Biz Box ルータ「N1200」
ファームウェアリリースノート
Rev.10.01.64

N1200 Rev.10.01.53 からの変更点

以下のとおり機能追加・機能改善が行われました。

1. 本バージョンで追加された機能

■追加機能

[1] 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。

- docomo L-03F
- EMOBILE GL08D
- IIJ mobile UX312NC
- NCXX UX102NC
- NCXX RT-WJ02
- NTTコム MF112A
- NTTコム UX302NC
- Sonet FS01BU

以下のメーカサイトも参考にしてください。

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

[2] GUIで、以下に対応した。

- [DHCP認証]で、DHCPオプションを設定できるようにした。

[3] NTT東日本/NTT西日本フレッツ光ネクストのリナンバリングに対応した

[4] VRRPv3の一部機能に対応した。

ipv6 INTERFACE vrrpコマンド、およびipv6 INTERFACE vrrp shutdown triggerコマンドを追加した。

以下のメーカサイトも参考にしてください。

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

〇インターフェース毎のVRRPv3の設定

[書式]

```
  ipv6 INTERFACE vrrp VRID IPV6_ADDRESS [priority=PRIORITY] [preempt=PREEMPT] [auth=AUTH]
[advertise-interval=TIME1] [down-interval=TIME2]
  no ipv6 INTERFACE vrrp VRID [VRID...]
```

[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] : -

IPV6_ADDRESS

［設定値］: 仮想ルーターのIPv6アドレス

［初期値］: -

PRIORITY

［設定値］: 優先度(1..254)

［初期値］: 100

PREEMPT : プリエンプトモード

［設定値］:

設定値	説明
on	プリエンプトモードを使用する
off	プリエンプトモードを使用しない

［初期値］: on

AUTH

［設定値］: テキスト認証文字列(8文字以内)

［初期値］: -

TIME1

［設定値］: VRRPv3広告の送信間隔(秒)

［初期値］: 1

TIME2

［設定値］: マスターがダウンしたと判定するまでの時間(秒)

［初期値］: 3

［説明］

指定した VRRPv3 グループを利用することを設定する。同じ VRRPv3 グループに所属するルーターの間では、VRID および仮想ルーターの IPv6 アドレスを一致させておかなくてはいけない。これらが食い違った場合の動作は予測できない。AUTH パラメーターを指定しない場合には、認証なしとして動作する。TIME1 および TIME2 パラメーターで、マスターが VRRPv3 広告を送信する間隔と、バックアップがそれを監視してダウンと判定するまでの時間を設定する。トラフィックが多いネットワークではこれらの値を初期値より長めに設定すると動作が安定することがある。これらの値はすべての VRRPv3 ルーターで一致している必要がある。

［ノート］

PRIORITY および PREEMPT パラメーターの設定は、仮想ルーターの IPv6 アドレスとして自分自身の LAN インターフェースに付与されているアドレスを指定している場 合には無視される。この場合、優先度は最高の 255 となり、常にプリエンプトモードで動作する。

○シャットダウントリガの設定

［書式］

```
ipv6 INTERFACE vrrp shutdown trigger VRID INTERFACE
ipv6 INTERFACE vrrp shutdown trigger VRID pp PEER_NUM [dlci=DLCI]
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 [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]：-

DLCI
[設定値]：DLCI番号
[初期値]：-

NETWORK
[設定値]：
■IPv6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
■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。 - 回線がISDN回線である時は、呼が接続されていない場合 回線が専用線である時には、LCPキープアライブによって通信相手が落ちたと判断した場合 - 回線がフレームリレーであって"dlci=DLCI"を指定している場合には、 PVC状態確認手順によって指定したDLCI番号が通信できないと判断した場合 - pp 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。

---

[5] 以下のコマンドについて、reboundオプションを追加した。

- ip icmp time-exceeded send
- ip icmp unreachable send
- ipv6 icmp time-exceeded send
- ipv6 icmp unreachable send

このオプションをonに設定することにより、受信したパケットに対するそれぞれのICMPエラーを経路と関係なく受信したインターフェースから送信することができる。

○ICMP Time Exceededを送信するか否かの設定

[書式]

ip icmp time-exceeded send SEND [rebound=SW]
ipv6 icmp time-exceeded send SEND [rebound=SW]
no ip icmp time-exceeded send
no ipv6 icmp time-exceeded send

[設定値及び初期値]

SEND

[設定値]:

設定値	説明
on	送信する
off	送信しない

[初期値]:on

SW ★

[設定値]:

設定値	説明
on	受信インターフェースから送信する
off	経路に従って送信する

[初期値]:off

[説明]

受信したIPパケットのTTLが0になってしまったため、そのパケットを破棄した場合に、同時にパケットの送信元に対して ICMP Time Exceeded を送信するか否かを設定する。rebound オプションをonに設定した場合には、経路設定に関係なく、元となるパケットを受信したインターフェースから送信する。 ★

○ICMP Destination Unreachableを送信するか否かの設定

[書式]

ip icmp unreachable send SEND [rebound=SW]

ipv6 icmp unreachable send SEND [rebound=SW]
no ip icmp unreachable send
no ipv6 icmp unreachable send

[設定値及び初期値]

SEND

[設定値]:

設定値	説明
on	送信する
off	送信しない

[初期値]:on

SW ★

[設定値]:

設定値	説明
on	受信インターフェースから送信する
off	経路に従って送信する

[初期値]:off

[説明]

経路テーブルに宛先が見つからない場合や、あるいはARPが解決できなくてIPパケットを破棄することになった場合に、同時にパケットの送信元に対して ICMP Destination Unreachable を送信するか否かを設定する。reboundオプションをonに設定した場合には、経路設定に関係なく、元となるパケットを受信したインターフェースから送信する。 ★

[6] IPsecトランスポートモードの設定で、テンプレートに対応した。

〇トランスポートモードのテンプレートの設定

[書式]

ipsec transport template ID1 ID2 [ID2 ...]
no ipsec transport ID1 [ID2 ...]

[設定値及び初期値]

ID1

[設定値]: 展開元のトランスポートID

[初期値]: -

ID2

[設定値]: 展開先のトランスポートID、または間にハイフン("-")をはさんで
トランスポートIDを範囲指定したもの

[初期値]: -

[説明]

指定したipsec transportコマンドの設定の展開先となるトランスポートIDを設定する。展開先のポリシーIDは展開先のトランスポートIDと同じ値が設定される。展開先のトランスポートIDに対して既に設定が存在する場合、展開先の設定が優先される。本コマンドによってVPN対地数まで ipsec transport コマンドの設定を展開することができる。VPN 対地数を超える範囲に展開することはできない。

2. 本バージョンで仕様変更された項目

■仕様変更

[1] モバイルインターネット機能で、以下の場合にデータ通信端末の再アタッチ処理を行うようにした。

- データ通信端末を接続／切断させたときの電波受信レベル取得で、データ通信端末から応答がないとき
- データ通信端末へのコマンド送信に失敗したとき

[2] モバイルインターネット機能で、データ通信端末のアタッチ直後の網への接続を抑制できるようにした。

○携帯端末を使用するか否かの設定

[書式]

```
mobile use INTERFACE USE [first-connect-wait-time=TIME]
```

[設定値及び初期値]

INTERFACE

[設定値]:

設定値	説明
usb1	USB1をモバイルインターネット接続に使用

[初期値]:-

USB

[設定値]:

設定値	説明
on	携帯端末を使用する
off	携帯端末を使用しない

[初期値]:off

TIME

[設定値]:

設定値	説明
0-300	携帯端末アタッチ後の発信抑制秒数

[初期値]:0

[説明]

指定のバスに接続された携帯端末をインターネット接続に使用するか否かを設定する。first-connect-wait-time オプションは、携帯端末のアタッチ後の発信抑制時間を設定し、網への接続を抑制する。mobile auto connect コマンドや、wan1 auto connect コマンド、pp always-on コマンド、wan1 always-on コマンドで on が設定されている場合の網への接続要求も、このコマンドで設定された発信抑制秒数の間は、発信が抑制される。

[3] SNMPのホスト設定コマンドで、IPアドレスの範囲やLANインターフェース名を設定できるようにした。

〇SNMPv1によるアクセスを許可するホストの設定

[書式]

snmp host HOST [RO_COMMUNITY [RW_COMMUNITY]]

no snmp host [HOST [RO_COMMUNITY [RW_COMMUNITY]]]

[設定値及び初期値]

HOST

[設定値]:

設定値	説明
IPアドレス	1個のIPアドレスまたは間にハイフン(-)をはさんだIPアドレス(範囲指定) ★
lanN	LANインターフェース名 ★
bridgeN	ブリッジインターフェース名 ★
any	すべてのホストからのアクセスを許可する
none	すべてのホストからのアクセスを禁止する

[初期値]: none

RO_COMMUNITY

[設定値]: 読み出し専用のコミュニティー名(16文字以内)

[初期値]: -

RW_COMMUNIT

[設定値]: 読み書き可能なコミュニティー名(16文字以内)

[初期値]: -

[説明]

SNMPv1 によるアクセスを許可するホストを設定する。'any'を設定した場合は任意のホストからのSNMPv1 によるアクセスを許可する。IP アドレスや lanN、bridgeN でホストを指定した場合には、同時にコミュニティー名も設定できる。 ★

RW_COMMUNITY パラメーターを省略した場合には、アクセスモードが読み書き可能であるアクセスが禁止される。RO_COMMUNITY パラメーターも省略した場合には、snmp community read-only コマンド、および snmp community read-write コマンドの設定値が用いられる。

[ノート]

HOST パラメーターに IP アドレスの範囲や lanN、bridgeN を指定できるのは N1200 の Rev.10.01.64 以降である。

〇SNMPv2cによるアクセスを許可するホストの設定

[書式]

snmpv2c host HOST [RO_COMMUNITY [RW_COMMUNITY]]

no snmpv2c host [HOST [RO_COMMUNITY [RW_COMMUNITY]]]

[設定値及び初期値]

HOST

[設定値]:

設定値	説明

IPアドレス	1個のIPアドレスまたは間にハイフン(-)をはさんだIPアドレス(範囲指定) ★
lanN	LANインターフェース名 ★
bridgeN	ブリッジインターフェース名 ★
any	すべてのホストからのアクセスを許可する
none	すべてのホストからのアクセスを禁止する

[初期値]: none

RO_COMMUNITY

[設定値]: 読み出し専用のコミュニティー名(16文字以内)

[初期値]: -

RW_COMMUNITY

[設定値]: 読み書き可能なコミュニティー名(16文字以内)

[初期値]: -

[説明]

SNMPv2c によるアクセスを許可するホストを設定する。'any'を設定した場合は任意のホストからのSNMPv2c によるアクセスを許可する。IP アドレスや lanN、bridgeN でホストを指定した場合には、同時にコミュニティー名も設定できる。 ★

RW_COMMUNITY パラメーターを省略した場合には、アクセスモードが読み書き可能であるアクセスが禁止される。RO_COMMUNITY パラメーターも省略した場合には、snmpv2c community read-only コマンド、および snmpv2c community read-write コマンドの設定値が用いられる。

[ノート]

HOST パラメーターに IP アドレスの範囲や lanN、bridgeN を指定できるのは N1200 の Rev.10.01.64 以降である。

○SNMPv3によるアクセスを許可するホストの設定

[書式]

```
snmpv3 host HOST user USER_ID ...
no snmpv3 host HOST [user USER_ID ...]
```

[設定値及び初期値]

HOST

[設定値]:

設定値	説明
IPアドレス	1個のIPアドレスまたは間にハイフン(-)をはさんだIPアドレス(範囲指定) ★
lanN	LANインターフェース名 ★
bridgeN	ブリッジインターフェース名 ★
any	すべてのホストからのアクセスを許可する
none	すべてのホストからのアクセスを禁止する

[初期値]: none

USER_ID: ユーザー番号

[設定値]: 1個の数字、または間にハイフン(-)をはさんだ数字(範囲指定)、およびこれらを任意に並べたもの(128個以内)

[初期値]:-

[説明]

SNMPv3 によるアクセスを許可するホストを設定する。'any'を設定した場合は任意のホストからの SNMPv3 によるアクセスを許可する。なお、アクセスのあったホストが HOST パラメーターに合致していても、USER_ID パラメーターで指定したユーザーに合致しなければアクセスはできない。

[ノート]

HOST パラメーターに IP アドレスの範囲や lanN、bridgeN を指定できるのは N1200 の Rev.10.01.64 以降である。

[4] 以下に示すIPv4の経路変更が発生した場合は、経路情報の更新内容を直ちにルーティング処理に反映するようにした。

- IPv4静的経路の設定変更
- PP/TUNNELインターフェースのアップダウンによるIPv4経路変更
- ICMPリダイレクト受信によるIPv4経路変更

なお、上記以外の場合には、経路情報の更新内容のルーティング処理への反映は従来通り1秒おきである。

[5] IKEv2で、リクエストメッセージの送信をメッセージIDで管理できるようにした。

〇IKEのメッセージID管理の設定

[書式]

```
ipsec ike message-id-control GATEWAY_ID SWITCH
no ipsec ike message-id-control GATEWAY_ID [SWITCH]
```

[設定値及び初期値]

GATEWAY_ID

[設定値]：セキュリティー・ゲートウェイの識別子

[初期値]：-

SWITCH

[設定値]：

設定値	説明
on	リクエストメッセージの送信をメッセージIDで管理する
off	リクエストメッセージの送信をメッセージIDで管理しない

[初期値]：off

[説明]

自機から IKEv2 のリクエストメッセージを送信するときのメッセージ ID 管理方法を設定する。on に設定しているとき、同じ IKE SA を使用して送信済みの IKE メッセージに対する全てのレスポンスメッセージを受信していない場合、新しい IKE メッセージは送信しない。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

[6] IKEv2で鍵交換を始動するとき、SAを構築するための各折衝パラメーターを、特定のコマンド設定値に限定して提案できるようにした。

〇折衝パラメーターを制限するか否かの設定

[書式]

```
ipsec ike proposal-limitation GATEWAY_ID SWITCH
no ipsec ike proposal-limitation GATEWAY_ID
```

[設定値及び初期値]

GATEWAY_ID

[設定値]：セキュリティー・ゲートウェイの識別子

[初期値]：-

SWITCH

[設定値]：

設定値	説明
on	折衝パラメーターを制限する
off	折衝パラメーターを制限しない

[初期値]：off

[説明]

IKEv2 で鍵交換を始動するときに、SA を構築するための各折衝パラメーターを、特定のコマンド設定値に限定して提案するか否かを設定する。このコマンドの設定が off のときは、サポート可能な折衝パラメーター全てを提案する。このコマンドが適用されるパラメーターと対応するコマンドは以下の通りである。

パラメーター	コマンド
暗号アルゴリズム	ipsec ike encryption
グループ	ipsec ike group
ハッシュアルゴリズム	ipsec ike hash
暗号・認証アルゴリズム	ipsec sa policy ※CHILD SA 作成時

[ノート]

本コマンドはIKEv1としての動作には影響を与えない。

[7] IKEv2で、INVALID_IKE_SPI Notifyメッセージを受信したとき、該当するIKE SAを削除するようにした。

[8] show exec listコマンドで、外部メモリに保存されている実行形式ファームウェアファイルの情報を表示するようにした。

〇ファームウェアファイルの一覧の表示

[書式]

show exec list

less exec list

[説明]

内蔵FlashROMおよび外部メモリに保存されている実行形式ファームウェアファイルの情報を表示する。起動中のファームウェアファイルには アスタリスク("*")印が表示される。ファームウェアファイルが保存されている外部メモリが接続されている場合には、そのファームウェアファイルの情報も表示される。 ★

[9] show status tunnelコマンドで、IKEv2のIKEキープアライブの状態を表示するようにした。

[10] bridge memberコマンドでトンネルインターフェースの範囲を指定可能にした。

○ブリッジインターフェースに収容するインターフェースを設定する

[書式]

bridge member BRIDGE_INTERFACE INTERFACE INTERFACE [...]

no bridge member BRIDGE_INTERFACE [INTERFACE ...]

[設定値及び初期値]

BRIDGE_INTERFACE

[設定値]: ブリッジインターフェース名

[初期値]: -

INTERFACE

[設定値]:

設定値	説明
lanN	LANインターフェース名
lanN.M	LAN分割インターフェース名
vlanN	VLANインターフェース名
tunnelN	TUNNELインターフェース名
tunnelN-tunnelM	TUNNELインターフェースの範囲　★

[初期値]: -

[説明]

仮想インターフェースであるブリッジインターフェースに収容するインターフェースを指定する。収容したインターフェース間でブリッジ動作が行われる。トンネルインターフェースを収容した場合、L2TPv3 トンネルが確立しているトンネルインターフェースでのみブリッジ動作が行われる。

[ノート]

・収容する LAN インターフェースについて

収容した実インターフェースに IPv4, IPv6 アドレスを付与してはならない。

収容した実インターフェースの IPv6 リンクローカルアドレスは削除される。

収容する LAN インターフェースの MTU はすべて同一の値でなければならない。

いずれかのブリッジインターフェースに収容した実インターフェースは、他のブリッジインターフェースに収容することはできない。

収容するインターフェースがスイッチングハブを持つインターフェースである場合、スイッチングハブのポート間で完結する通信は本機能によるブリッジ動作ではなく、スイッチングハブ LSI 内部で処理される。

VLAN インターフェース名を指定できるのは LAN 分割機能の拡張機能に対応した機種のみである。

・収容するトンネルインターフェースについて

収容するトンネルインターフェースの MTU は無効となり、トンネルインターフェースでフラグメントは行われず、カプセル化されたパケットの送信インターフェースの MTU に従ってフラグメントが発生する。

いずれかのブリッジインターフェースに収容したインターフェースは、他のブリッジインターフェースに収容することはできない。

収容するインターフェースとしてトンネルインターフェースを設定できるのはL2TPv3機能が実装されているモデルのみである。

・ブリッジインターフェースについ

ブリッジインターフェースのリンク状態は収容した LAN インターフェースまたはトンネルインターフェースのリンク状態に応じて変化する。

いずれかの収容したインターフェースがアップ状態だった場合、ブリッジインターフェースはアップ状態になる。

すべてのインターフェースがダウン状態だった場合、ブリッジインターフェースもダウン状態になる。

ブリッジインターフェースの MAC アドレスは、収容した LAN インターフェースのうち、インターフェース番号がもっとも小さいインターフェースのアドレ スを使用する。

[11] トンネルテンプレートで、L2TP/IPsecとL2TPv3に関連したコマンドに対応した。

〇トンネルテンプレートの設定

[書式]

tunnel template TUNNEL [TUNNEL ...]

no tunnel template

[設定値及び初期値]

TUNNEL

[設定値] : トンネルインターフェース番号、または間にハイフン(-)をはさんでトンネルインターフェース番号を範囲指定したもの

[初期値] : -

[説明]

tunnel select コマンドにて選択されたトンネルインターフェースを展開元として、当該インターフェースに設定されているコマンドの展開先となるトンネルインターフェースを設定する。

展開元のトンネルインターフェースに設定することで、展開先のトンネルインターフェースにも適用されるコマンドは以下のとおりである。なお、末尾に(*1)または(*2)が付加されているコマンドについては[ノート]を参照のこと。

- ipsec tunnel
- ipsec sa policy
- ipsec ikeで始まるコマンドのうち、パラメーターにセキュリティ・ゲートウェイの識別子をとるもの
- ipsec auto refresh (引数にセキュリティ・ゲートウェイの識別子を指定する場合)
- tunnel encapsulation (*1)
- tunnel ngn arrive permit (*1)
- tunnel ngn bandwidth (*1)
- tunnel ngn disconnect time (*1)
- tunnel ngn radius auth (*1)
- l2tpで始まるコマンド (*2) ★
- tunnel enable

上記コマンドのうち以下のコマンドについては、特定のパラメーターの値が展開元のトンネルインターフェース番号に一致する場合のみ、コマンドが展開される。

その場合、当該パラメーターの値は展開先のトンネルインターフェース番号に置換される。

コマンド	パラメーター
ipsec tunnel	ポリシーID
ipsec sa policy	ポリシーID
ipsec ikeで始まるコマンド	セキュリティ・ゲートウェイの識別子
ipsec auto refresh	セキュリティ・ゲートウェイの識別子
tunnel enable	トンネルインターフェース番号

ipsec sa policyコマンドでは、セキュリティ・ゲートウェイの識別子が展開先のトンネルインターフェース番号に置換される。

ipsec ike remote nameコマンドでは、相手側セキュリティ・ゲートウェイの名前の末尾に展開先のトンネルインターフェース番号が付加される。

展開元のトンネルインターフェースに設定されているコマンドと同じコマンドが、展開先のトンネルインターフェースに既に設定されている場合、展開先のトンネルインターフェースに設定されているコマンドが優先される。

コマンド展開後の、ルーターの動作時に参照される設定はshow config tunnelコマンドにexpandキーワードを指定することで確認できる。

[ノート]

トンネルインターフェースが選択されている時にのみ使用できる。

展開対象となるコマンドのうち、末尾に(*1)が付加されているコマンドについては、以下の機種リビジョンで対応している。

機種	リビジョン
N1200	Rev.10.01.43以降

展開対象となるコマンドのうち、末尾に(*2)が付加されているコマンドについては、以下の機種、リビジョンで対応している。

機種	リビジョン
N1200	Rev.10.01.64以降

[12] pingコマンド、ping6コマンドの送信間隔の上限値を3600秒に変更した。

〇pingの実行

[書式]

ping [-s DATALEN] [-c COUNT] [-sa IP_ADDRESS] [-w WAIT] HOST

[設定値及び初期値]

DATALEN

[設定値] : データ長

- Rev.10.01.39以降 ... (1..65535 byte)
- 上記以外 ... (64..65535 byte)

[初期値] : 64

COUNT

[設定値] : 実行回数(1..21474836)

[初期値] : Ctrl+cキーが入力されるまで繰り返す

IP_ADDRESS

[設定値] : 始点IPアドレス(xxx.xxx.xxx.xxx(xxxは十進数))

[初期値] : ルーターのインターフェースに付与されたアドレスの中から選択する

WAIT

[設定値] : パケット送信間隔秒数(0.1..3600.0) ★

[初期値] : 1.0

host

[設定値]：

pingをかけるホストのIPアドレス(xxx.xxx.xxx.xxx(xxxは十進数))

pingをかけるホストの名称

[初期値]：-

[説明]

ICMP Echo を指定したホストに送出し、ICMP Echo Reply が送られてくるのを待つ。送られてきたら、その旨表示する。コマンドが終了すると簡単な統計情報を表示する。COUNT パラメーターを省略すると、Ctrl+c キーを入力するまで実行を継続する。-w オプションを指定した時には、次のパケットを送信するまでの間に相手からの返事を確認できなかった時にはその旨のメッセージを表示する。-w オプションを指定していない時には、パケットが受信できなくても何もメッセージを表示しない。

〇ping6 の実行

[書式]

ping6 [-s DATALEN] [-c COUNT] [-sa IPV6_ADDRESS] [-w WAIT] DESTINATION

ping6 [-s DATALEN] [-c COUNT] [-sa IPV6_ADDRESS] [-w WAIT] DESTINATION%SCOPE_ID

ping6 [-s DATALEN] [-c COUNT] [-sa IPV6_ADDRESS] [-w WAIT] DESTINATION INTERFACE

ping6 [-s DATALEN] [-c COUNT] [-sa IPV6_ADDRESS] [-w WAIT] DESTINATION pp PEER_NUM

ping6 [-s DATALEN] [-c COUNT] [-sa IPV6_ADDRESS] [-w WAIT] DESTINATION tunnel TUNNEL_NUM

ping6 DESTINATION [COUNT]

ping6 DESTINATION%SCOPE_ID [COUNT]

ping6 DESTINATION INTERFACE [COUNT]

ping6 DESTINATION pp PEER_NUM [COUNT]

ping6 DESTINATION tunnel TUNNEL_NUM [COUNT]

[設定値及び初期値]

DATALEN

[設定値]：データ長(1..65535byte)

[初期値]：64

COUNT

[設定値]：実行回数(1..21474836)

[初期値]：Ctrl+cキーが入力されるまで繰り返す

IPV6_ADDRESS

[設定値]：始点IPv6アドレス

[初期値]：ルーターのインターフェースに付与されたアドレスの中から選択する

WAIT

[設定値]：パケット送信間隔秒数(0.1..3600.0) ★

[初期値]：1.0

DESTINATION

[設定値]：送信する宛先のIPv6アドレス、または名前

[初期値]：-

SCOPE_ID

[設定値]：スコープ識別子

[初期値]：-

INTERFACE

[設定値]：LANインターフェース名

[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]：-

[説明]

指定した宛先に対して ICMPv6 Echo Request を送信する。スコープ識別子は、show ipv6 address コマンドで表示できる。第1～第5書式は、Rev.10.01.39 以降のリビジョンで指定できる。それ以外のリビジョンでは、第6～第10書式で指定する。COUNT パラメーターを省略すると、Ctrl+c キーを入力するまで実行を継続する。-w オプションを指定した時には、次のパケットを送信するまでの間に相手からの返事を確認できなかった時にはその旨のメッセージを表示する。-w オプションを指定していない時には、パケットが受信できなくても何もメッセージを表示しない。

[ノート]

-sオプション、-cオプション、-saオプション、-wオプションはRev.10.01.39以降で使用可能。

[13] 帯域制御で、速度計算にプリアンブル、SFD(Start Frame Delimiter)、IFG(Inter Frame Gap)を含められるようにした。

〇キューイングアルゴリズムタイプの選択

[書式]

queue INTERFACE type TYPE [shaping-level=LEVEL] ★

queue pp type TYPE

no queue interface type [TYPE]

no queue pp type [TYPE]

[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

[初期値]：-

TYPE

[設定値]：

設定値	説明
fifo	First In, First Out形式のキューイング
priority	優先制御キューイング
shaping	帯域制御

[初期値]：fifo

LEVEL ★

[設定値]：帯域速度の計算を行うレイヤー

設定値	説明
1	レイヤー1
2	レイヤー2

［初期値］: 2

［説明］

指定したインターフェースに対して、キューイングアルゴリズムタイプを選択する。fifo は最も基本的なキューである。fifo の場合、パケットは必ず先にルーターに到着したものから送信される。パケットの順番が入れ替わることは無い。fifo キューにたまったパケットの数が queue INTERFACE length コマンドで指定した値を越えた場合、キューの最後尾、つまり最後に到着したパケットが破棄される。priority は優先制御を行う。queue class filter コマンドおよび queue INTERFACE class filter list コマンドでパケットをクラス分けし、送信待ちのパケットの中から最も優先順位の高いクラスのパケットを送信する。shaping は LAN インターフェースに対する帯域制御を行う。LAN インターフェースにだけ設定できる。shaping-level オプションは TYPE パラメーターに priority および shaping を指定しているときのみ指定可能。 ★

shaping-level に 1 を設定した場合、帯域速度の計算をプリアンブル、SFD(Start Frame Delimiter)、IFG(Inter Frame Gap)を含んだフレームサイズで行う。 ★

[14] SNMPv2c、SNMPv3でINFORMリクエストを送出後、既定の再送回数以内にレスポンスを受信できなかったときにログを出力するようにした。

[15] speed wan1コマンドで指定可能なインターフェース速度の最大値を1000Mに変更した。

[16] show status bri1コマンドでレイヤ1の起動状態を表示するようにした。

[17] pp bindコマンドで以下に対応した。

- パラメーターを64個以上指定できるようにした。
- 2つ目以降のインターフェースを範囲指定して設定したとき、show configコマンドでインターフェースが範囲で出力されるようにした。

[18] 状態メール通知機能やGUIの[レポートの作成]で以下のコマンドの実行結果を出力するようにした。

- show status bridge1
- show status l2tp

[19] GUIの[初期設定ウィザード]で、モバイルインターネット機能の[WANの設定 2/6]の「契約キャリア/プラン」の項目を、最新の対応状況に更新した。

3. 本バージョンで修正された項目

■バグ修正

[1] OpenSSL の以下の脆弱性対応を行った。

- CVE-2014-3570 (JPCERT/CC JVNVU#98974537)
- CVE-2014-8275 (JPCERT/CC JVNVU#98974537)
- CVE-2015-0287 (JPCERT/CC JVNVU#95877131)
- CVE-2015-0292 (JPCERT/CC JVNVU#95877131)

[2] L2TPv3 で、以下の条件を満たす場合にリブートすることがあるバグを修正した。

- L2TPv3 トンネルの先にある宛先に対する静的経路が設定されている。
- 上記経路情報によってルーティングされるパケットが発生し、かつ、宛先となるホストが存在しない。

[3] L2TP/IPsec で、以下の条件においてリブートすることがあるバグを修正した。
- クライアントの L2TP 用仮想インターフェースの IP アドレスとして、クライアントの実インターフェースの IP アドレスと同じものを設定して接続した場合
- クライアントの L2TP 用仮想インターフェースの IP アドレスとして、クライアントの実インターフェースの IP アドレスと同じものを接続時にルーターが割り当てた場合

[4] IKEv2 で、証明書失効リスト(CRL)ファイルを利用して PKI 証明書による認証を行う場合、接続するそれぞれのルーターから同時に鍵交換を始動すると接続後にリブートすることがあるバグを修正した。

[5] GUI の[パケットフィルター]-[動的フィルター]で設定できないプロトコルを ip dynamic filter コマンドで設定し、GUI の[パケットフィルター]-[動的フィルター]で当該フィルターを選択して設定を変更しようとするとリブートするバグを修正した。このようなフィルターは GUI では変更できないため、変更しようとするとエラー表示される。

[6] PP anonymous で複数の接続を受けた場合にリブートする可能性を排除した。

[7] pp bind コマンドで不正なパラメーターを入力したときに、入力エラーにならなかったり、リブートもしくはハングアップしたりすることがあるバグを修正した。

[8] NAT で、到達できない IP アドレスへの静的 IP マスカレードが設定され、そのエントリに従って処理されるパケットが発生した場合にリブートすることがあるバグを修正した。Rev.10.01.53 で発生する。

[9] 起動時にハングアップする可能性を排除した。

[10] dhcp scope option コマンドが設定されている状態でルーターを起動したとき、メモリリークするバグを修正した。Rev.10.01.53 で発生する。

[11] TFTP で FlashROM 上に保存されているファイルを取得しているとき、または FlashROM 上にファイルを転送しているときに通信が切断されると、以下の問題が発生するバグを修正した。
- メモリリークが発生する
- config ファイルを取得しているときに切断されると、それ以降、その config ファイルが認識されなくなる

[12] LAN 分割インターフェースで、show status lan コマンドを実行したり、SNMP で情報を取得したとき、送受信のオクテット数が 1 パケットにつき 4 オクテット多いバグを修正した。

[13] L2TPv3 で、ブリッジのラーニングテーブルに不正なエントリが登録されてしまうことがあるバグを修正した。本バグが発生した場合、L2TPv3 トンネル上でフレームのループが発生し、高負荷によってパケットの送受信が行えなくなる。

[14] L2TPv3 で、Ethernet II 以外の L2 フレームが正しくトンネリングされないバグを修正した。

[15] L2TPv3 で、ブリッジメンバーに含まれるインターフェースとブリッジメンバーに含まれないインターフェース間で通信できないバグを修正した。ファストパスが有効な場合のみで発生する。

[16] L2TPv3 で、ブリッジメンバーに含まれる物理 LAN インターフェースにおいてパケットの受信カウンターが正しくカウントされないことがあるバグを修正した。

[17] L2TPv3 で、複数のトンネルが確立した場合にトンネル間の通信が行えないことがあるバグを修正した。ファストパスが有効な場合のみで発生する。

[18] L2TP/IPsec および L2TPv3 で、トンネルインターフェースの MTU よりも大きなパケットがファストパスで処理されないバグを修正した。

[19] L2TP/IPsec および L2TPv3 で、ip/ipv6 tunnel tcp mss limit コマンドによる TCP セッションの MSS 調整が機能しないバグを修正した。

[20] L2TP/IPsec で、disconnect コマンドによって接続している端末を切断した場合、次に当該トンネルで受けた接続において接続後の鍵交換に失敗して切断されることがあるバグを修正した。

[21] L2TP/IPsec で、L2TP トンネル認証エラー等で接続が確立しなかった場合に、show status pp コマンドで不正な情報が出力されるバグを修正した。Rev.10.01.53 で発生する。

[22] L2TP/IPsec で、1 つのトンネルに対し 2 重接続されてしまうことがあるバグを修正した。

[23] L2TP/IPsec で、以下の条件のどちらかに合致するとそれ以降当該トンネルで接続を受けることができなくなるバグを修正した。

- ipsec ike retry コマンドの max_session(デフォルト値:3)で指定された数以上の接続を同時に受け、かつ接続相手の IP アドレスが同じである場合
  ("[IKE] initiator's cookie is refused (too many requests)"のログが DEBUG レベルの SYSLOG に出力される)
- 接続を受けたときにクッキー情報の生成に失敗した場合

[24] L2TP/IPsec で、AVP に関するログの誤記を修正した。

[25] Xauth 認証機能を使った IPsec 接続で内部 IP アドレスを付与したときにできる経路が、トンネルがダウンしたときに消えないことがあるバグを修正した。

[26] IPsec で、以下の条件をすべて満たす場合に IPsec トンネルを経由するノーマルパスの通信が行えないことがあるバグを修正した。

- LAN インターフェースまたは WAN インターフェースで DHCP によって IP アドレスを取得する設定がされている
- 上記インターフェースをゲートウェイとして IPsec が確立する
- トンネルインターフェースで ipsec ike local address コマンドが設定されていない

[27] RIPng で、他のプロトコルから得られた経路を削除できない場合があるバグを修正した。

[28] モバイルインターネット機能で、mobile dial number コマンドが設定されているとき PP インターフェース接続ができなくなるバグを修正した。

[対象端末]
- docomo　　L-03D, L-02C
- EMOBILE　　GL03D, GD01, D41HW, D33HW, D32HW, D31HW
- IIJ Mobile 510FU
- NTT コム　　WM320

[29] モバイルインターネット機能の WAN インターフェース接続で、以下のデータ通信端末を使用しているとき、網へ接続できなくなることがあるバグを修正した。
- docomo L-02C
- NTT コム WM320

[30] モバイルインターネット機能で、網に接続した状態で restart コマンドなどによってルーターの再起動を行うと、ごく稀に USIM カードが故障することがあるバグを修正した。

[31] ISDN の切断タイマーで切断されたとき、STATUS LED が点灯してしまうバグを修正した。以下のコマンドが対象となる。
- isdn fast disconnect time
- isdn forced disconnect time

[32] 外部メモリ起動の LED の動作で、以下のバグ修正を行った。
- 起動完了時に、ALARM LED と STATUS LED が点滅する。
- 起動失敗時に、ALARM LED と DOWNLOAD LED が点滅しないことがある。

[33] VRRP で、他の VRRP 関係のコマンドを設定したあと最後に ip INTERFACE vrrp コマンドを設定したとき、マスターがシャットダウンすべき条件下でもシャットダウンしないバグを修正した。

[34] ip INTERFACE vrrp コマンドで、IP_ADDRESS パラメーターに IPv6 アドレスを設定できてしまうバグを修正した。

[35] ip INTERFACE vrrp shutdown trigger コマンドで、NETWORK パラメーターに IPv6 のネットワークおよびアドレスを設定できてしまうバグを修正した。

[36] clear status tunnel コマンドを実行してもトンネルインターフェースの IPv6 の送受信パケット数やオクテット数がクリアされないことがあるバグを修正した。Rev.10.01.53 で発生する。

[37] pp bind コマンドで、TUNNEL インターフェースの範囲指定として誤ったキーワードを入力したとき、既に設定済みの pp bind コマンドの設定がクリアされてしまうバグを修正した。Rev.10.01.53 で発生する。

[38] ipsec log illegal-spi コマンドに on が設定されているとき、当該ログは 1 秒あたり最大 10 種類まで出力される仕様であるが、実際には 9 種類までしか出力されないバグを修正した。

[39] execute at-command コマンドを実行すると、それ以降、AT コマンドの送受信ができなくなることがあるバグを修正した。

[40] ip tos supersede コマンドで、パラメーターのフィルター番号に 256 より大きい番号を入力すると

違う番号で設定されるバグを修正した。

[41] ipv6 ospf area network コマンドを設定した後に以下のコマンドを実行しても、変更した設定を保存するか否かを問い合わせるメッセージが表示されないことがあるバグを修正した。

- exit
- quit
- restart

[42] 以下のコマンドの実行結果の誤記を修正した。

- show status usbhost
- show status external-memory
- show status sd

[43] GUI の[統計情報]-[トラフィック統計]で、PP インターフェースの PPTP と L2TP/IPsec のトラフィック情報が表示されないバグを修正した。

[44] GUI の以下の項目でネットマスクの入力が省略できないバグを修正した。

- [IPsec]-[XAUTH のユーザーの設定]-[新しいユーザーグループの追加]の割り当てる IP アドレスの範囲
- [IPsec]-[XAUTH のユーザーの設定]-[新しいユーザーの追加]の IP アドレスの範囲

■更新履歴

Aug. 2015, Rev.10.01.64 リリース