

Fujitsu Network SR-M コマンドリファレンス

V20

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
無線LANを使用した安全なネットワークを構築するために、本装置をご利用ください。

2020年12月 初版

2021年6月 第2版

2021年12月 第3版

2022年4月 第4版

2022年8月 第5版

2023年1月 第6版

2023年10月 第7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 2020-2023

本書の構成と使いかた

本書は、本装置のコンソールから入力するコマンドについて説明しています。

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。

本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

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

本書の構成

本書では構成定義コマンド、運用管理コマンド、その他のコマンド、および付録情報について説明しています。

マークについて

[機能]	コマンドの機能概要を記載しています。
[適用機種]	対象となる装置種別を記載しています。
[入力形式]	入力形式を記載しています。以下の規約に従って記載しています。 < > : パラメタ名称を示しています。 [] : 括弧内のオプションやパラメタを省略できることを示しています。 { } : 括弧内のオプションやパラメタのうち、どれかを選択することを示しています。
[オプション]	各オプションの意味を記載しています。
[パラメタ]	各パラメタの意味を記載しています。
[動作モード]	コマンドを実行可能な動作モードを記載しています。
[説明]	コマンドの解説を記載しています。
[注意]	コマンドの注意事項を記載しています。
[メッセージ]	コマンドの応答またはエラーメッセージを記載しています。
[初期値]	コマンドの初期値を記載しています。
[実行例]	コマンドの実行例を記載しています。
[未設定時]	コマンドの未設定時について説明し、設定したとみなされるコマンドを記載しています。

使用上の注意事項

構成定義コマンドを使用する場合は、以下の点にご注意ください。

- コマンドの設定および変更が終了したら、save コマンドを実行してから commit コマンドまたは reset コマンドを実行し、設定を有効にしてください。save コマンドを実行せず reset コマンドまたは電源再投入を行った場合は、コマンドの設定が元の状態に戻ります。また、save コマンドを実行しないで commit コマンドを実行した場合、一時的に設定は有効になりますが、reset コマンドまたは電源再投入を行った場合にコマンドの設定が元の状態に戻ります。ただし、password コマンドについては設定直後から有効となります。

- 構成定義コマンドを削除する場合は、delete コマンドを使用します。削除した構成定義コマンドは、show コマンド（コマンド名未指定）を実行しても、構成定義コマンド文字列として表示されません。

例. ログインパスワードの削除

```
# delete password admin set
```

- show コマンドにより構成定義を表示する場合、コマンド未設定時の値と同じ物は表示されません。

本文中で使用しているコマンドのパラメタに時間を指定する場合は、特別な指示がある場合を除き s（秒）、m（分）、h（時）、d（日）の単位をつけて設定します。

例：1m = 1分

なお、60s、60m、24h を指定した場合は、それぞれ、1m、1h、1d を指定したものとみなされます。

本装置のマニュアルの構成

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

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

目次

第1章	パスワード情報の設定	16
1.1	パスワード情報	17
1.1.1	password admin set	17
1.1.2	password user set	19
1.1.3	password aaa	21
1.1.4	password authtype	22
第2章	ポート情報の設定	23
2.1	ether 共通情報	24
2.1.1	ether use	24
2.1.2	ether mode	25
2.1.3	ether duplex	26
2.1.4	ether mdi	27
2.1.5	ether flowctl	28
2.1.6	ether type	29
2.1.7	ether vlan tag	30
2.1.8	ether vlan untag	31
2.1.9	ether downrelay wlan	32
2.1.10	ether downrelay recovery mode	33
2.1.11	ether description	34
2.1.12	ether icmpwatch address	35
2.1.13	ether icmpwatch interval	36
第3章	リンクアグリゲーション情報の設定	37
3.1	リンクアグリゲーション情報	38
3.1.1	linkaggregation algorithm	38
3.1.2	linkaggregation mode	39
3.1.3	linkaggregation lacp-timeout	40
3.1.4	linkaggregation downrelay wlan	41
3.1.5	linkaggregation downrelay recovery mode	42
3.1.6	linkaggregation icmpwatch address	43
3.1.7	linkaggregation icmpwatch interval	44
第4章	無線 LAN モジュール情報の設定	45
4.1	無線 LAN モジュール情報	46
4.1.1	ieee80211 use	46
4.1.2	ieee80211 mode	47
4.1.3	ieee80211 channel	49
4.1.4	ieee80211 bandwidth	50
4.1.5	ieee80211 secondary-channel	51
4.1.6	ieee80211 chanlist	53
4.1.7	ieee80211 sta limit	55
4.1.8	ieee80211 protection mode	56
4.1.9	ieee80211 rts threshold	57
4.1.10	ieee80211 dtim period	58
4.1.11	ieee80211 beacon interval	59
4.1.12	ieee80211 wmm mode	60
4.1.13	ieee80211 wmm ack	61
4.1.14	ieee80211 apscan mode	62
4.1.15	ieee80211 apscan expire	63
4.1.16	ieee80211 txpower	64
4.1.17	ieee80211 supportrate	66
4.1.18	ieee80211 supportmcs	68
4.1.19	ieee80211 vht-supportmcs	70
4.1.20	ieee80211 he-supportmcs	71
4.1.21	ieee80211 noise-detect use	72
4.1.22	ieee80211 radar-detect lamp-flash time	73

4.1.23	ieee80211 sr use	74
4.1.24	ieee80211 sr tx-threshold	75
4.1.25	ieee80211 l44ch-support	76
4.1.26	ieee80211 outdoormode	77
第5章	無線 LAN インタフェース情報の設定	78
5.1	無線インタフェース数情報	79
5.1.1	wlan-conf wlan-num	79
5.2	無線 LAN インタフェース情報	81
5.2.1	wlan use	81
5.2.2	wlan description	82
5.2.3	wlan type	83
5.2.4	wlan ssid	84
5.2.5	wlan hide	85
5.2.6	wlan apbridge	86
5.2.7	wlan auth	87
5.2.8	wlan wep mode	89
5.2.9	wlan wep key	90
5.2.10	wlan wep send	92
5.2.11	wlan wpa cipher	93
5.2.12	wlan wpa psk	94
5.2.13	wlan wpa sae password	95
5.2.14	wlan wpa rekey group	96
5.2.15	wlan wpa pmkcache mode	97
5.2.16	wlan wpa pmkcache num	98
5.2.17	wlan wpa pmkcache expire	99
5.2.18	wlan wpa eapol supptimeout	100
5.2.19	wlan wpa eapol maxreq	101
5.2.20	wlan wpa pmf mode	102
5.2.21	wlan wpa owe trans	103
5.2.22	wlan guard-interval	104
5.2.23	wlan macfilter	105
5.2.24	wlan macfilter default	107
5.2.25	wlan sta guarantee	108
5.2.26	wlan sta idle	109
5.2.27	wlan band-steering mode	110
5.2.28	wlan atf ratio	112
5.3	VLAN 情報	113
5.3.1	wlan vlan tag	113
5.3.2	wlan vlan untag	114
5.4	IEEE802.1X 認証情報	115
5.4.1	wlan dot1x use	115
5.4.2	wlan dot1x supptimeout	117
5.4.3	wlan dot1x maxreq	118
5.4.4	wlan dot1x reauthperiod	119
5.4.5	wlan dot1x aaa	120
5.4.6	wlan dot1x vid	121
5.4.7	wlan dot1x vlan assign	122
5.4.8	wlan dot1x backup	124
5.5	MAC アドレス認証情報	126
5.5.1	wlan macauth use	126
5.5.2	wlan macauth aaa	128
5.5.3	wlan macauth expire	129
5.5.4	wlan macauth vid	130
5.5.5	wlan macauth vlan assign	131
第6章	エアタイムフェアネス情報の設定	133
6.1	エアタイムフェアネス情報	134

6.1.1	atf use	134
第7章	VLAN情報の設定	135
7.1	VLAN 共通情報	136
7.1.1	vlan name	136
7.1.2	vlan description	137
7.2	フィルタ情報	138
7.2.1	vlan filter	138
第8章	MAC情報	140
8.1	MAC情報	141
8.1.1	mac age	141
第9章	LAN情報の設定	142
9.1	IP 関連情報	143
9.1.1	lan ip address	143
9.1.2	lan ip dhcp service	144
9.1.3	lan ip route	145
9.1.4	lan ip arp static	147
9.2	VLAN 関連情報	148
9.2.1	lan vlan	148
9.3	SNMP 関連情報	149
9.3.1	lan snmp trap linkdown	149
9.3.2	lan snmp trap linkup	150
第10章	IP 関連情報	151
10.1	IP 関連情報	152
10.1.1	ip arp age	152
第11章	認証情報の設定	153
11.1	IEEE802.1X 情報	154
11.1.1	dot1x use	154
11.2	MAC アドレス認証情報	155
11.2.1	macauth use	155
11.2.2	macauth password	156
11.2.3	macauth type	157
第12章	ACL情報の設定	158
12.1	ACL 情報	159
12.1.1	acl mac	159
12.1.2	acl ip	160
12.1.3	acl tcp	162
12.1.4	acl udp	163
12.1.5	acl icmp	164
12.1.6	acl description	165
第13章	AAA情報の設定	166
13.1	グループ ID 情報	167
13.1.1	aaa name	167
13.2	RADIUS 情報の設定	168
13.2.1	aaa radius service	168
13.2.2	aaa radius auth source	169
13.2.3	aaa radius auth message-authenticator	170
13.2.4	aaa radius accounting source	171
13.2.5	aaa radius client server-info auth secret	172
13.2.6	aaa radius client server-info auth address	173
13.2.7	aaa radius client server-info auth port	174
13.2.8	aaa radius client server-info auth deadtime	175

13.2.9	aaa radius client server-info auth priority	176
13.2.10	aaa radius client server-info auth source	177
13.2.11	aaa radius client server-info auth watch type	178
13.2.12	aaa radius client server-info auth watch user	179
13.2.13	aaa radius client server-info auth <number> watch interval	181
13.2.14	aaa radius client server-info auth watch retry	182
13.2.15	aaa radius client server-info auth watch timeout	183
13.2.16	aaa radius client server-info auth watch abnormal-interval	184
13.2.17	aaa radius client server-info accounting secret	185
13.2.18	aaa radius client server-info accounting address	186
13.2.19	aaa radius client server-info accounting port	187
13.2.20	aaa radius client server-info accounting deadtime	188
13.2.21	aaa radius client server-info accounting priority	189
13.2.22	aaa radius client server-info accounting source	190
13.2.23	aaa radius client retry	191
13.2.24	aaa radius client nas-identifier	192
13.2.25	aaa radius client nas-identifier-ssid	193
第 14 章 端末可視化機能情報の設定		194
14.1	端末可視化機能情報	195
14.1.1	devscan use	195
14.1.2	devscan vlan	196
14.1.3	devscan age	197
14.1.4	devscan dictionary dhcp	198
14.1.5	devscan dictionary oui	199
14.1.6	devscan dictionary mac	200
第 15 章 NXconciierge エージェント機能の設定		201
15.1	NXconciierge エージェント機能情報	202
15.1.1	management-agent mode	202
15.1.2	management-agent tenantkey	203
15.1.3	management-agent macfilter	204
15.1.4	management-agent serverlogin proxy auth send	205
15.1.5	management-agent serverlogin proxy address	206
第 16 章 装置情報の設定		207
16.1	SNMP 情報	208
16.1.1	snmp service	208
16.1.2	snmp agent contact	209
16.1.3	snmp agent sysname	210
16.1.4	snmp agent location	211
16.1.5	snmp agent address	212
16.1.6	snmp agent engineid	213
16.1.7	snmp manager	214
16.1.8	snmp trap coldstart	216
16.1.9	snmp trap linkdown	217
16.1.10	snmp trap linkup	218
16.1.11	snmp trap authfail	219
16.1.12	snmp trap noserror	220
16.1.13	snmp user name	221
16.1.14	snmp user address	222
16.1.15	snmp user notification	223
16.1.16	snmp user auth	224
16.1.17	snmp user priv	225
16.1.18	snmp user write	226
16.1.19	snmp user read	227
16.1.20	snmp user notify	228
16.1.21	snmp view subtree	229
16.2	システムログ情報	231

16.2.1	syslog server address	231
16.2.2	syslog server pri	232
16.2.3	syslog pri	233
16.2.4	syslog facility	234
16.2.5	syslog command-logging	235
16.2.6	syslog header	236
16.2.7	syslog source address	237
16.2.8	syslog filter regexp	238
16.3	自動時刻設定情報	241
16.3.1	time auto server	241
16.3.2	time auto interval	242
16.3.3	time zone	243
16.4	ProxyARP 情報	244
16.4.1	proxyarp use	244
16.5	スケジュール情報	245
16.5.1	schedule at	245
16.5.2	schedule syslog	247
16.6	装置ランプ情報	248
16.6.1	lamp mode	248
16.6.2	lamp delay	249
16.7	高速転送情報	250
16.7.1	system bridge acceleration mode	250
16.8	定期ログ情報	251
16.8.1	system monitoringinfo collect interval	251
16.9	外部メディアスタート機能の情報	252
16.9.1	storage setup mode	252
16.9.2	storage setup machine	253
16.10	アンテナ情報	254
16.10.1	antenna use	254
16.11	サーバー情報	255
16.11.1	serverinfo ftp	255
16.11.2	serverinfo ftp filter	256
16.11.3	serverinfo ftp filter default	257
16.11.4	serverinfo sftp	258
16.11.5	serverinfo telnet	259
16.11.6	serverinfo telnet filter	260
16.11.7	serverinfo telnet filter default	261
16.11.8	serverinfo ssh	262
16.11.9	serverinfo ssh filter	263
16.11.10	serverinfo ssh filter default	264
16.11.11	serverinfo http	265
16.11.12	serverinfo http filter	266
16.11.13	serverinfo http filter default	267
16.11.14	serverinfo https	268
16.11.15	serverinfo https filter	269
16.11.16	serverinfo https filter default	270
16.11.17	serverinfo snmp	271
16.11.18	serverinfo snmp filter	272
16.11.19	serverinfo snmp filter default	273
16.11.20	serverinfo time	274
16.11.21	serverinfo time filter	275
16.11.22	serverinfo time filter default	276
16.12	DNS サーバ情報	277
16.12.1	dns-resolver server	277
16.13	その他	278
16.13.1	addact	278

16.13.2	consoleinfo.....	280
16.13.3	telnetinfo.....	281
16.13.4	sysname.....	282
第 17 章	モード操作コマンド/ターミナル操作コマンド.....	283
17.1	モード操作.....	284
17.1.1	exit.....	284
17.1.2	configure.....	285
17.2	コマンド実行履歴.....	286
17.2.1	show logging command.....	286
17.2.2	clear logging command.....	288
第 18 章	システム操作および表示コマンド.....	289
18.1	システム操作および表示.....	290
18.1.1	show system information.....	290
18.1.2	show system status.....	292
18.1.3	show tech-support.....	294
18.1.4	show logging error.....	295
18.1.5	clear logging error.....	296
18.1.6	show logging syslog.....	297
18.1.7	clear logging syslog.....	298
18.1.8	show logging monitoringinfo.....	299
18.1.9	clear logging monitoringinfo.....	301
18.1.10	clear statistics.....	302
18.1.11	show date.....	303
18.1.12	date.....	304
18.1.13	rdate.....	305
18.1.14	reset.....	306
18.1.15	clear corefile.....	307
18.1.16	clear https certificate.....	308
第 19 章	構成定義情報の表示、削除、および操作コマンド.....	309
19.1	構成定義情報表示.....	310
19.1.1	show candidate-config.....	310
19.1.2	show running-config.....	311
19.1.3	show startup-config.....	312
19.1.4	diff.....	313
19.2	構成定義情報削除.....	314
19.2.1	delete.....	314
19.3	構成定義情報操作.....	315
19.3.1	load.....	315
19.3.2	save.....	317
19.3.3	commit.....	318
19.3.4	discard.....	319
19.4	ファイル操作コマンド.....	320
19.4.1	dir.....	320
19.4.2	copy.....	322
19.4.3	remove.....	324
19.4.4	rename.....	325
19.4.5	format.....	326
第 20 章	ログインユーザの状態などの表示、クリア操作コマンド.....	327
20.1	ログインユーザの状態などの表示.....	328
20.1.1	show users.....	328
20.2	ログインユーザの状態などのクリア.....	330
20.2.1	clear line.....	330
第 21 章	Ethernet のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド.....	331

21.1 Ethernet のカウンタ・ログ・統計・状態などの表示.....	332
21.1.1 show ether.....	332
21.1.2 show ether statistics.....	335
21.2 Ethernet のカウンタ・ログ・統計などのクリア.....	340
21.2.1 clear ether statistics.....	340
第 22 章 LACP のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド.....	341
22.1 LACP のカウンタ・ログ・統計・状態などの表示.....	342
22.1.1 show lacp.....	342
第 23 章 無線 LAN モジュールのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド.....	344
23.1 無線 LAN モジュールのカウンタ・ログ・統計・状態などの表示.....	345
23.1.1 show ieee80211 statistics.....	345
23.1.2 show ieee80211 status.....	348
23.2 周辺アクセスポイント情報の取得、表示.....	351
23.2.1 show ieee80211 apscan.....	351
第 24 章 無線 LAN インタフェースのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド.....	357
24.1 無線 LAN インタフェースのカウンタ・ログ・統計・状態などの表示.....	358
24.1.1 show wlan sta.....	358
24.1.2 show wlan statistics.....	363
24.1.3 show wlan status.....	365
24.1.4 show wlan wpa status.....	370
24.1.5 show wlan wpa statistics.....	373
24.2 無線 LAN 接続のカウンタ・ログ・統計などのクリア.....	376
24.2.1 clear wlan wpa statistics.....	376
第 25 章 バンドステアリング機能の表示コマンド.....	377
25.1 バンドステアリング情報の表示.....	378
25.1.1 show band-steering status.....	378
第 26 章 POE のログ・状態などの表示コマンド.....	379
26.1 POE のログ・状態などの表示.....	380
26.1.1 show poe drawing.....	380
第 27 章 USB 接続のカウンタ・ログ・統計・状態などの表示コマンド.....	381
27.1 USB 接続のカウンタ・ログ・統計・状態などの表示.....	382
27.1.1 show usb hcd status.....	382
27.1.2 show usb storage status.....	383
第 28 章 インタフェースのカウンタ・ログ・統計・状態などの表示コマンド.....	385
28.1 インタフェースのカウンタ・ログ・統計・状態などの表示.....	386
28.1.1 show interface.....	386
第 29 章 ARP エントリの表示、クリア操作コマンド.....	388
29.1 ARP エントリの表示.....	389
29.1.1 show arp.....	389
29.2 ARP エントリのクリア.....	391
29.2.1 clear arp.....	391
第 30 章 ルーティングテーブル情報・統計などの表示コマンド.....	392
30.1 IPv4 ルーティングテーブル情報・統計などの表示.....	393
30.1.1 show ip route.....	393
第 31 章 パケットの統計情報の表示、クリア操作コマンド.....	395
31.1 パケットの統計情報の表示.....	396
31.1.1 show ip traffic.....	396

第 32 章 DHCP のカウンタ・ログ・統計・状態などの表示コマンド	398
32.1 IPv4 DHCP のカウンタ・ログ・統計・状態などの表示	399
32.1.1 show ip dhcp	399
第 33 章 ブリッジのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド	401
33.1 ブリッジのカウンタ・ログ・統計・状態などの表示	402
33.1.1 show bridge	402
33.2 ブリッジのカウンタ・ログ・統計・状態などのクリア	404
33.2.1 clear bridge	404
第 34 章 VLAN のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド	405
34.1 VLAN のカウンタ・ログ・統計・状態などの表示	406
34.1.1 show vlan	406
第 35 章 SSH のカウンタ・ログ・統計・状態などの表示コマンド	408
35.1 SSH のカウンタ・ログ・統計・状態などの表示	409
35.1.1 show ssh server key	409
第 36 章 認証機能のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド	411
36.1 IEEE802.1X 認証のカウンタ・ログ・統計・状態などの表示	412
36.1.1 show dot1x port	412
36.1.2 show dot1x statistics port	414
36.1.3 show dot1x backup port	416
36.2 IEEE802.1X 認証のカウンタ・ログ・統計などのクリア	418
36.2.1 clear dot1x statistics	418
36.3 MAC アドレス認証のカウンタ・ログ・統計・状態などの表示	419
36.3.1 show macauth port	419
36.3.2 show macauth statistics port	421
36.4 MAC アドレス認証のカウンタ・ログ・統計などのクリア	422
36.4.1 clear macauth statistics	422
第 37 章 AAA のカウンタ・ログ・統計・状態などの表示コマンド	423
37.1 AAA のカウンタ・ログ・統計・状態などの表示	424
37.1.1 show aaa radius client server-info	424
第 38 章 NETTIME(time/sntp)サーバ、クライアントの統計情報の表示、クリア操作コマンド	426
38.1 NETTIME(time/sntp)統計情報の表示	427
38.1.1 show nettime statistics	427
38.2 NETTIME(time/sntp)統計情報のクリア	429
38.2.1 clear nettime statistics	429
第 39 章 SNMP 統計情報の表示、クリア操作コマンド	430
39.1 SNMP 統計情報の表示	431
39.1.1 show snmp statistics	431
39.2 SNMP 統計などのクリア	434
39.2.1 clear snmp statistics	434
第 40 章 ノード監視機能のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド	435
40.1 ノード監視機能のカウンタ・ログ・統計・状態などの表示	436
40.1.1 show icmpwatch	436
40.1.2 show icmpwatch statistics	437
40.2 ノード監視機能のカウンタ・ログ・統計・状態などのクリア	439
40.2.1 clear icmpwatch statistics	439
第 41 章 ソケット状態の表示コマンド	440
41.1 ソケット状態の表示	441

41.1.1	show socket	441
第 42 章	端末可視化機能の表示、クリア操作コマンド	443
42.1	端末可視化機能が検出した端末情報の表示	444
42.1.1	show devscan	444
42.1.2	show devscan mac	446
42.1.3	show devscan ip	448
42.1.4	show devscan hostname	450
42.1.5	show devscan description	452
42.1.6	show devscan unknown	454
42.2	端末可視化機能が検出した端末情報のクリア	455
42.2.1	clear devscan	455
第 43 章	NXconciierge エージェント機能の表示、クリア操作コマンド	456
43.1	NXconciierge エージェント機能の表示	457
43.1.1	show management-agent ca-certificate	457
43.1.2	show trace management-agent	458
43.2	NXconciierge エージェント情報のクリア	459
43.2.1	clear trace management-agent	459
第 44 章	DNS サーバ機能の表示コマンド	460
44.1	DNS サーバ機能の表示	461
44.1.1	show dns-resolver information	461
第 45 章	ポート制御コマンド	462
45.1	ポート制御	463
45.1.1	offline	463
45.1.2	online	465
第 46 章	無線 LAN 制御コマンド	467
46.1	無線 LAN 制御	468
46.1.1	wlanctl authenticator disconnect	468
第 47 章	USB ポート制御コマンド	470
47.1	USB ポート制御	471
47.1.1	usbctl	471
第 48 章	IEEE802.1X 制御コマンド	472
48.1	IEEE802.1X 制御	473
48.1.1	dot1xctl initialize	473
48.1.2	dot1xctl reconfirm	474
48.1.3	dot1xctl backup recovery	475
第 49 章	MAC アドレス認証制御コマンド	476
49.1	MAC アドレス認証制御	477
49.1.1	macauthctl initialize	477
第 50 章	RADIUS 制御コマンド	478
50.1	RADIUS 制御	479
50.1.1	radius recovery	479
第 51 章	定期ログ制御コマンド	480
51.1	定期ログ情報 FLASH メモリ格納制御	481
51.1.1	monitoringinfoctl collect	481
第 52 章	パケットキャプチャ制御コマンド	482
52.1	無線 LAN パケットキャプチャ制御コマンド	483
52.1.1	capturectl start ieee80211	483
52.1.2	capturectl stop ieee80211	484

52.1.3	capturectl remove ieee80211	485
52.1.4	capturectl start radius	486
52.1.5	capturectl stop radius	487
52.1.6	capturectl remove radius	488
第 53 章	I'm here コマンド	489
53.1	I'm here コマンド	490
53.1.1	iamhere	490
第 54 章	その他のコマンド	491
54.1	その他	492
54.1.1	ping	492
54.1.2	traceroute	494
54.1.3	telnet	496
第 55 章	commit コマンド実行時の影響について	497
第 56 章	SR-M50AP1 からの構成定義引継ぎについて	501
56.1	SR-M630AP1/610AP1 での未サポートコマンド	502
56.2	SR-M630AP1/610AP1 での未サポートパラメタ	506
56.3	SR-M630AP1/610AP1 にて動作仕様が変更となったコマンド	508
56.4	ハードウェア構成差分によりパラメタ変更が必要なコマンド	509
索引		510

第1章 パスワード情報の設定

1.1 パスワード情報

1.1.1 password admin set

[機能]

管理者パスワードの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

password admin set [<password> [encrypted]]

[オプション]

<password>

- ・ 省略
対話形式でパスワードを入力します。
- ・ パスワード
パスワードを、0x21, 0x23~0x7e の 64 文字以内の ASCII 文字列で指定します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)
- ・ 暗号化されたパスワード
show candidate-config、show running-config または show startup-config コマンドで表示される暗号化されたパスワードを encrypted と共に指定します。
show candidate-config、show running-config または show startup-config コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- ・ 暗号化パスワード指定
<password>に暗号化されたパスワードを指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本装置に管理者がログインするためのパスワードを設定します。
パスワードが推測されにくいように、8 文字以上で英字、数字、記号を混ぜたパスワードを設定してください。
パスワードを省略した場合は、対話形式でパスワードを入力できます。入力したパスワードは画面に表示されず、システムログ情報にも保存されないため、コマンド実行履歴出力の設定が有効な際もセキュリティ的に安全です。
対話形式でパスワードを入力する場合、入力文字を 1 文字削除する際は Delete キーを使用してください。
本コマンドは設定した直後に有効となります。
ログインユーザ名に admin、パスワードに本パスワードを入力すると、管理者クラスでログインでき、管理者クラス用コマンドを使用できます。

[注意]

管理者パスワードは必ず設定してください。管理者パスワードを設定していない場合、パスワードなしでログインできます。また、設定したパスワードは定期的に変更するようにしてください。
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、および設定を削除した場合、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。
show candidate-config、show running-config および show startup-config コマンドでは、暗号化されたパスワードが encrypted と共に表示されます。

[メッセージ]

Password:

<password>引数を省略した場合に表示されます。
パスワードを入力してください。
入力したパスワードは画面に表示されません。

Retype password:

<password>引数を省略した場合に表示されます。
再度、パスワードを入力してください。
入力したパスワードは画面に表示されません。

<ERROR> mismatched password

対話形式で2回入力したパスワードが一致しませんでした。
再度、パスワードの設定を行ってください。

<WARNING> weak admin's password: set the password

管理者パスワードが設定されていません。
管理者パスワードを設定してください。

<WARNING> weak admin's password: contain at least 8 characters

管理者パスワードが7文字以下です。
8文字以上の管理者パスワードを設定してください。

<WARNING> weak admin's password: contain a different kind of character

管理者パスワードが英字のみ、または数字のみです。
英字、数字、記号を混ぜて管理者パスワードを設定してください。
本メッセージは、ログイン時、およびload、discardコマンド実行時にも表示されます。

[未設定時]

管理者パスワードを設定しないものとみなされます。

1.1.2 password user set

[機能]

一般ユーザパスワードの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
password user set [<password> [encrypted]]
```

[オプション]

<password>

- ・ 省略
対話形式でパスワードを入力します。
- ・ パスワード
パスワードを、0x21, 0x23~0x7e の 64 文字以内の ASCII 文字列で指定します。
(入力可能な文字の一覧については、コマンドユーザズガイドを参照してください。)
- ・ 暗号化されたパスワード
show candidate-config、show running-config または show startup-config コマンドで表示される暗号化されたパスワードを encrypted と共に指定します。
show candidate-config、show running-config または show startup-config コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- ・ 暗号化パスワード指定
<password>に暗号化されたパスワードを指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本装置に一般ユーザがログインするためのパスワードを設定します。
パスワードが推測されにくいように、8 文字以上で英字、数字、記号を混ぜたパスワードを設定してください。
パスワードを省略した場合は、対話形式でパスワードを入力できます。入力したパスワードは画面に表示されず、システムログ情報にも保存されないため、コマンド実行履歴出力の設定が有効な際もセキュリティ的に安全です。

対話形式でパスワードを入力する場合、入力文字を 1 文字削除する際は Delete キーを使用してください。

本コマンドは設定した直後に有効となります。

ユーザ名に user、パスワードに本パスワードを入力すると、一般ユーザクラスでログインでき、一般ユーザクラス用コマンドを使用できます。

[注意]

設定したパスワードは定期的に変更するようにしてください。

一般ユーザパスワードを設定していない場合、一般ユーザクラスでログインすることはできません。

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、設定は行われますが、脆弱である旨の警告メッセージが表示されます。

ftp 接続時には、一般ユーザパスワードではログインできません。

また、show logging command コマンドでは管理者が実行したコマンドは表示されず、履歴番号は不連続になります。

show candidate-config、show running-config および show startup-config コマンドでは、暗号化されたパスワードが encrypted と共に表示されます。

[メッセージ]

Password:

<password>引数を省略した場合に表示されます。
パスワードを入力してください。
入力したパスワードは画面に表示されません。

Retype password:

<password>引数を省略した場合に表示されます。
再度、パスワードを入力してください。
入力したパスワードは画面に表示されません。

<ERROR> mismatched password

対話形式で2回入力したパスワードが一致しませんでした。
再度、パスワードの設定を行ってください。

<WARNING> weak user's password: contain at least 8 characters

一般ユーザパスワードが7文字以下です。
8文字以上の一般ユーザパスワードを設定してください。

<WARNING> weak user's password: contain a different kind of character

一般ユーザパスワードが英字のみ、または数字のみです。
英字、数字、記号を混ぜて一般ユーザパスワードを設定してください。
本メッセージは、ログイン時、および load、discard コマンド実行時にも表示されます。

[未設定時]

一般ユーザパスワードを設定しないものとみなされます。

1.1.3 password aaa

[機能]

ログインユーザの AAA 情報の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
password aaa <group_id>
```

[オプション]

<group_id>

- ・ AAA のグループ ID
AAA のグループ ID を、10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本装置にログインするときに参照する、AAA のグループ ID を指定します。

[注意]

管理者クラスでログインする場合は、管理者パスワード(password admin set)を必ず設定してください。設定していない場合はログインできません。

[未設定時]

AAA 情報を参照しないものとみなされます。

1.1.4 password authtype

[機能]

ログインユーザ認証の認証プロトコルの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
password authtype <authtype>
```

[オプション]

<authtype>

- chap_md5
認証プロトコルに MD5-CHAP を使用します。
- pap
認証プロトコルに PAP を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ログインユーザ認証の認証プロトコルを設定します。

[未設定時]

ログインユーザ認証の認証プロトコルとして MD5-CHAP が設定されたものとみなされます。

```
password authtype chap_md5
```

第 2 章 ポート情報の設定

- ポート定義番号の指定範囲

本章のコマンドの[オプション]に記載されている<number>(ether ポート定義番号)に指定する ether 定義の
通し番号(10進数)は、以下に示す範囲で指定してください。

範囲	機種
1~2	SR-M630AP1
1	SR-M610AP1

- ポート種別構成について

ether ポート定義番号に対応する、ポート種別の構成を以下に示します。

機種	100/1000/2.5GBASE-T	10/100/1000BASE-T
SR-M630AP1	ether 1	ether 2
SR-M610AP1	-	ether 1

2.1 ether 共通情報

2.1.1 ether use

[機能]

ether ポートの使用の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

ether <number> use <mode>

[オプション]

<number>

- ether ポート番号
使用するポート番号を、10 進数で指定します。

<mode>

ポートの使用モードを指定します。

- on
ether ポートを使用します。
- off
ether ポートを使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ether ポートの使用の設定を行います。

[未設定時]

ether ポートを使用するものとみなされます。

```
ether <number> use on
```

2.1.2 ether mode

[機能]

ether ポートの通信速度の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ether <number> mode <speed>
```

[オプション]

<number>

- ether ポート番号
使用するポート番号を、10 進数で指定します。

<speed>

通信速度

- auto
オートネゴシエーションにより通信速度を決定します。
- 2500
2.5Gbps 固定にします。(SR-M630AP1 のみ)
- 1000
1Gbps 固定にします。
- 100
100Mbps 固定にします。
- 10
10Mbps 固定にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ether ポートの通信速度の設定を行います。

100/1000/2.5GBASE-T ポートでは、auto/2500/1000 が設定可能です。(SR-M630AP1 のみ)

10/100/1000BASE-T ポートでは、auto/1000/100/10 が設定可能です。

[未設定時]

オートネゴシエーションモードが設定されたものとみなされます。

```
ether <number> mode auto
```

2.1.3 ether duplex

[機能]

ether ポートの全二重/半二重の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ether <number> duplex <duplex>
```

[オプション]

<number>

- ether ポート番号
使用するポート番号を、10 進数で指定します。

<duplex>

全二重/半二重モード

- full
全二重 (Full duplex) 固定で動作します。
- half
半二重 (Half duplex) 固定で動作します。

本コマンドは、ether mode コマンドで通信速度の固定値を指定した場合にだけ指定できます。
(通信速度を auto に設定すると、このコマンドの設定は無効になります。)

[動作モード]

構成定義モード (管理者クラス)

[説明]

ether ポートの全二重/半二重の設定を行います。

[注意]

- ether mode コマンドで 1000 および 2500 を指定した場合は、本コマンドの設定内容は無効となり、全二重モードで動作します。
- ether mode コマンドで auto を指定した場合は、本コマンドの設定内容は無効となり、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。

[未設定時]

全二重モードが設定されたものとみなされます。

```
ether <number> duplex full
```

2.1.4 ether mdi

[機能]

ether ポートの MDI の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

ether <number> mdi <mode>

[オプション]

<number>

- ether ポート番号
使用するポート番号を、10 進数で指定します。

<mode>

MDI のモードを指定します。

- auto
MDI/MDI-X 自動検出モードにします。
- mdi
MDI モード固定にします。
- mdix
MDI-X モード固定にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ether ポートの MDI のモードを設定します。

[注意]

- MDI/MDI-X 自動検出モードは、ether mode コマンドの設定が オートネゴシエーションの場合のみ有効となります。
(ether mode コマンドの設定が、100Mbps/10Mbps 固定の場合は無効となり、MDI 固定で動作します。)
- ether mode と ether mdi の設定に対する MDI 動作を以下に示します。

ether mdi 設定	auto	mdi	mdix
ether mode 設定			
auto	auto	mdi	mdix
2500, 1000	auto	mdi	mdix
100, 10	mdi	mdi	mdix

[未設定時]

MDI/MDI-X 自動検出モードが設定されたものとみなされます。

```
ether <number> mdi auto
```

2.1.5 ether flowctl

[機能]

ether ポートのフロー制御機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ether <number> flowctl <send> <receive>
```

[オプション]

<number>

- ether ポート番号
使用するポート番号を、10 進数で指定します。

<send>

- on
フロー制御パケットの送信を行います。
- off
フロー制御パケットの送信を行いません。

<receive>

- on
フロー制御パケットを受信した場合、フロー制御を行います。
- off
フロー制御パケットを受信した場合でも、フロー制御を行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ether ポートのフロー制御機能の動作を、送信機能と受信機能で設定します。
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、ether mode コマンドの通信速度によらず有効です。

[注意]

SR-M630AP1 の ether1 ポートでは、フロー制御機能は設定に関係なく動作しません (V20.05 版～)。

[未設定時]

フロー制御パケットを受信した場合のみ、フロー制御を行うように設定されたものとみなされます。

```
ether <number> flowctl off on
```

2.1.6 ether type

[機能]

ether ポートの種別の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ether <number> type normal
ether <number> type linkaggregation <group>
```

[オプション]

<number>

- ether ポート番号
使用するポート番号を、10 進数で指定します。

normal

通常ポート

linkaggregation

リンクアグリゲーション (SR-M630AP1 のみ)

<group>

- グループ番号
リンクアグリゲーショングループ番号を、10 進数で指定します。

範囲	機種
1	SR-M630AP1

[動作モード]

構成定義モード(管理者クラス)

[説明]

ether ポートのタイプを設定します。
通常ポートまたはリンクアグリゲーションから選択します。(SR-M630AP1 のみ)

[注意]

linkaggregation 指定時の注意

- リンクアグリゲーションは 1 ポートでは構成できません。
- ether duplex コマンドが半二重モードの場合は、リンクアグリゲーションは使用できません。
- リンクアグリゲーショングループ内のすべてのポートは、通信速度および VLAN を同じ設定にしてください。通信速度または VLAN の設定が異なる場合、ether2 ポートはリンクアップせず使用できません。システムログメッセージを参考に設定を変更してください。

[未設定時]

通常ポートが設定されたものとみなされます。

```
ether <number> type normal
```

2.1.7 ether vlan tag

[機能]

ether ポートの Tag あり VLAN 登録

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ether <number> vlan tag <tagged_vidlist>
```

[オプション]

<number>

- ether ポート番号
使用するポート番号を、10 進数で指定します。

<tagged_vidlist>

- tag 付き VLAN ID リスト
tag 付き VLAN ID を 1~4094 の 10 進数で指定します。
複数の VLAN ID を指定する場合は、","(カンマ)で区切ります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

Tagged VLAN ID の設定を行います。

[注意]

- 同一ポートに同じ VID を Tag 付き、Tag なしを設定した場合、Tag なしが優先されます。
- VLAN を追加登録する際には、すでに登録されている VLAN も含めた VLAN ID リストを指定してください。
- 高速転送モードを使用する場合(system bridge acceleration mode enable)、以下のコマンドで指定できる VLAN ID は合計で 24 個までです。24 個を超えて使用しないでください。

```
ether vlan tag  
ether vlan untag  
wlan vlan tag  
wlan vlan untag
```

[未設定時]

なし

2.1.8 ether vlan untag

[機能]

ether ポートの Tag なし VLAN 登録

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ether <number> vlan untag <untagged_vid>
```

[オプション]

<number>

- ether ポート番号
使用するポート番号を、10 進数で指定します。

<untagged_vid>

- tag なし VLAN ID
tag なし VLAN ID を 1~4094 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

Untagged VLAN ID の設定を行います。

[注意]

- 同一ポートに同じ VID を Tag 付き、Tag なしを設定した場合、Tag なしが優先されます。
- 高速転送モードを使用する場合(system bridge acceleration mode enable)、以下のコマンドで指定できる VLAN ID は合計で 24 個までです。24 個を超えて使用しないでください。

```
ether vlan tag
ether vlan untag
wlan vlan tag
wlan vlan untag
```

[未設定時]

ether vlan tag コマンドが設定されていない場合

VLAN ID として 1 が設定されたものとみなされます。

```
ether <number> vlan untag 1
```

ether vlan tag コマンドが設定されている場合

VLAN ID を設定しないものとみなされます。

2.1.9 ether downrelay wlan

[機能]

ether ポートのリンクダウンリレー機能（リンクインテグリティ）の連携動作無線 LAN インタフェースリストの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ether <number> downrelay wlan <wlanlist>
```

[オプション]

<number>

- ether ポート番号
使用するポート番号を、10 進数で指定します。

<wlanlist>

- 無線 LAN インタフェースリスト
本定義を設定した ether ポートがリンクダウンした場合に、連携して閉塞を行う無線 LAN インタフェースのリストを指定します。
複数の無線 LAN インタフェースを設定する場合、","(カンマ)で区切ります。
複数の無線 LAN インタフェースが続く場合、"-"(ハイフン)で区切ります(例:"1-16")。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本定義を設定した ether ポートがリンクダウンした場合に、連携して閉塞を行う無線 LAN インタフェースのリストを設定します。

リンクダウンリレー動作が行われた場合に、連携無線 LAN インタフェースが閉塞状態となりシステムログが出力されます。

[注意]

- ポートが閉塞状態の場合、online コマンドの閉塞解除指定でポート閉塞を解除してください。
- ether ポートの種別がリンクアグリゲーションであり、リンクアグリゲーションにリンクダウンリレー機能が設定されている場合、本定義は無効となります。
- リンクダウンリレー機能の連携動作無線 LAN インタフェースとして認証自動切替対象である無線 LAN インタフェースが指定された場合、認証自動切替対象であるすべての無線 LAN インタフェースが対象となります。

[未設定時]

無線 LAN インタフェースリスト情報を設定しないものとみなされ、リンクダウンリレー機能は動作しません。

2.1.10 ether downrelay recovery mode

[機能]

ether ポートのリンクダウンリレー機能（リンクインテグリティ）の閉塞解除動作の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ether <number> downrelay recovery mode <mode>
```

[オプション]

<number>

- ether ポート番号
使用するポート番号を、10 進数で指定します。

<mode>

連携動作ポートリストの閉塞解除動作を指定します。

- manual
コマンドで閉塞解除します。
- auto
リンクアップで自動的に閉塞解除します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

リンクダウンリレー機能で閉塞した無線 LAN インタフェースの復旧動作を設定します。
閉塞解除動作が manual の場合は、online コマンドによる復旧操作が必要となります。
閉塞解除動作が auto の場合は、リンクダウンリレー機能設定ポートのリンクアップで自動復旧します。
また、auto 時にリンクアップによる閉塞解除が行われた場合は、システムログを出力します。

[注意]

リンクダウンリレー機能を設定した ether ポートが閉塞状態の場合は、auto 設定時でもリンクアップ状態とはならないため、online コマンドによって閉塞状態を解除してください。

[未設定時]

連携動作無線 LAN インタフェースリストの閉塞解除動作に manual が設定されものとみなされます。

```
ether <number> downrelay recovery mode manual
```

2.1.11 ether description

[機能]

ether ポートの説明文の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ether <number> description <description>
```

[オプション]

<number>

- ・ ether ポート番号
使用するポート番号を、10 進数で指定します。

<description>

- ・ 説明文
この ether ポートの説明文を、0x21, 0x23~0x7e の 50 文字以内の ASCII 文字列で記入します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

この ether ポートについての説明文を記入します。

[未設定時]

説明文を記入しないものとみなされます。

2.1.12 ether icmpwatch address

[機能]

ether ポートのノード監視接続先アドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ether <number> icmpwatch address <dst_addr>
```

[オプション]

<number>

- ether ポート番号
使用するポート番号を、10 進数で指定します。

<dst_addr>

- ICMP ECHO パケットのあて先 IP アドレス
監視対象となる IP 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。
1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の監視を行うための動作情報を設定します。

<dst_addr>で指定したあて先 IP アドレスを使用して、経路情報に従い ICMP ECHO パケットを送信し、応答を受信することによって生存を確認します。

監視失敗となった場合、リンクダウンリレー機能（リンクインテグリティ）に連携します。

連携して閉塞を行う無線 LAN インタフェースは、ether downrelay wlan コマンドの設定に従います。

[注意]

- <dst_addr>には、自装置 IP アドレスを設定しないでください。
もし、上記のアドレスを指定した場合は、ノード監視機能は正常に動作しません。
- ether ポートの種別がリンクアグリゲーションであり、リンクアグリゲーションにノード監視機能が設定されている場合、本定義は無効となります。
"linkaggregation icmpwatch"にノード監視定義を設定してください。
- 本装置に IP アドレスが設定されていない場合、ノード監視機能は動作しません。

[未設定時]

ノード監視機能を利用しないものとみなされます。

2.1.13 ether icmpwatch interval

[機能]

ether ポートのノード監視の各種インターバルの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ether <number> icmpwatch interval <normal> <error> <timeout> [<retry>]
```

[オプション]

<number>

- ether ポート番号
使用するポート番号を、10 進数で指定します。

<normal>

- ICMP ECHO パケットの正常時送信間隔
ICMP ECHO パケットの正常時送信間隔を、1 秒～3600 秒(1 時間)の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどちらかを指定します。

<error>

- ICMP ECHO パケットの異常時送信間隔
ICMP ECHO パケットの異常時送信間隔を、1 秒～3600 秒(1 時間)の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどちらかを指定します。

<timeout>

- 監視タイムアウト
監視失敗とみなすまでのタイムアウト時間を、5～180 秒(3 分)の範囲で指定します。
単位は、m(分)、s(秒)のどちらかを指定します。

<retry>

- ICMP ECHO パケットの再送間隔
ICMP ECHO パケットの正常時送信に対して応答がないときの ICMP ECHO パケットの再送間隔を、1 秒～<timeout>-1 秒の範囲で指定します。
単位は、m(分)、s(秒)のどちらかを指定します。
省略時は、1s が指定されたものとして動作します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。

指定したあて先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。

ICMP ECHO パケットの応答が正常に受信できている間は正常時送信間隔で監視を行いますが、ICMP ECHO パケットの応答が受信できなくなると、障害発生とみなし、異常時送信間隔で監視を行います。

ICMP ECHO パケットの応答が受信できたときを復旧とみなし、正常時送信間隔での監視に戻ります。

[未設定時]

正常時送信間隔 10 秒、異常時送信間隔 1 分、監視タイムアウト 5 秒、再送間隔 1 秒が指定されたものとして動作します。

```
ether <number> icmpwatch interval 10s 1m 5s 1s
```

第3章 リンクアグリゲーション情報の設定

- ・リンクアグリゲーショングループ番号の指定範囲

本章のコマンドの[オプション]に記載されている<group>(リンクアグリゲーショングループ番号)に指定するグループの通し番号(10進数)は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
1	SR-M630AP1

3.1 リンクアグリゲーション情報

3.1.1 linkaggregation algorithm

[機能]

リンクアグリゲーションの負荷分散アルゴリズムの設定

[適用機種]

SR-M630AP1

[入力形式]

```
linkaggregation <group> algorithm <type>
```

[オプション]

<group>

- ・ リンクアグリゲーショングループ番号
使用するグループ番号を、10進数で指定します。

<type>

負荷分散アルゴリズムを指定します。

- ・ 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
- ・ both-mac-ip
送信元 MAC アドレス、送信先 MAC アドレス、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
- ・ both-ip-port
送信元 IP アドレス、送信先 IP アドレス、送信元ポート番号と送信先ポート番号の XOR による振り分け

[動作モード]

構成定義モード(管理者クラス)

[説明]

リンクアグリゲーションのグループごとにアルゴリズムを設定します。

[未設定時]

リンクアグリゲーションの負荷分散アルゴリズムに both-mac が設定されたものとみなされます。

```
linkaggregation <group> algorithm both-mac
```

3.1.2 linkaggregation mode

[機能]

リンクアグリゲーションの動作モード設定

[適用機種]

SR-M630AP1

[入力形式]

```
linkaggregation <group> mode <la_mode>
```

[オプション]

<group>

- ・ リンクアグリゲーショングループ番号
使用するグループ番号を、10進数で指定します。

<la_mode>

- ・ リンクアグリゲーション動作モード
以下の動作モードを設定します。

static

静的動作

active

LACP を使用した動的な active 動作

[動作モード]

構成定義モード(管理者クラス)

[説明]

リンクアグリゲーションの動作モードを設定します。

static を指定した場合は、LACP を使用しない静的なリンクアグリゲーションを構成します。

active を指定した場合は、LACP を使用した動的なリンクアグリゲーションです。

[未設定時]

リンクアグリゲーションの動作モードに static が設定されたものとみなされます。

```
linkaggregation <group> mode static
```

3.1.3 linkaggregation lacp-timeout

[機能]

リンクアグリゲーションの LACP タイムアウトの設定

[適用機種]

SR-M630AP1

[入力形式]

```
linkaggregation <group> lacp-timeout <mode>
```

[オプション]

<group>

- ・ リンクアグリゲーショングループ番号
使用するグループ番号を、10 進数で指定します。

<mode>

タイムアウト時間を指定します。

- ・ long
90 秒
- ・ short
3 秒

[動作モード]

構成定義モード(管理者クラス)

[説明]

相手装置から受信した LACP パケットを無効とみなすまでのタイムアウト時間を設定します。
long に設定した場合は 90 秒(30 秒×3 回)、short に設定した場合は 3 秒(1 秒×3 回)となります。

[未設定時]

リンクアグリゲーションの LACP タイムアウトに long が設定されたものとみなされます。

```
linkaggregation <group> lacp-timeout long
```

3.1.4 linkaggregation downrelay wlan

[機能]

リンクアグリゲーションのリンクダウンリレー機能（リンクインテグリティ）の連携動作無線 LAN インタフェースリストの設定

[適用機種]

SR-M630AP1

[入力形式]

```
linkaggregation <group> downrelay wlan <wlanlist>
```

[オプション]

<group>

- ・ リンクアグリゲーショングループ番号
使用するグループ番号を、10 進数で指定します。

<wlanlist>

- ・ 無線 LAN インタフェースリスト
本定義を設定した ether ポートがリンクダウンした場合に、連携して閉塞を行う無線 LAN インタフェースのリストを指定します。
複数の無線 LAN インタフェースを設定する場合、","(カンマ)で区切ります。
複数の無線 LAN インタフェースが続く場合、"-"(ハイフン)で区切ります(例:"1-16")。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本定義を設定したリンクアグリゲーションがリンクダウンした場合に、連携して閉塞を行う無線 LAN インタフェースのリストを設定します。

リンクダウンリレー動作が行われた場合に、連携無線 LAN インタフェースが閉塞状態となりシステムログが出力されます。

[注意]

- ・ ether ポートの種別がリンクアグリゲーションポートで、設定しているリンクアグリゲーショングループに本定義が設定されている場合、本定義が有効となり、ether ポートに設定されているリンクダウンリレー機能は無視されます。
- ・ ポートが閉塞状態の場合、online コマンドの閉塞解除指定でポート閉塞を解除してください。
- ・ リンクダウンリレー機能の連携動作無線 LAN インタフェースとして認証自動切替対象である無線 LAN インタフェースが指定された場合、認証自動切替対象であるすべての無線 LAN インタフェースが対象となります。
- ・ リンクアグリゲーションインタフェースは、物理ポートがリンクアップすることでリンクアップ状態となります。
LACP を利用する場合で、接続装置とのネゴシエーションが未確立な状態においてもインタフェース状態はリンクアップ状態となります。
そのため LACP を利用するリンクアグリゲーションインタフェースにてリンクインテグリティ機能を使用する場合は、linkaggregation icmpwatch address コマンドの設定が必要となります。

[未設定時]

無線 LAN インタフェースリスト情報を設定しないものとみなされ、リンクダウンリレー機能は動作しません。

3.1.5 linkaggregation downrelay recovery mode

[機能]

リンクアグリゲーションのリンクダウンリレー機能（リンクインテグリティ）の閉塞解除動作の設定

[適用機種]

SR-M630AP1

[入力形式]

```
linkaggregation <group> downrelay recovery mode <mode>
```

[オプション]

<group>

- ・ リンクアグリゲーショングループ番号
使用するグループ番号を、10進数で指定します。

<mode>

連携動作ポートリストの閉塞解除動作を指定します。

- ・ manual
コマンドで閉塞解除します。
- ・ auto
リンクアップで自動的に閉塞解除します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

リンクダウンリレー機能で閉塞した無線 LAN インタフェースの復旧動作を設定します。
閉塞解除動作が manual の場合は、online コマンドによる復旧操作が必要となります。
閉塞解除動作が auto の場合は、リンクダウンリレー機能設定ポートのリンクアップで自動復旧します。
また、auto 時にリンクアップによる閉塞解除が行われた場合は、システムログを出力します。

[注意]

リンクダウンリレー機能を設定した ether ポートが閉塞状態の場合は、auto 設定時でもリンクアップ状態とはならないため、online コマンドによって閉塞状態を解除してください。

[未設定時]

連携動作無線 LAN インタフェースリストの閉塞解除動作に manual が設定されものとみなされます。

```
linkaggregation <group> downrelay recovery mode manual
```

3.1.6 linkaggregation icmpwatch address

[機能]

リンクアグリゲーションのノード監視接続先アドレスの設定

[適用機種]

SR-M630AP1

[入力形式]

```
linkaggregation <group> icmpwatch address <dst_addr>
```

[オプション]

<group>

- ・ リンクアグリゲーショングループ番号
使用するグループ番号を、10 進数で指定します。

<dst_addr>

- ・ 監視接続先 IP アドレス
監視対象となる IP 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。
1. 0. 0. 1 ~ 126. 255. 255. 254
128. 0. 0. 1 ~ 191. 255. 255. 254
192. 0. 0. 1 ~ 223. 255. 255. 254

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の監視を行うための動作情報を設定します。

<dst_addr>で指定したあて先 IP アドレスを使用して、経路情報に従い ICMP ECHO パケットを送信し、応答を受信することによって生存を確認します。

監視失敗となった場合、リンクダウンリレー機能（リンクインテグリティ）に連携します。

連携して閉塞を行う無線 LAN インタフェースは、linkaggregation downrelay wlan コマンドの設定に従います。

[注意]

- ・ ether ポートの種別がリンクアグリゲーションポートで、設定しているリンクアグリゲーショングループに本定義が設定されている場合、本定義が有効となり、ether ポートに設定されているノード監視機能は無視されます。
- ・ <dst_addr>には、自装置 IP アドレスを設定しないでください。
もし、上記のアドレスを指定した場合は、ノード監視機能は正常に動作しません。
- ・ 本装置に IP アドレスが設定されていない場合、ノード監視機能は動作しません。
- ・ リンクアグリゲーションインタフェースは、物理ポートがリンクアップすることでリンクアップ状態となります。
LACP を利用する場合で、接続装置とのネゴシエーションが未確立な状態においてもインタフェース状態はリンクアップ状態となります。
そのため LACP を利用するリンクアグリゲーションインタフェースにてリンクインテグリティ機能を使用する場合は、本コマンドの設定が必要となります。

[未設定時]

リンクアグリゲーションでのノード監視機能を利用しないものとみなされます。

3.1.7 linkaggregation icmpwatch interval

[機能]

リンクアグリゲーションのノード監視の各種インターバルの設定

[適用機種]

SR-M630AP1

[入力形式]

```
linkaggregation <group> icmpwatch interval <normal> <error> <timeout> [<retry>]
```

[オプション]

<group>

- ・ リンクアグリゲーショングループ番号
使用するグループ番号を、10進数で指定します。

<normal>

- ・ ICMP ECHO パケットの正常時送信間隔
ICMP ECHO パケットの正常時送信間隔を、1秒～3600秒(1時間)の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどちらかを指定します。

<error>

- ・ ICMP ECHO パケットの異常時送信間隔
ICMP ECHO パケットの異常時送信間隔を、1秒～3600秒(1時間)の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどちらかを指定します。

<timeout>

- ・ 監視タイムアウト
監視失敗とみなすまでのタイムアウト時間を、5秒～180秒(3分)の範囲で指定します。
単位は、m(分)、s(秒)のどちらかを指定します。

<retry>

- ・ ICMP ECHO パケットの再送間隔
ICMP ECHO パケットの正常時送信に対して応答がないときの ICMP ECHO パケットの再送間隔を、1秒～<timeout>-1秒の範囲で指定します。
単位は、m(分)、s(秒)のどちらかを指定します。
省略時は、1s が指定されたものとして動作します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

接続先の生存確認を行うための動作情報を設定します。

指定したあて先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。

ICMP ECHO パケットの応答が正常に受信できている間は正常時送信間隔で監視を行いますが、ICMP ECHO パケットの応答が受信できなくなると、障害発生とみなし、異常時送信間隔で監視を行います。

ICMP ECHO パケットの応答が受信できたときを復旧とみなし、正常時送信間隔での監視に戻ります。

[未設定時]

正常時送信間隔 10 秒、異常時送信間隔 1 分、監視タイムアウト 5 秒、再送間隔 1 秒が指定されたものとして動作します。

```
linkaggregation <group> icmpwatch interval 10s 1m 5s 1s
```

第 4 章 無線 LAN モジュール情報の設定

- ieee80211 定義番号の指定範囲

本章のコマンドの[オプション]に記載されている<number>(ieee80211 定義番号)に指定する ieee80211 定義の通し番号(10 進数)は、以下に示す範囲で指定してください。

また本装置で設定できる無線 LAN モジュール番号と、無線 LAN 周波数帯の対応は以下のとおりです。

機種	範囲	無線 LAN モジュール番号	無線 LAN 周波数帯
SR-M630AP1	1~3	ieee80211 1	2.4GHz
		ieee80211 2	5GHz (W52, W53)
		ieee80211 3	5GHz (W56)
SR-M610AP1	1~2	ieee80211 1	2.4GHz
		ieee80211 2	5GHz (W52, W53, W56)

4.1 無線 LAN モジュール情報

4.1.1 ieee80211 use

[機能]

無線 LAN モジュールの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

ieee80211 <number> use <mode>

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<mode>

- on
無線 LAN モジュールを使用します。
- off
無線 LAN モジュールを使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線 LAN モジュールを使用するかどうかを設定します。

無線 LAN モジュール番号、無線 LAN インタフェースの最大値、無線 LAN インタフェース番号の関係は以下のように定義付けられています。

SR-M630AP1 を屋外で使用する場合は、W52, W53 の周波数帯を使用できないため、ieee80211 2 use off としてください。

無線 LAN モジュール番号	無線 LAN インタフェースの最大値	無線 LAN インタフェース番号
ieee80211 1	8	wlan 1~8
	16	wlan 1~16
ieee80211 2	8	wlan 9~16
	16	wlan 17~32
ieee80211 3 ※SR-M630AP1 のみ	8	wlan 17~24
	16	wlan 33~48

[未設定時]

無線 LAN モジュールを使用しないものとみなされます。

```
ieee80211 <number> use off
```

4.1.2 ieee80211 mode

[機能]

無線通信モードの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

ieee80211 <number> mode <mode>

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<mode>

- 11b
IEEE802.11b で通信を行います。
- 11b/g
IEEE802.11b または IEEE802.11g で通信を行います。
- 11b/g/n
IEEE802.11b、IEEE802.11g または IEEE802.11n で通信を行います。
- 11b/g/n/ax
IEEE802.11b、IEEE802.11g、IEEE802.11n または IEEE802.11ax で通信を行います。
- 11g
IEEE802.11g で通信を行います。
- 11g/n
IEEE802.11g または IEEE802.11n で通信を行います。
- 11g/n/ax
IEEE802.11g、IEEE802.11n または IEEE802.11ax で通信を行います。
- 11a
IEEE802.11a で通信を行います。
- 11a/n
IEEE802.11a または IEEE802.11n で通信を行います。
- 11a/n/ac
IEEE802.11a、IEEE802.11n または IEEE802.11ac で通信を行います。
- 11a/n/ac/ax
IEEE802.11a、IEEE802.11n、IEEE802.11ac または IEEE802.11ax で通信を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線通信モードの IEEE802.11a/b/g/n/ac/ax を設定します。

[注意]

11a、11a/n、11a/n/ac または 11a/n/ac/ax の W53(52、56、60、64)チャンネル、W56(100、104、108、112、116、120、124、128、132、136、140、144)チャンネルを設定した場合、DFS 機能のレーダ検出が作動するため通信可能状態になるまで 1 分間かかります。

また、設定した<channel>でレーダを検出したときは、ほかのチャンネルに変更され、レーダを検出したチャンネルは、以後 30 分間使用できなくなります。

[未設定時]

無線通信モードを設定しないものとみなされます。

4.1.3 ieee80211 channel

[機能]

無線 LAN チャンネルの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

ieee80211 <number> channel <channel>

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<channel>

- チャンネル番号
使用する無線 LAN チャンネル番号を 10 進数で指定します。
無線モジュール番号が 1 (2.4GHz 帯) の場合、1~13 の範囲で指定します。
無線モジュール番号が 2 または 3 (5GHz 帯) の場合、以下の中から指定します。

周波数帯	チャンネル番号
W52	36、40、44、48
W53	52、56、60、64
W56	100、104、108、112、116、120、124、128、132、136、140、144

- any
自動で選択されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線 LAN で使用するチャンネルを設定します。
帯域幅に 40、80 を設定した場合、プライマリチャンネルとなる番号を指定します。

[注意]

ノイズ回避機能(ieee80211 noise-detect use)を有効にしている場合は、本設定で行ったチャンネルと異なるチャンネルに変更される場合があります。
5GHz 帯のチャンネルで屋外を使用する場合は、W56 の範囲に限定して運用下さい。
無線 LAN インタフェースの動作タイプに wds-sta が設定された無線モジュールは、本設定は無効になります。
wds-sta が接続された wds-ap のチャンネルが動作チャンネルとなります。
チャンネル番号を any (自動選択) に設定した場合、本装置では混雑の少ない周波数帯を自動選択するため、特に W56 の周波数帯では 144 チャンネルが積極的に選ばれることがあります。無線端末側の 144 チャンネル対応状況によっては接続できない場合がありますので、その場合は ieee80211 144ch-support コマンドで 144 チャンネルを無効にしてお使いください。

[未設定時]

無線 LAN チャンネルに any が設定されたものとみなされます。

ieee80211 <number> channel any

4.1.4 ieee80211 bandwidth

[機能]

帯域幅の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

ieee80211 <number> bandwidth <width>

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<width>

- 20
20MHz の帯域幅を使用します。
- 40
40MHz の帯域幅を使用します。
- 80
80MHz の帯域幅を使用します。
本設定は無線モジュール番号が 2 または 3 (5GHz 帯) でのみ有効になります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線 LAN モジュールの帯域幅を指定します。各無線 LAN モジュールごとに独立した設定が可能です。チャンネルボンディング機能を使用する場合は帯域幅 40 以上を設定してください。本設定は 11n、11ac、11ax の無線方式で有効となります。

40MHz の帯域幅を使用する場合、セカンダリチャンネルオフセットの設定が必要となります。

[未設定時]

20MHz の帯域幅を設定 (チャンネルボンディング機能を使用しない) とみなされます。

```
ieee80211 <number> bandwidth 20
```

4.1.5 ieee80211 secondary-channel

[機能]

セカンダリチャンネルオフセットの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

ieee80211 <number> secondary-channel <offset>

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<offset>

- above
セカンダリチャンネルとしてプライマリチャンネルより大きいチャンネル番号を使用します。
- below
セカンダリチャンネルとしてプライマリチャンネルより小さいチャンネル番号を使用します。
- auto
設定したプライマリチャンネルに応じて above 設定か below 設定かを自動的に判定します。
なお帯域幅に 20 を設定した場合はセカンダリチャンネルを使用しないものと判定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

帯域幅に 40 を設定した場合に使用するセカンダリチャンネルを、プライマリチャンネル番号のオフセットとして指定します。

プライマリチャンネル番号(無線 LAN チャンネル番号)とセカンダリチャンネルオフセットが有効となる組み合わせは以下のとおりです。

周波数帯	プライマリ チャンネル番号	セカンダリチャンネル オフセット	セカンダリ チャンネル番号
2.4GHz	1	above	5
	2	above	6
	3	above	7
	4	above	8
	5	above	9
	6	below	1
		above	10
	7	below	2
		above	11
	8	below	3
		above	12
9	below	4	
	above	13	
10	below	5	
	above	6	
11	below	7	

周波数帯	プライマリ チャンネル番号	セカンダリチャンネル オフセット	セカンダリ チャンネル番号
	12	below	8
	13	below	9
W52	36	above	40
	40	below	36
	44	above	48
	48	below	44
W53	52	above	56
	56	below	52
	60	above	64
	64	below	60
W56	100	above	104
	104	below	100
	108	above	112
	112	below	108
	116	above	120
	120	below	116
	124	above	128
	128	below	124
	132	above	136
	136	below	132
	140	above	144
	144	below	140

auto 設定した場合は上記で設定したプライマリチャンネル番号に応じたセカンダリチャンネルオフセットを自動選択します。なお、セカンダリチャンネルオフセットを auto に設定しても、プライマリチャンネル番号を 5~7 に設定した場合は above、プライマリチャンネル番号を 8、9 に設定した場合は below のセカンダリチャンネル番号が選択されます。

[注意]

ieee80211 mode <mode>で、11b/g/n、11b/g/n/ax、11g/n、11g/n/ax、11a/n、11a/n/ac、11a/n/ac/ax を使用、かつ ieee80211 bandwidth <width>で 40 が設定されているときに意味を持ちます。

有効な組み合わせ以外では、無線 LAN アクセスポイントとして動作しません。

無線 LAN チャンネルの設定を any 設定した場合は本設定は必ず auto に設定してください。

[未設定時]

セカンダリチャンネルオフセットに auto が設定されたものとみなされます。

```
ieee80211 <number> secondary-channel auto
```

4.1.6 ieee80211 chanlist

[機能]

スキャンチャンネルリストの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> chanlist <band>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。
本コマンドでは"2"のみ設定可能です。

<band>

- 周波数帯
スキャンを行う 5GHz 帯の周波数帯を以下の中から指定します。
複数指定する場合は、","(カンマ)で区切ります(例: "w52, w53")。

w52

W52 の周波数帯のチャンネルをスキャン対象とする場合に指定します。

w53

W53 の周波数帯のチャンネルをスキャン対象とする場合に指定します。

w56

W56 の周波数帯のチャンネルをスキャン対象とする場合に指定します。
指定する周波数帯(w52、w53、w56)に対応するチャンネル番号は以下のとおりです。

周波数帯	チャンネル番号
W52	36、40、44、48
W53	52、56、60、64
W56	100、104、108、112、116、120、124、128、132、136、140、144

SR-M630AP1 において、ieee80211 2 use on とした場合、以下の設定が可能です。

機種名	設定例	スキャン対象とするチャンネル
SR-M630AP1	ieee80211 2 chanlist w52	36、40、44、48
	ieee80211 2 chanlist w53	52、56、60、64
	未設定	36、40、44、48、52、56、60、64

SR-M630AP1 において、ieee80211 3 use on とした場合、必ず W56 の全チャンネル番号がスキャン対象となります。

SR-M610AP1 において、ieee80211 2 use on とした場合、以下の設定が可能です。

機種名	設定例	スキャン対象とするチャンネル
SR-M610AP1	ieee80211 2 chanlist w52	36、40、44、48
	ieee80211 2 chanlist w53	52、56、60、64
	ieee80211 2 chanlist w56	100、104、108、112、116、120、124、128、132、136、140、144

機種名	設定例	スキャン対象とするチャンネル
	ieee80211 2 chanlist w52, w53	36、40、44、48、52、56、60、64
	ieee80211 2 chanlist w52, w56	36、40、44、48、100、104、108、112、116、 120、124、128、132、136、140、144
	ieee80211 2 chanlist w53, w56	52、56、60、64、100、104、108、112、116、 120、124、128、132、136、140、144
	未設定	36、40、44、48、52、56、60、64、100、104、 108、112、116、120、124、128、132、136、 140、144

[動作モード]

構成定義モード(管理者クラス)

[説明]

スキャンを行う 5GHz 帯の周波数帯を設定します。周波数帯を設定することにより、運用周波数帯を指定することができます。

[注意]

無線 LAN チャンネル番号に any 以外を設定している場合、本設定は無効になります。

本設定は 5GHz 側でのみ有効になります。

本装置を屋外でご使用になる場合は、5GHz 帯の無線 LAN モジュールは W56 の範囲に限定して運用してください。

DFS 機能がレーダを検出した場合、指定された範囲外の周波数帯に移動する場合があります。

屋外で使用する場合は注意してください。

[未設定時]

スキャンチャンネルリストを設定しないものとみなされます。

4.1.7 ieee80211 sta limit

[機能]

接続可能台数の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> sta limit <limit>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<limit>

- 接続可能台数
接続できる無線 LAN 端末台数を 1~118 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した無線 LAN モジュールに接続できる無線 LAN 端末台数の最大数を設定します。

ここで設定した接続可能台数を超えて無線 LAN 端末からの要求を受けると、アクセスポイントは無線 LAN 端末からの Authentication 要求を失敗させます。

接続可能台数は、指定した無線 LAN モジュールの仮想アクセスポイントすべてに設定されている最低保証台数の合計よりも多くなるように設定してください。

[注意]

最低保証台数が設定されていた場合、最低保証台数分は接続可能台数から確保されます。そのため、ここで設定した接続可能台数に到達する前に無線 LAN 端末からの Authentication 要求を失敗させることがあります。

最低保証されていない接続可能な無線 LAN 端末台数を増やすには、接続可能台数の設定値を増やしてください。

[未設定時]

接続可能台数に 50 が設定されたものとみなされます。

```
ieee80211 <number> sta limit 50
```

4.1.8 ieee80211 protection mode

[機能]

11g プロテクションモードの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> protection mode <mode>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<mode>

- cts
CTS 制御フレームを使用して衝突回避します。
- rtscts
RTS/CTS 制御フレームを使用して衝突回避します。
- disable
プロテクション機能を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

11b/11g 混在環境でのプロテクション(衝突回避)の設定を行います。
11b で動作する無線 LAN 端末やアクセスポイントが存在する環境では、フレームの衝突を軽減できます。

[未設定時]

11g プロテクションモードに rtscts が設定されたものとみなされます。

```
ieee80211 <number> protection mode rtscts
```

4.1.9 ieee80211 rts threshold

[機能]

RTS しきい値の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> rts threshold <length>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<length>

RTS 制御フレームを送信するしきい値を 1~2346 (byte) の 10 進数で指定します。
しきい値には FCS (4byte) が含まれます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

RTS/CTS に利用される RTS 制御フレームを送信するしきい値を設定します。

RTS/CTS は、隠れ端末問題と呼ばれる無線 LAN 上でフレーム衝突が発生する問題を回避するために、IEEE802.11 で規定されている仕組みです。

運用中に隠れ端末問題により通信性能問題が生じていて、設置環境の変更ができない場合に限り、本設定を変更してください。

本装置が無線 LAN 上に送信できるフレーム長は最大 1,536 バイトです。実際に送信されるフレーム長より本設定値を小さくすることで、RTS が送信されるようになります。ただし、A-MPDU として送信されるフレームは RTS スレッシュホールドによる制御の対象外となります。

[注意]

RTS しきい値を小さくすると制御フレームが極端に増加してスループットが低下したり、通信が不安定になったりする場合があります。256 バイト以上を推奨します。

[未設定時]

RTS しきい値に 2346 が設定されたものとみなされます。

```
ieee80211 <number> rts threshold 2346
```

4.1.10 ieee80211 dtim period

[機能]

DTIM 間隔の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> dtim period <period>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<period>

DTIM を付加するビーコンを送信する間隔を 1~15 の 10 進数で指定します。
1 を指定した場合、すべてのビーコンに DTIM を付加します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

DTIM を付加するビーコンを送信する間隔を設定します。
運用で問題が生じていない場合は、本設定を変更しないで運用してください。

[注意]

DTIM 間隔を大きくすることで接続する無線 LAN 端末の省電力状態の時間を長くすることができますが、通信時のレスポンスが低下する場合があります。

[未設定時]

DTIM 間隔に 1 が設定されたものとみなされます。

```
ieee80211 <number> dtim period 1
```

4.1.11 ieee80211 beacon interval

[機能]

ビーコン間隔の設定

※ ソフトウェア V20.03 まで未サポート

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

ieee80211 <number> beacon interval <interval>

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<interval>

ビーコンの送出間隔を 100~1000(1.024 ミリ秒単位)の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ビーコンの送出間隔を設定します。

運用で問題が生じていない場合は、本設定を変更しないで運用してください。

[注意]

無線インタフェースの数が多くなるとビーコン送信データのエアタイム占有率が上がり、データ通信に影響を与えます。そのため、2.4GHz 帯では無線インタフェースの数が 9 以上で、かつビーコンの送出間隔が 200 以下に設定された場合は 200(204.8msec)に設定されたものとみなされます。

[未設定時]

ビーコン送出間隔に 100 が設定されたものとみなされます。

```
ieee80211 <number> beacon interval 100
```

4.1.12 ieee80211 wmm mode

[機能]

WMM 優先制御の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> wmm mode <mode>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<mode>

- enable
WMM 優先制御を有効にします。
- disable
WMM 優先制御を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

WMM 優先制御をサポートする無線 LAN 端末または無線 LAN アクセスポイントへのパケットを、AC_VO(音声)、AC_VI(ビデオ)、AC_BE(ベストエフォート)、AC_BK(バックグラウンド)の4つのAC(Access Category)に分類し、優先制御して転送します。

[注意]

WMM 優先制御を行う対象は、WMM が有効となっている無線 LAN 端末または無線 LAN アクセスポイントに対してのみであり、WMM をサポートしていないか、無効となっている無線 LAN 端末または無線 LAN アクセスポイントへのパケットは常に AC_BE に分類されます。

WMM が無効の場合、11b、11b/g、11g、11a 通信モードで動作します。

[未設定時]

WMM 優先制御を有効が設定されたものとみなされます。

```
ieee80211 <number> wmm mode enable
```

4.1.13 ieee80211 wmm ack

[機能]

WMM 優先制御での ACK 応答要求の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> wmm ack <category> <mode>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<category>

- voice
AC_VO に対する ACK 応答要求を設定します。
- video
AC_VI に対する ACK 応答要求を設定します。
- besteffort
AC_BE に対する ACK 応答要求を設定します。
- background
AC_BK に対する ACK 応答要求を設定します。

<mode>

- enable
送信したデータフレームに対する ACK 応答を必要とします。
- disable
送信したデータフレームに対する ACK 応答を不要とします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

WMM 優先制御をサポートする無線 LAN 端末、または無線 LAN アクセスポイントへ送信するデータフレームに対する ACK の応答要否を AC (Access Category) ごとに設定します。

[注意]

WMM 優先制御を使用しないときは無効となります。

[未設定時]

すべての AC で ACK 応答が必要と設定されたものとみなされます。

```
ieee80211 <number> wmm ack <category> enable
```

4.1.14 ieee80211 apscan mode

[機能]

周辺アクセスポイント検出の動作モード設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

ieee80211 <number> apscan mode <mode>

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<mode>

- enable
周辺アクセスポイント検出機能を有効にします。
- disable
周辺アクセスポイント検出機能を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

周辺アクセスポイント検出の動作モードを設定します。

[未設定時]

周辺アクセスポイント検出の動作モードを無効にするものとみなされます。

```
ieee80211 <number> apscan mode disable
```

4.1.15 ieee80211 apscan expire

[機能]

周辺アクセスポイント情報の保持期間設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> apscan expire <expire>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<expire>

- 周辺アクセスポイント情報の保持期間
周辺アクセスポイント情報の保持期間を 1 分～1 日の範囲で指定します。
単位は、d (日)、h (時)、m (分)、s (秒) のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

検出した周辺アクセスポイント情報の保持期間を設定します。

[未設定時]

周辺アクセスポイント情報の保持期間に 1h が設定されたものとみなされます。

```
ieee80211 <number> apscan expire 1h
```

4.1.16 ieee80211 txpower

[機能]

無線送信出力の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

ieee80211 <number> txpower <power>

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<power>

無線送信出力を dbm をつけて直接指定します。

指定された値がそのまま実際の送信出力[dBm]となります。

設定可能範囲は 1dbm~23dbm です。

各通信モードの上限値を超える値を設定した場合、モードごとにそれぞれの上限値での出力となります。

各通信モードの上限値の目安は表を参照してください。

mode				送信電力 (dBm)	
				SR-M610AP1	SR-M630AP1
2.4GHz	11b			18	18
				21	20
	11n	[20MHz]		21	20
				21	19
	11ax	[20MHz]	21	20	
		[40MHz]	20	20	
5GHz	11a	W52/W53	[20MHz]	16	16
		W56	[20MHz]	21	21
	11n	W52/W53	[20MHz]	16	16
			[40MHz]	16	16
		W56	[20MHz]	21	21
			[40MHz]	20	20
	11ac	W52/W53	[20MHz]	16	16
			[40MHz]	16	16
			[80MHz]	16	16
		W56	[20MHz]	21	21
			[40MHz]	20	20
			[80MHz]	20	20
	11ax	W52/W53	[20MHz]	16	16
			[40MHz]	16	16
			[80MHz]	16	16

mode				送信電力 (dBm)	
				SR-M610AP1	SR-M630AP1
		W56	[20MHz]	21	21
			[40MHz]	20	20
			[80MHz]	21	20

表内の数値は以下の内訳です。

- ・ アンテナゲインは含みません。
- ・ アンテナコネクタ端の出力です。
- ・ 全モード、アンテナコネクタ 2 本分の合成電力です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

フレーム送信で使用する無線送信出力を設定します。

[注意]

実際の送信出力設定値は、無線 LAN モジュール状態表示コマンド(show ieee80211 status)で確認できます。

[未設定時]

無線送信出力の設定に 23dbm が設定されたものとみなされます。

```
ieee80211 <number> txpower 23dbm
```

4.1.17 ieee80211 supportrate

[機能]

無線通信時に使用するサポートレートの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

ieee80211 <number> supportrate <rate_list>

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<rate_list>

- サポートするレートのリスト
サポートレート(1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54)を 10 進数で指定します。
複数のレートを指定する場合は、","(カンマ)で区切ります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本装置がサポートするレートを設定します。

コマンドで設定した範囲の値でビーコンにて通知、および、接続時のネゴシエーションを行い、無線 LAN 端末との通信時に使用するレートを決定します。

無線通信モードの設定値に応じて、設定できるサポートレートは以下となります。

無線 LAN モジュール番号	無線通信モード	サポートレート
ieee80211 1	11b	1, 2, 5.5, 11
	11g, 11g/n, 11g/n/ax	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
	11b/g, 11b/g/n, 11b/g/n/ax	
ieee80211 2	11a, 11a/n, 11a/n/ac, 11a/n/ac/ax	6, 9, 12, 18, 24, 36, 48, 54
ieee80211 3 ※	11a, 11a/n, 11a/n/ac, 11a/n/ac/ax	6, 9, 12, 18, 24, 36, 48, 54

※ ieee80211 3 は SR-M630AP1 のみで有効です。

[注意]

無線通信モードにより必須でサポートする必要のあるレートがあるため、以下が設定されていない場合、無線 LAN アクセスポイントとして動作しません。

無線 LAN モジュール番号	無線通信モード	サポートレート
ieee80211 1	11b	1, 2, 5.5
	11g, 11g/n, 11g/n/ax	1, 2, 5.5, 6, 11, 12, 24
	11b/g, 11b/g/n, 11b/g/n/ax	1, 2, 5.5, 11

無線 LAN モジュール番号	無線通信モード	サポートレート
ieee80211 2	11a, 11a/n, 11a/n/ac, 11a/n/ac/ax	6, 12, 24
ieee80211 3 ※	11a, 11a/n, 11a/n/ac, 11a/n/ac/ax	6, 12, 24

※ ieee80211 3 は SR-M630AP1 のみで有効です。

[未設定時]

以下、無線通信モードに応じて動作します。

無線通信モードが 11b の場合

サポートレートは 1, 2, 5.5, 11 で動作します。

無線通信モードが 11g、11g/n、11g/n/ax、11b/g、11b/g/n、11b/g/n/ax の場合

サポートレートは 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 で動作します。

無線通信モードが 11a、11a/n、11a/n/ac、11a/n/ac/ax の場合

サポートレートは 6, 9, 12, 18, 24, 36, 48, 54 で動作します。

4.1.18 ieee80211 supportmcs

[機能]

11n 通信時に使用するサポート MCS の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> supportmcs <mcs_list>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<mcs_list>

- サポート MCS Index 番号のリスト
サポート MCS Index (0~15) を 10 進数で指定します。
複数の index を指定する場合は、","(カンマ)区切りで指定します。
連続した index を指定する場合は、"-"(ハイフン)で指定します(例:"0-7")。

[動作モード]

構成定義モード(管理者クラス)

[説明]

11n での通信時の MCS Index 値を指定します。

コマンドで設定した範囲の値でビーコンにて通知、および、接続時のネゴシエーションを行い、無線 LAN 端末との通信時に使用する MCS を決定します。

MCS Index 値は、1 ストリーム、2 ストリームで、それぞれ対応する値が全て同じ状態での設定のみサポートとなります。

そのため、どれかひとつのストリームに対して値を設定した場合、以下の表に基づき、未設定部分の MCS Index が補完されます。

MCS Index ストリーム数 1	MCS Index ストリーム数 2
0	8
1	9
2	10
3	11
4	12
5	13
6	14
7	15

設定例 1 : MCS Index 0 を設定した場合

```
ieee80211 1 supportmcs 0
```

上記の場合、ストリーム数 2 の 8 が補完され、以下に示す設定状態となります。

```
ieee80211 1 supportmcs 0,8
```

設定例 2 : MCS Index 0-2, 11-13 を設定した場合

```
ieee80211 1 supportmcs 0-2, 11-13
```

上記の場合、設定範囲に該当するストリームの MCS Index が補完され、以下に示す設定状態となります。

```
ieee80211 1 supportmcs 0-5, 8-13
```

[注意]

無線通信モードが 11g/n, 11b/g/n, 11b/g/n/ax, 11a/n, 11a/n/ac, 11a/n/ac/ax 以外の場合、設定値は意味を持ちません。

[未設定時]

サポート MCS Index は 0-15 で動作します。

4.1.19 ieee80211 vht-supportmcs

[機能]

11ac 通信時に使用する VHT サポート MCS の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> vht-supportmcs <mcs_list>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<mcs_list>

- VHT サポート MCS Index 番号のリスト
VHT サポート MCS Index を以下より指定します。
0-7
0-8
0-9

[動作モード]

構成定義モード(管理者クラス)

[説明]

11ac での通信時の VHT MCS Index 値を指定します。

コマンドで設定した範囲の値でビーコンにて通知、および、接続時のネゴシエーションを行い、無線 LAN 端末との通信時に使用する VHT MCS を決定します。

コマンドで設定した index 値により 2 ストリーム分の VHT サポート MCS Index を設定します。

[注意]

本設定は 5GHz 側でのみ有効となります。

無線通信モードが 11a/n/ac, 11a/n/ac/ax 以外の場合、設定値は意味を持ちません。

[未設定時]

VHT サポート MCS Index は 0-9 で動作します。

4.1.20 ieee80211 he-supportmcs

[機能]

11ax 通信時に使用する HE サポート MCS の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

ieee80211 <number> he-supportmcs <mcs_list>

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<mcs_list>

- HE サポート MCS Index 番号のリスト
HE サポート MCS Index を以下より指定します。
0-7
0-9
0-11

[動作モード]

構成定義モード(管理者クラス)

[説明]

11ax での通信時の HE MCS Index 値を指定します。

コマンドで設定した範囲の値でビーコンにて通知、および、接続時のネゴシエーションを行い、無線 LAN 端末との通信時に使用する HE MCS を決定します。

コマンドで設定した index 値により 2 ストリーム分の HE サポート MCS Index を設定します。

[注意]

無線通信モードが 11b/g/n/ax, 11g/n/ax, 11a/n/ac/ax 以外の場合、設定値は意味を持ちません。

[未設定時]

HE サポート MCS Index は 0-11 で動作します。

4.1.21 ieee80211 noise-detect use

[機能]

ノイズ回避機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> noise-detect use <use>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<use>

- off
ノイズ回避機能を使用しません。
- on
ノイズ回避機能を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ノイズ回避機能を使用するかどうかを設定します。本機能は周辺電波環境の混在状況に応じてノイズ状態検出時に混在していないチャンネルに自動的に切り替えて運用させることができます。

[未設定時]

ノイズ回避機能を使用しないものとみなされます。

```
ieee80211 <number> noise-detect use off
```

4.1.22 ieee80211 radar-detect lamp-flash time

[機能]

レーダ検出時の WIRELESS ランプ点滅時間の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> radar-detect lamp-flash time <time>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<time>

レーダ検出時の WIRELESS ランプ点滅時間 60~1800(秒単位)で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

レーダ検出時の WIRELESS ランプ点滅時間を設定します。

[注意]

本設定は 5GHz 側でのみ有効になります。

コマンドで指定した点滅時間より利用チャネル確認(CAC)時間が長い場合、WIRELESS ランプの点滅は利用チャネル確認(CAC)時間となります。

[未設定時]

レーダ検出時の WIRELESS ランプ点滅時間に 60 が設定されたとみなされます。

```
ieee80211 <number> radar-detect lamp-flash time 60
```

4.1.23 ieee80211 sr use

[機能]

空間再利用機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> sr use <mode>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<mode>

- on
空間再利用機能を有効にします。
- off
空間再利用機能を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

空間再利用機能を有効または無効に設定します。

[注意]

空間再利用機能は 11ax のみで動作します。

[未設定時]

空間再利用機能は有効に設定されたものとみなされます。

```
ieee80211 <number> sr use on
```

4.1.24 ieee80211 sr tx-threshold

[機能]

空間再利用機能で使用されるキャリアセンス送信閾値の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ieee80211 <number> sr tx-threshold <threshold>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<threshold>

送信閾値を 10 進数で指定します。
設定可能範囲は 62~82 です。
62 が設定された場合は、キャリアセンスの送信閾値が-62dBm となります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

空間再利用機能有効時に使用されるキャリアセンス送信閾値を設定します。

[注意]

空間再利用機能が無効に設定されている場合は、本コマンドは無効となります。

[未設定時]

空間再利用機能で使用されるキャリアセンス送信閾値は、-62dBm に設定されたものとみなされます。

```
ieee80211 <number> sr tx-threshold 62
```

4.1.25 ieee80211 144ch-support

[機能]

144 チャンネルの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

ieee80211 <number> 144ch-support <mode>

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<mode>

- enable
144 チャンネルを有効にします。
- disable
144 チャンネルを無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

144 チャンネルを有効または無効にするコマンドとなります。

[注意]

144 チャンネルを無効に設定した場合、以下の組み合わせでは無線 LAN アクセスポイントとして動作しません。

帯域幅	チャンネル番号
20MHz	144
40MHz	140、144
80MHz	132、136、140、144

無線モジュール番号は SR-M630AP1 では 3、SR-M610AP1 では 2 のみ有効です。それ以外の無線モジュール番号が指定された場合は本コマンドの設定内容は無効となります。

[未設定時]

144 チャンネルを有効に設定されたものとみなされます。

```
ieee80211 <number> 144ch-support enable
```

4.1.26 ieee80211 outdoormode

[機能]

屋外モードの設定

[適用機種]

SR-M610AP1

[入力形式]

```
ieee80211 <number> outdoormode <mode>
```

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<mode>

- off
屋外モードを無効に設定します。
- on
屋外モードを有効に設定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

屋外モードを有効に設定すると W56 のみの使用が可能となり、屋外モードを無効に設定すると W52、W53、W56 すべて使用可能となります。屋外モードを有効にした場合、レーダ検出時、ノイズ回避機能実行時やチャンネル設定を自動に設定した場合も W56 以外のチャンネルに移動することはありません。

[注意]

本コマンドにより設定を変更した場合は、装置再起動が必要です。

本コマンドを有効、かつスキャンチャンネルリストで w52 または w53 を指定した場合、スキャンチャンネルリスト設定は無効になります。

無線 LAN モジュール番号は、2 のみ有効です。1 が指定された場合は、本コマンドの設定内容は無効となります。

[未設定時]

屋外モードを無効に設定されたものとみなされます。

```
ieee80211 2 outdoormode off
```

第 5 章 無線 LAN インタフェース情報の設定

- wlan 定義番号の指定範囲

本章のコマンドの[オプション]に記載されている<number>(wlan 定義番号)に指定する wlan 定義の通し番号(10進数)は、以下に示す範囲で指定してください。

範囲	機種
1～48	SR-M630AP1
1～32	SR-M610AP1

5.1 無線インタフェース数情報

5.1.1 wlan-conf wlan-num

[機能]

無線 LAN インタフェースの最大数の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

wlan-conf wlan-num <num>

[オプション]

<num>

- 無線 LAN インタフェース数の設定
無線 LAN インタフェース数を 8 か 16 で設定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線 LAN モジュール毎の無線 LAN インタフェース数の最大数を設定します。

[注意]

本設定を変更した場合は、装置再起動が必要です。

設定した無線 LAN インタフェース数によって、実際に無線 LAN モジュールに割り当てられる無線 LAN インタフェース番号が変わります。無線モジュール 1 つあたり無線インタフェースを 16 個使用する場合は、本コマンドで 16 と設定する必要があります。

SR-M50AP1, SR-M20AP1, SR-M20AP2 (無線 LAN モジュール毎の無線 LAN インタフェース数の最大数が 8) で動作していた構成定義を取り込む場合は、8 と設定する必要があります。

無線 LAN インタフェース数、無線 LAN モジュール番号、および無線 LAN インタフェース番号の関係は以下のように定義付けられています。

SR-M630AP1 の場合

無線 LAN インタフェース数	無線 LAN インタフェース番号	無線 LAN モジュール番号
8	wlan 1 ~ 8	ieee80211 1
	wlan 9 ~ 16	ieee80211 2
	wlan 17 ~ 24	ieee80211 3
	wlan 25 ~ 48 ※1	-
16	wlan 1 ~ 16	ieee80211 1
	wlan 17 ~ 32	ieee80211 2
	wlan 33 ~ 48	ieee80211 3

SR-M610AP1 の場合

無線 LAN インタフェース数	無線 LAN インタフェース番号	無線 LAN モジュール番号
8	wlan 1 ~ 8	ieee80211 1
	wlan 9 ~ 16	ieee80211 2
	wlan 17 ~ 32 ※1	-

無線 LAN インタフェース数	無線 LAN インタフェース番号	無線 LAN モジュール番号
16	wlan 1 ~ 16	ieee80211 1
	wlan 17 ~ 32	ieee80211 2

※1. 無効となり、定義があっても無視されます。

[未設定時]

無線 LAN インタフェース数に 8 が設定されたものとみなされます。

```
wlan-conf wlan-num 8
```


5.2 無線 LAN インタフェース情報

5.2.1 wlan use

[機能]

無線 LAN インタフェースの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> use <mode>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<mode>

- on
無線 LAN インタフェースを使用します。
- off
無線 LAN インタフェースを使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線 LAN インタフェースを使用するかどうかを設定します。

無線 LAN インタフェースを使用するには、無線 LAN モジュールの設定を有効にする必要があります。

無線 LAN モジュール番号、無線 LAN インタフェースの最大値、無線 LAN インタフェース番号の関係は以下のよう
に定義付けられています。

無線 LAN モジュール番号	無線 LAN インタフェース の最大値	無線 LAN インタフェース番号
ieee80211 1	8	wlan 1~8
	16	wlan 1~16
ieee80211 2	8	wlan 9~16
	16	wlan 17~32
ieee80211 3 ※ SR-M630AP1 のみ	8	wlan 17~24
	16	wlan 33~48

[未設定時]

無線 LAN インタフェースを使用しないものとみなされます。

```
wlan <number> use off
```

5.2.2 wlan description

[機能]

説明文の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> description <description>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<description>

- 説明文
この無線 LAN インタフェースの説明文を、0x21, 0x23~0x7e の 50 文字以内の ASCII 文字列で記入します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

この無線 LAN インタフェースについての説明文を記入します。

[未設定時]

説明文を記入しないものとみなされます。

5.2.3 wlan type

[機能]

無線 LAN インタフェースの動作タイプ設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> type <type>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<type>

- ap
無線 LAN アクセスポイントとして動作します。
- ap-disaster
災害用無線 LAN アクセスポイントとして動作します。
- wds-ap
WDS 親機として動作します。
- wds-sta
WDS 子機として動作します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線 LAN インタフェースの動作タイプを設定します。

動作タイプ設定が ap の無線 LAN インタフェースを複数設定することで、仮想アクセスポイント環境を構築することができます。

ap と ap-disaster は、LED の点灯状態以外は全く同じ動作となります。

[注意]

動作タイプ設定に WDS 親機(wds-ap)、WDS 子機(wds-sta)を指定し、WDS ブリッジ機能を使用する場合は以下の点に注意してください。

- WDS 親機側の装置にのみ無線 LAN チャンネル番号を指定してください。WDS 子機側は WDS 親機の無線 LAN チャンネルに追従するため、無線 LAN チャンネル番号を指定しても無効となります。
- WDS 子機と同じ無線モジュールに WDS 親機の無線 LAN インタフェースを設定することは可能ですが無線 LAN チャンネル番号を指定しても無効となります。
- W53、W56 帯の無線 LAN チャンネル番号を指定した場合、または自動(any)を設定して W53、W56 帯に無線 LAN チャンネルが割り当てられた場合、無線 LAN アクセスポイントの場合と同様に、DFS 機能がレーダを検出した場合、約 1 分間通信ができなくなります。そのため、5GHz 帯のチャンネルを使用する場合は、W52 帯の無線 LAN チャンネルを使用することを推奨します。
- WDS ブリッジを行う無線 LAN アクセスポイント間では、WPA3-SAE 以外の認証モードを使用できません。
- 1 つの無線モジュールに設定できる WDS 子機は 1 つまでとなります。2 つ目以降は無効となります。

[未設定時]

無線 LAN インタフェースの動作タイプに ap が設定されたものとみなされます。

```
wlan <number> type ap
```

5.2.4 wlan ssid

[機能]

SSID の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> ssid <ssid>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<ssid>

- SSID
無線 LAN のネットワーク識別子を、32 文字以内の ASCII 文字列で指定します。
文字列は、0x22(ダブルクォーテーション)を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字で、0x20(空白文字)を使用する場合は、文字列をダブルクォーテーション(")で囲う必要があります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線 LAN でのネットワーク識別子である SSID を設定します。
ここで設定した SSID は、アクセスポイントの存在を周囲に広報するビーコンフレームに含まれて送信されます。

[注意]

無線 LAN アクセスポイントとして動作するときは、本設定が必須となります。
無線 LAN アクセスポイントとして動作する場合、ビーコンフレームは電波が届く範囲の無線 LAN 端末にアクセスポイントの存在を知らせているため、ユーティリティソフトを使えば第三者でも SSID を知ることができます。第三者が SSID を無断で設定し使用してしまう可能性があるため、必要に応じて SSID 非通知機能やセキュリティ機能を併せて使用することを推奨します。

[未設定時]

SSID を設定しないものとみなされます。

5.2.5 wlan hide

[機能]

SSID 非通知(ステルス機能)と ANY 接続拒否の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> hide <mode>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<mode>

- enable
SSID 非通知を有効にすると同時に、ANY 接続を拒否します。
- disable
SSID 非通知を無効にすると同時に、ANY 接続を受け入れます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SSID 非通知を有効にすると、アクセスポイントは SSID を隠蔽したビーコンフレームを送信します。
それと同時に、無線 LAN 端末から SSID を指定しない ANY 接続に対して接続拒否します。

[未設定時]

SSID 非通知(ステルス機能)と ANY 接続拒否を無効にするものとみなされます。

```
wlan <number> hide disable
```

5.2.6 wlan apbridge

[機能]

アクセスポイント内ブリッジ転送の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> apbridge <mode>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<mode>

- enable
アクセスポイント内ブリッジ転送を有効にします。
- disable
アクセスポイント内ブリッジ転送を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

アクセスポイント内ブリッジ転送を有効にすると、同一仮想アクセスポイントに繋がる無線 LAN 端末どうしの通信が行えます。

アクセスポイント内ブリッジ転送を無効にすると、同一仮想アクセスポイントに繋がる無線 LAN 端末どうしの通信を遮断します。こうすることにより、無線 LAN 端末間でのプライバシーを確保することができます。(プライバシー保護機能)

[未設定時]

アクセスポイント内ブリッジ転送を有効にするものとみなされます。

```
wlan <number> apbridge enable
```

5.2.7 wlan auth

[機能]

IEEE802.11 認証モードの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> auth <auth_algo>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<auth_algo>

- open
IEEE802.11 のオープン認証を行います。
- shared
IEEE802.11 の共通鍵認証を行います。
- wpa2
WPA2 による IEEE802.1X 認証を行います。
- wpa2-psk
WPA2 による事前共有キー (PSK) 認証を行います。
- wpa/wpa2
WPA または WPA2 を自動判別して IEEE802.1X 認証を行います。
- wpa/wpa2-psk
WPA または WPA2 を自動判別して事前共有キー (PSK) 認証を行います。
- wpa3
WPA3 による IEEE802.1X 認証を行います。
- wpa3-sae
WPA3-SAE 認証を行います。
- wpa2/wpa3
WPA2 または WPA3 を自動判別して IEEE802.1X 認証を行います。
- wpa2-psk/wpa3-sae
WPA2 または WPA3 を自動判別して WPA2-PSK 認証または WPA3-SAE 認証を行います。
- enhanced-open
エンハンスドオープン認証を行います。
- open/enhanced-open
オープン認証とエンハンスドオープン認証の移行モードでオープン認証を行います。
- open/enhanced-open_owe
オープン認証とエンハンスドオープン認証の移行モードでエンハンスドオープン認証を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IEEE802.11 の認証モードを設定します。

<auth_algo>に shared を指定する場合は、WEP キーに関する定義が必須となります。

オープン認証は、チャレンジに対するレスポンスを待たずに認証してしまうため実質的には認証を行わないのと同等となります。

wpa2-psk, wpa/wpa2-psk, wpa2-psk/wpa3-sae を使用するときは、事前共有キー (PSK) 設定が必須となります。
wpa3-sae を使用するときは、SAE パスワード設定が必須となります。

wpa2, wpa/wpa2, wpa3, wpa2/wpa3 を使用するときは、wlan 定義に IEEE802.1X 認証関連の設定が必須となります。

open/enhanced-open を使用するときは、ペアとなる open/enhanced-open_owe の設定が必須となります。

[注意]

11b/g/n, 11b/g/n/ax, 11g/n, 11g/n/ax, 11a/n, 11a/n/ac, 11a/n/ac/ax をした通信を行う場合、以下の設定はできません。

- ・ オープン認証で WEP 暗号を使う
- ・ 共通鍵認証

[未設定時]

IEEE802.11 認証モードに open が設定されたものとみなされます。

```
wlan <number> auth open
```

5.2.8 wlan wep mode

[機能]

WEP 使用の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wep mode <mode>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<mode>

- disable
WEP を使用しない通信が可能になります。
- enable
WEP を使用した通信が可能になります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線ネットワークへの接続にあたって WEP 暗号化を使用させるかどうかを設定します。

[注意]

- 通信モードに 11b/g/n, 11b/g/n/ax, 11g/n, 11g/n/ax, 11a/n, 11a/n/ac, 11a/n/ac/ax を指定した場合、WEP は使用できません。
- WEP 暗号と IEEE802.1X 認証または MAC アドレス認証を併用する場合、すべての無線 LAN インタフェースで、認証サーバから通知された VLAN を割り当てる機能を無効(wlan dot1x vlan assign disable / wlan macauth vlan assign disable) に設定し、端末に割り当てるデフォルト VLAN ID 機能(wlan dot1x vid/wlan macauth vid) を利用してください。

[未設定時]

WEP 使用設定に disable が設定されたものとみなされます。

```
wlan <number> wep mode disable
```

5.2.9 wlan wep key

[機能]

WEP キーの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wep key <index> <kind> <wep_key> [encrypted]
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<index>

登録する WEP キーの識別番号を、1~4 の 10 進数で指定します。

<kind>

WEP キー種別を指定します。

- hex
16 進数キーを使用します。
- text
文字列キーを使用します。

<wep_key>

WEP キーを指定します。

- 暗号化されていない WEP キー
<kind>の指定によって入力範囲が異なります。入力範囲を以下に示します。

キー種別 WEP キー長 (IV 除く)	hex 16 進数キー	text 文字列キー
WEP 64-bit (40-bit)	10 桁	5 文字
WEP 128-bit (104-bit)	26 桁	13 文字

指定した WEP キーが上記表の桁数、文字数以外の場合は設定異常となるため、正しい桁数、文字数を設定する必要があります。

文字列キーの場合、0x22(ダブルクォーテーション)を除く [0x20-0x7e]の範囲のコードで構成される ASCII 文字列で指定します。ただし、0x20(空白文字)を使用する場合は、文字列をダブルクォーテーション(")で囲う必要があります。

- 暗号化された WEP キー
暗号化された WEP キーを指定します。
show コマンドで表示される暗号化された WEP キーを encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化 WEP キー指定
<wep_key>に暗号化された WEP キーを指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

WEP 暗号に用いる WEP キーを指定します。

[未設定時]

WEP キーを設定しないものとみなされます。

5.2.10 wlan wep send

[機能]

使用する WEP キーの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wep send <index>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<index>

登録した WEP キーの中から実際に使用する WEP キーの識別番号を、1~4 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

実際に WEP 暗号で使用する WEP キーを選択します。

[注意]

WEP を使用する場合は、指定した識別番号の WEP キー設定が必須となります。

[未設定時]

使用する WEP キーの識別番号に 1 が設定されたものとみなされます。

```
wlan <number> wep send 1
```

5.2.11 wlan wpa cipher

[機能]

WPA/WPA2/WPA3 暗号化モードの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wpa cipher <cipher>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<cipher>

- aes
AES 暗号化を行います。
- auto
TKIP または AES で自動判別し暗号化を行います。
- 192bit-sec
192bit 暗号化を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

WPA/WPA2/WPA3 で使用する暗号化モードを設定します。

ここで設定した暗号化モードは、wlan auth <auth_algo>に WPA/WPA2/WPA3 に関する設定がされているときに意味を持ちます。

192bit 暗号化は wlan auth wpa3 の場合のみ設定可能です。

[注意]

mode を auto に設定している場合は、古い実装の暗号化方式を認識できない場合があります。

このため、接続ができず相性問題が生じる場合は、暗号化方式を以下のように指定してください。

- AES 固定とします。

TKIP 暗号化が選択された場合、11b、11b/g、11g、11a 通信モードで動作します。

wlan auth <auth_algo>に WPA3 に関する設定がされているときは auto は使用できません。aes または 192bit-sec を選択してください。

[未設定時]

WPA/WPA2/WPA3 暗号化モードに auto が設定されたものとみなされます。

```
wlan <number> cipher auto
```

5.2.12 wlan wpa psk

[機能]

WPA/WPA2/WPA3 事前共有キーの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wpa psk <kind> <key> [encrypted]
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<kind>

キー種別を指定します。

- hex
16 進数キーを使用します。
- text
文字列キー(パスワード)を使用します。

<key>

事前共有キー(PSK)を指定します。

- 暗号化されていない PSK
<kind>の指定によって入力範囲が異なります。入力範囲を以下に示します。

キー種別	hex 16 進数キー	text 文字列キー
事前共有キー	64 桁	8~63 文字

文字列キーの場合、0x22(ダブルクォーテーション)を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、0x20(空白文字)を使用する場合は、文字列をダブルクォーテーション(")で囲う必要があります。

16 進数キーの場合、指定したキーの桁数が 64 桁に満たない部分は 0x0 でパディングされます。

- 暗号化された PSK
暗号化された PSK を指定します。
show コマンドで表示される暗号化された PSK を encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化 PSK 指定
<psk>に暗号化された PSK を指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

WPA-PSK/WPA2-PSK/WPA3-SAE で用いる事前共有キーを指定します。

WPA3-SAE を利用する場合、wlan auth wpa2-psk/wpa3-sae が設定されていれば本設定を使用し、wlan wpa sae password は使用しません。

[未設定時]

PSK は設定しないものとみなされます。

5.2.13 wlan wpa sae password

[機能]

WPA3-SAE のパスワードの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wpa sae password <password> [encrypted]
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<password>

パスワードを指定します。

- 暗号化されていないパスワード
0x22(ダブルクォーテーション)を除く [0x20-0x7e]の範囲のコードで構成される 8~128 文字の ASCII 文字列で指定します。ただし、0x20(空白文字)を使用する場合は、文字列をダブルクォーテーション(")で囲う必要があります。
- 暗号化されたパスワード
暗号化されたパスワードを指定します。
show コマンドで表示される暗号化されたパスワードを encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化パスワード指定
<password>に暗号化されたパスワードを指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

WPA3-SAE で用いるパスワードを指定します。

wlan auth wpa3-sae が設定されている場合のみ本設定を使用します。wlan auth wpa2-psk/wpa3-sae が設定されている場合は wlan wpa psk 設定の事前共有キーを使用し、本設定は使用しません。

[未設定時]

パスワードは設定しないものとみなされます。

5.2.14 wlan wpa rekey group

[機能]

WPA/WPA2/WPA3 のグループキー更新間隔の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wpa rekey group <period>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

group <period>

- グループキー (GTK) の更新間隔
更新間隔を 600s (10 分) ~ 86400s (1 日) の範囲で指定します。
単位は、d (日)、h (時)、m (分)、s (秒) のどれかを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

WPA/WPA2/WPA3 で使用するグループキー (GTK) の更新間隔を設定します。

[未設定時]

WPA/WPA2/WPA3 グループキー更新間隔に 10m が設定されたものとみなされます。

```
wlan <number> rekey group 10m
```

5.2.15 wlan wpa pmkcache mode

[機能]

PMK キャッシュ機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wpa pmkcache mode <mode>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<mode>

- enable
PMK キャッシュ機能を有効にします。
- disable
PMK キャッシュ機能を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

PMK キャッシュ機能を設定します。

[注意]

PMK キャッシュ機能は、無線 LAN 端末とアクセスポイントの両装置で設定する必要があります。
設定が異なった場合、毎回 RADIUS サーバを利用して完全な認証を行うことになります。

[未設定時]

PMK キャッシュ機能を有効にするものとみなされます。

```
wlan <number> wpa pmkcache mode enable
```

5.2.16 wlan wpa pmkcache num

[機能]

PMK キャッシュ機能でのキャッシュ保持数の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wpa pmkcache num <num>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<num>

- PMK キャッシュ機能でのキャッシュ保持数
キャッシュ保持数の上限を 1~200 個の範囲で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

PMK キャッシュ機能でのキャッシュ保持数を設定します。

[注意]

PMK キャッシュ保持数が上限の状態、PMK キャッシュを追加する場合、もっとも生成時間が古いキャッシュを削除したあと、追加します。

運用で問題が生じていない場合は、本設定を変更しないで運用してください。

[未設定時]

PMK キャッシュのキャッシュ保持数に 200 個が設定されたものとみなされます。

```
wlan <number> wpa pmkcache num 200
```

5.2.17 wlan wpa pmkcache expire

[機能]

PMK キャッシュ機能でのキャッシュ保持期間の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wpa pmkcache expire <expire>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<expire>

- PMK キャッシュ機能でのキャッシュ保持期間
キャッシュ保持期間を 3600s(1 時間)~86400s(1 日)の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

PMK キャッシュ機能でのキャッシュ保持期間を設定します。

PMK キャッシュを新規追加した時点で、保持期限を設定し、保持期限が満了した場合、PMK キャッシュを削除します。

[注意]

運用で問題が生じていない場合は、本設定を変更しないで運用してください。

[未設定時]

PMK キャッシュのキャッシュ保持期間に 12 時間が設定されたものとみなされます。

```
wlan <number> wpa pmkcache expire 12h
```

5.2.18 wlan wpa eapol supptimeout

[機能]

無線 LAN インタフェースの EAPOL-KEY 応答待ち時間の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wpa eapol supptimeout <time>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<time>

EAPOL-KEY パケットの応答待ち時間を 1~600 秒で指定します。
単位は s(秒)を指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

端末(Supplicant)に対する EAPOL-KEY 応答待ち時間を設定します。
運用で問題が生じていない場合は、本設定を変更しないで運用してください。

[注意]

本設定を変更した場合、接続にかかる時間が長くなる場合があります。

[未設定時]

EAPOL-KEY 応答待ち時間として 2 秒が設定されてものとみなされます。

```
wlan <number> wpa eapol supptimeout 2s
```

5.2.19 wlan wpa eapol maxreq

[機能]

無線 LAN インタフェースの EAPOL-KEY 再送回数の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wpa eapol maxreq <count>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<count>

EAPOL-KEY 再送回数を 1~10 回で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

EAPOL-KEY 応答が受信できない場合の EAPOL-KEY 再送回数を指定します。
運用で問題が生じていない場合は、本設定を変更しないで運用してください。

[未設定時]

EAPOL-KEY 再送回数として 2 回が設定されたものとみなされます。

```
wlan <number> wpa eapol maxreq 2
```

5.2.20 wlan wpa pmf mode

[機能]

PMF 使用の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wpa pmf mode <mode>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<mode>

- enable
PMF 機能を有効(オプション)にします。
- required
PMF 機能を有効(必須)にします。
- disable
PMF 機能を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線ネットワークへの接続にあたって PMF を使用させるかどうかを設定します。

[注意]

- 認証モードが wpa2, wpa3, enhanced-open を含む認証方式であり、かつ AES を含む暗号化方式である場合のみ、PMF が有効に動作します。
- PMF 機能を有効(必須)にした場合、PMF をサポートしていない無線 LAN 端末は接続できません。
- PMF 機能を有効(オプション)にした場合、PMF をサポートしている無線 LAN 端末、サポートしていない無線 LAN 端末がともに接続できます。
- 以下の認証モードを利用する場合、PMF 機能は有効(必須)を設定してください。
wpa3, wpa3-sae, enhanced-open, open/enhanced-open_owe
- 以下の認証モードを利用する場合、PMF 機能は有効(必須)または有効(オプション)を設定してください。
wpa2/wpa3, wpa2-psk/wpa3-sae
- PMF 機能を有効(必須)または有効(オプション)に設定している場合、無線 LAN 端末と接続できない、または、PTK/GTK の定期鍵更新時に切断される場合があります。その場合、無線 LAN 端末のドライバソフトウェアや OS の最新化により、状況が改善するかを確認してください。
状況が改善しない場合、PMF 機能を無効に設定してください。

[未設定時]

PMF 使用設定に enable が設定されたものとみなされます。

```
wlan <number> wpa pmf mode enable
```

5.2.21 wlan wpa owe trans

[機能]

OPEN/Enhanced OPEN の移行モードの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> wpa owe_trans <wlan-number>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
OPEN 認証の無線 LAN インタフェース番号を、10 進数で指定します。

<wlan-number>

- ペアとなる無線 LAN インタフェース番号
ペアとなる Enhanced OPEN 認証の無線 LAN インタフェース番号を、10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

OPEN/Enhanced OPEN の移行モードでの OPEN 認証の無線 LAN インタフェースについて、ペアとなる Enhanced OPEN 認証の無線 LAN インタフェースを指定します。

[注意]

OPEN/Enhanced OPEN の移行モードでの OPEN 認証の無線 LAN インタフェースでは本設定が必須となります。

[未設定時]

ペアとなる無線 LAN インタフェース番号は設定しないものとみなされます。

5.2.22 wlan guard-interval

[機能]

ガードインターバルの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> guard-interval <mode>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<mode>

- auto
ガードインターバルとして、400 ナノ秒または 800 ナノ秒を使用します。
- long
ガードインターバルとして、800 ナノ秒を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

11n、11ac で使用するガードインターバルを指定します。

[注意]

11ax は常に 800 ナノ秒で動作します。

[未設定時]

ガードインターバルとして 400 ナノ秒または 800 ナノ秒を設定するものとみなされます。

```
wlan <number> guard-interval auto
```


5.2.23 wlan macfilter

[機能]

MAC アドレスフィルタの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> macfilter <count> <action> acl <acl_count>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<count>

- 優先順位
指定するフィルタ設定の優先順位を、10 進数で設定します。
小さい値が優先順位がより高いことを示します。

範囲	機種
0~117	SR-M630AP1 SR-M610AP1

<action>

フィルタリング対象に該当するフレームを透過するかどうかを指定します。

- pass
該当するフレームを透過します。
- reject
該当するフレームを遮断します。

<acl_count>

- ACL 定義番号
使用する ACL 定義の番号を、10 進数で指定します。
指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
MAC アドレスフィルタリングでは、ACL の以下の定義を使用します。
 - mac
送信元 MAC アドレスのみを使用します。
送信元 MAC アドレスに any または 00:00:00:00:00:00 または FF:FF:FF:FF:FF:FF が設定されている場合、そのフィルタ定義は無効となります。
mac 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

範囲	機種
0~599	SR-M630AP1 SR-M610AP1

[動作モード]

構成定義モード(管理者クラス)

[説明]

無線 LAN アクセスポイントでは、指定した ACL の送信元 MAC アドレスと一致した無線 LAN 端末からの Authentication 要求を、指定した<action>に従って透過または遮断します。
設定した優先度順に一致するか調べ、一致した時点でフィルタリングされ、それ以降の設定は参照されません。

[未設定時]

無線 LAN アクセスポイントでの MAC アドレスフィルタを無効にするものとみなされます。

5.2.24 wlan macfilter default

[機能]

MAC アドレスフィルタの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> macfilter default <action>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<action>

どのフィルタリングテーブルにも一致しなかったフレームをどう扱うかを指定します。

- pass
該当するフレームを透過します。
- reject
該当するフレームを遮断します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

どのフィルタリングテーブルにも一致しなかったフレームをどう扱うかを指定します。

[未設定時]

どのフィルタリングテーブルにも一致しないパケットは透過します。

```
wlan <number> macfilter default pass
```

5.2.25 wlan sta guarantee

[機能]

最低保証台数の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> sta guarantee <guarantee>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<guarantee>

- 最低保証台数
接続できる無線 LAN 端末の最低保証台数を 1～118 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した仮想アクセスポイントに接続できる無線 LAN 端末の最低保証台数を設定します。

同一の無線 LAN モジュールの仮想アクセスポイントに設定されている最低保証台数の合計が、無線 LAN モジュールの接続可能台数に収まるように設定してください。

[未設定時]

最低保証台数を設定しないものとみなされます。

5.2.26 wlan sta idle

[機能]

無通信切断時間の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> sta idle <time>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<time>

- 無通信切断時間
無通信切断までの時間を 1 分～5 分の範囲で指定します。
単位は、m(分)、s(秒)のどちらかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した仮想アクセスポイントの無通信切断時間を設定します。
<time>で設定された間、接続している無線 LAN 端末からの受信パケットがない場合に切断します。
運用で問題が生じていない場合は、本設定を変更しないで運用してください。

[注意]

設定時間を極端に短くした場合は、接続状態が不安定になることがあります。

[未設定時]

無通信切断時間に 5 分が設定されたものとみなされます。

```
wlan <number> sta idle 5m
```

5.2.27 wlan band-steering mode

[機能]

無線 LAN インタフェースのバンドステアリング機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> band-steering mode <mode>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<mode>

- enable
バンドステアリング機能を有効にします。
- disable
バンドステアリング機能を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

バンドステアリング機能を使用するかを 2.4GHz 周波数帯の無線 LAN インタフェースに設定します。

- 無線 LAN インタフェースの最大数の設定が 8 の場合 : wlan 1~8
- 無線 LAN インタフェースの最大数の設定が 16 の場合 : wlan 1~16

本機能を有効にした無線 LAN インタフェースの SSID 名を、5GHz 周波数帯の無線 LAN インタフェースに設定することで、バンドステアリング機能が動作します。

5GHz 周波数帯の無線 LAN モジュールを 2 個搭載する SR-M630AP1 では、2.4GHz 周波数帯と 5GHz 周波数帯の無線 LAN インタフェース間のバンドステアリングは動作しますが、5GHz 周波数帯同士の無線 LAN インタフェース間のバンドステアリングは動作しません。

例えば、無線 LAN インタフェースの最大数の設定が 16 の場合

```
wlan 1 band-steering mode enable
wlan 1 ssid test-ssid
wlan 17 ssid test-ssid
wlan 33 ssid test-ssid
バンドステアリング動作
wlan 1 <=====> wlan 17 間 : OK
wlan 1 <=====> wlan 33 間 : OK
wlan 17 <=====> wlan 33 間 : NG
```

[注意]

バンドステアリング機能を使用する無線 LAN インタフェースは以下の設定を一致させてください。

一致しない場合、バンドステアリング機能は有効になりません。

- SSID の設定
- SSID 非通知(ステルス機能)と ANY 接続拒否の設定
- IEEE802.11 認証モードの設定
※open 認証以外のモードは以下の設定も一致させてください。
 - shared
 - WEP 使用の設定

-
- WEP キーの設定
 - 使用する WEP キーの設定
 - WEP 動作タイプの設定
 - wpa2-psk, wpa/wpa2-psk, wpa2-psk/wpa3-sae
 - WPA/WPA2/WPA3 暗号化モードの設定
 - WPA/WPA2/WPA3 事前共有キーの設定
 - PMF 使用の設定
 - wpa3-sae
 - WPA/WPA2/WPA3 暗号化モードの設定
 - SAE パスワードの設定
 - PMF 使用の設定
 - wpa2, wpa/wpa2, wpa3, wpa2/wpa3
 - enhanced-open, open/enhanced-open, open/enhanced-open_owe
 - WPA/WPA2/WPA3 暗号化モードの設定
 - PMF 使用の設定
 - IEEE802.1X 認証機能を併用する場合
 - 無線 LAN インタフェースの IEEE802.1X 認証の設定
 - 無線 LAN インタフェースが参照する AAA 情報の設定
 - 無線 LAN インタフェースの端末(Supplicant)に割り当てるデフォルト VLAN ID の設定
 - 無線 LAN インタフェースの VLAN 割り当て方式の設定
 - MAC アドレス認証機能を併用する場合
 - 無線 LAN インタフェースの MAC アドレス認証の設定
 - 無線 LAN インタフェースの MAC アドレス認証で参照する AAA 情報の設定
 - 無線 LAN インタフェースの端末(Supplicant)に割り当てるデフォルト VLAN ID の設定
 - 無線 LAN インタフェースの VLAN 割り当て方式の設定

IEEE802.1X 認証または MAC アドレス認証にて、認証サーバから通知された VLAN を割り当てる機能(wlan dot1x vlan assign enable/wlan macauth vlan assign enable)を利用する場合、バンドステアリング機能は動作しません。

本機能を利用する場合は、認証サーバから通知された VLAN を割り当てる機能を<disable>に設定し、端末(Supplicant)に割り当てるデフォルト VLAN ID 機能(wlan dot1x vid/wlan macauth vid)を利用してください。

[未設定時]

バンドステアリング機能を使用しないものとみなされます。

```
wlan <number> band-steering mode disable
```

5.2.28 wlan atf ratio

[機能]

エアタイムフェアネスの配分の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> atf ratio <ratio>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<ratio>

- 時間配分を指定します。
時間配分を、1~99 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

各 SSID にエアタイムの配分を設定します。

エアタイムフェアネス機能が有効になっている場合、指定された割合でエアタイムを配分することにより SSID ごとに重みづけをすることができます。

atf use でエアタイムフェアネス機能が無効になっている場合は無視されます。

[注意]

2. 4G/5GHz それぞれの無線 LAN モジュール内に同一の SSID 名が複数存在する場合、無線インタフェース番号が最後の最も若番のインタフェースに対してのみ、時間配分<ratio>を設定してください。

SSID 名が重複する 2 番目以降のインタフェースに対しては<ratio>設定は不要です。

重複して<ratio>が設定されていた場合は 2 番目以降の設定値は無視されます。

[未設定時]

SSID による重みづけを行わないとみなされます。

5.3 VLAN 情報

5.3.1 wlan vlan tag

[機能]

無線 LAN インタフェースの Tag あり VLAN 情報の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> vlan tag <tagged_vidlist>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<tagged_vidlist>

- tag 付き VLAN ID リスト
tag 付き VLAN ID を 1~4094 の 10 進数で指定します。
複数の VLAN ID を指定する場合は、","(カンマ)で区切ります。

[動作モード]

構成定義モード(管理者クラス)

[説明]

Tagged VLAN ID の設定を行います。

[注意]

- 動作タイプとして wds-ap, wds-sta を指定した無線 LAN インタフェースでのみ、本コマンドが有効です。
- 同一無線 LAN インタフェースに Tag あり VLAN と Tag なし VLAN を混在設定することはできません。
混在設定された場合、Tag あり VLAN 設定は無効となります。
- VLAN を追加登録する際には、すでに登録されている VLAN も含めた VLAN ID リストを指定してください。
- IEEE802.1X 認証および MAC アドレス認証を有効にした無線 LAN インタフェースには、VLAN の設定はできません。設定された場合、無線 LAN インタフェースは利用できなくなります。
- 高速転送モードを使用する場合(system bridge acceleration mode enable)、以下のコマンドで指定できる VLAN ID は合計で 24 個までです。24 個を超えて使用しないでください。

```
ether vlan tag  
ether vlan untag  
wlan vlan tag  
wlan vlan untag
```

[未設定時]

Tagged VLAN ID を設定しないものとみなされます。

5.3.2 wlan vlan untag

[機能]

無線 LAN インタフェースの Tag なし VLAN 情報の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> vlan untag <untagged_vid>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<untagged_vid>

- tag なし VLAN ID
tag なし VLAN ID を 1~4094 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

Untagged VLAN ID の設定を行います。

[注意]

- IEEE802.1X 認証および MAC アドレス認証を有効にした無線 LAN インタフェースには、VLAN の設定はできません。設定された場合、無線 LAN インタフェースは利用できなくなります。
- 高速転送モードを使用する場合(system bridge acceleration mode enable)、以下のコマンドで指定できる VLAN ID は合計で 24 個までです。24 個を超えて使用しないでください。

```
ether vlan tag
ether vlan untag
wlan vlan tag
wlan vlan untag
```

[未設定時]

wlan vlan tag コマンドが設定されていない場合、VLAN ID として 1 が設定されたものとみなされます。

```
wlan <number> vlan untag 1
```

wlan vlan tag コマンドが設定されている場合、VLAN ID を設定しないものとみなされます。

5.4 IEEE802.1X 認証情報

5.4.1 wlan dot1x use

[機能]

無線 LAN インタフェースの IEEE802.1X 認証の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> dot1x use <mode>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<mode>

- IEEE802.1X 認証モードを指定します。
- on
IEEE802.1X 認証機能を有効にします。
 - off
IEEE802.1X 認証機能を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ポートアクセス制御として IEEE802.1X 認証モードを設定します。
IEEE802.1X 認証モードを有効にすると、認証により許容された端末(Supplicant)以外の通信は遮断されます。

[注意]

本モードが有効と指定された場合、dot1x use 定義でシステム側が無効となっている場合はポート認証は行われません。

IEEE802.1X 認証を有効にしたポートを VLAN に含めることはできません。VLAN 定義に含まれるポートで IEEE802.1X 認証を有効にした場合、そのポートは利用できなくなります。

認証処理時に VLAN ID の通知がない場合は wlan dot1x vid コマンド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。

接続中の再認証で RADIUS サーバから通知された VLAN ID が変更となった場合は、一旦認証失敗として切断します。

同一ポートで併用できる認証機能は以下のとおりです。

機種	IEEE802.1X 認証	MAC アドレス認証
SR-M630AP1 SR-M610AP1	○	○

1 つの無線 LAN インタフェースで MAC アドレス認証と併用した場合、両方の認証に成功した端末のみ接続できます。その場合、両方の認証で同じ VLAN を割り当てるようにしてください。

以下の認証モードを利用する場合、IEEE802.1X 認証機能は無効で動作します。

open, shared, enhanced-open, open/enhanced-open, open/enhanced-open_owe

[未設定時]

IEEE802.1X 認証モードを無効にするものとみなされます。

```
wlan <number> dot1x use off
```

5.4.2 wlan dot1x supptimeout

[機能]

無線 LAN インタフェースの EAP 応答待ち時間の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> dot1x supptimeout <time>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<time>

EAP パケットの応答待ち時間を 1~600 秒の範囲で指定します。
単位は、m(分)、s(秒)のどちらかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IEEE802.11 認証モードとして IEEE802.1X 認証を使用する場合における、端末(Supplicant)に対する EAP 応答待ち時間を設定します。
運用で問題が生じていない場合は、本設定を変更しないで運用してください。

[注意]

本設定を変更した場合、認証にかかる時間が長くなる場合があります。

[未設定時]

EAP 応答待ち時間として 30 秒が設定されたものとみなされます。

```
wlan <number> dot1x supptimeout 30s
```

5.4.3 wlan dot1x maxreq

[機能]

無線 LAN インタフェースの EAP 再送回数の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> dot1x maxreq <count>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<count>

EAP 再送回数を 1～10 回の範囲で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IEEE802.11 認証モードとして IEEE802.1X 認証を使用する場合における、EAP 応答が受信できない場合の EAP 再送回数を指定します。

運用で問題が生じていない場合は、本設定を変更しないで運用してください。

[未設定時]

EAP 再送回数として 3 回が設定されたものとみなされます。

```
wlan <number> dot1x maxreq 3
```

5.4.4 wlan dot1x reauthperiod

[機能]

無線 LAN インタフェースの再認証間隔の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> dot1x reauthperiod <time>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<time>

- infinity
再認証を行いません。この場合は、端末(Supplicant)からのログオフメッセージを受信するか、無線 LAN インタフェースのダウンを検出するまでは認証済みの状態が保持されます。
- 上記以外
再認証間隔を 3600~18000 秒の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

端末(Supplicant)の再認証間隔を指定します。
運用で問題が生じていない場合は、本設定を変更しないで運用してください。

[注意]

timeout が生じた場合、応答にかかる時間が長くなる可能性があります。

[未設定時]

再認証間隔として 3600 秒(1 時間)が設定されたものとみなされます。

```
wlan <number> dot1x reauthperiod 1h
```

5.4.5 wlan dot1x aaa

[機能]

無線 LAN インタフェースが参照する AAA 情報の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> dot1x aaa <group_id>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<group_id>

- unuse
AAA 情報を使用しません。
- AAA のグループ ID
AAA のグループ ID を、10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IEEE802.1X 認証時に参照する AAA のグループ ID を指定します。

[注意]

AAA グループ ID は必須設定項目です。IEEE802.1X 認証が有効である無線 LAN インタフェースで AAA グループ ID が未設定の場合、その無線 LAN インタフェースでは IEEE802.1X 認証が利用できなくなります。

[未設定時]

AAA 情報を使用しないものとみなされます。

```
wlan <number> dot1x aaa unuse
```

5.4.6 wlan dot1x vid

[機能]

端末(Supplicant)に割り当てるデフォルト VLAN ID

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> dot1x vid <vid>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<vid>

端末(Supplicant)に割り当てるデフォルト VLAN ID を、1~4094 の範囲で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IEEE802.1X 認証が成功したときに端末(Supplicant)に割り当てるデフォルト VLAN ID を指定します。

[注意]

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、RADIUS サーバから通知された VLAN ID が割り当てられます。

本設定で指定される 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。

IEEE802.1X 認証と MAC アドレス認証を併用する場合、wlan dot1x vid コマンドと wlan macauth vid コマンドは必ず同じ設定にしてください。

[未設定時]

デフォルト VLAN ID を設定しないものとみなされます。なお、本コマンドの設定がなく RADIUS サーバからの VLAN ID がない場合は、システムログに VLAN ID の通知がない旨表示のうえ、認証に成功した端末(Supplicant)を VLAN1 にマッピングします。

5.4.7 wlan dot1x vlan assign

[機能]

無線 LAN インタフェースの VLAN 割り当て方式の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> dot1x vlan assign <mode>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<mode>

RADIUS サーバから通知された VLAN ID を端末(Supplicant)に割り当てるかどうかを指定します。

- enable
VLAN ID を割り当てます。
- disable
VLAN ID を割り当てません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IEEE802.1X 認証が成功したときに RADIUS サーバから通知された VLAN ID の端末(Supplicant)への割り当て方式を設定します。

<mode>が enable の場合

RADIUS サーバから VLAN ID が通知されなかった場合、wlan dot1x vid コマンドで設定された VLAN ID が割り当てられます。

wlan dot1x vid コマンドが未設定の場合は VLAN1 が割り当てられます。

<mode>が disable の場合

RADIUS サーバからの VLAN ID 通知有無にかかわらず wlan dot1x vid コマンドで設定された VLAN ID が割り当てられます。

wlan dot1x vid コマンドが未設定の場合は VLAN1 が割り当てられます。

[注意]

V20.04 以前のソフトウェアでの注意事項

- 本コマンドは、V20.05 以降のソフトウェアで動作します。
V20.04 以前のソフトウェアでは、enable に設定されている場合でも disable とみなして動作します。

V20.05 以降のソフトウェアでの注意事項

- IEEE802.1X 認証と MAC アドレス認証を併用する場合、wlan dot1x vlan assign コマンドと wlan macauth vlan assign コマンドは必ず同じ設定にする必要があります。
- 以下の機能を利用する場合は、本コマンドを disable に設定する必要があります。
 - WEP 機能(wlan wep mode enable)
 - ProxyARP 機能(proxyarp use on)
 - バンドステアリング機能(wlan band-steering mode enable)

[未設定時]

RADIUS サーバから通知された VLAN ID を端末(Supplicant)に割り当てるものとみなされます。

```
wlan <number> dot1x vlan assign enable
```

5.4.8 wlan dot1x backup

[機能]

無線 LAN インタフェースの認証自動切替の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> dot1x backup <mode> [{<recovery_time>|<wlan_number>}]
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<mode>

- off
この無線 LAN インタフェースでは認証自動切替を行いません。
- master
この無線 LAN インタフェースを認証自動切替の対象とします。
- backup
認証自動切替対象とした無線 LAN インタフェースのバックアップとして動作します。

<recovery_time>

RADIUS サーバが復活してからバックアップを解除するまでの時間を指定します。

<mode>に master を指定した場合にだけ指定できます。

- <recovery_time>
RADIUS サーバが復活してからバックアップを解除するまでの時間を 0~600 秒(10 分)の範囲で指定します。
単位は、m(分)、s(秒)のどちらかを指定します。
0 秒を指定した場合は、即時復旧します。
- manual
自動復旧しません。

<wlan_number>

バックアップ対象の無線 LAN インタフェース番号を指定します。

<mode>に backup を指定した場合にだけ指定できます。

- バックアップ対象の無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IEEE802.1X 認証を行うことができない場合のバックアップを設定します。

master 指定した無線 LAN インタフェースには IEEE802.1X 認証の設定を行い、backup 指定した無線 LAN インタフェースには WPA-PSK などの IEEE802.1X 認証以外の認証設定を行います。

RADIUS 認証サーバが使用できる状態では、backup 指定した無線 LAN インタフェースを閉塞状態とします。

RADIUS 認証サーバが使用不可となった場合は、master 指定した無線 LAN インタフェースを閉塞状態とし、backup 指定した無線 LAN インタフェースを閉塞解除することで、IEEE802.1X 認証が使用できない場合に自動的に認証の切り替えを行うことができます。

[注意]

wlan dot1x use on としたインタフェースでは backup に設定することはできません。

[未設定時]

認証自動切替を行いません。

```
wlan <number> dot1x backup off
```

5.5 MAC アドレス認証情報

5.5.1 wlan macauth use

[機能]

無線 LAN インタフェースの MAC アドレス認証使用の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> macauth use <mode>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<mode>

- on
MAC アドレス認証機能を使用します。
- off
MAC アドレス認証機能を使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証機能の使用について設定します。

<mode>が on の場合、Authentication フレーム送信元端末の 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無線接続の開始を許可し、認められていなければパケットを破棄します。

<mode>が off の場合、MAC アドレス認証機能は無効です。

[注意]

また、本コマンドと同時に、wlan macauth aaa <group_id>で認証先データベースの指定を行ってください。

本コマンドを動的定義変更すると該当ポートはいったん閉塞し MAC アドレス認証状態を初期化します。

認証実行時に VLAN ID の通知がない場合は wlan macauth vid コマンド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 MAC アドレス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。

接続中の再認証で RADIUS サーバから通知された VLAN ID が変更となった場合は、一旦認証失敗として切断します。

同一ポートで併用できる認証機能は以下のとおりです。

機種	IEEE802.1X 認証	MAC アドレス認証
SR-M630AP1 SR-M610AP1	○	○

1 つの無線 LAN インタフェースで IEEE802.1X 認証と併用した場合、両方の認証に成功した端末のみ接続できます。その場合、両方の認証で同じ VLAN を割り当てるようにしてください。

以下の認証モードを使用する場合、認証サーバから通知された VLAN を割り当てる機能を無効 (wlan macauth vlan assign disable) にし、端末に割り当てるデフォルト VLAN ID 機能 (wlan macauth vid) を利用してください。

open, shared, open/enhanced-open, open/enhanced-open_owe

[未設定時]

MAC アドレス認証機能を使用しないものとみなされます。

```
wlan <number> macauth use off
```

5.5.2 wlan macauth aaa

[機能]

無線 LAN インタフェースの MAC アドレス認証で参照する AAA グループ ID の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> macauth aaa <group_id>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<group_id>

- グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証先データベースのグループ ID を設定します。

[注意]

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、そのポートは利用できなくなります。

本コマンドを動的定義変更すると該当ポートはいったん閉塞し MAC アドレス認証状態を初期化します。

[未設定時]

グループ ID の指定をしないものとみなされます。

```
wlan <number> macauth aaa unuse
```

5.5.3 wlan macauth expire

[機能]

無線 LAN インタフェースの MAC アドレス認証結果保持時間の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> macauth expire <success_time> <failure_time>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<success_time>

- 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。
単位は、s(秒)、m(分)、h(時)、d(日)のどれかを指定します。

<failure_time>

- 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。
単位は、s(秒)、m(分)、h(時)、d(日)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証結果の保持時間を設定します。
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。
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。

[未設定時]

MAC アドレス認証結果保持時間に認証成功保持時間 20 分、失敗保持時間 5 分が設定されたものとみなされます。

```
wlan <number> macauth expire 20m 5m
```

5.5.4 wlan macauth vid

[機能]

無線 LAN インタフェースの端末(Supplicant)に割り当てるデフォルト VLAN ID の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> macauth vid <vid>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<vid>

端末(Supplicant)に割り当てるデフォルト VLAN ID を、1~4094 の範囲で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証が成功したときに端末(Supplicant)に割り当てるデフォルト VLAN ID を指定します。

[注意]

本設定で指定される 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。

本コマンドを動的定義変更すると該当ポートはいったん閉塞し MAC アドレス認証状態を初期化します。

IEEE802.1X 認証と MAC アドレス認証を併用する場合、wlan dot1x vid コマンドと wlan macauth vid コマンドは必ず同じ設定にしてください。

[未設定時]

デフォルト VLAN ID を設定しないものとみなされます。

なお、本コマンドの設定がなく RADIUS サーバからの VLAN ID がない場合は、システムログに VLAN ID の通知がない旨表示のうえ、認証に成功した端末(Supplicant)を VLAN1 にマッピングします。

5.5.5 wlan macauth vlan assign

[機能]

無線 LAN インタフェースの VLAN 割り当て方式の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlan <number> macauth vlan assign <mode>
```

[オプション]

<number>

- 無線 LAN インタフェース番号
無線 LAN インタフェース番号を、10 進数で指定します。

<mode>

RADIUS サーバから通知された VLAN ID を端末(Supplicant)に割り当てるかどうかを指定します。

- enable
VLAN ID を割り当てます。
- disable
VLAN ID を割り当てません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証が成功したときに RADIUS サーバから通知された VLAN ID の、端末(Supplicant)への割り当て方式を設定します。

<mode>が enable の場合

RADIUS サーバから VLAN ID が通知された場合、その VLAN ID が割り当てられます。

RADIUS サーバから VLAN ID が通知されなかった場合、wlan macauth vid コマンドで設定された VLAN ID が割り当てられます。

wlan macauth vid コマンドが未設定の場合は VLAN1 が割り当てられます。

<mode> が disable の場合

RADIUS サーバからの VLAN ID 通知有無にかかわらず、wlan macauth vid コマンドで設定された VLAN ID が割り当てられます。

wlan macauth vid コマンドが未設定の場合は VLAN1 が割り当てられます。

[注意]

V20.04 以前のソフトウェアでの注意事項

- 本コマンドは、V20.05 以降のソフトウェアで動作します。
V20.04 以前のソフトウェアでは、enable に設定されている場合でも disable とみなして動作します。

V20.05 以降のソフトウェアでの注意事項

- IEEE802.1X 認証と MAC アドレス認証を併用する場合、wlan dot1x vlan assign コマンドと wlan macauth vlan assign コマンドは必ず同じ設定にする必要があります。
- 以下の機能を利用する場合は、本コマンドを disable に設定する必要があります。
 - WEP 機能(wlan wep mode enable)
 - ProxyARP 機能(proxyarp use on)
 - バンドステアリング機能(wlan band-steering mode enable)

[未設定時]

RADIUS サーバから通知された VLAN ID を端末(Supplicant)に割り当てるものとみなされます。

```
wlan <number> macauth vlan assign enable
```

第 6 章 エアタイムフェアネス情報の設定

6.1 エアタイムフェアネス情報

6.1.1 atf use

[機能]

エアタイムフェアネスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

atf use <mode>

[オプション]

<number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

<mode>

- on
エアタイムフェアネスを有効にします。
- off
エアタイムフェアネスを無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

エアタイムフェアネス機能の有効/無効を設定します。

[未設定時]

エアタイムフェアネス機能は無効とみなされます。

```
atf use off
```

第 7 章 VLAN 情報の設定

- VLAN ID の指定範囲

本章のコマンドの[オプション]に記載されている<vid>(VLAN VID)は、以下に示す範囲で指定してください。

範囲	機種
1~4094	SR-M630AP1 SR-M610AP1

7.1 VLAN 共通情報

7.1.1 vlan name

[機能]

VLAN 名の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
vlan <vid> name <name>
```

[オプション]

<vid>

- VLAN ID

VLAN ID を、10 進数で指定します。

※VLAN1 はデフォルト VLAN として装置起動時にポート VLAN として定義されており、“default”の VLAN 名で登録されています。

<name>

- VLAN 名

VLAN 名を、0x21、0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

(入力可能な文字の一覧については、コマンドユーザズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

VLAN の名前を設定します。

本コマンドが未設定の場合、VLAN1 は“default”と設定されます。

また、VLAN1 以外の VLAN 作成時には、'v'+<vid>の形式で設定されます。

(例:vid=5 の場合は、“v5”と設定されます。)

[注意]

“delete vlan <vid> name”とした場合、VLAN 名は初期値に戻りますが、VLAN 自体は削除されません。(VLAN の削除には、ether vlan コマンドの削除が必要です。)

[初期値]

```
vlan 1 name default
```

[未設定時]

```
vlan <vid> name 'v'+<vid>
```

7.1.2 vlan description

[機能]

VLAN の説明文の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
vlan <vid> description <description>
```

[オプション]

<vid>

- ・ VLAN ID
VLAN ID を、10 進数で指定します。

<description>

- ・ 説明文
この VLAN の説明文を、0x21, 0x23~0x7e の 50 文字以内の ASCII 文字列で記入します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

この VLAN についての説明文を記入します。

[未設定時]

説明文を記入しないものとみなされます。

7.2 フィルタ情報

7.2.1 vlan filter

[機能]

VLAN のフィルタの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
vlan <vid> filter <count> <action> <acl_count>
```

[オプション]

<vid>

- VLAN ID
VLAN ID を、10 進数で指定します。

<count>

- 優先順位
指定するフィルタ設定の優先順位を、10 進数で指定します。
小さい値が優先順位がより高いことを示します。

範囲	機種
0~235	SR-M630AP1 SR-M610AP1

<action>

- pass
アクセスコントロールリストの "acl ip"、"acl icmp"、"acl tcp"、および "acl udp" 定義に該当したパケットを透過させます。
- reject
アクセスコントロールリストの "acl ip"、"acl icmp"、"acl tcp"、および "acl udp" 定義に該当したパケットを破棄します。

<acl_count>

- ACL 定義番号
フィルタ設定したいパケットパターンを定義したアクセスコントロールリストの ACL 定義番号を指定します。

範囲	機種
0~599	SR-M630AP1 SR-M610AP1

[動作モード]

構成定義モード(管理者クラス)

[説明]

VLAN ごとのフィルタリングの設定を行います。

<acl_count>で指定したアクセスコントロールリスト内の "acl ip"、"acl icmp"、"acl tcp"、および "acl udp" 定義に該当した入力パケットに対して、<action>で指定したフィルタ処理を実施します。

[注意]

- <acl_count>で指定したアクセスコントロールリスト内に "acl ip" 定義が存在しない場合、および <acl_count>で指定したアクセスコントロールリストが存在しない場合はフィルタは適用されません。
- フィルタリング処理が適用されるのは、有線-無線インタフェース間の通信が対象となります。

-
- 本装置のフィルタリング機能は、IP フィルタとなります。
 - フィルタリング処理が適用されるのは、以下の通信となります。
 - 本装置あての通信
 - 有線–無線インタフェース間の通信
 - 無線–無線インタフェース間の通信（ただし、同一無線 LAN インタフェース内の折り返し通信は対象外）
 - IP フィルタ処理は、レイヤ 3 レベルでのソフトウェア処理のため、レイヤ 2 レベルでの VLAN 単位での制御はできず、IP フィルタ条件のみの制御となります。
そのため、本コマンドを設定する VLAN ID には意味を持ちません。ご使用される VLAN のうち任意の VLAN ID を 1 つ選んでいただき、装置全体のフィルタリングルールとして設定してください。

[未設定時]

設定されなかったものとして動作します。

第 8 章 MAC 情報

8.1 MAC 情報

8.1.1 mac age

[機能]

MAC アドレス学習テーブルのエイジングアウト時間の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

mac age <time>

[オプション]

<time>

- ・ エージングアウト時間

MAC アドレス学習テーブルのエイジングアウト時間を、10～1,000,000 秒の範囲の秒単位で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス学習テーブルのエイジングアウト時間を設定します。

[未設定時]

エイジングアウト時間に 300 秒が設定されたものとみなされます。

```
mac age 300
```

第 9 章 LAN 情報の設定

- lan 定義番号の指定範囲

本章のコマンドの[オプション]に記載されている<number>(lan 定義番号)に指定する lan 定義の通し番号(10進数)は、以下に示す範囲で指定してください。

範囲	機種
0~19	SR-M630AP1 SR-M610AP1

9.1 IP 関連情報

9.1.1 lan ip address

[機能]

IP アドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

lan <number> ip address <address>/<mask> <broadcast>

[オプション]

<number>

- lan 定義番号
lan 定義の通し番号を、10 進数で指定します。

<address>/<mask>

- IP アドレス/マスクビット数(またはマスク値)
LAN インタフェースに割り当てる IP 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。
IP アドレスの指定可能な範囲は以下のとおりです。
1. 0. 0. 1 ~ 126. 255. 255. 254
128. 0. 0. 1 ~ 191. 255. 255. 254
192. 0. 0. 1 ~ 223. 255. 255. 254
マスクビット数の場合は、2~30 の 10 進数で指定します。
マスク値の場合は、192. 0. 0. 0~255. 255. 255. 252 の範囲で指定します。
以下に、有効な記述形式を示します。
- IP アドレス/マスクビット数 (例: 192. 168. 1. 1/24)
- IP アドレス/マスク値 (例: 192. 168. 1. 1/255. 255. 255. 0)

<broadcast>

ブロードキャストアドレスを指定します。

- 1
255. 255. 255. 255 の場合に指定します。
- 2
<address>/<mask>から求められる、ネットワークアドレス + オール 0 の場合に指定します。
- 3
<address>/<mask>から求められる、ネットワークアドレス + オール 1 の場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本装置上の LAN インタフェースに、IP アドレス、マスクビット数(またはマスク値)、およびブロードキャストアドレスを設定します。

[注意]

本装置では<broadcast>に 0 を指定した場合でも、3 が設定されたものとみなして動作します。

[未設定時]

IP アドレスがないものとみなされます。

9.1.2 lan ip dhcp service

[機能]

DHCP 機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
lan <number> ip dhcp service <mode>
```

[オプション]

<number>

- lan 定義番号
lan 定義の通り番号を、10 進数で指定します。

<mode>

DHCP 機能のモードを指定します。

- client
LAN インタフェースに対して DHCP サービスを要求します。
- off
LAN インタフェースに対して DHCP 機能を提供しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

LAN インタフェースに対して、DHCP 機能情報を設定します。

[注意]

LAN インタフェースに lan ip address が設定されている場合、本コマンドは無効となります。
DHCP クライアント機能を使用する LAN インタフェースでは、スタティック ARP 機能は動作しません。

[未設定時]

DHCP クライアント機能を使用しないものとみなされます。

```
lan <number> ip dhcp service off
```


9.1.3 lan ip route

[機能]

IPv4 スタティック経路情報の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
lan <number> ip route <count> <address>/<mask> <next_hop> [<distance>]
```

[オプション]

<number>

- lan 定義番号
lan 定義の通し番号を、10 進数で指定します。

<count>

- スタティック経路情報定義番号
スタティック経路情報の定義番号を、10 進数で指定します。

範囲	機種
0~39	SR-M630AP1 SR-M610AP1

<address>/<mask>

- IPv4 アドレス/マスクビット数(またはマスク値)
あて先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
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)
- default
あて先ネットワークとしてデフォルトルートを設定する場合に指定します。
0.0.0.0/0(0.0.0.0/0.0.0.0)を指定するのと同じ意味になります。

<next_hop>

- 中継ルータ IPv4 アドレス
あて先ネットワークへパケットを送信するときの中継ルータの IPv4 アドレスを指定します。
- dhcp
DHCP サーバから受け取った router オプションのゲートウェイアドレスを中継ルータとして使用する場合に指定します。
<number>で指定した lan の定義上に、DHCP クライアントの設定がある場合のみ有効となります。

<distance>

- 優先度
このスタティック経路情報の優先度を、1~254 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。
省略時は、1 を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IPv4 スタティック経路(静的経路)情報を設定します。

<distance>で指定した優先度は、同じあて先への経路情報が複数ある場合、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。

DHCP クライアント運用を行う場合で、Router オプションでゲートウェイアドレスが通知された場合、ゲートウェイアドレス向け優先度 1 のデフォルトルートが自動生成されます。

この IPv4 スタティック経路は、DHCP クライアントが DHCP サーバから Router オプションを受け取った時点で有効となります。

ゲートウェイアドレスを受け取れるのは、IPv4 スタティック経路と同じ lan 定義番号で動作する DHCP クライアントからのみです。

IPv4 スタティック経路情報は、本装置全体で以下の数まで定義できます。

範囲	機種
40	SR-M630AP1 SR-M610AP1

[注意]

同じあて先へのスタティック経路情報は、同じ優先度で複数設定できません。

[未設定時]

IPv4 スタティック経路情報を使用しないものとみなされます。

ただし、DHCP クライアントを有効としたインタフェース上の場合、優先度が 1 で<next_hop>に dhcp が指定された default ルートが設定されたものとみなされます。

9.1.4 lan ip arp static

[機能]

スタティック ARP の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
lan <number> ip arp static <count> <dst> <mac>
```

[オプション]

<number>

- lan 定義番号
lan 定義の通し番号を、10 進数で指定します。

<count>

- スタティック ARP テーブル定義番号
指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正とみなされます。

範囲	機種
0～199	SR-M630AP1 SR-M610AP1

<dst>

- 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。
IP アドレスの指定可能な範囲は以下のとおりです。
1. 0. 0. 1 ~ 126. 255. 255. 254
128. 0. 0. 1 ~ 191. 255. 255. 254
192. 0. 0. 1 ~ 223. 255. 255. 254

<mac>

- 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。
xx:xx:xx:xx:xx:xx (xx は 2 桁の 16 進数) の形式で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ARP テーブルに静的な ARP エントリを設定する場合に、IP アドレスと MAC アドレスの対応を設定します。

[注意]

同じあて先 IP アドレスを持つスタティック ARP 定義を複数設定することはできません。
IP アドレスが設定されていないインタフェースでは、スタティック ARP 機能は動作しません。
DHCP クライアント機能を使用する LAN インタフェースでは、スタティック ARP 機能は動作しません。

[未設定時]

スタティック ARP 機能を使用しないものとみなされます。

9.2 VLAN 関連情報

9.2.1 lan vlan

[機能]

VLAN ID の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

lan <number> vlan <vid>

[オプション]

<number>

- ・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。

<vid>

VLAN ID を、1~4094 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

VLAN ID と lan 定義番号を関連付けを行います。

[注意]

- ・ <vid>で指定された VLAN が未登録の場合、設定は無効となります。
- ・ <vid>で指定された VLAN が複数の lan に対して設定された場合は、もっとも小さい lan 定義のみが有効となります。

[未設定時]

なし

9.3 SNMP 関連情報

9.3.1 lan snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
lan <number> snmp trap linkdown <mode>
```

[オプション]

<number>

- lan 定義番号
lan 定義の通し番号を、10 進数で指定します。

<mode>

- トラップの動作を指定します。
 - enable
トラップを有効にします。
 - disable
トラップを無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

linkDown トラップを有効または無効にするかを設定します。

[注意]

snmp trap linkdown で trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkDown トラップが有効とみなされます。

```
lan <number> snmp trap linkdown enable
```

9.3.2 lan snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
lan <number> snmp trap linkup <mode>
```

[オプション]

<number>

- ・ lan 定義番号
lan 定義の通し番号を、10 進数で指定します。

<mode>

- トラップの動作を指定します。
- ・ enable
トラップを有効にします。
 - ・ disable
トラップを無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

linkUp トラップを有効または無効にするかを設定します。

[注意]

snmp trap linkup で trap 動作が無効にされた場合は、本コマンド設定値は意味を持ちません。

[未設定時]

linkUp トラップが有効とみなされます。

```
lan <number> snmp trap linkup enable
```

第 10 章 IP 関連情報

10.1 IP 関連情報

10.1.1 ip arp age

[機能]

ARP エントリ有効時間の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ip arp age <time>
```

[オプション]

<time>

ARP エントリの有効時間(分)を、1~240 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ARP エントリの有効時間を設定します。

実際の有効時間は<time>/2 から 3×<time>/2 のランダムな値になります。

[未設定時]

20 分が設定されたものとみなされます。

```
ip arp age 20
```

第 11 章 認証情報の設定

11.1 IEEE802.1X 情報

11.1.1 dot1x use

[機能]

IEEE802.1X 認証モードの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

dot1x use <mode>

[オプション]

<mode>

IEEE802.1X 認証のモードを指定します。

- on
IEEE802.1X 認証を有効にします。
- off
IEEE802.1X 認証を無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IEEE802.1X 認証の利用有無を指定します。

[注意]

本モードが有効と指定された場合でも、wlan dot1x use 定義で設定が無効となっている場合は IEEE802.1X 認証は行われません。

[未設定時]

IEEE802.1X 認証を使用しないものとみなされます。

```
dot1x use off
```

11.2 MAC アドレス認証情報

11.2.1 macauth use

[機能]

MAC アドレス認証基本情報の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

macauth use <mode>

[オプション]

<mode>

MAC アドレス認証を装置として使用するかどうかを指定します。

- on
MAC アドレス認証を使用します。
- off
MAC アドレス認証を使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証を装置として使用するかどうかを指定します。

[注意]

本モードが有効と指定された場合でも、wlan macauth use 定義でポート側が無効となっている場合は MAC アドレス認証は行われません。

本コマンドを動的定義変更すると該当ポートはいったん閉塞し MAC アドレス認証状態を初期化します。

[未設定時]

MAC アドレス認証を装置として使用しないものとみなされます。

```
macauth use off
```

11.2.2 macauth password

[機能]

MAC アドレス認証情報(パスワード)の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
macauth password <password> [encrypted]
```

[オプション]

<password>

- ・ 認証パスワード

認証パスワードを、0x21, 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。

show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。

show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- ・ 暗号化認証パスワード指定

<password>に暗号化された認証パスワードを設定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証で使用する、認証情報(認証パスワード)を設定します。

本コマンドが未設定の場合は、認証端末の MAC アドレスが認証情報として使用されます。

[注意]

show コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

本コマンドを動的定義変更すると該当ポートはいったん閉塞し MAC アドレス認証状態を初期化します。

[未設定時]

MAC アドレス認証情報に認証端末の MAC アドレスを使用するものとみなされます。

11.2.3 macauth type

[機能]

MAC アドレス認証の認証プロトコルの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

macauth type <authtype>

[オプション]

<authtype>

- chap_md5
認証プロトコルに MD5-CHAP を使用します。
- pap
認証プロトコルに PAP を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証の認証プロトコルを設定します。

[未設定時]

MAC アドレス認証の認証プロトコルとして MD5-CHAP が設定されたものとみなされます。

```
macauth type chap-md5
```

第 12 章 ACL 情報の設定

- ACL 定義番号の指定範囲

本章のコマンドの[オプション]に記載されている<acl_count>に指定する ACL 定義番号(10 進数)は、以下に示す範囲で指定してください。

範囲	機種
0~599	SR-M630AP1 SR-M610AP1

12.1 ACL 情報

12.1.1 acl mac

[機能]

ACL MAC 定義

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
acl <acl_count> mac <src_mac> <dst_mac>
```

[オプション]

<acl_count>

- ACL 定義番号
ACL 定義の通し番号を、10 進数で指定します。

<src_mac>

ACL 対象とする送信元 MAC アドレスを指定します。

- any
すべての MAC アドレスを対象とする場合に指定します。
- 上記以外
対象とする MAC アドレスを指定します。ACL 対象とする送信元 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。

<dst_mac>

ACL 対象とするあて先 MAC アドレスを指定します。

- any
すべての MAC アドレスを対象とする場合に指定します。
- 上記以外
対象とする MAC アドレスを指定します。ACL 対象とする送信元 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。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ACL 定義で MAC アドレスのパターンを指定します。

[未設定時]

ACL 定義でどのような MAC アドレスのパターンでも対象とします。

12.1.2 acl ip

[機能]

ACL IPv4 定義

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
acl <acl_count> ip <src_addr>/<mask> <dst_addr>/<mask> [<protocol>]
```

[オプション]

<acl_count>

- ACL 定義番号
ACL 定義の通り番号を、10 進数で指定します。

<src_addr>/<mask>

ACL 対象とする送信元 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数(またはマスク値)
ACL 対象とする送信元 IP 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。
- IP アドレス/マスクビット数(例: 192.168.1.1/24)
- any
すべての送信元 IP アドレスを ACL 対象とする場合に指定します。
0.0.0.0/0 を指定するのと同じ意味になります。

<dst_addr>/<mask>

ACL 対象とするあて先 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数(またはマスク値)
ACL 対象とするあて先 IP アドレスとマスクビット数の組み合わせを指定します。
記述形式は、<src_addr>/<mask>と同様です。
- any
すべてのあて先 IP アドレスを ACL 対象とする場合に指定します。
0.0.0.0/0 を指定するのと同じ意味になります。

<protocol>

ACL 対象とするプロトコル番号を指定します。

- プロトコル番号
ACL 対象とするプロトコル番号を、0~255 の 10 進数で指定します(例: ICMP:1、TCP:6、UDP:17 など)。
- any
すべてのプロトコル番号を ACL 対象とする場合に指定します。
0 を指定するのと同じ意味になります。
省略時は、any を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ACL 定義で IPv4 パケットのパターンを指定します。

[注意]

TCP, UDP, ICMP などの L3 プロトコル利用時には必ず acl ip を定義してください。

[未設定時]

ACL 定義でどのような IP パケットのパターンでも対象とします。
(all any 設定時、未定義では acl 定義は存在しません)

12.1.3 acl tcp

[機能]

ACL TCP 定義

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
acl <acl_count> tcp <src_port> <dst_port>
```

[オプション]

<acl_count>

- ACL 定義番号
ACL 定義の通し番号を、10 進数で指定します。

<src_port>

ACL 対象とする送信元ポート番号を指定します。

- ポート番号
ACL 対象とする送信元ポート番号を、1~65535 の 10 進数で指定します。
複数のポート番号を指定する場合は、","(カンマ)で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン)を使用して指定します。
ポート番号は、","(カンマ)および"-"(ハイフン)を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
以下に、有効な記述形式を示します。
 - 1~65535 の 10 進数値 (例: 65535 = 65535 ポート)
 - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
 - ポート番号- (例: 1- = 1 から 65535 までのポート)
 - ポート番号 (例: -1000 = 1 から 1000 までのポート)
 - ポート番号, ポート番号, … (例: 10, 20, 30- = 10 と 20 と 30 以降のポート)
- any
すべての送信元ポート番号を ACL 対象とする場合に指定します。

<dst_port>

ACL 対象とするあて先ポート番号を指定します。

- ポート番号
ACL 対象とするあて先ポート番号を、1~65535 の 10 進数で指定します。
記述形式は、<src_port>と同様です。
- any
すべてのあて先ポート番号を ACL 対象とする場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ACL 定義で TCP パケットのパターンを指定します。

[注意]

利用時には必ず acl ip で protocol(tcp 6)を指定してください。

[未設定時]

ACL 定義でどのような TCP パケットのパターンでも対象とします。

12.1.4 acl udp

[機能]

ACL UDP 定義

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
acl <acl_count> udp <src_port> <dst_port>
```

[オプション]

<acl_count>

- ACL 定義番号
ACL 定義の通し番号を、10 進数で指定します。

<src_port>

ACL 対象とする送信元ポート番号を指定します。

- ポート番号
ACL 対象とする送信元ポート番号を、1~65535 の 10 進数で指定します。
複数のポート番号を指定する場合は、","(カンマ)で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン)を使用して指定します。
ポート番号は、","(カンマ)および"-"(ハイフン)を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
以下に、有効な記述形式を示します。
 - 1~65535 の 10 進数値 (例: 65535 = 65535 ポート)
 - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
 - ポート番号- (例: 1- = 1 から 65535 までのポート)
 - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
 - ポート番号, ポート番号, … (例: 10, 20, 30- = 10 と 20 と 30 以降のポート)
- any
すべての送信元ポート番号を ACL 対象とする場合に指定します。

<dst_port>

ACL 対象とするあて先ポート番号を指定します。

- ポート番号
ACL 対象とするあて先ポート番号を、1~65535 の 10 進数で指定します。
記述形式は、<src_port>と同様です。
- any
すべてのあて先ポート番号を ACL 対象とする場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ACL 定義で UDP パケットのパターンを指定します。

[注意]

利用時には必ず `acl ip` で `protocol(udp 17)` を指定してください。

[未設定時]

ACL 定義でどのような UDP パケットのパターンでも対象とします。

12.1.5 acl icmp

[機能]

ACL ICMP 定義

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
acl <acl_count> icmp <icmptype>
```

[オプション]

<acl_count>

- ACL 定義番号
ACL 定義の通し番号を、10 進数で指定します。

<icmptype>

ACL 対象とする ICMP TYPE を指定します。

- ICMP TYPE
ACL 対象とする送信元 ICMP TYPE を、0~255 の 10 進数で指定します。
複数の ICMP TYPE を指定する場合は、","(カンマ)で区切って指定します。また、範囲指定する場合は、「8-30」のように"-"(ハイフン)を使用して指定します。
ICMP TYPE は、","(カンマ)および"-"(ハイフン)を使用して、10 個まで指定できます。
以下に、有効な記述形式を示します。
 - 0~255 の 10 進数値 (例: 8 = ICMP TYPE 8)
 - ICMP TYPE-ICMP TYPE (例: 2-8 = 2 から 8 までの ICMP TYPE)
 - ICMP TYPE- (例: 8- = 8 から 255 までの ICMP TYPE)
 - -ICMP TYPE (例: -200 = 0 から 200 までの ICMP TYPE)
 - ICMP TYPE, ICMP TYPE, … (例: 0, 8, 30- = 0 と 8 と 30 以降の ICMP TYPE)
- any
すべての ICMP TYPE を ACL 対象とする場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ACL 定義で ICMP パケットのパターンを指定します。

[注意]

利用時には必ず `acl ip <protocol>(icmp 1)` を指定してください。

[未設定時]

ACL 定義でどのような ICMP パケットのパターンでも対象とします。

12.1.6 acl description

[機能]

ACL description 定義

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
acl <acl_count> description <description>
```

[オプション]

<acl_count>

- ・ ACL 定義番号
ACL 定義の通し番号を、10 進数で指定します。

<description>

- ・ 設定の説明
この ACL 定義番号で設定の説明を、0x21, 0x23~0x7e の 50 文字以内の ASCII 文字列で記入します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

この ACL 定義番号で設定の説明を記入します。

[未設定時]

設定の説明を記入しないものとみなされます。

第 13 章 AAA 情報の設定

- グループ ID の指定範囲

各コマンドの[オプション]に記載されている<group_id>(グループ ID)に指定するグループの通し番号(10進数)は、以下に示す範囲で指定してください。

範囲	機種
0~15	SR-M630AP1 SR-M610AP1

- RADIUS サーバ定義番号の指定範囲

各コマンドの[オプション]に記載されている<number>(RADIUS サーバ定義番号)に指定するグループ内の通し番号(10進数)は、以下に示す範囲で指定してください。

範囲	機種
0~3	SR-M630AP1 SR-M610AP1

※V20.05 以前のソフトウェアでは 0~1 となります。

13.1 グループ ID 情報

13.1.1 aaa name

[機能]

グループ名称の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

aaa <group_id> name <group_name>

[オプション]

<group_id>

- グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<group_name>

- 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。
(入力可能な文字の一覧については、コマンドユーザズガイドを参照してください。)

[動作モード]

構成定義モード(管理者クラス)

[説明]

グループ名を設定します。

[注意]

すでに同一名称のグループが登録されている場合は、異常終了します。

[未設定時]

グループ名を設定しないものとみなされます。

13.2 RADIUS 情報の設定

13.2.1 aaa radius service

[機能]

RADIUS サービスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius service <service> [<type>]
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<service>

- ・ client
RADIUS クライアント機能として使用します。
- ・ off
RADIUS 機能を使用しません。

<type>

<service>に client を指定した場合に有効なパラメタです。

- ・ auth
RADIUS 認証機能を有効にします。
- ・ accounting
RADIUS アカウンティング機能を有効にします。
- ・ both
RADIUS 認証機能と RADIUS アカウンティング機能を有効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

自装置で使用する RADIUS 機能の設定を行います。

[未設定時]

RADIUS 認証機能を使用しないものとみなされます。

```
aaa <group_id> radius service off
```

13.2.2 aaa radius auth source

[機能]

RADIUS 認証装置の自側 IP アドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius auth source <address>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<address>

- ・ 自側 IP アドレス
自側 RADIUS 認証サーバの 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。

IPv4

1. 0. 0. 1 ~ 126. 255. 255. 2544
128. 0. 0. 1 ~ 191. 255. 255. 254
192. 0. 0. 1 ~ 223. 255. 255. 254

[動作モード]

構成定義モード(管理者クラス)

[説明]

自側 RADIUS 認証装置の IP アドレスを設定します。
本装置を RADIUS 認証クライアントとして使用する場合は、RADIUS 認証サーバとの通信に使用する自側 IP アドレスを設定します。

[未設定時]

相手側の RADIUS 認証装置と通信を行う自側 IP アドレスを自動的に選択するものとみなされます。

13.2.3 aaa radius auth message-authenticator

[機能]

Message-Authenticator の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius auth message-authenticator <mode>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<mode>

- ・ off
Message-Authenticator による認証を行いません。
- ・ on
Message-Authenticator による認証を行います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

Message-Authenticator による認証を行うかどうかを設定します。
IEEE802.1X 認証時は本設定に関係なく Message-Authenticator による認証を行います。
本装置では、認証要求メッセージにのみ使用できます。

[未設定時]

Message-Authenticator による認証を行いません。

```
aaa <group_id> radius auth message-authenticator off
```

13.2.4 aaa radius accounting source

[機能]

RADIUS アカウンティング装置の自側 IP アドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius accounting source <address>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<address>

- ・ 自側 IP アドレス
自側 RADIUS アカウンティング装置の 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。

IPv4

1. 0. 0. 1 ~ 126. 255. 255. 254
128. 0. 0. 1 ~ 191. 255. 255. 254
192. 0. 0. 1 ~ 223. 255. 255. 254

[動作モード]

構成定義モード(管理者クラス)

[説明]

自側 RADIUS アカウンティング装置の IP アドレスを設定します。
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の通信に使用する自側 IP アドレスを設定します。

[未設定時]

相手側の RADIUS アカウンティング装置と通信を行う自側 IP アドレスを自動的に選択するものとみなされます。

13.2.5 aaa radius client server-info auth secret

[機能]

RADIUS 認証サーバ用共有鍵(RADIUS シークレット)の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info auth <number> secret <secret> [encrypted]
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<secret>

- ・ 共有鍵(RADIUS シークレット)
本装置と RADIUS 認証サーバとの間で取り決めた共有鍵(RADIUS シークレット)を、0x21, 0x23~0x7e の 64 文字以内の ASCII 文字列で指定します。
(入力可能な文字の一覧については、コマンドユーザズガイドを参照してください。)
- ・ 暗号化された共有鍵(RADIUS シークレット)
show コマンドで表示される暗号化された共有鍵(RADIUS シークレット)を encrypted と共に指定します。

encrypted

- ・ 暗号化共有鍵(RADIUS シークレット)指定
<secret>に暗号化された共有鍵(RADIUS シークレット)を指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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)を設定します。
show コマンドでは、暗号化された共有鍵(RADIUS シークレット)が encrypted と共に表示されます。

[未設定時]

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。

13.2.6 aaa radius client server-info auth address

[機能]

相手側 RADIUS 認証サーバの IP アドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info auth <number> address <address>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<address>

- ・ 相手側 IP アドレス
相手側となる RADIUS 認証装置の 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。

IPv4

1. 0. 0. 1 ~ 126. 255. 255. 254
128. 0. 0. 1 ~ 191. 255. 255. 254
192. 0. 0. 1 ~ 223. 255. 255. 254

[動作モード]

構成定義モード(管理者クラス)

[説明]

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。
複数サーバを指定することはできません。

[未設定時]

相手側 RADIUS 認証装置の IP アドレスを設定しないものとみなされます。RADIUS 認証機能を使用する場合は必ず設定してください。

13.2.7 aaa radius client server-info auth port

[機能]

認証サーバ UDP ポートの設定(旧 RFC 仕様対応)

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info auth <number> port <port>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<port>

- ・ 1812
最新 RFC 仕様の RADIUS 認証サーバに割り当てられた UDP ポート番号です。
- ・ 1645
旧 RFC 仕様の RADIUS 認証サーバに割り当てられた UDP ポート番号です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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。
認証要求する RADIUS 認証サーバが旧 RFC 仕様の UDP ポートで実装されている場合はポート番号に 1645 を設定してください。

[未設定時]

RADIUS 認証サーバの UDP ポート番号に 1812 を使用するものとみなされます。

```
aaa <group_id> radius client server-info auth <number> port 1812
```

13.2.8 aaa radius client server-info auth deadtime

[機能]

復旧待機時間の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info auth <number> deadtime <deadtime>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<deadtime>

- ・ 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、0~86400 (秒) の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。
0s を指定した場合は、自動的に alive 状態に復旧しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RADIUS サーバから aaa radius client retry コマンド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、以下のどれか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(radius recovery)で、手動で復旧させた場合
- ・ 認証自動切替機能(ICMP による監視)で正常応答状態となった場合

[未設定時]

自動的に復旧しないものとみなされます。

```
aaa <group_id> radius client server-info auth <number> deadtime 0s
```

13.2.9 aaa radius client server-info auth priority

[機能]

優先度の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info auth <number> priority <priority>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<priority>

- ・ 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、0～255 の範囲で指定します。
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。
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。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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、サーバ定義番号の小さい方が使われます。

[未設定時]

最優先が設定されたものとみなされます。

```
aaa <group_id> radius client server-info auth <number> priority 0
```

13.2.10 aaa radius client server-info auth source

[機能]

自側 IP アドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info auth <number> source <address>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<address>

- ・ 自側 IP アドレス
自側 RADIUS 認証サーバの 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。

IPv4

1. 0. 0. 1 ~ 126. 255. 255. 254
128. 0. 0. 1 ~ 191. 255. 255. 254
192. 0. 0. 1 ~ 223. 255. 255. 254

[動作モード]

構成定義モード(管理者クラス)

[説明]

自側 RADIUS 認証装置の IP アドレスを設定します。本定義の内容は、aaa radius auth source による、自側 RADIUS 認証装置の IP アドレスの設定より優先されます。

[未設定時]

aaa radius auth source による自側 RADIUS 認証装置の IP アドレスの設定に従うものとみなされます。

13.2.11 aaa radius client server-info auth watch type

[機能]

RADIUS サーバ監視種別の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info auth <number> watch type <type>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<type>

- ・ off
RADIUS サーバを監視しません。
- ・ icmp
RADIUS サーバを ICMP で監視します。
- ・ auth
RADIUS サーバを認証要求を使用して監視します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RADIUS サーバ監視種別を設定します。

[注意]

本設定は、認証自動切替機能を使用する場合の RADIUS サーバの生死を監視するために設定します。
監視種別に auth を指定した場合は、aaa radius client server-info auth watch user 定義も同時に定義しないと、認証による監視が行われません。

認証自動切替機能での切り替えが繰り返し行われるため、以下のコマンドは併用しないでください。

- ・ aaa radius client server-info auth deadtime コマンドを設定する。
- ・ 運用コマンド(radius recovery)で手動復旧させる。

[未設定時]

監視しないものとみなされます。

```
aaa <group_id> radius client server-info auth <number> watch type off
```

13.2.12 aaa radius client server-info auth watch user

[機能]

RADIUS サーバを監視する場合の認証情報の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info auth <number> watch user <id> [<password> [encrypted]]
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<id>

- ・ 認証 ID
認証 ID を、0x21, 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。

<password>

- ・ 省略
対話形式で認証パスワードを入力します。
- ・ 認証パスワード
認証パスワードを、0x21, 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。
- ・ 暗号化されたパスワード
show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- ・ 暗号化認証パスワード指定
<password>に暗号化された認証パスワードを設定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

認証で RADIUS サーバを監視する場合の認証情報を設定します。

認証パスワードを省略した場合は、対話形式でパスワードを入力できます。入力した認証パスワードの文字列は画面に表示されず、システムログ情報にも保存されないため、コマンド実行履歴出力の設定が有効な際もセキュリティ的に安全です。

対話形式で認証パスワードを入力する場合、入力文字を 1 文字削除する際は Delete キーを使用してください。

[注意]

show candidate-config、show running-config および show startup-config コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

[メッセージ]

Password:

<password>引数を省略した場合に表示されます。

認証パスワードを入力してください。
入力した認証パスワードは画面に表示されません。

Retype password:

<password>引数を省略した場合に表示されます。
再度、認証パスワードを入力してください。
入力した認証パスワードは画面に表示されません。

<ERROR> mismatched password

対話形式で2回入力した認証パスワードが一致しませんでした。
再度、認証情報の設定を行ってください。

[未設定時]

送信する認証情報を定義しないものとみなされます。

13.2.13 aaa radius client server-info auth <number> watch interval

[機能]

RADIUS サーバ監視の通常時の送信間隔の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info auth <number> watch interval <normal_interval>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<normal_interval>

- ・ 正常時送信間隔
正常時送信間隔を、1~600 秒(10 分)の範囲で指定します。
単位は、m(分)、s(秒)のどちらかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RADIUS サーバ監視の通常時の送信間隔を設定します。

[未設定時]

通常時、60 秒(1 分)ごとにサーバを監視するものとみなされます。

```
aaa <group_id> radius client server-info auth <number> watch interval 1m
```

13.2.14 aaa radius client server-info auth watch retry

[機能]

RADIUS サーバ監視の再送間隔の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info auth <number> watch retry <retry>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<retry>

- ・ 再送間隔
再送間隔を、1~60 秒(1 分)の範囲で指定します。
単位は、m(分)、s(秒)のどちらかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

通常時の監視で、応答が得られなかった場合の再送間隔を設定します。

[未設定時]

再送時、10 秒ごとにサーバを監視するものとみなされます。

```
aaa <group_id> radius client server-info auth <number> watch retry 10s
```

13.2.15 aaa radius client server-info auth watch timeout

[機能]

RADIUS サーバ監視のタイムアウト時間の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info auth <number> watch timeout <timeout>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<timeout>

- ・ タイムアウト時間
タイムアウト時間を、5~180 秒(3 分)の範囲で指定します。
単位は、m(分)、s(秒)のどちらかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RADIUS サーバ監視の再送タイムアウト時間を設定します。

[未設定時]

再送が 30 秒でタイムアウトするものとみなされます。

```
aaa <group_id> radius client server-info auth <number> watch timeout 30s
```

13.2.16 aaa radius client server-info auth watch abnormal-interval

[機能]

RADIUS サーバ監視の異常時の送信間隔の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info auth <number> watch abnormal-interval <abnormal_interval>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<abnormal_interval>

- ・ 異常時送信間隔
異常時送信間隔を、1～3600 秒(1 時間)の範囲で指定します。
単位は、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RADIUS サーバ監視の異常時の送信間隔を設定します。

[未設定時]

異常時、180 秒(3 分)ごとにサーバを監視するものとみなされます。

```
aaa <group_id> radius client server-info auth <number> watch abnormal-interval 3m
```

13.2.17 aaa radius client server-info accounting secret

[機能]

RADIUS アカウンティングサーバ用共有鍵(RADIUS シークレット)の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info accounting <number> secret <secret> [encrypted]
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<secret>

- ・ 共有鍵(RADIUS シークレット)
本装置と RADIUS アカウンティングサーバとの間で取り決めた共有鍵(RADIUS シークレット)を、0x21, 0x23～0x7e の 64 文字以内の ASCII 文字列で指定します。
(入力可能な文字の一覧については、コマンドユーザズガイドを参照してください。)
- ・ 暗号化された RADIUS シークレット文字列
show コマンドで表示される暗号化された共有鍵(RADIUS シークレット)を encrypted と共に指定します。

encrypted

- ・ 暗号化共有鍵(RADIUS シークレット)指定
<secret>に暗号化された共有鍵(RADIUS シークレット)を設定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

本装置と RADIUS アカウンティングサーバとの間で共有する共有鍵(RADIUS シークレット)を設定します。
show コマンドでは、暗号化された共有鍵(RADIUS シークレット)が encrypted と共に表示されます。

[未設定時]

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。

13.2.18 aaa radius client server-info accounting address

[機能]

相手側 RADIUS アカウンティングサーバの IP アドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info accounting <number> address <address>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<address>

- ・ 相手側 IP アドレス
相手側となる RADIUS アカウンティング装置の 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。

IPv4

1. 0. 0. 1 ~ 126. 255. 255. 254
128. 0. 0. 1 ~ 191. 255. 255. 254
192. 0. 0. 1 ~ 223. 255. 255. 254

[動作モード]

構成定義モード(管理者クラス)

[説明]

本装置と通信する RADIUS アカウンティングサーバの IP アドレスを設定します。

13.2.19 aaa radius client server-info accounting port

[機能]

アカウントティングサーバUDPポートの設定(旧 RFC 仕様対応)

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info accounting <number> port <port>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<port>

- ・ 1813
最新 RFC 仕様の RADIUS アカウントティングサーバに割り当てられた UDP ポート番号です。
- ・ 1646
旧 RFC 仕様の RADIUS アカウントティングサーバに割り当てられた UDP ポート番号です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RADIUS アカウントティングクライアントがアカウントティング要求する RADIUS アカウントティングサーバの UDP ポート番号を設定します。

アカウントティング要求する RADIUS アカウントティングサーバが旧 RFC 仕様の UDP ポートで実装されている場合はポート番号に 1646 を設定してください。

[未設定時]

RADIUS アカウントティングサーバの UDP ポート番号に 1813 を使用するものとみなされます。

```
aaa <group_id> radius client server-info accounting <number> port 1813
```

13.2.20 aaa radius client server-info accounting deadtime

[機能]

復旧待機時間の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info accounting <number> deadtime <deadtime>
```

[オプション]

<group_id>

- グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<deadtime>

- 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、0~86400 (秒) の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。
0s を指定した場合は、自動的に alive 状態に復旧しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RADIUS サーバから aaa radius client retry コマンド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、以下のどれか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(radius recovery)で、手動で復旧させた場合

[未設定時]

自動的に復旧しないものとみなされます。

```
aaa <group_id> radius client server-info accounting <number> deadtime 0s
```

13.2.21 aaa radius client server-info accounting priority

[機能]

優先度の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info accounting <number> priority <priority>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<priority>

- ・ 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、0～255 の範囲で指定します。
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。
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。

[動作モード]

構成定義モード(管理者クラス)

[説明]

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、サーバ定義番号の小さい方が使われます。

[未設定時]

最優先が設定されたものとみなされます。

```
aaa <group_id> radius client server-info accounting <number> priority 0
```

13.2.22 aaa radius client server-info accounting source

[機能]

自側 IP アドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client server-info accounting <number> source <address>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<number>

- ・ サーバ定義番号
相手装置の定義番号を 10 進数で指定します。

<address>

- ・ 自側 IP アドレス
自側 RADIUS アカウンティングサーバの 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。

IPv4

1. 0. 0. 1 ~ 126. 255. 255. 254
128. 0. 0. 1 ~ 191. 255. 255. 254
192. 0. 0. 1 ~ 223. 255. 255. 254

[動作モード]

構成定義モード(管理者クラス)

[説明]

自側 RADIUS アカウンティング装置の IP アドレスを設定します。本定義の内容は、aaa radius accounting source による、自側 RADIUS アカウンティング装置の IP アドレスの設定より優先されます。

[未設定時]

aaa radius accounting source による自側 RADIUS アカウンティング装置の IP アドレスの設定に従うものとみなされます。

13.2.23 aaa radius client retry

[機能]

RADIUS パケット再送回数・送信間隔の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client retry <interval> <retry>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<interval>

- ・ 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)の範囲で指定します。

<retry>

- ・ 再送回数
RADIUS サーバ未応答時のパケット再送回数を、1~10(回)の範囲で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

RADIUS サーバ未応答時のパケットの再送回数・送信間隔を設定します。
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。

[未設定時]

送信間隔に 5 秒、再送回数に 2 回が設定されたものとみなされます。
この場合は、サーバからの応答待ち受け時間はパケットの初回送信後、15 秒となります。

```
aaa <group_id> radius client retry 5 2
```

13.2.24 aaa radius client nas-identifier

[機能]

NAS 識別子の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client nas-identifier <nas_id>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<nas_id>

- ・ NAS 識別子
RADIUS 認証クライアントおよびアカウントクライアントが RADIUS サーバに送出する Nas-Identifier アトリビュートの値を、0x21, 0x23~0x7e の 64 文字以内の ASCII 文字列で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

Nas-Identifier アトリビュートで指定する NAS 識別子を設定します。認証およびアカウントで有効です。未設定時は、Nas-Identifier アトリビュートを送信しません。

[未設定時]

Nas-Identifier アトリビュートを送信しません。

13.2.25 aaa radius client nas-identifier-ssid

[機能]

NAS 識別子の SSID 利用設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
aaa <group_id> radius client nas-identifier-ssid <mode>
```

[オプション]

<group_id>

- ・ グループ ID
各グループを示す ID を 10 進数の通し番号で指定します。

<mode>

- ・ off
Nas-Identifier アトリビュートに SSID を設定しません。
- ・ on
Nas-Identifier アトリビュートに SSID を設定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

IEEE802.1X 認証、または MAC アドレス認証が利用する AAA グループにて本設定を有効にすると、aaa radius client nas-identifier コマンドの設定に関わらず、Nas-Identifier アトリビュートに当該無線 LAN インタフェースの SSID を設定します (装置へのログイン認証には影響しません)。

また、本設定が無効な場合、Nas-Identifier アトリビュートは aaa radius client nas-identifier コマンドに従って設定されます。

[注意]

本設定は、aaa radius client nas-identifier コマンドの設定より優先されます。

[未設定時]

Nas-Identifier アトリビュートに SSID を設定しません。

第 14 章 端末可視化機能情報の設定

14.1 端末可視化機能情報

14.1.1 devscan use

[機能]

端末可視化機能の使用の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

devscan use <mode>

[オプション]

<mode>

- on
端末可視化機能を使用します。
- off
端末可視化機能を使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

端末可視化機能を使用するかどうかを設定します。

[未設定時]

端末可視化機能を使用しないものとみなされます。

```
devscan use off
```

14.1.2 devscan vlan

[機能]

端末可視化機能が監視する VLAN セグメントの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

devscan vlan <vidlist>

[オプション]

<vidlist>

- VLAN ID

VLAN ID を、1~4094 の 10 進数で指定します。

複数の VLAN ID を設定する場合、"," (カンマ) で区切ります。

複数の番号が続く場合、"- " (ハイフン) で区切ります (例: "1-8, 100, 200")。

指定可能な VLAN ID は最大 16 個です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

端末可視化機能が監視するセグメントの VLAN ID を設定します。

[注意]

本コマンドを動的定義変更すると端末可視化機能を再起動するため収集されている端末情報は一旦消去されます。

[未設定時]

なし

14.1.3 devscan age

[機能]

端末情報のエージングアウト時間の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

devscan age <time>

[オプション]

<time>

- ・ エージングアウト時間

端末情報のエージングアウト時間を 0 日～30 日の範囲で指定します。

単位は、s (秒)、m (分)、h (時)、d (日) のどれかを指定します。

ただし、設定された値は設定値を超えない最大の 1 日の倍数に丸められます。

0 日を指定した場合はエージングアウトを行いません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

端末可視化機能が管理する端末情報のエージングアウト時間を設定します。

[注意]

エージングアウトの判定は、10 分毎に行われます。

[未設定時]

エージングアウトを行わないものとみなされます。

```
devscan age 0d
```

14.1.4 devscan dictionary dhcp

[機能]

機器識別用ユーザー辞書 (DHCP) の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

devscan dictionary dhcp <count> <fingerprint> <description>

[オプション]

<count>

- ・ ユーザー辞書 (DHCP) 定義番号
ユーザー辞書 (DHCP) 定義の通し番号を、0~99 の範囲の 10 進数で指定します。

<fingerprint>

- ・ DHCP フィンガープリント情報
機器識別に使用する DHCP フィンガープリント (DHCP パラメータ要求リスト オプション 55) を 0~255 の 10 進数と", "カンマで区切った最大 127 文字の文字列で指定します (例: "1, 15, 3, 6, 44, 46, 47, 31, 33, 249, 43")。

<description>

- ・ 機器情報
機器情報を 0x21, 0x23~0x7e の 63 文字以内の ASCII 文字列で記入します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)
文字列に空白が含まれる場合は、ダブルクォーテーション(")で囲みます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

端末可視化機能が使用する機器識別用のユーザー辞書 (DHCP による識別) を設定します。

[注意]

本コマンドを動的定義変更すると端末可視化機能を再起動するため収集されている端末情報は一旦消去されます。

[未設定時]

端末可視化機能はユーザー辞書 (DHCP) を使用せず、本体内蔵の辞書のみを使用し、機器の識別を行います。

14.1.5 devscan dictionary oui

[機能]

機器識別用ユーザー辞書(OUI)の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

devscan dictionary oui <count> <oui> <vendor>

[オプション]

<count>

- ・ ユーザー辞書(OUI)定義番号
ユーザー辞書(OUI)定義の通し番号を、0～99の範囲の10進数で指定します。

<oui>

- ・ OUI
機器識別に使用するOUI(Organizationally Unique Identifier)を6桁の16進数で指定します(例:"A8B2DA")。

<vendor>

- ・ ベンダー名
ベンダー名を0x21, 0x23～0x7eの63文字以内のASCII文字列で記入します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)
文字列に空白が含まれる場合は、ダブルクォーテーション(")で囲みます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

端末可視化機能が使用する機器識別用のユーザー辞書(OUIによる識別)を設定します。

[注意]

本コマンドを動的定義変更すると端末可視化機能を再起動するため収集されている端末情報は一旦消去されます。

[未設定時]

端末可視化機能はユーザー辞書(OUI)を使用せず、本体内蔵の辞書のみを使用し、機器の識別を行います。

14.1.6 devscan dictionary mac

[機能]

機器識別用ユーザー辞書(MAC アドレス)の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

devscan dictionary mac <count> <mac> <mask> <description>

[オプション]

<count>

- ・ ユーザー辞書 (MAC アドレス) 定義番号
ユーザー辞書 (MAC アドレス) 定義の通し番号を、0~99 の範囲の 10 進数で指定します。

<mac>

- ・ MAC アドレス
機器識別に使用する送信元 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。

<mask>

- ・ MAC アドレスマスク
機器識別に使用する送信元 MAC アドレスのマスク値を xx:xx:xx:xx:xx:xx (xx は 2 桁の 16 進数) の形式で指定します。

<description>

- ・ 機器情報
機器情報を 0x21, 0x23~0x7e の 63 文字以内の ASCII 文字列で記入します。
(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)
文字列に空白が含まれる場合は、ダブルクォーテーション(")で囲みます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

端末可視化機能が使用する機器識別用のユーザー辞書 (MAC アドレスによる識別) を設定します。

[注意]

本コマンドを動的定義変更すると端末可視化機能を再起動するため収集されている端末情報は一旦消去されます。

[未設定時]

端末可視化機能はユーザー辞書 (MAC アドレス) を使用せず、本体内蔵の辞書のみを使用し、機器の識別を行います。

第 15 章 NXconcierge エージェント機能の設定

15.1 NXconciierge エージェント機能情報

15.1.1 management-agent mode

[機能]

NXconciierge エージェント機能使用有無の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

management-agent mode <mode>

[オプション]

<mode>

NXconciierge エージェント機能を使用するかどうかを指定します。

- off

NXconciierge エージェント機能を使用しません。

- agent

NXconciierge エージェント機能搭載機として、NXconciierge エージェント機能を使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

NXconciierge エージェント機能を使用するかどうかを設定します。

[未設定時]

NXconciierge エージェント機能を使用しないものとみなされます。

```
management-agent mode off
```

15.1.2 management-agent tenantkey

[機能]

テナントキーの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

management-agent tenantkey <tenantkey> [encrypted]

[オプション]

<tenantkey>

テナントキーを指定します。

- ・ 暗号化されていないテナントキーを指定します。
0x22（ダブルクォーテーション）を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、0x20（空白文字）を使用する場合は、文字列鍵を"\" で囲う必要があります。
- ・ 暗号化されたテナントキーを指定します。
show コマンドで表示される暗号化されたテナントキーを encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- ・ 暗号化共通鍵指定
<tenantkey> に暗号化されたテナントキーを指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

テナントキーを設定します。

[注意]

本機能は、management-agent mode agent 設定時に有効です。

[未設定時]

テナントキーが設定されていないものとみなされます。

15.1.3 management-agent macfilter

[機能]

遮断する MAC アドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

management-agent macfilter <count> <mac>

[オプション]

<count>

- ・ 定義番号
定義番号を 0~49 の 10 進数で設定します。

<mac>

- ・ MAC アドレス
設定した送信元 MAC アドレスを有するフレームを遮断します。
xx:xx:xx:xx:xx:xx (xx は 2 桁の 16 進数) の形式で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

遮断する MAC アドレスを指定します。
本設定は、management-agent mode off の場合は無効となります。

[注意]

本設定は、他の MAC フィルタ設定よりも最優先で動作します。

[未設定時]

遮断する MAC アドレスが設定されていないものとみなされます。

15.1.4 management-agent serverlogin proxy auth send

[機能]

Proxy サーバ用認証情報設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

management-agent serverlogin proxy auth send <id> <password> [encrypted]

[オプション]

<id>

- ・ 認証 ID

認証 ID を、0x21, 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。

<password>

- ・ 認証パスワード

認証パスワードを、0x21, 0x23～0x7e の文字で構成される 128 文字以内の文字列を指定します。

show コマンドで表示される暗号化された認証パスワード文字列を encrypted とともに指定することもできます。その場合、表示された文字列をそのまま正確に入力してください。文字列は 128 文字を超えていてもかまいません。

- ・ 暗号化された認証パスワード

show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。

show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- ・ 暗号化認証パスワード指定

<password>に暗号化された認証パスワードを設定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[注意]

認証 ID およびパスワードが設定されていない場合、認証付き Proxy サーバとの接続が行えません。

[未設定時]

Proxy サーバ用認証情報を定義しないものとみなされます。

15.1.5 management-agent serverlogin proxy address

[機能]

proxy のアドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

management-agent serverlogin proxy address <fqdn> <port>

[オプション]

<fqdn>

値を設定する FQDN を指定します。

0x21, 0x23～0x7e の 128 文字以内の ASCII 文字列で指定します。

<port>

使用するポート番号を、1～65535 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[未設定時]

NXconciierge エージェント機能は、proxy を使わず直接サーバと接続します。

第 16 章 装置情報の設定

16.1 SNMP 情報

16.1.1 snmp service

[機能]

SNMP エージェント機能および SNMP トラップ機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

snmp service <mode>

[オプション]

<mode>

- on
SNMP エージェント機能および SNMP トラップ機能を有効にします。
- off
SNMP エージェント機能および SNMP トラップ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMP エージェント機能および SNMP トラップ機能を有効にするかどうかを設定します。

[未設定時]

SNMP エージェント機能を停止するものとみなされます。

```
snmp service off
```

16.1.2 snmp agent contact

[機能]

SNMP エージェント機能での管理者名の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

snmp agent contact <syscontact>

[オプション]

<syscontact>

- ・ 管理者名 (sysContact 値)
本装置の管理者名を表す MIB 変数 sysContact を、40 文字以内で指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

SNMP エージェント機能での管理者名を設定します。

[未設定時]

管理者名を設定しないものとみなされます。

16.1.3 snmp agent sysname

[機能]

SNMP エージェント機能での機器名称の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

snmp agent sysname <sysname>

[オプション]

<sysname>

- ・ 機器名称(sysName 値)

本装置の機器名称を表す MIB 変数 sysName を、32 文字以内で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMP エージェント機能での機器名称を設定します。

[未設定時]

機器名称を設定しないものとみなされます。

16.1.4 snmp agent location

[機能]

SNMP エージェント機能での機器設置場所の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

snmp agent location <syslocation>

[オプション]

<syslocation>

- ・ 機器設置場所(sysLocation 値)
本装置の設置場所を表す MIB 変数 sysLocation を、72 文字以内で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMP エージェント機能での機器設置場所を設定します。

[未設定時]

機器設置場所を設定しないものとみなされます。

16.1.5 snmp agent address

[機能]

SNMP エージェントアドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

snmp agent address <address>

[オプション]

<address>

- ・ エージェントアドレス

本装置のエージェントアドレスを指定します。

0.0.0.0 を指定した場合は、SNMP エージェントアドレスを削除します。

指定可能な範囲は以下のとおりです。

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMP エージェントのアドレスを設定します。本設定は TRAP 送信時の自局アドレスにも使用されます。SNMP エージェント機能を使用する場合は必ず設定してください。

[未設定時]

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。その場合、TRAP パケットの自局 IP アドレスは不定となります。

16.1.6 snmp agent engineid

[機能]

SNMP エンジン ID 名の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

snmp agent engineid <engineID>

[オプション]

<engineID>

- SNMP エンジン ID
SNMP エンジン ID を 1～27 文字で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 での SNMP エンジン ID を設定します。トラップ通知ホストなどで SNMP エンジン ID をあらかじめ取り決めておく必要がある場合は、設定を行ってください。

装置に設定される SNMP エンジン ID の値は以下のようになります。

- 本コマンドを設定した場合
第 1～5 オクテット : 0x800000d304 固定
第 6 オクテット以降 : 本コマンドで設定したエンジン ID
- 本コマンドを設定しない場合
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

[未設定時]

SNMP エンジン ID を自動生成します。

16.1.7 snmp manager

[機能]

SNMP ホスト情報の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

snmp manager <manager_number> <address> <community> <trap> [<write>]

[オプション]

<manager_number>

- ・ SNMP ホスト定義番号
SNMP ホスト定義の通し番号を、0～7 の 10 進数で指定します。

<address>

- ・ アクセス許可/トラップ送信アドレス
アクセス許可およびトラップを送信するあて先 IP アドレスを、XXX.XXX.XXX.XXX (XXX は 3 桁の 10 進数) の形式で指定します。
0.0.0.0 を指定すると、すべてのホストからのアクセスを許可し、trap 送信は行いません。
指定可能な範囲は以下のとおりです。
1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254

<community>

- コミュニティ名を指定します。
- ・ コミュニティ名
トラップを送信するときのコミュニティ名を、1～32 文字で指定します。
 - ・ public
任意の SNMP マネージャと通信する場合に指定します。

<trap>

- トラップ送信するかどうかを指定します。
- ・ off
トラップ送信しない場合に指定します。
 - ・ v1
SNMPv1 トラップ送信する場合に指定します。
 - ・ v2c
SNMPv2 トラップ送信する場合に指定します。

<write>

- SNMP マネージャからの書き込みを許可するかどうかを指定します。
- ・ enable
SNMP マネージャからの書き込みを許可する場合に指定します。
 - ・ disable
SNMP マネージャからの書き込みを許可しない場合に指定します。
省略時は、disable を指定したものとみなされます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMP ホストの情報を設定します。

[未設定時]

SNMP ホストの情報を設定しないものとみなされます。

16.1.8 snmp trap coldstart

[機能]

coldStart トラップの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
snmp trap coldstart <mode>
```

[オプション]

<mode>

トラップの動作を指定します。

- enable
トラップを有効にします。
- disable
トラップを無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

coldStart トラップを有効または無効にするかを設定します。

[未設定時]

coldStart トラップが有効とみなされます。

```
snmp trap coldstart enable
```

16.1.9 snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
snmp trap linkdown <mode>
```

[オプション]

<mode>

トラップの動作を指定します。

- enable
トラップを有効にします。
- disable
トラップを無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

linkDown トラップを有効または無効にするかを設定します。

[未設定時]

linkDown トラップが有効とみなされます。

```
snmp trap linkdown enable
```

16.1.10 snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
snmp trap linkup <mode>
```

[オプション]

<mode>

トラップの動作を指定します。

- enable
トラップを有効にします。
- disable
トラップを無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

linkUp トラップを有効または無効にするかを設定します。

[未設定時]

linkUp トラップが有効とみなされます。

```
snmp trap linkup enable
```

16.1.11 snmp trap authfail

[機能]

authenticationFailure トラップの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
snmp trap authfail <mode>
```

[オプション]

<mode>

トラップの動作を指定します。

- enable
トラップを有効にします。
- disable
トラップを無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

authenticationFailure トラップを有効または無効にするかを設定します。

[未設定時]

authenticationFailure トラップが有効とみなされます。

```
snmp trap authfail enable
```

16.1.12 snmp trap noserror

[機能]

nosError トラップの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
snmp trap noserror <mode>
```

[オプション]

<mode>

トラップの動作を指定します。

- enable
トラップを有効にします。
- disable
トラップを無効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

nosError トラップを有効または無効にするかを設定します。

[未設定時]

nosError トラップが有効とみなされます。

```
snmp trap noserror enable
```

16.1.13 snmp user name

[機能]

SNMP ユーザ名の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
snmp user <number> name <user_name>
```

[オプション]

<number>

- ・ ユーザ定義番号
ユーザ定義番号を 0～7 の 10 進数で指定します。

<user_name>

- ・ SNMP ユーザ名
SNMP ユーザ名を 1～32 文字で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 での SNMP ユーザ名を設定します。SNMPv3 機能を使用する場合は必ず設定してください。

[未設定時]

SNMP ユーザ名を設定しないものとみなされます。

16.1.14 snmp user address

[機能]

SNMP ホストアドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

snmp user <number> address <addr_number> <address>

[オプション]

<number>

- ・ ユーザ定義番号
ユーザ定義番号を 0～7 の 10 進数で指定します。

<addr_number>

- ・ SNMP ホスト定義番号
SNMP ホスト定義番号を 0～7 の 10 進数で指定します。

<address>

- ・ SNMP ホストアドレス
SNMPv3 アクセスを許可するホストの IP アドレスを、XXX.XXX.XXX.XXX (XXX は最大 3 桁の 10 進数) の形式で指定します。

指定可能な範囲は以下のとおりです。

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 での SNMP ホストアドレスを設定します。定義可能数は"snmp user notification"コマンドと合わせて本装置全体で 8 個まで定義できます。

[未設定時]

SNMP ホストアドレスを設定しないものとみなされます。

16.1.15 snmp user notification

[機能]

トラップ通知ホストアドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
snmp user <number> notification <addr_number> <address>
```

[オプション]

<number>

- ・ ユーザ定義番号
ユーザ定義番号を 0～7 の 10 進数で指定します。

<addr_number>

- ・ トラップ通知ホスト定義番号
トラップ通知ホスト定義番号を 0～7 の 10 進数で指定します。

<address>

- ・ トラップ通知ホストアドレス
トラップを通知するホストの IP アドレスを、XXX.XXX.XXX.XXX (XXX は最大 3 桁の 10 進数) の形式で指定します。

指定可能な範囲は以下のとおりです。

1. 0. 0. 1 ~ 126. 255. 255. 254

128. 0. 0. 1 ~ 191. 255. 255. 254

192. 0. 0. 1 ~ 223. 255. 255. 254

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 でのトラップ通知ホストアドレスを設定します。定義可能数は“snmp user address”コマンドと合わせて本装置全体で 8 個まで定義できます。

[未設定時]

トラップ通知ホストアドレスを設定しないものとみなされます。

16.1.16 snmp user auth

[機能]

認証プロトコルの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
snmp user <number> auth <protocol> [<password> [encrypted]]
```

[オプション]

<number>

- ・ ユーザ定義番号
ユーザ定義番号を 0～7 の 10 進数で指定します。

<protocol>

認証プロトコルを指定します。

- ・ none
認証プロトコルを使用しません。
- ・ md5
認証プロトコルとして MD5 (HMAC-MD5-96) を使用します。
- ・ sha
認証プロトコルとして SHA (HMAC-SHA-96) を使用します。

<password>

認証パスワードを指定します。

- ・ 暗号化されていない認証パスワード指定の場合
以下に、入力範囲を示します。

認証プロトコル	パスワード長
md5	8 文字～16 文字
sha	8 文字～20 文字

- ・ 暗号化された認証パスワード指定の場合
show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- ・ 暗号化認証パスワード指定
<password>に暗号化された認証パスワードを指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 での認証プロトコルを設定します。

[未設定時]

認証プロトコルを使用しないものとみなされます。

```
snmp user <number> auth none
```


16.1.17 snmp user priv

[機能]

暗号プロトコルの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
snmp user <number> priv <protocol> [<password> [encrypted]]
```

[オプション]

<number>

- ユーザ定義番号
ユーザ定義番号を 0～7 の 10 進数で指定します。

<protocol>

暗号プロトコルを指定します。

- none
暗号プロトコルを使用しません。
- des
暗号プロトコルとして DES (CBC-DES) を使用します。

<password>

暗号パスワードを指定します。

- 暗号化されていない暗号パスワード指定の場合
以下に、入力範囲を示します。

暗号プロトコル	パスワード長
des	8 文字～16 文字

- 暗号化された暗号パスワード指定の場合
show コマンドで表示される暗号化された暗号パスワードを encrypted と共に指定します。
show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化暗号パスワード指定
<password>に暗号化された暗号パスワードを指定する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 での暗号プロトコルを設定します。

[注意]

暗号プロトコルを使用する場合は必ず認証プロトコルを設定してください。
認証プロトコルの設定がない場合、暗号プロトコルの設定は使用されません。

[未設定時]

暗号プロトコルを使用しないものとみなされます。

```
snmp user <number> priv none
```

16.1.18 snmp user write

[機能]

MIB 書き込み許可ビューの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
snmp user <number> write <access>
```

[オプション]

<number>

- ・ ユーザ定義番号
ユーザ定義番号を 0～7 の 10 進数で指定します。

<access>

書き込み可能な MIB に対しての書き込み許可ビューを指定します。

- ・ none
MIB 書き込みを許可しない場合に指定します。
- ・ all
MIB 書き込みを許可する場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 での MIB 書き込み許可ビューを設定します。

[未設定時]

MIB 書き込みを許可しないものとみなされます。

```
snmp user <number> write none
```

16.1.19 snmp user read

[機能]

MIB 読み出し許可ビューの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
snmp user <number> read <access> [<view_number>]
```

[オプション]

<number>

- ・ ユーザ定義番号
ユーザ定義番号を 0～7 の 10 進数で指定します。

<access>

MIB 読み出し許可ビューを指定します。

- ・ all
サポートしているすべての MIB 読み出しを許可する場合に指定します。
- ・ none
MIB 読み出しを許可しない場合に指定します。
- ・ view
"snmp view subtree" コマンドで設定した MIB ビュー情報を使用する場合に指定します。

<view_number>

使用する "snmp view subtree" コマンドのビュー定義番号を 0～7 の 10 進数で指定します。ビュー定義番号は、<access> に view を指定した場合にのみ設定可能です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 での MIB 読み出し許可ビューを設定します。

設定したビュー定義番号に対応する "snmp view subtree" コマンド定義が存在しない場合、MIB 読み出しを許可しないものとみなされます。

[未設定時]

サポートしているすべての MIB 読み出しを許可するものとみなされます。

```
snmp user <number> read all
```

16.1.20 snmp user notify

[機能]

トラップ通知許可ビューの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
snmp user <number> notify <access> [<view_number>]
```

[オプション]

<number>

- ・ ユーザ定義番号
ユーザ定義番号を 0～7 の 10 進数で指定します。

<access>

トラップ通知許可ビューを指定します。

- ・ all
サポートしているすべてのトラップ通知を許可する場合に指定します。
- ・ none
トラップ通知を許可しない場合に指定します。
- ・ view
"snmp view subtree" コマンドで設定した MIB ビュー情報を使用する場合に指定します。

<view_number>

使用する "snmp view subtree" コマンドのビュー定義番号を 0～7 の 10 進数で指定します。ビュー定義番号は、<access> に view を指定した場合にのみ設定可能です。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 でのトラップ通知許可ビューを設定します。

設定したビュー定義番号に対応する "snmp view subtree" コマンド定義が存在しない場合、トラップ通知を許可しないものとみなされます。

[未設定時]

サポートしているすべてのトラップ通知を許可するものとみなされます。

```
snmp user <number> notify all
```

16.1.21 snmp view subtree

[機能]

SNMP MIB ビュー情報の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
snmp view <view_number> subtree <subtree_number> <view_type> <subtree_name>
```

[オプション]

<view_number>

- ビュー定義番号
ビュー定義番号を 0~7 の 10 進数で指定します。

<subtree_number>

- サブツリー定義番号
サブツリー定義番号を 0~15 の 10 進数で指定します。

<view_type>

<subtree_name>を MIB ビューに含むか、それとも除くかを指定します。

- include
<subtree_name>を MIB ビューに含む場合に指定します。
- exclude
<subtree_name>を MIB ビューから除く場合に指定します。

<subtree_name>

- サブツリー名
MIB ビュー対象とするサブツリー名を指定します。指定可能なサブツリー名は以下のとおりです。

サブツリー名		オブジェクト ID	備考
MIB グループ名	iso	1	
	internet	1.3.6.1	
	mib2	1.3.6.1.2.1	
	system	1.3.6.1.2.1.1	
	interfaces	1.3.6.1.2.1.2	
	at	1.3.6.1.2.1.3	
	ip	1.3.6.1.2.1.4	
	icmp	1.3.6.1.2.1.5	
	tcp	1.3.6.1.2.1.6	
	udp	1.3.6.1.2.1.7	
	transmission	1.3.6.1.2.1.10	
	snmp	1.3.6.1.2.1.11	
	ifMIB	1.3.6.1.2.1.31	
	enterprises	1.3.6.1.4.1	

サブツリー名		オブジェクト ID	備考
トラップ名	coldstart	1.3.6.1.6.3.1.1.5.1	
	linkdown	1.3.6.1.6.3.1.1.5.3	
	linkup	1.3.6.1.6.3.1.1.5.4	
	authfail	1.3.6.1.6.3.1.1.5.5	
	noserror	1.3.6.1.4.1.211.1.127.1.0.1	

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNMPv3 での MIB ビュー情報を設定します。

同じビュー定義番号を持つ MIB ビュー情報の設定で、同一サブツリー名が複数指定された場合、最小のサブツリー定義番号を持つサブツリー情報が有効となります。

[未設定時]

MIB ビュー情報を設定しないものとみなされます。

16.2 システムログ情報

16.2.1 syslog server address

[機能]

システムログ情報の受信サーバの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

syslog server <number> address <address>

[オプション]

<number>

- ・ 定義番号
サーバ情報の定義番号を、0～2 の 10 進数で指定します。

<address>

- ・ IP アドレス
システムログ情報(メッセージ)を受信するサーバの IP 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。

1. 0. 0. 1 ~ 126. 255. 255. 254

128. 0. 0. 1 ~ 191. 255. 255. 254

192. 0. 0. 1 ~ 223. 255. 255. 254

[動作モード]

構成定義モード(管理者クラス)

[説明]

システムログ情報(メッセージ)を受信するサーバの IP アドレスを設定します。

[未設定時]

システムログ情報を受信するサーバを設定しないものとみなされます。

16.2.2 syslog server pri

[機能]

受信サーバごとのシステムログ情報の出力対象プライオリティの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
syslog server <number> pri <mode>
```

[オプション]

<number>

- ・ 定義番号
サーバ情報の定義番号を、0～2 の 10 進数で指定します。

<mode>

- ・ プライオリティ
システムログ情報を出力する対象となるプライオリティを、以下の中から指定します。
複数指定する場合は、","(カンマ)で区切ります。

error

プライオリティ LOG_ERROR を対象とする場合に指定します。

warn

プライオリティ LOG_WARNING を対象とする場合に指定します。

notice

プライオリティ LOG_NOTICE を対象とする場合に指定します。

info

プライオリティ LOG_INFO を対象とする場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

syslog pri コマンドで指定したプライオリティの中から、受信サーバごとにシステムログ情報を出力する対象となるプライオリティを指定します。

[未設定時]

syslog pri コマンドで指定したものと同一内容とします。

16.2.3 syslog pri

[機能]

システムログ情報の出力対象プライオリティの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

syslog pri <mode>

[オプション]

<mode>

- ・ プライオリティ

システムログ情報を出力する対象となるプライオリティを、以下の中から指定します。
複数指定する場合は、","(カンマ)で区切ります。

error

プライオリティ LOG_ERROR を対象とする場合に指定します。

warn

プライオリティ LOG_WARNING を対象とする場合に指定します。

notice

プライオリティ LOG_NOTICE を対象とする場合に指定します。

info

プライオリティ LOG_INFO を対象とする場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

システムログ情報を出力する対象となるプライオリティを指定します。

[未設定時]

error, warn, info が設定されたものとみなされます。

```
syslog pri error, warn, info
```

16.2.4 syslog facility

[機能]

システムログ情報のファシリティの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

syslog facility <num>

[オプション]

<num>

- ・ ファシリティ
システムログ情報のファシリティを、0～23 の 10 進数で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

システムログ情報のファシリティを指定します。

[未設定時]

0 が設定されたものとみなされます。

```
syslog facility 0
```

16.2.5 syslog command-logging

[機能]

システムログ情報のコマンド実行履歴出力の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
syslog command-logging <mode>
```

[オプション]

<mode>

- enable
コマンド実行履歴をシステムログに出力します。
- disable
コマンド実行履歴をシステムログに出力しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

コマンド実行履歴をシステムログに出力するかどうかを指定します。

[注意]

セキュリティ確保のため、暗号化対象のパラメタについては、暗号化して出力します。

[未設定時]

コマンド実行履歴をシステムログに出力しないものとみなされます。

```
syslog command-logging disable
```

16.2.6 syslog header

[機能]

システムログ情報の HEADER 部追加の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

syslog header <mode>

[オプション]

<mode>

- enable
送信メッセージに HEADER 部を追加します。
- disable
送信メッセージに HEADER 部を追加しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

送信メッセージに HEADER 部を追加するかどうかを設定します。

[未設定時]

送信メッセージに HEADER 部を追加しないものとみなされます。

```
syslog header disable
```

16.2.7 syslog source address

[機能]

システムログ情報の送信元 IP アドレスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

syslog source address <address>

[オプション]

<address>

- ・ IP アドレス
送信メッセージの送信元 IP 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。
1. 0. 0. 1 ~ 126. 255. 255. 254
128. 0. 0. 1 ~ 191. 255. 255. 254
192. 0. 0. 1 ~ 223. 255. 255. 254

[動作モード]

構成定義モード(管理者クラス)

[説明]

送信メッセージの送信元 IP アドレスを設定します。

[注意]

本設定と同じ IP アドレスが自装置の lan に設定されている必要があります。同じ IP アドレスが lan に設定されていない場合、システムログは送信されません。

[未設定時]

送信メッセージの送信元 IP アドレスを指定しないものとみなされます。

16.2.8 syslog filter regexp

[機能]

システムログの出力を抑止する対象文字列の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
syslog fileter <count> regexp <targetstring>
```

[オプション]

<count>

- 定義番号
抑止対象文字列の定義番号を、0～9の10進数で指定します。

<targetstring>

- 抑止対象文字列
64文字以内のASCII文字列を指定します。

空白文字またはダブルクォーテーションを使用する場合は文字列をダブルクォーテーション(")で囲んでください。

指定可能な文字の範囲は以下のとおりです。

文字	範囲
半角アルファベット	a～z、A～Z
半角数値	0～9
半角記号	! " # \$ % & ' () * + , - . / : ; < = > ? @ [¥] ^ _ ` { } ~

正規表現に使用可能な特殊文字は以下のとおりです。

特殊文字	特殊文字の説明
.	任意の1文字。改行文字は除く。
*	直前の1文字の0回以上の繰り返しと一致。
^	行の先頭。
\$	行の末尾。
[]	カッコ内の任意の1文字と一致。「-」で範囲指定可。
[^]	カッコ内の任意の1文字と不一致。「-」で範囲指定可。
+	直前の文字の1個以上の繰り返しと一致。
?	直前の文字が0個または1個の場合に一致。
{ }	カッコ内の数値の繰り返しと一致。
	直前、直後どちらかのパターンに一致。
()	カッコ内をグループ化。マッチした内容は参照可。

特殊文字、およびシングルクォーテーション、ダブルクォーテーションを抑止対象文字列に含める場合は以下の例のように直前に ¥ を付与してエスケープしてください。

「¥」を付ける場合、更にエスケープ文字「¥」を付与することに注意してください。

ただし、ダブルクォーテーションは ¥ のみ付与してください。

(¥のエスケープについての詳細は、コマンドユーザズガイドを参照してください。)

記号	記号の説明	エスケープシーケンス
¥	文字としての¥	¥¥¥¥
?	文字としての?	¥¥?
'	シングルクォーテーション	¥¥'
”	ダブルクォーテーション	¥”
.	文字としてのドット	¥¥.

[動作モード]

構成定義モード(管理者クラス)

[説明]

抑止するシステムログの内容を設定します。

対象とする文字列は `targetstring` に設定します。

設定可能な文字列以外を設定した場合、または正規表現を設定した場合に設定に誤りがある場合はエラーとなります。

[実行例]

```
# syslog fileter 0 regexp "sshlogin.*admin"
#
```

[メッセージ]

```
<ERROR> invalid regular expression
```

無効な正規表現を設定しています。正規表現の内容を見直してください。

```
<ERROR> invalid collating element
```

無効な照合エレメントを参照しています。正規表現の内容を見直してください。

```
<ERROR> invalid character class
```

無効な文字クラス・タイプを参照しています。正規表現の内容を見直してください。

```
<ERROR> `¥' applied to unescapable character
```

正規表現の最後の文字が ¥ です。正規表現の内容を見直してください。

```
<ERROR> invalid backreference number
```

¥digit 内の数値が無効、またはエラーです。

```
<ERROR> brackets `[ ]' not balanced
```

[] が不揃いです。正規表現の内容を見直してください。

```
<ERROR> parentheses `( )' not balanced
```

¥(¥) または (¥) が不揃いです。正規表現の内容を見直してください。

```
<ERROR> invalid repetition count(s) in `{ }'
```

¥{ と ¥} の間の式が無効です。正規表現の内容を見直してください。

<ERROR> invalid character range in `[]`

範囲式内のエンドポイントが無効です。正規表現の内容を見直してください。

<ERROR> `?`, `*`, or `+` operand invalid

?, *, または + の前に有効な正規表現がありません。正規表現の内容を見直してください。

<ERROR> empty (sub)expression

空白文字のみで構成されています。正規表現の内容を見直してください。

<ERROR> invalid argument, e.g. negative-length string

引数が正しく設定されていません。コマンドのパラメタを確認してください。

<ERROR> illegal byte sequence (bad multibyte character)

無効なマルチバイト文字が設定されています。正規表現の内容を見直してください。

[未設定時]

すべてのシステムログが出力対象となります。

16.3 自動時刻設定情報

16.3.1 time auto server

[機能]

時刻情報の提供サーバの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

time auto server <address> <protocol>

[オプション]

<address>

- IPv4 アドレス
時刻情報を提供しているサーバの 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。
 - 1. 0. 0. 1 ~ 126. 255. 255. 254
 - 128. 0. 0. 1 ~ 191. 255. 255. 254
 - 192. 0. 0. 1 ~ 223. 255. 255. 254

<protocol>

- 使用するプロトコルを指定します。
- time
TIME プロトコル(TCP)を使用する場合に指定します。
 - sntp
簡易 NTP プロトコル(UDP)を使用する場合に指定します。
 - dhcp
DHCP サーバから広報される TIME プロトコルまたは簡易 NTP に従います。

[動作モード]

構成定義モード(管理者クラス)

[説明]

時刻提供サーバの情報を設定します。
time auto server の<address>で指定した時刻提供サーバから、<protocol>で指定したプロトコルを使用して、自動的に時刻を設定します。
本装置のインタフェースが DHCP クライアントとして動作している場合に限り、<protocol>で dhcp を指定することができます。この場合、DHCP サーバが広報する時刻提供サーバから指定されたプロトコルを使用して設定します。また、TIME プロトコルと SNTP が同時に広報された場合は、SNTP を優先します。
時刻提供サーバとの時刻同期は以下のタイミングで実行されます。

- 装置起動時 (time auto interval の設定に関わらず、装置起動時に実行されます)
- 定周期 (time auto interval に指定された間隔が経過する度に実行されます)
- 設定変更時 (time auto server、または time auto interval を変更し、commit コマンドを実行したときに実行されます)
- DHCP から時刻提供サーバが広報されたとき (初回広報時、および時刻提供サーバに変更があった場合に実行されます)

[未設定時]

自動時刻設定を行わないものとみなされます。

16.3.2 time auto interval

[機能]

時刻情報の自動設定間隔の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

time auto interval <time>

[オプション]

<time>

時刻情報を設定する間隔を指定します。

- ・ start
電源投入時またはリセット時に一度だけ、時刻情報を設定する場合に指定します。
- ・ 間隔
時刻情報を設定する間隔を、0 秒～最大 10 日の範囲で指定します。
単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

自動時刻を設定する間隔を設定します。

[未設定時]

時刻提供サーバを使用する場合だけ、電源投入時またはリセット時に一度だけ時刻情報設定するものとみなされます。

```
time auto interval start
```

16.3.3 time zone

[機能]

時刻情報のタイムゾーンの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

time zone <offset>

[オプション]

<offset>

- ・ 差分

本装置が使用するタイムゾーンを指定します。

GMT(グリニッジ標準時間)からの時差を指定します。日本で使用する場合は、0900 を指定してください。

-1500~1500 の範囲で指定してください。

[動作モード]

構成定義モード(管理者クラス)

[説明]

タイムゾーンを設定します。

[未設定時]

タイムゾーンとして、GMT(グリニッジ標準時間)が設定されたものとみなされます。

```
time zone 0
```

16.4 ProxyARP 情報

16.4.1 proxyarp use

[機能]

ProxyARP 機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

proxyarp use <mode>

[オプション]

<mode>

- on
ProxyARP 機能を使用します。
- off
ProxyARP 機能を使用しません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

有線 LAN 側から無線 LAN 側へ送信される ARP 要求に対して、ProxyARP 機能を使用するかどうかを設定します。

[注意]

IEEE802.1X 認証または MAC アドレス認証にて、認証サーバから通知された VLAN を割り当てる機能 (wlan dot1x vlan assign enable /wlan macauth vlan assign enable) を利用する場合、本機能を <off> に設定する必要があります。

[未設定時]

ProxyARP 機能を使用するものとみなされます。

```
proxyarp use on
```

16.5 スケジュール情報

16.5.1 schedule at

[機能]

システムスケジュールの日時指定コマンドの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

schedule <number> at <day> <time> <command>

[オプション]

<number>

スケジュール定義を指定します。

- スケジュール定義番号
スケジュール定義番号を、0～49 の 10 進数で指定します。

<day>

- 日
スケジュールの実行日または開始日を、1～31 の 10 進数で指定します。
- 曜日
スケジュールの実行曜日または開始曜日を、以下の中から指定します。

sun

日曜日

mon

月曜日

tue

火曜日

wed

水曜日

thu

木曜日

fri

金曜日

sat

土曜日

複数の曜日を指定する場合は、","(カンマ)で区切って指定します。

- any
スケジュールの実行日または開始日を毎日とする場合に指定します。
電源投入時または再起動時は、本オプションを指定してください。

<time>

- 実行時間
実行するとき、分を、0～9 の 4 桁の 10 進数で指定します
(例: 0635 = 午前 6 時 35 分、2330 = 午後 11 時 30 分)。
- pwon
電源投入時に実行する場合に指定します。
- rset
システム再起動時、または電源投入時に実行する場合に指定します。

<command>

実行するコマンド文字列を指定します。

-
- `reset`
装置を再起動する場合に指定します。
 - `reset config1`
構成定義 1 に切り替えて再起動する場合に指定します。
 - `reset config2`
構成定義 2 に切り替えて再起動する場合に指定します。
 - `offline wlan`
無線 LAN インタフェースを閉塞する場合に指定します。
 - `online wlan`
無線 LAN インタフェースを閉塞解除する場合に指定します。
- 上記以外のコマンドを指定した場合の動作は保証されません。
<time>に `pwon`、または `rset` を指定した場合、上記のコマンドは指定できません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

システムスケジュールを設定します。
このスケジュールに従って、指定した時刻にコマンドを実行します。

[未設定時]

スケジュール情報を設定しないものとみなされます。

16.5.2 schedule syslog

[機能]

システムスケジュールのシステムログ出力可否の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
schedule <number> syslog <syslog>
```

[オプション]

<number>

スケジュール定義を指定します。

- ・ スケジュール定義番号
スケジュール定義番号を、0～49の10進数で指定します。

<syslog>

- ・ yes
コマンド実行時の出力をシステムログで行う場合に指定します。
- ・ no
コマンド実行時の出力をシステムログで行わない場合に指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

スケジュールによって起動されたコマンドが出力するメッセージを、システムログに出力するかどうかを指定します。

スケジュールで起動するコマンドが指定されている場合にだけ有効です。

[未設定時]

コマンド実行時の出力をシステムログに出力しないものとみなされます。

```
schedule <number> syslog no
```

16.6 装置ランプ情報

16.6.1 lamp mode

[機能]

運用中ランプ動作の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

lamp mode <mode>

[オプション]

<mode>

- enable
運用中にランプを点灯します。
- disable
運用中にランプを消灯します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

装置のランプを点灯するか消灯するかどうかを設定します。

disableを設定した場合、電源投入またはリセット操作により装置を起動してから lamp delay で設定されている時間経過後に装置のランプが消灯します。

[未設定時]

運用中にランプを点灯するものとみなされます。

```
lamp mode enable
```

16.6.2 lamp delay

[機能]

運用開始時のランプ消灯までの遅延時間の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

lamp delay <time>

[オプション]

<time>

- ・ 消灯までの遅延時間

lamp mode disable 設定時の消灯までの遅延時間を 1～20 分の範囲で指定します。

単位は、m(分)またはs(秒)を指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

lamp mode disable 設定時の、装置起動時に消灯するまでの遅延時間を設定します。

[未設定時]

装置起動後、ランプ消灯までの遅延時間として 1 分を指定したものとみなされます。
本設定は、装置電源投入時および装置リセット時に適用されます。

```
lamp delay 1m
```

16.7 高速転送情報

16.7.1 system bridge acceleration mode

[機能]

ブリッジ高速転送モードの設定

※ ソフトウェア V20.03 まで未サポート

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

system bridge acceleration mode <mode>

[オプション]

<mode>

- disable
高速転送モードを使用しません。
- enable
高速転送モードを使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

ブリッジ高速転送モードを使用するかどうかを設定します。

[注意]

本設定を変更した場合は、装置再起動が必要です。

高速転送モードを使用する場合、以下のコマンドで指定できる VLAN ID は合計で 24 個までです。24 個を超えて使用しないでください。

- ether vlan tag
- ether vlan untag
- wlan vlan tag
- wlan vlan untag

[未設定時]

高速転送モードを使用しないものとみなされます。

```
system bridge acceleratio mode disable
```

16.8 定期ログ情報

16.8.1 system monitoringinfo collect interval

[機能]

定期ログ情報のFLASHメモリ自動格納間隔の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

system monitoringinfo collect interval <period>

[オプション]

<period>

- ・ 情報格納間隔

定期ログ情報のFLASHメモリ自動格納間隔を30～1440分(24時間)の範囲の10進数と時間単位で指定します。

時間単位には、s(秒)、m(分)、h(時)、d(日)のどれかを指定します。

0を指定した場合、定期ログ情報の自動格納を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

<period>に0以外を指定した場合、以下のタイミングで定期ログ情報がFLASHメモリに保存されます。

- ・ 装置起動の5分後に初回保存が行われます。
- ・ 初回保存を起点として、<period>に指定した時間が経過する度に保存されます。

[未設定時]

定期ログ情報の自動格納間隔に30分が設定されているとみなされます。

```
system monitoringinfo collect interval 30m
```

16.9 外部メディアスタート機能の情報

16.9.1 storage setup mode

[機能]

外部メディアスタート機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

storage setup mode <mode>

[オプション]

<mode>

- enable
外部メディアスタート機能を有効にします。
- disable
外部メディアスタート機能を停止します。
- auto
構成定義未設定時に外部メディアスタート機能を有効にします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

外部メディアスタート機能を有効にするかどうかを設定します。
外部メディアスタート機能は外部メディアが挿入された状態での電源投入時のみ動作します。

[未設定時]

外部メディアスタート機能を有効にするとみなされます。

```
storage setup mode enable
```

16.9.2 storage setup machine

[機能]

外部メディアスタート機能有効時の装置名の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

storage setup machine <name>

[オプション]

<name>

装置名を 32 文字以内で指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

外部メディアスタート機能の有効時の、ソフト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する装置名を指定します。

[未設定時]

装置名からハイフンを削除し小文字をすべて大文字に変換した名前を利用します。

16.10 アンテナ情報

16.10.1 antenna use

[機能]

無線 LAN アンテナの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

antenna use <side>

[オプション]

<side>

- internal
内蔵アンテナを使用します。
- external
外付けアンテナを使用します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

内蔵アンテナを使用するか、外付けアンテナを使用するかを設定します。

[未設定時]

内蔵アンテナを使用するものとみなされます。

```
antenna use internal
```

16.11 サーバー情報

16.11.1 serverinfo ftp

[機能]

FTP サーバ機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo ftp ip <mode>
```

[オプション]

<mode>

- on
FTP サーバ機能を有効にします。
- off
FTP サーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

FTP サーバ機能を有効にするかどうかを設定します。

[未設定時]

FTP サーバ機能を有効にするものとみなされます。

```
serverinfo ftp ip on
```

16.11.2 serverinfo ftp filter

[機能]

FTP サーバ機能に対するアプリケーションフィルタ設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo ftp filter <count> <action> acl <acl_count>
```

[オプション]

<count>

- ・ フィルタリング定義番号
フィルタリングの優先度を表す定義番号を、0～9 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。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- ・ accept
該当するパケットを透過します。
- ・ reject
該当するパケットを遮断します。

<acl_count>

- ・ ACL 定義番号
使用する ACL 定義の番号を、10 進数で指定します。
指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
アプリケーションフィルタでは、ACL の以下の定義を使用します。
 - － ip
送信元 IP アドレスとマスクビット数のみを使用します。
ip 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

FTP サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

FTP サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

16.11.3 serverinfo ftp filter default

[機能]

FTP サーバ機能に対するアプリケーションフィルタのデフォルト動作の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo ftp filter default <action>
```

[オプション]

<action>

FTP サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
該当するパケットを透過します。
- reject
該当するパケットを遮断します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

FTP サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過します。

```
serverinfo ftp filter default accept
```

16.11.4 serverinfo sftp

[機能]

SSH FTP サーバ機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo sftp ip <mode>
```

[オプション]

<mode>

- on
SSH FTP サーバ機能を有効にします。
- off
SSH FTP サーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SSH FTP サーバ機能を有効にするかどうかを設定します。

本設定が off、および `serverinfo ssh ip` コマンドの設定が off の場合、sftp クライアントからの IPv4 アドレスでの接続要求は拒否されます。

本設定が off、および `serverinfo ssh ip` コマンドの設定が on の場合、sftp クライアントからの IPv4 アドレスでの接続要求はパスワード入力したあとに拒否されます。

[注意]

SSH ホスト認証鍵の生成が完了したあとに sftp 接続できるようになります。

ssh および sftp 機能をすべて off の状態で本装置を起動して本機能を有効にした場合にも SSH ホスト認証鍵を生成し、数十秒～数分の処理時間を要します。その場合、セッション監視タイムアウトが発生するなどほかの処理に影響することが考えられますので、ご注意ください。

SSH サーバ機能無効時は SSH FTP サーバ機能は有効となりません。SSH FTP サーバ機能を使用する場合は、SSH サーバ機能を有効としてください。

[未設定時]

SSH FTP サーバ機能を有効にするものとみなされます。

```
serverinfo sftp ip on
```

16.11.5 serverinfo telnet

[機能]

TELNET サーバ機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo telnet ip <mode>
```

[オプション]

<mode>

- on
TELNET サーバ機能を有効にします。
- off
TELNET サーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

TELNET サーバ機能を有効にするかどうかを設定します。

[未設定時]

TELNET サーバ機能を有効にするものとみなされます。

```
serverinfo telnet ip on
```

16.11.6 serverinfo telnet filter

[機能]

TELNET サーバ機能に対するアプリケーションフィルタの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo telnet filter <count> <action> acl <acl_count>
```

[オプション]

<count>

- ・ フィルタリング定義番号
フィルタリングの優先度を表す定義番号を、0~9 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。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- ・ accept
該当するパケットを透過します。
- ・ reject
該当するパケットを遮断します。

<acl_count>

- ・ ACL 定義番号
使用する ACL 定義の番号を、10 進数で指定します。
指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
アプリケーションフィルタでは、ACL の以下の定義を使用します。
 - － ip
送信元 IP アドレスとマスクビット数のみを使用します。
ip 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

TELNET サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

TELNET サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

16.11.7 serverinfo telnet filter default

[機能]

TELNET サーバ機能に対するアプリケーションフィルタのデフォルト動作設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo telnet filter default <action>
```

[オプション]

<action>

TELNET サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
該当するパケットを透過します。
- reject
該当するパケットを遮断します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

TELNET サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過するものとみなされます。

```
serverinfo telnet filter default accept
```

16.11.8 serverinfo ssh

[機能]

SSH ログインサーバ機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo ssh ip <mode>
```

[オプション]

<mode>

- on
SSH ログインサーバ機能を有効にします。
- off
SSH ログインサーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SSH ログインサーバ機能を有効にするかどうかを設定します。
本設定が off の場合、ssh クライアントからの IPv4 アドレスでの接続要求は拒否されます。

[注意]

本設定を有効にすると、本装置電源投入時および reset コマンド実行時に SSH ホスト認証鍵を生成するようになり、数十秒～数分の処理時間を要します。

SSH ホスト認証鍵の生成が完了したあとに ssh 接続できるようになります。

ssh および sftp 機能をすべて off の状態で本装置を起動して本機能を有効にした場合にも SSH ホスト認証鍵を生成し、数十秒～数分の処理時間を要します。その場合、セッション監視タイムアウトが発生するなどほかの処理に影響することが考えられますので、ご注意ください。

本設定を無効にすると、SSH FTP サーバ機能も無効になります。

[未設定時]

SSH ログインサーバ機能を有効にするものとみなされます。

```
serverinfo ssh ip on
```

16.11.9 serverinfo ssh filter

[機能]

SSH サーバ機能に対するアプリケーションフィルタの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo ssh filter <count> <action> acl <acl_count>
```

[オプション]

<count>

- ・ フィルタリング定義番号
フィルタリングの優先度を表す定義番号を、0～9 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。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- ・ accept
該当するパケットを透過します。
- ・ reject
該当するパケットを遮断します。

<acl_count>

- ・ ACL 定義番号
使用する ACL 定義の番号を、10 進数で指定します。
指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
アプリケーションフィルタでは、ACL の以下の定義を使用します。
 - － ip
送信元 IP アドレスとマスクビット数のみを使用します。
ip 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SSH サーバ機能に対するアプリケーションフィルタを設定します。
本定義は、SSH ログインサーバ機能および SSH FTP サーバ機能の両方に対して有効となります。
SSH ログインサーバ機能、SSH FTP サーバ機能にそれぞれ異なるフィルタ設定をすることはできません。

[未設定時]

SSH サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

16.11.10 serverinfo ssh filter default

[機能]

SSH サーバ機能に対するアプリケーションフィルタのデフォルト動作設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo ssh filter default <action>
```

[オプション]

<action>

SSH サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
該当するパケットを透過します。
- reject
該当するパケットを遮断します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SSH サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過するものとみなされます。

```
serverinfo ssh filter default accept
```

16.11.11 serverinfo http

[機能]

HTTP サーバ機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo http ip <mode>
```

[オプション]

<mode>

- on
HTTP サーバ機能を有効にします。
- off
HTTP サーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

HTTP サーバ機能を有効にするかどうかを設定します。

[未設定時]

HTTP サーバ機能を有効にするものとみなされます。

```
serverinfo http ip on
```

16.11.12 serverinfo http filter

[機能]

HTTP サーバ機能に対するアプリケーションフィルタの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo http filter <count> <action> acl <acl_count>
```

[オプション]

<count>

- ・ フィルタリング定義番号
フィルタリングの優先度を表す定義番号を、0～9 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。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- ・ accept
該当するパケットを透過します。
- ・ reject
該当するパケットを遮断します。

<acl_count>

- ・ ACL 定義番号
使用する ACL 定義の番号を、10 進数で指定します。
指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
アプリケーションフィルタでは、ACL の以下の定義を使用します。
 - － ip
送信元 IP アドレスとマスクビット数のみを使用します。
ip 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

HTTP サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

HTTP サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

16.11.13 serverinfo http filter default

[機能]

HTTP サーバ機能に対するアプリケーションフィルタのデフォルト動作設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo http filter default <action>
```

[オプション]

<action>

HTTP サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
該当するパケットを透過します。
- reject
該当するパケットを遮断します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

HTTP サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過します。

```
serverinfo http filter default accept
```

16.11.14 serverinfo https

[機能]

HTTPS サーバ機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

serverinfo https ip <mode>

[オプション]

<mode>

- on
HTTPS サーバ機能を有効にします。
- off
HTTPS サーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

HTTPS サーバ機能を有効にするかどうかを設定します。

[未設定時]

HTTPS サーバ機能を有効にするものとみなされます。

```
serverinfo https ip on
```

16.11.15 serverinfo https filter

[機能]

HTTPS サーバ機能に対するアプリケーションフィルタの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo https filter <count> <action> acl <acl_count>
```

[オプション]

<count>

- ・ フィルタリング定義番号
フィルタリングの優先度を表す定義番号を、0～9 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。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- ・ accept
該当するパケットを透過します。
- ・ reject
該当するパケットを遮断します。

<acl_count>

- ・ ACL 定義番号
使用する ACL 定義の番号を、10 進数で指定します。
指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
アプリケーションフィルタでは、ACL の以下の定義を使用します。
 - － ip
送信元 IP アドレスとマスクビット数のみを使用します。
ip 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

HTTPS サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

HTTPS サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

16.11.16 serverinfo https filter default

[機能]

HTTPS サーバ機能に対するアプリケーションフィルタのデフォルト動作設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

serverinfo https filter default <action>

[オプション]

<action>

HTTPS サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
該当するパケットを透過します。
- reject
該当するパケットを遮断します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

HTTPS サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときに、パケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過します。

```
serverinfo https filter default accept
```

16.11.17 serverinfo sntp

[機能]

Sntp サーバ機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo sntp ip <mode>
```

[オプション]

<mode>

- on
Sntp サーバ機能を有効にします。
- off
Sntp サーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

Sntp サーバ機能を有効にするかどうかを設定します。

[未設定時]

Sntp サーバ機能を有効にするものとみなされます。

```
serverinfo sntp ip on
```

16.11.18 serverinfo sntp filter

[機能]

SNTP サーバ機能に対するアプリケーションフィルタの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo sntp filter <count> <action> acl <acl_count>
```

[オプション]

<count>

- ・ フィルタリング定義番号
フィルタリングの優先度を表す定義番号を、0~9 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。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- ・ accept
該当するパケットを透過します。
- ・ reject
該当するパケットを遮断します。

<acl_count>

- ・ ACL 定義番号
使用する ACL 定義の番号を、10 進数で指定します。
指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。
アプリケーションフィルタでは、ACL の以下の定義を使用します。
 - ip
送信元 IP アドレスとマスクビット数のみを使用します。
ip 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNTP サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

SNTP サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

16.11.19 serverinfo sntp filter default

[機能]

SNTP サーバ機能に対するアプリケーションフィルタのデフォルト動作設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo sntp filter default <action>
```

[オプション]

<action>

SNTP サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
該当するパケットを透過します。
- reject
該当するパケットを遮断します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

SNTP サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過するものとみなされます。

```
serverinfo sntp filter default accept
```

16.11.20 serverinfo time

[機能]

TCP による TIME サーバ機能の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo time ip <mode>
```

[オプション]

<mode>

- on
TCP による TIME サーバ機能を有効にします。
- off
TCP による TIME サーバ機能を停止します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

TCP による TIME サーバ機能を有効にするかどうかを設定します。

[未設定時]

TCP による TIME サーバ機能を有効にするものとみなされます。

```
serverinfo time ip on
```

16.11.21 serverinfo time filter

[機能]

TIME サーバ機能に対するアプリケーションフィルタの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
serverinfo time filter <count> <action> acl <acl_count>
```

[オプション]

<count>

- ・ フィルタリング定義番号

フィルタリングの優先度を表す定義番号を、0～9の10進数で指定します。

指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

優先度は数値の小さい方がより高い優先度を示します。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- ・ accept

該当するパケットを透過します。

- ・ reject

該当するパケットを遮断します。

<acl_count>

- ・ ACL 定義番号

使用する ACL 定義の番号を、10進数で指定します。

指定した<acl_count>の ACL が定義されていない場合、そのフィルタ定義は無効となり、無視されます。

アプリケーションフィルタでは、ACL の以下の定義を使用します。

- － ip

送信元 IP アドレスとマスクビット数のみを使用します。

ip 値が設定されていない場合、そのフィルタ定義は無効となり、無視されます。

[動作モード]

構成定義モード(管理者クラス)

[説明]

TIME サーバ機能に対するアプリケーションフィルタを設定します。

[未設定時]

TIME サーバ機能に対するアプリケーションフィルタを設定しないものとみなされます。

16.11.22 serverinfo time filter default

[機能]

TIME サーバ機能に対するアプリケーションフィルタのデフォルト動作設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

serverinfo time filter default <action>

[オプション]

<action>

TIME サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- accept
該当するパケットを透過します。
- reject
該当するパケットを遮断します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

TIME サーバ機能に対するどのアプリケーションフィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

どのアプリケーションフィルタテーブルにも一致しないパケットは透過するものとみなされます。

```
serverinfo time filter default accept
```

16.12 DNS サーバ情報

16.12.1 dns-resolver server

[機能]

DNS サーバアドレス設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

dns-resolver server <address1> [<address2>]

[オプション]

<index>

- ・ 登録番号
コマンド実行予約情報の登録番号を指定します。
必ず0を指定してください。

<address1>

- ・ DNS サーバ IP アドレス 1
DNS サーバの 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。
1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254

<address2>

- ・ DNS サーバ IP アドレス 2
DNS サーバの 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。
1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254

[動作モード]

構成定義モード(管理者クラス)

[説明]

DNS サーバのアドレスを設定します。

[注意]

- ・ LAN インタフェースが設定されている場合、本コマンドは有効となります。
- ・ DHCP クライアント機能を使用する場合、DHCP サーバから通知された DNS サーバは利用できません。
- ・ address1 と address2 の両方が登録された場合は、両方の DNS サーバに名前解決問合せを行い、先に名前解決応答された方を利用します。

[未設定時]

DNS サーバアドレスを設定しないものとみなされます。

16.13 その他

16.13.1 addact

[機能]

コマンド実行予約の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

addact <index> <date> <command>

[オプション]

<index>

- 登録番号
コマンド実行予約情報の登録番号を指定します。
必ず0を指定してください。

<date>

- 実行日時
コマンド実行日時を、yymmddHHMMの形式で指定します。

yy

西暦の下2桁を指定します。西暦2099年まで指定できます。

mm

月を、1~12の10進数で指定します。

dd

日付を、1~31の10進数で指定します。

HH

時間を、0~23の10進数で指定します。

MM

分を、0~59の10進数で指定します。

<command>

実行するコマンド文字列を指定します。

- reset
装置を再起動する場合に指定します。
- reset config1
構成定義1に切り替えて再起動する場合に指定します。
- reset config2
構成定義2に切り替えて再起動する場合に指定します。
上記以外のコマンドを指定した場合の動作は保証されません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

コマンド実行予約を設定します。

[注意]

以下に、スケジュール機能によってコマンドを実行する場合の注意事項を示します。

- 装置の時刻を正しく設定してください。

-
- ・ 実施時刻に、装置の電源を投入しておいてください。

[実行例]

以下に、2021 年 1 月 1 日 午前 2 時 に構成定義 2 に切り替えて再起動する場合の設定例を示します。

```
# addact 0 2101010200 reset config2  
#
```

[未設定時]

コマンドの実行予約を行わないものとみなされます。

16.13.2 consoleinfo

[機能]

シリアルコンソール接続サービスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

consoleinfo autologout <time>

[オプション]

<time>

- ・ 強制ログアウト時間

シリアルコンソールでログインしたままコマンド実行が行われない状態が続いたときに強制ログアウトさせる時間を、0～86400 秒(1 日)の範囲で指定します。

単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

0 秒を指定した場合は、強制ログアウトしません。

[動作モード]

構成定義モード(管理者クラス)

[説明]

シリアルコンソールでログインしたまま<time>で指定した時間内にコマンド実行されなかった場合、強制的にログアウトさせるように設定します。

[未設定時]

強制ログアウトさせないものとみなされます。

```
consoleinfo autologout 0s
```

16.13.3 telnetinfo

[機能]

TELNET 接続サービスの設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
telnetinfo autologout <time>
```

[オプション]

<time>

- ・ 自動切断時間

telnet 接続したクライアントからコマンド入出力が行われない状態で自動切断するまでの時間を、0～86400 秒(1 日)の範囲で指定します。

単位は、d(日)、h(時)、m(分)、s(秒)のどれかを指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

TELNET コネクションの入出力がない場合にコネクションを切断するまでの時間を設定します。

[未設定時]

TELNET コネクションの入出力の監視を行わないものとみなされます。

```
telnetinfo autologout 0s
```

16. 13. 4 sysname

[機能]

本装置の名称の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

sysname <name>

[オプション]

<name>

- ・ 名称

本装置の名称を、32 文字以内の ASCII 文字列で指定します。使用可能な文字はアルファベット (a~z、A~Z)、数字 (0~9)、ハイフン (-)、アンダースコア (_) です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置の名称を設定します。

本コマンドで設定する名称は、SNMP で使用する MIB 変数 sysName としても使用することができます。その場合、snmp agent sysname コマンドで設定している sysName を削除しておくことで本コマンドで設定したホスト名が sysName として使用されます。

本コマンドと snmp agent sysname コマンドとはネットワーク動作として直接の関連性はありませんが、ネットワークの管理上、同じ名称に統一する必要があります。

[注意]

本設定を変更した場合は、装置再起動が必要です。

[未設定時]

本装置の名称を設定しないものとみなされます。

第 17 章 モード操作コマンド/ターミナル操作コマンド

17.1 モード操作

17.1.1 exit

[機能]

運用管理モードに戻る、またはログアウトする

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

exit

[オプション]

なし

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

構成定義モードから運用管理モードに戻ります。

[注意]

運用管理モードの場合はログアウトします。
構成定義に変更がある場合はメッセージを表示して運用管理モードに戻ります。
構成定義階層機能については configure コマンドを参照してください。

[メッセージ]

```
<WARNING> the candidate-config has been changed but not committed.
```

構成定義情報を反映しないで運用管理モードに戻りました。変更および追加した構成定義情報はそのまま残っています。構成定義情報を反映しなくてもよいかを確認してください。

[実行例]

```
(config)# exit
<WARNING> the candidate-config has been changed but not committed.
# exitWARNING
Login:
```

17.1.2 configure

[機能]

構成定義モードに移行する

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

configure

[オプション]

なし

[動作モード]

運用管理モード(管理者クラス)

[説明]

運用管理モードから構成定義モードに移行します。

構成定義モードから運用管理モードに戻るには、exit コマンドを実行してください。

[実行例]

```
# configure
(config)#
```

17.2 コマンド実行履歴

17.2.1 show logging command

[機能]

コマンド実行履歴の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show logging command [{ brief | all }]
```

[オプション]

なし

コマンド実行履歴を詳細形式で表示します。

brief

コマンド実行履歴を簡易形式で表示します。

all

すべてのログイン回線で実行したコマンド履歴を表示します。

省略した場合は、使用中のログイン回線で実行したコマンド履歴を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

コマンド実行履歴を表示します。

一般ユーザクラスでは一般ユーザクラスで実行したコマンド実行履歴だけが表示され、履歴番号は不連続になります。管理者クラスでは一般ユーザクラスと管理者クラスで実行したコマンド実行履歴が表示されます。

- Ctrl+P キーまたは↑キーでその行を表示し、改行キーを押してコマンドを実行します。
- Ctrl+P キーまたは↑キーでその行を表示し、Ctrl+C を押して入力内容を破棄します。

コンソール/telnet/sshのシェルでCTRL+P キー、CTRL+N キー、↑キー、↓キーなどを入力してコマンド履歴をたどるとき、使用中ログイン回線で実行したコマンドだけが順次表示されます。

[注意]

履歴番号が 1000 を超えると、適する小さな履歴番号に戻ります。

[実行例]

```
# show logging command
01/01 15:58:55 * console 0 admin          1 show system information
01/01 15:19:04 * console 0 admin          2 show date
01/01 16:00:19 * console 0 admin          3 show logging command
(1)          (2) (3)          (4)          (5) (6)
#
# show logging command brief
  1 show system information
  2 show date
  3 show logging command
  6 show logging command brief
(5) (6)
#
# show logging command all
01/01 15:58:55 * console 0 admin          1 show system information
01/01 15:59:04 * console 0 admin          2 show date
01/01 16:00:19 * console 0 admin          3 show logging command
01/01 16:00:54 vty 0 user                 4 show interface
01/01 16:00:55 ssh 0 admin                5 show logging syslog
01/01 16:01:32 * console 0 admin          6 show logging command brief
01/01 16:02:48 * console 0 admin          7 show logging command all
(1)          (2) (3)          (4)          (5) (6)
#
```

- 1) コマンド実行日時
- 2) "*" : 使用中ログイン回線
- 3) コマンド実行ログイン回線名
- 4) コマンド実行ユーザ名
- 5) コマンド履歴番号
- 6) 実行コマンド

17.2.2 clear logging command

[機能]

コマンド実行履歴の消去

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
clear logging command [all]
```

[オプション]

all

すべてのログイン回線のコマンド実行履歴を消去します。

省略した場合、使用中のログイン回線で実行したコマンド実行履歴を消去します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

運用管理モードおよび構成定義モードでのコマンド実行履歴を消去します。

clear logging command all を実行すると、実行履歴番号は1に戻ります。

[実行例]

```
# clear logging command
#
```

第 18 章 システム操作および表示コマンド

18.1 システム操作および表示

18.1.1 show system information

[機能]

静的なシステム情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show system information

[オプション]

なし

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

装置の静的なシステム状態・情報を表示します。

[実行例]

```
# show system information
Current-time : Thu Oct 22 12:11:38 2020          ---(1)
Startup-time : Thu Oct 22 12:10:40 2020          ---(2)
System : SR-M630AP1                             ---(3)
Serial No. : 1000123                             ---(4)
Boot loader Ver. : 1.0                          ---(5)
Soft Ver. : V20.00 NY0002 Mon Oct 19 21:20:47 JST 2020 ---(6)
Running-software : software1                    ---(7)
Software1 Ver. : V20.00 NY0002 Mon Oct 19 21:20:47 JST 2020 ---(8)
Software2 Ver. : V20.00 NY0001 Wed Oct 14 11:17:00 JST 2020
Startup-config : Thu Oct 22 11:17:07 2020 configl ---(9)
Running-config : Thu Oct 22 12:10:40 2020        ---(10)
MAC : 00e00079aa62-00e00079aa63                 ---(11)
      00e00079aa64-00e00079aa64 (2.4GHz)
      00e00079aa65-00e00079aa66 (5GHz)
Memory : 1917MB                                 ---(12)
```

- 1) Current time
現在の日付、時刻が表示されます。
- 2) Startup time
装置を起動した日付、時刻が表示されます。
- 3) System
装置名が表示されます。
- 4) Serial No.
装置のシリアル番号が表示されます。
- 5) Boot loader Ver.
ブートローダの版数が xx.yy の形式で出力されます。xx.yy は 10 進数で表示されます。
- 6) Soft Ver.
起動しているソフトウェアのバージョン、版数、日付が表示されます。
バージョンは Vxx.yy の形式で表示されます。xx.yy は 2 桁の 10 進数です。

-
- 7) Running-software
起動しているソフトウェアが表示されます。
 - 8) Software1 Ver.
バンク 1 のソフトウェアのバージョン、版数、日付が表示されます。
Software2 Ver.
バンク 2 のソフトウェアのバージョン、版数、日付が表示されます。
バージョンは Vxx.yy の形式で表示されます。xx.yy は 2 桁の 10 進数です。
 - 9) Startup-config
装置起動時に読み込まれる構成定義の保存された日付、時刻およびファイル名が表示されます。
NXconciierge 連携において、管理ポータルからの構成定義変更指示を受ける場合、日付、時刻が更新されます。
 - 10) Running-config
現在動作中の構成定義を反映した日付、時刻が表示されます。
NXconciierge 連携において、管理ポータルからの構成定義変更指示を受ける場合、日付、時刻が更新されます。
 - 11) MAC
1 行目に有線 LAN の MAC アドレス、2 行目以降に無線 LAN の MAC アドレスが 12 桁の 16 進数で表示されます。
 - 12) Memory
装置に実装されているメモリサイズが表示されます。

18.1.2 show system status

[機能]

動的なシステム情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show system status

[オプション]

なし

動的なシステム情報を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

装置の動的なシステム情報を表示します。

[実行例]

```
# show system status
Current-time       : Thu Oct 22 12:16:49 2015      ---(1)
Startup-time      : Thu Oct 22 12:10:40 2015      ---(2)
restart_cause     : power on                      ---(3)
machine_state     : RUNNING                       ---(4)
corefile         : empty                          ---(5)
internal_state   : NORMAL                         ---(6)
internal_temp    : 39 C                           ---(7)
setup_mode       : enable                          ---(8)
operation_type   : WEBUI                          ---(9)
CONNECTOR       :                                ---(10)
usb             :
```

- 1) Current time
現在の日時
- 2) Startup time
システムの起動日時
- 3) restart_cause
システム起動要因
以下のシステム起動要因が表示されます。
power on
電源投入
reset
reset コマンド発行
reset switch
リセットスイッチ押下
system down
システムダウン発生
- 4) machine_state
装置状態

RUNNING

動作中

FALLBACK

縮退モードで起動中

- 5) corefile
異常時のメモリダンプファイル（コアファイル）の有無

empty

存在していない

exists

存在している

- 6) internal_state
内部温度状態

NORMAL

正常

HIGHALARM

高温異常

UNKNOWN

非監視状態、または状態不明

- 7) internal_temp
内部温度

- 8) setup_mode
storage factory setup mode(外部メディアスタート機能の有効/無効)の状態

enable

有効（工場出荷状態では enable、reset clear の実行で enable となる）

disable

無効（構成定義を保存、または装置外部からインストールすると disable となる）

- 9) operation_type
運用タイプ

WEBUI

WEB ユーザインタフェース設定による運用

CLI

コマンドラインインタフェース設定による運用

- 10) CONNECTOR
USB ポートに実装された USB デバイスの名称が表示されます。

18.1.3 show tech-support

[機能]

解析情報の一括表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show tech-support [detail] [save]

[オプション]

なし

結果を表示します。

detail

結果を詳細表示します。

save

結果を外部メディアに書き込みます。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

本装置の設定情報や各種ステータスなど解析に必要な情報が一括で表示されます。

ターミナルソフトウェアの出力キャプチャ機能を使用して、本コマンド実行時の出力内容を保存するか、外部メディアに書き込んでください。

18.1.4 show logging error

[機能]

エラーログの表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show logging error

[オプション]

なし

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

ROM または I/O ドライバによるハード診断エラー、およびシステムダウンのエラーログ情報を表示します。

[注意]

“Logging time:”で表示する時刻は、構成定義情報にタイムゾーン(time zone <offset>)が指定されていない状態では GMT(グリニッジ標準時間)での表示となります。

システムダウンのエラーログは電源再投入しても保持されますので、必要に応じて clear logging error コマンドでクリアしてください。

[実行例]

```
# show logging error
2020/01/01 17:06:21 192.168.1.1 SR-M630AP1: rasmng: [85010000:00000000] Thermal error [sensor#1]
2020/01/01 17:06:21 192.168.1.1 SR-M630AP1: rasmng: [85010000:00000000] Thermal error [sensor#2]
2020/01/01 18:38:11 192.168.1.1 SR-M630AP1: kernel: [85FF0010:00000022] error (SDHCI_INT_TIMEOUT).
2020/01/01 18:48:11 192.168.1.1 SR-M630AP1: kernel: [85FF0010:00000022] error (SDHCI_INT_CRC).
```

18.1.5 clear logging error

[機能]

エラーログのクリア

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

clear logging error

[オプション]

なし

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

すべてのエラーログを消去し、CHECK ランプを消灯します。

[実行例]

```
# clear logging error  
#
```

18.1.6 show logging syslog

[機能]

システムログ情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show logging syslog

[オプション]

なし

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

システムログ情報を表示します。

[注意]

本装置の電源 OFF、reset clear などご購入時の状態に戻す操作、または clear logging syslog コマンドを実行すると、システムログ情報はクリアされます。

ただし、リセットコマンド、リセットスイッチの押下、およびシステムエラーによる装置再起動の場合はクリアされません。

[実行例]

```
# show logging syslog
2020/01/01 15:52:31 192.168.1.1 SR-M630AP1 : init: system startup now.
2020/01/01 15:52:31 192.168.1.1 SR-M630AP1 : sshd: generating public/private host key pair.
2020/01/01 15:52:40 192.168.1.1 SR-M630AP1 : ethermng: ether 1 link up
2020/01/01 15:52:40 192.168.1.1 SR-M630AP1 : ethermng: lan 0 link up
```

18.1.7 clear logging syslog

[機能]

システムログ情報のクリア

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
clear logging syslog
```

[オプション]

なし

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

すべてのシステムログ情報をクリアします。

[実行例]

```
# clear logging syslog  
#
```

18.1.8 show logging monitoringinfo

[機能]

FLASH メモリ内定期ログ情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show logging monitoringinfo [current]
```

[オプション]

なし

FLASH メモリに格納された定期ログ情報をすべて表示します。

current

FLASH メモリに格納された定期ログ情報の中で最新の情報を 1 件のみ表示します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

FLASH メモリに格納された定期ログ情報を表示します。

[注意]

定期ログ情報の表示開始までには最大で 20 秒かかります。

表示されるまでの間、以下のメッセージを出力します。

```
Please wait a moment until output is starting.
```

[実行例]

定期ログ情報域が正常な場合

```
# show logging monitoringinfo
Please wait a moment until output is starting.

-----

[Monitoring info : 1]                               ---(1)
Logging time: Wed Sep 30 05:39:24 2020              ---(2)

# show system information                             ---(3)
---Wed Sep 30 05:39:24 JST 2020---
Current-time : Wed Sep 30 05:39:24 2020
Startup-time : Tue Sep 29 21:26:02 2020
System : SR-M630AP1
Serial No. : 305419896
Boot loader Ver. : 1.3
Soft Ver. : V20.00 NY0003 Thu Sep 24 14:14:41 JST 2020
Running-software : software1
Software1 Ver. : V20.00 NY0003 Thu Sep 24 14:14:41 JST 2020
Software2 Ver. : V20.00 NY0003 Thu Sep 24 14:14:41 JST 2020
Startup-config : Wed Sep 30 04:49:21 2020 config1
Running-config : Wed Sep 30 04:49:23 2020
MAC : 00e00079aa62-00e00079aa63
      00e00079aa64-00e00079aa64 (2.4GHz)
      00e00079aa65-00e00079aa66 (5GHz)
Memory : 1917MB
# show system status
---Wed Sep 30 05:39:24 JST 2020---
Current-time      : Wed Sep 30 05:39:24 2020
Startup-time     : Tue Sep 29 21:26:01 2020
restart_cause    : reset
machine_state    : RUNNING
internal_state   :
internal_temp    : 40 C
                  41 C
                  40 C
setup_mode       : disable
CONNECTOR
usb              :
:
```

- 1) Monitoring info
定期ログ番号(1~99)が表示されます。
current 指定の場合は、定期ログ番号は表示されません。
- 2) Logging time
ログ収集日時が表示されます。
- 3) コマンド実行結果
コマンドを実行した結果が表示されます。

18.1.9 clear logging monitoringinfo

[機能]

FLASH メモリ内定期ログ情報のクリア

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
clear logging monitoringinfo
```

[オプション]

なし

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

FLASH メモリに格納されたすべての定期ログ情報を消去します。

[注意]

定期ログ情報の消去には時間がかかる場合があります。

[実行例]

```
# clear logging monitoringinfo
```

18.1.10 clear statistics

[機能]

全統計情報のクリア

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

clear statistics

[オプション]

なし

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

すべての統計情報をクリアします。
但し、無線 LAN モジュール、無線 LAN インタフェースの統計情報はクリアされません。

[実行例]

```
# clear statistics  
#
```

18.1.11 show date

[機能]

現在の装置の日付、時刻の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show date

[オプション]

なし

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

現在の装置の日付、時刻を表示します。

[実行例]

```
# show date
Thu Feb 19 14:26:00 2020 ---(1)
```

1) 現在の日付、時刻が表示されます。

18.1.12 date

[機能]

現在の装置の日付、時刻の表示／設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

date [YYYY/MM/DD. hh:mm:ss]

[オプション]

なし

現在の装置の日付、時刻を表示します。

YYYY/MM/DD. hh:mm:ss

指定した日付、時刻を設定します。(管理者クラスのみ有効)

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

現在の装置の日付、時刻を表示したり、設定したりします。

[実行例]

日付、時刻を表示する場合

```
# date
Thu Feb 19 14:26:00 2020
#
```

日付、時刻を設定する場合

```
# date 2020/02/19.14:26:00
#
```

18.1.13 rdate

[機能]

リモートホストの日付、時刻を本装置に設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

rdate

[オプション]

なし

リモートホストの日付、時刻を本装置に設定します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

time auto server で指定したリモートホスト(タイムサーバ)の日付、時刻を取得し、本装置の日付、時刻として設定します。

[実行例]

```
# rdate
Thu Feb 19 14:26:00 2020
#
```

18.1.14 reset

[機能]

装置の再起動

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
reset [<filename>]
reset [<software>]
reset clear
```

[オプション]

なし

update 操作を実行した場合、更新したソフトウェアで起動します。
update 操作を実行していない場合、運用中のソフトウェアで起動します。

<filename>

起動時に読み込む startup-config ファイルを指定します。

- config1
構成定義情報 1 を読み込みます。
- config2
構成定義情報 2 を読み込みます。

<software>

起動するソフトウェアを指定します。

- software
運用中のソフトウェアと反対バンクのソフトウェアで起動します。
- software1
ソフトウェア 1 で起動します。
- software2
ソフトウェア 2 で起動します。

clear

設定をご購入時の状態に戻し、装置を再起動します。

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

装置を再起動します。

[注意]

再起動には約 80 秒かかります。

[実行例]

```
# reset
#
```

18.1.15 clear corefile

[機能]

core ファイルの削除

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

clear corefile

[オプション]

なし

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

core ファイルを削除します。

18.1.16 clear https certificate

[機能]

HTTPS 証明書情報の消去

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
clear https certificate
```

[オプション]

なし

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

HTTPS 証明書情報を消去して、HTTPS プロセスを再起動します。

HTTPS プロセスの再起動により証明書は新たに作成されます。

HTTPS 接続中に本コマンドを実行した場合は、再ログインが必要となります。

第 19 章 構成定義情報の表示、削除、および操作コマンド

19.1 構成定義情報表示

19.1.1 show candidate-config

[機能]

編集構成定義情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show candidate-config

[オプション]

なし

すべての構成定義情報を表示します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

現在編集中の構成定義情報を表示します。

[実行例]

```
# show candidate-config
#
# System : SR-M630AP1
# Soft Ver. : V20.00 NY0001 Thu Jul 16 09:29:32 JST 2020
# Config : Mon Feb 21 21:00:19 2021
#
lan 0 ip address 192.168.0.1/24 3
lan 0 vlan 1
#
```

19.1.2 show running-config

[機能]

動作中構成定義情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show running-config

[オプション]

なし

すべての構成定義情報を表示します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

現在動作中の構成定義情報を表示します。

[実行例]

```
# show running-config
#
# System : SR-M630AP1
# Soft Ver. : V20.00 NY0001 Thu Jul 16 09:29:32 JST 2020
# Config : Mon Feb 21 20:21:19 2021
#
lan 1 ip address 192.168.1.1/24 3
lan 1 vlan 1
#
```

19.1.3 show startup-config

[機能]

起動用構成定義情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show startup-config

[オプション]

なし

すべての構成定義情報を表示します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

保存してある起動用構成定義情報を表示します。

[実行例]

```
# show startup-config
#
# System : SR-M630AP1
# Soft Ver. : V20.00 NY0001 Thu Jul 16 09:29:32 JST 2020
# Config : Mon Feb 21 20:00:19 2021
#
lan 0 ip address 192.168.0.1/24 3
lan 0 vlan 1
syslog pri error, warn, info
syslog facility 23
telnetinfo autologout 5m
time zone 0900
#
```


19.1.4 diff

[機能]

構成定義情報の差分の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
diff <src_filename> <dst_filename>
```

[オプション]

<src_filename>

比較元のファイル名を指定します。

<dst_filename>

比較先のファイル名を指定します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

指定されたファイルの差分のみを表示します。<src_filename>にのみある情報には行の先頭に“< ”を、<dst_filename>にのみある情報には行の先頭に“> ”を付加して表示します。

ファイル名としては以下のものが指定できます。

<src_filename>として指定可能なファイル名	
candidate-config	編集中の構成定義ファイル
running-config	運用中の構成定義ファイル
startup-config	起動用の構成定義ファイル
config1	第1構成定義ファイル
config2	第2構成定義ファイル
/um0/任意のファイル名	USBメモリ上のファイル

<dst_filename>として指定可能なファイル名	
candidate-config	編集中の構成定義ファイル
running-config	運用中の構成定義ファイル
startup-config	起動用の構成定義ファイル
config1	第1構成定義ファイル
config2	第2構成定義ファイル
/um0/任意のファイル名	USBメモリ上のファイル

[実行例]

```
# diff candidate-config running-config
===
> vlan 1 name rmt1
===
< vlan 3 name rmt3
< vlan 4 name rmt4
< vlan 5 name rmt5
< vlan 6 name rmt6
---
> vlan 3 name inter3
===
< vlan 8 name rmt8
< vlan 9 name rmt9
< vlan 10 name rmt10
#
```

19.2 構成定義情報削除

19.2.1 delete

[機能]

編集集中構成定義情報の削除

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
delete <config>
```

[オプション]

<config>

- 構成定義コマンド
削除する構成定義コマンド名および引数を指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定した構成定義情報を削除して未設定状態にします。

<config>で指定したコマンド名と引数で始まるコマンドがすべて削除されます。

コマンド名だけを指定した場合は、そのコマンド名で始まる構成定義情報がすべて削除されます。

構成定義コマンドの引数がいくつまで指定できるかは、各コマンドによって異なりますが、大抵の場合、可変値の手前の引数まで指定できます。

[注意]

ログインパスワード情報は、以下のように set まで指定しないと削除できません。

```
delete password user set
```

[実行例]

lan 0 の DHCP 情報をすべて削除する場合の実行例を示します。

```
(config)# delete lan 0 ip dhcp
```

19.3 構成定義情報操作

19.3.1 load

[機能]

構成定義の読み込み

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

load <filename>

[オプション]

<filename>

読み込むファイル名を指定します。

[動作モード]

構成定義モード(管理者クラス)

[説明]

指定の構成定義を読み込みます。

設定中の内容は、すべて無効になります。

ファイル名としては以下が指定できます。

running-config	運用中の構成定義ファイル
startup-config	起動用の構成定義ファイル
config1	構成定義情報1のファイル
config2	構成定義情報2のファイル
/um0/任意のファイル名	USBメモリ上のファイル

[メッセージ]

```
load failed: config read error
```

構成定義を読み込めません。

構成定義ファイルが存在していることを確認し、再度本コマンドを実行してください。

```
<WARNING> weak admin's password: set the password
```

管理者パスワードが設定されていません。

管理者パスワードを設定してください。

```
<WARNING> weak admin's password: contain at least 8 characters
```

管理者パスワードが7文字以下です。

8文字以上の管理者パスワードを設定してください。

```
<WARNING> weak admin's password: contain a different kind of character
```

管理者パスワードが英字のみ、または数字のみです。

英字、数字、記号を混ぜて管理者パスワードを設定してください。

```
<WARNING> weak user's password: contain at least 8 characters
```

一般ユーザパスワードが7文字以下です。
8文字以上の一般ユーザパスワードを設定してください。

```
<WARNING> weak user's password: contain a different kind of character
```

一般ユーザパスワードが英字のみ、または数字のみです。
英字、数字、記号を混ぜて一般ユーザパスワードを設定してください。

[実行例]

```
# load config1  
#
```

19.3.2 save

[機能]

構成定義情報の保存

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

save [<filename>]

[オプション]

なし

candidate-config の内容を現在の startup-config ファイルに上書きします。

<filename>

candidate-config の内容を指定したファイルに上書きします。

[動作モード]

構成定義モード(管理者クラス)

[説明]

candidate-config の内容を指定したファイルに上書きします。

オプション省略時は現在の startup-config ファイルに上書きします。

ファイル名としては以下が指定できます。

startup-config	起動用の構成定義ファイル
config1	構成定義情報 1 のファイル
config2	構成定義情報 2 のファイル
/um0/任意のファイル名	USBメモリ上のファイル

[実行例]

```
# save
#
```

19.3.3 commit

[機能]

構成定義情報の動的反映

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

commit

[オプション]

なし

[動作モード]

構成定義モード(管理者クラス)

[説明]

構成定義コマンドで設定または変更した構成定義情報を、装置の再起動を行わずに反映します。

[注意]

構成定義情報の変更内容によっては、装置内部のアドレス情報などを反映するためにいったん通信インタフェースがダウンして通信が途切れることがありますのでご注意ください。詳細は、「commit コマンド実行時の影響について」を参照してください。

[メッセージ]

```
<ERROR> need to do reset after execute the save command.
```

反映ができない構成定義情報を追加または変更したため、構成定義情報を反映できません。
save コマンドを実行後に reset コマンドを実行して再起動してください。

```
<WARNING> the candidate-config is not changed.
```

構成定義情報を追加または変更していません。
commit コマンドを実行する必要はありません。

[実行例]

```
# commit  
#
```

19.3.4 discard

[機能]

構成定義情報の変更破棄

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

discard

[オプション]

なし

[動作モード]

構成定義モード(管理者クラス)

[説明]

candidate-config の変更内容を破棄し、running-config と同じ内容に戻します。

[メッセージ]

```
<WARNING> weak admin's password: set the password
```

管理者パスワードが設定されていません。
管理者パスワードを設定してください。

```
<WARNING> weak admin's password: contain at least 8 characters
```

管理者パスワードが7文字以下です。
8文字以上の管理者パスワードを設定してください。

```
<WARNING> weak admin's password: contain a different kind of character
```

管理者パスワードが英字のみ、または数字のみです。
英字、数字、記号を混ぜて管理者パスワードを設定してください。

```
<WARNING> weak user's password: contain at least 8 characters
```

一般ユーザパスワードが7文字以下です。
8文字以上の一般ユーザパスワードを設定してください。

```
<WARNING> weak user's password: contain a different kind of character
```

一般ユーザパスワードが英字のみ、または数字のみです。
英字、数字、記号を混ぜて一般ユーザパスワードを設定してください。

[実行例]

```
# discard
```

19.4 ファイル操作コマンド

19.4.1 dir

[機能]

ファイル一覧の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

dir [<filename>]

[オプション]

<filename>

表示するファイル名またはディレクトリ名を指定します。dir コマンドは一致したファイルまたはディレクトリのみを表示します。ディレクトリが指定された場合は、指定されたディレクトリ内に存在するファイルを表示します。

本オプションではワイルドカードが使用できます。使用可能なワイルドカードを以下に示します。

すべての文字列が一致します。文字列の長さに関係しません。

?

任意の1文字と一致します。

[<char>]

<char>に記述された文字のどれかが含まれる場合に一致します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

外部メディアのファイル一覧の表示を行います。

[実行例]

```
# dir
Directory of /um0                ---(1)

   (2)      (3)      (4)      (5)
2005/06/10 11:55          1445 CONFIG2.TXT
2005/06/10 11:55          1445 CONFIG3.TXT
2005/06/10 11:55          1445 CONFIG4.TXT
2005/06/10 11:55          1445 CONFIG11.TXT
2005/06/10 11:55          1445 CONFIG1.TXT
2005/06/13 03:16      2337531 FIRM
2005/06/13 01:58    <DIR>      TEST

                                total file          6
                                total directory       1

# dir test/*.*
Directory of /um0/test

2005/06/12 10:23          3142 CONFIG2.TXT
2005/06/13 01:58    <DIR>      BKUP

                                total file          1
                                total directory       1
```


-
- 1) USB メモリであれば/um0 になります。
 - 2) ファイルの更新日が表示されます。
 - 3) ディレクトリであれば<DIR>と表示されます。
 - 4) 通常ファイルであればファイルサイズが表示されます。単位は byte です。
 - 5) ファイル名またはディレクトリ名が表示されます。

19.4.2 copy

[機能]

ファイルのコピー

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

copy <src_filename> <dst_filename>

[オプション]

<src_filename>

コピー元のファイル名を指定します。

<dst_filename>

コピー先のファイル名を指定します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

ファイルのコピーを行います。ファイル名としては以下のものが指定できます。

<src_filename>として指定可能なファイル名	
all	ソフトウェアおよび構成定義ファイル
candidate-config	編集中の構成定義ファイル
running-config	運用中の構成定義ファイル
startup-config	起動用の構成定義ファイル
config1	第1構成定義ファイル
config2	第2構成定義ファイル
/um0/任意のファイル名	USBメモリ上のファイル
monitoringinfo	定期ログ情報ファイル
ftp://<ftp_user>[:<ftp_passwd>]@<ipv4address>/<filename>	FTPによるダウンロード元
software	現状のバンクのソフトウェア
software1	ソフトウェア1
software2	ソフトウェア2
corefile	コアファイル
devscan.csv	端末リストCSVファイル
web-data	Web運用モードの設定管理情報
eee80211.pcap	無線LANのパケットキャプチャファイル
radius.pcap	RADIUS認証のパケットキャプチャファイル

<dst_filename>として指定可能なファイル名	
startup-config	起動用の構成定義ファイル
config1	第1構成定義ファイル
config2	第2構成定義ファイル
/um0/任意のファイル名	USBメモリ上のファイル
ftp://<ftp_user>[:<ftp_passwd>]@<ipv4address>/<filename>	FTPによるアップロード先
software	現状のバンクと反対のソフトウェア
web-data	Web運用モードの設定管理情報
caroot.cer	ルート証明書

<ftp_user>

FTP サーバのユーザ名を、0x21, 0x23~0x7e の 32 文字以内の ASCII 文字列で指定します。

<ftp_passwd>

FTP サーバのパスワードを、0x21, 0x23~0x7e の 32 文字以内の ASCII 文字列で指定します。

<ipv4address>

FTP サーバの 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。

1. 0. 0. 1～ 126. 255. 255. 254
128. 0. 0. 1～ 191. 255. 255. 254
192. 0. 0. 1～ 223. 255. 255. 254

<filename>

ファイル名を、0x21, 0x23～0x7e の 116 文字以内の ASCII 文字列で指定します。

[注意]

<src_filename>に all を指定した場合、<dst_filename>は "/um0/"だけを指定してください。
"/um0/"以降にファイル名を指定しても無効になります。

[実行例]

```
# copy config1 /um0/config1  
#
```

19.4.3 remove

[機能]

ファイルの削除

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

remove <filename>

[オプション]

<filename>

削除するファイル名を指定します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

外部メディアのファイルの削除を行います。

[実行例]

```
# remove config1_cf
#
```

19.4.4 rename

[機能]

ファイル名の変更

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
rename <old_filename> <new_filename>
```

[オプション]

<old_filename>

変更前のファイル名を指定します。

<new_filename>

変更後の新しいファイル名を指定します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

外部メディアのファイル名の変更を行います。

[実行例]

```
# rename config1_cf config1_cf_old
#
```

19.4.5 format

[機能]

フォーマット

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

format

[オプション]

なし

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

外部メディアのフォーマットを行い、出荷状態に初期化します。

[実行例]

```
# format  
#
```

第 20 章 ログインユーザの状態などの表示、クリア操作コマンド

20.1 ログインユーザの状態などの表示

20.1.1 show users

[機能]

ログインユーザ情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show users [all]

[オプション]

なし

ログインしているユーザ情報の一覧を表示します。

all

ログインしていない回線も表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

本装置にログインしているユーザの情報を表示します。

[実行例]

```
# show users
U No Line      User Name      Class Remote Host      Since      Idle
-----
(1) (2) (3)      (4)           (5) (6)           (7)        (8)
*  1 console 0    admin         admin -             07/11.10:33 0:00:00
   2 vty 0    admin         user 192.168.1.10      07/11.10:34 0:00:04

# show users all
U No Line      User Name      Class Remote Host      Since      Idle
-----
*  1 console 0    admin         admin -             07/11.10:33 0:00:00
   2 vty 0    admin         user 192.168.1.10      07/11.10:34 0:00:06
   3 vty 1    -             - -             07/11.10:33 0:00:00
   4 vty 2    -             - -             07/11.10:33 0:00:00
   5 ftp 0    -             - -             07/11.10:33 0:00:00
   6 ssh 0    -             - -             07/11.10:33 0:00:00
   7 ssh 1    -             - -             07/11.10:33 0:00:00
   8 ssh 2    -             - -             07/11.10:33 0:00:00
   9 sftp 0    -             - -             07/11.10:33 0:00:00
  10 http 0    -             - -             07/11.10:33 0:00:00
```

1) 使用中ログイン回線マーク

*

本コマンドを実行したログイン回線を示します。

2) ログイン回線番号(通番)

ログイン回線の通し番号を示します。

3) ログイン回線名

ログイン回線名とインタフェース番号を表示します。

console 0

コンソール

vtty 0~2

Telnet

ftp 0

FTP

ssh 0~2

SSH

sftp 0

SFTP

http 0

HTTP または HTTPS

4) ユーザ名

ログインしているユーザ名を表示します。

5) 権限クラス

ログインユーザの権限クラスを表示します。

admin

管理者クラス

user

一般ユーザクラス

6) 接続元ホスト

接続中のホスト名を表示します。

接続だけしてユーザ認証していない場合でも表示されます。

7) ログイン時刻

ログイン時刻を表示します。

8) 無操作時間

ログインしている回線にて最終操作からの経過時間を表示します。

20.2 ログインユーザの状態などのクリア

20.2.1 clear line

[機能]

ログイン回線の強制切断

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
clear line <lines_number>
clear line <line_name> <interface_number>
```

[オプション]

<lines_number>

show users コマンドで表示される全ログイン回線の通し番号を 10 進数で指定します。

<line_name>

show users コマンドで表示されるログイン回線名を指定します。

<interface_number>

show users コマンドで表示されるログイン名に続くインタフェース番号を 10 進数で指定します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

指定したログイン回線を強制切断し、ユーザがログインしている場合には強制的にログアウトさせます。

[メッセージ]

```
<ERROR> invalid line
```

指定したログイン回線は接続されていないため強制切断できません。

show line users コマンドでログインユーザ情報を表示し、接続中のログイン回線を指定してください。

```
<ERROR> your login line
```

利用者自身のログイン回線のため強制切断できません。

exit コマンドでログアウトすることでログイン回線を切断してください。

[実行例]

```
# clear line vty 0
```

第 21 章 Ethernet のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

21.1 Ethernet のカウンタ・ログ・統計・状態などの表示

21.1.1 show ether

[機能]

Ethernet 物理ポートの情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show ether [line <line>]

[オプション]

なし

すべての情報を表示します。

line <line>

指定されたポート上の情報を表示します。

また、該当するポート番号が無効の場合は情報は表示されません。

範囲	機種
1~2	SR-M630AP1
1	SR-M610AP1

複数のポート番号を指定する場合、","(カンマ)で区切ります。

複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-2")。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

Ethernet ポートの情報を表示します。

line オプションを指定した場合は、対象ポートの情報が表示されます。

[実行例]

```
# show ether line 1-2

[ETHER PORT-1]
status      : auto 1000M Full MDI-X      ---(1)
media       : Metal                      ---(2)
flow control : send on, receive on      ---(3)
type        : Normal                    ---(4)
since       : Oct  2 17:31:26 2005      ---(5)
config      : mode(auto), mdi(auto)     ---(6)
linkcontrol  : downrelay(-)             ---(7)
[ETHER PORT-2]
status      : auto 1000M Full MDI-X
media       : Metal
flow control : send on, receive on
type        : Normal
since       : Oct  2 17:31:26 2005
config      : mode(auto), mdi(auto)
linkcontrol  : downrelay(-)
#
```

-
- 1) ポートの状態
接続完了時の速度、状態が表示されます。
disable
定義により使用しない状態であることを示します。
offline
オフライン状態であることを示します。
down
リンクダウン状態であることを示します。
auto
オートネゴシエーション有効であることを示します。
10M/100M/1000M/2.5G
現在リンクしている ether ポートの通信速度(10Mbps/100Mbps/1000Mbps/2.5Gbps)を示します。
Full/Half
現在リンクしている全二重/半二重の状態を示します。
MDI/MDI-X
現在リンクしている MDI の種別を示します。
 - 2) ether ポートのメディア種別
ether ポートのメディア種別が表示されます。
Metal
10/100/1000/2500BASE-TX ポートを使用していることを示します。
-
リンクアップ状態にないため不定であることを示します。
 - 3) フロー制御状態
フロー制御が送信/受信の順で表示されます。
on
フロー制御が有効であることを示します。
off
フロー制御が無効であることを示します。
-
リンクアップ状態にないため不定であることを示します。
 - 4) ポート種別
ポート種別が表示されます。
Normal
通常ポートとして使用していることを示します。
LinkAggregation
リンクアグリゲーションポートとして使用していることを示します。
所属するリンクアグリゲーショングループ番号も表示されます。
※リンクアップ状態でリンクアグリゲーションが多重化されたリンクとしてリンクアップ状態ではない場合は、"*LinkAggregation"の表示を付与します。
-
未使用ポートまたは定義矛盾により不定であることを示します。
 - 5) 状態遷移時刻
ポートの状態が現在の状態に変化した時刻が表示されます。
 - 6) 設定情報
ether mode, ether mdi コマンド設定値が表示されます。
mode(設定値)
ether mode の設定値を、mode(auto)のように表示します。
mdi(設定値)
ether mdi の設定値を、mdi(auto)のように表示します。
 - 7) リンク制御情報
リンク制御情報が表示されます。
-

downrelay(連携無線 LAN インタフェースリスト)

リンクダウンリレー機能 (リンクインテグリティ) 使用時の連携無線 LAN インタフェース情報が表示されます。

※ リンクダウンリレー機能が未使用の場合は“-”が表示されます。

21.1.2 show ether statistics

[機能]

Ethernet 物理ポートの統計情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show ether statistics [line <line>] [detail]
```

[オプション]

なし

すべての統計情報を表示します。

line <line>

指定されたポート上の統計情報を表示します。

また、該当するポート番号が無効の場合は統計情報は表示しません。

範囲	機種
1～2	SR-M630AP1
1	SR-M610AP1

複数のポート番号を指定する場合、","(カンマ)で区切ります。

複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-2")。

detail

ether ポートの統計情報に詳細情報を追加して表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

Ethernet 物理ポートの統計情報を表示します。

line オプションを指定した場合は、対象ポートの統計情報を表示します。

[注意]

統計情報は、本装置を再起動するとクリアされます。

[実行例]

```
# show ether statistics line 1

[ETHER PORT-1 STATISTICS]
[Input Statistics]
Octets           : 0           ---(1)
Frames           : 0           ---(2)
Discards
  All DiscardsPkts : 0           ---(3)
Errors
  All Errors       : 0           ---(4)

[Output Statistics]
Octets           : 0           ---(5)
Frames           : 0           ---(6)
Discards
  All DiscardsPkts : 0           ---(7)
Errors
  All Errors       : 0           ---(8)
```

- 1) 受信したデータのオクテット数
エラーフレームを含みます。
- 2) 受信した総フレーム数
エラーフレームを含みません。
- 3) 受信した全フレームのうち、廃棄した数
- 4) 受信した全フレームのうち、エラー検出した数
- 5) 全送信オクテット数
- 6) 送信した総フレーム数
エラーフレームを含みません。
- 7) 送信したフレームのうち、廃棄した数
- 8) 送信したフレームのうち、エラー検出した数

detail 指定時の実行例

```
# show ether statistics line 1 detail

[ETHER PORT-1 STATISTICS]
[Input Statistics]
Octets          : 0          ---(1)
Frames          : 0          ---(2)
Unicast        : 0          ---(3)
Multicast      : 0          ---(4)
Broadcast      : 0          ---(5)
Pause frames   : 0          ---(6)

Discards
Resource Full  : 0          ---(7)
Input Discards : 0          ---(8)
Errors
Undersize     : 0          ---(9)
FCSErrors    : 0          ---(10)
AlignmentErrors : 0        ---(11)
FragmentErrors : 0        ---(12)
Jabbers      : 0          ---(13)

[Output Statistics]
Octets          : 0          ---(14)
Frames          : 0          ---(15)
Unicast        : 0          ---(16)
Multicast      : 0          ---(17)
Broadcast      : 0          ---(18)
Pause frames   : 0          ---(19)

Discards
Underflow Discards : 0        ---(20)
Errors
Oversize      : 0          ---(21)
ExcessiveCollisions : 0        ---(22)
LateCollisions : 0          ---(23)

SingleCollisionFrames : 0        ---(24)
MultipleCollisionFrames : 0        ---(25)
DeferredTransmissions : 0          ---(26)

[Input Detail Statistics]
Frame size      frames
   64           : 0          ---(27)
  65-127       : 0          ---(28)
 128-255       : 0          ---(29)
 256-511       : 0          ---(30)
 512-1023      : 0          ---(31)
1024-1522 (Tagged) : 0          ---(32)

[Output Detail Statistics]
Frame size      frames
   64           : 0          ---(33)
  65-127       : 0          ---(34)
 128-255       : 0          ---(35)
 256-511       : 0          ---(36)
 512-1023      : 0          ---(37)
1024-1522 (Tagged) : 0          ---(38)
```

- 1) 受信したデータのオクテット数
エラーフレームを含みます。
- 2) 受信した総フレーム数
エラーフレームを含みません。
- 3) 受信したユニキャストフレーム数
エラーフレームを含みません。
- 4) 受信したマルチキャストフレーム数
エラーフレームを含みません。
- 5) 受信したブロードキャストフレーム数

-
- エラーフレームを含みません。
- 6) 受信したポーズフレーム数
※SR-M630AP1 の ether ポート 1 ではカウントされません。
 - 7) 受信バッファ溢れした数
 - 8) 破棄したフレーム数
 - 9) ショートサイズ(64 バイト未満)フレーム受信数
 - 10) データサイズ 64~1522(タグありなしにかかわらず)バイトで FCS エラーを検出したフレーム数
 - 11) データサイズ 64~1522(タグありなしにかかわらず)バイトでアライメントエラーを検出した受信フレーム数
 - 12) ショートサイズ(64 バイト未満)フレームで FCS エラーを検出したフレーム数
 - 13) オーバサイズ(タグなしでは 1519 バイト以上、タグありでは 1523 バイト以上)のフレーム数
オーバサイズで、FCS エラーの検出有無にかかわらずカウントされます。
 - 14) 全送信オクテット数
 - 15) 送信した総フレーム数
エラーフレームを含みません。
 - 16) 送出したユニキャストフレーム数
エラーフレームは含みません。
 - 17) 送出したマルチキャストフレーム数
エラーフレームは含みません。
 - 18) 送出したブロードキャストフレーム数
エラーフレームは含みません。
 - 19) 送出したポーズフレーム数
 - 20) 送出バッファのアンダーフロー状態により破棄されたフレーム数
 - 21) オーバサイズ(タグなしで 1519 バイト、タグありで 1523 バイト以上)フレーム送信数
 - 22) コリジョン多発によって送信が失敗したフレーム数
 - 23) レイトコリジョン発生回数
 - 24) 1 回のコリジョン発生後、送信が成功したフレーム数
 - 25) 複数回のコリジョン発生後、送信が成功したフレーム数
 - 26) 伝送路ビジーにより送信が遅延したフレーム数
 - 27) 64 バイトのフレームを受信した数
エラーフレームを含みます。
 - 28) 65~127 バイトのフレームを受信した数
エラーフレームを含みます。
 - 29) 128~255 バイトのフレームを受信した数
エラーフレームを含みます。
 - 30) 256~511 バイトのフレームを受信した数
エラーフレームを含みます。
 - 31) 512~1023 バイトのフレームを受信した数
エラーフレームを含みます。
 - 32) 1024~1522 バイトのフレームを受信した数
エラーフレームを含みます。
 - 33) 64 バイトのフレームを送信した数
エラーフレームを含みます。
 - 34) 65~127 バイトのフレームを送信した数
エラーフレームを含みます。
 - 35) 128~255 バイトのフレームを送信した数
エラーフレームを含みます。
 - 36) 256~511 バイトのフレームを送信した数
エラーフレームを含みます。
 - 37) 512~1023 バイトのフレームを送信した数
エラーフレームを含みます。
 - 38) 1024~1522 バイトのフレームを送信した数
-

エラーフレームを含みます。

21.2 Ethernet のカウンタ・ログ・統計などのクリア

21.2.1 clear ether statistics

[機能]

Ethernet 物理ポートの統計情報のクリア

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

clear ether statistics [line <line>]

[オプション]

なし

すべてのポートの統計情報をクリアします。

line <line>

指定されたポート上の統計情報をクリアします。

また、該当するポート番号が無効の場合は統計情報はクリアされません。

範囲	機種
1~2	SR-M630AP1
1	SR-M610AP1

複数のポート番号を指定する場合、","(カンマ)で区切ります。

複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-2")。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

Ethernet 物理ポートの統計情報をクリアします。

line オプションを指定した場合は、対象ポートの統計情報がクリアされます。

[実行例]

```
# clear ether statistics
#
```

第 22 章 LACP のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

22.1 LACP のカウンタ・ログ・統計・状態などの表示

22.1.1 show lacp

[機能]

LACP 情報の表示

[適用機種]

SR-M630AP1

[入力形式]

show lacp

[オプション]

なし

すべての情報を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

LACP 情報を表示します。

[実行例]

```
# show lacp
[group 1]
(1) (2)      (3)      (4)      (5)      (6)
port      mode      state      LAG-ID      port-parameter
-----
1  Actor   : active   ASCD      8000,00-0b-5d-89-02-ba,0002  8000,1
   Partner: active   ASCD      8000,00-0b-5d-89-01-22,0001  8000,1
2  Actor   : active   ASCD      8000,00-0b-5d-89-02-ba,0002  8000,2
   Partner: active   ASCD      8000,00-0b-5d-89-01-22,0001  8000,2
#
```

- 1) ポート番号
- 2) 右側の表示が本装置(Actor)の情報か、相手装置(Partner)の情報であることを示します。
- 3) LACP のモードが active か passive であることを示します。
有効な LACP 相手システムの情報が無い場合は passive が表示されます。
- 4) LACP の状態

T (LACP_Timeout)

LACPDU の受信タイムアウトが Short Timeout (3 秒) 状態であることを示します。
表示がない場合は Long Timeout (90 秒) 状態です。

A (Aggregation)

集約可能リンクであることを示します。表示がない場合は個別リンクです。

S (Synchronization)

アグリゲータと結合状態であることを示します。

C (Collecting)

フレーム受信可能状態であることを示します。

D (Distributing)

フレーム送信可能状態であることを示します。

d (defaulted)

本装置が保持している LACP 相手システム (Partner) の情報にデフォルトパラメタを適用していることを示します。

E (Expired)

LACP 相手システムの受信部が期限切れ状態であることを示します。

5) リンクアグリゲーション識別子

すべてが 0 である場合は、有効な LACP 相手システムの情報が無い状態です。

(a) (b) (c) (d) (e)
8000, 00-0b-5d-89-02-ba, 0002 8000, 2

a) システムプライオリティ

b) システム ID (MAC アドレス)

c) アグリゲーションキー

d) ポートプライオリティ

e) ポート番号

6) 左側の数字がポートプライオリティを示し、右側がポート番号を示します。

5) の説明にある (d) と (e) に相当します。

第 23 章 無線 LAN モジュールのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

無線 LAN モジュール番号、無線 LAN インタフェースの最大値、無線 LAN インタフェース番号の関係は以下のよう
に定義付けられています。

無線 LAN モジュール番号	無線 LAN インタフェースの最大値	無線 LAN インタフェース番号
ieee80211 1	8	wlan 1 ~ 8
	16	wlan 1 ~ 16
ieee80211 2	8	wlan 9 ~ 16
	16	wlan 17 ~ 32
ieee80211 3	8	wlan 17 ~ 24
	16	wlan 33 ~ 48

23.1 無線 LAN モジュールのカウンタ・ログ・統計・状態などの表示

23.1.1 show ieee80211 statistics

[機能]

無線 LAN モジュール統計情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show ieee80211 statistics [line <ieee80211_number>]
```

[オプション]

なし

すべての無線 LAN モジュールの統計情報を表示します。

line <ieee80211_number>

指定された無線 LAN モジュールの統計情報を表示します。

該当する無線 LAN モジュールが無効の場合は情報は表示されません。

- ・ ieee80211 定義番号

範囲	機種
1～3	SR-M630AP1
1～2	SR-M610AP1

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

無線 LAN モジュールの統計情報を表示します。

[実行例]

```
# show ieee80211 statistics line 1
[ieee80211 1]
tx packets           : 0           ---(1)
tx mgmt              : 7931        ---(2)
tx xretries          : 1233        ---(3)
tx bytes             : 0           ---(4)
rx badmic            : 0           ---(5)
rx packets           : 248         ---(6)
rx snr               : 52          ---(7)
rx bytes             : 2265318     ---(8)
be xmit              : 7987        ---(9)
ampdu tx aggregated  : 0           ---(10)
ampdu tx not aggregated : 0       ---(11)
Radio profile:
rx num data          : 0           ---(12)
rx num ctl           : 0           ---(13)
rx num mgmt          : 11203       ---(14)
noise floor          : -114        ---(15)
background
txq packets          : 0           ---(16)
besteffort
txq packets          : 0
video
txq packets          : 0
voice
txq packets          : 0
PHY stats:
rx phyerr            : 98          ---(17)
```

- 1) tx packets
パケット送信回数
- 2) tx mgmt
管理フレーム送信
- 3) tx xretries
再送が多すぎるため送信失敗
- 4) tx bytes
送信バイト数合計
- 5) rx badmic
不正 MIC のため受信失敗
- 6) rx packets
パケット受信回数
- 7) rx snr
受信フレームの信号強度
- 8) rx bytes
受信バイト数合計
- 9) be xmit
ビーコン送信
- 10) ampdu tx aggregated
集約送信完了
- 11) ampdu tx not aggregated
非集約フレーム送信完了
- 12) rx num data
受信データパケット数
- 13) rx num ctl
受信コントロールパケット数
- 14) rx num mgmt
受信管理パケット数
- 15) noise floor

-
- ノイズフロアー
- 16) txq packets
キュー毎の統計情報
 - 17) rx phyerr
受信した PHY エラー数

23.1.2 show ieee80211 status

[機能]

無線 LAN モジュール状態の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show ieee80211 status [line <ieee80211_number>]
```

[オプション]

なし

すべての無線 LAN モジュールの状態を表示します。

line <ieee80211_number>

指定された無線 LAN モジュールの状態を表示します。

- ・ ieee80211 定義番号

範囲	機種
1～3	SR-M630AP1
1～2	SR-M610AP1

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

無線 LAN モジュールの状態を表示します。

[メッセージ]

```
Waiting for wlan interface active.
```

無線 LAN インタフェース起動中のため、表示処理を続けることができません。

少し時間を置いてから、再度コマンドを実行してください。

[実行例]

```
# show ieee80211 status line 2
[ieee80211 2]
status          : up                      ---(1)
mode            : IEEE802.11a/n/ac        ---(2)
channel         : 48(5240Mhz), 36, 40, 44 ---(3)
antenna        : internal                 ---(4)
sta limit       : 50 stations             ---(5)
sta guarantee   : 3 stations             ---(6)
txpower        : 19 dBm                  ---(7)
protection mode : disable                 ---(8)
rts threshold   : 2346 bytes              ---(9)
dtim period     : 1                      ---(10)
beacon interval : 100(x1.024msec)        ---(11)
air time fairness : enable                ---(12)
WMM Information
wmm mode        : enable                  ---(13)
besteffort cwmin 4 cwmax 6 aifs 3 txopLimit 0 ---(14)
               cwmin 4 cwmax 10 aifs 7 txopLimit 0
background cwmin 4 cwmax 6 aifs 3 txopLimit 0 -ack
               cwmin 4 cwmax 10 aifs 3 txopLimit 0
video          cwmin 3 cwmax 4 aifs 1 txopLimit 94
               cwmin 3 cwmax 4 aifs 2 txopLimit 94
voice          cwmin 2 cwmax 3 aifs 1 txopLimit 47 -ack
               cwmin 2 cwmax 3 aifs 2 txopLimit 47
APSCAN Information
mode           : disable                  ---(15)
expire         : 3600sec                  ---(16)
HTCAPS        :                          ---(17)
RX LDPC
HT20/HT40
Dynamic SM Power Save
RX HT20 SGI
RX HT40 SGI
TX STBC
RX STBC 1-stream
Max AMSDU length: 7935 bytes
DSSS/CCK HT40
VHTCAPS      :                          ---(18)
Max MPDU length: 11454
Supported Channel Width: neither 160 nor 80+80
RX LDPC
TX STBC
SU Beamformer
SU Beamformee
MU Beamformer
RX antenna pattern consistency
TX antenna pattern consistency

# show ieee80211 status line 1
[ieee80211 1]
status          : disable                  ---(1)
```

1) 回線状態

2) 通信モードの情報

3) チャンネルの情報

IEEE802.11n チャンネルボンディング機能で2チャンネルを使用しているとき、チャンネル番号が2個表示されます。

左はプライマリチャンネル、右はセカンダリチャンネルを意味します。

IEEE802.11ac チャンネルボンディング機能で4チャンネルを使用しているとき、チャンネル番号が4個表示されます。

左はプライマリチャンネルを意味します。

4) アンテナの情報

internal

内蔵アンテナを使用

external

外部アンテナを使用

- 5) 接続可能台数
- 6) 最低保証台数
- 7) 無線送信出力の情報
- 8) 11g プロテクションモードの情報
- 9) RTS しきい値
- 10) DTIM 間隔
- 11) ビーコン送信間隔
- 12) エアタイムフェアネスの状態

enable

エアタイムフェアネス有効

disable

エアタイムフェアネス無効

- 13) WMM 優先制御の使用状態
- 14) WMM 優先制御パラメタの情報

-ack

ACK 応答不要

表示なし

ACK 応答必要

- 15) 周辺アクセスポイント検出の動作モード

disable

無効

enable

有効

- 16) 周辺アクセスポイント情報の保持期間 (秒)
- 17) HTCAPS
HT Capabilities Info
- 18) VHTCAPS
VHT Capabilities Info

23.2 周辺アクセスポイント情報の取得、表示

23.2.1 show ieee80211 apscan

[機能]

周辺アクセスポイント情報の収集と表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show ieee80211 apscan [line <ieee80211_number>] all-channel [detail]
show ieee80211 apscan [line <ieee80211_number>] history [detail]
```

[オプション]

line <ieee80211_number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。
省略時は、すべての無線 LAN モジュールを指定したものとみなされます。

all-channel

すべてのチャンネルで周辺アクセスポイント情報を収集し、その結果を表示します。

history

すでに取得済みの周辺アクセスポイント情報を表示します。

detail

周辺アクセスポイント情報を、詳細な形式で表示します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

周辺アクセスポイント情報を表示します。

以下に、周辺アクセスポイント情報の最大表示件数を示します。

項目	値
周辺アクセスポイント情報の最大表示件数	1000 件(無線 LAN モジュールごと)

[注意]

- SSID に 0x21, 0x23~0x7e 以外の文字が挿入されていた場合、当該文字をクエスチオン(?)で表示します。
- 無線 LAN インタフェースがない場合は、周辺アクセスポイント情報を収集することができません。この場合、以下のメッセージを出力します。

```
<ERROR> apscan failed. ieee80211 <number> no wlan interface for apscan.
```

- 周辺アクセスポイント検出機能が無効の場合、以下のメッセージを出力します。

```
<ERROR> apscan failed. ieee80211 <number> is unavailable for apscan.
```

- 現在運用しているチャンネル以外のチャンネルに対して周辺アクセスポイント情報を収集する場合、現在の通信のスループットが低下する場合があります。

[実行例]

```
# show ieee80211 apscan all-channel
[ieee80211 1]
(1)          (2)          (3)          (4) (5) (6)          (7)
BSSID        SSID          Security     CHAN RSSI MODE      Updated
11:12:13:14:15:16 abc1234      WPA2-PSK/WPA3-SAE (AES)  1  -43 11b/g/n/ax 13:46:19
17:18:19:1A:1B:1C def5678      WPA/WPA2-PSK (AES)     6  -52 11b/g/n    13:46:21
1D:1E:1F:20:21:22 ghi9012      WPA2-PSK (AUTO)       11 -39 11b/g     13:46:24
23:24:24:26:27:28 jkl3456      WPA/WPA2-PSK (AES)     9  -65 11b/g/n    13:46:22
Total: 4 APs          ---(8)
[ieee80211 2]
BSSID        SSID          Security     CHAN RSSI MODE      Updated
29:2A:2B:2C:2D:2E mno7890      WPA2-PSK/WPA3-SAE (AES) 36  -54 11a/n/ac/ax 13:46:29
2F:30:31:32:33:34 pqr1234      WPA/WPA2-PSK (AUTO)    40,36 -71 11a/n     13:46:30
35:35:37:38:39:3A stu5678      WPA2-PSK (AES)        52,56,60,64 -93 11a/n/ac 13:46:32
Total: 3 APs

# show ieee80211 apscan all-channel detail
[ieee80211 1]
1. BSSID      : 11:12:13:14:15:16    ---(1)
   SSID       : abc1234            ---(2)
   Updated    : Mar 26 13:46:54 2021 ---(7)
   Security   : WPA2-PSK/WPA3-SAE (AES) ---(3)
     rsn mcastcipher : AES          ---(10)
     ucastcipher  : AES
     keymanagement : PSK+SAE
   CHAN       : 1                  ---(4)
   RSSI       : -43                ---(5)
   MODE       : 11b/g/n/ax         ---(6)
   CHANWIDTH  : 20                 ---(9)
2. BSSID      : 17:18:19:1A:1B:1C
   SSID       : def5678
   Updated    : Mar 26 13:46:54 2021
   Security   : WPA2-PSK (AUTO)
     wpa2 mcastcipher : TKIP
     ucastcipher  : AES+TKIP
   keymanagement : PSK
   CHAN       : 1
   RSSI       : -46
   MODE       : 11b/g/n
   CHANWIDTH  : 20
   .
   .
   .
[ieee80211 2]
1. BSSID      : 29:2A:2B:2C:2D:2E
   SSID       : mno7890
   Updated    : Mar 26 13:47:23 2021
   Security   : WPA2-PSK/WPA3-SAE (AES) ---(3)
     rsn mcastcipher : AES          ---(10)
     ucastcipher  : AES
     keymanagement : PSK+SAE
   CHAN       : 36
   RSSI       : -56
   MODE       : 11b/g/n/ax
   CHANWIDTH  : 20
2. BSSID      : 2F:30:31:32:33:34
   SSID       : pqr1234
   Updated    : Mar 26 13:47:24 2021
   Security   : WPA/WPA2-PSK (AUTO)
     rsn mcastcipher : TKIP
     ucastcipher  : AES+TKIP
     keymanagement : PSK
     wpa mcastcipher : TKIP
     ucastcipher  : AES+TKIP
     keymanagement : PSK
   CHAN       : 40,36
```



```

RSSI           : -70
MODE           : 11a/n
CHANWIDTH     : 40

# show ieee80211 apscan history
[ieee80211 1]
(1)           (2)           (3)           (4) (5) (6)           (7)
BSSID         SSID         Security      CHAN RSSI MODE         Updated
3B:3C:3D:3E:3F:40 vwx9012      WPA/WPA2-PSK (AES)  6  -49 11b/g/n  13:51:45
41:42:43:44:45:46 yza3456      WPA2-PSK/WPA3-SAE (AES) 6  -44 11b/g/n/ax 13:51:45
Total: 2 APs                                     ---(8)
[ieee80211 2]
BSSID         SSID         Security      CHAN RSSI MODE         Updated
47:48:49:4A:4B:4C bcd7890      WPA2-PSK/WPA3-SAE (AES) 64 -65 11a/n/ac/ax 13:48:35
4D:4E:4F:50:51:52 efg1234      WPA/WPA2-PSK (AES)  64 -65 11a/n/ac  13:48:35
53:54:55:56:57:58 hij5678      WPA/WPA2-PSK (AES)  64 -66 11a/n/ac  13:48:35
Total: 3 APs

# show ieee80211 apscan history detail
[ieee80211 1]
1. BSSID      : 3B:3C:3D:3E:3F:40      ---(1)
   SSID       : vwx9012              ---(2)
   Updated    : Mar 26 13:51:52 2021 ---(7)
   Security   : WPA/WPA2-PSK (AES)   ---(3)
     rsn mcastcipher : AES          ---(10)
       ucastcipher  : AES
       keymanagement : PSK
     wpa mcastcipher : AES
       ucastcipher  : AES
       keymanagement : PSK
   CHAN      : 6                    ---(4)
   RSSI      : -49                  ---(5)
   MODE      : 11b/g/n              ---(6)
   CHANWIDTH : 20                   ---(9)
2. BSSID      : 41:42:43:44:45:46
   SSID       : yza3456
   Updated    : Mar 26 13:51:52 2021
   Security   : WPA2-PSK/WPA3-SAE (AES)
     rsn mcastcipher : AES
       ucastcipher  : AES
       keymanagement : PSK+SAE
   CHAN      : 6
   RSSI      : -63
   MODE      : 11b/g/n/ax
   CHANWIDTH : 20
[ieee80211 2]
1. BSSID      : 47:48:49:4A:4B:4C
   SSID       : bcd7890
   Updated    : Mar 26 13:48:43 2021
   Security   : WPA2-PSK/WPA3-SAE (AES)
     rsn mcastcipher : AES
       ucastcipher  : AES
       keymanagement : PSK+SAE
   CHAN      : 64
   RSSI      : -65
   MODE      : 11a/n/ac/ax
   CHANWIDTH : 20
2. BSSID      : 4D:4E:4F:50:51:52
   SSID       : efg1234
   Updated    : Mar 26 13:48:43 2021
   Security   : WPA/WPA2-PSK (AES)
     rsn mcastcipher : AES
       ucastcipher  : AES
       keymanagement : PSK
     wpa mcastcipher : AES
       ucastcipher  : AES
       keymanagement : PSK
   CHAN      : 64
   RSSI      : -65
   MODE      : 11a/n/ac

```

CHANWIDTH : 20

・
・
・

- 1) BSSID
BSSID の情報
- 2) SSID
SSID の情報

detail オプションなし

先頭から 16 文字までを表示します。
17 文字以上ある場合は"... "で表示します。

detail オプションあり

先頭から 40 文字(すべて)を表示します。

- 3) Security
認証・暗号化方式の情報

OPEN(none)

認証・暗号化なし

WEP

WEP 暗号化方式

E-OPEN

エンハンスドオープン認証

WPA、WPA2 および WPA3

以下の認証方式および暗号化方式を組み合わせで表示します。
認証方式で PSK 認証と IEEE802.1X 認証が混在した場合は、文字列の末尾に"?"を表示します。

認証方式	
WPA-PSK	WPA による事前共有キー (PSK) 認証
WPA	WPA による IEEE802.1X 認証
WPA2-PSK	WPA2 による事前共有キー (PSK) 認証
WPA2	WPA2 による IEEE802.1X 認証
WPA/WPA2-PSK	WPA または WPA2 による事前共有キー (PSK) 認証
WPA/WPA2	WPA または WPA2 による IEEE802.1X 認証
WPA3	WPA3 による IEEE802.1X 認証
WPA3-SAE	WPA3-SAE 認証
WPA2-PSK/WPA3-SAE	WPA2-PSK 認証または WPA3-SAE 認証
WPA2/WPA3	WPA2 または WPA3 による IEEE802.1X 認証

暗号化方式	
TKIP	TKIP 暗号化方式
AES	AES 暗号化方式
AUTO	自動判別
192BIT	192bit 暗号化方式 (WPA3 のみ)
Unknown	不明な認証・暗号化方式 上記に該当しない場合に表示します。

- 4) CHAN
チャンネル情報
IEEE802.11n、IEEE802.11ac または IEEE802.11ax のチャンネルボンディング機能を使用した場合、チャンネル番号が 2 個表示されます。
左側チャンネルはプライマリチャンネル、右側チャンネルはセカンダリチャンネルを意味します。
IEEE802.11ac または IEEE802.11ax のチャンネルボンディング機能で 4 チャンネルを使用しているとき、チャンネル番号が 4 個表示されます。

IEEE802.11ax のチャンネルボンディング機能で 8 チャンネルを使用しているとき、チャンネル番号が 8 個表示されます。

5) RSSI

受信信号強度 (dBm)

6) MODE

通信モード情報

11b

IEEE802.11b で動作

11b/g

IEEE802.11b/g で動作

11b/g/n

IEEE802.11b/g/n で動作

11b/g/n/ax

IEEE802.11b/g/n/ax で動作

11g

IEEE802.11g で動作

11g/n

IEEE802.11g/n で動作

11a

IEEE802.11a で動作

11a/n

IEEE802.11a/n で動作

11a/n/ac

IEEE802.11a/n/ac で動作

11a/n/ac/ax

IEEE802.11a/n/ac/ax で動作

7) Updated

最終更新時刻

8) Total

無線 LAN アクセスポイントの検出数

9) CHANWIDTH

無線 LAN アクセスポイントの運用帯域幅

20

20MHz 幅

40

40MHz 幅

80

80MHz 幅

160

160MHz 幅

10) WPA、WPA2 および WPA3 の詳細表示

rsn

無線 LAN アクセスポイントから受信した RSN information 情報を表示します。

wpa

無線 LAN アクセスポイントから受信した WPA information 情報を表示します。

mcastcipher

マルチキャストメッセージの暗号化方式

ucastcipher

ユニキャストメッセージの暗号化方式

以下の暗号化方式を表示します。

複数の暗号化方式をサポートしている場合は、暗号化方式を連結して表示します。

暗号化方式	
TKIP	TKIP 暗号化方式
AES	AES 暗号化方式
Unknown	不明な暗号化方式

keymanagement

認証方式

以下の認証方式を表示します。

複数の認証方式をサポートしている場合は、認証方式を連結して表示します。

認証方式	
PSK	事前共有キー (PSK) 認証
SAE	WPA3-SAE 認証
1X ※	IEEE802.1X 認証
Unknown	不明な認証方式

※ WPA2-1X, WPA3-1X, WPA3-1X(192bit)において複数をサポートする場合、2番目以降は「1X(XX-XX-XX-XX)」(「XX-XX-XX-XX」はAKM Suite)を表示する。

第 24 章 無線 LAN インタフェースのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

無線 LAN モジュール番号、無線 LAN インタフェースの最大値、無線 LAN インタフェース番号の関係は以下のよう
に定義付けられています。

無線 LAN モジュール番号	無線 LAN インタフェースの最大値	無線 LAN インタフェース番号
ieee80211 1	8	wlan 1 ~ 8
	16	wlan 1 ~ 16
ieee80211 2	8	wlan 9 ~ 16
	16	wlan 17 ~ 32
ieee80211 3	8	wlan 17 ~ 24
	16	wlan 33 ~ 48

24.1 無線 LAN インタフェースのカウンタ・ログ・統計・状態などの表示

24.1.1 show wlan sta

[機能]

無線 LAN インタフェースの STA 情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show wlan sta [number <wlan_number>] [detail]
```

[オプション]

なし

すべての無線 LAN インタフェースの STA(無線 LAN 端末)情報を表示します。

number <wlan_number>

- wlan 定義番号

指定された無線 LAN インタフェースの STA(無線 LAN 端末)情報を表示します。

また、該当する無線 LAN インタフェースが無効の場合は情報は表示されません。

範囲	機種
1～48	SR-M630AP1
1～32	SR-M610AP1

detail

詳細な STA(無線 LAN 端末)情報を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

接続している STA(無線 LAN 端末)情報を表示します。

[メッセージ]

構成定義の無線インタフェース数情報が 8 の場合、SR-M630AP1 では number 25 以降、SR-M610AP1 では number 17 以降を指定することができません。この場合、以下のメッセージを出力します。

```
<ERROR> invalid interface number because of wlan-conf wlan-num 8.
```

```
Waiting for wlan interface active.
```

無線 LAN インタフェース起動中のため、表示処理を続けることができません。

少し時間を置いてから、再度コマンドを実行してください。

[実行例]

```
# show wlan sta
[wlan 1]
Mode: 11g Channel: 1 Total: 1 stations(11b:0 11b/g:0 11b/g/n:0 11g:1 11g/n:0 11b/g/n/ax:0 11g/n/ax:0 11a:0
(1) (2) (3)
11a/n:0 11a/n/ac:0 11a/n/ac/ax:0)
MAC Address      AID  Mode Rate SNR  Security      AUTH  VID  IDLE    BW  IP Address
(4) (5) (6) (7) (8) (9) (10) (11) (12) (13) (14)
00:16:e3:00:00:01  1  11g  48M  57  WPA2-PSK(AES)  ok   3   10    20  192.168.100.100

[wlan 9]
Mode: 11a/n Channel: 36,40 Total: 1 stations(11b:0 11b/g:0 11b/g/n:0 11g:0 11g/n:0 11b/g/n/ax:0 11g/n/ax:0 11a:0 11a/n:1
11a/n/ac:0 11a/n/ac/ax:0)
MAC Address      AID  Mode Rate RSSI Security      AUTH  VID  IDLE    BW  IP Address
00:16:e3:00:00:03  2  11a/n 300M  57  WPA2-PSK(AES)  ok   5   6    40  192.168.101.101

Total:2 stations(11b:0 11b/g:0 11b/g/n:0 11g:1 11g/n:0 11b/g/n/ax:0 11g/n/ax:0 11a:0 11a/n:1 11a/n/ac:0 11a/n/ac/ax:0)
---(15)

# show wlan sta number 9 detail
[wlan 9]
Mode: 11a/n/ac Channel: 36,40 Total: 1 stations(11b:0 11b/g:0 11b/g/n:0 11g:0 11g/n:0 11b/g/n/ax:0 11g/n/ax:0
11a:0 11a/n:1 11a/n/ac:0 11a/n/ac/ax:0)
1. MAC address    : 00:16:e3:00:00:03
   Since          : Oct 24 10:33:17 2020 ---(16)
   AID            : 2
   Mode           : 11a/n
   Rate           : 300M
   SNR            : 57
   Security       : WPA2-PSK(AES)
   AUTH           : ok
   VID            : 5
   IDLE           : 6
   BW             : 40
   WPA            : no ---(17)
   WPA2           : yes ---(18)
   WPA3           : yes ---(19)
   IP Address     : 192.168.101.101
   HTCAPS        : Yes ---(20)
                  (0x9ad)
                  RX LDPC
                  HT20
                  SM Power Save disabled
                  RX HT20 SGI
                  TX STBC
                  RX STBC 1-stream
                  Max AMSDU length: 7935 bytes
                  No DSSS/CCK HT40
VHTCAPS         : Yes ---(21)
                  (0x039179b2)
                  Max MPDU length: 11454
                  Supported Channel Width: neither 160 nor 80+80
                  RX LDPC
                  short GI (80 MHz)
                  TX STBC
                  SU Beamformer
                  SU Beamformee
                  MU Beamformee
#
```

1) 無線 LAN インタフェースの無線通信モード設定

11b

IEEE802.11b で動作

11b/g

IEEE802.11b/g で動作

11b/g/n

IEEE802.11b/g/n で動作

11b/g/n/ax

IEEE802.11b/g/n/ax で動作

11g

IEEE802.11g で動作

11g/n

IEEE802.11g/n で動作

11a

IEEE802.11a で動作

11a/n

IEEE802.11a/n で動作

11a/n/ac

IEEE802.11a/n/ac で動作

11a/n/ac/ax

IEEE802.11a/n/ac/ax で動作

- 2) 無線 LAN インタフェースの無線 LAN チャンネル設定

IEEE802.11n チャンネルボンディング機能で2チャンネルを使用しているとき、チャンネル番号が2個表示されます。

左はプライマリチャンネル、右はセカンダリチャンネルを意味します。

IEEE802.11ac または IEEE802.11ax のチャンネルボンディング機能で4チャンネルを使用しているとき、チャンネル番号が4個表示されます。

左はプライマリチャンネルを意味します。

- 3) 無線 LAN 端末接続数(無線 LAN インタフェース全体)
4) 無線 LAN 端末の MAC アドレス
5) アソシエーション ID
6) 無線 LAN 端末の無線通信モード

11b

IEEE802.11b で動作

11b/g

IEEE802.11g で動作

11b/g/n

IEEE802.11n (2.4GHz 帯域) で動作

11b/g/n/ax

IEEE802.11ax (2.4GHz 帯域) で動作

11g

IEEE802.11g で動作

11g/n

IEEE802.11n (2.4GHz 帯域) で動作

11a

IEEE802.11a で動作

11a/n

IEEE802.11n (5GHz 帯域) で動作

11a/n/ac

IEEE802.11ac (5GHz 帯域) で動作

11a/n/ac/ax

IEEE802.11ax (5GHz 帯域) で動作

- 7) 無線レート (bps)

本装置において直前に行なわれたデータ送信の速度を示します。

※ 無線 LAN の制御で使用するフレーム (EAPOL フレームや NULL データフレーム) もデータ送信の対象となるため、これらのデータ送信が行われた直後の場合、無線レートが低く (5GHz 帯 : 6Mbps、2.4GHz 帯 : 1Mbps) 見える場合があります。

- 8) SNR

表示された値から dBm への変換方法は、以下のとおりとなります。

dBm	機種
(RSSI 表示値) + ノイズフロア	SR-M610AP1、SR-M630AP1

ノイズフロアとは、同じ無線モジュールの show ieee80211 statistics の「noise floor」を指します。

9) 認証・暗号化方式

以下の認証方式および暗号化方式を組み合わせて表示します。

－ WPA、WPA2、WPA3 でない場合

認証方式	
OPEN	IEEE802.11 のオープン認証
SHARED	IEEE802.11 の共通鍵認証
E-OPEN	エンハンストオープン認証

暗号化方式	
none	暗号化なし
WEP64	WEP 64-bit(40-bit)
WEP128	WEP 128-bit(104-bit)

－ WPA、WPA2 の場合

認証方式	
WPA	WPA による IEEE802.1X 認証
WPA-PSK	WPA による事前共有キー (PSK) 認証
WPA2	WPA2 による IEEE802.1X 認証
WPA2-PSK	WPA2 による事前共有キー (PSK) 認証

暗号化方式	
TKIP	TKIP 暗号化方式
AES	AES 暗号化方式

－ WPA3 の場合

認証方式	
WPA3-SAE	WPA3-SAE 認証
WPA3	WPA3 による IEEE802.1X 認証

暗号化方式	
AES	AES 暗号化方式
192BIT	192bit 暗号化方式 (WPA3 のみ)

10) IEEE802.11 の認証状態

11) VID

VLAN ID

tag 付き VLAN ID リストは detail 指定時のみ表示します。detail 指定なしの場合は 't' が表示されます。

12) 無通信時間

無通信時間が表示されます。

STA が省電力モードで動作している場合、STA からの死活監視フレームを受信し、無通信切断時間を超過して表示される場合があります。

13) 帯域幅

無線 LAN 端末とのユニキャスト通信で使用する帯域幅が表示されます。

14) 無線 LAN 端末の IP アドレス

無線 LAN 端末の IP アドレスを学習している場合のみ表示されます。

以下の場合、IP アドレスは表示されません。

- － ProxyARP 機能が無効の場合
- － アクセスポイント内ブリッジ転送 (apbridge) を無効にした場合
- － 無線 LAN 端末として、WDS 子機の接続を表示する場合

15) 無線 LAN 端末接続数 (無線 LAN モジュール全体)

16) 接続時刻

-
- 17) WPA 使用可否
 - 18) WPA2 使用可否
 - 19) WPA3 使用可否
 - 20) 無線 LAN 端末より受信した HT Capability Element 情報を表示
 - 21) 無線 LAN 端末より受信した VHT Capability Element 情報を表示

24.1.2 show wlan statistics

[機能]

無線 LAN インタフェース統計情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show wlan statistics [number <wlan_number>]
```

[オプション]

なし

すべての無線 LAN インタフェースの統計情報を表示します。

number <wlan_number>

- wlan 定義番号
指定された無線 LAN インタフェースの統計情報を表示します。
該当する無線 LAN インタフェースが無効の場合は情報は表示されません。

範囲	機種
1～48	SR-M630AP1
1～32	SR-M610AP1

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

無線 LAN インタフェースの統計情報を表示します。

[メッセージ]

構成定義の無線インタフェース数情報が 8 の場合、SR-M630AP1 では number 25 以降、SR-M610AP1 では number 17 以降を指定することができません。この場合、以下のメッセージを出力します。

```
<ERROR> invalid interface number because of wlan-conf wlan-num 8.
```

```
Waiting for wlan interface active.
```

無線 LAN インタフェース起動中のため、表示処理を続けることができません。
少し時間を置いてから、再度コマンドを実行してください。

[実行例]

```
# show wlan statistics number 1
[wlan 1]
rx ssidmismatch      : 15435          ---(1)
rx assoc bss         : 0              ---(2)
rx assoc badwpaie    : 0              ---(3)
rx deauth            : 0              ---(4)
rx disassoc          : 0              ---(5)
rx action            : 0              ---(6)
Packets Dropped      : 0              ---(7)
Packets Errored      : 0
Rx errors            : 0
Rx Dropped           : 0
Tx failures          : 0
Tx Dropped           : 0
Tx Mgmt Failures     : 0
Host Discard         : 0
Rx MIC Errors        : 0
sta limit over       : 15             ---(8)

**** 80211 unicast stats ****
tx packets           : 0              ---(9)
rx packets           : 0              ---(10)

**** 80211 multicast stats ****
tx packets           : 0
rx packets           : 0
```

- 1) rx ssidmismatch
SSID が不一致のフレーム受信
- 2) rx assoc bss
不正 bssid からのアソシエート受信
- 3) rx assoc badwpaie
不正な WPA IE のアソシエーション受信
- 4) rx deauth
認証が解除された受信
- 5) rx disassoc
ディスアソシエーション受信
- 6) rx action
アクションフレーム受信
- 7) 送信及び受信で破棄されたフレーム
- 8) sta limit over
接続台数制限により接続を拒否した数
- 9) tx packets
正常に送信されたフレーム
- 10) rx packets
正常に受信したフレーム

24.1.3 show wlan status

[機能]

無線 LAN インタフェース状態の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show wlan status [number <wlan_number>]
```

[オプション]

なし

すべての無線 LAN インタフェースの状態を表示します。

number <wlan_number>

- wlan 定義番号
指定された無線 LAN インタフェースの状態を表示します。

範囲	機種
1~48	SR-M630AP1
1~32	SR-M610AP1

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

無線 LAN インタフェースの状態を表示します。

[メッセージ]

構成定義の無線インタフェース数情報が 8 の場合、SR-M630AP1 では number 25 以降、SR-M610AP1 では number 17 以降を指定することができません。この場合、以下のメッセージを出力します。

```
<ERROR> invalid interface number because of wlan-conf wlan-num 8.
```

```
Waiting for wlan interface active.
```

無線 LAN インタフェース起動中のため、表示処理を続けることができません。
少し時間を置いてから、再度コマンドを実行してください。

[実行例]

```
# show wlan status number 9
[wlan 9]
status           : up (RUN)                ---(1)
since            : Oct 27 13:11:38 2020    ---(2)
mac address      : 00:90:cc:c6:d3:81       ---(3)
Mode: 11a/n Channel: 36,40 stations(11b:0 11b/g:0 11b/g/n:0 11g:0 11g/n:0 11b/g/n/ax:0 11g/n/ax:0
(4)             (5)             (6)
11a:0 11a/n:1 11a/n/ac:0 11a/n/ac/ax:0)
type             : AP                      ---(7)
ssid             : samplenet              ---(8)
hide             : disable                 ---(9)
bssid           : 00:90:cc:c6:d3:81       ---(10)
apbridge        : enable                   ---(11)
```

```

sta guarantee      : 3 stations          ---(12)
a-mpdu tx mode    : always              ---(13)
a-mpdu rx size    : 64 kbytes          ---(14)
a-mpdu rx density : no time restriction ---(15)
guard-interval    : auto               ---(16)
auth              : WPA2-PSK           ---(17)
WEP Information
wep mode          : disable            ---(18)
wep send         : key[1]             ---(19)
WPA Information
wpa mode          : enable            ---(20)
wpa cipher        : AES               ---(21)
wpa rekey group   : 10m              ---(22)
wpa rekey gmk     : 1d               ---(23)
wpa mcastcipher   : AES              ---(24)
wpa ucastcipher   : AES              ---(25)

# show wlan status number 10
[wlan 10]
status           : disable            ---(1)
since            : -                  ---(2)
mac address      : -                  ---(3)
# show wlan status number 11
[wlan 11]
status           : offline            ---(1)
since            : Oct 27 14:06:28 2020 ---(2)
mac address      : 00:90:cc:c6:d3:83  ---(3)

```

1) 回線状態

活性化中は以下のどれかが表示されます。

SCAN

スキャン中 (WDS-STA 使用時のみ)

RUN

動作中

非活性化状態では以下が表示されます。非活性化中は、4)以降の内容は表示されません。

— disable

閉塞中は以下のどれかが表示されます。閉塞中は、4)以降の内容は表示されません。

offline

offline コマンドによる閉塞中

offline (downrelay)

リンクインテグリティ(リンクダウンリレー)による閉塞中

offline (icmpwatch)

ノード監視(ICMP での監視)による閉塞状態

offline (dot1x backup)

認証自動切替機能による閉塞中

2) 回線状態の更新時間

3) MAC アドレス

4) 無線 LAN インタフェースの無線通信モード設定

11b

IEEE802.11b で動作

11b/g

IEEE802.11b/g で動作

11b/g/n

IEEE802.11b/g/n で動作

11b/g/n/ax

IEEE802.11b/g/n/ax で動作

11g

IEEE802.11g で動作

11g/n

IEEE802.11g/n で動作

11a

IEEE802.11a で動作

11a/n

IEEE802.11a/n で動作

11a/n/ac

IEEE802.11a/n/ac で動作

11a/n/ac/ax

IEEE802.11a/n/ac/ax で動作

- 5) 無線 LAN インタフェースの無線 LAN チャンネル設定

IEEE802.11n チャンネルボンディング機能で2チャンネルを使用しているとき、チャンネル番号が2個表示されます。

左はプライマリチャンネル、右はセカンダリチャンネルを意味します。

IEEE802.11ac または ieee80211.11ax のチャンネルボンディング機能で4チャンネルを使用しているとき、チャンネル番号が4個表示されます。

左はプライマリチャンネルを意味します。

- 6) 無線 LAN 端末接続数(無線 LAN インタフェース全体)

- 7) 動作タイプ

AP

無線 LAN アクセスポイント

AP-DISASTER

災害用無線 LAN アクセスポイント

WDS-AP

WDS 親機

WDS-STA

WDS 子機

- 8) SSID

- 9) SSID 非通知と ANY 接続拒否の情報

- 10) BSSID の情報

無線 LAN アクセスポイントの BSSID が表示されます。

WDS 子機の場合、WDS 親機の BSSID が表示されます。ただし、WDS 親機が見つからない場合 (スキャン中) は Not-Associated が表示されます。

- 11) アクセスポイント内ブリッジ転送動作

- 12) 最低保証台数

- 13) A-MPDU 送信モード

- 14) A-MPDU 最大受信サイズ

- 15) A-MPDU 間隔

- 16) ガードインターバル

11n、11ac、11ax で動作する場合のガードインターバルが表示されます。

auto

400 ナノ秒または 800 ナノ秒

long

800 ナノ秒

- 17) 認証方式の情報

OPEN

IEEE802.11 のオープン認証

SHARED

IEEE802.11 の共通鍵認証

WPA

WPA による IEEE802.1X 認証

WPA-PSK

WPA による事前共有キー (PSK) 認証

WPA2

WPA2 による IEEE802.1X 認証

WPA2-PSK

WPA2 による事前共有キー (PSK) 認証

WPA/WPA2

WPA または WPA2 による IEEE802.1X 認証

WPA/WPA2-PSK

WPA または WPA2 による事前共有キー (PSK) 認証

WPA3-SAE

WPA3-SAE 認証

WPA3

WPA3 による IEEE802.1X 認証

WPA2-PSK/WPA3-SAE

WPA2-PSK 認証または WPA3-SAE 認証

WPA2/WPA3

WPA2 または WPA3 による IEEE802.1X 認証

- 18) 動作モードの情報 (括弧内は動作中のキー長を示す)
- 19) 送信キーの情報
- 20) WPA 動作状況
- 21) 暗号化方式

TKIP

TKIP 暗号化方式

AES

AES 暗号化方式

AUTO

TKIP または AES

192BIT

192bit 暗号化方式

UNKNOWN

未設定

- 22) グループキー (GTK) 更新間隔の情報
- 23) グループマスターキー (GMK) 更新間隔の情報
- 24) 暗号化方式 (マルチキャストおよびブロードキャスト)

TKIP

TKIP 暗号化方式

AES

AES 暗号化方式

192BIT

192bit 暗号化方式

UNKNOWN

未設定

- 25) 暗号化方式 (ユニキャスト)

TKIP

TKIP 暗号化方式

AES

AES 暗号化方式

AUTO

TKIP または AES

192BIT

192bit 暗号化方式

UNKNOWN

未設定

24.1.4 show wlan wpa status

[機能]

WPA 状態情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show wlan wpa status [number <wlan_number>]
```

[オプション]

なし

すべての無線 LAN インタフェースの状態を表示します。

number <wlan_number>

- wlan 定義番号
指定された無線 LAN インタフェースの状態を表示します。
該当する無線 LAN インタフェースが無効の場合は情報は表示されません。

範囲	機種
1～48	SR-M630AP1
1～32	SR-M610AP1

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

WPA の動作状況を表示します。

[メッセージ]

構成定義の無線インタフェース数情報が 8 の場合、SR-M630AP1 では number 25 以降、SR-M610AP1 では number 17 以降を指定することができません。

この場合、以下のメッセージを出力します。

```
<ERROR> invalid interface number because of wlan-conf wlan-num 8.
```

```
Station tables are modified. Cannot continue print.
```

STA (無線 LAN 端末) 情報テーブル変更のため、表示処理を続けることができません。

少し時間を置いてから、再度コマンドを実行してください。

```
Waiting for wlan interface active.
```

無線 LAN インタフェース起動中のため、表示処理を続けることができません。

少し時間を置いてから、再度コマンドを実行してください。

[実行例]

IEEE802.1X 認証使用時

```
# show wlan wpa status

[wlan 1]
SSID : SRM-1X ---(1)
current STA number : 2 ---(2)
Last GTK rekey time : Mon Oct 19 21:39:43 2020 ---(3)
Last GMK rekey time : Tue Oct 20 07:29:13 2020 ---(4)

No. User EAP-Type PAE status STA MAC address
(5) (6) (7) (8) (9)
WPA-Type Cipher PTK status Since
(10) (11) (12) (13)
-----
1 user01 TTLS Authenticated 00:00:0e:12:34:56
WPA2 AES Initiation Done Mon Oct 19 19:29:17 2020
2 user02 PEAP Authenticated 00:00:0e:98:76:54
WPA2 AES Initiation Done Mon Oct 20 19:29:23 2020
```

PSK 使用時

```
# show wlan wpa status

[wlan 1]
SSID : SRM-PSK
current STA number : 2
Last GTK rekey time : Mon Oct 19 21:39:43 2020
Last GMK rekey time : Tue Oct 20 07:29:13 2020
MIC failure detection status : normal

No. User EAP-Type PAE status STA MAC address
WPA-Type Cipher PTK status Since
-----
1 - Authenticated 00:00:0e:12:34:56
WPA2 AES Initiation Done -
2 - Authenticated 00:00:0e:98:76:54
WPA2 AES Initiation Done -
```

- 1) SSID
- 2) 現在接続中の STA 数
- 3) 最後に GTK 鍵を更新した時間
- 4) 最後に GMK 鍵を更新した時間
- 5) STA 通番
- 6) IEEE802.1X 認証のユーザ名
- 7) IEEE802.1X 認証時に使用した EAP タイプ
IEEE802.1X 認証を使用しない場合は '-' (ハイフン) が表示されます。
- 8) IEEE802.1X 認証状態
-
IEEE802.1X 未使用
Authenticating
認証中
Authenticated
認証済み
Failure
認証失敗
- 9) STA の MAC アドレス
- 10) 認証タイプ
WPA
WPA 認証

WPA2

WPA2 認証

WPA3

WPA3 認証

E-OPEN

エンハンスドオープン認証

- 11) 暗号モード
- 12) PTK(Pairwise Transit Key)状態変数
- 13) 接続した時間(再認証時は更新されません)

24.1.5 show wlan wpa statistics

[機能]

WPA 統計情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show wlan wpa statistics [number <wlan_number>] [<mode>]
```

[オプション]

なし

すべての無線 LAN インタフェースの統計情報を表示します。

number <wlan_number>

- wlan 定義番号
指定された無線 LAN インタフェースの統計情報を表示します。
該当する無線 LAN インタフェースが無効の場合は情報は表示されません。

範囲	機種
1～48	SR-M630AP1
1～32	SR-M610AP1

<mode>

- 省略時
統計情報を表示します。
- detail
統計情報を詳細表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

WPA の統計情報を表示します。

[メッセージ]

構成定義の無線インタフェース数情報が 8 の場合、SR-M630AP1 では number 25 以降、SR-M610AP1 では number 17 以降を指定することができません。

この場合、以下のメッセージを出力します。

```
<ERROR> invalid interface number because of wlan-conf wlan-num 8.
```

```
Waiting for wlan interface active.
```

無線 LAN インタフェース起動中のため、表示処理を続けることができません。

少し時間を置いてから、再度コマンドを実行してください。

[実行例]

統計情報表示

```
# show wlan wpa statistics

[wlan 1]
current associated STA count      : 4
STA join count                   : 231
STA left count                   : 220
No response for Identity count   : 1
No response for EAPOL-Key count  : 0
PTK negotiation error count     : 1
GTK negotiation error count     : 0
Group rekey count               : 5
GMK rekey count                 : 2
Authentication succeed count    : 21
Authentication failure count    : 2
Unauthorized Association count (PMF) : 0
Deauthentication count          : 217
```

統計情報詳細表示

```
# show wlan wpa statistics detail
[wlan 1]
current associated STA count      : 4          ---(1)
STA join count                   : 231        ---(2)
STA left count                   : 220        ---(3)
No response for Identity count   : 1          ---(4)
No response for EAPOL-Key count  : 0          ---(5)
PTK negotiation error count     : 1          ---(6)
GTK negotiation error count     : 0          ---(7)
Group rekey count               : 5          ---(8)
GMK rekey count                 : 2          ---(9)
Authentication succeed count    : 21        ---(10)
Authentication failure count    : 2          ---(11)
Unauthorized Association count (PMF) : 0        ---(12)
Deauthentication count          : 217        ---(13)
  Unspecified reason              : 0          ---(14)
  Previous authentication no longer valid : 0        ---(15)
  Deauthenticated because sending station is leaving (or has left)
    IBSS or ESS                   : 0          ---(16)
  Disassociated due to inactivity : 0          ---(17)
  Disassociated because AP is unable to handle all currently
    associated stations           : 0          ---(18)
  Class 2 frame received from nonauthenticated station : 0        ---(19)
  Class 3 frame received from nonassociated station : 0        ---(20)
  Disassociated because sending station is leaving(or has left) BSS : 0        ---(21)
  Station requesting (re)association is not authenticated with
    responding station           : 0          ---(22)
  Invalid information element      : 0          ---(23)
  MIC failure                     : 0          ---(24)
  4-Way Handshake timeout         : 1          ---(25)
  Group Key Handshake timeout     : 0          ---(26)
  Information element in 4-Way Handshake different from
    (Re)Association Request/Probe Response/Beacon frame : 0        ---(27)
  Invalid group cipher            : 0          ---(28)
  Invalid pairwise cipher        : 0          ---(29)
  Invalid AKMP                   : 0          ---(30)
  Unsupported RSN information element version : 0        ---(31)
  Invalid RSN information element capabilities : 0        ---(32)
  IEEE 802.1X authentication failed : 0          ---(33)
  Cipher suite(s) is unable to be accepted : 0        ---(34)
```

- 1) 現在接続中の STA 数
- 2) 接続要求を受け付けた回数
- 3) 接続解除を受け付けた回数
- 4) IEEE802.1X 認証で Identity 要求に対する応答を受信できなかった回数
- 5) 鍵交換処理中に相手装置から EAPOL-Key の応答を受信できなかった回数
- 6) PTK(Pairwise Transit Key) 交換中のエラー発生回数
- 7) GTK(Group Temporal Key) 交換中のエラー発生回数
- 8) GTK 更新回数
- 9) GMK(Group Master Key) 更新回数

-
- 10) 認証成功回数
 - 11) 認証失敗回数
 - 12) 不正な (Re) Association Request を受信した回数 (PMF 機能有効時のみ)
 - 13) STA との接続が切断された回数
 - 14) ~34) は切断理由ごとの統計情報
 - 14) その他のエラー回数
 - 15) 事前認証が無効となっていたためにエラーとして扱われた回数
 - 16) IBSS または ESS モードで STA との接続が切断された回数
 - 17) 同期が外れたために切断された回数
 - 18) 装置内で STA の制御ができない状態に陥ったために切断された回数
 - 19) Class 2 のフレームを認証されていない STA から受信した回数
 - 20) Class 3 のフレームを Association されていない STA から受信した回数
 - 21) BSS モードで STA との接続が切断された回数
 - 22) 認証が拒否された STA から Association されたため切断した回数
 - 23) 不当な要求により切断された回数
 - 24) MIC Failure により切断された回数
 - 25) 4-Way Handshake (PTK 鍵交換) 中にタイムアウトが発生したため切断された回数
 - 26) Group Key Handshake (GTK 鍵交換) 中にタイムアウトが発生したため切断された回数
 - 27) 4-Way Handshake で通知された情報が Association 時に通知された情報と異なるため切断された回数
 - 28) Group Cipher が許容できないため切断された回数
 - 29) Pairwise Cipher が許容できないため切断された回数
 - 30) 不当な AKMP (Authentication and Key Management Protocol) が指定されたため切断された回数
 - 31) 未サポート RSN バージョンが指定されたため切断された回数
 - 32) 許容できない RSN Capability により切断された回数
 - 33) IEEE802.1X 認証が失敗したため切断された回数
 - 34) IEEE802.1X 認証方式が利用不可であったため切断された回数

24.2 無線 LAN 接続のカウンタ・ログ・統計などのクリア

24.2.1 clear wlan wpa statistics

[機能]

WPA 統計情報のクリア

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
clear wlan wpa statistics
```

[オプション]

なし

すべての無線 LAN インタフェースの WPA 統計情報をクリアします。

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[注意]

WPA 統計情報をクリアすると IEEE802.1X 認証統計情報も同時にクリアされます。

[説明]

WPA 統計情報をクリアします。

[メッセージ]

```
Waiting for wlan interface active.
```

無線 LAN インタフェース起動中のため、クリア処理を続けることができません。
少し時間を置いてから、再度コマンドを実行してください。

[実行例]

```
# clear wlan wpa statistics  
#
```

第 25 章 バンドステアリング機能の表示コマンド

25.1 バンドステアリング情報の表示

25.1.1 show band-steering status

[機能]

バンドステアリング情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show band-steering status

[オプション]

なし

バンドステアリング情報を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

バンドステアリング情報を表示します。

[実行例]

```
# show band-steering status
Channel 44 : Measured: 99 %* (overloaded)
Channel 5  : Measured: 10 %*
```

(1) (2)

- 1) チャンネル情報
チャンネル番号が表示されます。
- 2) 帯域使用率
帯域使用率が表示されます。

第 26 章 POE のログ・状態などの表示コマンド

26.1 POE のログ・状態などの表示

26.1.1 show poe drawing

[機能]

装置の受電状態の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show poe drawing

[オプション]

なし

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

装置の受電状態を表示します。

[実行例]

```
# show poe drawing

[Power Drawing]
AC-Adapter      : none          ---(1)
Ethernet Port 1 : drawing       ---(2)

#
```

1) AC アダプターの状態

AC アダプターの受電状態が表示されます。

none

非受電状態であることを示します。

drawing

受電中状態であることを示します。

2) Ethernet Port 1 の状態

Ethernet Port 1 の状態が表示されます。

none

非受電状態であることを示します。

drawing

受電中状態であることを示します。

第 27 章 USB 接続のカウンタ・ログ・統計・状態などの表示 コマンド

27.1 USB 接続のカウンタ・ログ・統計・状態などの表示

27.1.1 show usb hcd status

[機能]

USB ポートの状態表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show usb hcd status

[オプション]

なし

- ・ USB ポートの状態を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

USB ポートの状態を表示します。

[実行例]

```
# show usb hcd status

[USB HCD STATUS]
status           : enable           --- (1)
```

1) USB ポート状態

USB ポートの状態が表示されます。

disable

安全な取り外し可能状態

enable

使用可能状態

27.1.2 show usb storage status

[機能]

USB マスストレージ制御状態の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show usb storage status [usb]
```

[オプション]

なし

- ・ USB マスストレージ制御状態を表示します。

[usb]

- ・ USB ポートを表示対象とします。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

USB マスストレージ制御の現在の状態を表示します。

[実行例]

```
# show usb storage status

[USB]
Speed                : Full                ---(1)
[Storage specs]
Vendor               : FUJITSU             ---(2)
Product              : USB PortableDrive  ---(3)
Product Rev.         : 3.96                ---(4)
[USB specs]
Speed                : Full                ---(5)
[USB configuration]
Device address       : 1                  ---(6)
Interface            : 0                  ---(7)
Sub class            : 6                  ---(8)
LUN                  : 0                  ---(9)
BulkInEP             : 0x82              ---(10)
BulkOutEP            : 0x02              ---(11)
#
```

1) 速度

以下のどれかが表示されます。

注意:表示は USB デバイスとの通信速度ですが、転送スループットを表すものではありません。

Super

スーパースピードモード(5Gbps)

High

ハイスピードモード(480Mbps)

Full

フルスピードモード(12Mbps)

Low

ロースピードモード(1.5Mbps)

2) ベンダー情報

-
- USB デバイスのベンダー情報が表示されます。
- 3) プロダクト情報
USB デバイスのプロダクト情報が表示されます。
 - 4) プロダクトリビジョン情報
USB デバイスのプロダクトリビジョン情報が表示されます。
 - 5) 速度
USB プロトコル速度が表示されます。(3)と同一です。
 - 6) デバイスアドレス
USB バス上でデバイスを一意に指定するために、USBID によって割り当てられたデバイス番号が表示されます。
 - 7) インタフェース
USB マスストレージ制御スレッドが選択したインタフェースの番号が表示されます。
 - 8) サブクラス
USB デバイスのサブクラス情報が表示されます。クラス情報は、0 (=マスストレージクラス) です。
 - 9) LUN
USB マスストレージ制御スレッドが選択した LUN 番号が表示されます。
 - 10) BulkInEP
USB マスストレージ制御スレッドが選択したバルクインエンドポイント番号が表示されます。
 - 11) BulkOutEP
USB マスストレージ制御スレッドが選択したバルクアウトエンドポイント番号が表示されます。

第 28 章 インタフェースのカウンタ・ログ・統計・状態などの表示コマンド

<interface_name> で指定できる範囲は以下のとおりです。

範囲	機種
lan0～lan19 lo0	SR-M630AP1 SR-M610AP1

28.1 インタフェースのカウンタ・ログ・統計・状態などの表示

28.1.1 show interface

[機能]

インタフェース情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show interface [interface <interface_name>]

[オプション]

なし

lan および lo インタフェースの状態、種別を表示します。

interface <interface_name>

指定したインタフェースの状態、種別を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

インタフェース情報を表示します。

[実行例]

```
# show interface

lan0      Link encap:Ethernet  HWaddr 4A:12:09:99:9F:CF
-(1)-    -----(2)-----  -----(3)-----
        inet addr:192.168.1.31 Bcast:192.168.1.255 Mask:255.255.255.0 (4)
        inet6 addr: fe80::4812:9ff:fe99:9fcf/64 Scope:Link (5)
        UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
        -----(6)-----  ---(7)--  ---(8)--
        RX packets:4 errors:0 dropped:0 overruns:0 frame:0 (9)
        TX packets:7 errors:0 dropped:0 overruns:0 carrier:0 (10)
        collisions:0 txqueuelen:1000
        ----(11)----  ----(12)-----
        RX bytes:804 (804.0 B)  TX bytes:738 (738.0 B)
        -----(13)-----  -----(14)-----

lan1      Link encap:Ethernet  HWaddr D2:1B:6B:D0:1F:9F
        inet addr:192.168.2.31 Bcast:192.168.2.255 Mask:255.255.255.0
        inet6 addr: fe80::d01b:6bff:fed0:1f9f/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:110 (110.0 B)

lo        Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536 Metric:1
        RX packets:100 errors:0 dropped:0 overruns:0 frame:0
        TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:7888 (7.7 KiB)  TX bytes:7888 (7.7 KiB)
```

-
- 1) インタフェース名
 - 2) インタフェースタイプが以下の文字列で表示されます。

Ethernet

Ethernet タイプ

Local Loopback タイプ

Local Loopback

- 3) MAC アドレスが表示されます。
- 4) インタフェースの IPv4 アドレスが表示されます。
- 5) インタフェースの IPv6 アドレスが表示されます。
- 6) インタフェースフラグ
インタフェースフラグが以下の文字列で表示されます。

UP

動作中である。

BROADCAST

有効なブロードキャストアドレスが設定されている。

LOOPBACK

ループバックである。

POINTOPOINT

point-to-point リンクである。

RUNNING

システムリソースが割り当てられている。

PROMISC

promiscuous モードで動作する。

SIMPLEX

自装置が送信したパケットを受信できない。

MULTICAST

マルチキャストをサポートしている。

- 7) MTU サイズ
- 8) Metric 値
- 9) 受信パケット数
- 10) 送信パケット数
- 11) コリジョンパケット数
- 12) 送信キューサイズ
- 13) 受信バイト
- 14) 送信バイト

第 29 章 ARP エントリの表示、クリア操作コマンド

29.1 ARP エントリの表示

29.1.1 show arp

[機能]

ARP エントリの表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show arp [<ip_address>]
show arp summary
```

[オプション]

なし

すべての ARP エントリを詳細表示します。

<ip_address>

指定した IP アドレスの ARP エントリのみ表示します。

summary

ARP エントリ数を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

ARP テーブルのエントリを表示します。

[実行例]

```
# show arp
(1)          (2)          (3) (4)
IP Address  MAC Address      F  Interface
-----
20.0.0.1    00:00:e2:08:57:89    lan0
20.0.0.2    (incomplete)        lan0
20.0.0.255  00:00:02:01:14:00 P  lan0
Entry:3     (5)

# show arp summary
Entry:3     (5)

# show arp 20.0.0.1
IP Address  MAC Address      F  Interface
-----
20.0.0.1    00:00:e2:08:57:89    lan0
Entry:1
#
```

- 1) IP Address
ARP エントリの IP アドレスが表示されます。
- 2) MAC Address
ARP エントリの MAC アドレスが表示されます。
未解決の場合は(incomplete)が表示されます。
- 3) F
エントリ種別が表示されます。詳細を以下に示します。

P

permanent エントリ

4) Interface

ARP エントリのインタフェースが表示されます。

5) Entry

ARP エントリのエントリ数が表示されます。

29.2 ARP エントリのクリア

29.2.1 clear arp

[機能]

ARP エントリのクリア

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

clear arp [<ip_address>]

[オプション]

なし

すべての ARP エントリをクリアします。

<ip_address>

指定した IP アドレスの ARP エントリをクリアします。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

ARP テーブルからエントリをクリアします。

[実行例]

```
# clear arp
#
```

第 30 章 ルーティングテーブル情報・統計などの表示コマンド

30.1 IPv4 ルーティングテーブル情報・統計などの表示

30.1.1 show ip route

[機能]

ルーティングテーブル情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show ip route

[オプション]

なし

ルーティングテーブルに登録した経路情報を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

経路共通管理部に登録している経路情報を表示します。

[実行例]

すべての経路情報を表示する場合

```
# show ip route
Kernel IP routing table
(1)      (2)      (3)      (4)      (5)      (6)
Destination  Gateway    Genmask   Flags    Distance  Iface
default      192.168.1.100  0.0.0.0   UG              1    lan0
192.168.1.0  *          255.255.255.0  U              1    lan0
192.168.1.100 *          255.255.255.255 UH              1    lan0
```

- 1) Destination
あて先アドレスが表示されます。
- 2) Gateway
ゲートウェイアドレスが表示されます。
- 3) Genmask
対象ネットワークのネットマスクが表示されます。
- 4) Flags
ルーティングのフラグ。
U
ルーティングが有効であることを示します。
H
ホストのルーティングであることを示します。
G
ゲートウェイのルーティングであることを示します。
R
回復される動的なルーティングであることを示します。
D
デーモンなどにより書き換えられるルーティングであることを示します。

M

ルーティング・デーモンなどによって書き換えられるルーティングであることを示します。

C

キャッシュのエントリであることを示します。

- 5) Distance
経路優先度が表示されます。
- 6) Iface
出力インタフェース名が表示されます。

第 31 章 パケットの統計情報の表示、クリア操作コマンド

31.1 パケットの統計情報の表示

31.1.1 show ip traffic

[機能]

IP 関連の統計情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show ip traffic

[オプション]

なし

すべての IP 統計情報を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

IP 関連の統計情報を表示します。

[実行例]

```
# show ip traffic
Ip:
  4662 total packets received
  0 with invalid headers
  0 with invalid addresses
  0 forwarded
  0 with unknown protocol
  0 incoming packets discarded
  2184 incoming packets delivered
  1814 requests sent out
  0 outgoing packets dropped
  0 dropped because of missing route
  0 fragments dropped after timeout
  0 reassemblies required
  0 packets reassembled ok
  0 packet reassemblies failed
  0 fragments received ok
  0 fragments failed
  0 fragments created
Icmp:
  1 ICMP messages received
  0 input ICMP message failed
  0 bad checksums received
  ICMP input histogram:
    destination unreachable: 1
    timeout in transit: 0
    wrong parameters: 0
    source quenches: 0
    redirects: 0
    echo requests: 0
    echo replies: 0
    timestamp request: 0
    timestamp reply: 0
    address mask request: 0
    address mask replies: 0
```

```
1 ICMP messages sent
0 ICMP messages failed
ICMP output histogram:
  destination unreachable: 1
  time exceeded: 0
  wrong parameters: 0
  source quench: 0
  redirect: 0
  echo requests: 0
  echo replies: 0
  timestamp requests: 0
  timestamp replies: 0
  address mask requests: 0
  address mask replies: 0
Tcp:
  0 active connection openings
  0 passive connection openings
  0 failed connection attempts
  0 connection resets received
  0 connections established
  0 segments received
  0 segments sent out
  0 segments retransmitted
  0 bad segments received
  0 resets sent
  0 bad checksums received
Udp:
  1812 packets received
  1 packets to unknown port received
  0 packet receive errors
  1813 packets sent
  0 receive buffer errors
  0 send buffer errors
  0 bad checksums received
  370 ignored multicast received
#
```

第 32 章 DHCP のカウンタ・ログ・統計・状態などの表示コマンド

32.1 IPv4 DHCP のカウンタ・ログ・統計・状態などの表示

32.1.1 show ip dhcp

[機能]

IPv4 DHCP 運用状況の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show ip dhcp [interface <interface_name>]
```

[オプション]

なし

すべてのインタフェースの DHCP 運用状況を表示します。

interface <interface_name>

指定したインタフェースについての DHCP 運用状況を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

DHCP の以下の機能の運用状況を表示します。

IPv4 DHCP クライアントの運用状況表示

クライアント状態、リース開始時刻/終了時刻、サーバから獲得したオプション情報を表示します。

また、指定されたインタフェースで IPv4 DHCP クライアントが動作していない場合は何も表示されません。

また、インタフェースの指定がない場合は、すべてのインタフェースの DHCP 情報が表示されます。

[実行例]

IPv4 DHCP クライアントの場合

```
# show ip dhcp

[lan0] IPv4 DHCP Client Informations

Leased IP Address      : 192.168.1.2      --- (1)
Subnet Mask           : 255.255.255.0    --- (2)
Default Router Address : 192.168.1.1      --- (3)
DHCP Server Address   : 192.168.1.1      --- (4)
TIME Server Address   : 192.168.1.X      --- (5)
NTP Server Address    : 192.168.1.X      --- (6)
DNS Server Address    : 192.168.1.1      --- (7)
Domain Name           : fujitsu.com     --- (8)
Lease Time             : 0001.00:00:00    --- (9)
Renewal Time          : 0000.12:00:00    --- (10)
Rebinding Time        : 0000.18:00:00    --- (11)
Lease Expire          : Wed Mar 24 14:00:13 2021 --- (12)
Client Status         : BOUND           --- (13)

#
```

- 1) 獲得 IP アドレス
- 2) 獲得サブネットマスク
- 3) 獲得デフォルトルータアドレス
- 4) 獲得 DHCP サーバアドレス

-
- 5) 獲得タイムサーバアドレス
 - 6) 獲得 NTP サーバアドレス
 - 7) 獲得 DNS サーバアドレス
 - 8) 獲得ドメイン名
 - 9) リース時間
 - 10) リース更新時間 (T1)
 - 11) リース更新時間 (T2)
 - 12) リース有効期限
 - 13) DHCP クライアント状態

第 33 章 ブリッジのカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

33.1 ブリッジのカウンタ・ログ・統計・状態などの表示

33.1.1 show bridge

[機能]

ブリッジに関する状態および統計情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show bridge
show bridge vlan <vid>
show bridge summary
```

[オプション]

なし

学習テーブルの内容を表示します。

vlan <vid>

指定された VLAN で学習された学習テーブルの内容を表示します。

- ・ VLAN ID

VLAN ID を、1~4094 の 10 進数で指定します。

summary

学習テーブルの割り当て状況を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

ブリッジに関する状態、または統計情報を表示します。

[実行例]

学習テーブルの内容を表示する場合

```
# show bridge
Codes: D - Dynamic entry, S - Static entry
(1)          (2) (3)          (4)    (5)
Address      VLAN Interface      Status Remain time
-----
00:0e:00:78:2f:7a 10 ether1          D      164
00:a0:c9:13:f3:37 10 wlan1           D      164
00:a0:c9:f0:20:e9 20 ether2          D      196
00:b0:d0:6f:94:78 20 wlan2           D      196
00:16:01:42:1a:1a 50 wlan3           D      195
00:0c:6e:63:25:77 100 self            S      infinity

#show bridge summary
Registered station blocks :    6    (6)
  Dynamic entry           :    4    (7)
  Static entry            :    1    (8)
  System entry            :    0    (9)
```

- 1) 学習テーブルに登録されている MAC アドレス
- 2) VLAN ID
- 3) エントリされた端末が存在するポート

ether

ether ポート

linkaggregation

リンクアグリゲーションポート

wlan

無線 LAN インタフェース

- 4) 学習テーブルの状態
以下のどれかが表示されます。

D

動的学習テーブル

S

静的学習テーブル

- 5) 残り生存時間(秒)
学習エントリの生存時間が秒数で表示されます。
以下の場合、"infinity"と表示されます。
— 静的エントリ
- 6) 使用中の学習テーブル数
- 7) 動的学習による学習テーブル数
- 8) 静的学習による学習テーブル数
- 9) 装置内部使用による学習テーブル数

33.2 ブリッジのカウンタ・ログ・統計・状態などのクリア

33.2.1 clear bridge

[機能]

動的に学習したテーブルの初期化

[入力形式]

```
clear bridge
clear bridge vlan <vlan_id>
```

[オプション]

なし

動的に学習されているすべての MAC アドレスを学習テーブルから削除します。

vlan <vlan_id>

指定された VLAN で学習されているすべての MAC アドレスを学習テーブルから削除します。

- ・ VLAN ID

VLAN ID を、1~4094 の 10 進数で指定します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

動的に学習されている MAC アドレスを学習テーブルから削除します。

[実行例]

```
# clear bridge
#
```

第 34 章 VLAN のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

34.1 VLAN のカウンタ・ログ・統計・状態などの表示

34.1.1 show vlan

[機能]

VLAN 設定情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show vlan
show vlan summary
show vlan interface
show vlan vid <vlan_id>
```

[オプション]

なし

登録されている VLAN 構成の全 VLAN 情報と VLAN 数を表示します。

summary

登録されている VLAN 構成の VLAN 数のみを表示します。

interface

登録されている VLAN 構成の全 VLAN 情報を表示します。

vid <vlan_id>

VLAN ID で指定された VLAN の構成情報を表示します。

- VLAN ID
1~4094 の 10 進数で指定します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

VLAN の設定情報を表示します。

[実行例]

```
# show vlan
VID Interface Tag Type Description
-----
(1) (2) (3) (4) (5)
100 ether1 dot1q-tagged port v100
wlan15 untagged
wlan16 untagged
200 ether2 dot1q-tagged port v200
wlan3 untagged
wlan5 untagged
Total Count : 2 --- (6)
#
```

- 1) VLAN 番号

2) インタフェース

ether

ether ポート番号

linkaggregation

リンクアグリゲーションポート番号

wlan

無線 LAN インタフェース番号

3) Tag 種別

untagged

Untagged VLAN

dot1q-tagged

Tagged VLAN、または RADIUS サーバから払い出された認証 VLAN

4) VLAN 種別

port

- ポート VLAN

5) VLAN 名

6) VLAN 種別ごとのエントリ数 および VLAN エントリ総数

登録されている VLAN 数のみを表示する場合

```
# show vlan summary
Total Count : 2
#
```

登録されている VLAN 構成のみを表示する場合

```
# show vlan interface
VID Interface Tag Type Description
-----
(1) (2) (3) (4) (5)
100 ether1 dot1q-tagged port v100
wlan15 untagged
wlan16 untagged
200 ether2 dot1q-tagged port v200
wlan3 untagged
wlan5 untagged
#
```

指定 VLAN のみを表示する場合

```
# show vlan vid 100
VID Interface Tag Type Description
-----
(1) (2) (3) (4) (5)
100 ether1 dot1q-tagged port v100
wlan15 untagged
wlan16 untagged
#
```

第 35 章 SSH のカウンタ・ログ・統計・状態などの表示コマンド

35.1 SSH のカウンタ・ログ・統計・状態などの表示

35.1.1 show ssh server key

[機能]

SSH ホスト認証用公開鍵の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show ssh server key {dsa|rsa|ecdsa|ed25519}
```

[オプション]

dsa

本装置の SSH ホスト認証用 DSA 公開鍵を表示します。

rsa

本装置の SSH ホスト認証用 RSA 公開鍵を表示します。

ecdsa

本装置の SSH ホスト認証用 ECDSA 公開鍵を表示します。

ed25519

本装置の SSH ホスト認証用 ED25519 公開鍵を表示します。

[動作モード]

運用管理モード(一般クラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

本装置の SSH ホスト認証用公開鍵を表示します。

SSH プロトコルバージョン 2 (SSH2) のホスト認証で使用されます。

SSH ホスト認証には DSA 公開鍵暗号方式または RSA 公開鍵暗号方式または ECDSA 公開鍵暗号方式または ED25519 公開鍵暗号方式が使用され、どちらの公開鍵を表示するかを指定してください。

あらかじめ ssh クライアントまたは sftp クライアントにホスト認証用公開鍵を設定しておく必要がある場合に、本コマンドで表示された内容を設定してください。

[注意]

serverinfo ssh コマンドで SSH 関連機能をすべて無効にしてある場合は、SSH ホスト認証用公開鍵が生成されていないため、何も表示されません。

ただし、一度有効にしたあとに無効にした場合は、SSH ホスト認証用公開鍵が生成されているため表示されます。

[実行例]

DSA 公開鍵を表示する場合

```
# show ssh server key dsa
ssh-dss AzaCJB5CpVUXI1LXjzNV01kt/LHGhW101eJQDj11tGeeAAAFKoNjMatP
i8JWtZhrglDtxVVmBAIAB3Nc3MAAAAkGfa0nu7HMPdQAAAAIA4sIwVzNfTpxNtjJ
Qx1gJHrDjybKeBMmpnJ/RtGTJfvZW5T/aDc/aoB7PdF+appeXx9U8FsQF+EaMnfq
P31K2u3XAEoAzLa0JQC06VjoDQh15YIzKFo2AVaK41CeS3q81q8A4+jttJODt0UO
rVucQo0q+BdIgaCMDuaqmJQAotGvZvZQ/RMTSh6pMh+z9DdB1DLnPNxEyt61Sftz
Vk+rjgZ29In2V7ai4yu0fIhNL61yb0rrfoZ9YQW4P9rJuDxhvn2xvZQ/RMTSh6pM
6WIwA9m1zAst/YBxb9Jc07uPVhN8M624q8yKsQaMC1W1AAAW00+ZkaqccWLy9GU
xPksjfc+N7022akmykT8V6iMh4+7iAIBJYE6pWpsQU5nFP9rJuDx5R/QV4Q177od
96vNtgwv/hSseRFjyqrGxKewMb11FNjzWSAUyzW0p+GLR/mqBCFavMR14toxEsP3
UDNRpGpFdw== root@localhost --- (1)
#
```

-
- 1) 本装置のホスト認証用 DSA 公開鍵

RSA 公開鍵を表示する場合

```
# show ssh server key rsa
ssh-rsa AA94UAATdVfYAAxsAArx3AAIF7QAsTsTwAEeKogAFAlNoAA0AAAA j3F
AAD3C1yc2EAAAABiWAAAHsMXKAAB+shGQAHDmIABBSpjAARVYAAERAAJZ/IAAAAAB
0AB9QAB+2kSY6AAUAygACvAAB3NzaA7wtAAJ/kAADRQgABwmQAThHAAU0ySgAEJ
JMBAAx4= root@localhost --- (1)
#
```

- 1) 本装置のホスト認証用 RSA 公開鍵

ECDSA 公開鍵を表示する場合

```
# show ssh server key ecdsa
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAy
NTYAAABBBHQ8N8NOLb19V0G5VV5x0ZXYj3FsP643J9CicIOFE1BQPwesGkwUmFFc
wceuHZp2KU7vAMu9DGF2BNK4kszjA18= root@localhost --- (1)
#
```

- 1) 本装置のホスト認証用 ECDSA 公開鍵

ED25519 公開鍵を表示する場合

```
# show ssh server key ed25519
ssh-ed25519 AAAAC3NzaC11ZDI1NTE5AAAAICqFUS7yUVHu4I2zX2+5sjR4d0KY
D69Y+dcqv1k7Pv2z root@localhost --- (1)
#
```

- 1) 本装置のホスト認証用 ED25519 公開鍵

第 36 章 認証機能のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

36.1 IEEE802.1X 認証のカウンタ・ログ・統計・状態などの表示

36.1.1 show dot1x port

[機能]

IEEE802.1X 認証状態の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show dot1x port [<kind> [<portlist>]]
```

[オプション]

なし

すべてのインタフェースに関する IEEE802.1X 認証状態を表示します。

<kind>

ポート種別を指定します。

- wlan
無線 LAN インタフェース

<portlist>

- ポートリスト
認証成功端末を表示するインタフェース番号のリストを指定します。
複数のポート番号を指定する場合、","(カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-8")。
省略時は、すべてのインタフェースを指定したものとみなされます。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

認証機能情報として認証により許容された端末(Supplicant)についてユーザ名、認証方式、認証状態、統計情報を表示します。

[実行例]

```
# show dot1x port

[wlan]
Port  User          EAP-Type  Authentication  OK times  NG times  Status  VLAN
(1)  (2)          (3)      (4)            (5)      (6)      (7)     (8)
          MAC address (9)          Since (10)
-----
 1   user01      TLS       Authenticated   2         2         S4      1
          00:0e:13:25:0f:11 Tue Mar 16 11:30:17 2021
          user02      PEAP      Authenticated   2         2         S4      1
          00:a1:fd:dd:fc:ed Tue Mar 16 13:10:04 2021
 2   admin      TLS       Authenticated   2         0         S4      1
          00:0e:13:8e:55:22 Tue Mar 16 15:32:12 2021
 3   user       PEAP      Authenticated   1         0         S4      1
          00:a0:12:d4:ef:ac Tue Mar 16 18:02:11 2021
 4   -          -         -              0         0         S0      0
          00:00:00:00:00:00 -
```

1) インタフェース番号

-
- 2) ユーザ名
 - 3) 認証方式
 - 4) 認証状態

-

未設定または未接続ポートであることを示します。

Authenticating

認証中

Authenticated

認証済み

Failure

認証失敗

- 5) 認証により許容された回数
- 6) 認証失敗の回数
認証サーバまたは AAA から認証失敗が通知された場合またはユーザに割り当てる VLAN ID の設定に失敗した場合にカウントされます。
- 7) IEEE802.1X 認証の内部状態
 - S0**
認証前の状態
 - S1**
認証処理中の状態
 - S2**
課金開始処理中の状態
 - S3**
通常状態
 - S4**
課金停止処理中の状態
- 8) VLAN ID
- 9) 端末(Supplicant)の MAC アドレス
- 10) 認証に成功した時刻(再認証時は更新されません)

※認証を行っていないインタフェースでは、ユーザ名や認証方式などが“-”で表示されます。

36.1.2 show dot1x statistics port

[機能]

IEEE802.1X 認証統計情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show dot1x statistics port [<kind> [<portlist>]]
```

[オプション]

なし

すべてのインタフェースに関する IEEE802.1X 認証統計情報を表示します。

<kind>

ポート種別を指定します。

- wlan
無線 LAN インタフェース

<portlist>

- ポートリスト
認証成功端末を表示するインタフェース番号のリストを指定します。
複数のポート番号を指定する場合、","(カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-8")。
省略時は、すべてのインタフェースを指定したものとみなされます。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

IEEE802.1X 認証の統計情報を表示します。

[注意]

統計情報は、本装置を再起動するとクリアされます。

[実行例]

```
# show dot1x statistics port
[wlan]
Port 1 statistics:
      EAPOL frame received count : 0          ---(1)
      EAPOL frame sent count : 0             ---(2)
      EAPOL Start frame received count : 0    ---(3)
      EAPOL Logoff frame received count : 0   ---(4)
      EAP Identity Response received count : 0 ---(5)
      EAP response received count : 0        ---(6)
      EAP Identity Request sent count : 1     ---(7)
      EAP request sent count : 0             ---(8)
      Invalid EAPOL frame received count : 0  ---(9)
      EAP with illegal length frame received count : 0 ---(10)
      Version of EAPOL last received frame : 0 ---(11)
      Supplicant address of last received frame : 00:00:00:00:00:00 ---(12)
```

- 1) 受信 EAPOL フレーム数
- 2) 送信 EAPOL フレーム数
- 3) 受信 EAPOL-Start フレーム数

-
- 4) 受信 EAPOL-Logoff フレーム数
 - 5) 受信 EAP Identity response フレーム数
 - 6) EAP Identity 以外の受信 EAP response フレーム数
 - 7) 送信 EAP Identity request フレーム数
 - 8) EAP Identity 以外の送信 EAP request フレーム数
 - 9) 受信した無効な EAPOL フレーム数
 - 10) 受信した不当なパケット長の EAPOL フレーム数
 - 11) 最後に受信した EAPOL フレームのバージョン番号
 - 12) 最後に受信した端末(Supplicant)の MAC アドレス

36.1.3 show dot1x backup port

[機能]

認証自動切替状態の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show dot1x backup port [<kind> [<portlist>]]
```

[オプション]

なし

認証自動切替が有効なすべての無線 LAN インタフェースに対する認証自動切替の状態を表示します。

<kind>

ポート種別を指定します。

- wlan
無線 LAN インタフェース

<portlist>

- ポートリスト
表示するインタフェース番号のリストを指定します。
複数のポート番号を指定する場合、","(カンマ)で区切ります。
複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-8")。
省略時は、すべてのインタフェースを指定したものとみなされます。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

認証自動切替の状態を表示します。

[実行例]

```
# show dot1x backup port
Port  Mode   AAA Group  RADIUS State  Backup Status
(1)  (2)    (3)        (4)    (5)
-----
wlan1 master  0          alive   active
wlan4 backup          dead   standby
wlan3 master  1          dead   standby
wlan2 backup          active
wlan7 backup          active
wlan5 master  0          alive   standby (recovery remain 13s)
wlan6 backup          active
```

- 1) インタフェース名
- 2) 動作モード

master

マスタとして動作

backup

バックアップとして動作

- 3) AAA グループ番号
- 4) AAA グループの状態

alive

RADIUS サーバ動作中

dead

RADIUS サーバ停止中

5) ステータス

active

稼動状態(使用可能)

standby

待機状態(使用不可)

standby (recovery remain xxs)

待機状態(残り xx 秒で自動復旧)

standby (wait recovery command)

待機状態(復旧コマンド待ち)

force down

閉塞状態

36.2 IEEE802.1X 認証のカウンタ・ログ・統計などのクリア

36.2.1 clear dot1x statistics

[機能]

IEEE802.1X 認証統計情報のクリア

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
clear dot1x statistics
```

[オプション]

なし

すべてのポートに関する IEEE802.1X 認証の統計情報をクリアします。

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

IEEE802.1X 認証統計情報をクリアします。

[注意]

IEEE802.1X 認証統計情報をクリアすると WPA 統計情報も同時にクリアされます。

[実行例]

```
# clear dot1x statistics  
#
```

36.3 MAC アドレス認証のカウンタ・ログ・統計・状態などの表示

36.3.1 show macauth port

[機能]

MAC アドレス認証状態の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show macauth port [<kind> [<portlist>]]
```

[オプション]

なし

すべてのインタフェースの MAC アドレス認証状態を表示します。

<kind>

ポート種別を指定します。

- wlan

無線 LAN インタフェース

<portlist>

- ポートリスト

MAC アドレス認証状態を表示するポート番号のリストを指定します。

複数のポート番号を指定する場合、","(カンマ)で区切ります。

複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-8")。

省略時は、すべてのポート番号が指定されたものとみなされます。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証状態を表示します。

[実行例]

```
# show macauth port
[wlan]
Port  Mode  MAC Address          Status  VLAN  Since
-----
(1)  (2)  (3)                (4)    (5)  (6)
1     mac   00:13:21:f6:01:13   success  10   Mar 24 11:20:12 2021
2     mac   00:13:21:f6:02:23   success  20   Mar 24 10:00:22 2021
      mac   00:13:21:f6:02:43   failure  -    Mar 24 10:19:46 2021
10    mac   -                  idle    -    -
      mac   00:13:21:f6:0a:73   failure  -    Mar 24 12:11:00 2021
      mac   00:13:21:f6:0a:74   failure  -    Mar 24 12:11:01 2021
#
```

- 1) ポート番号
- 2) 認証方法(各ポートの先頭行に表示)

mac

MAC アドレスごとの認証を行う

- 3) MAC アドレス
- 4) 認証状態

idle

認証端末が未検出

response

認証結果待ち

success

認証成功

failure

認証失敗または認証制限数超過

- 5) VLAN ID
- 6) 認証開始、認証成功または認証失敗した時刻

36.3.2 show macauth statistics port

[機能]

MAC アドレス認証統計情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show macauth statistics port [<kind> [<portlist>]]
```

[オプション]

なし

すべてのインタフェースの MAC アドレス認証統計情報を表示します。

<kind>

ポート種別を指定します。

- wlan
無線 LAN インタフェース

<portlist>

- ポートリスト

MAC アドレス認証統計情報を表示する物理ポート番号のリストを指定します。

複数のポート番号を指定する場合、","(カンマ)で区切ります。

複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-8")。

省略時は、すべてのポート番号が指定されたものとみなされます。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

MAC アドレス認証の統計情報を表示します。

[実行例]

```
# show macauth statistics port

wlan 1 :
  MAC authentication request  : 8          ---(1)
  MAC authentication success  : 5          ---(2)
  MAC authentication failure  : 2          ---(3)
  MAC authentication logout   : 4          ---(4)
  MAC authentication excess   : 1          ---(5)

#
```

- 1) MAC アドレス認証要求回数
- 2) MAC アドレス認証成功回数
- 3) MAC アドレス認証失敗回数
- 4) MAC アドレス認証ログアウト回数
- 5) MAC アドレス認証未実行回数(認証制限数超過)

36.4 MAC アドレス認証のカウンタ・ログ・統計などのクリア

36.4.1 clear macauth statistics

[機能]

MAC アドレス認証統計情報のクリア

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
clear macauth statistics
```

[オプション]

なし

すべてのインタフェースの MAC アドレス認証統計情報をクリアします。

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

MAC アドレス認証の統計情報をクリアします。

[実行例]

```
# clear macauth statistics  
#
```

第 37 章 AAA のカウンタ・ログ・統計・状態などの表示コマンド

37.1 AAA のカウンタ・ログ・統計・状態などの表示

37.1.1 show aaa radius client server-info

[機能]

RADIUS 機能でのサーバ情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show aaa radius client server-info [group <group_id>]
```

[オプション]

なし

AAA グループすべてのサーバ情報を表示します。

group <group_id>

指定したグループに関するサーバ情報を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

RADIUS サーバの状態を表示します。

[実行例]

```
# show aaa radius client server-info group 0
[aaa group 0]
Type No. Server Address          Port Pri State recover      watch
(1) (2) (3)                      (4) (5) (6) (7)          (8)
Auth  0 192.168.0.101             1812 10 dead 293/300    icmp
Auth  1 192.168.0.100             1812 20 alive -          auth
Acct  0 192.168.0.100             1813  0 alive -          -
```

- 1) サーバの種別

Auth

認証サーバ

Acct

アカウントサーバ

- 2) サーバ定義番号
- 3) サーバ IP アドレス
- 4) サーバポート番号
- 5) 優先度
- 6) サーバの状態

alive

使用可能

dead

応答不能により使用不可

- 7) 復旧残り時間/復旧待機時間

※サーバ状態が使用可能である場合は、“-”が表示されます。

8) 監視種別

icmp

ICMP で監視

auth

認証で監視

off

監視なし

※アカウントングでは監視不可のため、“-”が表示されます。

第 38 章 NETTIME (time/sntp) サーバ、クライアントの統計情報の表示、クリア操作コマンド

38.1 NETTIME(time/sntp)統計情報の表示

38.1.1 show nettime statistics

[機能]

NETTIME(time/sntp)機能での統計情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show nettime statistics [<mode> [<protocol>]]

[オプション]

なし

稼動しているすべての情報を表示します。

<mode>

表示するモードを指定します。

- server
サーバ機能(時刻情報提供側)の情報を表示します。
- client
クライアント機能(時刻情報取得側)の情報を表示します。

<protocol>

表示するプロトコルを指定します。

- time
TIMEプロトコルの情報を表示します。
- sntp
簡易NTPプロトコルの情報を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

NETTIME(time/sntp)の統計情報を表示します。

[注意]

rdateコマンドによる本装置からの時刻取得は、NETTIME(time/sntp)統計情報には含まれません。

[実行例]

以下に、オプションごとの実行例を示します。

<mode> <protocol>

稼動している指定したモードのプロトコルのみ表示します。

```
# show nettime statistics client time
NETTIME client statistics information:
[time tcp]
    0 request transmission error
    0 transmitted synchronized request
    0 received response
    0 received invalid packet
    0 received clock not synchronized
    0 local clock updated
#
```

オプションなし

オプションなしの場合は、本装置で稼動しているすべての NETTIME 情報を表示します。

```
# show nettime statistics
NETTIME server statistics information:
[sntp udp]
    0 received synchronized request          ---(1)
    0 received invalid packet                ---(2)
    0 request discard (clock not synchronized) ---(3)
    0 response transmission error            ---(4)
    0 transmitted response                   ---(5)
[time tcp]
    0 received synchronized request
    0 received invalid packet
    0 request discard (clock not synchronized)
    0 response transmission error
    0 transmitted response
NETTIME client statistics information:
[sntp udp]
    0 request transmission error             ---(6)
    0 transmitted synchronized request       ---(7)
    0 received response                      ---(8)
    0 received invalid packet               ---(9)
    0 received clock not synchronized        ---(10)
    0 local clock updated                   ---(11)
#
```

• server

- 1) 時刻同期要求パケットを受信した総数
- 2) 1)の内時刻同期要求パケットが不正であった総数
- 3) 本装置が時刻同期していないために時刻同期要求を破棄した総数
- 4) 応答送信に失敗した総数
- 5) 応答を送信した総数

• client

- 6) 時刻同期要求パケット送信に失敗した総数
- 7) 時刻同期要求パケットを送信した総数
- 8) サーバからの応答を受信した総数
- 9) 8)の内応答パケットが不正であった総数
- 10) 9)の内サーバ側の時刻が同期していないために応答が無効となった総数
- 11) 応答により本装置の時刻を更新した総数

38.2 NETTIME(time/sntp)統計情報のクリア

38.2.1 clear nettime statistics

[機能]

NETTIME(time/sntp)統計情報のクリア

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
clear nettime statistics [<mode>]
```

[オプション]

なし

すべてのNETTIME(time/sntp)統計情報をクリアします。

<mode>

クリアするモードを指定します。

- server
サーバ機能の統計情報をクリアします。
- client
クライアント機能の統計情報をクリアします。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

NETTIME(time/sntp)の統計情報をクリアします。

[実行例]

```
# clear nettime statistics  
#
```

第 39 章 SNMP 統計情報の表示、クリア操作コマンド

39.1 SNMP 統計情報の表示

39.1.1 show snmp statistics

[機能]

SNMP 機能での統計情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show snmp statistics

[オプション]

なし

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

SNMP の統計情報を表示します。

[実行例]

```
# show snmp statistics
SNMP statistics information:
  0 Input Packets                    ---(1)
  0 Output Packets                   ---(2)
  0 Input Bad Versions                ---(3)
  0 Input Bad Community Names        ---(4)
  0 Input Bad Community Uses         ---(5)
  0 Input ASN Parse Errors           ---(6)
  0 Input Too Bigs                   ---(7)
  0 Input No Such Names              ---(8)
  0 Input Bad Values                 ---(9)
  0 Input Read Only                  ---(10)
  0 Input Gen Errors                 ---(11)
  0 Input Total Request Vars         ---(12)
  0 Input Total Set Vars             ---(13)
  0 Input Get Requests               ---(14)
  0 Input Get Next                   ---(15)
  0 Input Set Requests               ---(16)
  0 Input Get Responses              ---(17)
  0 Input Traps                      ---(18)
  0 Output Too Bigs                  ---(19)
  0 Output No Such Names             ---(20)
  0 Output Bad Values                ---(21)
  0 Output Gen Errors                ---(22)
  0 Output Get Requests              ---(23)
  0 Output Get Next                  ---(24)
  0 Output Set Requests              ---(25)
  0 Output Get Responses             ---(26)
  0 Output Traps                     ---(27)
SNMPv3 statistics information:
  0 Input Unknown Security Mdels     ---(28)
  0 Input Invalid Msgs               ---(29)
  0 Input Unknown PDU Handlers       ---(30)
  0 Input Unsupported SecLevels      ---(31)
  0 Input Not InTimeWindows          ---(32)
  0 Input Unknown User Names         ---(33)
  0 Input Unknown EngineIds         ---(34)
  0 Input Wrong Digests              ---(35)
  0 Input Decryption Errors          ---(36)
#
```

- 1) SNMP 受信メッセージの総数
- 2) SNMP 送信メッセージの総数
- 3) 未サポート SNMP メッセージ受信の総数
- 4) 未使用コミュニティの SNMP 受信メッセージの総数
- 5) コミュニティでは許されていないオペレーションを示す受信メッセージの総数
- 6) ASN.1 エラーの受信メッセージの総数
- 7) エラーステータスが tooBig の受信 PDU の総数
- 8) エラーステータスが noSuchName の受信 PDU の総数
- 9) エラーステータスが badValue の受信 PDU の総数
- 10) エラーステータスが readOnly の受信 PDU の総数
- 11) エラーステータスが genErr の受信 PDU の総数
- 12) MIB の収集が成功した MIB オブジェクトの総数
- 13) MIB の設定が成功した MIB オブジェクトの総数
- 14) 受信した GetRequestPDU の総数
- 15) 受信した GetNextRequestPDU の総数
- 16) 受信した SetRequestPDU の総数
- 17) 受信した GetResponsePDU の総数
- 18) 受信したトラップ PDU の総数
- 19) エラーステータスが tooBig の送信 PDU の総数
- 20) エラーステータスが noSuchName の送信 PDU の総数

-
- 21) エラーステータスが badValue の送信 PDU の総数
 - 22) エラーステータスが genErr の送信 PDU の総数
 - 23) 送信した GetRequestPDU の総数
 - 24) 送信した GetNextRequestPDU の総数
 - 25) 送信した SetRequestPDU の総数
 - 26) 送信した GetResponsePDU の総数
 - 27) 送信したトラップ PDU の総数
 - 28) 未サポートまたは不正な Security Mdels 受信の総数
 - 29) 不正な SNMP メッセージ受信の総数
 - 30) 未サポートまたは不正な PDU Handler 受信の総数
 - 31) 未サポートまたは不正な Security Level 受信の総数
 - 32) TimeWindows 外の SNMP メッセージ受信の総数
 - 33) 不正な User Names 受信の総数
 - 34) 不正な EngineId 受信の総数
 - 35) 認証失敗の総数
 - 36) 暗号失敗の総数

39.2 SNMP 統計などのクリア

39.2.1 clear snmp statistics

[機能]

SNMP 統計情報のクリア

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
clear snmp statistics
```

[オプション]

なし

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

SNMP の統計情報をクリアします。

[実行例]

```
# clear snmp statistics  
#
```

第 40 章 ノード監視機能のカウンタ・ログ・統計・状態などの表示、クリア操作コマンド

40.1 ノード監視機能のカウンタ・ログ・統計・状態などの表示

40.1.1 show icmpwatch

[機能]

ノード監視機能の状態表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show icmpwatch

[オプション]

なし

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

ノード監視機能の各種情報の表示

[実行例]

通常ポート使用時

```
# show icmpwatch
[PORT-1] --- (1)
icmpwatch status      : Normal      --- (2)
destination address   : 192.168.2.1  --- (3)

[PORT-2]
icmpwatch status      : Disable
destination address   : 192.168.2.1
#
```

リンクアグリゲーション使用時 (SR-M630AP1 のみ)

```
# show icmpwatch
[LA GROUP-1] --- (4)
icmpwatch status      : Normal
destination address   : 172.16.1.50
#
```

- 1) ether ポート番号
- 2) 監視状態

Normal

監視が正常に行われていることを示します。

Retry

監視が再送状態であることを示します。

Error

異常を検出したので、監視が正常に行われないことを示します。

Disable

監視機能が無効状態になっていることを示します。

- 3) 監視対象アドレス
- 4) リンクアグリゲーショングループ番号

40.1.2 show icmpwatch statistics

[機能]

ノード監視機能の統計情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show icmpwatch statistics
```

[オプション]

なし

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

ノード監視機能の統計情報を表示します。

ノード監視機能が有効になっている ether ポート、リンクアグリゲーショングループの情報が表示されます。

[実行例]

通常ポート使用時

```
# show icmpwatch statistics
[PORT-1] --- (1)
    20 transmitted icmp echo request packets --- (2)
    0 transmitted icmp echo request packets error --- (3)
    19 received icmp echo reply packets --- (4)
    0 received error --- (5)
    5 retransmitted icmp echo request packets --- (6)
    1 icmpwatch timeout --- (7)

[PORT-2]
    37 transmitted icmp echo request packets
    0 transmitted icmp echo request packets error
    37 received icmp echo reply packets
    0 received error
    0 retransmitted icmp echo request packets
    0 icmpwatch timeout

#
```

リンクアグリゲーション使用時 (SR-M630AP1 のみ)

```
# show icmpwatch statistics
[LA GROUP-1] --- (8)
    14 transmitted icmp echo request packets
    1 transmitted icmp echo request packets error
    14 received icmp echo reply packets
    0 received error
    0 retransmitted icmp echo request packets
    0 icmpwatch timeout

#
```

- 1) ether ポート番号
- 2) ICMP ECHO request 送信数
- 3) ICMP ECHO request 送信エラー数
- 4) ICMP ECHO reply 受信数
- 5) 受信エラー数
- 6) ICMP ECHO パケット再送数

-
- 7) タイムアウトとなった数
 - 8) リンクアグリゲーショングループ番号

40.2 ノード監視機能のカウンタ・ログ・統計・状態などのクリア

40.2.1 clear icmpwatch statistics

[機能]

ノード監視機能の統計情報のクリア

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
clear icmpwatch statistics
```

[オプション]

なし

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

SNMP の統計情報をクリアします。

[実行例]

```
# clear icmpwatch statistics  
#
```

第 41 章 ソケット状態の表示コマンド

41.1 ソケット状態の表示

41.1.1 show socket

[機能]

ソケット状態の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show socket

[オプション]

なし

すべてのソケットの状態を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

アプリケーション層ソフトウェアが利用しているソケットの状態を表示します。

[実行例]

```
# show socket
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
(1)   (2)   (3)   (4)                     (5)                     (6)
tcp    0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:37              0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
udp    0      0 0.0.0.0:123             0.0.0.0:*
udp    0      0 0.127.0.0:514           0.0.0.0:*
udp    0      0 0.0.0.0:8080            0.0.0.0:*
#
```

1) プロトコル

tcp または udp が表示されます。

2) 読み出し待ちデータ量

装置が受信したデータのうち、アプリケーション層ソフトウェアから読み出し待ちとなっているデータ量が表示されます。

3) 送達確認待ちデータ量

アプリケーション層ソフトウェアから送信されたデータのうち、送達確認がとれていないデータ量が表示されます。

4) 自側アドレス. ポート番号

自側アドレスとポート番号が表示されます。指定がない場合は * が表示されます。

5) 相手アドレス. ポート番号

相手アドレスとポート番号が表示されます。未定の場合は * が表示されます。

6) プロトコル内部状態

プロトコルが tcp の場合に、以下のどれかが表示されます。

CLOSED

セッション未確立

CLOSE_WAIT

セッション切断後、アプリケーション層ソフトウェアからの close 処理待ち

CLOSING

アプリケーション層ソフトウェアから close 処理要求され、FIN 交換後の ACK 受信待ち

ESTABLISHED

セッション確立状態

FIN_WAIT_1

FIN 送信後の ACK 受信待ち

FIN_WAIT_2

FIN 受信待ち

LAST_ACK

FIN 交換後の ACK 受信待ち

LISTEN

セッション受け付け可能

SYN_RCVD

SYN-ACK 送信後の ACK 受信待ち

SYN_SENT

SYN 送信後の SYN-ACK 受信待ち

TIME_WAIT

セッション切断後の保持中

第 42 章 端末可視化機能の表示、クリア操作コマンド

42.1 端末可視化機能が検出した端末情報の表示

42.1.1 show devscan

[機能]

端末可視化機能が検出した端末情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show devscan [vlan <vidlist>]
```

[オプション]

なし

端末可視化機能が監視しているすべての VLAN で検出された端末情報を表示します。

vlan <vidlist>

端末情報を表示する VLAN の VID を指定します。

複数の VLAN を指定する場合は、"," (カンマ) で区切って指定します。また、範囲指定する場合は、「1-3」のように"-"(ハイフン)を使用して指定します。

以下に、有効な記述形式を示します。

- ・ vidlist として 1, 2, 3, 5, 7 を指定する場合

(例) 1-3, 5, 7

- ・ vidlist として 1, 3, 5 を指定する場合

(例) 1, 3, 5

指定可能な VLAN ID は最大 16 個です。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

端末可視化機能が検出した端末情報を表示します。

[実行例]

```
# show devscan
[VLAN 1 ADDRESS 192.168.1.91]
(1)          (2)
MAC address  IP address  Port Vendor      Hostname      Description      First detected      Last updated
-----
(3)          (4)          (5)  (6)          (7)          (8)          (9)          (10)
00:23:26:3b:d5:84 192.168.1.42  W1 FUJITSU LIMITED  TULIP        Windows 10      2021-04-03 16:13:45 2021-04-12 09:48:36
8c:73:6e:82:1a:fd 192.168.1.51  W1 FUJITSU LIMITED  ROSE         Windows 7       2021-04-03 20:32:40 2021-04-12 09:48:36
Found 2 devices.  --- (11)
```

- 1) VLAN ID
監視しているセグメントの VLAN ID が表示されます。
- 2) 端末可視化機能が使用する IP アドレス
端末可視化機能が使用する内部パスに割り当てられた IP アドレスが表示されます。
- 3) MAC アドレス
検出した端末の MAC アドレスが表示されます。
- 4) IP アドレス
検出した端末の IP アドレスが表示されます。
- 5) ポート番号
検出した端末が存在する wlan 定義番号が表示されます。

英字、記号は以下を示します。

W

wlan 定義番号

6) ベンダー名

検出した端末のベンダー名が表示されます (最大 18 文字)。

本装置の OUI 辞書に登録されていない OUI の場合、“Unknown”と表示されます。

検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。

7) ホスト名又はコンピュータ名

検出した端末のホスト名、またはコンピュータ名 (NetBIOS 名) が表示されます (最大 16 文字)。

検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。

8) 説明文

検出した端末の OS 名、OS 版数、機種名などの説明文が表示されます (最大 20 文字)。

検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。

9) 最初に検出した日時

端末が最初に検出された日時が表示されます。

10) 最後に検出した日時

端末が最後に検出された日時が表示されます。

11) 検出した端末数

検出した端末数が表示されます。

42.1.2 show devscan mac

[機能]

端末可視化機能が検出した端末情報の MAC アドレス指定による表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show devscan mac <mac>
```

[オプション]

<mac>

MAC アドレス

端末の 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。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

端末可視化機能が検出した端末について、指定の MAC アドレスを持つ端末情報を表示します。

[実行例]

```
# show devscan mac 00:23:26:3b:d5:84
[VLAN 1]                               ----(1)
MAC address      : 00:23:26:3b:d5:84    ----(2)
IP address       : 192.168.1.42         ----(3)
Port             : wlan1               ----(4)
Vendor           : FUJITSU LIMITED     ----(5)
Hostname         : TULIP               ----(6)
Description      : Windows 10         ----(7)
First detected   : 2021-04-03 16:13:45 ----(8)
Last updated     : 2021-04-12 09:48:36 ----(9)
```

- 1) VLAN ID
指定した端末が検出された VLAN の VLAN ID が表示されます。
- 2) MAC アドレス
検出した端末の MAC アドレスが表示されます。
- 3) IP アドレス
検出した端末の IP アドレスが表示されます。
- 4) ポート番号
検出した端末が存在する wlan 定義番号が表示されます。
wlan
wlan 定義番号
- 5) ベンダー名
検出した端末のベンダー名が表示されます (最大 63 文字)。
本装置の OUI 辞書に登録されていない OUI の場合、“Unknown”と表示されます。
検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。
- 6) ホスト名又はコンピュータ名
検出した端末のホスト名、またはコンピュータ名 (NetBIOS 名) が表示されます (最大 32 文字)。
検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。
- 7) 説明文
検出した端末の OS 名、OS 版数、機種名などの説明文が表示されます (最大 63 文字)。

検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。

- 8) 最初に検出した日時
端末が最初に検出された日時が表示されます。
- 9) 最後に検出した日時
端末が最後に検出された日時が表示されます。

42.1.3 show devscan ip

[機能]

端末可視化機能が検出した端末情報の IP アドレス指定による表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show devscan ip <address>
```

[オプション]

<address>

IP アドレス

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

端末可視化機能が検出した端末について、指定の IP アドレスを持つ端末情報を表示します。

[実行例]

```
# show devscan ip 192.168.1.42
[VLAN 1]                               ----(1)
MAC address      : 00:23:26:3b:d5:84    ----(2)
IP address       : 192.168.1.42        ----(3)
Port             : wlan1               ----(4)
Vendor           : FUJITSU LIMITED     ----(5)
Hostname         : TULIP               ----(6)
Description      : Windows 10         ----(7)
First detected   : 2021-04-03 16:13:45 ----(8)
Last updated     : 2021-04-12 09:48:36 ----(9)
```

- 1) VLAN ID
指定した端末が検出された VLAN の VLAN ID が表示されます。
- 2) MAC アドレス
検出した端末の MAC アドレスが表示されます。
- 3) IP アドレス
検出した端末の IP アドレスが表示されます。
- 4) ポート番号
検出した端末が存在する wlan 定義番号が表示されます。
wlan
wlan 定義番号
- 5) ベンダー名
検出した端末のベンダー名が表示されます (最大 63 文字)。
本装置の OUI 辞書に登録されていない OUI の場合、“Unknown”と表示されます。
検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。
- 6) ホスト名又はコンピュータ名
検出した端末のホスト名、またはコンピュータ名 (NetBIOS 名) が表示されます (最大 32 文字)。
検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。
- 7) 説明文
検出した端末の OS 名、OS 版数、機種名などの説明文が表示されます (最大 63 文字)。
検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。

-
- 8) 最初に検出した日時
端末が最初に検出された日時が表示されます。
 - 9) 最後に検出した日時
端末が最後に検出された日時が表示されます。

42.1.4 show devscan hostname

[機能]

端末可視化機能が検出した端末情報のホスト名指定による表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show devscan hostname <hostname>
```

[オプション]

<hostname>

ホスト名

ホスト名を 0x21, 0x23~0x7e の 32 文字以内の ASCII 文字列で指定します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

端末可視化機能が検出した端末について、指定のホスト名を持つ端末情報を表示します。

[実行例]

```
# show devscan hostname TULIP
[VLAN 1]                               ----(1)
MAC address      : 00:23:26:3b:d5:84    ----(2)
IP address       : 192.168.1.42         ----(3)
Port             : wlan1                ----(4)
Vendor           : FUJITSU LIMITED     ----(5)
Hostname         : TULIP                ----(6)
Description      : Windows 10          ----(7)
First detected   : 2021-04-03 16:13:45 ----(8)
Last updated     : 2021-04-12 09:48:36 ----(9)
```

- 1) VLAN ID
指定した端末が検出された VLAN の VLAN ID が表示されます。
- 2) MAC アドレス
検出した端末の MAC アドレスが表示されます。
- 3) IP アドレス
検出した端末の IP アドレスが表示されます。
- 4) ポート番号
検出した端末が存在する wlan 定義番号が表示されます。
wlan
wlan 定義番号
- 5) ベンダー名
検出した端末のベンダー名が表示されます (最大 63 文字)。
本装置の OUI 辞書に登録されていない OUI の場合、“Unknown”と表示されます。
検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。
- 6) ホスト名又はコンピュータ名
検出した端末のホスト名、またはコンピュータ名 (NetBIOS 名) が表示されます (最大 32 文字)。
検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。
- 7) 説明文
検出した端末の OS 名、OS 版数、機種名などの説明文が表示されます (最大 63 文字)。

検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。

- 8) 最初に検出した日時
端末が最初に検出された日時が表示されます。
- 9) 最後に検出した日時
端末が最後に検出された日時が表示されます。

42.1.5 show devscan description

[機能]

端末可視化機能が検出した端末情報の説明文指定による表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show devscan description <description>
```

[オプション]

<description>

説明文

説明文を 0x21, 0x23~0x7e の 63 文字以内の ASCII 文字列で指定します。

(入力可能な文字の一覧については、コマンドユーザーズガイドを参照してください。)

文字列に空白が含まれる場合は、ダブルクォーテーション(")で囲みます。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

端末可視化機能が検出した端末について、Description 欄に本コマンドで指定された文字列を含む端末情報を表示します。

[実行例]

```
# show devscan description Windows
[VLAN 1]                               ----(1)
MAC address      : 00:23:26:3b:d5:84    ----(2)
IP address       : 192.168.1.42         ----(3)
Port             : wlan1               ----(4)
Vendor           : FUJITSU LIMITED     ----(5)
Hostname         : TULIP                ----(6)
Description      : Windows 10          ----(7)
First detected   : 2021-04-03 16:13:45 ----(8)
Last updated     : 2021-04-12 09:48:36 ----(9)

MAC address      : 00:23:26:3b:d5:85
IP address       : 192.168.1.43
Port             : wlan2
Vendor           : FUJITSU LIMITED
Hostname         : TULIP2
Description      : Windows 7
First detected   : 2021-04-03 16:13:45
Last updated     : 2021-04-12 09:48:36
```

- 1) VLAN ID
指定した端末が検出された VLAN の VLAN ID が表示されます。
- 2) MAC アドレス
検出した端末の MAC アドレスが表示されます。
- 3) IP アドレス
検出した端末の IP アドレスが表示されます。
- 4) ポート番号
検出した端末が存在する wlan 定義番号が表示されます。

wlan

wlan 定義番号

5) ベンダー名

検出した端末のベンダー名が表示されます (最大 63 文字)。

本装置の OUI 辞書に登録されていない OUI の場合、“Unknown”と表示されます。

検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。

6) ホスト名又はコンピュータ名

検出した端末のホスト名、またはコンピュータ名 (NetBIOS 名) が表示されます (最大 32 文字)。

検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。

7) 説明文

検出した端末の OS 名、OS 版数、機種名などの説明文が表示されます (最大 63 文字)。

検出した情報に認識できない文字が含まれる場合、“Unrecognized”と表示されます。

8) 最初に検出した日時

端末が最初に検出された日時が表示されます。

9) 最後に検出した日時

端末が最後に検出された日時が表示されます。

42.1.6 show devscan unknown

[機能]

端末可視化機能が識別に失敗した端末情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
show devscan unknown <kind>
```

[オプション]

<kind>

- dhcp
DHCP 解析に失敗した端末情報を表示します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

端末可視化機能が識別に失敗した端末情報を表示します。

[実行例]

```
# show devscan unknown dhcp
MAC address      Information
-----
(1)              (2)
00:23:26:3b:d5:84 1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 121, 249, 252
```

- 1) MAC アドレス
識別に失敗した端末の MAC アドレスが表示されます。
- 2) 端末情報
<kind>で指定した解析手段に必要な情報が表示されます。
<kind>に dhcp を指定した場合、DHCP フィンガープリント (DHCP パラメータ要求リスト オプション 55) 情報が表示されます。

42.2 端末可視化機能が検出した端末情報のクリア

42.2.1 clear devscan

[機能]

端末情報テーブルの初期化

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

clear devscan [vlan <vidlist>]

[オプション]

なし

すべての端末情報をテーブルから削除します。

vlan <vidlist>

端末情報を削除したいVLANのVIDを指定します。

複数のVLANを指定する場合は、","(カンマ)で区切って指定します。また、範囲指定する場合は、「1-3」のように"-"(ハイフン)を使用して指定します。

以下に、有効な記述形式を示します。

- ・ vidlistとして1, 2, 3, 5, 7を指定する場合
(例) 1-3, 5, 7
- ・ vidlistとして1, 3, 5を指定する場合
(例) 1, 3, 5

指定可能なVLAN IDは最大16個です。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

端末可視化機能が検出した端末情報をテーブルから削除します。

[実行例]

```
# clear devscan
#
```

第 43 章 NXconciierge エージェント機能の表示、クリア操作 コマンド

43.1 NXconciierge エージェント機能の表示

43.1.1 show management-agent ca-certificate

[機能]

NXconciierge エージェント機能を使用するルート証明書の有効期限情報を出力します。

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show management-agent ca-certificate

[オプション]

なし

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

端末可視化エンジンのバージョンを表示する。

[実行例]

```
# show management-agent ca-certificate
[Initial Certificate] Jan 28 12:00:00 2028 GMT
#
```

43.1.2 show trace management-agent

[機能]

NXconciierge エージェント機能のトレースの表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show trace management-agent

[オプション]

なし

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

NXconciierge エージェント機能のトレース情報を表示します。

43.2 NXconciierge エージェント情報のクリア

43.2.1 clear trace management-agent

[機能]

NXconciierge エージェント機能のトレース情報の消去

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
clear trace management-agent
```

[オプション]

なし

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

NXconciierge エージェント機能のトレース情報を消去します。

[注意]

NXconciierge エージェント機能のトレース情報は、本装置を再起動するとクリアされます。

第 44 章 DNS サーバ機能の表示コマンド

44.1 DNS サーバ機能の表示

44.1.1 show dns-resolver information

[機能]

DNS リゾルバの DNS サーバ情報の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

show dns-resolver information

[オプション]

なし

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

DNS リゾルバの DNS サーバ情報を表示します。

[実行例]

```
# show dns-resolver information
DNS Server Address : 192.168.1.128
DNS Server Address : 192.168.1.129
```

[注意]

DNS リゾルバに設定が無い場合は、表示されません。
最大で先頭から 3 個までの DNS サーバが使用されます。

第 45 章 ポート制御コマンド

45.1 ポート制御

45.1.1 offline

[機能]

切断、または閉塞の実施

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
offline ether [<port>]
offline wlan [<wlan_number>]
```

[オプション]

ether

すべての ether ポートを閉塞(リンクダウン)します。

ether <port>

指定された ether ポートを閉塞(リンクダウン)します。

複数の ether ポート番号を設定する場合、","(カンマ)で区切ります。

複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-2")。

範囲	機種
1~2	SR-M630AP1
1	SR-M610AP1

wlan

すべての無線 LAN インタフェースを閉塞します。

wlan <wlan_number>

指定された無線 LAN インタフェースを閉塞します。

複数の無線 LAN インタフェース番号を設定する場合、","(カンマ)で区切ります。

複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-8")。

範囲	機種
1~48	SR-M630AP1
1~32	SR-M610AP1

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

切断、または通信閉塞を行います。

[注意]

認証自動切替機能の対象である無線 LAN インタフェースに対して本コマンドが実行された場合、認証自動切替機能の対象であるすべての無線 LAN インタフェースが対象となります。

[実行例]

```
# offline ether 1
closed [1] ---(1)
# offline wlan 8
closed [8] ---(1)
#
```

1) 実行結果

閉塞した場合、以下のメッセージが表示されます。

- closed [<port>]
- closed [<wlan_number>]

すでに閉塞中の ether ポートまたは無線 LAN インタフェースに対して閉塞した場合、以下のメッセージが表示されます。

- <ERROR> already closed [<port>]
- <ERROR> already closed [<wlan_number>]

有効になっていない ether ポートまたは無線 LAN インタフェースに対して閉塞した場合、以下のメッセージが表示されます。

- <ERROR> cannot close [<port>]
- <ERROR> cannot close [<wlan_number>]

45.1.2 online

[機能]

接続、または閉塞解除の実施

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
online ether [<port>]
online wlan [<wlan_number>]
```

[オプション]

ether

すべての ether ポートを閉塞解除します。

ether <port>

指定された ether ポートを閉塞解除します。

複数の ether ポート番号を設定する場合、","(カンマ)で区切ります。

複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-2")。

範囲	機種
1~2	SR-M630AP1
1	SR-M610AP1

wlan

すべての無線 LAN インタフェースを閉塞解除します。

wlan <wlan_number>

指定された無線 LAN インタフェースを閉塞解除します。

複数の無線 LAN インタフェース番号を設定する場合、","(カンマ)で区切ります。

複数の番号が続く場合、"-"(ハイフン)で区切ります(例: "1-8")。

範囲	機種
1~48	SR-M630AP1
1~32	SR-M610AP1

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

接続、または閉塞解除を行います。

[注意]

認証自動切替機能の対象である無線 LAN インタフェースに対して本コマンドが実行された場合、認証自動切替機能の対象であるすべての無線 LAN インタフェースが対象となります。

[実行例]

```
# online ether 1
opened [1]                ---(1)
# online wlan 8
opened [8]                ---(1)
#
```

1) 実行結果

閉塞解除した場合、以下のメッセージが表示されます。

- opened [<port>]
- opened [<wlan_number>]

閉塞中でない ether ポートまたは無線 LAN インタフェースに対して閉塞解除した場合、以下のメッセージが表示されます。

- <ERROR> already opened [<port>]
- <ERROR> already opened [<wlan_number>]

有効になっていない ether ポートまたは無線 LAN インタフェースに対して閉塞解除した場合、以下のメッセージが表示されます。

- <ERROR> cannot open [<port>]
- <ERROR> cannot open [<wlan_number>]

第 46 章 無線 LAN 制御コマンド

46.1 無線 LAN 制御

46.1.1 wlanctl authenticator disconnect

[機能]

無線 LAN 接続端末(STA)の切断

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
wlanctl authenticator disconnect <wlan_number> [<macaddr>]
```

[オプション]

<wlan_number>

指定された無線 LAN インタフェースで接続される端末(STA)に対して処理を行います。
無線 LAN インタフェース番号を指定します。

- wlan 定義番号
無線 LAN インタフェース番号を指定します。
- all
すべての無線 LAN インタフェースを対象とします。

<macaddr>

指定された MAC アドレスを持つ端末(STA)のみに対して処理を行います。
(XX:XX:XX:XX:XX:XX の形式で、XX は 2 桁の 16 進数です。)

省略時は、<wlan_number>で指定された無線 LAN インタフェースに接続されるすべての端末(STA)に対して処理を行います。

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

無線 LAN インタフェースに接続中の無線端末を切断します。

[注意]

本コマンドを連続することにより、一時的に無線 LAN 端末の接続が行えない状態になる場合があります。

[メッセージ]

```
<ERROR> cannot disconnect.
```

以下の場合に表示されます。

- 指定された端末が接続されていない場合

```
cannot disconnect.
```

以下の場合に表示されます。

- 指定された端末が接続されていない場合 (<wlan_number>に all を指定した場合)

```
Waiting for wlan interface active.
```

無線 LAN インタフェース起動中のため、切断処理を続けることができません。
少し時間を置いてから、再度コマンドを実行してください。

[実行例]

```
# wlanctl authenticator disconnect 1 00:00:0e:12:34:56  
#
```

指定された MAC アドレスを持つ端末を、すべての無線 LAN インタフェースで検索し切断する場合

```
# wlanctl authenticator disconnect all 00:00:0e:12:34:56  
#
```

第 47 章 USB ポート制御コマンド

47.1 USB ポート制御

47.1.1 usbctl

[機能]

USB ポートの状態の制御

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

usbctl <mode> [usb]

[オプション]

<mode>

- enable
USB ポートを使用可能な状態にします。
- eject
USB ポートに実装されている USB デバイスを安全に取り外すために実行します。

[usb]

- USB ポートの状態の制御を行います。

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

USB ポートの状態の制御を行います。

USB ポートに実装されている USB デバイスを安全に取り外すために、usbctl eject コマンドを実行します。

また、USB デバイスの取り外し後は、USB デバイスを自動認識します。

usbctl enable コマンドを実行することで、過電流検出で USB ポートが使用不可能な状態の場合に、使用可能な状態にします。過電流検出状態以外で実行した場合は何も行われません。

[注意]

usbctl eject コマンド実行後は、USB デバイスを取り外してください。

[実行例]

```
# usbctl enable  
#
```

第 48 章 IEEE802.1X 制御コマンド

48.1 IEEE802.1X 制御

48.1.1 dot1xctl initialize

[機能]

IEEE802.1X 認証状態の初期化

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
dot1xctl initialize port <kind> <number> [<macaddr>]
```

[オプション]

<kind>

ポート種別を指定します。

- wlan
無線 LAN インタフェース

<number>

指定されたインタフェースの認証状態を変更します。

<macaddr>

指定された MAC アドレスを持つ端末 (Supplicant) の認証状態を変更します。
(XX:XX:XX:XX:XX:XX の形式で、XX は 2 桁の 16 進数です。)

[動作モード]

運用管理モード (管理者クラス)

構成定義モード (管理者クラス)

[説明]

指定されたインタフェースまたは端末 (Supplicant) の認証状態を初期状態に戻します。

[注意]

無線 LAN 端末に対して本コマンドを連続すると、一時的に無線 LAN 端末の接続が行えない状態になる場合があります。

[実行例]

```
# dot1xctl initialize port wlan 1  
#
```

48.1.2 dot1xctl reconfirm

[機能]

IEEE802.1X 再認証の実行

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
dot1xctl reconfirm port <kind> <number> [<macaddr>]
```

[オプション]

<kind>

ポート種別を指定します。

- wlan
無線 LAN インタフェース

<number>

指定されたインタフェースの認証状態を変更します。

<macaddr>

指定された MAC アドレスを持つ端末(Suppliant)の認証状態を変更します。

(XX:XX:XX:XX:XX:XX の形式で、XX は 2 桁の 16 進数です。)

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

指定されたインタフェースまたは端末(Suppliant)の再認証を開始します。

[注意]

本コマンドを連続することにより、ネットワークを不安定にするだけでなく、接続中の端末(Suppliant)が切断されてしまう場合があります。

[実行例]

```
# dot1xctl reconfirm port wlan 1  
#
```

48.1.3 dot1xctl backup recovery

[機能]

認証自動切替状態の復旧

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
dot1xctl backup recovery port <kind> <number>
```

[オプション]

<kind>

ポート種別を指定します。

- wlan
無線 LAN インタフェース

<number>

指定されたインタフェースの認証自動切替状態を復旧させます。

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

指定されたインタフェースの認証自動切替状態を復旧させます。

[注意]

IEEE802.1X 認証を使用する master 指定された無線 LAN インタフェースに対してだけ使用できます。

[実行例]

```
# dot1xctl backup recovery port wlan 1  
#
```

第 49 章 MAC アドレス認証制御コマンド

49.1 MAC アドレス認証制御

49.1.1 macauthctl initialize

[機能]

MAC アドレス認証状態の解除

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
macauthctl initialize port <kind> <number> [<macaddr>]
```

[オプション]

<kind>

ポート種別を指定します。

- wlan
無線 LAN インタフェース

<number>

ポート番号またはインタフェース番号を指定します。

<macaddr>

- MAC アドレス
認証端末の MAC アドレスを指定します。
(XX:XX:XX:XX:XX:XX の形式で、XX は 2 桁の 16 進数です。)

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

指定されたポートまたは端末の認証状態を初期状態に戻します。

[実行例]

```
# macauthctl initialize port wlan 1  
#
```

第 50 章 RADIUS 制御コマンド

50.1 RADIUS 制御

50.1.1 radius recovery

[機能]

RADIUS サーバの復旧

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
radius recovery group <group_id> auth <number>
radius recovery group <group_id> accounting <number>
```

[オプション]

<group_id>

- グループ ID
コマンド適用対象の AAA グループの ID を指定します。

auth <number>

- 認証サーバ定義番号
コマンド適用対象の認証サーバの定義番号を指定します。

accounting <number>

- アカウンティングサーバ定義番号
コマンド適用対象のアカウンティングサーバの定義番号を指定します。

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

dead 状態になった RADIUS サーバとの接続状態を手動で alive 状態に復旧させることができます。なお、RADIUS サーバとの接続状態を復旧させた場合でも、RADIUS サーバとの通信ができない場合は dead 状態になります。

[実行例]

```
# radius recovery group 1 auth 2
#
```

第 51 章 定期ログ制御コマンド

51.1 定期ログ情報 FLASH メモリ格納制御

51.1.1 monitoringinfoctl collect

[機能]

FLASH メモリへの定期ログ情報の格納

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
monitoringinfoctl collect
```

[オプション]

なし

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

FLASH メモリへの定期ログ情報の格納を即時に実行します。

[注意]

格納される定期ログ情報の合計サイズは 720Mbyte までです。

合計サイズが 720Mbyte を超えた場合、古い日付から順に上書きされます。

必要に応じて `clear logging monitoringinfo` コマンドでクリアしてください。

[その他]

FLASH メモリへ格納される定期ログ情報については、「`show logging monitoringinfo`」コマンドを参照してください。

[メッセージ]

```
Succeeded.
```

FLASH メモリへの定期ログ情報の格納が成功しました。

```
<ERROR> cannot write to flash memory.
```

FLASH メモリへの書き込みに失敗しました。

[実行例]

```
# monitoringinfoctl collect
# Succeeded.
```

第 52 章 パケットキャプチャ制御コマンド

52.1 無線 LAN パケットキャプチャ制御コマンド

52.1.1 capturectl start ieee80211

[機能]

無線 LAN パケットキャプチャの開始

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
capturectl start ieee80211 <ieee80211_number>
```

[オプション]

<ieee80211_number>

- 無線 LAN モジュール番号
無線 LAN モジュール番号を、10 進数で指定します。

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

無線 LAN パケットキャプチャの開始を指示します。
本装置～無線端末間の接続・認証シーケンスの packets を装置内のメモリに記録します。
本装置が送受信した管理フレーム(ビーコンを除く)と EAPOL フレームが対象です。
停止コマンドにより、蓄積したパケット情報を pcap 形式でファイルに出力します。

[メッセージ]

```
Start capture failed. ieee80211 <number> is in use.
```

無線モジュールでキャプチャ機能を使用中のため、キャプチャの開始ができません。
動作中のキャプチャを停止してから、再度コマンドを実行してください。

```
Start capture failed. ieee80211 <number> is unavailable.
```

指定した無線 LAN モジュールが無効のため、キャプチャの開始ができません。

[注意]

キャプチャデータは、最大サイズを超えるパケットを受信した場合、古い情報を上書きして記録します。

[実行例]

```
# capturectl start ieee80211 1  
#
```

52.1.2 capturectl stop ieee80211

[機能]

無線 LAN パケットキャプチャの停止

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
capturectl stop ieee80211
```

[オプション]

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

無線 LAN パケットキャプチャの停止を指示します。
停止コマンドにより、蓄積したパケット情報を pcap 形式でファイルに出力します。
生成されるファイル名は固定名 (ieee80211.pcap) で生成され、ファイルの最大サイズは以下のとおりです。

最大サイズ	機種
50M バイト	SR-M630AP1
25M バイト	SR-M610AP1

このファイルは、ftp/sftp get および copy コマンドでの取得ができます。

[注意]

キャプチャファイルに記録されるパケットデータは時刻順で記録されない場合があります。
キャプチャ解析アプリのソート機能を利用して参照してください。

[実行例]

```
# capturectl stop ieee80211  
#
```

52.1.3 capturectl remove ieee80211

[機能]

無線 LAN パケットキャプチャファイルの削除

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
capturectl remove ieee80211
```

[オプション]

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

無線キャプチャファイル(ieee80211.pcap)を削除する。

[メッセージ]

```
Remove capture failed. ieee80211 <number> is in use.
```

無線モジュールでキャプチャ機能を使用中のため、キャプチャファイルの削除できません。
動作中のキャプチャを停止してから、再度コマンドを実行してください。

[注意]

キャプチャデータは、最大サイズを超えるパケットを受信した場合、古い情報を上書きして記録します。

[実行例]

```
# capturectl remove ieee80211  
#
```

52.1.4 capturectl start radius

[機能]

RADIUS 認証の packets キャプチャの開始

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
capturectl start radius <number>
```

[オプション]

<number>

- ・ lan 定義番号

認証サーバに接続可能な LAN インタフェースの定義番号を 10 進数で指定します。

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

RADIUS 認証で使用する認証パケットのキャプチャの開始を指示します。

RADIUS 認証で使用する RADIUS サーバが接続した LAN インタフェース番号を指定することで、RADIUS サーバと無線端末とで送受信した認証フレームを記録します。

認証パケットは UDP ポート番号 1812 及び 1645 を送信先・送信元とするパケットです。

停止コマンドにより、蓄積したパケット情報を pcap 形式でファイルに出力します。

[メッセージ]

```
Start capture failed. lan <number> is in use.
```

LAN インタフェースでキャプチャ機能を使用中のため、キャプチャの開始ができません。

動作中のキャプチャを停止してから、再度コマンドを実行してください。

```
Start capture failed. lan <number> is unavailable.
```

指定した LAN インタフェースが無効のため、キャプチャの開始ができません。

[注意]

キャプチャデータは、最大サイズを超えるパケットを受信した場合、古い情報を上書きして記録します。

[実行例]

```
# capturectl start radius 0
#
```

52.1.5 capturectl stop radius

[機能]

RADIUS 認証の packets キャプチャの停止

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
capturectl stop radius
```

[オプション]

[動作モード]

運用管理モード(管理者クラス)

構成定義モード(管理者クラス)

[説明]

RADIUS 認証で使用する認証パケットのキャプチャの停止を指示します。
停止コマンドにより、蓄積したパケット情報をファイルに出力します。
生成されるファイル名は固定名(radius.pcap)で生成され、ファイルの最大サイズは以下のとおりです。

最大サイズ	機種
50M バイト	SR-M630AP1
25M バイト	SR-M610AP1

このファイルは、ftp/sftp get および copy コマンドでの取得ができます。

[注意]

キャプチャファイルに記録されるパケットデータは時刻順で記録されない場合があります。
キャプチャ解析アプリのソート機能を利用して参照してください。

[実行例]

```
# capturectl stop radius  
#
```

52.1.6 capturectl remove radius

[機能]

RADIUS 認証キャプチャファイルの削除

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
capturectl remove radius
```

[オプション]

[動作モード]

運用管理モード(管理者クラス)
構成定義モード(管理者クラス)

[説明]

RADIUS 認証キャプチャファイル(radius.pcap)を削除する。

[メッセージ]

```
Remove capture failed. lan <number> is in use.
```

[注意]

[実行例]

```
# capturectl remove radius  
#
```

第 53 章 I'm here コマンド

53.1 I'm here コマンド

53.1.1 iamhere

[機能]

I'm here ランプの手動点滅の設定

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

iamhere <mode> [<time>]

[オプション]

<mode>

I'm here ランプの点滅、および点滅解除の操作

- on

I'm here ランプの点滅を開始します。

[<time>]

I'm here ランプを点滅させる時間を指定します。

単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

指定可能な範囲は以下のとおりです。

1s~86400s

1m~1440m

1h~24h

1d

省略時は、I'm here ランプの点滅は自動的に解除されません。

- off

I'm here ランプの点滅を解除します。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

装置のランプを指定時間だけ点滅させます。

ランプを点滅させて本装置の設置場所を目視確認できます。

本コマンドを続けて実行した場合、最後に指定した時間だけ点滅します。

[実行例]

```
# iamhere on 30m
#
```

第 54 章 その他のコマンド

54.1 その他

54.1.1 ping

[機能]

ICMP エコー要求パケットの送信

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
ping <ip_address> [source <ip_address>] [repeat [<count>]] [size <dec>] [ttl <dec>] [timeout <dec>]
ping <host_name> [source <ip_address>] [repeat [<count>]] [size <dec>] [ttl <dec>] [timeout <dec>]
```

[オプション]

<ip_address>

- ・ 送出先 IP アドレス
送出先の IPv4 アドレスを指定します。
<ip_address>か<host_name>のどちらか一方を指定する必要があります。

<host_name>

- ・ 送信先ホスト名
送出先のホスト名を指定します。
ホスト名を指定した場合は、ホストデータベース情報に該当ホスト名が登録されているか、本装置が DNS サーバを使用可能な状態でなければなりません。
<ip_address>か<host_name>のどちらか一方を指定する必要があります。

source <ip_address>

- ・ 送信元 IP アドレス
送信元 IP アドレスを指定します。装置に定義されていないアドレスは指定できません。
送信先 IP アドレスとバージョンが一致しない場合はエラーとなります。

repeat [<count>]

- ・ 繰り返し回数
繰り返し回数を 0~65535 の 10 進数で指定します。
<count>を省略時は、0 を指定したものとみなされます。

size <dec>

- ・ データサイズ
送信する ICMP データ長を、46~9600 の 10 進数(単位:バイト)で指定します。
省略時は、46 バイトを指定したものとみなされます。

ttl <dec>

- ・ TTL 値
TTL 値を、1~255 の 10 進数で指定します。
省略時は、128 を指定したものとみなされます。

timeout <dec>

- ・ 応答監視時間
応答監視時間を、1~300 の 10 進数(単位:秒)で指定します。
省略時は、20 秒を指定したものとみなされます。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

指定したホスト (IP アドレスまたはホスト名) に対して、ICMP ECHO_REQUEST を送信し、ICMP ECHO_RESPONSE の受信を確認します。

[実行例]

a) オプションなし (IP アドレス指定のみ)

```
# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 46 data bytes
54 bytes from 192.168.1.1: seq=0 ttl=64 time=0.217 ms

--- 192.168.1.1 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.217/0.217/0.217 ms
#
```

b) ホスト名指定

```
# ping jp.fujitsu.com
PING jp.fujitsu.com (192.168.1.2): 46 data bytes
54 bytes from 192.168.1.2 seq=0 ttl=64 time=0.217 ms

--- jp.fujitsu.com ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.217/0.217/0.217 ms
#
```

c) 繰り返し (3 回指定)

```
# ping 192.168.1.1 repeat 3
PING 192.168.1.1 (192.168.1.1): 46 data bytes
54 bytes from 192.168.1.1: seq=0 ttl=64 time=0.218 ms
54 bytes from 192.168.1.1: seq=1 ttl=64 time=0.189 ms
54 bytes from 192.168.1.1: seq=2 ttl=64 time=0.175 ms

--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.175/0.194/0.218 ms
#
```

※オプションの指定順序は入力形式に従ってください。

54.1.2 traceroute

[機能]

ネットワーク経路の表示

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

```
traceroute <ip_address> [ source <src_ip_address> ] [ size <data_size> ] [ timeout <timeout> ]
traceroute <host_name> [ source <src_ip_address> ] [ size <data_size> ] [ timeout <timeout> ]
```

[オプション]

<ip_address>

- ・ 送出先 IP アドレス
送出先の IPv4 アドレスを指定します。
<ip_address>か<host_name>のどちらか一方を指定する必要があります。

<host_name>

- ・ 送出先ホスト名
送出先のホスト名を指定します。
ホスト名を指定した場合は、ホストデータベース情報に該当ホスト名が登録されているか、本装置が DNS サーバを使用可能な状態でなければなりません。
<ip_address>か<host_name>のどちらか一方を指定する必要があります。

source <src_ip_address>

- ・ 送信元 IP アドレス
送信元 IP アドレスを指定します。装置に定義されていないアドレスは指定できません。
送信先 IP アドレスとバージョンが一致しない場合はエラーとなります。

size <data_size>

- ・ データサイズ
送信する IP ヘッダを含むパケット長を、46~9600 の 10 進数(単位:バイト)で指定します。
省略時は、46 バイトを指定したものとみなされます。

timeout <timeout>

- ・ 応答監視時間
応答監視時間を、1~300 の 10 進数(単位:秒)で指定します。
省略時は、20 秒を指定したものとみなされます。

df

- ・ フラグメント禁止
送信するパケットに Don't Fragment bit を設定して経路の途中でフラグメントされないようにします。

[動作モード]

運用管理モード(一般ユーザクラス/管理者クラス)
構成定義モード(管理者クラス)

[説明]

ネットワーク経路を表示します。

指定した host (IP アドレスまたはホスト名)に対して、IP データグラムヘッダの生存時間(TTL)の値を 1 から 1 つずつ単調に増加させながら試験パケットを送信し、時間超過またはあて先到達不能の ICMP パケット受信によって、host までの経路情報を表示します。

traceroute で表示される文字には以下の意味があります。

[あて先が IPv4 アドレスの場合]

XX. XXX ms

ラウンドトリップタイム

!N

あて先到達不能(ネットワークへの経路なし)

!H

あて先到達不能(ホストへの経路なし)

!P

あて先到達不能(プロトコル到達不能)

!S

ソースルートルーティング失敗

!

TTL 値が異常

プローブのタイムアウト

また、tracert は以下のエラーを報告します。

```
tracert: bad address '<host_name>'
```

<host_name>で指定した送出先ホスト名から送出先 IP アドレスが解決できない。

```
tracert: sendto: Network unreachable
```

あて先 IP アドレスに到達できない。

(装置に存在しないアドレスを指定した場合など)

[実行例]

host から応答がある場合

```
# tracert 192.168.1.1
tracert to 192.168.1.1 (192.168.1.1), 30 hops max, 46 byte packets
 1  192.168.1.102 (192.168.1.102)  1.081 ms  1.716 ms  1.475 ms
#
```

host から応答がない場合

```
# tracert 192.168.1.1
tracert to 192.168.1.1 (192.168.1.1), 30 hops max, 46 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
   :
30  * * *
#
```

54.1.3 telnet

[機能]

telnet サーバへの接続

[適用機種]

SR-M630AP1 SR-M610AP1

[入力形式]

telnet <host> [<port>]

[オプション]

<host>

接続先ホスト(telnet サーバ)を、以下の形式で指定します。

- ・ ホスト名
- ・ IPv4 アドレス

<port>

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、telnet ポート番号である 23 を指定したものとみなされます。

[動作モード]

運用管理モード(一般クラス/管理者クラス)

構成定義モード(管理者クラス)

[説明]

telnet サーバが動作しているホストやルータに接続して、遠隔操作することができます。

[実行例]

```
# telnet 192.168.1.2          他ルータにtelnet接続
Escape character is '^]'    エスケープ文字表示
Login:                      他ルータのユーザ名入力
Password:                   他ルータのパスワード入力
# exit                      他ルータでexitコマンド実行
Connection closed by foreign host. 切断
#                            本ルータのプロンプト表示
```


第 55 章 commit コマンド実行時の影響について

各構成定義コマンドで構成定義を変更後に commit コマンドを実行したときの影響について以下に示します。なお、各構成定義コマンドの変更/追加/削除のそれぞれについて、影響は同じです。

種別		コマンド名	commit 実行時影響	
			SR-M630AP1	SR-M610AP1
パスワード情報		password admin set	(0)	
		password user set	(0)	
		password aaa	(1)	
		password authtype	(1)	
ポート情報の設定	ether 共通情報	ether use	(3)-1	(5)-2
		ether mode	(3)-1	(5)-2
		ether duplex	(3)-1	(5)-2
		ether mdi	(3)-1	(5)-2
		ether flowctl	(3)-1	(5)-2
		ether type	(3)-1	(5)-2
		ether vlan	(3)-1	(5)-2
		ether downrelay	(1)	
		ether downrelay wlan	(1)	
		ether downrelay recovery mode	(1)	
		ether icmpwatch	(1)	
		ether description	(1)	
リンクアグリゲーション情報		linkaggregation	(3)-1	(5)-2
		linkaggregation downrelay	(1)	
		linkaggregation icmpwatch	(1)	
無線 LAN モジュール情報の設定	無線 LAN モジュール情報	ieee80211 use	(5)	(3)-1
		ieee80211 mode	(5)	(3)-1
		ieee80211 channel	(5)	(3)-1
		ieee80211 bandwidth	(5)	(3)-1
		ieee80211 secondary-channel	(5)	(3)-1
		ieee80211 chanlist	(5)	(3)-1
		ieee80211 sta limit	(5)	(3)-1
		ieee80211 protection mode	(5)	(3)-1
		ieee80211 rts threshold	(5)	(3)-1
		ieee80211 dtim period	(5)	(3)-1
		ieee80211 beacon interval	(5)	(3)-1
		ieee80211 wmm mode	(5)	(3)-1
		ieee80211 wmm ack	(5)	(3)-1
		ieee80211 apscan mode	(5)	(3)-1
		ieee80211 apscan expire	(5)	(3)-1
		ieee80211 txpower	(5)	(3)-1
		ieee80211 supportrate	(5)	(3)-1
		ieee80211 supportmcs	(5)	(3)-1
		ieee80211 vht-supportmcs	(5)	(3)-1
		ieee80211 he-supportmcs	(5)	(3)-1
ieee80211 noise-detect	(5)	(3)-1		
ieee80211 radar-detect	(5)	(3)-1		
ieee80211 sr use	(5)	(3)-1		
ieee80211 sr tx-threshold	(5)	(3)-1		

種別	コマンド名	commit 実行時影響	
		SR-M630AP1	SR-M610AP1
	ieee80211 l4ch-support ieee80211 outdoormode	(5) (3)-1 (4)	
無線 LAN インタ フェース情報の 設定	無線 LAN インタ フェース情報	wlan use	(5) (3)-1
		wlan description	(1)
		wlan type	(5) (3)-1
		wlan ssid	(5) (3)-1
		wlan hide	(5) (3)-1
		wlan apbridge	(5) (3)-1
		wlan auth	(5) (3)-1
		wlan wep mode	(5) (3)-1
		wlan wep key	(5) (3)-1
		wlan wep send	(5) (3)-1
		wlan wpa cipher	(5) (3)-1
		wlan wpa psk	(5) (3)-1
		wlan wpa sae password	(5) (3)-1
		wlan wpa rekey group	(5) (3)-1
		wlan wpa pmkcache mode	(5) (3)-1
		wlan wpa pmkcache num	(5) (3)-1
		wlan wpa pmkcache expire	(5) (3)-1
		wlan wpa eapol supptimeout	(5) (3)-1
		wlan wpa eapol maxreq	(5) (3)-1
		wlan wpa pmf mode	(5) (3)-1
wlan wpa owe_trans	(5) (3)-1		
wlan guard-interval	(5) (3)-1		
wlan macfilter	(5) (9)		
wlan sta guarantee	(5) (3)-1		
wlan sta idle	(5) (3)-1		
wlan band-steering mode	(5) (3)-1		
wlan atf	(5) (3)-1		
VLAN 情報	wlan vlan	(5)-2 (3)-1	
IEEE802.1X 認証情 報	IEEE802.1X 認証情報	wlan dot1x use	(5) (3)-1
		wlan dot1x supptimeout	(5) (3)-1
		wlan dot1x maxreq	(5) (3)-1
		wlan dot1x reauthperiod	(5) (3)-1
		wlan dot1x aaa	(5) (3)-1
		wlan dot1x vid	(5) (3)-1
		wlan dot1x vlan assign	(5) (3)-1
wlan dot1x backup	(5) (3)-1		
MAC アドレス認証情 報	MAC アドレス認証情報	wlan macauth use	(5) (3)-1
		wlan macauth aaa	(5) (3)-1
		wlan macauth expire	(5) (3)-1
		wlan macauth vid	(5) (3)-1
		wlan macauth vlan assign	(5) (3)-1
無線インタフェ ース数情報	wlan-conf wlan-num	(4)	
エアタイムフェ アネス情報の設 定	エアタイムフェ アネス情報	atf use	(4)

種別	コマンド名	commit 実行時影響	
		SR-M630AP1	SR-M610AP1
VLAN 情報の設定	VLAN 共通情報	vlan name vlan description	(1) (1)
	フィルタ情報	vlan filter	(1) (9)
MAC 情報	MAC 情報	mac age	(1)
LAN 情報の設定	IP 関連情報	lan ip address	(3)-1(5)-2
		lan ip dhcp	(3)-1(5)-2
		lan ip route	(3)-1(5)-2
lan ip arp static		(3)-1(5)-2	
VLAN 関連情報	lan vlan	(3)-1(5)-2	
SNMP 関連情報	lan snmp	(1)	
IP 関連情報	IP 関連情報	ip arp age	(1)
認証情報の設定	IEEE802.1X 情報	dot1x	(5) (3)-1
	MAC アドレス認証情報	macauth	(5) (3)-1
ACL 情報の設定	ACL 情報	acl	(9)
AAA 情報の設定	グループ ID 情報	aaa name	(1)
	RADIUS 情報	aaa radius	(5) (3)-1
装置情報の設定	SNMP 情報	snmp	(1)
	システムログ情報	syslog	(1)
	自動時刻設定情報	time	(1)
	ProxyARP 情報	proxyarp	(5)-2(3)-1
	スケジュール情報	schedule	(1)
	装置ランプ情報	lamp	(0)
	高速転送情報	system bridge	(4)
	定期ログ情報	system monitoringinfo	(1)
	外部メディアスタート機能の情報	storage setup	(0)
	アンテナ情報	antenna use	(1)
	端末可視化機能の設定	devscan devscan age	(1) (10)
	DNS サーバ情報	dns-resolver server	(3)-1(5)-2
	NXconcierge エージェント機能情報の設定	management-agent mode	(0)
management-agent tenantkey		(0)	
management-agent macfilter		(0)	
management-agent serverlogin proxy		(0)	
その他	addact	(0)	
	consoleinfo	(1)	
	telnetinfo	(1)	
	sysname	(4)	
	serverinfo	(1) (9)	

-
- (0) コマンドを実行すると、その直後から有効になります。
 - (1) 該当箇所の該当機能だけ停止／再開になります。
 - (2) 該当論理インタフェースでの通信が中断されます。
 - (3) 該当 ether ポートがリンクダウン／リンクアップします。
 - (3)-1 全 ether ポートがリンクダウン／リンクアップします。
 - (4) 有効にする場合は、装置の再起動(リセット)が必要になります。
 - (5) 該当の無線 LAN モジュールおよび関連する無線 LAN 論理インタフェースが停止／再開になります。
再開が完了するまでの間、ether ポート/無線 LAN モジュールの通信は不可となります。
無線 LAN 論理インタフェース数や VLAN ID 数が多い場合、再開までに数分程度かかります。
 - (5)-1 無線 LAN モジュール定義の該当定義のみが変更された場合は、無線 LAN モジュールおよび無線 LAN インタフェースは停止／再開されません。ほかの定義と同時に変更された場合、(5)と同様になります。
 - (5)-2 全無線 LAN モジュールおよび無線 LAN 論理インタフェースが停止／再開になります。
再開が完了するまでの間、ether ポート/無線 LAN モジュールの通信は不可となります。
再開完了時間は定義されている無線 LAN 論理インタフェース数に比例し、数分程度かかる場合があります。
 - (6) (1)に加え、デジタル証明書／秘密鍵を利用する該当の無線 LAN モジュール、および、関連する無線 LAN 論理インタフェースが停止／再開になります。
 - (7) (1)に加え、該当機能を使用中の無線 LAN モジュールおよび無線 LAN インタフェースが停止／再開されません。
 - (8) (1)に加え、該当機能を使用中の ether ポートがリンクダウン／リンクアップします。
 - (9) ACL 定義を参照している機能が停止／再開されることがあります。
 - (10) 次回動作時から有効となります。
- ※1 登録された学習テーブルが削除される場合があります。

第 56 章 SR-M50AP1 からの構成定義引継ぎについて

56.1 SR-M630AP1/610AP1 での未サポートコマンド

SR-M630AP1/610AP1 では、SR-M50AP1 の以下のコマンドが未サポートとなります。

よって、SR-M50AP1 の構成定義をそのまま SR-M630AP1/610AP1 に展開した場合、以下のような動作となります。

- **password format**

- [機能]

- 暗号化パスワード文字列形式の設定

- [動作]

- common で動作します。

- **backup mode、backup standby、backup downrelay**

- [機能]

- バックアップポート機能の設定

- [動作]

- 無効となります。

- **ieee80211 basicrate**

- [機能]

- 無線通信時に使用するベーシックレートの設定

- [動作]

- 2.4GHz 帯（無線通信モードが 11b を含む）の場合

- ベーシックレートは 1, 2, 5.5, 11 で動作します。

- 2.4GHz 帯（無線通信モードが 11b を含まない）の場合

- ベーシックレートは 1, 2, 5.5, 6, 11, 12 で動作します。

- 5GHz 帯の場合

- ベーシックレートは 6, 12, 24 で動作します。

- **ieee80211 basicmcs**

- [機能]

- 11n 通信時に使用するベーシック MCS の設定

- [動作]

- 無効となります（ieee80211 supportmcs の設定に従います）。

- **ieee80211 vht-basicmcs**

- [機能]

- 11ac 通信時に使用する VHT ベーシック MCS の設定

- [動作]

- VHT ベーシック MCS Index は 0-7 の範囲で動作します。

- **ieee80211 beacon interval (V20.03 以前)**

- [機能]

- ビーコン間隔の設定

- [動作]

- 無効となります。

- **ieee80211 radar-detect chscan use**

- [機能]

- レーダー検出後のチャネルスキャン機能の設定

[動作]

無効となります。

• **ieee80211 module-recovery**

[機能]

無線 LAN モジュール異常リカバリ機能の設定

[動作]

無効となります。

• **wlan wds neighbor**

[機能]

WDS ブリッジの対向 MAC アドレス設定

[動作]

無効となります。

• **wlan wep type**

[機能]

WEP 動作タイプの設定

[動作]

無効となります。

• **wlan wpa countermeasures**

[機能]

MIC エラー検出の設定

[動作]

無効となります。

• **wlan forward broadcast**

[機能]

無線 LAN インタフェースへのブロードキャスト/マルチキャストフレーム転送の設定

[動作]

無効となります。

• **wlan wmm acimap**

[機能]

WMM 優先制御の AC 分類条件の設定

[動作]

無効となります。

• **wlan macauth authenticated-mac**

[機能]

無線 LAN インタフェースの MAC アドレス認証不要端末アドレスの設定

[動作]

無効となります。

• **vlan forward**

[機能]

VLAN の転送設定

[動作]

無効となります。

- **vlan ids**

- [機能]**

- IDS の設定

- [動作]**

- 無効となります。

- **macauth password (20.05 以前)**

- [機能]**

- MAC アドレス認証情報 (パスワード) の設定

- [動作]**

- 無効となります。MAC アドレス認証情報に認証端末の MAC アドレスが使用されます。

- **aaa user**

- [機能]**

- 無線 LAN 管理ログイン機能の設定

- [動作]**

- 無効となります。

- **nodemanager login service enable**

- [機能]**

- 無線 LAN 管理ログイン機能の設定

- [動作]**

- 無効となります。

- **syslog security、 syslog dupcut、 syslog logging nodemgr access**

- [機能]**

- シスログ情報の設定 (出力対象セキュリティ/重複メッセージ出力/無線 LAN 管理アクセス履歴出力)

- [動作]**

- 無効となります。

- **proxydns**

- [機能]**

- プロキシ DNS の設定

- [動作]**

- 無効となります。

- **proxyarp unicast**

- [機能]**

- ユニキャスト ARP 要求の設定

- [動作]**

- 無効となります。ユニキャスト ARP 要求は常に無線 LAN 側へ転送されます。

- **host name、 host ip address**

- [機能]**

- 認証情報の設定 (ユーザ ID/パスワードほか)

- [動作]**

- 無効となります。

- **system bridge acceleration mode (V20.03 以前)**

[機能]

ブリッジ高速転送モードの設定

[動作]

無効となります。

• **systemwatch**

[機能]

メモリ予兆監視情報の設定

[動作]

無効となります。

• **serverinfo dns**

[機能]

サーバ情報 (DNS サーバ)

[動作]

無効となります。

• **terminal**

[機能]

ターミナル操作機能の設定

[動作]

無効となります。

• **alias**

[機能]

コマンドエイリアス情報の設定

[動作]

無効となります。

• **serverinfo time ip tcp**

[機能]

TCP による TIME サーバ機能の設定

[動作]

無効となります。TIME サーバ機能の停止する場合は `serverinfo time ip` を使用してください。

• **serverinfo time ip udp**

[機能]

UDP による TIME サーバ機能の設定

[動作]

無効となります。UDP による TIME サーバ機能は未サポートです。

56.2 SR-M630AP1/610AP1 での未サポートパラメタ

SR-M630AP1/610AP1 では、SR-M50AP1 の以下のコマンドのパラメタ設定が未サポートとなります。
よって、SR-M50AP1 の構成定義をそのまま SR-M630AP1/610AP1 に展開した場合、以下のような動作となります。

- **ether type**

- [機能]

- ether ポートの種別の設定

- [動作]

- backup が設定されている場合は、設定が無効となります。未設定時の normal で動作します。

- **vlan filter default**

- [機能]

- どのフィルタテーブルにも不一致時の動作の設定

- [動作]

- <action>に、spi が設定されている場合は、設定が無効となります。未設定時の pass で動作します。

- **acl mac**

- [機能]

- ACL MAC 定義の設定

- [動作]

- <src_mac>および<dst_mac>に、bcst または mcast が設定されている場合は、設定が無効となります。

- **acl ip**

- [機能]

- ACL IP 定義の設定

- [動作]

- <type>パラメタは、設定値に関わらず any で動作します。

- **acl tcp**

- [機能]

- ACL TCP 定義の設定

- [動作]

- <tcpconnect>パラメタは、設定値に関わらず yes で動作します。

- **acl icmp**

- [機能]

- ACL ICMP 定義の設定

- [動作]

- <icmpcode>パラメタは、設定値に関わらず any で動作します。

- **ieee80211 chanlist**

- [機能]

- スキャンチャンネルリストの設定

- [動作]

- SR-M610 に設定する<band>周波数帯に、W52, W53, W56 がすべて含まれている場合は、コマンドがエラーとなります。

- 設定できない例)

- ieee80211 2 chanlist w52, w53, w56

- 5GHz 帯ですべての周波数帯をスキャン対象とする場合は本コマンドの実施は不要なので削除してください。

- **wlan type**

- **[機能]**

- 無線 LAN インタフェースの動作タイプ設定

- **[動作]**

- <type>に、wds または scanonly が設定されている場合は、設定が無効となります。

- `aaa radius client server-info auth` (V20.06 以前)

- `aaa radius client server-info accounting` (V20.06 以前)

- RADIUS サーバ定義番号の設定範囲が 0~1 のため、<number>に 2~3 が設定されている場合は無効となります。

56.3 SR-M630AP1/610AP1 にて動作仕様が変更となったコマンド

SR-M630AP1/610AP1 では、SR-M50AP1 の以下のコマンドの動作仕様の一部が変更となります。

よって、SR-M50AP1 の構成定義をそのまま SR-M630AP1/610AP1 に展開した場合、 以下のような動作となります。

• wlan macfilter

【機能】

MAC アドレスフィルタの設定

【動作】

SR-M630AP1/610AP1 では、wlan macfilter default コマンドにてデフォルト条件を設定するため、wlan macfilter コマンドでは pass/reject 条件のいずれかのみ定義する形式となります。

- wlan macfilter default 条件が pass の場合、wlan macfilter の reject 条件が有効となります。
- wlan macfilter default 条件が reject の場合、wlan macfilter の pass 条件が有効となります。

• serverinfo sftp ip

【機能】

SSH FTP サーバ機能の設定

【動作】

SR-M630AP1/610AP1 では、SSH サーバ機能無効時は SSH FTP サーバ機能は有効となりません。

SSH FTP サーバ機能を使用する場合は、SSH サーバ機能を有効としてください。

• serverinfo ssh ip

【機能】

SSH ログインサーバ機能の設定

【動作】

SR-M630AP1/610AP1 では、本設定を無効にすると、SSH FTP サーバ機能も無効になります。

• sysname

【機能】

本装置の名称の設定

【動作】

SR-M630AP1/610AP1 では、使用可能な文字がアルファベット (a~z、A~Z)、数字 (0~9)、ハイフン (-)、アンダースコア (_) に制限されます。

• time auto interval

【機能】

時刻情報の自動設定間隔の設定

【動作】

SR-M630AP1/610AP1 では、SNTP サーバ機能が有効で、かつ time auto server でプロトコルに簡易 NTP を設定している場合は、時刻情報の自動設定間隔は 32 秒~3960 秒の範囲で自動調整されます。

• vlan filter

【機能】

VLAN のフィルタの設定

【動作差異】

SR-M630AP1/610AP1 では、フィルタリング機能は IP フィルタとなります。

そのため、参照する ACL に、acl vlan を条件設定できません。

また、IP フィルタ処理は、レイヤ 3 レベルでのソフトウェア処理のため、レイヤ 2 レベルでの VLAN 単位での制御はできず、IP フィルタ条件のみの制御となります。

そのため、vlan filter コマンドを設定する VLAN ID には意味を持ちません。ご使用される VLAN のうち任意の VLAN ID を 1 つ選んでいただき、装置全体のフィルタリングルールとして設定してください。

56.4 ハードウェア構成差分によりパラメタ変更が必要なコマンド

SR-M630AP1 は、SR-M50AP1 とハードウェア構成の差分があり、無線モジュール番号に対応する無線チャンネル番号および無線 LAN 周波数帯が異なっています。そのため、SR-M50AP1 の構成定義をそのまま SR-M630AP1 に展開した場合、エラーとなる場合があります。以下に示すコマンドではパラメタの変更を行ってください。

・ `ieee80211 channel`

[機能]

無線 LAN チャンネルの設定

[動作]

SR-M630AP1 の無線モジュール番号 2 (W52, W53 用) に設定するチャンネル番号に、W56 が含まれている場合は、コマンドがエラーとなります。

[パラメタ変更]

無線モジュール番号 2 に設定する `ieee80211 channel` コマンドから、W56 のチャンネル番号(100~144)を外してください。

また、無線モジュール番号 3 に設定する `ieee80211 channel` コマンドに、W56 のチャンネル番号(100~144)を追加し実行してください。

[備考]

チャンネル番号に `any` を設定している場合は変更の必要はありません。

・ `ieee80211 chanlist`

[機能]

スキャンチャンネルリストの設定

[動作]

SR-M630AP1 の無線モジュール番号 2 (W52, W53 用) に設定する<band>周波数帯に、W56 が含まれている場合は、コマンドがエラーとなります。

設定できない例)

```
ieee80211 2 chanlist w52, w53, w56
```

```
ieee80211 2 chanlist w52, w56
```

```
ieee80211 2 chanlist w53, w56
```

```
ieee80211 2 chanlist w56
```

は設定できません。

[パラメタ変更]

無線モジュール番号 2 に設定する `ieee80211 chanlist` コマンドから、W56 を外して実行してください。

索引

A

aaa name..... 167
aaa radius accounting source..... 171
aaa radius auth message-authenticator..... 170
aaa radius auth source..... 169
aaa radius client nas-identifier..... 192
aaa radius client nas-identifier-ssid..... 193
aaa radius client retry..... 191
aaa radius client server-info accounting address 186
aaa radius client server-info accounting deadtime..
..... 188
aaa radius client server-info accounting port... 187
aaa radius client server-info accounting priority..
..... 189
aaa radius client server-info accounting secret. 185
aaa radius client server-info accounting source. 190
aaa radius client server-info auth <number> watch
interval..... 181
aaa radius client server-info auth address..... 173
aaa radius client server-info auth deadtime..... 175
aaa radius client server-info auth port..... 174
aaa radius client server-info auth priority..... 176
aaa radius client server-info auth secret..... 172
aaa radius client server-info auth source..... 177
aaa radius client server-info auth watch abnormal-
interval..... 184
aaa radius client server-info auth watch retry.. 182
aaa radius client server-info auth watch timeout 183
aaa radius client server-info auth watch type... 178
aaa radius client server-info auth watch user... 179
aaa radius service..... 168
acl description..... 165
acl icmp..... 164
acl ip..... 160
acl mac..... 159
acl tcp..... 162
acl udp..... 163
addact..... 278
antenna use..... 254
atf use..... 134

C

capturectl remove ieee80211..... 485
capturectl remove radius..... 488
capturectl start ieee80211..... 483
capturectl start radius..... 486
capturectl stop ieee80211..... 484
capturectl stop radius..... 487
clear arp..... 391
clear bridge..... 404
clear corefile..... 307
clear devscan..... 455
clear dotlx statistics..... 418
clear ether statistics..... 340
clear https certificate..... 308
clear icmpwatch statistics..... 439
clear line..... 330
clear logging command..... 288
clear logging error..... 296
clear logging monitoringinfo..... 301

clear logging syslog..... 298
clear macauth statistics..... 422
clear nettime statistics..... 429
clear snmp statistics..... 434
clear statistics..... 302
clear trace management-agent..... 459
clear wlan wpa statistics..... 376
commit..... 318
configure..... 285
consoleinfo..... 280
copy..... 322

D

date..... 304
delete..... 314
devscan age..... 197
devscan dictionary dhcp..... 198
devscan dictionary mac..... 200
devscan dictionary oui..... 199
devscan use..... 195
devscan vlan..... 196
diff..... 313
dir..... 320
discard..... 319
dns-resolver server..... 277
dotlx use..... 154
dotlxcctl backup recovery..... 475
dotlxcctl initialize..... 473
dotlxcctl reconfirm..... 474

E

ether description..... 34
ether downrelay recovery mode..... 33
ether downrelay wlan..... 32
ether duplex..... 26
ether flowctl..... 28
ether icmpwatch address..... 35
ether icmpwatch interval..... 36
ether mdi..... 27
ether mode..... 25
ether type..... 29
ether use..... 24
ether vlan tag..... 30
ether vlan untag..... 31
exit..... 284

F

format..... 326

I

iamhere..... 490
ieee80211 144ch-support..... 76
ieee80211 apscan expire..... 63
ieee80211 apscan mode..... 62
ieee80211 bandwidth..... 50
ieee80211 beacon interval..... 59
ieee80211 chanlist..... 53
ieee80211 channel..... 49

ieee80211 dtim period.....	58
ieee80211 he-supportmcs.....	71
ieee80211 mode.....	47
ieee80211 noise-detect use.....	72
ieee80211 outdoormode.....	77
ieee80211 protection mode.....	56
ieee80211 radar-detect lamp-flash time.....	73
ieee80211 rts threshold.....	57
ieee80211 secondary-channel.....	51
ieee80211 sr tx-threshold.....	75
ieee80211 sr use.....	74
ieee80211 sta limit.....	55
ieee80211 supportmcs.....	68
ieee80211 supportrate.....	66
ieee80211 txpower.....	64
ieee80211 use.....	46
ieee80211 vht-supportmcs.....	70
ieee80211 wmm ack.....	61
ieee80211 wmm mode.....	60
ip arp age.....	152

L

lamp delay.....	249
lamp mode.....	248
lan ip address.....	143
lan ip arp static.....	147
lan ip dhcp service.....	144
lan ip route.....	145
lan snmp trap linkdown.....	149
lan snmp trap linkup.....	150
lan vlan.....	148
linkaggregation algorithm.....	38
linkaggregation downrelay recovery mode.....	42
linkaggregation downrelay wlan.....	41
linkaggregation icmpwatch address.....	43
linkaggregation icmpwatch interval.....	44
linkaggregation lacp-timeout.....	40
linkaggregation mode.....	39
load.....	315

M

mac age.....	141
macauth password.....	156
macauth type.....	157
macauth use.....	155
macauthctl initialize.....	477
management-agent macfilter.....	204
management-agent mode.....	202
management-agent serverlogin proxy address.....	206
management-agent serverlogin proxy auth send.....	205
management-agent tenantkey.....	203
monitoringinfectl collect.....	481

O

offline.....	463
online.....	465

P

password aaa.....	21
password admin set.....	17
password authtype.....	22

password user set.....	19
ping.....	492
proxyarp use.....	244

R

radius recovery.....	479
rdate.....	305
remove.....	324
rename.....	325
reset.....	306

S

save.....	317
schedule at.....	245
schedule syslog.....	247
serverinfo ftp.....	255
serverinfo ftp filter.....	256
serverinfo ftp filter default.....	257
serverinfo http.....	265
serverinfo http filter.....	266
serverinfo http filter default.....	267
serverinfo https.....	268
serverinfo https filter.....	269
serverinfo https filter default.....	270
serverinfo sftp.....	258
serverinfo snmp.....	271
serverinfo snmp filter.....	272
serverinfo snmp filter default.....	273
serverinfo ssh.....	262
serverinfo ssh filter.....	263
serverinfo ssh filter default.....	264
serverinfo telnet.....	259
serverinfo telnet filter.....	260
serverinfo telnet filter default.....	261
serverinfo time.....	274
serverinfo time filter.....	275
serverinfo time filter default.....	276
show aaa radius client server-info.....	424
show arp.....	389
show band-steering status.....	378
show bridge.....	402
show candidate-config.....	310
show date.....	303
show devscan.....	444
show devscan description.....	452
show devscan hostname.....	450
show devscan ip.....	448
show devscan mac.....	446
show devscan unknown.....	454
show dns-resolver information.....	461
show dotlx backup port.....	416
show dotlx port.....	412
show dotlx statistics port.....	414
show ether.....	332
show ether statistics.....	335
show icmpwatch.....	436
show icmpwatch statistics.....	437
show ieee80211 apscan.....	351
show ieee80211 statistics.....	345
show ieee80211 status.....	348
show interface.....	386
show ip dhcp.....	399
show ip route.....	393

show ip traffic.....	396
show lacp.....	342
show logging command.....	286
show logging error.....	295
show logging monitoringinfo.....	299
show logging syslog.....	297
show macauth port.....	419
show macauth statistics port.....	421
show management-agent ca-certificate.....	457
show nettime statistics.....	427
show poe drawing.....	380
show running-config.....	311
show snmp statistics.....	431
show socket.....	441
show ssh server key.....	409
show startup-config.....	312
show system information.....	290
show system status.....	292
show tech-support.....	294
show trace management-agent.....	458
show usb hcd status.....	382
show usb storage status.....	383
show users.....	328
show vlan.....	406
show wlan sta.....	358
show wlan statistics.....	363
show wlan status.....	365
show wlan wpa statistics.....	373
show wlan wpa status.....	370
snmp agent address.....	212
snmp agent contact.....	209
snmp agent engineid.....	213
snmp agent location.....	211
snmp agent sysname.....	210
snmp manager.....	214
snmp service.....	208
snmp trap authfail.....	219
snmp trap coldstart.....	216
snmp trap linkdown.....	217
snmp trap linkup.....	218
snmp trap noserror.....	220
snmp user address.....	222
snmp user auth.....	224
snmp user name.....	221
snmp user notification.....	223
snmp user notify.....	228
snmp user priv.....	225
snmp user read.....	227
snmp user write.....	226
snmp view subtree.....	229
storage setup machine.....	253
storage setup mode.....	252
syslog command-logging.....	235
syslog facility.....	234
syslog filter regexp.....	238
syslog header.....	236
syslog pri.....	233
syslog server address.....	231
syslog server pri.....	232
syslog source address.....	237
sysname.....	282
system bridge acceleration mode.....	250
system monitoringinfo collect interval.....	251

T

telnet.....	496
telnetinfo.....	281
time auto interval.....	242
time auto server.....	241
time zone.....	243
traceroute.....	494

U

usbctl.....	471
-------------	-----

V

vlan description.....	137
vlan filter.....	138
vlan name.....	136

W

wlan apbridge.....	86
wlan atf ratio.....	112
wlan auth.....	87
wlan band-steering mode.....	110
wlan description.....	82
wlan dot1x aaa.....	120
wlan dot1x backup.....	124
wlan dot1x maxreq.....	118
wlan dot1x reauthperiod.....	119
wlan dot1x supptimeout.....	117
wlan dot1x use.....	115
wlan dot1x vid.....	121
wlan dot1x vlan assign.....	122
wlan guard-interval.....	104
wlan hide.....	85
wlan macauth aaa.....	128
wlan macauth expire.....	129
wlan macauth use.....	126
wlan macauth vid.....	130
wlan macauth vlan assign.....	131
wlan macfilter.....	105
wlan macfilter default.....	107
wlan ssid.....	84
wlan sta guarantee.....	108
wlan sta idle.....	109
wlan type.....	83
wlan use.....	81
wlan vlan tag.....	113
wlan vlan untag.....	114
wlan wep key.....	90
wlan wep mode.....	89
wlan wep send.....	92
wlan wpa cipher.....	93
wlan wpa eapol maxreq.....	101
wlan wpa eapol supptimeout.....	100
wlan wpa owe trans.....	103
wlan wpa pmf mode.....	102
wlan wpa pmkcache expire.....	99
wlan wpa pmkcache mode.....	97
wlan wpa pmkcache num.....	98
wlan wpa psk.....	94
wlan wpa rekey group.....	96
wlan wpa sae password.....	95
wlan-conf wlan-num.....	79

wlanctl authenticator disconnect..... 468

SR-M コマンドリファレンス

P3NK-7522-07Z0

発行日 2023年10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。