

FUJITSU Network SR-M コマンドリファレンス

V02

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。

2010年 4月初版
2011年 9月第2版
2013年 7月第3版
2014年 8月第4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 2010 - 2014

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。

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

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。

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

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

本書の構成

本書の第1～15章では構成定義コマンドを、第16～40章では表示および操作コマンドを、第41～49章では制御コマンドを、第50章ではその他のコマンドを説明しています。第51章では付録情報を説明しています。

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、terminal 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。コマンド未設定時の値を表示したい場合は、show コマンドに続けて、表示したいパラメタの直前のコマンドまで入力します。
例：LAN インタフェースの IP アドレスの表示

```
# show candidate-config lan 0 ip address  
192.168.1.1/24 3
```

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。

本書における商標の表記について

Microsoft、MS-DOS、Windows、Windows NT、Windows Server および Windows Vista は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

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

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

UNIX は、米国およびその他の国におけるオープン・グループの登録商標です。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

製品名の略称について

本書で使用している製品名は、以下のように略して表記します。

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

本装置のマニュアルの構成

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

マニュアル名称	内容
SR-M20AP1 ご利用にあたって	SR-M20AP1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。
SR-M20AP2 ご利用にあたって	SR-M20AP2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。
SR-M20AC1 ご利用にあたって	SR-M20AC1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。
SR-M20AC2 ご利用にあたって	SR-M20AC2の設置方法やソフトウェアのインストール方法を説明しています。
機能説明書	本装置の便利な機能について説明しています。
トラブルシューティング	トラブルが起きたときの原因と対処方法を説明しています。
メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
仕様一覧	本装置のハード／ソフトウェア仕様とMIB/Trap一覧を説明しています。
コマンドユーザーズガイド	コマンドを使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
コマンド設定事例集	コマンドを使用した、基本的な接続形態または機能の活用方法を説明しています。
コマンドリファレンス（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。
Web ユーザーズガイド	Web 画面を使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
Web リファレンス	Web 画面の項目の詳細な情報を説明しています。

目次

第1章	パスワード情報	21
1.1	password format	22
1.2	password admin set	24
1.3	password user set	26
1.4	password nodemgr set	28
1.5	password aaa	30
1.6	password authtype	31
第2章	ポート情報の設定	32
2.1	ether 共通情報	33
2.1.1	ether use	33
2.1.2	ether mode	34
2.1.3	ether duplex	35
2.1.4	ether mdi	36
2.1.5	ether flowctl	38
2.1.6	ether type	39
2.1.7	ether vlan tag	41
2.1.8	ether vlan untag	42
2.1.9	ether downrelay wlan	43
2.1.10	ether downrelay recovery mode	44
2.1.11	ether description	45
2.1.12	backup mode	46
2.1.13	backup standby	47
2.1.14	backup downrelay wlan	49
2.1.15	backup downrelay recovery mode	51
2.2	IEEE802.1X 認証情報	52
2.2.1	ether dot1x use	52
2.2.2	ether dot1x portcontrol	54
2.2.3	ether dot1x quietperiod	56
2.2.4	ether dot1x txperiod	57
2.2.5	ether dot1x supptimeout	58
2.2.6	ether dot1x maxreq	59
2.2.7	ether dot1x reauthperiod	60
2.2.8	ether dot1x aaa	61
2.2.9	ether dot1x wol	62
2.3	MAC アドレス認証情報	63
2.3.1	ether macauth use	63
2.3.2	ether macauth aaa	65
2.3.3	ether macauth authenticated-mac	66
2.3.4	ether macauth expire	67

	2.3.5 ether macauth wol	68
第 3 章	無線 LAN モジュール情報の設定	69
	3.1 無線 LAN モジュール情報	70
	3.1.1 ieee80211 use	70
	3.1.2 ieee80211 mode	72
	3.1.3 ieee80211 channel	74
	3.1.4 ieee80211 bandwidth	76
	3.1.5 ieee80211 secondary-channel	77
	3.1.6 ieee80211 chanlist	80
	3.1.7 ieee80211 sta limit	81
	3.1.8 ieee80211 protection mode	82
	3.1.9 ieee80211 ht-protection mode	83
	3.1.10 ieee80211 rts threshold	84
	3.1.11 ieee80211 dtim period	85
	3.1.12 ieee80211 beacon interval	86
	3.1.13 ieee80211 wmm mode	87
	3.1.14 ieee80211 wmm ack	88
	3.1.15 ieee80211 apscan mode	89
	3.1.16 ieee80211 apscan expire	90
	3.1.17 ieee80211 txpower	91
	3.1.18 ieee80211 antenna use	93
	3.1.19 ieee80211 noise-detect mode	94
	3.1.20 ieee80211 noise-detect channel layout	95
第 4 章	無線 LAN インタフェース情報の設定	96
	4.1 無線 LAN インタフェース情報	97
	4.1.1 wlan use	97
	4.1.2 wlan description	99
	4.1.3 wlan type	100
	4.1.4 wlan ssid	102
	4.1.5 wlan hide	103
	4.1.6 wlan apbridge	104
	4.1.7 wlan auth	105
	4.1.8 wlan wep mode	107
	4.1.9 wlan wep key	108
	4.1.10 wlan wep send	110
	4.1.11 wlan wep type	111
	4.1.12 wlan wpa cipher	113
	4.1.13 wlan wpa psk	114
	4.1.14 wlan wpa rekey group	116
	4.1.15 wlan wpa countermeasures	117
	4.1.16 wlan wpa pmkcache mode	118
	4.1.17 wlan wpa pmkcache num	119
	4.1.18 wlan wpa pmkcache expire	120
	4.1.19 wlan wpa eapol supptimeout	121
	4.1.20 wlan wpa eapol maxreq	122
	4.1.21 wlan supplicant dot1x use	123
	4.1.22 wlan supplicant eap protocol	124
	4.1.23 wlan supplicant eap id	125

4.1.24	wlan supplicant eap password	126
4.1.25	wlan supplicant eap peapversion	127
4.1.26	wlan supplicant eap inner protocol	128
4.1.27	wlan supplicant certificate ca	129
4.1.28	wlan supplicant certificate local	130
4.1.29	wlan supplicant certificate private_key	131
4.1.30	wlan ampdu tx mode	132
4.1.31	wlan ampdu rx size	133
4.1.32	wlan ampdu rx density	134
4.1.33	wlan guard-interval	135
4.1.34	wlan macfilter	136
4.1.35	wlan macfilter move	138
4.1.36	wlan roaming mode	139
4.1.37	wlan roaming threshold bmiss	140
4.1.38	wlan roaming threshold rssi	141
4.1.39	wlan roaming threshold rate	143
4.1.40	wlan wmm aclmap	144
4.1.41	wlan wmm aclmap move	146
4.1.42	wlan sta guarantee	147
4.1.43	wlan sta idle	148
4.1.44	wlan wds neighbor	149
4.1.45	wlan relay mode	150
4.1.46	wlan relay expire	151
4.2	VLAN 情報	152
4.2.1	wlan vlan tag	152
4.2.2	wlan vlan untag	153
4.3	フレーム転送情報	154
4.3.1	wlan forward broadcast	154
4.4	IEEE802.1X 認証情報	155
4.4.1	wlan dot1x use	155
4.4.2	wlan dot1x supptimeout	157
4.4.3	wlan dot1x maxreq	158
4.4.4	wlan dot1x reauthperiod	159
4.4.5	wlan dot1x aaa	160
4.4.6	wlan dot1x vid	161
4.4.7	wlan dot1x vlan assign	162
4.4.8	wlan dot1x backup	163
4.5	MAC アドレス認証情報	165
4.5.1	wlan macauth use	165
4.5.2	wlan macauth aaa	167
4.5.3	wlan macauth authenticated-mac	168
4.5.4	wlan macauth expire	169
4.5.5	wlan macauth vid	170
4.5.6	wlan macauth vlan assign	171
第 5 章	VLAN 情報の設定	173
5.1	VLAN 共通情報	174
5.1.1	vlan name	174
5.1.2	vlan forward	175
5.1.3	vlan description	177

	5.2	フィルタ情報	178
	5.2.1	vlan filter	178
	5.2.2	vlan filter move	180
	5.2.3	vlan filter default	181
	5.3	IDS 情報	183
	5.3.1	vlan ids use	183
第 6 章		MAC 情報	184
	6.1	MAC 情報	185
	6.1.1	mac age	185
第 7 章		LAN 情報の設定	186
	7.1	IP 関連情報	187
	7.1.1	lan ip address	187
	7.1.2	lan ip dhcp service	189
	7.1.3	lan ip route	190
	7.1.4	lan ip arp static	192
	7.2	VLAN 関連情報	194
	7.2.1	lan vlan	194
	7.3	SNMP 関連情報	195
	7.3.1	lan snmp trap linkdown	195
	7.3.2	lan snmp trap linkup	196
第 8 章		IP 関連情報	197
	8.1	IP 関連情報	198
	8.1.1	ip arp age	198
第 9 章		認証情報の設定	199
	9.1	IEEE802.1X 情報	200
	9.1.1	dot1x use	200
	9.2	MAC アドレス認証情報	201
	9.2.1	macauth use	201
	9.2.2	macauth password	202
	9.2.3	macauth type	203
第 10 章		サブリカント情報	204
	10.1	supplicant dot1x use	205
	10.2	supplicant certificate check validity	206
第 11 章		証明書関連情報の設定	207
	11.1	証明書関連情報	208
	11.1.1	certificate local name	208
	11.1.2	certificate local line	209
	11.1.3	certificate ca name	210
	11.1.4	certificate ca line	211
	11.1.5	certificate request line	212
	11.1.6	certificate private line	213

第 12 章	ACL 情報の設定	214
12.1	ACL 情報	215
12.1.1	acl mac	215
12.1.2	acl ip	217
12.1.3	acl tcp	220
12.1.4	acl udp	222
12.1.5	acl icmp	224
12.1.6	acl description	226
第 13 章	AAA 情報の設定	227
13.1	グループ ID 情報	228
13.1.1	aaa name	228
13.2	AAA ユーザ情報	229
13.2.1	aaa user id	229
13.2.2	aaa user password	230
13.2.3	aaa user user-role	232
13.3	Supplicant 情報	233
13.3.1	aaa user supplicant vid	233
13.3.2	aaa user supplicant mac	234
13.4	RADIUS 情報の設定	235
13.4.1	aaa radius service	235
13.4.2	aaa radius auth source	236
13.4.3	aaa radius auth message-authenticator	237
13.4.4	aaa radius accounting source	238
13.4.5	aaa radius client server-info auth secret	239
13.4.6	aaa radius client server-info auth address	240
13.4.7	aaa radius client server-info auth port	241
13.4.8	aaa radius client server-info auth deadtime	242
13.4.9	aaa radius client server-info auth priority	244
13.4.10	aaa radius client server-info auth source	245
13.4.11	aaa radius client server-info auth watch type	246
13.4.12	aaa radius client server-info auth watch user	248
13.4.13	aaa radius client server-info auth watch interval	249
13.4.14	aaa radius client server-info auth watch retry	250
13.4.15	aaa radius client server-info auth watch timeout	251
13.4.16	aaa radius client server-info auth watch abnormal-interval	252
13.4.17	aaa radius client server-info accounting secret	253
13.4.18	aaa radius client server-info accounting address	254
13.4.19	aaa radius client server-info accounting port	255
13.4.20	aaa radius client server-info accounting deadtime	256
13.4.21	aaa radius client server-info accounting priority	257
13.4.22	aaa radius client server-info accounting source	258
13.4.23	aaa radius client retry	259
13.4.24	aaa radius client nas-identifier	260
第 14 章	無線 LAN 管理機能の設定	261
14.1	無線 LAN 管理ログイン情報	263
14.1.1	nodemanager login service	263
14.2	無線 LAN 管理機器情報	264
14.2.1	nodemanager group name	264

14.2.2	nodemanager node name	265
14.2.3	nodemanager node group	266
14.2.4	nodemanager node address	267
14.2.5	nodemanager node user	268
14.2.6	nodemanager node wlan scan	269
14.2.7	nodemanager node wlan sta	270
14.2.8	nodemanager node wlan neighbor	271
14.3	MAC アドレスフィルタ情報	272
14.3.1	nodemanager wlan filterset description	272
14.3.2	nodemanager wlan filterset filter mac	273
14.3.3	nodemanager wlan filterset filter description	275
14.4	電波出力自動調整情報	276
14.4.1	nodemanager wlan autotxpower rssi	276
14.5	チャンネル自動調整情報	277
14.5.1	nodemanager wlan autochannel channel	277
14.5.2	nodemanager wlan autochannel layout	278
14.5.3	nodemanager wlan autochannel rssi	279
14.5.4	nodemanager wlan autochannel bandwidth	280
14.6	アクセスポイント情報取得情報	281
14.6.1	nodemanager collect interval	281
14.7	管理外無線 LAN アクセスポイント情報	283
14.7.1	nodemanager wlan scan unmanaged	283
14.8	稼動監視情報	284
14.8.1	nodemanager icmpwatch interval	284
14.8.2	nodemanager icmpwatch threshold	286
14.9	無線 LAN 監視情報	287
14.9.1	nodemanager wlan scan interval	287
14.9.2	nodemanager wlan scan error threshold	289
14.10	監視ログ・パラメタ情報	290
14.10.1	nodemanager log	290
14.10.2	nodemanager wlan sta rssi	291
第 15 章	装置情報の設定	292
15.1	SNMP 情報	293
15.1.1	snmp service	293
15.1.2	snmp agent contact	294
15.1.3	snmp agent sysname	295
15.1.4	snmp agent location	296
15.1.5	snmp agent address	297
15.1.6	snmp agent engineid	298
15.1.7	snmp manager	299
15.1.8	snmp trap coldstart	301
15.1.9	snmp trap linkdown	302
15.1.10	snmp trap linkup	303
15.1.11	snmp trap authfail	304
15.1.12	snmp trap noserror	305
15.1.13	snmp user name	306
15.1.14	snmp user address	307
15.1.15	snmp user notification	308
15.1.16	snmp user auth	309

15.1.17	snmp user priv	311
15.1.18	snmp user write	313
15.1.19	snmp user read	314
15.1.20	snmp user notify	315
15.1.21	snmp view subtree	316
15.2	システムログ情報	318
15.2.1	syslog server address	318
15.2.2	syslog server pri	319
15.2.3	syslog pri	320
15.2.4	syslog facility	321
15.2.5	syslog security	322
15.2.6	syslog dupcut	323
15.2.7	syslog command-logging	324
15.2.8	syslog logging nodemgr access	325
15.3	自動時刻設定情報	326
15.3.1	time auto server	326
15.3.2	time auto interval	327
15.3.3	time zone	328
15.4	ProxyDNS 情報	329
15.4.1	proxydns domain	329
15.4.2	proxydns domain move	332
15.4.3	proxydns address	333
15.4.4	proxydns address move	335
15.4.5	proxydns unicode	336
15.5	ProxyARP 情報	337
15.5.1	proxyarp use	337
15.5.2	proxyarp unicast	338
15.6	ホストデータベース情報	339
15.6.1	host name	339
15.6.2	host ip address	340
15.7	スケジュール情報	341
15.7.1	schedule at	341
15.7.2	schedule syslog	343
15.8	装置ランプ情報	344
15.8.1	lamp mode	344
15.8.2	lamp delay	345
15.9	その他	346
15.9.1	addact	346
15.9.2	watchdog service	348
15.9.3	consoleinfo	349
15.9.4	telnetinfo	350
15.9.5	mflag	351
15.9.6	sysname	352
15.9.7	serverinfo ftp	353
15.9.8	serverinfo ftp filter	354
15.9.9	serverinfo ftp filter move	355
15.9.10	serverinfo ftp filter default	356
15.9.11	serverinfo sftp	357
15.9.12	serverinfo telnet	358
15.9.13	serverinfo telnet filter	359

15.9.14	serverinfo telnet filter move	360
15.9.15	serverinfo telnet filter default	361
15.9.16	serverinfo ssh	362
15.9.17	serverinfo ssh filter	363
15.9.18	serverinfo ssh filter move	364
15.9.19	serverinfo ssh filter default	365
15.9.20	serverinfo http	366
15.9.21	serverinfo http filter	367
15.9.22	serverinfo http filter move	368
15.9.23	serverinfo http filter default	369
15.9.24	serverinfo dns	370
15.9.25	serverinfo dns filter	371
15.9.26	serverinfo dns filter move	372
15.9.27	serverinfo dns filter default	373
15.9.28	serverinfo snmp	374
15.9.29	serverinfo snmp filter	375
15.9.30	serverinfo snmp filter move	376
15.9.31	serverinfo snmp filter default	377
15.9.32	serverinfo time ip tcp	378
15.9.33	serverinfo time ip udp	379
15.9.34	serverinfo time filter	380
15.9.35	serverinfo time filter move	381
15.9.36	serverinfo time filter default	382
第 16 章	モード 操作コマンド/ターミナル操作コマンド	383
16.1	モード 操作	384
16.1.1	admin	384
16.1.2	su	386
16.1.3	exit	388
16.1.4	configure	389
16.1.5	end	390
16.1.6	quit	391
16.1.7	top	392
16.1.8	up	393
16.1.9	!	394
16.2	ターミナル操作	395
16.2.1	terminal pager	395
16.2.2	terminal window	398
16.2.3	terminal charset	399
16.2.4	terminal prompt	400
16.2.5	terminal timestamp	402
16.2.6	terminal bell	403
16.2.7	terminal logging	404
16.2.8	show terminal	405
16.3	コマンド実行履歴	406
16.3.1	show logging command	406
16.3.2	clear logging command	407
16.4	コマンドエイリアス	408
16.4.1	alias	408
16.4.2	show alias	410

16.4.3	clear alias	411
16.5	コマンド出力操作	412
16.5.1	more	412
16.5.2	tail	413
第 17 章	システム操作および表示コマンド	414
17.1	システム操作および表示	415
17.1.1	show system information	415
17.1.2	show system status	417
17.1.3	show tech-support	419
17.1.4	show logging error	420
17.1.5	clear logging error	422
17.1.6	show logging syslog	423
17.1.7	clear logging syslog	424
17.1.8	clear statistics	425
17.1.9	show date	426
17.1.10	date	427
17.1.11	rdate	428
17.1.12	reset	429
第 18 章	構成定義情報の表示、削除、および操作コマンド	430
18.1	構成定義情報表示	431
18.1.1	show candidate-config	431
18.1.2	show running-config	432
18.1.3	show startup-config	433
18.1.4	diff	434
18.2	構成定義情報削除	435
18.2.1	delete	435
18.3	構成定義情報操作	436
18.3.1	load	436
18.3.2	save	438
18.3.3	commit	439
18.3.4	discard	440
18.4	ファイル操作コマンド	442
18.4.1	dir	442
18.4.2	copy	444
18.4.3	remove	445
18.4.4	rename	446
18.4.5	format	447
第 19 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	448
19.1	Ethernet のカウンタ・ログ・統計・状態などの表示	449
19.1.1	show ether	449
19.1.2	show ether statistics	452
19.2	Ethernet のカウンタ・ログ・統計などのクリア	456
19.2.1	clear ether statistics	456

第 20 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	457
20.1	無線 LAN モジュールのカウンタ・ログ・統計・状態などの表示	458
20.1.1	show ieee80211 statistics	458
20.1.2	show ieee80211 status	462
20.2	無線 LAN モジュールのカウンタ・ログ・統計などのクリア	466
20.2.1	clear ieee80211 statistics	466
20.3	周辺アクセスポイント情報の取得、表示	467
20.3.1	show ieee80211 apscan	467
第 21 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	472
21.1	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	473
21.1.1	show wlan sta	473
21.1.2	show wlan ap	478
21.1.3	show wlan statistics	483
21.1.4	show wlan status	487
21.1.5	show wlan wpa status	492
21.1.6	show wlan wpa statistics	494
21.1.7	show wlan relay status	497
21.1.8	show wlan supplicant status	499
21.1.9	show wlan supplicant statistics	503
21.1.10	show wlan blockack session	505
21.2	無線 LAN 接続のカウンタ・ログ・統計などのクリア	507
21.2.1	clear wlan statistics	507
21.2.2	clear wlan wpa statistics	508
21.2.3	clear wlan relay table	509
21.2.4	clear wlan supplicant statistics	510
第 22 章	POE のログ・状態などの表示コマンド	511
22.1	POE のログ・状態などの表示	512
22.1.1	show poe drawing	512
第 23 章	USB 接続のカウンタ・ログ・統計・状態などの表示コマンド	513
23.1	USB 接続のカウンタ・ログ・統計・状態などの表示	514
23.1.1	show usb hcd status	514
23.1.2	show usb storage status	515
第 24 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	519
24.1	インタフェースのカウンタ・ログ・統計・状態などの表示	520
24.1.1	show interface	520
24.1.2	show interface brief	522
24.1.3	show interface summary	524
24.1.4	show interface detail	525
24.1.5	show interface statistics	528
24.2	インタフェースのカウンタ・ログ・統計・状態などのクリア	530
24.2.1	clear interface statistics	530
第 25 章	ARP エントリの表示、クリア操作コマンド	531
25.1	ARP エントリの表示	532
25.1.1	show arp	532
25.2	ARP エントリのクリア	534
25.2.1	clear arp	534

第 26 章	ルーティングテーブル情報・統計などの表示コマンド	535
26.1	IPv4 ルーティングテーブル情報・統計などの表示	536
26.1.1	show ip route	536
26.1.2	show ip route summary	538
26.1.3	show ip route kernel	539
第 27 章	パケットの統計情報の表示、クリア操作コマンド	542
27.1	パケットの統計情報の表示	543
27.1.1	show ip traffic	543
27.2	パケットの統計情報のクリア	546
27.2.1	clear ip traffic	546
第 28 章	DHCP のカウンタ・ログ・統計・状態などの表示コマンド	547
28.1	IPv4 DHCP のカウンタ・ログ・統計・状態などの表示	548
28.1.1	show ip dhcp	548
第 29 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	550
29.1	ブリッジのカウンタ・ログ・統計・状態などの表示	551
29.1.1	show bridge	551
29.2	ブリッジのカウンタ・ログ・統計・状態などのクリア	553
29.2.1	clear bridge	553
第 30 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	555
30.1	VLAN のカウンタ・ログ・統計・状態などの表示	556
30.1.1	show vlan	556
30.2	VLAN フィルタのカウンタ・ログ・統計・状態などの表示、クリア	559
30.2.1	show vlan filter	559
30.2.2	show vlan filter statistics	561
30.2.3	show vlan filter summary	562
30.2.4	clear vlan filter statistics	563
30.3	IDS のカウンタ・ログ・統計・状態などの表示、クリア	564
30.3.1	show vlan ids statistics	564
30.3.2	clear vlan ids statistics	567
第 31 章	SSH のカウンタ・ログ・統計・状態などの表示コマンド	568
31.1	SSH のカウンタ・ログ・統計・状態などの表示	569
31.1.1	show ssh server key	569
第 32 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	571
32.1	認証成功端末情報のカウンタ・ログ・統計・状態などの表示	572
32.1.1	show auth port	572
32.2	IEEE802.1X 認証のカウンタ・ログ・統計・状態などの表示	574
32.2.1	show dot1x port	574
32.2.2	show dot1x statistics port	577
32.2.3	show dot1x backup port	579
32.3	IEEE802.1X 認証のカウンタ・ログ・統計などのクリア	581
32.3.1	clear dot1x statistics	581
32.4	MAC アドレス認証のカウンタ・ログ・統計・状態などの表示	582
32.4.1	show macauth port	582
32.4.2	show macauth statistics port	584
32.5	MAC アドレス認証のカウンタ・ログ・統計などのクリア	586
32.5.1	clear macauth statistics	586

32.6	Wake On LAN パケットの統計情報の表示	587
32.6.1	show wol statistics	587
32.7	Wake On LAN パケットの統計情報のクリア	588
32.7.1	clear wol statistics	588
第 33 章	AAA 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	589
33.1	AAA のカウンタ・ログ・統計・状態などの表示	590
33.1.1	show aaa radius client server-info	590
33.1.2	show aaa radius client statistics	592
33.2	AAA のカウンタ・ログ・統計などのクリア	594
33.2.1	clear aaa radius client statistics	594
第 34 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	595
34.1	NETTIME(time/sntp) 統計情報の表示	596
34.1.1	show nettime statistics	596
34.2	NETTIME(time/sntp) 統計情報のクリア	598
34.2.1	clear nettime statistics	598
第 35 章	ProxyARP 情報の表示、クリア操作コマンド	599
35.1	ProxyARP 情報の表示	600
35.1.1	show proxyarp	600
35.1.2	show proxyarp statistics	601
35.2	ProxyARP 統計情報のクリア	602
35.2.1	clear proxyarp statistics	602
第 36 章	SNMP 統計情報の表示、クリア操作コマンド	603
36.1	SNMP 統計情報の表示	604
36.1.1	show snmp statistics	604
36.2	SNMP 統計などのクリア	607
36.2.1	clear snmp statistics	607
第 37 章	ソケット状態の表示コマンド	608
37.1	ソケット状態の表示	609
37.1.1	show socket	609
第 38 章	トレースの表示、クリア操作コマンド	613
38.1	トレースの表示	614
38.1.1	show trace ssh	614
38.2	トレースのクリア	616
38.2.1	clear trace ssh	616
第 39 章	証明書関連の表示コマンド	617
39.1	証明書関連の表示	618
39.1.1	show crypto certificate	618
第 40 章	管理機器の設定、ログ、状態などの表示コマンド	625
40.1	管理機器の設定、ログ、状態などの表示	626
40.1.1	show nodemanager group	626
40.1.2	show nodemanager node	627
40.1.3	show nodemanager update wlan filterset	633
40.1.4	show nodemanager node brief	634
40.1.5	show nodemanager logging wlan scan unmanaged	635

40.1.6	show nodemanager logging wlan scan	637
40.1.7	show nodemanager logging wlan scan managed brief	640
40.1.8	show nodemanager logging wlan scan managed	641
40.1.9	show nodemanager logging wlan scan unknown	646
40.1.10	show nodemanager logging wlan sta	648
40.1.11	show nodemanager logging wlan sta rssi	653
40.1.12	show nodemanager logging wlan reject	655
40.1.13	show nodemanager logging wlan trace	658
第 41 章	ポート制御コマンド	661
41.1	ポート制御	662
41.1.1	offline	662
41.1.2	online	664
第 42 章	無線 LAN 制御コマンド	666
42.1	無線 LAN 制御	667
42.1.1	wlanctl authenticator disconnect	667
第 43 章	USB ポート制御コマンド	668
43.1	USB ポート制御	669
43.1.1	usbctl	669
第 44 章	IEEE802.1X 制御コマンド	670
44.1	IEEE802.1X 制御	671
44.1.1	dot1xctl initialize	671
44.1.2	dot1xctl reconfirm	672
44.1.3	dot1xctl backup recovery	673
第 45 章	MAC アドレス認証制御コマンド	674
45.1	MAC アドレス認証制御	675
45.1.1	macauthctl initialize	675
第 46 章	RADIUS 制御コマンド	676
46.1	RADIUS 制御	677
46.1.1	radius recovery	677
第 47 章	証明書関連制御コマンド	678
47.1	証明書関連の制御	679
47.1.1	crypto certificate generate	679
47.1.2	crypto certificate local	683
47.1.3	crypto certificate ca	685
第 48 章	管理機器制御コマンド	687
48.1	管理機器制御	688
48.1.1	nodemanagerctl update wlan filterset	688
48.1.2	nodemanagerctl wlan autotxpower	690
48.1.3	nodemanagerctl wlan autochannel	693
48.1.4	nodemanagerctl reset	696
48.2	監視ログクリア	698
48.2.1	clear nodemanager logging	698
48.2.2	clear nodemanager logging wlan	699
48.2.3	clear nodemanager logging wlan sta	700

第 49 章	I'm here コマンド	701
49.1	I'm here コマンド	702
49.1.1	iamhere	702
第 50 章	その他のコマンド	703
50.1	その他	704
50.1.1	ping	704
50.1.2	traceroute	706
50.1.3	telnet	708
第 51 章	commit コマンド 実行時の影響について	710
索引		715

第1章 パスワード情報

1.1 password format

[機能]

暗号化パスワード 文字列形式の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

password format <format>

[オプション]

<format>

暗号化パスワード 形式

- common
共通パスワード 形式
他装置でも使用可能な暗号化パスワード 文字列。
- unique
装置固有パスワード 形式
本装置でのみ使用可能な暗号化パスワード 文字列。

[動作モード]

構成定義モード (管理者クラス)

[説明]

構成定義の各種パスワード項目に平文でパスワード文字列を設定すると、暗号化パスワード文字列に変換されます。show コマンドおよびsave コマンドを実行したとき、暗号化パスワード文字列に"encrypted"の文字列を付加した形式で表示および保存されます。

本コマンドでは、表示および保存するときの暗号化パスワード文字列形式を設定します。本設定は、構成定義のすべてのパスワード項目に対して有効です。本コマンドは、設定した直後に有効となります。

common に設定した場合、暗号化パスワード文字列は各装置で同じ共通パスワード形式になります。故障などにより装置交換した場合は、共通パスワード形式で保存してある構成定義を交換後の装置に復元することができます。common に設定した状態では、平文または共通パスワード形式のパスワード文字列を設定できます。装置固有パスワード形式のパスワード文字列は設定できません。

unique に設定した場合、暗号化パスワード文字列は装置ごとに異なる装置固有パスワード形式になります。装置固有パスワード形式で表示および保存した構成定義は、その装置にしか設定および復元することができません。本装置が故障するなどして代替装置に交換した場合は、保存しておいた構成定義をそのまま復元できなくなります。装置に保存した構成定義を代替装置に復元する必要がある場合は、共通パスワード形式で作成した構成定義ファイルを別の場所に保管しておいてください。

unique に設定した状態では、平文、共通パスワード形式およびその装置で表示した装置固有パスワード形式のパスワード文字列を設定できます。

TPM(Trusted Platform Module) が実装されている装置で unique に設定した場合、TPM を利用した装置固有パスワード形式になります。なお、unique に設定する際に TPM が正常か検査され、ハードエラーを検出した場合は以下のメッセージが出力されて設定は common になります。

```
<ERROR> detected HARD ERROR, cannot execute
```

[注意]

unique に設定すると、common に再設定したり本設定を削除することはできません。common に再設定したい場合は、reset clear コマンドを実行して工場出荷時設定に戻してから、構成定義を設定し直してください。

unique に設定したとき、設定済みのパスワード項目はすべて装置固有パスワード形式に変換されて表示および保存されます。

[未設定時]

common が設定されたものとみなされます。

```
password format common
```

1.2 password admin set

[機能]

管理者パスワードの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。また、admin コマンドを実行して管理者になる場合にも本コマンドで設定した管理者パスワードの入力が必要になります。

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。

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。

ログインユーザ情報に、装置内の AAA ユーザ情報 (aaa user id コマンド) または RADIUS サーバのユーザ情報を利用する場合でも、管理者パスワードが設定されている必要があります。

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 admin、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。

1.3 password user set

[機能]

一般ユーザパスワードの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

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]

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。
一般ユーザパスワードでログインした場合、terminal コマンドと alias コマンドで設定した内容は保存されず、admin コマンド実行時やログアウト時に設定した内容が破棄されます。
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 admin、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。

1.4 password nodemgr set

[機能]

無線 LAN 管理パスワードの設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

password nodemgr 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]

無線 LAN 管理機能が本装置にリモートログインするとき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。

本コマンドは設定した直後に有効となります。

[注意]

本パスワードを設定しなくても、本装置に nodemanager login service enable を設定することで、無線 LAN 管理装置から本装置をリモート管理できます。

本パスワードを設定した場合、無線 LAN 管理装置の管理機器情報にも同じパスワードを設定してください。

無線 LAN 管理用アカウントは、通常のログインアカウントとは動作が異なります。

以下に通常アカウントとの相違点を示します。

- telnet 接続および ssh 接続でのみログインできます。
- syslog logging nodemgr access コマンドにより、ログイン、ログアウトおよびコマンド実行のシスログ出力を抑制できます。
- コマンド入力プロンプトが"nodemgr#"に固定されます。
- terminal 設定は無視されます。
- コマンド実行履歴には管理者がコマンド実行したものとして記録されます。

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。

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 nodemgr's password: contain at least 8 characters

パスワードが7文字以下です。
8文字以上のパスワードを設定してください。

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

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 admin、load、discard コマンド実行時にも表示されます。

[未設定時]

無線 LAN 管理用パスワードを設定しないものとみなされます。

1.5 password aaa

[機能]

ログインユーザの AAA 情報の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
ログインする際の権限クラスは、以下のとおり決定します。

- RADIUS サーバを使用する場合
RADIUS サーバに登録された Filter-ID アトリビュートで決定します。
"administrator"であれば管理者クラス、"user"であれば一般ユーザクラスとなります。
- 本装置内のユーザ情報を使用する場合
AAA 情報に登録されている権限クラス (aaa user user-role) で決定します。

[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。

RADIUS サーバまたは本装置内のユーザ情報に権限クラスの設定がない場合は、正しい ID とパスワード
が入力された場合でも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。

1.6 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

- 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	10/100BASE-TX/1000BASE-T
SR-M20AP2 SR-M20AP1	ether 1 ~ 2
SR-M20AC2 SR-M20AC1	ether 1

- ポート番号の範囲指定について

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) には、以下のように複数ポートを範囲指定することができます。

- SR-M20AP2/20AP1 での複数ポート 範囲指定例

1	= port1
1-2	= port1 ~ port2
1,2	= port1,port2
-2	= port1 ~ port2

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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。
- 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。

[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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、1Gbps/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	
1000, 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[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-M20AP2	SR-M20AP1		
-----------	-----------	--	--

[入力形式]

ether <number> type normal
ether <number> type backup <group> <priority>

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

normal :通常ポート

backup :バックアップポート (SR-M20AP2/20AP1 のみ)

<group>

- グループ番号
バックアップグループ番号を、10進数で指定します。

範囲	機種
1	SR-M20AP2 SR-M20AP1

<priority>

- ポートの優先度
backup を指定したときに、優先ポートまたは待機ポートのどちらかを指定します。

master :優先ポート

backup :待機ポート

[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。
通常ポートまたはバックアップポートから選択します。

[注意]

backup 指定時の注意

バックアップグループに master または backup ポートが未定義の場合、該当グループのポートはリンクアップせず使用できません。

[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]



[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 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。
- ポート種別が通常ポートの場合、複数のポートに同一の VLAN ID を設定することができません。
設定された場合は、ポート番号の小さい方だけが有効となります。

[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-M20AP2 SR-M20AP1

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 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。
- ポート種別が通常ポートの場合、複数のポートに同一の VLAN ID を設定することができません。
設定された場合は、ポート番号の小さい方だけが有効となります。

[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]



[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 ポートの種別がバックアップポートであり、バックアップグループ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の閉塞解除動作の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 backup mode

[機能]

バックアップポートの使用ポート選択方法の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

backup <group> mode <mode>

[オプション]

<group>

- バックアップグループ番号
バックアップグループ番号を、10進数で指定します。

範囲	機種
1	SR-M20AP2 SR-M20AP1

<mode>

master ポートと backup ポートの両方が使用可能なときに使用するポートの選択方法を指定します。

master: master ポートを優先的に使用します。

earlier: 先にリンクアップして使用可能になったポートを使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

バックアップグループごとに使用ポートの選択方法を設定します。

[未設定時]

バックアップの切り替えモードとして master ポートを優先的に使用するよう設定されたものとみなされます。

```
backup <group> mode master
```

2.1.13 backup standby

[機能]

バックアップポートの待機状態の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

backup <group> standby <mode>

[オプション]

<group>

- バックアップグループ番号
バックアップグループ番号を、10進数で指定します。

範囲	機種
1	SR-M20AP2 SR-M20AP1

<mode>

バックアップポートの待機状態を指定します。

online : 待機状態であってもバックアップポートを閉塞しません。

offline : 待機状態でバックアップポートを閉塞します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

バックアップポートの待機状態を設定します。

待機状態を **offline** と指定した場合に、待機状態のバックアップポートを閉塞します。

閉塞となったポートの状態は Ethernet ポート制御コマンドの **offline** を実行した状態と同じです。

また、稼動しているバックアップポートがダウンすると閉塞解除を実行します。

閉塞解除を実行したポートがほかの機能により閉塞されていたり、異常が発生していなければ切り替わります。

[注意]

- バックアップポートの使用ポート選択方法が **master** と設定されている場合に、待機状態でバックアップポートを閉塞する設定としても、バックアップの優先ポートは閉塞しません。
バックアップの優先ポートを閉塞させたい場合は、バックアップポートの使用ポート選択方法を **earlier** に設定してください。
- 待機状態でバックアップポートを閉塞する設定とした場合に、バックアップポート機能以外が閉塞したポートを自動で閉塞解除しません。**offline** コマンドで閉塞したポートである場合も同じです。

[未設定時]

バックアップポートの待機状態として `online` が設定されたものとみなされます。

```
backup <group> standby online
```


2.1.14 backup downrelay wlan

[機能]

バックアップポートのリンクダウンリレー機能の連携動作無線 LAN インタフェースリストの設定

[適用機種]



[入力形式]

backup <group> downrelay wlan <wlanlist>

[オプション]

<group>

- バックアップグループ番号
バックアップグループ番号を、10 進数で指定します。

範囲	機種
1	SR-M20AP2 SR-M20AP1

<wlanlist>

- 無線 LAN インタフェースリスト
本定義を設定したバックアップ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]

本定義を設定したバックアップポートの稼働ポートがリンクダウンし、かつ待機ポートがスタンバイ状態以外の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]

- 本機能はバックアップポートの稼働ポートがリンクダウンし、かつ待機ポートがリンクアップ状態でないことを条件に動作するため、バックアップポートの待機状態を online に設定してください。
- 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 ポートの種別がバックアップポートであり、設定しているバックアップ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。
- 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。

2.1.15 backup downrelay recovery mode

[機能]

バックアップポートのリンクダウンリレー機能の閉塞解除動作の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

backup <group> downrelay recovery mode <mode>

[オプション]

<group>

- バックアップグループ番号
バックアップグループ番号を、10 進数で指定します。

範囲	機種
1	SR-M20AP2 SR-M20AP1

<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ず。

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

2.2 IEEE802.1X 認証情報

2.2.1 ether dot1x use

[機能]

ether ポートの IEEE802.1X 認証の設定

[適用機種]

 SR-M20AC2 SR-M20AC1

[入力形式]

ether <number> dot1x 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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 認証を行うために、AAA ユーザ情報、RADIUS 情報を設定しておく必要があります。
また、本コマンドと同時に、ether dot1x aaa <group_id>で認証先データベースの指定を行ってください。
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-M20AC2 SR-M20AC1		

[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。

```
ether <number> dot1x use off
```

2.2.2 ether dot1x portcontrol

[機能]

ether ポートの IEEE802.1X 認証状態の設定

[適用機種]



[入力形式]

```
ether <number> dot1x portcontrol <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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

デフォルト認証状態を指定します。

- auto
認証結果によりポートアクセス制御を行います。
- force-unauth
常に認証拒否します。
- force-auth
常に認証許容します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ポートのデフォルト認証状態を設定します。

[注意]

デフォルト認証状態として auto 以外を指定した場合、以下のような挙動となります。

- force-unauth が指定された場合
すべての通信が遮断されるため、利用できなくなります。
- force-auth が指定された場合
すべての通信が透過されるため、正規ユーザとして登録されていない端末 (Supplicant) でも常に利用が可能となります。

[未設定時]

端末 (Supplicant) からの認証情報を基にポートアクセス制御を行うものとみなされます。

```
ether <number> dot1x portcontrol auto
```

2.2.3 ether dot1x quietperiod

[機能]

ether ポートの認証失敗時再認証抑止時間の設定

[適用機種]

 SR-M20AC2 SR-M20AC1

[入力形式]

ether <number> dot1x quietperiod <time>

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

認証失敗後の再認証開始時間を 0 ~ 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。
0 秒を指定した場合は、認証失敗後の再認証抑止なしに即座に認証要求を受け付けます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

認証が拒否された端末 (Supplicant) との再認証を開始するまでの時間を設定します。

[未設定時]

認証失敗後、再認証を開始するまでの時間として 60 秒 (1 分) が設定されたものとみなされます。

```
ether <number> dot1x quietperiod 1m
```


2.2.4 ether dot1x txperiod

[機能]

ether ポートの認証開始要求送信待ち時間の設定

[適用機種]



[入力形式]

ether <number> dot1x txperiod <time>

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<time>

認証開始要求の送信待ち時間を 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]

ユーザ ID 要求の送信間隔を設定します。

[未設定時]

ユーザ ID 要求の送信間隔として 30 秒が設定されたものとみなされます。

```
ether <number> dot1x txperiod 30s
```

2.2.5 ether dot1x supptimeout

[機能]

ether ポートの EAP 応答待ち時間の設定

[適用機種]

 SR-M20AC2 SR-M20AC1

[入力形式]

ether <number> dot1x supptimeout <time>

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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]

端末 (Supplicant) に対する EAP 応答待ち時間を設定します。

[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。

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

2.2.6 ether dot1x maxreq

[機能]

ether ポートの EAP 再送回数の設定

[適用機種]

 SR-M20AC2 SR-M20AC1

[入力形式]

ether <number> dot1x maxreq <count>

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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]

EAP 応答が受信できない場合の EAP 再送回数を指定します。

[未設定時]

EAP 再送回数として 2 回が設定されたものとみなされます。

```
ether <number> dot1x maxreq 2
```

2.2.7 ether dot1x reauthperiod

[機能]

ether ポートの再認証間隔の設定

[適用機種]



[入力形式]

```
ether <number> dot1x reauthperiod <time>
```

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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、ポートのリンク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 15 ~ 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。

[注意]

短い再認証間隔設定で同時に複数ポートに対する再認証を行った場合、認証処理が完了する前に再認証処理が起動され認証が失敗することがあります。

[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。

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

2.2.8 ether dot1x aaa

[機能]

ether ポートの参照する AAA 情報の設定

[適用機種]



[入力形式]

```
ether <number> dot1x aaa <group_id>
```

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 認証の認証時参照する 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。

[未設定時]

AAA 情報を使用しないものとみなされます。

```
ether <number> dot1x aaa unuse
```

2.2.9 ether dot1x wol

[機能]

ether ポートの Wake On LAN パケット転送モードの設定

[適用機種]



[入力形式]

ether <number> dot1x wol <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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- enable
Wake On LAN パケットの転送を有効にします。
- disable
Wake On LAN パケットの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]

IEEE802.1X 認証ポートでの Wake On LAN パケット転送モードを設定します。
本機能を設定することにより、認証ポートに認証済み端末が存在しない場合でも Wake On LAN パケットを転送することができます。
同一ポートで、IEEE802.1X 認証と MAC アドレス認証を併用している場合、どちらかの設定で Wake On LAN パケット転送モードを有効とすることで Wake On LAN パケット転送モードが有効となります。

[未設定時]

IEEE802.1X 認証ポートでの Wake On LAN パケット転送モードが無効と設定されたものとみなされます。

```
ether <number> dot1x wol disable
```

2.3 MAC アドレス認証情報

2.3.1 ether macauth use

[機能]

ether ポートの MAC アドレス認証使用の設定

[適用機種]



[入力形式]

ether <number> macauth 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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 アドレス認証機能について設定します。
<mode>が on の場合、パケット送信元端末の MAC アドレス認証を行い、認められた MAC アドレスである場合に転送を行い、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]

MAC アドレス認証を行うために、AAA ユーザ情報、RADIUS 情報を設定しておく必要があります。
また、本コマンドと同時に、ether 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。
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-M20AC2 SR-M20AC1		

[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。

```
ether <number> macauth use off
```


2.3.2 ether macauth aaa

[機能]

ether ポートの 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]



[入力形式]

```
ether <number> macauth aaa <group_id>
```

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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 の指定がないものとして動作します。

```
ether <number> macauth aaa unuse
```

2.3.3 ether macauth authenticated-mac

[機能]

ether ポートの MAC アドレス認証不要端末アドレスの設定

[適用機種]



[入力形式]

ether <number> macauth authenticated-mac <count> <macaddr>

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<count>

- 定義番号
0 ~ 99 の 10 進数で指定します。

<macaddr>

- 認証不要端末 MAC アドレス
認証しないで通信を許可する 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]

構成定義モード (管理者クラス)

[説明]

MAC アドレス認証ポートで認証しないで通信を許可する端末 (プリンタなど) を設定します。

[注意]

- MAC アドレス認証が無効な場合に、設定は無効となります。
- <macaddr>に、00:00:00:00:00:00 およびブロードキャスト、マルチキャストは指定できません。
- 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]

設定されなかったものとして動作します。

2.3.4 ether macauth expire

[機能]

ether ポートの MAC アドレス認証結果保持時間の設定

[適用機種]



[入力形式]

ether <number> macauth expire <success_time> <failure_time>

[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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<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。

[注意]

認証成功および認証失敗保持時間の監視は 30 秒間隔で行っているため、最大 30 秒までの誤差が生じます。

[未設定時]

MAC アドレス認証結果保持時間として認証成功保持時間 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。

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

2.3.5 ether macauth wol

[機能]

ether ポートの Wake On LAN パケット転送モードの設定

[適用機種]



[入力形式]

ether <number> macauth wol <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。
複数の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")。
ポート番号の指定方法の詳細については、本章の冒頭を参照してください。

<mode>

- enable
Wake On LAN パケットの転送を有効にします。
- disable
Wake On LAN パケットの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]

MAC アドレス認証ポートでの Wake On LAN パケット転送モードを設定します。
本機能を設定することにより、認証ポートに認証済み端末が存在しない場合でも Wake On LAN パケットを転送することができます。
同一ポートで、MAC アドレス認証と IEEE802.1X 認証を併用している場合、どちらかの設定で Wake On LAN パケット転送モードを有効とすることで Wake On LAN パケット転送モードが有効となります。

[未設定時]

MAC アドレス認証ポートでの Wake On LAN パケット転送モードが無効と設定されたものとみなされます。

```
ether <number> macauth wol disable
```

第 3 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。

範囲	機種
1 ~ 2	SR-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

3.1 無線 LAN モジュール情報

3.1.1 ieee80211 use

[機能]

無線 LAN モジュールの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 インタフェース番号、および無線通信モード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インタフェース番号	無線通信モード
ieee80211 1	wlan 1 ~ 8	11b, 11b/g, 11b/g/n, 11g, 11g/n
ieee80211 2	wlan 9 ~ 16	11a
	wlan 9 ~ 12	11a/n

SR-M20AC2/20AC1 の場合は、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インタフェース番号	無線通信モード
ieee80211 1	wlan 1	11b, 11b/g, 11b/g/n, 11a, 11a/n

[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
```

3.1.2 ieee80211 mode

[機能]

無線通信モードの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
- 11g
IEEE802.11g で通信を行います。
SR-M20AC2/20AC1 では設定できません。
- 11g/n
IEEE802.11g または IEEE802.11n で通信を行います。
SR-M20AC2/20AC1 では設定できません。
- 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。

[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 を設定します。
SR-M20AP2/20AP1 の場合は、無線 LAN モジュール番号ごとに指定できる通信モードが異なります。
無線 LAN モジュール番号、無線 LAN インタフェース番号、および無線通信モード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インタフェース番号	無線通信モード
ieee80211 1	wlan 1 ~ 8	11b, 11b/g, 11b/g/n, 11g, 11g/n
	wlan 9 ~ 16	11a
ieee80211 2	wlan 9 ~ 12	11a/n

SR-M20AC2/20AC1 の場合は、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インタフェース番号	無線通信モード
ieee80211 1	wlan 1	11b, 11b/g, 11b/g/n, 11a, 11a/n

[注意]

11a または 11a/n の W53(52、56、60、64) チャンネル、W56(100、104、108、112、116、120、124、128、132、136、140) 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。

3.1.3 ieee80211 channel

[機能]

無線 LAN チャンネルの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
11b の場合、1 ~ 14 の範囲で指定します。
11b/g、11g、11b/g/n、11g/n の場合、1 ~ 13 の範囲で指定します。
11a、11a/n 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

ieee80211 bandwidth <width> で40を設定した場合、140チャンネルは使用できません。

- 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 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 mode) 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。

[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
```

3.1.4 ieee80211 bandwidth

[機能]

帯域幅の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

[動作モード]

構成定義モード (管理者クラス)

[説明]

11n で使用する帯域幅を指定します。
40MHz の帯域幅を使用する場合、セカンダリチャネルオフセットの設定が必要となります。

[未設定時]

20MHz の帯域幅が設定されたものとみなされます。

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

3.1.5 ieee80211 secondary-channel

[機能]

セカンダリチャネルオフセットの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
セカンダリチャネルとしてプライマリチャネルより大きいチャンネル番号を使用します。
- below
セカンダリチャネルとしてプライマリチャ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ネルを使用しないものと判定します。
SR-M20AC1/SR-M20AC2 では本設定はできません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

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

プライマリチャネル番号 (無線 LAN チャンネル番号) とセカンダリチャ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
		below	1
	6	above	10
		below	2
	7	above	11
		below	3
	8	above	12
		below	4
	9	above	13
	below	5	
	10	below	6
	11	below	7
	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	

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、プライマリチャンネル番号を 5~9 に設定した場合、セカンダリチャンネルオフセットを auto に設定しても、必ず 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、11g/n または 11a/n 以外を使用、または ieee80211 bandwidth <width> で 20 を設定した場合、設定は意味を持ちません。

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

SR-M20AC1/AC2 の場合は帯域幅に 40 を設定し、無線 LAN チャンネル番号に any 以外を設定した場合、above/below のいずれかの設定が必須となります。

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]

SR-M20AP1/SR-M20AP2 の場合

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
```

SR-M20AC1/SR-M20AC2 の場合

セカンダリチャネルオフセットを設定しないものとみなされます。

3.1.6 ieee80211 chanlist

[機能]

スキャンチャンネルリストの設定

[適用機種]



[入力形式]

ieee80211 <number> chanlist <chanlist>

[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。

<chanlist>

- スキャンチャンネルリスト
スキャンを行うチャンネル番号を、10 進数で指定します。
複数のチャンネル番号を設定する場合、","(カンマ) で区切ります (例: "1,6,11")。
複数のチャンネル番号が続く場合、"-"(ハイフン) で区切ります (例: "1-11")。
11b の場合、1~14 の範囲で指定します。
11b/g、11b/g/n の場合、1~13 の範囲で指定します。
11a、11a/n 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

[動作モード]

構成定義モード (管理者クラス)

[説明]

アクセスポイントスキャンを行うチャンネル番号を設定します。
隣接するアクセスポイントのチャンネル番号が判明している場合、スキャンを行うチャンネルを限定することにより、スキャン時間を短縮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。
- 設定したチャンネルリストが通信モードに対応する設定範囲に一致しない場合、設定は無効となります。

[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。

3.1.7 ieee80211 sta limit

[機能]

接続可能台数の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[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 1～100 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過して無線 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、装置全体での合計が以下の値に収まるように設定してください。

最大接続可能合計台数	機種
100	SR-M20AP2 SR-M20AP1

また、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
```

3.1.8 ieee80211 protection mode

[機能]

11g プロテクションモードの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
衝突回避は行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

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。
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。
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、本機能を有効にすることで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 disable が設定されたものとみなされます。

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

3.1.9 ieee80211 ht-protection mode

[機能]

HT プロテクションモードの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

ieee80211 <number> ht-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
衝突回避は行いません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

11n/11a/11g/11b 混在環境での HT プロテクション (衝突回避) の設定を行います。
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]

11b との混在環境の場合、HT プロテクションモードと 11g プロテクションモードの設定を行い、衝突回避を行ってください。

[未設定時]

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

```
ieee80211 <number> ht-protection mode disable
```

3.1.10 ieee80211 rts threshold

[機能]

RTS しきい値の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

[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
```

3.1.11 ieee80211 dtim period

[機能]

DTIM 間隔の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[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
```

3.1.12 ieee80211 beacon interval

[機能]

ビーコン間隔の設定

[適用機種]

SR-M20AP2 SR-M20AP1 

[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 20 ~ 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。

[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
```

3.1.13 ieee80211 wmm mode

[機能]

WMM 優先制御の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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>

- auto
WMM 優先制御を有効とするかどうかを自動で判別します。
11n を含む無線通信モードを使用する場合には WMM 優先制御を有効にし、11n を含まない無線通信モードを使用する場合には WMM 優先制御を無効にします。
- 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。

[未設定時]

WMM 優先制御を有効とするかどうかを自動で判別するものとみなされます。

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

3.1.14 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```


3.1.15 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-M20AP2 SR-M20AP1

[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。

[注意]

無線 LAN インタフェースの動作タイプ設定に wds を設定した場合、または無線 LAN インタフェースの設定がない場合は、周辺アクセスポイント検出の動作モード設定は使用できません。

[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
```

3.1.16 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-M20AP2 SR-M20AP1

[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
```

3.1.17 ieee80211 txpower

[機能]

無線送信出力の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 1 ~ 36(0.5dBm 単位) の 10 進数で指定します。

無線通信モードが **11b** の場合

設定値	送信出力
1-13	4.0 [dBm]
14-19	7.0 [dBm]
20-25	10.0 [dBm]
26-31	13.0 [dBm]
32-36	16.0 [dBm]

無線通信モードが **11g**、**11b/g** の場合

設定値	送信出力
1-9	2.0 [dBm]
10-15	5.0 [dBm]
16-21	8.0 [dBm]
22-27	11.0 [dBm]
28-36	14.0 [dBm]

無線通信モードが **11a** の場合

設定値	送信出力
1-9	2.0 [dBm]
10-15	5.0 [dBm]
16-21	8.0 [dBm]
22-36	11.0 [dBm]

無線通信モードが **11g/n**、**11b/g/n** でチャンネルボンディングなし (20MHz) の場合

設定値	送信出力
1-9	2.0 [dBm]
10-15	5.0 [dBm]
16-21	8.0 [dBm]
22-27	11.0 [dBm]
28-36	14.0 [dBm]

無線通信モードが **11g/n**、**11b/g/n** でチャンネルボンディングあり (**40MHz**) の場合

設定値	送信出力
1-7	1.0 [dBm]
8-13	4.0 [dBm]
14-19	7.0 [dBm]
20-25	10.0 [dBm]
26-36	13.0 [dBm]

無線通信モードが **11a/n** 場合 (チャンネルボンディングあり/なし共)

設定値	送信出力
1-9	2.0 [dBm]
10-15	5.0 [dBm]
16-21	8.0 [dBm]
22-36	11.0 [dBm]

[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]

使用される送信出力値は設定した値よりも小さくなる場合があります。実際の送信出力値は、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 36(18dBm) が設定されたものとみなされます。

```
ieee80211 <number> txpower 36
```

3.1.18 ieee80211 antenna use

[機能]

無線 LAN アンテナの設定

[適用機種]

SR-M20AP2 SR-M20AP1 

[入力形式]

ieee80211 <number> antenna use <side>

[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。

<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。

```
ieee80211 <number> antenna use internal
```

3.1.19 ieee80211 noise-detect mode

[機能]

ノイズ回避機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

ieee80211 <number> noise-detect 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
ノイズ回避機能を有効にします。
- disable
ノイズ回避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]

ノイズ回避機能の有効または無効を設定します。本機能を有効にした場合は、ノイズを検出時に別のチャンネルを選択して移動します。

[注意]

チャンネル選択時に以下の構成定義が自動的に変更かつ反映 (commit コマンド実行) されます。

```
ieee80211 <number> channel <channel>
```

上記以外の編集時の構成定義があると自動的に反映される場合があるため、設定変更の際は十分に注意をお願いします。

ただし構成定義の保存 (save コマンド実行) は自動的には行いません。

wlan type に ap 以外が指定された無線 LAN インターフェースが 1 つでも存在していた場合は、本機能は動作しません。

チャンネル選択時に移動予定の全チャンネルでレーダーを検出していた場合は、ノイズを検出した場合であってもチャンネルの移動は行いません。

[未設定時]

ノイズ回避機能を無効にするものとみなされます。

```
ieee80211 <number> noise-detect mode disable
```

3.1.20 ieee80211 noise-detect channel layout

[機能]

ノイズ回避機能におけるチャンネル切り替え時のチャンネル移動間隔

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

ieee80211 <number> noise-detect channel layout <num>

[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。

<num>

- チャンネルシフト数
チャンネルシフト数を 1~5 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]

ノイズ回避機能におけるチャンネル切り替え時のチャンネル移動間隔を設定します。
ノイズ検出時にチャンネルを切り替えるときに、現在運用中のチャンネル番号から本機能で設定したチャンネルシフト数を加算したチャンネル番号に切り替えます。

[注意]

本設定は 2.4GHz 側でのみ有効になります。5GHz 側はチャンネルシフト数は 4 固定です。

[未設定時]

ノイズ回避機能におけるチャンネル切り替え時のチャンネル移動間隔に 5 が設定されたものとみなされます。

```
ieee80211 <number> noise-detect channel layout 5
```

第 4 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 ~ 16	SR-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

4.1 無線 LAN インタフェース情報

4.1.1 wlan use

[機能]

無線 LAN インタフェースの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 インタフェース番号、および無線通信モード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インタフェース番号	無線通信モード
ieee80211 1	wlan 1 ~ 8	11b, 11b/g, 11b/g/n, 11g, 11g/n
	wlan 9 ~ 16	11a
ieee80211 2	wlan 9 ~ 12	11a/n

SR-M20AC2/20AC1 の場合は、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インタフェース番号	無線通信モード
ieee80211 1	wlan 1	11b, 11b/g, 11b/g/n, 11a, 11a/n

[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
```

4.1.2 wlan description

[機能]

説明文の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

4.1.3 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]



[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。
- wds
WDS として動作します。
- scanonly
スキャン専用モードとして動作します。

[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。

[注意]

無線 LAN インタフェースの動作タイプ設定をスキャン専用モードに設定した場合、ほかの無線 LAN インタフェースの動作タイプ設定は無効となります。また、周辺アクセスポイント検出の動作モードが無効に設定されている場合、本設定は無効となります。

無線 LAN インタフェースの動作タイプ設定に wds を指定し、WDS ブリッジ機能を使用する場合は、WDS ブリッジの対向 MAC アドレスを設定してください。また、無線通信モードおよび無線 LAN チャンネルの設定を対向装置と一致させる必要があります。無線 LAN チャンネルには固定のチャンネル番号 (any 以外) を指定してください。

無線 LAN チャンネルに any を設定し、かつ無線 LAN モジュールに対し無線 LAN アクセスポイントとして動作する無線 LAN インタフェースが存在しない場合、WDS ブリッジの動作は開始されません。

レーダを検出した場合、一時的に通信ができなくなったり、30 分間動作を停止する場合があります。

WDS ブリッジを行う無線 LAN アクセスポイント間では、IEEE802.11n を使用することはできません。設定された場合、無線通信モードが 11a/n のときは 11a で動作し、無線通信モードが 11b/g/n および 11g/n のときは 11g で動作します。

[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
```

4.1.4 wlan ssid

[機能]

SSID の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 アクセスポイントおよび無線 LAN 端末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。

4.1.5 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-M20AP2 SR-M20AP1

[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
```

4.1.6 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-M20AP2 SR-M20AP1 

[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。(プライバシープロテクション機能)

[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
```


4.1.7 wlan auth

[機能]

IEEE802.11 認証モードの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
- wpa
WPA による IEEE802.1X 認証を行います。
- wpa-psk
WPA による事前共有キー (PSK) 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。

[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。

wpa-psk, wpa2-psk, wpa/wpa2-psk 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。

wpa, wpa2, wpa/wpa2 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。

[注意]

本装置は EAP 認証時に受信したデジタル証明書の有効期間を検証するため、システム時刻は正しく設定してください。ご購入時のシステム時刻のままの場合、証明書の有効期限の検証に失敗することがあります。11b/g/n, 11g/n, 11a/n 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
```

4.1.8 wlan wep mode

[機能]

WEP 使用の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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, 11g/n, 11a/n を指定した場合、WEP は使用できません。

[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
```

4.1.9 wlan wep key

[機能]

WEP キーの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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	hex 16進数キー	text 文字列キー
WEP キー長 (IV 除く)		
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 キーが入力範囲未満の場合は指定した WEP キー長を超えて近い WEP キー長と判断され、満たない部分は 0x0 でパディングされます。

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。

4.1.10 wlan wep send

[機能]

使用する WEP キーの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

4.1.11 wlan wep type

[機能]

WEP 動作タイプの設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

wlan <number> wep type <type> [<length>] [rekey <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。

<type>

使用する WEP キーの種別を指定します。

- static
wlan wep key, wlan wep send コマンドで設定された WEP キーを使用します。
- dynamic
RADIUS サーバから配布された鍵情報から WEP キーを生成して使用します。

<length>

使用する WEP キーの長さを指定します。

<type> に dynamic を指定した場合にだけ指定できます。

- 64
64 ビット
- 128
128 ビット
省略時は、128 を指定されたものとみなされます。

rekey <period>

- WEP キーの更新間隔を指定します。
<type> に dynamic を指定した場合にだけ指定できます。
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。
省略時は、10m を指定され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]

オープン認証 + IEEE802.1X 認証時に使用する WEP キーの動作タイプを設定します。

<type> が static の場合、コマンドで登録された静的なキーを使用します。

<type> が dynamic の場合、キーを動的に生成して使用します。

<type> が dynamic の場合、rekey で指定された更新間隔で unicast 用、broadcast 用の両方のキーを更新します。

[注意]

WEP キーの種別については、supplicant 側の設定と合わせてください。
設定が異なっている場合、接続中にもかかわらずパケット送受信ができないことがあります。
本コマンドは以下の条件を満たした場合のみ有効となります。

- wlan auth コマンドで <auth_algo> に open を指定
- wlan wep mode コマンドで <mode> に enable を指定
- wlan dot1x use コマンドで <mode> に on を指定
- dot1x use コマンドで <mode> に on を指定

[未設定時]

wlan wep key, wlan wep send コマンドで設定された WEP キーを使用するものとみなされます。

```
wlan <number> wep type static
```


4.1.12 wlan wpa cipher

[機能]

WPA/WPA2 暗号化モードの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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>

- tkip
TKIP 暗号化を行います。
- 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。

[動作モード]

構成定義モード (管理者クラス)

[説明]

WPA/WPA2 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 に関する設定がされているときに意味を持ちます。

[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。

- WPA の場合は TKIP 固定とします。
- WPA2 の場合は AES 固定とします。

11n を使用した通信を行う場合、TKIP 暗号化は使用できません。

[未設定時]

WPA/WPA2 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
```

4.1.13 wlan wpa psk

[機能]

WPA/WPA2 事前共有キーの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 (パスフレーズ) 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 で用いる事前共有キーを指定します。

[未設定時]

PSK は設定しないものとみなされます。

4.1.14 wlan wpa rekey group

[機能]

WPA/WPA2 のグループキー更新間隔の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[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 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 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
```

4.1.15 wlan wpa countermeasures

[機能]

MIC エラー検出の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

wlan <number> wpa countermeasures <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
MIC エラー検出を有効にします。
- disable
MIC エラー検出を無効にします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

TKIP 暗号を使用する際、パケットの改ざんを防ぐために MIC エラーを検出するかどうかを選択します。60 秒に 2 回以上の MIC エラーを検出した場合、接続断を行います。その後、無線 LAN インタフェースは 60 秒間保留状態となり、接続が行えない状態となります。60 秒経過後、接続できる状態に戻ります。

[注意]

アクセスポイントで動作し、60 秒に 2 回以上の MIC エラーを検出した場合、接続しているすべての無線 LAN 端末を切断し、保留状態となります。

[未設定時]

MIC エラー検出を無効にするものとみなされます。

```
wlan <number> wpa countermeasures disable
```

4.1.16 wlan wpa pmkcache mode

[機能]

PMK キャッシュ機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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となります。

[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
```

4.1.17 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
SR-M20AP2/20AP1 の場合、キャッシュ保持数の上限を 1～200 個の範囲で指定します。
SR-M20AC2/20AC1 の場合、キャッシュ保持数の上限を 1～10 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]

SR-M20AP2/20AP1 の場合、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
```

SR-M20AC2/20AC1 の場合、PMK キャッシュのキャッシュ保持数に 10 個が設定されたものとみなされます。

```
wlan <number> wpa pmkcache num 10
```

4.1.18 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```


4.1.19 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-M20AP2 SR-M20AP1

[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 応答待ち時間は以下コマンドの設定に従います。

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

4.1.20 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-M20AP2 SR-M20AP1

[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 再送回数は以下コマンドの設定に従います。

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

4.1.21 wlan supplicant dot1x use

[機能]

無線 LAN インタフェースの IEEE802.1X サブリカントでの認証の設定

[適用機種]**[入力形式]**

```
wlan <number> supplicant 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]

OPEN 認証または SHARD 認証で IEEE802.1X 認証を行う必要がある場合に設定してください。
IEEE802.1X 認証モードを有効にすると、認証が許可されるまで通信が遮断されます。

[注意]

本モードが有効と指定された場合でも、supplicant dot1x use 定義でシステム側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 認証モードを無効にするものとみなされます。

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

4.1.22 wlan supplicant eap protocol

[機能]

EAP プロトコルの設定

[適用機種]



[入力形式]

wlan <number> supplicant eap protocol <proto>

[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。

<proto>

EAP で使用するプロトコルを指定します。

- md5
EAP-MD5 を使用します。
- tls
EAP-TLS を使用します。
- ttls
EAP-TTLS を使用します。
- peap
EAP-PEAP 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]

EAP で使用するプロトコルを設定します。
EAP-TTLS, EAP-PEAP を使用する場合は、内部認証プロトコルの設定が必須となります。

[注意]

本装置は EAP 認証時に受信したデジタル証明書の有効期間を検証するため、システム時刻を正しく設定してください。ご購入時のシステム時刻のままの場合、証明書の有効期限の検証に失敗することがあります。

[未設定時]

EAP のプロトコルを使用しないものとみなされます。

4.1.23 wlan supplicant eap id

[機能]

EAP ID の設定

[適用機種]



[入力形式]

wlan <number> supplicant eap id <id> [anonymous_id <anonymous_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。

<id>

- ID
EAP で使用する ID を、0x21,0x23 ~ 0x7e の 64 文字以内の ASCII 文字列で指定します。

<anonymous_id>

- 匿名 ID
EAP で使用する匿名 ID 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]

EAP の ID、および匿名 ID を設定します。
匿名 ID は、EAP-TTLS で ID を隠匿するために使用します。
匿名 ID が省略されている場合、自動的に"anonymous"が使用されます。

[未設定時]

EAP の ID、および匿名 ID を設定しないものとみなされます。

4.1.24 wlan supplicant eap password

[機能]

EAP パスワードの設定

[適用機種]



[入力形式]

wlan <number> supplicant eap 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
EAP で使用するパスワードを、0x21,0x23 ~ 0x7e の 128 文字以内の ASCII 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文字列をそのまま正確に指定します。

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]

EAP で使用するパスワードを設定します。
show 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。

[未設定時]

EAP で使用するパスワードを設定しないものとみなされます。

4.1.25 wlan supplicant eap peapversion

[機能]

PEAP バージョンの設定

[適用機種]



[入力形式]

wlan <number> supplicant eap peapversion <version>

[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。

<version>

PEAP のバージョンを指定します。

- 0
PEAP をバージョン 0 で使用します。
- 1
PEAP をバージョン 1 で使用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

PEAP のバージョンを設定します。

[未設定時]

PEAP をバージョン 0 で使用するものとみなされます。

```
wlan <number> supplicant eap peapversion 0
```

4.1.26 wlan supplicant eap inner protocol

[機能]

EAP 内部認証プロトコルの設定

[適用機種]



[入力形式]

wlan <number> supplicant eap inner protocol <auth>

[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>

内部認証プロトコルを指定します。

- chap
内部認証プロトコルとして CHAP を使用します。
EAP-TTLS を使用する場合に指定できます。
- pap
内部認証プロトコルとして PAP を使用します。
EAP-TTLS を使用する場合に指定できます。
- mschapv2
内部認証プロトコルとして MSCHAPv2 を使用します。
EAP-TTLS,EAP-PEAP を使用する場合に指定できます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

EAP-TTLS, EAP-PEAP で使用する内部認証方式を設定します。

[未設定時]

内部認証方式を設定しないものとみなされます。

4.1.27 wlan supplicant certificate ca

[機能]

認証局証明書情報の設定

[適用機種]**[入力形式]**

wlan <number> supplicant certificate ca <cert_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。

<cert_number>

- 認証局証明書識別番号
認証局証明書の識別番号を、0~4 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]

認証局証明書情報の設定を行います。

[注意]

本装置は EAP 認証時に受信したデジタル証明書の有効期間を検証するため、システム時刻を正しく設定してください。ご購入時のシステム時刻のままの場合、証明書の有効期限の検証に失敗することがあります。

[未設定時]

認証局証明書情報を使用しないものとみなされます。

4.1.28 wlan supplicant certificate local

[機能]

自装置証明書情報の設定

[適用機種]



[入力形式]

wlan <number> supplicant certificate local <cert_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。

<cert_number>

- 自装置証明書識別番号
自装置証明書の識別番号を、0~4 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]

自装置証明書情報の設定を行います。

[注意]

本装置は EAP 認証時に受信したデジタル証明書の有効期間を検証するため、システム時刻を正しく設定してください。ご購入時のシステム時刻のままの場合、証明書の有効期限の検証に失敗することがあります。自装置証明書生成時に生成された秘密鍵の識別番号も合わせて設定してください。

[未設定時]

自装置証明書情報を使用しないものとみなされます。

4.1.29 wlan supplicant certificate private_key

[機能]

秘密鍵識別番号の設定

[適用機種]**[入力形式]**

wlan <number> supplicant certificate private_key <key_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。

<key_number>

秘密鍵識別番号を指定します。

- 秘密鍵識別番号
秘密鍵の識別番号を、0～4 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]

使用する秘密鍵の識別番号を設定します。

[注意]

本装置は EAP 認証時に受信したデジタル証明書の有効期間を検証するため、システム時刻を正しく設定してください。ご購入時のシステム時刻のままの場合、証明書の有効期限の検証に失敗することがあります。

[未設定時]

秘密鍵識別番号を設定しないものとみなされます。

4.1.30 wlan ampdu tx mode

[機能]

A-MPDU 送信モードの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

wlan <number> ampdu tx mode <mode>

[オプション]

<number>

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

<mode>

A-MPDU 送信モードを指定します。

- auto
A-MPDU 送信を有効とします。A-MPDU 送信動作を行うかどうかは自動で判別します。
時間あたりのパケット転送量が WMM の AC ごとに決められた固定値を上回った場合に、A-MPDU 送信動作を行います。
- disable
A-MPDU 送信を無効とします。
- always
A-MPDU 送信を有効とします。常に A-MPDU 送信動作を行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

11n で使用する A-MPDU 送信モードを指定します。

[未設定時]

A-MPDU 送信モードを有効とし、送信動作は自動判別するものとみなされます。

```
wlan <number> ampdu tx mode auto
```

4.1.31 wlan ampdu rx size

[機能]

A-MPDU 最大受信サイズの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

wlan <number> ampdu rx size <size>

[オプション]**<number>**

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

<size>

A-MPDU 最大受信サイズを指定します。

- 8
8 kbyte とします。
- 16
16 kbyte とします。
- 32
32 kbyte とします。
- 64
64 kbyte とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

11n で使用する A-MPDU 最大受信サイズを指定します。

[未設定時]

A-MPDU 最大受信サイズは 8 kbyte とみなされます。

```
wlan <number> ampdu rx size 8
```

4.1.32 wlan ampdu rx density

[機能]

A-MPDU 間隔の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

wlan <number> ampdu rx density <density>

[オプション]

<number>

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

<density>

受信可能な A-MPDU の最小間隔をナノ秒単位で指定します。

- 250, 500, 1000, 2000, 4000, 8000, 16000 (nsec)
指定された値となります。
- 0
no time restriction(時間制限なし) 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]

11n で使用する A-MPDU 間隔を指定します。

[未設定時]

A-MPDU 間隔は no time restriction とみなされます。

```
wlan <number> ampdu rx density 0
```

4.1.33 wlan guard-interval

[機能]

ガードインターバルの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 で使用するガードインターバルを指定します。

[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
```

4.1.34 wlan macfilter

[機能]

MAC アドレスフィルタの設定

[適用機種]

SR-M20AP2	SR-M20AP1		
-----------	-----------	--	--

[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。
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。

範囲	機種
0 ~ 99	SR-M20AP2 SR-M20AP1

<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。
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-M20AP2 SR-M20AP1

【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。

ACL 参照定義は、ほかの ACL 参照定義 (VLAN のフィルタ、アプリケーションフィルタなど) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
1800	SR-M20AP2 SR-M20AP1

【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。

4.1.35 wlan macfilter move

[機能]

MAC アドレスフィルタの優先順序の変更

[適用機種]



[入力形式]

```
wlan <number> macfilter move <count> <new_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>

- 対象フィルタリング定義番号
優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
<count>に対する新しい順序を、10 進数で指定します。
すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

範囲	機種
0 ~ 99	SR-M20AP2 SR-M20AP1

[動作モード]

構成定義モード (管理者クラス)

[説明]

MAC アドレスフィルタの優先順序を変更します。

4.1.36 wlan roaming mode

[機能]

ローミング動作の設定

[適用機種]

 SR-M20AC2 SR-M20AC1

[入力形式]

wlan <number> roaming mode <mode>

[オプション]**<number>**

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

<mode>

ローミング動作を指定します。

- disable
ローミング動作を無効とします。
- enable
ローミング動作を有効とします。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ローミング動作を指定します。

複数アクセスポイント間での受信信号強度や送信レートのしきい値によるローミングを有効とする場合、ローミング動作を有効にしてください。

[未設定時]

ローミング動作を無効にするものとみなされます。

```
wlan roaming mode disable
```

4.1.37 wlan roaming threshold bmiss

[機能]

ローミングビーコン喪失回数しきい値の設定

[適用機種]

 SR-M20AC2 SR-M20AC1

[入力形式]

wlan <number> roaming threshold bmiss <count>

[オプション]

<number>

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

<count>

ビーコン喪失回数のしきい値を 1～255 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]

ローミングの発生契機となるビーコン連続喪失回数のしきい値を指定します。
ビーコン連続喪失を検出した場合、次アクセスポイントへのローミングを開始します。

[未設定時]

ローミングビーコン喪失回数しきい値は、7 が設定されたものとみなされます。

```
wlan roaming threshold bmiss 7
```

4.1.38 wlan roaming threshold rssi

[機能]

ローミング受信信号強度しきい値の設定

[適用機種]

[入力形式]

```
wlan <number> roaming threshold rssi 11a <rssi_11a>
wlan <number> roaming threshold rssi 11b <rssi_11b>
wlan <number> roaming threshold rssi 11g <rssi_11g>
wlan <number> roaming threshold rssi 11n <rssi_11n>
```

[オプション]

<number>

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

<rssi_11a>

802.11a で動作する場合のローミング受信信号強度しきい値を、4～20 の 10 進数で指定します。

<rssi_11b>

802.11b で動作する場合のローミング受信信号強度しきい値を、4～20 の 10 進数で指定します。

<rssi_11g>

802.11g で動作する場合のローミング受信信号強度しきい値を、4～20 の 10 進数で指定します。

<rssi_11n>

802.11n で動作する場合のローミング受信信号強度しきい値を、4～20 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]

ローミングの発生契機となる受信信号強度しきい値を指定します。

受信信号強度によるローミングは、接続中のアクセスポイントから受信する受信信号強度 (RSSI) の過去 10 回までの平均値と、指定したしきい値を比較し、しきい値を下回った場合、次アクセスポイントへのローミングを開始します。

受信信号強度しきい値から dBm への変換方法は、以下のとおりとなります。

単位	変換式
dBm	(受信信号強度しきい値) - 95

[注意]

受信信号強度によるローミングを動作させる場合、ローミング動作を有効に設定してください。

[未設定時]

ローミング受信信号強度しきい値は、7 が設定されたものとみなされます。

```
wlan roaming threshold rssi 11a 7  
wlan roaming threshold rssi 11b 7  
wlan roaming threshold rssi 11g 7  
wlan roaming threshold rssi 11n 7
```

4.1.39 wlan roaming threshold rate

[機能]

ローミング送信レートしきい値の設定

[適用機種]

 SR-M20AC2 SR-M20AC1

[入力形式]

```
wlan <number> roaming threshold rate 11a <rate_11a>
wlan <number> roaming threshold rate 11b <rate_11b>
wlan <number> roaming threshold rate 11g <rate_11g>
wlan <number> roaming threshold rate 11n <rate_11n>
```

[オプション]

<number>

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

<rate_11a>

802.11a で動作する場合のローミング送信レートしきい値 (Mbps) を 6 ~ 54 の 10 進数で指定します。

<rate_11b>

802.11b で動作する場合のローミング送信レートしきい値 (Mbps) を 1 ~ 11 の 10 進数で指定します。

<rate_11g>

802.11g で動作する場合のローミング送信レートしきい値 (Mbps) を 1 ~ 54 の 10 進数で指定します。

<rate_11n>

802.11n で動作する場合のローミング送信レートしきい値 (Mbps) を 6 ~ 300 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]

ローミング送信レートしきい値の設定を行います。

送信レートによるローミングは、接続中のアクセスポイントに送信するデータより算出する送信レート値と、指定したしきい値を比較し、しきい値を下回った場合、次アクセスポイントへのローミングを開始します。

[注意]

送信レートによるローミングを動作させる場合、ローミング動作を有効に設定してください。

[未設定時]

ローミング送信レートしきい値に、以下のように設定されたものとみなされます。

```
wlan roaming threshold rate 11a 12
wlan roaming threshold rate 11b 2
wlan roaming threshold rate 11g 2
wlan roaming threshold rate 11n 13
```

4.1.40 wlan wmm aclmap

[機能]

WMM 優先制御の AC 分類条件の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

wlan <number> wmm aclmap <count> <action> <value> <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 AC 分類条件定義の優先順位を、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。
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。
指定した値の定義がすでに存在する場合は、既存の定義を変更します。

範囲

機種

0 ~ 99

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

<action>

- ac
アクセスコントロールリストの "acl ip" 定義に該当した入力パケットが出力される際に使用される AC (Access Category) を変更します。

<value>

- voice
AC_VO (音声) に分類されます。
- video
AC_VI (ビデオ) に分類されます。
- besteffort
AC_BE (ベストエフォート) に分類されます。
- background
AC_BK (バックグラウンド) に分類されます。

<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、その定義は無効となり、無視されます。

ACL の以下の定義を使用します。

- ip

ip 値が設定されていない場合、その定義は無効となり、無視されます。

範囲	機種
0 ~ 599	SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[動作モード]

構成定義モード (管理者クラス)

[説明]

条件に一致したパケットを、指定した AC に分類します。設定した優先度順に一致するか調べ、一致した時点で処理され、それ以降の設定は参照されません。どの条件にも一致しなかった場合は、以下のデフォルト条件を使用して分類されます。

DSCP値	AC
0x38 ~ 0x3f 0x30 ~ 0x37	AC_VO (音声)
0x28 ~ 0x2f 0x20 ~ 0x27	AC_VI (ビデオ)
0x18 ~ 0x1f 0x00 ~ 0x07	AC_BE (ベストエフォート)
0x10 ~ 0x17 0x08 ~ 0x0f	AC_BK (バックグラウンド)

ACL 参照定義は、ほかの ACL 参照定義 (VLAN のフィルタ、アプリケーションフィルタなど) を含めて本装置全体で以下の数まで定義できます。

最大定義数	機種
1800	SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[注意]

WMM 優先制御を使用しないときは無効となります。

WMM 優先制御をサポートしない無線 LAN 端末または無線 LAN アクセスポイントへのパケットは、AC_BE に分類します。

[未設定時]

AC 分類条件を設定しないものとみなされます。

4.1.41 wlan wmm aclmap move

[機能]

WMM 優先制御の AC 分類条件の優先順位変更

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

wlan <number> wmm aclmap move <count> <new_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>

- 移動対象優先順位
移動する優先順位の番号を、10 進数で指定します。

<new_count>

- 移動先優先順位
移動先優先順位の番号を、10 進数で指定します。

範囲	機種
0 ~ 99	SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[動作モード]

構成定義モード (管理者クラス)

[説明]

WMM 優先制御の AC 分類条件定義の優先順位を変更します。
現在の優先順位が<count>である定義を<new_count>の優先順位に変更します。
変更後は優先順位番号が順番にソートされてリナンバリングされます。

4.1.42 wlan sta guarantee

[機能]

最低保証台数の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[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 ~ 100 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。

4.1.43 wlan sta idle

[機能]

無通信切断時間の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[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
```

4.1.44 wlan wds neighbor

[機能]

WDSブリッジの対向 MAC アドレス設定

[適用機種]

SR-M20AP2	SR-M20AP1		
-----------	-----------	--	--

[入力形式]

wlan <number> wds neighbor <mac>

[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。

<mac>

- MAC アドレス
WDSブリッジの対向 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]

WDSブリッジ機能によって通信を行う対向 MAC アドレスを設定します。
WDSブリッジ機能を使用する場合は、本コマンドを必ず実行してください。

[注意]

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

[未設定時]

対向 MAC アドレスを設定しないものとみなされます。

4.1.45 wlan relay mode

[機能]

無線 LAN 中継機能の動作モードの設定

[適用機種]



[入力形式]

wlan [<number>] relay 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>

無線 LAN 中継機能の動作モードを指定します。

- single
シングルクライアントモードで動作します。
- multi
マルチクライアントモードで動作します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

無線 LAN 中継機能の動作モードを指定します。

複数のノードを同時に収容する場合、マルチクライアントモードを指定してください。ただし、マルチクライアントモードに設定した場合、中継可能なフレームは、以下の通信のものに限定されます。

- IPv4 マルチキャスト (ブロードキャスト含む) あて
- IPv4 ユニキャストあて
- ARP
- DHCP

[未設定時]

無線 LAN 中継機能の動作モードにマルチクライアントモードが設定されたものとみなされます。

```
wlan relay mode multi
```

4.1.46 wlan relay expire

[機能]

ノード管理テーブルの有効期限の設定

[適用機種]

 SR-M20AC2 SR-M20AC1

[入力形式]

wlan [<number>] relay expire <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>

ノード管理テーブルの有効期限を指定します。

- 有効期限
使用されていないテーブルを保持する時間を、60 秒～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。
各単位での設定可能範囲は、60s～2592000s、1m～43200m、1h～720h、1d～30d です。

[動作モード]

構成定義モード (管理者クラス)

[説明]

いったん登録したノード管理テーブルの情報を、どの程度の期間保持したままにするかを指定します。
ノードとの間の通信がない状態で、設定された時間経過した場合、ノードの情報がテーブルから削除されます。

[未設定時]

有効期限として1日が設定されたものとみなされます。

```
wlan relay expire 1d
```

4.2 VLAN 情報

4.2.1 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-M20AP2 SR-M20AP1

[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 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。

[未設定時]

Tagged VLAN ID を設定しないものとみなされます。

4.2.2 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]



[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]

- 動作タイプとしてスキャン専用モードを設定した無線 LAN インターフェースでは、本コマンドは有効になりません。
- 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。

[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。

4.3 フレーム転送情報

4.3.1 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

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

wlan <number> forward broadcast <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
ブロードキャスト / マルチキャストフレームを転送します。
- disable
ブロードキャスト / マルチキャストフレームを転送しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

無線 LAN インタフェースへ転送時に、ブロードキャスト / マルチキャストフレームを転送するかどうかを設定します。

本定義で disable を指定した場合、ブロードキャスト / マルチキャストフレームは該当無線 LAN インタフェースへは転送されません。

ただし、以下のフレームは、本設定によらず転送します。

- ARP
- 本装置から送信するブロードキャスト / マルチキャストフレーム

[注意]

ProxyARP 機能が有効である場合、ProxyARP 機能による ARP 応答が優先されます。

[未設定時]

無線 LAN インタフェースへブロードキャスト / マルチキャストフレームの転送が有効とみなされます。

```
wlan <number> forward broadcast enable
```

4.4 IEEE802.1X 認証情報

4.4.1 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-M20AP2 SR-M20AP1

[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。

IEEE802.1X 認証を行うために、AAA ユーザ情報、RADIUS 情報を設定しておく必要があります。

また、本コマンドと同時に、wlan dot1x aaa <group_id> で認証先データベースの指定を行ってください。認証サーバの認証データベースまたはローカル認証データベースには必ず VLAN ID も登録してください。認証処理時に VLAN ID の通知がない場合は 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。

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-M20AP2 SR-M20AP1		

[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
```

4.4.2 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-M20AP2 SR-M20AP1

[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 認証および事前共有キー (PSK) 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
```

4.4.3 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-M20AP2 SR-M20AP1

[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 認証および事前共有キー (PSK) 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
```

4.4.4 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-M20AP2 SR-M20AP1

[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。

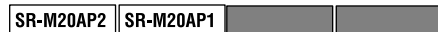
```
wlan <number> dot1x reauthperiod 1h
```

4.4.5 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]



[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
```


4.4.6 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]



[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]

AAA/RADIUS サーバから端末 (Supplicant) に割り当てる VLAN ID の通知があった場合はここで定義された VLAN ID ではなく、AAA/RADIUS サーバから通知された VLAN ID が割り当てられます。

本設定で指定される 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。

[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 AAA/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。

4.4.7 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-M20AP2 SR-M20AP1

[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>

AAA/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 AAA/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。

[注意]

<mode> が enable の場合

AAA/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

AAA/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。

[未設定時]

AAA/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
```

4.4.8 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]



[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
```

4.5 MAC アドレス認証情報

4.5.1 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-M20AP2 SR-M20AP1

[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]

MAC アドレス認証を行うために、AAA ユーザ情報、RADIUS 情報を設定しておく必要があります。

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。

認証サーバの認証データベースまたはローカル認証データベースには必ず VLAN ID も登録してください。認証実行時に 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。

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-M20AP2 SR-M20AP1		

[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
```

4.5.2 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-M20AP2 SR-M20AP1

[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
```

4.5.3 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

[適用機種]



[入力形式]

wlan <number> macauth authenticated-mac <count> <macaddr> <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。

<count>

- 定義番号
0 ~ 99 の 10 進数で指定します。

<macaddr>

- 認証不要端末 MAC アドレス
認証しないで通信を許可する 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。)

<vid>

- VLAN ID
認証不要端末に割り当てる 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]

MAC アドレス認証ポートで認証しないで通信を許可する端末 (プリンタなど) を設定します。

[注意]

- MAC アドレス認証が無効な場合は、設定は無効となります。
- <macaddr> に、00:00:00:00:00:00 およびブロードキャスト、マルチキャストは指定できません。
- <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。
- 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]

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をしないものとみなされます。

4.5.4 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]



[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。

[注意]

認証成功および認証失敗保持時間の監視は 30 秒間隔で行っているため、最大 30 秒までの誤差が生じます。

[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されます。

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

4.5.5 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]



[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]

AAA/RADIUS サーバから端末 (Supplicant) に割り当てる VLAN ID の通知があった場合はここで定義された VLAN ID ではなく、AAA/RADIUS サーバから通知された VLAN ID が優先的に割り当てられます。

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。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]

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 AAA/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。

4.5.6 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]



[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>

AAA/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 AAA/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。

[注意]

<mode> が enable の場合

AAA/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。
AAA/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

AAA/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。

[未設定時]

AAA/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 5 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-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

5.1 VLAN 共通情報

5.1.1 vlan name

[機能]

VLAN 名の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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>
```

5.1.2 vlan forward

[機能]

VLAN の転送設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

vlan <vid> forward <count> <dst_addr> <kind> <port>

[オプション]

<vid>

- VLAN ID
VLAN ID を、10 進数で指定します。

<count>

- 定義番号
0 ~ 199 の 10 進数で指定します。

<dst_addr>

- 転送先 MAC アドレス
静的に学習テーブルに追加する MAC アドレスを指定します。
(XX:XX:XX:XX:XX:XX の形式で、XX は 2 桁の 16 進数です。)

<kind>

ポート種別を指定します。

- ether
ether ポート
- wlan
無線 LAN インタフェース

<port>

- ポート番号
対象となるポート番号を、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]

静的な転送ルールを設定します。

[注意]

- <dst_addr>に、00:00:00:00:00:00 およびブロードキャスト、マルチキャストは指定できません。
- <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。
- <port>で指定されたポートが<vid>で指定された VLAN に設定されていない場合、設定は無効になります。
- <wlan_number>で指定された無線 LAN インタフェースが<vid>で指定された VLAN に設定されていない場合、設定は無効になります。

[未設定時]

未設定

5.1.3 vlan description

[機能]

VLAN の説明文の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

5.2 フィルタ情報

5.2.1 vlan filter

[機能]

VLAN のフィルタの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
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。

範囲	機種
0 ~ 99	SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

<action>

- pass
アクセスコントロールリストの"acl mac"、"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 mac"、"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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 mac"、"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。

また、ほかの ACL 参照定義 (無線 LAN MAC アドレスフィルタ、アプリケーションフィルタなど) を含めて装置全体で以下の数まで定義できます。

最大定義数	機種
1800	SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 mac"定義、"acl ip"定義がどれも存在しない場合、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。
- フィルタリングのデフォルト動作は"vlan filter default"定義に従います。
 "vlan filter default pass"(未設定時)の場合、"vlan filter"定義の<action>が pass のみであると、すべてのパケットがフィルタされません。
 "vlan filter default reject"を指定した場合、すべての Ethernet フレームが遮断されます。IP 通信するには特定の IP パケットだけでなく、ARP パケットも透過させる設定を行う必要があります。

[未設定時]

設定されなかったものとして動作します。

5.2.2 vlan filter move

[機能]

VLAN のフィルタの優先順位変更

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

vlan <vid> filter move <count> <new_count>

[オプション]

<vid>

- VLAN ID
VLAN ID を、10 進数で指定します。

<count>

- 移動対象優先順位
移動する優先順位の番号を、10 進数で指定します。

<new_count>

- 移動先優先順位
移動先優先順位の番号を、10 進数で指定します。

範囲	機種
0 ~ 99	SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[動作モード]

構成定義モード (管理者クラス)

[説明]

VLAN ごとのフィルタの優先順位を変更します。
現在の優先順位が<count>である定義を<new_count>の優先順位に変更します。
変更後は優先順位番号が順番にソートされてリナンバリングされます。

[未設定時]

編集コマンドのため設定されません。

5.2.3 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

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

vlan <vid> filter default <action> [<inside> <time>]

[オプション]

<vid>

- VLAN ID
VLAN ID を、10 進数で指定します。

<action>

どの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。

- pass
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。
- spi
該当する IP パケットに対して SPI を動作させます。

<inside>

action に spi を指定したときに、内側とみなす方向を指定します。

- wlan
無線インタフェース側を内側とみなされます。
- ether
有線インタフェース側を内側とみなされます。

<time>

- 割り当て時間
action に spi を指定したときに、接続に割り当てられたテーブルを解放するための無通信監視時間を、1 ~ 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。
省略時は、5 分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]

どの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。

[注意]

- "vlan filter default pass"(未設定時)の場合、"vlan filter"定義の<action>が pass のみであると、すべてのパケットがフィルタされません。
- "vlan filter default reject"を指定した場合、すべての Ethernet フレームが遮断されます。
IP 通信するには特定の IP パケットだけでなく、ARP パケットも透過させる設定を行う必要があります。

[未設定時]

どの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。

```
vlan <vid> filter default pass
```

5.3 IDS 情報

5.3.1 vlan ids use

[機能]

IDS の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

vlan <vid> ids use <mode>

[オプション]

<vid>

- VLAN ID
VLAN ID を、10 進数で指定します。

<mode>

- off
IDS を利用しません。
- on
IDS を利用します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

このインタフェースで、IPv4 パケットに対して IDS を利用するかどうかを設定します。

[未設定時]

IPv4 パケットに対して IDS を利用しないものとみなされます。

```
vlan <vid> ids use off
```

第 6 章 MAC 情報

6.1 MAC 情報

6.1.1 mac age

[機能]

MAC アドレス学習テーブルのエージングアウト時間の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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ー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ージングアウト時間を設定します。

[未設定時]

エー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 7 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-M20AP2 SR-M20AP1
0	SR-M20AC2 SR-M20AC1

7.1 IP関連情報

7.1.1 lan ip address

[機能]

IPアドレスの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0を指定したものとみなされます。

<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。

0.0.0.0
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。

- 0
0.0.0.0の場合に指定します。
- 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。

【未設定時】

IP アドレスがないものとみなされます。

```
lan <number> ip address 0.0.0.0/0 0
```

7.1.2 lan ip dhcp service

[機能]

DHCP 機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

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

[オプション]

<number>

- lan 定義番号
lan 定義の通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<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。

[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
```

7.1.3 lan ip route

[機能]

IPv4 スタティック経路情報の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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-M20AP2 SR-M20AP1
0 ~ 3	SR-M20AC2 SR-M20AC1

<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、通常はこの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。ここで、優先度1のデフォルトルートではなく、任意のあて先で任意の優先度のスタティック経路として生成したい場合は、<next_hop>に dhcp と指定する IPv4 スタティック経路を設定することで実現できます。この場合、優先度1のデフォルトルートは自動生成されません。

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。

最大定義数	機種
40	SR-M20AP2 SR-M20AP1
4	SR-M20AC2 SR-M20AC1

[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。

7.1.4 lan ip arp static

[機能]

スタティック ARP の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

<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ーフェースでは、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。

7.2 VLAN 関連情報

7.2.1 lan vlan

[機能]

VLAN ID の設定

[適用機種]

SR-M20AP2 SR-M20AP1 

[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。
省略時は、0 を指定したものとみなされます。

<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

7.3 SNMP 関連情報

7.3.1 lan snmp trap linkdown

[機能]

linkDown トラップの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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
```

7.3.2 lan snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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 8 章 IP 関連情報

8.1 IP 関連情報

8.1.1 ip arp age

[機能]

ARP エントリ有効時間の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

[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 9 章 認証情報の設定

9.1 IEEE802.1X 情報

9.1.1 dot1x use

[機能]

IEEE802.1X 認証モードの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 (SR-M20AP2/20AP1 のみ) や ether dot1x use 定義 (SR-M20AC2/20AC1 のみ) 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

9.2 MAC アドレス認証情報

9.2.1 macauth use

[機能]

MAC アドレス認証基本情報の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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、ether macauth use 定義や 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
```

9.2.2 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

9.2.3 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 10 章 サプリカント情報

10.1 supplicant dot1x use

[機能]

IEEE802.1X サプリカントでの認証モードの設定

[適用機種]

 SR-M20AC2 SR-M20AC1

[入力形式]

supplicant 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 サプリカントでの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ていても、wlan supplicant 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。

```
supplicant dot1x use off
```

10.2 supplicant certificate check validity

[機能]

証明書の有効期限チェックの設定

[適用機種]

SR-M20AC2 SR-M20AC1

[入力形式]

supplicant certificate check validity <remain> interval <interval>

[オプション]

<remain>

- 有効期限残日数
証明書の有効期間の終了日時の何日前から警告するかを指定します。
有効期限残日数は 86400s(1d) ~ 2592000s(30d) 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。

<interval>

- チェック間隔
証明書の有効期限チェックの間隔を指定します。
期間は 3600s(1h) ~ 604800s(7d) 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]

証明書の有効期限が切れる前に、システムログ情報で有効期間の終了日時が近いことを通知する場合に指定します。

[注意]

設定前に本装置の内部時刻を正しくセットしてください。

[未設定時]

証明書の有効期限チェックを行わないものとみなされます。

第 11 章 証明書関連情報の設定

11.1 証明書関連情報

11.1.1 certificate local name

[機能]

自装置証明書識別名の設定

[適用機種]



[入力形式]

certificate local [<number>] name <name>

[オプション]

<number>

自装置証明書識別番号を指定します。

- 自装置証明書識別番号
自装置証明書の識別番号を、0~4の10進数で指定します。
省略時は、0を指定したものとみなされます。

<name>

自装置証明書識別名を指定します。

- 自装置証明書識別名
0x21,0x23~0x7eの16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]

自装置証明書識別名の設定を行います。

通常は、crypto certificate generate コマンド、crypto certificate local コマンドで設定を行います。

[注意]

crypto certificate generate コマンド、crypto certificate local コマンドで設定を行った場合は上書きされます。

[未設定時]

自装置証明書識別名を設定しないものとみなされます。

11.1.2 certificate local line

[機能]

自装置証明書の設定

[適用機種]



[入力形式]

certificate local [<number>] line <line_number> <string>

[オプション]

<number>

自装置証明書識別番号を指定します。

- 自装置証明書識別番号
自装置証明書の識別番号を、0~4 の 10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<line_number>

自装置証明書の行番号を指定します。

- 行番号
行番号を、0~99 の 10 進数で指定します。

<string>

Base64 形式の証明書を指定します。

- 証明書データ
Base64 形式の自装置証明書を、+、/、=、A~Z、a~z、0~9 の 76 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]

自装置証明書を Base64 形式で 1 行ずつ設定を行います。
通常は、crypto certificate generate コマンド、crypto certificate local コマンドで設定を行います。

[注意]

crypto certificate generate コマンド、crypto certificate local コマンドで設定を行った場合は上書きされます。

[未設定時]

自装置証明書を設定しないものとみなされます。

11.1.3 certificate ca name

[機能]

認証局証明書識別名の設定

[適用機種]



[入力形式]

certificate ca [<number>] name <name>

[オプション]

<number>

認証局証明書識別番号を指定します。

- 認証局証明書識別番号
認証局証明書の識別番号を、0~4の10進数で指定します。
省略時は、0を指定したものとみなされます。

<name>

認証局証明書識別名を指定します。

- 認証局証明書識別名
0x21,0x23~0x7eの16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]

認証局証明書識別名の設定を行います。
通常は、crypto certificate ca コマンドで設定を行います。

[注意]

crypto certificate ca コマンドで設定を行った場合は上書きされます。

[未設定時]

認証局証明書識別名を設定しないものとみなされます。

11.1.4 certificate ca line

[機能]

認証局証明書の設定

[適用機種]



[入力形式]

certificate ca [<number>] line <line_number> <string>

[オプション]

<number>

認証局証明書識別番号を指定します。

- 認証局証明書識別番号
認証局証明書の識別番号を、0~4 の 10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<line_number>

認証局証明書の行番号を指定します。

- 行番号
行番号を、0~99 の 10 進数で指定します。

<string>

Base64 形式の証明書を指定します。

- 証明書データ
Base64 形式の相手装置証明書を、+、/、=、A~Z、a~z、0~9 の 76 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]

認証局証明書を Base64 形式で 1 行ずつ設定を行います。
通常は、crypto certificate ca コマンドで設定を行います。

[注意]

crypto certificate ca コマンドで設定を行った場合は上書きされます。

[未設定時]

認証局証明書を設定しないものとみなされます。

11.1.5 certificate request line

[機能]

証明書要求の設定

[適用機種]



[入力形式]

certificate request [<number>] line <line_number> <string>

[オプション]

<number>

証明書要求識別番号を指定します。

- 証明書要求識別番号
証明書要求の識別番号を、0～4の10進数で指定します。
省略時は、0を指定したものとみなされます。

<line_number>

証明書要求の行番号を指定します。

- 行番号
行番号を、0～99の10進数で指定します。

<string>

Base64形式の証明書要求を指定します。

- 証明書要求データ
Base64形式の証明書要求を、+、/、=、A～Z、a～z、0～9の76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]

証明書要求をBase64形式で1行ずつ設定を行います。
通常は、crypto certificate generate コマンドで設定を行います。

[注意]

crypto certificate generate コマンドで設定を行った場合は上書きされます。

[未設定時]

証明書要求を設定しないものとみなされます。

11.1.6 certificate private line

[機能]

秘密鍵の設定

[適用機種]



[入力形式]

certificate private [<number>] line <line_number> <string>

[オプション]

<number>

秘密鍵識別番号を指定します。

- 秘密鍵識別番号
秘密鍵の識別番号を、0～4の10進数で指定します。
省略時は、0を指定したものとみなされます。

<line_number>

秘密鍵の行番号を指定します。

- 行番号
行番号を、0～99の10進数で指定します。

<string>

暗号化された秘密鍵を指定します。

- 秘密鍵データ
暗号化された秘密鍵を指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

暗号化された秘密鍵の設定を行います。
通常は、crypto certificate generate コマンドで設定を行います。

[注意]

crypto certificate generate コマンドで設定を行った場合は上書きされます。

[未設定時]

秘密鍵を設定しないものとみなされます。

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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

12.1 ACL 情報

12.1.1 acl mac

[機能]

ACL MAC 定義

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
- bcast
ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
マルチキャスト 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。
- bcast
ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
マルチキャスト 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-M20AP2	SR-M20AP1	SR-M20AC2	SR-M20AC1
-----------	-----------	-----------	-----------

[入力形式]

```
acl <acl_count> ip <src_addr>/<mask> <dst_addr>/<mask> [<protocol> [any]]
acl <acl_count> ip <src_addr>/<mask> <dst_addr>/<mask> [<protocol> [tos <value>]]
acl <acl_count> ip <src_addr>/<mask> <dst_addr>/<mask> [<protocol> [dscp <value>]]
```

[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_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。

<type>

ACL 対象とする QoS の判断する方法を指定します。

- tos
TOS 値で ACL 対象を判断する場合に指定します。
- dscp
DSCP 値で ACL 対象を判断する場合に指定します。
- any
すべての TOS 値、すべての DSCP 値を ACL 対象とする場合に指定します。

<value>

ACL 対象とする TOS 値、または DSCP 値を指定します。

- TOS 値
ACL 対象とする TOS 値を、0~ff の 16 進数で指定します。
複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
TOS 値は、","(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。
 - 00~ff の 16 進数値 (例: ff = ff の TOS 値)
 - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
 - TOS 値- (例: 80- = 80 から ff までの TOS 値)
 - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
 - TOS 値,TOS 値,... (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- DSCP 値
ACL 対象とする DSCP 値を、0~63 の 10 進数で指定します。
複数の DSCP 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-63」のように"-"(ハイフン) を使用して指定します。
DSCP 値は、","(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。
 - 0~63 の 10 進数値 (例: 63 = 63 の DSCP 値)
 - DSCP 値-DSCP 値 (例: 32-47 = 32 から 47 までの DSCP 値)
 - DSCP 値- (例: 32- = 32 から 63 までの DSCP 値)
 - -DSCP 値 (例: -31 = 0 から 31 までの DSCP 値)
 - DSCP 値,DSCP 値,... (例: 10,20,30- = 10 と 20 と 30 以降の DSCP 値)

[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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

acl <acl_count> tcp <src_port> <dst_port> <tcpconnect>

[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。

<tcpconnect>

- yes
TCP プロトコルでコネクション接続要求を ACL 対象に含めます。
- no
TCP プロトコルでコネクション接続要求を ACL 対象に含めません。

[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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

acl <acl_count> icmp <icmptype> <icmpcode>

[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。

<icmpcode>

ACL 対象とする ICMP CODE を指定します。

- ICMP CODE
ACL 対象とする送信元 ICMP CODE を、0~255 の 10 進数で指定します。
複数の ICMP CODE 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 CODE 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 CODE 8)
 - ICMP CODE-ICMP CODE (例: 2-8 = 2 から 8 までの ICMP CODE)
 - ICMP CODE- (例: 8- = 8 から 255 までの ICMP CODE)
 - -ICMP CODE (例: -200 = 0 から 200 までの ICMP CODE)
 - ICMP CODE,ICMP CODE,... (例: 0,8,30- = 0 と 8 と 30 以降の ICMP CODE)
- any
すべての ICMP CODE 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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-M20AP2 SR-M20AP1
0	SR-M20AC2 SR-M20AC1

- AAA ユーザ情報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>](AAA ユーザ情報定義番号) 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 ~ 999	SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

- 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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 AAA ユーザ情報

13.2.1 aaa user id

[機能]

認証情報の設定 (ユーザ ID)

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
aaa [<group_id>] user [<number>] id <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。
省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<id>

- ユーザ ID
ユーザ 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。

[動作モード]

構成定義モード (管理者クラス)

[説明]

認証プロトコルに使用する、認証情報 (ユーザ ID) を設定します。
MAC アドレス認証で利用する場合は、アクセスを許可する端末の MAC アドレスを、16 進数 12 桁 (小文字、コロンで区切らない) で指定してください。

[未設定時]

認証情報 (ユーザ ID) を設定しないものとみなされます。

13.2.2 aaa user password

[機能]

認証情報の設定 (パスワード)

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

aaa [<group_id>] user [<number>] password [<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。
省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<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]

認証プロトコルに使用する、認証情報 (認証パスワード) 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。

MAC アドレス認証で利用し、macauth password を指定された場合は、macauth password で設定した認証情報を本コマンドで指定してください。macauth password を指定しない場合は、アクセスを許可する端末の MAC アドレスを、16 進数 12 桁 (小文字、コロンで区切らない) で指定してください。

[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。

[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]

認証情報 (パスワード) を設定しないものとみなされます。

13.2.3 aaa user user-role

[機能]

権限クラスの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
aaa [<group_id>] user [<number>] user-role <class>
```

[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。
省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<class>

権限クラスを指定します。

- administrator
権限クラスを管理者クラスとします。
- user
権限クラスを一般ユーザクラスとします。
- none
権限クラスを指定しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ログインユーザ情報として使用する場合に、ユーザの権限クラスを指定します。

[未設定時]

権限クラスを設定しないものとみなされます。

13.3 Supplicant 情報

13.3.1 aaa user supplicant vid

[機能]

ユーザに割り当てる VLAN ID の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

```
aaa [<group_id>] user [<number>] supplicant vid <vid>
```

[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。
省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<vid>

Supplicant に割り当てる 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]

Supplicant(ユーザ端末) に割り当てる VLAN ID を指定します。

[注意]

未設定の場合、ether コマンドで定義されたデフォルト VLAN 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。

[未設定時]

割り当てる VLAN ID が存在しないものとみなされます。

13.3.2 aaa user supplicant mac

[機能]

Supplicant MAC アドレスの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

aaa [<group_id>] user [<number>] supplicant mac <mac>

[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。
省略時は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
グループ内での通し番号を、10 進数で指定します。
省略時は、0 を指定したものとみなされます。

<mac>

- Supplicant の MAC アドレス
Supplicant(ユーザ端末) 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]

構成定義モード (管理者クラス)

[説明]

認証プロトコルで使用する、認証情報 (MAC アドレス) を設定します。

[未設定時]

認証情報 (MAC アドレス) を設定しないものとみなされます。

13.4 RADIUS 情報の設定

13.4.1 aaa radius service

[機能]

RADIUS サービスの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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
```

13.4.2 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 ~ 126.255.255.254
 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。

13.4.3 aaa radius auth message-authenticator

[機能]

Message-Authenticator の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

13.4.4 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

13.4.5 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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。
省略時は、0 を指定したものとみなされます。

<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 ユーザー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。

13.4.6 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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。

13.4.7 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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 port 1812
```

13.4.8 aaa radius client server-info auth deadline

[機能]

復旧待機時間の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

aaa [<group_id>] radius client server-info auth [<number>] deadline <deadline>

[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。
省略時は、0 を指定したものとみなされます。

<deadline>

- 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 deadtime 0s
```

13.4.9 aaa radius client server-info auth priority

[機能]

優先度の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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、使用する RADIUS サーバはランダムに決定されます。

[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 priority 0
```

13.4.10 aaa radius client server-info auth source

[機能]

自側 IP アドレスの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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。

13.4.11 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-M20AP2 SR-M20AP1

[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。
省略時は、0 を指定したものとみなされます。

<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 watch type off
```

13.4.12 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-M20AP2 SR-M20AP1

[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。
省略時は、0 を指定したものとみなされます。

<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。

[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。

13.4.13 aaa radius client server-info auth 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-M20AP2 SR-M20AP1

[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。
省略時は、0 を指定したものとみなされます。

<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 watch interval 1m
```

13.4.14 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-M20AP2 SR-M20AP1

[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。
省略時は、0 を指定したものとみなされます。

<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 watch retry 10s
```

13.4.15 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-M20AP2 SR-M20AP1

[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。
省略時は、0 を指定したものとみなされます。

<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 watch timeout 30s
```

13.4.16 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-M20AP2 SR-M20AP1

[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。
省略時は、0 を指定したものとみなされます。

<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 watch abnormal-interval 3m
```

13.4.17 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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。
省略時は、0 を指定したものとみなされます。

<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 ユーザー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。

13.4.18 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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。

13.4.19 aaa radius client server-info accounting port

[機能]

アカウントिंगサーバ UDP ポートの設定 (旧 RFC 仕様対応)

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<port>

- 1813
最新 RFC 仕様の RADIUS アカウントिंग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 アカウントिंग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 アカウントिंगクライアントがアカウントING要求する RADIUS アカウントINGサーバの UDP ポート番号を設定します。

アカウントING要求する RADIUS アカウントINGサーバが旧 RFC 仕様の UDP ポートで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ING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 port 1813
```

13.4.20 aaa radius client server-info accounting deadtime

[機能]

復旧待機時間の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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 deadtime 0s
```


13.4.21 aaa radius client server-info accounting priority

[機能]

優先度の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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、アカウントングの際に使用する RADIUS サーバを決める際に使用する優先度を指定します。同一グループの中で、dead 状態になっていないもっとも高い優先度の RADIUS サーバが使われます。もっとも高い優先度の RADIUS サーバが複数存在する場合は、使用する RADIUS サーバはランダムに決定されます。

[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 priority 0
```

13.4.22 aaa radius client server-info accounting source

[機能]

自側 IP アドレスの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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。

13.4.23 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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> client radius retry 5 2
```

13.4.24 aaa radius client nas-identifier

[機能]

NAS 識別子の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<nas_id>

- NAS 識別子
RADIUS 認証クライアントおよびアカウントングクライアントが RADIUS サーバに送出する Nas-Identifier アトリビュートの値を、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ングで有効です。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。

第 14 章 無線 LAN 管理機能の設定

- グループ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>(グループ定義番号) 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 ~ 4	SR-M20AP2 SR-M20AP1

- 管理機器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>(管理機器定義番号) に指定する管理機器の通し番号 (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 ~ 4	SR-M20AP2 SR-M20AP1

- MAC アドレスフィルタセット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 <set_num>(MAC アドレスフィルタセット定義番号) に指定する MAC アドレスフィルタセットの通し番号 (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 ~ 4	SR-M20AP2 SR-M20AP1

- MAC アドレスフィルタ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 <filter_num>(MAC アドレスフィルタ定義番号) に指定する MAC アドレスフィルタの通し番号 (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 ~ 99	SR-M20AP2 SR-M20AP1

- 管理外無線 LAN アクセスポイント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>(管理外無線 LAN アクセスポイント定義番号) に指定する管理外無線 LAN アクセスポイントの通し番号 (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 ~ 4	SR-M20AP2 SR-M20AP1

14.1 無線 LAN 管理ログイン情報

14.1.1 nodemanager login service

[機能]

ログイン機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager login service <mode>

[オプション]

<mode>

- enable
無線 LAN 管理機能用リモートログインアカウントを有効にします。
無線 LAN 管理機能から本装置にリモートログインして管理できます。
- disable
無線 LAN 管理機能用リモートログインアカウントを無効にします。
無線 LAN 管理機能から本装置にリモートログインできなくなり、管理できなくなります。

[動作モード]

構成定義モード (管理者クラス)

[説明]

無線 LAN 管理用リモートログインアカウントの有効/無効を設定します。
enable に設定することにより、本装置をリモート接続による無線 LAN 管理対象機器にできます。
disable に設定しても、本装置の無線 LAN 管理機能でローカル接続による無線 LAN 管理対象機器にすることができます。

[注意]

無線 LAN 管理用リモートログインアカウントのログインパスワードは、password nodemgr set コマンドで設定できます。
パスワードを設定していなくても、本設定を enable にすることにより本装置をリモート管理できます。
password nodemgr set コマンドで無線 LAN 管理パスワードを設定した場合は、設定したパスワードを無線 LAN 管理装置の無線 LAN 管理機器情報にも設定してください。

[未設定時]

無線 LAN 管理機能から本装置にリモートログインできないものとします。

```
nodemanager login service disable
```

14.2 無線 LAN 管理機器情報

14.2.1 nodemanager group name

[機能]

管理グループ名の設定

[適用機種]

SR-M20AP2	SR-M20AP1		
-----------	-----------	--	--

[入力形式]

nodemanager group <number> name <name>

[オプション]

<number>

- グループ定義番号
管理グループの通し番号を 10 進数で指定します。

<name>

- グループ名
管理グループ名を、0x21,0x23 ~ 0x7e の 8 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]

管理グループの名前を設定します。

[未設定時]

管理グループを設定しないものとみなされます。

14.2.2 nodemanager node name

[機能]

管理機器名の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager node <number> name <name>

[オプション]

<number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<name>

- 管理機器名
管理機器名を、0x21,0x23 ~ 0x7e の 8 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]

管理機器の名前を設定します。

[注意]

管理機器名が設定されていない管理機器は、無線 LAN 管理機能の対象となりません。

[未設定時]

管理機器を設定しないものとみなされます。

14.2.3 nodemanager node group

[機能]

管理機器の所属グループの設定

[適用機種]



[入力形式]

nodemanager node <number> group <group_number>

[オプション]

<number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<group_number>

- グループ定義番号
所属先の管理グループ通し番号を 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]

設定済みの管理機器を管理グループに所属させます。所属先の管理グループが削除された場合は、管理機器は自動的にどのグループにも所属していない状態になります。

[注意]

存在しないグループを指定した場合、設定済みのグループを削除した場合は、管理機器はどのグループにも所属しないものとして動作します。

管理機器に管理機器名が定義されていない場合、このコマンドの設定は無効になります。

[未設定時]

管理機器の所属グループを設定しないものとみなされます。

14.2.4 nodemanager node address

[機能]

管理機器の IP アドレスの設定

[適用機種]



[入力形式]

nodemanager node <number> address <address>

[オプション]

<number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<address>

- 管理機器 IP アドレス
IP アドレスの設定を変更する場合に指定します。
管理機器の IPv4 アドレスを指定します。
指定可能な範囲は以下のとおりです。

IPv4: 1.0.0.1 ~ 126.255.255.254
127.0.0.1(無線 LAN 管理機能が動作する機器を管理対象にする場合)
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]

管理機器の IP アドレスを設定します。

[注意]

管理機器に管理機器名が定義されていない場合、このコマンドの設定は無効になります。
管理機器の IP アドレスが設定されていない管理機器は、無線 LAN 管理機能の対象となりません。
無線 LAN 管理機能が動作する機器を管理対象にしたい場合は、そのアドレスとして、127.0.0.1 を設定してください。

[未設定時]

IP アドレスがないものとみなされます。

14.2.5 nodemanager node user

[機能]

リモートログイン時のユーザ名、パスワードの設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager node <number> user nodemgr <password> [encrypted]

[オプション]

<number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<password>

- パスワード
管理機器のパスワードを設定する場合に指定します。
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。
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]

管理機器へのリモートログインに使用するユーザ名、パスワードを設定します。
リモートログインに使用されるユーザ名は、常に "nodemgr" です。

[注意]

管理機器に管理機器名が定義されていない場合、このコマンドの設定は無効になります。

[未設定時]

リモートログイン時のユーザ名、パスワードを設定しないものとみなされます。

14.2.6 nodemanager node wlan scan

[機能]

管理機器用のスキャン要求の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

```
nodemanager node <number> wlan scan {enable | disable}
```

[オプション]

<number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

enable | disable

- スキャンフラグ
管理機器のスキャン要求を設定します。
指定可能な値は以下のとおりです。

disable :スキャン要求なし

enable :スキャン要求あり

[動作モード]

構成定義モード (管理者クラス)

[説明]

管理機器の「スキャン要求なし」、「スキャン要求あり」を設定します。

[注意]

管理機器に管理機器名が定義されていない場合、このコマンドの設定は無効になります。
スキャン要求を設定する無線 LAN アクセスポイントは、以下の条件を満たす必要があります。

- 無線 LAN インタフェースの動作タイプが、無線 LAN アクセスポイント、または、スキャン専用モードであること。
- 周辺アクセスポイント検出の動作モードが有効であること。

[未設定時]

管理機器のスキャンフラグに「スキャン要求あり」が設定されたものとみなされます。

```
nodemanager node <number> wlan scan enable
```

14.2.7 nodemanager node wlan sta

[機能]

無線 LAN 端末の情報取得の設定

[適用機種]

SR-M20AP2 SR-M20AP1  

[入力形式]

```
nodemanager node <number> wlan sta {enable | disable}
```

[オプション]

<number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

enable | disable

- 情報取得フラグ
管理機器の無線 LAN 端末情報取得を設定します。
指定可能な値は以下のとおりです。

disable :無線 LAN 端末の情報取得なし

enable :無線 LAN 端末の情報取得あり

[動作モード]

構成定義モード (管理者クラス)

[説明]

管理機器用の「無線 LAN 端末の情報取得なし」、「無線 LAN 端末の情報取得あり」を設定します。

[注意]

管理機器に管理機器名が定義されていない場合、このコマンドの設定は無効になります。

[未設定時]

管理機器の情報取得フラグに「無線 LAN 端末の情報取得あり」が設定されたものとみなされます。

```
nodemanager node <number> wlan sta enable
```

14.2.8 nodemanager node wlan neighbor

[機能]

近隣の管理機器の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

```
nodemanager node <number> wlan neighbor <node_num1> [<node_num2> [<node_num3>
<node_num4>]]
```

[オプション]

<number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<node_num1>,<node_num2>,<node_num3>,<node_num4>

- 近隣管理機器定義番号
近隣の管理機器の通し番号を 10 進数で指定します。
<number>と同じ値は指定できません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

近隣の管理機器を設定します。近隣管理機器情報は、管理機器間の関係を調整する場合に使用されます。

[注意]

管理機器に管理機器名が定義されていない場合、このコマンドの設定は無効になります。
近隣管理機器に未定義の近隣管理機器を設定した場合、このコマンドの設定は無効になります。

[未設定時]

近隣管理機器を設定しないものとみなされ、電波出力自動調整の対象から除外されます。


14.3 MAC アドレスフィルタ情報

14.3.1 nodemanager wlan filterset description

[機能]

MAC アドレスフィルタセットのコメントの設定

[適用機種]

SR-M20AP2 SR-M20AP1 

[入力形式]

nodemanager wlan filterset <set_num> description <desc>

[オプション]

<set_num>

- MAC アドレスフィルタセット定義番号
MAC アドレスフィルタセット定義番号を 10 進数で指定します。

<desc>

- コメント
MAC アドレスフィルタに対するコメントを、0x21,0x23 ~ 0x7e の 50 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]

MAC アドレスフィルタセットにコメントを設定します。

[未設定時]

MAC アドレスフィルタセットにコメントを設定しないものとみなされます。

14.3.2 nodemanager wlan filterset filter mac

[機能]

管理機器用の MAC アドレスフィルタの設定

[適用機種]



[入力形式]

nodemanager wlan filterset <set_num> filter <filter_num> mac <mac> <action>

[オプション]

<set_num>

- MAC アドレスフィルタセット定義番号
MAC アドレスフィルタセット定義番号を 10 進数で指定します。

<filter_num>

- MAC アドレスフィルタ定義番号
MAC アドレスフィルタセット内の MAC アドレスフィルタ定義番号を 10 進数で指定します。

<mac>

- 無線 LAN 端末 MAC アドレス
無線 LAN 端末の MAC アドレスを <set_num>, <filter_num> で指定した MAC アドレスフィルタに指定します。
指定可能な値は以下のとおりです。
 - any** : すべての MAC アドレスが対象
MAC アドレス
: 対象とする無線 LAN 端末の 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。

<action>

- アクション
MAC アドレスフィルタで設定された MAC アドレスの接続を許可するかどうかを指定します。
指定可能な値は以下のとおりです。
 - pass** : MAC アドレスの接続を許可 (透過)
 - reject** : MAC アドレスの接続を拒否 (遮断)

[動作モード]

構成定義モード (管理者クラス)

[説明]

管理機器用の MAC アドレスフィルタを設定します。

「管理機器への MAC アドレスフィルタ配布」で MAC アドレスフィルタを管理機器に反映すると、管理機器は MAC アドレスフィルタと一致した無線 LAN 端末の接続を <action> に従って許可または拒否します。

[注意]

本コマンドで追加した MAC アドレスの情報を、実際の管理機器に反映させるには `nodemanagerctl update wlan filterset` コマンドを使用します。

[未設定時]

MAC アドレスフィルタを設定しないものとみなされます。

14.3.3 nodemanager wlan filterset filter description

[機能]

MAC アドレスフィルタへのコメントの設定

[適用機種]**[入力形式]**

```
nodemanager wlan filterset <set_num> filter <filter_num> description <desc>
```

[オプション]**<set_num>**

- MAC アドレスフィルタセット定義番号
MAC アドレスフィルタセット定義番号を 10 進数で指定します。

<filter_num>

- MAC アドレスフィルタ定義番号
MAC アドレスフィルタセット内の MAC アドレスフィルタ定義番号を 10 進数で指定します。

<desc>

- コメント
MAC アドレスフィルタに対するコメントを、0x21,0x23 ~ 0x7e の 50 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]

MAC アドレスフィルタに無線 LAN 端末の MAC アドレスコメントを設定します。

[注意]

管理機器用の MAC アドレスフィルタが設定されていない場合、このコマンドの設定は無効になります。

[未設定時]

MAC アドレスフィルタに無線 LAN 端末の MAC アドレスコメントを設定しないものとみなされます。

14.4 電波出力自動調整情報

14.4.1 nodemanager wlan autotxpower rssi

[機能]

電波出力自動調整の RSSI 最低しきい値の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager wlan autotxpower rssi <low_rssi>

[オプション]

<low_rssi>

- 電波出力自動調整用 RSSI 最低しきい値
近隣の無線 LAN アクセスポイントで、設定対象の無線 LAN アクセスポイントの無線送信出力を判定するための RSSI 最低しきい値を 1～255 の範囲の 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]

電波出力自動調整機能は、任意の無線 LAN アクセスポイントの無線送信出力を自動的に調整する機能で、その電波の到達範囲が必要以上に大きくなるのを防止します。

電波出力自動調整用 RSSI 最低しきい値には、電波出力自動調整時に近隣の無線 LAN アクセスポイントで計測される、設定対象の無線 LAN アクセスポイントの RSSI のしきい値を指定します。

RSSI と信号強度 (dBm) 関係は、以下のとおりです。

$$\text{dBm} = (\text{RSSI 値}) - 95$$

[未設定時]

電波出力自動調整用 RSSI 最低しきい値は 20 が設定されたものとみなされます。

```
nodemanager wlan autotxpower rssi 20
```

14.5 チャネル自動調整情報

14.5.1 nodemanager wlan autochannel channel

[機能]

5GHz 帯のチャネル自動調整の割り当て範囲の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager wlan autochannel channel <mode>

[オプション]

<mode>

- w52
5GHz 無線 LAN W52 で規定されたチャネルの中で割り当てを行います。
- w53
5GHz 無線 LAN W53 で規定されたチャネルの中で割り当てを行います。
- w56
5GHz 無線 LAN W56 で規定されたチャネルの中で割り当てを行います。
- w52/53
5GHz 無線 LAN W52 と W53 で規定されたチャネルの中で割り当てを行います。
- w52/53/56
5GHz 無線 LAN W52、W53 および W56 で規定されたチャネルの中で割り当てを行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

チャネル自動調整で、5GHz 帯のチャネルの割り当て範囲を設定します。

[未設定時]

5GHz 帯のチャネル自動調整の割り当て範囲は、w52/53/56 が設定されたものとみなされます。

```
nodemanager wlan autochannel channel w52/53/56
```

14.5.2 nodemanager wlan autochannel layout

[機能]

2.4GHz 帯のチャンネル自動調整のレイアウトの設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager wlan autochannel layout <ch_number> <interval>

[オプション]

<ch_number>

- 2.4GHz 帯の開始チャンネル
1~5 の 10 進数で指定します。

<interval>

- 2.4GHz 帯のチャンネル割り当て間隔
3~5 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]

「管理機器のチャンネル自動調整」で、2.4GHz 帯のチャンネルを割り当てるときのチャンネルのレイアウトを設定します。

チャンネルレイアウトは、以下の式で求めることができます。

```
<ch_number>, <ch_number> + (1 * <inter-  
val>), ..., <ch_number> + (n * <interval>)
```

[未設定時]

2.4GHz 帯の開始チャンネルに 1、2.4GHz 帯のチャンネル割り当て間隔に 5 が設定されたものとみなされます。

```
nodemanager wlan autochannel layout 1 5
```

14.5.3 nodemanager wlan autochannel rssi

[機能]

2.4GHz 帯のチャンネル自動調整の判定用 RSSI しきい値の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager wlan autochannel rssi <rssi>

[オプション]

<rssi>

- 2.4GHz 帯のチャンネル自動調整の判定用 RSSI のしきい値
2.4GHz 帯のチャンネル自動調整で、使用済みのチャンネルを割り当てる場合の RSSI のしきい値を 1～128 の 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]

チャンネル自動調整の判定用 RSSI のしきい値は、2.4GHz 帯で使用済みチャンネルを設定する必要が発生した場合の、設定対象である無線 LAN アクセスポイントでの同チャンネルの RSSI のしきい値を指定します。使用済みチャンネルを設定する場合、この RSSI のしきい値以下であるチャンネルを設定するようにします。RSSI と信号強度 (dBm) 関係は、以下のとおりです。

$$\text{dBm} = (\text{RSSI 値}) - 95$$

[未設定時]

チャンネル自動調整の判定用 RSSI のしきい値は 20 が設定されたものとみなされます。


```
nodemanager wlan autochannel rssi 20
```

14.5.4 nodemanager wlan autochannel bandwidth

[機能]

チャンネル自動調整時の通信帯域幅の設定

[適用機種]

SR-M20AP2 SR-M20AP1 

[入力形式]

nodemanager wlan autochannel bandwidth <width>

[オプション]

<width>

- 20
無線 LAN の通信帯域幅を 20MHz に設定します。
- 40
無線 LAN の通信帯域幅を 40MHz 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]

40MHz が指定され、管理アクセスポイントが IEEE802.11n で通信可能な場合、チャンネルボンディング機能を使用したチャンネル調整を行います。

ただし、管理アクセスポイントの周辺のチャンネルの利用状況によっては、チャンネルボンディング機能を使用できないことがあります。

その場合は、20MHz の帯域幅でチャンネルの自動割り当てを行います。

[未設定時]

通信帯域幅として 20 が設定されたものとみなされます。

```
nodemanager wlan autochannel bandwidth 20
```


14.6 アクセスポイント 情報取得情報

14.6.1 nodemanager collect interval

[機能]

アクセスポイント 情報取得の時間パラメタの設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager collect interval <period> <wait_period> <time_out>

[オプション]

<period>

- 情報取得間隔
管理機器から情報取得の間隔を 1 ~ 600 秒の範囲の 10 進数で指定します。
単位は、m(分)、s(秒) のどちらかを指定します。

<wait_period>

- 情報取得待機間隔
管理機器からの情報取得の待機時間を 1 ~ 600 秒の範囲の 10 進数で指定します。
単位は、m(分)、s(秒) のどちらかを指定します。

<time_out>

- 情報取得タイムアウト時間
管理機器からの情報取得タイムアウト時間を 1 ~ 60 秒の範囲の 10 進数で指定します。
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]

無線 LAN 管理機能が管理機器や無線 LAN 端末の情報取得を行う際の時間パラメタを設定します。
情報取得間隔は、ある管理機器の情報を取得してから次の管理機器の情報取得するまでの間隔です。
情報取得待機間隔は、すべての情報取得対象の管理機器の情報取得したあと、次の情報取得を開始するまでの待ち時間です。
情報取得タイムアウト時間は、管理機器との通信時のタイムアウト時間です。タイムアウトが発生したら次の管理機器の情報取得を行います。
情報取得間隔は、10 秒を設定することを推奨します。
情報取得待機間隔は、10 秒を設定することを推奨します。
情報取得タイムアウト時間は、5 秒を設定することを推奨します。

[注意]

情報取得間隔が短いほどリアルタイムに近い情報を得ることができますが、本装置とネットワークの負荷は増大します。システム、ネットワークのパフォーマンスに応じて適切な値を設定してください。

[未設定時]

情報取得間隔、情報取得待機間隔、情報取得タイムアウト時間を設定しないものとみなされ、アクセスポイント情報の取得を行いません。

14.7 管理外無線 LAN アクセスポイント 情報

14.7.1 nodemanager wlan scan unmanaged

[機能]

管理外無線 LAN アクセスポイントの設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager wlan scan unmanaged <number> <name> <mac>

[オプション]

<number>

- 管理外無線 LAN アクセスポイント定義番号
管理外無線 LAN アクセスポイントの通し番号を 10 進数で指定します。

<name>

- 管理外無線 LAN アクセスポイント名
管理外無線 LAN アクセスポイント名を、0x21,0x23 ~ 0x7e の 8 文字以内の ASCII 文字列で指定します。

<mac>

- MAC アドレス
管理外無線 LAN アクセスポイントの 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]

指定した MAC アドレスを有する無線 LAN アクセスポイントを、管理外無線 LAN アクセスポイントとして指定した名前で設定します。

無線 LAN 監視が検出した無線 LAN アクセスポイントの MAC アドレスが、管理外無線 LAN アクセスポイントとして設定した MAC アドレスと一致する場合は、検出された無線 LAN アクセスポイントは不明無線 LAN アクセスポイントとみなされません。

使用している場所、目的などが明らかで監視する必要がない無線 LAN アクセスポイントを管理外無線 LAN アクセスポイントとして設定します。

すでに管理外無線 LAN アクセスポイントに設定されている無線 LAN アクセスポイントと同じ MAC アドレスを指定した場合、このコマンドの設定は無効になります。

[注意]

管理無線 LAN アクセスポイントの稼働情報を取得した結果、いったん管理外無線 LAN アクセスポイントとして設定された MAC アドレスが、あとから管理無線 LAN アクセスポイントの MAC アドレスと重複していることが判明する場合があります。この場合、MAC アドレスが重複した管理外無線 LAN アクセスポイントの情報は、システムによって自動的に削除されます。

[未設定時]

管理外無線 LAN アクセスポイントがないものとみなされます。

14.8 稼動監視情報

14.8.1 nodemanager icmpwatch interval

[機能]

稼動監視パラメタの設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager icmpwatch interval <period> <wait_period> <time_out>

[オプション]

<period>

- 稼動監視間隔
管理対象の管理機器に ping を送信する間隔時間を 1 ~ 600 秒の範囲の 10 進数で指定します。
単位は、m(分)、s(秒) のどちらかを指定します。

<wait_period>

- 稼動監視待機間隔
管理対象の管理機器への ping 送信の待機時間を 1 ~ 600 秒の範囲の 10 進数で指定します。
単位は、m(分)、s(秒) のどちらかを指定します。

<time_out>

- 稼動監視タイムアウト時間
管理対象の管理機器からの ping 応答待ちタイムアウト時間を 1 ~ 60 秒の範囲の 10 進数で指定します。
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]

無線 LAN 管理機能が、ping を使って有線 LAN 経由で管理機器の稼動状況を監視する際の待ち時間を設定します。稼動監視間隔は、ある管理機器に ping を送信し応答を得たあと、次の管理機器に ping を送信するまでの間隔です。

稼動監視待機間隔は、すべての監視対象の管理機器に ping を送信したあと、次の ping 送信を開始するまでの待ち時間です。

稼動監視タイムアウト時間は、管理機器からの ping 応答待ち許容時間です。管理機器からの ping 応答がなく稼動監視応答待ちタイムアウトとなった場合は、次の管理機器へ ping を送信します。

稼動監視間隔は、10 秒を設定することを推奨します。

稼動監視待機間隔は、10 秒を設定することを推奨します。

稼動監視応答待ちタイムアウト時間は、5 秒を設定することを推奨します。

[注意]

稼動監視間隔が短いほどリアルタイムに近い情報を得ることができますが、本装置とネットワークの負荷は増大します。システム、ネットワークのパフォーマンスに応じて適切な値を設定してください。

[未設定時]

稼働監視間隔、稼働監視待機間隔、稼働監視応答待ちタイムアウト時間を設定しないものとみなされ、稼働監視を行いません。

14.8.2 nodemanager icmpwatch threshold

[機能]

稼働監視 通信異常判定しきい値の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager icmpwatch threshold <count>

[オプション]

<count>

- 通信異常判定しきい値
稼働監視が通信異常の疑いありとみなすしきい値を 1～11 の範囲の 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]

稼働監視は、管理機器に ping を送り、その応答によって管理機器との通信状態を確認します。
管理機器との通信が確認できない回数が通信異常判定しきい値に達した場合は、「active? (通信異常の疑い)」のステータスになります。通信が確認できない回数が通信異常判定しきい値を超えると「inactive(通信異常)」のステータスになります。

[未設定時]

通信異常判定しきい値は 6 が設定されたものとみなされます。

```
nodemanager icmpwatch threshold 6
```

14.9 無線 LAN 監視情報

14.9.1 nodemanager wlan scan interval

[機能]

スキャンレポート取得パラメタの設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager wlan scan interval <period> <wait_period> <time_out>

[オプション]

<period>

- スキャンレポート取得間隔
監視用無線 LAN アクセスポイントからスキャンレポートを取得する間隔時間を 1 ~ 600 秒の範囲の 10 進数で指定します。
単位は、m(分)、s(秒) のどちらかを指定します。

<wait_period>

- スキャンレポート取得待機間隔
監視用無線 LAN アクセスポイントからのスキャンレポート取得の待機時間を 1 ~ 600 秒の範囲の 10 進数で指定します。
単位は、m(分)、s(秒) のどちらかを指定します。

<time_out>

- スキャンレポート取得タイムアウト時間
監視用無線 LAN アクセスポイントからスキャンレポート受信待ちタイムアウト時間を 1 ~ 60 秒の範囲の 10 進数で指定します。
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]

無線 LAN 管理機能が、スキャン要求設定コマンド (nodemanager node <number> wlan scan) によって設定した監視用無線 LAN アクセスポイントからスキャンレポートを取得する際の待ち時間を設定します。スキャンレポート取得間隔は、ある監視用無線 LAN アクセスポイントのスキャンレポートを取得してから次の監視用無線 LAN アクセスポイントのスキャンレポートを取得するまでの間隔です。

スキャンレポート取得待機間隔は、すべての監視用無線 LAN アクセスポイントからスキャンレポートを取得したあと、次のスキャンレポート取得を開始するまでの待ち時間です。

スキャンレポート取得タイムアウト時間は、監視用無線 LAN アクセスポイントからのスキャンレポート受信待ち許容時間です。監視用無線 LAN アクセスポイントからのスキャンレポート受信がなくスキャンレポート受信待ちタイムアウトとなった場合は、次の監視用無線 LAN アクセスポイントからスキャンレポート取得を行います。

スキャンレポート取得間隔は、10 秒を設定することを推奨します。

スキャンレポート取得待機間隔は、10 秒を設定することを推奨します。

スキャンレポート受信待ちタイムアウト時間は、60 秒を設定することを推奨します。

[注意]

スキャンレポート取得間隔が短いほどリアルタイムに近い情報を得ることができますが、本装置とネットワークの負荷は増大します。システム、ネットワークのパフォーマンスに応じて適切な値を設定してください。

[未設定時]

スキャンレポート取得間隔、スキャンレポート取得待機間隔、スキャンレポート受信待ちタイムアウト時間を設定しないものとみなされ、スキャンレポートの取得を行いません。

14.9.2 nodemanager wlan scan error threshold

[機能]

無線 LAN 監視 通信異常判定しきい値の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager wlan scan error threshold <count>

[オプション]

<count>

- 通信異常判定しきい値
無線 LAN 監視が通信異常の疑いありとみなすしきい値を 1~11 の範囲の 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]

無線 LAN 監視は、監視用無線 LAN アクセスポイントにより無線 LAN アクセスポイントを検出することによって通信状態を確認します。無線 LAN アクセスポイントの未検出が通信異常判定しきい値に達した場合は、「active? (通信異常の疑い)」のステータスになります。連続未検出が通信異常判定しきい値を超えると「inactive (通信異常)」のステータスになります。

[未設定時]

通信異常判定しきい値に 6 が設定されたものとみなされます。

```
nodemanager wlan scan error threshold 6
```

14.10 監視ログ・パラメタ情報

14.10.1 nodemanager log

[機能]

監視ログのパラメタの設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager log <lines>

[オプション]

<lines>

- 監視ログ保持件数
監視ログの最大件数を 100 ~ 10000 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]

監視ログ保持件数は保持する監視ログの最大件数を設定します。

[未設定時]

監視ログ保持件数に 1000 を設定したものとみなされます。

```
nodemanager log 1000
```

14.10.2 nodemanager wlan sta rssi

[機能]

無線 LAN 端末の RSSI 監視のパラメタの設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

nodemanager wlan sta rssi <param> <low_rssi>

[オプション]

<param>

- RSSI 評価母数
RSSI 評価値を求めるのに必要な RSSI データ数を 1 ~ 50 の範囲の 10 進数で指定します。

<low_rssi>

- RSSI 最低しきい値
RSSI 低下通知の契機となる RSSI の最低しきい値を 1 ~ 255 の範囲の 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]

無線 LAN 端末は端末の状態の変化によって RSSI が短期間に増減したり、アソシエーションが突然解除されることが想定されます。そのため RSSI 監視は電波品質の評価のために複数の RSSI データから評価値を求めます。RSSI 評価母数には、評価値を求める際の RSSI のデータ数を設定します。

RSSI と信号強度 (dBm) 関係は、以下のとおりです。

$$\text{dBm} = (\text{RSSI 値}) - 95$$

得られた RSSI 評価値が、RSSI 最低しきい値を下回るとき、電波品質の低下を通知するメッセージが監視ログに出力されます。

[注意]

無線 LAN 端末の RSSI 監視は、無線 LAN 端末の情報を取得する管理機器に対してのみ実行することができます。

[未設定時]

RSSI 評価母数に 10、RSSI 最低しきい値に 20 が設定されたものとみなされます。

```
nodemanager wlan sta rssi 10 20
```

第 15 章 装置情報の設定

15.1 SNMP 情報

15.1.1 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.1.2 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

15.1.3 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

15.1.4 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

15.1.5 snmp agent address

[機能]

SNMP エージェントアドレスの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

15.1.6 snmp agent engineid

[機能]

SNMP エンジン ID 名の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

15.1.7 snmp manager

[機能]

SNMP ホスト情報の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

15.1.8 snmp trap coldstart

[機能]

coldStart トラップの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.1.9 snmp trap linkdown

[機能]

linkDownトラップの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.1.10 snmp trap linkup

[機能]

linkUp トラップの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.1.11 snmp trap authfail

[機能]

authenticationFailure トラップの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```


15.1.12 snmp trap noserror

[機能]

nosError トラップの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.1.13 snmp user name

[機能]

SNMP ユーザ名の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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。

15.1.14 snmp user address

[機能]

SNMP ホストアドレスの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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。
省略時は、0 を指定したものとみなされます。

<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。

15.1.15 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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。
省略時は、0 を指定したものとみなされます。

<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。

15.1.16 snmp user auth

[機能]

認証プロトコルの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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
```

15.1.17 snmp user priv

[機能]

暗号プロトコルの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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
```


15.1.18 snmp user write

[機能]

MIB 書き込み許可ビューの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<access>

書き込み可能な MIB に対しての書き込みを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
```

15.1.19 snmp user read

[機能]

MIB 読み出し許可ビューの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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
```

15.1.20 snmp user notify

[機能]

トラップ通知許可ビューの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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
```

15.1.21 snmp view subtree

[機能]

SNMP MIB ビュー情報の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
省略時は、0 を指定したものとみなされます。

<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。
省略時は、0 を指定したものとみなされます。

<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	
radiusMIB	1.3.6.1.2.1.67	
enterprises	1.3.6.1.4.1	
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。

15.2 システムログ情報

15.2.1 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

15.2.2 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

15.2.3 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```


15.2.4 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.2.5 syslog security

[機能]

システムログ情報の出力対象セキュリティの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

syslog security <securetype>

[オプション]

<securetype>

- セキュリティ対象
セキュリティログ情報の出力対象を、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。
 - ids** IDS モジュールを対象とする場合に指定します。
 - proxydns**
 ProxyDNS モジュールを対象とする場合に指定します。
 - none** すべてのモジュールを対象外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セキュリティを指定します。

[未設定時]

すべてが設定されたものとみなされます。

```
syslog security ids,proxydns
```

15.2.6 syslog dupcut

[機能]

システムログ情報の重複メッセージ出力の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

syslog dupcut <cut>

[オプション]

<cut>

- yes
直前に出力されたメッセージが重複した場合、出力しません。
- no
重複チェックを行わず、すべてのメッセージを出力します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

システムログにメッセージを出力する際、直前に出力したメッセージと重複した場合に出力するかどうかを指定します。

[未設定時]

重複チェックを行わないものとみなされます。

```
syslog dupcut no
```

15.2.7 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.2.8 syslog logging nodemgr access

[機能]

シスログ情報の無線 LAN 管理アクセス履歴出力の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

syslog logging nodemgr access <mode>

[オプション]

<mode>

- enable
無線 LAN 管理のアクセス履歴をシステムログに出力します。
- disable
無線 LAN 管理のアクセス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]

無線 LAN 管理の以下に示すアクセス履歴をシステムログに出力するかどうかを指定します。

- ログイン
- ログアウト
- コマンド実行 (syslog command-logging enable 時)

[未設定時]

無線 LAN 管理のアクセス履歴をシステムログに出力するものとみなされます。

```
syslog logging nodemgr access enable
```

15.3 自動時刻設定情報

15.3.1 time auto server

[機能]

時刻情報の提供サーバの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

[未設定時]

自動時刻設定を行わないものとみなされます。

15.3.2 time auto interval

[機能]

時刻情報の自動設定間隔の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.3.3 time zone

[機能]

時刻情報のタイムゾーンの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

[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

15.4 ProxyDNS 情報

15.4.1 proxydns domain

[機能]

プロキシ DNS の順引き動作条件の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

proxydns domain <count> <qtype> <qname> <address>/<mask> reject (転送要求の破棄)
 proxydns domain <count> <qtype> <qname> <address>/<mask> static <ipaddress> (固定 DNS サーバ指定)
 proxydns domain <count> <qtype> <qname> <address>/<mask> dhcp <interface> (DHCP 指定)

[オプション]

<count>

- 転送先定義番号
 転送先定義番号として、0～49の10進数で指定します。
 指定した値は、設定完了時に順方向にソートされてリナンバリングされます。
 また、指定した定義番号と同じ値を持つ転送先定義番号が存在する場合は、既存定義の前に挿入されます。

<qtype>

- 問い合わせタイプ番号
 1～11または13～65535の10進数で指定します。
 以下に、問い合わせタイプの一部分を示します。

名称	番号	説明
A	1	ホストアドレス
NS	2	ドメインに対して認証されたネーム・サーバ
CNAME	5	別名 (Alias名、ドメイン名)
SOA	6	ゾーン管理開始
PTR	12	ドメイン名空間のほかの部分へのポインタ
HINFO	13	ホストが使用するCPUとOS
MX	15	ドメインに対するメール交換
SRV	33	サービス

- any
 PTR(12)を除くすべてのタイプを対象にする場合に指定します。

<qname>

- ホスト名
 条件となるホスト名を、80文字以内で指定します。
 ホスト名には、以下のワイルドカードを使用できます。
 - * (アスタリスク)
 0文字以上の任意の文字列とみなされます。

-
- ?(クエスチョンマーク)
任意の一文字とみなされます。

以下に、ワイルドカードを使用したホスト名の記述例および一致例を示します。

www.*.com

以下のどの文字列とも一致するとみなされます。

- www.testa.com
- www.test1.test.com

test 以下のどの文字列とも一致するとみなされます。

- www.test.com
- test.com
- test.co.jp

www.test?.com

以下のどの文字列とも一致するとみなされます。

- www.test1.com
- www.test2.com
- www.testA.com

なお、ホスト名をチェックするときに、大文字と小文字の区別はされません。

<address>/<mask>

- 送信元 IPv4 アドレス/マスクビット数 (またはマスク値)
対象となる送信元 IPv4 アドレスとマスクビット数の組み合わせを指定します。
マスク値は、最上位ビットから 1 で連続した値にしてください。
- any
すべてのアドレスを対象と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。

<ipaddress>

- DNS サーバ IP アドレス
要求を転送する 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

<interface>

DHCP クライアントが動作しているインタフェースを以下の範囲で指定します。

範囲	機種
lan0 ~ lan19	SR-M20AP2 SR-M20AP1
lan0	SR-M20AC2 SR-M20AC1

[動作モード]

構成定義モード (管理者クラス)

[説明]

プロキシ DNS の順引き動作条件を設定します。
各コマンドについて説明します。

転送要求の破棄

```
proxysql domain <count> <qtype> <qname> <address>/<mask> reject
```

指定した DNS 要求の転送を無効にするフィルタを設定します。

<qname> で指定するホスト名は、DNS データベースに登録されていても、そのホスト (群) へのアクセスを制限する場合に使用します。条件と一致した場合は破棄されます。

固定 DNS サーバの指定

```
proxysql domain <count> <qtype> <qname> <address>/<mask> static <ipaddress>
```

指定した DNS 要求の転送先 IP アドレスを指定します。

DHCP 指定

```
proxysql domain <count> <qtype> <qname> <address>/<mask> dhcp <interface>
```

指定のインタフェースで動作している DHCP クライアントが取得した DNS サーバへ DNS 要求を転送します。

[未設定時]

プロキシ DNS の順引き動作条件を設定しないものとみなされます。

15.4.2 proxydns domain move

[機能]

プロキシ DNS の順引き動作条件の順序の変更

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

proxydns domain move <count> <new_count>

[オプション]

<count>

- 変更前転送先定義番号
順序を変更する転送先定義番号を指定します。

<new_count>

- 新しい転送先定義番号
<count>に対して、新しい順序を指定します。
すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

プロキシ DNS の順引き動作条件の順序を変更します。
すでに存在する転送先定義番号と同じ番号を指定した場合は、指定した定義の前に挿入されます。

15.4.3 proxydns address

[機能]

プロキシ DNS の逆引き動作条件の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

proxydns address <count> <address>/<mask> reject (転送要求の破棄)
 proxydns address <count> <address>/<mask> static <ipaddress> (固定 DNS サーバ指定)
 proxydns address <count> <address>/<mask> dhcp <interface> (DHCP 指定)

[オプション]

<count>

- 転送先定義番号
 転送先定義番号として、0～49の10進数で指定します。
 指定した値は、設定完了時に順方向にソートされてリナンバリングされます。
 また、指定した定義番号と同じ値を持つ転送先定義番号が存在する場合は、既存定義の前に挿入されます。

<address>/<mask>

逆引き対象 IPv4 アドレス/マスクビット数を指定します。

- 逆引き対象 IPv4 アドレス/マスクビット数 (またはマスク値)
 逆引き対象 IPv4 アドレスとマスクビット数の組み合わせを指定します。
 マスク値は、最上位ビットから1で連続した値にしてください。
- any
 すべてのアドレスの逆引きを対象とする場合に指定します。

<ipaddress>

- DNS サーバ IP アドレス
 要求を転送する 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

<interface>

DHCP クライアントが動作しているインタフェースを以下の範囲で指定します。

範囲	機種
lan0 ~ lan19	SR-M20AP2 SR-M20AP1
lan0	SR-M20AC2 SR-M20AC1

[動作モード]

構成定義モード (管理者クラス)

[説明]

プロキシ DNS の逆引き動作条件を設定します。
各コマンドについて説明します。

転送要求の破棄

```
proxysql address <count> <address>/<mask> reject
```

指定した DNS 要求の転送を無効にするフィルタを設定します。

<qname> で指定するホスト名は、DNS データベースに登録されていても、そのホスト (群) へのアクセスを制限する場合に使用します。条件と一致した場合は破棄されます。

固定 DNS サーバの指定

```
proxysql address <count> <address>/<mask> static <ipaddress>
```

指定した DNS 要求の転送先 IP アドレスを指定します。

転送先への経路は、IP ルーティングに従って決められます。

DHCP 指定

```
proxysql address <count> <address>/<mask> dhcp <interface>
```

指定のインタフェースで動作している DHCP クライアントが取得した DNS サーバへ DNS 要求を転送します。

[未設定時]

プロキシ DNS の逆引き動作条件を設定しないものとみなされます。

15.4.4 proxydns address move

[機能]

プロキシ DNS の逆引き動作条件の順序の変更

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

proxydns address move <count> <new_count>

[オプション]

<count>

- 変更前転送先定義番号
順序を変更する転送先定義番号を指定します。

<new_count>

- 新しい転送先定義番号
<count>に対して、新しい順序を指定します。
すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

プロキシ DNS の逆引き動作条件の順序を変更します。
すでに存在する転送先定義番号と同じ番号を指定した場合は、指定した定義の前に挿入されます。

15.4.5 proxydns unicode

[機能]

プロキシ DNS の問い合わせパケットの透過の可否の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

proxydns unicode <action>

[オプション]

<action>

パケットを透過するかどうかを指定します。

- pass
該当するパケットを透過する場合に指定します。
- reject
該当するパケットを破棄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]

プロキシ DNS の問い合わせ名 (QNAME) に非表示文字が含まれる場合に、その問い合わせのパケットを透過するかどうかを設定します。

[未設定時]

該当パケットを破棄するものとみなされます。

```
proxydns unicode reject
```


15.5 ProxyARP 情報

15.5.1 proxyarp use

[機能]

ProxyARP 機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

[未設定時]

ProxyARP 機能を使用するものとみなされます。

```
proxyarp use on
```

15.5.2 proxyarp unicast

[機能]

ユニキャスト ARP 要求の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

proxyarp unicast <action>

[オプション]

<action>

- pass
ユニキャスト ARP 要求を無線 LAN 側へ転送します。
- reject
ユニキャスト ARP 要求を無線 LAN 側へ転送しません。

[動作モード]

構成定義モード (管理者クラス)

[説明]

ユニキャスト ARP 要求を無線 LAN 側へ転送するかどうかを設定します。
無線 LAN 側端末が存在しない場合は転送されません。

[未設定時]

ユニキャスト ARP 要求を無線 LAN 側へ転送するものとみなされます。

```
proxyarp unicast pass
```

15.6 ホストデータベース情報

15.6.1 host name

[機能]

ホストデータベース情報のホスト名の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

host <number> name <name>

[オプション]

<number>

- 定義番号
ホストデータベース情報の定義番号を、0～99の10進数で指定します。

<name>

- ホスト名
ホスト名を、英数字、"-"(ハイフン)、"."(ピリオド)で構成される80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]

本装置配下に接続されたホストのホスト名をホストデータベースに設定します。
本コマンドは、簡易DNSサーバ機能から利用されます。
以下に、機能とパラメタの関係を示します。

機能	パラメタ	name	ip_address
簡易DNSサーバ			
			:有効、 -:無効

[未設定時]

ホストデータベース情報のホスト名を設定しないものとみなされます。

15.6.2 host ip address

[機能]

ホストデータベース情報の IP アドレスの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

host <number> ip address <ip_address>

[オプション]

<number>

- 定義番号
ホストデータベース情報の定義番号を、0～99の10進数で指定します。

<ip_address>

- IP アドレス
ホストの IP アドレスを指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

本装置配下に接続されたホストの IP アドレスをホストデータベースに設定します。
本コマンドは、簡易 DNS サーバ機能から利用されます。
以下に、機能とパラメタの関係を示します。

機能	パラメタ	name	ip_address
簡易DNSサーバ			
			:有効、 -:無効

[未設定時]

ホストデータベース情報の IP アドレスを設定しないものとみなされます。

15.7 スケジュール情報

15.7.1 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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、0～19の10進数で指定します。
- any
未使用のスケジュール定義番号を使用して定義します。

<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。
- 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]

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。

15.7.2 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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、0～19の10進数で指定します。
- any
未使用のスケジュール定義番号を使用して定義します。

<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
```

15.8 装置ランプ情報

15.8.1 lamp mode

[機能]

運用中ランプ動作の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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

15.8.2 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.9 その他

15.9.1 addact

[機能]

コマンド実行予約の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 2036 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、1999 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 9901010200 reset config2
# show addact
0 9901010200 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。

15.9.2 watchdog service

[機能]

ウォッチドッグリセットの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

watchdog service <mode>

[オプション]

<mode>

- on
ウォッチドッグリセット機能を起動する場合に指定します。
- off
ウォッチドッグリセット機能を停止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]

ウォッチドッグリセット機能の起動または停止を設定します。

<mode>に"on"を指定した場合、本装置がハングアップすると16～48秒以内にリセットがかかり再起動します。

<mode>に"off"を指定した場合、本装置がハングアップしてもリセットがかかりません。

本設定は構成定義を保存したあと、本装置のリセットまたは電源の再投入を行うことによって反映されます。

[未設定時]

ウォッチドッグリセット機能が起動するものとみなされます。

watchdog service on

15.9.3 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.9.4 telnetinfo

[機能]

TELNET 接続サービスの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.9.5 mflag

[機能]

CE 保守ログインの可否の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

mflag <mode>

[オプション]

<mode>

- on
CE 専用パスワードによるログインを許可する場合に指定します。
- off
CE 専用パスワードによるログインを拒否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]

CE 保守ログインを許可するかどうかを設定します。

[未設定時]

CE 専用パスワードによるログインを拒否するものとみなされます。

```
mflag off
```

15.9.6 sysname

[機能]

本装置の名称の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

sysname <name>

[オプション]

<name>

- 名称
本装置の名称を、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]

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べきです。

[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。

15.9.7 serverinfo ftp

[機能]

FTP サーバ機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.9.8 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
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]

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。

15.9.9 serverinfo ftp filter move

[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優先順序の変更

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

serverinfo ftp filter move <count> <new_count>

[オプション]**<count>**

- 対象フィルタリング定義番号
優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
<count>に対する新しい順序を、0~9の10進数で指定します。
すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[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の優先順序を変更します。

15.9.10 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.9.11 serverinfo sftp

[機能]

SSH FTP サーバ機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 on、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]

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 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。

[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
```

15.9.12 serverinfo telnet

[機能]

TELNET サーバ機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.9.13 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
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]

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。

15.9.14 serverinfo telnet filter move

[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優先順序の変更

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

serverinfo telnet filter move <count> <new_count>

[オプション]

<count>

- 対象フィルタリング定義番号
優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
<count>に対する新しい順序を、0~9の10進数で指定します。
すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[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の優先順序を変更します。

15.9.15 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.9.16 serverinfo ssh

[機能]

SSH ログインサーバ機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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、および serverinfo sftp ip コマンドの設定が 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。

本設定が on、および serverinfo sftp ip コマンドの設定が on 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パスワード入力したあとに拒否されます。

[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。

[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
```

15.9.17 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
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]

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。

15.9.18 serverinfo ssh filter move

[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優先順序の変更

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

serverinfo ssh filter move <count> <new_count>

[オプション]

<count>

- 対象フィルタリング定義番号
優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
<count>に対する新しい順序を、0~9の10進数で指定します。
すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[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の優先順序を変更します。

15.9.19 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.9.20 serverinfo http

[機能]

HTTP サーバ機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1

[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
```

15.9.21 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]



[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。
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]

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。

15.9.22 serverinfo http filter move

[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優先順序の変更

[適用機種]



[入力形式]

```
serverinfo http filter move <count> <new_count>
```

[オプション]

<count>

- 対象フィルタリング定義番号
優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
<count>に対する新しい順序を、0~9の10進数で指定します。
すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[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の優先順序を変更します。

15.9.23 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-M20AP2 SR-M20AP1

[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
```

15.9.24 serverinfo dns

[機能]

DNS サーバ機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

serverinfo dns ip <mode>

[オプション]

<mode>

- on
DNS サーバ機能を有効にします。
- off
DNS 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]

DNS サーバ (スタティック) 機能および ProxyDNS 機能を有効にするかどうかを設定します。

[未設定時]

DNS サーバ機能を有効にするものとみなされます。

```
serverinfo dns ip on
```

15.9.25 serverinfo dns filter

[機能]

DNS 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

serverinfo dns 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]

DNS 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]

DNS 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。

15.9.26 serverinfo dns filter move

[機能]

DNS サーバ機能に対するアプリケーションフィルタの優先順序の変更

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

serverinfo dns filter move <count> <new_count>

[オプション]

<count>

- 対象フィルタリング定義番号
優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
<count>に対する新しい順序を、0~9の10進数で指定します。
すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[動作モード]

構成定義モード (管理者クラス)

[説明]

DNS サーバ機能に対するアプリケーションフィルタの優先順序を変更します。

15.9.27 serverinfo dns filter default

[機能]

DNS 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

serverinfo dns filter default <action>

[オプション]

<action>

DNS 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]

DNS 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 dns filter default accept
```

15.9.28 serverinfo sntp

[機能]

SNTP サーバ機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.9.29 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
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]

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。

15.9.30 serverinfo sntp filter move

[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優先順序の変更

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

serverinfo sntp filter move <count> <new_count>

[オプション]

<count>

- 対象フィルタリング定義番号
優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
<count>に対する新しい順序を、0~9の10進数で指定します。
すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[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の優先順序を変更します。

15.9.31 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

15.9.32 serverinfo time ip tcp

[機能]

TCP による TIME サーバ機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

serverinfo time ip tcp <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 tcp on
```

15.9.33 serverinfo time ip udp

[機能]

UDP による TIME サーバ機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

serverinfo time ip udp <mode>

[オプション]

<mode>

- on
UDP による TIME サーバ機能を有効にします。
- off
UDP 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]

UDP 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]

UDP 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 udp on
```

15.9.34 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

15.9.35 serverinfo time filter move

[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優先順序の変更

[適用機種]

SR-M20AP2	SR-M20AP1	SR-M20AC2	SR-M20AC1
-----------	-----------	-----------	-----------

[入力形式]

serverinfo time filter move <count> <new_count>

[オプション]**<count>**

- 対象フィルタリング定義番号
優先順序を変更するフィルタリング定義番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
<count>に対する新しい順序を、0~9の10進数で指定します。
すでにこの定義番号を持つ定義が存在する場合は、その定義の前に挿入されます。

[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の優先順序を変更します。

15.9.36 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

第 16 章 モード操作コマンド/ターミナル操作コマンド

16.1 モード操作

16.1.1 admin

[機能]

管理者クラスに移行する

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

admin [<user>]

[オプション]

<user>

- 管理者名
省略時は、"admin"を指定したものと動作します。

[動作モード]

運用管理モード (一般ユーザクラス)

[説明]

一般ユーザクラスから管理者クラスに移行します。
su コマンドと同じ機能です。
移行する際にパスワードを尋ねられますので、管理者パスワードを入力してください。
管理者クラスから一般ユーザクラスに戻るには、exit, end, quit, ! コマンドを実行します。

[注意]

terminal コマンドおよび alias コマンドで設定した内容は、管理者モードに引き継がれません。

[メッセージ]

Password:

管理者パスワードを入力してください。

<ERROR> Authentication failed

管理者パスワードが正しくないため、管理者クラスに移行できませんでした。
正しい管理者パスワードを入力してください。

<WARNING> weak <user> 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 <user> 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 <user> 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。

[実行例]

```
> admin  
Password:  
# exit  
> admin administrator  
Password:  
# exit  
>
```

16.1.2 su

[機能]

管理者クラスに移行する

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

su [<user>]

[オプション]

<user>

- 管理者名
省略時は、"admin"を指定したものと動作します。

[動作モード]

運用管理モード (一般ユーザクラス)

[説明]

一般ユーザクラスから管理者クラスに移行します。
admin コマンドと同じ機能です。
移行する際にパスワードを尋ねられますので、管理者パスワードを入力してください。
管理者クラスから一般ユーザクラスに戻るには、exit, end, quit, ! コマンドを使用します。

[注意]

terminal コマンドおよび alias コマンドで設定した内容は、管理者モードに引き継がれません。

[メッセージ]

Password:

管理者パスワードを入力してください。

<ERROR> Authentication failed

管理者パスワードが正しくないため、管理者クラスに移行できませんでした。
正しい管理者パスワードを入力してください。

<WARNING> weak <user> 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 <user> 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 <user> 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。

[実行例]

```
> su
Password:
# exit
> su administrator
Password:
# exit
>
```

16.1.3 exit

[機能]

クラス、モード、構成定義階層を戻る、またはログアウトする

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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]

運用管理モードでは、admin コマンドを実行して一般ユーザクラスから管理者クラスに移行していた場合は一般ユーザクラスに戻ります。それ以外の場合はログアウトします。

構成定義モードでは、構成定義階層機能が有効で最上位階層以外の場合はひとつ上位階層に移動します。それ以外の場合、構成定義を変更していなければ運用管理モードに戻り、構成定義を変更していればエラーメッセージが表示されて構成定義モードのままです。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。

[注意]

terminal コマンドおよび alias コマンドで設定した内容は、ログアウト時に破棄されます。

[メッセージ]

```
<ERROR> The candidate-config has been changed but not committed.
```

構成定義情報が反映されていません。

構成定義情報を反映してください。構成定義情報を反映しないで運用管理モードに戻る場合は、end コマンドまたは quit コマンドを使用してください。

[実行例]

```
(config)# exit
<ERROR> The candidate-config has been changed but not committed.
(config)# end
<WARNING> The candidate-config has been changed but not committed.
# exit
Login:
```

16.1.4 configure

[機能]

構成定義モードに移行する

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

構成定義モードに移行してから Ctrl+O キーを入力すると、構成定義階層機能が有効になります。

構成定義階層機能を有効にすると、入力した構成定義コマンドに応じて階層を移動したように振舞い、構成定義階層以降の引数を入力するだけで構成定義コマンドを実行できます。階層移動している状態でもコマンド名から入力することで通常のコマンドも実行できます。

構成定義階層は入力プロンプトに表示されます。

構成定義階層機能を無効にするには、Ctrl+G キーを入力してください。構成定義階層機能については、コマンドユーザズガイドの「シェルを使う」を参照してください。

構成定義モードから運用管理モードに戻るには、状況に応じて exit, end, quit, ! コマンドを実行してください。

[注意]

構成定義を変更した状態では exit コマンドおよび ! コマンドで運用管理モードに戻ることができません。end コマンドまたは quit コマンドで強制的に運用管理モードに戻ることができます。

構成定義階層機能が有効なとき、terminal prompt コマンドで入力プロンプト文字列を変更して構成定義階層を含めていない場合は、入力プロンプトに構成定義階層は表示されません。

[実行例]

```
# configure
(config)#                               (CTRL+Oキーを入力して構成定義階層機能を有効にする)
<NOTICE> Directory mode is enabled. To disable, type Ctrl+G.
(config)# lan 0 ip
(config-lan-0-ip)# address 192.168.0.1/24 3
(config-lan-0-ip)# show
address 192.168.0.1/24 3
(config-lan-0-ip)# show candidate-config
lan 0 ip address 192.168.0.1/24 3
(config-lan-0-ip)#                               (Ctrl+Gキーを入力して構成定義階層機能を無効にする)
<NOTICE> Directory mode is disabled.
(config)#
```

16.1.5 end

[機能]

運用管理モードに戻る

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

end

[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]

構成定義モードから運用管理モードに戻ります。
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。
quit コマンドと同じ機能です。

[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)# end  
#
```

16.1.6 quit

[機能]

運用管理モードに戻る

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

quit

[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]

構成定義モードから運用管理モードに戻ります。
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。
end コマンドと同じ機能です。

[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)# quit  
#
```

16.1.7 top

[機能]

構成定義階層を最上位階層に移動する

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

top

[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]

構成定義モードで構成定義階層機能が有効であれば、最上位階層に移動します。最上位階層の場合はそのままです。

構成定義階層機能が無効であれば、何もしません。

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。

[実行例]

```
(config-lan-0-ip)# top (lan 0 ip 階層で実行)
(config)#
```


16.1.8 up

[機能]

構成定義階層をひとつ上位階層に移動する

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

up

[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]

構成定義モードで構成定義階層機能が有効な場合、構成定義階層をひとつ上位階層に移動します。最上位階層の場合はそのままです。

構成定義階層機能が無効であれば、何もしません。

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。

[実行例]

```
(config-lan-0-ip)# up (lan 0 ip 階層で実行)
(config-lan-0)#
```

16.1.9 !

[機能]

クラス、モード、構成定義階層を戻る

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

!

[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]

運用管理モードでは、admin コマンドを実行して一般ユーザクラスから管理者クラスに移行していた場合は一般ユーザクラスに戻ります。それ以外の場合は運用管理モードのままログアウトはしません。

構成定義モードでは、構成定義階層機能が有効で最上位階層以外の場合はひとつ上位階層に移動します。それ以外の場合、構成定義を変更していなければ運用管理モードに戻り、構成定義を変更していればエラーメッセージが表示されて構成定義モードのままです。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。

exit コマンドとほとんど同じ機能ですが、運用管理モードでログアウトしないことだけが異なります。

[実行例]

```
# configure (構成定義モードに移行)
(config)# ! (運用管理モードに戻る)
# ! (ログアウトはせずそのまま)
#
```

16.2 ターミナル操作

16.2.1 terminal pager

[機能]

ページャー機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

terminal pager { enable | disable }

[オプション]

enable

ページャー機能を使用します。

disable

ページャー機能を使用しません。

[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]

ページャー機能を使用するかどうかを指定します。

ページャー機能を使用する場合、コマンドを実行したときにコマンドの表示出力が 1 画面分表示されたらキー入力待ちとなり、キー入力で続きを表示したり、表示をさかのぼって再表示することができます。コマンドの表示出力が 1 画面に満たない場合は、キー入力待ちにならずにコマンド実行が終了します。

ただし、一部のコマンドは表示量が多過ぎるため、さかのぼって再表示できなかつたり、キー入力待ちすることなく最後まで表示されます。

ページャー機能はコマンド実行に対してのみ有効で、コマンド補完出力 (引数一覧表示、引数説明表示、コマンド形式表示) などに対しては機能しません。

端末の画面サイズは 24 行 80 桁であるものとして動作します。画面サイズが 24 行 80 桁以外の場合は、terminal window コマンドで行数と桁数を設定してください。設定しない場合は表示が乱れます。telnet か ssh でログインした場合は、自動的に行数と桁数が設定されますが、もし画面表示が乱れる場合は terminal window コマンドで行数と桁数を設定してください。

キー入力待ちのとき、以下のようなプロンプトが表示されます。

MORE(xx%):

(xx は全体バイト数に対する表示済みバイト数の割合)

または

MORE: (さかのぼって再表示できない場合)

キー入力待ち時の入力キーと動作の一覧を以下に示します。^x は CTRL キーを押しながら x キーを押すことを、M-x は ESC キーを押してから x キーを押すことを表しています。

入力キー	動作	
1 2 3 4 5 6 7 8 9 0	行数、行番号、回数指定(以下のキー入力前に1以上を指定)	
c	最後まで表示	
f ^F ^V	SPACE	一画面または指定行数前進(途中の行は省略)
b ^B M-v	BS	一画面または指定行数後退(途中の行は省略)
z		一画面の行数を指定行数に変更し一画面前進
w		一画面の行数を指定行数に変更し一画面後退
j ^J e ^E ^N	RETURN	一行または指定行数前進(すべての行を表示)
k ^K y ^Y ^P		一行または指定行数後退(すべての行を表示)
d ^D		半画面の行数を指定行数に変更し半画面前進
u ^U		半画面の行数を指定行数に変更し半画面後退
g <		先頭画面または指定行番号以降表示
G >		最終画面または指定行番号以降表示
/検索パターン		順検索(指定回数)
?検索パターン		逆検索(指定回数)
n		同方向に再検索
N		逆方向に再検索
M-x		x(任意コマンド)を実行し、最後まで表示しても終了しない
r ^R ^L		画面再表示
^G		情報表示(行数、バイト数、割合)
h H		ヘルプ表示(キーバインド一覧)
q Q ^C		終了

1 逆戻りできない表示の場合は無効です。

行番号を指定する場合、画面上での行番号を指定します。コマンドが一行分として画面桁数以上出力した場合、画面上では複数の行として扱われます。先頭行番号は1です。

検索時にはプロンプトとしてスラッシュ(/)またはクエスチョン(?)が表示され、検索パターンを入力できるようになります。検索パターンは76文字まで入力できます。画面桁数が80桁未満の場合、画面桁数以上の検索パターンを入力すると画面表示が乱れますので、画面再表示を行ってください。

検索パターンで使用できる特殊文字を以下に示します。それ以外はその文字自身を検索します。

特殊文字	検索対象
.	任意の一文字
^	行頭 (ほかの文字と組み合わせて使用)
\$	行末 (ほかの文字と組み合わせて使用)
\<	単語開始 (ほかの文字と組み合わせて使用)
\>	単語終了 (ほかの文字と組み合わせて使用)
\x	x (xは < > 以外の文字)

検索で見つかった場合は、見つかった文字列が反転表示されます。

検索で見つからなかった場合は、以下のプロンプトが表示されるので、RETURNキーを入力してください。CTRL+Cを入力した場合は、コマンド出力表示が中断されます。

MORE : pattern not found (press RETURN)

情報表示した場合は、以下のようなプロンプトが表示されます。

```
MORE(line 1-22/515 lines, 1428/33473 bytes, 4%):
  a b c          d e          f
```

逆戻りできない表示の場合は以下のようなプロンプトが表示されます。

```
MORE(line 1-22 lines):
  a b
```

意味:

- a:** 画面最上行番号
- b:** 画面最下行番号
- c:** 全体行数
- d:** 表示バイト数
- e:** 全体バイト数
- f:** 表示バイト数に対する全体バイト数の割合 ($d \div e \times 100$)

ヘルプ表示時には、ヘルプ表示後、以下のプロンプトが表示されるので、RETURN キーを入力してください。CTRL+C を入力した場合は、コマンド出力表示が中断されます。

MORE : help (press RETURN)

[注意]

画面行数が 3 行以下の場合はページャー機能は動作しません。また、画面桁数がプロンプト文字列の長さ以下の場合は表示が乱れます。

本コマンドは運用管理コマンドですが、管理者クラスで設定した内容は save コマンドを実行することで構成定義情報として保存することができます。また、構成定義モードの delete コマンドで設定を削除することができます。

一般ユーザークラスで設定した内容は、ログアウト時や admin コマンド実行時に破棄され、保存することはできません。

[未設定時]

ページャー機能を使用しないものとみなされます。

```
terminal pager disable
```

16.2.2 terminal window

[機能]

ターミナル画面サイズの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

terminal window [column <column>] [line <line>]

[オプション]

column <column>

ターミナルの画面桁数を 10 進数で指定します。

line <line>

ターミナルの画面行数を 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]

ターミナルの画面サイズを指定します。

telnet 接続や ssh 接続の場合、接続時や画面サイズ変更時に telnet クライアントや ssh クライアントから通知されるターミナルの画面サイズが使用されます。

通知されたあとに本コマンドにより画面サイズを変更した場合は、本設定値が使用されます。

[注意]

本コマンドは運用管理コマンドですが、管理者クラスで設定した内容は save コマンドを実行することで構成定義情報として保存することができます。また、構成定義モードの delete コマンドで設定を削除することができます。

一般ユーザクラスで設定した内容は、ログアウト時や admin コマンド実行時に破棄され、保存することはできません。

正しい画面サイズを指定しなかった場合、コマンド入力やコマンド実行時の表示が乱れることがあります。

[未設定時]

ターミナル画面サイズを 80 桁、24 行にするものとみなされます。

```
terminal window column 80 line 24
```

16.2.3 terminal charset

[機能]

漢字コードの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

terminal charset {EUC | SJIS}

[オプション]**EUC**

ターミナルで使用する漢字コードに EUC コードを指定します。

SJIS

ターミナルで使用する漢字コードに ShiftJIS コードを指定します。

[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]

ターミナルで使用する漢字コードを指定します。

[注意]

本コマンドは運用管理コマンドですが、管理者クラスで設定した内容は save コマンドを実行することで構成定義情報として保存することができます。また、構成定義モードの delete コマンドで設定を削除することができます。

一般ユーザクラスで設定した内容は、ログアウト時や admin コマンド実行時に破棄され、保存することはできません。

[未設定時]

ターミナルで使用する漢字コードに EUC が設定されたものとみなされます。

```
terminal charset EUC
```

16.2.4 terminal prompt

[機能]

入力プロンプトの設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
terminal prompt login "<prompt>"
terminal prompt user "<prompt>"
terminal prompt admin "<prompt>"
```

[オプション]

login

ログイン時の入力プロンプトを指定します。

user

一般ユーザクラスでログインしたときのコマンド入力プロンプトを指定します。

admin

管理者クラスでログインしたときのコマンド入力プロンプトを指定します。

<prompt>

入力プロンプト文字列を指定します。最大 80 文字です。

[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) (user オプション)

運用管理モード (管理者クラス) (login,admin オプション)

構成定義モード (管理者クラス)

[説明]

ログインプロンプト、およびコマンド入力プロンプト文字列を指定します。

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。

プロンプト文字列中に以下に示すバックスラッシュで始まる特殊文字を含めると、その部分は展開した文字列に置き換わります。

特殊文字	展開文字列
\c	構成定義ファイル名がconfig2のときだけ「config2」
\C	構成定義ファイル名の番号 (1または2)
\d	日付(月/日 形式)
\h	ホスト名または機種名(.の手前まで)
\H	ホスト名または機種名(すべて)
\m	機種名
\p	クラスに応じたプロンプト文字列(空白文字含む)
\u	ログインユーザ名
\t	時刻(時:分:秒 形式、24時間制)
\T	時刻(時:分:秒 形式、12時間制)
\@	時刻(時:分NN 形式、12時間制、NN:amかpm)
\v	ファームウェアバージョン
\w	構成定義階層
\!	履歴番号
\\	バックスラッシュ(\)1個

"\c"は、本装置が bank0 の構成定義情報で起動している場合は何も表示されず、"\c"の前または後ろの空白 1 つも表示されません。

bank1 の構成定義情報で起動している場合は"bank1"が表示されます。

"\h"および"\H"は、sysname コマンド で設定したホスト名が表示されます。

ホスト名を設定していない場合は、機種名が表示されます。

"\p"および"\\$"の標準プロンプトを以下に示します。

状 態	標準プロンプト
ログイン前	:
一般ユーザログイン時	>
管理者ログイン時	#

[注意]

本コマンドは運用管理コマンドですが、管理者クラスで設定した内容は save コマンド を実行することで構成定義情報として保存することができます。また、構成定義モードの delete コマンド で設定を削除することができます。

一般ユーザクラスで設定した内容は、ログアウト時や admin コマンド 実行時に破棄され、保存することはできません。

[未設定時]

以下が設定されたものとみなされます。

```
terminal prompt login "Login: "
terminal prompt user "\h \c\w\p"
terminal prompt admin "\h \c\w\p"
```

[実行例]

```
# terminal prompt login "Welcome: "
# terminal prompt user "[\!] \h \w \p"
# terminal prompt admin "\h bank / \C \w \p"
#
```

16.2.5 terminal timestamp

[機能]

コマンド実行日時表示機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

terminal timestamp { enable | disable }

[オプション]

enable

コマンド実行時に日時を表示します。

disable

コマンド実行時に日時を表示しません。

[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]

コマンドを実行する際にコマンド実行日時を表示するかどうかを指定します。

[注意]

本コマンドは運用管理コマンドですが、管理者クラスで設定した内容は save コマンドを実行することで構成定義情報として保存することができます。また、構成定義モードの delete コマンドで設定を削除することができます。

一般ユーザクラスで設定した内容は、ログアウト時や admin コマンド実行時に破棄され、保存することはできません。

[未設定時]

コマンド実行時に日時を表示しないものとみなされます。

```
terminal timestamp disable
```

16.2.6 terminal bell

[機能]

操作エラーベル機能の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

terminal bell {enable|disable}

[オプション]

enable

操作エラー時に端末ベルを鳴らします。

disable

操作エラー時に端末ベルを鳴らしません。

[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]

以下の操作エラー時に端末ベルを鳴らすかどうかを設定します。

- 最大文字数 (1022 文字) を超えて入力しようとした場合
- 最大文字数 (1022 文字) を超える貼り付けを行った場合
- 補完候補がない場合

[注意]

本コマンドは運用管理コマンドですが、管理者クラスで設定した内容は save コマンドを実行することで構成定義情報として保存することができます。また、構成定義モードの delete コマンドで設定を削除することができます。

一般ユーザクラスで設定した内容は、ログアウト時や admin コマンド実行時に破棄され、保存することはできません。

[未設定時]

端末ベルを鳴らすものとみなされます。

```
terminal bell enable
```

16.2.7 terminal logging

[機能]

コマンド実行履歴情報の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

terminal logging line <line>

[オプション]

line <line>

コマンド実行履歴行数を 0~100 の 10 進数で指定します。
0 を指定すると、コマンド履歴を残しません。

[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]

コマンド実行履歴行数を指定します。
行数を変更した場合、履歴番号や履歴内容は引き継がれますが、0 から増やした場合は履歴番号が 1 からになります。

[注意]

本コマンドは運用管理コマンドですが、管理者クラスで設定した内容は save コマンドを実行することで構成定義情報として保存することができます。また、構成定義モードの delete コマンドで設定を削除することができます。

一般ユーザクラスで設定した内容は、ログアウト時や admin コマンド実行時に破棄され、保存することはできません。

[未設定時]

コマンド実行履歴行数に 24 行が設定されたものとみなされます。

```
terminal logging line 24
```

16.2.8 show terminal

[機能]

ターミナル情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show terminal

[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]

ターミナル情報を表示します。

[注意]

本コマンドは運用管理コマンドですが、構成定義情報として表示することもできます。その場合、candidate-config と running-config は同一の内容が表示されます。

構成定義情報として表示した場合は、未設定時値以外に設定した内容だけが桁そろえされずに表示されます。

[実行例]

```
# show terminal
pager      enable
window     column 80 line 24
charset    EUC
prompt     login "\p"
prompt     user  "\u@\h \c\p"
prompt     admin "\u@\h \c\w\p"
timestamp  disable
bell       enable
logging    line 24
#
```

16.3 コマンド実行履歴

16.3.1 show logging command

[機能]

コマンド実行履歴の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show logging command [brief]

[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。

[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。

履歴を編集集中で実行していない行には、履歴番号のあとに"*"が表示されます。

"*"が表示されている場合は、以下のどれかの方法で"*"を消すことができます。

- 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。
- Ctrl+P キーまたは キーでその行を表示し、Ctrl+U を押して空行にしてほかの履歴に移動します。

[注意]

履歴番号が 32767 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
Dec 01 15:58:55      1 show system information
Dec 01 15:59:04      2 show date
Dec 01 16:00:19      3 show logging command
# show logging command brief
  1 show system information
  2 show date
  3 show logging command
  4 show logging command brief
#
```

16.3.2 clear logging command

[機能]

コマンド実行履歴の消去

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

clear logging command

[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]

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。
コマンド実行履歴番号は 1 に戻ります。

[実行例]

```
# clear logging command  
#
```

16.4 コマンドエイリアス

16.4.1 alias

[機能]

コマンドエイリアス情報の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

alias <alias> "<command>"

[オプション]

<alias>

付与するコマンドエイリアス名を 80 文字以内で指定します。

先頭文字は英字、2 文字目以降は英字、数字、ハイフン (-) を指定できます。

<command>

コマンドエイリアスを実行したときに置き換えるコマンド名およびコマンドオプションをダブルクォーテーションで囲んで指定します。

"" を指定すると、定義が削除されます。

[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]

コマンド名といくつかのコマンドオプションをひとまとめにして新たなコマンドとして設定します。最大 30 件設定できます。

設定済みのコマンドエイリアス名を指定すると、以前の登録が削除され指定したコマンドが設定されます。

設定したコマンドエイリアスは即時反映され、すぐに使用できます。

設定したコマンドエイリアスを実行すると、設定してあるコマンド名およびコマンドオプションに置き換えられてコマンドが実行されます。

コマンド実行時、コマンドエイリアスに続けて入力したオプションは、コマンドエイリアスを置き換えたコマンド名およびオプションの後ろに続けて入力したものとみなされます。

コマンド実行履歴にはコマンドエイリアスを置き換える前の入力行がそのまま残ります。

[注意]

以下に示すコマンドエイリアス名は登録できません。

exit, end, quit, up, top, delete, show, clear,

commit, discard, save, load, reset, moff

上記以外の通常コマンド名をコマンドエイリアス名として登録することはできますが、登録した通常コマンドの動作が変わってしまうのでご注意ください。

本コマンドは運用管理コマンドですが、管理者クラスで設定した内容は save コマンドを実行することで構成定義情報として保存することができます。また、構成定義モードの delete コマンドで設定を削除することができます。

一般ユーザクラスで設定した内容は、ログアウト時や admin コマンド実行時に破棄され、保存することはできません。

[未設定時]

何も登録しないものとみなされます。

[実行例]

```
# alias history "show logging command brief"
# history
  1 alias history "show logging command brief"
  2 history
#
```

16.4.2 show alias

[機能]

コマンドエイリアス情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show alias [<name>]

[オプション]

なし

すべてのコマンドエイリアス情報を表示します。

<name>

指定したコマンドエイリアス名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]

コマンドエイリアス情報を表示します。

[注意]

本コマンドは運用管理コマンドですが、構成定義情報として表示することもできます。その場合、candidate-config と running-config は同一の内容が表示されます。

[実行例]

```
# show alias
history "show logging command brief"
dsplog "show logging syslog"
# show alias history
"show logging command brief"
#
```

16.4.3 clear alias

[機能]

コマンドエイリアス情報の削除

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

clear alias [<name>]

[オプション]

なし

すべてのコマンドエイリアス情報を削除します。

<name>

指定したコマンドエイリアス名の情報を削除します。

[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]

コマンドエイリアス情報を削除します。

[注意]

本コマンドは運用管理コマンドですが、構成定義モードの delete コマンドで削除することもできます。

[実行例]

```
# clear alias history
# clear alias
#
```

16.5 コマンド 出力操作

16.5.1 more

[機能]

コマンドの出力を画面単位に表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

<command> | more

[オプション]

<command>

実行するコマンドを指定します。

[動作モード]

運用管理モード (一般ユーザ/管理者クラス)

構成定義モード (管理者クラス)

[説明]

コマンドの出力結果を画面単位に表示します。

本コマンドは、terminal pager enable を指定したときと同じ動作になります。

詳しい説明、キー操作、注意事項については、terminal pager コマンドを参照してください。

[実行例]

```
# show running-config | more
ether 1 mdi auto
(中略)
telnetinfo autologout 5m
MORE(86%):          (qを入力して表示終了)
#
```

16.5.2 tail

[機能]

コマンド出力の末尾部分を表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

<command> | tail [<lines>]

[オプション]

<command>

実行するコマンドを指定します。

<lines>

表示する行数を 1 ~ 1000 の 10 進数で指定します。
省略時は、10 を指定したものと動作します。

[動作モード]

運用管理モード (一般ユーザ/管理者クラス)

構成定義モード (管理者クラス)

[説明]

指定したコマンドを実行し、そのコマンドの出力の末尾部分を指定した行数だけ表示します。
指定したコマンドの出力が指定した行数に満たない場合は、すべての出力が表示されることになります。
ページャー (terminal pager コマンド参照) が有効な場合は、本コマンドの出力 (指定したコマンドの出力の末尾部分) に対してページャーが動作します。

[注意]

コマンドパイプ文字 ("|") の前後には空白文字を入力してください。コマンドパイプ文字は一度しか指定できず、tail コマンドを複数指定することはできません。

行数は、改行文字までを 1 行として数えます。1 行が長い場合、画面上では複数行で表示され、引数で指定した行数と画面上の行数が一致しない場合があります。

実行に時間のかかるコマンドを指定した場合、表示開始までしばらく待たされることがあります。

本コマンドは show コマンドのような表示コマンドに対して動作します。

telnet コマンドのような制御コマンドに対しては、コマンドの出力をそのまますべて出力します。

[実行例]

```
# show logging syslog | tail 2
Jul  1 15:19:47 192.168.1.1 SR-M20AP2: sshd: generated public/private host key pair.
Jul  1 15:19:52 192.168.1.1 SR-M20AP2: logon: login admin on console
#
```

第 17 章 システム操作および表示コマンド

17.1 システム操作および表示

17.1.1 show system information

[機能]

静的なシステム情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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]

SR-M20AP2/20AP1 の場合

```
# show system information
Current time : Mon Jul 1 10:53:34 2013      ---(1)
Startup time : Mon Jul 1 10:34:19 2013      ---(2)
System : SR-M20AP2                          ---(3)
Serial No. : 00000123                       ---(4)
ROM Ver. : 1.0                              ---(5)
Firm Ver. : V02.09 NY0001 Mon Jul 1 08:40:15 JST 2013 ---(6)
Startup-config : Mon Jul 19 10:08:04 2013 config1 ---(7)
Running-config : Mon Jul 19 10:34:19 2013    ---(8)
MAC : 000b5d890016-000b5d890017            ---(9)
      000b5d890020-000b5d890027 (2.4GHz)
      000b5d890028-000b5d89002f (5GHz)
Memory : 64MB                              ---(10)
```

SR-M20AC2/20AC1 の場合

```
# show system information
Current time : Mon Jul 1 10:53:34 2013      ---(1)
Startup time : Mon Jul 1 10:34:19 2013      ---(2)
System : SR-M20AC2                          ---(3)
Serial No. : 00000123                       ---(4)
ROM Ver. : 1.0                              ---(5)
Firm Ver. : V02.09 NY0001 Mon Jul 1 08:40:15 JST 2013 ---(6)
Startup-config : Mon Jul 19 10:08:04 2013 config1 ---(7)
Running-config : Mon Jul 19 10:34:19 2013    ---(8)
MAC : 000b5d890036                          ---(9)
      000b5d890040-000b5d890047 (2.4GHz/5GHz)
Memory : 64MB                              ---(10)
```

- 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。

SR-M20AP2

SR-M20AP1

SR-M20AC2

SR-M20AC1

4) Serial No.

装置のシリアル番号が表示されます。

5) ROM Ver.

ROM 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) Firm Ver.

ファームウェア版数が Vxx.yy の形式で表示されます。

xx.yy は 2 桁の 10 進数で表示されます。

7) 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。

8) 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。

9) 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。

10) Memory

装置に実装されているメモリサイズが表示されます。

17.1.2 show system status

[機能]

動的なシステム情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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       : Mon Nov 17 14:00:45 2003      ---(1)
Startup-time      : Mon Nov 17 08:40:05 2003      ---(2)
restart_cause     : power on                      ---(3)
machine_state     : RUNNING                       ---(4)
cpu0_state        : NORMAL                        ---(5)
cpu0_temp         : 40 C                          ---(6)
```

- 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
- 5) cpu0_state
CPU 温度状態
- NORMAL**
: 正常
- HIGHWARNING**
: 高温警告
- HIGHALARM**
: 高温異常
- UNKNOWN**
: 非監視状態、または状態不明
- 6) cpu0_temp
CPU 温度

17.1.3 show tech-support

[機能]

解析情報の一括表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。(SR-M20AP2/20AP1 のみ)

[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。

[注意]

ページャー機能 (terminal pager enable コマンド 参照) が有効でも、本コマンドの出力は停止することなく表示されます。

17.1.4 show logging error

[機能]

エラーログの表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
----- Error Logs in FLASH -----
[0] Error Log:
flag=80,mode=00,unit=10,regsp=00000000
Firm information:
SR-M20AP2 V02.09 PTF:NY0001
Error information:
error code [85010000]
Logging time:
Mon Jul  1 11:51:17 2013
Hardware diagnostic error information:
Detail [00142224 00142228 00000080 0000341f]
      [00000000 00000000 00000000 00000000]
      .
      .

Extended Error Logs:

[1] Error Log:
flag=80,mode=00,unit=10,regsp=00000000
Firm information:
SR-M20AP2 V02.09 PTF:NY0001
Error information:
error code [85010000]
Logging time:
Mon Jul  1 11:51:17 2013
Hardware diagnostic error information:
Detail [00142224 00142228 00000080 00003520]
      [00000000 00000000 00000000 00000000]
      .
      .

----- Error Logs in DRAM -----
[0] Error Log:
flag=80,mode=00,unit=80,regsp=01183eb0,thread=cmdexec
Firm information:
SR-M20AP2 V02.09 PTF:NY0001
System down information:
down code [00000080:00000005]
Logging time:
Mon Jul  1 11:51:17 2013
Register:
      status [1040ff0c] cause [30000014] epc [00095804] badva [00954352]
      hi [00000000] lo [00000258]
      r0 [00000000] r1 [00640000] r2 [00000ebc] r3 [00000000]
      .
      .

User Stack:
      +0      +4      +8      +C      +0 +4 +8 +C
04ae9f60 04aea1d0 00886d58 04ae9fb8 04ae9fa0 .....mX.....
04ae9f70 00c6fcbb fea4cebb d8c4eab7 c1bcb0a1 .....
      .
      .

Interrupt Stack:
      +0      +4      +8      +C      +0 +4 +8 +C
04ae9e60 00000000 04aealf0 0121ff74 00000000 .....!.t....
04ae9e70 00000000 04ae9f60 00000005 01124844 .....`.HD
      .
      .

#

```

17.1.5 clear logging error

[機能]

エラーログのクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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  
#
```

17.1.6 show logging syslog

[機能]

システムログ情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。最新の情報からさかのぼって、1024 件以上表示できます。

[注意]

本装置の電源 OFF、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。

reset コマンドの実行やリセットスイッチの押下により本装置をリセットしてもシステムログ情報はクリアされませんが、例外としてファームウェア更新後にリセットされた場合は、システムログ情報はクリアされます。

[実行例]

```
# show logging syslog
Jul  1 15:52:31 192.168.1.1 SR-M20AP2: init: system startup now.
Jul  1 15:52:31 192.168.1.1 SR-M20AP2: sshd: generating public/private host key pair.
Jul  1 15:52:40 192.168.1.1 SR-M20AP2: protocol: ether 1 link up
Jul  1 15:52:40 192.168.1.1 SR-M20AP2: protocol: lan 0 link up
```

17.1.7 clear logging syslog

[機能]

システムログ情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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  
#
```


17.1.8 clear statistics

[機能]

全統計情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

[実行例]

```
# clear statistics  
#
```

17.1.9 show date

[機能]

現在の装置の日付、時刻の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 2009 ---(1)
```

- 1) 現在の日付、時刻が表示されます。

17.1.10 date

[機能]

現在の装置の日付、時刻の表示 / 設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 2009
#
```

日付、時刻を設定する場合

```
# date 2009/02/19.14:26:00
#
```

17.1.11 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 2009
#
```

17.1.12 reset

[機能]

装置の再起動

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
reset [<filename>]
reset clear
```

[オプション]

なし

装置を再起動します。

<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。

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 30 秒かかります。

[実行例]

```
# reset
#
```

第 18 章 構成定義情報の表示、削除、および 操作コマンド

18.1 構成定義情報表示

18.1.1 show candidate-config

[機能]

編集時構成定義情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show candidate-config [all] [<config>]

[オプション]

all

未設定時値も含むすべての構成定義情報を表示します。
省略時は、未設定時値から変更されている構成定義情報のみを表示します。

<config>

<config>で始まる構成定義情報を表示します。
表示される構成定義情報には<config>部分は含まれません。
省略時は、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]

現在編集時の構成定義情報を表示します。

[実行例]

```
# show candidate-config lan 0
ip address 192.168.0.1/24 3
#
```

18.1.2 show running-config

[機能]

動作中構成定義情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show running-config [all] [<config>]

[オプション]

all

未設定時値も含むすべての構成定義情報を表示します。
省略時は、未設定時値から変更されている構成定義情報のみを表示します。

<config>

<config>で始まる構成定義情報を表示します。
表示される構成定義情報には<config>部分は含まれません。
省略時は、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 lan 1
ip address 192.168.1.1/24 3
```


18.1.3 show startup-config

[機能]

起動用構成定義情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show startup-config [<config>]

[オプション]

<config>

<config>で始まる構成定義情報を表示します。

<config>には show running-config または show candidate-config で表示されるとおりに、省略可能オプションも省略しないで、数字も表示どおりの文字列で指定してください。

表示される構成定義情報には<config>部分は含まれません。

省略時は、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]

起動時に使用した構成定義情報、または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
lan 0 ip address 192.168.0.1/24 3
lan 0 vid 1
syslog pri error,warn,info
syslog facility 23
telnetinfo autologout 5m
time zone 0900
```

18.1.4 diff

[機能]

構成定義情報の差分の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。<filename1>にのみある情報には行の先頭に"<"を、<filename2>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。

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	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]

```
# 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
#
```

18.2 構成定義情報削除

18.2.1 delete

[機能]

編集構成定義情報の削除

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 set  
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
```

18.3 構成定義情報操作

18.3.1 load

[機能]

構成定義の読み込み

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
```

本装置の通信負荷が高く、構成定義を読み込めません。
通信負荷を停止して再度本コマンドを実行してください。

```
<WARNING> weak admin 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 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 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 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 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  
#
```

18.3.2 save

[機能]

構成定義情報の保存

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
#
```

18.3.3 commit

[機能]

構成定義情報の動的反映

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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  
#
```

18.3.4 discard

[機能]

構成定義情報の変更破棄

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

[注意]

本コマンド実行後に commit を実行すると、candidate-config と running-config の差分のみではなく、running-config 上のすべてのコマンドが動的反映されます。運用中は通信に影響を与えないよう、本コマンドを実行しないでください。

[メッセージ]

```
<WARNING> weak admin 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 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 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 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 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
```

18.4 ファイル操作コマンド

18.4.1 dir

[機能]

ファイル一覧の表示

[適用機種]

SR-M20AP2 SR-M20AP1

[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。文字列の長さは関係しません。

? 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。

18.4.2 copy

[機能]

ファイルのコピー

[適用機種]

SR-M20AP2 SR-M20AP1

[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

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
firmware	ファームウェア
/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

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
firmware	ファームウェア
/um0/任意のファイル名	USBメモリ上のファイル

[実行例]

```
# copy config1 /um0/config1
#
```

18.4.3 remove

[機能]

ファイルの削除

[適用機種]

SR-M20AP2	SR-M20AP1		
-----------	-----------	--	--

[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
#
```

18.4.4 rename

[機能]

ファイル名の変更

[適用機種]

SR-M20AP2	SR-M20AP1		
-----------	-----------	--	--

[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  
#
```

18.4.5 format

[機能]

フォーマット

[適用機種]

SR-M20AP2 SR-M20AP1

[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 19 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

19.1 Ethernet のカウンタ・ログ・統計・状態などの表示

19.1.1 show ether

[機能]

Ethernet 物理ポートの情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

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]

SR-M20AP2/20AP1 の実行例

```
# 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)

[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)

#
```

```
# 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        : Backup (group 1, master)      ---(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        : Backup (group 1, backup, standby)
since       : Oct  2 17:31:26 2005
config      : mode(auto), mdi(auto)
linkcontrol  : downrelay(-)

#
```

SR-M20AC2/20AC1 の実行例

```
# show ether

[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)

#
```

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。

要因によっては、以下のように示します。

offline (backup) : バックアップポート機能によるポート閉塞 (SR-M20AP2/20AP1 のみ)

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

現在リンクしている ether ポートの通信速度 (10Mbps/100Mbps/1000Mbps) 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 10/100/1000BASE-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。

Backup バックアップポートとして使用していることを示します。(SR-M20AP2/20AP1 のみ)

所属するバックアップグループ番号、および master/backup 種別も表示されます。

待機状態のポートについては、"standby"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。(SR-M20AP2/20AP1 のみ)

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。

19.1.2 show ether statistics

[機能]

Ethernet 物理ポートの統計情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

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]

SR-M20AP2/20AP1 の実行例

```
# show ether statistics line 1

[ETHER PORT-1 STATISTICS]
[Input Statistics]
Discards
  All DiscardsPkts      : 94732      ---(1)
  Errors
  All Errors            : 0          ---(2)

[Output Statistics]
Discards
  All DiscardsPkts      : 94732      ---(3)
  Errors
  All Errors            : 0          ---(4)
```

- 1) 受信した全フレームのうち、廃棄した数
- 2) 受信した全フレームのうち、エラー検出した数
- 3) 送信したフレームのうち、廃棄した数
- 4) 送信したフレームのうち、エラー検出した数

SR-M20AC2/20AC1 の実行例

```
# show ether statistics line 1

[ETHER PORT-1 STATISTICS]
[Input Statistics]
  Frames                : 6706618    ---(1)

  Errors
  All Errors            : 0          ---(2)

[Output Statistics]
  Frames                : 5109155    ---(3)

  Discards
  All DiscardsPkts      : 94732      ---(4)
  Errors
  All Errors            : 1234       ---(5)
```

- 1) 受信した総フレーム数
自局あてだけです。エラーは含みません。
- 2) 受信した全フレームのうち、エラー検出した数
自局あて以外も含みます。
- 3) 送信した総フレーム数
All DiscardsPkts で廃棄されたフレームを含みません。
- 4) 送信したフレームのうち、廃棄した数
- 5) 送信したフレームのうち、エラー検出した数

SR-M20AP2/20AP1 の detail 指定時の実行例

```
# show ether statistics line 1 detail

[ETHER PORT-1 STATISTICS]
[Input Statistics]
Discards
  Resource Full          : 0          ---(1)
  Input Discards        : 0          ---(2)
Errors
  Undersize              : 0          ---(3)
  FCSErrors              : 0          ---(4)
  AlignmentErrors        : 0          ---(5)
  FragmentErrors         : 0          ---(6)
  Jabbers                 : 0          ---(7)

[Output Statistics]
Discards
  Underflow Discards     : 0          ---(8)
Errors
  Oversize                : 0          ---(9)
  ExcessiveCollisions    : 0          ---(10)
  LateCollisions         : 0          ---(11)

SingleCollisionFrames   : 0          ---(12)
MultipleCollisionFrames : 0          ---(13)
DeferredTransmissions   : 0          ---(14)
```

- 1) 受信バッファ溢れした数
- 2) 以下の理由で、転送できないフレーム数
 - 設定されていない vlan id で受信した。
 - STP が forward 以外の状態で受信した。
- 3) ショートサイズ (64 バイト未満) フレーム受信数
- 4) 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
データサイズ 1519 ~ 1522 バイトのタグなしフレームで、FCS エラーを検出した場合は、Jabbers もカウントされます。
- 5) アライメントエラーを検出した受信フレーム数
データサイズ 1519 ~ 1522 バイトのタグなしフレームで、アライメントエラーを検出した場合は、Jabbers もカウントされます。
- 6) ショートサイズ (64 バイト未満) フレームで FCS エラーまたはアライメントエラーを検出したフレーム数
コリジョン発生時もカウントされます。
- 7) 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 エラーまたは FCS アライメントエラーの検出有無にかかわらずカウントされます。
- 8) アンダーフロー状態により破棄されたフレーム数
- 9) 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
- 10) コリジョン多発によって送信が失敗したフレーム数
- 11) レイトコリジョン発生回数
- 12) 1 回のコリジョン発生後、送信が成功したフレーム数
- 13) 複数回のコリジョン発生後、送信が成功したフレーム数
- 14) 伝送路ビジーにより送信が遅延したフレーム数

SR-M20AC2/20AC1 の detail 指定時の実行例

```
# show ether statistics line 1 detail

[ETHER PORT-1 STATISTICS]
[Input Statistics]
Frames                : 5080816
Errors
  FCSErrors           : 0          ---(1)
  Undersize            :             ---(2)
  Oversize             :             ---(3)
  Resource Full        :             ---(4)

[Output Statistics]
Frames                : 1361963

Discards
  All DiscardsPkts    : 94732     ---(5)
Errors
  ExcessiveCollisions : 0          ---(6)

Collision             : 0          ---(7)
```

- 1) FCS エラーを検出したフレーム数
- 2) ショートサイズ (64 バイト未満) フレーム受信数
- 3) 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
- 4) 受信バッファ溢れした数
- 5) 以下の理由で、送信起動前に廃棄した数
 - 送信タイムアウト
 - 送信待ちキューあふれ
- 6) コリジョン多発によって送信が失敗したフレーム数
- 7) コリジョン発生数

19.2 Ethernet のカウンタ・ログ・統計などのクリア

19.2.1 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

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 20 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 インタフェース番号、および無線通信モード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インタフェース番号	無線通信モード
ieee80211 1	wlan 1 ~ 8	11b, 11b/g, 11b/g/n, 11g, 11g/n
ieee80211 2	wlan 9 ~ 16	11a
	wlan 9 ~ 12	11a/n

SR-M20AC2/20AC1 の場合は、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インタフェース番号	無線通信モード
ieee80211 1	wlan 1	11b, 11b/g, 11b/g/n, 11a, 11a/n

20.1 無線 LAN モジュールのカウンタ・ログ・統計・状態などの表示

20.1.1 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 ~ 2	SR-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

[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           : 517          ---(1)
tx packets[voice]   : 0            ---(2)
tx packets[video]   : 0            ---(3)
tx packets[besteffort] : 0          ---(4)
tx packets[background] : 0          ---(5)
tx noack             : 10           ---(6)
rx crcerr           : 10018         ---(7)
rx fifoerr          : 0            ---(8)
rx badmic           : 0            ---(9)
rx phyerr           : 0            ---(10)
rx packets          : 248          ---(11)
rx packets[no WMM] : 465          ---(12)
rx packets[0]       : 0            ---(13)
rx packets[1]       : 0            ---(14)
rx packets[2]       : 0            ---(15)
rx packets[3]       : 0            ---(16)
rx packets[4]       : 0            ---(17)
rx packets[5]       : 0            ---(18)
rx packets[6]       : 0            ---(19)
rx packets[7]       : 0            ---(20)
rx rssi             : 52           ---(21)
be xmit             : 7987         ---(22)
per cal             : 70           ---(23)
apscan limit over  : 0            ---(24)
dfs detected        : 0            ---(25)
dfs detected all    : 0            ---(26)
dfs recovered       : 0            ---(27)
carrier detected    : 0            ---(28)
ampdu tx aggregated : 0            ---(29)
ampdu tx not aggregated : 0          ---(30)
```

- 1) tx packets
送信フレーム数
- 2) tx packets[voice]
送信フレーム数 (WMM クラス:Voice)
- 3) tx packets[video]
送信フレーム数 (WMM クラス:Video)
- 4) tx packets[besteffort]
送信フレーム数 (WMM クラス:besteffort)
- 5) tx packets[background]
送信フレーム数 (WMM クラス:background)
- 6) tx noack
No ACK 送信フレーム数
- 7) rx crcerr
CRC エラー検出回数
- 8) rx fifoerr
受信 FIFO オーバーラン検出回数
- 9) rx badmic
MIC エラー検出回数
- 10) rx phyerr
PHY エラー検出回数

-
- 11) rx packets
受信フレーム数
 - 12) rx packets[no WMM]
受信フレーム数 (WMM disable または対象外)
 - 13) rx packets[0]
受信フレーム数 (WMM 優先度 0)
 - 14) rx packets[1]
受信フレーム数 (WMM 優先度 1)
 - 15) rx packets[2]
受信フレーム数 (WMM 優先度 2)
 - 16) rx packets[3]
受信フレーム数 (WMM 優先度 3)
 - 17) rx packets[4]
受信フレーム数 (WMM 優先度 4)
 - 18) rx packets[5]
受信フレーム数 (WMM 優先度 5)
 - 19) rx packets[6]
受信フレーム数 (WMM 優先度 6)
 - 20) rx packets[7]
受信フレーム数 (WMM 優先度 7)
 - 21) rx rssi
受信フレームの信号強度
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) - 95	SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

- 22) be xmit
送信された beacon フレーム数
- 23) per cal
キャリブレーション実行回数
- 24) apscan limit over
周辺アクセスポイント情報の登録に失敗した数
- 25) dfs detected
レーダを検出した数
- 26) dfs detected all
同周波数帯 (W53 または W56) の全チャンネルでレーダを検出した数
- 27) dfs recovered
レーダ検出による利用不可中のチャンネルが復旧した数
- 28) carrier detected
キャリア (無変調波) を検出した数

- 29) `ampdu tx aggregated`
アグリゲートされて送信したフレーム数
- 30) `ampdu tx not aggregated`
アグリゲートされずに送信したフレーム数

20.1.2 show ieee80211 status

[機能]

無線 LAN モジュール状態の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 ~ 2	SR-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

[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。

[実行例]

```
# show ieee80211 status line 2
[ieee80211 2]
status           : up ---(1)
since            : Feb 27 13:11:38 2009 ---(2)
mode             : IEEE802.11a/n(max MCS15) ---(3)
channel          : 56(5280Mhz),52 ---(4)
antenna          : internal ---(5)
sta limit        : 4 stations ---(6)
sta guarantee    : 3 stations ---(7)
txpower          : 10(x0.5dBm) ---(8)
llg protection mode : disable ---(9)
ht protection mode : disable ---(10)
rts threshold    : 2346 bytes ---(11)
dtim period      : 1 ---(12)
beacon interval  : 100(x1.024msec) ---(13)
carrier-status   : normal ---(14)
a-mpdu tx size   : 8 kbytes ---(15)
WMM Information
wmm mode         : disable ---(16)
background cwmin 4 cwmax 10 aifs 7 txopLimit 0 ack enable ---(17)
                 cwmin 4 cwmax 10 aifs 7 txopLimit 0
besteffort cwmin 4 cwmax 6 aifs 3 txopLimit 0 ack disable
                 cwmin 4 cwmax 10 aifs 3 txopLimit 0
video          cwmin 3 cwmax 4 aifs 1 txopLimit 94 ack enable
                 cwmin 3 cwmax 4 aifs 2 txopLimit 94
voice          cwmin 2 cwmax 3 aifs 1 txopLimit 47 ack enable
                 cwmin 2 cwmax 3 aifs 2 txopLimit 47
DFS Information
detected         : channel 52(rest 29:43) ---(18)
                 : channel 112(rest 05:12)
APSCAN Information
mode             : enable ---(19)
expire           : 3600sec ---(20)
ERP Information
non ERP present  : ERP-STAs ---(21)
use protection   : do not use protection ---(22)
HT Operation
secondary channel : below ---(23)
STA channel width : 20/40 ---(24)
RIFS mode        : enable ---(25)
HT Protection    : not-HT-mixed mode ---(26)
NonGF HT STAs   : One or more associated STAs are not GF capable ---(27)
OBSS Non-HT STAs : non-HT-STAs ---(28)

# show ieee80211 status line 1
[ieee80211 1]
status           : disable ---(1)
since            : - ---(2)
```

1) 回線状態

2) 回線状態の更新時間

3) 通信モードの情報

4) 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。

5) アンテナの情報 (SR-M20AP2/20AP1 のみ)

internal 内蔵アンテナを使用

external 外部アンテナを使用

6) 接続可能台数 (SR-M20AP2/20AP1 のみ)

7) 最低保証台数 (SR-M20AP2/20AP1 のみ)

-
- 8) 無線送信出力の情報
 - 9) 11g プロテクションモードの情報
 - 10) ht プロテクションモードの情報
 - 11) RTS しきい値
 - 12) DTIM 間隔 (SR-M20AP2/20AP1 のみ)
 - 13) ビーコン送信間隔 (SR-M20AP2/20AP1 のみ)
 - 14) キャリア (無変調波) 検出状態 (SR-M20AP2/20AP1 のみ)
 - normal** キャリア (無変調波) 未検出状態
 - detected** キャリア (無変調波) 検出状態
 - 15) A-MPDU 最大送信サイズ
 - 16) WMM 優先制御の使用状態
 - 17) WMM 優先制御パラメタの情報
 - 18) DFS 情報 (SR-M20AP2/20AP1 のみ)
 - channel** レーダ検出による利用不可チャンネル
 - rest** 利用不可チャンネルが利用可能となるまでの時間
 - 19) 周辺アクセスポイント検出の動作モード (SR-M20AP2/20AP1 のみ)
 - disable** 無効
 - enable** 有効
 - scanonly**
 - スキャン専用モード
 - 20) 周辺アクセスポイント情報の保持期間 (秒)(SR-M20AP2/20AP1 のみ)
 - 21) 11b 無線装置の状態
 - ERP-STAs**
 - 11b 無線 LAN 端末、または 11b 無線 LAN アクセスポイントは未検出
 - non-ERP-STAs**
 - 11b 無線 LAN 端末、または 11b 無線 LAN アクセスポイントは検出済み
 - 22) 11g プロテクションの状態
 - use protection**
 - 11g プロテクション動作は有効
 - do not use protection**
 - 11g プロテクション動作は無効
 - 23) セカンダリチャンネルオフセット
 - above** プライマリチャンネルより上のチャンネル
 - below** プライマリチャンネルより下のチャンネル
 - none** セカンダリチャンネルなし
 - 24) 無線 LAN アクセスポイントの運用帯域幅
 - 20** 20MHz 幅

20/40 20/40MHz 幅双方可能

25) RIFS の状態

disable RIFS は無効

enable RIFS は有効

26) HT プロテクションの状態

no protection mode

BSS 内に 20MHz の 11n 無線 LAN 端末、無線 LAN アクセスポイントのみ存在。
または、40MHz の 11n 無線 LAN 端末、無線 LAN アクセスポイントのみ存在。

nonmember protection mode

BSS 外に 11n 以外の無線 LAN アクセスポイントが存在。

20MHz protection mode

BSS 内に 20MHz と 40MHz の 11n 無線 LAN 端末、または無線 LAN アクセスポイント
が混在。

non-HT mixed mode

上記以外

27) グリーンフィールドフォーマットの状態

all HT STAs that are associated are HT-GF capable.

アソシエート済みのすべての無線 LAN 端末は、グリーンフィールドフォーマットをサ
ポート。

one or more HT STAs that are not HT-GF capable are associated.

一部の無線 LAN 端末は、グリーンフィールドフォーマットが未サポート。

28) BSS 外の無線 LAN 端末、無線 LAN アクセスポイントの状態

use of protection for non-HT STAs by OBSSs is not needed

11n 無線 LAN 端末、無線 LAN アクセスポイントのみ存在。

there exists one or more non-HT

11n 以外の無線 LAN 端末、無線 LAN アクセスポイントが存在。

20.2 無線 LAN モジュールのカウンタ・ログ・統計などのクリア

20.2.1 clear ieee80211 statistics

[機能]

無線 LAN モジュール統計情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
clear ieee80211 statistics [line <ieee80211_number>]
```

[オプション]

なし

すべての無線 LAN 統計情報をクリアします。

line <ieee80211_number>

指定された無線 LAN モジュールの統計情報をクリアします。

- ieee80211 定義番号

範囲	機種
1 ~ 2	SR-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

[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 統計情報をクリアします。

[実行例]

```
# clear ieee80211 statistics  
#
```

20.3 周辺アクセスポイント情報の取得、表示

20.3.1 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
show ieee80211 apscan [line <ieee80211_number>] [detail]
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。

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。

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。
省略時は、現在運用中のチャンネルと同一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。
無線 LAN 端末として動作する場合、all-channel は指定できません。

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。
省略時は、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。

[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。
無線 LAN 端末として動作する場合、対象チャンネルは無線 LAN チャンネル設定やスキャンチャンネルリスト設定に従います。
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ョン (?) で表示します。
- 周辺アクセスポイント情報の収集が中断された場合、それまでに収集された周辺アクセスポイント情報を表示したのち、以下のメッセージを出力します。

```
ieee80211 <number> apscan was aborted.
```

- 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情報を収集できない状態にある場合、以下のメッセージを出力します。

```
<ERROR> apscan failed. ieee80211 <number> is unavailable for a while.
```

- スキャン専用モードでは、現在運用中のチャンネルと同一チャンネルのみの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> current channel scan is unavailable.
```

- 無線 LAN 端末として動作する場合、ほかの周辺アクセスポイント情報収集動作がすでに動作していると、新たな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> scan already in progress.
```

- 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 history

[ieee80211 1]
(1)          (2)          (3)          (4) (5) (6) (7)
BSSID        SSID        Security     CHAN RSSI MODE Updated
11:12:13:14:15:16 abc1234    OPEN(none)   1   16 11b   10:33:15
17:18:19:1A:1B:1C ghijklmnopqrst... WEP          5   17 11b/g  20:41:07
1D:1E:1F:20:21:22 def5?789    WPA-PSK(TKIP) 9   14 11b/g  22:07:03
29:2A:2B:2C:2D:2E abcdefghijklmnop Unknown      13  15 11b   23:18:03

Total: 4 APs          ---(8)

[ieee80211 2]
BSSID        SSID        Security     CHAN RSSI MODE Updated
21:22:23:24:25:26 xxx1234     WPA/WPA2-PSK(AES)? 36  14 11a   10:33:17
27:28:29:2A:2B:2C yyyyyy56789 WPA/WPA2(AUTO) 52  16 11a   20:41:07

Total: 2 APs
```

(続く)

(続き)

```
# show ieee80211 apscan history detail

[ieee80211 1]
 1. BSSID      : 11:12:13:14:15:16      ---(1)
    SSID       : abc1234              ---(2)
    Updated    : Feb 24 10:33:15 2009 ---(7)
    Security   : OPEN(none)          ---(3)
    CHAN       : 1                   ---(4)
    RSSI       : 16                  ---(5)
    MODE       : 11b                 ---(6)
    CHANWIDTH  : 20                  ---(9)
    SECONDARY  : none                ---(10)
 2. BSSID      : 17:18:19:1A:1B:1C
    SSID       : ghijklmnopqrstuvwzyz0123456789abcdefghij
    Updated    : Feb 24 20:41:07 2009
    Security   : WEP
    CHAN       : 5
    RSSI       : 17
    MODE       : 11b/g
    CHANWIDTH  : 20
    SECONDARY  : none

    .
    .
    .

[ieee80211 2]
 1. BSSID      : 21:22:23:24:25:26
    SSID       : xxx1234
    Updated    : Feb 24 10:33:17 2009
    Security   : WPA/WPA2-PSK(AES)?
      wpa mcastcipher : TKIP
      ucastcipher    : AES
      keymanagement  : PSK
      wpa2 mcastcipher : TKIP
      ucastcipher    : AES
      keymanagement  : 802.1X
    CHAN       : 36
    RSSI       : 14
    MODE       : 11a
    CHANWIDTH  : 20
    SECONDARY  : none
 2. BSSID      : 27:28:29:2A:2B:2C
    SSID       : yyyyy56789
    Updated    : Feb 24 20:41:07 2009
    Security   : WPA/WPA2(AUTO)
      wpa mcastcipher : TKIP
      ucastcipher    : TKIP+AES
      keymanagement  : 802.1X
      wpa2 mcastcipher : TKIP
      ucastcipher    : TKIP+AES
      keymanagement  : 802.1X
    CHAN       : 52
    RSSI       : 16
    MODE       : 11a
    CHANWIDTH  : 20
    SECONDARY  : none

#
```

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

Unknown

不明な認証・暗号化方式

WPA および WPA2

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 と WPA2 で認証方式または暗号化方式が特定できない場合は、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

暗号化方式

WEP64	WEP暗号化方式 (WEPキー:64bit)
WEP128	WEP暗号化方式 (WEPキー:128bit)
TKIP	TKIP暗号化方式
AES	AES暗号化方式
AUTO	自動判別

4) CHAN

チャンネル情報

IEEE802.11n 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。

5) RSSI

受信信号強度

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) - 95	SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

6) MODE

通信モード情報

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
20/40 20/40MHz 幅双方可能

- 10) SECONDARY
セカンダリチャンネルオフセット

above プライマリチャンネルよりも上位チャンネル
below プライマリチャンネルよりも下位チャンネル
none セカンダリチャンネルなし

- 11) WPA および WPA2 の詳細表示

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

WEP64	WEP暗号化方式 (WEPキー:64bit)
WEP128	WEP暗号化方式 (WEPキー:128bit)
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
802.1X	IEEE802.1X認証
Unknown	不明な認証方式

第 21 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 インタフェース番号、および無線通信モード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インタフェース番号	無線通信モード
ieee80211 1	wlan 1 ~ 8	11b, 11b/g, 11b/g/n, 11g, 11g/n
ieee80211 2	wlan 9 ~ 16	11a
	wlan 9 ~ 12	11a/n

SR-M20AC2/20AC1 の場合は、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インタフェース番号	無線通信モード
ieee80211 1	wlan 1	11b, 11b/g, 11b/g/n, 11a, 11a/n

21.1 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

21.1.1 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-M20AP2 SR-M20AP1

[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 ~ 16	SR-M20AP2 SR-M20AP1

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。

[実行例]

```
# show wlan sta
[wlan 1]
Mode: 11g Channel: 1 Total: 1 stations(11b:0 11g:1 11g/n:0 11a:0 11a/n:0)
(1) (2) (3)
MAC Address AID Mode Rate RSSI Security AUTH VID IDLE PS WMM BW IP Address
(4) (5) (6) (7) (8) (9) (10) (11) (12) (13)(14)(15)(16)
00:16:e3:00:00:01 1 11g 48M 57 WPA-PSK(TKIP) ok 3 10 10 yes 20 192.168.100.100

[wlan 9]
Mode: 11a/n Channel: 36,40 Total: 1 stations(11b:0 11g:0 11g/n:0 11a:0 11a/n:1)
MAC Address AID Mode Rate RSSI Security AUTH VID IDLE PS WMM BW IP Address
00:16:e3:00:00:03 2 11a/n 300M 57 WPA2-PSK(AES) ok 5 10 10 yes 40 192.168.101.101

Total:2 stations(11b:0 11g:1 11g/n:0 11a:0 11a/n:1) --(17)

# show wlan sta number 9 detail
[wlan 9]
Mode: 11a/n Channel: 36,40 Total: 1 stations(11b:0 11g:0 11g/n:0 11a:0 11a/n:1)
1. MAC address : 00:16:e3:00:00:03
   Since : Feb 24 10:33:17 2009 ---(18)
   AID : 2
   Mode : 11a/n
   Rate : 300M
   RSSI : 57
   TXSEQ : 0/ 0/ 0/ 0/ 0/ 0/ 0/ 0 ---(19)
   RXSEQ : 10/102/73/105/75/106/62/63 ---(20)
   CAPS : ESS ---(21)
         : PRIVACY
   ERP : - ---(22)
   Security : WPA2-PSK(AES)
   AUTH : ok
   VID : 5
   IDLE : 10
   PS : 10/50
   WMM : yes
   BW : 40
   WPA : no ---(23)
   WPA2 : yes ---(24)
   IP Address : 192.168.101.101
   MIMO-PS : disable ---(25)
   HT-CAPS : CHANNEL_WIDTH(40) ---(26)
            : SHORT_GI(20MHz)
            : SHORT_GI(40MHz)
   Supported-MCS : 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 ---(27)
   Select-MCS : 8,9,10,11,12,13,14,15 ---(28)
#
```

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
- 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

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。

- 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
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

7) 無線レート (bps)

8) 受信信号強度

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) - 95	SR-M20AP2 SR-M20AP1

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で表示します。

- WPA、WPA2 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

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

10) 認証状態

11) VID

VLAN ID

-
- 12) 無通信時間
- 13) 省電力状態
- 数値 バッファ中パケット数 (詳細表示時は、バッファ最大数も表示)
- active** 非省電力状態
- 14) WMM 使用可否
- 15) 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。
- 16) 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。
- 17) 無線 LAN 端末接続数 (無線 LAN モジュール全体)
- 18) 接続時刻
- 19) 送信シーケンス番号
- WMM 使用端末の場合は、TID ごと (左から 0~7) に表示
- 20) 受信シーケンス番号
- WMM 使用端末の場合は、TID ごと (左から 0~7) に表示
- 21) Capability Information field を表示
- ESS
 - IBSS
 - CF_POLLABLE
 - CF_POLLREQ
 - PRIVACY
 - SHORT_PREAMBLE
 - PBCC
 - CHANNEL_AGILITY
 - SHORT_SLOTTIME
 - RSN
 - DSSS_OFDM
- 22) ERP information Element を表示
- -
 - NonERP Present
 - Use Protection
 - Barker Preamble Mode
- 23) WPA 使用可否
- 24) WPA2 使用可否
- 25) MIMO Power Save 状態を表示
- disable** 無効状態
- static** スタティック動作

dynamic

ダイナミック動作

26) 無線 LAN 端末より受信した HT Capability Element 情報を表示

- -: 表示項目なし
- CHANNEL_WIDTH(40) : 20/40MHz 帯域幅をサポート
- HT_GREENFIELD : グリーンフィールドフォーマットをサポート
- SHORT_GI(20MHz) : 20MHz 帯域のショートガードインターバルをサポート
- SHORT_GI(40MHz) : 40MHz 帯域のショートガードインターバルをサポート
- HT_DELAYED_BLOCKACK : HT Delayed Block Ack をサポート
- AMSDU_LENGTH(7935) : A-MSDU 最大長として、7935 オクテットを示す
- AMPDU_SPACE(1/4us) : A-MPDU 最小間隔として、250 ナノ秒を示す
- AMPDU_SPACE(1/2us) : A-MPDU 最小間隔として、500 ナノ秒を示す
- AMPDU_SPACE(1us) : A-MPDU 最小間隔として、1000 ナノ秒を示す
- AMPDU_SPACE(2us) : A-MPDU 最小間隔として、2000 ナノ秒を示す
- AMPDU_SPACE(4us) : A-MPDU 最小間隔として、4000 ナノ秒を示す
- AMPDU_SPACE(8us) : A-MPDU 最小間隔として、8000 ナノ秒を示す
- AMPDU_SPACE(16us) : A-MPDU 最小間隔として、16000 ナノ秒を示す

27) 無線 LAN 端末より受信した HT Capability Element の Supported MCS Set Field 情報を表示

HT Information Element の Supported Basic MCS Set Field 情報で、HT Capability Element と同じ MCS を受信した場合は数値の後ろに"b"を付けて表示します。

28) ユニキャストフレームの送信に利用する MCS を表示

21.1.2 show wlan ap

[機能]

無線 LAN インタフェースの接続アクセスポイント情報の表示

[適用機種]



[入力形式]

```
show wlan ap [number <wlan_number>] [detail]
```

[オプション]

なし

すべての無線 LAN インタフェースのアクセスポイント情報を表示します。

number <wlan_number>

- wlan 定義番号
指定された無線 LAN インタフェースのアクセスポイント情報を表示します。
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	SR-M20AC2 SR-M20AC1

detail

詳細な無線 LAN アクセスポイント情報を表示します。

[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]

接続しているアクセスポイント情報を表示します。

[実行例]

```
# show wlan ap
[wlan 1]
Mode: 11a/n Channel: 36,40
(1)          (2)
BSSID          AID Mode Rate RSSI Security      AUTH WMM BW
(3)          (4) (5) (6) (7) (8)      (9) (10)(11)
00:16:e3:00:00:01  1 11a/n 300M  57 WPA2-PSK(AES)  ok yes 40

      Total:1 APs(11b:0 11g:0 11g/n:0 11a:0 11a/n:1)          ---(12)

# show wlan ap number 1 detail
[wlan 1]
Mode: 11a/n Channel: 36,40
1. BSSID          : 00:16:e3:00:00:01
   Since          : Feb 24 10:33:17 2009          ---(13)
   AID            : 1
   Mode           : 11a/n
   Rate           : 300M
   RSSI           : 57
   Beacon Interval : 100(x1.024msec)             ---(14)
   TXSEQ          : 0/ 0/ 0/ 0/ 0/ 0/ 0/ 0       ---(15)
   RXSEQ          : 10/102/73/105/75/106/62/63    ---(16)
   CAPS           : ESS                          ---(17)
                  : PRIVACY
                  : SHORT_SLOTTIME
   ERP            : -                            ---(18)
   Security       : WPA2-PSK(AES)
   AUTH           : ok
   WMM            : yes
   BW             : 40
   WPA            : no                          ---(19)
   WPA2           : yes                         ---(20)
   MIMO-PS        : disable                     ---(21)
   HT-CAPS        : CHANNEL_WIDTH(40)          ---(22)
                  : SHORT_GI(20MHz)
                  : SHORT_GI(40MHz)
   Supported-MCS  : 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 ---(23)
   Select-MCS     : 8,9,10,11,12,13,14,15      ---(24)

#
```

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
- 11a** IEEE802.11a で動作
- 11a/n** IEEE802.11a/n で動作

2) 使用中の無線 LAN チャンネル番号

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。

3) BSSID

4) アソシエーション ID

5) 無線 LAN アクセスポイントの無線通信モード

- 11b** IEEE802.11b 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

6) 無線レート (bps)

7) 受信信号強度

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) - 95	SR-M20AC2 SR-M20AC1

8) 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で表示します。

- WPA、WPA2 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

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

none	暗号化なし
TKIP	TKIP暗号化方式
AES	AES暗号化方式

9) 認証状態

10) WMM 使用可否

11) 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。

12) 無線 LAN アクセスポイント数

13) 接続時刻

- 14) ビーコン間隔
- 15) 送信シーケンス番号
WMM 使用アクセスポイントの場合は、TID ごと (左から 0~7) に表示
- 16) 受信シーケンス番号
WMM 使用アクセスポイントの場合は、TID ごと (左から 0~7) に表示
- 17) Capability Information field を表示
 - ESS
 - IBSS
 - CF_POLLABLE
 - CF_POLLREQ
 - PRIVACY
 - SHORT_PREAMBLE
 - PBCC
 - CHANNEL_AGILITY
 - SHORT_SLOTTIME
 - RSN
 - DSSS_OFDM
- 18) ERP information Element を表示 (11g,11b/g)
 - -
 - NonERP Present
 - Use Protection
 - Barker Preamble Mode
- 19) WPA 使用可否
- 20) WPA2 使用可否
- 21) MIMO Power Save 状態を表示
 - disable** 無効状態
 - static** スタティック動作
 - dynamic**
ダイナミック動作
- 22) 無線 LAN アクセスポイントより受信した HT Capability Element 情報を表示
 - -: 表示項目なし
 - CHANNEL_WIDTH(40) : 20/40MHz 帯域幅をサポート
 - HT_GREENFIELD : グリーンフィールドフォーマットをサポート
 - SHORT_GI(20MHz) : 20MHz 帯域のショートガードインターバルをサポート
 - SHORT_GI(40MHz) : 40MHz 帯域のショートガードインターバルをサポート
 - HT_DELAYED_BLOCKACK : HT Delayed Block Ack をサポート
 - AMSDU_LENGTH(7935) : A-MSDU 最大長として、7935 オクテットを示す
 - AMPDU_SPACE(1/4us) : A-MPDU 最小間隔として、250 ナノ秒を示す

-
- AMPDU_SPACE(1/2us) : A-MPDU 最小間隔として、500 ナノ秒を示す
 - AMPDU_SPACE(1us) : A-MPDU 最小間隔として、1000 ナノ秒を示す
 - AMPDU_SPACE(2us) : A-MPDU 最小間隔として、2000 ナノ秒を示す
 - AMPDU_SPACE(4us) : A-MPDU 最小間隔として、4000 ナノ秒を示す
 - AMPDU_SPACE(8us) : A-MPDU 最小間隔として、8000 ナノ秒を示す
 - AMPDU_SPACE(16us) : A-MPDU 最小間隔として、16000 ナノ秒を示す
- 23) 無線 LAN アクセスポイントより受信した HT Capability Element の Supported MCS Set Field 情報を表示
- HT Information Element の Supported Basic MCS Set Field 情報で、HT Capability Element と同じ MCS を受信した場合は数値の後ろに"b"を付けて表示します。
- 24) ユニキャストフレームの送信に利用する MCS を表示

21.1.3 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 ~ 16	SR-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

[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。

[実行例]

```
# show wlan statistics number 1
[wlan 1]
rx wrongbss          : 0          ---(1)
rx notassoc          : 0          ---(2)
rx noprivacy         : 0          ---(3)
rx unencrypted       : 0          ---(4)
rx mgtdiscard        : 80         ---(5)
rx beacon            : 25         ---(6)
rx chanmismatch      : 29         ---(7)
rx ssidmismatch      : 15435      ---(8)
rx deauth            : 0          ---(9)
rx disassoc          : 0          ---(10)
rx unauth            : 0          ---(11)
rx defrag            : 0          ---(12)
rx mgmt              : 0          ---(13)
rx action            : 0          ---(14)
rx relay             : 26383      ---(15)
rx notrelay no table : 3          ---(16)
rx notrelay not support : 2      ---(17)
rx notrelay no memory : 0        ---(18)
rx a-msdu decap     : 0          ---(19)
tx mgmt              : 0          ---(20)
tx notassoc         : 0          ---(21)
tx classify          : 0          ---(22)
tx nobuf            : 0          ---(23)
tx nonode           : 0          ---(24)
tx relay            : 865201     ---(25)
tx notrelay table over : 321      ---(26)
tx notrelay not support : 201    ---(27)
tx notrelay no memory : 0        ---(28)
ps unassoc          : 0          ---(29)
ps badaid           : 0          ---(30)
ps qempty           : 0          ---(31)
ps expire           : 0          ---(32)
ps limit over       : 0          ---(33)
sta timeout         : 0          ---(34)
macfilter rejected  : 0          ---(35)
sta limit over      : 15         ---(36)
ampdu rx oor        : 0          ---(37)
```

- 1) rx wrongbss
BSSID 値が装置と異なるフレームを受信した数
- 2) rx notassoc
associate されていない送信元からのフレームを受信した数
- 3) rx noprivacy
wep 無効時に暗号化されているフレームを受信した数
- 4) rx unencrypted
wep 有効時に暗号化されていないフレームを受信した数
- 5) rx mgtdiscard
管理フレームを無視した数
- 6) rx beacon
ビーコンフレームを受信した数
- 7) rx chanmismatch
DS パラメタと異なるチャンネルからフレームを受信した数
- 8) rx ssidmismatch
ssid が動作中のものと異なるフレームを受信した数
- 9) rx deauth
認証解除要求を受けた数

- 10) rx disassoc
接続解除要求を受けた数
- 11) rx unauth
802.1x などによる認証許可が下りていないポートにフレームを受信した数
- 12) rx defrag
デフラグメンテーションがエラーとなった数
- 13) rx mgmt
管理フレームを受信した数
- 14) rx action
アクションフレームを受信した数
- 15) rx relay
この無線 LAN インタフェースから受信し、無線 LAN 中継機能で中継したデータフレーム数 (SR-M20AC2/20AC1 のみ)
- 16) rx notrelay no table
この無線 LAN インタフェースから受信したが、中継先不明で破棄されたデータフレーム数 (SR-M20AC2/20AC1 のみ)
- 17) rx notrelay not support
この無線 LAN インタフェースから受信したが、未サポートプロトコルとして破棄されたデータフレーム数 (SR-M20AC2/20AC1 のみ)
- 18) rx notrelay no memory
この無線 LAN インタフェースから受信したが、メモリ不足で破棄されたデータフレーム数 (SR-M20AC2/20AC1 のみ)
- 19) rx a-msdu decap
処理した A-MSDU の数
- 20) tx mgmt
管理フレームを送信した数
- 21) tx notassoc
未アソシエーションの STA への送信しようとした数
- 22) tx classify
WMM AC 割り当て時にエラーとなった数
- 23) tx nobuf
送信時にバッファ獲得できずにエラーした数
- 24) tx nonode
送信時にあて先となる node が見つからないフレーム数
- 25) tx relay
無線 LAN 中継機能によって、この無線 LAN インタフェースへ送信されたデータフレーム数 (SR-M20AC2/20AC1 のみ)
- 26) tx notrelay table over
この無線 LAN インタフェースへの送信時に、空きテーブルなしで破棄されたデータフレーム数 (SR-M20AC2/20AC1 のみ)
- 27) tx notrelay not support
この無線 LAN インタフェースへの送信時に、未サポートプロトコルとして破棄されたデータフレーム数 (SR-M20AC2/20AC1 のみ)

-
- 28) tx notrelay no memory
この無線 LAN インタフェースへの送信時に、メモリ不足で破棄されたデータフレーム数 (SR-M20AC2/20AC1 のみ)
 - 29) ps unassoc
associate されていない端末から ps-poll を受信した数
 - 30) ps badaid
associate 済みの aid 値とは異なる aid 値が入った ps-poll を受信した数
 - 31) ps qempty
ps-poll を受けたがキューは空であった数
 - 32) ps expire
バッファリングしていたが最大保持時間が過ぎたため破棄したパケットの数
 - 33) ps limit over
バッファリングしていたが最大保持数を越えたため破棄したパケットの数
 - 34) sta timeout
無通信タイマのタイムアウトにより端末を切断した数
 - 35) macfilter rejected
MAC アドレスフィルタで破棄された数
 - 36) sta limit over
接続台数制限により接続を拒否した数
 - 37) ampdu rx oor
A-MPDU フレームで、処理できた MPDU 数

21.1.4 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 ~ 16	SR-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

[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。

[実行例]

```
# show wlan status number 9
[wlan 9]
status          : up (RUN)                ---(1)
since           : Feb 27 13:11:38 2009    ---(2)
mac address     : 00:90:cc:c6:d3:81       ---(3)
Mode: 11a/n Channel: 36,40 Total: 1 stations(11b:0 11g:0 11g/n:0 11a:0 11a/n:1)
(4)             (5)             (6)
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)
bmiss threshold : 7                      ---(13)
beacon status   : normal                 ---(14)
a-mpdu tx mode  : auto                   ---(15)
a-mpdu rx size  : 8 kbytes               ---(16)
a-mpdu rx density : no time restriction  ---(17)
guard-interval  : auto                   ---(18)
auth            : WPA2-PSK                ---(19)
WEP Information
wep mode        : disable                ---(20)
wep send        : key[1]                 ---(21)
wep type        : static                 ---(22)
wep rekey       : 10m                    ---(23)
WPA Information
wpa mode        : enable                  ---(24)
wpa cipher      : AES                    ---(25)
wpa rekey group : 10m                    ---(26)
wpa rekey gmk   : 1d                     ---(27)
wpa mcastcipher : AES                    ---(28)
wpa ucastcipher : AES                    ---(29)
wpa countermeasures : normal             ---(30)

# 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           : Feb 27 14:06:28 2009   ---(2)
mac address     : 00:90:cc:c6:d3:83       ---(3)
```

1) 回線状態

活性中は以下のどれかが表示されます。

INIT	停止中	
		・ DFS による同周波数帯全チャネル利用不可時
		・ スキャン専用モードでの周辺アクセスポイント検出動作時
SCAN	スキャン中	
AUTH	認証中	
ASSOC	アソシエーション中	
CAC	運用前モニタリング中	
RUN	動作中	
CSA	チャネル変更通知中	
SLEEP	一時停止中	

非活性状態では以下が表示されます。非活性中は、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 (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

11g IEEE802.11g で動作 (SR-M20AP2/20AP1 のみ)

11g/n IEEE802.11g/n で動作 (SR-M20AP2/20AP1 のみ)

11a IEEE802.11a で動作

11a/n IEEE802.11a/n 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。

6) 無線 LAN 端末接続数 (無線 LAN インタフェース全体)

SR-M20AC2/20AC1 では表示されません。

7) 動作タイプ

AP 無線 LAN アクセスポイント

STA 無線 LAN 端末

WDS WDS

SCANONLY

スキャン専用モード

8) SSID

9) SSID 非通知と ANY 接続拒否の情報

SR-M20AC2/20AC1 では表示されません。

10) BSSID の情報

SR-M20AC2/20AC1 では以下のように表示されます。

- Associate 済みの場合はその無線 LAN アクセスポイントの BSSID が表示されます。

- Associate していない場合は何も表示されません。

動作タイプが"WDS"の場合、以下のように表示されます。

- WDS ブリッジの対向 MAC アドレスが表示されます。

-
- 11) アクセスポイント内ブリッジ転送動作
SR-M20AC2/20AC1 では表示されません。
- 12) 最低保証台数
SR-M20AC2/20AC1 では表示されません。
- 13) ビーコンミスしきい値
SR-M20AC2/20AC1 以外は表示されません。
- 14) ビーコン送出状態
SR-M20AC2/20AC1 では表示されません。
- normal** ビーコン送出中
- stopped(not running)**
ビーコン停止中 (回線状態が RUN または CSA 以外のため)
- stopped(off)**
ビーコン停止中 (回線閉塞のため)
- stopped(carrier detected)**
ビーコン停止中 (キャリア (無変調波) 検出のため)
- 15) A-MPDU 送信モード
- 16) A-MPDU 最大受信サイズ
- 17) A-MPDU 間隔
- 18) ガード インターバル
11n 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
- 19) 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
- 20) 動作モードの情報 (括弧内は動作中のキー長を示す)
- 21) 送信キーの情報
- 22) WEP 動作タイプの情報
SR-M20AC2/20AC1 では表示されません。

static コマンドで登録された静的な WEP キーを使用

dynamic

WEP キーを動的に生成して使用

23) WEP キー更新間隔の情報 (WEP 動作タイプが dynamic の場合のキー更新間隔)
SR-M20AC2/20AC1 では表示されません。

24) WPA 動作状況

25) 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

26) グループキー (GTK) 更新間隔の情報
SR-M20AC2/20AC1 では表示されません。

27) グループマスターキー (GMK) 更新間隔の情報
SR-M20AC2/20AC1 では表示されません。

28) 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

29) 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

30) TKIP 時の MIC エラー検出状態

normal

detected

21.1.5 show wlan wpa status

[機能]

WPA 状態情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1

[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 ~ 16	SR-M20AP2 SR-M20AP1

[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。

[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)
Next GTK rekey time : Mon Mar 9 21:39:43 2009 ---(3)
Next GMK rekey time : Tue Mar 10 07:29:13 2009 ---(4)
MIC failure detection status : normal ---(5)

No. User EAP-Type PAE status STA MAC address
(6) (7) (8) (9) (10)
WPA-Type Cipher suite PTK status Since
(11) (12) (13) (14)
-----
1 user01 TTLS Authenticated 00:00:0e:12:34:56
WPA2 AES Initiation Done Mon Mar 9 19:29:17 2009
2 user02 PEAP Authenticated 00:00:0e:98:76:54
WPA2 TKIP Initiation Done Mon Mar 9 19:29:23 2009
```

PSK 使用時

```
# show wlan wpa status

[wlan 1]
SSID                      : SRM-PSK
current STA number        : 2
Next GTK rekey time       : Mon Mar  9 21:39:43 2009
Next GMK rekey time       : Tue Mar 10 07:29:13 2009
MIC failure detection status : normal

No.  User          EAP-Type   PAE status   STA MAC address
     WPA-Type      Cipher suite PTK status   Since
-----
  1   WPA          AES        Authenticated 00:00:0e:12:34:56
     WPA          AES        Initiation Done -
  2   WPA2         TKIP       Authenticated 00:00:0e:98:76:54
     WPA2         TKIP       Initiation Done -
```

- 1) SSID
- 2) 現在接続中の STA 数
- 3) 次 GTK 鍵更新時間
- 4) 次 GMK 鍵更新時間
- 5) MIC failure 検出状態表示
 - normal** MIC エラー未検出
 - watch** MIC エラーを 1 回検出し、監視中
 - error** 複数回の MIC エラーを検出し、全 STA の排除中
- 6) STA 通番
- 7) IEEE802.1X 認証のユーザ名
- 8) 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。
- 9) 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
- 10) STA の MAC アドレス
- 11) WPA タイプ
- 12) 暗号モード
- 13) PTK(Pairwise Transit Key) 状態変数
- 14) 接続した時間 (再認証時は更新されません)

21.1.6 show wlan wpa statistics

[機能]

WPA 統計情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1

[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 ~ 16	SR-M20AP2 SR-M20AP1

<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。

[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
Single MIC failure detection count : 2
Multi MIC failure detection count : 2
Last MIC failure detection time  : Mar 25 07:27:50 2009
Authentication succeed count     : 21
Authentication failure count    : 2
Replayed frame detecting count   : 15
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)
Single MIC failure detection count : 2          ---(10)
Multi MIC failure detection count : 2          ---(11)
Last MIC failure detection time  : Mar 25 07:27:50 2009 ---(12)
Authentication succeed count     : 21        ---(13)
Authentication failure count    : 2          ---(14)
Replayed frame detecting count   : 15        ---(15)
Deauthentication count           : 217       ---(16)
  Unspecified reason              : 0          ---(17)
  Previous authentication no longer valid : 0          ---(18)
  Deauthenticated because sending station is leaving (or has left)
    IBSS or ESS                   : 0          ---(19)
  Disassociated due to inactivity : 0          ---(20)
  Disassociated because AP is unable to handle all currently
    associated stations           : 0          ---(21)
  Class 2 frame received from nonauthenticated station : 0          ---(22)
  Class 3 frame received from nonassociated station   : 0          ---(23)
  Disassociated because sending station is leaving(or has left) BSS : 0          ---(24)
  Station requesting (re)association is not authenticated with
    responding station           : 0          ---(25)
  Invalid information element     : 0          ---(26)
  MIC failure                     : 1          ---(27)
  4-Way Handshake timeout        : 1          ---(28)
  Group Key Handshake timeout    : 0          ---(29)
  Information element in 4-Way Handshake different from
    (Re)Association Request/Probe Response/Beacon frame : 0          ---(30)
  Invalid group cipher            : 0          ---(31)
  Invalid pairwise cipher        : 0          ---(32)
  Invalid AKMP                   : 0          ---(33)
  Unsupported RSN information element version : 0          ---(34)
  Invalid RSN information element capabilities : 0          ---(35)
  IEEE 802.1X authentication failed : 0          ---(36)
  Cipher suite(s) is unable to be accepted : 0          ---(37)
```

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) MIC(Message Integrity Code) シングルエラー発生回数
 - 11) MIC マルチエラー発生回数
 - 12) 最後に MIC エラーを検出した時刻
 - 13) 認証成功回数
 - 14) 認証失敗回数
 - 15) リプレイパケットを検出した回数
 - 16) STA との接続が切断された回数
 - 17) ~ 37) は切断理由ごとの統計情報
 - 17) その他のエラー回数
 - 18) 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
 - 19) IBSS または ESS モードで STA との接続が切断された回数
 - 20) 同期が外れたために切断された回数
 - 21) 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
 - 22) 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
 - 23) Class 3 のフレームを Association されていない STA から受信した回数
 - 24) BSS モードで STA との接続が切断された回数
 - 25) 認証が拒否された STA から Association されたため切断した回数
 - 26) 不当な要求により切断された回数
 - 27) MIC Failure により切断された回数
 - 28) 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
 - 29) 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
 - 30) 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
 - 31) Group Cipher が許容できないため切断された回数
 - 32) Pairwise Cipher が許容できないため切断された回数
 - 33) 不当な AKMP(Authentication and Key Management Protocol) が指定されたため切断された回数
 - 34) 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
 - 35) 許容できない RSN Capability により切断された回数
 - 36) IEEE802.1X 認証が失敗したため切断された回数
 - 37) IEEE802.1X 認証方式が利用不可であったため切断された回数

21.1.7 show wlan relay status

[機能]

無線 LAN 中継機能の情報の表示

[適用機種]



[入力形式]

show wlan relay status [number <wlan_number>]

[オプション]

なし

すべての無線 LAN インタフェースの無線 LAN 中継機能の情報を表示します。

number <wlan_number>

- wlan 定義番号
指定された無線 LAN インタフェースの無線 LAN 中継機能の情報を表示します。
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。

[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 中継機能のステータス情報および接続ノードの情報を表示します。

[実行例]

```
# show wlan relay status
[wlan 1]
IEEE802.11 Wireless LAN relay Information
mode           : multi           ---(1)
expire         : 1d              ---(2)
node           : 3                ---(3)

[node own]     ---(4)
MAC address    :00:00:0e:12:34:51 ---(5)
IP address     :                  ---(6)

[node 1]       ---(7)
MAC address    :00:00:0e:12:34:56 ---(8)
IP address     :                  ---(9)
Since          :May  8 19:29:17 2009 ---(10)
Last           :May  8 21:11:35 2009 ---(11)

[node 2]
MAC address    :00:00:0e:98:76:54
IP address     :100.100.100.100
Since          :May  8 19:29:17 2009
Last           :May  8 20:43:21 2009

[node 3]
MAC address    :00:00:0e:11:22:33
IP address     :200.200.200.200
Since          :May  8 19:29:17 2009
Last           :May  8 19:43:01 2009
```

-
- 1) mode
無線 LAN 中継機能の動作モード
 - 2) expire
無線 LAN 中継の expire 時間
 - 3) node
この無線 LAN インタフェースを使用して通信しているノード数
 - 4) own
自装置識別情報
 - 5) MAC address
自装置が使用する MAC アドレス
 - 6) IP address
自装置に割り当てられている IP アドレス
 - 7) node
表示しているノードのテーブル番号
 - 8) MAC address
ノードの MAC アドレス
 - 9) IP address
ノードの IPv4 アドレス
 - 10) Since
テーブルを作成した時刻
 - 11) Last
最後に当該ノードからのパケットを受信した時刻

21.1.8 show wlan supplicant status

[機能]

無線 LAN インタフェースでのサブリカント情報の表示

[適用機種]



[入力形式]

show wlan supplicant status [number <wlan_number>]

[オプション]

なし

すべての無線 LAN インタフェースのサブリカント情報を表示します。

number <wlan_number>

- wlan 定義番号
指定された無線 LAN インタフェースのサブリカント情報を表示します。
該当する無線 LAN インタフェースが無効の場合は表示されません。

[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]

サブリカント機能のステータス情報を表示します。

[実行例]

```
#show wlan supplicant status
[wlan 1]
supplicant state           : CONNECTED           ---(1)
ssid                       : samplenet           ---(2)
bssid                      : 00:00:0e:ee:ee:ee         ---(3)
WPA Information
wpa auth                   : WPA2                   ---(4)
wpa mcastcipher            : TKIP              ---(5)
wpa ucastcipher            : TKIP              ---(6)
MIC failure detection status : normal             ---(7)
IEEE802.1X Information
PAE state                  : AUTHENTICATED      ---(8)
EAP peer Information
EAP state                  : SUCCESS            ---(9)
EAP protocol               : EAP-TTLS(MSCHAPv2) --- (10)
```

```
#show wlan supplicant status
[wlan 1]
supplicant state           : DISCONNECTED      ---(1)
ssid                       : samplenet           ---(2)
```

1) サブリカントの状態

INACTIVE

初期化状態

DISCONNECTED

接続未完

SCANNING

周辺アクセスポイント検出中

ASSOCIATING

アソシエーション中

ASSOCIATED

アソシエーション完了

4WAY_HANDSHAKE

暗号化方式ネゴシエーション中

2WAY_HANDSHAKE

暗号化方式 (マルチキャストおよびブロードキャスト) ネゴシエーション中

CONNECTED

接続完了

2) SSID

3) BSSID

1) の状態が INACTIVE/DISCONNECTED/SCANNING のときには表示されません。

以降の情報は、1) の状態が INACTIVE/DISCONNECTED/SCANNING/ASSOCIATING のときには表示されません。

4) WPA 認証

WPA WPA による IEEE802.1X 認証

WPA2 WPA2 による IEEE802.1X 認証

WPA-PSK

WPA による事前共有キー認証

WPA2-PSK

WPA2 による事前共有キー認証

wpa 認証/暗号を使用しない場合は何も表示されません。

5) 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 暗号方式

AES AES 暗号方式

wpa 認証/暗号を使用しない場合は何も表示されません。

6) 暗号化方式 (ユニキャスト)

TKIP TKIP 暗号方式

AES AES 暗号方式

wpa 認証/暗号を使用しない場合は何も表示されません。

7) MIC failure 検出状態表示

normal MIC エラー未検出

watch MIC エラーを 1 回検出し、監視中

8) IEEE802.1X PAE の状態

LOGOFF

初期化状態

DISCONNECTED

接続未完

CONNECTING

接続中

AUTHENTICATING

認証処理中

HELD 処理待ち合わせ中

AUTHENTICATED

認証完了

RESTART

再認証開始

IEEE802.1X 認証を使用しない場合は何も表示されません。

9) EAP 状態

INITIALIZE

初期状態

IDLE パケット受信待ち

RECEIVED

EAP パケット受信

GET_METHOD

新メソッド受信

METHOD

メソッド処理中

SEND_RESPONSE

応答パケット送信

DISCARD

EAP パケット破棄

IDENTITY

IDENTITY 受信

NOTIFICATION

NOTIFICATION 受信

RETRANSMIT

EAP パケット再送

SUCCESS

処理成功

FAILURE

処理失敗

DISABLED

非活性

EAP 認証を使用しない場合は何も表示されません。

10) EAP プロトコル

EAP-MD5

EAP-TLS

EAP-TTLS

EAP-PEAPv0

EAP-PEAPv1

EAP 認証を使用しない場合は何も表示されません。

なお、EAP-TTLS,EAP-PEAP の場合、つづけて内部認証方式を示します。

PAP

CHAP

MSCHAPv2

21.1.9 show wlan supplicant statistics

[機能]

無線 LAN インタフェースでのサブリカント認証統計情報の表示

[適用機種]



[入力形式]

show wlan supplicant statistics [number <wlan_number>]

[オプション]

なし

すべての無線 LAN インタフェースのサブリカント認証統計情報を表示します。

number <wlan_number>

指定された無線 LAN インタフェースのサブリカント認証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表示されません。

[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]

サブリカント認証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 wlan supplicant statistics
[wlan 1]
IEEE802.1X Information
  EAPOL frame received count      : 0          ---(1)
  EAPOL frame sent count          : 0          ---(2)
  EAPOL Start frame sent count    : 0          ---(3)
  EAP Identity Response sent count: 0          ---(4)
  EAP response sent count         : 0          ---(5)
  EAP Identity Request received count: 0        ---(6)
  EAP request received count      : 0          ---(7)
  Invalid EAPOL frame received count: 0        ---(8)
  EAP with illegal length frame received count: 0      ---(9)
  Version of EAPOL last received frame: 0        ---(10)
  Authenticator address of last received frame: 00:00:00:00:00:00 ---(11)
IEEE802.11 Information
  RSN 4WayHandshake failure count : 0          ---(12)
MIC failure Information
  Single MIC failure detection count: 2          ---(13)
  Multi MIC failure detection count : 2          ---(14)
  Last MIC failure detection time   : Mar 25 07:27:50 2009 --(15)
```

- 1) 受信 EAPOL フレーム数
- 2) 送信 EAPOL フレーム数

-
- 3) 送信 EAPOL-Start フレーム数
 - 4) 送信 EAP Identity response フレーム数
 - 5) 送信 EAP response フレーム数
 - 6) 受信 EAP Identity request フレーム数
 - 7) 受信 EAP request フレーム数
 - 8) 受信した無効な EAPOL フレーム数
 - 9) 受信した不当なパケット長の EAPOL フレーム数
 - 10) 最後に受信した EAPOL フレームのバージョン番号
 - 11) 最後に受信した端末 (Authenticator) の MAC アドレス
 - 12) 4WayHandshake に失敗した数
 - 13) MIC(Message Integrity Code) シングルエラー発生回数
 - 14) MIC マルチエラー発生回数
 - 15) 最後に MIC エラーを検出した時刻

21.1.10 show wlan blockack session

[機能]

BlockAck セッション情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show wlan blockack session [number <wlan_number>]

[オプション]

なし

すべての BlockAck セッション情報を表示します。

number <wlan_number>

- wlan 定義番号
指定された無線 LAN インタフェースの BlockAck セッション情報を表示します。
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 ~ 16	SR-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

[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]

BlockAck セッション情報を表示します。

[実行例]

```
# show wlan blockack session
[wlan 1]
MAC Address      TID  Ori/Rec  Status
(1)             (2)   (3)     (4)
00:16:e3:00:00:02 0    Rec      Run
00:16:e3:00:00:02 1    Rec      Run
00:16:e3:00:00:02 1    Ori      Wait
00:16:e3:00:00:02 2    Ori      Run
00:16:e3:00:00:02 3    Ori      Nak
00:16:e3:00:00:03 3    Rec      Run
00:16:e3:00:00:04 15   Rec      Run

[wlan 2]
MAC Address      TID  Ori/Rec  Status
00:16:e3:00:00:11 0    Rec      Run
00:16:e3:00:00:11 0    Ori      Run
~
```

1) MAC Address

無線 LAN アクセスポイントおよび無線 LAN 端末の MAC アドレス

2) TID

3) Ori/Rec

BlockAck セッションの確立を要求した側の場合、Ori (originator)

BlockAck セッションの確立を要求された側の場合、Rec (recipient)

4) Status

Run BlockAck セッションが確立中

Wait BlockAck セッションの確立を要求中

Nak BlockAck セッションの確立を要求したが、相手側に拒否されたとき

21.2 無線 LAN 接続のカウンタ・ログ・統計などのクリア

21.2.1 clear wlan statistics

[機能]

無線 LAN 統計情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
clear 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クリアします。

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クリアします。

範囲	機種
1 ~ 16	SR-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

[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 統計情報をクリアします。

[実行例]



```
# clear wlan statistics  
#
```

21.2.2 clear wlan wpa statistics

[機能]

WPA 統計情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1  

[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。

[実行例]

```
# clear wlan wpa statistics  
#
```

21.2.3 clear wlan relay table

[機能]

ノード管理テーブルの解放

[適用機種]

		SR-M20AC2	SR-M20AC1
--	--	-----------	-----------

[入力形式]

clear wlan relay table [number <wlan_number>] [mac <mac>]

[オプション]

number <wlan_number>

- wlan 定義番号
解放するノード管理テーブルの無線 LAN インタフェースを指定します。
また、該当する無線 LAN インタフェースが無効の場合は解放されません。
省略時は、すべての無線 LAN インタフェースが解放対象となります。

mac <mac>

- MAC アドレス
解放するノード管理テーブルの MAC アドレスを指定します。
指定した MAC アドレスに一致する情報を持つテーブルが解放されます。
省略時は、すべてのテーブルが解放対象となります。

[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]

登録済みとなっている端末の情報を強制的に解放する場合に実行します。

21.2.4 clear wlan supplicant statistics

[機能]

無線 LAN インタフェースでのサブリカント認証統計情報のクリア

[適用機種]

 SR-M20AC2 SR-M20AC1

[入力形式]

clear wlan supplicant statistics

[オプション]

なし

すべての無線 LAN インタフェースに関するサブリカント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]

サブリカント認証統計情報をクリアします。

[実行例]

```
# clear wlan supplicant statistics
#
```

第 22 章 POE のログ・状態などの表示コマンド

22.1 POE のログ・状態などの表示

22.1.1 show poe drawing

[機能]

装置の受電状態の表示

[適用機種]

SR-M20AP2 SR-M20AP1

[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)
Ethernet Port 2  : drawing       ---(3)

#
```

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。

3) Ethernet Port 2 の状態

Ethernet Port 2 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 23 章 USB 接続のカウンタ・ログ・統計・ 状態などの表示コマンド

23.1 USB 接続のカウンタ・ログ・統計・状態などの表示

23.1.1 show usb hcd status

[機能]

USB ポートの閉塞状態表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

show usb hcd status

[オプション]

なし

USB ポートの閉塞状態を表示します。

[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 ポートの閉塞状態を表示します。

[実行例]

```
# show usb hcd status
[USB HCD STATUS]
status                : enable          --- (1)
```

1) 閉塞状態

USB ポートの閉塞状態が表示されます。

disable 閉塞状態

enable 閉塞解除状態

23.1.2 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-M20AP2 SR-M20AP1

[入力形式]

show usb storage status

[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]

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

[Thread]
Status           : Active           ---(1)

[Device #1]
Status           : Idle             ---(2)
Speed            : Full             ---(3)
Geometry probing : Success          ---(4)
  Test unit ready : Success          ---(5)
  Inquiry         : Success
  Mode sense      : Success
  Read capacity   : Success
  Read format capacities : ----
Hold data        : Not exist        ---(6)
Error status     : Get device specs [5/5] (Read format capacities) ---(7)
  Error reason    : Transfer URB failure ---(8)
  Error event     : 0x3200000d      ---(9)
  Request sense code : (02, 10, 00)      ---(10)
[Storage specs]
Vendor           : FUJITSU          ---(11)
Product          : USB PortableDrive ---(12)
Product Rev.     : 3.96             ---(13)
Total sectors    : 500400          ---(14)
Cylinders        : 695             ---(15)
Heads            : 15              ---(16)
Sectors per track : 48            ---(17)
[USB specs]
Speed            : Full             ---(18)
Max LUN          : 3               ---(19)
[USB configuration]
Device address   : 1               ---(20)
Interface        : 0               ---(21)
Sub class       : 6                ---(22)
LUN              : 0               ---(23)
BulkInEP        : 0x82            ---(24)
BulkOutEP       : 0x02            ---(25)
```

1) USB マスストレージ制御スレッド 状態

以下のどれかが表示されます。

Uinit 未初期化

Waiting for USBD active

起動中 (USB 起動待ち)

Waiting for entry class completed

起動中 (エントリクラス処理完了待ち)

Active 活性

以下の情報は、USB デバイスの接続を認識した場合に表示されます。

2) USB デバイス制御状態

以下のどれかが表示されます。

Uinit 未初期化

Initializing [1/2] (Set configuration)

初期化中 (Set configuration)

Initializing [2/2] (Get max lun)

初期化中 (Get max lun)

Get device specs [1/5] (Test unit ready)

デバイス諸元獲得中 (Test unit ready)

Get device specs [2/5] (Inquiry)

デバイス諸元獲得中 (Inquiry)

Get device specs [3/5] (Mode sense)

デバイス諸元獲得中 (Mode sense)

Get device specs [4/5] (Read capacity)

デバイス諸元獲得中 (Read capacity)

Get device specs [5/5] (Read format capacities)

デバイス諸元獲得中 (Read format capacities)

Idle アイドル (転送要求待ち)

Transferring

転送中

Waiting for unplugging

USB デバイス取り外し待ち (異常検出)

Unplugging

取り外し処理中

3) 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。

Full フルスピードモード (12Mbps)

Low ロースピードモード (1.5Mbps)

- 4) ジオメトリ検出状況
マスストレージデバイスの全セクタ数、シリンダ数、ヘッド数、1トラックあたりのセクタ数をジオメトリと呼びます。
以下のどれかが表示されます。
- Success** 成功
 - Success(partly guessed)**
成功 (情報の一部は推測されました)
 - Failed** 失敗
 - Not yet** 検出はまだ行われていません
- 5) ジオメトリ検出状況 詳細表示
ジオメトリ検出は、SCSI コマンド (TEST_UNIT_READY, INQUIRY, MODE SENSE(6), READ CAPACITY, READ FORMAT CAPACITIES) によって、行われます。
各コマンドの実施状態が、以下のどれかで表示されます。
- Success** 成功
 - Failed (no data)**
失敗 (データなし)
 - Failed (retry out)**
失敗 (リトライアウト)
 - Failed** 失敗 (その他)
 - 実施されていない
- 6) 保持しているデータの有無
ファイルシステムから受けた転送要求の有無が表示されます。
以下のどちらかが表示されます。
- Exists** 存在する
 - Not exists**
存在しない
- 以下、7), 8), 9), 10) の情報は、エラーが発生し転送動作を継続できなくなった場合だけ表示されます。
- 7) エラー発生時の状態
エラーが発生したときの USB デバイス制御状態 (2) が表示されます。
- 8) エラー原因
転送動作を継続できなくなった原因が表示されます。
- 9) エラーイベント
内部情報が表示されます。
- 10) リクエストセンスコード
USB デバイス側でエラーを検出した際に設定される USB デバイス側のエラー情報が表示されます。
- 11) 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。
- 12) 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。

-
- 13) 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。
 - 14) 全セクタ数
USB デバイスの保持する全セクタ数が表示されます。
 - 15) シリンダ数
USB デバイスのシリンダ数が表示されます。
 - 16) ヘッド数
USB デバイスのヘッド数が表示されます。
 - 17) トラックあたりのセクタ数
USB デバイスの1トラック (1 ヘッド、1 シリンダ) あたりのセクタ数が表示されます。
 - 18) 速度
USB プロトコル速度が表示されます。(3) と同一です。
 - 19) 最大 LUN
USB デバイスの持つ LUN の最大値が表示されます。本装置では、LUN=0 以外のデバイスをサポートしません。
 - 20) 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。
 - 21) 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。
 - 22) 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。
 - 23) 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。
 - 24) 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。
 - 25) 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 24 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 vlan1 ~ vlan4094	SR-M20AP2 SR-M20AP1
lan0 lo0	SR-M20AC2 SR-M20AC1

24.1 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 interface

[機能]

インタフェース情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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          MTU 1500    <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
-(1)-          -(2)-    -----(3)-----
  Type: port vlan
  VLAN ID is 20
  MAC address: 00:00:0e:f1:41:dc
  Status: up since Jul 24 14:44:48 2009
  IP address/masklen:
    192.168.1.1/24      Broadcast 192.168.1.255
lan1          MTU 1500    <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
  Type: port vlan
  VLAN ID is 30
  MAC address: 00:00:0e:f1:41:dc
  Status: up since Jul 24 14:44:48 2009
  IP address/masklen:
    192.168.3.1/24      Broadcast 192.168.3.255
lo0          MTU 16384    <UP,LOOPBACK,RUNNING,MULTICAST>
  Type: loopback
  Status: up since Jul 24 14:44:48 2009
  IP address/masklen:
    127.0.0.1/32
#
# show interface interface vlan20
vlan20       MTU 1500    <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
  Type: port vlan
  VLAN ID is 20
  Status: up since Jul 24 14:44:48 2009
#
```


- 1) インタフェース名
- 2) MTU サイズ
- 3) 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。

- 4) Type

インタフェースタイプが以下の文字列で表示されます。

port vlan

ポート VLAN

loopback

ループバックインタフェース

VLAN ID

VLAN ID が表示されます。

MAC address

このインタフェースで利用される MAC アドレスが表示されます。

Status

インタフェースの状態と、この状態になった時刻が表示されます。

up 利用可能

down 利用不可

IP address/masklen

インタフェースの IPv4 アドレスが表示されます。

24.1.2 show interface brief

[機能]

インタフェース情報の簡易表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show interface brief [interface <interface_name>]

[オプション]

なし

lan および lo インタフェースを簡易表示します。

interface <interface_name>

指定したインタフェースを簡易表示します。

[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簡易表示します。

[実行例]

```
# show interface brief
Interface      Status      Type
-----
(1)            (2)         (3)
lan0           up          port vlan
lan1           up          port vlan
lo0           up          loopback
#
# show interface brief interface vlan20
Interface      Status      Type
-----
(1)            (2)         (3)
vlan20        up          port vlan
#
```

- 1) Interface
インタフェース名が表示されます。
- 2) Status
インタフェースの状態が表示されます。
up 利用可能
down 利用不可
- 3) Type
インタフェースタイプが表示されます。

port vlan

ポート VLAN

loopback

ループバックインタフェース

24.1.3 show interface summary

[機能]

インタフェースエントリ数の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show interface summary

[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]

インタフェースのエントリ数を表示します。

[実行例]

```
# show interface summary
There are 3 interfaces (up status 3 interfaces)
  Loopback interface      :   1 (up status   1 interfaces) ---(1)
  Port VLAN interface     :   2 (up status   2 interfaces) ---(2)
#
```

- 1) ループバックインタフェース
- 2) ポート VLAN

24.1.4 show interface detail

[機能]

インタフェース情報の詳細表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show interface detail [interface <interface_name>]

[オプション]

なし

lan および lo インタフェースを詳細表示します。

interface <interface_name>

指定したインタフェースを詳細表示します。

[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]

インタフェース情報を詳細表示します。

[実行例]

```
# show interface detail
lan0          MTU 1500    <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
-(1)-          -(2)-    -----(3)-----
Type: port vlan
VLAN ID is 20
MAC address: 00:00:0e:f1:41:dc
Status: up since Jul 24 14:44:48 2009
IP address/masklen:
  192.168.1.1/24      Broadcast 192.168.1.255
statistics:
  in packets:          60845 out packets:          39355
  bytes:               323823 bytes:             243227
  unicasts:            59606 unicasts:         38519
  multicasts/broadcasts: 1238 multicasts/broadcasts: 835
  discards:            157   discards:         10
                                drop:              0
lan1          MTU 1500    <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
Type: port vlan
VLAN ID is 30
MAC address: 00:00:0e:f1:41:dc
Status: up since Jul 24 14:44:48 2009
IP address/masklen:
  192.168.3.1/24      Broadcast 192.168.3.255
statistics:
  in packets:          39660 out packets:          44317
  bytes:               222002 bytes:             136670
  unicasts:            38834 unicasts:         43482
  multicasts/broadcasts: 825 multicasts/broadcasts: 835
  discards:             81   discards:         2
                                drop:              0
lo0          MTU 16384    <UP,LOOPBACK,RUNNING,MULTICAST>
Type: loopback
Status: up since Jul 24 14:44:48 2009
IP address/masklen:
  127.0.0.1/32
statistics:
  in packets:          174974 out packets:          174974
  bytes:              12391593 bytes:             12391593
  unicasts:            174974 unicasts:         174974
  multicasts/broadcasts: 0 multicasts/broadcasts: 0
  discards:             0   discards:         0
                                drop:              0
#
# show interface detail interface vlan20
vlan20        MTU 1500    <UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST>
Type: port vlan
VLAN ID is 20
Status: up since Jul 24 14:44:48 2009
statistics:
  in packets:          60845 out packets:          39355 (4)
  bytes:               323823 bytes:             243227
  unicasts:            59606 unicasts:         38519
  multicasts/broadcasts: 1238 multicasts/broadcasts: 835
  discards:            157   discards:         10
                                drop:              0
#
```

- 1) インタフェース名
- 2) MTU サイズ
- 3) 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。

4) Type

インタフェースタイプが以下の文字列で表示されます。

port vlan

ポート VLAN

loopback

ループバックインタフェース

VLAN ID

VLAN ID が表示されます。

MAC address

このインタフェースで利用される MAC アドレスが表示されます。

Status

インタフェースの状態と、この状態になった時刻が表示されます。

up 利用可能

down 利用不可

IP address/masklen

インタフェースの IPv4 アドレスが表示されます。

statistics

自局あてであるインタフェースの統計情報が表示されます。

24.1.5 show interface statistics

[機能]

インタフェース統計情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show interface statistics [interface <interface_name>]

[オプション]

なし

lan および lo インタフェースの統計情報を表示します。

interface <interface_name>

指定したインタフェースの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]

インタフェースの統計情報を表示します。

[実行例]

```

# show interface statistics
lan0          Status: up      Type: port vlan
-(1)-         -(2)-         ---(3)---
  statistics:
    in packets:      60845 out packets:      39355
    bytes:           323823 bytes:           243227
    unicasts:        59606  unicasts:        38519
    multicasts/broadcasts: 1238 multicasts/broadcasts: 835
    discards:        157   discards:        10
                                drop:           0

lan1          Status: up      Type: port vlan
  in packets:      39660 out packets:      44317
  bytes:           222002 bytes:           136670
  unicasts:        38834  unicasts:        43482
  multicasts/broadcasts: 825 multicasts/broadcasts: 835
  discards:        81   discards:        2
                                drop:           0

lo0           Status: up      Type: loopback
  statistics:
    in packets:      174974 out packets:      174974
    bytes:           12391593 bytes:           12391593
    unicasts:        174974  unicasts:        174974
    multicasts/broadcasts: 0 multicasts/broadcasts: 0
    discards:        0   discards:        0
                                drop:           0

#
# show interface statistics interface vlan20
vlan20        Status: up      Type: port vlan
  statistics:
    in packets:      60845 out packets:      39355
    bytes:           323823 bytes:           243227
    unicasts:        59606  unicasts:        38519
    multicasts/broadcasts: 1238 multicasts/broadcasts: 835
    discards:        157   discards:        10
                                drop:           0

#

```

1) インタフェース名

2) Status

インタフェースの状態が表示されます。

up 利用可能

down 利用不可

3) Type

インタフェースタイプが表示されます。

port vlan

ポート VLAN

loopback

ループバックインタフェース

24.2 インタフェースのカウンタ・ログ・統計・状態などのクリア

24.2.1 clear interface statistics

[機能]

インタフェースの統計情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
clear interface statistics [interface <interface_name>]
```

[オプション]

なし

すべてのインタフェースの統計情報をクリアします。

interface <interface_name>

指定したインタフェース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]

インタフェースの統計情報をクリアします。

[実行例]

```
# clear interface statistics  
#
```

第 25 章 ARP エントリの表示、クリア操作 コマンド

25.1 ARP エントリの表示

25.1.1 show arp

[機能]

ARP エントリの表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

[メッセージ]

```
Routing tables are modified. Cannot continue print.
```

ルーティング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。

【実行例】

```

# show arp
IP Address      MAC Address      F  Rest  Interface Port
-----
(1)            (2)            (3) (4)  (5)    (6)
20.0.0.1       00:00:e2:08:57:89  01146 lan0   ether1
20.0.0.2       (incomplete)      lan0   wlan1
20.0.0.255     00:00:02:01:14:00 P  perm  lan0
Entry:3

# show arp summary
Entry:3

# show arp 20.0.0.1
IP Address      MAC Address      F  Rest  Interface Port
-----
20.0.0.1       00:00:e2:08:57:89  01146 lan0   ether1
Entry:1
---(7)

#

```

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) Rest

ARP エントリの残り生存時間を秒数で示します。Permanent エントリの場合は "perm" と表示されます。

5) Interface

ARP エントリのインタフェースが表示されます。

6) Port

送信時に利用される ether ポート番号または無線 LAN インタフェースが表示されます。

ether ether ポート

wlan 無線 LAN インタフェース

7) Entry

ARP エントリのエントリ数が表示されます。

25.2 ARP エントリのクリア

25.2.1 clear arp

[機能]

ARP エントリのクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 26 章 ルーティングテーブル情報・統計などの表示コマンド

26.1 IPv4 ルーティングテーブル情報・統計などの表示

26.1.1 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
show ip route [all]
show ip route connected [all]
show ip route static [all]
show ip route destination <ip_address>/<mask> [all]
show ip route destination <ip_address>/<mask> longer-prefixes [all]
```

[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。

all

ルーティングテーブルに非登録の経路情報を含めてすべての経路情報を表示します。

connected

インタフェース経路情報のみを表示します。

static

スタティック経路情報のみを表示します。

destination <ip_address>/<mask>

指定したアドレスとマスクに一致した経路情報のみを表示します。

<mask>は、マスクビット数またはマスク値で指定します。マスク値の場合は、最上位ビットから1で連続した値にしてください。

destination <ip_address>/<mask> longer-prefixes

指定した経路情報に含まれる経路情報すべてを表示します。

<mask>は、マスクビット数またはマスク値で指定します。マスク値の場合は、最上位ビットから1で連続した値にしてください。

[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 all
FP Destination/Mask Gateway Distance UpTime Interface
-----
(1) (2) (3) (4) (5) (6)
*C 192.168.10.0/24 192.168.10.50 0 00:00:01 lan0
*C 192.168.16.0/24 192.168.16.50 0 00:00:01 lan1
*C 192.168.17.0/24 192.168.17.50 0 00:00:01 lan2
```

1) FP

カーネルフラグ (F) および経路を注入したプロトコルの種別 (P) が表示されます。

以下に、表示されるカーネルフラグ (F) を示します。

* : カーネルへ登録した経路を示します。

空白 : カーネルへ登録していない経路を示します。

以下に、経路注入元プロトコル種別 (P) を示します。

S : スタティック経路情報を示します。

C : インタフェース (interface route) 経路情報を示します。

2) Destination/Mask

あて先アドレス / マスク長が表示されます。

3) Gateway

ゲートウェイアドレスが表示されます。

4) Distance

経路優先度が表示されます。

5) UpTime

経路情報更新時からの経過時間が表示されます。

01:23:45 : 1 時間 23 分 45 秒経過 (経過時間が 24 時間以内の場合)

6d23h45m

: 6 日と 23 時間 45 分経過 (経過時間が 7 日以内の場合)

3w6d23h : 3 週間と 6 日と 23 時間経過

6) Interface

出力インタフェース名が表示されます。使用不可能状態のインタフェースは、インタフェース名に続いて (inactive) が表示されます。

26.1.2 show ip route summary

[機能]

ルーティングテーブルの経路情報数の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show ip route summary [all]

[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の数を表示します。

all

ルーティングテーブルに非登録の経路情報を含めてすべての経路情報の数を表示します。

[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]

経路共通管理部に登録している経路情報数を表示します。

[実行例]

```
# show ip route summary
Route Source   Networks
-----
(1)            (2)
Static         2
Connected      1
Total          3
```

1) Route Source

経路を注入したプロトコルの種別が表示されます。

Static : スタティック経路情報を示します。

Connected

: インタフェース経路情報を示します。

2) Networks

経路数が表示されます。

26.1.3 show ip route kernel

[機能]

IP カーネルのルーティングテーブルの表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
show ip route kernel
show ip route kernel longest-match <ip_address>
show ip route kernel summary
```

[オプション]

longest-match <ip_address>

IP カーネルのルーティングテーブルのうち、指定されたアドレスに longest match するエントリを表示します。

summary

IP カーネルのルーティングテーブルの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]

IP カーネルのルーティングテーブルの、現在の状態を表示します。

[実行例]

```
# show ip route kernel
Routing Tables for Internet

Destination/Masklen Gateway          Flag   Interface
-----
(1)          (2)          (3)    (4)
10.0.0.0/8   192.168.1.5  UGS    lan0
127.0.0.1    127.0.0.1    UH     lo0
192.168.1.0/24 link#1       U      lan0
192.168.1.5  link#1       UH     lan0
192.168.1.11 00:a0:c9:d8:90:4e UH     lan0
224.0.0.0/4  127.0.0.1    UG     lo0
Entry:6                                           ---(5)

# show ip route kernel longest-match 10.0.0.1
Routing Tables for Internet

Destination/Masklen Gateway          Flag   Interface
-----
10.0.0.0/8     192.168.1.5  UGS    lan0
Entry:1

# show ip route kernel longest-match 20.0.0.1
Routing Tables for Internet

Destination/Masklen Gateway          Flag   Interface
-----
Entry:0

# show ip route kernel summary
Entry:6

#
```

1) Destination/Masklen

あて先ネットワークアドレスとマスク値が表示されます。

ホスト経路の場合はマスク値は表示されません。

2) Gateway

ゲートウェイアドレスが表示されます。

ダイレクト経路はゲートウェイの MAC アドレスが表示されます。ゲートウェイのアドレス解決ができていない場合は link#x(x はシステムがインタフェースごとに自動的に付与するインタフェースインデックス番号) が表示されます。

3) Flag

エントリ種別が表示されます。詳細を以下に示します。

U (Up) 経路が有効であることを示します。

G (Gateway)

ゲートウェイなどによる中継を必要とする経路を示します。

H (Host) ホストエントリを示します。

S (Static)

スタティックルートを示します。

R (Reject)

破棄経路 (ICMP unreachable 送信あり) であることを示します。

B (Blackhole)

破棄経路 (ICMP unreachable 送信なし) であることを示します。

- 4) Interface
送出先インタフェースが表示されます。
- 5) Entry
装置内部で使用する経路を除いたエントリ数が表示されます。

第 27 章 パケットの統計情報の表示、クリア 操作コマンド

27.1 パケットの統計情報の表示

27.1.1 show ip traffic

[機能]

IP 関連の統計情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
show ip traffic
show ip traffic { tcp | udp | ip | icmp }
```

[オプション]

なし

すべての IP 統計情報を表示します。

tcp

TCP パケットの統計情報を表示します。

udp

UDP パケットの統計情報を表示します。

ip

IP パケットの統計情報を表示します。

icmp

ICMP パケットの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
tcp:
  170 packets sent
    145 data packets (29694 bytes)
    1 data packet (18 bytes) retransmitted
    0 resends initiated by MTU discovery
    19 ack-only packets (10 delayed)
    0 URG only packets
    0 window probe packets
    0 window update packets
    5 control packets
  217 packets received
    145 acks (for 29706 bytes)
    1 duplicate ack
    0 acks for unsent data
    121 packets (14492 bytes) received in-sequence
    0 completely duplicate packets (0 bytes)
    0 old duplicate packets
    0 packets with some dup. data (0 bytes duped)
    3 out-of-order packets (42 bytes)
    0 packets (0 bytes) of data after window
    0 window probes
    0 window update packets
    0 packets received after close
    0 discarded for bad checksums
    0 discarded for bad header offset fields
    0 discarded because packet too short
  3 connection requests
  4 connection accepts
  0 bad connection attempts
  0 listen queue overflows
  6 connections established (including accepts)
  2 connections closed (including 1 drop)
    1 connection updated cached RTT on close
    1 connection updated cached RTT variance on close
    0 connections updated cached ssthresh on close
  1 embryonic connection dropped
  145 segments updated rtt (of 145 attempts)
  1 retransmit timeout
    0 connections dropped by rexmit timeout
  0 persist timeouts
    0 connections dropped by persist timeout
  22 keepalive timeouts
    0 keepalive probes sent
    0 connections dropped by keepalive
  22 correct ACK header predictions
  64 correct data packet header predictions
udp:
  250 datagrams received
  0 with incomplete header
  0 with bad data length field
  0 with bad checksum
  0 dropped due to no socket
  224 broadcast/multicast datagrams dropped due to no socket
  0 dropped due to full socket buffers
  0 not for hashed pcb
  26 delivered
  0 tunneling packets that can't find gif
```

(続<)

(続き)

```
26 datagrams output
ip:
  467 total packets received
  0 bad header checksums
  0 with size smaller than minimum
  0 with data size < data length
  0 with ip length > max ip packet size
  0 with header length < data size
  0 with data length < header length
  0 with bad options
  0 with incorrect version number
  0 fragments received
  0 fragments dropped (dup or out of space)
  0 fragments dropped after timeout
  0 packets reassembled ok
  467 packets for this host
  0 packets for unknown/unsupported protocol
  0 packets forwarded
  0 packets not forwardable
  0 redirects sent
  197 packets sent from this host
  0 packets sent with fabricated ip header
  0 output packets dropped due to no bufs, etc.
  0 output packets discarded due to no route
  0 output datagrams fragmented
  0 fragments created
  0 datagrams that can't be fragmented
  0 tunneling packets that can't find gif
icmp:
  0 calls to icmp_error
  0 errors not generated because old message was icmp
  0 messages with bad code fields
  0 messages < minimum length
  0 bad checksums
  0 messages with bad length
  0 message responses generated
#
```

27.2 パケットの統計情報のクリア

27.2.1 clear ip traffic

[機能]

IP 関連の統計情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

clear ip traffic

[オプション]

なし

IP 関連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]

IP 関連の統計情報をクリアします。

[注意]

IP フォワーディング機能を使用している場合、IP パケットの統計情報は、Ethernet 物理ポートの統計情報を加算して表示しています。そのため本コマンドでクリアを行っても IP パケットの統計情報の一部はクリアされません。すべての IP パケットの統計情報をクリアするためには、Ethernet 物理ポート統計情報のクリアを行ってください。

[実行例]

```
# clear ip traffic
#
```

第 28 章 DHCP のカウンタ・ログ・統計・状態などの表示コマンド

28.1 IPv4 DHCP のカウンタ・ログ・統計・状態などの表示

28.1.1 show ip dhcp

[機能]

IPv4 DHCP 運用状況の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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          : Mon Mar 16 14:00:13 2009 --- (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 29 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

29.1 ブリッジのカウンタ・ログ・統計・状態などの表示

29.1.1 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
SR-M20AC2/20AC1 では指定できません。

- 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, A - Authenticated entry
Address          VLAN Interface      Status Remain time Hit  Discard
-----
(1) (2) (3) (4) (5) (6) (7)
00:0e:00:78:2f:7a 10 ether1          D    164    100    0
00:a0:c9:13:f3:37 10 wlan1           D    164    100    0
00:a0:c9:f0:20:e9 20 ether2          D    196    50    0
00:b0:d0:6f:94:78 20 wlan2           D    196    50    0
00:16:01:42:1a:1a 50 wlan3           A    infinity 120    0
00:0c:6e:63:25:77 100 wlan5           S    infinity 200    0
```

- 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
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
A 動的学習テーブル (認証成功端末)
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
- 動的学習テーブル (認証成功端末)
- 動的学習テーブル (無線 LAN 端末)

6) 学習エントリヒット数

このエントリがヒットした回数が表示されます。

7) 破棄数

このエントリで破棄された回数が表示されます。

学習テーブルの割り当て状況を表示する場合

```
#show bridge summary
Registered station blocks :    6      ---(1)
  Dynamic entry           :    4      ---(2)
  Static entry            :    1      ---(3)
  Authenticated entry     :    1      ---(4)
  System entry            :    0      ---(5)
Free station blocks       : 3994     ---(6)
```

- 1) 使用中の学習テーブル数
- 2) 動的学習による学習テーブル数
- 3) 静的学習による学習テーブル数
- 4) 動的学習による学習テーブル数 (認証成功端末)
- 5) 装置内部使用による学習テーブル数
- 6) 未使用の学習テーブル数

29.2 ブリッジのカウンタ・ログ・統計・状態などのクリア

29.2.1 clear bridge

[機能]

動的に学習したテーブルの初期化

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
clear bridge
clear bridge vlan <vid>
clear bridge mac <macaddr> <vid>
```

[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 <vid>

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。
SR-M20AC2/20AC1 では指定できません。

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

mac <macaddr> <vid>

指定された VLAN で学習されている指定された MAC アドレスを学習テーブルから削除します。
vid は、SR-M20AC2/20AC1 では指定できません。

- MAC アドレス
学習テーブルから削除する 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。)
- 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。

[注意]

以下のアドレスは削除されません。

- vlan forward コマンド定義によって静的に登録されたアドレス
- 認証成功端末のアドレス
- 無線 LAN 端末のアドレス

[実行例]

```
# clear bridge  
#
```

第 30 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

30.1 VLAN のカウンタ・ログ・統計・状態などの表示

30.1.1 show vlan

[機能]

VLAN 設定情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。
SR-M20AC2/20AC1 では指定できません。

- 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]

SR-M20AP2/20AP1 の実行例

```
# 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)

#
```

SR-M20AC2/20AC1 の実行例

```
# show vlan

VID  Interface      Tag           Type      Description
-----
(1) (2)            (3)          (4)      (5)
1   ether1         untagged     port      default
    wlan1         untagged

Total Count : 1      ---(6)

#
```

- 1) VLAN 番号
- 2) インタフェース
 - ether** - ether 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
- 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
SR-M20AP2/20AP1 の実行例

```
# 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
SR-M20AP2/20AP1 の実行例

```
# show vlan vid 100
```

VID	Interface	Tag	Type	Description
(1)	(2)	(3)	(4)	(5)
100	ether1	dot1q-tagged	port	v100
	wlan15	untagged		
	wlan16	untagged		

```
#
```

30.2 VLAN フィルタのカウンタ・ログ・統計・状態などの表示、クリア

30.2.1 show vlan filter

[機能]

フィルタテーブル表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
show vlan filter [vid <vlan_id>] [all]
```

[オプション]

なし

すべての VLAN のフィルタテーブルを表示します。

vid <vlan_id>

指定した VLAN のフィルタテーブルを表示します。
SR-M20AC2/20AC1 では指定できません。

all

時間切れのフィルタテーブルを含めて表示します。

[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]

フィルタテーブルを表示します。

[実行例]

```
# show vlan filter
[VLAN1]---(1)
default: spi---(2)

static table: 3---(3)
      action acl_count
[ 0] reject          0
[ 1] reject          1
[ 2] reject          2
(4)      (5)          (6)

dynamic table: 4---(7)
      action src(dst) IP/mask:port          proto SYN remain
      dst(src) IP/mask:port
[ 0]   pass 172.16.1.81/32:54299            6   Y   22
      172.16.1.104/32:any
[ 1]   pass 172.16.1.81/32:58456            6   Y   21
      172.16.1.104/32:any
[ 2]   pass 172.16.1.81/32:61220            6   Y   20
      172.16.1.104/32:any
[ 3]   pass 172.16.1.81/32:65412            6   Y   18
      172.16.1.104/32:any
(8)

SPI table: 4---(9)
      action src(dst) IP/mask:port          proto SYN remain
      dst(src) IP/mask:port
[ 0]   pass 172.16.1.104/32:any             1   -   24
      172.16.1.81/32:any
[ 1]   pass 172.16.1.104/32:138            17  -   23
      172.16.1.255/32:138
[ 2]   pass 172.16.1.104/32:137            17  -   23
      172.16.1.255/32:137
[ 3]   pass 172.16.1.104/32:62284           6   -   22
      172.16.1.81/32:21
```

- 1) VLAN 名
- 2) どのフィルタテーブルにも不一致時の動作
- 3) 静的フィルタテーブル数
- 4) フィルタ通番
- 5) フィルタ動作
- 6) ACL 番号
- 7) 動的フィルタテーブル数
- 8) フィルタテーブルタイマ [*10 秒]
オプションに all を指定した場合は時間切れのテーブルに関しては expire と表示されます。
- 9) SPI フィルタテーブル数

30.2.2 show vlan filter statistics

[機能]

フィルタの統計情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show vlan filter statistics [vid <vlan_id>]

[オプション]

なし

すべての VLAN のフィルタ統計情報を表示します。

vid <vlan_id>

指定した VLAN の統計情報を表示します。

SR-M20AC2/20AC1 では指定できません。

[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]

フィルタの統計情報を表示します。

[実行例]

```
# show vlan filter statistics
[VLAN1]---(1)
packet
pass(static)          12---(2)
pass(dynamic)        40---(3)
pass(SPI)            72---(4)
reject                13---(5)
total                 137---(6)
```

- 1) VLAN 名
- 2) 静的フィルタで透過したパケット数
- 3) 動的フィルタで透過したパケット数
- 4) SPI フィルタで透過したパケット数
- 5) 遮断したパケット数
- 6) 処理したパケット数

30.2.3 show vlan filter summary

[機能]

フィルタのフィルタテーブル数の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show vlan filter summary [vid <vlan_id>] [total] [all]

[オプション]

なし

すべての VLAN のフィルタテーブル数を表示します。

vid <vlan_id>

指定した VLAN のフィルタテーブル数を表示します。
SR-M20AC2/20AC1 では指定できません。

total

装置全体のフィルタテーブル数を表示します。

all

時間切れのフィルタテーブルを含めたフィルタテーブル数を表示します。

[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]

フィルタのフィルタテーブル数を表示します。

[実行例]

```
# show vlan filter summary
[VLAN1]---(1)
  static table           3---(2)
  dynamic table         4---(3)
  SPI table              4---(4)
```

- 1) VLAN 名
- 2) 静的フィルタテーブル数
- 3) 動的フィルタテーブル数
- 4) SPI フィルタテーブル数

30.2.4 clear vlan filter statistics

[機能]

フィルタの統計情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

clear vlan filter 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]

フィルタ統計情報をクリアします。

[実行例]

```
# clear vlan filter statistics  
#
```

30.3 IDS のカウンタ・ログ・統計・状態などの表示、クリア

30.3.1 show vlan ids statistics

[機能]

IDS の統計情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show vlan ids statistics [vid <vlan_id>]

[オプション]

なし

すべての VLAN の IDS 統計情報を表示します。

vid <vlan_id>

指定した VLAN の統計情報を表示します。

SR-M20AC2/20AC1 では指定できません。

[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]

IDS の統計情報を表示します。

[実行例]

```
# show vlan ids statistics
[VLAN1]---(1)
IPv4 IDS
event
Unknown IP protocol          4 ---(2)
Land attack                   0 ---(3)
Short IP header               1 ---(4)
Malformed IP packet          0 ---(5)
IP option
Malformed IP option           3 ---(6)
Security IP option            0 ---(7)
Loose routing IP option       0 ---(8)
Record route IP option        0 ---(9)
Stream ID IP option           0 ---(10)
Strict routing IP option      0 ---(11)
Timestamp IP option           0 ---(12)
ICMP
ICMP source quench            0 ---(13)
ICMP timestamp request        0 ---(14)
ICMP timestamp reply          0 ---(15)
ICMP information request      0 ---(16)
ICMP information reply        0 ---(17)
ICMP address mask request     0 ---(18)
ICMP address mask reply       0 ---(19)
UDP
UDP short header              2 ---(20)
UDP bomb                       0 ---(21)
TCP
TCP no bits set                1 ---(22)
TCP SYN and FIN                0 ---(23)
TCP FIN and no ACK             3 ---(24)
FTP
FTP improper port              0 ---(25)
```

- 1) VLAN 名
- 2) Protocol フィールドが 134 以上のとき
- 3) 始点 IP アドレスと終点 IP アドレスが同じとき
- 4) IP ヘッダの長さが length フィールドの長さよりも短いとき
- 5) length フィールドと実際のパケットの長さが違うとき
- 6) オプションヘッダの構造が不正であるとき
- 7) Security and handling restriction header を受信したとき
- 8) Loose source routing header を受信したとき
- 9) Record route header を受信したとき
- 10) Stream identifier header を受信したとき
- 11) Strict source routing header を受信したとき
- 12) Internet timestamp header を受信したとき
- 13) source quench を受信したとき
- 14) timestamp request を受信したとき
- 15) timestamp reply を受信したとき
- 16) information request を受信したとき
- 17) information reply を受信したとき
- 18) address mask request を受信したとき
- 19) address mask reply を受信したとき

-
- 20) UDP の length フィールドの値が 8 よりも小さいとき
 - 21) UDP ヘッダの length フィールドの値が大き過ぎるとき
 - 22) フラグに何もセットされていないとき
 - 23) SYN と FIN が同時にセットされているとき
 - 24) ACK のない FIN を受信したとき
 - 25) PORT や PASV コマンドで指定されるポート番号が 1024 ~ 65535 の範囲でないとき

30.3.2 clear vlan ids statistics

[機能]

IDS の統計情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

clear vlan ids 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]

IDS 統計情報をクリアします。

[実行例]

```
# clear vlan ids statistics
#
```

第 31 章 SSH のカウンタ・ログ・統計・状態 などの表示コマンド

31.1 SSH のカウンタ・ログ・統計・状態などの表示

31.1.1 show ssh server key

[機能]

SSH ホスト 認証用公開鍵の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show ssh server key {dsa|rsa}

[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。

[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 コマンドおよび serverinfo sftp 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
i8JWtZhrglDtxVVmBAIAB3Nc3MAAAAkGfA0nu7HMPdQAAAIA4sIwVzNfTpxNt jJ
QxlgJHrDjybKeBMmpnJ/RtGTJfvZW5T/aDc/aoB7PdF+appeXx9U8FsQF+EaMNFq
P3lK2u3XAEoAzLa0JQC06VjoDQh15YIzKFo2AVaK4lCeS3q81q8A4+jttJ0Dt0U0
rVucQo0q+BdIgaCMDuaqmJQAotGvZvZQ/RMTSh6pMh+z9DdB1DLnPNxEyt61Sftz
Vk+rjgZ29In2V7ai4yuOfIhNL6lybOrrfoZ9YQW4P9rJuDxhvn2xvZQ/RMTSh6pM
6WIwA9mlzAst/YBxbb9Jc07uPVhN8M624q8yKsQaMClWlAAAW00+ZkaqccWLy9GU
xPksjfc+N7022akmykT8V6iMh4+7iAIBJYE6pWpsQU5nFP9rJuDx5R/QV4Q177od
96vNtqgw/hSseRFjyqrGxKewMbl1FNjzWSAUyzW0p+GLR/mqBCFavMRl4toxEsp3
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 AA94UAATdVfYAAxsAArx3AAIF7QAsTsTwAEeKogAFAlNoAA00AAAAj3F
AAD3ClYc2EAAAABiWAAAHsMXKAAB+shGQAHdMIABBSpjAARVYAAERAAJZ/IAAAAB
0AB9QAB+2kSY6AAUygcCvAAB3NzaA7wtAAJ/kAADRQgABwmQATHHAAUtOySgAEJ
JMBAAx4= root@localhost --- (1)
#
```

1) 本装置のホスト認証用 RSA 公開鍵

第 32 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

32.1 認証成功端末情報のカウンタ・ログ・統計・状態などの表示

32.1.1 show auth port

[機能]

認証成功端末情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show auth port [<kind> [<portlist>]]

[オプション]

なし

すべてのインタフェースの認証状態を表示します。

<kind>

ポート種別を指定します。

- ether
ether ポート
SR-M20AP2/20AP1 の場合、指定できません。
- wlan
無線 LAN インタフェース
SR-M20AC2/20AC1 の場合、指定できません。

<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 (IEEE802.1X 認証、MAC アドレス認証) での認証成功端末情報を表示します。

[実行例]

SR-M20AP2/20AP1 の場合

```
# show auth port

[wlan]
Port  Mode  MAC Address          Function  VLAN
-----
(1)  (2)   (3)                 (4)      (5)
1     mac   00:13:21:f6:10:11   dot1x    10
2     mac   00:13:21:f6:11:22   dot1x    20
      00:13:21:f6:12:33   dot1x    100
9     mac   00:13:21:f6:13:44   macauth  10
      dot1x
10    -     -                   -        -
#
```

SR-M20AC2/20AC1 の場合

```
# show auth port

[ether]
Port  Mode  MAC Address          Function  VLAN
-----
1     mac   00:13:21:f6:01:11   macauth  1
2     mac   00:13:21:f6:02:22   dot1x    1
#
```

- 1) インタフェース番号
- 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) 認証成功した機能

dot1x IEEE802.1X 認証

macauth MAC アドレス認証

- 5) VLAN ID

認証成功端末が存在しないインタフェースは、インタフェース番号以外の項目が "-" で表示されます。

32.2 IEEE802.1X 認証のカウンタ・ログ・統計・状態などの表示

32.2.1 show dot1x port

[機能]

IEEE802.1X 認証状態の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

- ether
ether ポート
SR-M20AP2/20AP1 の場合、指定できません。
- wlan
無線 LAN インタフェース
SR-M20AC2/20AC1 の場合、指定できません。

<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]

SR-M20AP2/20AP1 の場合

```
# 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          Since
      (9)                   (10)
-----
  1   user01  TTLS      Authenticated   2          2          S4      1
      00:0e:13:25:0f:11    Mon Mar 16 11:30:17 2009
      user02  PEAP      Authenticated   2          2          S4      1
      00:a1:fd:dd:fc:ed    Mon Mar 16 13:10:04 2009
  2   admin  TLS       Authenticated   2          0          S4      1
      00:0e:13:8e:55:22    Mon Mar 16 15:32:12 2009
  3   user   PEAP      Authenticated   1          0          S4      1
      00:a0:12:d4:ef:ac    Mon Mar 16 18:02:11 2009
  4   -      -         -               0          0          S0      0
      00:00:00:00:00:00    -
```

SR-M20AC2/20AC1 の場合

```
# show dot1x port

[ether]
Port  User      EAP-Type  Authentication  OK times  NG times  Status  VLAN
      MAC address          Since
-----
  1   user01  TTLS      Authenticated   2          2          S4      1
      00:0e:13:25:0f:01    Mon Mar 16 19:29:17 2009
  2   admin  TLS       Authenticated   2          0          S4      1
      00:0e:13:8e:55:02    Mon Mar 16 16:32:12 2009
```

- 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。

32.2.2 show dot1x statistics port

[機能]

IEEE802.1X 認証統計情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

- ether
ether ポート
SR-M20AP2/20AP1 の場合、指定できません。
- wlan
無線 LAN インタフェース
SR-M20AC2/20AC1 の場合、指定できません。

<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]

SR-M20AP2/20AP1 の場合

```
# 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)
```

SR-M20AC2/20AC1 の場合

```
# show dot1x statistics port
[ether]
Port 1 statistics:
      EAPOL frame received count : 0
      EAPOL frame sent count : 0
      EAPOL Start frame received count : 0
      EAPOL Logoff frame received count : 0
      EAP Identity Response received count : 0
      EAP response received count : 0
      EAP Identity Request sent count : 1
      EAP request sent count : 0
      Invalid EAPOL frame received count : 0
      EAP with illegal length frame received count : 0
      Version of EAPOL last received frame : 0
      Supplicant address of last received frame : 00:00:00:00:00:00
```

- 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

32.2.3 show dot1x backup port

[機能]

認証自動切替状態の表示

[適用機種]

SR-M20AP2 SR-M20AP1

[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
wlan3  master 1         dead          standby
wlan2  backup
wlan7  backup
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

32.3 IEEE802.1X 認証のカウンタ・ログ・統計などのクリア

32.3.1 clear dot1x statistics

[機能]

IEEE802.1X 認証統計情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
#
```

32.4 MAC アドレス認証のカウンタ・ログ・統計・状態などの表示

32.4.1 show macauth port

[機能]

MAC アドレス認証状態の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

- ether
ether ポート
SR-M20AP2/20AP1 の場合、指定できません。
- wlan
無線 LAN インタフェース
SR-M20AC2/20AC1 の場合、指定できません。

<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]

SR-M20AP2/20AP1 の場合

```
# 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 2009
2     mac   00:13:21:f6:02:23   success 20    Mar 24 10:00:22 2009
      00:13:21:f6:02:43   failure -     Mar 24 10:19:46 2009
6     mac   00:13:21:f6:06:33   permanent 20    Mar 24 10:00:12 2009
10    mac   -                   idle    -     -
      00:13:21:f6:0a:73   failure -     Mar 24 12:11:00 2009
      00:13:21:f6:0a:74   failure -     Mar 24 12:11:01 2009

#
```

SR-M20AC2/20AC1 の場合

```
# show macauth port

[ether]
Port  Mode  MAC Address          Status  VLAN  Since
-----
1     mac   00:13:22:f6:01:13   success 1     Mar 24 10:20:19 2009
      00:13:22:f6:01:43   failure -     Mar 24 10:21:34 2009

#
```

- 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
 - permanent**
 - 認証不要端末
 - 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

32.4.2 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

- ether
ether ポート
SR-M20AP2/20AP1 の場合、指定できません。
- wlan
無線 LAN インタフェース
SR-M20AC2/20AC1 の場合、指定できません。

<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]

SR-M20AC2/20AC1 の場合

```
# show macauth statistics
ether 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)

32.5 MAC アドレス認証のカウンタ・ログ・統計などのクリア

32.5.1 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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
#
```

32.6 Wake On LAN パケットの統計情報の表示

32.6.1 show wol statistics

[機能]

Wake On LAN パケットの統計情報表示

[適用機種]

 SR-M20AC2 SR-M20AC1

[入力形式]

show wol 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]

各認証機能 (IEEE802.1X 認証、MAC アドレス認証) で Wake On LAN パケット転送機能が有効なポートの Wake On LAN パケット統計情報を表示します。

[注意]

本コマンドで表示されるのは、Wake On LAN パケット転送機能により転送された Wake On LAN パケットの統計情報です。ブリッジにより、Wake On LAN パケットが転送された場合は、統計情報にカウントされません。

[実行例]

```
# show wol statistics

receive count      : 1                (1)
[ether 1]
  forward count    : 1                (3)
  drop count       : 0                (4)
```

- 1) 本装置が Wake On LAN パケットを受信した回数
- 2) 転送先ポート名
- 3) 転送成功回数
- 4) 転送失敗回数

32.7 Wake On LAN パケットの統計情報のクリア

32.7.1 clear wol statistics

[機能]

Wake On LAN パケットの統計情報クリア

[適用機種]

 SR-M20AC2 SR-M20AC1

[入力形式]

clear wol statistics

[オプション]

なし

すべてのポートの Wake On LAN パケット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]

Wake On LAN パケットの統計情報をクリアします。

[実行例]

```
# clear wol statistics
#
```

第 33 章 AAA 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 AAA のカウンタ・ログ・統計・状態などの表示

33.1.1 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-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 アカウンティングサーバ

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。

33.1.2 show aaa radius client statistics

[機能]

RADIUS クライアント機能の統計情報表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

```
show aaa radius client statistics [group <group_id> [{auth | accounting} [<number>]]]
```

[オプション]

なし

AAA グループすべての統計情報を表示します。

group <group_id>

指定したグループに関する統計情報を表示します。

group <group_id> auth

指定したグループの認証に関する統計情報を表示します。

group <group_id> auth <number>

指定したグループの指定した認証定義番号に関する統計情報を表示します。

group <group_id> accounting

指定したグループのアカウントリングに関する統計情報を表示します。

group <group_id> accounting <number>

指定したグループの指定したアカウントリング定義番号に関する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]

RADIUS クライアントの統計情報を表示します。

[実行例]

```

# show aaa radius client statistics
aaa 0 auth 0 statistics information:
    100 Round Trip Time(ms)          ---(1)
     2 Access Requests               ---(2)
     0 Access Retransmissions        ---(3)
     1 Access Accepts                ---(4)
     0 Access Rejects               ---(5)
     0 Access Challenges             ---(6)
     0 Malformed Access Responses    ---(7)
     0 Bad Authenticators            ---(8)
     0 Pending Requests              ---(9)
     0 Timeouts                      ---(10)
     0 Unknown Types                 ---(11)
     0 Packets Dropped               ---(12)
aaa 0 accounting 0 statistics information:
    100 Round Trip Time(ms)          ---(13)
     1 Requests                      ---(14)
     0 Retransmissions               ---(15)
     1 Responses                     ---(16)
     0 Malformed Responses           ---(17)
     0 Bad Authenticators            ---(18)
     0 Pending Requests              ---(19)
     0 Timeouts                      ---(20)
     0 Unknown Types                 ---(21)
     0 Packets Dropped               ---(22)

```

- 1) 認証サーバの RTT 値
- 2) Access-Request 送信数
- 3) Access-Request 再送数
- 4) Access-Accept 受信数
- 5) Access-Rejects 受信数
- 6) Access-Challenges 受信数
- 7) 異常な Access-Responses 受信数
- 8) 不正な Authenticator 受信数
- 9) 応答を受信していないパケット数
- 10) タイムアウトになった回数
- 11) パケットの種別を特定できなかった回数
- 12) 破棄されたパケット数
- 13) アカウンティングサーバの RTT 値
- 14) Accounting-Request 送信数
- 15) Accounting-Request 再送数
- 16) Accounting-Response 受信数
- 17) 異常な Accounting-Response 受信数
- 18) 不正な Authenticator 受信数
- 19) 応答を受信していないパケット数
- 20) タイムアウトになった回数
- 21) パケットの種別を特定できなかった回数
- 22) 破棄されたパケット数

33.2 AAA のカウンタ・ログ・統計などのクリア

33.2.1 clear aaa radius client statistics

[機能]

RADIUS クライアント機能の統計情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

```
clear aaa radius client statistics [group <group_id> [{auth|accounting} [<number>]]]
```

[オプション]

なし

AAA グループすべての統計情報をクリアします。

group <group_id>

指定したグループに関する統計情報をクリアします。

group <group_id> auth

指定したグループの認証に関する統計情報をクリアします。

group <group_id> auth <number>

指定したグループの指定した認証定義番号に関する統計情報をクリアします。

group <group_id> accounting

指定したグループのアカウントリングに関する統計情報をクリアします。

group <group_id> accounting <number>

指定したグループの指定したアカウントリング定義番号に関する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]

RADIUS クライアントの統計情報をクリアします。

[実行例]

```
# clear aaa radius client statistics  
#
```

第 34 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

34.1 NETTIME(time/sntp) 統計情報の表示

34.1.1 show nettime statistics

[機能]

NETTIME(time/sntp) 機能での統計情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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>

稼働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、本装置で稼働しているすべての 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
[time udp]
    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

34.2 NETTIME(time/sntp) 統計情報のクリア

34.2.1 clear nettime statistics

[機能]

NETTIME(time/sntp) 統計情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 35 章 ProxyARP 情報の表示、クリア操作 コマンド

35.1 ProxyARP 情報の表示

35.1.1 show proxyarp

[機能]

ProxyARP 情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show proxyarp

[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]

ProxyARP の動作状態を表示します。

[実行例]

```
# show proxyarp
ProxyARP : enabled          ---(1)

IP Address      MAC Address      Port
-----
(2)             (3)             (4)
192.168.1.200   00:23:26:6e:0c:f8 wlan2
192.168.1.100   00:23:e3:96:f0:3f wlan1
```

1) ProxyARP 動作状態

enabled : ProxyARP が動作しています。

enabled(unicast reject)

: ProxyARP が動作していますが、ユニキャスト ARP 要求は無線 LAN 側へ転送しません。

disabled

: ProxyARP は動作していません。

2) 無線 LAN 端末の IP アドレス

3) 無線 LAN 端末の MAC アドレス

4) 無線 LAN 端末が存在する無線 LAN インタフェース

35.1.2 show proxyarp statistics

[機能]

ProxyARP の統計情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show proxyarp 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]

ProxyARP 動作時の統計情報を表示します。

[実行例]

```
# show proxyarp statistics
action                count
-----
reply                  5          ---(1)
forward                268       ---(2)
discard                0          ---(3)
```

- 1) ProxyARP 応答数
- 2) 無線 LAN インタフェース側へ転送対象となった ARP 要求数
- 3) 破棄した ARP 要求数

35.2 ProxyARP 統計情報のクリア

35.2.1 clear proxyarp statistics

[機能]

ProxyARP の統計情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

clear proxyarp 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]

ProxyARP の統計情報をクリアします。

[実行例]

```
# clear proxyarp statistics
```

第 36 章 **SNMP** 統計情報の表示、クリア操作コマンド

36.1 SNMP 統計情報の表示

36.1.1 show snmp statistics

[機能]

SNMP 機能での統計情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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

36.2 SNMP 統計などのクリア

36.2.1 clear snmp statistics

[機能]

SNMP 統計情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 37 章 ソケット 状態の表示コマンド

37.1 ソケット状態の表示

37.1.1 show socket

[機能]

ソケット状態の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

(続き)

```

udp      0      0 127.0.0.1.2645      *.*
udp      0      0 *.67                *.*
udp      0      0 *.53                *.*
udp      0      0 *.67                *.*
udp      0      0 127.0.0.1.52000     *.*
udp      0      0 *.67                *.*
udp      0      0 *.67                *.*
udp      0      0 127.0.0.1.2642     *.*
udp      0      0 *.37                *.*
udp      0      0 *.67                *.*
udp      0      0 127.0.0.1.2639     *.*
udp      0      0 127.0.0.1.2638     *.*
udp      0      0 127.0.0.1.161      *.*
udp      0      0 127.0.0.1.8900     *.*
udp      0      0 127.0.0.1.2631     *.*
udp      0      0 *.123               *.*
udp      0      0 *.67                *.*
udp      0      0 127.0.0.1.2633     *.*
udp      0      0 127.0.0.1.2632     *.*
udp      0      0 127.0.0.1.2634     *.*
udp      0      0 127.0.0.1.2635     *.*
udp      0      0 127.0.0.1.2637     *.*
udp      0      0 *.500               *.*
udp      0      0 127.0.0.1.2628     *.*
udp      0      0 127.0.0.1.2629     *.*
udp      0      0 127.0.0.1.2621     *.*
udp      0      0 127.0.0.1.2623     *.*
udp      0      0 127.0.0.1.2627     *.*
udp      0      0 127.0.0.1.2624     *.*
udp      0      0 127.0.0.1.2625     *.*
udp      0      0 127.0.0.1.2622     *.*
#

```

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 38 章 トレースの表示、クリア操作コマンド

38.1 トレースの表示

38.1.1 show trace ssh

[機能]

SSH サーバ機能のトレース情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

show trace ssh

[オプション]

なし

[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]

SSH サーバ機能のトレース情報を表示します。

[注意]

SSH サーバ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。

[実行例]

```
# show trace ssh
[1] sshd Thu Sep 30 14:34:37 2004
-----
(1) (2) (3)
      This platform does not support both privilege separation and
      -----
                                     (4)
compression
-----
(4)
[2] sshd Thu Sep 30 14:34:37 2004
      Compression disabled
[3] sshd Thu Sep 30 14:34:37 2004
      infol: sshd version OpenSSH_3.9p1
[4] sshd Thu Sep 30 14:34:37 2004
      infol: private host key: #0 type 0 RSA1
[5] sshd Thu Sep 30 14:34:37 2004
      infol: read PEM private key done: type RSA
[6] sshd Thu Sep 30 14:34:37 2004
      infol: private host key: #1 type 1 RSA
[7] sshd Thu Sep 30 14:34:37 2004
      infol: read PEM private key done: type DSA
[8] sshd Thu Sep 30 14:34:37 2004
      infol: private host key: #2 type 2 DSA
[9] sshd Thu Sep 30 14:34:37 2004
      infol: Bind to port 22 on 0.0.0.0.
[10] sshd Thu Sep 30 14:34:37 2004
      Server listening on 0.0.0.0 port 22.
[11] sshd Thu Sep 30 14:34:37 2004
      infol: Bind to port 22 on ::.
[12] sshd Thu Sep 30 14:34:37 2004
      Server listening on :: port 22.
[13] sshd Thu Sep 30 14:34:37 2004
      Generating 768 bit RSA key.
[14] sshd Thu Sep 30 14:34:38 2004
      RSA key generation complete.
```

- 1) トレース番号
トレース番号が表示されます。
- 2) スレッド名
スレッド名が表示されます。
- 3) トレース採取時間
トレース採取時間が表示されます。
- 4) トレース内容
トレースの内容が表示されます。

38.2 トレースのクリア

38.2.1 clear trace ssh

[機能]

SSH サーバ機能トレース情報のクリア

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

clear trace ssh

[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]

SSH サーバ機能のトレース情報をクリアします。

[注意]

SSH サーバ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。

[実行例]

```
# clear trace ssh  
#
```


第 39 章 証明書関連の表示コマンド

39.1 証明書関連の表示

39.1.1 show crypto certificate

[機能]

証明書情報の表示

[適用機種]



[入力形式]

show crypto certificate [base64] [candidate]

[オプション]

なし

動作中のすべての証明書情報 (証明書要求、自装置証明書、認証局証明書) を表示します。

base64

Base64 形式で証明書情報 (証明書要求、自装置証明書) を表示する場合に指定します。

candidate

編集中の構成定義から証明書情報を表示する場合に指定します。

[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/CE クラス)

構成定義モード (管理者クラス)

[説明]

証明書に関する情報を表示します。

[注意]

証明書によっては [実行例] と異なる表示が行われることがあります。

[実行例]

(1) オプションなし

```
# show crypto certificate
[Certificate Request]
[1] Number : 0
    Version : 0
    Subject : C=JP, ST=Kanagawa, L=Kawasaki,
             O=Fujitsu Limited, OU=Tech Div.,
             CN=shisya.fujitsu.com, emailAddress=hoge@fujitsu.com
    Subject Public Key Info:
        Public Key Algorithm : rsaEncryption
        RSA Public Key : (1024 bit)
    Requested Extensions:
        X509v3 Key Usage:
            Digital Signature, Certificate Sign
        Signature Algorithm : sha1WithRSAEncryption

[Local Certificate]
[1] Number : 0, Name : mycert
    Version : 1
    Serial Number : 1 (0x1)
    Signature Algorithm : sha1WithRSAEncryption
    Issuer : C=JP, ST=Kanagawa, L=Kawasaki,
            O=Fujitsu Limited, OU=Tech Div.,
            CN=shisya.fujitsu.com, emailAddress=hoge@fujitsu.com
    Validity
        Not Before: Fri Jul 20 11:07:58 2007
        Not After : Mon Dec 31 11:07:58 2007
    Subject : C=JP, ST=Kanagawa, L=Kawasaki,
             O=Fujitsu Limited, OU=Tech Div.,
             CN=shisya.fujitsu.com, emailAddress=hoge@fujitsu.com
    Subject Public Key Info:
        Public Key Algorithm : rsaEncryption
        RSA Public Key : (1024 bit)
    X509v3 extensions:
        X509v3 Key Usage:
            Digital Signature, Certificate Sign
        X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:1
    Signature Algorithm : sha1WithRSAEncryption
    5c:3c:df:94:6f:35:ce:55:83:78:45:9e:b3:71:ba:67:ed:80:
    b0:bf:fc:bb:a1:24:79:a6:94:dc:65:99:55:0a:05:8d:60:54:
    08:cf:5f:cc:08:db:f5:c8:69:3d:6a:df:12:3a:54:20:33:9c:
    e2:d1:b5:f2:a4:3d:29:d4:e0:77:52:cb:74:9b:31:b1:de:2d:
    e3:b1:5b:8a:24:a6:e7:d2:ab:32:b1:46:50:12:93:05:4b:b2:
    5d:60:7b:88:44:de:67:58:f0:63:a8:7e:bc:0a:a4:03:f3:33:
    de:27:69:55:73:07:2c:52:88:45:14:a0:3c:9a:bf:66:b0:48:
    95:35

[CA Certificate]
[1] Number : 0, Name : cacert
    Version : 3
    Serial Number: 0
    Signature Algorithm : md5WithRSAEncryption
    Issuer : C=JP, ST=Kanagawa, L=kawasaki,
            O=Fujitsu Limited
            OU=Tech Div.,
            CN=honsya.fujitsu.com,
            emailAddress=hoge@fujitsu.com
    Validity
        Not Before: Jan 4 07:50:53 2006
        Not After : Feb 3 07:50:53 2006
    Subject : C=JP, ST=Kanagawa, L=kawasaki,
             O=Fujitsu Limited
             OU=Tech Div.,
             CN=honsya.fujitsu.com,
             emailAddress=hoge@fujitsu.com
    Subject Public Key Info:
        Public Key Algorithm : rsaEncryption
        RSA Public Key : (1024 bit)
```

(続く)

(続き)

```
Signature Algorithm : md5WithRSAEncryption
c2:9b:e5:cb:f0:24:e9:dd:6f:32:07:6d:70:86:18:e5:2d:78:
8d:02:9d:da:d9:c1:f4:2b:47:cf:e6:f2:1b:89:7b:e4:88:2a:
87:6b:85:c5:92:29:6d:8b:92:1a:f5:4e:4b:ec:c8:97:5c:a2:
21:e9:71:33:9a:7b:40:f5:2c:fc:10:16:53:57:8f:52:6a:cb:
ad:ab:1e:b4:46:e0:20:55:f4:a5:7c:a5:58:5f:02:6d:6d:3c:
1f:d4:8c:20:37:e4:77:a7:62:9d:dc:69:90:0d:d5:99:59:4f:
40:a4:b0:0a:46:80:17:69:00:f8:b0:1a:a3:42:1a:b2:c9:23:
9b:4e
```

#

(2) 編集中の構成定義からすべての証明書情報(証明書要求、自装置証明書)を表示

```
# show crypto certificate candidate
[Certificate Request]
[1] Number : 0
    Version : 0
    Subject : C=JP, ST=Kanagawa, L=Kawasaki,
             O=Fujitsu Limited, OU=Tech Div.,
             CN=shisya.fujitsu.com, emailAddress=hoge@fujitsu.com
    Subject Public Key Info:
        Public Key Algorithm : rsaEncryption
        RSA Public Key : (1024 bit)
    Requested Extensions:
        X509v3 Key Usage:
            Digital Signature, Certificate Sign
    Signature Algorithm : sha1WithRSAEncryption

[Local Certificate]
[1] Number : 0, Name : mycert
    Version : 1
    Serial Number : 1 (0x1)
    Signature Algorithm : sha1WithRSAEncryption
    Issuer : C=JP, ST=Kanagawa, L=Kawasaki,
            O=Fujitsu Limited, OU=Tech Div.,
            CN=shisya.fujitsu.com, emailAddress=hoge@fujitsu.com
    Validity
        Not Before: Fri Jul 20 11:07:58 2007
        Not After : Mon Dec 31 11:07:58 2007
    Subject : C=JP, ST=Kanagawa, L=Kawasaki,
            O=Fujitsu Limited, OU=Tech Div.,
            CN=shisya.fujitsu.com, emailAddress=hoge@fujitsu.com
    Subject Public Key Info:
        Public Key Algorithm : rsaEncryption
        RSA Public Key : (1024 bit)
    X509v3 extensions:
        X509v3 Key Usage:
            Digital Signature, Certificate Sign
        X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:1
    Signature Algorithm : sha1WithRSAEncryption
    5c:3c:df:94:6f:35:ce:55:83:78:45:9e:b3:71:ba:67:ed:80:
    b0:bf:fc:bb:a1:24:79:a6:94:dc:65:99:55:0a:05:8d:60:54:
    08:cf:5f:cc:08:db:f5:c8:69:3d:6a:df:12:3a:54:20:33:9c:
    e2:d1:b5:f2:a4:3d:29:d4:e0:77:52:cb:74:9b:31:b1:de:2d:
    e3:b1:5b:8a:24:a6:e7:d2:ab:32:b1:46:50:12:93:05:4b:b2:
    5d:60:7b:88:44:de:67:58:f0:63:a8:7e:bc:0a:a4:03:f3:33:
    de:27:69:55:73:07:2c:52:88:45:14:a0:3c:9a:bf:66:b0:48:
    95:35

[CA Certificate]
[1] Number : 0, Name : cacert
    Version : 3
    Serial Number: 0
    Signature Algorithm : md5WithRSAEncryption
    Issuer : C=JP, ST=Kanagawa, L=kawasaki,
            O=Fujitsu Limited
            OU=Tech Div.,
            CN=honsya.fujitsu.com,
            emailAddress=hoge@fujitsu.com
```

(続く)

(続き)

```

Validity
  Not Before: Jan 4 07:50:53 2006
  Not After : Feb 3 07:50:53 2006
Subject : C=JP, ST=Kanagawa, L=kawasaki,
         O=Fujitsu Limited
         OU=Tech Div.,
         CN=honsya.fujitsu.com,
         emailAddress=hoge@fujitsu.com
Subject Public Key Info:
  Public Key Algorithm : rsaEncryption
  RSA Public Key : (1024 bit)
Signature Algorithm : md5WithRSAEncryption
c2:9b:e5:cb:f0:24:e9:dd:6f:32:07:6d:70:86:18:e5:2d:78:
8d:02:9d:da:d9:c1:f4:2b:47:cf:e6:f2:1b:89:7b:e4:88:2a:
87:6b:85:c5:92:29:6d:8b:92:1a:f5:4e:4b:ec:c8:97:5c:a2:
21:e9:71:33:9a:7b:40:f5:2c:fc:10:16:53:57:8f:52:6a:cb:
ad:ab:1e:b4:46:e0:20:55:f4:a5:7c:a5:58:5f:02:6d:6d:3c:
1f:d4:8c:20:37:e4:77:a7:62:9d:dc:69:90:0d:d5:99:59:4f:
40:a4:b0:0a:46:80:17:69:00:f8:b0:1a:a3:42:1a:b2:c9:23:
9b:4e

```

#

(3) base64 オプションを指定して動作中の証明書情報 (証明書要求、自装置証明書) を表示

```

# show crypto certificate base64
[Certificate Request]
[1] Number : 0
-----BEGIN CERTIFICATE REQUEST-----
MIICMDCAZkCAQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYDVQKIWhwLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTGltaxRlZDESMBAG
A1UECxMjVGVjaCBEaXYuMRswGQYDVQDEExJzaGlzeWUuZnVqaXRzdS5jb20xHZA
BgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAMk7Bq9Ciaxhl7fYIkwbRLI64EAjP1RnDrEnLJ/ds9ErIoT4sPBC
Z9a0mvdz0nRlK8HmNmDGMo1DRufBWueSvs9Qgl0zykQu+R3YKPMNMJ3gL06tiNk1
6TtNNUAK+OGda0brLL6t6+jE/UlKskjt7UzdHlan1AroLkLtkrVqcBPjAgMBAAGG
UDBOBgkqhkiG9w0BCQ4xQTA/MASGA1UdDwQEAwIChDAPBgNVHREEDAGhwTaqAEB
MB8GA1UdEQQYMBaCFHNoaXN5YSlhLmZ1aml0c3UuY29tMA0GCSqGSIb3DQEBBQUA
A4GBACRKhb8k108Jf7w9YNgzHN+ORyY2sIrhqpytSquNonvcZaEgVe9yUqQ
WOIqhgggINKSRW82odtTFi97Ttgalyi jj5GeaVCLaSE6FH9lLhcLlArY2dArRYM/
Zv62xudPCLwew49N8GA+Dq+9G3wCSYA0kFQNJmm/HIpUnb
-----END CERTIFICATE REQUEST-----

```

```

[Local Certificate]
[1] Number : 0, Name : mycert
-----BEGIN CERTIFICATE-----
MIIDBjCCAm8CAQEWdQYJKoZIhvcNAQEFBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQKIWhwLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaxRlZDESMBAGAlUECxMjVGVjaCBEaXYuMRswGQYDVQDEExJzaGlzeWUu
ZnVqaXRzdS5jb20xHZAAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhCN
MDcwNzIwMDIwNzU4WhcNMDcxMjMxMDIwNzU4WjCBnzELMAkGA1UEBHMCS1AxETAP
BgNVBAGTCeThbmFnYXdhMREwDwYDVQHEwhLYXdhc2FraTEYMBYGA1UEChMFRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLLWUuZnVqaXRzdS5jb20wDQYJKoZIhvcNAQEB
Y5SmdWppdHNLmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHNLmNvbTcB
nzANBgkqhkiG9w0BAQEFAAOBjQAwGykCgYEAyTsGrOKJrGHXt9giTbtEsjrgQCM/
VGc0sScsn92z0SsihPw8Fxn1rSa93PSdGUrweY2YMYy jUNG58Fa55K+z1CCXTPK
RC75Hdgo8w0wneAvTq2I2Sxp0001QAr44Z1rRussvq3r6MT9TUqySO3tTN0fVqfU
CuguQu2StWpwE+MCAwEAANVMFMwCwYDVR0PBAQDAgKEMA8GA1UdEQQIMAaHBMCo
AQEwHwYDVR0RBBgwFoIUc2hpc3lhLWUuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAGw
BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UzbXOVYN4RZ6zcbpn7YCwv/y7
oSR5ppTcZz1VCgWNYFQIz1/MCNvlyGk9at8S0lQgM5zi0bXypD0p10B3Ust0mzGx
3i3jsVuKJkbn0qsysUZQEpmfS7JdYHuIRN5nWPBjqH68CqQD8zPeJ21VcwcsUohF
FKA8mr9msEiVNQ==
-----END CERTIFICATE-----

```

#

(4) base64 オプションを指定して編集中の構成定義から証明書情報 (証明書要求、自装置証明書) を表示

```
# show crypto certificate base64 candidate
[Certificate Request]
[1] Number : 0
-----BEGIN CERTIFICATE REQUEST-----
MIICMCCAzkCAQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYDVQQIEWhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTGltaxRlZDESMBAG
A1UECXMJVGVjaCBEaXYuMRswGQYDVQDEExJzaGlzeWEuZnVqaXRzdS5jb20xHzAd
BgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAMk7Bq9Ciaxh17fYIkwbrLI64EAjP1RnDrEnLJ/ds9ErIoT4sPBc
Z9a0mvdz0nRlK8HmNmDGMo1DRufBWueSvs9Qgl0zykQu+R3YKPMNMJ3gL06tiNk1
6TtNNUAK+OGda0brLL6t6+jE/UlKskjt7UzdHlan1AroLkLtkrVqcBPjAgMBAAAG
UDBOBqkqhkiG9w0BCQ4xQTA/MASGA1UdDwQEAwIChDAPBgNVHREEDAGhwTAgAEB
MB8GA1UdEQQYMBaCFHNoaXN5S1hLmZ1aml0c3UuY29tMA0GCSqGSIb3DQEBBQUA
A4GBACRKhb8k108Jf7w9YNgzHN+ORyY2sIrrqhpytSquNonvcZzaEgVeqyUgQ
WOIqhggINKSRW82odtTFi97TtgalayiJj5GeaVCLaSE6FH9lLhcLlArY2dArRYM/x
Zv62xudPCLvwe+w49N8gA+Dq+9G3wCSYA0kFQNJmm/HIpuNb
-----END CERTIFICATE REQUEST-----

[Local Certificate]
[1] Number : 0, Name : mycert
-----BEGIN CERTIFICATE-----
MIIDBjCCAm8CAQEwDQYJKoZIhvcNAQEFBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaxRlZDESMBAGA1UECXMJVGVjaCBEaXYuMRswGQYDVQDEExJzaGlzeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDcwNzIwMDIwNzU4WhcNMDcxMjMxMDIwNzU4WjCBnzELMAkGA1UEBhMCSlAxETAP
BgNVBAGTCEthbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPrnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEw1UZWN0IERpdi4xGzAZBgNVBAMTEuNoaXN5
YS5mdWppdHh1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHh1LmNvbTcB
nzANBqkqhkiG9w0BAQEFAAOBjQAwYkCgYEAyTsGrOKJrGHXt9giTBtEsjrgQCM/
VGcOsScsn92z0SsihPiw8Fxn1rSa93PSdGUrweY2YMYyJUNG58Fa55K+z1CCXTPK
RC75Hdgo8w0wneAvTq2I2SXP001QAr44Z1rRussvq3r6MT9TUqySO3tTN0fVqfU
CuguQu2StWpwe+MCAwEAaNVFMwCwYDVR0PBQAQDAGKEMA8GA1UdEQQIMAAHBMCO
AQEwHwYDVR0RBBgwFoIUc2hpc3lhLWUuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAgw
BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UzbXOVYN4RZ6zcbpn7YCwv/y7
oSR5ppTcZZ1VCgWNYFQIz1/MCNvlyGk9at8S0lQgM5zi0bXypD0p10B3Ust0mzGx
3i3jsVuKJkbn0qsysUZQEpmFMS7JdYHuIRN5nWPBjqH68CqQD8zPeJ21VcwcsUohF
FKA8mr9msEiVNQ==
-----END CERTIFICATE-----

#
```

```

[1] Number : 0, Name : mycert
-----
(1) (2) (3)
Version : 3
-----
(4)
Serial Number: 0
-----
(5)
Signature Algorithm : md5WithRSAEncryption
-----
(6)
Issuer : C=JP, ST=Kanagawa, L=kawasaki,
-----
(7) (8) (9)
O=Fujitsu Limited
-----
(10)
OU=Tech Div.,
-----
(11)
CN=shisya.fujitsu.com,
-----
(12)
emailAddress=hoge@fujitsu.com
-----
(13)
Validity
Not Before: Jan 4 07:50:53 2006
-----
(14)
Not After : Feb 3 07:50:53 2006
-----
(15)
Subject : C=JP, ST=Kanagawa, L=kawasaki,
-----
(16) (17) (18)
O=Fujitsu Limited
-----
(19)
OU=Tech Div.,
-----
(20)
CN=shisya.fujitsu.com,
-----
(21)
emailAddress=hoge@fujitsu.com
-----
(22)
Subject Public Key Info:
Public Key Algorithm : rsaEncryption
-----
(23)
RSA Public Key : (1024 bit)
-----
(24)
X509v3 extensions:
X509v3 Key Usage:
Digital Signature, Certificate Sign
-----
(25)
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:1
-----
(26)
Signature Algorithm : md5WithRSAEncryption
-----
(27)
c2:9b:e5:cb:f0:24:e9:dd:6f:32:07:6d:70:86:18:e5:2d:78:
8d:02:9d:da:d9:c1:f4:2b:47:cf:e6:f2:1b:89:7b:e4:88:2a:
87:6b:85:c5:92:29:6d:8b:92:1a:f5:4e:4b:ec:c8:97:5c:a2:
21:e9:71:33:9a:7b:40:f5:2c:fc:10:16:53:57:8f:52:6a:cb:
ad:ab:1e:b4:46:e0:20:55:f4:a5:7c:a5:58:5f:02:6d:6d:3c:
1f:d4:8c:20:37:e4:77:a7:62:9d:dc:69:90:0d:d5:99:59:4f:
40:a4:b0:0a:46:80:17:69:00:f8:b0:1a:a3:42:1a:b2:c9:23:
9b:4e
-----
(28)

```

-
- 1) 証明書の表示番号
 - 2) 識別番号
 - 3) 識別名
 - 4) バージョン
 - 5) シリアル番号
 - 6) 署名アルゴリズム
 - 7) 国コード
 - 8) 都道府県
 - 9) 市区町村
 - 10) 組織または会社
 - 11) 組織ユニットまたは部門
 - 12) ホスト名
 - 13) E メールアドレス
 - 14) 証明書の発行日時
 - 15) 証明書の有効期限
 - 16) 国コード
 - 17) 都道府県
 - 18) 市区町村
 - 19) 組織または会社
 - 20) 組織ユニットまたは部門
 - 21) 通常名
 - 22) E メールアドレス
 - 23) 公開鍵アルゴリズム
 - 24) 公開鍵の内容
 - 25) 証明書の利用方法
 - 26) 証明書の規制
 - 27) 署名アルゴリズム
 - 28) 署名の内容

第 40 章 管理機器の設定、ログ、状態などの表示コマンド

- グループ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 <group_number> (グループ定義番号) 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 ~ 4	SR-M20AP2 SR-M20AP1

- 管理機器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 <node_number> (管理機器定義番号) に指定する管理機器の通し番号 (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 ~ 4	SR-M20AP2 SR-M20AP1

- MAC アドレスフィルタセット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 <set_num> (MAC アドレスフィルタセット定義番号) に指定する MAC アドレスフィルタセットの通し番号 (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 ~ 4	SR-M20AP2 SR-M20AP1

- 管理外無線 LAN アクセスポイント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> (管理外無線 LAN アクセスポイント定義番号) に指定する管理外無線 LAN アクセスポイントの通し番号 (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 ~ 4	SR-M20AP2 SR-M20AP1

40.1 管理機器の設定、ログ、状態などの表示

40.1.1 show nodemanager group

[機能]

管理グループ一覧の表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

show nodemanager group

[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]

管理グループの一覧を表示します。

[実行例]

```
# show nodemanager group
Group      Node
-----
(1)        (2)
0:GroupA   1
1:GroupB   3
#
```

- 1) グループ定義番号:グループ名
- 2) グループ所属の管理機器数

40.1.2 show nodemanager node

[機能]

管理機器の詳細情報表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

show nodemanager node [node <node_number>]

[オプション]

なし

すべての管理機器の情報を表示します。

<node_number>

- 管理機器定義番号
管理機器の通し番号を 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]

管理機器の詳細情報を表示します。

[実行例]

```
# show nodemanager node 0
Node Name           : AP01[0]           ---(1)
Group Name          : GroupA[0]         ---(2)
IP Address           : 192.168.1.2      ---(3)
Port Number         : 23                ---(4)
Node Type           : WLAN              ---(5)
Administrator Name  : nodemgr          ---(6)
Password            : acedafe(encrypted) ---(7)
Scan Flag           : enabled           ---(8)
STA Information Flag : enabled         ---(9)
Neighbor            : AP_02[1] GroupA[0]
                    : (10) (11)
                    : AP_03[2] GroupA[0]
                    : AP_04[3] GroupA[0]
                    : AP_05[4] GroupA[0]
Node Status         : running           ---(12)
LAN Status          : active            ---(13)
Firm Version        : V02.00 NY0001     ---(14)
Config Update       : July 30 09:30:00 2009 ---(15)
Status Update       : July 30 12:00:10 2009 ---(16)
```

(続く)

(続き)

```
[WLAN#1]
TYPE           : AP                      ---(17)
MAC            : 00:00:0e:f5:43:d1       ---(18)
WLAN Status    : active                  ---(19)
RSSI           : 53 / AP_02[1] GroupA[0]
                (20) (21) (22)
MODE           : 11g/n Channel:1,5 STA:3
                (23) (24) (25)
SSID           : Si-R_WLAN_AP01_00_01 wpa-psk aes
                (26) (27) (28)
```

```
[WLAN#2]
TYPE           : AP
MAC            : 00:00:0e:f5:43:d2
WLAN Status    : active
RSSI           : 54 / AP_02[1] GroupA[0]
MODE           : 11g/n Channel:1,5 STA:3
SSID           : Si-R_WLAN_AP01_01_02 wpa aes
```

```
[WLAN#3]
TYPE           : AP
MAC            : 00:00:0e:f5:43:d3
WLAN Status    : active
RSSI           : 48 / AP_02[1] GroupA[0]
MODE           : 11g/n Channel:1,5 STA:3
SSID           : Si-R_WLAN_AP01_01_03 wpa aes
```

```
[WLAN#4]
TYPE           : AP
MAC            : 00:00:0e:f5:43:d4
WLAN Status    : active
RSSI           : 38 / AP_02[1] GroupA[0]
MODE           : 11g/n Channel:1,5 STA:3
SSID           : Si-R_WLAN_AP01_01_04 wpa aes
```

```
[WLAN#5]
TYPE           :
MAC            :
WLAN Status    : unknown
RSSI           :
MODE           :
SSID           :
```

```
[WLAN#6]
TYPE           :
MAC            :
WLAN Status    : unknown
RSSI           :
MODE           :
SSID           :
```

```
[WLAN#7]
TYPE           :
MAC            :
WLAN Status    : unknown
RSSI           :
MODE           :
SSID           :
```

```
[WLAN#8]
TYPE           :
MAC            :
WLAN Status    : unknown
RSSI           :
MODE           :
SSID           :
```

(続く)

(続き)

```
[WLAN#9]
TYPE           : AP
MAC            : 00:00:0e:f5:43:d9
WLAN Status    : active
RSSI           : 52 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_09 wpa/wpa2-psk aes

[WLAN#10]
TYPE           : AP
MAC            : 00:00:0e:f5:43:da
WLAN Status    : active
RSSI           : 44 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_10 wpa2 auto

[WLAN#11]
TYPE           : AP
MAC            : 00:00:0e:f5:43:db
WLAN Status    : active
RSSI           : 49 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_11 wpa2 tkip

[WLAN#12]
TYPE           : AP
MAC            : 00:00:0e:f5:43:dc
WLAN Status    : active
RSSI           : 58 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_12 wpa2 auto

[WLAN#13]
TYPE           : AP
MAC            : 00:00:0e:f5:43:dd
WLAN Status    : active
RSSI           : 53 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_13 wpa2 auto

[WLAN#14]
TYPE           : AP
MAC            : 00:00:0e:f5:43:de
WLAN Status    : active
RSSI           : 49 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_14 wpa2 aes

[WLAN#15]
TYPE           : AP
MAC            : 00:00:0e:f5:43:df
WLAN Status    : active
RSSI           : 31 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_15 wpa2 aes

[WLAN#16]
TYPE           : AP
MAC            : 00:00:0e:f5:43:e0
WLAN Status    : active
RSSI           : 58 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_16 wpa2 aes

#
```

- 1) 管理機器名 [管理機器定義番号]
- 2) グループ名 [グループ定義番号]
- 3) IP アドレス
- 4) ポート番号
- 5) 管理機器のタイプ

WLAN : 無線 LAN アクセスポイント

6) ユーザ名

7) パスワード

暗号化形式で表示されます。

8) スキャンフラグ

監視用管理機器として運用するかどうかが表示されます。

disabled

: スキャン要求なし

enabled : スキャン要求あり

9) 情報取得フラグ

管理機器への無線 LAN 端末情報取得ありかどうかが表示されます。

disabled

: 無線 LAN 端末の情報取得なし

enabled : 無線 LAN 端末の情報取得あり

10) 近隣管理機器名 [管理機器定義番号]

11) 近隣管理機器が属するグループのグループ名 [グループ定義番号]

12) 稼動情報

無線 LAN アクセスポイントの稼動情報の収集状況が表示されます。

running : 稼動情報収集中

stop : ログイン失敗

failure : コマンド実行失敗など、なんらかのエラーにより情報取得不可

unknown

: 管理停止中、または未取得

13) 有線 LAN 監視状態

active : 稼動中

active? : 通信異常の疑い

inactive : 通信異常

unknown

: 監視停止中、または未取得

14) ファームウェアバージョン

15) 設定変更日時

無線 LAN アクセスポイント構成定義の設定変更日時が表示されます。

16) 情報更新日時

無線 LAN アクセスポイント稼動情報の情報更新日時が表示されます。

17) 無線 LAN のタイプ

AP : 無線 LAN アクセスポイント

SCANONLY

: スキャン専用モード

WDS : WDS

unknown

: 不明

18) 以降の情報は、無線 LAN のタイプが AP の場合のみ有効となります。

18) MAC アドレス

19) 無線 LAN 監視状態

無線 LAN スキャンによる状態の監視結果が表示されます。AP が動作中であっても、DFS などにより AP の動作チャンネルが変わるなどして、監視用 AP の運用チャンネルから外れた場合にも active?、inactive の状態になることがあります。

active :稼動中

active? : 無線 LAN スキャンで一時的に検出できない

inactive : 無線 LAN スキャンで検出できなかった

unknown

: 監視停止中、または未取得

20) RSSI

受信信号強度

空白 : 0

空白以外 : RSSI

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) - 95	SR-M20AP2 SR-M20AP1

21) 当該無線 LAN アクセスポイントの RSSI を検出した監視用無線 LAN アクセスポイント名 [管理機器定義番号]

22) 監視用無線 LAN アクセスポイントが属するグループのグループ名 [グループ定義番号]

23) モード

空白 : 未取得

11b : IEEE802.11b で動作

11b/g : IEEE802.11b/g で動作

11b/g/n : IEEE802.11b/g/n 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

24) チャンネル

空白 : 未取得

空白以外 : チャンネル番号

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。

25) 無線 LAN 端末数

無線 LAN アクセスポイントに接続している無線 LAN 端末数が表示されます。

空白 : 未取得
空白以外 : 無線 LAN 端末数

26) SSID

27) 認証モード

無線 LAN アクセスポイントとの認証モードが表示されます。

空白 : 未取得
open : IEEE802.11 のオープン認証
shared : IEEE802.11 の共通認証
wpa : WPA を使った IEEE802.1X 認証
wpa-psk
: WPA を使った事前共通キー (PSK) 認証
wpa2 : WPA2 を使った IEEE802.1X 認証
wpa2-psk
: WPA2 を使った事前共通キー (PSK) 認証
wpa/wpa2
: WPA または WPA2 を自動判別した IEEE802.1X 認証
wpa/wpa2-psk
: WPA または WPA2 を自動判別した事前共有キー (PSK) 認証

28) 暗号化方式

無線 LAN アクセスポイントとの暗号化方式が表示されます。

空白 : 未取得
tkip : TKIP 暗号
aes : AES(CCMP) 暗号
auto : TKIP または AES を自動判別
wep64 : 暗号化されていない WEP キー (64bit)
wep128 : 暗号化されていない WEP キー (128bit)
wep152 : 暗号化されていない WEP キー (152bit)

40.1.3 show nodemanager update wlan filterset

[機能]

管理機器用の MAC アドレスフィルタセットの内容表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

show nodemanager update wlan filterset <set_num>

[オプション]

<set_num>

- MAC アドレスフィルタセット定義番号
表示対象の MAC アドレスフィルタセット定義番号を指定します。

[動作モード]

構成定義モード (管理者クラス)

[説明]

管理機器用の MAC アドレスフィルタセットの内容を表示します。

[実行例]

```
# show nodemanager update wlan filterset 0
No. MAC Address      Action Description
-----
(1) (2)              (3)  (4)
0 00:00:0e:f5:43:d1 pass  GroupA/AP_A01/STATION_001
1 00:00:0e:f5:43:d2 pass  GroupA/AP_A01/STATION_002
2 00:00:0e:f5:43:d5 pass  GroupA/AP_A02/STATION_031
30 any                reject GroupA/AP_A02/STATION_004
#
```

- 1) MAC アドレスフィルタ定義番号
- 2) 無線 LAN 端末 MAC アドレス

MAC アドレス

: 対象 MAC アドレス

any : すべての MAC アドレスが対象

- 3) アクション

該当する MAC アドレスを有する端末の接続を許可するかどうかが表示されます。

pass : 端末の接続を許可

reject : 端末の接続を拒否

- 4) コメント

40.1.4 show nodemanager node brief

[機能]

管理機器の一覧表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

show nodemanager node brief [node <node_number>]

[オプション]

なし

すべての管理機器の情報を表示します。

<node_number>

- 管理機器定義番号
管理機器の通し番号を 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]

管理機器の一覧を表示します。

[実行例]

```
# show nodemanager node brief
Node          Group          Type Scan      IP Address
-----
(1)           (2)           (3) (4)      (5)
0:AP_A01     0:GroupA      WLAN enabled 192.168.10.10
1:AP_A02     0:GroupA      WLAN disabled 192.168.10.11
2:AP_A03     0:GroupA      WLAN disabled 192.168.10.12
#
```

- 1) 管理機器定義番号:管理機器名
- 2) グループ定義番号:グループ名
- 3) 管理機器のタイプ
WLAN : 無線 LAN アクセスポイント
- 4) スキャンフラグ
監視用管理機器として運用するかどうかが表示されます。
disabled : スキャン要求なし
enabled : スキャン要求あり
- 5) IP アドレス

40.1.5 show nodemanager logging wlan scan unmanaged

[機能]

管理外無線 LAN アクセスポイントの監視状況の表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

show nodemanager logging wlan scan unmanaged [<number>]

[オプション]

なし

すべての管理外無線 LAN アクセスポイントの監視状況を表示します。

<number>

- 管理外無線 LAN アクセスポイント定義番号
管理外無線 LAN アクセスポイントの通し番号を 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]

管理外無線 LAN アクセスポイントの監視状況を表示します。

[実行例]

```
# show nodemanager logging wlan scan unmanaged
WLAN Name      : UMAP_01[0]                --- (1)
MAC            : 00:00:0e:f5:43:d8        --- (2)
MODE          : 11b/g                    --- (3)
CHANNEL       : 11                       --- (4)
RSSI          : 43 / AP_01[0] GroupA[0]
               (5) (6) (7)
               0 / AP_02[1] GroupB[1]
               54 / AP_03[2] GroupC[2]
               16 / AP_04[3] GroupD[3]
STATE         : found                    --- (8)
FOUND TIME    : 2009/05/15 15:25:20      --- (9)
LOST TIME     :                          --- (10)
SSID         : APaa_aa                  --- (11)

WLAN Name      : UMAP_02[1]
MAC            : 00:00:0e:f5:43:c1
MODE          : 11a
CHANNEL       : 52
RSSI          : 58 / AP_01[0] GroupA[0]
               0 / AP_02[1] GroupB[1]
               45 / AP_03[2] GroupC[2]
               12 / AP_04[3] GroupD[3]
STATE         : lost
FOUND TIME    : 2009/05/15 14:10:20
LOST TIME     : 2009/05/15 16:13:14
SSID         : APbb_bb

#
```

- 1) 管理外無線 LAN アクセスポイント名 [管理外無線 LAN アクセスポイント定義番号]

2) MAC アドレス

3) モード

- 空白 : 未取得
- 11b** : IEEE802.11b
- 11b/g** : IEEE802.11b または 11g
- 11b/g/n** : IEEE802.11b, 11g または 11n
- 11g** : IEEE802.11g
- 11g/n** : IEEE802.11g または 11n
- 11a** : IEEE802.11a
- 11a/n** : IEEE802.11a または 11n

4) チャンネル

- 空白 : 未取得
- 空白以外 : チャンネル番号

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。

5) RSSI

受信信号強度

- 空白 : 未取得
- 空白以外 : RSSI

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) - 95	SR-M20AP2 SR-M20AP1

6) 当該無線 LAN アクセスポイントの RSSI を検出した監視用無線 LAN アクセスポイント名 [管理機器定義番号]

7) 監視用無線 LAN アクセスポイントが属するグループのグループ名 [グループ定義番号]

8) 状態

管理外無線 LAN アクセスポイントの検出状態

- 空白 : 未取得
- found** : 管理外無線 LAN アクセスポイント検出中
- lost** : 管理外無線 LAN アクセスポイント検出後に消失

9) 管理外無線 LAN アクセスポイントの検出日時

10) 管理外無線 LAN アクセスポイントの消失日時

11) SSID

40.1.6 show nodemanager logging wlan scan

[機能]

監視ログの表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

show nodemanager logging wlan scan

[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]

監視ログを古い順から表示します。監視ログには、以下の情報を記録しています。

- 有線、無線の監視の開始、停止
- 有線の監視結果
- 無線の監視結果
- 無線 LAN 端末の RSSI の監視結果

構成定義コマンドで設定した監視ログ保持件数以内の最新ログを表示します。

[実行例]

```
# show nodemanager logging wlan scan
2009/05/15 12:34:52 L_START ---(1)
2009/05/15 12:34:56 L_ACTIVE 00:00:0e:f5:43:d1 MG AP_01[0] ---(2)
2009/05/15 12:35:57 L_INACTV 00:00:0e:f5:43:d2 MG AP_03[2] ---(3)
2009/05/15 12:36:09 W_START ---(4)
2009/05/15 12:36:12 W_ACTIVE 00:00:0e:f5:43:d1 MG AP_01[0] 11 ---(5)
2009/05/15 12:36:42 W_ACTIVE 00:00:0e:f5:43:d8 UM UM_AP_01[0] 6 ---(6)
2009/05/15 12:37:13 W_ACTIVE 00:00:0e:f5:43:d7 UK - 13 ---(7)
2009/05/15 12:38:22 W_INACTV 00:00:0e:f5:43:d1 MG AP_01[0] ---(8)
2009/05/15 12:39:43 W_INACTV 00:00:0e:f5:43:d7 UK - ---(9)
2009/05/15 12:40:14 UNDER_R 00:00:0e:f5:45:a1 ST AP_01[0] 19 ---(10)
2009/05/15 12:40:25 OVER_R 00:00:0e:f5:45:a1 ST AP_01[0] 21 ---(11)
2009/05/15 12:40:35 L_STOP ---(12)
2009/05/15 12:40:35 W_STOP ---(13)
#
```

- 1) 有線監視開始
- 2) 有線監視で管理無線 LAN アクセスポイントの稼動中を検出した例
- 3) 有線監視で管理無線 LAN アクセスポイントの通信異常を検出した例
- 4) 無線監視開始
- 5) 無線監視で管理無線 LAN アクセスポイントの稼動中を検出した例
- 6) 無線監視で管理外無線 LAN アクセスポイントの稼動中を検出した例

-
- 7) 無線監視で不明無線 LAN アクセスポイントの稼動中を検出した例
 - 8) 無線監視で管理無線 LAN アクセスポイントの消失を検出した例
 - 9) 無線監視で不明無線 LAN アクセスポイントの消失を検出した例
 - 10) 無線 LAN 端末の RSSI が最低しきい値以下を検出した例
 - 11) 無線 LAN 端末の RSSI が最低しきい値より大きな値を検出した例
この表示は、10) の表示が出た無線 LAN 端末のみを対象とします。
 - 12) 有線監視停止
 - 13) 無線監視停止

表示情報の詳細説明を以下に示します。

```

2009/05/15 12:34:56 L_ACTIVE 00:00:0e:f5:43:d1 MG AP_01[0]
(1) (2) (3) (4) (5) (6)
2009/05/15 12:35:57 L_INACTV 00:00:0e:f5:43:d2 MG AP_03[2]
2009/05/15 12:36:12 W_ACTIVE 00:00:0e:f5:43:d1 MG AP_01[0] 11
(7)
2009/05/15 12:36:42 W_ACTIVE 00:00:0e:f5:43:d8 UM UM_AP_01[0] 6
(8)
2009/05/15 12:37:13 W_ACTIVE 00:00:0e:f5:43:d7 UK - 13
(9)
2009/05/15 12:37:14 UNDER_R 00:00:0e:f5:45:a1 ST AP_01[0] 21
(10)
2009/05/15 12:38:22 W_INACTV 00:00:0e:f5:43:d1 MG AP_01[0]
(6)
2009/05/15 12:39:43 W_INACTV 00:00:0e:f5:43:d7 UK -
(9)

```

- 1) 履歴の登録日
- 2) 履歴の登録時刻
- 3) イベントタイプ

履歴記録の原因となったイベントの種類が表示されます。

L_START

: 有線監視開始

L_STOP

: 有線監視停止

W_START

: 無線監視開始

W_STOP

: 無線監視停止

L_ACTIVE

: 有線監視 稼動検出

L_INACTV

: 有線監視 非稼動検出

W_ACTIVE

: 無線監視 稼動検出

W_INACTV

: 無線監視 非稼動検出

OVER_R

: RSSI 最低しきい値からの復帰を検出

UNDER_R

: RSSI 最低しきい値以下への遷移を検出

4) 無線 LAN アクセスポイントの MAC アドレス

5) 無線 LAN アクセスポイントタイプ

履歴の対象となった無線 LAN アクセスポイントの種類が表示されます。

MG : 管理無線 LAN アクセスポイント

UM : 管理外無線 LAN アクセスポイント

UK : 不明無線 LAN アクセスポイント

ST : 無線 LAN 端末

6) 無線 LAN アクセスポイント名 [管理機器定義番号]

無線 LAN アクセスポイントタイプが管理無線 LAN アクセスポイントの場合に表示されます。

7) チャンネル

イベントタイプが無線監視 稼働検出の場合に表示されます。

8) 管理外無線 LAN アクセスポイント名 [管理外無線 LAN アクセスポイント定義番号]

無線 LAN アクセスポイントタイプが管理外無線 LAN アクセスポイントの場合に表示されます。

9) ハイフン

無線 LAN アクセスポイントタイプが不明無線 LAN アクセスポイントの場合に表示されます。不明無線 LAN アクセスポイントには名前がないため、名前の代わりにハイフンを表示します。

10) RSSI

イベントタイプが RSSI 最低しきい値以下検出の場合に表示されます。

40.1.7 show nodemanager logging wlan scan managed brief

[機能]

管理無線 LAN アクセスポイントの監視状況の一覧表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

show nodemanager logging wlan scan managed brief

[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]

管理機器のタイプに無線 LAN が指定されているものについて、その監視状況の一覧を表示します。

[実行例]

```
# show nodemanager logging wlan scan managed brief
Node      Gr LAN      WLAN STATUS      IP Address
          act act?  inact unknown
-----
(1)      (2) (3)      (4) (5) (6) (7)      (8)
0:AP_A01  1 active   3   4   9      0 192.168.10.11
1:AP_A02  1 active   0   0   0      16 192.168.10.12
2:AP_A03  1 active   0  16   0      0 192.168.10.13
3:AP_A04  1 active   2   0  14      0 192.168.10.14
#
```

- 1) 管理機器定義番号:無線 LAN アクセスポイント名
- 2) グループ定義番号
- 3) 有線 LAN 監視状態

active : 稼動中

active? : 通信異常の疑い

inactive : 通信異常

unknown

: 監視停止中、または未取得

- 4) 稼動中の無線 LAN 数
- 5) 通信異常の疑いがある無線 LAN 数
- 6) 通信異常の無線 LAN 数
- 7) 監視停止中の無線 LAN 数
- 8) IP アドレス

40.1.8 show nodemanager logging wlan scan managed

[機能]

管理無線 LAN アクセスポイントの監視状況の表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

```
show nodemanager logging wlan scan managed [{node <node_number> | group
<group_number>}] [inactive]
```

[オプション]

なし

すべての管理機器の情報を表示します。

<node_number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<group_number>

- グループ定義番号
管理グループの通し番号を 10 進数で指定します。

inactive

- 通信異常管理機器表示
有線監視と無線監視のどちらかが通信異常または通信異常の疑いになっている管理機器だけを表示します。

[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]

管理無線 LAN アクセスポイントの監視状況を表示します。inactive オプションを指定した場合は、有線、無線のどちらかが通信異常または通信異常の疑いのある管理無線 LAN アクセスポイントだけを表示します。

[実行例]

```
# show nodemanager logging wlan scan managed node 0
WLAN Name      : AP01[0]          ---(1)
Group Name     : GroupA[0]       ---(2)
IP Address     : 192.168.1.2     ---(3)
LAN Status     : active         ---(4)

[WLAN#1]
TYPE          : AP              ---(5)
MAC           : 00:00:0e:f5:43:d1 ---(6)
WLAN Status   : active         ---(7)
RSSI          : 53 / AP_02[1] GroupA[0]
              (8) (9) (10)
MODE          : 11g/n Channel:1,5 STA:3
              (11) (12) (13)
SSID          : Si-R_WLAN_AP01_00_01 wpa-psk aes
              (14) (15) (16)

[WLAN#2]
TYPE          : AP
MAC           : 00:00:0e:f5:43:d2
WLAN Status   : active
RSSI          : 54 / AP_02[1] GroupA[0]
MODE          : 11g/n Channel:1,5 STA:3
SSID          : Si-R_WLAN_AP01_01_02 wpa-psk aes

[WLAN#3]
TYPE          : AP
MAC           : 00:00:0e:f5:43:d3
WLAN Status   : active
RSSI          : 68 / AP_02[1] GroupA[0]
MODE          : 11g/n Channel:1,5 STA:3
SSID          : Si-R_WLAN_AP01_01_03 wpa-psk aes

[WLAN#4]
TYPE          : AP
MAC           : 00:00:0e:f5:43:d4
WLAN Status   : active
RSSI          : 38 / AP_02[1] GroupA[0]
MODE          : 11g/n Channel:1,5 STA:3
SSID          : Si-R_WLAN_AP01_01_04 wpa aes

[WLAN#5]
TYPE          :
MAC           :
WLAN Status   : unknown
RSSI          :
MODE          :
SSID          :

[WLAN#6]
TYPE          :
MAC           :
WLAN Status   : unknown
RSSI          :
MODE          :
SSID          :

[WLAN#7]
TYPE          :
MAC           :
WLAN Status   : unknown
RSSI          :
MODE          :
SSID          :

[WLAN#8]
TYPE          :
MAC           :
WLAN Status   : unknown
RSSI          :
MODE          :
SSID          :
```

(続<)

(続き)

```

[WLAN#9]
TYPE           : AP
MAC            : 00:00:0e:f5:43:d9
WLAN Status    : active
RSSI           : 52 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_09 wpa/wpa2-psk aes

[WLAN#10]
TYPE           : AP
MAC            : 00:00:0e:f5:43:da
WLAN Status    : active
RSSI           : 44 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_10 wpa2 auto

[WLAN#11]
TYPE           : AP
MAC            : 00:00:0e:f5:43:db
WLAN Status    : active
RSSI           : 29 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_11 wpa2 tkip

[WLAN#12]
TYPE           : AP
MAC            : 00:00:0e:f5:43:dc
WLAN Status    : active
RSSI           : 58 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_12 wpa2 auto

[WLAN#13]
TYPE           : AP
MAC            : 00:00:0e:f5:43:dd
WLAN Status    : active
RSSI           : 43 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_13 wpa2 auto

[WLAN#14]
TYPE           : AP
MAC            : 00:00:0e:f5:43:de
WLAN Status    : active
RSSI           : 59 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_14 wpa2 aes

[WLAN#15]
TYPE           : AP
MAC            : 00:00:0e:f5:43:df
WLAN Status    : active
RSSI           : 31 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_15 wpa2 aes

[WLAN#16]
TYPE           : AP
MAC            : 00:00:0e:f5:43:e0
WLAN Status    : active
RSSI           : 48 / AP_02[1] GroupA[0]
MODE           : 11a Channel:40 STA:5
SSID           : Si-R_WLAN_AP01_01_16 wpa2 aes

#

```

- 1) 無線 LAN アクセスポイント名 [管理機器定義番号]
- 2) グループ名 [グループ定義番号]
- 3) IP アドレス
- 4) 有線 LAN 監視状態

active : 稼動中

active? : 通信異常の疑い
inactive : 通信異常
unknown
: 監視停止中、または未取得

5) 無線 LAN のタイプ

AP : 無線 LAN アクセスポイント
SCANONLY
: スキャン専用モード
WDS : WDS
unknown
: 不明

6) 以降の情報は、無線 LAN のタイプが AP の場合のみ有効となります。

6) MAC アドレス

7) 無線 LAN 監視状態

active : 稼動中
active? : 通信異常の疑い
inactive : 通信異常
unknown
: 監視停止中、または未取得

8) RSSI

受信信号強度

空白 : 0
空白以外 : RSSI

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) - 95	SR-M20AP2 SR-M20AP1

9) 当該無線 LAN アクセスポイントの RSSI を検出した監視用無線 LAN アクセスポイント名 [管理機器定義番号]

10) 監視用無線 LAN アクセスポイントが属するグループのグループ名 [グループ定義番号]

11) モード

空白 : 未取得
11b : IEEE802.11b
11b/g : IEEE802.11b または 11g
11b/g/n : IEEE802.11b, 11g または 11n
11g : IEEE802.11g
11g/n : IEEE802.11g または 11n

11a : IEEE802.11a
11a/n : IEEE802.11a または 11n

12) チャンネル

空白 : 未取得
 空白以外 : チャンネル番号

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。

13) 無線 LAN 端末数

無線 LAN アクセスポイントに接続している無線 LAN 端末数

空白 : 未取得
 空白以外 : 無線 LAN 端末数

14) SSID

15) 認証モード

無線 LAN アクセスポイントとの認証モード

空白 : 未取得
open : IEEE802.11 のオープン認証
shared : IEEE802.11 の共通認証
wpa : WPA を使った IEEE802.1X 認証
wpa-psk
 : WPA を使った事前共通キー (PSK) 認証
wpa2 : WPA2 を使った IEEE802.1X 認証
wpa2-psk
 : WPA2 を使った事前共通キー (PSK) 認証
wpa/wpa2
 : WPA または WPA2 を自動判別した IEEE802.1X 認証
wpa/wpa2-psk
 : WPA または WPA2 を自動判別した事前共有キー (PSK) 認証

16) 暗号化方式

無線 LAN アクセスポイントとの暗号化方式

空白 : 未取得
tkip : TKIP 暗号
aes : AES(CCMP) 暗号
auto : TKIP または AES を自動判別
wep64 : 暗号化されていない WEP キー (64bit)
wep128 : 暗号化されていない WEP キー (128bit)
wep152 : 暗号化されていない WEP キー (152bit)

40.1.9 show nodemanager logging wlan scan unknown

[機能]

不明無線 LAN アクセスポイントの監視状況の表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

show nodemanager logging wlan scan unknown [<mac>]

[オプション]

なし

すべての不明無線 LAN アクセスポイントの監視状況を表示します。

<mac>

- MAC アドレス
不明無線 LAN アクセスポイントの MAC アドレスを指定します。

[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]

不明無線 LAN アクセスポイントの監視状況を表示します。

[実行例]

```
# show nodemanager wlan scan log unknown
MAC          : 00:90:cc:c6:d3:81          --- (1)
MODE         : 11b/g                      --- (2)
CHANNEL      : 13                         --- (3)
RSSI         : 33 / AP_01[0] GroupA[0]
              (4) (5) (6)
              0 / AP_02[1] GroupB[1]
              54 / AP_03[2] GroupC[2]
              16 / AP_04[3] GroupD[3]
STATE        : found                      --- (7)
FOUND TIME   : 2009/05/15 13:37:20        --- (8)
LOST TIME    :                            --- (9)
SSID         : AP00_00                     --- (10)

MAC          : 00:90:cc:c6:d3:82
MODE         : 11b/g
CHANNEL      : 12
RSSI         : 28 / AP_01[0] GroupA[1]
              0 / AP_02[1] GroupB[2]
              45 / AP_03[2] GroupC[3]
              12 / AP_04[3] GroupD[4]
STATE        : lost
FOUND TIME   : 2009/05/15 12:12:20
LOST TIME    : 2009/05/15 15:00:05
SSID         : AP11_01

#
```

- 1) MAC アドレス

2) モード

11b	: IEEE802.11b
11b/g	: IEEE802.11b または 11g
11b/g/n	: IEEE802.11b, 11g または 11n
11g	: IEEE802.11g
11g/n	: IEEE802.11g または 11n
11a	: IEEE802.11a
11a/n	: IEEE802.11a または 11n

3) チャンネル

空白	: 未取得
空白以外	: チャンネル番号

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。

4) RSSI

受信信号強度

空白	: 0
空白以外	: RSSI

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) - 95	SR-M20AP2 SR-M20AP1

5) 当該無線 LAN アクセスポイントの RSSI を検出した監視用無線 LAN アクセスポイント名 [管理機器定義番号]

6) 監視用無線 LAN アクセスポイントが属するグループのグループ名 [グループ定義番号]

7) 状態

不明無線 LAN アクセスポイントの検出状態

found	: 不明無線 LAN アクセスポイント検出中
lost	: 不明無線 LAN アクセスポイント検出後に消失

8) 不明無線 LAN アクセスポイントの検出日時

9) 不明無線 LAN アクセスポイントの消失日時

10) SSID

40.1.10 show nodemanager logging wlan sta

[機能]

無線 LAN インタフェースの無線 LAN 端末情報の表示

[適用機種]



[入力形式]

```
show nodemanager logging wlan sta [{node <node_number> | group <group_number>}]
show nodemanager logging wlan sta mac <mac> [{node <node_number> | group
<group_number>}]
show nodemanager logging wlan sta detail [{node <node_number> | group <group_number>}]
```

[オプション]

なし

すべての無線 LAN 端末の MAC アドレスを対象とします。

mac

<mac>

- MAC アドレス
対象とする無線 LAN 端末の 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。

detail

- 詳細情報
詳細な無線 LAN 端末情報を表示します。

node <node_number> | group <group_number>

なし

すべての無線 LAN アクセスポイントを対象とします。

<node_number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<group_number>

- グループ定義番号
管理グループの通し番号を 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]

接続している無線 LAN 端末情報を表示します。
対象管理機器のパラメタの省略時は、全無線 LAN アクセスポイントの情報を表示します。
node <node_number> 指定時は、指定された無線 LAN アクセスポイントの情報を表示します。
group <group_number> 指定時は、指定グループの情報を表示します。

[メッセージ]

```
Unable to get STA Information from node:<number>.
```

管理機器 <number> から、無線 LAN 端末情報を取得できませんでした。

[実行例]

```
# show nodemanager logging wlan sta
[node:0]
---(1)---
[wlan 1]
Mode: 11g/n Channel: 1 Total: 1 stations(11b:0 11g:0 11g/n:1 11a:0 11a/n:0)
(2) (3) (4)
MAC Address AID Mode Rate RSSI Security AUTH VID IDLE PS WMM BW IP Address
(5) (6) (7) (8) (9) (10) (11) (12) (13) (14)(15)(16)(17)
00:16:e3:00:00:01 1 11g/n 65M 57 WPA-PSK(AES) ok 10 10 10 yes 20 192.168.100.100

[wlan 9]
Mode: 11a Channel: 36 Total: 2 stations(11b:0 11g:0 11g/n:0 11a:2 11a/n:0)
MAC Address AID Mode Rate RSSI Security AUTH VID IDLE PS WMM BW IP Address
00:16:e3:00:00:02 2 11a 48M 57 WPA-PSK(AES) - - 0 active yes 20 192.168.100.101
00:16:e3:00:00:03 3 11a 48M 57 WPA2-PSK(TKIP) ok 300 0 0 no 20 192.168.100.102

Total:3 stations(11b:0 11g:0 11g/n:1 11a:2 11a/n:0) --(18)

# show nodemanager logging wlan sta mac 00:16:e3:00:00:03
[node:0]
[wlan 1]
Mode: 11g/n Channel: 1 Total: 0 stations(11b:0 11g:0 11g/n:1 11a:0 11a/n:0)
MAC Address AID Mode Rate RSSI Security AUTH VID IDLE PS WMM BW IP Address

[wlan 9]
Mode: 11a Channel: 36 Total: 1 stations(11b:0 11g:0 11g/n:0 11a:2 11a/n:0)
MAC Address AID Mode Rate RSSI Security AUTH VID IDLE PS WMM BW IP Address
00:16:e3:00:00:03 3 11a 48M 57 WPA2-PSK(TKIP) ok 300 0 0 no 20 192.168.100.102

Total:1 stations(11b:0 11g:0 11g/n:1 11a:2 11a/n:0) --(18)

# show nodemanager logging wlan sta detail
[node:0]
[wlan 1]
Mode: 11g/n Channel: 1 Total: 1 stations(11b:0 11g:0 11g/n:1 11a:0 11a/n:0)
1. MAC address : 00:16:e3:00:00:01
Since : Feb 24 10:33:17 2009 ---(19)
AID : 1
Mode : 11g/n
Rate : 65M
RSSI : 57
TXSEQ : 0/ 0/ 0/ 0/ 0/ 0/ 0/ 0 ---(20)
RXSEQ : 10/102/73/105/75/106/62/63 ---(21)
CAPS : ESS ---(22)
: PRIVACY
: SHORT_PREAMBLE
ERP : - ---(23)
Security : WPA-PSK(AES)
AUTH : ok
VID : 10
IDLE : 10
PS : 10/50
WMM : yes
BW : 20
WPA : yes ---(24)
WPA2 : yes ---(25)
IP Address : 192.168.100.100
MIMO-PS : static ---(26)
HT-CAPS : SHORT_GI (20MHz) ---(27)
: SHORT_GI (40MHz)
: HT_DELAYED_BLOCKACK
: AMSDU_LENGTH(7935)
: AMPDU_SPACE(1us)
Supported-MCS : 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 ---(28)
CoExistence : update Feb 24 10:33:17 2009 ---(29)
: none

#
```

1) 管理機器定義番号

2) 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
- 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

3) 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。

- 4) 無線 LAN 端末接続数 (無線 LAN インタフェース全体)
- 5) 無線 LAN 端末の MAC アドレス
- 6) アソシエーション ID
- 7) 無線 LAN 端末の無線通信モード

- 11b** IEEE802.11b で動作
- 11g** IEEE802.11g で動作
- 11a** IEEE802.11a で動作
- 11g/n** IEEE802.11g/n(2.4GHz 帯域) で動作
- 11a/n** IEEE802.11a/n(5GHz 帯域) で動作

8) 無線レート (bps)

9) 受信信号強度

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) - 95	SR-M20AP2 SR-M20AP1

10) 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で表示します。

- WPA、WPA2 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

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

- 11) 認証状態
- 12) VID
VLAN ID
- 13) 無通信時間
- 14) 省電力状態
数値 バッファ中パケット数 (詳細表示時は、バッファ最大数も表示)
active 非省電力状態
- 15) WMM 使用可否
- 16) 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。
- 17) 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。
- 18) 無線 LAN 端末接続数 (無線 LAN モジュール全体)
- 19) 接続時刻
- 20) 送信シーケンス番号
WMM 使用端末の場合は、TID ごと (左から 0~7) に表示
- 21) 受信シーケンス番号
WMM 使用端末の場合は、TID ごと (左から 0~7) に表示
- 22) Capability Information field を表示
 - ESS
 - IBSS
 - CF_POLLABLE
 - CF_POLLREQ
 - PRIVACY
 - SHORT_PREAMBLE
 - PBCC
 - CHANNEL_AGILITY
 - SHORT_SLOTTIME

-
- RSN
 - DSSS_OFDM
- 23) ERP information Element を表示 (11g,11b/g)
- -
 - NonERP Present
 - Use Protection
 - Barker Preamble Mode
- 24) WPA 使用可否
- 25) WPA2 使用可否
- 26) MIMO Power Save 状態を表示
- disable** 無効状態
 - static** スタティック動作
 - dynamic** ダイナミック動作
- 27) 無線 LAN 端末より受信した HT Capability Element 情報を表示
- -: 未受信、または表示項目なし
 - CHANNEL_WIDTH(40) : 20/40MHz 帯域幅をサポート
 - HT_GREENFIELD : グリーンフィールドフォーマットをサポート
 - SHORT_GI(20MHz) : 20MHz 帯域のショートガードインターバルをサポート
 - SHORT_GI(40MHz) : 40MHz 帯域のショートガードインターバルをサポート
 - HT_DELAYED_BLOCKACK : HT Delayed Block Ack をサポート
 - AMSDU_LENGTH(7935) : A-MSDU 最大長として、7935 オクテットを示す
 - AMPDU_SPACE(1/4us) : A-MPDU 最小間隔として、250 ナノ秒を示す
 - AMPDU_SPACE(1/2us) : A-MPDU 最小間隔として、500 ナノ秒を示す
 - AMPDU_SPACE(1us) : A-MPDU 最小間隔として、1000 ナノ秒を示す
 - AMPDU_SPACE(2us) : A-MPDU 最小間隔として、2000 ナノ秒を示す
 - AMPDU_SPACE(4us) : A-MPDU 最小間隔として、4000 ナノ秒を示す
 - AMPDU_SPACE(8us) : A-MPDU 最小間隔として、8000 ナノ秒を示す
 - AMPDU_SPACE(16us) : A-MPDU 最小間隔として、16000 ナノ秒を示す
- 28) 無線 LAN 端末より受信した HT Capability Element の Supported MCS Set Field 情報を表示
- 29) 20/40MHzBSS 共存機能が検出した、20/40MHzBSS 禁止事象
- update** 更新日時
 - none** 未検出
 - 40MHz Intolerant** 40MHz 動作の不寛容
 - 20MHz BSS Request** 20MHz BSS での運用要求
 - Intolerant channel** 20/40MHz BSS 不可のチャンネルを検出した

40.1.11 show nodemanager logging wlan sta rssi

[機能]

無線 LAN 端末の RSSI 最大値/最小値の一覧表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

```
show nodemanager logging wlan sta rssi [{node <node_number> | group <group_number>}]
```

[オプション]

なし

すべての無線 LAN アクセスポイントを対象とします。

<node_number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<group_number>

- グループ定義番号
管理グループの通し番号を 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]

無線 LAN 端末の RSSI 最大値と RSSI 最小値の一覧を表示します。
パラメタの省略時は、全無線 LAN アクセスポイントの情報を表示します。
group <group_number> 指定時は、指定グループの情報を表示します。
node <node_number> 指定時は、指定された無線 LAN アクセスポイントの情報を表示します。
RSSI と信号強度 (dBm) 関係は、以下のとおりです。

$$\text{dBm} = (\text{RSSI 値}) - 95$$

[注意]

無線 LAN 端末の RSSI 最大値/最小値一覧を表示するためには、「無線 LAN 端末の情報取得設定」を enable に設定しておく必要があります。

[実行例]

```
# show nodemanager logging wlan sta rssi
Node      Grp  MAX  MAC              WLAN  MIN  MAC              WLAN
-----
(1)      (2) (3) (4)              (5)  (6) (7)              (8)
0:AP_A01  0  55  00:00:0e:f5:43:c1  1  47  00:00:0e:f5:43:c3  16
1:AP_A02  0  50  00:00:0e:f5:43:c5  1  40  00:00:0e:f5:43:c8  1
2:AP_A03  0  55  00:00:0e:f5:43:c9  12 38  00:00:0e:f5:43:ca  3
3:AP_A04  0  53  00:00:0e:f5:43:cf  9  44  00:00:0e:f5:43:cc  9
#
```

- 1) 管理機器定義番号:無線 LAN アクセスポイント名

-
- 2) グループ定義番号
 - 3) RSSI 最大値
無線 LAN 端末の RSSI 最大値が表示されます。
 - 4) RSSI 最大値の無線 LAN 端末 MAC アドレス
 - 5) RSSI 最大値の無線 LAN 端末の接続先 WLAN 番号
 - 6) RSSI 最小値
無線 LAN 端末の RSSI 最小値が表示されます。
 - 7) RSSI 最小値の無線 LAN 端末 MAC アドレス
 - 8) RSSI 最小値の無線 LAN 端末の接続先 WLAN 番号

40.1.12 show nodemanager logging wlan reject

[機能]

接続拒否の無線 LAN 端末情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

```
show nodemanager logging wlan reject [sta <mac>] [{node <node_number> | group
<group_number>}]
```

[オプション]

<mac>

なし

すべての無線 LAN 端末の MAC アドレスを対象とします。

<mac>

- MAC アドレス
対象とする無線 LAN 端末の 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。

node <node_number> | group <group_number>

なし

すべての無線 LAN アクセスポイントを対象とします。

<node_number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<group_number>

- グループ定義番号
管理グループの通し番号を 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]

接続拒否となった無線 LAN 端末の情報を表示します。
パラメタの省略時は、全無線 LAN アクセスポイントの情報を表示します。
node <node_number> 指定時は、指定された無線 LAN アクセスポイントの情報を表示します。
group <group_number> 指定時は、指定グループの情報を表示します。

[メッセージ]

```
Unable to get STA reject data from node:<number>.
```

管理機器 <number> から、接続拒否情報を取得できませんでした。

[実行例]

```
# show nodemanager logging wlan reject node 0
[node:0]
---(1)---
[0001] Mar 02 06:28:40 2009: wlan 1 00:16:e3:00:00:02 DEAUTH: MIC Error
-(2)-- -----(3)----- -(4)-- -----(5)----- -(6)-- ----(7)----
[0002] Mar 02 06:28:41 2009: wlan 10 00:16:e3:00:00:03 REJECT: auth mode mismatch
h shared:wpa

#
```

- 1) 管理機器定義番号
- 2) ログの出力行番号
- 3) 接続を拒否した時刻
- 4) 無線 LAN インタフェース番号
- 5) 接続を拒否した端末の MAC アドレス
- 6) 拒否種別

REJECT 接続時の拒否

DEAUTH

接続後の拒否 (Deauthentication 送信)

DISASSOC

接続後の拒否 (Disassociation 送信)

- 7) 詳細情報

拒否種別	詳細情報	拒否理由
REJECT	unsupported algo=<algo> <algo> 端末が提示した認証方式値	サポートしていない認証方式で認証要求された
REJECT	auth mode mismatch <auth_model>:<auth_mode2> <auth_model> 端末が提示した認証方式 ・ open オープン認証 ・ shared SHARED認証 <auth_mode2> 期待する認証方式 ・ open オープン認証 ・ shared SHARED認証 ・ wpa WPAまたはWPA2 ・ wep off オープン認証(暗号化なし)	利用できない認証方式で認証要求された
REJECT	shared key authentication failed	SHARED認証に失敗した
REJECT	AP in countermeasures state	TKIP MICエラー検出による接続拒否中に接続要求を受信した
REJECT	dot1x authentication denied	IEEE802.1X認証で拒否した
REJECT	retry over in Authenticating state	IEEE802.1X認証中に再送タイムアウトが発生した

(続く)

(続き)

拒否種別	詳細情報	拒否理由
REJECT	not received PMK information	認証サーバから鍵情報が通知されなかった
REJECT	dot1x VLAN registration failed	ポートへのVLAN登録に失敗した
REJECT	over dot1x supplicant limit	収容可能なsupplicant数を超過して認証要求を受信した
DEAUTH	received log-off <state> <state> log-off受信時の認証状態 <ul style="list-style-type: none"> • in Connecting state 認証開始時 • in Authenticating state 認証中 • in Authenticated state 認証完了後 	supplicantからログオフ要求を受信した
DEAUTH	retry over in Connecting state	IEEE802.1x認証開始時に再送タイムアウトが発生した
DEAUTH	MIC ERROR was detected	TKIP MICエラーを60秒間に2回以上検出した
DEAUTH	cannot handshake by retry over for <state> <state> 鍵交換失敗時の状態 <ul style="list-style-type: none"> • PTK in 2/4 PTK交換(4-way handshake)の最初の応答受信待ち • PTK in 4/4 PTK交換(4-way handshake)の3つ目の応答受信待ち • GTK in 2/2 GTK交換(2-way handshake)の応答受信待ち 	鍵交換処理中にリトライサーバにより鍵交換が失敗した
DEAUTH	EAPOL-Key msg 2/4 mismatch WPA IE	STAが本装置と接続したときのプロトコルパラメタと異なるパラメタが設定されたEAPOL-Keyを受信した
DEAUTH	deauthenticated by wlanctl command	制御コマンド(wlanctl)により強制切断した
DEAUTH	link error or reconfiguration	<ul style="list-style-type: none"> • 構成定義変更により強制切断した • 制御コマンド(dot1xctl)により認証を初期化した • インタフェースダウンが発生した
REJECT	macauth authentication denied	MACアドレス認証で拒否した
REJECT/ DEAUTH	macauth authentication failed	MACアドレス認証に失敗した(認証サーバからの失敗通知)
REJECT/ DEAUTH	lack of authentication resource	MACアドレス認証に失敗した(認証資源枯渇)
REJECT	macauth reached max terminals	MACアドレス認証の最大同時認証端末数まで達した
REJECT/ DEAUTH	macauth reached max failure terminals	MACアドレス認証の失敗保持端末数が最大まで達した
REJECT/ DEAUTH	macauth VLAN registration failed	ポートへのVLAN登録に失敗した

40.1.13 show nodemanager logging wlan trace

[機能]

無線 LAN 通信のトレース情報の表示

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

```
show nodemanager logging wlan trace [sta <mac>] [{node <node_number> | group  
<group_number>}]
```

[オプション]

<mac>

なし

すべての無線 LAN 端末の MAC アドレスを対象とします。

<mac>

- MAC アドレス
対象とする無線 LAN 端末の 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。

node <node_number> | group <group_number>

なし

すべての無線 LAN アクセスポイントを対象とします。

<node_number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<group_number>

- グループ定義番号
管理グループの通し番号を 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]

無線 LAN 通信のトレース情報を表示します。
パラメタの省略時は、全無線 LAN アクセスポイントの情報を表示します。
node <node_number> 指定時は、指定された無線 LAN アクセスポイントの情報を表示します。
group <group_number> 指定時は、指定グループの情報を表示します。

[メッセージ]

```
Unable to get STA trace data from node:<number>.
```

管理機器 <number> から、無線 LAN 通信のトレース情報を取得できませんでした。

[実行例]

```
# show nodemanager logging wlan trace node 2
[node:2]
---(1)---
[0001] Mar 02 06:28:40 2009: wlan 1 00:16:e3:00:00:02 RX ASSOC_REQ: fc=0x0101
-(2)-- -----(3)----- -(4)-- -----(5)----- (6) ---(7)--- ----(8)---
dur=0x0101 seq=10
-----
[0002] Mar 02 06:28:41 2009: wlan 1 00:16:e3:00:00:03 TX ASSOC_RESP: fc=0x0101
dur=0x0101 seq=10 status=0 aid=10
[0003] Mar 02 06:28:42 2009: wlan 1 00:16:e3:00:00:03 RX ACTION: fc=0x0101 dur
=0x0101 seq=10 category=1 action=0

#
```

- 1) 管理機器定義番号
- 2) ログの出力行番号
- 3) トレースを取得した時刻
- 4) 無線 LAN インタフェース番号
- 5) 送信元・送信先の無線 LAN 端末 MAC アドレス
- 6) 送受信

TX 送信

RX 受信

- 7) 種別

ASSOC_REQ

Association Request

ASSOC_RESP

Association Response

REASSOC_REQ

Reassociation Request

REASSOC_RESP

Reassociation Response

DISASSOC

Disassociation

AUTH Authentication

DEAUTH

Deauthentication

ACTION

Action

EAP_REQUEST

EAP-Request

EAP_RESPONSE

EAP-Response

EAP_SUCCESS

EAP-Success

EAP_FAILURE

EAP-Failure

EAPOL_START

EAPOL-Start

EAPOL_LOGOFF

EAPOL-Logoff

EAPOL_KEY

EAPOL-Key

EAPOL_ASF_ALERT

EAPOL-Encapsulated-ASF-Alert

RAD_ACCS_REQ

RADIUS (AAA) への Access-Request

RAD_ACCS_CHAL

RADIUS (AAA) からの Access-Challenge

RAD_ACCS_ACCEPT

RADIUS (AAA) からの Access-Accept

RAD_ACCS_FAIL

RADIUS (AAA) からの Access-Reject or Accept(NG) or Challenge(NG)

RAD_ACCT_REQ

RADIUS (AAA) への Accounting Request

8) 詳細情報

第 41 章 ポート制御コマンド

41.1 ポート制御

41.1.1 offline

[機能]

切断、または閉塞の実施

[適用機種]

SR-M20AP2	SR-M20AP1	SR-M20AC2	SR-M20AC1
-----------	-----------	-----------	-----------

[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-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

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 ~ 16	SR-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

[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>]

41.1.2 online

[機能]

接続、または閉塞解除の実施

[適用機種]

SR-M20AP2	SR-M20AP1	SR-M20AC2	SR-M20AC1
-----------	-----------	-----------	-----------

[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-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

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 ~ 16	SR-M20AP2 SR-M20AP1
1	SR-M20AC2 SR-M20AC1

[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 42 章 無線 LAN 制御コマンド

42.1 無線 LAN 制御

42.1.1 wlanctl authenticator disconnect

[機能]

無線 LAN 接続端末 (STA) の切断

[適用機種]

SR-M20AP2 SR-M20AP1

[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。

<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]

WPA,WPA2,IEEE802.1X 認証、または事前共有キー (PSK) 認証を使用している無線 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.
```

以下のどちらかの場合に表示されます。

- オープン認証、共通鍵認証が設定され IEEE802.1X 認証が使用されていない無線 LAN インタフェースを指定した場合
- 指定された端末が接続されていない場合

[実行例]

```
# wlanctl authenticator disconnect 1 00:00:0e:12:34:56
#
```

第 43 章 USB ポート制御コマンド

43.1 USB ポート 制御

43.1.1 usbctl

[機能]

USB ポートの閉塞、または閉塞解除の実施

[適用機種]

SR-M20AP2	SR-M20AP1		
-----------	-----------	--	--

[入力形式]

usbctl <mode>

[オプション]

<mode>

- enable
USB ポートの閉塞状態を解除します。
- disable
USB ポートを閉塞状態にします。

[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]

USB ポートの閉塞 / 閉塞解除制御を行います。

閉塞解除時には、過電流を検出している状態の場合に、給電再開、および過電流検出状態をクリアします。

閉塞時には、給電を停止するため、USB メモリ取り付け状態でも、USB メモリが取り外されたように見えます。

[実行例]

```
# usbctl enable
#
```

第 44 章 IEEE802.1X 制御コマンド

44.1 IEEE802.1X 制御

44.1.1 dot1xctl initialize

[機能]

IEEE802.1X 認証状態の初期化

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

- ether
ether ポート
SR-M20AP2/20AP1 の場合、指定できません。
- wlan
無線 LAN インタフェース
SR-M20AC2/20AC1 の場合、指定できません。

<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  
#
```

44.1.2 dot1xctl reconfirm

[機能]

IEEE802.1X 再認証の実行

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

- ether
ether ポート
SR-M20AP2/20AP1 の場合、指定できません。
- wlan
無線 LAN インタフェース
SR-M20AC2/20AC1 の場合、指定できません。

<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 (Supplicant) が切断されてしまう場合があります。

[実行例]

```
# dot1xctl reconfirm port wlan 1  
#
```


44.1.3 dot1xctl backup recovery

[機能]

認証自動切替状態の復旧

[適用機種]

SR-M20AP2	SR-M20AP1		
-----------	-----------	--	--

[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 45 章 MAC アドレス認証制御コマンド

45.1 MAC アドレス認証制御

45.1.1 macauthctl initialize

[機能]

MAC アドレス認証状態の解除

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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。

- ether
ether ポート
SR-M20AP2/20AP1 の場合、指定できません。
- wlan
無線 LAN インタフェース
SR-M20AC2/20AC1 の場合、指定できません。

<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 ether 1  
#
```

第 46 章 RADIUS 制御コマンド

46.1 RADIUS 制御

46.1.1 radius recovery

[機能]

RADIUS サーバの復旧

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 47 章 証明書関連制御コマンド

47.1 証明書関連の制御

47.1.1 crypto certificate generate

[機能]

秘密鍵、証明書要求の設定

[適用機種]

 SR-M20AC2 SR-M20AC1

[入力形式]

crypto certificate generate

[オプション]

なし

対話形式で秘密鍵、証明書要求の設定を行います。

[動作モード]

構成定義モード (管理者クラス)

[説明]

秘密鍵、証明書要求の設定を行います。

コマンド実行後、指示に従い自装置の情報を:(コロンの)以降に入力してください。

秘密鍵と証明書要求は同じ識別番号で設定され、鍵ペアと判断されます。

本コマンドは運用管理コマンドですが、設定した内容は以下の構成定義コマンドとして設定されます。

秘密鍵 : certificate private line

証明書要求
: certificate request line

設定した内容は save コマンドを実行することで構成定義情報として保存することができます。

また、定義反映を行う場合は、commit コマンドまたは save コマンド実行後に reset コマンドを行ってください。

[注意]

すでに"crypto certificate generate"コマンド、"crypto certificate local"コマンドで設定を行っている場合は以前と違う情報で上書きされます。

本コマンドで定義した内容は、以下の構成定義情報を delete コマンドで削除できます。

秘密鍵 : certificate private line

証明書要求
: certificate request line

[実行例]

(1) 秘密鍵、証明書要求の設定を行う場合

:(コロン) より後ろの部分を入力します

```
(config)# crypto certificate generate
RSA key pair number[0-4] :0
generate RSA key pair.
Are you sure?[y/n] :y
RSA key pair and Certificate request will be overwritten. (上書きすることを通知するメッセージ
Are you sure?[y/n] :y                                     は鍵ペアが未設定の場合は表示されません)
key bit(512-2048) :1024
certificate request hash(sha1 or md5) :sha1
Country Name(2 letter code) :JP
State or Province Name :Kanagawa
Locality Name :Kawasaki
Organization Name :Fujitsu Limited
Organizational Unit Name :Tech Div.
Common Name :shisya.fujitsu.com
Email Address :hoge@fujitsu.com
Please wait to create RSA private key and Certificate request.
certificate private 0 line 0 HABNg39no/6PrWicHYI2Ambcsqbwvcr8d03hsDstuY8MrRKghUF20fCP7FxV2qC1S
nTnboIjjha3bPcJc18RaddXs3UsG
certificate private 0 line 1 U@GVXBb3qUablFzippI/G7RzvQIoIdVko7D3UyPqyzSmhXprLJfCkUbIro/UGy5k
qCfQlyJtEvBElrN69StqUqk0qxn
certificate private 0 line 2 8/6xVM07inyDX5uY7lPgSMEI10WpPG7UXYXG/xD3bbi3qOY@whH15nAKdqMivVx8
HJzVcNCdNpGg8@ty360s@rWYqas
certificate private 0 line 3 xaXDBs9Y5n0KZwSb96WZhS8vBtZs1dzhATnWvaejIXyFYdgAhPYP1rMdqBNyuBhoT
CSglN2vXZNvwXN3a0IInBWrBNW
certificate private 0 line 4 OjLsXNgMwc8cgTCwOZL6dWrKGU3qtnjTpYzsvHVVUCtPhb9yEwq0M2rTU/eX@77lu
kOmPXy5XrqipSbwfgrdHOus3
certificate private 0 line 5 700AlBhmaYN7rlbaLSmzrQD07s2QDNvwi87dHypF4KC8BP0HwemUYQxq32vijbQ@
qlIOflH4YKB5LvAXJeJ4qRa@IA
certificate private 0 line 6 FKjaEBaCl0NTGk9nMdluE@2/DvoXtIzqNo90o6NUN/5oz/qxpLaHzshl9@oKCL8e
0dMoYRy7gOeeQI2oU1DrF6iHdDY
certificate private 0 line 7 HFZBzMEtC9NMqEGqFlEY@edgfRo1IAM9qa3/ip2HBgcUHZHqNVgSePHeBdtrikubN
KWC@wSmZ3AdJ/@rzClhXhBrg6j
certificate private 0 line 8 bo2HYUZA6hvPtZpECC21pTYH8i401AkqhlkiK0QXS4P3gCMMIaPMN51zMQ@QFX8jq
flSP0eRMwjFscD/TVRPTlyNAtOG
certificate private 0 line 9 8ocM49xUiyGyibznxgZnWnsZOYy8i8GXMkb6VKBGog22TfTfmona4D1wz464IYfMPw
kw6rq/9eYqW7lHXB4jJDRULC/UK
certificate private 0 line 10 TyyPu9KD5xY0wKGLYBbdZc60aVT445YpewrHiAuolDpd6FcPZULLj@wa7gHuOA/7
Vzpu7VQhaXJzlxzdDOT2iRQT97MVQ
certificate private 0 line 11 2XH/r4JKRiZpn5LP4/Hr5uwZDQG5h21fEdvVp80bKbL4a81/1Pt0cfMXoA7IbC8
Mrc0ZkMxGGkVOeMqlC2Bgt5YE1
certificate private 0 line 12 ei9ZnNGLgtXJrrXWq4zk9tuzH@0ZXe0INO0uAgVH5ktLiTOX2gsSz2fRq2D4Q6
hi
certificate request 0 line 0 MIICMCCA ZkCAQAwgZ8xCzAJBgNVBAYTAkpMRwEwDwYDVQQIEWhLYW5hZ2Z3YTER
certificate request 0 line 1 MA8GAlUEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Zlaml0c3UgTGltaXRlZDESMBAG
certificate request 0 line 2 AlUECxmJVGvjaCBEaXYuMRswGQYDVQDEExJzaGlzeWEuZnVqaXRzdS5jb20xHzAd
certificate request 0 line 3 BgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
certificate request 0 line 4 gY0AMIGJAoGBAMk7Bq9Ciaxhl7fYIkwbRLI64EAjP1RnDrEnLj/ds9ErIoT4sPbc
certificate request 0 line 5 Z9a0mvdz0nr1K8HmNmDGMo1DRuFBWueSvs9Qgl0zykQu+R3YKPMNMJ3gLO6tiNkl
certificate request 0 line 6 6TtNNUAK+OGda0brLL6t6+jE/UlKskjt7UzdHlan1AroLkLtkrVqcBPjAgMBAAGg
certificate request 0 line 7 UDBoBgkqhkiG9w0BCQ4xQTA/MASGAlUdDwQEAwIChDAPBgNVHREECDAghwTAqAEB
certificate request 0 line 8 MB8GAlUdeQQYMBaCFHN0aXN5S1hLmZlaml0c3UuY29tMA0GCSqGSIb3DQEBBQUA
certificate request 0 line 9 A4GBACRKhb8x8k108Jf7w9YNgzHN+ORyY2sIrhqpytSquNonvcZzaEgVeqyqUqQ
certificate request 0 line 10 WOIQhgGINKSRW82odtTFi97TgalYijj5GeaVCLaSe6FH91LhcLlArY2dArRYM/x
certificate request 0 line 11 Zv62xudPCLvwe+w49N8gA+Dq+9G3wCSYA0kFQNJmm/HIPUnb
Created RSA private key and Certificate request.
(config)#
```


自装置の情報

```

RSA key pair number[0-4] :
-----
(1)
key bit(512-2048) :
-----
(2)
certificate request hash(sha1 or md5) :
-----
(3)
Country Name(2 letter code) :
-----
(4)
State or Province Name :
-----
(5)
Locality Name :
-----
(6)
Organization Name :
-----
(7)
Organizational Unit Name :
-----
(8)
Common Name :
-----
(9)
Email Address :
-----
(10)

```

- 1) 鍵ペアの識別番号
鍵ペアの識別番号を 0~4 の 10 進数で指定します。
- 2) 鍵長
鍵長 (bit) を 512~2048 の 10 進数で指定します。
- 3) 証明書要求で使用するハッシュアルゴリズム
ハッシュアルゴリズムを指定します。
 - sha1** ハッシュアルゴリズムとして SHA1 を使用します。
 - md5** ハッシュアルゴリズムとして MD5 を使用します。
- 4) 国 (C)
0x21,0x23~0x7e の 2 文字の ASCII 文字列で指定します。
- 5) 都道府県 (ST)
0x22(ダブルクォーテーション) と 0x2f(スラッシュ) を除く [0x20-0x7e] の範囲のコードで構成される 64 文字以内の ASCII 文字列で指定します。
- 6) 市区町村 (L)
0x22(ダブルクォーテーション) と 0x2f(スラッシュ) を除く [0x20-0x7e] の範囲のコードで構成される 64 文字以内の ASCII 文字列で指定します。
- 7) 組織または会社 (O)
0x22(ダブルクォーテーション) と 0x2f(スラッシュ) を除く [0x20-0x7e] の範囲のコードで構成される 64 文字以内の ASCII 文字列で指定します。
- 8) 組織ユニットまたは部門 (OU)
0x22(ダブルクォーテーション) と 0x2f(スラッシュ) を除く [0x20-0x7e] の範囲のコードで構成される 64 文字以内の ASCII 文字列で指定します。
- 9) ホスト名 (CN)
0x22(ダブルクォーテーション) と 0x2f(スラッシュ) を除く [0x20-0x7e] の範囲のコードで構成される 64 文字以内の ASCII 文字列で指定します。

10) E メールアドレス

0x21,0x23 ~ 0x7e の 64 文字以内の ASCII 文字列で指定します。

47.1.2 crypto certificate local

[機能]

自装置証明書の取り込み

[適用機種]



[入力形式]

crypto certificate local <number> name <name>

[オプション]

<number>

自装置証明書識別番号を指定します。

- 自装置証明書識別番号
自装置証明書の識別番号を、0~4 の 10 進数で指定します。

name <name>

自装置証明書識別名を指定します。

- 自装置証明書識別名
0x21,0x23 ~ 0x7e の 16 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]

自装置証明書を取り込みます。

証明書の入力は Base64 形式で行い、開始行と終了行には以下の文字列を指定してください。

開始行 : `---BEGIN CERTIFICATE---`

終了行 : `---END CERTIFICATE---`

証明書の取り込みは開始と終了の行を除いた、100 行までで指定してください。

自装置証明書の設定が行われると以下の構成定義が設定されます。

自装置証明書

: certificate local name

certificate local line

設定した内容は save コマンドを実行することで構成定義情報として保存することができます。

また、定義反映を行う場合は、commit コマンドまたは save コマンド実行後に reset コマンドを行ってください。

[注意]

すでに<number>で指定した"crypto certificate generate"コマンド、"crypto certificate local"コマンドで設定を行っている場合は上書きされます。

取り込んだ自装置証明書情報が証明書として有効でない場合は構成定義の設定は行いません。

本コマンドで定義した内容は、以下の構成定義情報を delete コマンドで削除できます。

自装置証明書

: certificate local name

certificate local line

[実行例]

```
(config)# crypto certificate local 0 name mycert
Please input.
-----BEGIN CERTIFICATE-----
MIIDBjCCAm8CAQEWdQYJKoZIhvcNAQEFBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Zlaml0
c3UgTGltaxRlZDESMBAGALUECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJzaGlzeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDcwNzIwMDIwNzU4WhcNMDCxMjMxMDIwNzU4WjCBnzELMAkGA1UEBHMCSlAxETAP
BgNVBAGTCethbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaWlpdGVkMRlWEAYDVQQLLEw1UZWN0IERpdj4xGzAZBgNVBAMTEhNoaXN5
YS5mdWppdHNIbMnVbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHNIbMnVbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCyYEAyTsGrOKJrGHXt9giTBtEsjrgQCM/
VGcOsScsn92z0SsihPiw8Fxn1rSa93PSdGUrweY2YMYyJUNG58Fa55K+z1CCXTPK
RC75Hdgo8w0wneAvTq2I2SXp0001QAr44Z1rRusssvq3r6MT9TUqyS03tTN0fVqfU
CuguQu2StWpWE+MCAwEAAAANVMFMwCwYDVR0PBAQDAGKEMA8GA1UdEQQIMAaHBMCo
AQEWHwYDVR0RBGgwFoIUC2hpc3lhLWUeZnVqaXRzdS5jb20wEgYDVR0TAQH/BAGw
BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UzbzXOVYN4RZ6zcbpn7YCwv/y7
oSR5ppTcZz1VCgWNYFQIz1/MCNv1yGk9at8S01QgM5zi0bXypD0p1OB3Ust0mzGx
3i3jsVuKJKbn0qsysUZQEpMFS7JdYHuIRN5nWPBjqH68CqQD8zPeJ21VcwcsUohF
FKA8mr9msEiVNQ==
-----END CERTIFICATE-----
certificate local 0 name mycert
certificate local 0 line 0 MIIDBjCCAm8CAQEWdQYJKoZIhvcNAQEFBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate local 0 line 1 VQQIEWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Zlaml0
certificate local 0 line 2 c3UgTGltaxRlZDESMBAGALUECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJzaGlzeWEu
certificate local 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate local 0 line 4 MDcwNzIwMDIwNzU4WhcNMDCxMjMxMDIwNzU4WjCBnzELMAkGA1UEBHMCSlAxETAP
certificate local 0 line 5 BgNVBAGTCethbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate local 0 line 6 aXRzdSBMaWlpdGVkMRlWEAYDVQQLLEw1UZWN0IERpdj4xGzAZBgNVBAMTEhNoaXN5
certificate local 0 line 7 YS5mdWppdHNIbMnVbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHNIbMnVbTCB
certificate local 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCyYEAyTsGrOKJrGHXt9giTBtEsjrgQCM/
certificate local 0 line 9 VGcOsScsn92z0SsihPiw8Fxn1rSa93PSdGUrweY2YMYyJUNG58Fa55K+z1CCXTPK
certificate local 0 line 10 RC75Hdgo8w0wneAvTq2I2SXp0001QAr44Z1rRusssvq3r6MT9TUqyS03tTN0fVqfU
certificate local 0 line 11 CuguQu2StWpWE+MCAwEAAAANVMFMwCwYDVR0PBAQDAGKEMA8GA1UdEQQIMAaHBMCo
certificate local 0 line 12 AQEWHwYDVR0RBGgwFoIUC2hpc3lhLWUeZnVqaXRzdS5jb20wEgYDVR0TAQH/BAGw
certificate local 0 line 13 BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UzbzXOVYN4RZ6zcbpn7YCwv/y7
certificate local 0 line 14 oSR5ppTcZz1VCgWNYFQIz1/MCNv1yGk9at8S01QgM5zi0bXypD0p1OB3Ust0mzGx
certificate local 0 line 15 3i3jsVuKJKbn0qsysUZQEpMFS7JdYHuIRN5nWPBjqH68CqQD8zPeJ21VcwcsUohF
certificate local 0 line 16 FKA8mr9msEiVNQ==
(config)#
```

47.1.3 crypto certificate ca

[機能]

認証局証明書の取り込み

[適用機種]



[入力形式]

crypto certificate ca <number> name <name>

[オプション]

<number>

認証局証明書識別番号を指定します。

- 認証局証明書識別番号
認証局証明書の識別番号を、0~4 の 10 進数で指定します。

name <name>

認証局証明書識別名を指定します。

- 認証局証明書識別名
0x21,0x23~0x7e の 16 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]

認証局証明書を取り込みます。

証明書の入力は Base64 形式で行い、開始行と終了行には以下の文字列を指定してください。

開始行 : ---BEGIN CERTIFICATE---

終了行 : ---END CERTIFICATE---

認証局証明書の取り込みは開始と終了の行を除いた、100 行までで指定してください。

認証局証明書の設定が行われると以下の構成定義が設定されます。

認証局証明書

: certificate ca name

certificate ca line

設定した内容は save コマンドを実行することで構成定義情報として保存することができます。

また、定義反映を行う場合は、commit コマンドまたは save コマンド実行後に reset コマンドを行ってください。

[注意]

すでに<number>で指定した認証局証明書識別番号に"crypto certificate ca"コマンドで設定を行っている場合は上書きされます。

取り込んだ認証局証明書情報が証明書として有効でない場合は構成定義の設定は行いません。

本コマンドで定義した内容は、以下の構成定義情報を delete コマンドで削除できます。

認証局証明書

: certificate ca name

certificate ca line

[実行例]

```
(config)# crypto certificate ca 0 name cacert
Please input.
-----BEGIN CERTIFICATE-----
MIIDBjCCAm8CAQEWdQYJKoZIhvcNAQEFBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1am10
c3UgTGltaxRlZDESMBAGAlUECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJzaGlzeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDCwNzIwMDIwNzU4WhcNMDCxMjMxMDIwNzU4WjCBnzELMAkGA1UEBhMCSlAxETAP
BgNVBAGTCEthbMFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMFRnVq
aXRzdSBMaW1pdGVkMRlWEAYDVQQLLEw1UZWN0IERpdj4xGzAZBgNVBAMTElNoaXN5
YS5mdWppdHNIbMnVbTEfMBOGCSqGSIb3DQEJARYQaG9nZUBmdWppdHNIbMnVbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCyYEAyTsGr0KJrGHXt9giTBTESjrgQCM/
VGcOsScsn92z0SsihPw8Fxn1rSa93PSdGUrweY2YMYyJUNG58Fa55K+z1CCXTPK
RC75Hdgo8w0wneAvTq2I2SXp0001QAr44Z1rRussvq3r6MT9TUqySO3tTN0fVqfU
CuguQu2StWpWE+MCAwEAAANVMFMwCwYDVR0PBAQDAGKEMA8GA1UdEQQIMAaHBMCo
AQEWHwYDVR0RBGwFoIUC2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAgw
BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UzbXOVYN4RZ6zcbpn7YCwv/y7
oSR5ppTcZz1VCgWNYFQIz1/MCNv1yGk9at8S01QgM5zi0bXypD0p10B3Ust0mzGx
3i3jsVuKJKbn0qsysUZQEPMFS7JdYHuIRN5nWPBjqH68CqQD8zPeJ21VcwcsUohF
FKA8mr9msEiVNQ==
-----END CERTIFICATE-----
certificate ca 0 name cacert
certificate ca 0 line 0 MIIDBjCCAm8CAQEWdQYJKoZIhvcNAQEFBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate ca 0 line 1 VQQIEWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1am10
certificate ca 0 line 2 c3UgTGltaxRlZDESMBAGAlUECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJzaGlzeWEu
certificate ca 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate ca 0 line 4 MDCwNzIwMDIwNzU4WhcNMDCxMjMxMDIwNzU4WjCBnzELMAkGA1UEBhMCSlAxETAP
certificate ca 0 line 5 BgNVBAGTCEthbMFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMFRnVq
certificate ca 0 line 6 aXRzdSBMaW1pdGVkMRlWEAYDVQQLLEw1UZWN0IERpdj4xGzAZBgNVBAMTElNoaXN5
certificate ca 0 line 7 YS5mdWppdHNIbMnVbTEfMBOGCSqGSIb3DQEJARYQaG9nZUBmdWppdHNIbMnVbTCB
certificate ca 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCyYEAyTsGr0KJrGHXt9giTBTESjrgQCM/
certificate ca 0 line 9 VGcOsScsn92z0SsihPw8Fxn1rSa93PSdGUrweY2YMYyJUNG58Fa55K+z1CCXTPK
certificate ca 0 line 10 RC75Hdgo8w0wneAvTq2I2SXp0001QAr44Z1rRussvq3r6MT9TUqySO3tTN0fVqfU
certificate ca 0 line 11 CuguQu2StWpWE+MCAwEAAANVMFMwCwYDVR0PBAQDAGKEMA8GA1UdEQQIMAaHBMCo
certificate ca 0 line 12 AQEWHwYDVR0RBGwFoIUC2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAgw
certificate ca 0 line 13 BgEB/wIBATANBgkqhkiG9w0BAQUFAAOBgQBcPN+UzbXOVYN4RZ6zcbpn7YCwv/y7
certificate ca 0 line 14 oSR5ppTcZz1VCgWNYFQIz1/MCNv1yGk9at8S01QgM5zi0bXypD0p10B3Ust0mzGx
certificate ca 0 line 15 3i3jsVuKJKbn0qsysUZQEPMFS7JdYHuIRN5nWPBjqH68CqQD8zPeJ21VcwcsUohF
certificate ca 0 line 16 FKA8mr9msEiVNQ==
(config)#
```

第 48 章 管理機器制御コマンド

- MAC アドレスフィルタセット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 <set_num> (MAC アドレスフィルタセット定義番号) に指定する MAC アドレスフィルタセットの通し番号 (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 ~ 4	SR-M20AP2 SR-M20AP1

- 管理機器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 <node_number> (管理機器定義番号) に指定する管理機器の通し番号 (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 ~ 4	SR-M20AP2 SR-M20AP1

- グループ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 <group_number> (グループ定義番号) 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 ~ 4	SR-M20AP2 SR-M20AP1

48.1 管理機器制御

48.1.1 nodemanagerctl update wlan filterset

[機能]

管理機器への MAC アドレスフィルタ配布

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

```
nodemanagerctl update wlan filterset <set_num> { node <node_number> | group  
<group_number> | all }
```

[オプション]

<set_num>

- MAC アドレスフィルタセット定義番号
MAC アドレスフィルタセットの番号を指定します。

<node_number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<group_number>

- グループ定義番号
管理グループの通し番号を 10 進数で指定します。

all

すべての管理機器へ MAC アドレスフィルタを配布します。

[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]

本装置中の MAC アドレスフィルタセットを元に、MAC アドレスベースのフィルタ設定を管理機器に配布します。

オプションに管理機器定義番号が指定された場合は、指定された管理機器のみが配布対象となります。

オプションにグループ定義番号が指定された場合は、指定された管理グループに所属する管理機器が配布対象となります。

オプションにすべての管理機器が指定された場合は、すべての管理機器が配布対象となります。

本コマンドでは、各管理機器で save,commit を行い MAC アドレスフィルタ情報を設定します。

[注意]

本機能は管理機器の ACL の 0~99 番を使用します。管理機器管理者が独自に 0~99 の ACL 番号に ACL を定義していた場合は、その設定は失われます。そのため管理機器独自の ACL は 99 番以降を用いる必要があります。

本機能は管理機器の MAC filter の 0~99 番を使用します。管理機器管理者が独自に 0~99 の filter 番号にフィルタを定義していた場合は、その設定は失われます。

[メッセージ]

```
<node_number>:管理機器名 <group_number>:グループ名 Start filterset updating.
```

管理機器 (<node_number>:管理機器名) の MAC アドレスフィルタの配布を開始しました。

```
Succeeded.
```

管理機器の MAC アドレスフィルタを配布しました。

```
Unable to update MAC base access control.
Failed.
```

管理機器の MAC アドレスフィルタを配布できませんでした。

```
The configuration data is not registered.
Failed.
```

管理機器の構成定義データが登録されていません。

[実行例]

```
# nodemanagerctl update wlan filterset 1 node all
Node      Group      Information
-----
(1)       (2)       (3)
0:ap0     0:group0   Start filterset updating.
          0:group0   Succeeded.

1:ap1     0:group0   Start filterset updating.
          0:group0   Succeeded.

2:ap2     0:group0   Start filterset updating.
          0:group0   Unable to update MAC base access control.
          0:group0   Failed.

3:ap3     0:group0   Start filterset updating.
          0:group0   The configuration data is not registered.
          0:group0   Failed.

#
```

- 1) 管理機器定義番号:無線 LAN アクセスポイント名
- 2) グループ定義番号:グループ名
- 3) 実行状況

48.1.2 nodemanagerctl wlan autotxpower

[機能]

管理機器の電波出力自動調整

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

```
nodemanagerctl wlan autotxpower {node <node_number> | group <group_number> | all}
```

[オプション]

<node_number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<group_number>

- グループ定義番号
管理グループの通し番号を 10 進数で指定します。

all

すべての管理機器の無線送信出力を自動で調整します。

[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]

オプションで指定された WLAN(または、すべての WLAN) の電波到達範囲が必要最小限になるように、無線送信出力を自動的に調整します。

電波出力自動調整機能を実行するには、近隣管理機器が以下の条件を満たす必要があります。

- 近隣管理機器が 1 つ以上登録してあること。
- 近隣管理機器で無線送信出力調整対象の管理機器と同じ無線 LAN モジュールが動作していること。
- 近隣管理機器の無線 LAN モジュールの動作タイプは、無線 LAN アクセスポイント、または、スキャン専用モードであること。

[注意]

自動調整の間は無線 LAN への端末接続が不安定になります。本機能は無線 LAN の本運用を行っていないときに使用してください。

自動調整後は管理機器の電波の到達範囲が狭くなる可能性があります。そのため、自動調整実施後は、無線 LAN 端末の接続確認を行うことを推奨します。

無線送信出力の調整は、電波自動調整の RSSI 最低しきい値の設定に近い値になるまで、以下の処理を繰り返すため時間がかかります。

- 1) 近隣の無線 LAN アクセスポイントでの周辺アクセスポイント情報の取得
必要時間：約 (60 秒 * 近隣の無線 LAN アクセスポイント台数)
- 2) 電波送信出力の確認
RSSI 最低しきい値に近い値であれば終了

- 3) 無線 LAN アクセスポイントの無線送信出力設定
必要時間：10 秒程度
- 4) 無線送信出力の安定待ち
必要時間：90 秒
- 5) 1) の処理から繰り返し

[メッセージ]

```
<node_number>:管理機器名 <group_number>:グループ名 Start txpower updating.
```

管理機器 (<node_number>:管理機器名) の無線送信出力の調整を開始しました。

```
Succeeded.
```

管理機器の無線送信出力の調整に成功しました。

```
The configuration data is not registered.  
Failed.
```

管理機器の構成定義データが登録されていません。

```
The node has not had identified MACs for wlan.  
Failed.
```

管理機器の無線 LAN の MAC アドレスが特定できていません。

```
The node has not modules consisted of AP type only.  
Failed.
```

管理機器の無線 LAN モジュールのタイプが AP のみではありません。

```
Configuration data for neighbor <node_numX> is not registered.  
Failed.
```

近隣管理機器<node_numX>の構成定義データが登録されていません。

```
The node does not have any neighbor nodes.  
Failed.
```

管理機器には、近隣管理機器が登録されていません。

```
Active data for neighbor <node_numX> is not gathered.  
Failed.
```

近隣管理機器<node_numX>の稼働情報が未収集です。

```
Modules of neighbor <node_numX> are not valid.  
Failed.
```

近隣管理機器<node_numX>の無線 LAN モジュールの構成が適切ではありません。

```
Check the current txpower:
  Unable to get current txpower.
Failed.
```

管理機器の無線送信出力を取り出すことができませんでした。

```
Check the state of modules of neighbors:
  neighbor<node_numX> ... Unable to get current txpower.
Failed.
```

近隣管理機器<node_numX>の無線送信出力を取り出すことができませんでした。

```
Check the state of modules of neighbors:
  neighbor<node_numX> ... NG
Failed.
```

近隣管理機器<node_numX>で、管理機器の調整対象と同じ無線モジュールが動作していません。

```
Scanning RSSI of modules of neighbors:
  neighbor<node_numX>: Unable to get RSSI.
Failed.
```

近隣管理機器<node_numX>で、無線 LAN のスキャンに失敗しました。

[実行例]

```
# nodemanagerctl wlan autotxpower all
Node      Group      Information
-----
(1)      (2)      (3)
0:node0          Start txpower setting(RSSI threshold is 10)
                Check the current txpower:
                module1 ... 1
                module2 ... not set
                Check the state of modules of neighbors:
                neighbor1(1:nodel) ... OK
                Scanning RSSI of the target node on neighbors:
                neighbor1(1:nodel): module1: 43
                Change txpower:
                module1 ... 1
                Wait for 90 seconds until WLAN is stable
                Scanning RSSI of the target node on neighbors:
                neighbor1(1:nodel): module1: 43
                New txpowers are:
                module1: 1
                module2: not set
                Succeeded.
```

- 1) 管理機器定義番号:無線 LAN アクセスポイント名
- 2) グループ定義番号:グループ名
- 3) 実行状況

48.1.3 nodemanagerctl wlan autochannel

[機能]

管理機器のチャンネル自動調整

[適用機種]



[入力形式]

```
nodemanagerctl wlan autochannel {node <node_number> | group <group_number> | all}
```

[オプション]

<node_number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<group_number>

- グループ定義番号
管理グループの通し番号を 10 進数で指定します。

all

すべての管理機器のチャンネルを自動で調整します。

[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]

オプションで指定された管理機器 (または、すべての管理機器) のチャンネルについて、周囲の無線 LAN アクセスポイントと干渉を抑制するように自動的にチャンネルを調整します。

nodemanager wlan autochannel bandwidth コマンドで通信帯域幅として 20MHz が指定されている場合、以下のように割り当てます。

- 2.4GHz 帯の調整時には、「2.4GHz 帯のチャンネル自動調整の判定用 RSSI のしきい値」を割り当ての条件として使用します。
- 5GHz 帯の調整時には、「5GHz 帯のチャンネル自動調整の割り当て範囲の設定」を割り当て条件として使用します。

通信帯域幅として 40MHz が指定されている場合、チャンネルボンディング可能なチャンネルペアのうち、チャンネルの RSSI が低いものからチャンネルペアが選択されます。チャンネルボンディング可能なチャンネルペアが見つからなかった場合は、通信帯域幅として 20MHz が指定されているものとして、上記の方法でチャンネルを調整します。

無線通信モードと自動割り当てのチャンネルの関係を以下に示します。

無線通信モードの設定	自動割り当てのチャンネル
11b, 11b/g, 11g, 11g/n, 11b/g/n	2.4GHz帯のチャンネル自動調整のレイアウトの設定の計算結果で得られるチャンネルのどれかを優先的に割り当てる。割り当て時に上記チャンネルすべてのRSSIが「2.4GHz帯のチャンネル自動調整の判定用RSSIのしきい値」を超えていた場合、全チャンネル中、RSSIが最低のものを割り当てる。
11a, 11a/n	「5GHz帯のチャンネル自動調整の割り当て範囲の設定」で設定した範囲のチャンネルを割り当てる。

[注意]

チャンネルの自動調整対象の管理機器は、無線 LAN モジュールを使用するように設定されている必要があります。

自動調整の間は無線 LAN への端末接続が不安定になります。

[メッセージ]

```
<node_number>:管理機器名 <group_number>:グループ名 Start channel setting.
```

管理機器 (<node_number>:管理機器名) のチャンネル自動調整を開始しました。

```
Succeeded.
```

管理機器のチャンネルの調整に成功しました。

```
Check the states of modules:
Can't get the states of modules.
Failed.
```

管理機器の無線 LAN モジュールの状態の獲得に失敗しました。

```
Check the states of modules:
The node has not identified the type of wlan.
Failed.
```

管理機器の無線 LAN モジュールのタイプが未採取のため失敗しました。

```
Check the states mode on module1:
Can't get the mode of module1.
Failed.
```

管理機器の無線 LAN モジュールのモードの特定に失敗しました。

```
Scanning states of channels around the node:
Can't scan.
Failed.
```

管理機器での無線 LAN スキャンに失敗しました。

[実行例]

```
# nodemanagerctl wlan autochannel all
Node          Group          Information
-----
(1)           (2)           (3)
0:AP-A01     0:GroupA      Start channel setting.
                Parameters:
                2.4GHz RSSI threshold: 20
                2.4GHz channel layout: start: 1, interval: 3
                5GHz target channel: w52/53/56
                Check the states of modules:
                module1 ... not set
                module2 ... OK
                Check the mode of module2:
                11a/n
                Scanning states of channels around the node:
                5GHz
                Channel  RSSI | Channel  RSSI
                36      32  | 100      unused
                40      62  | 104      unused
                44      unused | 108      unused
                48      unused | 112      0
                52      unused | 116      unused
                56      unused | 120      unused
                60      unused | 124      unused
                64      unused | 128      44
                | 132      unused
                | 136      unused
                | 140      unused
                5GHz (2nd-chan)
                Channel  RSSI | Channel  RSSI
                36      unused | 100      unused
                40      unused | 104      unused
                44      unused | 108      unused
                48      unused | 112      unused
                52      unused | 116      unused
                56      unused | 120      unused
                60      unused | 124      unused
                64      unused | 128      unused
                | 132      unused
                | 136      unused
                | 140      unused
                Set new channels:
                module2 ... 44, 48
                Succeeded.

#
```

- 1) 管理機器定義番号:無線 LAN アクセスポイント名
- 2) グループ定義番号:グループ名
- 3) 実行状況

48.1.4 nodemanagerctl reset

[機能]

管理機器の装置リセット

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

```
nodemanagerctl reset {node <node_number> | group <group_number> | all}
```

[オプション]

<node_number>

- 管理機器定義番号
管理機器の通し番号を 10 進数で指定します。

<group_number>

- グループ定義番号
管理グループの通し番号を 10 進数で指定します。

all

すべての管理機器を対象とします。

[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]

管理対象の管理機器を再起動します。グループ定義番号が指定された場合は、管理グループに所属するすべての管理機器を再起動します。特定の 1 台を再起動させたい場合は、管理機器定義番号で指定します。

無線 LAN 管理機能が動作する機器が管理機器として設定されている場合 (構成定義のアドレスとして、127.0.0.1 を指定したものは対象外となります)。

[メッセージ]

```
<node_number>:管理機器名 <group_number>:グループ名 Start reset.
```

管理機器 (<node_number>:管理機器名) の再起動を開始しました。

```
Succeeded.
```

管理機器を再起動しました。

```
Unable to reset.  
Failed.
```

管理機器を再起動できませんでした。


```
The configuration data is not registered.  
Failed.
```

管理機器の構成定義データが登録されていません。

```
The node is oneseif.  
Failed.
```

管理機器は、無線 LAN 管理機能が動作する機器のためリセットできませんでした。

[実行例]

```
# nodemanagerctl reset all  
Node          Group          Information  
-----  
(1)           (2)           (3)  
0:ap0         0:group0      Start reset.  
Succeeded.  
  
1:ap1         0:group0      Start reset.  
Succeeded.  
  
2:ap2         0:group0      Start reset.  
Unable to reset.  
Failed.  
  
3:ap3         Start reset.  
The configuration data is not registered.  
Failed.  
  
4:ap4         Start reset.  
The node is oneseif.  
Failed.  
  
#
```

- 1) 管理機器定義番号:無線 LAN アクセスポイント名
- 2) グループ定義番号:グループ名
- 3) 実行状況

48.2 監視ログクリア

48.2.1 clear nodemanager logging

[機能]

すべての監視ログのクリア

[適用機種]

SR-M20AP2	SR-M20AP1		
-----------	-----------	--	--

[入力形式]

clear nodemanager logging

[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]

すべての監視ログをクリアします。

[実行例]

```
# clear nodemanager logging  
#
```

48.2.2 clear nodemanager logging wlan

[機能]

無線 LAN アクセスポイントの監視ログのクリア

[適用機種]

SR-M20AP2 SR-M20AP1

[入力形式]

clear nodemanager logging wlan

[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]

無線 LAN アクセスポイントの監視ログをクリアします。

[実行例]

```
# clear nodemanager logging wlan  
#
```

48.2.3 clear nodemanager logging wlan sta

[機能]

無線 LAN 端末の監視ログのクリア

[適用機種]

SR-M20AP2	SR-M20AP1		
-----------	-----------	--	--

[入力形式]

clear nodemanager logging wlan sta

[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]

無線 LAN 端末の監視ログをクリアします

[実行例]

```
# clear nodemanager logging wlan sta  
#
```

第 49 章 I'm here コマンド

49.1 I'm here コマンド

49.1.1 iamhere

[機能]

I'm here ランプの手動点滅の設定

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[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 50 章 その他のコマンド

50.1 その他

50.1.1 ping

[機能]

ICMP エコー要求パケットの送信

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
ping <ip_address> [source <ip_address>] [repeat [<count>]] [size <dec>] [tos <hex>] [ttl <dec>]
[timeout <dec>] [df]
ping <host_name> [v4] [source <ip_address>] [repeat [<count>]] [size <dec>] [tos <hex>] [ttl <dec>]
[timeout <dec>] [df]
```

[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。

v4

- 送出先ホスト名の IP バージョン指定
<host_name>指定時に、<host_name>から解決した送出先 IP アドレスのバージョンを指定します。
省略時は、v4 とみなされます。
解決した IP アドレスのバージョンと本指定が一致しない場合はエラーとなります。

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。

tos <hex>

- TOS 値
TOS 値を、0x00 ~ 0xff の 16 進数で指定します。
省略時は、0x00 を指定したものとみなされます。

ttl <dec>

- TTL 値
TTL 値を、0 ~ 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。

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]

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
192.168.1.1 is alive.
#
```

b) ホスト名指定

```
# ping jp.fujitsu.com
192.168.1.2 is alive.
#
```

c) 繰り返し (3 回指定)

```
# ping 192.168.1.1 repeat 3
PING 192.168.1.1: 56 data bytes.
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.768 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.736 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.736 ms

----192.168.1.1 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/ave/max = 0.736/0.746/0.768
#
```

オプションの指定順序は入力形式に従ってください。

50.1.2 traceroute

[機能]

ネットワーク経路の表示

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

```
traceroute <ip_address> [ source <src_ip_address> ] [ size <data_size> ] [ timeout <timeout> ] [ mpls ] [ df ]  
traceroute <host_name> [v4] [ source <src_ip_address> ] [ size <data_size> ] [ timeout <timeout> ] [ mpls ] [ df ]
```

[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。

v4

- 送出先ホスト名の IP バージョン指定
<host_name>指定時に、<host_name>から解決した送出先 IP アドレスのバージョンを指定します。
省略時は、v4 とみなされます。
解決した IP アドレスのバージョンと本指定が一致しない場合はエラーとなります。

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。

```

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)
!F                   : あて先到達不能 (フラグメントが必要)
!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、traceroute は以下のエラーを報告します。

```
traceroute: unknown host <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。

```
traceroute: can't assign source address
```

送信元 IP アドレスの割り当てに失敗した。

(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

```

# traceroute 192.168.1.1
traceroute to 192.168.1.1 from 192.168.5.2, 30 hops max, 46 byte packets
 1  192.168.5.1                20.000 ms  20.000 ms  20.000 ms
 2  192.168.1.1                41.000 ms  41.000 ms  41.000 ms
#

```

host から応答がない場合

```

# traceroute 192.168.1.1
traceroute to 192.168.1.1 from 192.168.5.2, 30 hops max, 46 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
   :
30  * * *
#

```

50.1.3 telnet

[機能]

telnet サーバへの接続

[適用機種]

SR-M20AP2 SR-M20AP1 SR-M20AC2 SR-M20AC1

[入力形式]

telnet <host> [<port>] [escape { <char> | none }] [srcaddr <srcaddr>] [tos <tos>]

[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。

escape { <char> | none }

エスケープ文字を指定します。エスケープ文字を使用しない場合は "none" を指定します。

telnet 接続中にエスケープ文字キーに続けて "q" キーを入力すると、telnet 接続を強制的に切断することができます。

エスケープ文字としてコントロール文字を指定する場合、"^" に続けて文字を指定します。たとえば、CTRL+A であれば "^A" を指定します。

"none" 以外の文字列を指定した場合、最初の文字をエスケープ文字に指定したものとみなされます。

省略時は、"^" (CTRL+) を指定したものとみなされます。

srcaddr <srcaddr>

ソースアドレス (本ルータのアドレス) を、IPv4 アドレス形式で指定します。

省略時は、適切なアドレスが設定されます。

tos <tos>

TOS 値を 0 ~ ff の範囲の 16 進数で指定します。

省略時は、0 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。

telnet サーバから以下の情報を求められた場合は、本装置の情報 (括弧内の値) を通知します。

- 端末タイプ (VT100)
- 通信速度 (9600bps)
- 画面サイズ (画面行数、画面桁数)

【実行例】

```
# telnet 192.168.1.2
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'
Login:
Password:
# exit
Connection closed by foreign host.
#
```

他ルータにtelnet接続
接続手続き中
接続完了
エスケープ文字表示
他ルータのユーザ名入力
他ルータのパスワード入力
他ルータでexitコマンド実行
切断
本ルータのプロンプト表示

第 51 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-M20AP2 SR-M20AP1	SR-M20AC2 SR-M20AC1
パスワード情報	password format	(0)	(0)
	password admin set	(0)	(0)
	password user set	(0)	(0)
	password aaa	(1)	(1)
	password authtype	(1)	(1)
ポート情報の設定 ether共通情報	ether use	(3)	(3)
	ether mode	(3)	(3)
	ether duplex	(3)	(3)
	ether mdi	(3)	(3)
	ether flowctl	(3)	(3)
	ether type	(3)	-
	ether vlan	(3)	-
	ether downrelay	(3)	-
	ether downrelay wlan	(3)	-
	ether downrelay recovery mode	(3)	-
	ether description	(1)	(1)
	backup	(3)	-
	backup mode	(3)	-
	backup standby	(3)	-
	backup downrelay	(3)	-
	backup downrelay wlan	(3)	-
	backup downrelay recovery mode	(3)	-
IEEE802.1X認証情報	ether dot1x use	-	(3)
	ether dot1x portcontrol	-	(3)
	ether dot1x quietperiod	-	(3)
	ether dot1x txperiod	-	(3)
	ether dot1x supptimeout	-	(3)
	ether dot1x maxreq	-	(3)
	ether dot1x reauthperiod	-	(3)
	ether dot1x aaa	-	(3)
	ether dot1x wol	-	(3)
MACアドレス認証情報	ether macauth use	-	(3)
	ether macauth aaa	-	(3)
	ether macauth authenticated-mac	-	(3)
	ether macauth expire	-	(3)
	ether macauth wol	-	(3)
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)	(5)
	ieee80211 mode	(5)	(5)
	ieee80211 channel	(5)	(5)
	ieee80211 bandwidth	(5)	(5)
	ieee80211 secondary-channel	(5)	(5)
	ieee80211 chanlist	-	(5)
	ieee80211 sta limit	(5)	-
	ieee80211 protection mode	(5)	(5)
	ieee80211 rts threshold	(5)	(5)
	ieee80211 dtim period	(5)	-
	ieee80211 beacon interval	(5)	-
	ieee80211 wmm mode	(5)	(5)
	ieee80211 wmm ack	(5)	(5)
	ieee80211 apscan mode	(5)	-
	ieee80211 apscan expire	(5)	-
	ieee80211 txpower	(5)-1	(5)-1
	ieee80211 antenna use	(5)-1	-
	ieee80211 noise-detect	(5)-1	-

(続く)

(続き)

種別	コマンド名	commit実行時影響	
		SR-M20AP2 SR-M20AP1	SR-M20AC2 SR-M20AC1
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)	(5)
	wlan description	(1)	(1)
	wlan type	(5)	-
	wlan ssid	(5)	(5)
	wlan hide	(5)	-
	wlan apbridge	(5)	-
	wlan auth	(5)	(5)
	wlan wep mode	(5)	(5)
	wlan wep key	(5)	(5)
	wlan wep send	(5)	(5)
	wlan wep type	(5)	-
	wlan wpa cipher	(5)	(5)
	wlan wpa psk	(5)	(5)
	wlan wpa rekey group	(5)	-
	wlan wpa countermeasures	(5)	(5)
	wlan wpa pmkcache mode	(5)	(5)
	wlan wpa pmkcache num	(5)	(5)
	wlan wpa pmkcache expire	(5)	(5)
	wlan wpa eapol supptimeout	(5)	-
	wlan wpa eapol maxreq	(5)	-
	wlan supplicant dot1x use	-	(5)
	wlan supplicant eap	-	(5)
	wlan supplicant certificate	-	(5)
	wlan guard-interval	(5)	(5)
	wlan macfilter	(5)(9)	-
	wlan macfilter move	(5)	-
	wlan roaming mode	-	(5)
	wlan roaming threshold bmiss	-	(5)
	wlan roaming threshold rssi	-	(5)
	wlan roaming threshold rate	-	(5)
	wlan wmm aclmap	(5)(9)	(5)
	wlan wmm aclmap move	(5)	(5)
	wlan sta guarantee	(5)	-
	wlan sta idle	(5)	-
	wlan wds neighbor	(5)	-
	wlan relay mode	-	(5)
	wlan relay expire	-	(5)
VLAN情報	wlan vlan	(5)	-
フレーム転送情報	wlan forward broadcast	(5)	-
IEEE802.1X認証情報	wlan dot1x use	(5)	-
	wlan dot1x supptimeout	(5)	-
	wlan dot1x maxreq	(5)	-
	wlan dot1x reauthperiod	(5)	-
	wlan dot1x aaa	(5)	-
	wlan dot1x vid	(5)	-
	wlan dot1x vlan assign	(5)	-
	wlan dot1x backup	(5)	-
MACアドレス認証情報	wlan macauth use	(5)	-
	wlan macauth aaa	(5)	-
	wlan macauth authenticated-mac	(5)	-
	wlan macauth expire	(5)	-
	wlan macauth vid	(5)	-
	wlan macauth vlan assign	(5)	-

(続く)

(続き)

種別	コマンド名	commit実行時影響			
		SR-M20AP2	SR-M20AC2	SR-M20AP1	SR-M20AC1
VLAN情報の設定 VLAN共通情報	vlan name	(1)		(1)	
	vlan forward	(2)	1	(2)	1
	vlan description	(1)		(1)	
フィルタ情報	vlan filter	(1)(9)		(1)	
	vlan filter move	(1)		(1)	
	vlan filter default	(1)		(1)	
IDS情報	vlan ids use	(1)		(1)	
MAC情報 MAC情報	mac	(1)	1	(1)	1
	mac age				
LAN情報の設定 IP関連情報	lan ip address	(1)		(1)	
	lan ip dhcp	(1)		(1)	
	lan ip route	(1)		(1)	
	lan ip arp static	(1)		(1)	
VLAN関連情報	lan vlan	(2)		(2)	
SNMP関連情報	lan snmp	(1)		(1)	
IP関連情報 IP関連情報	ip arp age	(1)		(1)	
認証情報の設定 IEEE802.1X情報	dot1x use	(7)		(8)	
MACアドレス認証情報	macauth use	(7)		(8)	
	macauth password	(7)		(8)	
	macauth type	(7)		(8)	
サブリカント情報	supplicant dot1x use	-		(5)	
	supplicant certificate check	-		(1)	
	validity			(1)	
証明書関連情報の設定 証明書関連情報	certificate local name	-		(6)	
	certificate local line	-		(6)	
	certificate ca name	-		(6)	
	certificate ca line	-		(6)	
	certificate request line	-		(1)	
	certificate private line	-		(6)	
ACL情報の設定 ACL情報	acl	(9)		(9)	
AAA情報の設定 グループID情報	aaa name	(1)		(1)	
AAAユーザ情報	aaa user	(1)		(1)	
Supplicant情報	aaa user supplicant	(1)		(1)	
RADIUS情報	aaa radius	(1)		(1)	

(続く)

(続き)

種別	コマンド名	commit実行時影響	
		SR-M20AP2 SR-M20AP1	SR-M20AC2 SR-M20AC1
無線LAN管理機能の設定	nodemanager	(1)	-
装置情報の設定			
SNMP情報	snmp	(1)	(1)
システムログ情報	syslog	(1)	(1)
自動時刻設定情報	time	(1)	(1)
ProxyDNS情報	proxydns	(1)	(1)
ProxyARP情報	proxyarp use proxyarp unicast	(1) (1)	(1) (1)
ホストデータベース情報	host	(1)	(1)
スケジュール情報	schedule	(1)	(1)
装置ランプ情報	lamp	(1)	(1)
その他	addact watchdog service consoleinfo telnetinfo mflag sysname serverinfo	(0) (4) (1) (1) (1) (4) (1)	(0) (4) (1) (1) (1) (4) (1)

- (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。
- (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。
- (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。
- (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 / 再開されます。
- (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。
 - 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。

索引

【欧文】

A

aaa name	228
aaa radius accounting source	238
aaa radius auth message-authenticator	237
aaa radius auth source	236
aaa radius client nas-identifier	260
aaa radius client retry	259
aaa radius client server-info accounting address	254
aaa radius client server-info accounting deadtime	256
aaa radius client server-info accounting port	255
aaa radius client server-info accounting priority	257
aaa radius client server-info accounting secret	253
aaa radius client server-info accounting source	258
aaa radius client server-info auth address	240
aaa radius client server-info auth deadtime	242
aaa radius client server-info auth port	241
aaa radius client server-info auth priority	244
aaa radius client server-info auth secret	239
aaa radius client server-info auth source	245
aaa radius client server-info auth watch abnormal-interval	252
aaa radius client server-info auth watch interval	249
aaa radius client server-info auth watch retry	250
aaa radius client server-info auth watch timeout	251
aaa radius client server-info auth watch type	246
aaa radius client server-info auth watch user	248
aaa radius service	235

aaa user id	229
aaa user password	230
aaa user supplicant mac	234
aaa user supplicant vid	233
aaa user user-role	232
acl description	226
acl icmp	224
acl ip	217
acl mac	215
acl tcp	220
acl udp	222
addact	346
admin	384
alias	408

B

backup downrelay recovery mode	51
backup downrelay wlan	49
backup mode	46
backup standby	47

C

certificate ca line	211
certificate ca name	210
certificate local line	209
certificate local name	208
certificate private line	213
certificate request line	212
clear aaa radius client statistics	594
clear alias	411
clear arp	534
clear bridge	553
clear dot1x statistics	581
clear ether statistics	456
clear ieee80211 statistics	466
clear interface statistics	530
clear ip traffic	546
clear logging command	407
clear logging error	422
clear logging syslog	424
clear macauth statistics	586
clear nettime statistics	598

- clear nodemanager logging 698
clear nodemanager logging wlan 699
clear nodemanager logging wlan sta 700
clear proxyarp statistics 602
clear snmp statistics 607
clear statistics 425
clear trace ssh 616
clear vlan filter statistics 563
clear vlan ids statistics 567
clear wlan relay table 509
clear wlan statistics 507
clear wlan supplicant statistics 510
clear wlan wpa statistics 508
clear wol statistics 588
commit 439
configure 389
consoleinfo 349
copy 444
crypto certificate ca 685
crypto certificate generate 679
crypto certificate local 683
- D**
- date 427
delete 435
diff 434
dir 442
discard 440
dot1x use 200
dot1xctl backup recovery 673
dot1xctl initialize 671
dot1xctl reconfirm 672
- E**
- end 390
ether description 45
ether dot1x aaa 61
ether dot1x maxreq 59
ether dot1x portcontrol 54
ether dot1x quietperiod 56
ether dot1x reauthperiod 60
ether dot1x supptimeout 58
ether dot1x txperiod 57
ether dot1x use 52
ether dot1x wol 62
ether downrelay recovery mode 44
ether downrelay wlan 43
ether duplex 35
ether flowctl 38
ether macauth aaa 65
ether macauth authenticated-mac 66
ether macauth expire 67
ether macauth use 63
ether macauth wol 68
ether mdi 36
ether mode 34
ether type 39
ether use 33
ether vlan tag 41
ether vlan untag 42
exit 388
- F**
- format 447
- H**
- host ip address 340
host name 339
- I**
- iamhere 702
ieee80211 antenna use 93
ieee80211 apscan expire 90
ieee80211 apscan mode 89
ieee80211 bandwidth 76
ieee80211 beacon interval 86
ieee80211 chanlist 80
ieee80211 channel 74
ieee80211 dtim period 85
ieee80211 ht-protection mode 83
ieee80211 mode 72
ieee80211 noise-detect channel layout 95
ieee80211 noise-detect mode 94
ieee80211 protection mode 82
ieee80211 rts threshold 84
ieee80211 secondary-channel 77
ieee80211 sta limit 81
ieee80211 txpower 91
ieee80211 use 70
ieee80211 wmm ack 88
ieee80211 wmm mode 87
ip arp age 198
- L**
- lamp delay 345
lamp mode 344
lan ip address 187
lan ip arp static 192

lan ip dhcp service	189
lan ip route	190
lan snmp trap linkdown	195
lan snmp trap linkup	196
lan vlan	194
load	436

M

mac age	185
macauth password	202
macauth type	203
macauth use	201
macauthctl initialize	675
mflag	351
more	412

N

nodemanager collect interval	281
nodemanager group name	264
nodemanager icmpwatch interval	284
nodemanager icmpwatch threshold	286
nodemanager log	290
nodemanager login service	263
nodemanager node address	267
nodemanager node group	266
nodemanager node name	265
nodemanager node user	268
nodemanager node wlan neighbor	271
nodemanager node wlan scan	269
nodemanager node wlan sta	270
nodemanager wlan autochannel bandwidth	280
nodemanager wlan autochannel channel	277
nodemanager wlan autochannel layout	278
nodemanager wlan autochannel rssi	279
nodemanager wlan autotxpower rssi	276
nodemanager wlan filterset description	272
nodemanager wlan filterset filter description	275
nodemanager wlan filterset filter mac	273
nodemanager wlan scan error threshold	289
nodemanager wlan scan interval	287
nodemanager wlan scan unmanaged	283
nodemanager wlan sta rssi	291
nodemanagerctl reset	696
nodemanagerctl update wlan filterset	688
nodemanagerctl wlan autochannel	693
nodemanagerctl wlan autotxpower	690

O

offline	662
online	664

P

password aaa	30
password admin set	24
password authtype	31
password format	22
password nodemgr set	28
password user set	26
ping	704
proxyarp unicast	338
proxyarp use	337
proxydns address	333
proxydns address move	335
proxydns domain	329
proxydns domain move	332
proxydns unicode	336

Q

quit	391
------------	-----

R

radius recovery	677
rdate	428
remove	445
rename	446
reset	429

S

save	438
schedule at	341
schedule syslog	343
serverinfo dns	370
serverinfo dns filter	371
serverinfo dns filter default	373
serverinfo dns filter move	372
serverinfo ftp	353
serverinfo ftp filter	354
serverinfo ftp filter default	356
serverinfo ftp filter move	355
serverinfo http	366
serverinfo http filter	367
serverinfo http filter default	369
serverinfo http filter move	368
serverinfo sftp	357
serverinfo snmp	374
serverinfo snmp filter	375

serverinfo snmp filter default	377	show nodemanager logging wlan scan	637
serverinfo snmp filter move	376	show nodemanager logging wlan scan managed	641
serverinfo ssh	362	show nodemanager logging wlan scan managed brief	640
serverinfo ssh filter	363	show nodemanager logging wlan scan unknown	646
serverinfo ssh filter default	365	show nodemanager logging wlan scan unmanaged	635
serverinfo ssh filter move	364	show nodemanager logging wlan sta	648
serverinfo telnet	358	show nodemanager logging wlan sta rssi	653
serverinfo telnet filter	359	show nodemanager logging wlan trace	658
serverinfo telnet filter default	361	show nodemanager node	627
serverinfo telnet filter move	360	show nodemanager node brief	634
serverinfo time filter	380	show nodemanager update wlan filterset	633
serverinfo time filter default	382	show poe drawing	512
serverinfo time filter move	381	show proxyarp	600
serverinfo time ip tcp	378	show proxyarp statistics	601
serverinfo time ip udp	379	show running-config	432
show aaa radius client server-info	590	show snmp statistics	604
show aaa radius client statistics	592	show socket	609
show alias	410	show ssh server key	569
show arp	532	show startup-config	433
show auth port	572	show system information	415
show bridge	551	show system status	417
show candidate-config	431	show tech-support	419
show crypto certificate	618	show terminal	405
show date	426	show trace ssh	614
show dot1x backup port	579	show usb hcd status	514
show dot1x port	574	show usb storage status	515
show dot1x statistics port	577	show vlan	556
show ether	449	show vlan filter	559
show ether statistics	452	show vlan filter statistics	561
show ieee80211 apscan	467	show vlan filter summary	562
show ieee80211 statistics	458	show vlan ids statistics	564
show ieee80211 status	462	show wlan ap	478
show interface	520	show wlan blockack session	505
show interface brief	522	show wlan relay status	497
show interface detail	525	show wlan sta	473
show interface statistics	528	show wlan statistics	483
show interface summary	524	show wlan status	487
show ip dhcp	548	show wlan supplicant statistics	503
show ip route	536	show wlan supplicant status	499
show ip route kernel	539	show wlan wpa statistics	494
show ip route summary	538	show wlan wpa status	492
show ip traffic	543	show wol statistics	587
show logging command	406	snmp agent address	297
show logging error	420	snmp agent contact	294
show logging syslog	423	snmp agent engineid	298
show macauth port	582	snmp agent location	296
show macauth statistics port	584		
show nettime statistics	596		
show nodemanager group	626		
show nodemanager logging wlan reject	655		

snmp agent sysname	295
snmp manager	299
snmp service	293
snmp trap authfail	304
snmp trap coldstart	301
snmp trap linkdown	302
snmp trap linkup	303
snmp trap noserror	305
snmp user address	307
snmp user auth	309
snmp user name	306
snmp user notification	308
snmp user notify	315
snmp user priv	311
snmp user read	314
snmp user write	313
snmp view subtree	316
su	386
supplicant certificate check validity	206
supplicant dot1x use	205
syslog command-logging	324
syslog dupcut	323
syslog facility	321
syslog logging nodemgr access	325
syslog pri	320
syslog security	322
syslog server address	318
syslog server pri	319
sysname	352

T

tail	413
telnet	708
telnetinfo	350
terminal bell	403
terminal charset	399
terminal logging	404
terminal pager	395
terminal prompt	400
terminal timestamp	402
terminal window	398
time auto interval	327
time auto server	326
time zone	328
top	392
traceroute	706

U

up	393
usbctl	669

V

vlan description	177
vlan filter	178
vlan filter default	181
vlan filter move	180
vlan forward	175
vlan ids use	183
vlan name	174

W

watchdog service	348
wlan ampdu rx density	134
wlan ampdu rx size	133
wlan ampdu tx mode	132
wlan apbridge	104
wlan auth	105
wlan description	99
wlan dot1x aaa	160
wlan dot1x backup	163
wlan dot1x maxreq	158
wlan dot1x reauthperiod	159
wlan dot1x supptimeout	157
wlan dot1x use	155
wlan dot1x vid	161
wlan dot1x vlan assign	162
wlan forward broadcast	154
wlan guard-interval	135
wlan hide	103
wlan macauth aaa	167
wlan macauth authenticated-mac	168
wlan macauth expire	169
wlan macauth use	165
wlan macauth vid	170
wlan macauth vlan assign	171
wlan macfilter	136
wlan macfilter move	138
wlan relay expire	151
wlan relay mode	150
wlan roaming mode	139
wlan roaming threshold bmiss	140
wlan roaming threshold rate	143
wlan roaming threshold rssi	141
wlan ssid	102
wlan sta guarantee	147
wlan sta idle	148
wlan supplicant certificate ca	129
wlan supplicant certificate local	130
wlan supplicant certificate private_key	131
wlan supplicant dot1x use	123

wlan supplicant eap id	125
wlan supplicant eap inner protocol	128
wlan supplicant eap password	126
wlan supplicant eap peapversion	127
wlan supplicant eap protocol	124
wlan type	100
wlan use	97
wlan vlan tag	152
wlan vlan untag	153
wlan wds neighbor	149
wlan wep key	108
wlan wep mode	107
wlan wep send	110
wlan wep type	111
wlan wmm aclmap	144
wlan wmm aclmap move	146
wlan wpa cipher	113
wlan wpa countermeasures	117
wlan wpa eapol maxreq	122
wlan wpa eapol supptimeout	121
wlan wpa pmkcache expire	120
wlan wpa pmkcache mode	118
wlan wpa pmkcache num	119
wlan wpa psk	114
wlan wpa rekey group	116
wlanctl authenticator disconnect	667

【その他】

!	394
---	-----

SR-M コマンドリファレンス

P3NK-4202-04Z0

発行日 2014年8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。