設定メニューの詳細設定で「ether 情報」をクリックします**。 「ether 情報」ページが表示されます。
- **16.** 「ether 情報」でポート番号1の [修正] ボタンをクリックします。 ether1 情報の設定項目と「基本情報」が表示されます。
- 17. 以下の項目を指定します。

転送許可ポート →設定する(25)

転送許可ポート	 ○ 設定しない ③ 設定する
	25

- 18. 【保存】ボタンをクリックします。
- **19.** 「IEEE802.1ah **関連」をクリックします**。 「基本情報」が表示されます。

- IEEE802.1ah機能 →カスタマーポート
 "カスタマーポート"を選択すると、「バックボーンサービスデフォルト動作」以降の設定項目が表示されます。
- バックボーンサービスデフォルト動作 →転送する
- バックボーンサービスID →0(手順6.で追加された番号)
- STP BPDU トンネリング
- LACPDUトンネリング →無効にする
- LLDPDU トンネリング

→無効にする

→無効にする

■基本情報	3
IEEE802.1ah機能	 ●動作しない ●カスタマーボート ●プロバイダーボート
バックボーンサービスデフォルト動作	 ○ 破棄する ● 転送する バックボーンサービスID ● 優照
Tagモード	 ● サービスVLAN ● カスタマーVLAN
STP BPDUトンネリング	 ● 無効にする ○ 有効にする 優先順位 □ ▼
LACPDUトンネリング	 ● 無効にする ● 有効にする 優先順位 □ ▼
LLDPDUトンネリング	 ● 無効にする ○ 有効にする 優先順位 □ ▼

「
ボックボーンサービス ID」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定するバック
ボーンサービス ID 欄の「選択」ボタンをクリックして設定します。

21. 【保存】ボタンをクリックします。

プロバイダーポートの ether 情報を設定する

- **22. 設定メニューの詳細設定で「ether情報」をクリックします**。 「ether情報」ページが表示されます。
- **23.** 「ether 情報」でポート番号 25 の [修正] ボタンをクリックします。 ether25 情報の設定項目と「基本情報」が表示されます。
- 24. 以下の項目を指定します。
 - VLAN Tagged

→300

転送許可ポート →設定する(1)

	Tagged	300
VLAN	Untagged	
転送評	₣可ポート	 ○ 設定しない ● 設定する 1

- 25. [保存] ボタンをクリックします。
- **26.** 「IEEE802.1ah **関連」をクリックします**。 「基本情報」が表示されます。
- 27. 以下の項目を指定します。
 - IEEE802.1ah 機能

→プロバイダーポート

■基本情報	3
IEEE802.1ah機能	 ●動作しない ●カスタマーボート ●プロバイダーボート

28. [保存] ボタンをクリックします。

- **29. 「プロバイダーバックボーンサービス情報」をクリックします**。 「プロバイダーバックボーンサービス情報」が表示されます。
- 30. 以下の項目を指定します。
 - バックボーンサービス ID

→0 (手順6. で追加された番号)

<バックボーンサービス !	青報入力フィールド>
バックボーンサービスID	0 参照

「バックボーンサービス ID」を指定する際は、[参照]ボタンをクリックして表示された画面から設定するバックボーンサービス ID 欄の [選択] ボタンをクリックして設定します。

31. [追加] ボタンをクリックします。

一覧に追加されます。

32. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。 「IEEE802.1ah 情報」-「基本情報」 • IEEE802.1ah 機能 →使用する • サービス VLAN のタグプロトコル ID →8100 • バックボーンVLANタグプロトコルID →8100 • バックボーン送信元 MAC アドレス →00:22:22:00:00:00 「IEEE802.1ah 情報」-「バックボーンサービス関連」 • インスタンス ID → 100 「IEEE802.1ah 情報」-「バックボーンサービス関連」-「共通情報」 バックボーンVLAN ID →300 「IEEE802.1ah 情報」-「バックボーンサービス関連」-「バックボーンMACアドレス情報」 • バックボーンあて先 MAC アドレス →00:11:11:00:00:00 あて先不明フレーム →マルチキャスト • バックボーンあて先 MAC アドレス →00:33:33:00:00:00 あて先不明フレーム →マルチキャスト 「ether情報」 「ether1情報」-「基本情報」 転送許可ポート →設定する(25) 「ether1 情報」-「IEEE802.1ah 関連」-「基本情報」 • IEEE802.1ah 機能 →カスタマーポート • バックボーンサービスデフォルト動作 →転送する バックボーンサービス ID **→**0 STP BPDU トンネリング →無効にする • LACPDU トンネリング →無効にする • LLDPDUトンネリング →無効にする 「ether情報」 「ether25情報」-「基本情報」 • VLAN →300 Tagged 転送許可ポート →設定する(1) 「ether25情報」-「IEEE802.1ah 関連」-「基本情報」 →プロバイダーポート • IEEE802.1ah 機能 「ether25 情報」-「IEEE802.1ah 関連」-「プロバイダーバックボーンサービス情報」 • バックボーンサービス ID →0

本装置3を設定する

「本装置1を設定する」を参考に、本装置3を設定します。 「IEEE802.1ah 情報」-「基本情報」 • IEEE802.1ah 機能 →使用する • サービス VLAN のタグプロトコル ID →8100 • バックボーン VLAN タグプロトコル ID →8100 • バックボーン送信元 MAC アドレス →00:33:33:00:00:00 「IEEE802.1ah 情報」-「バックボーンサービス関連」 • インスタンス ID → 100 「IEEE802.1ah 情報」-「バックボーンサービス関連」-「共通情報」 バックボーンVLAN ID →300 「IEEE802.1ah 情報」-「バックボーンサービス関連」-「バックボーンMACアドレス情報」 • バックボーンあて先 MAC アドレス →00:11:11:00:00:00 あて先不明フレーム →マルチキャスト • バックボーンあて先 MAC アドレス →00:22:22:00:00:00 あて先不明フレーム →マルチキャスト 「ether情報」 「ether1情報」-「基本情報」 転送許可ポート →設定する(25) 「ether1 情報」-「IEEE802.1ah 関連」-「基本情報」 • IEEE802.1ah 機能 →カスタマーポート • バックボーンサービスデフォルト動作 →転送する バックボーンサービス ID **→**0 STP BPDU トンネリング →無効にする • LACPDU トンネリング →無効にする • LLDPDUトンネリング →無効にする 「ether情報」 「ether25情報」-「基本情報」 • VLAN →300 Tagged 転送許可ポート →設定する(1) 「ether25情報」-「IEEE802.1ah 関連」-「基本情報」 →プロバイダーポート • IEEE802.1ah 機能 「ether25 情報」-「IEEE802.1ah 関連」-「プロバイダーバックボーンサービス情報」 • バックボーンサービス ID →0

40.2 IEEE802.1ah 機能を S-TAG サービスインタフェースとして使う

ここでは、IEEE802.1ah 機能を S-TAG(サービス VLAN タグ)サービスインタフェースとして使用する場合の設定方法を説明します。



• 仮想 MAC アドレス	: 00:22:22:00:00:00
[本装置 3]	
 カスタマーポート 	: ether1 バックボーンサービス(2)でカプセル化を行う バックボーンサービス(2)に一致しないパケットは 破棄する
 プロバイダーポート 	:ether25 バックボーンサービス(2)でデカプセル化を行う
• 仮想 MAC アドレス	: 00:33:33:00:00:00

こんな事に気をつけて

バックボーンサービスで関連付けられるカスタマーポートとプロバイダーポートを、ポート間アクセス制御で互いに転送許可ポートとして設定することで、構成により発生する以下の不要なfloodingパケットを抑止することができます。

- 同一のサービスインスタンス ID が設定されたバックボーンサービスを利用するカスタマーポート間で発生する flooding パケット
- ・ プロバイダーポートと IEEE802.1ah 未使用ポート間、およびプロバイダーポート間で発生する flooding パケット

上記の設定条件に従って IEEE802.1ah 機能を S-TAG サービスインタフェースとして使用する場合の設定例を示します。

→88a8

→00:11:11:00:00:00

本装置1を設定する

IEEE802.1ah 情報を設定する

 1. 設定メニューの詳細設定で「IEEE802.1ah 情報」をクリックします。

 「IEEE802.1ah 情報」ページと「基本情報」が表示されます。

2. 以下の項目を指定します。

- IEEE802.1ah 機能
 →使用する
- サービス VLAN タグプロトコル ID → 88a8
- バックボーン VLAN タグプロトコル ID
- バックボーン送信元 MAC アドレス

基本情報	3
IEEE802.1ah機能	○使用しない ⊙使用する
MACアトレス自動学 習	⊙有効にする ○無効にする
サービスVLANタグブ ロトコルID	88a8
バックボーンVLANタ クブロトコルID	88a8
バックボーン送信元 MACアトレス	00:11:11:00:00:00

- 3. [保存] ボタンをクリックします。
- **4.** 「バックボーンサービス関連」をクリックします。 「バックボーンサービス情報」が表示されます。

• インスタンス ID

→ 100

<バックボーンサービス情報入力フィールド>	
インスタンスID	100

6. [追加] ボタンをクリックします。

一覧に追加されます。

7. 追加された「サービス ID」の [修正] ボタンをクリックします。

バックボーンサービス情報の設定項目と「共通情報」が表示されます。

8. 以下の項目を指定します。

- サービス VLAN ID → 100
- バックボーンVLAN ID → 1000

■共通情報	3
説明文	
インスタンスID	100
サービスVLAN ID	1000
バックボーンVLAN ID	300
バックボーンVLAN 優先順位	 ●受信フレームのcos値から引き継ぐ ●新規に設定する 優先順位 ●

- 9. [保存] ボタンをクリックします。
- 10. 「バックボーン MAC アドレス情報」をクリックします。

「バックボーンMACアドレス情報」が表示されます。

- 11. 以下の項目を指定します。
 - バックボーンあて先 MAC アドレス あて先不明フレーム

→00:22:22:00:00:00 →マルチキャスト



12. [追加] ボタンをクリックします。

一覧に追加されます。

- 13. 「IEEE802.1ah 情報」をクリックし、「バックボーンサービス関連」をクリックします。
- 14. 以下の項目を指定します。
 - インスタンスID → 200
- **15. [追加] ボタンをクリックします**。 一覧に追加されます。

16. 追加された「サービスID」の [修正] ボタンをクリックします。

バックボーンサービス情報の設定項目と「共通情報」が表示されます。

- サービス VLAN ID → 200
- バックボーンVLAN ID → 2000
- 17. [保存] ボタンをクリックします。
- **18.** 「バックボーンMACアドレス情報」をクリックします。 「バックボーンMACアドレス情報」が表示されます。
- 19. 以下の項目を指定します。
 - バックボーンあて先MACアドレス → 00:33:33:00:00:00
 あて先不明フレーム →マルチキャスト
- **20. [追加] ボタンをクリックします**。 一覧に追加されます。

カスタマーポートの ether 情報を設定する

21. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether 情報」ページが表示されます。

22. 「ether 情報」でポート番号1の [修正] ボタンをクリックします。 ether1 情報の設定項目と「基本情報」が表示されます。

23. 以下の項目を指定します。

転送許可ポート

→設定する(25)

転送許可ポート	 ○ 設定しない ● 設定する
	25

- 24. [保存] ボタンをクリックします
- **25.** 「IEEE802.1ah 関連」をクリックします。

「基本情報」が表示されます。

IEEE802.1ah 機能 →カスタマーポート
 "カスタマーポート"を選択すると、「バックボーンサービスデフォルト動作」以降の設定項目が表示されます。

→無効にする

- バックボーンサービスデフォルト動作 →破棄する
- STP BPDU トンネリング →無効にする
- LACPDUトンネリング →無効にする
- LLDPDUトンネリング

■基本情報	3
IEEE802.1ah機能	 ●動作しない ●カスタマーボート ●プロバイダーボート
バックボーンサービスデフォルト動作	 ● 破棄する ● 転送する バックボーンサービスID ●照
Tagቺ∽ŀ	● サービスVLAN ● カスタマーVLAN
STP BPDUトンネリング	 ● 無効にする ○ 有効にする 優先順位 0 ▼
LACPDUトンネリング	 ● 無効にする ● 有効にする 優先順位 0 ▼
LLDPDUトンネリング	 ● 無効にする ● 有効にする 優先順位 0 ▼

- 27. [保存] ボタンをクリックします。
- **28.** 「カスタマーバックボーンサービス情報」をクリックします。 「カスタマーバックボーンサービス情報」が表示されます。
- 29. 以下の項目を指定します。
 - バックボーンサービス ID

→0(手順6.で追加された番号)

<バックボーンサービス情報入力	フィール	レドン
バックボーンサービスID	0	参照

「バックボーンサービスID」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定するバックボーンサービスID欄の「選択」ボタンをクリックして設定します。

30. [追加] ボタンをクリックします。

一覧に追加されます。

- 31. 以下の項目を指定します。
 - バックボーンサービスID →1 (手順15.で追加された番号)
- **32.** 【追加】ボタンをクリックします。 一覧に追加されます。

プロバイダーポートの ether 情報を設定する

33. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether 情報」ページが表示されます。

34. 「ether 情報」でポート番号 25 の [修正] ボタンをクリックします。 ether 25 情報の設定項目と「基本情報」が表示されます。

35. 以下の項目を指定します。

- VLAN
- Tagged → 1000,2000
- 転送許可ポート →設定する(1)

N/LAN	JUU,2UUU
Untagged	
転送許可ポート●) 設定しばい) 設定する 1

- 36. [保存] ボタンをクリックします。
- **37.** 「IEEE802.1ah **関連」をクリックします**。 「基本情報」が表示されます。
- 38. 以下の項目を指定します。

• IEEE802.1ah 機能	→プロバイダーポート	
■基本情報		3
IEEE802.1ah 機能	 ●動作しない ●カスタマーボート ● プロバイダーボート 	

- **39.** [保存] ボタンをクリックします。
- **40.** 「プロバイダーバックボーンサービス情報」をクリックします。 「プロバイダーバックボーンサービス情報」が表示されます。
- 41. 以下の項目を指定します。
 - バックボーンサービス ID →0(手順6. で追加された番号)

<バックボーンサービス情報入り	カフィールド>
バックボーンサービスID	0 参照

「バックボーンサービスID」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定するバック ボーンサービスID欄の「選択」ボタンをクリックして設定します。

42. [追加] ボタンをクリックします。

一覧に追加されます。

- 43. 以下の項目を指定します。
 - バックボーンサービスID →1 (手順15. で追加された番号)

- **44.** [追加] ボタンをクリックします。 一覧に追加されます。
- **45. 画面左側の[設定反映]ボタンをクリックします。** 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。 「IEEE802.1ah 情報」-「基本情報」 • IEEE802.1ah 機能 →使用する • サービス VLAN タグプロトコル ID → 88a8 • バックボーンVLANタグプロトコルID → 88a8 • バックボーン送信元 MAC アドレス →00:22:22:00:00:00 「IEEE802.1ah 情報」-「バックボーンサービス関連」 インスタンスID → 100 「IEEE802.1ah 情報」-「バックボーンサービス関連」-「共通情報」 サービス VLAN ID → 100 バックボーン VLAN ID → 1000 「IEEE802.1ah 情報」-「バックボーンサービス関連」-「バックボーン MAC アドレス情報」 バックボーンあて先MACアドレス →00:11:11:00:00:00 あて先不明フレーム →マルチキャスト 「ether情報」 「ether1情報」-「基本情報」 転送許可ポート →設定する(25) 「ether1情報」-「IEEE802.1ah 関連」-「基本情報」 • IEEE802.1ah 機能 →カスタマーポート バックボーンサービスデフォルト動作 →破棄する • STP BPDU トンネリング →無効にする →無効にする • LACPDUトンネリング • LLDPDU トンネリング →無効にする 「ether1 情報」-「IEEE802.1ah 関連」-「カスタマーバックボーンサービス情報」 • バックボーンサービス ID **→**0 「ether情報」 「ether 25 情報」-「基本情報」 VLAN → 1000 Tagged 転送許可ポート →設定する(1) 「ether 25 情報」-「IEEE802.1ah 関連」-「基本情報」 • IEEE802.1ah 機能 →プロバイダーポート 「ether 25 情報」-「IEEE802.1ah 関連」-「プロバイダーバックボーンサービス情報」 • バックボーンサービス ID →0

本装置3を設定する

「本装置1を設定する」を参考に、本装置3を設定します。 「IEEE802.1ah 情報」-「基本情報」 • IEEE802.1ah 機能 →使用する MAC アドレス自動学習 →有効にする • サービス VLAN タグプロトコル ID →88a8 • バックボーン VLAN タグプロトコル ID → 88a8 • バックボーン送信元 MAC アドレス →00:33:33:00:00:00 「IEEE802.1ah 情報」-「バックボーンサービス関連」 インスタンス ID →200 「IEEE802.1ah 情報」-「バックボーンサービス関連」-「共通情報」 サービス VLAN ID →200 バックボーンVLAN ID →2000 「IEEE802.1ah 情報」-「バックボーンサービス関連」-「バックボーン MAC アドレス情報」 バックボーンあて先 MAC アドレス →00:11:11:00:00:00 あて先不明フレーム →マルチキャスト 「ether情報」 「ether1 情報」-「基本情報」 →設定する (25) 転送許可ポート 「ether1 情報」-「IEEE802.1ah 関連」-「基本情報」 • IEEE802.1ah 機能 →カスタマーポート バックボーンサービスデフォルト動作 →破棄する • STP BPDU トンネリング →無効にする • LACPDU トンネリング →無効にする • LLDPDU トンネリング →無効にする 「ether1 情報」-「IEEE802.1ah 関連」-「カスタマーバックボーンサービス情報」 • バックボーンサービス ID **→**0 「ether情報」 「ether 25 情報」-「基本情報」 VLAN →2000 Tagged 転送許可ポート →設定する(1) 「ether 25 情報」-「IEEE802.1ah 関連」-「基本情報」 • IEEE802.1ah 機能 →プロバイダーポート 「ether 25 情報」- 「IEEE802.1ah 関連」- 「プロバイダーバックボーンサービス情報」 • バックボーンサービス ID **→**0

40.3 IEEE802.1ah 機能でL2 トンネリング動作を使う

ここでは、IEEE802.1ah機能使用時にLACPのトンネリング機能を使用する場合の設定方法を説明します。



前記 カスタマーネットワーク間を、LACPを使用しリンクアグリゲーションとして接続するには、物理ポート単位に1対1の接続構成を維持するため、それぞれサービスインスタンスIDを割り当てる必要があります。

● 設定条件

[IEEE802.1ah 共通]

 サービス VLAN のタグプロトコル ID 	: 0x8100
• バックボーン VLAN のタグプロトコル ID	: 0x88a8
[バックボーンサービス(1)]	
• サービスインスタンス ID	: 0x100
・ バックボーン VLAN	: 300
[バックボーンサービス(2)]	
• サービスインスタンス ID	: 0x101
・ バックボーン VLAN	: 300
[バックボーンサービス(3)]	
• サービスインスタンス ID	: 0x102
・ バックボーン VLAN	: 300
[本装置1]	
 カスタマーポート 	 : ether1 バックボーンサービス(1)でカプセル化を行う LACPのトンネリング設定を行う(優先順位:5) : ether2 バックボーンサービス(2)でカプセル化を行う LACPのトンネリング設定を行う(優先順位:5) : ether3 バックボーンサービス(3)でカプセル化を行う LACPのトンネリング設定を行う(優先順位:5)
 プロバイダーポート 	:ether25 バックボーンサービス(1,2,3)でデカプセル化を行う
 仮想 MAC アドレス 	: 00:11:11:00:00:00

[本装置2]

 カスタマーポート 	: ether1 バックボーンサービス(1)でカプセル化を行う LACPのトンネリング設定を行う(優先順位:5) : ether2 バックボーンサービス(2)でカプセル化を行う LACPのトンネリング設定を行う(優先順位:5) : ether3 バックボーンサービス(3)でカプセル化を行う LACPのトンネリング設定を行う(優先順位:5)
 プロバイダーポート 	:ether25 バックボーンサービス(1,2,3)でデカプセル化を行う
• 仮想 MAC アドレス	: 00:22:22:00:00:00

こんな事に気をつけて バックボーンサービスで関連付けられるカスタマーポートとプロバイダーポートを、ポート間アクセス制御で互いに転

- 送許可ポートとして設定することで、構成により発生する以下の不要なfloodingパケットを抑止することができます。 ・ 同一のサービスインスタンスIDが設定されたバックボーンサービスを利用するカスタマーポート間で発生する floodingパケット
- ・ プロバイダーポートと IEEE802.1ah 未使用ポート間、およびプロバイダーポート間で発生する flooding パケット

上記の設定条件に従ってIEEE802.1ah機能使用時にLACPのトンネリング機能を使用する場合の設定例を示します。

本装置1を設定する

IEEE802.1ah 情報を設定する

1. 設定メニューの詳細設定で「IEEE802.1ah 情報」をクリックします。

「IEEE802.1ah 情報」ページと「基本情報」が表示されます。

- 2. 以下の項目を指定します。
 - IEEE802.1ah 機能
 - サービス VLAN タグプロトコル ID
 - バックボーン VLAN タグプロトコル ID
- →00:11:11:00:00:00

→使用する

→8100

→88a8

バックボーン送信元 MAC アドレス

■基本情報	
IEEE802.1ah機能	○使用しない ⊙使用する
MACアドレス自動学 習	⊙有効にする ○無効にする
サービスVLANタグブ ロトコルID	8100
バックボーンVLANタ クブロトコルID	88a8
ハックホーン送信元 MACアトレス	00:11:11:00:00:00

3. [保存] ボタンをクリックします。

4. 「バックボーンサービス関連」をクリックします。

「バックボーンサービス情報」が表示されます。

- 5. 以下の項目を指定します。
 - インスタンスID → 100

<バックボーンサービス情報入	カフィールド>
インスタンスID	100

6. [追加]をクリックします。

一覧に追加されます。

7. 追加された「サービスID」の [修正] ボタンをクリックします。

バックボーンサービス情報の設定項目と「共通情報」が表示されます。

8. 以下の項目を指定します。

• バックボーンVLAN ID

→300

■共通情報		3
説明文		
インスタンスID	100	
サービスVLAN ID		
バックボーンVLAN ID	300	
バックボーンVLAN 優先順位	 ●受信フレームのcos値から引き継ぐ ●新規に設定する 優先順位 ● 	

9. [保存]をクリックします。

10. 「バックボーンMACアドレス情報」をクリックします。

「バックボーンMACアドレス情報」が表示されます。

11. 以下の項目を指定します。

バックボーンあて先 MAC アドレス → 00:22:22:00:00:00
 あて先不明フレーム →ユニキャスト

<あて先MACアドレス情報入力フィールド>		
バックボーンあて先MACアドレ ス	00:22:22:00:00:00 あて先不明フレー ム ・ ・ マルチキャスト ・ ・ ・ マーキャスト	

12. [追加]ボタンをクリックします。

一覧に追加されます。

- **13.** 「IEEE802.1ah **情報」をクリックし、「バックボーンサービス関連」をクリックします**。 「バックボーンサービス情報」が表示されます。
- 14. 以下の項目を指定します。

インスタンス ID → 101

15. [追加] ボタンをクリックします。 一覧に追加されます。

16. 追加された「サービスID」の [修正] ボタンをクリックします。

バックボーンサービス情報の設定項目と「共通情報」が表示されます。

- 17. 以下の項目を指定します。
 - バックボーン VLAN ID → 300
- 18. [保存] ボタンをクリックします。
- **19.** 「バックボーンMACアドレス情報」をクリックします。

「バックボーンMACアドレス情報」が表示されます。

- 20. 以下の項目を指定します。
 - バックボーンあて先 MAC アドレス → 00:22:22:00:00:00
 あて先不明フレーム →ユニキャスト
- **21. [追加] ボタンをクリックします**。 一覧に追加されます。
- **22.** 「IEEE802.1ah 情報」をクリックし、「バックボーンサービス関連」をクリックします。 「バックボーンサービス情報」が表示されます。
- 23. 以下の項目を指定します。
 ・ インスタンスID → 102
- **24. [追加]をクリックします**。 一覧に追加されます。
- 25. 追加された「サービス ID」の [修正] ボタンをクリックします。
 - バックボーンVLAN ID → 300
- 26. [保存] ボタンをクリックします。
- **27.** 「バックボーン MAC アドレス情報」をクリックします。 「バックボーン MAC アドレス情報」が表示されます。

28. 以下の項目を指定します。

- バックボーンあて先 MAC アドレス → 00:22:22:00:00:00
 あて先不明フレーム →ユニキャスト
- 29. [追加] ボタンをクリックします。
- **30. 設定メニューの詳細設定で「ether情報」をクリックします**。 「ether情報」ページが表示されます。
- **31.** 「ether 情報」でポート番号1の [修正] ボタンをクリックします。 ether1 情報の設定項目と「基本情報」が表示されます。
- 32. 以下の項目を指定します。
 - 転送許可ポート →設定する(25)

転送許可ポート	 ○ 設定しない ③ 設定する
	25

- 33. [保存] ボタンをクリックします。
- 34. 「IEEE802.1ah 関連」をクリックします。 「基本情報」が表示されます。
- 35. 以下の項目を指定します。
 - IEEE802.1ah 機能 →カスタマーポート "カスタマーポート"を選択すると、「バックボーンサービスデフォルト動作」以降の設定項目が表示されます。 →転送する
 - バックボーンサービスデフォルト動作
 - →0(手順6.で追加された番号)
 - STP BPDU トンネリング →無効にする LACPDUトンネリング →有効にする
 - 優先順位

バックボーンサービス ID

• LLDPDU トンネリング

→5

→無効にする

■基本情報 3 ○動作しない IEEE802.1ah機能 ⊙カスタマーボート ○プロバイダーボート ○ 破棄する 転送する バックボーンサービスデフォルト動作 バックボーンサービスID 💿 参照 ⊙ サービスVLAN Tagモード ○ カスタマーVLAN ⊙ 無効にする ○ 有効にする STP BPDUトンネリング 優先順位 0 ▼ ○無効にする ⊙ 有効にする LACPDUトンネリング 優先順位 5 🗸 ⊙ 無効にする ○有効にする LLDPDUトンネリング 優先順位 🛛 🔽



[保存] ボタンをクリックします。 36.

37. 手順12.~18.を参考に、ETHER2ポートを設定します。

• IEEE802.1ah 機能 →カスタマーポート バックボーンサービスデフォルト動作 →転送する • バックボーンサービス ID →1 (手順15.で追加された番号) • STP BPDU トンネリング →無効にする • LACPDU トンネリング →有効にする 優先順位 →5 →無効にする LLDPDUトンネリング

38. 手順12.~18.を参考に、ETHER3ポートを設定します。

IEEE802.1ah 機能
 ブックボーンサービスデフォルト動作
 ブックボーンサービスID
 STP BPDU トンネリング
 LACPDU トンネリング
 →有効にする
 ●5
 LLDPDU トンネリング
 →無効にする

プロバイダーポートの ether 情報を設定する

- **39. 設定メニューの詳細設定で「ether情報」をクリックします**。 「ether情報」ページが表示されます。
- **40.** 「ether 情報」でポート番号25の [修正] ボタンをクリックします。 ether25 情報の設定項目と「基本情報」が表示されます。

41. 以下の項目を指定します。

- VLAN
 - Tagged

→300

転送許可ポート

→設定する (1-3)

VLAN	Tagged	300
	Untagged	
転送許	可ポート	 ○ 設定しない ● 設定する 1-3

- 42. [保存] ボタンをクリックします。
- **43.** 「IEEE802.1ah **関連」をクリックします**。 「基本情報」が表示されます。
- 44. 以下の項目を指定します。
 - IEEE802.1ah 機能 →プロバイダーポート
- 45. [保存] ボタンをクリックします。
- **46. 「プロバイダーバックボーンサービス情報」をクリックします**。 「プロバイダーバックボーンサービス情報」が表示されます。
- 47. 以下の項目を指定します。
 - バックボーンサービス ID →0 (手順6. で追加された番号)

<バックボーンサービス情報入力フィールド> バックボーンサービスID 0 参照

「バックボーンサービス ID」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定するバック ボーンサービス ID 欄の [選択] ボタンをクリックして設定します。

48. [追加] ボタンをクリックします。

- ・ バックボーンサービス ID → 1(手順 15. で追加された番号)
- 50. [追加] ボタンをクリックします。
- 51. 以下の項目を指定します。
 ・ バックボーンサービスID →2(手順24.で追加された番号)
- 52. [追加] ボタンをクリックします。
- **53. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。 「IEEE802.1ah 情報」-「基本情報」 • IEEE802.1ah 機能 →使用する • サービス VLAN タグプロトコル ID →8100 • バックボーン VLAN タグプロトコル ID →88a8 • バックボーン送信元 MAC アドレス →00:22:22:00:00:00 「IEEE802.1ah 情報」-「バックボーンサービス関連」 インスタンス ID → 100 「IEEE802.1ah 情報」-「バックボーンサービス関連」- [共通情報] バックボーンVLAN ID $\rightarrow 300$ 「IEEE802.1ah 情報」-「バックボーンサービス関連」-「バックボーン MAC アドレス情報」 バックボーンあて先MACアドレス →00:11:11:00:00:00 →ユニキャスト あて先不明フレーム 「IEEE802.1ah 情報」-「バックボーンサービス関連」 インスタンスID → 101 「IEEE802.1ah 情報」-「バックボーンサービス関連」-「共通情報」 バックボーン VLAN ID → 300 • バックボーン VLAN 優先順位 →受信フレームの cos 値から引き継ぐ 「IEEE802.1ah 情報」-「バックボーンサービス関連」-「バックボーン MAC アドレス情報」 バックボーンあて先 MAC アドレス → 00:11:11:00:00:00 あて先不明フレーム →ユニキャスト 「IEEE802.1ah 情報」-「バックボーンサービス関連」 インスタンス ID → 102 「IEEE802.1ah 情報」-「バックボーンサービス関連」- [共通情報] • バックボーンVLAN ID →300 「IEEE802.1ah 情報」-「バックボーンサービス関連」-「バックボーン MAC アドレス情報」 バックボーンあて先MACアドレス →00:11:11:00:00:00 あて先不明フレーム →ユニキャスト

「ether情報」	
「ether1 情報」-「基本情報」	
 転送許可ポート 	→設定する(25)
「ether1情報」-「IEEE802.1ah関連」-「基本情	報」
• IEEE802.1ah 機能	→カスタマーポート
 バックボーンサービスデフォルト動作 	→転送する
• バックボーンサービス ID	→ 0
• STP BPDU トンネリング	→無効にする
• LACPDU トンネリング	→有効にする
優先順位	→ 5
 LLDPDUトンネリング 	→無効にする
「ether情報」	
「ether2情報」-「基本情報」	
 転送許可ポート 	→設定する(25)
「ether2情報」-「IEEE802.1ah関連」-「基本情	報」
• IEEE802.1ah 機能	→カスタマーポート
 バックボーンサービスデフォルト動作 	→転送する
• バックボーンサービス ID	→ 1
• STP BPDU トンネリング	→無効にする
• LACPDU トンネリング	→有効にする
優先順位	→ 5
• LLDPDUトンネリング	→無効にする
「ether情報」	
「ether3情報」-「基本情報」	
 転送許可ポート 	→設定する(25)
「ether3情報」-「IEEE802.1ah関連」-「基本情	報」
• IEEE802.1ah 機能	→カスタマーポート
 バックボーンサービスデフォルト動作 	→転送する
• バックボーンサービス ID	→ 2
• STP BPDU トンネリング	→無効にする
• LACPDU トンネリング	→有効にする
優先順位	→ 5
 LLDPDUトンネリング 	→無効にする
「ether情報」	
「ether25情報」-「基本情報」	
• VLAN	
Tagged	→ 300
 転送許可ポート 	→設定する(1-3)
「ether25情報」-「IEEE802.1ah関連」-「基本情	青報」
• IEEE802.1ah 機能	→プロバイダーポート

「ether25 情報」-「プロバイダーバックボーンサービス情報」

• バックボーンサービス ID

- →0 →1
- →2

41 L2 暗号機能を使う

適用機種 SR-S224CP1

L2暗号機能を使用することで、本装置間の通信セキュリティを確保することができます。



● 設定条件

[本装置1]

- ETHER27 ポートを使用する
- 暗号アルゴリズム
- 暗号条件

- : AES-CTR-128
- : 送信元 IP アドレスがネットワークA(10.10.100.0/24)のフレームのみ 暗号する

[本装置2]

•

- ETHER27 ポートを使用する
- 暗号アルゴリズム :AES-CTR-128
 - 暗号条件 : あて元 IP アドレスがネットワーク A (10.10.100.0/24) のフレームのみ 暗号する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

- (1) 送信元 IP アドレスがネットワークAの ACL を設定する
- **1. 設定メニューの詳細設定で「ACL 情報」をクリックします**。 「ACL 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 定義名

→acl0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	aci0	

3. [追加] ボタンをクリックします。

「ACL 定義情報(acl0)」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP 定義情報」が表示されます。

5. 以下の項目を指定します。

•	プロトコル	→すべて
•	送信元情報	
	IPアドレス	→ 10.10.100.0
	アドレスマスク	→24 (255.255.255.0)
•	あて先情報	

IPアドレス	→指定しない
アドレスマスク	→0 (0.0.0.0)

٠	QoS	→指定なし
٠	QoS	→指定なし

■IP定義			
ブロトコル		すべて (番号指定: ~ その他 ~ を選択時のみ有効で す)	
送信元情	IPアドレス	10.10.100.0	
報	アドレスマ スク	24 (255.255.255.0)	
あて先情	IPアドレス		
報	アドレスマ スク	0 (0.0.0)	
QoS		指定なし ♥ ToS、または、DSCPを選択時に値を入力してく ださい	

6. [保存] ボタンをクリックします。

(2)送信元IPアドレスがネットワークA以外のACLを設定する

7. 手順1.~6.を参考に、以下の項目を設定します。

「ACL情報」

• QoS →指定なし

(3) ETHER27 ポートで暗号情報および暗号条件を設定する

8. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether 情報」ページが表示されます。

9. 「ether 情報」でポート番号が27の [修正] ボタンをクリックします。 ether 27 情報の設定項目と「基本情報」が表示されます。

10. 「L2暗号関連」をクリックします。

L2 暗号関連の設定項目と「基本情報」が表示されます。

11. 以下の項目を指定します。

暗号機能(送信用)

•	暗号アルゴリズム	→aes-ctr-128	
•	暗号鍵 鍵識別 鍵	→文字列 → ABCDEFGHIJKLMNOP	
•	認証鍵 鍵識別 鍵	→文字列 → ABCDEF1234567890	
復	復号機能(受信用)		
•	暗号アルゴリズム	→aes-ctr-128	

- 暗号鍵
 鍵識別 →文字列
 鍵 →ABCDEFGHIJKLMNOP
- 認証鍵 鍵識別 鍵

- →文字列
- → ABCDEF1234567890

■基本情報			
	暗号アルゴリ ズム		aes-ctr-128 💌
陪早継於	暗号鍵	鍵識別	○16進数 ⊙文字列
(送信用)		鏈	••••••
	認証鍵	<mark>鍵識別</mark>	○16進数
		鏈	•••••
	暗号アル ズム	ルゴリ	aes-ctr-128 💌
復早継終	暗号鍵	<mark>鍵識別</mark>	○16進数 ⊙文字列
(受信用)		鏈	•••••
	認証鍵	<mark>鏈識別</mark>	○16進数
		鏈	•••••

- 12. [保存] ボタンをクリックします。
- 13. 「暗号化条件」をクリックします。

「暗号化条件」が表示されます。

- 14. 以下の項目を指定します。
 - 動作 →暗号化する
 - ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<暗号化条件入力フィールド>		
動作	●暗号化する●暗号化しない	
ACL定義番号	0 参照	

- 15. [追加] ボタンをクリックします。
- 16. 手順13.~15.を参考に、以下の項目を設定します。
 - 動作 →暗号化しない
 - ACL 定義番号 →1
- **17. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

「ACL情報」

定義名

「ACL定義情報 (acl0)」-「IP 定義情報」

•	プロトコル	→すべて
•	送信元情報	
	IPアドレス	→指定しない
	アドレスマスク	→0 (0.0.0)
•	あて先情報	
	IPアドレス	→ 10.10.100.0
	アドレスマスク	→24 (255.255.255.0)
•	QoS	→指定なし
ΓA	CL 情報」	
•	定義名	→acl1
ГA	CL定義情報(acl1)」-「IP定義情	青報」
•	プロトコル	→すべて
•	送信于情報	
-		→指定しない
	アドレスマスク	→0 (0.0.0.0)
•	あて先情報	
-	旧アドレス	→指定しない
	アドレスマスク	→0 (0.0.00)
•	005	→指定なし、
Гa		
Ie		埜平 牧]
眙	号機能 (受信用)	
•	暗号アルゴリズム	→aes-ctr-128
•	暗号鍵	
	鍵識別 275	→文字列
	<i>铤</i>	→ABCDEFGHIJKLMNOP
•	認証鍵	
	鍵: 武) / · · · · · · · · · · · · · · · · · ·	→又字列
	, , 建 ,	→ ABCDEF 1234567890
復	号機能(受信用)	
•	暗号アルゴリズム	→aes-ctr-128
•	暗号鍵	
	鍵識別	→文字列
	<i>键</i>	→ABCDEFGHIJKLMNOP
•	認証鍵	
	鍵:武別 27	→又字列
_	JUE	→ ABCDEF 1234567890
le	ther 27 情報」- 1L2 暗号関連」-	暗号化条件]
•	動作	→暗号化する
•	ACL定義番号	→0
•	動作	→暗号化しない
•	ACL定義番号	→ 1

42 無線 LAN 管理機能を使う

適用機種 全機種

42.1 無線 LAN 管理機能の環境を設定する

適用機種 全機種

ここでは、複数の無線LANアクセスポイントによって構成されたネットワークを無線LAN管理機能で管理する 場合の設定方法を説明します。



無線LANの監視を実施する場合は、1台以上の無線LANアクセスポイントを監視用に設定してください。

無線 LAN 管理機能で監視できる無線 LAN チャネルは、監視用に設定した無線 LAN アクセスポイントの周辺アクセスポイント検出機能の設定に依存します。周辺アクセスポイント検出機能の設定方法は、弊社製の無線 LAN アクセスポイント (SR-M20AP1)のマニュアルを参照してください。

こんな事に気をつけて

- 管理機器のログイン時の入力プロンプトは、システムデフォルトのままとしてください。管理機器のログイン時の入 カプロンプトを変更された場合、無線LAN管理機器の動作は不定となります。
- 管理機器で nodemgr アカウントの情報を変更した場合、無線 LAN 管理機能の対応するアカウント情報も同時に変更 するようにしてください。

● 設定条件

•	议定不计	
٠	無線 LAN 管理対象	
	管理グループ	
	グループ名	: GroupA
	無線 LAN アクセスポイント 1	
	管理機器名	: AP_A01
	IPアドレス	: 192.168.1.10
	アカウント	:ユーザID:nodemgr、パスワード:nodemgr1
	無線 LAN アクセスポイント2	
	管理機器名	: AP_A02
	IPアドレス	: 192.168.1.11
	アカウント	:ユーザID:nodemgr、パスワード:nodemgr2
•	監視用無線 LAN アクセスポイント	
	周辺アクセスポイント検出機能をスキャン専用	モードで運用
	使用する無線LANモジュール	: ieee80211 1、ieee80211 2
	管理機器名	: Watcher
	IPアドレス	: 192.168.1.20
	監視用アカウント	:ユーザID:nodemgr、パスワード:nodemgr3
•	管理外無線 I AN アクセスポイント	
	MACアドレス	: 00.90.cc.c8.d1.51
•	管理情報取得の時間パラメタ(アクセフポイン)	トモニターング田)
•	自注 同報 取得の 時间 パリスタ () ノビス パイノ 情報 取得問隔	ドビータワンク用/ ・10 秒
	情報取得待機問隔	10秒
	情報取得タイムアウト時間	• 5利
_		
•	監視のパフメダ(アクセスホイノトモニダリノ: 右娘 I A N	
	病派LAN 稼動監視問愿	• 10 利
	1%到血1元回府 寂乱时妇法继問原	10秒
	稼動監視タイムアウト時間	- 101多
		· 545
	スキャンレポート取得問隔	• 10 秋
	スキャンレホート取得高橋	: 10秒
	スキャンレホート取得内協同橋	· 10秒
•	監視ログのハラメダ(アクセスホイントモーダ) 影視ログロ共体数	リンク/クライアントモ_タリンク用) - 100/#
	この時代は、1000年月代数	· 100 î +
•	無線LAN端末のRSSI監視のパラメタ(クライフ	アントモニタリング用)
	RSSI評価母数	:10 個
	RSSI最低しきい値	: 20

上記の設定条件に従って設定を行う場合の設定例を示します。

管理グループを設定する

1. 設定メニューの無線LAN管理設定で「無線LAN管理情報」をクリックします。 「無線LAN管理情報」ページが表示されます。

- **2. 「管理グループ情報」をクリックします**。 「管理グループ情報」が表示されます。
- 3. 以下の項目を指定します。
 - グループ名

→ GroupA

<管理グループ情報入力フィールド>	
グループ名	GroupA

4. [追加] ボタンをクリックします。

無線 LAN アクセスポイントを設定する

- 設定メニューの無線LAN 管理設定で「無線LAN 管理情報」をクリックします。
 「無線LAN 管理情報」ページが表示されます。
- 「管理機器情報」をクリックします。
 「管理機器情報」が表示されます。
- 7. 以下の項目を指定します。
 - 管理機器名 → AP_A01

<管理機器情報入力フィールド>	
管理機器名	AP_A01

8. [追加] ボタンをクリックします。

管理機器情報の設定項目と「基本情報」が表示されます。
9. 無線LANアクセスポイント1について、以下の項目を指定します。

• グループ

• IPアドレス

- → GroupA
- → 192.168.1.10
- 無線LAN管理パスワード → nodemgr1
- 無線 LAN 管理パスワード(確認用)
- 監視用
- 無線 LAN 端末の情報取得

→情報取得する

→ nodemgr1

→使用しない

■基本情	報 [?]
管理機 器名	AP_A01
グループ	0:GroupA 💌
IPアドレ ス	192.168.1.10
無線LAN	
管理バス	•••••
ワード	
無線LAN	
管理バス	
ワード	
(確認用)	
監視用	○使用する ●使用しない
無線LAN	
端末の	
情報取	
得	

監視用を「使用する」に設定した無線LAN管理機器の無線LANの監視を実施する場合は、監視用を「使用する」に
設定した無線LAN管理機器を相互に監視できる範囲内に2台以上設置してください。

- 10. 【保存】ボタンをクリックします。
- **11.** 無線LAN アクセスポイント1と同様に、無線LAN アクセスポイント2について、以下の項目を指定します。

「無線LAN管理情報」-「管理機器情報」

• 管理機器名	→ AP_A02
「管理機器情報(1)」-「基本	情報」
• グループ	→GroupA
• IPアドレス	→ 192.168.1.11
● 無線 LAN 管理パスワード	→nodemgr2
● 無線 LAN 管理パスワード	(確認用) → nodemgr2
● 監視用	→使用しない
 無線LAN端末の情報取得 	→情報取得する

12. [保存] ボタンをクリックします。

監視用無線LANアクセスポイントを設定する

無線LANアクセスポイント1、2と同様に、監視用無線LANアクセスポイントについて、以下の項目 13. を設定します。

「無線LAN管理情報」-「管理機器情報」

• 管理機器名	→ Watcher
「管理機器情報(4)」-「基本情報」	
• IPアドレス	→ 192.168.1.20
• 無線 LAN 管理パスワード	→ nodemgr3
• 無線LAN管理パスワード(確認用)	→ nodemgr3
● 監視用	→使用する
• 無線 LAN 端末の情報取得	→情報取得しない

 ・ 無線 LAN 端末の情報取得

管理外無線 LAN アクセスポイントを設定する

管理外無線 LAN アクセスポイントとして登録します。



使用目的が明確で管理不要な無線LANアクセスポイントを管理外無線LANアクセスポイントとして設定すると、不明無線LANアクセスポイントのモニタリングが容易となります。

14. 設定メニューの無線LAN 管理設定で「無線LAN 管理情報」をクリックします。

「無線 LAN 管理情報」ページが表示されます。

- 「管理外機器情報」をクリックします。 15. 「管理外機器情報」が表示されます。
- 16. 以下の項目を指定します。
 - 管理外機器名 →UMAP01
 - MACアドレス →00:90:cc:c8:d1:51

<管理外機器情報入力フィールド>				
管理外機器名 UMAP01				
MACアドレス	00:90:cc:c8:d1:51			

「追加」ボタンをクリックします。 17.

管理情報取得の時間パラメタを設定する

設定メニューの無線LAN 管理設定で「無線LAN 管理パラメタ情報」をクリックします。 18.

「無線LAN管理パラメタ情報」ページが表示されます。

「無線LAN管理パラメタ情報」をクリックします。 19.

「無線LAN 管理パラメタ | が表示されます。

20. 以下の項目を指定します。

•	管理-管理情報取得	→する
	情報取得間隔	→10秒
	情報取得待機間隔	→10秒
	情報取得タイムアウト	→5秒

■無	線LAN管理パラメタ				3
管理	管理情報取得	 ●しない ●する 情報取得間隔 情報取得待機間隔 情報取得タイムアウト 	10 10 5	秒 秒 秒	



種 置 一管理
-管理
情報取得のパラメタ
「情報取得間隔」と
「情報取得待機間隔」の設定は、
監視ポリシーに従って
最適な値 を設定するようにしてください。

21. [保存] ボタンをクリックします。

有線LAN、無線LANの監視パラメタを設定する

有線 LAN、無線 LAN の監視パラメタ、監視ログのパラメタや無線 LAN 端末の RSSI 監視のパラメタなどを設定し ます。

設定メニューの無線LAN 管理設定で「無線LAN 管理パラメタ情報」をクリックします。 22.

「無線 LAN 管理パラメタ情報」ページが表示されます。

「無線LAN管理パラメタ情報」をクリックします。 23.

「無線LAN管理パラメタ」が表示されます。

24. 以下の項目を指定します。

•	監視-有線LAN	→する
	稼動監視間隔	→10秒
	稼動監視待機間隔	→10秒
	稼動監視タイムアウト	→5秒
	通信異常判定しきい値	→6□
•	監視-無線 LAN	→する
	スキャンレポート取得間隔	→10秒
	スキャンレポート取得待機間隔	→10秒
	スキャンレポート取得タイムアウト	→60秒
	通信異常判定しきい値	→6□
•	監視-無線LAN端末のRSSI監視	
	RSSI評価母数	→ 10 🗆
	RSSI最低しきい値	→20

 監視-監視ログ 保持件数

→100件

	有線LAN	 ●しない ●する 稼動監視間隔 10 秒 稼動監視待機間隔 10 秒 稼動監視タイムアウト 5 秒 通信異常判定しきい値
監視	無線LAN	 ●しない ●する スキャンレボート取得間隔 10 秒 スキャンレボート取得待機間隔 10 秒 スキャンレボート取得なイムアウト 6 回
	無線LAN端末のRSSI 監視	RSSI評価母数 10 回 RSSI最低しぎい値 20
	監視ログ	保持件数 100 件

は下のパラメタは、監視ポリシーに従って最適な値を設定するようにしてください。 ・監視−有線LANのパラメタ「稼動監視間隔」と「稼動監視待機間隔」

・監視-無線LANのパラメタ「スキャンレポート取得間隔」と「スキャンレポート取得待機間隔」

- 25. [保存] ボタンをクリックします。
- 26. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

42.2 アクセスポイントモニタリングを行う

適用機種 全機種

無線 LAN 管理機能は、アクセスポイントモニタリングをすることができます。

- モニタリングは各管理機器にアクセスして収集した結果を出力していますので、構成定義の設定直後や、ネットワー 補足 クの状況によっては収集が完了しておらず、途中の状態が表示される場合があります。この場合は、しばらく時間を 置いたあと、再度モニタリング結果を表示してみてください。
 - ・使用目的が明確で管理不要な無線LANアクセスポイントを管理外無線LANアクセスポイントとして設定すると、不 明無線 LAN アクセスポイントのモニタリングが容易となります。

ここでは、「42.1 無線 LAN 管理機能の環境を設定する | (P.394) で構築した環境に対するアクセスポイントモニ タリングの設定例を示します。

管理無線LAN アクセスポイントのモニタリング結果の一覧を表示する

1. 表示メニューで「無線 LAN 管理関連」の「管理無線 LAN アクセスポイントの監視状況の一覧表示」 をクリックします。

「管理無線 LAN アクセスポイントの監視状況の一覧表示」ページが表示され、管理無線 LAN アクセスポイントの 監視状況の一覧が確認できます。

■ 参照 画面の表示結果については、コマンドリファレンス -運用管理編 - 「show nodemanager logging wlan scan managed brief」を参照してください。

管理無線 LAN アクセスポイントの有線 LAN、無線 LAN のモニタリング結果を表示する

表示メニューで「無線LAN管理関連」の「管理機器の詳細情報表示」をクリックします。 1. 「管理機器の詳細情報表示」ページが表示され、稼動状況が確認できます。

管理無線 LAN アクセスポイントの無線 LAN のモニタリング結果を表示する

1. 表示メニューで「無線LAN 管理関連」の「管理無線LAN アクセスポイントの監視状況の表示」をク リックします。

「管理無線 LAN アクセスポイントの監視状況の表示」ページが表示され、管理無線 LAN アクセスポイントの監視 状況が確認できます。

画面の表示結果については、コマンドリファレンス - 運用管理編 - 「show nodemanager logging wlan scan 🖝 参照 managed」を参照してください。

管理外無線 LAN アクセスポイントのモニタリング結果を表示する

1. 表示メニューで「無線 LAN 管理関連」の「管理外無線 LAN アクセスポイントの監視状況の表示」を クリックします。

「管理外無線 LAN アクセスポイントの監視状況の表示」ページが表示され、管理外無線 LAN アクセスポイントの 監視状況が確認できます。



画面の表示結果については、コマンドリファレンス -運用管理編 - 「show nodemanager logging wlan scan unmanaged」を参照してください。

[●] 参照 画面の表示結果については、コマンドリファレンス - 運用管理編 - 「show nodemanager node」を参照してくださ い。

不明無線 LAN アクセスポイントのモニタリング結果を表示する

1. 表示メニューで「無線LAN 管理関連」の「不明無線LAN アクセスポイントの監視状況の表示」をクリックします。

「不明無線 LAN アクセスポイントの監視状況の表示」ページが表示され、不明無線 LAN アクセスポイントの監視状況が確認できます。

42.3 クライアントモニタリングを行う

適用機種 全機種

無線 LAN 管理機能は、無線 LAN アクセスポイントと接続している無線 LAN 端末のクライアントモニタリングを することができます。



モニタリングは各管理機器にアクセスして収集した結果を出力していますので、構成定義の設定直後や、ネットワー クの状況によっては収集が完了しておらず、途中の状態が表示される場合があります。この場合は、しばらく時間を 置いたあと、再度モニタリング結果を表示してみてください。

ここでは、「42.1 無線 LAN 管理機能の環境を設定する | (P.394) で構築した環境に対するクライアントモニタリ ングの設定例を示します。

無線LAN端末の受信信号強度のモニタリング結果を表示する

1. 表示メニューで「無線LAN 管理関連」の「無線LAN 端末のRSSI 最大値/最小値の一覧表示」をク リックします。

「無線 LAN 端末の RSSI 最大値/最小値の一覧表示」ページが表示され、無線 LAN 端末の受信信号強度状況が確 認できます。

無線 LAN 端末の接続状況をモニタリングする

1. 表示メニューで「無線 LAN 管理関連」の「無線 LAN インタフェースの無線 LAN 端末情報の表示」を クリックします。

「無線 LAN インタフェースの無線 LAN 端末情報の表示 | ページが表示されます。

2. 無線LAN端末情報を表示させる管理機器を選択します。

選択した管理機器の無線LAN端末情報が確認できます。

画面の表示結果については、コマンドリファレンス -運用管理編 - 「show nodemanager logging wlan sta」を参照 ● 参照 してください。

「無線LAN 端末の接続拒否情報をモニタリングする

表示メニューで「無線 LAN 管理関連」の「接続拒否の無線 LAN 端末情報の表示」をクリックします。 1. 「接続拒否の無線 LAN 端末情報の表示」ページが表示されます。

2. 接続拒否の無線LAN 端末情報を表示させる管理機器を選択します。

選択した管理機器の無線 LAN 端末情報が確認できます。



画面の表示結果については、コマンドリファレンス -運用管理編 - 「show nodemanager logging wlan reject」を参 照してください。

 [●] 参照 画面の表示結果については、コマンドリファレンス - 運用管理編 - 「show nodemanager logging wlan starssi | を 参照してください。

無線LAN インタフェースのトレース情報をモニタリングする

- **1. 表示メニューで「無線 LAN 管理関連」の「無線 LAN 通信のトレース情報の表示」をクリックします**。 「無線 LAN 通信のトレース情報の表示」ページが表示されます。
- 2. 無線LAN通信のトレース情報を表示させる管理機器を選択します。

選択した管理機器の無線 LAN 通信のトレース情報が確認できます。

42.4 無線 LAN アクセスポイントに MAC アドレスフィルタを配布する (MACアドレスフィルタ配布)

適用機種 全機種

無線 LAN 管理機能は、無線 LAN アクセスポイントへの無線 LAN 端末の(MAC アドレスによる)接続許可情報を 一括管理して配布することができます。



管理機器のMACアドレスフィルタをクリアしたい場合は、MACアドレスフィルタを設定していないMACアドレス フィルタセットを配布してください。

● 設定条件

- ・ 無線 LAN の接続を許可する端末
 無線LAN端末1(MACアドレス:00:00:0e:f5:43:d1) 無線LAN端末2(MACアドレス:00:00:0e:f5:43:d2) 無線LANの接続を拒否する端末 上記以外
- MACアドレスフィルタの配布先 無線LANアクセスポイント1 無線LANアクセスポイント2

ここでは、「42.1 無線 LAN 管理機能の環境を設定する」(P.394) で構築した環境に対する MAC アドレスフィル 夕配布の設定例を示します。

- 1. 設定メニューの無線LAN 管理設定で「MAC アドレスフィルタセット情報」をクリックします。 「MAC アドレスフィルタセット情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - MACアドレスフィルタセット名 → GroupA_MacFilterSet

<MACアドレスフィルタセット情報入力フィールド> MACアドレスフィルタセット名 GroupA_MacFilterSet

- 3. [追加] ボタンをクリックします。
- 「MACアドレスフィルタセット情報」でMACアドレスフィルタセット名が GroupA_MacFilterSetの 4. [MACアドレスフィルタ] ボタンをクリックします。

MAC アドレスフィルタ情報の設定項目と「MAC アドレスフィルタ情報」が表示されます。

5. 以下の項目を指定します。

• MAC アドレスフィルタ

→00:00:0e:f5:43:d1,pass,STATION_001 00:00:0e:f5:43:d2,pass,STATION_002 any, reject

	<macアドレスフィルタ入力フィールド></macアドレスフィルタ入力フィールド>				
MAC アドスィリンフルタ	<macアドレスフィルタ入力フィールド> 00:00:0e:f5:43:d1,pass,STATION_001 00:00:0e:f5:43:d2,pass,STATION_002 any,reject</macアドレスフィルタ入力フィールド>	<			
		>			

- 6. [保存] ボタンをクリックします。
- 7. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。
- 操作メニューで「無線LAN 管理操作」の「MAC アドレスフィルタ配布」をクリックします。 8. 「MACアドレスフィルタ配布」ページが表示されます。
- 9. 以下の項目を指定します。
 - AP_A01のMACアドレスフィルタセット名 → 0:GroupA_MacFilterSet
 - AP_A02のMACアドレスフィルタセット名 → 0:GroupA_MacFilterSet

■管理機器一覧						
グルーフ	1	管理機器				
定義番 号	グループ 名	定義番 号	管理機器 名	タイ ブ	MAC / Fレスノイルスピット名	
0	GroupA	0	AP_A01	wlan	0:GroupA_MacFilterSet 💌	
	GroupA	1	AP_A02	wlan	0:GroupA_MacFilterSet 💌	

| MACアドレスフィルタを配布しない管理機器のMACアドレスフィルタセット名は、空欄のままとしてください。

[MACアドレスフィルタ配布] ボタンをクリックします。 10.

MAC アドレスフィルタ配布の実行結果が表示され、管理対象となった無線 LAN アクセスポイントに MAC アドレ スフィルタの配布が行われます。



■ 参照 画面の実行結果については、コマンドリファレンス - 運用管理編 - 「nodemanagerctl update wlan filterset」を参照 してください。

42.5 無線 LAN アクセスポイントの電波出力を調整する (電波出力自動調整)

適用機種 全機種

無線 LAN 管理機能は、無線 LAN アクセスポイントの電波出力を調整することができます。



近隣管理機器には、電波出力自動調整機能で設定対象の無線LANアクセスポイントの無線を到達させたい無線LAN アクセスポイントを設定します。ただし、電波出力自動調整による送信出力の調整には時間がかかりますので、必要 以上に近隣管理機器を設定しないようにしてください。電波出力自動調整は、構成定義で設定した"電波自動調整の RSSI最低しきい値"に近い値になるまで、以下の処理を繰り返します。

- 1. 近隣管理機器での周辺アクセスポイント情報の取得 必要時間:約60秒×近隣管理機器の台数
- 2. 電波出力の確認 RSSI最低しきい値に近い値であれば終了
- 3. 無線LANアクセスポイントの無線送信出力の設定 必要時間:約10秒
- 4. 無線送信出力の安定待ち 必要時間:約90秒
- 5. 手順1.の処理から繰り返し

こんな事に気をつけて

- 電波出力自動調整は、無線LANインタフェースの動作タイプがAPのみ(未設定を含む)で構成される無線LANアクセスポイントを対象とするようにしてください。
- 電波出力自動調整の近隣機器には、以下の条件を満たす無線LANアクセスポイントを指定してください。
 調整対象と同じ無線LANモジュールが動作している。
 - その無線LANモジュールの動作タイプは、AP、SCANONLYまたは未設定のみから構成される。
- 電波出力自動調整の実施中は、無線の状態が不安定になる可能性があります。よって、メンテナンスなどの通常運用
 時以外で電波出力自動調整を行うようにしてください。

● 設定条件

- 電波出力を調整する無線LANアクセスポイント 無線LANアクセスポイント1 無線LANアクセスポイント2
- 無線LANアクセスポイント1の近隣管理機器
 無線LANアクセスポイント2、監視用無線LANアクセスポイント
- ・ 無線 LAN アクセスポイント2の近隣管理機器
 無線 LAN アクセスポイント1、監視用無線 LAN アクセスポイント
- 電波出力自動調整のRSSI最低しきい値 : 20

ここでは、「42.1 無線 LAN 管理機能の環境を設定する」(P.394) で構築した環境に対する電波出力自動調整の設定例を示します。

1. 設定メニューの無線LAN管理設定で「無線LAN管理情報」をクリックします。

「無線 LAN 管理情報」ページが表示されます。

2. 「管理機器情報」をクリックします。

「管理機器情報」が表示されます。

「管理機器情報」で管理機器名がAP_A01の「修正」ボタンをクリックします。
 管理機器情報の設定項目と「基本情報」が表示されます。

以下の項目を指定します。 4.

● 近隣管	音理機器	→1、4	
近隣管 理機器	1:AP_A02 💙 4:Watcher 💙	v v	

- 5. [保存] ボタンをクリックします。
- AP A01と同様に、AP A02について、以下の項目を指定します。 6.
 - 近隣管理機器 **→**0、4
- 7. [保存] ボタンをクリックします。
- 8. 設定メニューの無線LAN管理設定で「無線LAN管理パラメタ情報」をクリックします。 「無線 LAN 管理パラメタ情報」ページが表示されます。
- 「無線LAN管理パラメタ情報」をクリックします。 9. 「無線 LAN 管理パラメタ | が表示されます。
- 10. 以下の項目を指定します。
 - 管理-電波出力自動調整 RSSI 最低しきい値 →20

電波出力自動調整 RSSI最低しきい値 20 理

- [保存] ボタンをクリックします。 11.
- 12. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。
- 13. 操作メニューで「無線 LAN 管理操作」の「無線 LAN 電波出力の自動調整」をクリックします。 「無線 LAN 電波出力の自動調整」ページが表示されます。

14. 以下の項目を指定します。

- AP_A01の電波出力自動調整をチェック
- AP_A02の電波出力自動調整をチェック

■管理機器一覧							
グループ	電波出力						
定義番号	グループ名	定義番号	管理機器名	タイプ	自動調整		
0	GroupA	0	AP_A01	wlan			
	GroupA	1	AP_A02	wlan	 Image: A start of the start of		

15. [電波出力自動調整] ボタンをクリックします。

電波出力自動調整の実行結果が表示され、管理対象となった無線LANアクセスポイントの電波出力が自動的に調 整されます。



電波出力の自動調整を開始したあとにキャンセルした場合、現在処理中の無線 LAN アクセスポイントの電波出力の調 │ 整が完了するまでバックグラウンドで処理を行います。この間、無線 LAN 管理機能のほかの操作はできません。



■ 参照 画面の実行結果については、コマンドリファレンス - 運用管理編 - 「nodemanagerctl wlan autotxpower」を参照し てください。

42.6 無線 LAN アクセスポイントの無線 LAN チャネルを調整する

適用機種 全機種

無線 LAN 管理機能は、無線 LAN アクセスポイントの無線 LAN チャネルを自動的に調整することができます。

こんな事に気をつけて

無線 LAN チャネル自動調整の実施中は、無線の状態が不安定になる可能性があります。よって、メンテナンスなどの通 常運用時以外で無線 LAN チャネル自動調整を行うようにしてください。

● 設定条件

- IEEE802.11n 通信時に使用する帯域幅 通信帯域幅 : 40MHz
- 5GHz帯のチャネル自動調整 割当範囲 : w52/53/56
- 2.4GHz帯のチャネル自動調整
 判定用 RSSI しきい値 : 20
 開始チャネル : 1
 チャネル割当間隔 : 5

ここでは、「42.1 無線 LAN 管理機能の環境を設定する」(P.394) で構築した環境に対する無線 LAN チャネル自動 調整の設定例を示します。

- **1. 設定メニューの無線LAN 管理設定で「無線LAN 管理パラメタ情報」をクリックします**。 「無線LAN 管理パラメタ情報」ページが表示されます。
- 2. 「無線LAN管理パラメタ情報」をクリックします。

「無線LAN管理パラメタ」が表示されます。

- 3. 以下の項目を指定します。
 - 管理-チャネル自動調整-共通 通信帯域幅 →40MHz
 - 管理-チャネル自動調整-5GHz帯
 割当範囲 → w52/53/56
 - 管理-チャネル自動調整-2.4GHz帯
 判定用 RSSI しきい値 → 20
 開始チャネル → 1
 チャネル割当間隔 → 5



- 4. [保存] ボタンをクリックします。
- 5. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

6. 操作メニューで「無線LAN 管理操作」の「無線LAN チャネルの自動調整」をクリックします。

「無線 LAN チャネルの自動調整」ページが表示されます。

7. 以下の項目を指定します。

- AP_A01のチャネル自動調整をチェック
- AP_A02のチャネル自動調整をチェック

■管理機器一覧						
グループ 管理機器					チャネル	
定義番号	グループ名	定義番号	管理機器名	タイプ	自動調整	
0	GroupA	0	AP_A01	wlan		
	GroupA	1	AP_A02	wlan		

8. [チャネル自動調整] ボタンをクリックします。

無線 LAN チャネル自動調整の実行結果が表示され、管理対象となった無線 LAN アクセスポイントの無線 LAN チャネルが自動的に調整されます。



▲ 無線LAN チャネルの自動調整を開始したあとにキャンセルした場合、現在処理中の無線LAN アクセスポイントの無線LAN チャネルの調整が完了するまでバックグラウンドで処理を行います。この間、無線LAN 管理機能のほかの操 作はできません。



● 参照 画面の実行結果については、コマンドリファレンス - 運用管理編 - 「nodemanagerct wlan autochannel」を参照し てください。

索引

Α

.266, 291
151
238
238

	١	
-	c	
	,	
	-	

В			

BSR	(ブー	・トスト	、ラップ	ルータ)	 ō

С

6

C ΤΛC #ビフ インタフェフ	
L-TAG リーヒスインタフェース	

C-TAG サービスインタフェ	ニース
(IEEE802 1ad 機能)	358

D

Е

I

C-TAG サービスインタフ	⁷ エース
(IEEE802.1ad 機能)	

C-TAG サービスインタフ	^ノ ェース
(IEEE802.1ad 機能)	

DHCP スヌープ機能108

DNS サーバの自動切り替え機能(逆引き)......333 DNS サーバの自動切り替え機能(順引き)……331

ether L3 監視機能159

Ο

MAC アドレス認証機能143 MAC アドレスフィルタ配布 405 MAC フィルタリング機能27

LAN のネットワーク間接続169

L

Μ

OSPFv2 でネットワークを構築	. 215
OSPF 機能(IPv6)	. 245
OSPF 経路の制御	. 235

OSPF 機能	(IPv6)	 	 	245
OSPF 経路の	D制御 .	 	 	235

OSPF 機能(IPv6)	. 245
OSPF 経路の制御	. 235

PIM-DM	 	 253
PIM-SM		256

QoS 機能60

RIP 経路の制御185 RIP 経路の制御 (IPv6)200 RIP マルチパス機能184 RP(ランデブーポイント)......256

SNTP170 SPT(最短経路)......256

S-TAG サービスインタフェース

PIM-DM	
PIM-SM	
DroverDNC	221

	252
	. 200
DIMENA	250
PIIVI-5IVI	. 200
	~~ .

PIM-DM	
PIM-SM	

	0.50
PIM-DM	
PIM-SM	

PIM-DM	
PIM-SM	
ProvuDNS	331

Р

Q

R

S

PIM-DM	253
PIM-SM	256

411

IEEE802.1ad 機能	354
IEEE802.1ah 機能	
IEEE802.1X 認証機能	115
IGMP スヌープ機能	111
IGMP パケット	111
IPv6 ネットワークの追加	177
IPv6 フィルタリング	273
IP アドレス	185, 266
IP アドレスの自動割り当て	
IP フィルタリング機能	
IP フィルタリングの条件	
IP フィルタリングの設計方針	

Т

TIME プロトコル	170
TOS 值	

U

URL フィルタ機能	

V

VLAN 機能	 9
VRRP 機能	

W

Web 認証機能	 22

あ

アクセスポイントモニタリング	401
あて先情報	
アドレスマスク	
アプリケーションフィルタ機能	

え

エリア ID	215
エリア境界ルータ	235

か

簡易ホッ	トスタンハ	(イ榜	戦能.	 294,	295
				- /	

き

満引き!	333

<

クライアントモニタリング	403
クラスタリング機能	
グループ ID	

こ

し

システムログ	347
システムログの確認	349
準スタブエリア	228
順引き	331

す

スイッチング HUB	9
スケジュール機能	350
スタティック MAC フォワーディング機能	57
スタティックルーティング	261
スタブエリア	228

せ

制御	265
セキュリティ	265
接続端末数制限機能	149

そ

送信元情報		66,	291
ソースポー	۲		157

た

ターゲット・ポート	157
タグ VLAN 機能	

τ

電波出力自動調整	

と

動画 · 音声	253
ドメイン	331

は

バックアップポート機能	
バックアップルータ	
バックボーンエリア	

ßı

フィルタリング条件(ルーティング)	185
フィルタリングの設計方針(ルーティング).	186
負荷分散通信	312
プロトコル	6, 291
プロトコル VLAN 機能	14

ほ

方向	185, 200
ポート VLAN 機能	9
ポート閉塞機能	166
ポートベースサービスインタフェース	
(IEEE802.1ad 機能)	

ポートベースサービスインタフェース	
(IEEE802.1ah 機能)	
ポート・ミラーリング機能	
ホストデータベース	
ホストデータベース情報	
ポリシーベースネットワーク	

ま

マスタルータ	
マニュアル構成	8
マルチキャスト機能	
マルチキャストパケット	111, 256

チキャスト機能
チキャストパケット

マスタルータ		.294
マニュアル構成		
マルチキャスト機能		.25
フルチキャフトパケット	111	25

能	
ルの自動調整	

ራ

む

無線 LAN 管理機能	
無線 LAN チャネルの自動調整	

無線 LAN チャネルの自動調整	409

無線 LAN チャネルの自動調整	

無線 LAN	チャネルの自動調整	409

無線 LAN チャネルの自動調整	40

無線 LAN チャネルの自動調整	409

無線 LAN チャネルの自動調整	40

無線 LAN チャネルの自動調整	40

無線 LAN チャネルの自動調整	40
_	

無線 LAN チャネルの自動調整	40

11		
<i></i>		

ゎ			
0			

/		

メトリック値

ゆ

Х	トリ	ック	値	 	• • •	 	 	 	 	 	185,	200	I

優先順位	
優先制御情報書き換え機能	63
優先制御機能	60
ユニキャスト	253

b

リモート認証	133
リンクアグリゲーション機能	17

る

ループ検出機能	
7	

ろ

ローカル認証	 122

SR-Sシリーズ セキュアスイッチ Web 設定事例集

P3NK-3852-06Z0

発行日	2013年1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。