

RGW5000 シリーズ 設定マニュアル

Ver1.2 対応

目次

1. 設定の方法	6
1.1. 接続方法.....	6
1.2. 設定方法.....	7
1.3. ユーザーモードと特権モード.....	7
1.4. コマンドラインシェルによる設定.....	7
1.5. コマンドラインシェル機能一覧.....	8
1.6. コマンド一覧.....	9
1.7. 各コマンドの説明.....	12
1.7.1 パスワードの設定.....	12
1.7.2 ホスト名の設定.....	12
1.7.3 IPアドレスの設定.....	12
1.7.4 静的ルートの設定.....	13
1.7.5 静的ルートの削除.....	13
1.7.6 ICMP Redirect送出的設定.....	13
1.7.7 無線モードの設定.....	14
1.7.8 無線周波数の設定.....	14
1.7.9 無線送信速度の設定.....	14
1.7.10 無線WEP機能設定.....	15
1.7.11 無線WEPキー番号設定.....	15
1.7.12 無線WEPキー値設定.....	15
1.7.13 無線タイプの設定.....	15
1.7.14 無線SSIDの設定.....	16
1.7.15 MACアドレスフィルター設定.....	16
1.7.16 MACアドレスフィルターのアドレス登録.....	16
1.7.17 MACアドレスフィルターのアドレス削除.....	16
1.7.18 MACアドレスフィルターの表示.....	17
1.7.19 AP間通信フィルター設定.....	17
1.7.20 AP間通信フィルターのアドレス登録.....	17
1.7.21 AP間通信MACフィルターのアドレス削除.....	17
1.7.22 AP間通信フィルターの登録アドレス表示.....	18
1.7.23 ステルスAPの設定.....	18
1.7.24 RIPを使用するか否かの設定.....	18
1.7.25 RIPを静的経路を送信するか否かの設定.....	18
1.7.26 RIPの動作の設定.....	19
1.7.27 RIPのバージョンの設定.....	19

1.7.28	フィルターを使用するか否かの設定	19
1.7.29	フィルターの設定	20
1.7.30	フィルターの削除	21
1.7.31	NATを使用するか否かの設定	21
1.7.32	NATのmapアクションの設定	21
1.7.33	NATのbimapアクションの設定	22
1.7.34	NATのrdrアクションの設定	22
1.7.35	NATの削除	22
1.7.36	DHCPサーバーを使用するか否かの設定	23
1.7.37	DHCPサーバーで配布するIPアドレスの設定	23
1.7.38	DHCPサーバーで配布するIPアドレスの有効期限	23
1.7.39	DHCPサーバーで配布するDNSサーバーの設定	23
1.7.40	DHCPサーバーで配布するDNSサーバーの削除	23
1.7.41	DHCPサーバーで配布するドメイン名の設定	24
1.7.42	DHCPサーバーで配布するデフォルトルートの設定	24
1.7.43	DHCPリレーエージェントの設定	24
1.7.44	SNMPサーバー機能を使用するか否かの設定	24
1.7.45	SNMPコミュニティ名の設定	24
1.7.46	SNMPのlocationの設定	25
1.7.47	SNMPのcontactの設定	25
1.7.48	SNMPのアクセスの設定	25
1.7.49	SNMP TRAPの設定	25
1.7.50	syslog機能を使用するか否かの設定	26
1.7.51	syslogを転送するホストの設定	26
1.7.52	syslogを転送するファシリティの設定	26
1.7.53	syslogを転送するファシリティの削除	26
1.7.54	SSHのホストキーの生成	27
1.7.55	SSHの認証方法の設定	27
1.7.56	SSHの公開鍵のダウンロード	27
1.7.57	SSHの使用するバージョンの切り替え	28
1.7.58	telnetアクセスの設定	28
1.7.59	SSHアクセスの設定	28
1.7.60	保存	28
1.7.61	static ARPの設定	29
1.7.62	ARPの削除	29
1.7.63	コールドスタート	29

1.7.64	ファームウェアのアップデート	29
1.7.65	タイムゾーンの追加	29
1.7.66	タイムゾーンの表示	30
1.7.67	設定可能なタイムゾーンの表示	30
1.7.68	NTPを使用するか否かの設定	30
1.7.69	NTPサーバーの追加	30
1.7.70	NTPの設定表示	30
1.7.71	日付と時刻の設定	31
1.7.72	ブリッジの設定	31
1.7.73	ブリッジの学習済みMACアドレスのクリア	31
1.7.74	ブリッジの状態表示	31
1.7.75	再起動	32
1.7.76	ARPのクリア	32
1.7.77	ホスト名の表示	32
1.7.78	IPアドレスの表示	32
1.7.79	静的ルートの表示	32
1.7.80	DHCPのリース状態の表示	32
1.7.81	フィルタリング状態の表示	32
1.7.82	ARPテーブルの表示	33
1.7.83	起動時からの経過時間の表示	33
1.7.84	ファームウェアのバージョンの表示	33
1.7.85	日付と時刻の表示	33
1.7.86	無線の受信レベル表示	33
1.7.87	無線設定の表示	33
1.7.88	SNMP設定の表示	33
1.7.89	SSH設定の表示	34
1.7.90	設定内容の確認	34
1.7.91	コマンド形式の保存内容の確認	34
1.7.92	ping	34
1.7.93	traceroute	34
1.7.94	無線テストコマンド	34
1.7.95	ログアウト	35
1.7.96	特権モードへの移行	35
1.7.97	コマンドヘルプの表示	35
1.7.98	ヒストリーの参照	35
1.8.	ファームウェアアップデート手順	37

1.8.1 準備するもの	37
1.8.2 アップデート手順	37
1.8.3 アップデート例	37
1.9. 制限事項	39
1.9.1 DHCP	39
1.9.2 NTP機能	39
1.9.3 AP間通信機能	39
1.9.4 その他	39
2. 工場出荷時の設定	40
3. 設定のためのヒント	41
3.1. 無線	41
3.1.1 通信モード	41
3.1.2 WEP	41
3.1.3 無線中継	41
3.1.4 ブリッジモード	42
3.1.5 AP間通信	43
3.2. ファイヤーウォール	43
3.2.1 IPフィルター	43
3.2.2 NAT	49

1. 設定の方法

1.1. 接続方法

本機の設定を行うためにはログインする必要があります。ログインはシリアル通信で行う方法と、LAN 上のホストから telnet もしくは SSH で行う方法があります。シリアル通信で設定する場合には、パソコン等のターミナルソフトを使用してください。ターミナルソフトの設定は下記の通りです。

データ伝達速度 19200 bps
キャラクタビット長 8
パリティチェック 無し
ストップビット長 1
フロー制御 なし

SSH で接続するためには事前に SSH の設定をする必要があります。その際にはシリアル通信または telnet で本機に接続し設定を行ってください。

詳細は「SSH のホストキーの生成」を参照ください。

1.2. 設定方法

設定方法には、コンソールからコマンドを入力することにより設定を行うコマンドラインシェルがあります。

1.3. ユーザーモードと特権モード

コマンドラインシェルは、特権モードとユーザーモードの2つのモードがあります。

モード	説明	プロンプト
特権モード	すべてのコマンドが実行可能なモード	“\$”
ユーザーモード	基本コマンドと表示コマンドのみが実行可能なモード	“>”

1.4. コマンドラインシェルによる設定

telnet で接続すると login プロンプトが表示されます。

login:

ユーザー名 admin を入力します。

login: admin<CR>

続いてパスワードを入力します（パスワードが admin の場合）。

password: admin<CR> （注：入力したパスワードは表示されません。）

ログインに成功すると、プロンプト > が表示されます。

設定を変更する場合には特権モードへ移行する必要があります。

特権モードへ移行するコマンドを入力します。

>administrator<CR>

続いて特権モードのパスワードを入力します（パスワードが admin の場合）。

password: admin<CR> （注：入力したパスワードは表示されません。）

プロンプト\$が表示されます。

SSH での接続については、「SSH のホストキーの生成」を参照ください。

また、パスワードは「工場出荷時の設定」を参照してください。

1.5. コマンドラインシェル機能一覧

機能	説明																		
コマンドの補完	TAB キーを押下することによって、補完可能な部分までのコマンド文字列を挿入します。																		
コマンドのヘルプ	<p>? キーを押下することによって、使用可能なコマンドの一覧、またはコマンドの説明を表示します。</p> <p>例)</p> <pre>\$ ip ? * ip address * ip icmp redirect * ip route add * ip route delete</pre> <p>ip ではコマンドが成立していないので、ip で始まるコマンドを表示。</p> <pre>\$ ip address ? usage: ip address "Interface Ippaddress Netmask" e.g. : \$ ip address ether0 192.168.0.100 255.255.255.0</pre> <p>ip address でコマンドが成立しているため、使用法と例を表示。</p>																		
コマンド行の編集	<p>コマンド行の編集機能をサポートする。キーのバインドは以下のとおりです。</p> <table border="1"> <thead> <tr> <th>キー</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>Ctrl-H (BackSpace)</td> <td>カーソルの前の 1 文字を削除</td> </tr> <tr> <td>Ctrl-A</td> <td>カーソルをコマンド行の先頭に移動</td> </tr> <tr> <td>Ctrl-E</td> <td>カーソルをコマンド行の最後尾に移動</td> </tr> <tr> <td>Ctrl-D</td> <td>カーソル上の文字を削除</td> </tr> <tr> <td>Ctrl-U</td> <td>コマンド行全体を削除</td> </tr> <tr> <td>Ctrl-F (→)</td> <td>カーソルを右へ移動</td> </tr> <tr> <td>Ctrl-B (←)</td> <td>カーソルを左へ移動</td> </tr> <tr> <td>Ctrl-K</td> <td>カーソル以降の文字を削除</td> </tr> </tbody> </table>	キー	説明	Ctrl-H (BackSpace)	カーソルの前の 1 文字を削除	Ctrl-A	カーソルをコマンド行の先頭に移動	Ctrl-E	カーソルをコマンド行の最後尾に移動	Ctrl-D	カーソル上の文字を削除	Ctrl-U	コマンド行全体を削除	Ctrl-F (→)	カーソルを右へ移動	Ctrl-B (←)	カーソルを左へ移動	Ctrl-K	カーソル以降の文字を削除
キー	説明																		
Ctrl-H (BackSpace)	カーソルの前の 1 文字を削除																		
Ctrl-A	カーソルをコマンド行の先頭に移動																		
Ctrl-E	カーソルをコマンド行の最後尾に移動																		
Ctrl-D	カーソル上の文字を削除																		
Ctrl-U	コマンド行全体を削除																		
Ctrl-F (→)	カーソルを右へ移動																		
Ctrl-B (←)	カーソルを左へ移動																		
Ctrl-K	カーソル以降の文字を削除																		
コマンドの履歴	<p>入力したコマンドの履歴を保持する。</p> <table border="1"> <thead> <tr> <th>キー</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>Ctrl-P (↑)</td> <td>前の履歴を呼び出す</td> </tr> <tr> <td>Ctrl-N (↓)</td> <td>後の履歴を呼び出す</td> </tr> </tbody> </table>	キー	説明	Ctrl-P (↑)	前の履歴を呼び出す	Ctrl-N (↓)	後の履歴を呼び出す												
キー	説明																		
Ctrl-P (↑)	前の履歴を呼び出す																		
Ctrl-N (↓)	後の履歴を呼び出す																		

1.6. コマンド一覧

設定項目	コマンド
パスワードの設定	passwd
ホスト名の設定	hostname
IP アドレスの設定	ip address
静的ルートの設定	ip route add
静的ルートの削除	ip route delete
ICMP Redirect 送出的設定	ip icmp redirect
無線モードの設定	wireless mode
無線周波数の設定	wireless channel
無線送信速度の設定	wireless txrate
無線 WEP 機能設定	wireless wep encryption
無線 WEP 使用キー番号設定	wireless wep key use
無線 WEP キー値設定	wireless wep key value
無線タイプ設定	wireless type
無線 SSID 設定	wireless ssid
MAC アドレスフィルター設定	wireless macfilter
MAC アドレスフィルターのアドレス登録	wireless macfilter add
MAC アドレスフィルターのアドレス削除	wireless macfilter delete
AP 間通信設定設定	wireless wdsfilter
AP 間通信フィルターのアドレス登録	wireless wdsfilter add
AP 間通信フィルターのアドレス削除	wireless wdsfilter delete
ステルス AP 設定	wireless ssidsuppress
static ARP のエントリーを設定	arp add
ARP エントリーの削除	arp delete
RIP を使用するか否かの設定	rip
RIP で静的経路を送信するか否かの設定	rip static-supply
RIP の動作の設定	rip action
RIP のバージョンの設定	rip version
フィルターを使用するか否かの設定	filter
フィルターの設定	filter add
フィルターの削除	filter delete
NAT を使用するか否かの設定	nat
NAT の map アクションの設定	nat add map
NAT の bimap アクションの設定	nat add bimap
NAT の map-block アクションの設定	nat add map-block
NAT の rdr アクションの設定	nat add rdr
NAT の削除	nat delete
DHCP を使用するか否かの設定	dhcp
DHCP で配布する IP アドレスの設定	dhcp pool
DHCP で配布する IP アドレスの有効期間の設定	dhcp expire
DHCP で配布する DNS サーバーの設定	dhcp dns add
DHCP で配布する DNS サーバーの削除	dhcp dns delete
DHCP で配布するドメイン名の設定	dhcp domain

設定項目	コマンド
DHCP で配布するデフォルトルートの設定	dhcp defaultroute
DHCP リレーエージェントの設定	dhcp relay
SNMP 機能を使用するか否かの設定	snmp
SNMP コミュニティ名の設定	snmp community
SNMP の location の設定	snmp location
SNMP の contact の設定	snmp contact
SNMP のアクセス設定	snmp access
SNMP の TRAP 設定	snmp trap
Syslog の設定	syslog
Syslog を転送するホスト設定	syslog host
Syslog を転送するファシリティーの設定	syslog add
Syslog を転送するファシリティーの削除	syslog delete
SSH ホストキーの生成	ssh keygen
SSH 認証方法の生成設定	ssh authentication
SSH 公開鍵のダウンロード	ssh keyget
SSH の使用するバージョンの切り替え	ssh version
telnet アクセスの設定	access telnet
ssh アクセスの設定	access ssh
保存	save
コールドスタート	cold start
ファームウェアのアップデート	update
タイムゾーンの追加	timezone
タイムゾーンの表示	show timezone
設定可能なタイムゾーンの表示	show timezone all
NTP を使用するか否かの設定	ntp
NTP サーバーの追加	ntp server add
NTP の設定表示	show ntp
日付と時刻の設定	date
ブリッジの設定	bridge
ブリッジの学習済みの MAC アドレスのクリア	bridge flush
ブリッジの状態表示	show bridge
ファームウェアのバージョン表示	show version
ARP キャッシュのクリア	clear arp
ホスト名の表示	show hostname
設定内容の確認	show setup
IP アドレスの表示	show ip address
静的ルートの表示	show ip route
日付と時刻の表示	show date
DHCP のリース状態の表示	show dhcp
フィルタリングの状態の表示	show filtering
NAT の状態表示	show nat
SSH の状態表示	show ssh
ARP テーブルの表示	show arp
起動からの経過時間の表示	show uptime
無線の受信レベルの表示	show wireless signal strength

設定項目	コマンド
無線設定の表示	show wireless status
MAC アドレスフィルターの表示	show wireless macfilter
AP 間通信フィルターの登録アドレス表示	show wireless wdsfilter
SNMP の設定の表示	show snmp
再起動	restart
Ping	ping
Traceroute	traceroute
無線テストコマンド	wireless txttest
ログアウト	quit / exit / bye
特権モードへの移行	administrator
コマンドヘルプの表示	help
ヒストリーの参照	history

1.7. 各コマンドの説明

注意：設定が終わりましたら設定を保存し再起動してください。

1.7.1 パスワードの設定

入力形式	<code>passwd user</code>
パラメーター	<i>user</i> <ul style="list-style-type: none"> ・ <i>user</i> : ユーザーモードのパスワード ・ <i>administrator</i> : 特権モードのパスワード
説明	パスワードを設定する
ノート	特権モードのパスワード変更は特権モードのみ実行可 入力を中止する場合は Ctrl-D を入力 入力する文字列は英数文字のみ。文字数は8文字までです。 パスワードを紛失すると、設定の参照・更新はできなくなります。

1.7.2 ホスト名の設定

入力形式	<code>hostname hostname</code>
パラメーター	<i>hostname</i> <ul style="list-style-type: none"> ・ ドメイン名まで付加した形式のホスト名
説明	ホスト名を設定する
ノート	特権モードのみ実行可
例	<code>\$ hostname mypc.mydomain.co.jp</code>

1.7.3 IP アドレスの設定

入力形式	<code>ip address Interface Ipaddress Netmask</code>
パラメーター	<i>Interface</i> <ul style="list-style-type: none"> ・ インターフェース名 イーサネット:ether0 無線:wless0 <i>Ipaddress</i> <ul style="list-style-type: none"> ・ IP アドレス <i>Netmask</i> <ul style="list-style-type: none"> ・ ネットマスク
説明	指定したインターフェースに対して IP アドレスを設定する
ノート	特権モードのみ実行可
例	<code>\$ ip address wless0 192.168.0.100 255.255.255.0</code>

1.7.4 静的ルートの設定

入力形式	<code>ip route add <i>Destination Netmask Gateway</i></code>
パラメーター	<i>Destination</i> ・宛先 IP アドレス <i>Netmask</i> ・宛先ネットマスク <i>Gateway</i> ・ゲートウェイの IP アドレス
説明	静的ルートを設定する <i>Netmask</i> を省略するとホストルートの設定となります
ノート	特権モードのみ実行可
例	<pre>\$ ip route add 10.0.0.0 255.0.0.0 192.168.0.1 \$ ip route add default 192.168.0.254 (デフォルトルートの場合) \$ ip route add 192.168.32.3 192.168.33.2 (ホストルートの場合)</pre>

1.7.5 静的ルートの削除

入力形式	<code>ip route delete <i>Destination Netmask Gateway</i></code>
パラメーター	<i>Destination</i> ・宛先 IP アドレス <i>Netmask</i> ・宛先ネットマスク <i>Gateway</i> ・ゲートウェイの IP アドレス
説明	静的ルートを削除する
ノート	特権モードのみ実行可
例	<pre>\$ ip route delete 10.10.0.0 255.255.0.0 \$ ip route delete default (デフォルトルートの場合) \$ ip route delete 192.168.32.3 (ホストルートの場合)</pre>

1.7.6 ICMP Redirect 送出手の設定

入力形式	<code>ip icmp redirect <i>flag</i></code>
パラメーター	<i>flag</i> ・ enable 使用する ・ disable 使用しない
説明	ICMP Redirect 送出手機能を使用するか否かの設定
ノート	特権モードのみ実行可
例	<code>\$ ip icmp redirect enable</code>

1.7.7 無線モードの設定

入力形式	wireless mode <i>mode</i>
パラメーター	<i>mode</i> <ul style="list-style-type: none"> ・ 11b IEEE 802.11b ・ 11g IEEE 802.11g
説明	無線モードの設定
ノート	特権モードのみ実行可
例	\$ wireless mode 11b

1.7.8 無線周波数の設定

入力形式	wireless channel <i>Channel</i>																																
パラメーター	<i>Channel</i> <ul style="list-style-type: none"> ・ 無線の周波数チャンネル 1-13 <table border="1" style="margin-left: 40px; border-collapse: collapse; text-align: center;"> <thead> <tr> <th>チャンネル</th> <th>周波数 (MHz)</th> <th>チャンネル</th> <th>周波数 (MHz)</th> </tr> </thead> <tbody> <tr><td>1</td><td>2412</td><td>8</td><td>2447</td></tr> <tr><td>2</td><td>2417</td><td>9</td><td>2452</td></tr> <tr><td>3</td><td>2422</td><td>10</td><td>2457</td></tr> <tr><td>4</td><td>2427</td><td>11</td><td>2462</td></tr> <tr><td>5</td><td>2432</td><td>12</td><td>2467</td></tr> <tr><td>6</td><td>2437</td><td>13</td><td>2472</td></tr> <tr><td>7</td><td>2442</td><td></td><td></td></tr> </tbody> </table>	チャンネル	周波数 (MHz)	チャンネル	周波数 (MHz)	1	2412	8	2447	2	2417	9	2452	3	2422	10	2457	4	2427	11	2462	5	2432	12	2467	6	2437	13	2472	7	2442		
チャンネル	周波数 (MHz)	チャンネル	周波数 (MHz)																														
1	2412	8	2447																														
2	2417	9	2452																														
3	2422	10	2457																														
4	2427	11	2462																														
5	2432	12	2467																														
6	2437	13	2472																														
7	2442																																
説明	無線の周波数を設定する。																																
ノート	特権モードのみ実行可 無線 LAN 端末の場合は、無線周波数は自動的に無線 LAN 基地局に合わせるため固定での設定はできません。																																
例	\$ wireless channel 3																																

1.7.9 無線送信速度の設定

入力形式	wireless txrate <i>Rate</i>																																																						
パラメーター	<i>Rate</i> <ul style="list-style-type: none"> ・ 無線の送信速度 1 2 5 11 6 9 12 18 24 36 48 54 auto <table border="1" style="margin-left: 40px; border-collapse: collapse; text-align: center;"> <thead> <tr> <th>設定値</th> <th>送信速度</th> <th>モード</th> <th>設定値</th> <th>送信速度</th> <th>モード</th> </tr> </thead> <tbody> <tr><td>1</td><td>1Mbps</td><td>11g/11b</td><td>24</td><td>24Mbps</td><td>11g</td></tr> <tr><td>2</td><td>2Mbps</td><td>11g/11b</td><td>36</td><td>36Mbps</td><td>11g</td></tr> <tr><td>5</td><td>5.5Mbps</td><td>11g/11b</td><td>48</td><td>48Mbps</td><td>11g</td></tr> <tr><td>11</td><td>11Mbps</td><td>11g/11b</td><td>54</td><td>54Mbps</td><td>11g</td></tr> <tr><td>6</td><td>6Mbps</td><td>11g</td><td>auto</td><td>自動</td><td>11g/11b</td></tr> <tr><td>9</td><td>9Mbps</td><td>11g</td><td></td><td></td><td></td></tr> <tr><td>12</td><td>12Mbps</td><td>11g</td><td></td><td></td><td></td></tr> <tr><td>18</td><td>18Mbps</td><td>11g</td><td></td><td></td><td></td></tr> </tbody> </table>	設定値	送信速度	モード	設定値	送信速度	モード	1	1Mbps	11g/11b	24	24Mbps	11g	2	2Mbps	11g/11b	36	36Mbps	11g	5	5.5Mbps	11g/11b	48	48Mbps	11g	11	11Mbps	11g/11b	54	54Mbps	11g	6	6Mbps	11g	auto	自動	11g/11b	9	9Mbps	11g				12	12Mbps	11g				18	18Mbps	11g			
設定値	送信速度	モード	設定値	送信速度	モード																																																		
1	1Mbps	11g/11b	24	24Mbps	11g																																																		
2	2Mbps	11g/11b	36	36Mbps	11g																																																		
5	5.5Mbps	11g/11b	48	48Mbps	11g																																																		
11	11Mbps	11g/11b	54	54Mbps	11g																																																		
6	6Mbps	11g	auto	自動	11g/11b																																																		
9	9Mbps	11g																																																					
12	12Mbps	11g																																																					
18	18Mbps	11g																																																					
説明	無線の送信速度を設定する																																																						
ノート	特権モードのみ実行可 無線 LAN アクセスポイントの場合、無線送信速度の設定は auto になります。																																																						

例	\$ wireless txrate 11
---	-----------------------

1.7.10 無線 WEP 機能設定

入力形式	wireless wep encryption <i>flag</i>
パラメーター	<i>flag</i> <ul style="list-style-type: none"> ・ enable ・・・使用する ・ disable ・・・使用しない
説明	パケット送信時に WEP を使用するか否かを設定する
ノート	特権モードのみ実行可
例	\$ wireless wep encryption enable

1.7.11 無線 WEP キー番号設定

入力形式	wireless wep key use <i>flag</i>
パラメーター	<i>flag</i> <ul style="list-style-type: none"> ・ 1～4
説明	WEP のどのキー番号を使用するかを設定する
ノート	特権モードのみ実行可
例	\$ wireless wep key use 1

1.7.12 無線 WEP キー値設定

入力形式	wireless wep key value <i>flag value</i>
パラメーター	<i>flag</i> <ul style="list-style-type: none"> ・ キー番号 (1～4) <i>value</i> <ul style="list-style-type: none"> ・ ASCII(5char/13char)、又は Hex(0x で始まる最大 10/26 桁の 16 進数)
説明	WEP キー値の設定
ノート	特権モードでのみ実行可 キー長は <i>value</i> の長さで自動判断する。 WEP が無効の時に WEP キーを設定し、save コマンドを実行しても WEP キーの値は保存されません。
例	\$ wireless wep key value MyKey

1.7.13 無線タイプの設定

入力形式	wireless type <i>value</i>
パラメーター	<i>value</i> <ul style="list-style-type: none"> ・ ap: 無線 LAN アクセスポイント(インフラストラクチャ) ・ sta: 無線 LAN 端末(インフラストラクチャ) ・ adhoc: 擬似 Ad-hoc
説明	無線の通信タイプを設定
ノート	特権モードでのみ実行可
例	\$ wireless type ap

1.7.14 無線 SSID の設定

入力形式	wireless ssid value
パラメーター	value ・ SSID(最大 32char.)
説明	SSID を指定する。
ノート	特権モードでのみ実行可
例	\$ wireless ssid NetBSD_IBSS

1.7.15 MAC アドレスフィルター設定

入力形式	wireless macfilter flag
パラメーター	flag ・ enable 使用する ・ disable 使用しない
説明	MAC アドレスフィルター機能の有効、無効の設定
ノート	特権モードのみ実行可。 注) AP 間通信における他の無線 LAN アクセスポイントとの通信、および他の無線 LAN アクセスポイントを介した通信に対して、この MAC アドレスフィルターは適用されない。
例	\$ wireless macfilter enable

1.7.16 MAC アドレスフィルターのアドレス登録

入力形式	wireless macfilter add value
パラメーター	value 通信を許可する MAC アドレスを指定 MAC アドレスは 2 桁ずつセミコロンで区切った 12 桁の数値。 桁数が一致しない場合、0-9、a-f 以外の文字の場合はエラーとする。
説明	無線 LAN 通信を許可する MAC アドレスを設定する。
ノート	特権モードのみ実行可。 設定 MAC アドレスが無い場合は、すべての端末との通信を許可する。 MAC アドレスフィルターの最大エントリー数は 50。
例	\$ wireless macfilter add 11:22:33:44:55:66

1.7.17 MAC アドレスフィルターのアドレス削除

入力形式	wireless macfilter delete value
パラメーター	value 削除する MAC アドレスを指定 MAC アドレスは 2 桁ずつセミコロンで区切った 12 桁の数値。 桁数が一致しない場合、0-9、a-f 以外の文字の場合はエラーとする。 all と入力した場合にはすべてのアドレスを削除する。
説明	無線 LAN 通信を許可する MAC アドレスを削除する。
ノート	特権モードのみ実行可。 設定 MAC アドレスが無い場合は、すべての端末との通信を許可する。
例	\$ wireless macfilter delete 11:22:33:44:55:66 \$ wireless macfilter delete all

1.7.18 MAC アドレスフィルターの表示

入力形式	show wireless macfilter
パラメーター	なし
説明	フィルターの有効、無効およびフィルターに登録されている MAC アドレスを表示する。
ノート	
例	\$ show wireless macfilter

1.7.19 AP 間通信フィルター設定

入力形式	wireless wdsfilter <i>flag</i>
パラメーター	<i>flag</i> <ul style="list-style-type: none"> ・ enable 使用する ・ disable 使用しない
説明	AP 間通信での通信制限の有効、無効の設定
ノート	特権モードのみ実行可。 無効としても登録してある MAC アドレスは消えない。
例	\$ wireless wdsfilter enable

1.7.20 AP 間通信フィルターのアドレス登録

入力形式	wireless wdsfilter add <i>value</i>
パラメーター	<i>value</i> 通信を許可する MAC アドレスを指定 MAC アドレスは 2 桁ずつセミコロンで区切った 12 桁の数値。 桁数が一致しない場合、0-9、a-f 以外の文字の場合はエラーとする。
説明	AP 間通信で通信を許可する AP の MAC アドレスを設定する。
ノート	特権モードのみ実行可。 設定 MAC アドレスが無い場合は、すべての端末との通信を許可する。 MAC アドレスフィルターの最大エントリー数は 10。
例	\$ wireless wdsfilter add 11:22:33:44:55:66

1.7.21 AP 間通信 MAC フィルターのアドレス削除

入力形式	wireless wdsfilter delete <i>value</i>
パラメーター	<i>value</i> 削除する MAC アドレスを指定 MAC アドレスは 2 桁ずつセミコロンで区切った 12 桁の数値。 桁数が一致しない場合、0-9、a-f 以外の文字の場合はエラーとする。 all と入力した場合にはすべてのアドレスを削除する。
説明	AP 間通信で通信を許可する AP の MAC アドレスを削除する。
ノート	特権モードのみ実行可。 設定 MAC アドレスが無い場合は、すべての端末との通信を許可する。
例	\$ wireless wdsfilter delete 11:22:33:44:55:66 \$ wireless wdsfilter delete all

1.7.22 AP 間通信フィルターの登録アドレス表示

入力形式	show wireless wdsfilter
パラメーター	なし
説明	フィルターの有効、無効およびフィルターに登録されている AP の MAC アドレスを表示する。
ノート	
例	\$ show wireless wdsfilter

1.7.23 ステルス AP の設定

入力形式	wireless ssidsuppress <i>flag</i>
パラメーター	<i>flag</i> <ul style="list-style-type: none"> ・ enable 使用する ・ disable 使用しない
説明	wireless type が ap 時にビーコンから SSID 情報をなくす
ノート	特権モードのみ実行可。
例	\$ wireless ssidsuppress enable

1.7.24 RIP を使用するか否かの設定

入力形式	rip <i>flag</i>
パラメーター	<i>flag</i> <ul style="list-style-type: none"> ・ enable ……使用する ・ disable ……使用しない
説明	RIP を使用するか否かを設定する
ノート	特権モードのみ実行可
例	\$ rip enable

1.7.25 RIP を静的経路を送信するか否かの設定

入力形式	rip static-supply <i>flag</i>
パラメーター	<i>flag</i> <ul style="list-style-type: none"> ・ enable ……静的経路を送信する ・ disable ……静的経路を送信しない
説明	RIP で静的経路を送信するか否かを設定する
ノート	特権モードのみ実行可
例	\$ rip static-supply enable

1.7.26 RIP の動作の設定

入力形式	<code>rip action interface action</code>
パラメーター	<i>interface</i> <ul style="list-style-type: none"> ・ インターフェース名 <i>action</i> <ul style="list-style-type: none"> ・ <code>supply</code> . . . 経路の送信および受信を行う ・ <code>listen</code> . . . 経路の受信のみを行う ・ <code>disable</code> . . . 経路の送信も受信も行わない
説明	RIP の動作を設定
ノート	特権モードのみ実行可
例	<code>\$ rip action wless0 supply</code>

1.7.27 RIP のバージョンの設定

入力形式	<code>rip version interface version</code>
パラメーター	<i>interface</i> <ul style="list-style-type: none"> ・ インターフェース名 <i>version</i> <ul style="list-style-type: none"> ・ <code>ripv2</code> . . . RIPv2(マルチキャスト)を使用する ・ <code>ripv12</code> . . . RIPv2(マルチキャスト)、RIPv1 (ブロードキャスト)を使用する ・ <code>ripv1</code> . . . RIPv1 (ブロードキャスト)を使用する
説明	RIP のバージョンを設定
ノート	特権モードのみ実行可
例	<code>\$ rip version wless0 ripv2</code>

1.7.28 フィルターを使用するか否かの設定

入力形式	<code>filter flag</code>
パラメーター	<i>flag</i> <ul style="list-style-type: none"> ・ <code>enable</code> . . . 使用する ・ <code>disable</code> . . . 使用しない
説明	IP フィルターを使用するか否かを設定する
ノート	特権モードのみ実行可
例	<code>\$ filter enable</code>

1.7.29 フィルターの設定

入力形式	<code>filter add number action inout [log level facility.level] [quick] [on interface] [proto proto] [from [!] address [port] to [!] address [port]][flags] [with] [keep] [group]</code>
パラメーター	<p><i>number</i></p> <ul style="list-style-type: none"> 0-65535 . . . フィルター番号 <p><i>action</i></p> <ul style="list-style-type: none"> block . . . パケットを破棄する印を付ける pass . . . パケットを通過する印を付ける <p><i>inout</i></p> <ul style="list-style-type: none"> in . . . インターフェースから入り、RGW に入るパケットに対するルール out . . . RGW からインターフェースに出るパケットに対するルール <p><i>log</i></p> <ul style="list-style-type: none"> log . . . フィルタリングを syslog 出力する際に指定する level . . . level キーワードに続けて、syslog の facility と level を指定 facility . . . syslog の facility(auth,user,daemon) level . . . syslog の level(info,notice,warning,err...) <p>後述の syslog コマンドで指定された host へ転送される</p> <p><i>quick</i></p> <ul style="list-style-type: none"> quick . . . ルールを即座に適応する <p><i>on interface</i></p> <ul style="list-style-type: none"> on ether0 wless0 lo0 . . . インターフェースを指定 <p><i>proto</i></p> <ul style="list-style-type: none"> tcp/udp udp tcp icmp <p><i>address</i></p> <ul style="list-style-type: none"> any 1.2.3.4/24 形式 1.2.3.4 mask 255.255.255.0 形式 <p><i>port</i></p> <ul style="list-style-type: none"> port{= != < > <= >= eq ne lt gt le ge}番号 <p><i>flags</i></p> <ul style="list-style-type: none"> TCP フラグである FSRPAU の組み合わせ proto tcp 時に指定可能 (F=FIN,S=SYN,R=RST,P=PUSH,A=ACK,U=URG) <p><i>with</i></p> <ul style="list-style-type: none"> with ipopts . . . IP オプション付 with short . . . 短すぎるパケット with frag . . . フラグメント化されたパケット <p><i>keep</i></p> <ul style="list-style-type: none"> keep state . . . セッションの状態を管理する keep state によるフィルター制御を行う <p><i>group</i></p> <ul style="list-style-type: none"> head N . . . 新規グループ N を作成 group N . . . ルールをグループ N に入れる
説明	IP パケットのフィルタリングを設定する
ノート	特権モードのみ実行可。フィルター番号によってソートされ昇順で設定される。
例	<code>\$ filter add 100 block out proto tcp from 100.100.0.0/16 to any port = 80</code>

1.7.30 フィルターの削除

入力形式	<code>filter delete <i>number</i></code>
パラメーター	<i>number</i> ・ 0-65535 …… フィルター番号
説明	IP パケットのフィルタリングを削除する
ノート	特権モードのみ実行可
例	<code>\$ filter delete 100</code>

1.7.31 NAT を使用するか否かの設定

入力形式	<code>nat <i>flag</i></code>
パラメーター	<i>flag</i> ・ enable …… 使用する ・ disable …… 使用しない
説明	NAT を使用するか否かの設定
ノート	特権モードのみ実行可
例	<code>\$ nat enable</code>

1.7.32 NAT の map アクションの設定

入力形式	<code>nat add map <i>number interface address1 -> address2</i> [portmap <i>proto ports</i> proxy port <i>portname tag/protocol</i>]</code>
パラメーター	<i>number</i> ・ 0-255 …… NAT 番号 (nat add *コマンドで共通) <i>interface</i> ・ インターフェース名 <i>address1</i> ・ プライベート側 IP アドレス ・ 1234/24 形式 <i>address2</i> ・ グローバル側 IP アドレス ・ 1234/24 形式 <i>proto</i> ・ tcp/udp udp tcp <i>ports</i> ・ auto {ポート番号の下限}:{ポート番号の上限} 形式 <i>portname</i> ・ ポートの名前 (例: ftp) <i>tag</i> ・ タグ <i>protocol</i> ・ プロトコル
説明	NAT の map アクションを設定する
ノート	特権モードでのみ実行可。nat 設定に共通な nat 番号によってソートされ昇順で設定される。
例	<code>\$ nat add map 10 ether0 10.0.0.0/8 -> 210.100.100.101/32 portmap tcp/udp 1025:65000</code> <code>\$ nat add map 15 ether0 10.0.0.0/8 -> 0/32 proxy port ftp ftp/tcp</code>

1.7.33 NAT の bimap アクションの設定

入力形式	<code>nat add bimap <i>number interface address1 -> address2</i></code>
パラメータ	<p><i>number</i></p> <ul style="list-style-type: none"> ・ 0-255 . . . NAT 番号 (nat add *コマンドで共通) <p><i>interface</i></p> <ul style="list-style-type: none"> ・ インターフェース名 <p><i>address1</i></p> <ul style="list-style-type: none"> ・ プライベート側 IP アドレス ・ 1234/24 形式 <p><i>address2</i></p> <ul style="list-style-type: none"> ・ グローバル側 IP アドレス ・ 1234/24 形式
説明	NAT の bimap アクションを設定する
ノート	特権モードでのみ実行可。nat 設定に共通な nat 番号によってソートされ昇順で設定される。
例	<code>\$ nat add bimap 3 ether0 10.0.0.5/32 -> 210.100.100.101/32</code>

1.7.34 NAT の rdr アクションの設定

入力形式	<code>nat add rdr <i>number interface address1 port port -> address2 port port [proto]</i></code>
パラメータ	<p><i>number</i></p> <ul style="list-style-type: none"> ・ 0-255 . . . NAT 番号 (nat add *コマンドで共通) <p><i>interface</i></p> <ul style="list-style-type: none"> ・ インターフェース名 <p><i>address1</i></p> <ul style="list-style-type: none"> ・ プライベート側 IP アドレス ・ 1234/24 形式 <p><i>address2</i></p> <ul style="list-style-type: none"> ・ グローバル側 IP アドレス <p><i>port</i></p> <ul style="list-style-type: none"> ・ ポート番号 <p><i>proto</i></p> <ul style="list-style-type: none"> ・ tcp/udp tcp udp (既定値 : tcp)
説明	NAT の rdr アクションを設定する
ノート	特権モードでのみ実行可。nat 設定に共通な nat 番号によってソートされ昇順で設定される。
例	<code>\$ nat add rdr 5 ether0 10.0.0.5/32 port 7777 -> 210.100.100.101 port 20</code>

1.7.35 NAT の削除

入力形式	<code>nat delete <i>number</i></code>
パラメータ	<p><i>number</i></p> <ul style="list-style-type: none"> ・ 0-255 . . . NAT 番号
説明	NAT のエントリを削除する
ノート	特権モードでのみ実行可
例	<code>\$ nat delete 3</code>

1.7.36 DHCP サーバーを使用するか否かの設定

入力形式	<code>dhcp flag [interface]</code>
パラメーター	<code>flag</code> <ul style="list-style-type: none"> ・ <code>enable</code> . . . 使用する ・ <code>disable</code> . . . 使用しない <code>interface</code> <ul style="list-style-type: none"> ・ DHCP サーバー機能を使用するインターフェース名 省略時は <code>ether0</code> とみなす。 <code>disable</code> 時は不要
説明	DHCP サーバーの機能を使用するか否かの設定をする
ノート	特権モードのみ実行可 配布する IP アドレスが、対応するインターフェースのネットワークになければならない。 ※37 ページの制限事項を参照してください。
例	<code>\$ dhcp enable</code>

1.7.37 DHCP サーバーで配布する IP アドレスの設定

入力形式	<code>dhcp pool ipaddress1 ipaddress2</code>
パラメーター	<code>ipaddress1</code> <ul style="list-style-type: none"> ・ IP アドレスの先頭 <code>ipaddress2</code> <ul style="list-style-type: none"> ・ IP アドレスの最後
説明	DHCP サーバーで配布する IP アドレスの範囲を設定する
ノート	特権モードのみ実行可
例	<code>\$ dhcp pool 192.168.0.1 192.168.0.254</code>

1.7.38 DHCP サーバーで配布する IP アドレスの有効期限

入力形式	<code>dhcp expire period</code>
パラメーター	<code>period</code> <ul style="list-style-type: none"> ・ IP アドレスの有効期間 (秒)
説明	DHCP サーバーで配布する IP アドレスの有効期間の設定をする
ノート	特権モードのみ実行可
例	<code>\$ dhcp expire 7200</code>

1.7.39 DHCP サーバーで配布する DNS サーバーの設定

入力形式	<code>dhcp dns add ipaddress</code>
パラメーター	<code>ipaddress</code> <ul style="list-style-type: none"> ・ DNS サーバーの IP アドレス
説明	DHCP サーバーで配布する DNS サーバーを設定する
ノート	特権モードのみ実行可。最大 2 個登録可です。
例	<code>\$ dhcp dns add 210.100.100.101</code>

1.7.40 DHCP サーバーで配布する DNS サーバーの削除

入力形式	<code>dhcp dns delete ipaddress</code>
パラメーター	<code>ipaddress</code> <ul style="list-style-type: none"> ・ DNS サーバーの IP アドレス
説明	DHCP サーバーで配布する DNS サーバーを削除する
ノート	特権モードのみ実行可
例	<code>\$ dhcp dns delete 210.100.100.101</code>

1.7.41 DHCP サーバーで配布するドメイン名の設定

入力形式	<code>dhcp domain <i>domainname</i></code>
パラメーター	<i>domainname</i> ・ドメイン名
説明	DHCP サーバーで配布するドメイン名を設定する。 <i>domainname</i> を省略するとドメイン名の配布は行わない
ノート	特権モードのみ実行可
例	<code>\$ dhcp domain example.com</code>

1.7.42 DHCP サーバーで配布するデフォルトルートの設定

入力形式	<code>dhcp defaultroute [<i>defaultroute</i>]</code>
パラメーター	<i>defaultroute</i> ・デフォルトルートの IP アドレス
説明	DHCP サーバーで配布するデフォルトルートを設定する。 <i>defaultroute</i> を省略するとデフォルトルートの配布は行わない
ノート	特権モードのみ実行可
例	<code>\$ dhcp defaultroute 172.30.100.2</code>

1.7.43 DHCP リレーエージェントの設定

入力形式	<code>dhcp relay <i>flag</i></code>
パラメーター	<i>flag</i> ・IP アドレス . . . DHCP サーバーの IP アドレス ・disable . . . 使用しない
説明	DHCP リレーエージェントの設定をする
ノート	特権モードのみ実行可
例	<code>\$ dhcp relay 172.10.0.1</code>

1.7.44 SNMP サーバー機能を使用するか否かの設定

入力形式	<code>snmp <i>flag</i></code>
パラメーター	<i>flag</i> ・enable . . . 使用する ・disable . . . 使用しない
説明	SNMP サーバーを使用するか否かの設定をする
ノート	特権モードのみ実行可
例	<code>\$ snmp enable</code>

1.7.45 SNMP コミュニティ名の設定

入力形式	<code>snmp community <i>name</i></code>
パラメーター	<i>name</i> ・コミュニティ名
説明	SNMP コミュニティ名の設定をする。最大 31 文字まで。スペースを入れることは出来ません。
ノート	特権モードのみ実行可
例	<code>\$ snmp community secret</code>

1.7.46 SNMP の location の設定

入力形式	snmp location <i>str</i>
パラメーター	<i>str</i> ・ 文字列
説明	SNMP の location の設定をする。最大 255 文字まで
ノート	特権モードのみ実行可
例	\$ snmp location Gotanda

1.7.47 SNMP の contact の設定

入力形式	snmp contact <i>str</i>
パラメーター	<i>str</i> ・ 文字列
説明	SNMP の contact の設定をする。最大 255 文字まで
ノート	特権モードのみ実行可
例	\$ snmp contact Administrator<admin@example.com>

1.7.48 SNMP のアクセスの設定

入力形式	snmp access [<i>ipaddress / network</i>]
パラメーター	<i>ipaddress</i> ・ IP アドレス “all” <i>network</i> ・ ネットマスク 255.255.255.0 形式を付与したネットワーク・アドレス
説明	SNMP で RGW にアクセス可能なホストの範囲を指定する
ノート	特権モードでのみ実行可。 IP フィルターのチェックが先に働き、その後このアクセスの設定によるチェックが行われます。
例	\$ snmp access 192.168.0.0 255.255.255.0

1.7.49 SNMP TRAP の設定

入力形式	snmp trap <i>mode flag [community [port]]</i>
パラメーター	<i>mode</i> ・ v1 v2 inform v1:snmp v1 v2:snmp v2 inform:NOTIFICATION <i>flag</i> ・ IP アドレス . . . trap を送信するホストの IP アドレス ・ disable . . . 使用しない <i>community</i> ・ trap 送信に使用するコミュニティー名 disable 時は不要 <i>port</i> ・ ポート番号 (省略時は 162 を使用) disable 時は不要
説明	再起動時・不正アクセスを検出した際、snmp trap を送信するホストと trap のタイプを指定する。 コミュニティー名にスペースを入れることは出来ません。
ノート	特権モードでのみ実行可。
例	\$ snmp trap v2 210.100.100.101 root

1.7.50 syslog 機能を使用するか否かの設定

入力形式	<code>syslog <i>flag</i></code>
パラメーター	<i>flag</i> <ul style="list-style-type: none"> ・ enable . . . 使用する ・ disable . . . 使用しない
説明	syslog 機能を使用するか否かを設定する
ノート	特権モードでのみ実行可
例	<code>\$ syslog enable</code>

1.7.51 syslog を転送するホストの設定

入力形式	<code>syslog host <i>ipaddress</i></code>
パラメーター	<i>ipaddress</i> <ul style="list-style-type: none"> ・ IP アドレス . . . syslog を転送するホストの IP アドレス
説明	syslog を転送するホストの IP アドレスを設定する
ノート	特権モードでのみ実行可
例	<code>\$ syslog host 172.10.0.1</code>

1.7.52 syslog を転送するファシリティの設定

入力形式	<code>syslog add <i>facility level</i></code>
パラメーター	<i>facility</i> <ul style="list-style-type: none"> ・ kern user auth authpriv syslog cron ftp uucp local0~7 daemon * <i>level</i> <ul style="list-style-type: none"> ・ emerg alert crit err warning notice info debug none *
説明	syslog で転送するファシリティ及びそのレベルを設定する。
ノート	特権モードでのみ実行可。
例	<code>\$ syslog add * info</code>

1.7.53 syslog を転送するファシリティの削除

入力形式	<code>syslog delete <i>facility level</i></code>
パラメーター	<i>facility</i> <ul style="list-style-type: none"> ・ kern user auth authpriv syslog cron ftp uucp local0~7 daemon * <i>level</i> <ul style="list-style-type: none"> ・ emerg alert crit err warning notice info debug none *
説明	削除する syslog のファシリティ及びそのレベルを設定する。
ノート	特権モードでのみ実行可。
例	<code>\$ syslog delete kern crit</code>

1.7.54 SSH のホストキーの生成

入力形式	<code>ssh keygen version [overwrite]</code>
パラメーター	<p><i>version</i></p> <ul style="list-style-type: none"> ・ v1: SSHv1 のホストキーを生成 ・ v2: SSHv2 のホストキーを生成 ・ v12:SSHv1、SSHv2 のホストキーを生成 <p><i>overwrite</i></p> <p>既に生成したホストキーを上書きする場合に指定する。</p>
説明	RGW の SSH ホストキーを生成する。
ノート	特権モードでのみ実行可。 本コマンドの完了には、しばらく時間がかかります。
例	<code>\$ ssh keygen v1</code>

1.7.55 SSH の認証方法の設定

入力形式	<code>ssh authentication way</code>
パラメーター	<p><i>way</i></p> <ul style="list-style-type: none"> ・ passwd: パスワード認証が有効 ・ key: 公開鍵認証が有効 ・ both: パスワード認証・公開鍵ともに認証が有効
説明	SSH の認証方法を指定する。
ノート	特権モードでのみ実行可。 工場出荷時は both
例	<code>\$ ssh authentication key</code>

1.7.56 SSH の公開鍵のダウンロード

入力形式	<code>ssh keyget version URL</code>
パラメーター	<p><i>version</i></p> <ul style="list-style-type: none"> ・ v1: SSHv1 の公開鍵をダウンロードする ・ v2: SSHv2 の公開鍵をダウンロードする <p><i>URL</i></p> <ul style="list-style-type: none"> ・ 公開鍵がある URL
説明	RGW に公開鍵をダウンロードする。
ノート	本コマンドでダウンロードした公開鍵でのアクセスが有効になります。 特権モードでのみ実行可。
例	<code>\$ ssh keyget v1 http://192.168.0.100/~rgw/identity.pub</code>

1.7.57 SSH の使用するバージョンの切り替え

入力形式	<code>ssh version <i>version</i></code>
パラメーター	<i>version</i> <ul style="list-style-type: none"> ・ v1: SSHv1 ・ v2: SSHv2 ・ v12:両方
説明	RGW で使用する SSH のバージョンを指定する。
ノート	本コマンドでダウンロードした公開鍵でのアクセスが有効になります。 特権モードでのみ実行可。
例	<code>\$ ssh version v12</code>

1.7.58 telnet アクセスの設定

入力形式	<code>access telnet [<i>ipaddress</i> / <i>network</i>]</code>
パラメーター	<i>ipaddress</i> <ul style="list-style-type: none"> ・ IP アドレス “all” <i>network</i> <ul style="list-style-type: none"> ・ ネットマスク 255.255.255.0 形式のネットワーク・アドレス
説明	telnet で RGW にアクセス可能なホストの範囲を指定する
ノート	特権モードでのみ実行可。 IP フィルターのチェックが先に働き、その後このアクセスの設定によるチェックが行われます。

1.7.59 SSH アクセスの設定

入力形式	<code>access ssh [<i>ipaddress</i> / <i>network</i>]</code>
パラメーター	<i>ipaddress</i> <ul style="list-style-type: none"> ・ IP アドレス “all” <i>network</i> <ul style="list-style-type: none"> ・ ネットマスク 255.255.255.0 形式のネットワーク・アドレス
説明	ssh で RGW にアクセス可能なホストの範囲を指定する
ノート	特権モードでのみ実行可。 IP フィルターのチェックが先に働き、その後このアクセスの設定によるチェックが行われます。

1.7.60 保存

入力形式	<code>save</code>
パラメーター	なし
説明	設定内容を保存する
ノート	特権モードでのみ実行可。システムファイルに反映されると共に、設定ファイルがコマンドの形式で保存される。

1.7.61 static ARP の設定

入力形式	<code>arp add <i>ipaddress macaddress</i></code>
パラメーター	<i>ipaddress</i> ・ IP アドレス <i>macaddress</i> ・ MAC アドレス
説明	static ARP のエントリーを設定する
ノート	特権モードでのみ実行可。
例	<code>\$ arp add 10.0.0.1 11:22:33:44:55:66</code>

1.7.62 ARP の削除

入力形式	<code>arp delete <i>ipaddress</i></code>
パラメーター	<i>ipaddress</i> ・ IP アドレス
説明	IP アドレスに対応する ARP エントリーを削除する
ノート	特権モードでのみ実行可。
例	<code>\$ arp delete 10.0.0.1</code>

1.7.63 コールドスタート

入力形式	<code>cold start</code>
パラメーター	なし
説明	機器を工場出荷時状態に戻す
ノート	特権モードのみ実行可。設定を工場出荷時に戻した後に、再起動する。

1.7.64 ファームウェアのアップデート

入力形式	<code>update <i>url</i></code>
パラメーター	<i>url</i> ・ ダウンロードするファイルの URL
説明	ファイルをダウンロードし、ファームウェアをアップデートする アップデートに成功すると、本機は再起動する。
ノート	特権モードのみ実行可

1.7.65 タイムゾーンの追加

入力形式	<code>timezone <i>Zonename</i></code>
パラメーター	<i>Zonename</i> ・ タイムゾーン名
説明	タイムゾーンを設定する。 タイムゾーンの設定の保存は自動的に行われる。
ノート	特権モードのみ実行可
例	<code>\$timezone Japan</code>

1.7.66 タイムゾーンの表示

入力形式	show timezone
パラメーター	なし
説明	現在のタイムゾーンを表示する
ノート	特権モードのみ実行可
例	\$ show timezone

1.7.67 設定可能なタイムゾーンの表示

入力形式	show timezone all
パラメーター	なし
説明	設定可能なタイムゾーンを全て表示する
ノート	特権モードのみ実行可
例	\$ show timezone all

1.7.68 NTP を使用するか否かの設定

入力形式	ntp flag
パラメーター	<i>flag</i> <ul style="list-style-type: none"> ・ enable . . . 使用する ・ disable . . . 使用しない
説明	NTP を使用するか否かの設定
ノート	特権モードのみ実行可 工場出荷状態で disable
例	\$ ntp enable

1.7.69 NTP サーバーの追加

入力形式	ntp server add <i>Server</i>
パラメーター	<i>Server</i> <ul style="list-style-type: none"> ・ NTP サーバー
説明	参照する NTP サーバーを設定する。
ノート	特権モードのみ実行可
例	\$ ntp server add 192.168.0.1

1.7.70 NTP の設定表示

入力形式	show ntp
パラメーター	なし
説明	NTP の設定を表示する
ノート	特権モードのみ実行可
例	\$ show ntp

1.7.71 日付と時刻の設定

入力形式	<code>date yyyy/mm/dd HH:MM</code>
パラメーター	<code>yyyy</code> ・年 <code>mm</code> ・月 <code>dd</code> ・日 <code>HH</code> ・時 <code>MM</code> ・分
説明	日付と時刻を設定する
ノート	特権モードのみ実行可。 本コマンドは、設定した時点でシステムに反映される
例	<code>\$ date 2000/12/24 12:30</code>

1.7.72 ブリッジの設定

入力形式	<code>bridge flag</code>
パラメーター	<code>flag</code> ・enable 使用する ・disable 使用しない
説明	ブリッジ機能を使用するか否かの設定を行う
ノート	特権モードのみ実行可 ブリッジは無線 LAN アクセスポイント時のみ有効
例	<code>\$ bridge enable</code>

1.7.73 ブリッジの学習済み MAC アドレスのクリア

入力形式	<code>bridge flush</code>
パラメーター	なし
説明	学習した MAC アドレスをクリアする
ノート	特権モードのみ実行可
例	<code>\$ bridge flush</code>

1.7.74 ブリッジの状態表示

入力形式	<code>show bridge</code>
パラメーター	なし
説明	ブリッジの状態を表示する
ノート	
例	<code>\$ show bridge</code>

1.7.75 再起動

入力形式	restart
パラメーター	なし
説明	システムを再起動する
ノート	特権モードのみ実行可。reboot でも可。

1.7.76 ARP のクリア

入力形式	clear arp
パラメーター	なし
説明	ARP テーブルをクリアする
ノート	特権モードのみ実行可。

1.7.77 ホスト名の表示

入力形式	show hostname
パラメーター	なし
説明	システムに登録されているホスト名を表示する
ノート	

1.7.78 IP アドレスの表示

入力形式	show ip address
パラメーター	なし
説明	システムに登録されている IP アドレスを表示する
ノート	イーサネットと無線に割当てられた IP アドレスを表示する

1.7.79 静的ルートの表示

入力形式	show ip route
パラメーター	なし
説明	システムに登録されている静的ルートを表示する
ノート	カーネルが自動的に生成するルート（直接接続されたネットワークに対するルートなど）は表示しない

1.7.80 DHCP のリース状態の表示

入力形式	show dhcp
パラメーター	なし
説明	DHCP のリース状態を表示する
ノート	リース時間表示のタイムゾーンは GMT です。

1.7.81 フィルタリング状態の表示

入力形式	show filtering
パラメーター	なし
説明	フィルタリングの状態（ルールにマッチしたパケット数）を表示する
ノート	各ルールの先頭の数字はルールにマッチしたパケット数であり、フィルター番号ではない。フィルター番号を表示するには、show setup コマンドを使用すること。

1.7.82 ARP テーブルの表示

入力形式	show arp
パラメーター	なし
説明	ARP テーブルの表示する
ノート	

1.7.83 起動時からの経過時間の表示

入力形式	show uptime
パラメーター	なし
説明	起動してからの経過時間を表示する
ノート	

1.7.84 ファームウェアのバージョンの表示

入力形式	show version
パラメーター	なし
説明	RGW のファームウェア・バージョン情報を表示する
ノート	

1.7.85 日付と時刻の表示

入力形式	show date
パラメーター	なし
説明	現在の日付と時刻を表示する
ノート	

1.7.86 無線の受信レベル表示

入力形式	show wireless signal strength
パラメーター	なし
説明	時刻、無線周波数(chan)、受信レベル(rssi)、送信速度(rate)を 0.5 秒間隔で表示する
ノート	

1.7.87 無線設定の表示

入力形式	show wireless status
パラメーター	なし
説明	無線のステータスを表示する
ノート	このコマンドは内部ドライバーの状態を表示する保守用の物です。設定値の確認には show setup コマンドを使用してください。

1.7.88 SNMP 設定の表示

入力形式	show snmp
パラメーター	なし
説明	SNMP 設定を表示する
ノート	

1.7.89 SSH 設定の表示

入力形式	show ssh
パラメーター	なし
説明	SSH の状態を表示する
ノート	

1.7.90 設定内容の確認

入力形式	show setup
パラメーター	なし
説明	設定内容を確認する
ノート	

1.7.91 コマンド形式の保存内容の確認

入力形式	show config
パラメーター	なし
説明	コマンド形式の保存内容を表示する
ノート	

1.7.92 ping

入力形式	ping <i>Ipaddress</i>
パラメーター	Ipaddress ・相手先 IP アドレス
説明	相手先 IP アドレスに対して ICMP Echo を発行する
ノート	

1.7.93 traceroute

入力形式	traceroute <i>Ipaddress</i>
パラメーター	Ipaddress ・相手先 IP アドレス
説明	相手先 IP アドレスに対して traceroute を実行する
ノート	

1.7.94 無線テストコマンド

入力形式	wireless txttest [long]
パラメーター	long ・ 1472 バイト長の ICMP エコー要求を送信する。このパラメーターを省略した場合には 64 バイト長となる。
説明	無線側ネットワークのブロードキャストアドレスに対して ICMP エコー要求を送信する。 コンソールには現在の時刻、周波数(chan)、受信レベル(rssi)、送信速度(rate)が 0.5 秒間隔で表示される。
ノート	特権モードでのみ実行可

1.7.95 ログアウト

入力形式	quit 又は exit 又は bye
パラメーター	なし
説明	コマンドラインシェルからログアウトする
ノート	

1.7.96 特権モードへの移行

入力形式	administrator
パラメーター	なし
説明	特権モードへ移行する
ノート	

1.7.97 コマンドヘルプの表示

入力形式	help <i>command</i>
パラメーター	<i>command</i> ・ コマンド名
説明	コマンドのヘルプを表示する
ノート	

1.7.98 ヒストリーの参照

入力形式	history
パラメーター	なし
説明	現在のヒストリーを表示する
ノート	

・注意事項

コマンドラインシェルはシリアル通信、telnet と SSH で行う方法がありますが、同時に複数のコマンドラインシェルを動作させると以下のメッセージが表示されます。

WARNING:another administrator is still alive. (既にコマンドラインシェルが動作中であることが検出された場合)

ATTENTION:Two or more administrator are active now!!! (動作中の全てのコマンドラインシェルに対して表示される)

同時に別々の設定を行うと、予期しない設定になることがあります。このような場合には、必要最小限の設定を行い、**restart** などを行うことを推奨します。

コマンドラインシェルは無通信時間を監視します。約 300 秒間、入力がない場合には、自動的にセッションを切断します。ただし、各コマンド実行中の無通信監視は行いません。

設定の変更を行った場合は必ず **SAVE** コマンドを実行してください。**SAVE** コマンドを実行することにより設定は保存され、電源断や再起動を行っても設定値が復元されます。

1.8. ファームウェアアップデート手順

1.8.1 準備するもの

- http または ftp サーバー 1 台
- RGW へログインするための端末 1 台
- 新しいファームウェア

1.8.2 アップデート手順

1. http または ftp サーバー(以下、サーバーと表記します)に新しいファームウェアをコピーします。
2. サーバーと RGW を接続し、TCP/IP で通信できるようにします。
3. 端末からシリアルインターフェース または telnet にて、RGW にログインします。
4. 特権モードになり `update` コマンドでファームウェアを更新します。
`$ update ファームウェアの URL`
 例) `$ update http://www.example.com/rgw5000-xxx.bin`
5. ファームウェアの更新後、機器は自動的に再起動します。

ファームウェアのバージョンは `show version` コマンドで確認できます。

例) `> show version`

RGW5000 Ver.1.2

Build date: Nov 1 22:45:38 JST 2005

1.8.3 アップデート例

NetBSD/evbsh3 (router) (console)

login: admin

Password:

Copyright (c) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003

The NetBSD Foundation, Inc. All rights reserved.

Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994

The Regents of the University of California. All rights reserved.

```
> administrator
Password:
$ update http://www.example.com/rgw5000-xxx.bin
Connected to 58.156.228.185.
220-
220 example.com FTP server (NetBSD-ftpd 20020615) ready.
331 Guest login ok, type your name as password.
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
200 Type set to I.
250 CWD command successful.
local: /var/chroot/ftpd/update.firm remote: rgw5000-xxx.bin
229 Entering Extended Passive Mode (||65041|)
150 Opening BINARY mode data connection for 'rgw5000-xxx.bin' (5212172 bytes).
100% |*****| 5090 KB 3.49 MB/s 00:00 ETA
226 Transfer complete.
5212172 bytes received in 00:01 (3.46 MB/s)
221-
    Data traffic for this session was 5212172 bytes in 1 file.
    Total traffic for this session was 5213029 bytes in 1 transfer.
221 Thank you for using the FTP service on example.com.
object information:
T[p(M#:0x10002,c:683208171,l:0x4f87f6,al:0x4f87f8,T#:0x10002)]
[c:683208171,al:0x4f87f6]
updating firmware...
wwwwwwwwwwwwwwww
update completed.
Sep 30 11:28:43 reboot: rebooted by admin
rebooting...
```

1.9. 制限事項

コマンドラインシェルには以下の制限があります。

1.9.1 DHCP

- DHCP を起動するには、DHCP の各項目を設定してから

```
$ dhcp enable
```

とコマンドを入力する必要があります。

また DHCP サーバー機能は DHCP リレーエージェント機能と同時には使用できません。

1.9.2 NTP 機能

- RGW5000 の NTP 機能を使用する場合に、NTP サーバーとの時刻差が 1000 秒以上ある場合、時刻同期をせずに NTP 機能が停止するようになっております。ご使用の際には RGW5000 の時刻を確認して頂き NTP サーバーとの時刻差が 1000 秒以下になるように、時刻を設定してください。
- NTP サーバーの NTP reply パケットに Reference Clock ID が定義されていないと時刻の同期ができません。NTP サーバーが RFC-1305、RFC-1059、RFC-1119 のいずれかに準拠していることをご確認ください。

1.9.3 AP 間通信機能

- 本製品の AP 間通信は、本製品同士(1 対向)でご使用ください。
- AP 間通信において無線越しの無線端末に対して MAC アドレスフィルターを設定しても適用されません。

1.9.4 その他

「3. 設定のためのヒント」をご覧ください。

2. 工場出荷時の設定

工場出荷時の設定は以下のとおりである。

設定情報	内容
ユーザーモードのアカウント (CLI)	“admin”
ユーザーモードのパスワード (CLI)	“admin”
特権モードのパスワード (CLI)	“admin”
ホスト名	router
IP アドレスとネットマスク	イーサネット側 : 172.30.100.2/24 無線側 : 10.12.1.2/24
静的ルート	なし
デフォルトルート	10.12.1.1
MAC アドレスフィルター	使用しない
AP 間通信フィルター	使用しない
ステルス AP	使用しない
アクセス制御	アクセス制御なし
RIP	使用しない
SNMP	使用しない。trap はなし
DHCP	使用しない
IP Filter	使用しない
NAT	使用しない
ブリッジ	使用しない
SYSLOG	使用しない
SSH 使用バージョン	Ver.1, Ver.2
SSH ホストキーの生成	未生成
SSH 公開鍵ダウンロード	未設定
SSH 認証方式	パスワード認証・公開鍵認証
無線通信モード/タイプ	11b/無線 LAN 端末
WEP	使用する。キー : MAC アドレスから生成される 26 桁の 16 進数、キー・インデックス : 1
NTP	使用しない
タイムゾーン	Japan

3. 設定のためのヒント

本章では、RGW を設定する際のヒントを示します。

3.1. 無線

3.1.1 通信モード

RGW5000 の無線通信には、擬似 Ad-hoc とインフラストラクチャの2つの方式があります。また、インフラストラクチャには親機（無線 LAN アクセスポイント）と子機（無線 LAN 端末）の区別があります。

これらの切替えは、コマンドラインインターフェースの無線タイプ設定を使って行います。なお、擬似 Ad-hoc は弊社製品 RGW2400 の Ad-hoc と互換性がありますが、IEEE 802.11Ad-hoc とは互換性がありません。

無線 LAN アクセスポイントでは、以下の制限があります。

- 無線空間の中継では、IP フィルターが働きません。
- 無線の転送速度は、子機側の設定に依存します。したがって、`wireless txrate` コマンドで設定できません。自動的に `auto` になります。

3.1.2 WEP

RGW が無線空間に送出するデータ (MPDU) を暗号化することができます。この暗号化には秘密鍵方式の WEP (Wired Equivalent Privacy) が利用できます。各 RGW にはそれぞれ4つまでの鍵を登録することができます。暗号化通信を利用するためには、自分と相手の鍵と鍵の ID を共通にする必要があります。

3.1.3 無線中継

RGW 1 台で、無線空間をパケット中継することができます。

中継の方法は2つあります。

無線のタイプが擬似 Ad-hoc の場合、IP 層での中継になります。

インフラストラクチャの場合、無線 LAN アクセスポイントが MAC 層での中継を行います。

ただし、1 台での中継は、同じ無線チャンネルを使った転送になりますので、実効速度が2分の1以下に落ちます。

IP 層での中継の場合、中継を行う局は `ICMP redirect` を送出しないように設定しなけれ

ばなりません。状況により、ホスト・ルーティングも必要になります。詳細は、弊社ホームページをご覧ください。

MAC層での中継は、中継を行う局でのIPフィルタは働きませんのでご注意ください。

RGW 2台を使って、Ethernet同士を接続すると、各RGWは異なる無線チャンネルを使うことができますので、RGW 1台での中継より一般的に実効速度が上がります。

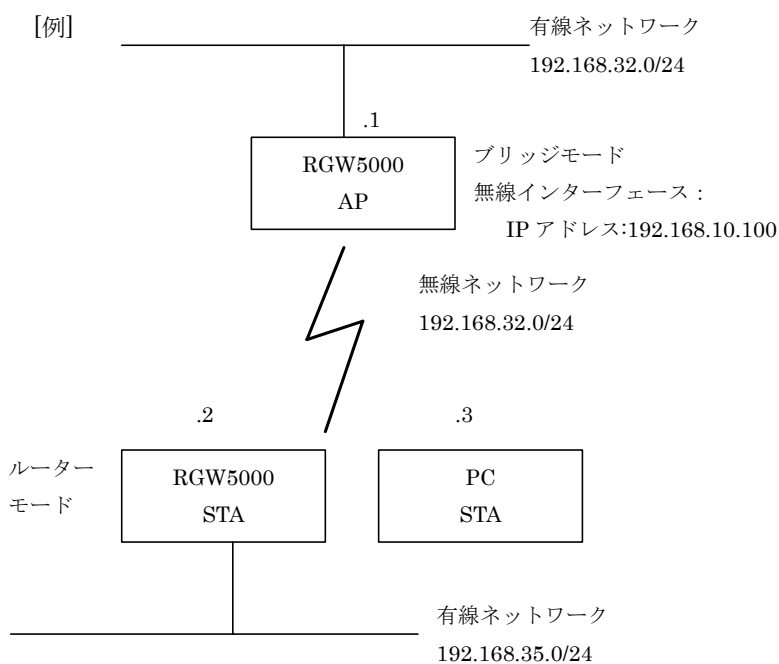
3.1.4 ブリッジモード

ブリッジモードは無線タイプが無線LANアクセスポイントの時のみ可能です。

ブリッジモードに設定すると、有線ネットワークと無線ネットワークがブリッジされて、同じ1つのネットワークとして結合されます。

ブリッジモードで通信する際に、無線側のインターフェースにはIPアドレスは本来不要ですが、ファームウェアの仕様上、仮のIPアドレスを設定ください。

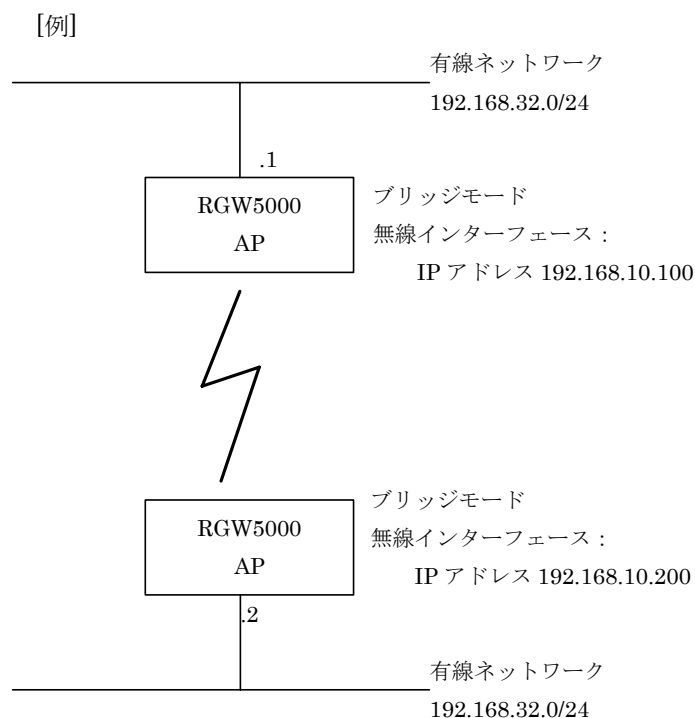
この仮のIPアドレスは有線側のネットワークと異なるネットワークのアドレスを入力ください。



3.1.5 AP 間通信

2 台の無線 LAN アクセスポイントをそれぞれブリッジモードに設定すると、AP 間通信機能により、2 つの有線ネットワーク間をブリッジングすることが可能になります。

ブリッジモードで通信する際に、無線側のインターフェースには IP アドレスは本来不要ですが、ファームウェアの仕様上、仮の IP アドレスを設定ください。この仮の IP アドレスは有線側のネットワークと異なるネットワークのアドレスを入力ください。



3.2. ファイヤーウォール

3.2.1 IP フィルター

IP フィルター・ルールのコマンドは前章で説明していますが、ここでは各パラメータの意味など例を交えて説明します。

ここで、もう一度、フィルター・ルールのコマンドを示します。

```
filter add number action inout [log level facility.level] [quick] [on interface] [proto
```

proto] [from [!] address [port] to [!] address [port]][flags] [with] [keep] [group]

各フィルター・ルールは番号を持ち、RGW が受けた IP パケットはその順番ですべてのルールで評価されます。そして、最後にマッチしたルールに従って処理されます（例外あり、後述）。 RGW の IP フィルターは、デフォルト許可(通過)の設定になっています。つまり、どのルールにもマッチしないパケットは許可されます。なお、RGW に設定する順序とルールが持つフィルター番号は独立したものです。

- **action** には”pass”もしくは”block”を設定し、ルールにマッチしたとき通過させるか破棄するかアクションを指定します。
- **inout** には”in”もしくは”out”を設定し、RGW に入ってくるパケットか RGW から出て行くパケットかを指定します。

```
filter add 10 block in from any to any
filter add 11 pass in from any to any
```

この2つのルールが指定されていた場合、RGW が受信したすべてのパケットは、最初に 10 番のルールがチェックされます。すべてのパケットがマッチし、ここでは **block** (塞ぐ) のアクションになります。さらに次の 11 番のルールがチェックされます。11 番でもすべてのパケットがマッチし、ここでは **pass** (通過) のアクションになります。以上の結果、最後にマッチした 11 番のルールの動作 (**pass=通過**) を行います。結局、以上の2つのルールの場合、全てのパケットが通過します。

- **quick** には”quick”が指定可能です。”quick”が指定されたルールにマッチすると、そのパケットは後続のフィルター・ルールで評価されません。たとえば、ホスト 192.168.1.2 からのパケットを RGW が受け付けないようにするには、このアドレスからパケットを受けた場合、**block** し、それ以降のルールをチェックする必要はありません。そのような場合、**quick** キーワードを指定することで、マッチした場合のアクションを直ちに適応することができます。

```
filter add 15 block in quick from 192.168.1.2 to any
filter add 16 pass in from any to any
```

この設定では、192.168.1.2 からきたパケットは、**quick** 指定で 15 番のルールで **block** されます。次の 16 番のルールで、すべてのパケットを **pass** するようになっています。

すが、15 番のルールにマッチしたパケットは **quick** 指定のため、次のルールのチェックは行われません。

- **on interface** には **wless0**(無線側)もしくは **ether0**(Ethernet 側)の指定が可能です。また、**lo0**(ループバック・デバイス)も指定が可能です。フィルターを有効にすると **lo0** に対する I/O は自動的に **quick pass** されます。RGW 内部には、デバイス **lo0** に IP アドレス **127.0.0.1** を持ち、内部の処理に利用しています。このアドレスには、外部からアクセスすることはできません。逆に、この **lo0** デバイスの **127.0.0.1** に対するアクセスを **block** すると、RGW の動作に支障が発生しますので、ご注意ください。この **on interface** がない場合、すべてのインターフェースが対象となります。

```
filter add 20 pass in quick on lo0 from any to 127.0.0.1
filter add 21 block in from 192.168.0.0/16 to any
filter add 22 pass in on wless0 from 192.168.0.0/24 to any
filter add 23 block out on ether0 from 172.16.0.0/12 to any
```

20 番のルールでは、ループバック・デバイスのアクセスを直ちに許可しています。21 番のルールでは、**192.168.0.0/16** 予約済みのプライベートネットワーク用のアドレスからのパケットを **block** しています。しかし、無線側(**wless0**)は **192.168.0.0/24** のネットワークに接続しているので、22 番では **192.168.0.0/24** のみ **pass** を指定しています。最後にマッチしたルールに従いますので、ここまでのルールでは、例えば **192.168.0.3** からのパケットが無線側からきた場合は **pass** しますが、Ethernet 側からきた場合や、**192.168.1.2** からのパケットは **block** されることとなります。23 番のルールでは予約済みのプライベートネットワーク用のアドレス **172.16.0.0/12** からのパケットを Ethernet 側に出さないようにするルールです。

- **proto** には **"tcp/udp"**、**"tcp"**、**"udp"** もしくは **"icmp"** が指定可能で、これらのプロトコル種別をもとにフィルター・ルールを設定することができます。**proto** がない場合には、すべての種別にマッチします。以下の例では、Ethernet 側からの **tcp** と **udp** パケットは **pass** しますが、Ethernet 側からの **icmp** は **block** されることとなります。

```
filter add 40 pass in on ether0 proto tcp/udp from any to any
filter add 41 block in on ether0 proto icmp from any to any
```

- すすでにお分かりのとおり、**from** や **to** に IP アドレスやネットワークを指定することで、パケットの発信元・宛先をもとにルールを設定することができます。すべての

ホストを表す”any”も指定可能です。

- **port** には TCP/UDP の際のポート番号を指定することができ、特定のポートを指定したフィルター・ルールを設定することができます。**port** は TCP および UDP のパケットにおいて有効です。また、**port** を指定しないときには、全てのポートがルールの対象になります。以下の例では、無線側から 80 番ポートへ向けての TCP パケットは **pass** します。

```
filter add 50 pass in on wless0 proto tcp from any to any port = 80
```

- **flags** には TCP フラグの F(FIN),S(SYN),R(RST),P(PUSH),A(ACK),U(URG)が指定可能で、これらフラグの種類に応じたフィルター・ルールの設定ができます。同時に複数のフラグを指定することもできます。**flags** で指定したフラグにマッチしない TCP フラグのパケットは、フィルター・ルールにはマッチしません。
- **with** には”**ipopts**”,”**short**”,”**frag**”が指定可能です。**ipopt** は IP ヘッダに IP オプションを持つパケットを検出することができます。**short** は不正に IP ヘッダが短いパケットを検出することができます。**frag** はフラグメント化された IP パケットを検出することができます。

```
filter add 60 block in quick from any to any with short
```

このフィルター・ルールでは、不正に短い IP ヘッダを持つパケットを、直ちに **block** します。

- **keep state** を指定すると、状態を管理したフィルター・ルールの設定が可能です。**keep state** が指定された場合、新しい TCP セッションが確立されたときに、そのセッションの情報を内部に保持します。そして、RGW 内部に記憶されそのセッション以降のパケットは双方向とも別のフィルター・ルールによるチェックを行うことなく、**pass** させることができます。UDP パケットの場合も、**keep state** が指定された場合、UDP パケットの発信・宛先双方の IP アドレスとポート番号を 60 秒間記憶し、IP アドレスもポート番号も同じ逆方向の UDP パケットのみを **pass** することができます。**icmp** の場合、**keep state** の指定を行うと、その **icmp** に対する **reply** が 600 秒間 **pass** することができます。

```
filter add 70 pass out quick on ether0 proto udp from any to any keep state
```

```
filter add 71 pass out quick on ether0 proto tcp from any to any flags S keep state
filter add 72 block in quick on ether0 proto tcp from any to any flags FUP
```

70 番のルールでは、Ethernet 側に出て行く udp パケットを pass し、そのレスポンスである udp パケットを 60 秒間 pass します。

71 番のルールでは、Ethernet 側に出て行く S フラグのついた tcp パケットを pass し、以降そのセッションのパケットは入出力とも pass します。

72 番のルールでは、F(FIN),U(URG),P(PSH)フラグのパケットが Ethernet 側からきたとき、直ちに block します。しかし、先のチェックの 70 と 71 番のルールで状態管理されているものは、このルールまで到達しません。

- **head** はフィルター・ルールにマッチしたパケットに識別番号を与える指示子です。そのルールにマッチしたパケットは、その識別番号を **group** に持つフィルター・ルールによるチェックを行います。これらの **head** と **group** により、フィルター・ルールのグループを生成することができます。また、この **head** を持つフィルター・ルールに **quick** を指定することで、その識別番号と同じ **group** を持つルールをチェックしたあと、他のルールのチェックが行われません。

```
filter add 100 pass in on ether0 from any to any
filter add 101 block in quick on ether0 from 192.168.0.0/24 to any
filter add 102 block in quick on ether0 from 172.16.0.0/12 to any
filter add 110 block out on wless0 from any to any
filter add 111 pass out quick on wless0 proto tcp/udp from any to any flags S keep state
filter add 112 pass out quick on wless0 proto icmp from any to any keep state
```

以上のルール・セットを **head** と **group** で最適化すると、次のようになります。

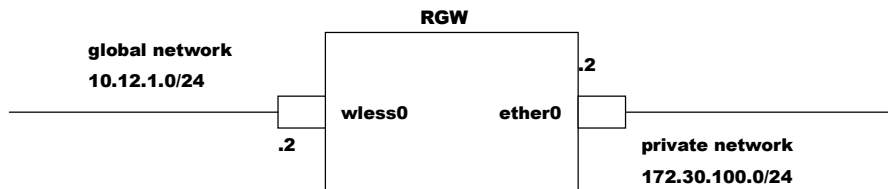
```
filter add 100 pass in on ether0 from any to any head 1
filter add 101 block in quick on ether0 from 192.168.0.0/24 to any group 1
filter add 102 block in quick on ether0 from 172.16.0.0/12 to any group 1
filter add 110 block out on wless0 from any to any head 2
filter add 111 pass out quick on wless0 proto tcp/udp from any to any flags S keep state
                                group 2
filter add 112 pass out quick on wless0 proto icmp from any to any keep state group 2
```

head と **group** で最適化したルール・セットでは、最初に 100 番のルールがマッチす

ると、101 から 102 番のルールが順次チェックされます。101 から 102 番のルールでは **quick** が指定されていますので、マッチすると直ちに **block** されます。101 から 102 番のルールにマッチしないと、100 番のルールにより直ちに **pass** されます。無線側(wless0)へ出るパケットは、100 番のルールにマッチしないので、次に評価されるルールは 110 番になります。110 番のルールにマッチすると、111 と 112 番のルールが順次チェックされます。それぞれのルールにマッチすると、それぞれのルールに対応したアクションを行います。111 と 112 番のルールにマッチしないと、110 番のアクションの **block** が採用されます。

このように **head** と **group** を使ったフィルター・ルールのグループ化は、複雑なルール・セットを分かりやすくするとともに、フィルタリングの性能向上が望めます。なお、**head** や **group** に指定される値はフィルター番号と関係はありません。

3.2.2 NAT



上図のネットワーク構成において、private 側のネットワークにつながるクライアントから、global 側へのアクセスを行うには、

```
nat add map nnn wless0 172.30.100.0/24 -> 10.12.1.2/32
```

のコマンドで可能になります。このコマンドでは、内部の発信元の IP アドレス (172.30.100.0/24) が、RGW で 10.12.1.2 に書き換わり global 側に出て行きます。しかし、TCP/UDP のパケットは発信元のポート番号は変わりません。発信元のポート番号を重複しないように変更するには `portmap` キーワードを指定します。

```
nat add map nnn wless0 172.30.100.0/24 -> 10.12.1.2/32 portmap tcp/udp 20000:30000
```

このコマンドでは、TCP と UDP パケットは IP アドレスの変換に加え、発信元のポート番号も 20000 から 30000 の範囲で変換が行われるようになります。portmap キーワードのポート番号の範囲には `auto` も指定が可能です。

このコマンドは

```
nat add map nnn wless0 172.30.100.0/24 -> 0/32 portmap tcp/udp 20000:30000
```

と同じ働きをします。

また、いくつかのアプリケーション・プロトコルは NAT で動作しないことが知られています。RGW の NAT では、ftp に `proxy` で対応しており、以下のコマンドでクライアントが `passive mode` にせずアクセスが可能になります。

```
nat add map nnn wless0 172.30.100.0/24 -> 0/32 proxy port ftp ftp/tcp
```

以上をまとめると、一般的な NAT のルールは以下のようになります。

```
nat add map 10 wless0 172.30.100.0/24 -> 0/32 proxy port ftp ftp/tcp
nat add map 11 wless0 172.30.100.0/24 -> 0/32 portmap tcp/udp auto
nat add map 12 wless0 172.30.100.0/24 -> 0/32
```

NAT の各ルールは番号順に評価されます。たとえば、12番のコマンドを10番より前に指定すると、全ての 172.30.100.0/24 から global 側へ出て行くパケットは IP アドレスのみの変換が行われるだけになり、期待した NAT の動作をしないでしょう。

icmp のパケットは IP アドレスの変換が行われるだけです。例えば複数のクライアントから global 側の同じホストに対する ping は、最初に要求したクライアントへのみ応答が返ってきます。

NAT の内側にサーバーを置き、それを global 側から到達可能にすることも可能です。

```
nat add bimap 100 wless0 172.30.100.3/32 -> 10.12.0.2/32
```

このコマンドにより、NAT の外側から 10.12.0.2 に対するアクセスは、NAT 内側の 172.30.100.3 のホストに対するアクセスに対応します。

bimap ではホストに対する spoof が可能でしたが、rdr ではサービスの spoof が可能になります。例えば、

```
nat add rdr 101 wless0 10.12.0.2/32 port 80 -> 172.30.100.4/32 port 8000
```

このコマンドにより、NAT の外側から 10.12.0.2 のポート 80 番に対するアクセスは、NAT 内側の 172.30.100.4 のホストポート 8000 番に対するアクセスになります。この rdr により、ポート毎（サービス毎）にパケットを別ホストの別ポートに振り分けることができます。

注意：RGW に入ってくるパケットは、NAT によるアドレス変換が IP フィルターの処理の前に行われます。一方、RGW から出るパケットは、IP フィルターの処理が NAT によるアドレス変換の前に行われます。