Rev.15.02.05 リリースノート

〇RTX830 Rev.15.02.01 からの変更点

（メーカーリリース版Rev.15.02.03を含む）

■機能追加

[1] 本機にアクセスするときのセキュリティーを強化した。

(1) login password [encrypted]コマンド、administrator password [encrypted]コマンド、login userコマンドを設定したときにパスワード強度を出力するようにした。
パスワードを空に設定した場合は、設定を促すメッセージを出力するようにした。

- パスワード未設定
  "Password is not set. Please set the password in order to enhance the security."
- パスワード強度 弱
  "Password Strength : Weak"
- パスワード強度 中
  "Password Strength : Fair"
- パスワード強度 強
  "Password Strength : Strong"

- パスワード強度 最強

"Password Strength : Very strong"

(2) シリアル、TELNET、SSH、リモートセットアップで、login passwordコマンドの設定値が工場出荷状態のまま無名ユーザーがログインしたときに、以下のメッセージを出力するようにした。

"The login password is factory default setting. Please request an administrator to change the password by the 'login password' command."

(3) シリアル、TELNET、SSH、リモートセットアップで、administrator passwordコマンドの設定値が工場出荷状態のままadministratorコマンドで管理者権限に昇格したときに、以下のメッセージを出力するようにした。

"The administrator password is factory default setting. Please change the password by the 'administrator password' command."

(4) 以下の手段でログインに3回連続で失敗したら1分間ログインできなくなるようにした。

- シリアルコンソール
- リモートセットアップ
- TELNET
- SSH
- SFTP

アクセス制限時の動作は以下の通り。

- アクセス制限は接続種別ごとに行われる

ただし、TELNETとSSHに関しては接続元IPアドレスごとに制限される

- アクセス制限がかかったときは、以下のINFOレベルのSYSLOGを出力する

"Login access from 接続種別 was restricted. [: IPアドレス]"

- 接続種別は"Serial", "Remote", "TELNET", "SSH"のいずれか
- IPアドレスはTELNETまたはSSHのときに表示される
- アクセス制限中にログインしようとすると、コンソールとSYSLOGには以下のメッセージを出力する
  ユーザー名は無名ユーザー以外でアクセスしたときに表示される

コンソール："Error: Login access is restricted."
SYSLOG："Login failed for 接続種別[: IPアドレス [ユーザー名]]"

(5) Web GUIへのログインに3回連続で失敗したら1分間ログインできなくなるようにした。

アクセス制限時の動作は以下の通り。

- アクセス制限はクライアントのIPアドレスごとに管理される
- ステータスコード403を返し、アクセス制限中であることを表示する
- アクセス制限がかかったときは、以下のINFOレベルのSYSLOGを出力する

"Login access from HTTP was restricted. : IPアドレス"

- アクセス制限中にログインしようとすると、SYSLOGには以下のメッセージを出力する

"Login failed for HTTP: IPアドレス"

(6) Web GUIにメッセージボード機能を追加した。

ログインパスワードまたは管理者パスワードが工場出荷状態のままログインしたとき、メッセージボードに警告が表示される。

(7) Web GUIにアクセスし、ログインしないで認証ダイアログを閉じたときに表示されるページを「Error 401」に変更した。

(8) 工場出荷状態の設定にtelnetd host lanコマンドを追加した。

(9) pptp hostnameコマンドの初期値を機種名から空文字("")にした。

(10) PPTPのベンダー名を設定できるようにした。

○PPTPのベンダー名の設定

[書式]

pptp vendorname NAME

no pptp vendorname

[設定値および初期値]

NAME

[設定値] : ベンダー名（64バイト以下）

[初期値] : -

[説明]

PPTPベンダー名を設定する。

[ノート]

本コマンドで設定した値がStart-Control-Connection-Requestと
Start-Control-Connection-Replyのベンダー名にセットされる。
本コマンドが設定されていないときはベンダー名に空文字がセットされる。

RTX1210 Rev.14.01.26以降、RTX830 Rev.15.02.03以降のファームウェアで

使用可能。

それ以外のファームウェアではベンダー名に"YAMAHA Corporation"がセットされる。

(11) HTTPレスポンスヘッダから、機種を特定できる文字列を削除した。

変更前

Server: 機種名

WWW-Authenticate: Basic realm="[機種名]"

変更後

Server: Router

WWW-Authenticate: Basic realm="[Router]"

[2] CLIの機能を拡張した。

コンソール: 変数、エイリアス、マクロ、ヒストリー

http://www.rtpro.yamaha.co.jp/RT/docs/cli/vamh.html

設定の一括更新とロールバック

http://www.rtpro.yamaha.co.jp/RT/docs/cli/load.html

外部仕様書をよくご確認のうえ、ご利用ください。

[3] EMFS機能を追加した。

http://www.rtpro.yamaha.co.jp/RT/docs/emfs/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[4] YNOエージェント機能で、GUI Forwarderに対応した。

http://www.rtpro.yamaha.co.jp/RT/docs/yno/agent/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[5] YNOエージェント機能で、HTTPSプロキシサーバーが存在する環境でYNOマネージャーに接続できるようにした。

〇YNOで使用するHTTPSプロキシサーバーの設定

[書式]

yno https-proxy PROXY_SERVER PORT

no yno https-proxy [PROXY_SERVER [PORT]]

[設定値及び初期値]

PROXY_SERVER

[設定値] : HTTPSプロキシサーバーのホスト名、もしくはIPアドレス

[初期値] : -

PORT

[設定値] : HTTPSプロキシサーバーのポート番号 (1..65535)

[初期値] : -

[説明]

YNOで使用するHTTPSプロキシサーバーを設定する。

PROXY_SERVERには、HTTPSプロキシサーバーのFQDN形式のホスト名、またはIPアドレスを255文字以内の半角英数字および半角記号で指定する。

PORTには、HTTPSプロキシサーバーのポート番号を指定する。

[ノート]

ユーザー認証が必要なHTTPSプロキシサーバーを使用することはできない。

[6] 「v6プラス」接続サービスに対応した。

http://www.rtpro.yamaha.co.jp/RT/docs/v6plus/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[7] モバイルインターネット機能で、以下のデータ通信端末に対応した。

- グリーンハウス GH-UDG-MCLTED
- ソフトバンク 604HW

http://www.rtpro.yamaha.co.jp/RT/docs/mobile-internet/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[8] Oracle Cloud InfrastructureとのIPsec接続に対応した。

[9] IPsec over IPIPのファストパスに対応した。

[10] L2TPv3を用いたL2VPNで、IEEE802.1Qタグ付きフレームをファストパスで処理するようにした。

[11] L2TPv3を用いたL2VPNで、トンネルインターフェースに以下のフィルターを設定・適用できるようにした。

- イーサネットフィルター
- IPフィルター

http://www.rtpro.yamaha.co.jp/RT/docs/l2tpv3/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[12] IKEv2で、鍵交換の始動パケットを受信しない機能を追加した。

これにより一部の機器やサービスとの接続が安定する可能性がある。

〇鍵交換の始動パケットを受信するか否かの設定

[書式]

ipsec ike negotiation receive GATEWAY_ID SWITH

no ipsec ike negotiation receive GATEWAY_ID

[設定値及び初期値]

GATEWAY_ID ..... セキュリティ・ゲートウェイの識別子

SWITCH

on ..... 鍵交換の始動パケットを受信する

off ..... 鍵交換の始動パケットを受信しない

[初期値]：on

[説明]

IKEv2で、鍵交換の始動パケットを受信するか否かを設定する。

受信しないに設定した場合は、結果として受動側としては動作せず、必ず始動側として動作するようになる。

[ノート]

本コマンドはIKEv1の動作には影響を与えない。

offにする場合には、ipsec ike remote addressまたはipsec ike remote nameをIPアドレスで設定しておく必要がある。

[13] L2MSで、以下の機器に対応した。

- SWX3200-52GT
- SWX3200-28GT
- SWX3100-10G
- SWX2310P-28GT

- SWX2310P-18G
- SWX2310P-10G
- WLX313

http://www.rtpro.yamaha.co.jp/RT/docs/swctl/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[14] スイッチのCONFIGバックアップ機能に対応した。

〇スイッチの設定を保存するファイル名の指定

[書式]

switch config filename NAME

no switch config filename [NAME]

[設定値及び初期値]

NAME

[設定値] : ファイル名 (半角99文字以下、全角49文字以下)

[初期値] : -

[説明]

スイッチの設定を保存するファイル名を指定する。

本コマンドが省略された場合は、switch selectコマンドで指定された文字列に.confを付けたものをファイル名とする。

ただし:(コロン)は_(アンダースコア)に置き換えられる。

複数のswitch selectコマンドで同じファイル名を指定することができる。

switch config directoryコマンドで指定されたディレクトリがRTFS領域である場合は、ファイル名にマルチバイト文字を使用することはできない。

本コマンドを実行する前にswitch selectコマンドでスイッチを指定しておく必

要がある。

○スイッチの設定ファイルを格納するディレクトリの指定

[書式]

switch config directory PATH

no switch config directory [PATH]

[設定値及び初期値]

PATH

[設定値] : 相対パスまたは絶対パス (半角256文字以下、全角128文字以下)

[初期値] : /sw_config

[説明]

スイッチの設定ファイルを格納するディレクトリを指定する。

相対パスを指定した場合、環境変数PWDを起点としたパスと解釈される。

PWDはsetコマンドで変更可能であり、初期値は"/"である。

PATHがRTFS領域となる場合は、PATHにマルチバイト文字を使用することはできない。

○スイッチの設定の取得

[書式]

switch control config get [SW]

switch control config get [[INTERFACE] all]

[設定値及び初期値]

SW

[設定値] :

設定値	説明
MACアドレスもしくは経路	指定したスイッチのみ
all	全てのスイッチ

[初期値] : -

INTERFACE

[設定値] : LANインターフェース名、ブリッジインターフェース名

[初期値] : -

[説明]

スイッチの設定ファイルを取得して保存する。

SWパラメータにMACアドレスもしくは経路を指定した場合は、指定したスイッチの設定ファイルを取得する。allを指定すると、マスターが認識している全てのスイッチの設定ファイルを取得する。

INTERFACEパラメータを指定すると、指定のインターフェースにつながっているスイッチを対象とする。INTERFACEパラメータを省略した場合は、allを指定した時と同様になる。

[ノート]

本コマンドで取得したスイッチの設定ファイルの名前には、switch config filenameコマンドで指定したファイル名を使用する。

スイッチの設定ファイルはswitch config directoryコマンドで指定したディレクトリに保存される。

本コマンドはschedule atコマンドで指定することができる。

〇スイッチの設定の復元

[書式]

switch control config set [SW]

switch control config set [[INTERFACE] all]

[設定値及び初期値]

SW

[設定値] :

設定値　　説明

MACアドレスもしくは経路 指定したスイッチのみ

all 全てのスイッチ

[初期値] : -

INTERFACE

[設定値] : LANインターフェース名、ブリッジインターフェース名

[初期値] : -

[説明]

マスターに保存されているスイッチの設定ファイルを使用して、スイッチの設定を復元する。

SWパラメータにMACアドレスもしくは経路を指定した場合は、指定したスイッチの設定を復元する。allを指定すると、マスターが認識している全てのスイッチの設定を復元する。

INTERFACEパラメータを指定すると、指定のインターフェースにつながっているスイッチを対象とする。INTERFACEパラメータを省略した場合は、allを指定した時と同様になる。

[ノート]

本コマンドで復元に使用するスイッチの設定ファイルには switch config filenameコマンドで指定した設定ファイルを使用する。

スイッチの設定ファイルはswitch config directoryコマンドで指定したディレクトリに保存されている必要がある。

本コマンドはschedule atコマンドで指定することができる。

[15] FQDNフィルター機能に対応した。

http://www.rtpro.yamaha.co.jp/RT/docs/fqdn_filter/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[16] PPPoEパススルー機能に対応した。

http://www.rtpro.yamaha.co.jp/RT/docs/pppoe/pppoe_pass_through.html

外部仕様書をよくご確認のうえ、ご利用ください。

[17] DNSサーバーへのAAAAレコードの問い合わせを制限するコマンドを追加した。

〇DNSサーバーへのAAAAレコードの問い合わせを制限するか否かを設定する

[書式]

dns service aaaa filter SW

no dns service aaaa filter [SW]

[設定値及び初期値]

sw

[設定値] :

設定値	説明
on	AAAAレコードの問い合わせを制限する
off	AAAAレコードの問い合わせを制限しない

[初期値] : off

[説明]

DNSサーバーへのAAAAレコードのに問い合わせを制限するか否かを設定する。

IPv6での接続環境がないのにAAAAレコードが引けてしまうことで接続に失敗する場合は、このコマンドによりAAAAレコードの問い合わせに対して、AAAAレコードを回答しないようにする。

自機がDNSリレーサーバーになっている通信及び自機発の通信が影響を受ける。

[18] トリガメール通知機能とLuaのメール通知機能でSMTPSに対応した。

メール通知機能

http://www.rtpro.yamaha.co.jp/RT/docs/mail-service-status/index.html

Luaスクリプト機能

http://www.rtpro.yamaha.co.jp/RT/docs/lua/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[19] Luaスクリプト機能のrt.httprequest関数で、以下の機能に対応した。

- HTTPSによる通信
- Bearer認証

これに伴い、Luaスクリプト機能バージョンを1.08とした。

http://www.rtpro.yamaha.co.jp/RT/docs/lua/rt_api.html

外部仕様書をよくご確認のうえ、ご利用ください。

[20] SNMPトラップを送信するイベントが発生してからトラップを送信するまでの間隔を指定できるようにした。

〇SNMPトラップの送信の遅延時間の設定

[書式]

snmp trap delay-timer WAIT

snmp trap delay-timer off

no snmp trap delay-timer [WAIT]

[設定値および初期値]

WAIT

[設定値]:SNMPトラップを送信するまでの遅延時間の秒数(1 .. 21474836)

[初期値]:-

[説明]

SNMPトラップを送信するイベントが発生してからトラップを送信するまでの遅延時間を指定する。

offを設定した場合、即座にSNMPトラップを送信する。

設定する遅延時間は最低限保証する値であり、設定値以上遅延する場合もある。

[21] DHCPでIPアドレスを取得したときにデフォルト経路を追加するか否かを設定するコマンドを追加した。

〇DHCPでIPアドレスを取得したときにデフォルト経路を追加するか否かを設定

[書式]

ip INTERFACE dhcp auto default-route-add SWITCH

no ip INTERFACE dhcp auto default-route-add [SWITCH]

[設定値及び初期値]

INTERFACE

[設定値] :

LANインターフェース名

WANインターフェース名

ブリッジインターフェース名

[初期値] : -

SWITCH

[設定値] :

設定値　説明

---

on　DHCPでIPアドレスを取得したときにデフォルト経路に追加する

off　DHCPでIPアドレスを取得したときにデフォルト経路に追加しない

[初期値] : on

[説明]

指定したインターフェースを使用中、DHCPでIPアドレスを取得したときにデフォルト経路を追加するか否かを設定する。

すでにDHCPでIPアドレスを取得しているインターフェースに対してこのコマンドの設定が変更された場合、次にDHCPでIPアドレスを取得した時点から新しい設定が反映される。

[22] DHCPでIPアドレスを取得したときにimplicit経路を追加するか否かを設定するコマンドを追加した。

〇DHCPでIPアドレスを取得したときにimplicit経路を追加するか否かを設定

[書式]

ip INTERFACE dhcp auto interface-route-add SWITCH

no ip INTERFACE dhcp auto interface-route-add [SWITCH]

[設定値及び初期値]

INTERFACE

[設定値] :

LANインターフェース名

WANインターフェース名

ブリッジインターフェース名

SWITCH

[設定値] :

設定値　説明

---

on　　DHCPでIPアドレスを取得したときにimplicit経路を追加する

off　　DHCPでIPアドレスを取得したときにimplicit経路を追加しない

[初期値] : on

[説明]

指定したインターフェースを使用中、DHCPでIPアドレスを取得したときにアドレスを取得したインターフェースのimplicit経路を追加するか否かを設定する。

すでにDHCPでIPアドレスを取得しているインターフェースに対してこのコマンドの設定が変更された場合、次にDHCPでIPアドレスを取得した時点から新しい設定が反映される。

[23] schedule atコマンドで指定時間後にコマンドを実行することができるようにした。

〇スケジュールの設定

[書式]

schedule at ID [DATE] TIME * COMMAND...

schedule at ID [DATE] TIME pp PEER_NUM COMMAND...

schedule at ID [DATE] TIME tunnel TUNNEL_NUM COMMAND...

schedule at ID [DATE] TIME switch SWITCH COMMAND...

schedule at ID +TIMER * COMMAND...　★

schedule at ID +TIMER pp PEER_NUM COMMAND...　★

schedule at ID +TIMER tunnel TUNNEL_NUM COMMAND...　★

schedule at ID +TIMER switch SWITCH COMMAND...

no schedule at ID [[DATE]...]

[設定値及び初期値]

ID

[設定値] : スケジュール番号

[初期値] : -

DATE : 日付(省略可)

[設定値] :

- 月/日

- 省略時は */* とみなす

月の設定例　　設定内容

1,2　　1月と2月

2-　　2月から12月まで

2-7　　2月から7月まで

-7　　1月から7月まで

*　　毎月

日の設定例　　設定内容

1　　1日のみ

1,2　　1日と2日

2-　　2日から月末まで

2-7　　2日から7日まで

-7　　1日から7日まで

mon　　月曜日のみ

sat,sun　　土曜日と日曜日

mon-fri　　月曜日から金曜日

-fri 日曜日から金曜日

* 毎日

[初期値] : -

TIME : 時刻

[設定値] :

設定値 説明

---

hh:mm[:ss] 時(0..23または*):分(0..59または*):秒(0..59)、
秒は省略可

startup 起動時

usb-attached USBデバイス認識時

sd-attached microSDデバイス認識時

[初期値] : -

TIMER ★

[設定値] : COMMANDを実行するまでの時間(秒、1..3600)

[初期値] : -

PEER_NUM

[設定値] :

- 相手先情報番号

- anonymous

[初期値] : -

TUNNEL_NUM

[設定値] : トンネルインタフェースの番号

[初期値] : -

SWITCH : スイッチ

[設定値] :

- MACアドレス

- 経路

[初期値] : -

COMMAND

[設定値] : 実行するコマンド(制限あり)

[初期値] : -

[説明]

TIMEで指定した時刻、またはTIMERで指定した時間後にCOMMANDで指定されたコマンドを実行する。 ★

第2、第3、第4、第6、第7、第8書式で指定された場合には、それぞれあらかじめ指定された相手先情報番号/トンネル番号/スイッチでの、pp select/tunnel select/switch selectコマンドが発行済みであるように動作する。 ★

schedule atコマンドは複数指定でき、同じ時刻に指定されたものはIDの小さな順に実行される。

TIMEはhh:mm形式で指定されたときは秒指定なしとみなされ、hh:mm:ss形式で指定されたときは秒指定ありとみなされる。秒数に"-"を用いた範囲指定や"*"による全指定をすることはできない。

以下のコマンドは指定できない。

administrator、administrator password、administrator password encrypted、ap select、auth user、auth user group、bgp configure refresh、cold start 、console info とconsole promptを除くconsoleで始まるコマンド、copy、copy exec、date、delete、exit、external-memory performance-test go、help、http revision-up go、http revision-up schedule、interface reset、ipsec transport template、ipv6 bgp configure refresh、ipv6 ospf configure refresh、lessで始まるコマンド、login password、login password encrypted、login timer、login user、luac、make directory、nslookup、ospf configure refresh、packetdump、ping、ping6、pp select、

quit、remote setup、rename、rtfs format、rtfs garbage collect、save、
schedule at、scp、showで始まるコマンド、ssh、sshd host key generate、
sshd session、switch control function get FUNCTION、switch select、
system packet-buffer、telnet、telnetd session、time、timezone、
traceroute、traceroute6、tunnel select、tunnel template、user attribute

[ノート]

入力時、COMMANDパラメータに対してTABキーによるコマンド補完は行うが、シンタックスエラーなどは実行時まで検出されない。schedule atコマンドにより指定されたコマンドを実行する場合には、何を実行しようとしたかをINFOタイプのSYSLOGに出力する。

DATEに数字と曜日を混在させて指定はできない。

startupを指定したスケジュールはルーター起動時に実行される。電源を入れたらすぐ発信したい場合などに便利。

RT250iでは第3書式は使用できない。

第4書式は RTX1210、RTX1200、RTX830、RTX810で使用できる。

usb-attachedを指定できるのはRev.10.01系以降である。

TIMEパラメータでの秒指定はRTX1200 Rev.10.01.16以降、および、Rev.11.01系以降で利用できる。

第5～8書式はRTX830 Rev.15.02.03以降で使用できる。 ★

[設定例]

ウィークデイの8:00-17:00だけ接続を許可する

```
# schedule at 1 */mon-fri 8:00 pp 1 isdn auto connect on
# schedule at 2 */mon-fri 17:00 pp 1 isdn auto connect off
# schedule at 3 */mon-fri 17:05 * disconnect 1
```

毎時0分から15分間だけ接続を許可する

```
# schedule at 1 *:00 pp 1 isdn auto connect on
# schedule at 2 *:15 pp 1 isdn auto connect off
# schedule at 3 *:15 * disconnect 1
```

今度の元旦にルーティングを切替える

schedule at 1 1/1 0:0 * ip route NETWORK gateway pp 2

毎日12時から13時の間だけ20秒間隔で Lua スクリプトを実行する

schedule at 1 12:*:00 * lua script.lua

schedule at 2 12:*:20 * lua script.lua

schedule at 3 12:*:40 * lua script.lua

毎日3時にスイッチを再起動する

schedule at 1 */* 03:00 switch 00:a0:de:01:02:03 switch control function execute restart

schedule at 2 */* 03:00 switch lan1:4 switch control function execute restart

コマンド設定時から10分後に再起動する ★

schedule at 1 +600 * restart ★

[24] Web GUIのかんたん設定で、YNOエージェント機能を設定できるようにした。

[25] Web GUIのLANマップのタグVLAN画面で、SWX2300のタグVLANを設定できるようにした。

[26] Web GUIのLANマップでスイッチのCONFIGバックアップ機能に対応した。
また、LANマップ上からスレーブのCONFIGファイルのファイル名や保存先を変更できるようにした。

■仕様変更

[1] ルーター経由のSNMPによるスイッチの状態取得機能で、以下のスイッチのカウンターの値を取得できるようにした。

- SWX2100-8G
- SWX2100-16G
- SWX2100-24G
- SWX2100-5PoE

- SWX2100-10PoE

[2] TCPセッションのMSS制限の設定をする以下のコマンドで、初期値をoffからautoに変更した。

- ip INTERFACE tcp mss limit
- ip pp tcp mss limit
- ip tunnel tcp mss limit
- ipv6 INTERFACE tcp mss limit
- ipv6 pp tcp mss limit
- ipv6 tunnel tcp mss limit

[3] マルチポイントトンネルの確立時に自動追加される対向拠点のトンネルアドレスへの経路の種別をtemporaryからimplicitへ変更した。

[4] モバイルインターネット機能で、NTTコム UX302NCの網からの切断処理を変更した。

[5] 以下のデータ通信端末を使用するとき、show status usbhostコマンドでデータ通信端末のRevisionを表示するようにした。

- NTTコム UX302NC

[6] 送受信パケット数やオクテット数などのカウンターを32ビットから64ビットに拡張した。

[7] 以下のコマンドのLENGTHパラメーターの設定値の最大値を変更した。

○パケット通信量制限の設定

[書式]

mobile access limit length LENGTH [alert=ALERT[,ALERT_CANCEL]]

no mobile access limit length [LENGTH]

[設定値及び初期値]

LENGTH

[設定値] :

設定値　　説明

1-9223372036854775807　バイト数、送受信する累積パケットデータ長の上限値★

off　　制限しない

[初期値] : 50M(RTX1210 Rev.14.01.20 以降、Rev.15.02 系以降)

200000(上記以外)

ALERT

[設定値] : 警告値、データ長あるいは[%]指定

[初期値] : -

ALERT_CANCEL

[設定値] : 警告解除値、データ長あるいは[%]指定

[初期値] : -

[説明]

選択されている相手について、送受信するパケットの累積データ長の上限値を設定する。

上限に達した場合は通信を強制的に切断し、その後の通信もブロックする。

LENGTH、ALERTおよびALERT_CANCELパラメーターの後ろに'k'または、'M'、'G'をつけると、それぞれk byteまたはM byte、G byteとして扱われる。

累積値は、

・clear mobile access limitation コマンドの発行

・mobile access limit duration コマンドの再設定

・システムの再起動

でクリアされ、発信制限が解除される。

show status ppコマンドで、現在までの累積パケットデータ長を確認できる。
ALERTで警告値を設定すると、その警告値を上回った時にログに表示することができる。
またmobile access limit durationコマンドで累積期間を設定している場合には、ALERT_CANCELで指定した警告解除値を下回った時にログに表示することができる。
警告解除値を指定しない場合は、期間累積のデータ長が0になるまで警告を解除しない。

[ノート]

警告値は上限値よりも小さく、警告解除値は警告値よりも小さくなければならない。
携帯端末のパケット通信は128バイトごとに課金されるが、ルーターと携帯端末間で送受信されるデータが128バイト単位である保証はない。
例えばルーターが512バイト(128バイト×4)のデータを送受信したとしても、4パケット分の通信料金である保証はなく、携帯網ではそれより多くのパケットに分割されて送受信されている可能性がある。
また、ルーターと携帯端末の間を流れるデータは非同期データであり、データの内容によっては本来のデータよりも長くなることがある。
従って、本コマンドで設定するデータ長はあくまで目安にしかならないので注意が必要である。
offを設定したときは警告が表示される。

LENGTH, ALERT, ALERT_CANCELパラメータへの2147483647より大きな値の設定は、RTX830 Rev.15.02.03以降で指定可能。★

〇接続毎パケット通信量制限の設定

[書式]

mobile access limit connection length LENGTH [alert=ALERT]

no mobile access limit connection length [LENGTH]

[設定値及び初期値]

LENGTH

[設定値] :

設定値　　説明

1-9223372036854775807　バイト数、送受信するパケットデータ長の上限値★

off　　制限しない

[初期値] : off

ALERT

[設定値] : 警告値、データ長あるいは[%]指定

[初期値] : -

[説明]

選択されている相手について、1回の接続で送受信するパケットのデータ長の上限値を設定する。上限に達した場合は通信を強制的に切断する。

ALERTを指定して上限に達する前に警告を発生させることができる。警告はログに表示される。

[ノート]

携帯端末のパケット通信は128バイトごとに課金されるが、ルーターと携帯端末間で送受信されるデータが128バイト単位である保証はない。

例えばルーターが512バイト(128バイト×4)のデータを送受信したとしても、4パケット分の通信料金である保証はなく、携帯網ではそれより多くのパケットに分割されて送受信されている可能性がある。

また、ルーターと携帯端末の間を流れるデータは非同期データであり、データの内容によっては本来のデータよりも長くなることがある。

従って、本コマンドで設定するデータ長はあくまで目安にしかならないので注意

が必要である。

Rev.10.01.11以降で使用可能。

LENGTH, ALERTパラメータへの2147483647より大きな値の設定は、RTX830 Rev.15.02.03以降で指定可能。★

〇パケット通信量制限の設定

[書式]

WAN access limit length LENGTH [alert=ALERT[,ALERT_CANCEL]]

no WAN access limit length [LENGTH]

[設定値及び初期値]

WAN

[設定値] :

設定値	説明
wan1	WAN インタフェース名

[初期値] : -

LENGTH

[設定値] :

設定値	説明
1-9223372036854775807	バイト数、送受信する累積パケットデータ長の上限値★
off	制限しない

[初期値] : 50M(RTX1210 Rev.14.01.20 以降、Rev.15.02 系以降)

200000(上記以外)

ALERT

[設定値] : 警告値、データ長あるいは[%]指定

[初期値] : -

ALERT_CANCEL

[設定値] : 警告解除値、データ長あるいは[%]指定

[初期値] : -

[説明]

指定したWAN インタフェースについて、送受信するパケットの累積データ長の上限値を設定する。

上限に達した場合は通信を強制的に切断し、その後の通信もブロックする。

累積値は、

・clear mobile access limitationコマンドの発行

・WAN access limit durationコマンドの再設定

・システムの再起動

でクリアされ、発信制限が解除される。

show status wan1コマンドで、現在までの累積パケットデータ長を確認できる。

ALERT で警告値を設定すると、その警告値を上回った時にログに表示することができる。

またWAN access limit durationコマンドで累積期間を設定している場合には、ALERT_CANCELで指定した警告解除値を下回った時にログに表示することができる。

警告解除値を指定しない場合は、期間累積のデータ長が0になるまで警告を解除しない。

[ノート]

警告値は上限値よりも小さく、警告解除値は警告値よりも小さくなければならない。

携帯端末のパケット通信は128バイトごとに課金されるが、ルーターと携帯端

末間で送受信されるデータが128バイト単位である保証はない。
例えばルーターが512バイト(128バイト×4)のデータを送受信したとしても、
4パケット分の通信料金である保証はなく、携帯網ではそれより多くのパケット
に分割されて送受信されている可能性がある。
また、ルーターと携帯端末の間を流れるデータは非同期データであり、データの
内容によっては本来のデータよりも長くなることがある。
従って、本コマンドで設定するデータ長はあくまで目安にしかならないので注意
が必要である。
off を設定したときは警告が表示される。

SRT100は Rev.10.00.60以降で使用可能。
RTX1200は Rev.10.01.32以降で使用可能。
LENGTH, ALERT, ALERT_CANCELパラメータへの2147483647より大きな値の設定
は、RTX830 Rev.15.02.03以降で指定可能。★

〇接続毎パケット通信量制限の設定

[書式]

WAN access limit connection length LENGTH [alert=ALERT]
no WAN access limit connection length [LENGTH]

[設定値及び初期値]

WAN

[設定値] :

設定値	説明
wan1	WAN インタフェース名

[初期値] : -

LENGTH

[設定値] :

設定値　　説明

1-9223372036854775807　バイト数、送受信するパケットデータ長の上限値★

off　　制限しない

[初期値] : off

ALERT

[設定値] : 警告値、データ長あるいは[%]指定

[初期値] : -

[説明]

指定したWANインタフェースについて、1回の接続で送受信するパケットのデータ長の上限値を設定する。上限に達した場合は通信を強制的に切断する。

ALERTを指定して上限に達する前に警告を発生させることができる。警告はログに表示される。

[ノート]

携帯端末のパケット通信は128バイトごとに課金されるが、ルーターと携帯端末間で送受信されるデータが128バイト単位である保証はない。

例えばルーターが512バイト(128バイト×4)のデータを送受信したとしても、4パケット分の通信料金である保証はなく、携帯網ではそれより多くのパケットに分割されて送受信されている可能性がある。

また、ルーターと携帯端末の間を流れるデータは非同期データであり、データの内容によっては本来のデータよりも長くなることがある。

従って、本コマンドで設定するデータ長はあくまで目安にしかならないので注意が必要である。

SRT100はRev.10.00.60以降で使用可能。

RTX1200はRev.10.01.32以降で使用可能。

LENGTH, ALERTパラメータへの2147483647より大きな値の設定は、RTX830 Rev.15.02.03以降で指定可能。★

[8] IPv6ファストパスのセッション処理性能を改善した。

[9] 以下のコマンドを入力したときの処理負荷を軽減した。適用しているインターフェース数が多いほど軽減の効果が大きく表れる。

- ip INTERFACE secure filter
- ip filter
- ip filer set
- ipv6 INTERFACE secure filter
- ipv6 filter
- queue INTERFACE class filter list
- queue class filter

[10] IPキープアライブを複数設定している場合はキープアライブパケットの送信タイミングをランダムに分散させているが、ルーターに高負荷がかかるとランダム性を保てなくなることがあったため、高負荷が発生してもランダム性を保つようにした。

[11] DHCPサーバー機能で、リースするIPアドレスの重複チェック設定がある場合の処理性能を上げた。

[12] DHCPサーバー機能で、スコープにリースできるアドレスがなかったときに以下のメッセージをDEBUGレベルのSYSLOGに出力するようにした。

[DHCPD] Can't lease address because scope No.X is full.

[13] dhcp scope bindコマンドでOUI(ベンダーID)を指定してIPアドレスを予約できるよ

うにした。

○ DHCP予約アドレスの設定

[書式]

dhcp scope bind SCOPE_NUM IP_ADDRESS [TYPE] ID

dhcp scope bind SCOPE_NUM IP_ADDRESS MAC_ADDRESS

dhcp scope bind SCOPE_NUM IP_ADDRESS ipcp

dhcp scope bind SCOPE_NUM IP_ADDRESS-IP_ADDRESS MAC_ADDRESS★

no dhcp scope bind SCOPE_NUM IP_ADDRESS

no dhcp scope bind SCOPE_NUM IP_ADDRESS-IP_ADDRESS★

[設定値及び初期値]

SCOPE_NUM

[設定値] : スコープ番号 (1..65535)

[初期値] : -

IP_ADDRESS

[設定値] :

設定値	説明
xxx.xxx.xxx.xxx(xxxは十進数)	予約するIPアドレス
*	割り当てるIPアドレスを指定しない

[初期値] : -

TYPE : Client-Identifierオプションのtypeフィールドを決定する

[設定値] :

設定値	説明
text	0x00

ethernet　0x01

[初期値] : -

ID

[設定値] :

設定値　　説明

TYPEがethernetの場合　MACアドレス

TYPEがtextの場合　　文字列

TYPEが省略された場合　2桁十六進数の列で先頭はtypeフィールド

[初期値] : -

MAC_ADDRESS

[設定値] : xx:xx:xx:xx:xx:xx(xxは十六進数)

予約DHCPクライアントのMACアドレス

xx:xx:xx:*のように下位3オクテットをアスタリスク(*)にするこ

とで、OUI(ベンダーID)のみの指定となる ★

[初期値] : -

ipcp : IPCPでリモート側に与えることを示すキーワード

[初期値] : -

[説明]

IPアドレスを割り当てるDHCPクライアントを固定的に設定する。

Rev.8.03以降のファームウェアでは、IPアドレスを固定せずにクライアントだけ

を指定することもできる。この形式を削除する場合はクライアント識別子を省略

できない。

[ノート]

IPアドレスは、SCOPE_NUMパラメータで指定されたDHCPスコープ範囲内でなければならない。1つのDHCPスコープ内では、1つのMACアドレスに複数のIPアドレスを設定することはできない。他のDHCPクライアントにリース中のIPアドレスを予約設定した場合、リース終了後にそのIPアドレスの割り当てが行われる。

dhcp scopeコマンドを実行した場合、関連する予約はすべて消去される。
ただし、RTX810のRev.11.01.31以降、RTX5000/RTX3500のRev.14.00.22以降、および、Rev.15.02系以降では、予約情報は消去されない。
ipcpの指定は、同時に接続できるBチャネルの数に限られる。また、IPCPで与えるアドレスはLAN側のスコープから選択される。

コマンドの第1書式を使う場合は、あらかじめdhcp server rfc2131 compliant onあるいはuse-clientid機能を使用するよう設定されていなければならない。
またdhcp server rfc2131 compliant offあるいはuse-clientid機能が使用されないよう設定された時点で、コマンドの第2書式によるもの以外の予約は消去される。

コマンドの第1書式でのクライアント識別子は、クライアントがオプションで送ってくる値を設定する。typeパラメータを省略した場合には、typeフィールドの値も含めて入力する。typeパラメータにキーワードを指定する場合には typeフィールド値は一意に決定されるのでClient-Identifierフィールドの値のみを入力する。

コマンドの第2書式によるMACアドレスでの予約は、クライアントの識別にDHCPパケットのchaddrフィールドを用いる。この形の予約機能は、RTの設定がdhcp server rfc2131 compliant offあるいはuse-clientid機能を使用しない設定になっているか、もしくはDHCPクライアントがDHCPパケット中にClient-Identifierオプションを付けてこない場合でないと動作しない。

クライアントがClient-Identifierオプションを使う場合、コマンドの第2書式で
の予約は、dhcp server rfc2131 compliant onあるいはuse-clientidパラメータ
が指定された場合には無効になるため、新たにClient-Identifierオプションで
送られる値で予約し直す必要がある。

コマンドの第2書式で1つのOUI(ベンダーID)を複数設定することができる。★
OUI(ベンダーID)設定とMACアドレス設定の両方がある場合、MACアドレス設定を
優先する。★

OUI(ベンダーID)設定は以下のファームウェアで指定可能。★
RTX1210 Rev.14.01.28以降★
RTX830 Rev.15.02.03以降★

[設定例]
A. # dhcp scope bind 1 192.168.100.2 ethernet 00:a0:de:01:23:45
B. # dhcp scope bind 1 192.168.100.2 text client01
C. # dhcp scope bind 1 192.168.100.2 01 00 a0 de 01 23 45 01 01 01
D. # dhcp scope bind 1 192.168.100.2 00:a0:de:01:23:45
E. # dhcp scope bind 1 192.168.100.10-192.168.100.19 00:a0:de:*★

1. dhcp server rfc2131 compliant onあるいはuse-clientid機能を使用する
   設定の場合

   A. B. C.の書式では、クライアントの識別にClient-Identifierオプションを
   使用する。
   D.の書式ではDHCPパケットのchaddrフィールドを使用する。ただし、
   Client-Identifierオプションが存在する場合、この設定は無視される。

DHCPサーバーはchaddrフィールドの値よりClient-Identifierオプションの値の方が優先して使用される。
show status dhcpコマンドを実行してクライアントの識別子を確認することで、クライアントがClient-Identifierオプションを使っているか否かを判別することも可能である。

リースしているクライアントとしてMACアドレスが表示されていればClient-Identifierオプションは使用していないリースしているクライアントとして十六進数の文字列、あるいは文字列が表示されていれば、Client-Identifierオプションが使われているClient-Identifierオプションを使うクライアントへの予約は、ここに表示される十六進数の文字列あるいは文字列を使用する

2. dhcp server rfc2131 compliant offあるいはuse-clientid機能を使用しない場合

A. B. C.の書式では指定できない。Client-Identifierオプションは無視される。
D.の書式ではDHCPパケットのchaddrフィールドを使用する。

なお、クライアントとの相互動作に関して以下の留意点がある。

個々の機能を単独で用いるとクライアント側で思わぬ動作を招く可能性があるため、dhcp server rfc2131 compliant onあるいはdhcp server rfc2131 compliant offで使用することを推奨する。
ルーターの再起動やスコープの再設定によりリース情報が消去されている場合、アドレスの延長要求をした時やリース期間内のクライアントを再起動した時にクライアントが使用するIPアドレスは変わることがある。

これを防ぐためにはdhcp server rfc2131 compliant on(あるいは
remain-silent機能を有効にする)設定がある。
この設定にすると、ヤマハルーターがリース情報を持たないクライアントから
のDHCPREQUESTに対してDHCPNAKを返さず無視するようになる。
この結果、リース期限満了時にクライアントが出すDHCPDISCOVERにRequested
IP Addressオプションが含まれていれば、そのクライアントには引き続き同じ
IPアドレスをリースすることができる。

E.の書式では、OUI(ベンダーID)のみ指定し、そのOUI(ベンダーID)を持つ機器に
のみIPアドレスを割り当てることができる。★

[14] 同一ネットワークのDHCPスコープを複数設定できるようにした。

○ DHCP スコープの定義

[書式]

dhcp scope SCOPE_NUM IP_ADDRESS-IP_ADDRESS/NETMASK [except EX_IP ...] [gateway GW_IP] [expire TIME] [maxexpire TIME]

no dhcp scope SCOPE_NUM [IP_ADDRESS-IP_ADDRESS/NETMASK [except EX_IP...] [gateway GW_IP] [expire TIME] [maxexpire TIME]]

[設定値及び初期値]

SCOPE_NUM

[設定値] : スコープ番号 (1..65535)

[初期値] : -

IP_ADDRESS-IP_ADDRESS

[設定値] : 対象となるサブネットで割り当てるIPアドレスの範囲

[初期値] : -

NETMASK

[設定値] :

xxx.xxx.xxx.xxx(xxxは十進数)

0xに続く十六進数

マスクビット数

[初期値] : -

EX_IP

[設定値] : IPアドレス指定範囲の中で除外するIPアドレス(空白で区切って

複数指定可能、'-'を使用して範囲指定も可能)

[初期値] : -

GW_IP

[設定値] : IPアドレス対象ネットワークのゲートウェイのIPアドレス

[初期値] : -

TIME : 時間

[設定値] :

設定値　　説明

1..2147483647　分

xx:xx　　時間 : 分

infinity　　無期限リース

[初期値] :

expire time=72:00

maxexpire time=72:00

[説明]

DHCPサーバーとして割り当てるIPアドレスのスコープを設定する。

除外IPアドレスは複数指定できる。リース期間としては無期限を指定できるほか、

DHCPクライアントから要求があった場合の許容最大リース期間を指定できる。

[ノート]

RTX1210 Rev.14.01.28以降、RTX830 Rev.15.02.03以降では、同一ネットワーク

のDHCPスコープを複数設定できる。★

複数のDHCPスコープで同一のIPアドレスを含めることはできない。IPアドレス範囲にネットワークアドレス、ブロードキャストアドレスを含む場合、割り当て可能アドレスから除外される。

DHCPリレーエージェントを経由しないDHCPクライアントに対してgatewayキーワードによる設定パラメータが省略されている場合にはルーター自身のIPアドレスを通知する。

DHCPスコープの設定を上書きによって変更した場合、変更前に設定していたリース情報、予約情報およびオプション情報は消去される。ただし、RTX810のRev.11.01.31以降、RTX5000/RTX3500のRev.14.00.22以降、および、Rev.15.02系以降では、予約情報とオプション情報は消去されない。

expireの設定値はmaxexpireの設定値以下でなければならない。

工場出荷状態およびcold startコマンド実行後の本コマンドの設定値については「1.7 工場出荷設定値について」を参照してください。

[15] ap config filenameコマンドで、以下の変更を行った。

- ファイル名に設定できる文字数を半角256文字(全角128文字)以下から、半角99文字(全角49文字)以下とした。
- ap config directoryコマンドで指定されたディレクトリがRTFS領域である場合は、ファイル名にマルチバイト文字を使用できないようにした。

〇アクセスポイントの設定を保存するファイル名の指定

[書式]

ap config filename NAME

no ap config filename [NAME]

[設定値及び初期値]

NAME

[設定値] : ファイル名 (半角99文字以下、全角49文字以下) ★

[初期値] : -

[説明]

アクセスポイントの設定を保存するファイル名を指定する。

本コマンドが省略された場合は、ap selectコマンドで指定された文字列に.conf

を付けたものをファイル名とする。

ただし:(コロン)は_(アンダースコア)に置き換えられる。

複数のap selectコマンドで同じファイル名を指定することができる。

ap config directoryコマンドで指定されたディレクトリがRTFS領域である場合は、

ファイル名にマルチバイト文字を使用することはできない。★

本コマンドを実行する前にap selectコマンドでアクセスポイントを指定しておく

必要がある。

[16] ap config directoryコマンドで、以下の変更を行った。

- ディレクトリのパスに設定できる文字数を半角256文字(全角128文字)以下とした。
- ディレクトリのパスがRTFS領域となる場合は、マルチバイト文字を使用できない

ようにした。

〇アクセスポイントの設定ファイルを格納するディレクトリの指定

[書式]

ap config directory PATH

no ap config directory [PATH]

[設定値及び初期値]

PATH

[設定値] : 相対パスまたは絶対パス(半角256文字以下、全角128文字以下)★

[初期値] : /ap_config

[説明]

アクセスポイントの設定ファイルを格納するディレクトリを指定する。

相対パスを指定した場合、環境変数PWDを起点としたパスと解釈される。

PWDはsetコマンドで変更可能であり、初期値は"/"である。

PATHがRTFS領域となる場合は、PATHにマルチバイト文字を使用することはできない。★

[17] 以下のコマンドで複数の相手先番号を指定できるようにした。

- pp enable
- pp disable
- tunnel enable
- tunnel disable

〇相手先の使用許可の設定

[書式]

pp enable PEER_NUM [PEER_NUM ...]

no pp enable PEER_NUM

[設定値及び初期値]

PEER_NUM

[設定値] :

設定値	説明	
番号	相手先情報番号	
番号1-番号2	番号1から番号2までの相手先情報番号	★
番号1-	番号1以上のすべての相手先情報番号	★
-番号1	番号1以下のすべての相手先情報番号	★
anonymous	anonymousインターフェース	

+------------+----------------------------------+

¦ all ¦ すべての相手先情報番号 ¦

+------------+----------------------------------+

[初期値] : -

[説明]

相手先を使用できる状態にする。工場出荷時、すべての相手先はdisable状態なので、使用する場合は必ずこのコマンドでenable状態にしなければならない。

複数指定した場合には、その全てで使用できる状態になる。★

[ノート]

必ず、1. pp disable、2. disconnect、3. pp の設定変更、4. pp enable、5. connectの手順を踏んで設定を変更する。

pp enableコマンドを実行すると内部情報の初期化が行われる。ppの設定変更の有無に関わらず、ppが接続中にpp enableを実行すると、内部情報の初期化により、ppに紐付けられているtunnel等が切断される場合がある。

〇相手先の使用不許可の設定

[書式]

pp disable PEER_NUM [PEER_NUM ...]

[設定値及び初期値]

PEER_num

[設定値] :

+------------+----------------------------------+

¦ 設定値 ¦ 説明 ¦

+------------+----------------------------------+

¦ 番号 ¦ 相手先情報番号 ¦

+------------+----------------------------------+

¦ 番号1-番号2 ¦ 番号1から番号2までの相手先情報番号¦★

+------------+----------------------------------+

¦ 番号1- ¦ 番号1以上のすべての相手先情報番号 ¦★

+------------+--------------------------------+

¦ -番号1　　¦ 番号1以下のすべての相手先情報番号 ¦★

+------------+--------------------------------+

¦ anonymous　¦ anonymousインターフェース　　¦

+------------+--------------------------------+

¦ all　　¦ すべての相手先情報番号　　¦

+------------+--------------------------------+

[初期値] : -

[説明]

相手先を使用できない状態にする。

相手先の設定を行う場合はdisable状態であることが望ましい。

複数指定した場合には、その全てで使用できない状態になる。★

○トンネルインターフェースの使用許可の設定

[書式]

tunnel enable TUNNEL_NUM [TUNNEL_NUM ...]

no tunnel enable TUNNEL_NUM

[設定値及び初期値]

TUNNEL_NUM

[設定値] :

+------------+--+

¦ 設定値　　¦ 説明　　¦

+------------+--+

¦ 番号　　¦ トンネルインターフェース番号　　¦

+------------+--+

¦ 番号1-番号2 ¦ 番号1から番号2までのトンネルインターフェース番号¦★

+------------+--+

¦ 番号1-　　¦ 番号1以上のすべてのトンネルインターフェース番号 ¦★

+------------+--+

| -番号1 | 番号1以下のすべてのトンネルインターフェース番号 |★

+----------+--+

| all | すべてのトンネルインターフェース |

+----------+--+

[初期値] : -

[説明]

トンネルインターフェースを使用できる状態にする。

工場出荷時は、すべてのトンネルインターフェースはdisable状態であり、使用する場合は本コマンドにより、インターフェースを有効にしなければならない。

複数指定した場合には、その全てで使用できる状態になる。★

○トンネルインターフェースの使用不許可の設定

[書式]

tunnel disable TUNNEL_NUM [TUNNEL_NUM ...]

[設定値及び初期値]

TUNNEL_NUM

[設定値] :

+----------+--+

| 設定値 | 説明 |

+----------+--+

| 番号 | トンネルインターフェース番号 |

+----------+--+

| 番号1-番号2 | 番号1から番号2までのトンネルインターフェース番号|★

+----------+--+

| 番号1- | 番号1以上のすべてのトンネルインターフェース番号 |★

+----------+--+

| -番号1 | 番号1以下のすべてのトンネルインターフェース番号 |★

+----------+--+

| all | すべてのトンネルインターフェース |

+------------+---+

[初期値] : -

[説明]

トンネルインターフェースを使用できない状態にする。

トンネル先の設定を行う場合は、disable状態で行うのが望ましい。

複数指定した場合には、その全てで使用できない状態になる。★

[18] show status ppコマンドで、Mobile接続時の累積時間表示を「日時分秒」形式に変更した。

[19] show status ppコマンドで、Mobile接続以外のPP接続も累積時間を表示するようにした。

[20] clear status ppコマンドで累積時間をリセットするようにした。

[21] ip routeコマンドで宛先に0.0.0.0/0を指定した場合、defaultと表示されるようにした。

[22] nat descriptor masquerade port rangeコマンドで設定できるポート範囲の個数を16に増やした。

〇IPマスカレードで利用するポートの範囲の設定

[書式]

nat descriptor masquerade port range NAT_DESCRIPTOR PORT_RANGE [...]

no nat descriptor masquerade port range NAT_DESCRIPTOR [PORT_RANGE ...]

[設定値及び初期値]

NAT_DESCRIPTOR

[設定値] : NAT ディスクリプタ番号 (1..2147483647)

[初期値] : -

PORT_RANGE

[設定値] : 間に - をはさんだポート番号の範囲

[初期値] :

4096 ：PORT_RANGE=60000-64095

10000：PORT_RANGE=60000-64095 54096-59999

20000：PORT_RANGE=60000-64095 49152-59999 44096-49151

40000：PORT_RANGE=60000-64095 49152-59999 24096-49151

65534：PORT_RANGE=49152-65534 30000-49151 10000-29999 1024-9999

RTX1210：PORT_RANGE=60000-64095 49152-59999 44096-49151

(初期設定ポート数は20000)

[説明]

IP マスカレードで利用するポート番号の範囲を設定する。

ポート番号は、まず最初に設定した範囲から利用される。最初の範囲がすべて使用中になったら、次の範囲のポート番号を使い始める。このように、設定した順番にポート番号が利用される。

RTX5000/RTX3500はNATの最大同時セッション数が65534であるが、初期設定ではウェルノウンポートを除いた64511個のポートしか使用できないため、同時セッション数を65534まで拡張する場合は、本コマンドで65534個のポートを使用できるようにポート範囲を広げる必要がある。

Rev.14.01系以降では、同一のポート番号を使用して複数の接続先とのセッションを確立できるため、本コマンドで設定したポート数を超えるセッションの確立が可能である。Rev.14.01系以降では、最大セッション数はnat descriptor masquerade session limit totalコマンドで設定する。 ただしRev.14.01系以降においても、nat descriptor backward-compatibilityコマンドでtypeパラメーターを1に変更した場合は、最大セッション数は本コマンドで設定したポート数

と同等となるため、最大セッション数を変更する場合は本コマンドの設定を変更する必要がある。

[ノート]

機種ごとの最大使用ポート数と利用可能なポート範囲の個数を下表に示す。

機種	最大使用ポート数	ポート範囲の個数
RTX830 Rev.15.02.03以降	65534	16 ★
RTX1210 Rev.14.01.26以降	65534	16
RTX830 Rev.15.02.01	65534	4
RTX1210 Rev.14.01.20以前	65534	4
RTX5000、RTX3500、RTX1210、RTX830	65534	4
RTX3000	40000	3
RTX1200	20000	3
RTX810	10000	2
上記以外	4096	1

[23] VRRPのシャットダウントリガーの設定で、TUNNELインターフェースに対応した。

○VRRPシャットダウントリガーの設定

[書式]

ip INTERFACE vrrp shutdown trigger VRID INTERFACE

ip INTERFACE vrrp shutdown trigger VRID pp PEER_NUM

ip INTERFACE vrrp shutdown trigger VRID tunnel TUNNEL_NUM ★

ip INTERFACE vrrp shutdown trigger VRID route NETWORK [NEXTHOP]

no ip INTERFACE vrrp shutdown trigger VRID INTERFACE

no ip INTERFACE vrrp shutdown trigger VRID pp PEER_NUM

no ip INTERFACE vrrp shutdown trigger VRID tunnel TUNNEL_NUM ★

no ip INTERFACE vrrp shutdown trigger VRID route NETWORK

[設定値及び初期値]

INTERFACE

[設定値] : LANインターフェース名

[初期値] : -

VRID

[設定値] : VRRPグループID(1..255)

[初期値] : -

PEER_NUM

[設定値] : 相手先情報番号

[初期値] : -

TUNNEL_NUM ★

[設定値] : トンネルインターフェース番号

[初期値] : -

NETWORK

[設定値] :

ネットワークアドレス

IPアドレス/マスク長

default

[初期値] : -

NEXTHOP

[設定値] :

インターフェース名

IPアドレス

[初期値] : -

[説明]

設定したVRRPグループでマスタールーターとして動作している場合に、指定した条件によってシャットダウンすることを設定する。

形式	説明
LANインターフェース形式	指定したLANインターフェースがリンクダウンす

	¦るか、あるいはlan keepaliveでダウンが検知さ ¦れると、シャットダウンする。
pp形式	¦指定した相手先情報番号に該当する回線で通信で ¦きなくなった場合にシャットダウンする。通信で ¦きなくなるとは、ケーブルが抜けるなどレイヤ1 ¦が落ちた場 合と、以下の場合である。 ¦ ・pp keepalive use設定によりダウンが検出さ ¦ れた場合
tunnel形式	¦指定したトンネルインターフェースが以下の条件 ¦によりダウンした場合にシャットダウンする。 ¦ ・IPsecトンネルで、ipsec ike keepalive use ¦ 設定によりダウンが検出された場合 ¦ ・L2TP/IPsec、L2TPv3、L2TPv3/IPsecのいずれ ¦ かのトンネルで、l2tp keepalive use設定に ¦ よりダウンが検出された場合 ¦ ・PPTPトンネルで、pptp keepalive use設定に ¦ よりダウンが検出された場合 ¦ ・IPIPトンネルで、ipip keepalive use設定に ¦ よりダウンが検出された場合
route 形式	¦指定した経路が経路テーブルに存在しないか、 ¦NEXTHOP で指定したインターフェースもしくはIP ¦アドレスで指定するゲートウェイに向いていない ¦場合に、シャットダウンする。NEXTHOPを省略し ¦た場合には、経路がどのような先を向いていても ¦存在する限りはシャットダウンしない。

----------+----------

[24] VRRPv3のシャットダウントリガーの設定で、TUNNELインターフェースに対応した。

〇VRRPv3シャットダウントリガーの設定

[書式]

ipv6 INTERFACE vrrp shutdown trigger VRID INTERFACE

ipv6 INTERFACE vrrp shutdown trigger VRID pp PEER_NUM

ipv6 INTERFACE vrrp shutdown trigger VRID tunnel TUNNEL_NUM ★

ipv6 INTERFACE vrrp shutdown trigger VRID route NETWORK [NEXTHOP]

no ipv6 INTERFACE vrrp shutdown trigger VRID INTERFACE

no ipv6 INTERFACE vrrp shutdown trigger VRID pp PEER_NUM

no ipv6 INTERFACE vrrp shutdown trigger VRID tunnel TUNNEL_NUM ★

no ipv6 INTERFACE vrrp shutdown trigger VRID route NETWORK

[設定値及び初期値]

INTERFACE

[設定値] : LANインターフェース名

[初期値] : -

VRID

[設定値] : VRRPv3グループID(1..255)

[初期値] : -

PEER_NUM

[設定値] : 相手先情報番号

[初期値] : -

TUNNEL_NUM ★

[設定値] : トンネルインターフェース番号

[初期値] : -

NETWORK

[設定値] :

IPv6プレフィックス/プレフィックス長

default

[初期値] : -

NEXTHOP

[設定値] :

インターフェース名

IPv6アドレス

[初期値] : -

[説明]

設定したVRRPv3グループでマスタールーターとして動作している場合に、指定した条件によってシャットダウンすることを設定する。

形式	説明
LANインターフェース形式	指定したLANインターフェースがリンクダウンするか、あるいはlan keepaliveでダウンが検知されると、シャットダウンする。
pp形式	指定した相手先情報番号に該当する回線で通信できなくなった場合にシャットダウンする。通信できなくなるとは、ケーブルが抜けるなどレイヤ1が落ちた場 合と、以下の場合である。 ・pp keepalive use設定によりダウンが検出された場合
tunnel形式	指定したトンネルインターフェースが以下の条件によりダウンした場合にシャットダウンする。 ・IPsecトンネルで、ipsec ike keepalive use設定によりダウンが検出された場合

| ・L2TP/IPsec、L2TPv3、L2TPv3/IPsecのいずれ
| かのトンネルで、l2tp keepalive use設定に
| よりダウンが検出された場合
| ・PPTPトンネルで、pptp keepalive use設定に
| よりダウンが検出された場合
| ・IPIPトンネルで、ipip keepalive use設定に
| よりダウンが検出された場合

---

route 形式 | 指定した経路が経路テーブルに存在しないか、
| NEXTHOPで指定したインターフェースもしくは
| IPv6アドレスで指定するゲートウェイに向いてい
| ない場合に、シャットダウンする。NEXTHOPを省
| 略した場合には、経路がどのような先を向いてい
| ても存在する限りはシャットダウンしない。

---

[25] 以下のコマンドで、サブネットマスクに0を設定できるようにした。

- ipsec ike local id
- ipsec ike remote id

[26] schedule atコマンドで以下のコマンドを実行できるようにした。

- pp select
- tunnel select
- switch select
- ap select

[27] show status ynoの表示内容を変更した。

[28] 通信帯域が細い回線経由でのWeb GUIやカスタムGUIへのアクセス性能を改善した。

[29] Web GUIの表示速度を改善した。

[30] Web GUIのLANマップで、LANマップの設定ダイアログの「端末の更新間隔」に対象機種を記載した。

[31] WebGUIのLANマップで、スレーブの温度異常による給電停止が発生したときの通知メッセージの文言を変更した。

[32] Web GUIのLANマップのタグVLANページで、アップリンクポートを表す矢印アイコンの色を変更した。

[33] Web GUIの以下の画面で使用される「ファイルの一覧」ダイアログのレイアウト、文言を変更した。
- LANマップのSWX2200のファームウェア更新ダイアログ
- 管理の[保守]-[CONFIGファイルの管理]-[CONFIGファイルのインポート/エクスポート]
- 管理の[保守]-[ファームウェアの更新]-[外部メモリからファームウェアを更新]

[34] Web GUIの管理の[アクセス管理]-[ユーザーの設定]で、自分自身のユーザーを削除したり、ユーザー名を変更できないようにした。

[35] Web GUIのLANマップのヘルプで、スレーブのCONFIGバックアップ機能の注意事項を変更した。

[36] Web GUIの以下のヘルプで、「推奨のIPフィルターを設定する」を選択した場合に設定されるIPフィルターについての説明を変更した。
- かんたん設定の[プロバイダー接続]

- 詳細設定の[プロバイダー接続]

[37] Web GUIの以下のページで、適用するフィルターやNATディスクリプターを、クリックで選択するように変更した。
- 詳細設定の[ルーティング]-[フィルター型ルーティングの設定]
- 詳細設定の[NAT]-[インターフェースへの適用の設定]
- 詳細設定の[セキュリティ]-[IPフィルター]-[適用されているIPフィルターの一覧]
-[インターフェースへの適用の設定]

[38] Web GUIで、アドレスやポート番号等をカンマまたはハイフンまたは半角スペースで区切って入力できるようにした

[39] Web GUIで、デザインやレイアウト等を修正し、視認性や操作性を改善した。

[40] Web GUIの管理の[アクセス管理]-[ユーザーの設定]の「ユーザーの設定」で、各ユーザーの自動ログアウトまでの時間を設定できるようにした。

[41] Web GUIの画面右上に自動ログアウトまでの時間を表すアイコンを表示するようにした。
また、画面右上のユーザー名から開くユーザーメニュー内に、自動ログアウトまでの時間を表示するようにした。

[42] Web GUIの管理の[アクセス管理]-[ユーザーの設定]の「ユーザーの設定」の設定入力ページで、設定項目の順序を変更した。

■バグ修正

[1] YNOエージェント機能で、YNOマネージャーとの通信中に稀にリブートすることがあるバグを修正した。

[2] IPsecによるデータコネクトの拠点間接続で、トンネルインターフェースにout方向のフィルターが設定されていると、稀にハングアップすることがあるバグを修正した。

[3] L2TPv3経由でタグ付きIPv6パケットを受信したとき、リブートすることがあるバグを修正した。

[4] モバイルインターネット接続のWANインターフェース接続経由でL2TPv3接続をするとリブートすることがあるバグを修正した。

[5] BGPを使用しているとき、トンネルインターフェースがダウンすると稀にリブートすることがあるバグを修正した。

[6] L2MSのマスターとして動作しているとき、 マスターのLAN1とスレーブのポート間でループが発生するとリブートするバグを修正した。

[7] ip INTERFACE tcp mss limitコマンド(初期値 off)にoff以外の値を設定しているとき、不正なフォーマットのウィンドウスケールオプションを含んだTCPパケットを受信するとリブートすることがあるバグを修正した。

[8] UPnP機能で、content-lengthヘッダがない、またはcontent-lengthヘッダの値が0であるPOSTリクエストを受信するとリブートするバグを修正した。

[9] SFTPでログインをして、systemディレクトリ内でファイルの一覧を表示するとリブートすることがあるバグを修正した。

[10] dhcp client optionコマンドでパラメーターが足りないときにリブートするバグを修正した。

[11] vlan INTERFACE 802.1qコマンドが設定されているとき、IEEE802.1Qタグが複数付加されたフレームを受信するとリブートする可能性を排除した。

[12] 以下の場合にリブートやハングアップが発生したりシステムが不安定になることがあるバグを修正した。

- すべてのLANインターフェースにIPアドレスが付与されていない状態でip LANインターフェース address dhcpコマンドを設定したとき
- no ip LANインターフェース addressコマンドですべてのLANインターフェースのIPアドレスを削除したとき

[13] ipv6 routeコマンドで、宛先に::/0を指定したときにリブートするバグを修正した

[14] nat descriptor masquerade port rangeコマンドで、ポート範囲を1つも指定せずに実行するとリブートするバグを修正した。

[15] Web GUIの詳細設定の[NAT]で、静的NATとIPフィルターが設定されているインターフェースに対して、以下の操作を行うとリブートするバグを修正した。

- [NATディスクリプターの設定]で静的NATの設定を削除・変更する
- [インターフェースへの適用の設定]でNATディスクリプターの適用を外す

[16] YNOエージェント機能で、以下のタイミングでメモリーリークが発生することがあるバグを修正した。

- yno useコマンドの設定をonに変更したとき
- yno useコマンドがonに設定されている状態で、下記のコマンドの設定を変更したとき
  - yno access code
  - yno log
- YNOマネージャーの[機器管理]-[アクセスコード]でアクセスコードを変更し、ルーターのyno access codeコマンドの設定値が変更されたとき

[17] OSPFv3の使用中にメモリーリークが発生するバグを修正した。

[18] L2MSのマスターとして動作している状態で以下のいずれかの条件を満たしたとき、メモリーリークが発生するバグを修正した。

- スレーブスイッチ(SWX2300シリーズ、SWX2100-24G)でSFP受光レベル異常が発生した
- スレーブスイッチ(SWX2300シリーズ、SWX2100-24G)で送信キュー使用率異常が発生した

[19] SIP通信中の呼に対してOPTIONSリクエストを受信したときにレスポンスを返すと、メモリーリークが発生するバグを修正した。

[20] heartbeat2 transmit enableコマンドで、メモリーリークが発生することがあるバグを修正した。

[21] YNOエージェント機能で、実行中CONFIGがルーターに保存されていないときに、YNOマネージャーの「機器一覧」のコマンド実行ページからコマンドが実行できないバグを修正した。

[22] モバイルインターネット機能のPPインターフェース接続で、網への接続ができなくなることがあるバグを修正した。

[23] マルチポイントトンネルで、IPv6トンネルローカルアドレスに基づいて自動生成されたIPv6 implicit経路がトンネルダウン時に消滅するバグを修正した。

[24] マルチポイントトンネルで、トンネル確立前に設定した対向拠点のトンネルアドレ

スをゲートウェイアドレスとするIPv4静的経路が有効にならないバグを修正した。

[25] PP[03]インターフェース経由でIPsecトンネルの接続をしているとき、トンネルインターフェース宛の通信がファストパスで処理されないバグを修正した。

[26] ipsec ike local addressコマンドでvrrpを指定しVRRPの状態に連動させている IPsec IKEv1トンネルにおいて、トンネル確立前にVRRPマスタールーターが切り替わると、ipsec ike retryコマンドの再送設定回数(初期値 10)に到達するまで旧マスタールーター(非マスタールーター)からのIKEパケットの再送が停止しないバグを修正した。

[27] L2TP/IPsecで、1つのトンネルに対して複数のクライアントが接続できてしまうことがあるバグを修正した。現象が発生した場合は先に接続していたクライアントが切断される。

[28] L2TPv3経由でタグ付きパケットを受信したとき、TCPのMSS調整が行われないバグを修正した。

[29] L2MSのマスターとして動作しているとき、L2MSスレーブとして動作しているルーターの機器情報を正しく取得できないことがあるバグを修正した。
このバグにより、YNOマネージャーの[機器一覧]-[機器詳細]-[一覧マップ]でL2MSスレーブとして動作しているルーターのIPアドレスが表示されないことがあった。

[30] 同時に複数の機能でICMP Echoの応答を待っているとき、応答が返って来ても稀に正しく認識できずに応答なしと誤判定されることがあるバグを修正した。

[31] 対話形式でないユーザーインターフェースからLuaスクリプト機能の以下のコマンドや関数を実行したとき、シリアルコンソールが正しく動作しなくなるバグを修正した。

- luaコマンド (-vオプション指定時)
- luacコマンド (-vオプション及び-lオプション指定時)
- print関数

[32] Luaスクリプト機能で、ソケット通信ライブラリを使用するとルーター本体のLEDが正常に動作しなくなるバグを修正した。

[33] TCPでSIPの不正アクセスを受けたときに、SIPの通信ができなくなってしまうことがあるバグを修正した。

[34] ファストパスで処理されたIPv6パケットについて、以下のMIB変数のカウントが行われないバグを修正した。
- 1.3.6.1.2.1.2.2.1.10.x ifInOctets
- 1.3.6.1.2.1.2.2.1.11.x ifInUcastPkts

[35] ファストパスで処理されたIPv6パケットについて、以下のMIB変数のカウントが行われないことがあるバグを修正した。
- 1.3.6.1.2.1.2.2.1.17.x ifOutUcastPkts

[36] IPIPトンネルおよびIPsecトンネルで、トンネルインターフェースのIPv6パケットについて、以下のMIB変数のカウントが行われないバグを修正した。
- 1.3.6.1.2.1.2.2.1.10.x ifInOctets
- 1.3.6.1.2.1.2.2.1.11.x ifInUcastPkts
- 1.3.6.1.2.1.2.2.1.16.x ifOutOctets
- 1.3.6.1.2.1.2.2.1.17.x ifOutUcastPkts

[37] 以下のコマンドで動的アドレスのプレフィックス長を省略した時に、正しくフィルタリングされないバグを修正した。
- ipv6 filter

- ipv6 filter dynamic
- ipv6 inbound filter
- ipv6 policy filter

[38] dhcp client release linkdownコマンドがonに設定されているとき、同コマンドのタイマー値よりも長くリンクダウンしたにもかかわらず、経路情報等が削除されないバグを修正した。
本バグにより、リンクアップ後に新たにDHCPサーバーから得た経路情報が反映されないことがあった。

[39] RIP-2の認証キーの文字列を半角16文字で設定すると通信できないバグを修正した。

[40] SWX2300シリーズから送信負荷の異常を通知されたとき、キューの番号と負荷の状態のログが正しく表示されないバグを修正した。

[41] ip pp remote address poolコマンドで、最大トンネル対地数分のIPアドレスを設定できないバグを修正した。

[42] ip INTERFACE intrusion detection thresholdコマンドが入力できるバグを修正した。

[43] dns staticコマンドとip hostコマンドで、64文字以上のラベルを持つFQDNを入力できてしまうバグを修正した。

[44] console characterコマンドの設定値がja.utf8のとき、show dns cacheコマンドの出力結果の日本語が文字化けするバグを修正した。

[45] show lan-mapコマンドでdetailオプションを2回タブ補完できるバグを修正した。

[46] 以下のコマンドで不正なパラメーターを入力したときのエラーメッセージを修正した。

- no dhcp client option
- no ip keepalive
- no ipsec sa policy
- switch control function set macaddress-aging-timer

[47] show status bridge1コマンドで、表示を途中で中断できないバグを修正した。

[48] ip INTERFACE rip sendコマンドでパラメーターチェックの不備を修正した。

[49] show lan-mapコマンドを実行して表示される項目名の誤記を修正した。

[50] show ip route detailコマンドを実行したとき、RIP、OSPF、BGPで通知された経路の「付加情報」に誤った文字列が出力されることがあるバグを修正した。

[51] show status userコマンドで、ユーザー名が正しく表示されないことがあるバグを修正した。

[52] show ipv6 connectionコマンドでVLANインターフェースがタブ補完されないバグを修正した。

[53] 以下のコマンドヘルプの誤記を修正した。

- ip route
- ipsec sa policy
- ipsec transport
- ipsec tunnel
- ipv6 filter

- no ipsec sa policy
- no ipsec transport
- pp bind
- show ip connection
- show ipv6 connection
- url filter

[54] Web GUIで、SYSLOG画面やTECHINFO画面のページ表示中あるいは「テキストファイルで取得」中にWebブラウザーを閉じるなどしてルーターからWebブラウザーへデータを送信できなくなると、数分間Web GUIの応答がなくなることがあるバグを修正した。

[55] Web GUIを開いたままルーターを再起動すると、ブラウザによってはログアウトダイアログ表示後に認証ダイアログが表示されるバグを修正した。

[56] Web GUIで、ヘッダー部分に表示されている「？」アイコンをクリックしてもヘルプが開かないことがあるバグを修正した。

[57] Web GUIの以下のページで、チェックボックスやラジオボタンに対応するテキストをクリックしても、チェックボックスやラジオボタンの状態が切り替わらないバグを修正した。
- ダッシュボード
- かんたん設定
  - [VPN]-[拠点間接続]-[IPsecに関する設定]
  - [VPN]-[リモートアクセス]-[共通設定]
- 詳細設定
  - [NAT]-[NATディスクリプターの設定]

[58] Web GUIのダッシュボードのガジェットでツールチップに表示される情報が、マウスが示している箇所とは別の情報が表示されたり、最新の情報が表示されないことが

あるバグを修正した。

[59] Web GUIのダッシュボードのトラフィック情報ガジェットのINグラフの表示に、ファストパスで処理されたIPv6パケットがカウントされていないバグを修正した。

[60] Web GUIのダッシュボードのトラフィック情報(TUNNEL)ガジェットのグラフ表示に、IPv6パケットが反映されないバグを修正した。

[61] Web GUIのダッシュボードのURLのキーワードチェック統計ガジェットで、画面分離するとページタイトルが「不正アクセス検知機能」と表示されるバグを修正した。

[62] Web GUIの以下のページで、外部メモリー内のファームウェアファイルまたはCONFIGファイルのパスを表示するとき、全角文字が含まれていると文字化けして表示されるバグを修正した。

- ダッシュボードのシステム情報ガジェット
- 管理の[保守]-[ファームウェアの更新]-[外部メモリからファームウェアを更新]
- 管理の[保守]-[CONFIGファイルの管理]-[CONFIGファイルのインポート]
- 管理の[保守]-[CONFIGファイルの管理]-[CONFIGファイルのエクスポート]
- 管理の[保守]-[再起動と初期化]-[再起動]

[63] L2MSスレーブの機器名または端末情報DBの機器名に特定の文字コードが含まれていると、Web GUIでLANマップが表示できないバグを修正した。

[64] WLX202のVLANの設定を変更したとき、WebGUIの[LANマップ]-[タグVLANページ]でWLX202のタグVLAN情報を更新できなくなることがあるバグを修正した。

[65] 同じ経路のスレーブが複数台存在する構成でLANマップを使用しているとき、Web GUIの一覧マップでスレーブが正しく表示されないことがあるバグを修正した。

[66] Web GUIのLANマップで、端末管理機能を有効、無効、有効の順番で切り替えたとき、ヤマハ無線APに接続されている端末が検出できなくなるバグを修正した。

[67] Web GUIのLANマップの以下の画面で各種設定や保守操作を行ったとき、正しくエラーメッセージが表示されないことがあるバグを修正した。
- マップ画面の「スイッチの設定・保守」ダイアログ
- マップ画面の「ポートの設定」ダイアログ
- タグVLAN画面の「VLAN間フィルター」設定ダイアログ

[68] Web GUIのLANマップからHTTPプロキシー経由でL2MSのスレーブルーターにアクセスして、以下のページでLAN1のアドレスを変更した場合に、Web GUIを開き直すために表示されるリンクの遷移先が正しくないバグを修正した。
- かんたん設定の[基本設定]-[LAN1アドレス]
- 詳細設定の[LAN]

[69] Web GUIのLANマップで、スレーブがリンクダウンした直後に[スレーブの管理]ダイアログを開こうとすると、プログレスバーが表示されたままになることがあるバグを修正した。

[70] Web GUIのLANマップで、すでにCONFIGファイルが保存されているときにスレーブCONFIGの保存先を外部メモリのルートディレクトリに変更できないバグを修正した。

[71] Web GUIのLANマップのスナップショット機能でWLX402の経路異常が検知されたとき、以下の機能で表示されるWLX402の経路情報にアップリンクポートが表記されないバグを修正した。
- Web GUI のマップページ
- LANマップのメール通知
- SYSLOG

[72] Web GUIのLANマップで、異常が検知されているSFPポートのポートアイコンが正しく表示されないバグを修正した。

[73] Web GUIのLANマップのタグVLANページで、以下のバグを修正した。
- スレーブ機器が画面から見切れたとき、水平スクロールバーが表示されないことがある
- 水平スクロールしたとき、機器の画像が移動しない

[74] Web GUIのかんたん設定の[日付と時刻]で、一般ユーザー権限でログインしたときに日時の同期の「今すぐ同期」ボタンがグレーアウトしていないバグを修正した。

[75] Web GUIのかんたん設定の[基本設定]-[管理パスワード]で、管理パスワードが暗号化なしで設定されていても「パスワードの暗号化」の「暗号化する」が選択されているバグを修正した

[76] Web GUIのかんたん設定の[基本設定]-[管理パスワード]の入力内容の確認画面で、注意文が表示されないバグを修正した。

[77] Web GUIで以下の操作を行うと、必要なポート開放がされないことがあるバグを修正した。
- プロバイダー接続設定がある状態で、かんたん設定の[VPN]からVPN接続の設定を追加する
- VPN接続の設定がある状態で、かんたん設定の[プロバイダー接続]から、「推奨のIPフィルターを設定する」を選択して設定変更を行う

[78] Web GUIのかんたん設定の[プロバイダー接続]-[IPフィルターの設定]で、16個以上静的IPマスカレードが設定されているインターフェースに対してIPフィルターの設定を行ったとき、15個までしか静的IPマスカレードのためのIPフィルターが設定さ

れないバグを修正した。

[79] wan1インターフェースにIPアドレスとNATディスクリプターまたはDNSの設定があり、デフォルト経路の設定がないとき、Web GUIの以下のページで、WAN1と表示されるべきところがLAN3と表示されるバグを修正した。
- かんたん設定の[プロバイダー接続]の「設定の一覧」
- 詳細設定の[プロバイダー接続]の「設定の一覧」

[80] Web GUIのかんたん設定の[VPN]-[拠点間接続]-[経路に関する設定]で、[接続先のLAN側のアドレス]の最大設定数を超えても入力欄を追加できてしまうバグを修正した。

[81] Web GUIの以下のページでトンネルインターフェースを削除したとき、トンネルインターフェースに設定されているIPフィルターの設定が削除されないバグを修正した。
- かんたん設定の[VPN]-[拠点間接続]
- かんたん設定の[VPN]-[クラウド接続]

[82] Web GUIのかんたん設定の[VPN]-[拠点間接続]-[IPsecに関する設定]で、VPN接続を新規に追加したとき、ipsec ike local addressコマンドが自動で設定されないバグを修正した。

[83] Web GUIのかんたん設定の[VPN]-[クラウド接続]から設定名に半角スペースや一部の記号を含む文字列を設定し、「AWS からの設定情報取得」を実行すると「CONFIG 作成」でエラーになるバグを修正した。

[84] Web GUIの詳細設定と管理で、アコーディオンメニューの表示・非表示が切り替わらない可能性を排除した。

[85] Web GUIで「<」や「>」、「&」などの記号を使用して設定を行うと、テキストボッ

クス内の文字が正しく表示されないことがあるバグを修正した。

[86] Web GUIの詳細設定のPPPoE接続、IPv6 PPPoE接続の[プロバイダー接続]で、pppoe auto disconnectコマンドがoffに設定されていても、pppoe disconnect timeコマンドが設定されていると、「自動切断する」と表示されるバグを修正した。

[87] Web GUIの以下のページで、WAN側IPアドレスとデフォルトゲートウェイの入力欄にそれぞれ異なるネットワークのアドレスを入力して「確認」ボタンを押したとき、エラーの表示が正しくないバグを修正した。
- 詳細設定の[プロバイダー接続]-[設定内容]-[基本設定]
- 詳細設定の[プロバイダー接続]-[プロバイダー接続の設定]

[88] Web GUIの詳細設定の[プロバイダー接続]で、11以上の番号のPPインターフェースの設定をするとき、基本設定の入力ページと入力内容の確認ページの「PP[XX]のIPアドレス」の項目名のPP番号が誤って表示されるバグを修正した。

[89] Web GUIの詳細設定の[プロバイダー接続]で、ポート開放の設定をするとき、IPフィルターの設定可能数のチェックが行われていないバグを修正した。

[90] Web GUIの詳細設定の[プロバイダー接続]で、ポート開放の[複製]ボタンを押したとき、テキストボックスに"undefined"と表示されることがあるバグを修正した。

[91] Web GUIの詳細設定の[プロバイダー接続]-[プロバイダー接続の設定]で、接続種別が「モバイル接続（イーサネット方式）」のとき、インターフェース名にURLエンコード文字が含まれてしまうバグを修正した。
Webブラウザーとして Firefoxを使用したときのみ発生する。

[92] Web GUIの詳細設定の[プロバイダー接続]の[ポート開放の設定]で、「転送用ポートの開放」の「ポート番号」が16文字以上のとき、以下のバグを修正した。

- 正しく表示されない
- 入力値を変更せずに設定すると、一時的に通信が途切れることがある

[93] Web GUIの以下のページで、LAN分割機能が有効なときにVLANと表示されるべきところがLANと表示されるバグを修正した。
- 詳細設定の[NAT]
- 詳細設定の[セキュリティ]-[IPフィルター]
- 詳細設定の[セキュリティ]-[URLフィルター]
- 詳細設定の[セキュリティ]-[不正アクセス検知]
- 詳細設定の[DNSサーバー]
- 詳細設定の[メール通知]
- 管理の[アクセス管理]-[各種サーバーの設定]

[94] Web GUIの詳細設定の[URLフィルター]-[インターフェースへの適用状況]で、PPインターフェースにキーワードチェックのデフォルトルールを設定できないバグを修正した。

[95] Web GUIの詳細設定の[セキュリティー]-[不正アクセス検知]で、PPTP以外のトンネルインターフェースに対してWinnyもしくはShareの設定を有効にしても、IPフィルターが設定されないバグを修正した。

[96] Web GUIの管理の[アクセス管理]-[各種サーバーの設定]で、アクセスを許可するホストの設定が正しく変更できないことがあるバグを修正した。

[97] Web GUIの管理の[本体の設定]-[日付と時刻の設定]で「日時同期」の「定期間隔」を「使用しない」に変更したときに「同期日時」の「字:分:秒」および「問い合わせ先NTPサーバー」の項目がグレーアウトしないバグを修正した。

[98] Web GUIの管理の[アクセス管理]-[ユーザーの設定]で、ユーザーが最大数設定され

ているときに「新規」ボタンを押すと、設定画面に進むことができてしまうバグを修正した。

[99] Web GUIの管理の[保守]-[コマンドの実行]を開いたときにヘルプアイコンにフォーカスがあたるバグを修正した。

[100] Web GUIの管理の[保守]-[コマンドの実行]で、「<」や「>」などの記号が出力されるコマンドを実行すると、「コマンド実行結果」で文字化けして表示されるバグを修正した。

[101] Web GUIの管理の[保守]-[CONFIGファイルの管理]で、インポートまたはエクスポートするファイルパスが長いとき、入力内容の確認ページの表示が崩れるバグを修正した。

[102] Web GUIの管理の以下のページで、ディレクトリーの一覧から選択したファイル名に半角スペースが含まれるとき、別のファイル名で設定されてしまうバグを修正した。

- [外部デバイス連携]-[USB / microSD]-[SYSLOGの外部メモリーへの保存]
- [外部デバイス連携]-[USB / microSD]-[外部メモリー内のファイルを用いた起動]
- [外部デバイス連携]-[USB / microSD]-[ボタン操作による外部メモリーからのインポート]
- [保守]-[ファームウェアの更新]-[外部メモリからファームウェアを更新]
- [保守]-[CONFIGファイルの管理]-[CONFIGファイルのインポート]
- [保守]-[CONFIGファイルの管理]-[CONFIGファイルのエクスポート]

[103] Web GUIで誤記および表記のゆれを修正した。

[104] IPsec(IKEv1、IKEv2)、L2TP/IPsec、L2TPv3/IPsecで複数のトンネルが設定されてい

るとき、以下の条件をすべて満たす場合に事前共有鍵が短い方のトンネルが接続できなくなることがあるバグを修正した。

- 事前共有鍵の長さが異なるトンネルが存在する
- 長い方の事前共有鍵の先頭に短い方の事前共有鍵が含まれている

[条件と合致する設定例]

- 例1
  トンネル1の事前共有鍵: AAAA
  トンネル2の事前共有鍵: AAAABBBB
- 例2
  トンネル1の事前共有鍵: ABCD
  トンネル2の事前共有鍵: AB

例1では、トンネル1が接続できなくなることがある。
例2では、トンネル2が接続できなくなることがある。

[条件と合致しない設定例]

- 例1
  トンネル1の事前共有鍵: AAAA
  トンネル2の事前共有鍵: AAAA
- 例2
  トンネル1の事前共有鍵: AB
  トンネル2の事前共有鍵: ACB
- 例3
  トンネル1の事前共有鍵: AAAA
  トンネル2の事前共有鍵: BBBBAAAA

[105] DHCPサーバー機能でDHCPINFORMメッセージを受信したとき、以下の条件をすべて満たすとリブートするバグを修正した。

- 指定されたIPアドレスと同じネットワークアドレスのスコープが設定されている
- 指定されたIPアドレスを含むスコープが設定されていない

Rev.15.02.03でのみ発生する。

[106] 以下のコマンドがすべて設定されているとき、UPnPのポートマッピングのリクエストを受信するとリブートするバグを修正した。
- nat descriptor backward-compatibility 1
- upnp use on

Rev.15.02.03でのみ発生する。
