

SR-S シリーズ セキュアスイッチ

Webリファレンス 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

2010 年 11 月第 4 版

2011 年 6 月第 5 版

2012 年 7 月第 6 版

2012 年 9 月第 7 版

2013 年 1 月第 8 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

はじめに	2
本書の使いかた	8
本書の読者と前提知識	8
本書における商標の表記について	9
本装置のマニュアルの構成	10
1 「設定メニュー」を表示する	11
2 「設定メニュー」の画面体系	12
2.1 基本設定	12
2.2 詳細設定	13
2.3 無線 LAN 管理設定	19
3 パスワード情報	20
3.1 基本情報	20
3.2 ログインパスワード情報	21
3.3 ログインユーザ情報	22
4 装置情報	23
4.1 装置名称情報	23
4.2 タイムサーバ情報	24
4.3 システムログ情報	25
4.4 異常時動作情報	26
4.5 IPv4 ループバック情報	27
4.6 IPv6 ループバック情報	28
4.7 サーバ機能情報	29
4.7.1 アプリケーションフィルタ情報	30
4.8 POE 情報	33
4.9 資源情報	33
4.10 ダンプスイッチ情報	34
4.11 外部メディアスタート機能情報	34
4.12 ハッシュ情報	35
4.13 冷却ファン情報	36
5 スケジュール情報	37
5.1 構成定義切り替え予約情報	37
6 ether 情報	38
6.1 基本情報	40
6.2 ポート種別情報	45
6.2.1 ポート種別情報（初期表示または通常選択時）	45
6.2.2 ポート種別情報（リンクアグリゲーション選択時）	45
6.2.3 ポート種別情報（バックアップ選択時）	46
6.2.4 ポート種別情報（ミラー選択時）	47
6.3 MAC 関連	48
6.3.1 ストーム制御情報	48
6.3.2 接続端末数制限情報	49
6.4 STP 関連	50
6.4.1 基本情報	50
6.4.2 MSTP インスタンス情報	51
6.5 LLDP 関連	52
6.6 認証共通情報	54
6.7 IEEE802.1X 認証情報	55
6.7.1 IEEE802.1X 認証情報（初期表示または使用しない選択時）	55
6.7.2 IEEE802.1X 認証情報（使用する選択時）	56

6.8	Web 認証関連	59
6.8.1	基本情報	59
6.8.2	認証不要端末情報	61
6.9	MAC アドレス認証関連	62
6.9.1	基本情報	62
6.9.2	認証不要端末情報	64
6.10	DHCP スヌープ情報	65
6.11	フィルタ情報	66
6.12	QoS 関連	71
6.12.1	基本情報	71
6.12.2	QoS 情報	72
6.13	接続先監視情報	77
6.14	トラップ情報	78
6.15	L2 暗号関連	79
6.15.1	基本情報	79
6.15.2	暗号化条件	81
6.16	IEEE802.1ad 関連	83
6.16.1	基本情報	83
6.16.2	VLAN タグマッピングルール情報	84
6.17	IEEE802.1ah 関連	86
6.17.1	基本情報	86
6.17.2	カスタマーバックボーンサービス情報	88
6.17.3	プロバイダーバックボーンサービス情報	90
7	リンクアグリゲーショングループ情報	92
7.1	基本情報	93
7.2	接続先監視情報	96
7.3	IEEE802.1ad 関連	97
7.3.1	基本情報	97
7.3.2	VLAN タグマッピングルール情報	98
7.4	IEEE802.1ah 関連	100
7.4.1	基本情報	100
7.4.2	カスタマーバックボーンサービス情報	102
7.4.3	プロバイダーバックボーンサービス情報	103
8	バックアップグループ情報	105
9	etherblock 情報	107
9.1	フィルタ情報	107
9.2	QoS 情報	111
10	LACP 情報	115
10.1	基本情報	115
11	VLAN 情報	116
11.1	基本情報	117
11.1.1	基本情報（初期表示または指定しない選択時）	117
11.1.2	基本情報（システム定義プロトコルから指定選択時）	118
11.1.3	基本情報（プロトコルをユーザ定義指定選択時）	119
11.2	静的 MAC 学習テーブル情報	120
11.3	DHCP スヌープ情報	120
11.4	IGMP スヌープ情報	121
11.5	フィルタ情報	122
11.6	IPv6 フィルタ情報	127
11.7	QoS 情報	132
11.8	IPv6 QoS 情報	137
11.9	ARP 認証関連	142

	11.9.1	ARP 認証情報	142
	11.9.2	認証不要端末情報	144
12		MAC 情報	145
	12.1	基本情報	145
	12.2	ストーム制御情報	146
	12.3	MAC テーブルフラッシュ情報	147
13		LAN 情報	148
	13.1	共 thông 情報	149
	13.1.1	基本情報	149
	13.1.2	VRRP グループ情報	150
	13.2	IP 関連	155
	13.2.1	IP アドレス情報	155
	13.2.2	RIP 情報	156
	13.2.3	OSPF 情報	157
	13.2.4	スタティック経路情報	159
	13.2.5	IP フィルタリング情報	161
	13.2.6	RIP フィルタリング情報	166
	13.2.7	DSCP 値書き換え情報	168
	13.2.8	DHCP 情報	173
	13.2.9	マルチキャスト情報	175
	13.2.10	ARP 情報	176
	13.2.11	スタティック ARP 情報	176
	13.3	IPv6 関連	177
	13.3.1	IPv6 基本情報	177
	13.3.2	IPv6 RIP 情報	181
	13.3.3	IPv6 OSPF 情報	182
	13.3.4	IPv6 スタティック経路情報	184
	13.3.5	IPv6 DHCP 情報	185
	13.3.6	IPv6 フィルタリング情報	189
	13.3.7	IPv6 RIP フィルタリング情報	194
	13.3.8	IPv6 DSCP 値書き換え情報	196
14		IP 情報	199
	14.1	基本情報	199
15		IPv6 情報	200
	15.1	基本情報	200
	15.2	ホスト情報	200
16		ルーティングプロトコル情報	201
	16.1	ルーティングマネージャ情報	201
	16.1.1	再配布情報	201
	16.1.2	優先度情報	203
	16.1.3	ECMP 情報	204
	16.2	RIP 関連	205
	16.2.1	RIP タイマ情報	205
	16.2.2	RIP マルチバス情報	206
	16.2.3	RIP 再配布フィルタリング情報	206
	16.2.4	RIP ユニキャスト送信情報	208
	16.2.5	RIP 相手フィルタリング情報	209
	16.3	OSPF 関連	210
	16.3.1	ルータ ID 情報	210
	16.3.2	OSPF エリア情報	211
	16.3.3	AS 境界ルータ情報	217
	16.3.4	AS 外部経路集約情報	217
	16.3.5	OSPF 再配布フィルタリング情報	218

16.4	IPv6 ルーティングマネージャ情報	220
16.4.1	IPv6 再配布情報	220
16.4.2	IPv6 優先度情報	222
16.5	IPv6 RIP 関連	223
16.5.1	IPv6 RIP タイマ情報	223
16.5.2	IPv6 RIP マルチパス情報	224
16.5.3	IPv6 RIP 再配布フィルタリング情報	224
16.6	IPv6 OSPF 関連	226
16.6.1	IPv6 ルータ ID 情報	226
16.6.2	IPv6 OSPF エリア情報	227
16.6.3	IPv6 AS 境界ルータ情報	230
16.6.4	IPv6 OSPF 再配布フィルタリング情報	231
17	マルチキャスト情報	233
17.1	IP マルチキャスト情報	233
17.2	IP マルチキャストスタティック RP 情報	235
17.3	IP マルチキャストスタティック経路情報	236
18	QoS 情報	237
18.1	送信アルゴリズム情報	237
18.2	COS キュー情報	238
19	STP 情報	239
19.1	基本情報	239
19.1.1	基本情報（初期表示または使用する選択時）	239
19.1.2	基本情報（使用しない選択時）	241
19.2	MSTP インスタンス情報	242
19.3	IEEE802.1ad 情報	243
20	LLDP 情報	244
20.1	基本情報	244
21	認証情報	246
21.1	IEEE802.1X 認証情報	246
21.2	Web 認証情報	247
21.3	MAC アドレス認証情報	248
22	IGMP スヌープ情報	249
22.1	基本情報	249
23	ループ検出情報	250
23.1	基本情報	250
24	AAA 情報	251
24.1	グループ ID 情報	251
24.1.1	共通情報	252
24.1.2	AAA ユーザ情報	253
24.1.3	RADIUS 関連	257
25	ACL 情報	263
25.1	ACL 定義情報	264
25.1.1	基本定義情報	264
25.1.2	IP 定義情報	265
25.1.3	TCP 定義情報	266
25.1.4	UDP 定義情報	266
25.1.5	ICMP 定義情報	267
25.1.6	IPv6 定義情報	267
25.1.7	VLAN 定義情報	268
25.1.8	MAC 定義情報	269

26	SNMP 情報	270
26.1	基本情報	270
26.2	SNMPv1/v2c 情報	272
26.3	SNMPv3 情報	274
26.3.1	ユーザ情報	274
26.3.2	MIB ビュー情報	277
26.4	トラップ情報	278
27	IEEE802.1ad 情報	279
27.1	基本情報	279
27.2	VLAN タグマッピングルール情報	280
28	IEEE802.1ah 情報	281
28.1	基本情報	281
28.2	バックボーンサービス関連	282
28.2.1	共通情報	282
28.2.2	バックボーン MAC アドレス情報	283
29	ProxyDNS 情報／URL フィルタ情報	284
29.1	順引き情報	285
29.2	逆引き情報	287
30	ホストデータベース情報	288
31	無線 LAN 管理情報	290
31.1	管理グループ情報	290
31.2	管理機器情報	291
31.2.1	基本情報	292
31.3	管理外機器情報	293
32	MAC アドレスフィルタセット情報	294
32.1	MAC アドレスフィルタ情報	294
32.1.1	MAC アドレスフィルタ情報（一括設定）	295
32.1.2	MAC アドレスフィルタ情報（個別設定）	296
33	無線 LAN 管理パラメタ情報	297
33.1	無線 LAN 管理パラメタ	297

索引	300
-----------------	------------

本書の使いかた

本書では、本装置の設定メニューで表示される画面について説明しています。

また、CD-ROM 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。



警告 製造物責任法（PL）関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。



注意 製造物責任法（PL）関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。

本書における商標の表記について

Microsoft、MS-DOS、Windows、Windows NT、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	
Microsoft® Windows Vista® Home Basic operating system	
Microsoft® Windows Vista® Enterprise operating system	
Microsoft® Windows® 7 64bit Home Premium	Windows 7
Microsoft® Windows® 7 32bit Professional	

本装置のマニュアルの構成

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

マニュアル名称	内容
ご利用にあたって	本装置の設置方法やソフトウェアのインストール方法を説明しています。
機能説明書	本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	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 (本書)	Web 画面の項目の詳細な情報を説明しています。

1 「設定メニュー」を表示する

「設定」タブをクリックしたときに表示される「設定メニュー」について説明します。
ここでは、SR-S724TC1 の場合を例に説明します。

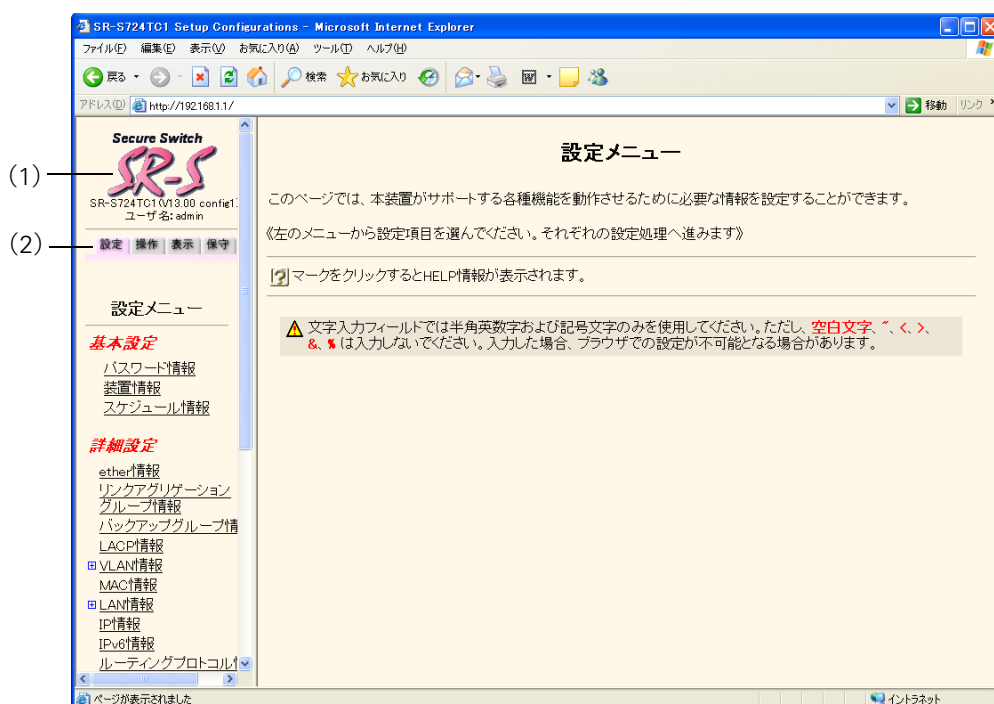
こんな事に気をつけて

「設定メニュー」を表示するときは、管理者 (admin) でログインしてください。

参照 Web ユーザーズガイド「1.3 本装置にログインする」(P.11)



WWWブラウザのタイトルバーには、初期状態で機種名が表示されます。
「装置情報」 - 「装置名称情報」の装置名称を設定することで表示内容を変更できます。



画面左側に表示されるタブについて、以下に説明します。

- (1) 本装置ロゴ : クリックすると、トップページが表示されます。
- (2) 「設定」タブ : クリックすると、設定メニューが表示されます。



「操作」タブ、「表示」タブおよび「保守」タブについて

Web ユーザーズガイド「2.1 操作メニューを使う」(P.23)、「2.2 表示メニューを使う」(P.36)、「2.3 保守メニューを使う」(P.40)

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)

2 「設定メニュー」の画面体系

[設定] タブをクリックして表示される設定用メニューの画面項目と体系について示します。

2.1 基本設定

パスワード情報	基本情報		
	ログインパスワード情報		
	ログインユーザ情報		
装置情報	装置名称情報		
	タイムサーバ情報		
	システムログ情報		
	異常時動作情報		
	IPv4 ループバック情報		
	IPv6 ループバック情報		
	サーバ機能情報	アプリケーションフィルタ情報	アプリケーションフィルタ情報 (条件にあてはまらない場合の動作)
	POE 情報		
	資源情報		
	ダンプスイッチ情報		
	外部メディアスタート機能情報		
	ハッシュ情報		
	冷却ファン情報		
スケジュール情報	構成定義切り替え予約情報		

2.2 詳細設定

ether 情報	基本情報	
	ポート種別情報	ポート種別情報（初期表示または通常選択時）
		ポート種別情報（リンクアグリゲーション選択時）
		ポート種別情報（バックアップ選択時）
		ポート種別情報（ミラー選択時）
	MAC 関連	ストーム制御情報
		接続端末数制限情報
	STP 関連	基本情報
		MSTP インスタンス情報
	LLDP 関連	
	認証共通情報	
	IEEE802.1X 認証情報	IEEE802.1X 認証情報（初期表示または使用しない選択時）
		IEEE802.1X 認証情報（使用する選択時）
	Web 認証関連	基本情報
		認証不要端末情報
	MAC アドレス認証関連	基本情報
		認証不要端末情報
	DHCP スヌープ情報	
	フィルタ情報	
	QoS 関連	基本情報
		QoS 情報
	接続先監視情報	
	トラップ情報	
	L2 暗号関連	基本情報
		暗号化条件

ether 情報	IEEE802.1ad 関連	基本情報	基本情報（初期表示またはプロバイダーポート選択時）
			基本情報（カスタマーポート選択時）
		VLAN タグマッピングルール 情報	
	IEEE802.1ah 関連	基本情報	基本情報（初期表示またはプロバイダーポート選択時）
			基本情報（カスタマーポート選択時）
		カスタマーバックボーンサービス情報	
	プロバイダーバックボーンサービス情報		
リンクアグリゲーショングループ情報	基本情報		
	接続先監視情報		
	IEEE802.1ad 関連	基本情報	基本情報（初期表示およびプロバイダーポート選択時）
			基本情報（カスタマーポート選択時）
		VLAN タグマッピングルール 情報	
	IEEE802.1ah 関連	基本情報	基本情報（初期表示およびプロバイダーポート選択時）
			基本情報（カスタマーポート選択時）
		カスタマーバックボーンサービス情報	
		プロバイダーバックボーンサービス情報	
	バックアップグループ情報		
etherblock 情報	フィルタ情報		
	QoS 情報		
LACP 情報	基本情報		
VLAN 情報	基本情報	基本情報（初期表示または指定しない選択時）	
		基本情報（システム定義プロトコルから指定選択時）	
		基本情報（プロトコルをユーザ定義指定選択時）	

VLAN 情報	静的 MAC 学習テーブル情報		
	DHCP スヌープ情報		
	IGMP スヌープ情報		
	フィルタ情報		
	IPv6 フィルタ情報		
	QoS 情報		
	IPv6 QoS 情報		
	ARP 認証関連	ARP 認証情報	ARP 認証情報（初期表示または使用しない選択時）
			ARP 認証情報（使用する選択時）
		認証不要端末情報	
MAC 情報	基本情報		
	ストーム制御情報		
	MAC テーブルフラッシュ情報		
LAN 情報	共通情報	基本情報	
		VRRP グループ情報	基本情報
			VRRP トリガ情報
	IP 関連	IP アドレス情報	
		RIP 情報	
		OSPF 情報	
		スタティック経路情報	
		IP フィルタリング情報	
		RIP フィルタリング情報	
		DSCP 値書き換え情報	
		DHCP 情報	
		マルチキャスト情報	
		ARP 情報	
		スタティック ARP 情報	

LAN 情報	IPv6 関連	IPv6 基本情報	
		IPv6 RIP 情報	
		IPv6 OSPF 情報	
		IPv6 スタティック経路情報	
		IPv6 DHCP 情報	IPv6 DHCP 情報（初期表示 または使用しない選択時）
			IPv6 DHCP 情報（リレー エージェント機能を使用す る選択時）
			IPv6 DHCP 情報（サーバ機 能を使用する選択時）
		IPv6 フィルタリング情報	
		IPv6 RIP フィルタリング情報	
		IPv6 DSCP 値書き換え情報	
IP 情報	基本情報		
IPv6 情報	基本情報		
	ホスト情報		
ルーティングプロト コル情報	ルーティングマネージャ情 報	再配布情報	
		優先度情報	
		ECMP 情報	
	RIP 関連	RIP タイマ情報	
		RIP マルチバス情報	
		RIP 再配布フィルタリング 情報	
		RIP ユニキャスト送信情報	
		RIP 相手フィルタリング情報	
	OSPF 関連	ルータ ID 情報	
		OSPF エリア情報	OSPF エリア基本情報
			経路集約情報
			サマリ LSA 入出力可否情報
			バーチャルリンク情報

ルーティングプロトコル情報	OSPF 関連	AS 境界ルータ情報		
		AS 外部経路集約情報		
		OSPF 再配布フィルタリング情報		
	IPv6 ルーティングマネージャ情報	IPv6 再配布情報		
		IPv6 優先度情報		
	IPv6 RIP 関連	IPv6 RIP タイマ情報		
		IPv6 RIP マルチバス情報		
		IPv6 RIP 再配布フィルタリング情報		
	IPv6 OSPF 関連	IPv6 ルータ ID 情報		
		IPv6 OSPF エリア情報	IPv6 OSPF エリア基本情報	IPv6 経路集約情報
				IPv6 エリア間ブリフィックス LSA 入出力可否情報
		IPv6 AS 境界ルータ情報		
		IPv6 OSPF 再配布フィルタリング情報		
マルチキャスト情報	IP マルチキャスト情報			
	IP マルチキャストステティック RP 情報			
	IP マルチキャストステティック経路情報			
QoS 情報	送信アルゴリズム情報			
	COS キュー情報			
STP 情報	基本情報	基本情報（使用しない選択時）		
		基本情報（初期表示または使用する選択時）		
	MSTP インスタンス情報			
	IEEE802.1ad 情報			
LLDP 情報	基本情報			

IEEE802.1ah 情報	基本情報	
	バックボーンサービス関連	共通情報
		バックボーンMAC アドレス 情報
ProxyDNS 情報／ URL フィルタ情報	順引き情報	
	逆引き情報	
ホストデータベース 情報		

2.3 無線 LAN 管理設定

無線 LAN 管理情報	管理グループ情報	
	管理機器情報	基本情報
	管理外機器情報	
MAC アドレスフィルタ セット情報	MAC アドレスフィルタ情報	MAC アドレスフィルタ情報 (一括設定)
		MAC アドレスフィルタ情報 (個別設定)
無線 LAN 管理パラメタ情 報	無線 LAN 管理パラメタ	

3 パスワード情報

適用機種 全機種

[操作] 「設定メニュー」→基本設定「パスワード情報」

パスワード情報		
基本情報	ログインパスワード情報	ログインユーザ情報
このページでは、パスワードに関する情報についての設定ができます。		

3.1 基本情報

[操作] 「設定メニュー」→基本設定「パスワード情報」→[基本情報]

■基本情報 

暗号化パスワード形式 ☐ 装置固有パスワード形式にする

※装置固有パスワード形式にする設定を更新するとそれ以降、暗号化パスワード形式の修正はできません。

設定終了後、更新をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

暗号化パスワード形式

本装置に設定する各種パスワード文字列は暗号化されて保存されます。

装置固有パスワード形式にしない場合は、保存した構成定義情報は他装置に復元することができます。

装置固有パスワード形式にした場合は、保存した構成定義情報は自装置にのみ復元することができ、他装置に復元することができなくなります。装置固有パスワード形式にすることで、セキュリティを強化することができます。

なお、暗号化パスワード形式の設定は更新直後から有効になります。

こんな事に気をつけて

- “装置固有パスワード形式にする”を選択し更新すると、それ以降、暗号化パスワード形式の修正はできません。
- 装置固有パスワード形式を使用した構成定義は、他装置に復元できません。

3.2 ログインパスワード情報

[操作] 「設定メニュー」→基本設定「パスワード情報」→[ログインパスワード情報]

この装置にログインするためのパスワードを設定します。
管理者パスワードはユーザ名がadminの場合に使用するパスワード、一般ユーザパスワードはユーザ名がuserの場合に使用するパスワードです。

ログイン時のユーザによって権限クラスが決定され、権限クラスにより実行できる画面が異なります。adminでログインすると管理者クラス、userでログインすると一般ユーザクラスになります。

なお、コンソール、TELNET および SSH によるログイン時にもこの管理者パスワード および 一般ユーザパスワードを使用します。

また、FTP および SFTPによるログイン時には管理者パスワードを使用します。

■ログインパスワード情報



管理者パスワード	
管理者パスワードの確認	
一般ユーザパスワード	
一般ユーザパスワードの確認	

設定終了後、更新をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

本装置を操作するときのパスワードを設定します。

ログイン時のユーザによって権限クラスが決定され、権限クラスにより実行できる画面が異なります。パスワード入力によって操作できる時間は10分間です。それ以降の操作では再びパスワード入力して処理を行ってください。

なお、パスワードの設定は更新直後から有効になります。

管理者パスワード

ログインユーザ名がadminの場合に、8～64文字でパスワードを指定します。adminでログインすると権限クラスが管理者クラスになります。

こんな事に気をつけて

7文字以下、英字だけ、数字だけのパスワードを設定した場合、および、管理者パスワードの設定を削除した場合は、設定および削除は行われますが、脆弱である旨の警告メッセージが表示されます。

一般ユーザパスワード

ログインユーザ名がuserの場合に、8～64文字でパスワードを指定します。userでログインすると権限クラスが一般ユーザクラスになります。

こんな事に気をつけて

7文字以下、英字だけ、数字だけのパスワードを設定した場合、および、管理者パスワードの設定を削除した場合は、設定および削除は行われますが、脆弱である旨の警告メッセージが表示されます。

管理者パスワードの確認

上記で指定した管理者パスワードをもう一度指定します。

一般ユーザパスワードの確認

上記で指定した一般ユーザパスワードをもう一度指定します。

3.3 ログインユーザ情報

[操作] 「設定メニュー」→基本設定「パスワード情報」→[ログインユーザ情報]

この装置にログインする場合のユーザ認証で参照するAAA情報を設定できます。
 ユーザ名、パスワード、および権限クラスをAAAグループまたはRADIUSサーバに設定することができます。
 権限クラスにより実行できる画面が異なります。
 ログインユーザ情報によるユーザ認証を行うには、ログインパスワード情報の管理者パスワードが設定されている必要があります。
 なお、コンソール、TELNET、FTP および SSH によるログイン時にもログインユーザ情報を参照してユーザ認証を行います。

■ログインユーザ情報 

参照するAAA情報	☒ 参照しない
	☐ 参照する
	AAAグループID 認証プロトコル ☒ CHAP ☐ PAP

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

本装置にログインするときのユーザ認証で参照する AAA 情報を設定します。

ユーザ名、パスワードおよび権限クラスを AAA グループまたは RADIUS サーバに設定することができます。ログイン時のユーザによって権限クラスが決定され、権限クラスにより実行できる画面が異なります。パスワード入力によって操作できる時間は 10 分間です。それ以降の操作では再びパスワード入力して処理を行ってください。

なお、ログインユーザ情報によるユーザ認証を行うには、ログインパスワード情報の管理者パスワードが設定されている必要があります。

参照する AAA 情報

ユーザ認証で AAA 情報を参照する場合は、“参照する” を選択します。

AAA グループ ID

ユーザ認証を行う場合に参照する AAA のグループ ID を指定します。AAA のグループ ID を、0～9 の範囲の 10 進数で指定します。

認証プロトコル

ユーザ情報を RADIUS サーバに設定してユーザ認証を行う場合に使用する認証プロトコルを指定します。

4 装置情報

適用機種 全機種

[操作] 「設定メニュー」→基本設定「装置情報」

装置情報		
装置名称情報	タイムサーバ情報	システムログ情報
異常時動作情報	IPv4 ループバック情報	IPv6 ループバック情報
サーバ機能情報	資源情報	ダンプスイッチ情報
外部メディアスタート機能情報	ハッシュ情報	

装置固有の機能についての設定ができます。

SR-S308TL1、310TL2、316TL1、318TL2、324TL2、716C2、724TC1、748TC1 のみ、「ハッシュ情報」が表示されます。

SR-S716C2、724TC1、748TC1 のみ、「IPv4 ループバック情報」が表示されます。

SR-S724TC1、748TC1 のみ、「IPv6 ループバック情報」が表示されます。

SR-S224PS1 のみ、「POE 情報」が表示されます。

SR-S308TL1、310TL2、316TL1、318TL2、324TL2、324TC1、328TR1、348TC1、724TC1、748TC1 のみ、「資源情報」が表示されます。

SR-S308TL1、310TL2、316TL1、318TL2、324TL2 のみ、「冷却ファン情報」が表示されます。

4.1 装置名称情報

[操作] 「設定メニュー」→基本設定「装置情報」→「装置名称情報」

■装置名称情報

?

装置名称

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

装置名称

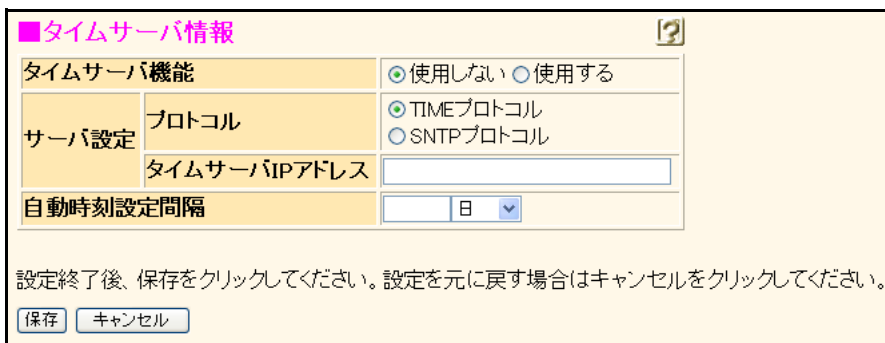
本装置の任意な名称を 32 文字以内で指定します。

こんな事に気をつけて

「SNMP 情報」の機器名称で“装置名称を使用する”を選択した場合、この名称が SNMP の機器名称として使用されます。

4.2 タイムサーバ情報

[操作] 「設定メニュー」→基本設定「装置情報」→[タイムサーバ情報]



タイムサーバ機能

ネットワーク上のタイムサーバから時刻情報を取得することによって、内部時刻を自動的に設定する場合は、“使用する”を選択します。

自動時刻設定間隔

タイムサーバから定期的に時刻情報を取得するときの取得周期を0～10日の範囲で指定します。省略または0を設定すると、起動（再起動）時だけ時刻情報を取得します。

サーバ設定

使用するタイムサーバを指定します。プロトコルを選択して、タイムサーバIPアドレスを指定します。

プロトコル

タイムサーバから時刻情報を取得するときのプロトコルを選択します。

TIME プロトコル

TIME プロトコル（TCP）を使用する場合に指定します。

SNTP プロトコル

簡易 NTP プロトコル（UDP）を使用する場合に指定します。

タイムサーバIPアドレス

タイムサーバのIPv4 アドレスまたはIPv6 アドレスを指定します。0.0.0.0を指定した場合、タイムサーバ機能を使用しないものとして動作します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0::～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

4.3 システムログ情報

[操作] 「設定メニュー」→基本設定「装置情報」→[システムログ情報]

■システムログ情報

?

システムログ送信	サーバ1	☒ 送信しない ☐ 送信する 送信先ホスト
	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
重複メッセージの出力		☒ する ☐ しない
コマンド履歴の出力		☐ する ☒ しない
対象イベント	IEEE802.1X認証	☒ 認証成功 ☒ 再認証成功 ☒ 認証失敗 ☒ 認証解除
	Web認証	☒ 認証成功 ☒ 認証失敗 ☒ 認証解除
	MACアドレス認証	☒ 認証成功 ☒ 再認証成功 ☒ 認証失敗 ☒ 認証解除
	ARP認証	☒ 認証成功 ☒ 認証失敗 ☒ 再認証失敗

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

接続切断、トラブルなどのさまざまな情報のシステムログをネットワーク上のsyslogサーバに対して送信することができます。その場合のファシリティ、プライオリティは以下のとおりです。

ファシリティ : local7 (23)

プライオリティ : error、warn、info、notice (※1)

※1) noticeはセキュリティログを使用する場合だけ出力されます。

 **参照** プライオリティ、ファシリティの設定は、「[コマンドリファレンス - 構成定義編 -](#)」のsyslog priおよびsyslog facilityを参照してください。

システムログ送信

syslog形式でsyslogサーバにシステムログ情報を送信する場合は、「送信する」を選択します。

送信先のサーバは3台まで登録できます。

サーバ1 / 2 / 3

送信先ホスト

送信先のIPアドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

ヘッダ部の追加

syslog サーバに送信するシステムログ情報にヘッダ部（タイムスタンプおよびホスト名）を追加する場合は、“する”を選択します。

送信元 IP アドレス

ホスト名が未設定の場合に、ヘッダ部に設定する IP アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

セキュリティログ

URL フィルタにより遮断されたパケットのログ情報、DHCP サーバが割り当てた IP アドレスログのログ情報を採取します。

重複メッセージの出力

システムログにメッセージを出力するとき、直前に出力したメッセージと重複した場合に出力する場合は、“する”を選択します。

コマンド履歴の出力

コマンド実行履歴をシステムログに出力する場合は、“する”を選択します。

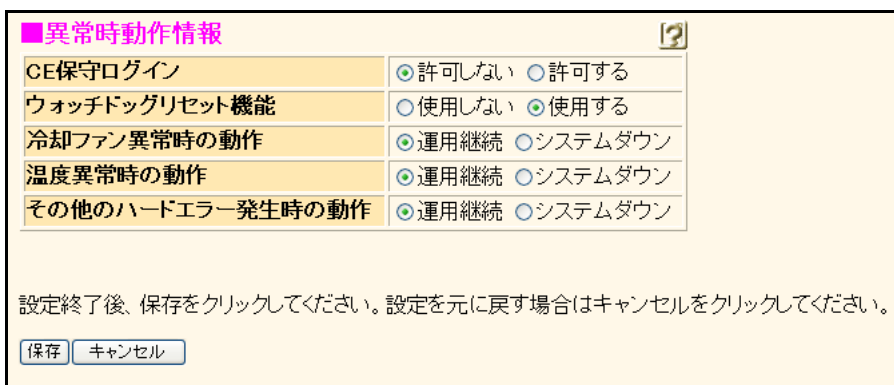
対象イベント

以下の機能ごとに出力対象とするイベントを設定します。

- IEEE802.1X 認証
- Web 認証
- MAC アドレス認証
- ARP 認証

4.4 異常時動作情報

[操作] 「設定メニュー」→基本設定「装置情報」→[異常時動作情報]



■異常時動作情報	
CE保守ログイン	☒ 許可しない ☐ 許可する
ウォッチドッグリセット機能	☐ 使用しない ☒ 使用する
冷却ファン異常時の動作	☒ 運用継続 ☐ システムダウン
温度異常時の動作	☒ 運用継続 ☐ システムダウン
その他のハードエラー発生時の動作	☒ 運用継続 ☐ システムダウン

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

本装置になんらかの異常が発生した場合の動作を設定します。

SR-S208TC2、224TC2、208PD1 では、表示が上記の画面とは異なります。

CE 保守ログイン

CE ログインを許可する場合は、“許可する”を選択します。CE ログインを許可することで、CE の保守作業を円滑に進めることができます。

ウォッチドッグリセット機能

ウォッチドッグリセット機能を使用する場合は、“使用する”を選択します。“使用する”を選択した場合、本装置がハングアップすると 16～48 秒以内にリセットがかかり再起動します。

冷却ファン異常時の動作 (SR-S208TC2、224TC2、208PD1 除く)

冷却ファン異常を検出した場合にシステムダウンを行うか（縮退モードへ遷移）、そのまま運用を継続するかを選択します。

その他のハードエラー発生時の動作 (SR-S208TC2、224TC2、208PD1 除く)

冷却ファン、温度異常および電源異常以外のハードエラーを検出した場合にシステムダウンを行うか（縮退モードへ遷移）、そのまま運用を継続するかを選択します。

温度異常時の動作 (SR-S208TC2、224TC2、208PD1 除く)

温度異常を検出した場合にシステムダウンを行うか（縮退モードへ遷移）、そのまま運用を継続するかを選択します。

4.5 IPv4 ループバック情報

適用機種 SR-S716C2, 724TC1, 748TC1

[操作] 「設定メニュー」→基本設定「装置情報」→[IPv4 ループバック情報]

IP アドレス

ループバックインタフェースに割り当てる追加 IP アドレスを指定します。ループバックインタフェースに割り当てた IP アドレスを通信に使用する場合は、以下の範囲で通信可能なアドレスを指定します。

省略または 0.0.0.0 を設定した場合、ループバックアドレスを使用しないものとします。

有効範囲)

1.0.0.1-126.255.255.254

128.0.0.1-191.255.255.254

192.0.0.1-223.255.255.254

こんな事に気をつけて

- ほかのインタフェースと違うネットワークの IP アドレスを設定してください。
- 127.0.0.1 はループバックインタフェースにすでに設定されています。ループバック情報として 127.0.0.1 を設定する必要はありません。

OSPF 機能

ループバックに割り当てた IP アドレスを OSPF で広報するかどうかを選択します。“使用する”を選択した場合、IP アドレスが設定されているときだけ OSPF で広報します。広報する IP アドレスは、設定した IP アドレスだけです。すでに設定されている IP アドレス 127.0.0.1 は広報しません。

ループバックインタフェースも含めて、OSPF を使用できるインタフェースは、仕様一覧「[2.3 システム最大値一覧](#)」(P.53) を参照してください。

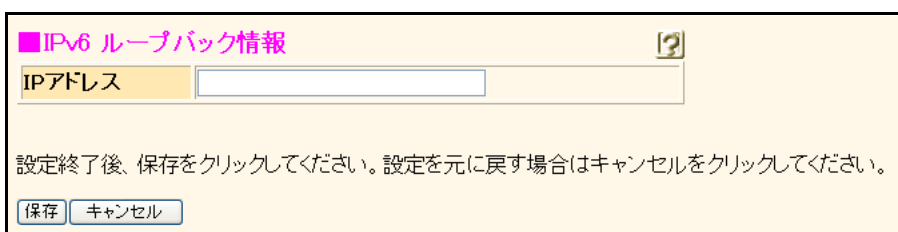
エリア定義番号

広報を行う OSPF エリア情報の定義番号を指定します。指定する定義番号の OSPF エリア情報はあらかじめ設定しておく必要があります。OSPF エリア情報の設定は、「ルーティングプロトコル情報」の「OSPF 関連」にあります。省略時は、0 が設定されます。

4.6 IPv6 ループバック情報

適用機種 SR-S724TC1, 748TC1

[操作] 「設定メニュー」→基本設定「装置情報」→[IPv6 ループバック情報]



■ IPv6 ループバック情報

IP アドレス

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

IP アドレス

ループバックインタフェースに割り当てる追加 IPv6 アドレスを 128 ビットで指定します。本装置ではプレフィックス長は 128 に固定となります。

省略時は、ループバックアドレスを使用しないものとします。

こんな事に気をつけて

- ほかのインタフェースと違うネットワークの IPv6 アドレスを設定してください。
- ::1 はループバックインタフェースにすでに設定されています。ループバック情報として ::1 を設定する必要はありません。
- リンクローカルアドレスは指定できません。

4.7 サーバ機能情報

[操作] 「設定メニュー」→基本設定「装置情報」→[サーバ機能情報]

■サーバ機能情報
 ※機能毎に利用端末を制限したい場合は、アプリケーションフィルタ機能の“設定”より設定してください。

機能名	動作	アプリケーションフィルタ機能
FTPサーバ機能	☒ IPv4 / IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
TELNETサーバ機能	☒ IPv4 / IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
SSHサーバ機能	SSH ☒ IPv4 / IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
	SFTP ☒ IPv4 / IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	
HTTPサーバ機能	☒ IPv4 / IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
DNSサーバ機能	☒ IPv4 / IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
SNTPサーバ機能	☒ IPv4 / IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
TIMEサーバ機能	TCP ☒ IPv4 / IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
	UDP ☒ IPv4 / IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

[保存](#) [キャンセル](#)

本装置の各サーバ機能を有効にするか停止するかを設定します。

機能名

以下の各サーバ機能で、IPv4 と IPv6 の両方の機能を有効にする場合は、動作の“IPv4 / IPv6”を選択します。

IPv4の機能のみ有効にする場合は、“IPv4”を選択します。

IPv6の機能のみ有効にする場合は、“IPv6”を選択します。

すべての機能を停止する場合は、“停止”を選択します。

機能ごとに利用端末を制限したい場合は、アプリケーションフィルタ機能の「設定」ボタンをクリックして設定してください。

- FTPサーバ機能
- TELNETサーバ機能
- SSHサーバ機能（SSH/SFTP）
- HTTPサーバ機能
- DNSサーバ機能
- SNTPサーバ機能
- TIMEサーバ機能（TCP/UDP）

4.7.1 アプリケーションフィルタ情報

[操作] 「設定メニュー」→基本設定「装置情報」→「サーバ機能情報」
→「アプリケーションフィルタ機能」[設定]→「アプリケーションフィルタ情報」

■アプリケーションフィルタ情報(FTP) ACL定義参照

※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。

優先順位	動作	ACL定義番号	操作
条件にあてはまらない場合の動作	透過		修正 初期化
全削除			
<アプリケーションフィルタ情報入力フィールド>			
動作	☒ 透過 ☐ 遮断		
ACL定義番号	参照		
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、このアプリケーションに設定されているアプリケーションフィルタ定義が表示されています。処理は優先順位1から順に行われます。アプリケーションフィルタの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53)を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件に一致した場合に定義された動作を行います。「条件にあてはまらない場合の動作」の「初期化」ボタンをクリックすると、初期状態（透過）が設定されます。

こんな事に気をつけて

WWWに対するアクセスを制限する設定を行った場合、本装置に対しWWWブラウザからアクセスできなくなる場合があります。

動作

アプリケーションフィルタの動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- IPv6 定義

指定する定義番号欄の「選択」ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

- [操作] 「設定メニュー」→基本設定「装置情報」→[サーバ機能情報]
 →「アプリケーションフィルタ機能」[設定]→[アプリケーションフィルタ情報]
 →「ACL 定義番号の [参照]」

表示条件入力			
表示個数		表示範囲	
10		0~0	
■ACL 情報 閉じる			
定義番号	IP定義	IPv6定義	選択
	プロトコル 送信元IPアドレス/マスク あて先IPアドレス/マスク QoS種別 QoS値	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 QoS種別 QoS値	
0	すべて	すべて	選択
	192.168.1.0/24	2001:db8:1111:1000::/64	
	any	any	
	any	any	
閉じる			

「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」および「IPv6 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「アプリケーションフィルタ情報」のに設定する定義番号欄の[選択] ボタンをクリックすると、「アプリケーションフィルタ情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

4.7.1.1 アプリケーションフィルタ情報（条件にあてはまらない場合の動作）

[操作] 「設定メニュー」→基本設定「装置情報」→「サーバ機能情報」
 →「アプリケーションフィルタ機能」[設定] →「アプリケーションフィルタ情報」
 →「条件にあてはまらない場合の動作」[修正]

「条件にあてはまらない場合の動作」は、このアプリケーションに設定されているアプリケーションフィルタ定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。

こんな事に気をつけて

WWWに対するアクセスを制限する設定を行った場合、本装置に対しWWWブラウザからアクセスできなくなる場合があります。

動作

アプリケーションフィルタのどれにも一致しない場合の動作を以下の2つから選択します。

- 透過
アプリケーションフィルタ定義のどれにも一致しない場合にパケットを透過します。
- 遮断
アプリケーションフィルタ定義のどれにも一致しない場合にパケットを遮断します。

4.8 POE 情報

適用機種 SR-S224PS1

[操作] 「設定メニュー」→基本設定「装置情報」→[POE 情報]

■POE情報

POE対応機器の検出方法

☒ 抵抗検出
 ☐ 抵抗およびコンデンサ検出

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

POE 対応機器の検出方法

POE 対応機器の検出方法を選択します。

こんな事に気をつけて

本設定を変更してもすでに給電中のポートに対して再検出は行いません。再検出が必要な場合は、ケーブルを再接続するか、「ether 情報」の「基本情報」でポート給電の設定を変更し、給電を一度停止させてください。
レガシータイプの PD（受電装置）を接続する場合は、「抵抗およびコンデンサ検出」に設定してください。

4.9 資源情報

適用機種 SR-S308TL1, 310TL2, 316TL1, 318TL2, 324TL2, 324TC1, 328TR1, 348TC1, 724TC1, 748TC1

[操作] 「設定メニュー」→基本設定「装置情報」→[資源情報]

■資源情報

フィルタ/QoS資源の配分

機能

☒ すべて
 ☐ フィルタのみ
 ☐ QoSのみ

プロトコル

☒ すべて
 ☐ IPv4のみ
 ☐ IPv6のみ

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

フィルタ/QoS 資源の配分

フィルタおよび QoS 用のハードウェア資源を使用する機能およびプロトコルを選択します。

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。使用する機能を選択してください。

- ・ フィルタ情報／IP フィルタ情報（IPv4）
- ・ IPv6 フィルタ情報／IPv6 フィルタリング情報（IPv6）
- ・ QoS 情報／DSCP 値書き換え情報（IPv4）
- ・ IPv6 QoS 情報／IPv6 DSCP 値書き換え情報（IPv6）

4.10 ダンプスイッチ情報

[操作] 「設定メニュー」→基本設定「装置情報」→[ダンプスイッチ情報]

ダンプスイッチ

外部メディアへダンプを行うかどうかを設定します。“許可する”を選択した場合は、外部メディアを挿入し、ダンプスイッチを押して、システム情報のダンプを行います。

4.11 外部メディアスタート機能情報

[操作] 「設定メニュー」→基本設定「装置情報」→[外部メディアスタート機能情報]

外部メディアスタート機能

外部メディア（コンパクトフラッシュカードまたはUSBメモリ）を接続することで、PCレスでの設定変更／ファーム更新を可能にします。

装置名称

装置名称を32文字以内で指定します。省略時は初期値の装置名を利用します。

外部メディアスタート機能の有効時、ファームウェアおよび構成定義の退避／復旧の際のファイル名に付加します。

4.12 ハッシュ情報

適用機種 SR-S308TL1, 310TL2, 316TL1, 318TL2, 324TL2, 716C2, 724TC1, 748TC1

[操作] 「設定メニュー」→基本設定「装置情報」→「ハッシュ情報」

SR-S716C2、724TC1、748TC1 では、「第二アルゴリズム」は表示されません。

アルゴリズム

ハッシュアルゴリズムを選択します。

こんな事に気をつけて

スイッチチップは、以下のエントリをハッシュ管理しています。

- SR-S716C2 の場合
ARP エントリ
- SR-S724TC1/748TC1 の場合
ARP/Neighbor Cache エントリ

ハッシュエントリの格納数には上限があるため、ハッシュエントリが溢れると、ARP/Neighbor Cache エントリの上限に達していなくても ARP/Neighbor Cache エントリがスイッチチップに登録できなくなり、ソフトウェアルーターティンクとなります。

ハッシュ溢れによるエントリ未登録の発生時には、ハッシュアルゴリズムを変更することで、登録可能になる場合があります。

- SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合
認証端末の MAC アドレスエントリ

ハッシュエントリの格納数には上限があるため、ハッシュエントリが溢れると、認証端末数の上限に達していなくても認証端末の MAC アドレスがスイッチチップに登録できなくなり、認証失敗となります。

ハッシュ溢れによる認証失敗（エントリ未登録）の発生時には、ハッシュアルゴリズムを変更することで、登録可能になる場合があります。

第二アルゴリズム

(SR-S308TL1/310TL2/316TL1/318TL2/324TL2)

第二ハッシュアルゴリズムを選択します。

こんな事に気をつけて

スイッチチップは認証端末の MAC アドレスエントリをハッシュ管理しています。

ハッシュエントリの格納数には上限があるため、ハッシュエントリが溢れると、認証端末数の上限に達していなくても認証端末の MAC アドレスがスイッチチップに登録できなくなり認証失敗となります。

ハッシュ溢れによる認証失敗（エントリ未登録）の発生時には、本アルゴリズムを変更することで、登録可能になる場合があります。

4.13 冷却ファン情報

適用機種 SR-S308TL1, 310TL2, 316TL1, 318TL2, 324TL2

[操作] 「設定メニュー」→基本設定「装置情報」→[冷却ファン情報]

■冷却ファン情報

冷却ファン回転数

☒ 通常回転 ☐ 停止

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

冷却ファン回転数

冷却ファンの回転数を選択します。

こんな事に気をつけて

冷却ファンを停止に設定する場合は、設置温度条件が異なりますので注意してください。

設置温度条件は以下のとおりです。

通常回転（冷却ファン動作時）：0～45℃

停止（冷却ファン停止時）：0～35℃

5 スケジュール情報

適用機種 全機種

[操作] 「設定メニュー」→基本設定「スケジュール情報」

スケジュール情報	
構成定義切り替え予約情報	
このページでは、スケジュール予約情報を設定できます。	
 スケジュール機能を使用する際には、正しい時刻が設定されているか確認してください。現在の時刻は Tue Nov 14 15:55:11 2006 です。	

5.1 構成定義切り替え予約情報

[操作] 「設定メニュー」→基本設定「スケジュール情報」→[構成定義切り替え予約情報]

■構成定義切り替え予約情報		
実行日時	構成定義切り替え予約	操作
1	-	修正 削除

保存した情報は、設定反映後に有効になります。

[操作] 「設定メニュー」→基本設定「スケジュール情報」→[構成定義切り替え予約情報]→[修正]

実行日時	20 年 月 日 時 分
1 動作	構成定義情報1で再起動 ▼
保存 キャンセル 一覧へ戻る	

本装置は構成定義情報が2つ存在します。指定時刻に運用する構成定義情報を切り替えることができます。
 なお、現在運用中の構成定義情報は保守メニューの「構成定義情報切り替え」で確認することができます。

こんな事に気をつけて

指定時刻になると、本装置は自動的に再起動され、構成定義情報が切り替わります。その際、データ通信中の場合は接続が切断されます。

実行日時

構成定義情報を切り替える日時を西暦で2000～2036年の範囲で指定します。

動作

切り替える構成定義情報を指定します。

6 ether情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「ether情報」

ether情報

ether情報

■ether情報

?

ポート 番号	ポート種別	VLAN ID		操作	
		Tagged	Untagged		
1	通常		10	修正	初期化
2	通常			修正	初期化
3	通常			修正	初期化
4	通常			修正	初期化
5	通常			修正	初期化
6	通常			修正	初期化
7	通常			修正	初期化
8	通常			修正	初期化
9	通常			修正	初期化
10	通常			修正	初期化
11	通常			修正	初期化
12	通常			修正	初期化
13	通常			修正	初期化
14	通常			修正	初期化
15	通常			修正	初期化
16	通常			修正	初期化

全初期化

<<複数ポート指定>>

- 複数のポート番号を設定する場合“,”(カンマ)で区切ります。(例:1,5)
- 複数の番号が続く場合“-”(ハイフン)で区切ります(例: 1-8)

※ポートリストを指定せずに修正、初期化を行うと全てのポートに有効になります。

ポート
リスト

修正

初期化

保存した情報は、設定反映後に有効になります。

etherポートの一覧が表示されています。etherポート数は、仕様一覧「[1.1.1 本体装置](#)」(P9)を参照してください。処理するボタンをクリックし、次のページへ進みます。

ポートリスト

設定するポート番号を指定します。

複数のポート番号を指定する場合は、“,” (カンマ) で区切ります。

記述例) 1,5

複数のポート番号を続けて指定する場合は、“-” (ハイフン) で区切ります。

記述例) 1-8

こんな事に気をつけて

ポートリストを指定しないで [修正] ボタンまたは [初期化] ボタンをクリックすると、すべてのポートに有効になります。

異なるポート種別を含む範囲指定はできません。

同時に指定可能なポートリストは、以下のとおりです。

機種	ポートリスト
SR-S208TC2、308TL1	1～8または9
SR-S224TC2	1～24または25～26
SR-S208PD1	1～10
SR-S224PS1	1～24または25～28
SR-S224CP1	1～24または25～26 または27～28
SR-S248TC1	1～48または49～50 または51～52
SR-S310TL2	1～8または9～10
SR-S316TL1、318TL2	1～16または17～18
SR-S324TL2	1～20または21～24
SR-S316C2、716C2	1～16
SR-S324TC1、724TC1	1～20または21～24 または25～26
SR-S328TR1	1～20または21～24 または25～28
SR-S348TC1、748TC1	1～44または45～48 または49～52

[操作] 「設定メニュー」→詳細設定「ether 情報」→ [修正]

ether 情報 - ether1 情報		
基本情報	ポート種別情報	MAC 関連
STP 関連	LLDP 関連	認証共通情報
IEEE802.1X 認証情報	Web 認証関連	MAC アドレス認証関連
DHCP スヌープ情報	フィルタ情報	QoS 関連
接続先監視情報	トラップ情報	IEEE802.1ad 関連
IEEE802.1ah 関連		

SR-S308TL1、310TL2、316TL1、318TL2、324TL2、316C2、324TC1、328TR1、348TC1、716C2、724TC1、748TC1 のみ、「認証共通情報」が表示されます。

SR-S224CP1 のみ、「L2 暗号関連」が表示されます。

SR-S328TR1 のみ、「IEEE802.1ad 関連」および「IEEE802.1ah 関連」が表示されます。

6.1 基本情報

[操作] 「設定メニュー」→詳細設定「ether情報」→[修正]→[基本情報]

■基本情報	
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
フロー制御	送信: ☒ しない ☐ する 受信: ☒ する ☐ しない
VLAN	Tagged: Untagged:
転送許可ポート	☒ 設定しない ☐ 設定する
ループ検出	☒ 使用する ☐ 使用しない ループ判定対象フレーム: ☒ 本装置が送信した監視フレームのみ ☐ すべての監視フレーム
LACPポート優先度	32768
起動時の閉塞状態	☒ 閉塞しない ☐ 閉塞する
リンクダウン回数の上限値	
リンクダウン連携	☒ 使用しない ☐ 使用する 連携ポートリスト: リンクアップ時の動作: ☒ 閉塞解除しない ☐ 閉塞解除する 閉塞要因: ☒ リンクダウン連携 ☐ すべて

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

SR-S208PD1、224PS1、248TC1、308TL1、310TL2、316TL1、318TL2、324TL2、328TR1 では、表示が上記の画面とは異なります。

こんな事に気をつけて

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」の設定を利用してポート閉塞を解除してください。

ポート使用

説明文

ether ポートを使用する場合は、“使用する”を選択します。 この ether ポートの説明文を、50 文字以内で設定します。

メディア種別 (SR-S208PD1、248TC1、308TL1、 316TL1 除く)

使用するメディア種別を選択します。機種によって、設定できるポートが異なります。設定できるポート番号は、以下のとおりです。

機種	設定できるポート番号
SR-S208TC2	9
SR-S224TC2	25～26
SR-S224PS1、224CP1	25～28
SR-S310TL2	9～10
SR-S318TL2	17～18
SR-S316C2、716C2	すべて
SR-S324TL2、324TC1、 328TR1、724TC1	21～24
SR-S348TC1、748TC1	45～48

こんな事に気をつけて

- “自動”を選択し、通常ポートおよびSFPポートが共に接続されている場合は、SFPポートが優先されます。
- “自動”を選択し、通常ポートが使用されている状態でSFPポートを接続すると、使用するポートがSFPポートに切り替わり、通常ポートはリンクダウン状態となります。
- SR-S324TC1/328TR1/348TC1/724TC1/748TC1で、100BASE-FXモジュールを使用する場合は、“SFPポート”を選択してください。

通信速度

etherポートの通信速度を選択します。

こんな事に気をつけて

- 10/100/1000BASE-Tポートで“100Mbps”または“10Mbps”を選択する場合は、メディア種別を“通常ポート (RJ45)”に設定してください (“自動”および“SFPポート”では、ポートは使用できません)。
- SR-S224CP1のENCポートでは、“10Mbps”は設定できません。また、“自動”を設定した場合も、10Mbpsではリンクアップしません。
- SR-S308TL1/310TL2/316TL1/318TL2/324TL2/324TC1/328TR1/348TC1/724TC1/748TC1で、100BASE-FXモジュールを使用する場合は、“100Mbps”を選択してください。

全二重／半二重

etherポートの全二重／半二重を選択します。

こんな事に気をつけて

- メディア種別が“SFPポート”の場合は、設定は無効となり、全二重モードで動作します。
- 通信速度が“1000Mbps”の場合は、設定は無効となり、全二重モードで動作します。
- 通信速度が“自動”の場合は、設定は無効となり、接続装置とのオートネゴシエーションの結果により動作します。
- SR-S224CP1のENCポートでは、全二重モード固定で動作します。また、通信速度を“自動”に設定した場合も、半二重モードではリンクアップしません。

MDI

etherポートのMDIを選択します。

こんな事に気をつけて

- メディア種別が“SFPポート”の場合は、設定は無効となります。
- “自動”を選択した場合、通信速度が“自動”の場合のみ有効となり、通信速度が“自動”以外の場合では、MDI-Xとして動作します。
- 通信速度が“1000Mbps”または“自動”の場合で、“MDI”を選択した場合、設定は無効となりMDI-Xとして動作します。

フロー制御

etherポートのフロー制御機能の動作を、送信と受信の機能ごとに選択します。

バックプレッシャー機能は、半二重モードの場合に有効です。

フロー制御機能は、通信速度の設定にかかわらず有効です。

送信

フロー制御パケットの送信の設定

受信

フロー制御パケットを受信した場合のフロー制御の設定

省電力モード (SR-S310TL2、324TL2、318TL2、328TR1)

省電力モード (IEEE802.3az, Energy-Efficient Ethernet) を使用する場合は、“使用する”を選択します。

こんな事に気をつけて

以下の場合には省電力モードは有効となりません。

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

VLAN

“Tagged” および “Untagged” とともに省略時は、“Untagged” にデフォルト VLAN (VLAN ID=1) が設定されます。

Tagged

Tagged VLAN ID を設定します。

こんな事に気をつけて

IEEE802.1X 認証、Web 認証および MAC アドレス認証を有効にしたポートには、VLAN を設定できません。設定された場合はポートが使用できなくなります。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
- 「ether 情報」 - 「認証共通情報」で、VLAN タグ付きフレームを“透過する”に設定した場合の、タグ VLAN 設定

Untagged

Untagged VLAN ID を設定します。

こんな事に気をつけて

- IEEE802.1X 認証および MAC アドレス認証を有効にしたポートには、VLAN を設定できません。設定された場合はポートが使用できなくなります。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
- SR-S224PS1/224CP1/248TC1/308TL1/310TL2/316TL1/318TL2/324TL2/316C2/324TC1/328TR1/348TC1/716C2/724TC1/748TC1 では、VLAN ID リストとして複数の VLAN を記述することができますが、以下の条件があります。
 - ポート VLAN については、1 つしか定義できません。プロトコル VLAN が設定されていない VLAN を複数記述した場合は、もっとも小さい番号の VLAN のみが有効となります。
 - SR-S308TL1/310TL2/316TL1/318TL2/324TL2/316C2/324TC1/328TR1/348TC1/716C2/724TC1/748TC1 のプロトコル VLAN については、システム定義プロトコル (IPv4/IPv6/FNA の 3 定義) およびユーザ定義 (最大 8 定義) を合わせた VLAN 定義ができます。
 - SR-S224PS1/224CP1/248TC1 のプロトコル VLAN については、システム定義プロトコル (IPv4/IPv6 の 2 定義) およびユーザ定義 (最大 3 定義) を合わせた VLAN 定義ができます。

転送許可ポート

転送を許可するポートリストを指定します。

省略時は、すべてのポートに対し転送が許可されます。

こんな事に気をつけて

- ポートリストで設定したポートがリンクアグリゲーションポートまたはバックアップポートであった場合は、リンクアグリゲーションまたはバックアップグループのすべてのポートが転送許可されます。
- SR-S208TC2/224TC2/208PD1 では、1 ポートのみ指定可能となります。

ループ検出

ループ検出機能を有効にする場合は、“使用する”を選択します。

なお、“使用する”を選択した場合でも、「ループ検出情報」の「基本設定」の設定が“使用しない”となっている場合は動作しません。

ループ判定対象フレーム

ループ判定対象とするフレームを選択します。

ポート給電 (SR-S224PS1)

給電モードを使用する場合は、“使用する”を選択します。ポート番号が1～24の場合に設定できます。

LACP ポート優先度

LACP ポート優先度を1～65535の範囲の10進数で指定します。LACP ポート優先度は、リンクアグリゲーショングループが結合ポートを選択する優先度として使用します。値が小さいほど優先度が高くなり、同じ優先度のポートではポート番号の小さいほうが高優先と判断します。

省略時は、32768が設定されます。LACP を使用しない場合の設定は無効です。

起動時の閉塞状態

装置起動時、および動的定義反映時の ether ポートの閉塞／非閉塞を選択します。

- 閉塞しない
装置起動時、および動的定義反映時にポート非閉塞状態で動作を開始します。
- 閉塞する
装置起動時、および動的定義反映時にポート閉塞状態で動作を開始します。

装置起動時、および動的定義反映時の ether ポート状態と閉塞状態の関係は、以下のとおりです。

起動時の閉塞状態	装置起動時／動的定義変更時の ether ポートの状態		
	リンクアップ可能	リンクアップ不可能	ポート閉塞済み
閉塞しない	リンクアップ／通信可能	リンクダウン／通信不可能	閉塞状態のまま通信不可能
閉塞する	閉塞状態に入り通信不可能	閉塞状態に入り通信不可能	閉塞状態のまま通信不可能

リンクダウン回数の上限値

該当ポートを閉塞状態にするための上限値として、リンクダウン回数を1～10の範囲の10進数で指定します。リンクアップ後のリンクダウン回数が上限値に達したときに、このポートは閉塞状態となります。省略時は、上限値なしとみなし、リンクダウンによって閉塞状態になることはありません。

リンクダウン連携

この ether ポートでリンクダウン連携を使用する場合は、“使用する”を選択します。“使用する”を選択した場合は、以降の“連携ポートリスト”、“リンクアップ時の動作”および“閉塞要因”を設定してください。

こんな事に気をつけて

- ether ポートの種別が、リンクアグリゲーションポートで、リンクアグリゲーションのリンクダウン連携の連携ポートリスト情報設定がある場合は、リンクアグリゲーションのリンクダウン連携機能が有効となり、本定義は無視されます。
- ether ポートの種別がバックアップポートで、バックアップポートのリンクダウン連携の連携ポートリスト情報設定がある場合は、バックアップポートのリンクダウン連携機能が有効となり、本定義は無視されます。

連携ポートリスト

このポートインタフェースがリンクダウンしたときに連携してリンクダウン（ポート閉塞）させるポートリストを、以下の範囲の10進数で指定します。

機種	ポートリスト
SR-S208TC2、308TL1	1～9
SR-S224TC2	1～26
SR-S208PD1、310TL2	1～10
SR-S224PS1、224CP1、328TR1	1～28
SR-S248TC1、348TC1、748TC1	1～52
SR-S316TL1、318TL2	1～18
SR-S324TL2	1～24
SR-S316C2、716C2	1～16
SR-S324TC1、724TC1	1～26

ポートリストを複数指定する場合は、“,”で区切ります。範囲指定の場合は“-”で区切ります。省略時は、該当ポートがリンクダウンしても連携動作しません。

こんな事に気をつけて

この設定項目が省略されている場合は、連携動作しないため、以降の“リンクアップ時の動作”項目の設定内容は適用されません。

リンクアップ時の動作

本定義ポートがリンクアップしたときに、連携ポートリストに設定した、ポートの閉塞状態の解除を行うかどうかを選択します。

- 閉塞解除しない
リンクアップ時に閉塞状態の解除を行いません。
- 閉塞解除する
リンクアップ時に閉塞状態の解除を行います。本設定を選択した場合は、以降の“解除対象の要因”を設定してください。

こんな事に気をつけて

“閉塞解除しない”、“閉塞解除する”のどちらを選択しても「操作メニュー」の「閉塞／閉塞解除」設定によって連携ポートリストの閉塞状態の解除が可能です。

閉塞要因

リンクアップ時に、連携ポートリストに設定されたポートの閉塞状態の解除を行う場合に、解除対象とする閉塞要因を選択します。

- リンクダウン連携
連携ポートリストの閉塞状態がリンクダウン連携による閉塞要因のみ解除対象に指定します。
- すべて
連携ポートリストの閉塞状態の閉塞要因に依存しない解除対象に指定します。

こんな事に気をつけて

- 連携ポートリストに設定されたポートに対する動的定義反映時には、設定に依存しないで閉塞状態の解除が行われます。
- 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」の設定を利用してポート閉塞を解除してください。

6.2 ポート種別情報

6.2.1 ポート種別情報（初期表示または通常選択時）

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]
→ [ポート種別情報（ポート種別：初期表示または通常）]

■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

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

初期表示またはポート種別に“通常”を選択した場合に表示されます。

ポート種別

ether ポートのタイプを、以下の4つから選択します。

- 通常
通常ポートとして使用する場合に選択します。
- リンクアグリゲーション
リンクアグリゲーションとして使用する場合に選択します。
- バックアップ
バックアップポートとして使用する場合に選択します。
- ミラー
ミラーポートとして使用する場合に選択します。

6.2.2 ポート種別情報（リンクアグリゲーション選択時）

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]
→ [ポート種別情報（ポート種別：リンクアグリゲーション）]

■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

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

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

ポート種別に“リンクアグリゲーション”を選択した場合に表示されます。

「ポート種別」の項目は、「ポート種別情報（初期表示または通常選択時）」を参照してください。

リンクアグリゲーショングループ情報

グループ番号

リンクアグリゲーションのグループ番号を、以下の範囲で選択します。

機種	グループ番号
SR-S208TC2、308TL1	1～4
SR-S224TC2	1～6
SR-S208PD1、310TL2	1～5
SR-S224PS1、224CP1、328TR1	1～14
SR-S248TC1、348TC1、748TC1	1～26
SR-S316TL1、318TL2、324TL2、316C2、716C2	1～8
SR-S324TC1、724TC1	1～13

アンカポート番号

リンクアグリゲーションのアンカポート番号を選択します。

こんな事に気をつけて

ポート種別に“リンクアグリゲーション”を選択し、以下のような定義条件の矛盾があった場合、該当ポートはリンクアップせず使用できません。ログメッセージを参考に設定を変更してください。

- 設定したアンカポートが正しく設定されていない場合は無効になります。
- アンカポートは、グループ内のもっとも番号の小さい ether ポートに設定する必要があります。
- 全二重／半二重の設定が“半二重”の場合は、リンクアグリゲーションは使用できません。
- グループ内のすべてのポートは、同一の通信速度に設定してください。
- グループ内のすべてのポートは、同一の VLAN に所属するように設定してください。
- グループを構成するメンバポートは、必ず連続したポートとなるように設定してください。
- IEEE802.1X 認証、Web 認証、MAC アドレス認証のどれかが有効に設定されているポートでは、リンクアグリゲーションは設定できません。

6.2.3 ポート種別情報（バックアップ選択時）

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]
→ [ポート種別情報（ポート種別：バックアップ）]

■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

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
 ☐ 待機ポート

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

ポート種別に“バックアップ”を選択した場合に表示されます。

「ポート種別」の項目は、「ポート種別情報（初期表示または通常選択時）」を参照してください。

バックアップグループ情報

グループ番号

バックアップのグループ番号を、以下の範囲で選択します。

機種	グループ番号
SR-S208TC2、308TL1	1～4
SR-S224TC2、324TC1、724TC1	1～13
SR-S208PD1、310TL2	1～5
SR-S224PS1、224CP1、328TR1	1～14
SR-S248TC1、348TC1、748TC1	1～26
SR-S316TL1、318TL2	1～9
SR-S324TL2	1～12
SR-S316C2、716C2	1～8

優先度

“優先ポート” または “待機ポート” のどちらかを選択します。

こんな事に気をつけて

- ・ 同一グループで “優先ポート” または “待機ポート” が選択されたポートが複数存在する場合は、番号の小さいポートが有効となり、番号の大きいポートは使用できません。
- ・ 同一グループで “優先ポート” または “待機ポート” が未定義の場合は、設定は無効になりバックアップポートは使用できません。

6.2.4 ポート種別情報（ミラー選択時）

[操作] 「設定メニュー」→詳細設定「ether情報」→[修正]→[ポート種別情報（ポート種別：ミラー）]

ポート種別に “ミラー” を選択した場合に表示されます。

「ポート種別」の項目は、「ポート種別情報（初期表示または通常選択時）」を参照してください。s

ミラー情報

ミラーポートで対象とするソースポート番号およびミラー動作モードを設定します。

こんな事に気をつけて

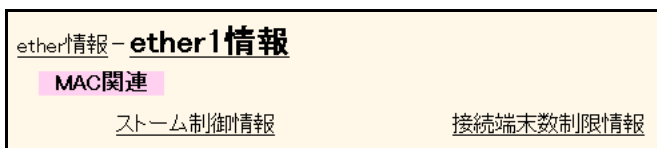
- ・ ミラーのターゲット・ポートは装置で1ポートしか設定できません。
- ・ ミラーのターゲット・ポートは運用ポートとしても使用できます。

- ・ ターゲット・ポートに出力されるパケットのあて先 MAC アドレス、送信元 MAC アドレス、VLAN タグの有無とその内容については、実際にソースポートで送受信されたパケットと異なる場合があります。
- ・ STP を有効とした場合は、ターゲット・ポート番号によって、ソースポートの設定可能な範囲が以下になります。（SR-S316C1/716C1 の場合）

ターゲット・ポート	ソースポート設定範囲
1～8	1～8
9～16	9～16

6.3 MAC 関連

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[MAC 関連]



SR-S208TC2、224TC2、208PD1 では、「ストーム制御情報」は表示されません。

6.3.1 ストーム制御情報

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

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[MAC 関連]→[ストーム制御情報]

■ストーム制御情報

ストーム制御機能

☒ 使用しない
☐ 使用する

しきい値(pps)

しきい値を超えた場合の操作

ブロードキャスト

マルチキャスト

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

こんな事に気をつけて

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。

ストーム制御機能

ブロードキャスト／マルチキャストストーム制御機能を使用する場合は、“使用する”を選択します。

しきい値

ブロードキャストとマルチキャストストームのトラフィックのしきい値を、1秒間のパケット数として、以下の範囲の10進数で指定します。

機種	しきい値
SR-S224PS1、224CP1、248TC1	1～200000
SR-S316C2、716C2	1～2000000
SR-S308TL1、310TL2、316TL1、318TL2、324TL2、324TC1、328TR1、348TC1、724TC1、748TC1	1～30000000

ブロードキャスト

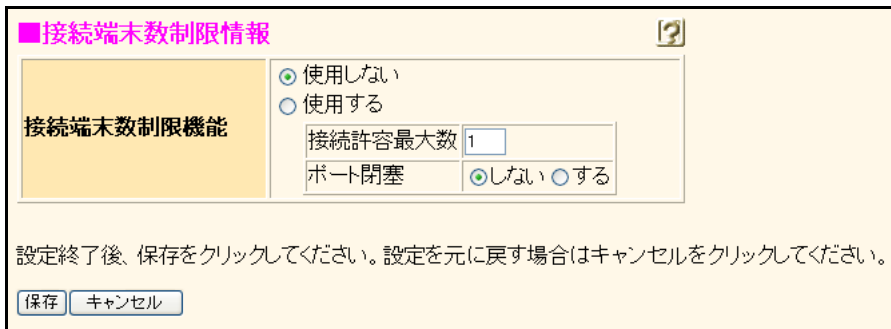
ブロードキャストストームのトラフィックが“しきい値”を超えた場合の動作を選択します。

マルチキャスト

マルチキャストストームのトラフィックが“しきい値”を超えた場合の動作を選択します。

6.3.2 接続端末数制限情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[MAC 関連]→[接続端末数制限情報]



こんな事に気をつけて

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。

接続端末数制限機能

接続端末数制限機能を使用する場合は、“使用する”を選択します。

“使用する”を選択した場合、本装置起動後に接続した端末の MAC アドレス情報を管理し、接続許容最大数を超える不正な接続を検出します。

接続許容最大数

接続端末数制限機能の接続許容端末数を、1～30 の範囲の 10 進数で指定します。

省略時は、1 が設定されます。

ポート閉塞

接続端末数制限機能の接続許容端末数を超える接続端末検出時のポート閉塞モードを選択します。

6.4 STP 関連

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[STP 関連]

6.4.1 基本情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[STP 関連]→[基本情報]

STP 機能

STP 機能を利用して経路制御を行う場合は、“使用する”を選択します。

STP 動作バージョン

STP 機能の動作バージョンを選択します。

こんな事に気をつけて

“指定なし”を選択した場合は、「STP 情報」の STP 動作モードで選択した動作モードに従って動作します。

パスコスト

STP で利用するパスコストを選択します。“指定する”を選択する場合は、1～200000000 の範囲の 10 進数で指定します。パスコストの適性値が不明な場合は“自動決定”を選択すると、自動的にパスコストが決定されます。

こんな事に気をつけて

“指定する”を選択してパスコストの値を指定しない場合は、無効となります。

インタフェース優先度

STP で使用するインタフェースごとの優先度を選択します。値が小さいほど、優先度は高くなります。

こんな事に気をつけて

16 で割り切れる以下の値のみ設定できます。

0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240

6.4.2 MSTP インスタンス情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[STP 関連]→[MSTP インスタンス情報]

■MSTPインスタンス情報

インスタンスID	パスコスト	インタフェース優先度	操作
1	自動決定	128	修正 初期化
2	自動決定	128	修正 初期化
3	自動決定	128	修正 初期化
4	自動決定	128	修正 初期化
5	自動決定	128	修正 初期化
6	自動決定	128	修正 初期化
7	自動決定	128	修正 初期化
8	自動決定	128	修正 初期化
9	自動決定	128	修正 初期化
10	自動決定	128	修正 初期化
11	自動決定	128	修正 初期化
12	自動決定	128	修正 初期化
13	自動決定	128	修正 初期化
14	自動決定	128	修正 初期化
15	自動決定	128	修正 初期化

[全初期化](#)

保存した情報は、設定反映後に有効になります。

現在、設定されている MSTP インスタンス情報の一覧が表示されています。MSTP インスタンス情報の定義数は、1～15 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[STP 関連]→[MSTP インスタンス情報]→[修正]

<MSTPインスタンス情報入力フィールド>

1

パスコスト	☒ 自動決定 ☐ 指定する
インタフェース優先度	128 ▼

[保存](#) [キャンセル](#) [一覧へ戻る](#)

こんな事に気をつけて

「STP 情報」の STP 動作モードが“MSTP”に設定されていない場合は、無効となります。

パスコスト

STP で利用するパスコストを選択します。“指定する”を選択する場合は、1～200000000 の範囲の 10 進数で指定します。パスコストの適性値が不明な場合は“自動決定”を選択すると、自動的にパスコストが決定されます。

こんな事に気をつけて

“指定する”を選択してパスコストの値を指定しない場合は、無効となります。

インタフェース優先度

STP で使用するインタフェースごとの優先度を選択します。値が小さいほど、優先度は高くなります。

こんな事に気をつけて

16 で割り切れる以下の値のみ設定できます。

0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240

6.5 LLDP 関連

[操作] 「設定メニュー」 → 詳細設定 「ether 情報」 → [修正] → [LLDP 情報]

■LLDP関連

動作

☒ 送受信しない
☐ 送受信する
☐ 送信のみ
☐ 受信のみ

送信オプション情報

種別	情報名
基本情報	☒ ポート解説 (Port Description)
	☒ システム名 (System Name)
	☒ システム解説 (System Description)
	☒ システム機能 (System Capabilities)
	☒ 管理アドレス (Management Address)
IEEE802.1 情報	☐ ポートVLAN ID (Port VLAN ID)
	☐ プロトコルVLAN ID (Port And Protocol VLAN ID)
	☐ VLAN名 (VLAN Name)
	☐ プロトコルVLAN識別 (Protocol Identity)
IEEE802.3 情報	☐ MAC/PHY 定義/状態 (MAC/PHY Configuration/Status)
	☐ MDI給電 (Power Via MDI)
	☐ リンクアグリゲーション (Link Aggregation)
	☐ 最大フレーム長 (Maximum Frame Size)

送信VLAN情報

☒ すべて
☐ VLAN ID 指定

受信情報更新通知

☒ しない ☐ する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

LLDP (Link Layer Discovery Protocol : 隣接探索プロトコル) のポートごとの設定を行います。

こんな事に気をつけて

LLDP 送信間隔時間などの装置全体に関する設定は、「設定メニュー」の「LLDP 情報」で行ってください。

動作

LLDPの動作を選択します。

- “送受信する” または “送信のみ” を選択した場合
本ポートに関する LLDP 情報を定期的に隣接装置に送信します。
- 送受信する” または “受信のみ” を選択した場合
隣接装置からの LLDP 情報を受信します。

受信した LLDP 情報は、LLDP 情報に含まれている有効時間が経過するまで保持します。

送信オプション情報

送信するオプション情報を選択します。

LLDP 情報には、常に送信する必須情報 (装置識別、ポート識別、有効時間) と、送信するかどうかを選択できるオプション情報があります。

オプション情報をすべて送信しないようにしても、必須情報が常に送信されます。

送信する LLDP 情報は最大 1500 バイトに制限されるため、情報が 1500 バイトを超えると 1500 バイト以内に収まった情報だけを送信します。送信する情報が多いときは不要なオプション情報を送信しないように設定してください。

送信VLAN情報

送信オプション情報の“IEEE802.1 情報”でVLAN情報を送信するように設定したとき、送信するVLAN情報のVLAN IDを指定します。

- “すべて”を選択した場合
すべてのVLANの情報を送信します。
- “VLAN ID 指定”を選択した場合
送信するVLAN IDを1～4094の範囲の10進数で指定します。
VLAN IDを複数指定する場合は“,”で区切ります。
VLAN IDの範囲を指定する場合は“-”で区切ります。

受信情報更新通知

以下に示すような要因でLLDP受信情報（隣接情報）が更新されたとき、SNMPトラップを送信して更新されたことを通知するかどうかを選択します。

- 新たなLLDP情報を受信した
- 受信していたLLDP情報の有効時間が経過して受信情報を破棄した
- 有効時間が0のLLDP情報を受信して受信情報を破棄した
- LLDP最大受信数を超過してLLDP情報を受信したため受信情報を破棄した
- 「表示メニュー」-「LLDP関連」-「隣接情報」の「隣接情報クリア」ボタンをクリックして受信情報を破棄した
- clear lldp neighbors コマンドを実行して受信情報を破棄した

こんな事に気をつけて

受信情報更新通知を“する”に設定した場合、「SNMP情報」-「トラップ情報」の“lldpRemTablesChange”を“有効にする”に設定してください。

6.6 認証共通情報

適用機種 SR-S308TL1, 310TL2, 316TL1, 318TL2, 324TL2, 316C2, 324TC1, 328TR1, 348TC1, 716C2, 724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[認証共通情報]

VLAN タグ付きフレーム

認証ポートでの VLAN タグ付きフレームの動作モードを選択します。

- 破棄する
VLAN タグ付きフレームを破棄します。
- 透過する
VLAN タグ付きフレームを認証しないで透過します。

こんな事に気をつけて

IEEE802.1X 認証、Web 認証または MAC アドレス認証が有効でない場合、本設定は無効となります。

認証許容端末数

IEEE802.1X 認証、Web 認証および MAC アドレス認証を合わせた認証ポートでの認証許容端末数を、以下の範囲の 10 進数で指定します。省略時は、以下が設定されます。

機種	認証許容端末数	
	範囲	省略時の設定
SR-S308TL1、310TL2、316TL1、318TL2、324TL2	1～64	1
SR-S316C2、324TC1、328TR1、348TC1、716C2、724TC1、748TC1	1～100	24

こんな事に気をつけて

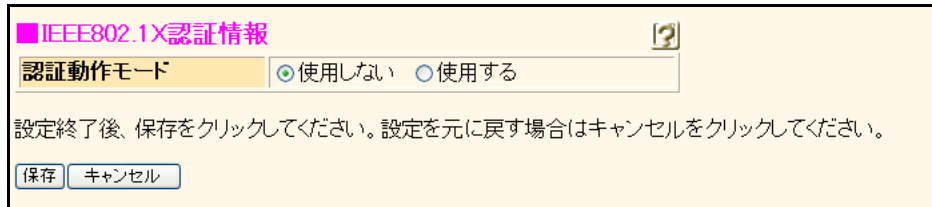
- ポートの認証方式がポートごとの認証の場合は、設定は無効となります。
- 認証許容端末数は、すべての認証ポートの設定値の合計が上限値以下である必要があります。
認証ポートで昇順に認証許容端末数をカウントし、上限値を超えたポートは無効となり利用できません。

機種	上限値
SR-S308TL1、310TL2、316TL1、318TL2、324TL2	64
SR-S348TC1、748TC1	1248
SR-S316C2、324TC1、328TR1、716C2、724TC1	1024

6.7 IEEE802.1X 認証情報

6.7.1 IEEE802.1X 認証情報（初期表示または使用しない選択時）

〔操作〕 「設定メニュー」→詳細設定「ether 情報」→〔修正〕→〔IEEE802.1X 認証情報〕
→〔IEEE802.1X 認証情報（認証動作モード：初期表示または使用しない）〕



■IEEE802.1X 認証情報 ⓘ

認証動作モード ☒ 使用しない ☐ 使用する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

初期表示または認証動作モードに“使用しない”を選択した場合に表示されます。

認証動作モード

IEEE802.1X 動作モードを選択します。

- 使用しない
IEEE802.1X を使用しない場合に選択します。
- 使用する
IEEE802.1X のオーセンティケータ動作を使用する場合に選択します。

6.7.2 IEEE802.1X 認証情報（使用する選択時）

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[IEEE802.1X 認証情報]
→[IEEE802.1X 認証情報（認証動作モード：使用する）]

■ IEEE802.1X 認証情報	
認証動作モード	☐ 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 ☐ ポートごと
ポート認証制御	☒ 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 回
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
デフォルト割り当て VLAN ID	1
WOL 転送モード	☒ 転送しない ☐ 転送する
許容する EAPOL MAC アドレス	☒ PAE グループアドレスのみ ☐ PAE グループアドレスとポート MAC アドレス ☐ PAE グループアドレスとユーザ定義 MAC アドレス

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

認証動作モードに“使用する”を選択した場合に表示されます。

認証動作モード

IEEE802.1X 動作モードを選択します。

- 使用しない
IEEE802.1X を使用しない場合に選択します。
- 使用する
IEEE802.1X のオーセンティケータ動作を使用する場合に選択します。

こんな事に気をつけて

- IEEE802.1X 認証を利用する場合は“IEEE802.1X 認証情報”も設定してください。
- “使用する”を選択したポートに VLAN を指定することはできません。設定された場合はポートが使用できなくなります。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
 - 「ether 情報」-「認証共通情報」で、VLAN タグ付きフレームを“透過する”に設定した場合の、タグ VLAN 設定
- 認証サーバの認証データベース、またはローカル認証データベースには必ず VLAN ID も登録してください。認証処理時に VLAN ID の通知がない場合は“デフォルト割り当て VLAN ID”で設定されたデフォルト VLAN にマッピングします。また、認証された端末が割り当てられた VLAN ID を持つポートが IEEE802.1X 認証ポート以外に存在しない場合はエラーとなり、常に認証が失敗します。

認証方式

IEEE802.1X 認証方式を選択します。“デフォルト”を選択した場合は、“IEEE802.1X 認証機能定義”の設定を使用します。

こんな事に気をつけて

- 認証方式としてポートごとの認証を選択し、そのポートに接続される端末（Supplicant）の1台が認証許可された場合は、同じポートに接続されるほかの端末からのアクセスがすべて透過として扱われます。
- 同一ポートでWeb 認証またはMAC アドレス認証を同時に有効とする場合は、すべての認証機能の認証方式が同じとなるように設定してください。

ポート認証制御

ポートのIEEE802.1X 認証状態を、以下の3つから選択します。

- 自動
IEEE802.1X 認証機能によるポートアクセス制御機能を利用する場合に選択します。
- 認証拒否
常に認証が拒否されるポートとして利用する場合に選択します。
- 認証許可
常に認証成功となるポートとして利用する場合に選択します。

認証失敗時再認証抑止時間

認証が失敗したあと、認証を抑止する時間を0～600秒の範囲の10進数で指定します。0秒を指定した場合、認証に失敗した場合でも次の認証を抑止しません。省略時は、1分が設定されます。

認証開始送信間隔

認証を開始するメッセージの送信間隔を1～600秒の範囲の10進数で指定します。省略時は、30秒が設定されます。

EAP 応答待ち時間

サブリカントからの応答を待ち合わせる時間を1～600秒の範囲の10進数で指定します。省略時は、30秒が設定されます。

EAP 再送回数

サブリカントからの応答が応答待ち時間内に受信できない場合に再送する回数を、1～10回の範囲の10進数で指定します。省略時は、2回が設定されます。

再認証間隔

認証が成功したサブリカントを一定時間ごとに再認証するかについて指定します。再認証を行う場合は、その間隔を15秒～5時間の範囲の10進数で指定します。省略時は、1時間が設定されます。

参照する AAA 情報

IEEE802.1X 認証を行う場合に参照する AAA 情報のグループIDを指定します。AAAのグループIDを、0～9の範囲の10進数で指定します。省略時は、0が設定されます。

デフォルト割り当て VLAN ID

AAA または認証サーバからサブリカントに割り当てる VLAN ID の情報が得られなかった場合に割り当てる VLAN ID を指定します。省略時は、デフォルト VLAN（VID=1）が設定されます。

こんな事に気をつけて

- AAA/RADIUS サーバから端末（Supplicant）に割り当てる VLAN ID の通知があった場合は、ここで定義された VLAN ID ではなく AAA/RADIUS サーバから通知された VLAN ID が割り当てられます。
- 本設定で設定された VLAN ID と同じ VLAN ID を持つインタフェースを別のポートに対して必ず設定してください。同一 VLAN ID を持つインタフェースがない場合、認証結果にかかわらず認証が失敗します。
- 認証前の状態で登録済みの VLAN ID は、認証成功した端末に割り当てることはできません。（SR-S308TL1/310TL2/316TL1/318TL2/324TL2/316C2/324TC1/328TR1/348TC1/716C2/724TC1/748TC1 の場合）
 - 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
 - 「ether 情報」-「認証共通情報」で、VLAN タグ付きフレームを“透過する”に設定した場合の、タグ VLAN 設定

WOL 転送モード

WOL フレームの転送モードを指定します。端末の電源をリモートから制御する場合は“転送する”を選択します。

許容する EAPOL MAC アドレス

受信を許容する EAPOL フレームのあて先 MAC アドレス種別を以下の3つから選択します。

- PAE グループアドレスのみ
PAE グループアドレス (01:80:c2:00:00:03) をあて先 MAC アドレスに持つ EAPOL フレームのみを受信します。
- PAE グループアドレスとポート MAC アドレス
PAE グループアドレスまたは受信ポートに割り当てられた MAC アドレスをあて先 MAC アドレスに持つ EAPOL フレームのみを受信します。
- PAE グループアドレスとユーザ定義 MAC アドレス
PAE グループアドレスまたは指定された MAC アドレスをあて先 MAC アドレスに持つ EAPOL フレームのみを受信します。本モードを選択した場合は、受信可能な MAC アドレスを必ず指定してください。

6.8 Web 認証関連

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[Web 認証関連]

ether 情報 - ether1 情報	
Web 認証関連	
基本情報	認証不要端末情報

SR-S308TL1、310TL2、316TL1、318TL2、316C2、324TC1、328TR1、348TC1、716C2、724TC1、748TC1 のみ、「認証不要端末情報」が表示されます。

6.8.1 基本情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[Web 認証関連]→[基本情報]

■基本情報

認証機能

☒ 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 ☐ ポートごと

デフォルト割り当て VLAN

1

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
☐ 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

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

認証機能

Web 認証を行う場合は、“使用する”を選択します。

“使用する”を選択した場合、WWW ブラウザを使用して端末を認証し、認証に成功した端末の通信のみを許可することができます。

こんな事に気をつけて

- Web 認証を行うために、AAA ユーザ情報、RADIUS 情報を設定しておく必要があります。
- “使用する”を選択したポートには、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 は指定することはできません。設定された場合はポートが使用できなくなります。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。
 - 「ether 情報」-「認証共通情報」で、VLAN タグ付きフレームを“透過する”に設定した場合の、タグ VLAN 設定

参照する AAA 情報

Web 認証を行う場合に参照する AAA のグループ ID を 0～9 の範囲の 10 進数で指定します。省略時は、0 が設定されます。

認証方式

Web 認証方式を選択します。

こんな事に気をつけて

- 認証方式としてポートごとの認証を選択した場合、そのポートに接続される端末 (Supplicant) の 1 台が認証許可された場合、同じポートに接続されるほかの端末からのアクセスがすべて透過として扱われます。また、認証に成功した端末が使用を終了した場合は、ポートのリンクダウンまたは、“Web 認証有効時間” で指定されたタイミングで、ほかの端末からのアクセスも遮断されます。
- 同一ポートで IEEE802.1X 認証または MAC アドレス認証を同時に有効とする場合は、すべての認証機能の認証方式が同じとなるように設定してください。
(SR-S308TL1/310TL2/316TL1/318TL2/324TL2/
316C2/324TC1/328TR1/348TC1/716C2/724TC1/
748TC1 の場合)

デフォルト割り当て VLAN ID

AAA または認証サーバからサブリカントに割り当てる VLAN ID の情報が得られなかった場合に割り当てる VLAN ID を指定します。

省略時はデフォルト VLAN (VID=1) が設定されます。

こんな事に気をつけて

- AAA/RADIUS サーバから端末 (Supplicant) に割り当てる VLAN ID の通知があった場合は、ここで定義された VLAN ID ではなく、AAA/RADIUS サーバから通知された VLAN ID が割り当てられます。
- 本設定で設定された VLAN ID と同じ VLAN ID を持つインタフェースを別のポートに対して必ず設定してください。同一 VLAN ID を持つインタフェースがない場合は、認証結果にかかわらず認証が失敗します。
- 認証前の状態で登録済みの VLAN ID は、認証成功した端末に割り当てることはできません。
 - Web 認証用のタグなしのポート VLAN
 - 「ether 情報」 - 「認証共通情報」で、VLAN タグ付きフレームを“透過する”に設定した場合の、タグ VLAN 設定

Web 認証有効時間

Web 認証が成功した場合の認証有効時間を指定します。

“エーリアウト後指定時間経過時”を指定した場合、Web 認証完了後、認証端末が MAC アドレス学習テーブルよりエーリアウトしてから 0～60 の範囲で指定した時間が経過した場合に認証を解除します。

“認証完了後指定時間経過時”を指定した場合、Web 認証完了後、5～1500 で指定した時間で認証を解除します。

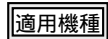
こんな事に気をつけて

Web 認証有効時間の監視は 30 秒間隔で行っているため、認証解除時間には最大 30 秒までの誤差が生じます。

WOL 転送モード

WOL フレームの転送モードを指定します。端末の電源をリモートから制御する場合は“転送する”を選択します。

6.8.2 認証不要端末情報



SR-S308TL1, 310TL2, 316TL1, 318TL2, 324TL2, 316C2, 324TC1, 328TR1, 348TC1, 716C2, 724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[Web 認証関連]→[認証不要端末情報]

■ 認証不要端末情報

※追加・修正情報は一覧ので設定してください。

定義番号	MAC アドレス	VLAN ID	操作
全削除			

< 認証不要端末情報入力フィールド >

MAC アドレス

VLAN ID

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている認証不要端末が表示されています。認証不要端末数は、24 個まで設定できます。
処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

- Web 認証が無効な場合または認証方式としてポートごとの認証を選択した場合は、設定は無効となります。
- 同一 MAC アドレスを複数のポートへ登録することはできません。
- 登録された認証不要端末を、別のポートへ接続した場合は正常に通信できない場合があります。

MAC アドレス

認証しないで通信を許可する端末の MAC アドレスを指定します。

こんな事に気をつけて

00:00:00:00:00:00 およびブロードキャスト、マルチキャストは指定できません。

VLAN ID

認証しないで通信を許可する端末を登録する VLAN ID を 1 ～ 4094 の範囲で指定します。

こんな事に気をつけて

VLAN ID が未登録の場合、設定は無効となります。

6.9 MAC アドレス認証関連

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[MAC アドレス認証関連]

ether 情報 - ether 1 情報	
MAC アドレス認証関連	
基本情報	認証不要端末情報

6.9.1 基本情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[MAC アドレス認証関連]→[基本情報]

■基本情報

認証機能

☒ 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 ☐ ポートごと
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

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

認証機能

MAC アドレス認証を行う場合は、“使用する” を選択します。

“使用する” を選択した場合、パケット送信元端末の MAC アドレス認証を行い、認められた MAC アドレスである場合に中継を行い、認められていなければパケット破棄します。

こんな事に気をつけて

- MAC アドレス認証を行うために、AAA ユーザ情報、RADIUS 情報を設定しておく必要があります。
- “使用する” を選択したポートに VLAN を指定することはできません。設定された場合はポートが使用できなくなります。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
 - 「ether 情報」-「認証共通情報」で、VLAN タグ付きフレームを“透過する”に設定した場合の、タグ VLAN 設定

参照する AAA 情報

MAC アドレス認証を行う場合に参照する AAA のグループ ID を、0～9 の範囲の 10 進数で指定します。

省略時は、0 が設定されます。

こんな事に気をつけて

AAA グループ ID は必須設定項目です。MAC アドレス認証が有効であるポートで AAA グループ ID が未設定の場合は、そのポートは利用できなくなります。

認証方式

MAC アドレス認証方式を選択します。

こんな事に気をつけて

- 認証方式としてポートごとの認証を選択し、そのポートに接続される端末 (Supplicant) の一台が認証許可された場合は、同じポートに接続されるほかの端末からのアクセスがすべて透過として扱われます。また、認証に成功した端末が使用を終了した場合は、学習された MAC アドレスがエージングされるタイミングで、ほかの端末からのアクセスは遮断された状態に戻ります。
- 同一ポートで IEEE802.1X 認証または Web 認証を同時に有効とする場合は、すべての認証機能の認証方式が同じとなるように設定してください。

デフォルト割り当て VLAN ID

AAA または認証サーバからサブリカントに割り当てる VLAN ID の情報が得られなかった場合に割り当てる VLAN ID を指定します。

省略時は、デフォルト VLAN (VID=1) が設定されます。

こんな事に気をつけて

- AAA/RADIUS サーバから端末 (Supplicant) に割り当てる VLAN ID の通知があった場合は、ここで定義された VLAN ID ではなく、AAA/RADIUS サーバから通知された VLAN ID が割り当てられます。
- 本設定で設定された VLAN ID と同じ VLAN ID を持つインタフェースを別のポートに対して必ず設定してください。同一 VLAN ID を持つインタフェースがない場合、認証結果にかかわらず認証が失敗します。
- 認証前の状態で登録済みの VLAN ID は、認証成功した端末に割り当てることはできません。(SR-S308TL1/310TL2/316TL1/318TL2/324TL2/316C2/324TC1/328TR1/348TC1/716C2/724TC1/748TC1 の場合)
 - 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
 - 「ether 情報」 - 「認証共通情報」で、VLAN タグ付きフレームを“透過する”に設定した場合の、タグ VLAN 設定

認証成功保持時間

MAC アドレス認証が成功した場合の保持時間を、60 ～ 86400 秒の範囲で指定します。

認証成功端末で、認証成功保持時間を経過した場合に再認証を実施します。

省略時は、20 分が設定されます。

認証失敗保持時間

MAC アドレス認証が失敗した場合の保持時間を、60 ～ 86400 秒の範囲で指定します。

認証失敗端末で、認証失敗保持時間を経過するまでの間は、再認証を実施しません。

省略時は、5 分が設定されます。

WOL 転送モード

WOL フレームの転送モードを指定します。端末の電源をリモートから制御する場合は“転送する”を選択します。

6.9.2 認証不要端末情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[MAC アドレス認証関連]
→[認証不要端末情報]

■認証不要端末情報
※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	MACアドレス	VLAN ID	操作
全削除			
＜認証不要端末情報入力フィールド＞			
MACアドレス			
VLAN ID			
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている認証不要端末が表示されます。認証不要端末数は、24 個まで設定できます。
処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

- MAC アドレス認証が無効な場合、または認証方式としてポートごとの認証を選択した場合は、設定は無効となります。
- 同一 MAC アドレスを複数のポートへ登録することはできません。
- Web 認証不要端末として設定された MAC アドレスは登録することはできません。(SR-S308TL1/310TL2/316TL1/318TL2/324TL2/316C2/324TC1/328TR1/348TC1/716C2/724TC1/748TC1 の場合)
- 登録された認証不要端末を、別のポートへ接続した場合、正常に通信できないときがあります。
- 同一 etherblock 内で転送許可ポートを設定したポートが存在する場合は、認証不要端末は 1 つ（もっとも小さい定義番号で指定された認証不要端末）だけ設定可能となります。(SR-S208TC2/224TC2/208PD1 の場合)

MAC アドレス

認証しないで通信を許可する端末の MAC アドレスを指定します。

こんな事に気をつけて

00:00:00:00:00:00、ブロードキャストおよびマルチキャストは指定できません。

VLAN ID

認証しないで通信を許可する端末を登録する VLAN ID を 1 ～ 4094 の範囲で指定します。

こんな事に気をつけて

- VLAN ID が未登録の場合、設定は無効となります。
- Web 認証機能を併せて使用したポートでは、Web 認証用の VLAN ID を指定することはできません。
(SR-S308TL1/310TL2/316TL1/318TL2/324TL2/316C2/324TC1/328TR1/348TC1/716C2/724TC1/748TC1 の場合)
- 同一ポート内の認証不要端末は、すべて同一の VLAN ID だけ設定可能となります。
(SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合)

6.10 DHCP スヌープ情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[DHCP スヌープ情報]

■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
☐ すべての端末

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

ポートの通信許可

通信許可する端末を選択します。

こんな事に気をつけて

- DHCP サーバはポートの通信許可を“すべての端末”に設定したポートに接続してください。
- ポートが所属する「VLAN 情報」の DHCP スヌープ情報で、DHCP スヌープ機能が“使用しない”に設定されている場合、このポートでは DHCP スヌープ機能は無効となり、すべての端末が通信可能となります。
- “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のどれかに一致する場合、このポートでは DHCP スヌープ機能は無効となり、すべての端末が通信可能となります。
 - IEEE802.1X 認証、Web 認証、MAC アドレス認証のどれかが有効に設定されている場合
 - 「ポート種別」にリンクアグリゲーションが設定されている場合
 - タグ VLAN が設定されている場合
 - プロトコル 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 の場合)

6.11 フィルタ情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[フィルタ情報]

現在、この ether ポートに設定されているフィルタ定義の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件に一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

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。

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)

参照 「装置情報」-「資源情報」画面は、[\[4.9 資源情報\] \(P33\)](#) を参照してください。

ヒント

◆ フィルタの定義数

● SR-S208TC2/224TC2/208PD1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 30 ルール

● SR-S224PS1/224CP1/248TC1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 60～100 ルール（認証成功端末数による）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合

装置で 128 個

指定された ACL 情報の内容によって装置で 128 ルール

● SR-S316C2/716C2 の場合

ポートごとに 10 個

指定された ACL 情報の内容によってポートごとに 100 ルール

● SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合

装置で 128 個（初期値）

指定された ACL 情報の内容によって装置で 128 ルール（初期値）

定義可能上限値は、「装置情報」-「資源情報」の「フィルタ/QoS 資源の配分」の設定で、最大で 512 個まで拡張することができます。

◆ 優先順位**● SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合**

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (2) 「etherblock 情報」-「フィルタ情報」の設定
- (3) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (4) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (5) 「ether 情報」-「QoS 関連」-「QoS 情報」（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (6) 「etherblock 情報」-「QoS 情報」
- (7) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」-「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (10) 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (11) 「VLAN 情報」-「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S316C2/716C2 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定
- (2) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (4) 「ether 情報」-「QoS 関連」-「QoS 情報」
- (5) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (6) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (7) 「VLAN 情報」-「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」-「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2/324TC1/328TR1/348TC1/724TC1/748TC1 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定
- (2) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）

◆ ルール

● SR-S208TC2/224TC2/208PD1 の場合

ACL の内容によって、以下のように消費するルール数が異なります。

<ルール1>

- 「ether 情報」 - 「フィルタ情報」
- 「etherblock 情報」 - 「フィルタ情報」
- 「VLAN 情報」 - 「フィルタ情報」
- 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- 「etherblock 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「IPv6 フィルタ情報」
- 「VLAN 情報」 - 「IPv6 QoS 情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: TCP または UDP の送信元ポート数 × あて先ポート数 × 2
- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: ICMP の ICMP TYPE の個数 × ICMP CODE の個数 × 2
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: 2
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: 1

<ルール2>

- 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
- 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
- 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

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

ACL の内容によって、以下のように消費するルール数が異なります。それぞれの ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

こんな事に気をつけて

- 自装置 IP アドレスあてパケットや IP オプション付きパケットなど、ソフト処理となるパケットに対する「LAN 情報」-「IP 関連」-「IP フィルタリング情報」設定や「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」設定はスイッチのフィルタ・QoS 設定上限オーバとなった場合も適用されます。
- WWW や DHCP に対するアクセスを制限する設定を行った場合、WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。
- 以下の設定はすべての etherblock に適用されます。(SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合)
 - 「VLAN 情報」-「フィルタ情報」
 - 「VLAN 情報」-「QoS 情報」
 - 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」
 - 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」
 - 「VLAN 情報」-「IPv6 フィルタ情報」
 - 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」
 - 「VLAN 情報」-「IPv6 QoS 情報」
- 当該 etherblock で、IEEE802.1X 認証成功端末、Web 認証成功端末、MAC アドレス認証成功端末および DHCP スヌープ許可端末の合計が 152 台以下の場合、ルールによる上限は etherblock ごとに 100 個となりますが、152 台を超えた場合は 1 認証成功端末につき使用可能なルール数が 1 個減少します。(SR-S224PS1/224CP1/248TC1 の場合)
- 自装置 IP アドレスあてパケットは acl 定義に該当した場合もフィルタされません。自装置 IP アドレスあてパケットは「LAN 情報」-「IP 関連」-「IP フィルタリング情報」で設定してください。(SR-S716C2 の場合)
- "ether macfilter" コマンド、"vlan macfilter" コマンド、"lan ip filter" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 200 個まで設定可能です。(SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合)
- "ether macfilter" コマンド、"ether qos aclmap" コマンド、"vlan macfilter" コマンド、"vlan qos aclmap" コマンド、"lan ip filter" コマンド、"lan ip dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 700 個まで設定可能です。(SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合)

動作

フィルタの動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- MAC 定義
- VLAN 定義
- TCP 定義
IP 定義のプロトコルが 6 の場合にだけ有効です。
- UDP 定義
IP 定義のプロトコルが 17 の場合にだけ有効です。
- ICMP 定義
IP 定義のプロトコルが 1 の場合にだけ有効です。

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[フィルタ情報]→「ACL 定義番号の [参照]」

表示条件入力					
表示個数		表示範囲			
10		0~0			
■ACL 情報					閉じる
定義番号	IP定義	MAC定義	VLAN定義	TCP/UDP/ICMP定義	選択
	プロトコル 送信元IPアドレス/マスク あて先IPアドレス/マスク QoS種別 QoS値	送信元MACアドレス あて先MACアドレス フォーマット種別 LSAP/type値	VLAN ID プライオリティ		
	すべて	bcast	20		
	192.168.1.0/24	bcast	5		
0	any	llc			選択
	any	1fff			
					閉じる

「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」、「MAC 定義情報」および「VLAN 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

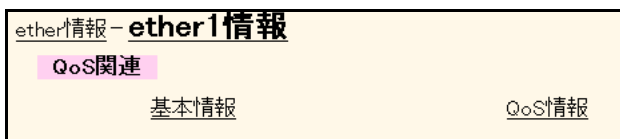
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「フィルタ情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「フィルタ情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

6.12 QoS 関連

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[QoS 関連]



6.12.1 基本情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[QoS 関連]→[基本情報]

SR-S308TL1、310TL2、316TL1、318TL2、324TL2、316C2、324TC1、328TR1、348TC1、716C2、724TC1、748TC1 のみ、「送信アルゴリズム」の項目が表示されます。

ポート優先順位

ether ポートのデフォルトキューの優先度を 0～7 の範囲で選択します。値が大きいほど高優先となります。

送信アルゴリズム (SR-S308TL1、310TL2、316TL1、318TL2、324TL2、316C2、324TC1、328TR1、348TC1、716C2、724TC1、748TC1)

ether ポートの QoS の送信アルゴリズムを選択します。

“Weighted round robin 方式” を選択した場合は、各キューの重みを、0～15 の範囲の 10 進数で指定します。

こんな事に気をつけて

Weighted round robin 方式で重みを 0 に設定したキューは、Strict priority 方式と同じ動作となり、1 以上の重みを設定したキューより優先されます。

6.12.2 QoS 情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[QoS 関連]→[QoS 情報]

現在、この ether ポートに設定されている QoS 処理定義の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件に一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

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。

QoS 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)

☛ 参照 「装置情報」-「資源情報」画面は、[\[4.9 資源情報\] \(P33\)](#) を参照してください。

💡 ヒント

◆ 定義数

- SR-S208TC2/224TC2/208PD1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 30 ルール

- SR-S224PS1/224CP1/248TC1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 60～100 ルール（認証成功端末数による）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合

装置で 128 個

指定された ACL 情報の内容によって装置で 128 ルール

● SR-S316C2/716C2 の場合

ポートごとに 10 個

指定された ACL 情報の内容によってポートごとに 100 ルール

● SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合

装置で 128 個（初期値）

指定された ACL 情報の内容によって装置で 128 ルール（初期値）

定義可能上限値は、「装置情報」-「資源情報」の「フィルタ/QoS 資源の配分」の設定で、最大で 512 個まで拡張することができます。

◆ 優先順位

● SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (2) 「etherblock 情報」-「フィルタ情報」の設定
- (3) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (4) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (5) 「ether 情報」-「QoS 関連」-「QoS 情報」（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (6) 「etherblock 情報」-「QoS 情報」
- (7) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」-「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (10) 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (11) 「VLAN 情報」-「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S316C2/716C2 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定
- (2) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (4) 「ether 情報」-「QoS 関連」-「QoS 情報」
- (5) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (6) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (7) 「VLAN 情報」-「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」-「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2/324TC1/328TR1/348TC1/724TC1/748TC1 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「QoS 関連」-「QoS 情報」
- (2) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）

◆ ルール

● SR-S208TC2/224TC2/208PD1 の場合

ACL の内容によって、以下のように消費するルール数が異なります。

<ルール1>

- 「ether 情報」 - 「フィルタ情報」
- 「etherblock 情報」 - 「フィルタ情報」
- 「VLAN 情報」 - 「フィルタ情報」
- 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- 「etherblock 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「IPv6 フィルタ情報」
- 「VLAN 情報」 - 「IPv6 QoS 情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： TCP または UDP の送信元ポート数 × あて先ポート数 × 2
- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： ICMP の ICMP TYPE の個数 × ICMP CODE の個数 × 2
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： 2
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： 1

<ルール2>

- 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
- 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
- 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

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

ACL の内容によって、以下のように消費するルール数が異なります。それぞれの ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

こんな事に気をつけて

- 自装置 IP アドレスあてパケットや IP オプション付きパケットなど、ソフト処理となるパケットに対する「LAN 情報」-「IP 関連」-「IP フィルタリング情報」設定や「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」設定はスイッチのフィルタ・QoS 設定上限オーバとなった場合も適用されます。
- 以下の設定はすべての etherblock に適用されます。(SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合)
 - 「VLAN 情報」-「フィルタ情報」
 - 「VLAN 情報」-「QoS 情報」
 - 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」
 - 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」
 - 「VLAN 情報」-「IPv6 フィルタ情報」
 - 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」
 - 「VLAN 情報」-「IPv6 QoS 情報」
- 当該 etherblock で、IEEE802.1X 認証成功端末、Web 認証成功端末、MAC アドレス認証成功端末および DHCP スヌープ許可端末の合計が 152 台以下の場合は、ルールによる上限は etherblock ごとに 100 個となりますが、152 台を超えた場合は 1 認証成功端末につき使用可能なルール数が 1 個減少します。(SR-S224PS1/224CP1/248TC1 の場合)
- "ether qos aclmap" コマンド、"vlan qos aclmap" コマンド、"lan ip dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 200 個まで設定可能です。(SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合)
- "ether macfilter" コマンド、"ether qos aclmap" コマンド、"vlan macfilter" コマンド、"vlan qos aclmap" コマンド、"lan ip filter" コマンド、"lan ip dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 700 個まで設定可能です。(SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合)

動作

QoS 処理の動作を以下の 4 つから選択します。

- cos 値書き換え
条件と一致した場合にパケットの cos 値 (Tagged VLAN の Tag Control Information (TCI) フィールドの user priority 値) を書き換えます。
 - cos 値指定
書き換え後の cos 値を 0～7 の範囲の 10 進数で指定します。
 - ip precedence 値
cos 値をパケットの ip precedence 値に書き換えます。
- ip precedence 値書き換え
条件と一致した場合にパケットの ip precedence 値 (IP ヘッダの TOS フィールドの上位 3 ビット) を書き換えます。
 - ip precedence 値指定
書き換え後の ip precedence 値を 0～7 の範囲の 10 進数で指定します。
 - cos 値
ip precedence 値を cos 値に書き換えます。
- dscp 値書き換え
条件と一致した場合にパケットの dscp 値 (IP ヘッダの TOS フィールドの上位 6 ビット) を書き換えます。
書き換え後の dscp 値を 0～63 の範囲の 10 進数で指定します。

- 出力キュー指定
条件と一致した場合にパケットが出力されるときに使用される出力ポートのキューを変更します。
使用する出力ポートのキュー番号を、以下の範囲の 10 進数で指定します。大きい値が出力優先順位がより高いキューであることを表します。

機種	キュー番号
SR-S208TC2、224TC2、 208PD1、224PS1、224CP1、 248TC1、308TL1、310TL2、 316TL1、318TL2、324TL2	0～3
SR-S316C2、716C2、324TC1、 328TR1、348TC1、724TC1、 748TC1	0～7

ACL 定義番号

〔参照〕 ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- MAC 定義
- VLAN 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の〔選択〕 ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。〔OK〕 ボタンをクリックして、設定をやり直してください。

〔操作〕 「設定メニュー」→詳細設定「ether 情報」→〔修正〕→〔QoS 関連〕→〔QoS 情報〕
→「ACL 定義番号の〔参照〕」

表示条件入力					
表示回数		表示範囲			
10		0~0			
■ACL 情報 閉じる					
定義番号	IP 定義	MAC 定義	VLAN 定義	TCP/UDP/ICMP 定義	選択
	プロトコル 送信元IPアドレス/マスク あて先IPアドレス/マスク QoS種別 QoS値	送信元MACアドレス あて先MACアドレス フォーマット種別 LSAP/type値	VLAN ID プライオリティ		
0	すべて	bcast	20		選択
	192.168.1.0/24	bcast	5		
	any	llc			
	any	1fff			
					閉じる

「ACL 情報」-〔追加〕／〔修正〕-「IP 定義情報」、「MAC 定義情報」および「VLAN 定義情報」で設定した ACL 定義が表示されています。ここに表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示回数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。〔OK〕 ボタンをクリックして、設定をやり直してください。

「QoS 情報」の ACL 定義番号に設定する定義番号欄の〔選択〕 ボタンをクリックすると、「QoS 情報」に ACL 定義番号が設定され、画面が閉じます。〔ACL 定義参照〕 ボタンをクリックした場合は、〔選択〕 ボタンは表示されません。〔閉じる〕 ボタンをクリックして、画面を閉じてください。

6.13 接続先監視情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[接続先監視情報]

接続先監視

ether ポートで接続先監視機能として ether L3 監視機能を使用する場合は、“使用する”を選択します。ether L3 監視機能は監視ポートから ICMP ECHO パケットを送信し、監視先相手の応答の有無で生存を確認します。一定時間、応答が返って来なかった場合は、監視異常とし、監視ポートを閉塞させます。

“使用する”を選択した場合は、以下の設定をしてください。

こんな事に気をつけて

- ether のポート種別がリンクアグリゲーションポートの場合、「リンクアグリゲーショングループ情報」の「接続先監視情報」で接続先監視を設定してください。
- この機能を使用する場合は、自装置に IP アドレスを設定してください。
- IEEE802.1X 認証、Web 認証、MAC アドレス認証のどれかが有効に設定されているポートでは、ether L3 監視機能は正常に動作しません。
- 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。

あて先 IP アドレス

監視対象となる接続先の IP アドレスを指定します。IP アドレスは、以下の範囲で指定します。

有効範囲)

1.0.0.1 ～ 126.255.255.254

128.0.0.1 ～ 191.255.255.254

192.0.0.1 ～ 223.255.255.254

こんな事に気をつけて

- あて先 IP アドレスに自装置の IP アドレスを指定しないでください。自装置の IP アドレスを設定した場合は、ether L3 監視機能は正常に動作しません。
- あて先 IP アドレスには ether L3 監視を使用する ether ポートに設定した IP アドレスと異なったネットワークのアドレスを指定しないでください。異なったネットワークアドレスを指定した場合は、ether L3 監視機能は正常に動作しません。

正常時送信間隔

ICMP ECHO パケットの応答が正常に受信されている状態で、次に ICMP ECHO パケットを送信する間隔を、1 ～ 60 秒の範囲の 10 進数で指定します。

省略時は、10 秒が設定されます。

タイムアウト時間

ICMP ECHO パケット送信から生存確認失敗とするまでの時間を、5 ～ 180 秒の範囲の 10 進数で指定します。タイムアウト時間までに応答がない場合は、異常を検出します。

省略時は、5 秒が設定されます。

こんな事に気をつけて

STP 機能を使用している場合は、タイムアウト時間を長めに設定してください。

再送間隔

ICMP ECHO パケットの正常時の送信に対して応答がない場合、ICMP ECHO パケットを再送する間隔を、1 ～ (タイムアウト時間 - 1) 秒の範囲の 10 進数で指定します。

省略時は、1 秒が設定されます。

6.14 トラップ情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[トラップ情報]

■トラップ情報

linkDown

☒有効にする
 ☐無効にする

linkUp

☒有効にする
 ☐無効にする

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

トラップ情報

以下の各トラップを有効にするか無効にするかを選択します。

- linkDown
SNMP ホストに対して linkDown トラップを通知します。
SNMP エージェント機能を使用しない場合は、この設定は意味を持ちません。
- linkUp
SNMP ホストに対して linkUp トラップを通知します。
SNMP エージェント機能を使用しない場合は、この設定は意味を持ちません。

6.15 L2 暗号関連

適用機種 SR-S224CP1

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[L2 暗号関連]

ether 情報 - **ether 27 情報**

L2 暗号関連

基本情報 暗号化条件

6.15.1 基本情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[L2 暗号関連]→[基本情報]

■基本情報

暗号機能 (送信用)	暗号アルゴリズム	暗号化しない ▼
	暗号鍵 鍵識別	☒ 16進数 ☐ 文字列
	暗号鍵 鍵	
	認証鍵 鍵識別	☒ 16進数 ☐ 文字列
認証鍵 鍵		
復号機能 (受信用)	暗号アルゴリズム	暗号化しない ▼
	暗号鍵 鍵識別	☒ 16進数 ☐ 文字列
	暗号鍵 鍵	
	認証鍵 鍵識別	☒ 16進数 ☐ 文字列
認証鍵 鍵		

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

暗号機能（送信用）／ 復号機能（受信用）

暗号機能の場合は、送信フレームを暗号処理するかどうかを指定します。

復号機能の場合は、受信フレームを復号処理するかどうかを指定します。

暗号アルゴリズム

暗号アルゴリズムを選択します。“暗号化しない”を選択した場合は、フレームの暗号化／復号化を行いません。

暗号鍵

鍵識別

鍵の識別を指定します。

鍵

暗号アルゴリズムで使用する暗号鍵を 16 進数および文字列を使用して、以下の範囲で指定します。

暗号アルゴリズム	入力範囲	
	16 進数鍵	文字列鍵
AES-STR-128	1 ～ 32 桁	16 文字
AES-STR-192	1 ～ 48 桁	24 文字
AES-STR-256	1 ～ 64 桁	32 文字

16 進数指定で最大桁数に満たない場合は、自動的に “0” でパディングされます。

文字列で指定する場合は、各アルゴリズムの入力範囲の鍵長で指定してください。

認証鍵

鍵識別

鍵の識別を指定します。

鍵

認証アルゴリズムは AES-XCBC を使用します。認証鍵を 16 進数および文字列を使用して、以下の範囲で指定します。

認証アルゴリズム	入力範囲	
	16 進数鍵	文字列鍵
AES-XCBC	1 ～ 32 桁	16 文字

16 進数指定で最大桁数に満たない場合は、自動的に “0” でパディングされます。

文字列で指定する場合は、16 文字固定の鍵長で指定してください。

こんな事に気をつけて

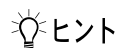
暗号処理／復号処理を行う場合は、暗号鍵および認証鍵の設定が必要です。

6.15.2 暗号化条件

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[L2 暗号関連]→[暗号化条件]

現在、この ether ポートに設定されている暗号化条件の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にフレームのチェックを行い、すべての条件に一致した場合に定義された動作を行います。



ヒント

◆ 暗号化条件の定義数

暗号条件の定義は 200 個まで定義できますが、適用される暗号条件定義は、指定された ACL 情報の内容によってポートごとに 200 ルールまでとなります。

◆ ルール

ACL の内容によって、以下のように消費するルール数が異なります。それぞれの ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数×あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数× ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

動作

動作を以下の 2 つから選択します。

- 暗号化する
条件と一致した場合にフレームを暗号化して送信します。
- 暗号化しない
条件と一致した場合にフレームを暗号化しないで送信します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- MAC 定義

- VLAN 定義
- IP 定義
- IPv6 定義
- TCP 定義
IP 定義および IPv6 定義のプロトコルが 6 の場合にだけ有効です。
- UDP 定義
IP 定義および IPv6 定義のプロトコルが 17 の場合にだけ有効です。
- ICMP 定義
IP 定義のプロトコルが 1 の場合または、IPv6 定義のプロトコルが 58 の場合にだけ有効です。

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] 「設定メニュー」→詳細設定「ether情報」→[修正]→[L2暗号関連]→[暗号化条件]
→[ACL定義番号の[参照]]

表示条件入力					
表示個数		表示範囲			
10		0~0			
■ACL情報					開じる
定義番号	IP定義	IPv6定義	MAC定義	VLAN定義	TCP/UDP/ICMP定義
	プロトコル 送信元IPアドレス/マスク あて先IPアドレス/マスク QoS種別 QoS値	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 QoS種別 QoS値	送信元MACアドレス あて先MACアドレス フォーマット種別 LSAP/type値	VLAN ID プライオリティ	
0	すべて		any		
	any		01:80:c2:00:00:00		
	any		any		
	any				

閉じる

「ACL情報」- [追加] / [修正] - 「IP定義情報」、「MAC定義情報」で設定したACL定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL定義情報の一覧に見たい情報だけを表示させることができます。

参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「暗号化条件」のACL定義番号に設定する定義番号欄の[選択] ボタンをクリックすると、「暗号化条件」にACL定義番号が設定され、画面が閉じます。[ACL定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

6.16 IEEE802.1ad 関連

適用機種 SR-S328TR1

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[IEEE802.1ad 関連]

ether 情報 - **ether 1 情報**

IEEE802.1ad 関連

基本情報 VLANタグマッピングルール情報

6.16.1 基本情報

6.16.1.1 基本情報（初期表示またはプロバイダーポート選択時）

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[IEEE802.1ad 関連]
→[基本情報（IEEE802.1ad 機能：初期表示またはプロバイダーポート）]

■基本情報

IEEE802.1ad 機能

☒ 動作しない
☐ カスタマーポート
☐ プロバイダーポート

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

初期表示または IEEE802.1ad 機能に“プロバイダーポート”を選択した場合に表示されます。

IEEE802.1ad 機能

ether ポートの IEEE802.1ad 機能の動作を選択します。

- 動作しない
IEEE802.1ad 機能が動作しません。
- カスタマーポート
カスタマーポートとして動作します。
- プロバイダーポート
プロバイダーポートとして動作します。

こんな事に気をつけて

- ether ポートのポート種別がリンクアグリゲーションを指定した場合、本設定は無効となります。
- “カスタマーポート”を選択したポートに VLAN を指定することはできません。設定された場合はポートが使用できなくなります。
- “プロバイダーポート”を選択した場合、プロバイダネットワーク側で使用するサービス VLAN を Tagged VLAN に指定してください。

6.16.1.2 基本情報（カスタマーポート選択時）

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[IEEE802.1ad 関連]
→[基本情報（IEEE802.1ad 機能：カスタマーポート）]

IEEE802.1ad 機能に“カスタマーポート”を選択した場合に表示されます。

「IEEE802.1ad 機能」の項目は、「IEEE802.1ad 機能（初期表示またはプロバイダーポート選択時）」を参照してください。

VLAN タグマッピングルールデフォルト動作

VLAN タグマッピングルール情報で指定した VLAN タグマッピングルールに一致しなかったフレームの動作を指定します。

- 破棄する
フレームを破棄します。
- 転送する
フレームを転送します。

VLAN タグマッピングルール番号

[参照] ボタンをクリックすると、有効な VLAN タグマッピングルール情報が表示されます。
“転送する”を選択した場合に、使用する VLAN タグマッピングルールを選択してください。

こんな事に気をつけて

VLAN タグマッピングルールの適用には条件があります。
装置やポートでの適用可能上限を超えた場合は適用されません。適用条件は、機能説明書「[VLAN タグマッピングルールの適用条件](#)」(P.145) を参照してください。

6.16.2 VLAN タグマッピングルール情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[IEEE802.1ad 関連]
→[VLAN タグマッピングルール情報]

現在、この ether ポートに設定されている VLAN タグマッピングルール定義の一覧です。

装置全体で 4000 個まで設定できます。カスタマーポートで使用する、VLAN タグマッピングルール番号を指定します。
処理するボタンをクリックし、次のページへ進みます。

マッピングルール番号

[参照] ボタンをクリックして、VLAN タグマッピングルール定義番号を指定します。別の画面に「IEEE802.1ad 情報」で設定した VLAN タグマッピングルール 定義が表示されます。

こんな事に気をつけて

- VLAN タグマッピングルールの適用には条件があります。装置やポートにおける適用可能上限を超えた場合は適用されません。適用条件は、機能説明書「[VLAN タグマッピングルールの適用条件](#)」(P.145) を参照してください。
- 設定したマッピングルールの“カスタマー VLAN ID”が重複する場合、定義番号が小さいほうが有効となり定義番号が大きいほうは無効となります。

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[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の [参照]」

表示条件入力		
表示回数 10	表示範囲 0~0	
■VLANタグマッピングルール情報 開じる		
マッピングルール番号	説明文	操作
0	カスタマーVLAN ID サービスVLAN ID -	選択
	500	
開じる		

「IEEE802.1ad 情報」-「VLAN タグマッピングルール情報」で設定した VLAN タグマッピングルール定義情報が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示回数および表示範囲を指定することができます。設定することによって、VLAN タグマッピングルール定義情報の一覧に見たい情報だけを表示させることができます。

参照する VLAN タグマッピングルール情報が存在しない場合は、「参照可能な VLAN タグマッピングルール情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「VLAN タグマッピングルール情報」のマッピングルール番号に設定する定義番号欄の [選択] ボタンをクリックすると、入力フィールドに選択した番号が表示されます。[追加] ボタンをクリックすると、「VLAN タグマッピングルール情報」に追加されます。

6.17 IEEE802.1ah 関連

適用機種 SR-S328TR1

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[IEEE802.1ah 関連]

ether 情報 - **ether 1 情報**

IEEE802.1ah 関連

基本情報 カスタマーバックボーンサービス情報 プロバイダーバックボーンサービス情報

6.17.1 基本情報

6.17.1.1 基本情報（初期表示またはプロバイダーポート選択時）

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[IEEE802.1ah 関連]
→[基本情報（IEEE802.1ah 機能：初期表示またはプロバイダーポート）]

■基本情報

IEEE802.1ah 機能

☒ 動作しない
☐ カスタマーポート
☐ プロバイダーポート

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

初期表示または IEEE802.1ah 機能に“プロバイダーポート”を選択した場合に表示されます。

IEEE802.1ah 機能

ether ポートでの IEEE802.1ah 機能の動作を設定します。

- 動作しない
IEEE802.1ah 機能が動作しません。
- カスタマーポート
カスタマーポートとして動作します。
- プロバイダーポート
プロバイダーポートとして動作します。

こんな事に気をつけて

- ether ポートのポート種別がリンクアグリゲーションポートの場合、本設定は無効になります。リンクアグリゲーション情報の IEEE802.1ah 機能に設定してください。
- “カスタマーポート”を選択したポートに VLAN を指定することはできません。設定された場合はポートが使用できなくなります。
- “プロバイダーポート”を選択した場合、プロバイダネットワーク側で使用するバックボーン VLAN を Tagged VLAN に指定してください。

6.17.1.2 基本情報（カスタマーポート選択時）

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[IEEE802.1ah 関連]
→[基本情報（IEEE802.1ah 機能：カスタマーポート）]

■基本情報

IEEE802.1ah機能	☐ 動作しない ☒ カスタマーポート ☐ プロバイダーポート
バックボーンサービスデフォルト動作	☒ 破棄する ☐ 転送する バックボーンサービスID 参照
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 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

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

IEEE802.1ah 機能に“カスタマーポート”を選択した場合に表示されます。

「IEEE802.1ah 機能」の項目は、「IEEE802.1ah 機能（初期表示またはプロバイダーポート選択時）」を参照してください。

バックボーンサービスデフォルト動作

カスタマーバックボーンサービス情報のバックボーンサービス ID で指定されたサービス VLAN に一致しなかったフレームの動作を指定します。

- 破棄する
フレームを破棄します。
- 転送する
フレームを転送します。

バックボーンサービス ID

参照ボタンをクリックすると、有効なバックボーンサービス ID 情報が表示されます。デフォルト動作で“転送する”を選択した場合に使用するバックボーンサービス ID を選択してください。

こんな事に気をつけて

バックボーンサービス ID の適用には条件があります。装置やポートでの適用可能上限を超えた場合は適用されません。適用条件は機能説明書「[バックボーンサービスの適用条件について](#)」(P.148) を参照してください。

Tag モード

カスタマーポートで転送対象とする Tag モードを設定します。

- サービス VLAN
「IEEE802.1ah 情報」の“サービス VLAN タグプロトコル ID”で設定されたタグプロトコル ID を、転送対象のタグプロトコル ID とします。
- カスタマー VLAN
“8100”を転送対象のタグプロトコル ID とします。

STP BPDU トンネリング

STP の L2 トンネリング動作の設定を行います。

- 無効にする
BPDU (STP) トンネリング動作を無効にします。
- 有効にする
BPDU (STP) トンネリング動作を有効にします。

優先順位

バックボーンVLANに割り当てる優先順位を選択します。

こんな事に気をつけて

IEEE802.1ah 機能の動作に“カスタマーポート”を設定した場合のみ有効となります。

LACPDU トンネリング

LACP の L2 トンネリング機能の設定を行います。

- 無効にする
LACPDU トンネリング動作を無効にします。
- 有効にする
LACPDU トンネリング動作を有効にします。

優先順位

バックボーンVLANに割り当てる優先順位を選択します。

こんな事に気をつけて

IEEE802.1ah 機能の動作に“カスタマーポート”を設定した場合のみ有効となります。

LLDPDU トンネリング

LLDP の L2 トンネリング機能の設定を行います。

- 無効にする
LLDPDU トンネリング動作を無効にします。
- 有効にする
LLDPDU トンネリング動作を有効にします。

優先順位

バックボーンVLANに割り当てる優先順位を選択します。

こんな事に気をつけて

- IEEE802.1ah 機能の動作に“カスタマーポート”を設定した場合のみ有効となります。
- 本設定を有効に設定する場合は、「ether 情報」の「LLDP 機能」を使用しないでください。「LLDP 機能」を“使用する”に設定してある場合、本設定は無効となります。

6.17.2 カスタマーバックボーンサービス情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正] → [IEEE802.1ah 関連]
→ [カスタマーバックボーンサービス情報]

表示条件入力

表示個数
10

表示範囲
カスタマーバックボーンサービス定義は存在しません

■カスタマーバックボーンサービス情報

※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	バックボーンサービスID	操作
全削除		

<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

参照

追加

キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、この ether ポートに設定されているカスタマーバックボーンサービス情報の一覧です。装置全体で 4000 個まで設定できます。カスタマーポートで使用する、バックボーンサービス ID を指定します。
処理するボタンをクリックし、次のページへ進みます。

バックボーンサービスID

[参照] ボタンをクリックすると、有効なバックボーンサービスID情報が表示されます。カスタマーポートで設定するバックボーンサービスIDを選択してください。

こんな事に気をつけて

- 本設定で指定したバックボーンサービスIDで、“サービスVLAN ID” の設定がない場合は無効となります。
- 同一ポートで指定したバックボーンサービスIDの「IEEE802.1ah 情報」 - 「バックボーンサービス関連」の“サービスVLAN ID” が重複する場合、定義番号の小さいほうが有効となり定義番号の大きいほうは無効となります。
- バックボーンサービスIDの適用には条件があります。装置やポートでの適用可能上限を超えた場合は適用されません。適用条件は、機能説明書「[バックボーンサービスの適用条件について](#)」(P.148) を参照してください。

[操作] 「設定メニュー」→詳細設定「ether情報」→[修正]→[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の [参照]」

表示条件入力			
表示個数		表示範囲	
10		0~0	
■バックボーンサービス情報 開じる			
サービスID	説明文		操作
	インスタンスID		
	サービスVLAN ID		
	バックボーンVLAN ID		
0	100		選択
	100		
	300		
開じる			

「IEEE802.1ah 情報」 - 「バックボーンサービス関連」で設定したバックボーンサービス定義情報が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、カスタマーバックボーンサービス定義情報の一覧に見たい情報だけを表示させることができます。

参照するVLANタグマッピングルール情報が存在しない場合は、「参照可能なバックボーンサービス情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「カスタマーバックボーンサービス情報」のバックボーンサービスIDに設定する定義番号欄の[選択] ボタンをクリックすると、入力フィールドに選択した番号が表示されます。[追加] ボタンをクリックすると、「カスタマーバックボーンサービス情報」に追加されます。

6.17.3 プロバイダーバックボーンサービス情報

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[IEEE802.1ah 関連]
→[プロバイダーバックボーンサービス情報]

現在、この ether ポートに設定されているプロバイダーバックボーンサービス情報の一覧です。
装置全体で 2000 個まで設定できます。プロバイダーポートで使用する、バックボーンサービス ID を指定します。
処理するボタンをクリックし、次のページへ進みます。

バックボーンサービス ID

[参照] ボタンをクリックすると、有効なバックボーンサービス ID 情報が表示されます。プロバイダーポートで設定するバックボーンサービス ID を選択してください。

こんな事に気をつけて

- 本設定で指定したバックボーンサービス ID で、“バックボーン VLAN ID” および “バックボーンアて先 MAC アドレス” の設定がない場合は無効となります。
- バックボーンサービス ID の適用には条件があります。装置やポートでの適用可能上限を超えた場合は適用されません。適用条件は、機能説明書「[バックボーンサービスの適用条件について](#)」(P.148) を参照してください。

[操作] 「設定メニュー」→詳細設定「ether 情報」→[修正]→[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の[参照]」

表示条件入力		
表示個数		表示範囲
10		0~0
バックボーンサービス情報 開じる		
サービスID	説明文	操作
0	インスタンスID	選択
	サービスVLAN ID	
	バックボーンVLAN ID	
	100	選択
	100	
	300	
開じる		

「IEEE802.1ah 情報」-「バックボーンサービス関連」で設定したバックボーンサービス定義情報が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、プロバイダーバックボーンサービス定義情報の一覧に見たい情報だけを表示させることができます。

参照する VLAN タグマッピングルール情報が存在しない場合は、「参照可能なバックボーンサービス情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「プロバイダーバックボーンサービス情報」のバックボーンサービスIDに設定する定義番号欄の[選択] ボタンをクリックすると、入力フィールドに選択した番号が表示されます。[追加] ボタンをクリックすると、「プロバイダーバックボーンサービス情報」に追加されます。

7 リンクアグリゲーショングループ情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「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情報
 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情報

グループ番号	動作モード	負荷分散アルゴリズム	バックアップグループ番号	バックアップポート優先度	操作
1	static	both-mac			修正 初期化
2	static	both-mac			修正 初期化
3	static	both-mac			修正 初期化
4	static	both-mac			修正 初期化
5	static	both-mac			修正 初期化
6	static	both-mac			修正 初期化
7	static	both-mac			修正 初期化
8	static	both-mac			修正 初期化

全初期化

保存した情報は、設定反映後に有効になります。

リンクアグリゲーショングループの一覧が表示されています。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]

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

接続先監視情報

IEEE802.1ad関連

IEEE802.1ah関連

SR-S328TR1 のみ、「IEEE802.1ad 関連」および「IEEE802.1ah 関連」が表示されます。

7.1 基本情報

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]→[基本情報]

■基本情報

動作モード

static

負荷分散アルゴリズム

both-mac

最小メンバーポート数

1

バックアップ

☒ 使用しない
☐ 使用する

バックアップグループ番号

1

バックアップポート優先度

☒ 優先ポート
☐ 待機ポート

リンクダウン連携

☒ 使用しない
☐ 使用する

連携ポートリスト

リンクアップ時の動作

☒ 閉塞解除しない
☐ 閉塞解除する

閉塞要因

☒ リンクダウン連携
☐ すべて

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

動作モード

リンクアグリゲーション動作モードを以下から選択します。

- static
静的動作
- active
LACP を使用した動的な active 動作
- passive
LACP を使用した動的な passive 動作

負荷分散アルゴリズム

リンクアグリゲーションの負荷分散アルゴリズムを以下から選択します。

- sa-mac
送信元 MAC アドレスによる振り分け
- da-mac
送信先 MAC アドレスによる振り分け
- both-mac
送信元 MAC アドレスと送信先 MAC アドレスの XOR による振り分け
- sa-ip
送信元 IP アドレスによる振り分け
- da-ip
送信先 IP アドレスによる振り分け
- both-ip
送信元 IP アドレスと送信先 IP アドレスの XOR による振り分け

最小メンバポート数

リンクアグリゲーションを通信可能とさせる最小メンバポート数を選択します。

冗長構成などでリンクアグリゲーションをある帯域が確保できるまで通信させたくない場合に使用します。ある帯域を下回る場合はリンクアグリゲーションを通信不能にします。

バックアップ

リンクアグリゲーションをバックアップとして使用する場合は、“使用する”を選択します。“使用する”を選択した場合は、以降の“バックアップグループ番号”および“バックアップポート優先度”を設定してください。

バックアップグループ番号

バックアップグループ番号を選択します。

こんな事に気をつけて

- ・ 同一バックアップグループで“優先ポート”または“待機ポート”と設定されたポートと同じ優先度のリンクアグリゲーションが存在する場合は、バックアップポートとしてポートが有効となり、リンクアグリゲーションは無効となります。
- ・ 同一バックアップグループで“優先ポート”または“待機ポート”と設定されたリンクアグリゲーションが複数存在する場合は、リンクアグリゲーショングループ番号の小さいリンクアグリゲーションが有効となり、リンクアグリゲーショングループ番号の大きいリンクアグリゲーションは無効となります。
- ・ 同一バックアップグループで“優先ポート”または“待機ポート”がポートおよびリンクアグリゲーションで未設定の場合にそのバックアップグループは無効になります。

バックアップポート優先度

優先度として“優先ポート”または“待機ポート”を選択します。

リンクダウン連携

このリンクアグリゲーションポートでリンクダウン連携を使用する場合は、“使用する”を選択します。“使用する”を選択した場合は、以降の“連携ポートリスト”、“リンクアップ時の動作” および“閉塞要因”を設定してください。

こんな事に気をつけて

リンクアグリゲーションの種別がバックアップリンクアグリゲーションで、バックアップポートのリンクダウン連携の連携ポートリスト情報設定がある場合は、バックアップポートのリンクダウン連携機能が有効となり、本定義は無視されます。

連携ポートリスト

このポートインタフェースがリンクダウンしたときに連携してリンクダウン（ポート閉塞）させるポートリストを、以下の範囲の10進数で指定します。

機種	ポートリスト
SR-S208TC2、308TL1	1～9
SR-S224TC2	1～26
SR-S208PD1、310TL2	1～10
SR-S224PS1、224CP1、328TR1	1～28
SR-S248TC1、348TC1、748TC1	1～52
SR-S316TL1、318TL2	1～18
SR-S324TL2	1～24
SR-S316C2、716C2	1～16
SR-S324TC1、724TC1	1～26

ポートリストを複数指定する場合は、“,”で区切ります。範囲指定の場合は“-”で区切ります。省略時は、該当ポートがリンクダウンしても 連携動作しません。

こんな事に気をつけて

この設定項目が省略されている場合は、連携動作しないため、以降の“リンクアップ時の動作”項目の設定内容は適用されません。

リンクアップ時の動作

本定義ポートがリンクアップしたときに、連携ポートリストに設定した、ポートの閉塞状態の解除を行うかどうかを選択します。

- 閉塞解除しない
リンクアップ時に閉塞状態の解除を行いません。
- 閉塞解除する
リンクアップ時に閉塞状態の解除を行います。本設定を選択した場合は、以降の“解除対象の要因”を設定してください。

こんな事に気をつけて

“閉塞解除しない”、“閉塞解除する”のどちらを選択しても「操作メニュー」の「閉塞／閉塞解除」設定によって連携ポートリストの閉塞状態の解除が可能です。

閉塞要因

リンクアップ時に、連携ポートリストに設定されたポートの閉塞状態の解除を行う場合に、解除対象とする閉塞要因を選択します。

- リンクダウン連携
連携ポートリストの閉塞状態がリンクダウン連携による閉塞要因のみ解除対象に指定します。
- すべて
連携ポートリストの閉塞状態の閉塞要因に依存しないで解除対象に指定します。

こんな事に気をつけて

連携ポートリストに設定されたポートに対する動的定義反映時には、設定に依存しないで閉塞状態の解除が行われます。

7.2 接続先監視情報

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]
→[接続先監視情報]

■接続先監視情報

接続先監視

☒ 使用しない
☐ 使用する

あて先IPアドレス
 正常時送信間隔 10 秒
 タイムアウト時間 5 秒
 再送間隔 1 秒

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

接続先監視

ether ポートで接続先監視機能として ether L3 監視機能を使用する場合は、“使用する”を選択します。ether L3 監視機能は監視ポートから ICMP ECHO パケットを送信し、監視先相手の応答の有無で生存を確認します。一定時間、応答が返って来なかった場合は、監視異常とし、監視ポートを閉塞させます。

“使用する”を選択した場合は、以下の設定をしてください。

こんな事に気をつけて

- この機能を使用する場合は、自装置に IP アドレスを設定してください。
- IEEE802.1X 認証、Web 認証、MAC アドレス認証のどれかが有効に設定されているポートでは、ether L3 監視機能は正常に動作しません。
- 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。

あて先 IP アドレス

監視対象となる接続先の IP アドレスを指定します。IP アドレスは、以下の範囲で指定します。

有効範囲)

1.0.0.1 ～ 126.255.255.254

128.0.0.1 ～ 191.255.255.254

192.0.0.1 ～ 223.255.255.254

こんな事に気をつけて

- あて先 IP アドレスに自装置の IP アドレスを指定しないでください。自装置の IP アドレスを設定した場合は、ether L3 監視機能は正常に動作しません。
- あて先 IP アドレスには ether L3 監視を使用する ether ポートに設定した IP アドレスと異なったネットワークのアドレスを指定しないでください。異なったネットワークアドレスを指定した場合は、ether L3 監視機能は正常に動作しません。

正常時送信間隔

ICMP ECHO パケットの応答が正常に受信されている状態で、次に ICMP ECHO パケットを送信する間隔を、1 ～ 60 秒の範囲の 10 進数で指定します。

省略時は、10 秒が設定されます。

タイムアウト時間

ICMP ECHO パケット送信から生存確認失敗とするまでの時間を、5 ～ 180 秒の範囲の 10 進数で指定します。タイムアウト時間までに応答がない場合は、異常を検出します。

省略時は、5 秒が設定されます。

こんな事に気をつけて

STP 機能を使用している場合は、タイムアウト時間を長めに設定してください。

再送間隔

ICMP ECHO パケットの正常時の送信に対して応答がない場合、ICMP ECHO パケットを再送する間隔を、1 ～ (タイムアウト時間 - 1) 秒の範囲の 10 進数で指定します。

省略時は、1 秒が設定されます。

7.3 IEEE802.1ad 関連

適用機種 SR-S328TR1

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]
→[IEEE802.1ad 関連]

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

VLAN タグマッピングルール情報

7.3.1 基本情報

7.3.1.1 基本情報（初期表示およびプロバイダーポート選択時）

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]
→[IEEE802.1ad 関連]→[基本情報（IEEE802.1ad 機能：初期表示またはプロバイダーポート）]

■ 基本情報

IEEE802.1ad 機能

☒ 動作しない
☐ カスタマーポート
☐ プロバイダーポート

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

初期表示または IEEE802.1ad 機能に“プロバイダーポート”を選択した場合に表示されます。

IEEE802.1ad 機能

リンクアグリゲーションの IEEE802.1ad 機能の動作を選択します。

- 動作しない
IEEE802.1ad 機能が動作しません。
- カスタマーポート
カスタマーポートとして動作します。
- プロバイダーポート
プロバイダーポートとして動作します。

こんな事に気をつけて

- “カスタマーポート”を選択したリンクアグリゲーションのメンバポートに VLAN を指定することはできません。設定された場合はポートが使用できなくなります。
- “プロバイダーポート”を選択した場合、リンクアグリゲーションのメンバポートにプロバイダネットワーク側で使用するサービス VLAN を Tagged VLAN に指定してください。

7.3.1.2 基本情報（カスタマーポート選択時）

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]
→[IEEE802.1ad 関連]→[基本情報（IEEE802.1ad 機能：カスタマーポート）]

IEEE802.1ad 機能に“カスタマーポート”を選択した場合に表示されます。

「IEEE802.1ad 機能」の項目は、「IEEE802.1ad 機能（初期表示またはプロバイダーポート選択時）」を参照してください。

VLAN タグマッピングルールデフォルト動作

VLAN タグマッピングルール情報で指定した VLAN タグマッピングルールに一致しなかったフレームの動作を指定します。

- 破棄する
フレームを破棄します。
- 転送する
フレームを転送します。

VLAN タグマッピングルール番号

[参照] ボタンをクリックすると、有効な VLAN タグマッピングルール情報が表示されます。

“転送する”を選択した場合に、使用する VLAN タグマッピングルールを選択してください。

こんな事に気をつけて

VLAN タグマッピングルールの適用には条件があります。装置やポートにおける適用可能上限を超えた場合は適用されません。適用条件は、機能説明書「[VLAN タグマッピングルールの適用条件](#)」(P.145)を参照してください。

7.3.2 VLAN タグマッピングルール情報

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]
→[IEEE802.1ad 関連]→[VLAN マッピングルール情報]

現在、このリンクアグリゲーショングループに設定されている VLAN タグマッピングルール定義の一覧です。
装置全体で 4000 個まで設定できます。カスタマーポートで使用する、VLAN タグマッピングルール番号を指定します。
処理するボタンをクリックし、次のページへ進みます。

マッピングルール番号

[参照] ボタンをクリックして、VLAN タグマッピングルール定義番号を指定します。別の画面に「IEEE802.1ad 情報」で設定した VLAN タグマッピングルール 定義が表示されます。

こんな事に気をつけて

- VLAN タグマッピングルールの適用には条件があります。装置やポートにおける適用可能上限を超えた場合は適用されません。適用条件は、機能説明書「[VLAN タグマッピングルールの適用条件](#)」(P.145) を参照してください。
- 設定したマッピングルールの“カスタマー VLAN ID”が重複する場合、定義番号が小さいほうが有効となり定義番号が大きいほうは無効となります。

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]
→[IEEE802.1ad 関連]→[基本情報 (IEEE802.1ad 機能：カスタマーポート)]
→「マッピングルール番号の [参照]」

表示条件入力		
表示個数	表示範囲	
10	0~1	
■VLANタグマッピングルール情報 閉じる		
マッピングルール番号	説明文	操作
	カスタマーVLAN ID	
	サービスVLAN ID	
0	10 1000	選択
1	20,30 2000	選択
閉じる		

「IEEE802.1ad 情報」-「VLAN タグマッピングルール情報」で設定した VLAN タグマッピングルール定義情報が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、VLAN タグマッピングルール情報の一覧に見たい情報だけを表示させることができます。

参照する VLAN タグマッピングルール情報が存在しない場合は、「参照可能な VLAN タグマッピングルール情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「VLAN タグマッピングルール情報」のマッピングルール番号に設定する定義番号欄の [選択] ボタンをクリックすると、入力フィールドに選択した番号が表示されます。[追加] ボタンをクリックすると、「VLAN タグマッピングルール情報」に追加されます。

7.4 IEEE802.1ah 関連

適用機種 SR-S328TR1

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]
→ [IEEE802.1ah 関連]

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**

IEEE802.1ah 関連

基本情報 カスタマーバックボーンサービス情報 プロバイダーバックボーンサービス情報

7.4.1 基本情報

7.4.1.1 基本情報（初期表示およびプロバイダーポート選択時）

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]
→ [IEEE802.1ah 関連] → [基本情報 (IEEE802.1ah 機能：初期表示またはプロバイダーポート)]

■ **基本情報** ?

IEEE802.1ah 機能

- ☒ 動作しない
- ☐ カスタマーポート
- ☐ プロバイダーポート

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

初期表示または IEEE802.1ah 機能に“プロバイダーポート”を選択した場合に表示されます。

IEEE802.1ah 機能

リンクアグリゲーションでの IEEE802.1ah 機能の動作を設定します。

- 動作しない
IEEE802.1ah 機能が動作しません。
- カスタマーポート
カスタマーポートとして動作します。
- プロバイダーポート
プロバイダーポートとして動作します。

こんな事に気をつけて

- “カスタマーポート”を選択したリンクアグリゲーションのメンバポートに VLAN を指定することはできません。設定された場合はポートが使用できなくなります。
- “プロバイダーポート”を選択した場合、リンクアグリゲーションのメンバポートにプロバイダネットワーク側で使用するバックボーン VLAN を Tagged VLAN に指定してください。

7.4.1.2 基本情報（カスタマーポート選択時）

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]
→[IEEE802.1ah 関連]→[基本情報（IEEE802.1ah 機能：カスタマーポート）]

■基本情報

IEEE802.1ah機能	☐ 動作しない ☒ カスタマーポート ☐ プロバイダーポート
バックボーンサービスデフォルト動作	☒ 破棄する ☐ 転送する バックボーンサービスID 参照
Tagモード	☒ サービスVLAN ☐ カスタマーVLAN

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

IEEE802.1ah 機能に“カスタマーポート”を選択した場合に表示されます。

「IEEE802.1ah 機能」の項目は、「IEEE802.1ah 機能（初期表示またはプロバイダーポート選択時）」を参照してください。

バックボーンサービスデフォルト動作

カスタマーバックボーンサービス情報で指定したバックボーンサービス ID で指定されたサービス VLAN に一致しなかったフレームの動作を指定します。

- 破棄する
フレームを破棄します。
- 転送する
フレームを転送します。

バックボーンサービス ID

[参照] ボタンをクリックすると、有効なバックボーンサービス ID 情報が表示されます。デフォルト動作で“転送する”選択した場合に使用するバックボーンサービス ID を選択してください。

こんな事に気をつけて

バックボーンサービス ID の適用には条件があります。装置やポートにおける適用可能上限を超えた場合は適用されません。適用条件は、機能説明書「[バックボーンサービスの適用条件について](#)」(P.148) を参照してください。

Tag モード

カスタマーポートで転送対象とする Tag モードを設定します。

- サービス VLAN
「IEEE802.1ah 情報」の“サービス VLAN タグプロトコル ID”で設定されたタグプロトコル ID を、転送対象のタグプロトコル ID とします。
- カスタマー VLAN
"8100" を転送対象のタグプロトコル ID とします。

7.4.2 カスタマーバックボーンサービス情報

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]
→[IEEE802.1ah 関連]→[カスタマーバックボーンサービス情報]

現在、このリンクアグリゲーショングループに設定されているカスタマーバックボーンサービス情報の一覧です。装置全体で 4000 個まで設定できます。カスタマーポートで使用する、バックボーンサービス ID を指定します。処理するボタンをクリックし、次のページへ進みます。

バックボーンサービス ID

[参照] ボタンをクリックすると、有効なバックボーンサービス ID 情報が表示されます。カスタマーポートで設定するバックボーンサービス ID を選択してください。

こんな事に気をつけて

- 本設定で指定したバックボーンサービス ID で、“サービス VLAN ID” の設定がない場合は無効となります。
- 同一ポートで指定したバックボーンサービス ID の「IEEE802.1ah 情報」-「バックボーンサービス関連」の“サービス VLAN ID” が重複する場合、定義番号の小さいほうが有効となり定義番号の大きいほうは無効となります。
- バックボーンサービス ID の適用には条件があります。装置やポートにおける適用可能上限を超えた場合は適用されません。適用条件は、機能説明書「[バックボーンサービスの適用条件について](#)」(P.148) を参照してください。

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]
 →[IEEE802.1ah 情報]→[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の[参照]」

表示条件入力		
表示回数	表示範囲	
10	0~0	
■バックボーンサービス情報		
サービスID	説明文	操作
0	インスタンスID	選択
	サービスVLAN ID	
	バックボーンVLAN ID	
	100	選択
	100	
	300	
開じる		

「IEEE802.1ah 情報」-「バックボーンサービス関連」で設定したバックボーンサービス定義情報が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示回数および表示範囲を指定することができます。設定することによって、カスタマーバックボーンサービス定義情報の一覧に見たい情報だけを表示させることができます。

参照する VLAN タグマッピングルール情報が存在しない場合は、「参照可能なバックボーンサービス情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「カスタマーバックボーンサービス情報」のバックボーンサービスIDに設定する定義番号欄の[選択] ボタンをクリックすると、入力フィールドに選択した番号が表示されます。[追加] ボタンをクリックすると、「カスタマーバックボーンサービス情報」に追加されます。

7.4.3 プロバイダーバックボーンサービス情報

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]
 →[IEEE802.1ah 関連]→[プロバイダーバックボーンサービス情報]

表示条件入力	
表示回数	表示範囲
10	プロバイダーバックボーンサービス定義は存在しません
■プロバイダーバックボーンサービス情報	
※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	バックボーンサービスID
全削除	
<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	参照
追加 キャンセル	
保存した情報は、設定反映後に有効になります。	

現在、このリンクアグリゲーショングループに設定されているプロバイダーバックボーンサービス情報の一覧です。装置全体で2000個まで設定できます。プロバイダーポートで使用する、バックボーンサービスIDを指定します。処理するボタンをクリックし、次のページへ進みます。

バックボーンサービスID

[参照] ボタンをクリックすると、有効なバックボーンサービスID情報が表示されます。プロバイダーポートで設定するバックボーンサービスIDを選択してください。

こんな事に気をつけて

- 本設定で指定したバックボーンサービスIDで、“バックボーンVLAN ID” および “バックボーンアて先 MAC アドレス” の設定がない場合は無効となります。
- バックボーンサービスIDの適用には条件があります。装置やポートにおける適用可能上限を超えた場合は適用されません。適用条件は、機能説明書「[バックボーンサービスの適用条件について](#)」(P.148) を参照してください。

[操作] 「設定メニュー」→詳細設定「リンクアグリゲーショングループ情報」→[修正]
→[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の [参照]」

表示条件入力

表示回数: 10 表示範囲: 0~0

■バックボーンサービス情報 [開じる]

サービスID	説明文	操作
0	インスタンスID	選択
	サービスVLAN ID	
	バックボーンVLAN ID	
	100	
	100	
	300	

[開じる]

「IEEE802.1ah 情報」-「バックボーンサービス関連」で設定したバックボーンサービス定義情報が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示回数および表示範囲を指定することができます。設定することによって、プロバイダーバックボーンサービス定義情報の一覧に見たい情報だけを表示させることができます。

参照する VLAN タグマッピングルール情報が存在しない場合は、「参照可能なバックボーンサービス情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「プロバイダーバックボーンサービス情報」のバックボーンサービスIDに設定する定義番号欄の[選択] ボタンをクリックすると、入力フィールドに選択した番号が表示されます。[追加] ボタンをクリックすると、「プロバイダーバックボーンサービス情報」に追加されます。

8 バックアップグループ情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「バックアップグループ情報」

バックアップグループ情報
バックアップグループ情報

■バックアップグループ情報

グループ番号	優先使用ポート	待機状態	操作
1	master	閉塞しない	修正 初期化
2	master	閉塞しない	修正 初期化
3	master	閉塞しない	修正 初期化
4	master	閉塞しない	修正 初期化
5	master	閉塞しない	修正 初期化
6	master	閉塞しない	修正 初期化
7	master	閉塞しない	修正 初期化
8	master	閉塞しない	修正 初期化

保存した情報は、設定反映後に有効になります。

バックアップグループの一覧が表示されています。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」→詳細設定「バックアップグループ情報」→[修正]

<バックアップグループ情報入力フィールド>

優先使用ポート
☒ master
☐ 先にリンクアップしたポート

待機状態
☒ 閉塞しない ☐ 閉塞する

リンクダウン連携
☒ 使用しない
☐ 使用する

連携ポートリスト

リンクアップ時の動作
☒ 閉塞解除しない
☐ 閉塞解除する

閉塞要因
☒ リンクダウン連携
☐ すべて

優先使用ポート

優先ポートと待機ポートの両方が使用可能のときに使用するポートを以下から選択します。

- master
優先ポートを優先的に使用します。
- 先にリンクアップしたポート
優先ポートと待機ポートのどちらか先にリンクアップして使用可能になったポートを使用します。

待機状態

バックアップ待機ポートの待機状態を以下から選択します。

- 閉塞しない
待機状態でポート閉塞しません。
- 閉塞する
待機状態でポート閉塞します。

こんな事に気をつけて

- 優先使用ポートが“master”と設定されている場合に、バックアップ待機ポートの待機状態をポート閉塞する設定としても、バックアップの優先ポートは閉塞しません。バックアップの優先ポートを閉塞させたい場合は、優先使用ポートを“先にリンクアップしたポート”に設定してください。
- バックアップ待機ポートの待機状態をポート閉塞する設定とした場合に、バックアップポート機能以外が閉塞したポートを自動で閉塞解除しません。「操作メニュー」で閉塞したポートである場合も同じです。

リンクダウン連携

このバックアップグループでリンクダウン連携を使用する場合は、“使用する”を選択します。“使用する”を選択した場合は、以降の“連携ポートリスト”、“リンクアップ時の動作”および“閉塞要因”を設定してください。

連携ポートリスト

このバックアップグループがリンクダウンしたときに連携してリンクダウン（ポート閉塞）させるポートリストを、以下の範囲の10進数で指定します。

機種	ポートリスト
SR-S208TC2、308TL1	1～9
SR-S224TC2	1～26
SR-S208PD1、310TL2	1～10
SR-S224PS1、224CP1、328TR1	1～28
SR-S248TC1、348TC1、748TC1	1～52
SR-S316TL1、318TL2	1～18
SR-S324TL2	1～24
SR-S316C2、716C2	1～16
SR-S324TC1、724TC1	1～26

ポートリストを複数指定する場合は、“,”で区切ります。範囲指定の場合は“-”で区切ります。省略時は、該当ポートがリンクダウンしても連携動作しません。

リンクアップ時の動作

このバックアップグループがリンクアップしたときに、連携ポートリストに設定した、ポートの閉塞状態の解除を行うかどうかを選択します。

- 閉塞解除しない
リンクアップ時に閉塞状態の解除を行いません。
- 閉塞解除する
リンクアップ時に閉塞状態の解除を行います。本設定を選択した場合は、以降の“解除対象の要因”を設定してください。

こんな事に気をつけて

“閉塞解除しない”、“閉塞解除する”のどちらを選択しても「操作メニュー」の「閉塞／閉塞解除」設定によって連携ポートリストの閉塞状態の解除が可能です。

閉塞要因

リンクアップ時に、連携ポートリストに設定されたポートの閉塞状態の解除を行う場合に、解除対象とする閉塞要因を選択します。

- リンクダウン連携
連携ポートリストの閉塞状態がリンクダウン連携による閉塞要因のみ解除対象に指定します。
- すべて
連携ポートリストの閉塞状態の閉塞要因に依存しない解除対象に指定します。

こんな事に気をつけて

連携ポートリストに設定されたポートに対する動的定義反映時には、設定に依存しないで閉塞状態の解除が行われます。

9 etherblock 情報

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

[操作] 「設定メニュー」→詳細設定「etherblock 情報」

etherblock 情報	
etherblock 情報	
■ etherblock 情報	
ポート番号	操作
1	修正 初期化
2	修正 初期化
3	修正 初期化
全初期化	
保存した情報は、設定反映後に有効になります。	

[操作] 「設定メニュー」→詳細設定「etherblock 情報」→[修正]

etherblock 情報 - etherblock 1 情報	
フィルタ情報	QoS 情報

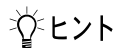
9.1 フィルタ情報

[操作] 「設定メニュー」→詳細設定「etherblock 情報」→[修正]→[フィルタ情報]

■ フィルタ情報			
ACL 定義参照			
※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。			
優先順位	動作	ACL 定義番号	操作
		ACL 定義名	
<フィルタ情報入力フィールド>			
動作		☒ 透過 ☐ 遮断	
ACL 定義番号		参照	
		追加 キャンセル	
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。			
保存した情報は、設定反映後に有効になります。			

現在、この etherblock に設定されている MAC フィルタリング定義が表示されています。処理は優先順位 1 から順に行われます。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件に一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。



ヒント

◆ フィルタの定義数

● SR-S208TC2/224TC2/208PD1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 30 ルール

● SR-S224PS1/224CP1/248TC1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 60～100 ルール（認証成功端末数による）

◆ 優先順位

優先順位は、以下のとおりです。

- (1) 「ether 情報」 - 「フィルタ情報」の設定（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (2) 「etherblock 情報」 - 「フィルタ情報」の設定
- (3) 「VLAN 情報」 - 「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (4) 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (5) 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (6) 「etherblock 情報」 - 「QoS 情報」
- (7) 「VLAN 情報」 - 「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」 - 「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (10) 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (11) 「VLAN 情報」 - 「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

◆ ルール

● SR-S208TC2/224TC2/208PD1 の場合

ACL の内容によって、以下のように消費するルール数が異なります。

<ルール1>

- 「ether 情報」 - 「フィルタ情報」
- 「etherblock 情報」 - 「フィルタ情報」
- 「VLAN 情報」 - 「フィルタ情報」
- 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- 「etherblock 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「IPv6 フィルタ情報」
- 「VLAN 情報」 - 「IPv6 QoS 情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: TCP または UDP の送信元ポート数 × あて先ポート数 × 2
- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: ICMP の ICMP TYPE の個数 × ICMP CODE の個数 × 2
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: 2
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: 1

<ルール2>

- 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
- 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
- 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

● SR-S224PS1/224CP1/248TC1 の場合

ACL の内容によって、以下のように消費するルール数が異なります。それぞれの ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

こんな事に気をつけて

- 自装置 IP アドレスあてパケットや IP オプション付きパケットなど、ソフト処理となるパケットに対する「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」設定や「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」設定はスイッチのフィルタ・QoS 設定上限オーバとなった場合も適用されます。
- WWW や DHCP に対するアクセスを制限する設定を行った場合、WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。
- 以下の設定はすべての etherblock に適用されます。
 - 「VLAN 情報」 - 「フィルタ情報」
 - 「VLAN 情報」 - 「QoS 情報」
 - 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
 - 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
 - 「VLAN 情報」 - 「IPv6 フィルタ情報」
 - 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」
 - 「VLAN 情報」 - 「IPv6 QoS 情報」
- 当該 etherblock で、IEEE802.1X 認証成功端末、Web 認証成功端末、MAC アドレス認証成功端末および DHCP スヌープ許可端末の合計が 152 台以下の場合、ルールによる上限は etherblock ごとに 100 個となりますが、152 台を超えた場合は 1 認証成功端末につき使用可能なルール数が 1 個減少します。(SR-S224PS1/224CP1/248TC1 の場合)

動作

フィルタの動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- MAC 定義
- VLAN 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] 「設定メニュー」→詳細設定「etherblock 情報」→ [修正] → [フィルタ情報]
→ [ACL 定義番号の [参照]]

表示条件入力					
表示回数		表示範囲			
10		0~0			
■ACL 情報					
	IP 定義	MAC 定義	VLAN 定義	TCP/UDP/ICMP 定義	選択
定義番号	プロトコル 送信元IPアドレス/マスク あて先IPアドレス/マスク QoS種別 QoS値	送信元MACアドレス あて先MACアドレス フォーマット種別 LSAP/type値	VLAN ID プライオリティ		
0	すべて	bcast	20		
	192.168.1.0/24	bcast	5		
	any	llc			選択
	any	1fff			
					閉じる

「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」、「MAC 定義情報」および「VLAN 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示回数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「フィルタ情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「フィルタ情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

9.2 QoS 情報

[操作] 「設定メニュー」→詳細設定「etherblock 情報」→[修正]→[QoS 情報]

■QoS情報 ACL定義参照

※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。

優先順位	動作	ACL定義番号	操作
		ACL定義名	

<QoS情報入力フィールド>

動作

☒ 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

書き換え値 ☒ ip precedence値指定 ☐ ☐ cos値

☐ dscp値書き換え

書き換え値

☐ 出力キュー指定 ☐

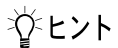
ACL定義番号 参照

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このetherblockに設定されているQoS処理定義のACL定義が表示されています。処理は優先順位1から順に行われます。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件に一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。



ヒント

◆フィルタの定義数

●SR-S208TC2/224TC2/208PD1の場合

etherblockごとに10個

指定されたACL情報の内容によってetherblockごとに30ルール

●SR-S224PS1/224CP1/248TC1の場合

etherblockごとに10個

指定されたACL情報の内容によってetherblockごとに60～100ルール（認証成功端末数による）

◆優先順位

優先順位は、以下のとおりです。

- (1) 「ether 情報」 - 「フィルタ情報」の設定（etherポート間の優先順位はetherポート番号が小さいほうが高い）
- (2) 「etherblock 情報」 - 「フィルタ情報」の設定
- (3) 「VLAN 情報」 - 「フィルタ情報」の設定（VLAN間の優先順位はVLAN IDが小さいほうが高い）
- (4) 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」（LAN間の優先順位はLAN定義番号が小さいほうが高い）
- (5) 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」（etherポート間の優先順位はetherポート番号が小さいほうが高い）
- (6) 「etherblock 情報」 - 「QoS 情報」
- (7) 「VLAN 情報」 - 「QoS 情報」（VLAN間の優先順位はVLAN IDが小さいほうが高い）
- (8) 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」（LAN間の優先順位はLAN定義番号が小さいほうが高い）

- (9) 「VLAN 情報」 - 「IPv6 フィルタ情報」の設定 (VLAN 間の優先順位は VLAN ID が小さいほうが高い)
- (10) 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」 (LAN 間の優先順位は lan 定義番号が小さいほうが高い)
- (11) 「VLAN 情報」 - 「IPv6 QoS 情報」 (VLAN 間の優先順位は VLAN ID が小さいほうが高い)

◆ ルール

● SR-S208TC2/224TC2/208PD1 の場合

ACL の内容によって、以下のように消費するルール数が異なります。

<ルール1>

- ・ 「ether 情報」 - 「フィルタ情報」
- ・ 「etherblock 情報」 - 「フィルタ情報」
- ・ 「VLAN 情報」 - 「フィルタ情報」
- ・ 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- ・ 「etherblock 情報」 - 「QoS 情報」
- ・ 「VLAN 情報」 - 「QoS 情報」
- ・ 「VLAN 情報」 - 「IPv6 フィルタ情報」
- ・ 「VLAN 情報」 - 「IPv6 QoS 情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- ・ TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: TCP または UDP の送信元ポート数 × あて先ポート数 × 2
- ・ TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: TCP または UDP の送信元ポート数 × あて先ポート数
- ・ ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: ICMP の ICMP TYPE の個数 × ICMP CODE の個数 × 2
- ・ ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- ・ TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: 2
- ・ TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: 1

<ルール2>

- ・ 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
- ・ 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
- ・ 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- ・ TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ・ ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- ・ TCP/UDP/ICMP を設定しない ACL の場合 : 1

● SR-S224PS1/224CP1/248TC1 の場合

ACL の内容によって、以下のように消費するルール数が異なります。それぞれの ACL のルール数は、以下の計算式によって求められます。

- ・ TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ・ ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- ・ TCP/UDP/ICMP を設定しない ACL の場合 : 1

こんな事に気をつけて

- 自装置 IP アドレスあてパケットや IP オプション付きパケットなど、ソフト処理となるパケットに対する「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」設定や「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」設定はスイッチのフィルタ・QoS 設定上限オーバとなった場合も適用されます。
- 以下の設定はすべての etherblock に適用されます。
 - 「VLAN 情報」 - 「フィルタ情報」
 - 「VLAN 情報」 - 「QoS 情報」
 - 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
 - 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
 - 「VLAN 情報」 - 「IPv6 フィルタ情報」
 - 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」
 - 「VLAN 情報」 - 「IPv6 QoS 情報」
- 当該 etherblock で、IEEE802.1X 認証成功端末、Web 認証成功端末、MAC アドレス認証成功端末および DHCP スヌープ許可端末の合計が 152 台以下の場合は、ルールによる上限は etherblock ごとに 100 個となりますが、152 台を超えた場合は 1 認証成功端末につき使用可能なルール数が 1 個減少します。(SR-S224PS1/224CP1/248TC1 の場合)

動作

QoS 処理の動作を以下の 4 つから選択します。

- cos 値書き換え
条件と一致した場合にパケットの cos 値 (Tagged VLAN の Tag Control Information (TCI) フィールドの user priority 値) を書き換えます。
 - cos 値指定
書き換え後の cos 値を 0～7 の範囲の 10 進数で指定します。
 - ip precedence 値
cos 値をパケットの ip precedence 値に書き換えます。
- ip precedence 値書き換え
条件と一致した場合にパケットの ip precedence 値 (IP ヘッダの TOS フィールドの上位 3 ビット) を書き換えます。
 - ip precedence 値指定
書き換え後の ip precedence 値を 0～7 の範囲の 10 進数で指定します。
 - cos 値
ip precedence 値を cos 値に書き換えます。
- dscp 値書き換え
条件と一致した場合にパケットの dscp 値 (IP ヘッダの TOS フィールドの上位 6 ビット) を書き換えます。書き換え後の dscp 値を 0～63 の範囲の 10 進数で指定します。

- 出力キュー指定
条件と一致した場合にパケットが出力されるときに使用される出力ポートのキューを変更します。使用する出力ポートのキュー番号を、0～3 の範囲の 10 進数で指定します。大きい値が出力優先順位がより高いキューであることを表します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- MAC 定義
- VLAN 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] 「設定メニュー」→詳細設定「etherblock 情報」→[修正]→[QoS 情報]
→「ACL 定義番号の [参照]」

表示条件入力					
表示個数		表示範囲			
10		0~0			
■ ACL 情報 閉じる					
定義番号	IP定義	MAC定義	VLAN定義	TCP/UDP/ICMP定義	選択
	プロトコル 送信元IPアドレス/マスク あて先IPアドレス/マスク QoS種別 QoS値	送信元MACアドレス あて先MACアドレス フォーマット種別 LSAP/type値	VLAN ID プライオリティ		
0	すべて	bcast	20		
	192.168.1.0/24	bcast	5		
	any	llc			選択
	any	1fff			
閉じる					

「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」、「MAC 定義情報」および「VLAN 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「QoS 情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「QoS 情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

10 LACP 情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「LACP 情報」

LACP 情報
基本情報

10.1 基本情報

[操作] 「設定メニュー」→詳細設定「LACP 情報」→[基本情報]

基本情報	
システム優先度	32768
LACPDU 転送モード	☒ 転送しない ☐ 転送する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

システム優先度

システム優先度を 1～65535 の範囲で指定します。システム優先度はリンクアグリゲーショングループが相手リンクアグリゲーショングループとの情報交換で、どちらが優先になるかを決定するのに使用します。同じ優先度である場合は、システム ID（代表 MAC アドレス + 1）の値が小さいほうが高優先と判断します。

省略時は、32768 が設定されます。

LACPDU 転送モード

LACPDU 転送モードを指定します。LACP 機能が無効になったとき、“転送する”と設定されている場合に LACPDU フレームを転送します。

ただし、リンクアグリゲーションが設定されている場合は、LACPDU フレームの転送は行いません。

11 VLAN 情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「VLAN 情報」

VLAN情報
[VLAN情報](#)

■**VLAN情報**

※追加情報は一覧の最後尾の追加フィールドで設定してください。 

VLAN ID	VLAN種別	プロトコル条件	VLAN名	操作
全削除				

<VLAN情報追加フィールド>

VLAN ID	
追加 キャンセル	

保存した情報は、設定反映後に有効になります。

現在、設定されている VLAN が表示されています。処理するボタンをクリックし、次のページへ進みます。

VLAN ID

追加する VLAN の VLAN ID を、1 ～ 4094 の範囲の 10 進数で指定します。

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→[追加]

VLAN1情報

[基本情報](#)
[静的MAC学習テーブル情報](#)
[DHCPスヌープ情報](#)

[IGMPスヌープ情報](#)
[フィルタ情報](#)
[IPv6フィルタ情報](#)

[QoS情報](#)
[IPv6 QoS情報](#)
[ARP認証関連](#)

11.1 基本情報

11.1.1 基本情報（初期表示または指定しない選択時）

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→[追加]
→[基本情報（プロトコル定義：初期表示または指定しない）]

初期表示またはプロトコル定義に“指定しない”を選択した場合に表示されます。
SR-S208TC2、224TC2、208PD1 では、「プロトコル定義」の項目は表示されません。

VLAN 名

VLAN 名を設定する場合は、0x21 および 0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

省略時は、以下のようにシステムで自動設定されます。

VLAN ID	VLAN 名
1	"default"
2～4094	"v2"～"v4094"

説明文

この VLAN の説明文を、50 文字以内で設定します。

プロトコル定義（SR-S208TC2、224TC2、208PD1 除く）

プロトコル定義の設定をするかどうかを、以下から選択します。

- 指定しない
プロトコル VLAN として使用しません。
- システム定義プロトコルから指定
テンプレート定義されたプロトコルから選択します。
- プロトコルをユーザ定義指定
プロトコルをフレーム形式で直接指定します。

こんな事に気をつけて

プロトコル定義を削除しても VLAN 自体は削除されません。

11.1.2 基本情報（システム定義プロトコルから指定選択時）



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

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→[追加]
→[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）]

■基本情報

VLAN名

☒ 設定を省略する(システム自動設定)
☐ 設定する

説明文

プロトコル定義

☐ 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

プロトコル種別

☒ IPv4 ☐ IPv6 ☐ FNA

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

プロトコル定義に“システム定義プロトコルから指定”を選択した場合に表示されます。

「VLAN 名」、「説明文」および「プロトコル定義」の項目は、「基本情報（初期表示または指定しない選択時）」を参照してください。

プロトコル種別

プロトコル種別を以下の3つから選択します。

- IPv4
IPv4 プロトコルVLAN（Ethernet形式：0800, 0806, 8035）
- IPv6
IPv6 プロトコルVLAN（Ethernet形式：86dd）
- FNA
FNA プロトコルVLAN（LLC形式：8080, 0000, 0001）

こんな事に気をつけて

- 同一のプロトコル定義条件を複数の異なるVLANで定義することができます。ただし、複数定義されたVLANが同一ポートで競合する場合は、もっとも小さい番号のVLANのみが有効となります。
- SR-S224PS1/224CP1/248TC1では、FNAプロトコルVLANは設定できません。

11.1.3 基本情報（プロトコルをユーザ定義指定選択時）

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

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→[追加]
→[基本情報（プロトコル定義：プロトコルをユーザ定義指定）]

プロトコル定義に“プロトコルをユーザ定義指定”を選択した場合に表示されます。

「VLAN 名」、「説明文」および「プロトコル定義」の項目は、「基本情報（初期表示または指定しない選択時）」を参照してください。

プロトコル条件

ユーザ定義によるプロトコル条件を設定します。

機種によって、設定できる条件数が異なります。設定できるプロトコル条件数は、以下のとおりです。

機種	設定できるプロトコル条件
SR-S224PS1、224CP1、248TC1	3条件
SR-S308TL1、310TL2、316TL1、318TL2、324TL2、316C2、324TC1、328TR1、348TC1、716C2、724TC1、748TC1	8条件

フォーマット種別

フォーマット種別を以下から選択します。

- Ethernet形式
- SNAP形式

- LLC形式

type 値 /LSAP

フォーマット種別で“Ethernet形式”および“SNAP形式”を選択した場合はEtherType 値を、“LLC形式”を選択した場合はLLC 値（DSAP,SSAP）を、4桁の16進数で指定します。

こんな事に気をつけて

- システム定義されているプロトコル（IPv4、IPv6、FNA）と同一のプロトコル条件をユーザ定義で設定することもできます。ただし、両方で定義されたVLANが同一ポートで競合する場合は、もっとも小さい番号のVLANのみが有効となります。
- SR-S224PS1/224CP1/248TC1では、LLC形式については最大2条件までが有効となります。

11.2 静的MAC学習テーブル情報

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→[追加]→[静的MAC学習テーブル情報]

現在、設定されている静的MAC学習テーブルの一覧が表示されています。静的MAC学習テーブルは、装置で最大400まで設定できます。処理するボタンをクリックし、次のページへ進みます。

MACアドレス

静的に学習テーブルに追加するMACアドレスを指定します。

こんな事に気をつけて

00:00:00:00:00:00、ブロードキャストおよびマルチキャストアドレスは指定できません。

ポート番号

対象となるポート番号を選択します。

こんな事に気をつけて

- 指定されたポートに指定VLANが設定されていない場合は、設定は無効になります。
- 指定されたポートがリンクアグリゲーションポートのメンバーポートである場合は、リンクアグリゲーションポートに対して転送設定します。
- 指定されたポートがバックアップポートの場合は、バックアップポートの稼働ポートに対して転送設定します。

11.3 DHCPスヌープ情報

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→[追加]→[DHCPスヌープ情報]

DHCPスヌープ機能

DHCPスヌープ機能を使用するかどうかを選択します。

“使用する”を選択した場合、DHCPでIPアドレスが割り当てられた端末の通信だけを許可することができます。

こんな事に気をつけて

- 本機能を使用する場合は「ether 情報」-「DHCPスヌープ情報」でポートの通信許可を設定してください。
- IPv4 DHCP 機能を有効にしたVLAN内では、本機能は無効となり、すべての端末が通信許可されます。
- 「ether 情報」-「転送許可ポート」を設定したポートが存在する場合、本機能は無効となり、すべての端末が通信許可されます。
(SR-S208TC2/224TC1/208PD1の場合)

11.4 IGMP スヌープ情報

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→[追加]→[IGMP スヌープ情報]

■IGMPスヌープ情報

静的ルータポート ☒ 自動認識 ☐ 設定する
ルータポート

Querierモード ☒ Querier動作可 ☐ Querier動作不可

IGMP送信元アドレス ☒ 設定しない ☐ 設定する
送信元IPアドレス

IGMP代理応答モード ☒ 代理応答しない ☐ 代理応答する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

静的ルータポート

静的なマルチキャストルータポートを指定します。複数台のマルチキャストルータが接続される場合は、必ず設定してください。また、マルチキャストルータが存在しない場合、かつ複数台のIGMPスヌープ装置をカスケード接続する場合も設定が必要です。

Querier モード

マルチキャストルータが存在しない場合に代理でQuerierとして動作するかを指定します。

こんな事に気をつけて

マルチキャストルータが存在しないでQuerierモードが“Querier動作不可”を選択した場合は、リスナー情報の収集が正常に動作できないため、通信ができない場合があります。

IGMP 代理応答モード

IGMP Membership report の代理応答のモードを指定します。“代理応答しない”とした場合は、端末からのIGMPパケットが転送されます。

こんな事に気をつけて

IGMP V1/V2 が混在する環境では“IGMP代理応答モード”に“代理応答しない”を選択してください。

IGMP 送信元アドレス

IGMPスヌープ機能が送信するIGMPパケットの送信元アドレスを指定します。指定しない場合は、0.0.0.0を送信元アドレスとして設定します。

こんな事に気をつけて

マルチキャストルータが存在する場合は、その装置のアドレスより大きな値を指定してください。

11.5 フィルタ情報

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→[追加]→[フィルタ情報]

現在、このVLANに設定されているフィルタ定義のACL 定義が表示されています。処理は優先順位1から順に行われます。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件に一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

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。

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)

☞ 参照 「装置情報」-「資源情報」画面は、[\[4.9 資源情報\] \(P33\)](#) を参照してください。

💡 ヒント

◆ フィルタの定義数

● SR-S208TC2/224TC2/208PD1 の場合

etherblock ごとに 10 個

指定されたACL 情報の内容によって etherblock ごとに 30 ルール

● SR-S224PS1/224CP1/248TC1 の場合

etherblock ごとに 10 個

指定されたACL 情報の内容によって etherblock ごとに 60～100 ルール（認証成功端末数による）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合

装置で 128 個

指定されたACL 情報の内容によって装置で 128 ルール

● SR-S316C2/716C2 の場合

ポートごとに 10 個

指定されたACL 情報の内容によってポートごとに 100 ルール

● SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合

装置で 128 個（初期値）

指定された ACL 情報の内容によって装置で 128 ルール（初期値）

定義可能上限値は、「装置情報」-「資源情報」の「フィルタ/QoS 資源の配分」の設定で、最大で 512 個まで拡張することができます。

◆ 優先順位

● SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (2) 「etherblock 情報」-「フィルタ情報」の設定
- (3) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (4) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (5) 「ether 情報」-「QoS 関連」-「QoS 情報」（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (6) 「etherblock 情報」-「QoS 情報」
- (7) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」-「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (10) 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (11) 「VLAN 情報」-「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S316C2/716C2 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定
- (2) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (4) 「ether 情報」-「QoS 関連」-「QoS 情報」
- (5) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (6) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (7) 「VLAN 情報」-「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」-「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2/324TC1/328TR1/348TC1/724TC1 /748TC1 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定
- (2) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）

◆ ルール

● SR-S208TC2/224TC2/208PD1 の場合

ACL の内容によって、以下のように消費するルール数が異なります。

<ルール1>

- 「ether 情報」 - 「フィルタ情報」
- 「etherblock 情報」 - 「フィルタ情報」
- 「VLAN 情報」 - 「フィルタ情報」
- 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- 「etherblock 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「IPv6 フィルタ情報」
- 「VLAN 情報」 - 「IPv6 QoS 情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： TCP または UDP の送信元ポート数 × あて先ポート数 × 2
- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： ICMP の ICMP TYPE の個数 × ICMP CODE の個数 × 2
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： 2
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： 1

<ルール2>

- 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
- 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
- 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 ： TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 ： ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 ： 1

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

ACL の内容によって、以下のように消費するルール数が異なります。それぞれの ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 ： TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 ： ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 ： 1

こんな事に気をつけて

- 自装置 IP アドレスあてパケットや IP オプション付きパケットなど、ソフト処理となるパケットに対する「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」設定や「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」設定はスイッチのフィルタ・QoS 設定上限オーバとなった場合も適用されます。
- 指定した ACL の VLAN 定義で指定された VLAN ID が適用する VLAN ID と矛盾する場合、フィルタは適用されません。
- WWW や DHCP に対するアクセスを制限する設定を行った場合、WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。
- 以下の設定はすべての etherblock に適用されます。(SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合)
 - 「VLAN 情報」 - 「フィルタ情報」
 - 「VLAN 情報」 - 「QoS 情報」
 - 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
 - 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
 - 「VLAN 情報」 - 「IPv6 フィルタ情報」
 - 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」
 - 「VLAN 情報」 - 「IPv6 QoS 情報」
- 当該 etherblock で、IEEE802.1X 認証成功端末、Web 認証成功端末、MAC アドレス認証成功端末および DHCP スヌープ許可端末の合計が 152 台以下の場合、ルールによる上限は etherblock ごとに 100 個となりますが、152 台を超えた場合は 1 認証成功端末につき使用可能なルール数が 1 個減少します。(SR-S224PS1/224CP1/248TC1 の場合)
- 自装置 IP アドレスあてパケットは acl 定義に該当した場合もフィルタされません。自装置 IP アドレスあてパケットは「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」で設定してください。(SR-S716C2 の場合)
- "ether macfilter" コマンド、"vlan macfilter" コマンド、"lan ip filter" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 200 個まで設定可能です。(SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合)
- "ether macfilter" コマンド、"ether qos aclmap" コマンド、"vlan macfilter" コマンド、"vlan qos aclmap" コマンド、"lan ip filter" コマンド、"lan ip dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 700 個まで設定可能です。(SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合)

動作

フィルタの動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- MAC 定義
- VLAN 定義
- TCP 定義
IP 定義のプロトコルが 6 の場合だけ有効です。
- UDP 定義
IP 定義のプロトコルが 17 の場合だけ有効です。
- ICMP 定義
IP 定義のプロトコルが 1 の場合だけ有効です。

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→[追加]→[フィルタ情報]
→「ACL 定義番号の [参照]」

表示条件入力					
表示個数		表示範囲			
10		0~0			
ACL 情報 閉じる					
定義番号	IP定義	MAC定義	VLAN定義	TCP/UDP/ICMP定義	選択
	プロトコル 送信元IPアドレス/マスク あて先IPアドレス/マスク QoS種別 QoS値	送信元MACアドレス あて先MACアドレス フォーマット種別 LSAP/type値	VLAN ID プライオリティ		
	すべて	bcast	20		
	192.168.1.0/24	bcast	5		
0	any	llc			選択
	any	1fff			
					閉じる

「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」、「MAC 定義情報」および「VLAN 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「フィルタ情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「フィルタ情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

11.6 IPv6 フィルタ情報

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→「追加」→「IPv6 フィルタ情報」

現在、このVLANに設定されているフィルタ定義のACL定義が表示されています。処理は優先順位1から順に行われます。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件に一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

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。

IPv6 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“IPv6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)

☞ 参照 「装置情報」-「資源情報」画面は、[「4.9 資源情報」\(P33\)](#) を参照してください。

💡 ヒント

◆ フィルタの定義数

● SR-S208TC2/224TC2/208PD1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 30 ルール

● SR-S224PS1/224CP1/248TC1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 60～100 ルール（認証成功端末数による）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合

装置で 128 個

指定された ACL 情報の内容によって装置で 128 ルール

● SR-S316C2/716C2 の場合

ポートごとに 10 個

指定された ACL 情報の内容によってポートごとに 100 ルール

● SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合

装置で 128 個（初期値）

指定された ACL 情報の内容によって装置で 128 ルール（初期値）

定義可能上限値は、「装置情報」 - 「資源情報」の「フィルタ/QoS 資源の配分」の設定で、最大で 512 個まで拡張することができます。

◆ 優先順位

● SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」 - 「フィルタ情報」の設定（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (2) 「etherblock 情報」 - 「フィルタ情報」の設定
- (3) 「VLAN 情報」 - 「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (4) 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (5) 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (6) 「etherblock 情報」 - 「QoS 情報」
- (7) 「VLAN 情報」 - 「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」 - 「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (10) 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (11) 「VLAN 情報」 - 「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S316C2/716C2 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」 - 「フィルタ情報」の設定
- (2) 「VLAN 情報」 - 「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (4) 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- (5) 「VLAN 情報」 - 「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (6) 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (7) 「VLAN 情報」 - 「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」 - 「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2/324TC1/328TR1/348TC1/724TC1 /748TC1 の場合

優先順位は、以下のとおりです。

- (1) 「VLAN 情報」 - 「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (2) 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）

◆ ルール

● SR-S208TC2/224TC2/208PD1 の場合

ACL の内容によって、以下のように消費するルール数が異なります。

<ルール1>

- 「ether 情報」 - 「フィルタ情報」
- 「etherblock 情報」 - 「フィルタ情報」
- 「VLAN 情報」 - 「フィルタ情報」
- 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- 「etherblock 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「IPv6 フィルタ情報」
- 「VLAN 情報」 - 「IPv6 QoS 情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： TCP または UDP の送信元ポート数 × あて先ポート数 × 2
- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： ICMP の ICMP TYPE の個数 × ICMP CODE の個数 × 2
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： 2
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： 1

<ルール2>

- 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
- 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
- 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 ： TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 ： ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 ： 1

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

ACL の内容によって、以下のように消費するルール数が異なります。それぞれの ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 ： TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 ： ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 ： 1

こんな事に気をつけて

- 自装置 IPv6 アドレスあてパケットやホップバイホップオプション付きパケットなど、ソフト処理となるパケットに対する「LAN 情報」-「IP 関連」-「IP フィルタリング情報」設定や「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」設定、「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」設定はスイッチのフィルタ・QoS 設定上限オーバとなった場合も適用されます。
- 指定した ACL の VLAN 定義で指定された VLAN ID が適用する VLAN ID と矛盾する場合、フィルタは適用されません。
- WWW や DHCP に対するアクセスを制限する設定を行った場合、WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。
- 以下の設定はすべての etherblock に適用されます。(SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合)
 - 「VLAN 情報」-「フィルタ情報」
 - 「VLAN 情報」-「QoS 情報」
 - 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」
 - 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」
 - 「VLAN 情報」-「IPv6 フィルタ情報」
 - 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」
 - 「VLAN 情報」-「IPv6 QoS 情報」
- ACL で指定したアクセスコントロールリストが使用するスイッチ内部メモリが上限値を超える場合はフィルタは適用されません。たとえば、指定したアクセスコントロールリスト内の IPv6 定義で、送信元およびあて先 IPv6 アドレスのプレフィックス長の組み合わせで、以下の範囲を超えて指定した場合は、使用するスイッチ内部メモリが上限値を超えるため、フィルタ条件を 2 つのアクセスコントロールリストに分割し適用する必要があります。(SR-S224PS1/224CP1/248TC1/316C2/716C2 の場合)

送信元プレフィックス長の設定ビット数	あて先プレフィックス長の設定可能ビット数
113 ~ 128	0 (ANY) ~ 48
81 ~ 112	0 (ANY) ~ 64
49 ~ 80	0 (ANY) ~ 96
0 (ANY) ~ 48	0 (ANY) ~ 128

また、TCP/UDP/ICMP 条件を any 以外で同時に設定した場合、あて先プレフィックス長の設定可能ビット数が 32bit 減少します。

- 当該 etherblock で、IEEE802.1X 認証成功端末、Web 認証成功端末、MAC アドレス認証成功端末および DHCP スヌープ許可端末の合計が 152 台以下の場合は、ルールによる上限は etherblock ごとに 100 個となりますが、152 台を超えた場合は 1 認証成功端末につき使用可能なルール数が 1 個減少します。(SR-S224PS1/224CP1/248TC1 の場合)
- 自装置 IPv6 アドレスあてパケットは acl 定義に該当した場合もフィルタされません。自装置 IPv6 アドレスあてパケットは「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」で設定してください。(SR-S716C2 の場合)
- "vlan ip6filter" コマンド、"lan ip6 filter" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 200 個まで設定可能です。(SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合)
- "ether macfilter" コマンド、"ether qos aclmap" コマンド、"vlan macfilter" コマンド、"vlan qos aclmap" コマンド、"lan ip filter" コマンド、"lan ip dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 700 個まで設定可能です。(SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合)

動作

フィルタの動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

ACL 定義番号

「参照」 ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
- TCP 定義
IPv6 定義のプロトコルが 6 の場合だけ有効です。
- UDP 定義
IPv6 定義のプロトコルが 17 の場合だけ有効です。
- ICMP 定義
IPv6 定義のプロトコルが 58 の場合だけ有効です。

指定する定義番号欄の「選択」 ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。「OK」 ボタンをクリックして、設定をやり直してください。

「操作」 「設定メニュー」→詳細設定「VLAN 情報」→「追加」→「IPv6 フィルタ情報」
→「ACL 定義番号の「参照」」

「ACL 情報」 - 「追加」 / 「修正」 - 「IPv6 定義情報」、「TCP 定義情報」および「UDP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示回数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。「OK」 ボタンをクリックして、設定をやり直してください。

「IPv6 フィルタ情報」の ACL 定義番号に設定する定義番号欄の「選択」 ボタンをクリックすると、「IPv6 フィルタ情報」に ACL 定義番号が設定され、画面が閉じます。「ACL 定義参照」 ボタンをクリックした場合は、「選択」 ボタンは表示されません。「閉じる」 ボタンをクリックして、画面を閉じてください。

11.7 QoS 情報

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→「追加」→「QoS 情報」

■QoS情報 ACL定義参照

※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。

優先順位	動作	ACL定義番号	操作
		ACL定義名	
<QoS情報入力フィールド>			
動作	☒ 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 書き換え値 ☒ ip precedence値指定 ☐ 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 参照		
			追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、このVLANに設定されているQoS処理定義のACL定義が表示されています。処理は優先順位1から順に行われます。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件に一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

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。

QoS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）

参照 「装置情報」-「資源情報」画面は、[「4.9 資源情報」\(P33\)](#)を参照してください。

💡 ヒント

◆ 定義数

- SR-S208TC2/224TC2/208PD1の場合

etherblockごとに10個

指定されたACL情報の内容によってetherblockごとに30ルール

- SR-S224PS1/224CP1/248TC1の場合

etherblockごとに10個

指定されたACL情報の内容によってetherblockごとに60～100ルール（認証成功端末数による）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合

装置で 128 個

指定された ACL 情報の内容によって装置で 128 ルール

● SR-S316C2/716C2 の場合

ポートごとに 10 個

指定された ACL 情報の内容によってポートごとに 100 ルール

● SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合

装置で 128 個（初期値）

指定された ACL 情報の内容によって装置で 128 ルール（初期値）

定義可能上限値は、「装置情報」 - 「資源情報」の「フィルタ/QoS 資源の配分」の設定で、最大で 512 個まで拡張することができます。

◆ 優先順位

● SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」 - 「フィルタ情報」の設定（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (2) 「etherblock 情報」 - 「フィルタ情報」の設定
- (3) 「VLAN 情報」 - 「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (4) 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (5) 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (6) 「etherblock 情報」 - 「QoS 情報」
- (7) 「VLAN 情報」 - 「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」 - 「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (10) 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (11) 「VLAN 情報」 - 「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S316C2/716C2 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」 - 「フィルタ情報」の設定
- (2) 「VLAN 情報」 - 「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (4) 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- (5) 「VLAN 情報」 - 「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (6) 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (7) 「VLAN 情報」 - 「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」 - 「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2/324TC1/328TR1/348TC1/724TC1 /748TC1 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- (2) 「VLAN 情報」 - 「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）

◆ ルール

● SR-S208TC2/224TC2/208PD1 の場合

ACL の内容によって、以下のように消費するルール数が異なります。

<ルール1>

- 「ether 情報」 - 「フィルタ情報」
- 「etherblock 情報」 - 「フィルタ情報」
- 「VLAN 情報」 - 「フィルタ情報」
- 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- 「etherblock 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「IPv6 フィルタ情報」
- 「VLAN 情報」 - 「IPv6 QoS 情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： TCP または UDP の送信元ポート数 × あて先ポート数 × 2
- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： ICMP の ICMP TYPE の個数 × ICMP CODE の個数 × 2
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： 2
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： 1

<ルール2>

- 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
- 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
- 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

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

ACL の内容によって、以下のように消費するルール数が異なります。それぞれの ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

こんな事に気をつけて

- 自装置 IP アドレスあてパケットや IP オプション付きパケットなど、ソフト処理となるパケットに対する「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」設定や「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」設定はスイッチのフィルタ・QoS 設定上限オーバとなった場合も適用されます。
- 指定した ACL の VLAN 定義で指定された VLAN ID が適用する VLAN ID と矛盾する場合は、QoS 処理されません。
- 以下の設定はすべての etherblock に適用されます。(SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合)
 - 「VLAN 情報」 - 「フィルタ情報」
 - 「VLAN 情報」 - 「QoS 情報」
 - 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
 - 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
 - 「VLAN 情報」 - 「IPv6 フィルタ情報」
 - 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」
 - 「VLAN 情報」 - 「IPv6 QoS 情報」
- 当該 etherblock で、IEEE802.1X 認証成功端末、Web 認証成功端末、MAC アドレス認証成功端末および DHCP スヌープ許可端末の合計が 152 台以下の場合は、ルールによる上限は etherblock ごとに 100 個となりますが、152 台を超えた場合は 1 認証成功端末につき使用可能なルール数が 1 個減少します。(SR-S224PS1/224CP1/248TC1 の場合)
- "ether qos aclmap" コマンド、"vlan qos aclmap" コマンド、"lan ip dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 200 個まで設定可能です。(SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合)
- "ether macfilter" コマンド、"ether qos aclmap" コマンド、"vlan macfilter" コマンド、"vlan qos aclmap" コマンド、"lan ip filter" コマンド、"lan ip dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 700 個まで設定可能です。(SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合)

動作

QoS 処理の動作を以下の 4 つから選択します。

- cos 値書き換え
条件と一致した場合にパケットの cos 値 (Tagged VLAN の Tag Control Information (TCI) フィールドの user priority 値) を書き換えます。
 - cos 値指定
書き換え後の cos 値を 0 ～ 7 の範囲の 10 進数で指定します。
 - ip precedence 値
cos 値をパケットの ip precedence 値に書き換えます。
- ip precedence 値書き換え
条件と一致した場合にパケットの ip precedence 値 (IP ヘッダの TOS フィールドの上位 3 ビット) を書き換えます。
 - ip precedence 値指定
書き換え後の ip precedence 値を 0 ～ 7 の範囲の 10 進数で指定します。
 - cos 値
ip precedence 値を cos 値に書き換えます。

- dscp 値書き換え
条件と一致した場合にパケットの dscp 値 (IP ヘッダの TOS フィールドの上位 6 ビット) を書き換えます。書き換え後の dscp 値を 0 ～ 63 の範囲の 10 進数で指定します。
- 出力キュー指定
条件と一致した場合にパケットが出力されるときに使用される出力ポートのキューを変更します。使用する出力ポートのキュー番号を、以下の範囲の 10 進数で指定します。大きい値が出力優先順位がより高いキューであることを表します。

機種	キュー番号
SR-S208TC2、224TC2、 208PD1、224PS1、224CP1、 248TC1、308TL1、310TL2、 316TL1、318TL2、324TL2	0 ～ 3
SR-S316C2、716C2、324TC1、 328TR1、348TC1、724TC1、 748TC1	0 ～ 7

ACL 定義番号

「参照」 ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- MAC 定義
- VLAN 定義
- TCP 定義
IP 定義のプロトコルが 6 の場合だけ有効です。
- UDP 定義
IP 定義のプロトコルが 17 の場合だけ有効です。
- ICMP 定義
IP 定義のプロトコルが 1 の場合だけ有効です。

指定する定義番号欄の「選択」 ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。「OK」 ボタンをクリックして、設定をやり直してください。

「操作」 「設定メニュー」→詳細設定「VLAN 情報」→「追加」→「QoS 情報」→「ACL 定義番号の「参照」

表示条件入力					
表示回数		表示範囲			
10		0~0			
ACL 情報 閉じる					
定義番号	IP 定義	MAC 定義	VLAN 定義	TCP/UDP/ICMP 定義	選択
	プロトコル 送信元IPアドレス/マスク あて先IPアドレス/マスク QoS種別 QoS値	送信元MACアドレス あて先MACアドレス フォーマット種別 LSAP/type値	VLAN ID プライオリティ		
0	すべて	bcast	20		
	192.168.1.0/24	bcast	5		
	any	llc			
	any	1fff			
					選択
閉じる					

「ACL 情報」 - 「追加」 / 「修正」 - 「IP 定義情報」、「MAC 定義情報」および「VLAN 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示回数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。「OK」 ボタンをクリックして、設定をやり直してください。

「QoS 情報」の ACL 定義番号に設定する定義番号欄の「選択」 ボタンをクリックすると、「QoS 情報」に ACL 定義番号が設定され、画面が閉じます。「ACL 定義参照」 ボタンをクリックした場合は、「選択」 ボタンは表示されません。「閉じる」 ボタンをクリックして、画面を閉じてください。

11.8 IPv6 QoS 情報

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→「追加」→「IPv6 QoS 情報」

現在、このVLANに設定されているIPv6 QoS 処理定義のACL 定義が表示されています。処理は優先順位1から順に行われます。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件に一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

SR-S308TL1、310TL2、316TL1、318TL2、324TL2、324TC1、328TR1、348TC1、724TC1、748TC1のみ、「dscp 値書き換え」の項目が表示されます。

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。

IPv6 QoS 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“IPv6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）

☞ 参照 「装置情報」-「資源情報」画面は、[\[4.9 資源情報\] \(P33\)](#) を参照してください。

💡 ヒント

◆ 定義数

● SR-S208TC2/224TC2/208PD1の場合

etherblockごとに10個

指定されたACL 情報の内容によってetherblockごとに30ルール

● SR-S224PS1/224CP1/248TC1の場合

etherblockごとに10個

指定されたACL 情報の内容によってetherblockごとに60～100ルール（認証成功端末数による）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2の場合

装置で128個

指定されたACL 情報の内容によって装置で128ルール

● SR-S316C2/716C2 の場合

ポートごとに 10 個

指定された ACL 情報の内容によってポートごとに 100 ルール

● SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合

装置で 128 個（初期値）

指定された ACL 情報の内容によって装置で 128 ルール（初期値）

定義可能上限値は、「装置情報」-「資源情報」の「フィルタ/QoS 資源の配分」の設定で、最大で 512 個まで拡張することができます。

◆ 優先順位

● SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (2) 「etherblock 情報」-「フィルタ情報」の設定
- (3) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (4) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (5) 「ether 情報」-「QoS 関連」-「QoS 情報」（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (6) 「etherblock 情報」-「QoS 情報」
- (7) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」-「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (10) 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (11) 「VLAN 情報」-「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S316C2/716C2 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定
- (2) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (4) 「ether 情報」-「QoS 関連」-「QoS 情報」
- (5) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (6) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (7) 「VLAN 情報」-「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」-「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2/324TC1/328TR1/348TC1/724TC1 /748TC1 の場合

優先順位は、以下のとおりです。

- (1) 「VLAN 情報」-「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (2) 「LAN 情報」-「IPv6 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）

◆ ルール

● SR-S208TC2/224TC2/208PD1 の場合

ACL の内容によって、以下のように消費するルール数が異なります。

<ルール1>

- 「ether 情報」 - 「フィルタ情報」
- 「etherblock 情報」 - 「フィルタ情報」
- 「VLAN 情報」 - 「フィルタ情報」
- 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- 「etherblock 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「IPv6 フィルタ情報」
- 「VLAN 情報」 - 「IPv6 QoS 情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： TCP または UDP の送信元ポート数 × あて先ポート数 × 2
- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： ICMP の ICMP TYPE の個数 × ICMP CODE の個数 × 2
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： 2
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： 1

<ルール2>

- 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
- 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
- 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 ： TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 ： ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 ： 1

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

ACL の内容によって、以下のように消費するルール数が異なります。それぞれの ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 ： TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 ： ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 ： 1

こんな事に気をつけて

- 自装置 IPv6 アドレスあてパケットやホップバイホップオプション付きパケットなど、ソフト処理となるパケットに対する「LAN 情報」-「IP 関連」-「IP フィルタリング情報」設定や「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」設定、「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」設定はスイッチのフィルタ・QoS 設定上限オーバとなった場合も適用されます。
- 指定した ACL の VLAN 定義で指定された VLAN ID が適用する VLAN ID と矛盾する場合は、QoS 処理されません。
- 以下の設定はすべての etherblock に適用されます。(SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合)
 - 「VLAN 情報」-「IPv6 フィルタ情報」
 - 「VLAN 情報」-「IPv6 QoS 情報」
 - 「LAN 情報」-「IP 関連」-「IPv6 フィルタリング情報」
 - 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」
 - 「VLAN 情報」-「IPv6 フィルタ情報」
 - 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」
 - 「VLAN 情報」-「IPv6 QoS 情報」
- ACL で指定したアクセスコントロールリストが使用するスイッチ内部メモリが上限値を超える場合はフィルタは適用されません。たとえば、指定したアクセスコントロールリスト内の IPv6 定義で、送信元およびあて先 IPv6 アドレスのプレフィックス長の組み合わせで、以下の範囲を超えて指定した場合は、使用するスイッチ内部メモリが上限値を超えるため、フィルタ条件を 2 つのアクセスコントロールリストに分割し適用する必要があります。(SR-S224PS1/224CP1/248TC1/316C2/716C2 の場合)

送信元プレフィックス長の設定ビット数	あて先プレフィックス長の設定可能ビット数
113 ~ 128	0 (ANY) ~ 48
81 ~ 112	0 (ANY) ~ 64
49 ~ 80	0 (ANY) ~ 96
0 (ANY) ~ 48	0 (ANY) ~ 128

また、TCP/UDP/ICMP 条件を any 以外で同時に設定した場合、あて先プレフィックス長の設定可能ビット数が 32bit 減少します。

- 当該 etherblock で、IEEE802.1X 認証成功端末、Web 認証成功端末、MAC アドレス認証成功端末および DHCP スヌープ許可端末の合計が 152 台以下の場合は、ルールによる上限は etherblock ごとに 100 個となりますが、152 台を超えた場合は 1 認証成功端末につき使用可能なルール数が 1 個減少します。(SR-S224PS1/224CP1/248TC1 の場合)
- 自装置 IPv6 アドレスあてパケットは acl 定義に該当した場合も QoS 処理されません。(SR-S716C2 の場合)
- "vlan ip6qos aclmap" コマンド、"lan ip6 dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 200 個まで設定可能です。(SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合)
- "ether macfilter" コマンド、"ether qos aclmap" コマンド、"vlan macfilter" コマンド、"vlan qos aclmap" コマンド、"lan ip filter" コマンド、"lan ip dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 700 個まで設定可能です。(SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合)

動作

QoS 処理の動作を以下の 2 つから選択します。

- dscp 値書き換え
(SR-S308TL1/310TL2/316TL1/318TL2/324TL2/324TC1/328TR1/348TC1/724TC1/748TC1)
条件と一致した場合にパケットの dscp 値 (IP ヘッダの TOS フィールドの上位 6 ビット) を書き換えます。書き換え後の dscp 値を 0 ~ 63 の範囲の 10 進数で指定します。

- 出力キュー指定
条件と一致した場合にパケットが出力されるときに使用される出力ポートのキューを変更します。使用する出力ポートのキュー番号を、以下の範囲の 10 進数で指定します。大きい値が出力優先順位がより高いキューであることを表します。

機種	キュー番号
SR-S208TC2、224TC2、208PD1、224PS1、224CP1、248TC1、308TL1、310TL2、316TL1、318TL2、324TL2	0 ~ 3
SR-S316C2、716C2、324TC1、328TR1、348TC1、724TC1、748TC1	0 ~ 7

ACL 定義番号

〔参照〕 ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
IPv6 定義のプロトコルが 6 の場合だけ有効です。
- UDP 定義
IPv6 定義のプロトコルが 17 の場合だけ有効です。
- ICMP 定義
IPv6 定義のプロトコルが 58 の場合だけ有効です。

指定する定義番号欄の〔選択〕 ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。〔OK〕 ボタンをクリックして、設定をやり直してください。

〔操作〕 「設定メニュー」→詳細設定「VLAN 情報」→〔追加〕→〔IPv6 QoS 情報〕→
「ACL 定義番号の〔参照〕」

表示条件入力				
表示回数		表示範囲		
10		0~0		
■ ACL 情報 開じる				
定義番号	IPv6 定義	TCP/UDP/ICMP 定義	選択	
0	tcp	TCP 定義	選択	
	2001:db8:1111:1000::/64	送信元ポート番号		any
	any	あて先ポート番号		21
	any	UDP 定義		送信元ポート番号
		あて先ポート番号	53	
開じる				

「ACL 情報」 - 〔追加〕／〔修正〕 - 「IPv6 定義情報」、「TCP 定義情報」および「UDP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示回数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。〔OK〕 ボタンをクリックして、設定をやり直してください。

「IPv6 QoS 情報」の ACL 定義番号に設定する定義番号欄の〔選択〕 ボタンをクリックすると、「IPv6 QoS 情報」に ACL 定義番号が設定され、画面が閉じます。〔ACL 定義参照〕 ボタンをクリックした場合は、〔選択〕 ボタンは表示されません。〔閉じる〕 ボタンをクリックして、画面を閉じてください。

11.9 ARP 認証関連

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→[追加]→[ARP 認証関連]

11.9.1 ARP 認証情報

11.9.1.1 ARP 認証情報（初期表示または使用しない選択時）

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→[追加]→[ARP 認証関連]
→[ARP 認証情報（ARP 認証情報：初期表示または使用しない）]

初期表示またはARP 認証情報に“使用しない”を選択した場合に表示されます。

ARP 認証情報

ARP パケットに対して、MAC アドレスの認証を行う場合は、“使用する”を選択します。

“使用する”を選択した場合、ARP パケットに対して送信元端末の MAC アドレスの認証を行い、登録されていなければ syslog を表示します。

11.9.1.2 ARP 認証情報（使用する選択時）

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→[追加]→[ARP 認証関連]
→[ARP 認証情報（ARP 認証情報：使用する）]

■ARP認証情報	
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 時間
ダミーMACアドレス	02:ff:ff:ff:ff:ff
認証成功保持時間	20 分
認証失敗保持時間	20 分
端末数超過時動作	☒ 認証失敗 ☐ 認証成功
認証プロトコル	☒ CHAP ☐ PAP

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

ARP 認証情報に“使用する”を選択した場合に表示されます。

「ARP 認証情報」の項目は、「ARP 認証情報（初期表示または使用する選択時）」を参照してください。

参照する AAA 情報

ARP 認証を行う場合に参照する AAA のグループ ID を、0～9 の範囲の 10 進数で指定します。

省略はできません。

通信妨害

ARP 認証を行った結果、登録されていない MAC アドレスであった場合、その MAC アドレスに対して通信妨害を行うかどうかを設定します。

通信妨害を行う場合、通信妨害間隔を 0 秒および 1～43200 秒の範囲で指定します。0 秒を指定した場合は、通信妨害は認証時のみに行い、定期的な通信妨害は行いません。

省略時は、0 秒が設定されます。

ダミー MAC アドレス

通信妨害を行う場合に使用するダミーの MAC アドレスを指定します。

省略時は、02:ff:ff:ff:ff:ff が設定されます。

こんな事に気をつけて

ネットワーク上に存在しない MAC アドレスを設定してください。存在する MAC アドレスを設定した場合、その MAC アドレスの装置が正常に通信できなくなります。

認証成功保持時間

ARP 認証が成功した場合の保持時間を、60～86400 秒の範囲の 10 進数で指定します。

省略時は、20 分が設定されます。

認証失敗保持時間

ARP 認証が失敗した場合の保持時間を、60～86400 秒の範囲の 10 進数で指定します。

省略時は、20 分が設定されます。

端末数超過時動作

ARP 認証結果を保持可能な端末数を超えた場合の動作を設定します。

認証プロトコル

ARP 認証の認証プロトコルを設定します。

11.9.2 認証不要端末情報

[操作] 「設定メニュー」→詳細設定「VLAN 情報」→[追加]→[ARP 認証関連]→[認証不要端末情報]

■ 認証不要端末情報

※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。

表示条件入力

表示回数

表示範囲

50

定義は存在しません

定義番号

IPアドレス

操作

全削除

< 認証不要端末情報追加フィールド >

IPアドレス

追加

キャンセル

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

ARP パケットに対して、MAC アドレスの認証を行わずに通信を許可する端末を設定します。

IP アドレス

認証しないで通信を許可する端末の IP アドレスを指定します。

有効範囲)

1.0.0.1 ～ 126.255.255.254

128.0.0.1 ～ 191.255.255.254

192.0.0.1 ～ 223.255.255.254

12 MAC 情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「MAC 情報」

MAC 情報		
基本情報	ストーム制御情報	MAC テーブルフラッシュ情報

SR-S208TC2、224TC2、208PD1 のみ、「ストーム制御情報」が表示されます。

12.1 基本情報

[操作] 「設定メニュー」→詳細設定「MAC 情報」→[基本情報]

■基本情報 

自動学習	☒ する ☐ しない
エージアウト時間	300 秒

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

SR-S208TC2、224TC2、208PD1 では、「自動学習」の項目は表示されません。

自動学習（SR-S208TC2、224TC2、208PD1 除く）

MAC 自動学習を有効にする場合は、“する” を選択します。

エージアウト時間

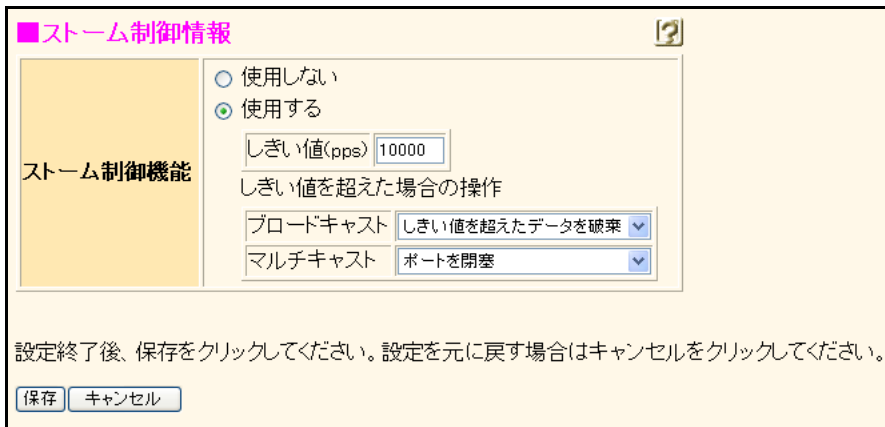
MAC アドレス学習テーブルのエージアウト時間を 10～1000000 秒の範囲の 10 進数で指定します。

省略時は、300 秒が設定されます。

12.2 ストーム制御情報

適用機種 SR-S208TC2, 224TC2, 208PD1

[操作] 「設定メニュー」→詳細設定「MAC 情報」→[ストーム制御情報]



ストーム制御機能

ブロードキャスト／マルチキャストストーム制御を使用する場合は、“使用する”を選択します。

しきい値

ブロードキャストとマルチキャストストームのトラフィックのしきい値を、1秒間のパケット数として、1～200000の範囲の10進数で指定します。

ブロードキャスト

ブロードキャストストームのトラフィックが“しきい値”を超えた場合の動作を選択します。

マルチキャスト

マルチキャストストームのトラフィックが“しきい値”を超えた場合の動作を選択します。

こんな事に気をつけて

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。

12.3 MAC テーブルフラッシュ情報

[操作] 「設定メニュー」→詳細設定「MAC 情報」→[MAC テーブルフラッシュ情報]

現在、設定されている MAC テーブルフラッシュ情報の定義が表示されています。監視する MAC アドレスは、最大 4 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

指定した MAC アドレスの学習ポートの監視を行い、学習しているポートの移動を検出した場合に、移動する前のポートに関連した MAC アドレス学習テーブル情報を初期化します。

MAC アドレス

監視する MAC アドレスを設定します。最後の 1 バイトは設定値にかかわらず、0x00～0xff までの範囲を対象とみなします。

こんな事に気をつけて

- ブロードキャスト、マルチキャストアドレスは指定できません。
- MAC アドレスは、最後の 1 バイトは設定値にかかわらず、0x00～0xff までの範囲指定とみなすため、先頭の 5 バイトの値が重複する指定はできません。
- すでに学習テーブルに登録されている MAC アドレスを監視する場合は、MAC アドレス監視情報の設定反映後、ケーブルを再接続または MAC アドレス学習エントリを初期化してください。

初期化モード

指定した MAC アドレスの学習ポートが移動したときの、MAC アドレス学習テーブルの初期化モードを設定します。

13 LAN 情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「LAN 情報」

LAN情報

LAN情報

■LAN情報

※追加情報は一覧の最後尾の追加フィールドで設定してください。

インタフェース	VLAN ID	プロトコル	操作
LAN0	10	IPv4 使用する [192.168.1.1] IPv6 使用しない	修正 削除

<LAN情報追加フィールド>

VLAN ID

追加 キャンセル

保存した情報は、設定反映後に有効になります。

現在、設定されている LAN インタフェースが表示されています。LAN インタフェースの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

VLAN ID

LAN インタフェースに関連付けする VLAN ID を 1 ～ 4094 の範囲で指定します。

こんな事に気をつけて

- 指定された VLAN ID が未登録の場合、設定は無効となります。
- 指定された VLAN ID が複数の LAN インタフェースで設定された場合は、もっとも定義番号の小さい LAN インタフェースだけが有効となります。

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]

LAN0情報

共通情報	IP関連	IPv6関連
------	------	--------

このページではLAN情報を設定することができます。上記の各関連項目をクリックすると詳細な設定項目が表示されます。

13.1 共通情報

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正] → [共通情報]

LAN0 情報	
共通情報	IP 関連
基本情報	VRRP グループ情報

SR-S716C2、724TC1、748TC1 のみ、「VRRP グループ情報」が表示されます。

13.1.1 基本情報

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正] → [共通情報] → [基本情報]

■ 基本情報

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

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

SR-S724TC1、748TC1 のみ、「VRRP 機能」の「TRAP モード」の設定項目が表示されます。

VLAN ID

LAN インタフェースに関連付けする VLAN ID を 1～4094 の範囲で指定します。

こんな事に気をつけて

- 指定された VLAN ID が未登録の場合、設定は無効となります。
- 指定された VLAN ID が複数の LAN インタフェースで設定された場合は、もっとも定義番号の小さい LAN インタフェースだけが有効となります。

VRRP 機能 (SR-S716C2、724TC1、748TC1)

VRRP 機能を使用する場合は、“使用する”を選択します。VRRP を使用するとルータの冗長構成を組むことができます。VRRP を使用しない場合は、以降の設定は無効になります。

パスワード

マスタが送信する Advertisement パケットに認証情報を含める場合に、パスワードを 8 文字以内で指定します。このインタフェースから送信されるすべての Advertisement パケットに適用されます。たとえば、同じネットワークでグループ ID を重複させて別グループとして扱う、などの特別な環境である場合に設定します。

なお、仮想 IP アドレスが IPv6 アドレスである VRRP グループは、パスワードを設定した場合であっても Advertisement パケットに認証情報は含まれません。

TRAP モード (SR-S724TC1、748TC1)

- 旧仕様
IPv4 VRRP が送信する TRAP モードとして旧仕様 (RFC2787) を使用します。
- 新仕様
IPv4 VRRP が送信する TRAP モードとして新仕様 (draft-ietf-vrrp-unified-mib-06) を使用します。

こんな事に気をつけて

仮想 IP アドレスが IPv6 アドレスである VRRP グループは、“旧仕様”を選択した場合であっても“新仕様”を使用します。

13.1.2 VRRP グループ情報

適用機種 SR-S716C2, 724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[共通情報]→[VRRP グループ情報]

■VRRPグループ情報						
グループ番号	グループID	プライオリティ	AD送信間隔	プリエンプトモード	仮想IPアドレス	操作
0	-	-	-	-	-	修正 削除
1	-	-	-	-	-	修正 削除

保存した情報は、設定反映後に有効になります。

現在、このインタフェースに設定されている VRRP グループ情報の定義が表示されています。VRRP グループは、それぞれのインタフェースで2個まで、かつ装置全体で最大20個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[共通情報]→[VRRP グループ情報]
→[修正]

LAN01情報 - VRRPグループ0情報	
基本情報	VRRPトリガ情報

13.1.2.1 基本情報

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[共通情報]→[VRRP グループ情報]
→[修正]→[基本情報]

■基本情報	
グループID	
プライオリティ	☒ 優先度指定 優先度 仮想IPアドレス ☐ 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
プリエンプトモード	☒ ON ☐ OFF 移行禁止時間 0 秒
仮想IPアドレスあて ICMP ECHO	☒ 応答しない ☐ 応答する 応答送信元 IPアドレス ☒ 仮想IPアドレス ☐ インタフェースアドレス

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

SR-S716C2 では、表示が上記の画面とは異なります。

グループID

VRRP グループのグループID を1～255の範囲で指定します。VRRP グループは、指定したグループID で識別（グループ化）されます。グループID は、装置内で重複しないように指定してください。

プライオリティ

優先度指定または優先度固定（最優先）を選択します。

- **優先度指定**
優先度および仮想IPアドレスを設定します。VRRP グループ内で1番プライオリティが高いグループメンバがマスタとなります。プライオリティは数値が大きいほど高くなります。
優先度は、なるべくグループ内で差をつけるように設定してください。トリガを使用する場合は、優先度に1を指定しないでください。また、トリガを使用する場合は、“優先度固定（最優先）”を選択すると該当グループがバックアップ状態となったときにVRRP が設定されたLANが通信不能となるため、“優先度指定”を選択してください。
- **優先度固定（最優先）**
プライオリティが255であるVRRP グループメンバとして動作します。また、仮想IPアドレスはこのインタフェースのIPアドレスとなります。
SR-S724TC1/748TC1 では、IPv4 または IPv6 のどちらかを選択します。

優先度

プライオリティの優先度指定を選択した場合に、1～254の範囲で指定します。

仮想IPアドレス

プライオリティの優先度指定を選択した場合に、VRRP グループ内では、同じ仮想IPアドレスを指定します。VRRP グループ内に優先度固定（最優先）と設定されたVRRP グループメンバが存在する場合は、そのメンバに設定されたインタフェースのIPアドレスを指定します。自装置のインタフェースに設定されたIPアドレスを指定しないでください。

有効範囲)

10.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

fe80::1～fe80::ffff:ffff:ffff:ffff

AD 送信間隔

マスタが送信する Advertisement パケットの送信間隔を1～255秒の範囲で指定します。VRRP グループ内では同じ値を使用します。本装置とVRRPを構成するほかの装置にも同じ値を指定します。省略時は、1秒が設定されます。

プリエンプトモード

通常は、“ON”を選択します。

“OFF”を選択した場合、自装置VRRP グループメンバの優先度が高くても、マスタである他装置のVRRP グループメンバがすでに存在すると、マスタになることはできません。“OFF”を選択した場合は、ネットワークの状態が不安定で、マスタの交代が頻繁に発生する場合に有効です。移行禁止時間（秒）は、マスタより先にバックアップのシステムが立ち上がり、本来マスタになるべきVRRP グループに制御が移らないのを防ぎます。

移行禁止時間

システム立ち上がりからプリエンプトモードOFF状態を抑止する時間です。0～900秒の範囲で指定します。省略時は、0秒が設定されます。

仮想IPアドレスあてICMP ECHO

仮想IPアドレスあてICMP ECHO パケットに応答する場合は、“応答する”を選択します。

“応答する”を選択した場合は、応答パケットの送信元IPアドレスを設定します。

応答送信元IPアドレス

“仮想IPアドレス”または“インタフェースアドレス”のどちらかを選択します。

13.1.2.2 VRRP トリガ情報

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[共通情報]→[VRRP グループ情報]
→[修正]→[VRRP トリガ情報]

■VRRPトリガ情報
※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。

トリガ定義番号	トリガ種別	減算プライオリティ	インタフェース	あて先IPアドレス	操作
全削除					
<VRRPトリガ情報入力フィールド>					
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 すべて				
	☐ ルートダウントリガ(route) ネットワーク ☒ IPv4デフォルトルート ☐ IPv6デフォルトルート ☐ 経路を指定する ※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。				
	インタフェース 指定なし				
	☐ ノードダウントリガ(node) あて先IPアドレス				
	送出インタフェース 指定なし 再送間隔 5 秒 タイムアウト時間 16 秒 正常時送信間隔 17 秒 異常時送信間隔 30 秒				
追加 キャンセル					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、このVRRPグループメンバに設定されているVRRPトリガ情報の定義が表示されています。VRRPトリガの定義数は、仕様一覧「2.3 システム最大値一覧」(P53)を参照してください。処理するボタンをクリックし、次のページへ進みます。

設定した条件が発生した場合に、該当するVRRPグループメンバの優先度を下げます。条件にあてはまるすべてのトリガに適用されます。このインタフェースに異常が発生しない限り、減算されるプライオリティの最小は1です。

SR-S724TC1、748TC1以外では、トリガ種別のネットワークの表示が上記の画面とは異なります。

減算プライオリティ

設定した条件が発生した場合、「VRRP グループ情報」の[基本情報]で設定したプライオリティを減算する値を1～254の範囲で指定します（プライオリティ1より低い値までは減算されません）。省略時は、254が設定されます。

トリガ種別

トリガとなる種別を以下の3つから選択します。

- インタフェースダウントリガ (ifdown)
指定されたインタフェースがダウンした場合にトリガを適用します。有効ではないインタフェースは動作上、無視されます。
- ルートダウントリガ (route)
指定された経路情報が存在しない、または中継インタフェースが変化した場合にトリガを適用します。
- ノードダウントリガ (node)
設定したノードに対して ICMP ECHO パケットを送信します。応答がタイムアウトした場合にトリガを適用します。
あて先 IP アドレスが IPv4 アドレスの場合は、ICMP ECHO パケット送信元 IP アドレスは、VRRP が設定された LAN インタフェースの IPv4 アドレスとなります。応答を受信するための経路情報が正しくない場合は、不当に異常を検出することがあります。
あて先 IP アドレスが IPv6 アドレスの場合は、プロトコルが選択した本装置 IPv6 アドレスが送信元 IP アドレスとなります。

インタフェース

トリガの対象となるインタフェースを選択します。

インタフェースダウントリガ (ifdown) を指定する場合

“すべて” を選択した場合は、すべての LAN インタフェースが対象です。

ルートダウントリガ (route) を指定する場合

“指定なし” を選択した場合は、経路情報が存在すればトリガは適用されません。それ以外では経路情報によるパケット送出インタフェースが設定と異なる、または経路情報が存在しない場合にトリガが適用されます。

ネットワーク (SR-S724TC1、748TC1)

“IPv4 デフォルトルート”、“IPv6 デフォルトルート”または“経路を指定する”を選択します。

“経路を指定する”を選択した場合は、IPv4 アドレス/マスクビット形式または IPv6 アドレス/プレフィックス長形式で指定します。

IPv4 アドレスを指定する場合

あて先または中継先ネットワークの IPv4 アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に有効な記述形式を示します。

IPv4 アドレス/マスクビット数

(例: 192.168.1.0/24)

IPv4 アドレス/マスク値

(例: 192.168.1.0/255.255.255.0)

また、0.0.0.0/0 (0.0.0.0/0.0.0.0) を指定した場合は、IPv4 デフォルトルートとなります。

IPv6 アドレスを指定する場合

あて先または中継先ネットワークの IPv6 アドレスとプレフィックス長の組み合わせを指定します。マルチキャストアドレスやリンクローカルアドレスは指定できません。また、::/0 以外の組み合わせでの :: やプレフィックス長 0 も指定できません。

::/0 を指定した場合は、IPv6 デフォルトルートとなります。

ネットワーク (SR-S724TC1、748TC1 以外)

“デフォルトルート”または“経路を指定する”を選択します。

“経路を指定する”を選択した場合は、以降のあて先 IP アドレス、あて先アドレスマスクを設定します。

あて先 IP アドレス/あて先アドレスマスク

あて先 IP アドレスとあて先アドレスマスクでホスト経路またはネットワーク経路を設定します。

あて先 IP アドレス

ICMP ECHO パケットの送出先 IP アドレスを指定します。IP アドレスは、以下の範囲で指定します。

有効範囲) (SR-S724TC1/748TC1)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.25.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fe80:: ~ fe80::ffff:ffff:ffff:ffff

有効範囲) (SR-S724TC1/748TC1 以外)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.25.255.254

192.0.0.1 ~ 223.255.255.254

送出インタフェース

ICMP ECHO パケットを送出するインタフェースを指定します。“指定なし”の場合は送出時の経路情報によって決定されます。

こんな事に気をつけて

SR-S724TC1/748TC1 で、あて先 IP アドレスに IPv6 リンクローカルアドレスを設定した場合は、その IPv6 リンクローカルアドレスのインタフェースを指定してください。

再送間隔

ICMP ECHO パケットの応答が受信されない場合に、再送する時間を 1 ～ 60 秒の範囲で指定します。送信から指定した再送間隔まで応答がない場合に、ICMP ECHO パケットを再送します。省略時は、5 秒が設定されます。

タイムアウト時間

ICMP ECHO パケットの再送を繰り返しても応答が受信されず、タイムアウトするまでの時間を、([再送間隔+1] ～ 240) 秒の範囲で指定します。タイムアウトによって、トリガが適用されます。省略時は、(再送間隔×3+1) 秒が設定されます。

正常時送信間隔

ICMP ECHO パケットの応答が正常に受信されている状態で、次に ICMP ECHO パケットを送信する時間を、([タイムアウト時間+1] ～ 255) 秒の範囲で指定します。正常に受信されている状態での周期送信間隔です。省略時は、タイムアウト時間+1 秒が設定されます。

異常時送信間隔

ICMP ECHO パケットのタイムアウトが発生してから応答が受信されるまでの、周期送信する間隔を 1 ～ 255 秒の範囲で指定します。応答が受信された場合は、トリガを適用しないで正常状態に戻ります。省略時は、30 秒が設定されます。

13.2 IP 関連

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]

LAN0情報		
共通情報	IP関連	IPv6関連
IPアドレス情報	RIP情報	OSPF情報
スタティック経路情報	IPフィルタリング情報	RIPフィルタリング情報
DSCP値書き換え情報	DHCP情報	マルチキャスト情報
ARP情報	スタティックARP情報	

SR-S716C2、724TC1、748TC1 のみ、「RIP 情報」、「OSPF 情報」、「RIP フィルタリング情報」、「マルチキャスト情報」および「ARP 情報」が表示されます。

13.2.1 IP アドレス情報

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[IP アドレス情報]

■IPアドレス情報

IPアドレス

192.168.1.1

ネットマスク

2 (192.0.0.0)

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

※DHCPのサーバ機能使用時、IPアドレスを変更する場合は DHCP 機能の“割当て先頭アドレス”も確認してください。

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

このインタフェースのIPアドレス情報を設定します。

IP アドレス

本装置のIPアドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

こんな事に気をつけて

IPアドレスに0.0.0.0を指定すると通信ができなくなります。

ネットマスク

本装置のネットマスクを指定します。

ブロードキャストアドレス

ブロードキャストアドレスを以下から選択します。通常は、“ネットワークアドレス+オール1”を選択します。

- 0.0.0.0
- 255.255.255.255
- ネットワークアドレス+オール0
(ネットワークアドレスのホスト部をオール0にしたもの)
- ネットワークアドレス+オール1
(ネットワークアドレスのホスト部をオール1にしたもの)

13.2.2 RIP 情報

適用機種 SR-S716C2, 724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[RIP 情報]

RIP 情報

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

0

《 RIP V2 使用時に認証バケットを破棄しない時は RIP V2 パスワードを設定してください。》

認証バケット

☐ 破棄する
☒ 破棄しない

パスワード

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

RIP を使用できるインターフェースの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

RIP 機能は、IP フォワーディングの設定がされている場合にだけ有効となります。

RIP 送信

RIP 情報を送信するかどうかを選択します。送信する設定にすると、RIP 情報を定期的に送信します。RIP 送信を行う場合は、RIP の種類を選択します。

- V1 で送信する
ルーティングプロトコルに RIP V1 を使用し、ブロードキャストで送信します。
- V2 で送信する
ルーティングプロトコルに RIP V2 を使用し、ブロードキャストで送信します。
- V2 (Multicast) で送信する
ルーティングプロトコルに RIP V2 を使用し、マルチキャストで送信します。

RIP 受信

RIP 情報を受信するかどうかを選択します。RIP 受信を行う場合は、RIP の種類を選択します。

- V1 で受信する
ルーティングプロトコルに RIP V1 を使用し、受信します。
- V2、V2 (Multicast) で受信する
ルーティングプロトコルに RIP V2 を使用し、ブロードキャストおよびマルチキャストを受信します。

メトリック値

RIP 送信時に加算するメトリック値を選択します。

認証パケット

RIP V2 使用時にだけ有効な設定です。RIP V2 では、同じパスワードグループでだけ RIP 情報の交換を行うことができます。パスワード認証による RIP 情報の交換を行う場合は、“破棄しない”を選択し、パスワードを16文字以内で指定します。“破棄する”を選択した場合は、パスワード認証による RIP 情報の交換は行いません。

13.2.3 OSPF 情報

適用機種 SR-S716C2, 724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[OSPF 情報]

■OSPF情報

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パケット送信間隔

10 秒

隣接ルータ停止確認間隔

40 秒

パケット再送間隔

5 秒

LSUパ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認証鍵ID

MD5認証鍵

パケット送信

☐ 抑止する
☒ 抑止しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

ループバックインタフェースも含めて、OSPF を使用できるインタフェースの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。

こんな事に気をつけて

OSPF 機能は、IP フォワーディングの設定がされている場合にだけ有効となります。

OSPF 機能

OSPF を使用する場合は、“使用する”を選択します。

エリア定義番号

エリアの定義番号を10進数で指定します。OSPF エリア情報は、「ルーティングプロトコル情報」-「OSPF 関連」で設定することができます。省略時は、0が設定されます。

出力コスト

OSPF 出力コストを 1～65535 の範囲で指定します。省略時は、1 が設定されます。

指定ルータ優先度

指定ルータおよび副指定ルータを決定するための優先度を 0～255 の範囲で指定します。値が大きいほど優先度は高くなります。省略時は、1 が設定されます。

こんな事に気をつけて

値が 0 の場合は、指定ルータおよび副指定ルータにはなりません。

Hello パケット送信間隔

OSPF 隣接関係の維持に使用する、Hello パケットの送信間隔を指定します。通常は、10 秒を指定します。

有効範囲)
1～18 時間
1～1092 分
1～65535 秒

こんな事に気をつけて

OSPF 隣接ルータ間で同じ Hello パケットの送信間隔を指定してください。

隣接ルータ停止確認間隔

OSPF 隣接関係の維持に使用する、隣接ルータ停止確認間隔を指定します。隣接ルータ停止確認間隔は、Hello パケット送信間隔より大きな値を指定する必要があります。Hello パケット送信間隔の 4 倍を設定することをお勧めします。通常は、40 秒を指定します。

有効範囲)
1～18 時間
1～1092 分
1～65535 秒

こんな事に気をつけて

OSPF 隣接ルータ間で同じ隣接ルータ停止確認間隔を指定してください。隣接ルータ停止確認間隔は、装置起動時に指定ルータおよび副指定ルータの選出を開始するまでの待機時間にも使用されます。大きな値を指定した場合は、経路交換の開始が遅れます。

パケット再送間隔

OSPF パケットを再送する間隔を指定します。省略時は、5 秒が設定されます。

有効範囲)
1～18 時間
1～1092 分
3～65535 秒

LSU パケット送信遅延時間

LSU (Link State Update) パケットの送信遅延時間を指定します。LSU パケットでは、LSA (Link State Advertisement) を作成してからの経過時間に対し、この設定時間を加算して広報します。省略時は、1 秒が設定されます。

有効範囲)
1～18 時間
1～1092 分
1～65535 秒

こんな事に気をつけて

一般的な装置では、LSU を作成してからの経過時間が 1 時間となった LSA を破棄します。このため、LSU 送信遅延時間に 1 時間以上を設定した場合は、正しくルーティングできない場合があります。

認証方式

パケット認証方式を選択します。

鍵種別

テキスト認証で使用する鍵の種別を選択します。

認証鍵

テキスト認証で使用する鍵を指定します。鍵種別が“文字列”の場合は、8 文字以内で指定します。鍵種別が“16 進数”の場合は、16 進数を使用して 16 桁以内で指定します。16 桁未満の鍵を指定した場合、左詰めで設定され、残りは 16 桁になるまで 0x0 でパディングされます。

MD5 認証鍵 ID

MD5 認証鍵 ID を 1～255 の範囲で指定します。

MD5 認証鍵

MD5 認証鍵を指定します。16 文字以内で指定します。

パケット送信

OSPFパケットの送信を抑止する場合は、“抑止する”を選択します。

13.2.4 スタティック経路情報

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[スタティック経路情報]

■スタティック経路情報

※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。

あて先IPアドレス/マスク	中継ルータアドレス	メトリック値	優先度	操作
全削除				

<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

あて先アドレスマスク

中継ルータアドレス

メトリック値

優先度

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、設定されているスタティック経路情報の定義が表示されています。スタティック経路の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53)を参照してください。処理するボタンをクリックし、次のページへ進みます。

SR-S716C2、724TC1、748TC1のみ、「メトリック値」の項目が表示されます。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。

- デフォルトルート
中継ルータアドレスを指定します。
- 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、中継ルータアドレスを指定します。なお、あて先IPアドレスに0.0.0.0、あて先アドレスマスクに0 (0.0.0.0)を設定した場合、“デフォルトルート”を指定したものとして動作します。

メトリック値

(SR-S716C2、724TC1、748TC1)

スタティック経路情報をRIPに再配布するときのメトリック値を、1～14から選択します。RIPに再配布したときは、設定したRIPメトリック値+1のメトリック値でRIPテーブルに登録されます。

優先度

スタティック経路情報の優先度を1～254の範囲の10進数で指定します。優先度は数値の小さい方がより高い優先度を示します。

SR-S716C2、724TC1、748TC1 の場合

スタティック経路情報以外の優先度には、以下の初期値が設定されています。

プロトコル	優先度
OSPF	110
RIP	120

複数のスタティック経路情報でECMP機能を使用するときは、あて先、RIPメトリック値、優先度がそれぞれ同じとなるようにスタティック経路情報を設定します。また、ECMP機能を使用する場合は、「ルーティングプロトコル情報」 - 「ルーティングマネージャ情報」にあるECMP情報で、ECMPを使用するように設定します。ECMPとなるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で4個まで定義できます。

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定するときは、以下の点に注意してください。

- 優先度が同じで、メトリック値が違うスタティック経路情報は同時に設定できません。
- デフォルトルートは、同じ優先度で複数設定することはできません（ECMPとして設定できません）。

13.2.5 IP フィルタリング情報

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[IP フィルタリング情報]

現在、このネットワークに設定されている IP フィルタリング情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

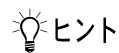
こんな事に気をつけて

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。

IP フィルタリング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)

☞ 参照 「装置情報」-「資源情報」画面は、[「4.9 資源情報」\(P33\)](#) を参照してください。



ヒント

◆ フィルタの定義数

● SR-S208TC2/224TC2/208PD1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 30 ルール

● SR-S224PS1/224CP1/248TC1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 60～100 ルール（認証成功端末数による）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合

装置で 128 個

指定された ACL 情報の内容によって装置で 128 ルール

● SR-S316C2/716C2 の場合

ポートごとに 10 個

指定された ACL 情報の内容によってポートごとに 100 ルール

● SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合

装置で 128 個（初期値）

指定された ACL 情報の内容によって装置で 128 ルール（初期値）

定義可能上限値は、「装置情報」 - 「資源情報」の「フィルタ/QoS 資源の配分」の設定で、最大で 512 個まで拡張することができます。

◆ 優先順位

● SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」 - 「フィルタ情報」の設定（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (2) 「etherblock 情報」 - 「フィルタ情報」の設定
- (3) 「VLAN 情報」 - 「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (4) 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (5) 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (6) 「etherblock 情報」 - 「QoS 情報」
- (7) 「VLAN 情報」 - 「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」 - 「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (10) 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (11) 「VLAN 情報」 - 「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S316C2/716C2 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」 - 「フィルタ情報」の設定
- (2) 「VLAN 情報」 - 「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (4) 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- (5) 「VLAN 情報」 - 「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (6) 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (7) 「VLAN 情報」 - 「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」 - 「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2/324TC1/328TR1/348TC1/724TC1 /748TC1 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」 - 「フィルタ情報」の設定
- (2) 「VLAN 情報」 - 「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）

◆ ルール

● SR-S208TC2/224TC2/208PD1 の場合

ACL の内容によって、以下のように消費するルール数が異なります。

<ルール1>

- 「ether 情報」 - 「フィルタ情報」
- 「etherblock 情報」 - 「フィルタ情報」
- 「VLAN 情報」 - 「フィルタ情報」
- 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- 「etherblock 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「IPv6 フィルタ情報」
- 「VLAN 情報」 - 「IPv6 QoS 情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: TCP または UDP の送信元ポート数 × あて先ポート数 × 2
- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: ICMP の ICMP TYPE の個数 × ICMP CODE の個数 × 2
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: 2
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: 1

<ルール2>

- 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
- 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
- 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

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

ACL の内容によって、以下のように消費するルール数が異なります。それぞれの ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

こんな事に気をつけて

- 自装置 IP アドレスあてパケットや IP オプション付きパケットなど、ソフト処理となるパケットに対する「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」設定や「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」設定はスイッチのフィルタ・QoS 設定上限オーバとなった場合も適用されます。
- WWW や DHCP に対するアクセスを制限する設定を行った場合、WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。
- 以下の設定はすべての etherblock に適用されます。(SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合)
 - 「VLAN 情報」 - 「フィルタ情報」
 - 「VLAN 情報」 - 「QoS 情報」
 - 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
 - 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
 - 「VLAN 情報」 - 「IPv6 フィルタ情報」
 - 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」
 - 「VLAN 情報」 - 「IPv6 QoS 情報」
- 当該 etherblock で、IEEE802.1X 認証成功端末、Web 認証成功端末、MAC アドレス認証成功端末および DHCP スヌープ許可端末の合計が 152 台以下の場合、ルールによる上限は etherblock ごとに 100 個となりますが、152 台を超えた場合は 1 認証成功端末につき使用可能なルール数が 1 個減少します。(SR-S224PS1/224CP1/248TC1 の場合)
- "ether macfilter" コマンド、"vlan macfilter" コマンド、"lan ip filter" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 200 個まで設定可能です。(SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合)
- "ether macfilter" コマンド、"ether qos aclmap" コマンド、"vlan macfilter" コマンド、"vlan qos aclmap" コマンド、"lan ip filter" コマンド、"lan ip dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 700 個まで設定可能です。(SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合)

動作

IP フィルタリングの動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- TCP 定義
IP 定義のプロトコルが 6 の場合にのみ有効です。
- UDP 定義
IP 定義のプロトコルが 17 の場合にのみ有効です。
- ICMP 定義
IP 定義のプロトコルが 1 の場合にのみ有効です。

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[IP フィルタリング情報]
→「ACL 定義番号の [参照]」

表示条件入力			
表示個数		表示範囲	
10		0~0	
ACL 情報 開じる			
定義番号	IP 定義	TCP/UDP/ICMP 定義	選択
0	プロトコル 送信元IPアドレス/マスク 宛て先IPアドレス/マスク QoS種別 QoS値		選択
	すべて 192.168.1.0/24 any any		
開じる			

「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IP フィルタリング情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「IP フィルタリング情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

13.2.6 RIP フィルタリング情報

適用機種 SR-S716C2, 724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[RIP フィルタリング情報]

■RIP フィルタリング情報

※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。

優先順位	動作	方向	フィルタリング条件	メトリック値	操作
全削除					
<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				
	アドレスマスク	0 (0.0.0.0)			
メトリック値					
追加 キャンセル					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている RIP フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。RIP フィルタリングの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

動作

フィルタリング条件に該当する RIP 経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

方向

フィルタリング条件に該当するかチェックするタイミングを以下の 2 つから選択します。

- 受信
RIP パケット受信時に、フィルタリング条件に該当するかチェックします。
- 送信
RIP パケット送信時に、フィルタリング条件に該当するかチェックします。

フィルタリング条件

フィルタリング条件を選択します。

- すべて
すべての経路情報がフィルタリングの対象となります。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、RIP 経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。なお、IP アドレスに 0.0.0.0、アドレスマスクに 0 を指定した場合、デフォルトルートをフィルタリング対象とします。

検索条件

- 完全に一致
指定したIPアドレスとアドレスマスクが完全に一致したRIP経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したIPアドレスと、RIP経路情報のそれぞれを、指定したアドレスマスクでマスクした結果が一致した場合、そのRIP経路情報をフィルタリング対象とします。

メトリック値

フィルタリング結果で透過になったRIP経路情報のメトリック値を変更できます。送信時のRIP経路にメトリック値を設定した場合、「RIP情報」で設定した加算メトリック値は加算されません。省略または0を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

フィルタリング条件で“すべて”を選択したときは、メトリック値を設定しても無効となります。

13.2.7 DSCP 値書き換え情報

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[DSCP 値書き換え情報]

現在、このネットワークに設定されている DSCP 値書き換え情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された DSCP 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

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。

DSCP 値書き換え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)

☞ 参照 「装置情報」-「資源情報」画面は、[\[4.9 資源情報\] \(P33\)](#) を参照してください。

💡 ヒント

◆ 定義数

● SR-S208TC2/224TC2/208PD1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 30 ルール

● SR-S224PS1/224CP1/248TC1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 60～100 ルール（認証成功端末数による）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合

装置で 128 個

指定された ACL 情報の内容によって装置で 128 ルール

● SR-S316C2/716C2 の場合

ポートごとに 10 個

指定された ACL 情報の内容によってポートごとに 100 ルール

● SR-S324TC1/328TR1/348TC1/724TC1 /748TC1 の場合

装置で 128 個（初期値）

指定された ACL 情報の内容によって装置で 128 ルール（初期値）

定義可能上限値は、「装置情報」-「資源情報」の「フィルタ/QoS 資源の配分」の設定で、最大で 512 個まで拡張することができます。

◆ 優先順位**● SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合**

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (2) 「etherblock 情報」-「フィルタ情報」の設定
- (3) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (4) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (5) 「ether 情報」-「QoS 関連」-「QoS 情報」（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (6) 「etherblock 情報」-「QoS 情報」
- (7) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」-「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (10) 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (11) 「VLAN 情報」-「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S316C2/716C2 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定
- (2) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (4) 「ether 情報」-「QoS 関連」-「QoS 情報」
- (5) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (6) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (7) 「VLAN 情報」-「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」-「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2/324TC1/328TR1/348TC1/724TC1 /748TC1 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「QoS 関連」-「QoS 情報」
- (2) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）

◆ ルール

● SR-S208TC2/224TC2/208PD1 の場合

ACL の内容によって、以下のように消費するルール数が異なります。

<ルール1>

- 「ether 情報」 - 「フィルタ情報」
- 「etherblock 情報」 - 「フィルタ情報」
- 「VLAN 情報」 - 「フィルタ情報」
- 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- 「etherblock 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「IPv6 フィルタ情報」
- 「VLAN 情報」 - 「IPv6 QoS 情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： TCP または UDP の送信元ポート数 × あて先ポート数 × 2
- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： ICMP の ICMP TYPE の個数 × ICMP CODE の個数 × 2
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
： 2
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
： 1

<ルール2>

- 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
- 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
- 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

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

ACL の内容によって、以下のように消費するルール数が異なります。それぞれの ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

こんな事に気をつけて

- 自装置 IP アドレスあてパケットや IP オプション付きパケットなど、ソフト処理となるパケットに対する「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」設定や「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」設定はスイッチのフィルタ・QoS 設定上限オーバとなった場合も適用されます。
- 以下の設定はすべての etherblock に適用されます。(SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合)
 - 「VLAN 情報」 - 「フィルタ情報」
 - 「VLAN 情報」 - 「QoS 情報」
 - 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
 - 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
 - 「VLAN 情報」 - 「IPv6 フィルタ情報」
 - 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」
 - 「VLAN 情報」 - 「IPv6 QoS 情報」
- 当該 etherblock で、IEEE802.1X 認証成功端末、Web 認証成功端末、MAC アドレス認証成功端末および DHCP スヌープ許可端末の合計が 152 台以下の場合は、ルールによる上限は etherblock ごとに 100 個となりますが、152 台を超えた場合は 1 認証成功端末につき使用可能なルール数が 1 個減少します。(SR-S224PS1/224CP1/248TC1 の場合)
- "ether qos aclmap" コマンド、"vlan qos aclmap" コマンド、"lan ip dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 200 個まで設定可能です。(SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合)
- "ether macfilter" コマンド、"ether qos aclmap" コマンド、"vlan macfilter" コマンド、"vlan qos aclmap" コマンド、"lan ip filter" コマンド、"lan ip dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 700 個まで設定可能です。(SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合)

新 DSCP

IP パケットに新しく指定する DSCP フィールド値を 0～63 の範囲の 10 進数で指定します。

ACL 定義番号

〔参照〕 ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- TCP 定義
IP 定義のプロトコルが 6 の場合だけ有効です。
- UDP 定義
IP 定義のプロトコルが 17 の場合だけ有効です。
- ICMP 定義
IP 定義のプロトコルが 1 の場合だけ有効です。

指定する定義番号欄の〔選択〕ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。〔OK〕ボタンをクリックして、設定をやり直してください。

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[DSCP 値書き換え情報]
→「ACL 定義番号の [参照]」

表示条件入力			
表示個数		表示範囲	
10		0~0	
■ACL 情報 閉じる			
定義番号	IP 定義	TCP/UDP/ICMP 定義	選択
0	すべて		
	192.168.1.0/24		
	any		選択
	any		
閉じる			

「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「DSCP 値書き換え情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「DSCP 値書き換え情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

13.2.8 DHCP 情報

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[DHCP 情報]

■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

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

☐ サーバ機能を使用する

割当て先頭IPアドレス

割当てアドレス数

リース期間

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

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

※“割当て先頭アドレス”が本装置のIPアドレスと同じネットワークアドレス内であることを確認してください。

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

SR-S716C2、724TC1、748TC1のみ、「リレー機能を使用する」が表示されます。

DHCP 機能

それぞれのインタフェースのDHCP 機能を設定することができます。

- 使用しない
DHCP 機能を使用しません。
- リレー機能を使用する (SR-S716C2/724TC1/748TC1)
ほかのネットワークのDHCP サーバを、このネットワークのDHCP サーバとして使用することもできます。その場合は、利用するDHCP サーバのIPアドレスを指定します。
- サーバ機能を使用する
本装置を該当インタフェースのネットワークのDHCP サーバとして使用します。

割当て先頭 IP アドレス

DHCP サーバ機能によって、割り当てる連続したアドレス群の先頭のIPアドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254

割当てアドレス数

DHCP サーバ機能で割り当てるアドレス数を 1～253 の範囲で指定します。省略時は、32 が設定されます。

ホストデータベース機能を使用すると、特定の DHCP クライアントに対して固有の IP アドレスを割り当てることができます。この場合の IP アドレスは、割当て先頭 IP アドレスと割当てアドレス数によって規定される動的割り当て範囲である必要はありません。

リース期間

DHCP サーバ機能によって割り当てた IP アドレスを貸し出す期間を、0 秒～365 日の範囲で指定します。なお、指定された 10 秒以下の値は切り上げられます。0 を指定した場合は、無期限が設定されます。省略時は、1 日が設定されます。

デフォルトルータ広報

DHCP サーバで広報するデフォルトルータの IP アドレスを指定します。省略するか 0.0.0.0 を指定すると DHCP サーバによる広報は行いません。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

DNS サーバ広報

DNS サーバの IP アドレスを指定します。省略するか 0.0.0.0 を指定すると DHCP サーバによる広報は行いません。ProxyDNS を使用する場合は、本装置の IP アドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

セカンダリ DNS サーバ広報

セカンダリ DNS サーバの IP アドレスを指定します。省略するか 0.0.0.0 を指定すると DHCP サーバによる広報は行いません。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

ドメイン名広報

ドメイン名を 80 文字以内で指定します。省略時は、DHCP サーバによる広報は行いません。

なお、RFC1034 では英数字、“-”（ハイフン）、“.”（ピリオド）でドメイン名をつけることを推奨しています。

MAC アドレスチェック

DHCP サーバおよび DHCP リレーエージェント機能を使用する際、DHCP クライアントの MAC アドレスチェックを行うかどうかを選択します。

- ホストデータベース
ホストデータベース情報を使用します。
- AAA
AAA 情報を使用します。
参照する AAA 情報のグループ ID を 0～9 の範囲の 10 進数で指定します。
認証プロトコルを CHAP と PAP から選択します。

こんな事に気をつけて

MAC アドレスチェック機能を使用する場合、必要に応じて、ホストデータベース情報、AAA ユーザ情報、RADIUS 情報を設定してください。ホストデータベース情報と AAA 情報の両方を使用する場合、ホストデータベース情報が優先されます。

13.2.9 マルチキャスト情報

適用機種 SR-S716C2, 724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[マルチキャスト情報]

マルチキャストを使用できるインタフェースの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。

マルチキャスト機能

LAN 上でマルチキャスト機能を使用する場合は、マルチキャスト・プロトコルを選択します。

こんな事に気をつけて

- マルチキャスト機能を使用するすべてのインタフェース上で、同じプロトコルを選択してください。同時に複数のプロトコルを使用することはできません。
- NAT 機能と併用することはできません。

PIM プリファレンス値

PIM の Assert メッセージに格納されるプリファレンス値を 1～65535 の範囲の 10 進数で指定します。初期値は 1024 です。

並列な経路の存在のためにマルチキャストパケットが重複した場合は、PIM Assert メッセージによって、片側の転送経路が遮断されます。この際、プリファレンス値の小さい方の経路が有効になります。PIM Assert メッセージの発行時には、Assert 対象となるパケットの発信元へのユニキャスト経路を参照し、発信元へ向かうインタフェースのプリファレンス値を Assert メッセージに格納します。Assert メッセージが出力されるインタフェースのプリファレンス値が格納されるわけではありません。

上流ルータの種類

本装置より上流にルータが存在し、そのルータを経由してマルチキャストパケットが転送される場合、どの種類のルータからのマルチキャストパケット転送を許可するかを指定します。

上流ルータが PIM ルータでない場合（マルチキャストパケットをスタティック経路によって転送するルータであった場合）に転送を許可する場合は、“すべて”を選択します。

受信インタフェースと同一の IP セグメントから送信された（直接接続されたホストからの）マルチキャストパケットは、上流ルータの設定にかかわらず転送が行われます。

13.2.10 ARP 情報

適用機種 SR-S716C2, 724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[ARP 情報]

■ARP情報

ProxyARP機能 ☒ 使用する ☐ 使用しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

ProxyARP 機能

本装置を経由して到達できる IPv4 アドレスに対する ARP 要求に対し代理応答する機能です。代理応答させない場合は“使用しない”を選択します。

13.2.11 スタティック ARP 情報

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IP 関連]→[スタティック ARP 情報]

■スタティックARP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	あて先IPアドレス	MACアドレス	操作
全削除			

＜スタティックARP情報入力フィールド＞

あて先IPアドレス

MACアドレス

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているスタティック ARP 情報の定義が表示されています。スタティック ARP の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

同じあて先へのスタティック ARP 情報を複数設定することはできません。

あて先 IP アドレス

スタティック ARP テーブルに登録するあて先 IP アドレスを指定します。

MAC アドレス

あて先 IP アドレスへパケットを送信する場合に使用する MAC アドレスを指定します。

こんな事に気をつけて

同じあて先へのスタティック ARP 情報を複数設定することはできません。

13.3 IPv6 関連

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IPv6 関連]

LAN0情報		
共通情報	IP関連	IPv6関連
IPv6基本情報	IPv6 RIP情報	IPv6 OSPF情報
IPv6スタティック経路情報	IPv6 DHCP情報	IPv6フィルタリング情報
IPv6 RIPフィルタリング情報	IPv6 DSCP値書き換え情報	

SR-S724TC1、748TC1 のみ、「IPv6 RIP 情報」、「IPv6 OSPF 情報」および「IPv6 RIP フィルタリング情報」が表示されます。

SR-S308TL1、310TL2、316TL1、318TL2、324TL2、324TC1、328TR1、348TC1、724TC1、748TC1 のみ、「IPv6 DSCP 値書き換え情報」が表示されます。

13.3.1 IPv6 基本情報

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IPv6 関連]→[IPv6 基本情報]

■ 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

アドレスまたはプレフィックス

☐ エニキャストアドレスを指定する

アドレス

☐ 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

アドレスまたはプレフィックス

☐ エニキャストアドレスを指定する

アドレス

☐ 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

アドレスまたはプレフィックス

☐ エニキャストアドレスを指定する

アドレス

☒ 使用しない	最大送信間隔	600	秒
☐ 受信する	最小送信間隔	200	秒
☐ 送信する	Router Lifetime	1800	秒
	MTU		
	Reachable Time	0	ミリ秒
	Retrans Timer	0	ミリ秒
	Cur Hop Limit	64	
	フラグ	00	

プレフィックス			
Valid Lifetime	☐ 期限なし	☒ 期限あり	30 日
Pref. Lifetime	☐ 期限なし	☒ 期限あり	7 日
フラグ	c0		

プレフィックス			
Valid Lifetime	☐ 期限なし	☒ 期限あり	30 日
Pref. Lifetime	☐ 期限なし	☒ 期限あり	7 日
フラグ	c0		

プレフィックス			
Valid Lifetime	☐ 期限なし	☒ 期限あり	30 日
Pref. Lifetime	☐ 期限なし	☒ 期限あり	7 日
フラグ	c0		

プレフィックス			
Valid Lifetime	☐ 期限なし	☒ 期限あり	30 日
Pref. Lifetime	☐ 期限なし	☒ 期限あり	7 日
フラグ	c0		

SR-S724TC1、748TC1 以外では、表示が上記の画面とは異なります。

IPv6

IPv6 通信を行う場合は、“使用する”を選択します。

インタフェース ID

インタフェース ID を設定します。

- 自動
装置の MAC アドレスから自動生成されるインタフェース ID を使用します。通常は、この設定を使用します。
- 指定する
フィールドに 16 桁の 16 進数で表記したインタフェース ID を入力します。表記方法は、16 ビットごとに区切り文字 (:) で区切ります。ほかの装置と同じインタフェース ID とならないような値を利用します。
記述例)
2001:db8:7654:3210

IPv6 アドレス

この装置で使用する IPv6 アドレスを 4 個まで設定できます。

- ルータ広報で受信したプレフィックスを使用する
RA (Router Advertisement メッセージ) で取得したプレフィックスを使用してアドレスを自動生成する場合に選択します。
- ユニキャストアドレスを指定する
ユニキャストアドレスを指定する場合に選択します。
- エニキャストアドレスを指定する
エニキャストアドレスを指定する場合に選択します。

アドレスまたはプレフィックス

本装置の IPv6 アドレスを標準的な IPv6 アドレス表記方式で指定します。本装置ではプレフィックス長は 64 に固定されます。インタフェース ID 部分がすべて 0 の場合は、設定されたアドレスはプレフィックスとして解釈され、実際に利用するアドレスはそれにインタフェース ID を付与したものとなります。リンクローカルアドレスは指定できません。

記述例)
2001:db8:1111:1000:1:2:3:4

完全な IPv6 アドレスとして解釈されます。

2001:db8:1111:1000::

プレフィックスとして解釈され、インタフェース ID 部分にはインタフェース ID が付与されます。

アドレス

本装置のエニキャストアドレスを標準的な IPv6 アドレス表記方式で指定します。

本装置ではプレフィックス長は 128 に固定されます。インタフェース ID によるアドレス生成は行われません。

ルータ広報

RA (router advertisement) 機能を設定します。

- 使用しない
RA (router advertisement) 機能を使用しません。
- 受信する
RA をもとに ND (Neighbor Discovery) のパラメタ、デフォルトルートおよびグローバルアドレスを本装置に自動設定することができます。
- 送信する (SR-S724TC1、748TC1)
“IPv6 アドレス”で指定したユニキャストアドレスを RA で送信することができます。送信する場合は、以下の項目を指定します。

こんな事に気をつけて

- RA 受信機能を利用する場合、IPv6 フォワーディング機能を“使用しない”に設定してください。
- RA 送信機能を利用する場合、IPv6 フォワーディング機能を“使用する”に設定してください。

最大送信間隔

ルータ広報メッセージの最大送信間隔を指定します。初期値は 600 秒です。省略はできません。

有効範囲)
4 ~ 1800

最小送信間隔

ルータ広報メッセージの最小送信間隔を指定します。初期値は 200 秒です。省略はできません。

有効範囲)
3 ~ 最大送信間隔の 3 / 4

Router Lifetime

ルータ広報で送信する Router Lifetime の内容を指定します。初期値は 1800 秒です。省略はできません。

有効範囲)
0 または最大送信間隔 ~ 9000

MTU

ルータ広報で送信する MTU option の内容を指定します。
無指定の場合は、MTU option を含めません。

有効範囲)
1280 ～ 1500

Reachable Time

ルータ広報で送信する Reachable Time の内容を指定します。
省略値は 0 ミリ秒です。

有効範囲)
0 ～ 3600000

Retrans Timer

ルータ広報で送信する Retrans Timer の内容を指定します。
省略値は 0 ミリ秒です。

有効範囲)
0 ～ 4294967295

Cur Hop Limit

ルータ広報で送信する Cur Hop Limit の内容を指定します。
省略値は 64 です。

有効範囲)
0 ～ 255

フラグ

ルータ広報の本体部分に設定するフラグフィールドの内容を 2 桁の 16 進数で指定します。この領域の値として、RFC2461 で以下の値が定義されています。
必要に応じて以下の値の論理和を指定します。省略値は 00 です。

- Managed address configuration flag : 80
- Other stateful configuration flag : 40

プレフィックス

RA メッセージに含める広報プレフィックス情報を設定します。IPv6 アドレスの “アドレスまたはプレフィックス” に設定した値を指定してください。

Valid Lifetime

ルータ広報のプレフィックス情報ごとに設定する Valid Lifetime を指定します。通常は、“30 日” を使用します。

有効範囲)
0 ～ 365 日
0 ～ 8760 時間
0 ～ 525600 分
0 ～ 31536000 秒

Pref. Lifetime

ルータ広報のプレフィックス情報ごとに設定する Preferred Lifetime を指定します。通常は、“7 日” を使用します。

有効範囲)
0 ～ 365 日
0 ～ 8760 時間
0 ～ 525600 分
0 ～ 31536000 秒

フラグ

ルータ広報のプレフィックス情報ごとに設定するフラグフィールドの内容を 2 桁の 16 進数で指定します。この領域の値として、RFC2461 で以下の値が定義されています。必要に応じて以下の値の論理和を指定します。
通常は、“c0” を使用します。

- on-link flag : 80
- autonomous address-configuration flag : 40

13.3.2 IPv6 RIP 情報

適用機種 SR-S724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「LAN 情報」→ [修正] → [IPv6 関連] → [IPv6 RIP 情報]

IPv6 RIP情報

RIP送信

☒ 送信しない
☐ 送信する

メトリック値 0

RIP受信

☒ 受信しない ☐ 受信する

集約経路送信

集約経路	破棄経路 設定
☐ デフォルトルート ☒ ネットワーク指定 	☒ 設定する
	☒ 設定する
	☒ 設定する
	☒ 設定する

サイトローカルプレフィックス

☐ 交換しない ☒ 交換する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

装置全体でのIPv6 RIPを使用できるインタフェースの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.53)を参照してください。

RIP 送信

RIPを送信する場合は、“送信する”を選択します。

メトリック値

“送信する”を選択した場合に、加算するメトリック値を選択します。

RIP 受信

RIPを受信する場合は、“受信する”を選択します。

集約経路送信

RIPで送信する集約経路情報を設定します。

集約経路

送信する集約経路情報として、“デフォルトルート”または、“ネットワーク指定”を選択します。

- デフォルトルート
集約経路情報としてデフォルトルートだけを広報します。
- ネットワーク指定
集約経路情報をプレフィックス／プレフィックス長で指定します。指定した集約経路情報は広報され、集約経路情報に含まれる経路情報は広報されません。

こんな事に気をつけて

集約経路情報は、集約される経路情報がないときでも広報されます。また、同じあて先の経路情報がルーティングテーブルにないときでも広報され、ルーティングテーブルには設定されません。

破棄経路設定

それぞれの集約経路情報で、破棄経路を設定するかどうかをチェックします。チェックすることにより、広報した集約経路情報により本装置に送られた IP パケットをルーティングするための経路情報がないときに、そのあて先へは到達不能であることを ICMPv6 で通知することができます。

チェックしないときは、そのあて先への経路がないことが ICMPv6 で通知されます。

チェックしたときは、集約経路情報と同じあて先の経路情報が破棄経路としてルーティングテーブルに設定されます。

サイトローカルプレフィックス

サイトローカルプレフィックスを交換する場合は、“交換する”を選択します。

13.3.3 IPv6 OSPF 情報

適用機種 SR-S724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IPv6 関連]→[IPv6 OSPF 情報]

■ IPv6 OSPF 情報

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 パケット送信間隔

10 秒

隣接ルータ停止確認間隔

40 秒

パケット再送間隔

5 秒

LSU パケット送信遅延時間

1 秒

パケット送信

☐ 抑止する
☒ 抑止しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

装置全体での IPv6 OSPF を使用できるインタフェースの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。

OSPF 機能

OSPF を使用する場合は、“使用する”を選択します。

エリア定義番号

エリア定義番号を指定します。

OSPF エリア情報は、「ルーティングプロトコル情報」の「IPv6 OSPF 関連」で設定することができます。

省略時は、0 が設定されます。

出力コスト

OSPF 出力コストを 1 ～ 65535 の範囲で指定します。省略時は、1 が設定されます。

指定ルータ優先度

指定ルータおよび副指定ルータを決定するための優先度を 0 ～ 255 の範囲で指定します。値が大きいほど優先度は高くなります。省略時は、1 が設定されます。

こんな事に気をつけて

値が 0 の場合は、指定ルータおよび副指定ルータにはなりません。

Hello パケット送信間隔

OSPF 隣接関係の維持に使用する、Hello パケットの送信間隔を指定します。省略時は、10 秒が設定されます。

有効範囲)

1 ～ 18 時間

1 ～ 1092 分

1 ～ 65535 秒

こんな事に気をつけて

OSPF 隣接ルータ間で同じ Hello パケットの送信間隔を指定してください。

隣接ルータ停止確認間隔

OSPF 隣接関係の維持に使用する、隣接ルータ停止確認間隔を指定します。

隣接ルータ停止確認間隔は、Hello パケット送信間隔 より大きな値を指定する必要があります。Hello パケット送信間隔 の 4 倍を設定することをお勧めします。省略時は、40 秒が設定されます。

有効範囲)

1 ～ 18 時間

1 ～ 1092 分

1 ～ 65535 秒

こんな事に気をつけて

- OSPF 隣接ルータ間で同じ隣接ルータ停止確認時間を指定してください。
- 隣接ルータ停止確認間隔は、装置起動時に指定ルータおよび副指定ルータの選出を開始するまでの待機時間にも使用されます。大きな値を設定した場合は、経路交換の開始が遅れます。

パケット再送間隔

OSPF パケットを再送する間隔を指定します。省略時は、5 秒が設定されます。

有効範囲)

1 ～ 18 時間

1 ～ 1092 分

3 ～ 65535 秒

LSU パケット送信遅延時間

LSU (Link State Update) パケットの送信遅延時間を指定します。

LSU パケットでは、LSA (Link State Advertisement) を作成してから経過時間に対し、この設定時間を加算して広報します。省略時は、1 秒が設定されます。

有効範囲)

1 ～ 18 時間

1 ～ 1092 分

1 ～ 65535 秒

こんな事に気をつけて

LSA は、生成されてから 1 時間が経過すると破棄されます。LSU 送信遅延時間に 1 時間以上を指定しないでください。正しくルーティングできない場合があります。

パケット送信

OSPF パケットの送信を抑止する場合は、“抑止する”を選択します。

13.3.4 IPv6 スタティック経路情報

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IPv6 関連]→[IPv6 スタティック経路情報]

■IPv6スタティック経路情報

※追加・修正情報は一覧ので設定してください。

あて先プレフィックス／プレフィックス長	中継ルータアドレス	メトリック値	優先度	操作
全削除				

<IPv6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

あて先プレフィックス／プレフィックス長

中継ルータアドレス

メトリック値

優先度

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているスタティック経路情報の定義が表示されています。IPv6 スタティック経路の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53)を参照してください。処理するボタンをクリックし、次のページへ進みます。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。

- デフォルトルート
中継ルータアドレスを指定します。
- ネットワーク指定
あて先ネットワークとプレフィックス長、中継ルータアドレスを指定します。あて先ネットワークにリンクローカルアドレスは指定できません。ICMPv6 Redirect を正常に動作させるためには、中継ルータアドレスは、リンクローカルアドレスで指定する必要があります。なお、あて先プレフィックス／プレフィックス長に::0を設定した場合、“デフォルトルート”を指定したものととして動作します。

メトリック値

このスタティック経路情報を RIP (IPv6) に再配布するときのメトリック値を、1～14から選択します。

RIP (IPv6) が動作する場合だけ有効になります。

優先度

スタティック経路情報の優先度を1～254の範囲の10進数で指定します。省略時は、1が設定されます。優先度は、同じあて先への経路情報が複数ある場合に優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。

スタティック経路情報以外の優先度には、以下の初期値が設定されています。

プロトコル	優先度
RA	12
OSPF	110
RIP	120
DHCP	10

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定する場合は、優先度が同じスタティック経路情報を、同時に設定できません。

13.3.5 IPv6 DHCP 情報

13.3.5.1 IPv6 DHCP 情報（初期表示または使用しない選択時）

〔操作〕 「設定メニュー」→詳細設定「LAN 情報」→〔修正〕→〔IPv6 関連〕
→〔IPv6 DHCP 情報（DHCP 機能：初期表示または使用しない選択時）〕

初期表示または DHCP 機能に“使用しない”を選択した場合に表示されます。

SR-S724TC1、748TC1 のみ、「リレーエージェント機能を使用する」の項目が表示されます。

DHCP 機能

それぞれのインタフェースの IPv6 DHCP 機能を以下の 3 つから選択します。

- 使用しない
IPv6 DHCP 機能を使用しません。
- リレーエージェント機能を使用する（SR-S724TC1、748TC1）
IPv6 DHCP リレーエージェントとして使用します。
- サーバ機能を使用する
本装置を該当インタフェースのネットワークの IPv6 DHCP サーバとして使用します。

13.3.5.2 IPv6 DHCP 情報（リレーエージェント機能を使用する選択時）

適用機種 SR-S724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IPv6 関連]
→[IPv6 DHCP 情報（DHCP 機能：リレーエージェントを使用する選択時）]

■ IPv6 DHCP 情報

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

リレー先サーバアドレス

送信元アドレス

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

DHCP 機能に“リレーエージェント機能を使用する”を選択した場合に表示されます。

「DHCP 機能」の項目は、「IPv6 DHCP 情報（初期表示または使用しない選択時）」を参照してください。

リレーエージェント機能

リレー先インタフェース

IPv6 DHCP クライアントからの要求を中継し、送出するインタフェースを選択します。

リレー先サーバアドレス

リレー先サーバの IPv6 アドレスを設定します。
存在するリレー先インタフェースを指定してください。

送信元アドレス

サーバへのリレーパケットを送信する際の送信元アドレスとして、本装置に設定されている自側 IPv6 アドレスのどれかを指定します。

13.3.5.3 IPv6 DHCP 情報（サーバ機能を使用する選択時）

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IPv6 関連]
→[IPv6 DHCP 情報（DHCP 機能：サーバ機能を使用する選択時）]

■IPv6 DHCP情報

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

サーバ機能

DUID

☒ 自動
☐ 指定する

プリファレンス値

アドレス配布

☒ しない
☐ する

割当て開始アドレス

割当てアドレス数

Valid Lifetime ☒ 期限なし
☐ 期限あり 日

Pref. Lifetime ☒ 期限なし
☐ 期限あり 日

プレフィックス配布

☒ しない
☐ する

プレフィックス

Valid Lifetime ☒ 期限なし
☐ 期限あり 日

Pref. Lifetime ☒ 期限なし
☐ 期限あり 日

自動経路設定 ☒ する ☐ しない

配布先クライアントDUID

DNSサーバアドレス配布

プライマリ

セカンダリ

DNSドメイン名配布

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

DHCP 機能に“サーバ機能を使用する”を選択した場合に表示されます。

「DHCP 機能」の項目は、「IPv6 DHCP 情報（初期表示または使用しない選択時）」を参照してください。

サーバ機能

DUID

- 自動
DUID-LL フォーマットで自動生成される DUID を使用します。通常は、この設定を使用します。
- 指定する
260 桁以内の 16 進数で表記した DUID を指定します。

プリファレンス値

DHCP サーバのプリファレンス値を 0～255 の範囲の 10 進数で指定します。DHCP クライアントはこの値が大きい DHCP サーバを選択します。省略時は 0 が設定されます。

アドレス配布

DHCP クライアントに割り当てる IPv6 アドレスを設定します。クライアントに IPv6 アドレスを割り当てる場合は、“する”を選択し、以降の項目を設定します。

“しない”を選択した場合、ホストデータベース設定による静的なアドレス割り当てだけが行われます。

割当て開始アドレス

クライアントに割り当てる連続した IPv6 アドレス群の先頭の IPv6 アドレスを設定します。

有効範囲)

::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

割当てアドレス数

クライアントに割り当てる IPv6 アドレス数を 0 ～ 300 の範囲で設定します。ホストデータベース機能を使用すると特定の IPv6 DHCP クライアントに対して固有の IPv6 アドレスを割り当てることができます。この場合の IPv6 アドレスは、割当て開始 IPv6 アドレスと割当てアドレス数によって規定される動的割り当て範囲である必要はありません。

Valid Lifetime

割り当てる IPv6 アドレスの Valid Lifetime を指定します。

有効範囲)

0 ～ 365 日

0 ～ 8760 時間

0 ～ 525600 分

0 ～ 31536000 秒

Pref. Lifetime

割り当てる IPv6 アドレスの Preferred Lifetime を指定します。Pref. Lifetime は、Valid Lifetime より短い時間になるように設定してください。

有効範囲)

0 ～ 365 日

0 ～ 8760 時間

0 ～ 525600 分

0 ～ 31536000 秒

プレフィックス配布

DHCP クライアントに割り当てるプレフィックスを設定します。クライアントにプレフィックスを割り当てる場合は、“する”を選択し、以降の項目を設定します。

プレフィックス

クライアントに割り当てるプレフィックスとプレフィックス長を設定します。プレフィックス長は 48 ～ 64 の範囲で指定します。

Valid Lifetime

割り当てるプレフィックスの Valid Lifetime を指定します。

有効範囲)

0 ～ 365 日

0 ～ 8760 時間

0 ～ 525600 分

0 ～ 31536000 秒

Pref. Lifetime

割り当てるプレフィックスの Preferred Lifetime を指定します。Pref. Lifetime は、Valid Lifetime より短い時間になるように設定してください。

有効範囲)

0 ～ 365 日

0 ～ 8760 時間

0 ～ 525600 分

0 ～ 31536000 秒

自動経路設定

クライアントに割り当てたプレフィックスへの経路を自動で設定する場合は、“する”を選択します。

配布先クライアント DUID

配布先クライアントの DUID を、260 桁以内の 16 進数で指定します。

DNS サーバアドレス配布

配布する DNS サーバの IPv6 アドレスを設定します。

省略すると DHCP サーバによる配布を行いません。

DNS ドメイン名配布

配布する DNS ドメイン名を設定します。

省略すると DHCP サーバによる配布を行いません。

13.3.6 IPv6 フィルタリング情報

[操作]「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IPv6 関連]→[IPv6 フィルタリング情報]

現在、このネットワークに設定されている IPv6 フィルタリング情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

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。

IPv6 フィルタリング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“IPv6 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)

☛ 参照 「装置情報」-「資源情報」画面は、[4.9 資源情報 \(P33\)](#) を参照してください。

💡 ヒント

◆ フィルタの定義数

- SR-S208TC2/224TC2/208PD1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 30 ルール

- SR-S224PS1/224CP1/248TC1 の場合

etherblock ごとに 10 個

指定された ACL 情報の内容によって etherblock ごとに 60～100 ルール（認証成功端末数による）

- SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合

装置で 128 個

指定された ACL 情報の内容によって装置で 128 ルール

- SR-S316C2/716C2 の場合

ポートごとに 10 個

指定された ACL 情報の内容によってポートごとに 100 ルール

● SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合

装置で 128 個（初期値）

指定された ACL 情報の内容によって装置で 128 ルール（初期値）

定義可能上限値は、「装置情報」-「資源情報」の「フィルタ/QoS 資源の配分」の設定で、最大で 512 個まで拡張することができます。

◆ 優先順位**● SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合**

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (2) 「etherblock 情報」-「フィルタ情報」の設定
- (3) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (4) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (5) 「ether 情報」-「QoS 関連」-「QoS 情報」（ether ポート間の優先順位は ether ポート番号が小さいほうが高い）
- (6) 「etherblock 情報」-「QoS 情報」
- (7) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」-「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (10) 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (11) 「VLAN 情報」-「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S316C2/716C2 の場合

優先順位は、以下のとおりです。

- (1) 「ether 情報」-「フィルタ情報」の設定
- (2) 「VLAN 情報」-「フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (3) 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (4) 「ether 情報」-「QoS 関連」-「QoS 情報」
- (5) 「VLAN 情報」-「QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (6) 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」（LAN 間の優先順位は LAN 定義番号が小さいほうが高い）
- (7) 「VLAN 情報」-「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (8) 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）
- (9) 「VLAN 情報」-「IPv6 QoS 情報」（VLAN 間の優先順位は VLAN ID が小さいほうが高い）

● SR-S308TL1/310TL2/316TL1/318TL2/324TL2/324TC1/328TR1/348TC1/724TC1/748TC1 の場合

優先順位は、以下のとおりです。

- (1) 「VLAN 情報」-「IPv6 フィルタ情報」の設定（VLAN 間の優先順位は VLAN ID が小さいほうが高い）
- (2) 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」（LAN 間の優先順位は lan 定義番号が小さいほうが高い）

◆ ルール

● SR-S208TC2/224TC2/208PD1 の場合

ACL の内容によって、以下のように消費するルール数が異なります。

<ルール1>

- 「ether 情報」 - 「フィルタ情報」
- 「etherblock 情報」 - 「フィルタ情報」
- 「VLAN 情報」 - 「フィルタ情報」
- 「ether 情報」 - 「QoS 関連」 - 「QoS 情報」
- 「etherblock 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「QoS 情報」
- 「VLAN 情報」 - 「IPv6 フィルタ情報」
- 「VLAN 情報」 - 「IPv6 QoS 情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: TCP または UDP の送信元ポート数 × あて先ポート数 × 2
- TCP または UDP を設定する ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: ICMP の ICMP TYPE の個数 × ICMP CODE の個数 × 2
- ICMP を設定する ACL の場合、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定する ACL の場合
: 2
- TCP/UDP/ICMP を設定しない ACL の場合で、かつ MAC フォーマットで ether または llc を設定しない ACL の場合
: 1

<ルール2>

- 「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」
- 「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」
- 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 フィルタリング情報」

上記の場合に消費する ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

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

ACL の内容によって、以下のように消費するルール数が異なります。それぞれの ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数 × あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数 × ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

こんな事に気をつけて

- 自装置 IPv6 アドレスあてパケットやホップバイホップオプション付きパケットなど、ソフト処理となるパケットに対する「LAN 情報」-「IP 関連」-「IP フィルタリング情報」設定や「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」設定、「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」設定はスイッチのフィルタ・QoS 設定上限オーバとなった場合も適用されます。
- WWW や DHCP に対するアクセスを制限する設定を行った場合、WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。
- 以下の設定はすべての etherblock に適用されます。(SR-S208TC2/224TC2/208PD1/224PS1/224CP1/248TC1 の場合)
 - 「VLAN 情報」-「フィルタ情報」
 - 「VLAN 情報」-「QoS 情報」
 - 「LAN 情報」-「IP 関連」-「IP フィルタリング情報」
 - 「LAN 情報」-「IP 関連」-「DSCP 値書き換え情報」
 - 「VLAN 情報」-「IPv6 フィルタ情報」
 - 「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」
 - 「VLAN 情報」-「IPv6 QoS 情報」
- ACL で指定したアクセスコントロールリストが使用するスイッチ内部メモリが上限値を超える場合はフィルタは適用されません。たとえば、指定したアクセスコントロールリスト内の IPv6 定義で、送信元およびあて先 IPv6 アドレスのプレフィックス長の組み合わせで、以下の範囲を超えて指定した場合は、使用するスイッチ内部メモリが上限値を超えるため、フィルタ条件を 2 つのアクセスコントロールリストに分割し適用する必要があります。(SR-S224PS1/224CP1/248TC1/316C2/716C2 の場合)

送信元プレフィックス長の設定ビット数	あて先プレフィックス長の設定可能ビット数
113 ~ 128	0 (ANY) ~ 48
81 ~ 112	0 (ANY) ~ 64
49 ~ 80	0 (ANY) ~ 96
0 (ANY) ~ 48	0 (ANY) ~ 128

また、TCP/UDP/ICMP 条件を any 以外で同時に設定した場合、あて先プレフィックス長の設定可能ビット数が 32bit 減少します。

- 当該 etherblock で、IEEE802.1X 認証成功端末、Web 認証成功端末、MAC アドレス認証成功端末および DHCP スヌープ許可端末の合計が 152 台以下の場合は、ルールによる上限は etherblock ごとに 100 個となりますが、152 台を超えた場合は 1 認証成功端末につき使用可能なルール数が 1 個減少します。(SR-S224PS1/224CP1/248TC1 の場合)
- 自装置 IPv6 アドレスあてパケットは acl 定義に該当した場合もフィルタされません。自装置 IPv6 アドレスあてパケットは「LAN 情報」-「IPv6 関連」-「IPv6 フィルタリング情報」で設定してください。(SR-S716C2 の場合)
- "vlan ip6filter" コマンド、"lan ip6 filter" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 200 個まで設定可能です。(SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合)
- "ether macfilter" コマンド、"ether qos aclmap" コマンド、"vlan macfilter" コマンド、"vlan qos aclmap" コマンド、"lan ip filter" コマンド、"lan ip dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 700 個まで設定可能です。(SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合)

動作

IP フィルタリングの動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
- TCP 定義
IPv6 定義のプロトコルが 6 の場合にのみ有効です。
- UDP 定義
IPv6 定義のプロトコルが 17 の場合にのみ有効です。
- ICMP 定義
IPv6 定義のプロトコルが 58 の場合にのみ有効です。

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。
なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正] → [IPv6 関連] → [IPv6 フィルタリング情報]
→ 「ACL 定義番号の [参照]」

表示条件入力			
表示回数		表示範囲	
10		0~0	
■ ACL 情報			
定義番号	IPv6 定義	TCP/UDP/ICMP 定義	選択
	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		
	QoS種別		
	QoS値		
0	tcp	TCP 定義	
	2001:db8:1111:1000::/64	送信元ポート番号	any
	any	あて先ポート番号	21
	any		選択
		UDP 定義	
		送信元ポート番号	any
		あて先ポート番号	53
			開じる

「ACL 情報」 - [追加] / [修正] - 「IPv6 定義情報」、 「TCP 定義情報」 および 「UDP 定義情報」 で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示回数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IPv6 フィルタリング情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「IPv6 フィルタリング情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

13.3.7 IPv6 RIP フィルタリング情報

適用機種 SR-S724TC1, 748TC1

[操作] 「設定メニュー」 → 詳細設定 「LAN 情報」 → [修正] → [IPv6 関連] → [IPv6 RIP フィルタリング情報]

■IPv6 RIPフィルタリング情報
 ※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。

優先順位	動作	方向	フィルタリング条件	メトリック値	操作
全削除					
<IPv6 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			
	プレフィックス / プレフィックス長	/			
メトリック値					
追加 キャンセル					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されているRIPフィルタリング定義が表示されています。処理は優先順位1から順に行われます。装置全体でのRIPフィルタリングの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53)を参照してください。処理するボタンをクリックし、次のページへ進みます。

RIP受信（送信）時には、優先順位の高い定義から順に受信（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。なお、一致した以降の条件は参照されません。また、受信（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。

動作

フィルタリング対象に該当するRIP経路情報の動作を以下の2つから選択します。

- 透過
条件と一致した場合にRIP経路情報を透過します。
- 遮断
条件と一致した場合にRIP経路情報を遮断します。

方向

フィルタリングをRIP受信時に行うか、RIP送信時に行うかを選択します。

- 受信
RIP受信時に、フィルタリングを行います。
- 送信
RIP送信時に、フィルタリングを行います。

フィルタリング条件

フィルタリング条件を選択します。

- **すべて**
すべての経路情報がフィルタリングの対象となります。
- **デフォルトルート**
デフォルトルートをフィルタリング対象とします。
- **経路情報指定**
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、RIP 経路の検索条件として、“完全に一致” または、“マスクした結果が一致” を選択します。

検索条件

検索条件を選択します。

- **完全に一致**
指定したプレフィックスとプレフィックス長が完全に一致した RIP 経路情報をフィルタリング対象とします。
- **マスクした結果が一致**
指定したプレフィックスと、RIP 経路情報のそれぞれを、指定したプレフィックス長でマスクした結果が一致した場合、その RIP 経路情報をフィルタリング対象とします。

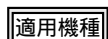
メトリック値

フィルタリング結果で透過になった RIP 経路情報のメトリック値を変更できます。送信時の RIP 経路にメトリック値を設定した場合、「RIP 情報」で設定した加算メトリック値は加算されません。省略または 0 を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

フィルタリング条件で“すべて”を選択したときは、メトリック値を設定しても無効となります。

13.3.8 IPv6 DSCP 値書き換え情報



SR-S308TL1, 310TL2, 316TL1, 318TL2, 324TL2, 324TC1, 328TR1, 348TC1, 724TC1, 748TC1

[操作] 「設定メニュー」 → 詳細設定 「LAN 情報」 → [修正] → [IPv6 関連] → [IPv6 DSCP 値書き換え情報]

現在、このネットワークに設定されている DSCP 値書き換え情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された DSCP 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

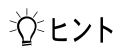
こんな事に気をつけて

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。

IPv6 DSCP 値書き換え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「IPv6 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)

☞ 参照 「装置情報」 - 「資源情報」画面は、[\[4.9 資源情報\] \(P33\)](#) を参照してください。



ヒント

◆ 定義数

- SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合

装置で 128 個

指定された ACL 情報の内容によって装置で 128 ルール

- SR-S324TC1/328TR1/348TC1/724TC1 /748TC1 の場合

装置で 128 個 (初期値)

指定された ACL 情報の内容によって装置で 128 ルール (初期値)

定義可能上限値は、「装置情報」 - 「資源情報」の「フィルタ/QoS 資源の配分」の設定で、最大で 512 個まで拡張することができます。

◆ 優先順位

優先順位は、以下のとおりです。

- (1) 「VLAN 情報」 - 「IPv6 QoS 情報」 (VLAN 間の優先順位は VLAN ID が小さいほうが高い)
- (2) 「LAN 情報」 - 「IPv6 関連」 - 「IPv6 DSCP 値書き換え情報」 (LAN 間の優先順位は lan 定義番号が小さいほうが高い)

◆ ルール

ACL の内容によって、以下のように消費するルール数が異なります。それぞれの ACL のルール数は、以下の計算式によって求められます。

- TCP または UDP を設定する ACL の場合 : TCP または UDP の送信元ポート数×あて先ポート数
- ICMP を設定する ACL の場合 : ICMP の ICMP TYPE の個数× ICMP CODE の個数
- TCP/UDP/ICMP を設定しない ACL の場合 : 1

こんな事に気をつけて

- 自装置 IP アドレスあてパケットや IP オプション付きパケットなど、ソフト処理となるパケットに対する「LAN 情報」 - 「IP 関連」 - 「IP フィルタリング情報」設定や「LAN 情報」 - 「IP 関連」 - 「DSCP 値書き換え情報」設定はスイッチのフィルタ・QoS 設定上限オーバーとなった場合も適用されます。
- "vlan ip6qos aclmap" コマンド、"lan ip6 dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 200 個まで設定可能です。(SR-S308TL1/310TL2/316TL1/318TL2/324TL2 の場合)
- "ether macfilter" コマンド、"ether qos aclmap" コマンド、"vlan macfilter" コマンド、"vlan qos aclmap" コマンド、"lan ip filter" コマンド、"lan ip dscp" コマンド、"serverinfo filter" コマンドなどの ACL を参照する定義は装置全体で 400 個まで設定可能です。(SR-S324TC1/328TR1/348TC1/724TC1/748TC1 の場合)

新 DSCP

IPv6 パケットに新しく指定する DSCP 値を 0～63 の範囲の 10 進数で指定します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
- TCP 定義
IPv6 定義のプロトコルが 6 の場合にのみ有効です。
- UDP 定義
IPv6 定義のプロトコルが 17 の場合にのみ有効です。
- ICMP 定義
IPv6 定義のプロトコルが 58 の場合にのみ有効です。

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] 「設定メニュー」→詳細設定「LAN 情報」→[修正]→[IPv6 関連]→[IPv6 DSCP 値書き換え情報]
→「ACL 定義番号の[参照]」

表示条件入力

表示個数 10		表示範囲 0~0	
------------	--	-------------	--

■ACL情報 [閉じる]

定義番号	IPv6定義 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 QoS種別 QoS値	TCP/UDP/ICMP定義	選択
0	tcp 2001:db8:1111:1000::/64 any any	TCP定義 送信元ポート番号 any あて先ポート番号 21 UDP定義 送信元ポート番号 any あて先ポート番号 53	選択

[閉じる]

「ACL 情報」 - [追加] / [修正] - 「IPv6 定義情報」、「TCP 定義情報」および「UDP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IPv6 DSCP 値書き換え情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「IPv6 DSCP 値書き換え情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

14 IP 情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「IP 情報」

IP 情報
基本情報

14.1 基本情報

[操作] 「設定メニュー」→詳細設定「IP 情報」→[基本情報]

■基本情報

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

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

SR-S716C2、724TC1、748TC1 のみ、「IP フォワーディング機能」の項目が表示されます。

ARP エントリ有効時間

ARP エントリの有効時間を 1～240 分の範囲で指定します。省略時は、20 分が設定されます。

IP フォワーディング機能 (SR-S716C2、724TC1、748TC1)

IP フォワーディング機能を使用する場合は、“使用する”を選択します。

15 IPv6 情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「IPv6 情報」

IPv6 情報	
<u>基本情報</u>	<u>ホスト情報</u>

SR-S724TC1、748TC1 のみ、「基本情報」が表示されます。

15.1 基本情報

適用機種 SR-S724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「IPv6 情報」→[基本情報]

■基本情報

IPv6 フォワーディング機能 ☒ 使用しない ☐ 使用する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

IPv6 フォワーディング機能

IPv6 フォワーディング機能を使用する場合は、“使用する”を選択します。

15.2 ホスト情報

[操作] 「設定メニュー」→詳細設定「IPv6 情報」→[ホスト情報]

■ホスト情報

重複アドレス検出機能 ☐ 使用しない ☒ 使用する

NS送信回数

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

重複アドレス検出機能

重複アドレス検出機能を使用する場合は、“使用する”を選択します。

NS 送信回数

重複アドレスを検出するための NS 送信回数を 1～30 の範囲の 10 進数で指定します。省略時は、1 が設定されます。

16 ルーティングプロトコル情報

適用機種 SR-S716C2, 724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」

ルーティングプロトコル情報					
ルーティングマ ネージャ情報	RIP関連	OSPF関連	IPv6 ルーティ ングマネージャ情報	IPv6 RIP関連	IPv6 OSPF関連
このページではルーティングプロトコル情報を設定することができます。上記の各関連項目をクリックすると詳細な設定項目が表示されます。					

16.1 ルーティングマネージャ情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[ルーティングマネージャ情報]

ルーティングプロトコル情報					
ルーティングマ ネージャ情報	RIP関連	OSPF関連	IPv6 ルーティ ングマネージャ情報	IPv6 RIP関連	IPv6 OSPF関連
再配布情報		優先度情報		ECMP情報	

SR-S724TC1、748TC1のみ、「IPv6 ルーティングマネージャ情報」、「IPv6 RIP 関連」および「IPv6 OSPF 関連」が表示されます。

16.1.1 再配布情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[ルーティングマネージャ情報]
→[再配布情報]

再配布情報

RIP	インタフェース経路情報	☐ 再配布しない ☒ 再配布する
	スタティック経路情報	☐ 再配布しない ☒ 再配布する
	OSPF経路情報	☒ 再配布しない ☐ 再配布する メトリック値: 0
OSPF	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 メトリックタイプ: type2
	スタティック経路情報	☒ 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
	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

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

RIP

RIPに再配布する経路情報を設定します。

インタフェース経路情報

インタフェース経路情報を RIP に再配布する場合は、“再配布する”を選択します。

スタティック経路情報

スタティック経路情報を RIP に再配布する場合は、“再配布する”を選択します。

OSPF 経路情報

OSPF 経路情報を RIP に再配布する場合は、“再配布する”を選択します。

メトリック値

RIP に再配布する際のメトリック値を選択します。

OSPF

OSPF に再配布する経路情報を設定します。

インタフェース経路情報

インタフェース経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

スタティック経路情報

スタティック経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

RIP 経路情報

RIP 経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

16.1.2 優先度情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→「ルーティングマネージャ情報」→「優先度情報」

■優先度情報	
優先度	RIP 120
	OSPF 110

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

優先度

複数のルーティングプロトコルで同じ経路情報を受信した場合や受信した経路情報がスタティック経路情報と同じだった場合、どの経路情報を優先的に使用するかを優先度で判断します。優先度を1～254の範囲の10進数で指定し、より小さい値が、より高い優先度を示します。

RIP

RIP 経路情報の優先度を指定します。省略時は、120が設定されます。

OSPF

OSPF 経路情報の優先度を指定します。省略時は、110が設定されます。

こんな事に気をつけて

- 優先度は、ほかのプロトコルやスタティック経路情報に設定されている値と同じ値は指定しないでください。
- スタティック経路情報の優先度の初期値は1です。

16.1.3 ECMP 情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[ルーティングマネージャ情報]
→ [ECMP 情報]

■ECMP情報 ⓘ

ECMP機能	☒ 使用しない ☐ ハッシュ方式
OSPF使用ECMP数	1

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

ECMP 機能

IPv4 ルーティング機能で、ECMP（Equal-Cost Multipath）を使用しない場合は、“使用しない”を選択します。また、ECMPを使用する場合は、ハッシュ方式を選択します。

- ハッシュ方式
ハッシュ方式とは、送信元IPアドレス、あて先IPアドレスを元にハッシュ値を計算し、その値に従って送出パスを決定する方式です。通信の連続性および到達順はほぼ保証されますが、トラフィックが一部の通信パスにかたよる可能性があります。

OSPF 使用 ECMP 数

OSPFが生成した経路情報で、ECMPで扱う経路の最大値を1～4の範囲で指定します。ECMP機能を使用しない場合は、設定は無効となります。

こんな事に気をつけて

デフォルトルートは ECMP として扱われません。

16.2 RIP 関連

[操作] 「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]

ルーティングプロトコル情報		
ルーティングマネージャ情報	RIP 関連	OSPF 関連
	IPv6 ルーティングマネージャ情報	IPv6 RIP 関連
		IPv6 OSPF 関連
RIP タイマ情報	RIP マルチパス情報	RIP 再配布フィルタリング情報
RIP ユニキャスト送信情報	RIP 相手フィルタリング情報	

16.2.1 RIP タイマ情報

[操作] 「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 タイマ情報]

■RIP タイマ情報

?

定期広報タイマ	間隔	30 秒
	ゆらぎ幅	50 %
有効期限タイマ		3 分
ガーベージタイマ		2 分

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

定期広報タイマ

間隔

RESPONSE パケットで定期的に経路を広報する間隔を指定します。初期値は 30 秒です。指定できる範囲は以下のとおりです。

有効範囲)
10～3600 秒
1～60 分
1 時間

ゆらぎ幅

定期広報タイマのゆらぎ幅を指定します。初期値は 50 % です。指定できる範囲は以下のとおりです。

有効範囲)
0～50 %

有効期限タイマ

RESPONSE パケットで更新されない経路情報の有効期限を指定します。初期値は 3 分です。指定できる範囲は以下のとおりです。

有効範囲)
10～3600 秒
1～60 分
1 時間

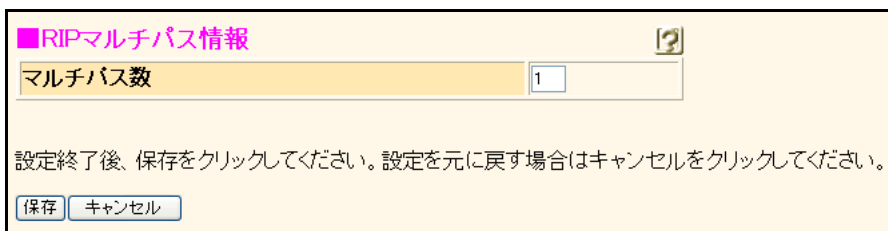
ガーベージタイマ

有効期限が切れた場合に、その経路情報をメトリック 16 で広報する時間を指定します。初期値は 2 分です。指定できる範囲は以下のとおりです。

有効範囲)
10～3600 秒
1～60 分
1 時間

16.2.2 RIP マルチパス情報

[操作] 「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]

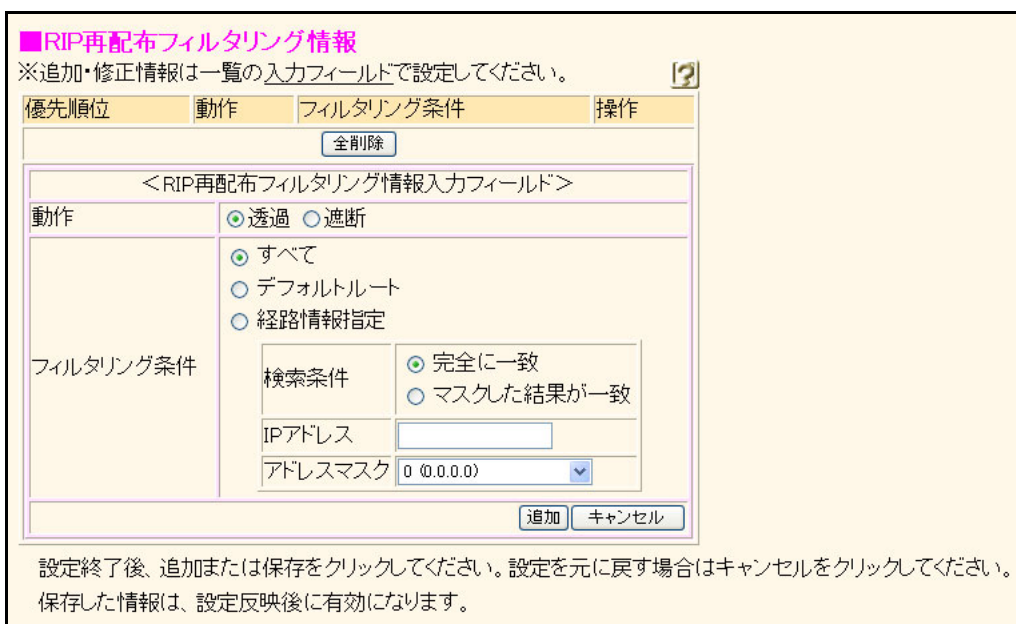


マルチパス数

RIPで受信可能な同じあて先への経路情報数を、1～2の範囲の10進数で指定します。省略時は、1が設定されます。

16.2.3 RIP 再配布フィルタリング情報

[操作] 「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 再配布フィルタリング情報]



現在、設定されている RIP 再配布フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。RIP 再配布フィルタリング情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53)を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

動作

RIPに再配布する経路情報の動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

対象とするフィルタリング条件を設定します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。なお、IPアドレスに0.0.0.0、アドレスマスクに0を指定した場合、デフォルトルートをフィルタリング対象とします。

検索条件

- 完全に一致
指定したIPアドレスとアドレスマスクが完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したIPアドレスと、再配布経路情報のそれぞれを指定したアドレスマスクでマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

こんな事に気をつけて

すべてのフィルタリング条件に一致しない経路情報は遮断されます。

16.2.4 RIP ユニキャスト送信情報

[操作] 「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]

■RIPユニキャスト送信情報

※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。

送信先IPアドレス 送信RIPバージョン 操作

全削除

<RIPユニキャスト送信情報入力フィールド>

送信先IPアドレス

送信RIPバージョン ☐ V1 ☒ V2

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、設定されている RIP ユニキャスト送信情報の定義が表示されています。RIP ユニキャスト送信情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

送信先 IP アドレス

RIP をユニキャストで送信する送信先の IP アドレスを指定します。

有効範囲)

10.0.1 ～ 126.255.255.254

128.0.0.1 ～ 191.255.255.254

192.0.0.1 ～ 223.255.255.254

送信 RIP バージョン

ユニキャストで送信する RIP のバージョンを選択します。

16.2.5 RIP 相手フィルタリング情報

[操作] 「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 相手フィルタリング情報]

現在、設定されている RIP 相手フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。RIP 相手フィルタリング情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した相手情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

動作

受信した RIP 情報の動作を以下の 2 つから選択します。

- 透過
フィルタリング条件と一致した場合に、相手ルータからの RIP パケットを透過します。
- 遮断
フィルタリング条件と一致した場合に、相手ルータからの RIP パケットを遮断します。

フィルタリング条件

対象とする相手情報を設定します。

- すべて
すべての相手ルータからの RIP パケットをフィルタリング対象とします。
- 相手側 IP アドレス指定
指定した RIP 送信元 IP アドレスをフィルタリング対象とします。
有効範囲)
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

こんな事に気をつけて

すべてのフィルタリング条件に一致しない相手ルータからの RIP パケットは遮断されます。

16.3 OSPF 関連

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[OSPF 関連]

ルーティングプロトコル情報		
ルーティングマネージャ情報	RIP関連	OSPF関連
IPv6 ルーティングマネージャ情報 ルータID情報 AS外部経路集約情報	IPv6 RIP関連 OSPFエリア情報 OSPF再配布フィルタリング情報	IPv6 OSPF関連 AS境界ルータ情報

16.3.1 ルータ ID 情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[OSPF 関連]→[ルータ ID 情報]

ルータID情報

?

ルータID

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

ルータ ID

OSPF 接続で、自装置を唯一に示す ID を設定します。ID は、ほかルータと重複しない値を指定し、一般的には自装置の IPv4 アドレスを使用します。

設定を省略または 0.0.0.0 を指定した場合、以下のとおり ID を自動的に選択し、使用します。

- ループバックインタフェースに追加 IP アドレスが設定されている場合は、その IP アドレスを選択し、使用します。
- ループバックインタフェースに追加 IP アドレスが設定されていない場合は、LAN インタフェースに設定されている IPv4 アドレスの中からインタフェースの Up / Down の状態に関係なく最大の IPv4 アドレスを選択し、使用します。

こんな事に気をつけて

OSPF ルータ ID は、ほかの装置と重複しないように指定してください。正しくルーティングできない場合があります。

16.3.2 OSPF エリア情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[OSPF 関連]→[OSPF エリア情報]

■OSPFエリア情報				
エリア定義番号	エリアID	エリア種別	コスト値	操作
追加 全削除				
保存した情報は、設定反映後に有効になります。				

現在、この装置に設定されている OSPF エリア情報の定義が表示されています。エリア定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[OSPF 関連]→[OSPF エリア情報]→[追加]

ルーティングプロトコル情報 - OSPF エリア情報 (0)		
OSPF エリア基本情報	経路集約情報	サマリLSA入出力可否情報
バーチャルリンク情報		

16.3.2.1 OSPF エリア基本情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[OSPF 関連]→[OSPF エリア情報]→[追加]→[OSPF エリア基本情報]

■OSPFエリア基本情報	
エリアID	
エリア種別	☒ 通常エリア ☐ スタブエリア ☐ 準スタブエリア
デフォルトルートコスト値	1 ※ エリア種別がスタブエリアまたは準スタブエリアの場合のみ有効です。
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
保存 キャンセル	

エリアID

エリアIDをアドレス（ドット形式）または10進数を使用して指定します。

こんな事に気をつけて

OSPFを利用する場合は、エリアIDを必ず設定してください。

こんな事に気をつけて

バックボーンエリアにスタブエリアまたは準スタブエリアを設定した場合も、通常エリアとして動作します。

エリア種別

バックボーンエリア以外のエリアに対し、エリア種別を選択します。

デフォルトルートコスト値

エリア境界ルータがスタブエリアまたは準スタブエリアに広報するデフォルトルートのコストを0～16777215の範囲で指定します。

16.3.2.2 経路集約情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[OSPF 関連]→[OSPF エリア情報]
→[追加]→[経路集約情報]

■経路集約情報
 ※追加・修正情報は一覧ので設定してください。 

集約経路	操作
全削除	
<経路集約情報入力フィールド>	
ネットワークアドレス	
ネットマスク	0 0.0.0.0 
コスト	
追加 キャンセル	

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

現在、この装置に設定されている経路集約情報の定義が表示されています。1 エリアでの経路集約情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

ネットワークアドレス

エリア内部経路で集約するネットワークアドレスを指定します。

ネットマスク

ネットマスクを選択します。

コスト

集約経路情報のコストを0～16777215の範囲の10進数で指定します。省略時は、集約される経路情報の中でもっとも大きい値のコストが使用されます。

16.3.2.3 サマリLSA入出力可否情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[OSPF 関連]→[OSPF エリア情報]
→[追加]→[サマリLSA入出力可否情報]

■サマリLSA入出力可否情報
※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。

優先順位	動作	方向	対象経路情報	操作
全削除				
<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			
	アドレスマスク	0 (0.0.0.0) v		
追加 キャンセル				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているサマリLSA入出力可否定義が表示されています。処理は優先順位1から順に行われます。サマリLSA入出力可否の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53)を参照してください。処理するボタンをクリックし、次のページへ進みます。

サマリLSAの入力時は、優先順位の高い定義から順に入力方向の対象経路情報を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の対象経路情報は参照されません。

また、入力方向のすべての対象経路情報に一致しないサマリLSA経路情報は遮断されます。サマリLSAの出力時は、優先順位の高い定義から順に出力方向の対象経路情報を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の対象経路情報は参照されません。また、出力方向のすべての対象経路情報に一致しないサマリLSA経路情報は遮断されます。

動作

対象経路情報に該当するサマリLSAの動作を以下の2つから選択します。

- 透過
対象経路情報と一致した場合にサマリLSAをエリア間で透過します。
- 遮断
対象経路情報と一致した場合にサマリLSAをエリア間で遮断します。

方向

サマリLSA入出力可否の判断を行うタイミングを選択します。

- 入力
サマリ入出力可否の判断を、ほかのエリアからの入力時に行う場合に選択します。
- 出力
サマリ入出力可否の判断を、ほかのエリアからの出力時に行う場合に選択します。

対象経路情報

入出力可否の対象となる経路情報を選択します。

- すべて
すべてのサマリ LSA を入出力可否情報の対象とします。
- 経路情報指定
入出力可否の対象とする経路情報を指定します。
経路情報を指定するときは、サマリ LSA 経路の検索条件として、“完全に一致” または、“マスクした結果が一致” を選択します。“完全に一致” を選択すると、指定した IP アドレスとアドレスマスクが完全に一致したサマリ LSA 経路情報を入出力可否の対象とします。
“マスクした結果が一致” を選択すると、指定した IP アドレスと、サマリ LSA 経路情報を、指定したアドレスマスクでマスクした結果が一致した場合、そのサマリ LSA 経路情報を入出力可否の対象とします。

こんな事に気をつけて

「OSPF 関連」の「集約経路情報」で設定している集約経路情報は、そのエリアからの出力時には遮断できません。以下の経路情報は、サマリ LSA 入出力可否の対象となりません。

- 各エリアの AS 境界ルータから注入された AS 外部経路
- スタブエリアおよび準スタブエリアのエリア境界ルータが注入するデフォルト経路
- type4 のサマリ LSA

16.3.2.4 バーチャルリンク情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[OSPF 関連]→[OSPF エリア情報]
→[追加]→[バーチャルリンク情報]

■バーチャルリンク情報

※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。

接続先ルータ ID	Hello パケット送信間隔	隣接ルータ停止確認間隔	認証方式	操作
	パケット再送間隔	LSU パケット送信遅延時間		

全削除

<バーチャルリンク情報入力フィールド>

接続先ルータID

Hello パケット送信間隔 秒

隣接ルータ停止確認間隔 秒

パケット再送間隔 秒

LSU パケット送信遅延時間 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
 認証鍵ID
 認証鍵

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、この装置に設定されているバーチャルリンク情報の定義が表示されています。バーチャルリンク情報の定義数は、仕様一覧「2.3 システム最大値一覧」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

接続先ルータ ID

接続先ルータの OSPF ルータ ID を指定します。

Hello パケット送信間隔

バーチャルリンク接続先との OSPF 隣接関係の維持に使用する Hello パケットの送信間隔を指定します。奨励値は“10 秒”です。

有効範囲)

1～18 時間

1～1092 分

1～65535 秒

こんな事に気をつけて

バーチャルリンク接続先と同じ Hello パケット送信間隔を指定してください。異なる値を指定するとルーティングを行うことができません。

隣接ルータ停止確認間隔

バーチャルリンクでの OSPF 隣接関係の維持に使用する、隣接ルータ停止確認間隔を指定します。Hello パケット送信間隔より大きな値を設定する必要があります。Hello パケット送信間隔の 4 倍をお勧めします。通常は、40 秒を指定します。

有効範囲)
1 ～ 18 時間
1 ～ 1092 分
1 ～ 65535 秒

こんな事に気をつけて

バーチャルリンク接続先と同じ隣接ルータ停止確認間隔を指定してください。異なる値を指定するとルーティングを行うことができません。

パケット再送間隔

バーチャルリンクで OSPF パケットを再送する間隔を指定します。

有効範囲)
1 ～ 18 時間
1 ～ 1092 分
1 ～ 65535 秒

LSU パケット送信遅延時間

LSU (Link State Update) パケットの送信遅延時間を指定します。LSU パケットでは、LSA (Link State Advertisement) を作成してからの経過時間に対し、この設定時間を加算して広報します。

有効範囲)
1 ～ 18 時間
1 ～ 1092 分
1 ～ 65535 秒

こんな事に気をつけて

一般的な装置では、LSU を作成してからの経過時間が 1 時間となった LSA を破棄します。このため、LSU 送信遅延時間に 1 時間以上を設定した場合は、正しくルーティングできない場合があります。

認証方式

パケットに対する認証方式を選択します。

鍵種別

テキスト認証で使用する鍵の種別を選択します。

認証鍵

テキスト認証で使用する鍵を指定します。鍵種別が“文字列”の場合は、8 文字以内で指定します。鍵種別が“16 進数”の場合は、16 進数を使用して 16 桁以内で指定します。16 桁未満の鍵を指定した場合、左詰めで設定され、残りは 16 桁になるまで 0x0 でパディングされます。

MD5 認証鍵 ID

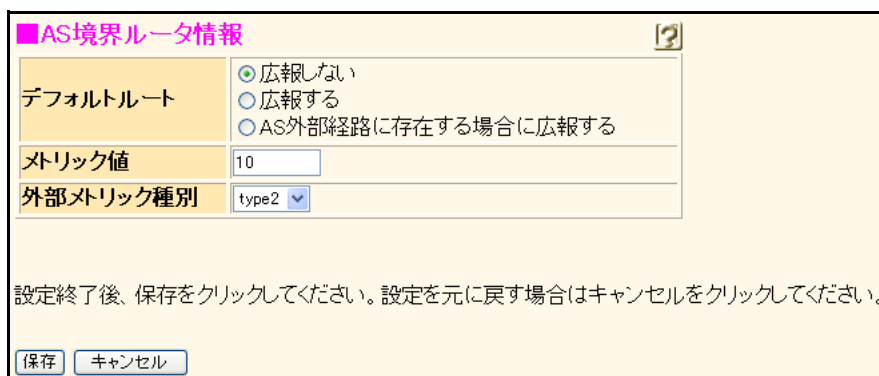
バーチャルリンクの MD5 認証で使用する鍵 ID を 1 ～ 255 の範囲で指定します。

MD5 認証鍵

バーチャルリンクの MD5 認証で使用する鍵を 16 文字以内で指定します。

16.3.3 AS境界ルータ情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[OSPF 関連]→[AS 境界ルータ情報]



デフォルトルート

デフォルトルートを広報する際の条件を選択します。

外部メトリック種別

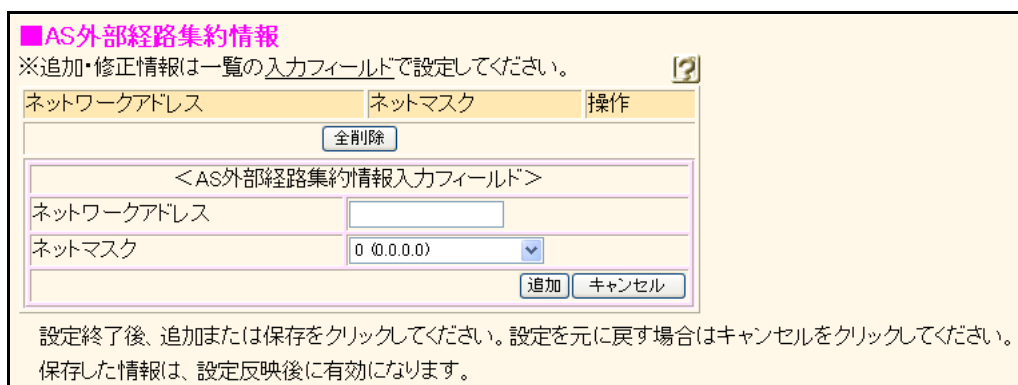
外部メトリックの種別を選択します。

メトリック値

デフォルトルートのメトリック値を0～16777214の範囲で指定します。

16.3.4 AS外部経路集約情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[OSPF 関連]→[AS 外部経路集約情報]



現在、このネットワークに設定されているAS外部経路集約情報の定義が表示されています。AS外部経路集約情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53)を参照してください。処理するボタンをクリックし、次のページへ進みます。

ネットワークアドレス

AS外部経路で集約するネットワークアドレスを指定します。

ネットマスク

ネットマスクを選択します。

16.3.5 OSPF 再配布フィルタリング情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[OSPF 関連]
→[OSPF再配布フィルタリング情報]

■OSPF再配布フィルタリング情報
※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。

優先順位	動作	フィルタリング条件	操作
[全削除]			
＜OSPF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	 アドレスマスク 0 0.0.0.0	
メトリック	☒ 指定しない ☐ 指定する		
	メトリック値		
	メトリックタイプ	type2	
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている OSPF 再配布フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。OSPF 再配布フィルタリング情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53)を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があつた時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

こんな事に気をつけて

すべてのフィルタリング条件に一致しない再配布経路情報は遮断されます。

動作

OSPF に再配布する再配布経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

対象とするフィルタリング条件を設定します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致” または、“マスクした結果が一致” を選択します。なお、IP アドレスに 0.0.0.0、アドレスマスクに 0 を指定した場合、デフォルトルートをフィルタリング対象とします。

検索条件

- 完全に一致
指定したIPアドレスとアドレスマスクが完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したIPアドレスと、再配布経路情報のそれぞれを、指定したアドレスマスクでマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

こんな事に気をつけて

デフォルトルート OSPF に再配布する場合は、「AS 境界 ルータ情報」の設定も必要となります。

メトリック

経路情報を OSPF に再配布する際のメトリック値、メトリックタイプを指定する場合は、“指定する”を選択します。“指定しない”を選択した場合は、「ルーティングマネージャ情報」で設定したメトリック値、および、メトリックタイプとなります。なお、本設定は動作に“透過”を設定した場合に有効です。

メトリック値

OSPF に再配布する際のメトリック値を 0 ～ 16777214 の範囲で指定します。

こんな事に気をつけて

動作に遮断を指定した場合、メトリック値は指定できません。

メトリックタイプ

OSPF に再配布する際のメトリックタイプを選択します。

16.4 IPv6 ルーティングマネージャ情報

適用機種 SR-S724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[IPv6 ルーティングマネージャ情報]

ルーティングプロトコル情報	
ルーティングマネージャ情報	RIP関連 OSPF関連 IPv6 ルーティングマネージャ情報 IPv6 RIP関連 IPv6 OSPF関連
IPv6再配布情報	IPv6優先度情報

16.4.1 IPv6再配布情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[IPv6 ルーティングマネージャ情報]
→[IPv6再配布情報]

■IPv6再配布情報

?

RIP	インタフェース経路情報	☐ 再配布しない ☒ 再配布する
	スタティック経路情報	☐ 再配布しない ☒ 再配布する
	OSPF経路情報	☒ 再配布しない ☐ 再配布する メトリック値: 0
	DHCP経路情報	☒ 再配布しない ☐ 再配布する メトリック値: 0
OSPF	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: メトリックタイプ: type2
	スタティック経路情報	☒ 再配布しない ☐ 再配布する メトリック値: メトリックタイプ: type2
	RIP経路情報	☒ 再配布しない ☐ 再配布する メトリック値: メトリックタイプ: type2
	DHCP経路情報	☒ 再配布しない ☐ 再配布する メトリック値: メトリックタイプ: type2

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

RIP

RIPに再配布する経路情報を設定します。

インタフェース経路情報

インタフェース経路情報をRIPに再配布する場合は、“再配布する”を選択します。

スタティック経路情報

スタティック経路情報を RIP に再配布する場合は、“再配布する”を選択します。

OSPF 経路情報

OSPF 経路情報を RIP に再配布する場合は、“再配布する”を選択します。

メトリック値

RIP に再配布する際のメトリック値を選択します。

DHCP 経路情報

DHCP 経路情報を RIP に再配布する場合は、“再配布する”を選択します。

メトリック値

RIP に再配布する際のメトリック値を選択します。

OSPF

OSPF に再配布する経路情報を設定します。

インタフェース経路情報

インタフェース経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

スタティック経路情報

スタティック経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

RIP 経路情報

RIP 経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

SPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

DHCP 経路情報

DHCP 経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

16.4.2 IPv6 優先度情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[IPv6 ルーティングマネージャ情報]
→[IPv6 優先度情報]

■ IPv6 優先度情報

優先度

RIP	
OSPF	
DHCP	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

優先度

複数のルーティングプロトコルで同じ経路情報を受信した場合や受信した経路情報がスタティック経路情報と同じだった場合、どの経路情報を優先的に使用するかを優先度で判断します。

優先度は、1～254の10進数で指定し、より小さい値が、より高い優先度を示します。

RIP

RIP 経路情報の優先度を指定します。省略時は、120が設定されます。

OSPF

OSPF 経路情報の優先度を指定します。省略時は、110が設定されます。

DHCP

DHCP 経路情報の優先度を指定します。省略時は、10が設定されます。

こんな事に気をつけて

- 優先度は、ほかのプロトコルやスタティック経路情報に設定されている値と同じ値は指定しないでください。
- スタティック経路情報の優先度の初期値は 1 です。

16.5 IPv6 RIP 関連

適用機種 SR-S724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→ [IPv6 RIP 関連]

ルーティングプロトコル情報		
ルーティングマネージャ情報	RIP関連	OSPF関連
IPv6 ルーティングマネージャ情報	IPv6 RIP関連	IPv6 OSPF関連
IPv6 RIPタイマ情報	IPv6 RIPマルチパス情報	IPv6 RIP再配布フィルタリング情報

16.5.1 IPv6 RIP タイマ情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→ [IPv6 RIP 関連]
→ [IPv6 RIP タイマ情報]

■ IPv6 RIPタイマ情報

?

定期広報タイマ	30 秒
有効期限タイマ	180 秒
ガーベージタイマ	120 秒

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

定期広報タイマ

RESPONSE パケットで定期的に経路を広報する間隔を指定します。初期値は 30 秒です。

有効範囲)
10～3600 秒
1～60 分
1 時間

ガーベージタイマ

有効期限が切れた場合に、その経路情報をメトリック 16 で広報する時間を指定します。初期値は 120 秒です。

有効範囲)
10～3600 秒
1～60 分
1 時間

有効期限タイマ

RESPONSE パケットで更新されない経路情報の有効期限を指定します。初期値は 180 秒です。

有効範囲)
10～3600 秒
1～60 分
1 時間

16.5.2 IPv6 RIP マルチパス情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→ [IPv6 RIP 関連]
→ [IPv6 RIP マルチパス情報]

■IPv6 RIPマルチパス情報

マルチパス数

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

マルチパス数

RIPで受信可能な同じ先への経路情報数を1～2の範囲で指定します。省略時は、1が設定されます。

16.5.3 IPv6 RIP 再配布フィルタリング情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→ [IPv6 RIP 関連]
→ [IPv6 RIP 再配布フィルタリング情報]

■IPv6 RIP再配布フィルタリング情報

※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。

優先順位	動作	フィルタリング条件	操作
全削除			
＜IPv6 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 ☐ 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	
	アドレス/プレフィックス		
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、設定されているRIP再配布フィルタリング情報の定義が表示されています。処理は優先順位1から順に行われます。装置全体でのRIP再配布フィルタリング情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53)を参照してください。処理するボタンをクリックし、次ページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。

なお、一致した以降の条件は参照されません。

動作

RIPに再配布する経路情報の動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

対象とするフィルタリング条件を選択します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。

検索条件

検索条件を選択します。

- 完全に一致
指定したプレフィックスとプレフィックス長が完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したプレフィックスと、再配布経路情報のそれぞれを、指定したプレフィックス長でマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

こんな事に気をつけて

すべてのフィルタリング条件に一致しない経路情報は遮断されます。

16.6 IPv6 OSPF 関連

適用機種 SR-S724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→ [IPv6 OSPF 関連]

ルーティングプロトコル情報		
ルーティングマネージャ情報	RIP関連	OSPF関連
IPv6 ルータID情報 IPv6 OSPF再配布フィルタリング情報		IPv6 OSPFエリア情報 IPv6 AS境界ルータ情報

16.6.1 IPv6 ルータ ID 情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→ [IPv6 OSPF 関連]
→ [IPv6 ルータ ID 情報]

■IPv6 ルータID情報

?

ルータID

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

ルータ ID

IPv6 OSPF 接続での自装置を一意に示す ID を指定します。
ID はほかのルータと重複しない値を指定してください。
ルータ ID の設定を削除する場合は、ルータ ID の値を省略したうえで保存してください。

こんな事に気をつけて

IPv6 OSPF を利用する場合は、OSPF ルータ ID を必ず設定してください。未設定時の自動設定機能はありません。

16.6.2 IPv6 OSPF エリア情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[IPv6 OSPF 関連]
→[IPv6 OSPF エリア情報]

■IPv6 OSPFエリア情報				
エリア定義番号	エリアID	エリア種別	コスト値	操作
追加 全削除				

保存した情報は、設定反映後に有効になります。

現在、設定されている OSPF エリア情報の定義が表示されています。装置全体でのエリア定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[IPv6 OSPF 関連]
→[IPv6 OSPF エリア情報]→[追加]

ルーティングプロトコル情報 - IPv6 OSPF エリア情報(0)		
IPv6 OSPF エリア基本情報	IPv6 経路集約情報	IPv6 エリア間プレフィックスLSA入出力可否情報

16.6.2.1 IPv6 OSPF エリア基本情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[IPv6 OSPF 関連]
→[IPv6 OSPF エリア情報]→[追加]→[IPv6 OSPF エリア基本情報]

■IPv6 OSPFエリア基本情報	
エリアID	
エリア種別	☒ 通常エリア ☐ スタブエリア
デフォルトルートコスト値	1 ※ エリア種別がスタブエリアの場合のみ有効です。

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

エリア ID

エリア ID を 0.0.0.0～255.255.255.255 の IPv4 アドレス表記（ドット形式）または 0～4294967295 の 10 進数表記で指定します。バックボーンエリアの場合は、0.0.0.0 または 0 を指定します。

こんな事に気をつけて

OSPF を利用する場合は、エリア ID を必ず設定してください。

エリア種別

バックボーンエリア以外のエリアに対し、エリア種別を選択します。

こんな事に気をつけて

バックボーンエリアでスタブエリアと設定した場合も、通常エリアとして動作します。

デフォルトルートコスト値

エリア境界ルータがスタブエリアに広報するデフォルトルートのコストを 1～16777215 の範囲で指定します。

16.6.2.1.1 IPv6 経路集約情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[IPv6 OSPF 関連]
→[IPv6 OSPF エリア情報]→[追加]→「IPv6 経路集約情報」

■IPv6 経路集約情報

※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。 ?

集約経路	操作
全削除	

<IPv6 経路集約情報入力フィールド>

プレフィックス/プレフィックス長

コスト

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、設定されている経路集約情報の定義が表示されています。1 エリアでの経路集約情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

プレフィックス／プレフィックス長

エリア内部経路を集約する経路情報を指定します。

コスト

集約経路情報のコストを、10進数を使用して0～16777215の範囲で指定します。省略時は、集約される経路情報の中で、もっとも大きい値のコストが使用されます。

16.6.2.1.2 IPv6 エリア間プレフィックスLSA入出力可否情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[IPv6 OSPF 関連]
→[IPv6 OSPF エリア情報]→[追加]→「IPv6 エリア間プレフィックスLSA入出力可否情報」

現在、設定されているエリア間プレフィックスLSA入出力可否定義の定義が表示されています。処理は優先順位1から順に行われます。装置全体でのエリア間プレフィックスLSA入出力可否の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53)を参照してください。処理するボタンをクリックし、次ページへ進みます。

エリア間プレフィックスLSAの入力時は、優先順位の高い定義から順に入力方向の対象経路情報を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の対象経路情報は参照されません。また、入力方向のすべての対象経路情報に一致しないエリア間プレフィックスLSA経路情報は遮断されます。

エリア間プレフィックスLSAの出力時は、優先順位の高い定義から順に出力方向の対象経路情報を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の対象経路情報は参照されません。また、出力方向のすべての対象経路情報に一致しないエリア間プレフィックスLSA経路情報は遮断されます。

動作

対象経路情報に該当するエリア間プレフィックスLSAの動作を以下の2つから選択します。

- 透過
条件と一致した場合に経路情報を透過します。
- 遮断
条件と一致した場合に経路情報を遮断します。

方向

エリア間プレフィックスLSA入出力可否の判断をほかのエリアからの入力時に行うか、ほかのエリアへの出力時に行うかを選択します。

対象経路情報

入出力可否の対象となる経路情報を選択します。

- すべて
すべてのエリア間プレフィックスLSAが入出力可否の対象となります。
- 経路情報指定
入出力可否の対象とする経路情報を指定できます。経路情報を指定するときは、エリア間プレフィックスLSA経路の検索条件として、“完全に一致”または“マスクした結果が一致”を選択します。

検索条件

検索条件を選択します。

- 完全に一致
指定したプレフィックスとプレフィックス長が完全に一致したエリア間プレフィックス LSA 経路情報を入出力可否の対象とします。
- マスクした結果が一致
指定したプレフィックスと、エリア間プレフィックス LSA 経路情報を、指定したプレフィックス長でマスクした結果が一致した場合、そのエリア間プレフィックス LSA 経路情報を入出力可否の対象とします。

こんな事に気をつけて

- 「IPv6 OSPF 関連」の「IPv6 経路集約情報」で設定している経路集約情報は、そのエリアからの出力時には遮断できません。
- 以下の経路情報は、エリア間プレフィックス LSA 入出力可否の対象となりません。
 - スタブエリアのエリア境界ルータが注入するデフォルト経路

16.6.3 IPv6 AS 境界ルータ情報

〔操作〕 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→ [IPv6 OSPF 関連]
→ [IPv6 AS 境界ルータ情報]

■ IPv6 AS境界ルータ情報

デフォルトルート/TD>

☒ 広報しない
☐ 広報する
☐ AS外部経路に存在する場合に広報する

メトリック値

10

外部メトリック種別

type2

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

デフォルトルート

デフォルトルートを広報する際の条件を選択します。

外部メトリック種別

外部メトリックの種別を選択します。

メトリック値

デフォルトルートのメトリック値を 0～16777214 の範囲の 10 進数で指定します。省略時は、10 が設定されます。

16.6.4 IPv6 OSPF 再配布フィルタリング情報

[操作] 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→[IPv6 OSPF 関連]
→[IPv6 OSPF 再配布フィルタリング情報]

■IPv6 OSPF再配布フィルタリング情報
※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。

優先順位	動作	フィルタリング条件	操作
全削除			
<IPv6 OSPF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 プレフィックス/ プレフィックス長 /		
メトリック	☒ 指定しない ☐ 指定する		
	メトリック値 メトリックタイプ type2		
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている OSPF 再配布フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。装置全体での OSPF 再配布フィルタリング情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次ページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。

なお、一致した以降の条件は参照されません。

動作

OSPF に再配布する再配布経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

対象とするフィルタリング条件を選択します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致”または“マスクした結果が一致”を選択します。
なお、::/0 を指定した場合、デフォルトルートをフィルタリング対象とします。

検索条件

検索条件を選択します。

- 完全に一致
指定したプレフィックスとプレフィックス長が完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したプレフィックスと、再配布経路情報のプレフィックスのそれぞれを、指定したプレフィックス長でマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

こんな事に気をつけて

デフォルトルート OSPF に再配布する場合は、「IPv6 AS 境界ルータ情報」の設定も必要となります。

メトリック

経路情報を OSPF に再配布する際のメトリック値、メトリックタイプを指定する場合は、“指定する”を選択します。“指定しない”を選択した場合は、「IPv6 ルーティングマネージャ情報」で設定したメトリック値、および、メトリックタイプとなります。なお、本設定は動作に“透過”を設定した場合に有効です。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。

こんな事に気をつけて

動作に遮断を指定した場合、メトリック値は指定できません。

メトリックタイプ

OSPF に再配布する際のメトリックタイプを選択します。

17 マルチキャスト情報

適用機種 SR-S716C2, 724TC1, 748TC1

[操作] 「設定メニュー」→詳細設定「マルチキャスト情報」

マルチキャスト情報

[IPマルチキャスト情報](#)

[IPマルチキャストスタティックRP情報](#)

[IPマルチキャストスタティック経路情報](#)

17.1 IPマルチキャスト情報

[操作] 「設定メニュー」→詳細設定「マルチキャスト情報」→[IPマルチキャスト情報]

■IPマルチキャスト情報

L2	宛先不明マルチキャストパケット	☒ フラッディングする ☐ フラッディングしない
IGMP	IGMP Membership Report 送信抑止	☒ する ☐ しない
PIM-SM	RP候補	☒ しない ☐ する IPアドレス 0.0.0.0 プライオリティ 0
	BSR候補	☒ しない ☐ する IPアドレス 0.0.0.0 プライオリティ 0
	SPTへの経路変更	☒ する ☐ しない
	register	☒ チェックサム ☐ ヘッダ部 ☐ パケット全体

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

L2

宛先不明マルチキャストパケット

宛先不明マルチキャストパケットの動作の設定です。
 本設定はマルチキャスト・ルーティング動作時（スタティック経路、PIM-DM、PIM-SM）だけ有効となります。
 マルチキャスト・ルーティング未動作時は、本設定にかかわらず、宛先不明マルチキャストパケットは同一VLAN内にフラッディングされます。

IGMP

IGMP Membership Report 送信抑止

IGMP Query 受信時の応答動作を指定します。

- する
 IGMPv2 (RFC2236) 仕様に従い、他ホストからのIGMP Membership Report を受信した場合は、重複によるトラフィック増加の防止のため、本装置からはIGMP Membership Report を送出しません。
- しない
 常に送信します。

PIM-SM

RP 候補

ランデブー・ポイント (RP) の設定です。マルチキャスト・ルーティングプロトコルに PIM-SM を利用する場合は、RP として動作するルータがネットワーク上に 1 台以上が必要です。RP の設定は、1 台のルータだけで行っても、複数のルータで行ってもかまいません。トラフィックを分散する場合は、複数台のルータで RP の設定を行っておきます。

IP アドレス

RP として動作するインタフェースの IP アドレスを指定します。設定を省略または 0.0.0.0 を指定した場合、RP として動作できるインタフェースを自動で検索します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

プライオリティ

RP のプライオリティ情報を 0 ~ 255 の範囲の 10 進数で指定します。数が小さいほど優先度は高くなります。初期値は 0 です。

BSR 候補

ブート・ストラップ・ルータ (BSR) の設定です。マルチキャスト・ルーティングプロトコルに PIM-SM を利用する場合は、BSR として動作するルータがネットワーク上に必要です。BSR の設定は、1 台のルータだけで行っても、複数のルータで行ってもかまいません。障害に強いネットワークを構成する場合は、複数台のルータで BSR の設定を行っておきます。

IP アドレス

BSR として動作するインタフェースの IP アドレスを指定します。設定を省略または 0.0.0.0 を指定した場合、BSR として動作できるインタフェースを自動で検索します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

プライオリティ

BSR のプライオリティ情報を 0 ~ 255 の範囲の 10 進数で指定します。数が大きいほど優先度は高くなります。初期値は 0 です。

SPT への経路変更

SPT (Shortest Path Tree) への経路変更を選択します。SPT の設定は、マルチキャストパケットを受信者となる last hop router 上で行います。

register

PIM Register パケットを設定します。マルチキャストパケットを送信するルータ上で行います。

チェックサム

PIM Register パケットの送信時のチェックサムの計算方法を設定することができます。

PIM Register パケットのチェックサムの計算範囲は、RFC2362 ではヘッダ部だけで計算するように定義されていますが、一部のルータはパケット全体で計算します。このようなルータが RP を行う場合は、PIM Register パケットが受信されない可能性があるため、チェックサムの計算範囲を“パケット全体”に変更する必要があります。

本装置は PIM Register パケットの受信時に、ヘッダ部 (RFC2362 準拠) とパケット全体の 2 つの方法で計算するため、本装置が RP を行う場合は、どちらの計算方法のパケットを受信しても問題はありません。

17.2 IP マルチキャストスタティック RP 情報

[操作] 「設定メニュー」→詳細設定「マルチキャスト情報」→[IP マルチキャストスタティック RP 情報]

■IPマルチキャストスタティックRP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	IPアドレス プライオリティ	操作
全削除		
<IPマルチキャストスタティックRP情報入力フィールド>		
IPアドレス		
プライオリティ		
		追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

現在、設定されている IP マルチキャストスタティック RP 情報の定義が表示されています。処理するボタンをクリックし、次ページへ進みます。

IP アドレス

RP として動作するインタフェースの IP アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

プライオリティ

RP のプライオリティ情報を 0 ~ 255 の範囲の 10 進数で指定します。数が小さいほど優先度は高くなります。

省略時は、0 が設定されます。

17.3 IP マルチキャストスタティック経路情報

[操作] 「設定メニュー」→詳細設定「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]

■IPマルチキャストスタティック経路情報
 ※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	配送元ホストアドレス マルチキャストグループアドレス 入力インタフェース 出力インタフェース グループ参加	インタフェース情報	操作

全削除

＜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
マルチキャストグループアドレス	
入力インタフェース	LAN0 ▾
出力インタフェース	
グループ参加	☒ しない ☐ する

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

現在、設定されている IP マルチキャストスタティック経路情報の定義が表示されています。IP マルチキャストスタティック経路の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

配送元ホストアドレス

配送元ホストを IPv4 アドレスで指定します。

有効範囲)

1.0.0.1 ～ 126.255.255.254

128.0.0.1 ～ 191.255.255.254

192.0.0.1 ～ 223.255.255.254

出力インタフェース

出力するインタフェースを指定します。複数指定する場合は、"," で区切ります。範囲指定の場合は "-" で区切ります。出力インタフェースは 20 個まで設定できます。

記述例)

lan0,lan2-lan4

マルチキャストグループアドレス

マルチキャストグループアドレスを 224.0.1.0 ～ 239.255.255.255 の範囲の IPv4 アドレスで指定します。

グループ参加

入力インタフェースでマルチキャストグループに参加するかどうかを指定します。"する"を選択した場合、入力インタフェースでは IGMP によるグループ参加を行います。

入力インタフェース

入力するインタフェースを選択します。

18 QoS 情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「QoS 情報」

QoS 情報

送信アルゴリズム情報

QoSキュー情報

SR-S308TL1、310TL2、316TL1、318TL2、324TL2、316C2、324TC1、328TR1、348TC1、716C2、724TC1、748TC1 では、「送信アルゴリズム情報」は表示されません。

18.1 送信アルゴリズム情報

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

[操作] 「設定メニュー」→詳細設定「QoS 情報」→「送信アルゴリズム情報」

■送信アルゴリズム情報

送信アルゴリズム

☒ strict priority方式
☐ Weighted round robin方式

キュー0の重み
 キュー1の重み
 キュー2の重み
 キュー3の重み

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

送信アルゴリズム

QoSの送信アルゴリズムを選択します。

“Weighted round robin 方式” を選択した場合は、各キューの重みを、0～255の範囲の10進数で指定します。

こんな事に気をつけて

Weighted round robin 方式で重みを0に設定したキューは、Strict priority 方式と同じ動作となり、1以上の重みを設定したキューより優先されます。

18.2 COSキュー情報

[操作] 「設定メニュー」→詳細設定「QoS 情報」→[COS キュー情報]

■COSキュー情報

バケットのCOS値

格納キュー

0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

COS キュー情報

パケットの COS 値と格納キューの対応を設定します。

指定した COS 値を持つパケットを指定したキューに格納します。

パケットは一度、出力ポート（自装置あてポート含む）の以下の個数のキューにキューイングされますが、その際、どのキューにキューイングされるかは、出力パケットの COS 値によって決定されます。

機種	キューの個数
SR-S208TC2、224TC2、208PD1、 224PS1、224CP1、248TC1、 308TL1、310TL2、316TL1、 318TL2、324TL2	4
SR-S316C2、324TC1、328TR1、 348TC1、716C2、724TC1、 748TC1	8

キュー番号が大きい程、出力優先順位が高いキューです。
指定されていないキューは使用されません。

19 STP 情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「STP 情報」

STP 情報		
基本情報	MSTP インスタンス情報	IEEE802.1ad 情報

SR-S328TR1 のみ、「IEEE802.1ad 情報」が表示されます。

19.1 基本情報

19.1.1 基本情報（初期表示または使用する選択時）

[操作] 「設定メニュー」→詳細設定「STP 情報」→[基本情報（STP 機能：初期表示または使用する）]

■基本情報

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 秒

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

32768

STP 動作モード

☒ STP
☐ RSTP
☐ MSTP

最大ホップカウント

20

MST 構成要素

リージョン名

region1

リビジョンレベル

0

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

初期表示または STP 機能に“使用する”を選択した場合に表示されます。

STP 機能

STP 機能を使用するかどうかを選択します。

- 使用しない
STP 機能を使用しない場合に選択します。
- 使用する
STP 機能を使用する場合に選択します。

ブリッジのハロー待ち時間

ルートブリッジまたは代表ブリッジから送出される構成情報 BPDU の待ち時間を 6～40 秒の範囲の 10 進数で指定します。省略時は、20 秒が設定されます。

フォワーディング遅延時間

構成情報 BPDU が一番時間がかかる経路に届く時間を 4 ～ 30 秒の範囲の 10 進数で指定します。この設定項目は本装置がルートブリッジとして動作する場合のみ有効です。省略時は、15 秒が設定されます。

ブリッジのハロー送出間隔

ルートブリッジになったときに送出する構成情報 BPDU の送信間隔を 1 ～ 10 秒の範囲の 10 進数で指定します。この設定項目は本装置がルートブリッジとして動作する場合のみ有効です。省略時は、2 秒が設定されます。

ブリッジの優先度

ルートブリッジ決定アルゴリズムで使用するブリッジの優先度を選択します。ブリッジの優先度は値の小さいほうがより優先となります。省略時は、32768 が設定されます。

こんな事に気をつけて

4096 で割り切れる以下の値のみ設定できます。

0, 4096, 8192, 12288, 16384, 20480, 24576, 28672,
32768, 36864, 40960, 45056, 49152, 53248, 57344,
61440

こんな事に気をつけて

ブリッジのハロー待ち時間、フォワーディング遅延時間およびブリッジのハロー送出間隔は、以下の設定値関連チェックを行います。1 つでも該当する設定値になる場合は、ブリッジのハロー待ち時間、フォワーディング遅延時間、ブリッジのハロー送出間隔の設定が無効となります。

- ブリッジのハロー待ち時間とフォワーディング遅延時間の設定値のチェック
ブリッジのハロー待ち時間 $\leq 2 \times$ (フォワーディング遅延時間 - 1.0 秒)
- ブリッジのハロー待ち時間とブリッジのハロー送出間隔の設定値のチェック
ブリッジのハロー待ち時間 $\geq 2 \times$ (ブリッジのハロー送出間隔 + 1.0 秒)

ブリッジのハロー待ち時間、フォワーディング遅延時間、ブリッジのハロー送出間隔の関連チェックで有効となる設定条件は、以下となります。

$2 \times$ (フォワーディング遅延時間 - 1.0 秒) $\geq$ ブリッジのハロー待ち時間 $\geq 2 \times$ (ブリッジのハロー送出間隔 + 1.0 秒)

STP 動作モード

STP の動作モードを以下から選択します。

- STP
STP (dot1d) を使用する場合に選択します。
- RSTP
RSTP (dot1w) を使用する場合に選択します。
- MSTP
MSTP (dot1s) を使用する場合に選択します。

最大ホップカウント

ルートブリッジが送信する BPDU フレームの最大ホップカウントを 1 ～ 40 の範囲の 10 進数で指定します。受信した BPDU フレームのホップカウントが 0 の場合、本装置は自身をルートブリッジとして、最大ホップカウントを設定した BPDU フレームを送信し始めます。省略時は、20 が設定されます。

リージョン名

リージョン名を、0x21 および 0x23 ～ 0x7e のコードで構成される 32 文字以内の ASCII 文字列で指定します。省略時は、“region1” が設定されます。

リビジョンレベル

リビジョンレベルを 0 ～ 255 の範囲の 10 進数で指定します。省略時は、0 が設定されます。

19.1.2 基本情報（使用しない選択時）

[操作] 「設定メニュー」→詳細設定「STP 情報」→「基本情報（STP 機能：使用しない）」

■基本情報

STP機能	☒ 使用しない ☐ 使用する
BPDU転送モード	☒ 転送しない ☐ 転送する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

STP 機能に “使用しない” を選択した場合に表示されます。

「STP 機能」の項目は、「基本情報（初期表示または使用する選択時）」を参照してください。

BPDU 転送モード

STP 機能が無効になったときの、BPDU フレームの転送有無を選択します。

こんな事に気をつけて

BPDU フレームは、VLAN タグが付与されないため、BPDU 転送モードで “転送する” が選択されている場合は、「ether 情報」の VLAN（Untagged）設定に従って転送されます。

19.2 MSTP インスタンス情報

[操作] 「設定メニュー」→詳細設定「STP 情報」→[MSTP インスタンス情報]

■MSTPインスタンス情報			
インスタンスID	ブリッジの優先度	MSTP-インスタンスへのVLAN割り当て (VLAN ID)	操作
1	32768		修正 初期化
2	32768		修正 初期化
3	32768		修正 初期化
4	32768		修正 初期化
5	32768		修正 初期化
6	32768		修正 初期化
7	32768		修正 初期化
8	32768		修正 初期化
9	32768		修正 初期化
10	32768		修正 初期化
11	32768		修正 初期化
12	32768		修正 初期化
13	32768		修正 初期化
14	32768		修正 初期化
15	32768		修正 初期化

全初期化

保存した情報は、設定反映後に有効になります。

現在、設定されている MSTP インスタンス情報が表示されています。インスタンス情報定義は 15 個まで設定することができます。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」→詳細設定「STP 情報」→[MSTP インスタンス情報] → [修正]

＜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
MSTP-インスタンスへのVLAN割り当て (VLAN ID)	

保存 キャンセル 一覧へ戻る

ブリッジの優先度

ルートブリッジ決定アルゴリズムで使用するブリッジの優先度を選択します。ブリッジの優先度は値の小さいほうがより優先となります。

こんな事に気をつけて

4096 で割り切れる以下の値のみ設定できます。

0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

MSTP インスタンスへのVLAN 割り当て (VLAN ID)

VLAN ID を 1 ～ 4094 の範囲の 10 進数で指定します。

VLAN ID を複数指定する場合は、”,” で区切ります。範囲指定の場合は “-” で区切ります。

こんな事に気をつけて

- 「ether 情報」の VLAN (Untagged/Tagged) が設定されていない場合は、無効となります。
- 本設定を指定しない場合は、無効となります。

19.3 IEEE802.1ad 情報

適用機種 SR-S328TR1

[操作] 「設定メニュー」→詳細設定「STP 情報」→ [IEEE802.1ad 情報]

IEEE802.1ad 情報

STP 動作ポート

☒ プロバイダーポート
☐ カスタマーポート

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

STP 動作ポート

IEEE802.1ad 使用時の STP 動作ポートを設定します。

- プロバイダーポート
プロバイダーポートで STP 動作を行います。
- カスタマーポート
カスタマーポートで STP 動作を行います。

こんな事に気をつけて

- 本設定は、IEEE802.1ad 動作時のみ有効です。
- IEEE802.1ad 未使用のポートは本コマンドで指定されたポートを含んだスパンニングツリーを構築します。

20 LLDP 情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「LLDP 情報」

LLDP 情報
基本情報

20.1 基本情報

[操作] 「設定メニュー」→詳細設定「LLDP 情報」→「基本情報」

■基本情報	
送信間隔時間	30 秒
最小送信間隔時間	2 秒
保持回数	4 回
送信停止時遅延時間	2 秒
受信情報更新通知最小間隔時間	5 秒

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

LLDP（Link Layer Discovery Protocol：隣接探索プロトコル）の装置全体に関する設定を行います。

こんな事に気をつけて

ポートごとの設定は、「ether 情報」-「LLDP 関連」で行ってください。

送信間隔時間

LLDP 情報を定期的に送信する間隔時間を 5～32768 秒の範囲で指定します。

最小送信間隔時間

最小送信間隔時間を 1 秒～（0.25 × 送信間隔時間）の範囲で指定します。

設定変更などにより LLDP 情報が変化したときに即座に LLDP 情報を送信しますが、最後に LLDP 情報を送信してから最小送信間隔時間経過していない場合は、最小送信間隔時間経過するまで待ってから LLDP 情報を送信します。

保持回数

本装置の LLDP 情報を受信した隣接装置が本装置の LLDP 情報を保持すべき有効時間を、送信間隔時間の回数で 2～10 回の範囲で指定します。

本装置の LLDP 情報の有効時間（TTL）は以下の式により計算されます。

$$\text{有効時間} = \text{送信間隔時間} \times \text{保持回数}$$

ただし、計算結果が 65535 秒を超えた場合は、有効時間を 65535 秒とします。

送信停止時遅延時間

「ether 情報」 - 「LLDP 関連」の「動作」で LLDP 情報を送信しないように設定変更したとき、送信処理を初期状態に戻すまでの遅延時間を 1 ～ 10 秒の範囲で指定します。

受信情報更新通知最小間隔時間

受信情報更新通知の最小間隔時間を 5 ～ 3600 秒の範囲で指定します。

受信情報（隣接情報）が更新されたときに SNMP トラップを送信して受信情報が更新されたことを通知します。そのあと、最小間隔時間が経過するまでの間に受信情報が何度更新されても SNMP トラップを送信しないで、最小間隔時間経過後に SNMP トラップを 1 回だけ送信して受信情報が更新されたことを再通知します。

21 認証情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「認証情報」

認証情報		
IEEE802.1X認証情報	Web認証情報	MACアドレス認証情報
このページでは、認証機能についての設定ができます。		

21.1 IEEE802.1X 認証情報

[操作] 「設定メニュー」→詳細設定「認証情報」→[IEEE802.1X 認証情報]

■IEEE802.1X認証情報

?

IEEE802.1X認証	☒ 使用しない ☐ 使用する
認証方式	☒ MACアドレスごと ☐ ポートごと
EAPOL転送モード	☒ 転送しない ☐ 転送する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

IEEE802.1X 認証

IEEE802.1X 認証を装置として使用する場合は、“使用する”を選択します。

“使用する”を選択した場合、パケット送信元端末の IEEE802.1X 認証を行い、認められた端末である場合に中継を行い、認められていなければパケット破棄します。

こんな事に気をつけて

“使用する”を選択した場合でも、「ether 情報」の IEEE802.1X 認証情報で、認証機能を“使用しない”と設定されている場合は、認証は行われません。

EAPOL 転送モード

IEEE802.1X 認証で利用する EAPOL フレームの転送モードを指定します。

“転送する”を選択した場合、EAPOL フレームを受信したポートの VLAN タグなしで設定された VLAN ID と同一 VLAN ID のポートに転送します。

こんな事に気をつけて

- EAPOL フレームは IEEE802.1D で転送が禁止されているフレームです。
- IEEE802.1X 認証を使用する場合、EAPOL フレームは転送できません。“転送する”は選択しないでください。

認証方式

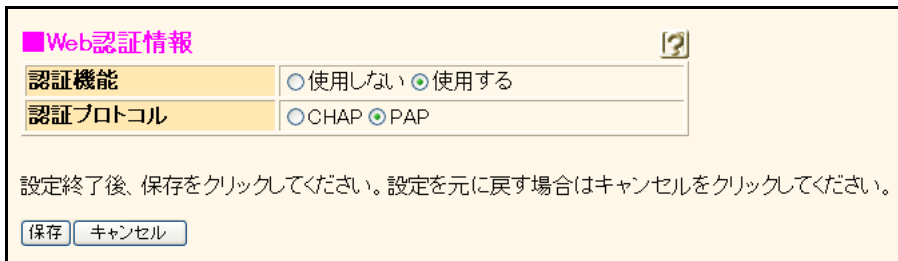
認証方式としてシステムデフォルト認証単位を指定します。

こんな事に気をつけて

認証方式としてポートごとの認証を選択し、そのポートに接続される端末（Supplicant）の 1 台が認証許可された場合は、同じポートに接続されるほかの端末からのアクセスがすべて透過として扱われます。

21.2 Web 認証情報

[操作] 「設定メニュー」→詳細設定「認証情報」→[Web 認証情報]



The image shows a web-based configuration interface for Web authentication. At the top, there is a title bar with a pink square icon and the text 'Web 認証情報' (Web Authentication Information), followed by a help icon. Below this, there are two rows of configuration options. The first row is '認証機能' (Authentication Function) with two radio buttons: '使用しない' (Do not use) and '使用する' (Use), where '使用する' is selected. The second row is '認証プロトコル' (Authentication Protocol) with two radio buttons: 'CHAP' and 'PAP', where 'PAP' is selected. Below these options, there is a text instruction: '設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。' (After setting is complete, click Save. To return to the original settings, click Cancel). At the bottom, there are two buttons: '保存' (Save) and 'キャンセル' (Cancel).

■Web 認証情報	?
認証機能	☐ 使用しない ☒ 使用する
認証プロトコル	☐ CHAP ☒ PAP

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

認証機能

Web 認証を装置として使用する場合は、“使用する”を選択します。

“使用する”を選択した場合、WWW ブラウザを使用して端末の認証を実施し、認証に成功した端末の通信のみを許可することができます。

こんな事に気をつけて

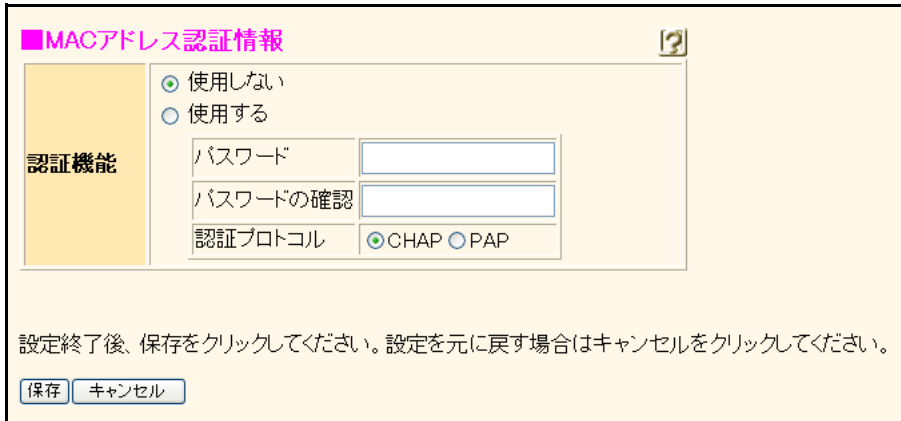
- “使用しない”を選択したポートでは、Web 認証は行いません。
- “使用する”を選択した場合でも、「ether 情報」の Web 認証情報で、認証機能を“使用しない”と設定されているポートでは、認証は行われません。

認証プロトコル

Web 認証の認証プロトコルを選択します。

21.3 MAC アドレス認証情報

[操作] 「設定メニュー」→詳細設定「認証情報」→[MAC アドレス認証情報]



■MACアドレス認証情報

認証機能

☒ 使用しない
☐ 使用する

パスワード
 パスワードの確認
 認証プロトコル ☒ CHAP ☐ PAP

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

認証機能

MAC アドレス認証を装置として使用する場合は、“使用する”を選択します。

“使用する”を選択した場合、パケット送信元端末のMAC アドレス認証を行い、認められたMAC アドレスである場合に中継を行い、認められていなければパケット破棄します。

こんな事に気をつけて

“使用する”を選択した場合でも、「ether 情報」のMAC アドレス認証情報で、認証機能を“使用しない”と設定されている場合は、認証は行われません。

パスワード

MAC アドレス認証で使用するパスワードを、0x21 および 0x23～0x7e の文字で構成される 128 文字以内の文字列で指定します。省略時は、認証端末のMAC アドレスをパスワードとして使用します。

パスワードの確認

上記で指定したパスワードをもう一度指定します。

認証プロトコル

MAC アドレス認証の認証プロトコルを選択します。

22 IGMP スヌープ情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「IGMP スヌープ情報」

IGMPスヌープ情報

基本情報

22.1 基本情報

[操作] 「設定メニュー」→詳細設定「IGMP スヌープ情報」→[基本情報]

■基本情報

IGMPスヌープ機能	☒ 使用しない ☐ 使用する
ローカルグループの転送契機	☒ マルチキャスト・パケット受信 ☐ IGMP Membership Report 受信 ☐ リスナ登録を行わない
宛先不明マルチキャストパケット	☒ フラッディングしない ☐ フラッディングする

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

IGMP スヌープ機能

IGMP スヌープ機能を使用する場合は、“使用する”を選択します。

こんな事に気をつけて

マルチキャストルーティングとの併用はできません。マルチキャストルーティングと本機能が有効となっている場合は、IGMP スヌープ機能は無効となります。

- リスナ登録を行わない
ローカルグループあてのマルチキャスト・パケットおよびIGMP Membership Reportを受信した場合にリスナ登録をしないで宛先不明マルチキャストパケットとみなします。
宛先不明マルチキャストパケット受信時の動作が“フラッディングする”の場合は、ローカルグループあてのマルチキャスト・パケットおよびIGMP Membership Reportは同一VLAN内にフラッディングされます。

ローカルグループの転送契機

IGMP スヌープのローカルグループの転送契機を指定します。

- マルチキャスト・パケット受信
ローカルグループあてのマルチキャストパケットを受信したときに転送を開始します。
- IGMP Membership Report 受信
ローカルグループに対する IGMP Membership Reportを受信したときに転送を開始します。

宛先不明マルチキャストパケット

宛先不明マルチキャストパケット受信時の動作を指定します。

- フラッディングしない
パケットを破棄します。
- フラッディングする
同一VLAN内にフラッディングします。

23 ループ検出情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「ループ検出情報」

ループ検出情報

基本情報

23.1 基本情報

[操作] 「設定メニュー」→詳細設定「ループ検出情報」→[基本情報]

■基本情報

ループ検出機能

☒ 使用しない
☐ 使用する

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 10 秒

復旧監視回数 60

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

ループ検出機能

ループ検出機能を有効にする場合は、“使用する”を選択します。

ループ検出時の動作

ループ検出時の該当ポートの動作を選択します。

- 何もしない
システムログを表示します。
- 遮断する
該当ポートのフレーム送受信を遮断します。
ポートを遮断した状態でループ監視を継続し、復旧監視回数まで連続してループが検出されなかった場合、またはポートがリンクダウンした場合、遮断状態を解除します。

こんな事に気をつけて

- STP 機能が有効なポートでは、ポート遮断は動作しません。
- 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。

こんな事に気をつけて

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。

ループ検出用フレームの送信間隔

ループ検出用フレームの送信間隔を 1～32767 秒の範囲で指定します。単位は、h (時)、m (分)、s (秒) のどれかを設定します。省略時は、10 秒が設定されます。

復旧監視回数

ループ検出後、状態復旧と判定するための監視回数を 1～65535 の範囲で設定します。省略時は、60 回が設定されます。

- 閉塞する
該当ポートを閉塞します。

24 AAA 情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「AAA 情報」

AAA 情報
グループID情報

24.1 グループID 情報

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報]

■グループID情報
※追加情報は一覧の最後尾の追加フィールドで設定してください。

グループID	グループ名	操作
[全削除]		
<グループID情報追加フィールド>		
グループ名		[追加] [キャンセル]

保存した情報は、設定反映後に有効になります。

現在、設定されているグループID 情報が表示されています。グループID 情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

本装置では、通信アクセスを許可するユーザIDの認証情報と各種付加情報を通して、依頼された接続情報の検索を行い、返答として要求された接続情報が通知されます。

グループ名

グループ名を 0x21、0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報]→[追加]

AAA情報 - グループID情報(0)

共通情報	AAAユーザ情報	RADIUS関連
このページではグループID情報を設定することができます。 上記の各項目をクリックしてください。詳細な設定項目が表示されます。		

24.1.1 共通情報

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報]→[追加]→[共通情報]

AAA情報 - グループID情報(0)		
共通情報	AAAユーザ情報	RADIUS関連
基本情報		

24.1.1.1 基本情報

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報]→[追加]→[共通情報]
→[基本情報]

■基本情報

?

グループ名	
ゲストVLAN	☒ 接続を許可しない ☐ 接続を許可する 割り当てるVLAN ID

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

グループ名

グループ名を 0x21、0x23～0x7e を使用して 32 文字以内で指定します。

ゲストVLAN

“接続を許可する”を指定した場合は、Supplicant（ユーザ端末）の認証が失敗したときに、ゲストユーザとして接続を許可します。“割り当てるVLAN ID”で指定した値がゲスト用のVLANとして割り当てられます。“割り当てるVLAN ID”を省略時は、デフォルトVLAN（VID=1）が割り当てられます。“接続を許可しない”を指定した場合は、ゲストユーザの接続は許可されません。

24.1.2 AAA ユーザ情報

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報]→[追加]→[AAA ユーザ情報]

AAA情報 - グループID情報(0)		
共通情報	AAAユーザ情報	RADIUS関連
AAAユーザ情報		

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報]→[追加]→[AAA ユーザ情報]
→[AAA ユーザ情報]

■AAAユーザ情報

※追加情報は一覧の最後尾の追加フィールドで設定してください。

定義番号

ユーザID

操作

全削除

<AAAユーザ情報追加フィールド>

ユーザID

追加

キャンセル

保存した情報は、設定反映後に有効になります。

現在、設定されている AAA ユーザ情報が表示されています。AAA ユーザ情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

ユーザID

ユーザID を 0x21、0x23～0x7e を使用して 128 文字以内で指定します。

MAC アドレス認証で利用する場合は、アクセスを許可する端末の MAC アドレスを 16 進数 12 桁（コロンで区切らない）で指定してください。

省略時は、認証情報を使用できません。

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報]→[追加]→[AAA ユーザ情報]
→[AAA ユーザ情報]→[追加]

AAA情報 - グループID情報(0) - AAAユーザ情報(0)		
認証情報	IP関連	サブリカント関連
このページではAAAユーザ情報を設定することができます。 上記の各項目をクリックしてください。詳細な設定項目が表示されます。		

24.1.2.1 認証情報

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報]→[追加]→[AAA ユーザ情報]
→[AAA ユーザ情報]→[追加]→[認証情報]

AAA情報 - グループID情報(0) - AAAユーザ情報(0)		
認証情報	IP関連	サブリカント関連
認証情報		

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報]→[追加]→[AAA ユーザ情報]
→[AAA ユーザ情報]→[追加]→[認証情報]→[認証情報]

■ 認証情報

ユーザID

認証パスワード

権限クラス

☒ 指定しない
 ☐ 管理者クラス
 ☐ 一般ユーザクラス

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

ユーザID

ユーザIDを0x21、0x23～0x7eを使用して128文字以内の文字列で指定します。

MACアドレス認証で利用する場合は、アクセスを許可する端末のMACアドレスを16進数12桁（コロンで区切らない）で指定してください。

省略時は、認証情報を使用できません。

認証パスワード

認証パスワードを0x21、0x23～0x7eを使用して128文字以内で指定します。

MACアドレス認証で利用する場合は、アクセスを許可する端末のMACアドレスを16進数12桁（コロンで区切らない）で指定してください。

省略時は、認証情報のパスワードは使用できません。表示画面では暗号化された認証パスワードが表示されます。

権限クラス

ログインユーザを設定する場合の権限クラスを選択します。

- 指定しない
権限クラスを指定しません。
- 管理者クラス
権限クラスを管理者クラスとします。
- 一般ユーザクラス
権限クラスを一般ユーザクラスとします。

24.1.2.2 IP 関連

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報]→[追加]→[AAA ユーザ情報]
→[AAA ユーザ情報]→[追加]→[IP 関連]

AAA情報	グループID情報(0)	AAAユーザ情報(0)
認証情報	IP関連	サブリカント関連
IP基本情報		

24.1.2.2.1 IP 基本情報

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報]→[追加]→[AAA ユーザ情報]
→[AAA ユーザ情報]→[追加]→[IP 関連]→[IP 基本情報]

■IP基本情報

?

相手側IPアドレス

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

相手側 IP アドレス

相手側 IP アドレスを指定します。設定を省略または 0.0.0.0 を指定した場合、IP アドレスなし (unnumbered) として動作します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

24.1.2.3 サプリカント関連

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報]→[追加]→[AAA ユーザ情報]
→[AAA ユーザ情報]→[追加]→[サプリカント関連]

AAA情報 - グループID情報(0) - AAAユーザ情報(0)		
認証情報	IP関連	サプリカント関連
サプリカント情報		

24.1.2.3.1 サプリカント情報

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報]→[追加]→[AAA ユーザ情報]
→[AAA ユーザ情報]→[追加]→[サプリカント関連]→[サプリカント情報]

■サプリカント情報

割り当てるVLAN ID

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
☐ MACアドレスをチェックする

MACアドレス

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

割り当てるVLAN ID

サプリカント（ユーザ端末）に割り当てるVLAN IDを1～4094の範囲で指定します。省略時は、認証元の設定に従います。

サプリカントMACアドレスによる識別

サプリカント（ユーザ端末）のMACアドレスをチェックするかどうかを選択します。

MACアドレスをチェックする場合は、MACアドレスにサプリカントのMACアドレスをxx:xx:xx:xx:xx:xx（xxは2桁の16進数）の形式で指定します。MACアドレスが一致しない場合は認証が成功しません。

複数のユーザ情報を用いて、同じユーザ名で異なるMACアドレスを登録することで、複数のMACアドレスを登録することができます。

MACアドレスをチェックしない場合は、サプリカントのMACアドレスを用いずパスワード情報だけを用いて認証を行います。この設定は、IEEE802.1X認証またはWeb認証を行う場合にだけ有効です。

24.1.3 RADIUS 関連

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループ ID 情報]→[追加]→[RADIUS 関連]
「RADIUS 関連」-「基本情報」の RADIUS サービスで、“使用しない”を選択した場合

AAA情報 - グループID情報(0)		
共通情報	AAAユーザ情報	RADIUS関連
基本情報		

「RADIUS 関連」-「基本情報」の RADIUS サービスで、“クライアント機能”を選択した場合

AAA情報 - グループID情報(0)		
共通情報	AAAユーザ情報	RADIUS関連
基本情報	サーバ情報	送信情報

24.1.3.1 基本情報

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループ ID 情報]→[追加]→[RADIUS 関連]
→[基本情報]

■基本情報

RADIUSサービス

使用しない

☐ 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

自側アカウンティングIPアドレス

Message Authenticator

☐ 使用する ☒ 使用しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

RADIUS サービス

本装置で使用する RADIUS 機能を以下から選択します。
選択する RADIUS サービスによって、「RADIUS 情報」の表示が異なります。

- 使用しない
RADIUS 機能を使用しません。
- クライアント機能
本装置を RADIUS クライアントとして使用します。

“クライアント機能”を選択した場合は、以下から使用するサービスを指定します。

- 認証
RADIUS 認証機能を使用します。
- アカウンティング
RADIUS アカウンティング機能を使用します。

自側認証 IP アドレス

自側 RADIUS 認証装置の IP アドレスを指定します。

有効範囲)
1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254
::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

本装置を RADIUS 認証クライアントとして使用する場合は、RADIUS 認証サーバと通信するときに使用する IP アドレスを設定します。省略時は、相手側の RADIUS 認証装置と通信する自側 IP アドレスを自動的に選択するものとみなされます。

自側アカウンティングIP アドレス

自側 RADIUS アカウンティング装置の IP アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

本装置を RADIUS アカウンティングクライアントとして使用する場合は、RADIUS アカウンティングサーバと通信するときに使用する IP アドレスを設定します。省略時は、相手側の RADIUS アカウンティング装置と通信する自側 IP アドレスを自動的に選択するものとみなされます。

Message-Authenticator

Message-Authenticator による認証を行う場合は、“使用する”を選択します。本装置では、認証要求メッセージにのみ使用します。

24.1.3.2 サーバ情報（クライアント機能）

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループ ID 情報]→[追加]→[RADIUS 関連]→[サーバ情報（クライアント機能）]

■サーバ情報(クライアント機能)				
	サーバIPアドレス	復旧待機時間	優先度	操作
認証情報 1	-	0秒	0	修正 削除
認証情報 2	-	0秒	0	修正 削除
認証情報 3	-	0秒	0	修正 削除
認証情報 4	-	0秒	0	修正 削除
アカウンティング情報 1	-	0秒	0	修正 削除
アカウンティング情報 2	-	0秒	0	修正 削除
アカウンティング情報 3	-	0秒	0	修正 削除
アカウンティング情報 4	-	0秒	0	修正 削除
全削除				

保存した情報は、設定反映後に有効になります。

「RADIUS 関連」-「基本情報」の RADIUS サービスで、“クライアント機能”を選択した場合に表示されます。

現在、設定されているサーバ情報（クライアント機能）が表示されています。処理するボタンをクリックし、次のページへ進みます。

認証情報

認証情報 1	共有鍵	
	サーバIPアドレス	
	サーバUDPポート	☒ 1812 ☐ 1645
	復旧待機時間	0 秒 v
	優先度	0
	自側認証IPアドレス	
	保存 キャンセル 一覧へ戻る	

共有鍵

本装置と RADIUS 認証サーバとの間で共有する共有鍵（RADIUS シークレット）を 64 文字以内の文字列で指定します。

省略時は、共有鍵（RADIUS シークレット）を設定しないものとみなされます。

サーバIPアドレス

本装置と通信する RADIUS 認証サーバの IP アドレスを設定します。

有効範囲)

1.0.0.1 ～ 126.255.255.254

128.0.0.1 ～ 191.255.255.254

192.0.0.1 ～ 223.255.255.254

::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

サーバUDPポート

RADIUS 認証クライアントが認証要求する RADIUS 認証サーバの UDP ポート番号を設定します。

- 1812
認証要求する RADIUS 認証サーバが最新の RFC 仕様の UDP ポートで取り付けられている場合
- 1645
認証要求する RADIUS 認証サーバが旧 RFC 仕様の UDP ポートで取り付けられている場合

復旧待機時間

RADIUS サーバが dead 状態になってから、自動的に再び alive 状態に復旧するまでの時間を指定します。単位は、日、時間、分、秒のどれかを指定します。

有効範囲)

0 ～ 86400 秒

0 ～ 1440 分

0 ～ 24 時間

0 ～ 1 日

0 秒を指定した場合は、自動的に alive 状態に復旧しません。省略時は、自動的に復旧しません。

RADIUS サーバから送信間隔と再送間隔で設定した応答待ち受け時間を経過しても応答が得られなかった場合、その RADIUS サーバは dead 状態となり、優先度は最非優先となります。dead 状態となった RADIUS サーバは、alive 状態のサーバが存在する限り使わなくなります。本設定は、dead 状態になってから、設定した優先度となる alive 状態へ自動的に復旧するための待ち時間を設定します。

dead 状態から alive 状態に復旧するためには、以下の条件を満たす必要があります。

- 本設定の時間が経過した場合
- 利用可能なすべてのサーバが dead 状態となったあと、dead 状態の RADIUS サーバにパケットを送信し、応答が得られた場合
- 運用コマンドで、手動で復旧させた場合

優先度

同一グループ内でのRADIUSサーバを使用する優先度を指定します。0を最優先、255を最非優先とし、数字が小さい程、高い優先度となります。

有効範囲)

0～255

255を指定した場合は、そのRADIUSサーバは常にdead状態となります。省略時は、0が設定されます。

同一グループ内の複数のRADIUSサーバから、認証の際に使用するRADIUSサーバを決める際に使用する優先度を指定します。同一グループの中で、dead状態になっていない、もっとも高い優先度のRADIUSサーバが使われます。もっとも高い優先度のRADIUSサーバが複数存在する場合は、使用するRADIUSサーバはランダムに決定されます。

自側認証IPアドレス

自側RADIUS認証装置でこのクライアントに対して使用するIPアドレスを設定します。本定義の内容は、RADIUS関連「基本情報」の自側認証IPアドレスの設定より優先されます。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0::～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

このクライアントでRADIUS認証サーバとの通信に使用するIPアドレスを設定してください。省略時は、RADIUS関連「基本情報」の自側認証IPアドレスの設定に従います。

アカウント情報

アカウント情報 1	共有鍵	
	サーバIPアドレス	
	サーバUDPポート	☒ 1813 ☐ 1646
	復旧待機時間	0 秒 v
	優先度	0
	自側アカウントing IPアドレス	
	保存 キャンセル 一覧へ戻る	

共有鍵

本装置とRADIUSアカウントingサーバとの間で共有する共有鍵（RADIUSシークレット）を64文字以内の文字列で指定します。

省略時は、共有鍵（RADIUSシークレット）を設定しないものとみなされます。

サーバIPアドレス

本装置と通信するRADIUSアカウントingサーバのIPアドレスを設定します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0::～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

サーバUDPポート

RADIUSアカウントingクライアントがアカウントing要求するRADIUSアカウントingサーバのUDPポート番号を設定します。

- 1813
アカウントing要求するRADIUSアカウントingサーバが最新のRFC仕様のUDPポートで取り付けられている場合
- 1646
アカウントing要求するRADIUSアカウントingサーバが旧RFC仕様のUDPポートで取り付けられている場合

復旧待機時間

RADIUS サーバが dead 状態になってから、自動的に再び alive 状態に復旧するまでの時間を指定します。単位は、日、時間、分、秒のどれかを指定します。

有効範囲)

0～86400 秒

0～1440 分

0～24 時間

0～1 日

0 秒を指定した場合は、自動的に alive 状態に復旧しません。省略時は、自動的に復旧しません。

RADIUS サーバから送信間隔と再送間隔で設定した応答待ち受け時間を経過しても応答が得られなかった場合、その RADIUS サーバは dead 状態となり、優先度は最非優先となります。dead 状態となった RADIUS サーバは、alive 状態のサーバが存在する限り使われなくなります。本設定は、dead 状態になってから、設定した優先度となる alive 状態へ自動的に復旧するための待ち時間を設定します。

dead 状態から alive 状態に復旧するためには、以下の条件を満たす必要があります。

- 本設定の時間が経過した場合
- 利用可能なすべてのサーバが dead 状態となったあと、dead 状態の RADIUS サーバにパケットを送信し、応答が得られた場合
- 運用コマンドで、手動で復旧させた場合

優先度

同一グループ内での RADIUS サーバを使用する優先度を指定します。0 を最優先、255 を最非優先とし、数字が小さい程、高い優先度となります。

有効範囲)

0～255

255 を指定した場合はその RADIUS サーバは常に dead 状態となります。省略時は、0 が設定されます。

同一グループ内の複数の RADIUS サーバから、アカウントिंगの際に使用する RADIUS サーバを決める際に使用する優先度を指定します。同一グループの中で、dead 状態になっていない、もっとも高い優先度の RADIUS サーバが使われます。もっとも高い優先度の RADIUS サーバが複数存在する場合は、使用する RADIUS サーバはランダムに決定されます。

自側アカウンティング IP アドレス

自側 RADIUS アカウンティング装置でこのクライアントに対して使用する IP アドレスを設定します。本定義の内容は、RADIUS 関連「基本情報」の自側アカウンティング IP アドレスの設定より優先されます。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0::～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

このクライアントで RADIUS アカウンティングサーバとの通信に使用する IP アドレスを設定してください。省略時は、RADIUS 関連「基本情報」の自側アカウンティング IP アドレスの設定に従います。

24.1.3.3 送信情報（クライアント機能）

[操作] 「設定メニュー」→詳細設定「AAA 情報」→[グループID 情報] → [追加] → [RADIUS 関連]
→ [送信情報（クライアント機能）]

■送信情報(クライアント機能)

送信間隔

5 秒

再送回数

2 回

NAS識別子

認証セキュリティ

☒高い ☐通常

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

送信間隔

RADIUS サーバ未応答時のパケットの送信間隔を 1 ～ 10 秒の範囲の 10 進数で指定します。

再送回数

RADIUS サーバ未応答時のパケットの再送回数を 1 ～ 10 回の範囲の 10 進数で指定します。

サーバからの応答待ち受け時間は、送信間隔 ×（再送回数 + 1）秒となります。省略時は、送信間隔を 5 秒、再送回数を 2 回として動作します。この場合は、サーバからの応答待ち受け時間パケットの初回送信後、15 秒となります。

NAS 識別子

RADIUS 認証クライアントおよびアカウントティングクライアントが RADIUS サーバに送出する NAS-Identifier アトリビュートの値を 64 文字以内で指定します。省略時は、NAS-Identifier アトリビュートを送信しません。

認証セキュリティ

RADIUS サーバ無応答時のセキュリティ動作を選択します。

- 高い
認証に失敗したものとして動作します。
- 通常
認証に成功したものとして動作します。

25 ACL 情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「ACL 情報」

現在、設定されている ACL 定義が表示されています。ACL の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

定義名

ACL 定義を識別する定義名を 50 文字以内で指定します。

[操作] 「設定メニュー」→詳細設定「ACL 情報」→[選択削除]

削除対象

削除する定義を選択して、[削除] ボタンをクリックします。削除後、ACL 情報が再表示されます。

25.1 ACL 定義情報

[操作] 「設定メニュー」→詳細設定「ACL 情報」→[追加] / [修正]

ACL情報
ACL定義情報(acl0)

☒ 基本定義情報
☐ IP定義情報
☐ TCP定義情報

☐ UDP定義情報
☐ ICMP定義情報
☐ IPv6定義情報

☐ VLAN定義情報
☐ MAC定義情報

 先頭の[]は定義の有無を表します。定義が存在する場合[✓]が表示されます。

このページではACL情報を設定することができます。
上記の各項目をクリックしてください。詳細な設定項目が表示されます。

25.1.1 基本定義情報

[操作] 「設定メニュー」→詳細設定「ACL 情報」→[追加] / [修正] → [基本定義情報]

■基本定義情報


定義名

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

定義名

ACL 定義を識別する定義名を 50 文字以内で指定します。

25.1.2 IP 定義情報

[操作] 「設定メニュー」→詳細設定「ACL 情報」→「追加」／「修正」→「IP 定義情報」

■IP定義情報		?
プロトコル	すべて 番指定: "その他"を選択時のみ有効です	
送信元情報	IPアドレス	
	アドレスマスク	0 (0.0.0.0)
宛先情報	IPアドレス	
	アドレスマスク	0 (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	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

プロトコル

IP 定義としてプロトコルを以下の 6 つから選択します。() 内はプロトコル番号です。

- すべて
- TCP (6)
- UDP (17)
- ICMP (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、1～255の範囲の10進数で指定します。

送信元／あて先情報

IP 定義としてのアドレス情報を設定します。

IPアドレス／アドレスマスク

IP 定義としての IP アドレスおよびアドレスマスクを指定します。

チェック対象となるバケットのIPアドレスと定義するアドレスマスクの論理積、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。省略または0.0.0.0/0を指定した場合、すべてのIPアドレス／アドレスマスクを対象とします。

QoS

対象とする QoS を判断する方法を以下の 3 つから選択します。

- 指定なし
すべてのTOS値、および、すべてのDSCP値を対象とする場合に選択します。
- TOS
TOS値で対象を判断する場合に選択します。
有効範囲) 0～ffの16進数
- DSCP
DSCP値で対象を判断する場合に選択します。
有効範囲) 0～63の10進数

25.1.3 TCP 定義情報

[操作] 「設定メニュー」→詳細設定「ACL 情報」→[追加] / [修正] →[TCP 定義情報]

■TCP定義情報

送信元ポート番号

あて先ポート番号

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

削除

送信元／あて先ポート番号

TCP 定義としてポート番号を 1～65535 の範囲の 10 進数で指定します。省略時は、すべてのポート番号が TCP 定義の対象となります。また、ポート番号を複数指定する場合は“,”で区切ります。送信元情報とあて先情報で合わせて 10 組まで指定できます。

25.1.4 UDP 定義情報

[操作] 「設定メニュー」→詳細設定「ACL 情報」→[追加] / [修正] →[UDP 定義情報]

■UDP定義情報

送信元ポート番号

あて先ポート番号

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

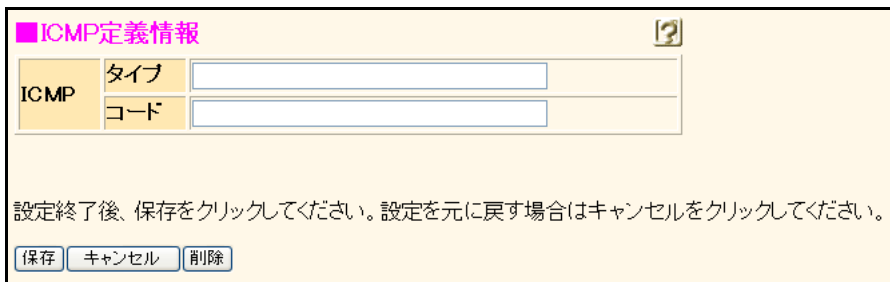
削除

送信元／あて先ポート番号

UDP 定義としてポート番号を 1～65535 の範囲の 10 進数で指定します。省略時は、すべてのポート番号が UDP 定義の対象となります。また、ポート番号を複数指定する場合は“,”で区切ります。送信元情報とあて先情報で合わせて 10 組まで指定できます。

25.1.5 ICMP 定義情報

[操作] 「設定メニュー」→詳細設定「ACL 情報」→ [追加] / [修正] → [ICMP 定義情報]



ICMP

タイプ

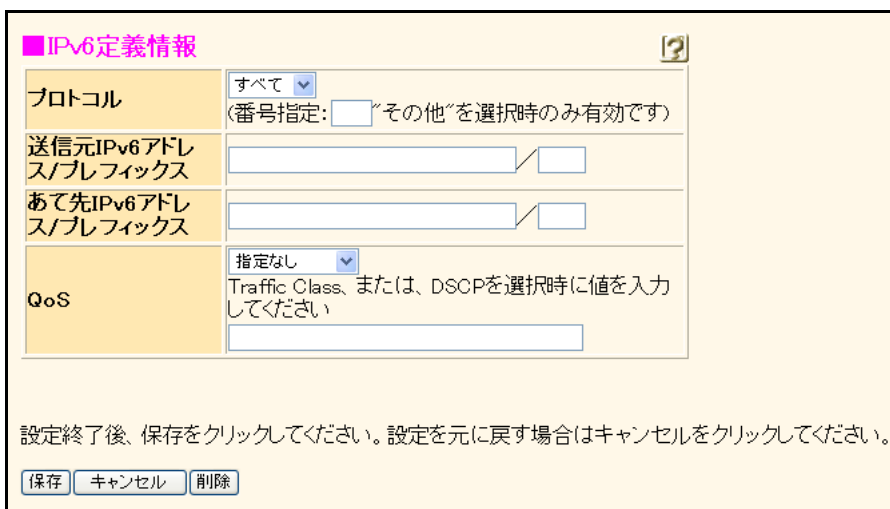
ICMP 定義として ICMP パケットのタイプ値を 0～255 の範囲の 10 進数で指定します。省略時は、すべての ICMP タイプ値を対象とします。また、ICMP タイプ値を複数指定する場合は “,” で区切ります。10 組まで指定できます。

コード

ICMP 定義として ICMP パケットのコード値を 0～255 の範囲で指定します。省略時は、すべての ICMP コード値を対象とします。また、ICMP コード値を複数指定する場合は “,” で区切ります。10 組まで指定できます。

25.1.6 IPv6 定義情報

[操作] 「設定メニュー」→詳細設定「ACL 情報」→ [追加] / [修正] → [IPv6 定義情報]



プロトコル

対象とするプロトコルを以下の 5 つから選択します。() 内はプロトコル番号です。

- すべて
- TCP (6)
- UDP (17)
- ICMPv6 (58)
- その他

任意のプロトコル番号を指定する場合は、“その他” を選択し、1～255 の範囲の 10 進数で指定します。

送信元／あて先 IPv6 アドレス

対象とする IPv6 アドレスおよびプレフィックス長を指定します。::/0 を指定した場合、または、省略時は、すべての IPv6 アドレス／プレフィックス長を対象とします。以下が等しい場合に条件に一致します。

- パケットの IPv6 アドレスと定義するプレフィックス長の論理積
- 定義する IPv6 アドレスとプレフィックス長の論理積

QoS

対象とする QoS を判断する方法を以下の3つから選択します。

- 指定なし
すべての Traffic Class 値、および、すべての DSCP 値を対象とする場合に選択します。
- Traffic Class
Traffic Class 値で対象を判断する場合に選択します。
有効範囲)
0～ff の 16 進数
- DSCP
DSCP 値で対象を判断する場合に選択します。
有効範囲)
0～63 の 10 進数

25.1.7 VLAN 定義情報

[操作] 「設定メニュー」→詳細設定「ACL 情報」→[追加] ／ [修正] → [VLAN 定義情報]

VLAN 定義情報

?

VLAN ID	
COS 値	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

VLAN ID

対象とする VLAN ID を 1～4094 の範囲の 10 進数で指定します。省略時は、すべての VLAN ID を対象とします。

COS 値

対象とする COS 値を 0～7 の範囲の 10 進数で指定します。省略時は、すべての COS 値を対象とします。

25.1.8 MAC 定義情報

[操作] 「設定メニュー」→詳細設定「ACL 情報」→[追加] / [修正] → [MAC 定義情報]

■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

☐ Ethernet形式

LSAP

type値

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル 削除

送信元／あて先 MAC アドレス

対象とする MAC アドレスを以下の項目から選択します。
 “指定する”を選択する場合は、アドレス指定に MAC アドレスを 16 進数で指定します。

- すべて
すべての MAC アドレスを対象とします。
- ブロードキャスト
ブロードキャスト MAC アドレスを対象とします。
- マルチキャスト
ブロードキャスト MAC アドレスおよびマルチキャスト MAC アドレスを対象とします。
- 指定する
アドレス指定に指定する MAC アドレスを対象とします。MAC アドレスは、「xx:xx:xx:xx:xx:xx」(xx は 2 桁の 16 進数) の形式で指定します。

フォーマット種別

対象とするフォーマットを以下の項目から選択します。
 LSAP または type 値が未入力の場合は、すべての値が対象となります。

- すべて
すべてのパケットを対象とします。
- LLC 形式
LLC 形式のパケットを対象とします。
LSAP を 0 ～ ffff の範囲の 16 進数で指定します。
- Ethernet 形式
Ethernet 形式のパケットを対象とします。
type 値を 5dd ～ ffff の範囲の 16 進数で指定します。

26 SNMP 情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「SNMP 情報」

SNMP 情報		
基本情報	SNMPv1/v2c 情報	SNMPv3 情報
トラップ情報		

26.1 基本情報

[操作] 「設定メニュー」→詳細設定「SNMP 情報」→[基本情報]

■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

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

機器設置場所

エージェントアドレス

エンジンID

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

SNMP エージェント機能

SNMP エージェント機能を使用すると、SNMP ホストの動作しているほかのシステムから本装置の状態を監視できます。SNMP エージェント機能を使用する場合は“使用する”を選択し、以下の項目を設定します。

こんな事に気をつけて

“使用する”から“使用しない”に設定を変更した場合は、定義されているすべての SNMP 情報が削除されます。

機器管理者

本装置の管理者名を 40 文字以内で指定します。省略時は、機器管理者名を設定しないものとみなされます。

機器名称

機器名称として装置名称を使用する場合は、“装置名称を使用する”を選択します。“指定する”を選択した場合は、本装置の名称を 32 文字以内で指定します。省略時は、機器名称を設定しないものとみなされます。

機器設置場所

本装置の設置場所を 72 文字以内で指定します。省略時は、機器設置場所を設定しないものとみなされます。

エージェントアドレス

SNMP エージェントの IP アドレスを指定します。省略時は、エージェントアドレスを設定しないものとみなされます。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

エンジン ID

SNMPv3 の SNMP エンジン ID を 27 文字以内で指定します。省略時は、エンジン ID を自動生成します。

装置に設定される SNMP エンジン ID の値は、以下のとおりです。

- 設定した場合
 - 第 1 ~ 5 オクテット：0x800000d304 固定
 - 第 6 オクテット以降：本設定のエンジン ID
- 省略した場合
 - 第 1 ~ 5 オクテット：0x800000d380 固定
 - 第 6 オクテット以降：ランダム値

26.2 SNMPv1/v2c 情報

[操作] 「設定メニュー」→詳細設定「SNMP 情報」→[SNMPv1/v2c 情報]

■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 IPアドレス トラップ ☒ 送信しない ☐ V1 ☐ V2 書き込み要求 ☒ 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 IPアドレス トラップ ☒ 送信しない ☐ V1 ☐ V2 書き込み要求 ☒ 許可しない ☐ 許可する
SNMPホスト3	☒ 指定しない ☐ 指定する コミュニティ名 IPアドレス トラップ ☒ 送信しない ☐ V1 ☐ V2 書き込み要求 ☒ 許可しない ☐ 許可する
SNMPホスト4	☒ 指定しない ☐ 指定する コミュニティ名 IPアドレス トラップ ☒ 送信しない ☐ V1 ☐ V2 書き込み要求 ☒ 許可しない ☐ 許可する
SNMPホスト5	☒ 指定しない ☐ 指定する コミュニティ名 IPアドレス トラップ ☒ 送信しない ☐ V1 ☐ V2 書き込み要求 ☒ 許可しない ☐ 許可する
SNMPホスト6	☒ 指定しない ☐ 指定する コミュニティ名 IPアドレス トラップ ☒ 送信しない ☐ V1 ☐ V2 書き込み要求 ☒ 許可しない ☐ 許可する
SNMPホスト7	☒ 指定しない ☐ 指定する コミュニティ名 IPアドレス トラップ ☒ 送信しない ☐ V1 ☐ V2 書き込み要求 ☒ 許可しない ☐ 許可する

SNMPホスト8	☒ 指定しない
	☐ 指定する
	コミュニティ名
	IPアドレス
	トラップ ☒ 送信しない ☐ V1 ☐ V2
書き込み要求 ☒ 許可しない ☐ 許可する	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

SNMP ホスト

SNMPによるアクセスを許可するホストを設定します。ホストは8個まで定義できます。“publicとする”を選択すると、コミュニティ名“public”で任意のホストからのアクセスを許可します。コミュニティ名を変える場合やホストを限定する場合は、“指定する”を選択し、コミュニティ名・IPアドレス・トラップ・書き込み要求を指定します。

コミュニティ名

SNMPにより情報交換するグループのコミュニティ名を32文字以内で指定します。

IPアドレス

SNMPによるアクセスを許可するホストのIPアドレスを指定します。“0.0.0.0”を指定すると、任意のホストからのアクセスを許可します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

トラップ

このSNMPホストに対してSNMPv1トラップを送信する場合は、“V1”を、SNMP v2トラップを送信する場合は、“V2”を選択します。

ただし、任意のホスト（0.0.0.0）を指定している場合は、トラップの送信は行われません。

書き込み要求

このSNMPホストから書き込み要求を許可する場合は、“許可する”を選択します。

ただし、任意のホスト（0.0.0.0）を指定している場合は、書き込み要求は許可されません。

26.3 SNMPv3 情報

[操作] 「設定メニュー」→詳細設定「SNMP 情報」→[SNMPv3 情報]

SNMP情報

SNMPv3情報

[ユーザ情報](#)
[MIBビュー情報](#)

26.3.1 ユーザ情報

[操作] 「設定メニュー」→詳細設定「SNMP 情報」→[SNMPv3 情報]→[ユーザ情報]

■ユーザ情報 ?

定義 番号	ユー ザ名	SNMPホストア ドレス	トラップ通知ホ ストアドレス	セキュリティ プロトコル	MIBビュー MIB書き込み MIB読み出し トラップ通知	操作
1						修正 削除
2						修正 削除
3						修正 削除
4						修正 削除
5						修正 削除
6						修正 削除
7						修正 削除
8						修正 削除

[全削除](#)

保存した情報は、設定反映後に有効になります。設定を元に戻す場合はキャンセルをクリックしてください。

現在、設定されている SNMPv3 情報が表示されています。SNMPv3 情報は、装置全体で 8 個まで設定することができます。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」→「詳細設定」[SNMP情報]→「SNMPv3情報」→「ユーザ情報」→「修正」

ユーザ名		
ホストアドレス	SNMPホスト	トラップ通知ホスト
セキュリティプロトコル	認証プロトコル	認証なし ▼
	認証パスワード	
	暗号プロトコル	暗号なし ▼
	暗号パスワード	
MIBビュー	MIB書き込み	☒ 許可しない ☐ 許可する
	MIB読み出し	☒ 許可する ☐ 許可しない ☐ MIBビュー情報を使用 ビュー定義番号 MIBビュー情報参照
	トラップ通知	☒ 許可する ☐ 許可しない ☐ MIBビュー情報を使用 ビュー定義番号 MIBビュー情報参照
	保存 キャンセル 一覧へ戻る	

ユーザ名

SNMPv3のSNMP ユーザ名を32文字以内で指定します。
SNMPv3機能を使用する場合は、必ず設定してください。

ホストアドレス

SNMPv3によるアクセスを許可するホストのIPアドレスとトラップを通知するホストのIPアドレスを指定します。アクセスを許可するホストのIPアドレスとトラップを通知するホストのIPアドレスは、装置全体で合わせて8個まで定義できます。省略時は、ホストアドレスを設定しないものとみなされます。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

セキュリティプロトコル

認証プロトコル

SNMPv3による認証プロトコルを選択します。“認証なし”を選択した場合、認証プロトコルは使用されません。

認証パスワード

SNMPv3による認証プロトコルで使用する、認証パスワードを以下の範用の文字列で指定します。

認証プロトコル	パスワード長
MD5	8～16文字
SHA	8～20文字

認証プロトコルに“認証なし”を選択した場合は、省略
できます。

暗号プロトコル

SNMPv3 による暗号プロトコルを選択します。

“暗号なし” を選択した場合、暗号プロトコルは使用されません。また、暗号プロトコルを指定した場合は、認証プロトコルを指定してください。

暗号パスワード

SNMPv3 による暗号プロトコルで使用する、暗号パスワードを以下の範囲の文字列で指定します。

暗号プロトコル	パスワード長
DES	8～16文字

暗号プロトコルに“暗号なし”を選択した場合は、省略できます。

MIB ビュー

MIB 書き込み

SNMPv3 による MIB 書き込みのアクセス権を許可する場合は、“許可する”を選択します。

MIB 読み出し

SNMPv3 による MIB 読み出しのアクセス権を許可する場合は、“許可する”を選択します。

“MIB ビュー情報を参照”を選択した場合は、必ずビュー定義番号を指定してください。

トラップ通知

SNMPv3 によるトラップ通知のアクセス権を許可する場合は、“許可する”を選択します。

“MIB ビュー情報を参照”を選択した場合は、必ずビュー定義番号を指定してください。

ビュー定義番号

[MIB ビュー情報参照] をクリックして、ビュー定義番号を指定します。

指定する定義番号欄の [選択] ボタンをクリックし、ビュー定義番号を設定します。自動的に画面が閉じます。

なお、参照するビュー定義が存在しない場合は、「参照可能な MIB ビュー情報が存在しません」が表示されます。

[OK] ボタンをクリックして、設定をやり直してください。

[操作] 「設定メニュー」→詳細設定「SNMP 情報」→[SNMPv3 情報]→[ユーザ情報]→[修正]
→「ビュー定義番号の [MIB ビュー情報参照]」

定義番号	サブツリー名	ビュータイプ	操作
0	system	含む	選択

「MIB ビュー情報」 - [追加] / [修正] で設定した MIB ビュー定義情報が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

参照するビュー定義が存在しない場合は、「参照可能な MIB ビュー情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「ユーザ情報」の MIB ビュー定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「ユーザ情報」にビュー定義番号が設定され、画面が閉じます。

26.3.2 MIB ビュー情報

[操作] 「設定メニュー」→詳細設定「SNMP 情報」→[SNMPv3 情報]→[MIB ビュー情報]

現在、設定されている MIB ビュー情報の定義が表示されています。MIB ビュー情報は、装置全体で 8 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」→詳細設定「SNMP 情報」→[SNMPv3 情報]→[MIB ビュー情報]→[追加]

サブツリー名

MIB ビュー対象とするサブツリー名を選択します。

同じビュー定義番号を持つ MIB ビュー情報の設定で、同一サブツリー名を複数選択した場合、最初を選択したサブツリー情報が有効となります。

ビュータイプ

選択したサブツリー名を MIB ビューに含むか、それとも除くかを指定します。

26.4 トラップ情報

[操作] 「設定メニュー」→詳細設定「SNMP 情報」→ [トラップ情報]

■トラップ情報

coldStart	☒ 有効にする ☐ 無効にする
linkDown	☒ 有効にする ☐ 無効にする
linkUp	☒ 有効にする ☐ 無効にする
authenticationFailure	☒ 有効にする ☐ 無効にする
newRoot	☒ 有効にする ☐ 無効にする
topologyChange	☒ 有効にする ☐ 無効にする
vrrpTrapNewMaster	☒ 有効にする ☐ 無効にする
vrrpTrapAuthFailure	☒ 有効にする ☐ 無効にする
vrrpTrapProtoError	☒ 有効にする ☐ 無効にする
nosError	☒ 有効にする ☐ 無効にする
lldpRemTablesChange	☒ 有効にする ☐ 無効にする

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

SR-S724TC1、748TC1 以外では、表示が上記の画面とは異なります。

トラップ情報

以下の各トラップを有効にするか無効にするかを選択します。

- coldStart
本装置の起動時および再起動時に 1 回だけ通知します。
- linkDown
本装置の通信リンクに障害があったときに通知します。また、装置の再起動時や構成定義反映時にも送信される場合があります。
- linkUp
本装置の通信リンクの中のどれかが UP 状態になったときに通知します。
- authenticationFailure
SNMP の認証失敗時に通知します。
- newRoot
本装置がルートブリッジになるときに通知します。
- topologyChange
本装置がブリッジネットワークの構成変更を検出したとき、つまりラーニング状態からフォワーディング状態に、またはフォワーディング状態からブロッキング状態に変更するときに通知します。
- vrrpTrapNewMaster (SR-S716C2、724TC1、748TC1)
本装置が VRRP グループでマスタとなったときに通知します。
- vrrpTrapAuthFailure (SR-S716C2、724TC1、748TC1)
本装置で受信した VRRP-AD メッセージの認証方法が異常、または VRRP グループに設定された認証方法やパスワードが一致しないときに通知します。
- vrrpTrapProtoError (SR-S724TC1、748TC1)
本装置で受信した VRRP-AD メッセージがプロトコルエラーであったときに通知します。
- nosError
本装置になんらかの異常（ハードウェア異常）が発生したときに通知します。このトラップは異常が発生したことをだけ通知します。
- lldpRemTablesChange
隣接装置情報管理テーブルに変化があったときに通知します。

27 IEEE802.1ad 情報

適用機種

SR-S328TR1

[操作] 「設定メニュー」→詳細設定「IEEE802.1ad 情報」

IEEE802.1ad 情報

基本情報

VLANタグマッピングルール情報

27.1 基本情報

[操作] 「設定メニュー」→詳細設定「IEEE802.1ad 情報」→「基本情報」

■基本情報

IEEE802.1ad機能 ☒ 使用しない ☐ 使用する

タグプロトコルID

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

IEEE802.1ad 機能

IEEE802.1ad 機能の使用の設定を行います。

こんな事に気をつけて

IEEE802.1ah 機能が有効となっている場合、本設定を有効にしても、IEEE802.1ad 機能は無効となります。

タグプロトコルID

サービス VLAN ID で使用されるタグプロトコルID を1～ffffの16進数を指定します。

省略時はタグプロトコルIDに"88a8"を指定したものとみなされます。

27.2 VLAN タグマッピングルール情報

[操作] 「設定メニュー」→詳細設定「IEEE802.1ad 情報」→「VLAN タグマッピングルール情報」

表示条件入力

表示個数

表示範囲

10

VLANタグマッピングルール定義は存在しません

VLANタグマッピングルール情報

※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。

マッピング ルール番号	説明文	操作
	カスタマーVLAN ID	
	サービスVLAN ID	
	サービスVLAN優先順位	

全削除

<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

サービスVLAN優先順位

0

追加

キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

現在設定されている VLAN タグマッピングルール定義の一覧です。装置全体で 4000 個まで設定できます。

説明文

この VLAN タグマッピングルール定義の説明文を、50 文字以内で設定します。

カスタマー VLAN ID

VLAN タグマッピング対象とするカスタマー VLAN ID を指定します。

"," (カンマ) や "-" (ハイフン) を使用したリスト形式で複数の VLAN ID を指定可能です。

サービス VLAN ID

サービス VLAN に割り当てる VLAN ID を指定します。

サービス VLAN 優先順位

サービス VLAN に割り当てる優先順位を、0～7 の 10 進数で指定します。

280

IEEE802.1ad 情報

28 IEEE802.1ah 情報

適用機種 SR-S328TR1

[操作] 「設定メニュー」→詳細設定「IEEE802.1ah 情報」

IEEE802.1ah 情報

基本情報

[バックボーンサービス関連](#)

28.1 基本情報

[操作] 「設定メニュー」→詳細設定「IEEE802.1ah 情報」→「基本情報」

■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	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

IEEE802.1ah 機能

IEEE802.1ah 機能の使用の設定を行います。

MAC アドレス自動学習

IEEE802.1ah 機能の MAC アドレス自動学習の有効／無効を設定します。

サービス VLAN タグプロトコル ID

S-TAG サービスインタフェース動作時にカスタマーポートで受信したフレームの Tagged VLAN をサービス VLAN と認識するタグプロトコルIDを、1～ffff の16進数で指定します。また、ポートベースサービスインタフェース動作時においても VLAN タグありフレームをカプセリングする際、バックボーンVLANの優先順位に受信フレームの cos 値を引き継ぐ場合には設定が必要となります。

省略時はタグプロトコルIDに"88a8"を指定したものとみなされます。

バックボーンVLAN タグプロトコルID

バックボーンVLANに割り当てるタグプロトコルIDを1～ffff の16進数で指定します。

省略時はタグプロトコルIDに"88a8"を指定したものとみなされます。

バックボーン送信元MAC アドレス

バックボーンあて先 MAC アドレスを指定します。

xx:xx:xx:xx:xx:xx (xx は 2 桁の 16 進数) の形式で指定します。

こんな事に気をつけて

- IEEE802.1ah 機能を使用する場合は必ず指定してください。
- プロバイダーバックボーンネットワーク内で一意な MAC アドレスとなるよう上位3バイトを指定してください。下位3バイトはインスタンスIDがシステムで連結されます。
- MAC アドレスに、ブロードキャストおよびマルチキャストアドレスは指定できません。

28.2 バックボーンサービス関連

[操作] 「設定メニュー」→詳細設定「IEEE802.1ah 情報」→「バックボーンサービス関連」

表示条件入力

表示回数: 10
表示範囲: バックボーンサービス定義は存在しません

■バックボーンサービス情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

サービスID	インスタンスID	操作
[全削除]		

<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: []

[追加] [キャンセル]

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在設定されているバックボーンサービス定義の一覧です。装置全体で2000個まで設定できます。

インスタンスID

バックボーンサービスインスタンスタグに割り当てるインスタンスIDを100～fffffeの16進数で指定します。

[操作] 「設定メニュー」→詳細設定「IEEE802.1ah 情報」→「バックボーンサービス関連」→ [追加]
→ [修正]

IEEE802.1ah情報 - **バックボーンサービス(0)情報**

共通情報 | バックボーンMACアドレス情報

28.2.1 共通情報

[操作] 「設定メニュー」→詳細設定「IEEE802.1ah 情報」→「バックボーンサービス関連」→ [追加]
→ [修正] →「共通情報」

■共通情報

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: []

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: 0

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

[保存] [キャンセル]

説明文

このバックボーンサービスの説明文を、50 文字以内で設定します。

インスタンス ID

バックボーンサービスインスタンスタグに割り当てるインスタンス ID を 100 ～ fffffe の 16 進数で指定します。

サービス VLAN ID

カスタマーポートで転送対象とするサービス VLAN の VLAN ID を指定します。

"," (カンマ) や "-" (ハイフン) を使用したリスト形式で複数の VLAN ID を指定可能です。

バックボーン VLAN ID

バックボーン VLAN に割り当てる VLAN ID を指定します。

バックボーン VLAN 優先順位

バックボーン VLAN に割り当てる優先順位を受信したフレームの cos 値から引き継ぐか、または新規に設定するかを指定します。

新規に設定する場合は、優先順位を 0 ～ 7 の 10 進数で指定します。

こんな事に気をつけて

“受信フレームの cos 値から引き継ぐ” 設定で Tag なしフレームを転送する場合、バックボーン VLAN の優先順位には "0" が設定されます。

28.2.2 バックボーン MAC アドレス情報

[操作] 「設定メニュー」→詳細設定「IEEE802.1ah 情報」→「バックボーンサービス関連」→ [追加]
→ [修正] → 「バックボーン MAC アドレス情報」

表示条件入力

表示回数: 10 | 表示範囲: バックボーン先MACアドレス情報が存在しません

■バックボーンMACアドレス情報

※追加・修正情報は一覧ので設定してください。

定義番号	バックボーンあて先MACアドレス	操作
全削除		

<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:

あて先不明フレーム: ☒ マルチキャスト ☐ ユニキャスト

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

バックボーンあて先 MAC アドレス

バックボーンあて先 MAC アドレスに割り当てる MAC アドレスを指定します。

また、あて先不明フレームのバックボーンあて先 MAC アドレスを指定します。

マルチキャスト

"01:1e:83" に “インスタンス ID” で指定した値を下位 3 バイトに連結したマルチキャストアドレスを使用します。

ユニキャスト

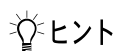
本設定の MAC アドレスで指定したユニキャストアドレスの上位 3 バイトに “インスタンス ID” で指定した値を下位 3 バイトに連結したアドレスを使用します。

29 ProxyDNS 情報／URL フィルタ情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「ProxyDNS 情報 URL フィルタ情報」

ProxyDNS 情報／URL フィルタ情報	
順引き情報	逆引き情報
このページでは ProxyDNS と URL フィルタの設定ができます。URL フィルタは順引き情報で設定します。	



ヒント

◆ 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
パソコンに本装置の IP アドレスを DNS サーバとして登録しておくと、接続先によって問い合わせる DNS サーバを自動的に切り替えます。
- DNS サーバ機能
ホストデータベース情報にホスト名と IP アドレスのペアを登録しておくと、ProxyDNS は該当ホスト名へのアクセスを登録された IP アドレスへのアクセスとして切り替えます。
- URL フィルタ機能
特定のドメイン名（範囲指定も可）へのアクセスを禁止することができます。この機能は順引き情報設定で設定します。
- DNS 問い合わせタイプフィルタ機能
送信元 IP アドレス範囲から送信される特定の問い合わせタイプの DNS パケットを破棄することができます。この機能は順引き情報設定で設定します。

29.1 順引き情報

[操作] 「設定メニュー」→詳細設定「ProxyDNS 情報 URL フィルタ情報」→[順引き情報]

■順引き情報
 ※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。

優先順位	ドメイン名 タイプ 送信元IPアドレス	動作	DNSサーバアドレス	操作
				全削除

<順引き情報入力フィールド>

ドメイン名:

タイプ: (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:

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

順引き情報はドメイン名により DNS サーバを切り替える範囲を指定する場合、特定のドメイン名へのアクセスを禁止する場合、送信元 IP アドレス範囲からの特定の問い合わせタイプの DNS パケットを破棄する場合など、ドメイン名・問い合わせタイプ・送信元 IP アドレスの組み合わせによりいろいろな使い方ができます。定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

ドメイン名

対象とするドメイン名の範囲を 80 文字以内で指定します。ただし、以下のように、“*” および “?” はワイルドカードとして使用されるため、ドメイン名には使用できません。なお、ドメイン名のチェックには大文字／小文字の区別はありません。

“*” : 0 文字以上の任意の文字に一致する

“?” : 1 文字の任意文字に一致する

記述例)

条件	一致
www*.com	www.testa.com、www.test1.test.com
test	www.test.com、test.com、test.co.jp
www.test?.com	www.test1.com、www.test2.com、www.testA.com

タイプ

対象とする問い合わせタイプを以下から選択します。() 内はタイプの番号です。

- すべて (PTR (12) を除く)
- A (1)
- NS (2)
- CNAME (5)
- SOA (6)
- HINFO (13)
- MX (15)
- AAAA (28)
- SRV (33)
- その他

任意のタイプを指定する場合は、“その他” を選択し、1～11、13～65535 の範囲の 10 進数で指定します。

送信元IP アドレス

フィルタリング条件としての送信元IPアドレスを、IPv4 アドレス／マスクビット形式、またはIPv6 アドレス／プレフィックスの形式で設定します。0.0.0.0/0、::/0 を指定した場合、または、省略時は、すべてのアドレスを対象とするものとして動作します。

動作

対象ドメイン、問い合わせタイプ、送信元IPアドレスに対する動作を以下の2つから選択します。

- 廃棄する
該当ドメインの転送を無効にするフィルタ（URL フィルタ）または、該当問い合わせタイプのDNS パケットの転送を無効にするフィルタ（問い合わせタイプ フィルタ）として利用します。
- 設定したDNS サーバへ問い合わせる
特定のDNS サーバへ問い合わせます。問い合わせるDNS サーバのIPv4 アドレスまたはIPv6 アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

29.2 逆引き情報

[操作] 「設定メニュー」→詳細設定「ProxyDNS 情報 URL フィルタ情報」→[逆引き情報]

■逆引き情報

※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。

優先順位	ネットワークアドレス	動作	DNSサーバアドレス	操作
全削除				
<逆引き情報入力フィールド>				
	ネットワークアドレス すべて (指定する"を選択時のみ有効です。) ※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	追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

逆引き情報はIPアドレスによりDNSサーバを切り替える範囲を指定する場合に使用します。定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53)を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

ネットワークアドレス

対象とするネットワークアドレスを以下の4つから選択します。

- すべて
IPv4アドレスとIPv6アドレスの両方を選択します。
- IPv4 すべて
IPv4アドレスをすべて選択します。
- IPv6 すべて
IPv6アドレスをすべて選択します。
- 指定する
IPv4アドレス/マスクビット形式、またはIPv6アドレス/プレフィックスの形式で指定します。

動作

対象ドメインに対する動作を以下の2つから選択します。

- 廃棄する
該当ネットワークの転送を無効にするフィルタを指定します。
- 設定したDNSサーバへ問い合わせる
特定のDNSサーバへ問い合わせます。問い合わせるDNSサーバのIPv4アドレス、またはIPv6アドレスを指定します。
有効範囲)
1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254
::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

30 ホストデータベース情報

適用機種 全機種

[操作] 「設定メニュー」→詳細設定「ホストデータベース情報」

ホストデータベース情報		
1～20	21～40	41～60
61～80	81～100	全表示

[操作] 「設定メニュー」→詳細設定「ホストデータベース情報」→[全表示]

■ホストデータベース情報				
\	ホスト名	IPv4アドレス	MACアドレス	操作
		IPv6アドレス	DUID	
1	-	-	-	修正 削除
2	-	-	-	修正 削除
3	-	-	-	修正 削除
4	-	-	-	修正 削除
5	-	-	-	修正 削除

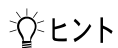
96	-	-	-	修正 削除
97	-	-	-	修正 削除
98	-	-	-	修正 削除
99	-	-	-	修正 削除
100	-	-	-	修正 削除
全削除				

保存した情報は、設定反映後に有効になります。

現在、設定されているホストデータベース情報の定義が表示されています。ホストデータベースの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」→詳細設定「ホストデータベース情報」→[修正]

1	ホスト名	
	IPv4アドレス	
	IPv6アドレス	
	MACアドレス	
	DUID	
保存 キャンセル 一覧へ戻る		



ヒント

◆ ホストデータベースには以下の機能があります。

- DNS サーバ機能
「ホスト名」「IPv4 アドレス」または「IPv6 アドレス」のペアを登録することにより、ProxyDNS の DNS サーバ機能を使用することができます。
 - IPv4 DHCP スタティック機能
「IPv4 アドレス」「MAC アドレス」のペアを登録することにより、DHCP で割り当てられる IP アドレスを端末固有のものとすることができます。
 - IPv6 DHCP スタティック機能
「IPv6 アドレス」「DUID」のペアを登録することにより、IPv6 DHCP で割り当てられる IPv6 アドレスを端末固有のものとすることができます。
-

ホスト名

DNS サーバ機能で使用されます。80 文字以内で指定します。使用できる文字は半角英数字、“.”、“-” です。その他の記号は使用できません。

IPv4 アドレス

DNS サーバ機能および IPv4 DHCP スタティック機能で使用されます。

IPv6 アドレス

DNS サーバ機能および IPv6 DHCP スタティック機能で使用されます。

MAC アドレス

IPv4 DHCP スタティック機能で使用されます。MAC アドレスは以下の形式で指定します。

xx:xx:xx:xx:xx:xx (xx は 2 桁の 16 進数)

DUID

IPv6 DHCP スタティック機能で使用されます。260 桁以内の 16 進数で表記した DUID を指定します。

31 無線 LAN 管理情報

適用機種 全機種

[操作] 「設定メニュー」→無線 LAN 管理設定「無線 LAN 管理情報」

無線 LAN 管理情報		
管理グループ情報	管理機器情報	管理外機器情報
このページでは、無線 LAN 管理に関する情報についての設定ができます。		

31.1 管理グループ情報

[操作] 「設定メニュー」→無線 LAN 管理設定「無線 LAN 管理情報」→[管理グループ情報]

■管理グループ情報

※追加情報は一覧の最後尾の追加フィールドで設定してください。

定義番号	グループ名	操作
全削除		

＜管理グループ情報入力フィールド＞

グループ名

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている管理グループ情報が表示されています。管理グループの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

アクセスポイント群を管理・監視しやすいように任意のグループとしてまとめることができます。

グループ名

グループを識別するグループ名を 8 文字以内で指定します。文字列には、0x21 および 0x23～0x7e のコードで構成される ASCII 文字列を指定します。

31.2 管理機器情報

[操作] 「設定メニュー」→無線 LAN 管理設定「無線 LAN 管理情報」→[管理機器情報]

■管理機器情報

※追加情報は一覧の最後尾の追加フィールドで設定してください。

定義番号	管理機器名	グループ	タイプ	IPアドレス	操作
全削除					
<管理機器情報入力フィールド>					
管理機器名		NewAP0			
追加 キャンセル					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている管理機器の定義が表示されています。管理機器の定義数は、仕様一覧「2.3 システム最大値一覧」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

管理機器名

管理機器を識別する管理機器名を8文字以内で指定します。文字列には、0x21 および 0x23～0x7e のコードで構成される ASCII 文字列を指定します。

[操作] 「設定メニュー」→無線 LAN 管理設定「無線 LAN 管理情報」→[管理機器情報]→[修正]

管理機器情報(0) 基本情報

31.2.1 基本情報

[操作] 「設定メニュー」→無線 LAN 管理設定「無線 LAN 管理情報」→[管理機器情報]→[修正]
→[基本情報]

■基本情報

管理機器名

NewAP1

グループ

IPアドレス

無線LAN管理パスワード

無線LAN管理パスワード(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

☒情報取得する ☐情報取得しない

近隣管理機器

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

キャンセル

管理機器名

管理機器を識別する管理機器名を8文字以内で指定します。文字列には、0x21 および 0x23～0x7e のコードで構成される ASCII 文字列を指定します。

グループ

管理機器が属するグループの定義番号を選択します。
管理機器がグループに属さない場合、空白を指定します。

設定値	意味
空白	管理機器は、グループに属しません。
数値	管理機器が属するグループの定義番号です。

IP アドレス

管理機器の IPv4 アドレスを指定します。

指定可能な範囲は以下のとおりです。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

無線 LAN 管理パスワード

管理機器へ無線 LAN 管理でログインするためのパスワードを64文字以内で指定します。文字列には、0x21 および 0x23～0x7e のコードで構成される ASCII 文字列を指定します。

また、入力したパスワードを検証するため、無線 LAN 管理パスワード（確認用）にも同じ値を指定します。

監視用

管理機器を無線 LAN の監視用として使用する場合は、“使用する”を選択します。

こんな事に気をつけて

監視用無線 LAN アクセスポイントは、以下の条件を満たす必要があります。

- 無線 LAN インタフェースの動作タイプが、無線 LAN アクセスポイント、または、スキャン専用モードであること。
- 周辺アクセスポイント検出の動作モードが有効であること。

無線 LAN 端末の情報取得

無線 LAN アクセスポイントに接続された無線 LAN 端末の情報取得を行う場合は、“情報取得する”を選択します。

近隣管理機器

無線 LAN の電波出力自動調整機能を使用する場合に、当該管理機器の無線電波が近隣にある管理機器（無線 LAN アクセスポイント）のうち、どの管理機器で検出させたいかを指定します。

近隣管理機器には、4 つまでの管理機器を指定することができます。

近隣管理機器の指定がない場合、当該管理機器は無線 LAN の電波出力自動調整機能の対象から除外されます。

31.3 管理外機器情報

[操作] 「設定メニュー」→無線 LAN 管理設定「無線 LAN 管理情報」→[管理外機器情報]

■管理外機器情報

※追加情報は一覧の最後尾の追加フィールドで設定してください。

定義番号	管理外機器名	MACアドレス	操作
全削除			
＜管理外機器情報入力フィールド＞			
管理外機器名	Unmng0		
MACアドレス			
			追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、設定されている管理外機器の定義が表示されています。管理外機器の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

使用している場所、目的などが明らかで管理・監視する必要がない機器を設定することができます。

管理外機器名

管理外機器を識別する管理外機器名を8文字以内で指定します。文字列には、0x21 および 0x23～0x7e のコードで構成される ASCII 文字列を指定します。

MAC アドレス

管理外機器の MAC アドレスを指定します。MAC アドレスは、xx:xx:xx:xx:xx:xx（xx は 2 桁の 16 進数）の形式で指定します。

32 MAC アドレスフィルタセット情報

適用機種 全機種

[操作] 「設定メニュー」→無線 LAN 管理設定「MAC アドレスフィルタセット情報」

MACアドレスフィルタセット情報

MACアドレスフィルタセット情報

■MACアドレスフィルタセット情報

※追加情報は一覧の最後尾の追加フィールドで設定してください。

定義番号	MACアドレスフィルタセット名	定義済フィルタ数	操作
0	FilterSet0	1	修正 削除 MACアドレスフィルタ

全削除

<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

FilterSet1

追加

キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、設定されている MAC アドレスフィルタセット情報が表示されています。MAC アドレスフィルタセットの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P53) を参照してください。処理するボタンをクリックし、次のページへ進みます。

MAC アドレスフィルタ名

MAC アドレスフィルタを識別する MAC アドレスフィルタセット名を 50 文字以内で指定します。文字列には、0x21 および 0x23 ～ 0x7e のコードで構成される ASCII 文字列を指定します。

32.1 MAC アドレスフィルタ情報

[操作] 「設定メニュー」→無線 LAN 管理設定「MAC アドレスフィルタセット情報」→ [追加]
→ [MAC アドレスフィルタ]

MACアドレスフィルタ情報(1)

MACアドレスフィルタ情報

32.1.1 MAC アドレスフィルタ情報（一括設定）

[操作] 「設定メニュー」→無線LAN 管理設定「MAC アドレスフィルタセット情報」→ [追加]
→ [MAC アドレスフィルタ]

■MACアドレスフィルタ情報(一括設定)

<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

保存 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

MAC アドレスフィルタ

MAC アドレスフィルタセットに設定する MAC アドレス
フィルタを一括で指定します。

MAC アドレスフィルタは、以下の形式で指定します。

指定の MAC アドレスを許可する場合

MAC アドレス ,pass,[コメント]

指定の MAC アドレスを拒否する場合

MAC アドレス ,reject,[コメント]

MAC アドレス

個別の MAC アドレスを対象とする場合は、
xx:xx:xx:xx:xx:xx (xx は 2 桁の 16 進数) の形式で
指定します。

すべての MAC アドレスを対象とする場合は、any
を指定します。

コメント

50 文字以内で指定します。文字列には、0x21 およ
び 0x23 ～ 0x7e のコードで構成される ASCII 文字
列を指定します。

省略できます。

32.1.2 MAC アドレスフィルタ情報（個別設定）

〔操作〕 「設定メニュー」→無線 LAN 管理設定「MAC アドレスフィルタセット情報」→〔追加〕
→〔MAC アドレスフィルタ〕→〔保存〕

■MACアドレスフィルタ情報(個別設定)

※追加情報は一覧の最後尾の追加フィールドで設定してください。

定義番号	MACアドレス	アクセス制御	コメント	操作
0	00:00:00:00:00:01	拒否	FilterSet0	修正 削除

全削除

＜MACアドレスフィルタ入力フィールド＞

MACアドレス	
アクセス制御	☒ 許可 ☐ 拒否
コメント	MAC_filter_for_1

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

MAC アドレスフィルタセットに1つ以上のMACアドレスフィルタが設定されている場合、MACアドレスフィルタの設定は個別設定で設定します。

MAC アドレス

個別のMACアドレスを対象とする場合は、
xx:xx:xx:xx:xx:xx（xxは2桁の16進数）の形式で指定します。

すべてのMACアドレスを対象とする場合は、anyを指定します。

アクセス制御

管理機器にMACアドレスフィルタを適用する際の動作を指定します。

- 許可
指定のMACアドレスが管理機器に繋がることを許可します。
- 拒否
指定のMACアドレスが管理機器に繋がることを拒否します。

コメント

50文字以内で指定します。文字列には、0x21 および 0x23～0x7e のコードで構成されるASCII文字列を指定します。

省略できます。

33 無線 LAN 管理パラメタ情報

適用機種 全機種

[操作] 「設定メニュー」→無線 LAN 管理設定「無線 LAN 管理パラメタ情報」

無線 LAN 管理パラメタ情報

無線 LAN 管理パラメタ情報

このページでは、無線 LAN 管理機能に関するパラメタについての設定ができます。

33.1 無線 LAN 管理パラメタ

[操作] 「設定メニュー」→無線 LAN 管理設定「無線 LAN 管理パラメタ情報」→[無線 LAN 管理パラメタ]

■無線 LAN 管理パラメタ

?

管理	管理情報取得		☒ しない ☐ 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
	チャンネル自動調整	共通	通信帯域幅 20 MHz 割当範囲 w52/53/56
		5GHz帯	判定用RSSIしきい値 20 開始チャンネル 1 チャンネル割当間隔 5
		2.4GHz帯	
電波出力自動調整		RSSI最低しきい値 20	
監視	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 6 回
	無線 LAN		☒ しない ☐ 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 5 秒 通信異常判定しきい値 6 回
	無線 LAN 端末の RSSI 監視		RSSI評価母数 10 回 RSSI最低しきい値 20
	監視ログ		保持件数 1000 件

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

管理情報取得

管理機器や無線 LAN 端末の情報取得を行う際の時間パラメタを設定します。

情報取得間隔

ある管理機器の情報を取得してから次の管理機器の情報を取得するまでの間隔の秒数を、1～600の範囲の10進数で指定します。

情報取得待機間隔

すべての情報取得対象の管理機器の情報を取得したあと、次の情報取得を開始するまでの待ち時間の秒数を、1～600の範囲の10進数で指定します。

情報取得タイムアウト

管理機器との通信時のタイムアウト時間の秒数を、1～60の範囲の10進数で指定します。

こんな事に気をつけて

情報取得間隔が短いほどリアルタイムに近い情報を得ることができますが、本装置とネットワークの負荷は増大します。システム、ネットワークのパフォーマンスに応じて適切な値を設定してください。

チャンネル自動調整（共通）

通信帯域幅

無線 LAN チャンネル自動調整時の通信帯域幅を指定します。

- 20
無線 LAN の通信帯域幅に 20MHz を使用します。
- 40
無線 LAN の通信帯域幅に 40MHz を使用します。

チャンネル自動調整（5GHz 帯）

割当範囲

5GHz 帯の無線 LAN チャンネル自動調整時に、割り当てるチャンネルの範囲を指定します。

- w52
5GHz 無線 LAN W52 で規程されたチャンネルの中で割り当てを行います。
- w53
5GHz 無線 LAN W53 で規程されたチャンネルの中で割り当てを行います。

- w56
5GHz 無線 LAN W56 で規程されたチャンネルの中で割り当てを行います。
- w52/53
5GHz 無線 LAN W52 と W53 で規程されたチャンネルの中で割り当てを行います。
- w52/53/56
5GHz 無線 LAN W52、W53 および W56 で規程されたチャンネルの中で割り当てを行います。

チャンネル自動調整（2.4GHz 帯）

判定用 RSSI しきい値

2.4GHz 帯の無線 LAN チャンネル自動調整時に、使用済みのチャンネルを割り当てる場合の RSSI のしきい値を 1～128 の範囲の10進数で指定します。

開始チャンネル

2.4GHz 帯の無線 LAN チャンネルを割り当てるときのチャンネルのレイアウトの開始チャンネルを 1～5 の範囲の10進数で指定します。

チャンネル割当間隔

2.4GHz 帯の無線 LAN チャンネルを割り当てるときのチャンネルのレイアウトのチャンネル割当間隔を、3～5 の範囲の10進数で指定します。

チャンネルレイアウトは以下の式で求めることができます。

$\text{<ch_number>, <ch_number> + (1 \times \text{<interval>}), \dots, <ch_number> + (n \times \text{<interval>})$

開始チャンネル：<ch_number>

チャンネル割当間隔：<interval>

電波出力自動調整

RSSI 最低しきい値

電波出力自動調整時に近隣の管理機器で計測される、調整対象の管理機器の RSSI のしきい値を 1～255 の範囲の10進数で指定します。

有線 LAN

管理機器の稼動監視の時間パラメタを設定します。

稼動監視間隔

ある管理機器に ping を送信し応答を得たあと、次の管理機器に ping を送信するまでの間隔の秒数を、1 ～ 600 の範囲の 10 進数で指定します。

稼動監視待機間隔

すべての監視対象の管理機器に ping を送信したあと、次の ping 送信を開始するまでの待ち時間の秒数を、1 ～ 600 の範囲の 10 進数で指定します。

稼動監視タイムアウト

管理機器からの ping 応答のタイムアウト時間の秒数を、1 ～ 60 の範囲の 10 進数で指定します。

こんな事に気をつけて

稼動監視間隔が短いほどリアルタイムに近い情報を得ることができますが、本装置とネットワークの負荷は増大します。システム、ネットワークのパフォーマンスに応じて適切な値を設定してください。

通信異常判定しきい値

有線 LAN の稼動監視で、指定した回数連続して ping に無応答の場合、対象の管理機器の有線 LAN を通信異常の疑いありと報告します。通信が確認できない連続回数が通信異常判定しきい値を超えると、対象の管理機器の有線 LAN を通信異常と報告します。

通信異常判定しきい値は 1 ～ 11 の範囲の 10 進数で指定します。

無線 LAN

監視用管理機器への無線 LAN のスキャンレポート取得の時間パラメタを設定します。

スキャンレポート取得間隔

ある監視用管理機器のスキャンレポートを取得してから次の監視用管理機器のスキャンレポートを取得するまでの間隔の秒数を、1 ～ 600 の範囲の 10 進数で指定します。

スキャンレポート取得待機間隔

すべての監視用管理機器からスキャンレポートを取得したあと、次のスキャンレポート取得を開始するまでの待ち時間の秒数を、1 ～ 600 の範囲の 10 進数で指定します。

スキャンレポート取得タイムアウト

監視用管理機器との通信時のタイムアウト時間の秒数を、1 ～ 60 の範囲の 10 進数で指定します。

こんな事に気をつけて

スキャンレポート取得間隔が短いほどリアルタイムに近い情報を得ることができますが、本装置とネットワークの負荷は増大します。システム、ネットワークのパフォーマンスに応じて適切な値を設定してください。

通信異常判定しきい値

無線 LAN の監視で、指定した回数連続して無線 LAN の監視結果に監視対象の管理機器が検出されない場合、その管理機器の無線 LAN を通信異常の疑いありと報告します。連続未検出回数が通信異常判定しきい値を超えると、対象の管理機器の無線 LAN を通信異常と報告します。

通信異常判定しきい値は 1 ～ 11 の範囲の 10 進数で指定します。

無線 LAN 端末の RSSI 監視

管理機器に接続している無線 LAN 端末からの RSSI を評価した結果が RSSI 最低しきい値を下回った場合、監視ログにその無線 LAN 端末と RSSI の評価値の情報を出力します。

RSSI 評価母数

1 ～ 50 の範囲の 10 進数で指定します。

RSSI 最低しきい値

1 ～ 255 の範囲の 10 進数で指定します。

こんな事に気をつけて

無線 LAN 端末の RSSI 監視は、無線 LAN 端末の情報を取得する管理機器に対してのみ実行することができます。

監視ログ

監視ログを設定します。

保持件数

監視ログの保持件数を、100 ～ 10000 の範囲の 10 進数で指定します。

索引

A

AAA 情報	251
AAA ユーザ情報	253
ACL 情報	263
ACL 定義情報	264
ARP 情報	176
ARP 認証情報	142, 143
AS 外部経路集約情報	217
AS 境界ルータ情報	217

C

COS キュー情報	238
-----------	-----

D

DHCP 情報	173
DHCP スヌープ情報	120
DNS サーバ機能	284, 289
DNS サーバの自動切り替え機能	284
DNS 問い合わせタイプフィルタ機能	284
DSCP 値書き換え情報	168

E

ECMP 情報	204
etherblock 情報	107
ether 情報	38

I

ICMP 定義情報	267
IEEE802.1ad 関連	
ether 情報	83
リンクアグリゲーショングループ情報	97
IEEE802.1ad 情報	279
STP 情報	243
IEEE802.1ah 関連	
ether 情報	86
リンクアグリゲーショングループ情報	100
IEEE802.1ah 情報	281
IEEE802.1X 認証情報	
ether 情報	55, 56
認証情報	246
IGMP スヌープ情報	249
VLAN 情報	121
IPv4 DHCP スタティック機能	289
IPv4 ループバック情報	27
IPv6 DHCP スタティック機能	289

IPv6 OSPF 関連	226
IPv6 AS 境界ルータ情報	230
IPv6 OSPF エリア情報	227
IPv6 OSPF 再配布フィルタリング情報	231
IPv6 ルータ ID 情報	226
IPv6 QoS 情報	137
IPv6 RIP 関連	223
IPv6 RIP 再配布フィルタリング情報	224
IPv6 RIP タイマ情報	223
IPv6 RIP マルチパス情報	224
IPv6 関連	177
IPv6 DHCP 情報	185
IPv6 DSCP 値書き換え情報	196
IPv6 OSPF 情報	182
IPv6 RIP 情報	181
IPv6 基本情報	177
IPv6 スタティック経路情報	184
IPv6 フィルタリング情報	189
IPv6 基本情報	177
IPv6 情報	200
IPv6 スタティック経路情報	184
IPv6 定義情報	267
IPv6 フィルタ情報	127
IPv6 ループバック情報	28
IP アドレス情報	155
IP 関連	
AAA 情報	255
LAN 情報	155
IP 基本情報	255
IP 情報	199
IP 定義情報	265
IP フィルタリング情報	161
IP マルチキャスト情報	233
IP マルチキャストスタティック経路情報	236

L

L2 暗号関連	79
LACP 情報	115
LAN 情報	148
LLDP 関連	52

M

MAC アドレス認証情報	
ether 情報	62
認証情報	248
MAC アドレスフィルタ情報	294
MAC アドレスフィルタセット情報	294
MAC 関連	48
MAC 情報	145
MAC 定義情報	269
MAC テーブルフラッシュ情報	147

MSTP インスタンス情報

ether 情報	51
STP 情報	242

O

OSPF エリア基本情報	211
OSPF エリア情報	211
OSPF 関連	210
OSPF 再配布フィルタリング情報	218
OSPF 情報	157

P

POE 情報	33
ProxyDNS 情報	284

Q

QoS 関連	71
QoS 情報	237
etherblock 情報	111
ether 情報	72
VLAN 情報	132

R

RADIUS 関連	257
RIP 相手フィルタリング情報	209
RIP 関連	205
RIP 再配布フィルタリング情報	206
RIP 情報	156
RIP タイマ情報	205
RIP フィルタリング情報	166
RIP マルチパス情報	206
RIP ユニキャスト送信情報	208

S

SNMPv1/v2c 情報	272
SNMPv3 情報	274
SNMP 情報	270
STP 関連	50
STP 情報	239

T

TCP 定義情報	266
----------------	-----

U

UDP 定義情報	266
URL フィルタ機能	284
URL フィルタ情報	284

V

VLAN 情報	116
VLAN タグマッピングルール情報	
ether 情報	
IEEE802.1ad 関連	84
リンクアグリゲーショングループ情報	
IEEE802.1ad 関連	98
VLAN 定義情報	268
VRRP グループ情報	150
VRRP トリガ情報	152

W

Web 認証関連	59
Web 認証情報	247

あ

アプリケーションフィルタ情報	30, 32
暗号化条件	81

い

異常時動作情報	26
---------------	----

か

外部メディアスタート機能情報	34
カスタマーバックボーンサービス情報	
ether 情報	
IEEE802.1ah 関連	88
リンクアグリゲーショングループ情報	
IEEE802.1ah 関連	102
画面体系	12
管理外機器情報	293
管理機器情報	291
管理グループ情報	290

き

基本情報

AAA 情報	
RADIUS 関連	257
共通情報	252
ether 情報	40
IEEE802.1ad 関連	83, 84
IEEE802.1ah 関連	86, 87
L2 暗号関連	79
MAC アドレス認証関連	62
QoS 関連	71
STP 関連	50
Web 認証関連	59
IGMP スヌープ情報	249
IPv6 情報	200
IP 情報	199
LACP 情報	115

LAN 情報	
VRRP グループ情報	150
共通情報	149
LLDP 情報	244
MAC 情報	145
SNMP 情報	270
STP 情報	239, 241
VLAN 情報	117, 118, 119
パスワード情報	20
無線 LAN 管理情報	292
リンクアグリゲーショングループ情報	93
IEEE802.1ad 関連	97, 98
IEEE802.1ah 関連	100, 101
ループ検出情報	250
基本定義情報	264
逆引き情報	287
共通情報	
AAA 情報	252
IEEE802.1ah 情報	
バックボーン関連	282
LAN 情報	149

く

グループ ID 情報	251
------------------	-----

け

経路集約情報	212
--------------	-----

こ

構成定義切り替え予約情報	37
--------------------	----

さ

サーバ機能情報	29
サーバ情報	258
再配布情報	201
サブリカント関連	256
サブリカント情報	256
サマリ LSA 入出力可否情報	213

し

資源情報	33
システムログ情報	25
順引き情報	285

す

スケジュール情報	37
スタティック ARP 情報	176
スタティック経路情報	159
ストーム制御情報	
ether 情報	48
MAC 情報	146

せ

静的 MAC 学習テーブル情報	120
接続先監視情報	
ether 情報	77
リンクアグリゲーショングループ情報	96
接続端末数制限情報	49
設定メニュー	11

そ

送信アルゴリズム情報	237
送信情報	262
装置情報	23
装置名称情報	23

た

タイムサーバ情報	24
ダンプスイッチ情報	34

と

トラップ情報	278
ether 情報	78

に

認証共通情報	54
認証情報	246
AAA 情報	254
認証不要端末情報	
MAC アドレス認証関連	64
Web 認証関連	61

は

バーチャルリンク情報	215
パスワード情報	20
バックアップグループ情報	105
バックボーン MAC アドレス情報	
IEEE802.1ah 情報	
バックボーンサービス関連	283
バックボーンサービス関連	282
ハッシュ情報	35

ふ

フィルタ情報	
etherblock 情報	107
ether 情報	66
VLAN 情報	122
プロバイダーバックボーンサービス情報	
eterh 情報	
IEEE802.1ah 関連	90
リンクアグリゲーショングループ情報	
IEEE802.1ah 関連	103

ほ

ポート種別情報

バックアップ選択時	46
ミラー選択時	47
初期表示または通常選択時	45
ホスト情報	200
ホストデータベース情報	288

ま

マニュアル構成	10
マルチキャスト情報	233
LAN 情報	175

む

無線 LAN 管理情報	290
無線 LAN 管理パラメタ	297
無線 LAN 管理パラメタ情報	297

ゆ

優先度情報	203
-------------	-----

り

リンクアグリゲーショングループ情報	92
-------------------------	----

る

ルータ ID 情報	210
ルーティングプロトコル情報	201
ルーティングマネージャ情報	201
ループ検出情報	250

れ

冷却ファン情報	36
---------------	----

ろ

ログインパスワード情報	21
ログインユーザ情報	22

SR-S シリーズ セキュアスイッチ Web リファレンス

P3NK-3862-08Z0

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。