FutureNet VXR-x86
ユーザーズガイド

Ver.8.2.0 対応版

CENTURY SYSTEMS

目次

はじめに

◆ ご注意

1 本装置の故障、誤動作、不具合、あるいは停電などの外部要因によって、通信の機会を逸したために生じた損害などの純粋経済損失につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承ください。

2 通信情報が漏洩した事による経済的、精神的損害につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承ください。

3 本書の内容の一部または全部を無断で転載、複写することを禁じます。

4 本書およびソフトウェア、ハードウェア、外観の内容について、将来予告なしに変更することがあります。

5 本書の内容については万全を期しておりますが、万一ご不審な点や誤り、記載漏れなどお気づきの点がありましたらご連絡ください。

◆ 商標の表示

□ 「FutureNet」はセンチュリー・システムズ株式会社の登録商標です。

□ その他の記載されている商品名、会社名は、各社の商標または登録商標です。

第1章

本装置の概要

Ⅰ．本装置の特長

FutureNet VXRの「製品概要」、「製品の特徴」、「仕様」等については、弊社のWebサイトを参照してください。

◆ FutureNet VXR-x86
http://www.centurysys.co.jp/products/router/vxrx86.html

Ⅱ．動作環境

各種クラウドサービスや独自に構築するプライベートクラウド環境に VXR-x86 を追加することができます。

■ VXR-x86 の動作環境

CPU	メモリ	ディスク容量	イーサーネットインタフェース
Intel互換（推奨）	128Mバイト以上 (512Mバイト以上推奨)	1Gバイト以上	1つ以上

■ホスト OS の動作環境

CPU	OS	仮想化ソフトウェア
Intel CPU (Intel VT対応要)	CentOS6.4(64bit)	KVM+QEMU kernel version : 2.6.32-431.29.2.el6.x86_64 qemu version : qemu-kvm-0.12.1.2
	Ubuntu14.04(64bit)	KVM+qemu kernel version : 3.13.0-32-generic qemu version : qemu-kvm-2.0.0

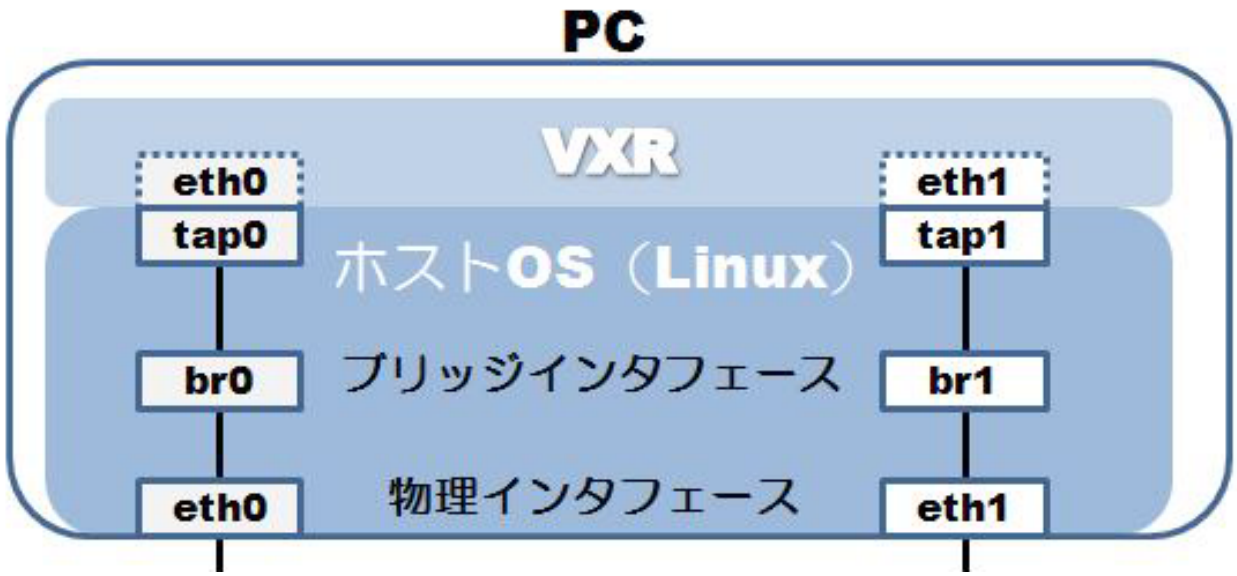
III．VXR-x86 のセットアップ

VXR-x86 をインストールした物理 PC を、ルータとして利用する場合の設定例を示します。

■インタフェース

インタフェース名	説明
eth<X>	外部と通信するための物理インタフェースです。
tap<X>	仮装NIC（Network Interface Card）です。ホストOSとVXR-x86間での通信に使用します。
br<X>	ホストOSの物理インタフェース（eth）とVXR-x86のインタフェース（実際にはtap）をブリッジ接続するインタフェースです。

■構成図



■ブリッジインタフェースの作成

ホスト OS 上で、ブリッジインタフェースを作成します。

```
#ifconfig eth0 0
#ifconfig eth1 0
#brctl addbr br0
#brctl addbr br1
#brctl addif br0 eth0
#brctl addif br1 eth1
#ifconfig br0 0
#ifconfig br1 0
```

III．VXR-x86 のセットアップ

■ qemu-ifup スクリプトの作成

・ブリッジインタフェースにゲスト OS の仮想イーサネットインタフェース(tapX)を参加させるためのスクリプトを作成します(/etc/qemu-ifup，/etc/qemu-ifup-br1)。

・このスクリプトは qemu-kvm 起動時に使用します（このスクリプトには実行権を付与するようにして下さい)。

・なお、このスクリプトの作成については、下記 URL を参考に作成して下さい。
https://wiki.archlinux.org/index.php/QEMU

III．VXR-x86 のセットアップ

■ VXR-x86 の起動

・VXR-x86 の起動コマンド例を示します。

```
#qemu-kvm -enable-kvm -m 1024 -smp 2 -cpu host -drive file=VXR.img,if=virtio -net nic,macaddr=00:80:
6d:ff:ff:10,model=virtio -net tap,ifname=tap0,script=/etc/qemu-ifup -net nic,vlan=1,macaddr=00:80:
6d:ff:ff:11,model=virtio -net tap,ifname=tap1,vlan=1,script=/etc/qemu-ifup-br1,vhost=on -nographic -
monitor pty -serial pty -name vxr-x86
```

・指定可能なオプションの例を示します。

オプション	説明
-m メモリ	割り当てるメモリ量を指定します。(単位はMバイト。512Mバイト以上推奨)
-smp CPU	割り当てるCPU数を指定します。
-drive file=イメージファイル	VXR-x86のイメージファイルを指定します。
vlan=X	ネットワークの識別用に利用します。 なお省略した場合は「vlan=0」となります。
macaddr=XX:XX:XX:XX:XX:XX	MACアドレスを指定します。
model=TYPE	virtio/e1000/rtl8139のいづれかを指定します（※virtio推奨）。 なお、fast-forwardingはe1000/virtio指定時のみ動作します。
-serial xxx	ptyを指定すると、minicomなどのターミナルソフトから接続することができます。 なお-serialオプションを指定しない、または-serial mon:stdioを指定すると、起動したターミナルがシリアルの代わりになります。
-name	ゲストOSの定義名を指定します。

・起動コマンド実行後、以下のような起動メッセージが出力されます。

```
char device redirected to /dev/pts/12
Executing /etc/qemu-ifup
Bringing up tap0 for bridged mode…
Adding tap0 to br0…
Executing /etc/qemu-ifup-br1
Bringing up tap1 for bridged mode…
Adding tap1 to br1…
char device redirected to /dev/pts/14
```

■ VXR-x86 へのアクセス

・VXR-x86 は初期状態で各インタフェースに IP アドレスは設定されていません。そのため、初期セットアップにはシリアルポートを使用する必要があります。

・接続する場合は、VXR-x86 起動時に出力される起動メッセージの最後の「/dev/pts/X」に minicom を使用して接続します。

・上記起動メッセージの場合、/dev/pts/14 を指定します。

```
#minicom -p /dev/pts/14
```

■ VXR-x86 へのログイン

・ログイン ID およびパスワードに「admin」を入力し、ログインします。

```
Century Systems VXR Series
vxr-x86 login: admin
Password: admin
```

第2章

Licenseの概要

第２章 License の概要

Ⅰ．License の概要

◆ License の概要

VXR には、大きく分けて２種類の License があります。

・Trial License
　試用版 License です。
　本ライセンスは、期限付きライセンスです。Trial License の発行は、原則として、１ユーザに１回限りです。

・Product License
　製品版 License です。
　Product License に、Option License を追加することで、期間延長や機能追加などを行うことが出来ます。

※各 License の詳細については、弊社にお問い合わせください。

■ No License

初期状態（Trial License ／ Product License のいずれの License もない状態）で、VXR を起動した場合、license 登録用のモードで起動します。
ethernet 0 のみ使用可能です。configuration mode への移行や、設定の保存 / 復帰は出来ません。
利用可能な機能（コマンド）は、下記のとおりです。

・No License で利用可能な機能（コマンド）

install license (input|file)	License をインストールします。
show product	製品情報を表示します。
show license	ライセンス情報を表示します。
show interface ethernet 0	インタフェース（ethernet 0）情報を表示します。
show ip default-gateway	デフォルトゲートウェイを表示します。
show clock	現在時刻を表示します。
interface ethernet 0 ip address	ethernet 0 に IP アドレスを付与します。
ip default-gateway	デフォルトゲートウェイを設定します。
clock set	現在時刻を設定します。
restart	システムを再起動します。
shutdown	システムを停止します。

Ⅱ . License の登録

◆ License の登録

License は、CLI より、コピー＆ペースト、または License ファイルのインポートによって登録を行います。
License 登録の際は、日付と時刻が正しいことを確認してください。

■日付と時刻の確認

・日付と時刻が正しいことを確認します（2015 年 6 月 19 日 12 時 31 分 41 秒の表示例です）。

```
vxr-x86#show clock
Fri Jun 19 12:31:41 JST 2015
```

・日時が大幅に異なる場合は、現在時刻を設定します（2015 年 6 月 30 日 11 時 00 分 00 秒に設定する例です）。

```
vxr-x86#clock set 11:00:00 30 6 2015
```

■ License の確認

・初期状態で、show license を実行すると、次のようなメッセージが表示されます。

```
vxr-x86#show license
% Valid license not found. Please install license key.
```

・License がインストールされている場合は、License 情報が表示されます（使用する License によって、表示が異なります）。

```
vxr-x86#show license
[License information]
Type             : Trial License
ID               : VVVV-WWWW-XXXX-YYYY-ZZZZ
Issued           : 20150619
Issuer           : Century Systems Co., Ltd.
Term of validity : 30 days
Licensed to Trial Test License
```

■ License の登録

・コピー＆ペーストで、License をインストールします。

```
vxr-x86#install license input
Escape character is ';'.
Enter the license key:                              ライセンスキー（↓）をコピー＆ペーストします。
U2FsdGVkX1/2Hb6rPOddiMlYZi/eZuYxib9m8OPj/hB+mHfPMLArDNHqVWzISCDG
RwWp44/Hwfwj85idOMEEOaoJOSKC3EP7wdNItsgMZ1FZxcUPA3lk+OpN5v2bsTbr
・・・・・・・・・・・・・・・・省略・・・・・・・・・・・・・・・・
bqypCutjGzS+lT+a/XwMDmp5noICbP2cnCa5mY3PiIOAJNpn/GWdJUxUswU2/eDu
7RbGScZ5a5NbCUph/JXONw==;                          ←セミコロン（;）を入力します。
License is correct. Proceed with restart? [y/n]: y  ←システム再起動の可否（y/n）を選択します。
% Install license succeed, and restarting...
```

・License file をインポートする場合は、インタフェース、デフォルトゲートウェイの設定が必要になります。

```
vxr-x86#interface ethernet 0 ip address 192.168.0.1/24    ←インタフェースの設定をします。
vxr-x86#ip default-gateway 192.168.0.254                   ←デフォルトゲートウェイを設定します。
vxr-x86#install license file ssh://user@A.B.C.D/FILENAME（または、ftp://A.B.C.D/FILENAME）
```

III. License の削除

◆ License の削除

License を他のターゲットに移動する等の理由で、License を削除する場合は、CLI より削除を行います。

■ License のアンインストール

・以下は、Product License をアンインストールする例です。

```
vxr-x86#uninstall license
License will be removed, OK? [y/n]: y          ←y/n(yes/no)を選択します。
% License removed.
Restart or shutdown? [(r)estart/(s)hutdown]: r←再起動(r)/停止(s)を選択します。
Restarting ...
```

・Trial License のアンインストールは出来ません。

```
vxr-x86#uninstall slicense
% Trial license cannot be removed.
```

Ⅳ. License のアップグレード

◆ License のアップグレード

License のアップグレードは、CLI より、コピー＆ペースト、または License ファイルのインポートによって行います。

■ License のアップグレード

・コピー＆ペーストで、License のアップグレードを行います。

```
vxr-x86#install license input
Escape character is ';'.
Enter the license key:                                  ライセンスキー（↓）をコピー＆ペーストします。
U2FsdGVkX1/2Hb6rPOddiMlYZi/eZuYxib9m8OPj/hB+mHfPMLArDNHqVWzISCDG
RwWp44/Hwfwj85idOMEEOaoJOSKC3EP7wdNItsgMZ1FZxcUPA3lk+OpN5v2bsTbr
・・・・・・・・・・・・・・・・省略・・・・・・・・・・・・・・・・
bqypCutjGzS+lT+a/XwMDmp5noICbP2cnCa5mY3PiIOAJNpn/GWdJUxUswU2/eDu
7RbGScZ5a5NbCUph/JXONw==;                               ←セミコロン（;）を入力します。
License is correct. Proceed with restart? [y/n]: y  ←システム再起動の可否（y/n）を選択します。
% Install license succeed, and restarting...
```

・License file をインポートする場合は、インタフェース、デフォルトゲートウェイの設定が必要になります。

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#interface ethernet 0                ←インタフェース ethernet0 に、
vxr-x86(config-if)#ip address 192.168.0.1/24        ← IP アドレスを設定します。
vxr-x86(config-if)#exit
vxr-x86(config)#ip route 0.0.0.0/0 192.168.0.254    ←デフォルトゲートウェイを設定します。
vxr-x86#install license file ssh://user@A.B.C.D/FILENAME（または、ftp://A.B.C.D/FILENAME）
```

第3章

設定方法の概要

Ⅰ．本装置へのログイン(CLI)

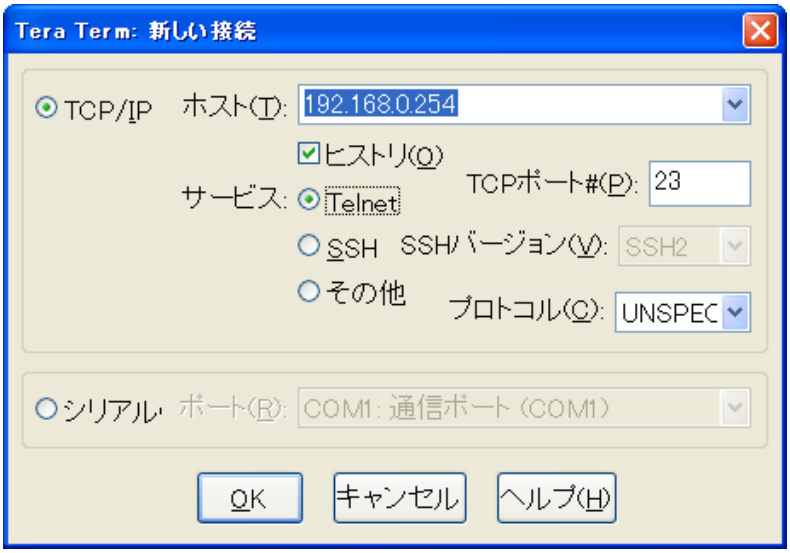
◆本装置へのログイン(Telnet 接続)

・本装置に Telnet 接続するには、インタフェースへの IP アドレスの付与、および Telnet Server の起動が必要です。

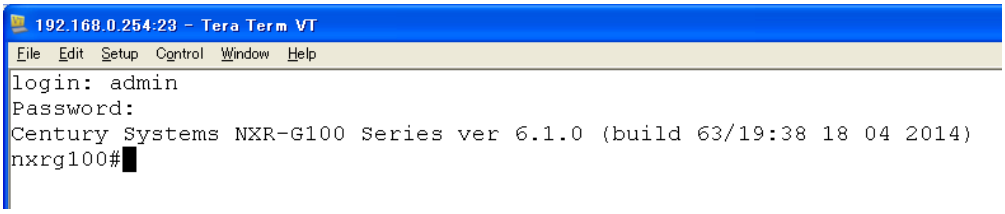
・（minicom を使用して）事前に下記のような設定をしてください。

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#interface ethernet 0
vxr-x86(config-if)#ip address 192.168.0.254/24
vxr-x86(config-if)#exit
vxr-x86(config)#telnet-server enable
telnet-server starting...
vxr-x86(config)#exit
vxr-x86#
```

1．Telnet 接続を開始すると、ログイン画面が表示されます。



2．ユーザ名、パスワード共に「admin」（工場出荷設定）を入力してログインします。



以上で、本装置へのログイン(Telnet 接続)は完了です。

Ⅰ．本装置へのログイン(CLI)

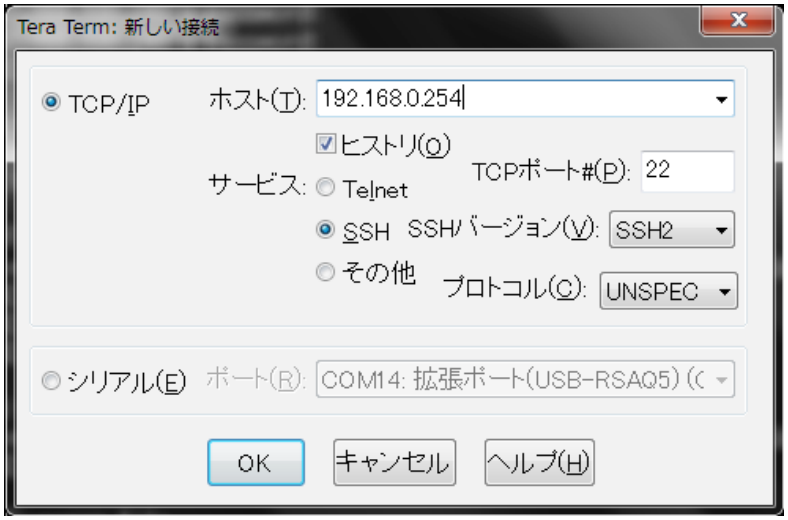
◆本装置へのログイン(SSH 接続)

・本装置に SSH 接続するには、インタフェースへの IP アドレスの付与、および SSH Server の起動が必要です。

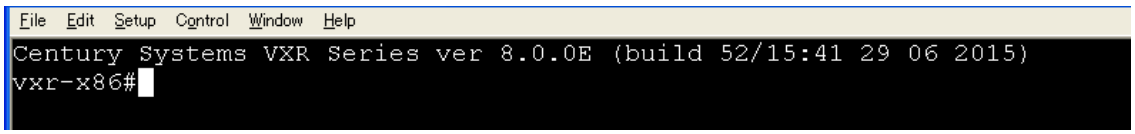
・（minicom を使用して）事前に下記のような設定をしてください。

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#interface ethernet 0
vxr-x86(config-if)#ip address 192.168.0.254/24
vxr-x86(config-if)#exit
vxr-x86(config)#ssh-server enable
ssh-server starting...
Generating SSH1 RSA host key ... Success
Generating SSH2 RSA host key ... Success
vxr-x86(config)#exit
vxr-x86#
```

1．SSH 接続を開始すると、ログイン画面が表示されます。



2．ユーザ名、パスワード共に「admin」（工場出荷設定）を入力してログインします。



以上で、本装置へのログイン(SSH 接続)は完了です。

Ⅱ．本装置へのログイン(GUI)

◆本装置へのログイン（GUI）

・本装置に GUI 接続するには、インタフェースへの IP アドレスの付与、および HTTP Server の起動が必要です。

・（minicom を使用して）事前に下記のような設定をしてください。

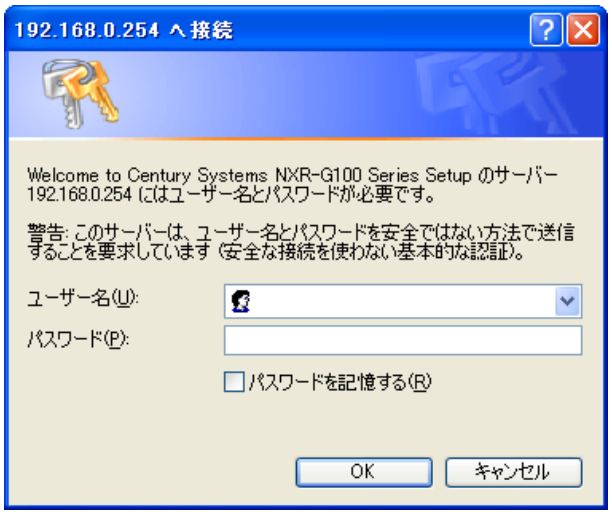
```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#interface ethernet 0
vxr-x86(config-if)#ip address 192.168.0.254/24
vxr-x86(config-if)#exit
vxr-x86(config)#http-server enable
http-server starting ... done
vxr-x86(config)#exit
vxr-x86#
```

1 .Web ブラウザを起動します。

ブラウザのアドレス欄に、上記で設定した IP アドレスとポート番号を入力してください。

http://192.168.0.254:880/ （※ポート番号 880 は変更することができません。）

2 ．認証ダイアログ画面が表示されます。ユーザ名、パスワード共に「admin」（初期値）を入力します。



3 ．下記のような画面が表示されます。以上で本装置へのログインは完了です。

Ⅲ．コマンド実行モード

CLI のコマンド実行環境には以下の２つのモードがあります。
各モードでは、それぞれ実行できるコマンドの種類が異なります。

◆ユーザーモード(VIEW モード)

ログイン直後のモードです。
ユーザモードでは、ネットワークやサービスの情報を表示するコマンドのみ実行することが可能です。
本モードでのプロンプトは、「『ホスト名』#」で表示されます。
logout/exit コマンドを入力すると、CLI を終了し、ログアウトします。
configure terminal コマンドを入力すると特権モードに入ることができます。

◆特権モード(CONFIGURATION モード)

特権モードでは、ユーザモードで実行可能なコマンドに加え、内部システム情報、
コンフィグレーション情報を表示するコマンドや、本装置に対して設定をおこなうコマンドの実行が可能になります。
本モードでのプロンプトは、「『ホスト名』(config)#」で表示されます。
exit コマンドを入力するか、「Ctrl」+「c」を入力するとユーザーモードに戻ることができます。
更に、各設定の詳細設定をおこなうには、特権モードから各種モードへ移行します。

<CLI ログアウト時の表示例>

```
vxr-x86#exit
Century Systems VXR Series
vxr-x86 login:
```

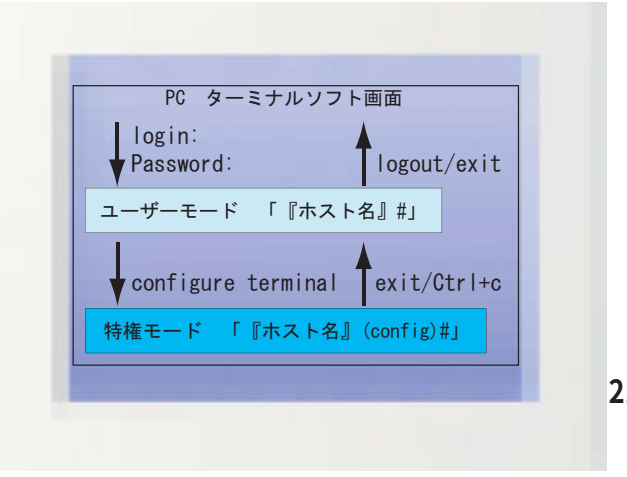
<特権モードへ移行時の表示例>

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#
```

<ユーザーモードへ移行時の表示例>

```
vxr-x86(config)#exit
vxr-x86#
```

<モード間の移行>



Ⅳ．コマンド入力時の補助機能

◆コマンド補完機能

コマンド入力時に、コマンドを特定できる部分まで入力すれば自動的に補完する機能です。
例えば、show interface コマンドの場合、sh int とだけ入力しても実行できます。
また、sh と入力して「Tab」キーを押すと show、int と入力して「Tab」キーを押すと interface と、自動的に残りのワード部分を補完して表示します。

◆コマンドヒストリ機能

過去に実行したコマンドを表示する機能です。
「↑」キー、または「Ctrl」+「p」を入力すると、過去に実行したコマンドを一つずつさかのぼって表示することができます。
また、「↓」キーや「Ctrl」+「n」を入力すると、一つずつ新しい実行コマンドへ戻りながら表示します。

◆コマンドヘルプ機能

後に続くワードの候補の一覧と、その意味を表示する機能です。
ワードの後ろにスペースを入れ、「?」キーを入力すると、候補の一覧を表示することができます。
例えば、show ?と入力すると、後に続くコマンドワードと、そのワードの意味を表示します。
また、スペースを入れずに「?」を入力すると、直前のワードの意味を表示します。
<cr>と表示されるものは、そこで入力が完了するコマンドがあることを意味します。

＜スペースの後ろに「?」キー入力時の表示例＞

```
vxr-x86#show ?
  arp             Address Resolution Protocol (ARP)
  bgp             BGP information
  class           Show class access-list status
  clock           System Clock
  config          Configurations
  crp             Century Registration Protocol (CRP) informations
--More--
```

＜直後に「?」キー入力時の表示例＞

```
vxr-x86#?
Exec commands:
  clear       Reset functions
  clock       Adjusting System Clock
  configure   Enter configuration mode
  connect     Attempt connect Functions
  copy        Import or Export files
  debug       Debugging functions (see also 'undebug')
  delete      Delete files
--More--
```

Ⅳ．コマンド入力時の補助機能

◆コマンドページャ機能

コマンドの表示結果が接続ターミナルのウィンドウサイズより大きい場合に、行送りで表示する機能です。
terminal lengthコマンドを実行することによって本機能を有効にすることができます。
例えば、terminal length 20 を実行すると、ページサイズが 20 行に設定され、コマンド結果を 1 ページ(20 行)ずつ表示します。
表示中のページをスクロールしたい場合は、「Space」キーで 1 ページずつ、「Enter」キーで 1 行ずつ行送りします。ただし、スクロールダウンはできません。
terminal no length を実行すると、ページャ機能は無効になります。

◆grep 機能

CLIでのみ利用可能な機能で、情報表示の際に文字列を指定することができます。多くの情報が表示されて、目的とする情報を見付けることが困難な場合に役立つ機能です。
情報表示(show)系のすべてのコマンドの後に、「|(パイプ)」+「option」+「文字列」を入力します。利用可能な option は、以下のとおりです。

- begin　　指定した文字列を含む行以降を表示します。
- include　指定した文字列を含む行のみを表示します。
- exclude　指定した文字列を含まない行を表示します。

Ｖ．本装置のモード構造

本装置のモード構造は以下のとおりです。設定方法については、次章以降に記します。

```
view mode
      |---- global mode
                  |---- interface mode                    (続き)
                  |---- interface tunnel mode               |---- access-server profile mode
                  |---- interface ppp mode                  |---- interface virtual-template mode
                  |---- dns mode                            |---- ngn-sip client mode
                  |---- l2tp mode                           |---- ngn-sip server mode
                  |---- l2tpv3 tunnel mode                  |---- ipv6 dhcp-server mode
                  |---- l2tpv3 xconnect mode                |---- ipv6 dhcp-client mode
                  |---- l2tpv3 group mode                   |---- l2tpv3 access-list mode
                  |---- rip mode                            |---- address-family ipv6 mode
                  |---- ospf mode
                  |---- bgp mode
                  |---- ntp mode
                  |---- snmp mode
                  |---- syslog mode
                  |---- dhcp-server mode
                  |---- dhcp-relay mode
                  |---- ipsec local policy mode
                  |---- ipsec isakmp policy mode
                  |---- ipsec tunnel policy mode
                  |---- UPnP mode
                  |---- QoS (class-policy mode)
                  |---- QoS (class-filter mode)
                  |---- crp client mode
                  |---- route-map mode
                  |---- Web Authenticate mode
                  |---- WarpLink mode
                  |---- Extended track IP reachability mode
                  |---- Extended track IPv6 reachability mode
                  |---- ipv6 dhcp-server mode
                  |---- ipv6 dhcp-client mode
                  |---- l2tpv3 access-list mode
                  |---- address-family ipv6 mode
                  |---- Monitor-log mode
                  |---- mail server mode
                  |---- interface bridge mode
                  |---- DDNS mode
                (続く)
```

第4章

view(exec) mode

view(exec) mode

■ show

○ show config

<説　　明>　running-config(現在動作中の設定情報)を表示します。
<書　　式>　show config (|xml)

○ show config file

<説　　明>　ファイルパスとファイル名を指定して、設定情報を表示します。
<書　　式>　show config file FILENAME xml
<　例　>　show config file disk0:vxr.xml xml

○ show startup-config

<説　　明>　startup-config(flashに保存されている設定情報)を表示します。
<書　　式>　show startup-config xml
<備　　考>　startup-configの表示は、XML形式のみ対応しています。

○ show config section

<説　　明>　指定した機能の設定情報を表示します。
<書　　式>　show config
　　(crp|dhcp-relay|dhcp-server|dns|ntp|qos|route-map
　　|router rip|router ospf|router bgp|snmp|syslog|upnp
　　|warplink|web-authenticate)
　　show config ssl
　　show config ssl tunnel (|<0-2>)

view(exec) mode

○ **show config ipsec**

＜説　　明＞

・IPsec の設定情報（isakmp policy/local policy/tunnel policy）を表示します。

・ID を指定することで、特定の isakmp policy/local policy/tunnel policy の設定情報だけを表示させることができます。

＜書　　式＞

```
show config ipsec (|isakmp policy|local policy|tunnel)
show config ipsec (|isakmp policy <1-65535>|local policy <1-255>|tunnel <1-65535>)
```

○ **show config l2tpv3**

＜説　　明＞

・L2TPv3 の設定情報（group/tunnel/xconnect）を表示します。

・ID を指定することで、特定の Group/Tunnel/Xconnect の設定情報だけを表示させることができます。

＜書　　式＞

```
show config l2tpv3 (|group|tunnel|xconnect)
show config l2tpv3 (|group <1-4095>|tunnel <0-4095>|xconnect <1-4294967295>)
```

○ **show config ipv6 dhcp-client**

＜説　　明＞　ipv6 dhcp-client の設定を表示します。

＜書　　式＞　show config ipv6 dhcp-client (|WORD)

＜備　　考＞　ipv6 dhcp-client WORD で設定した「WORD」を指定します。

view(exec) mode

◆ show ip route
<説　　明>　ルーティングテーブルを表示します。
<書　　式>　show ip route (|bgp|connected|ospf|rip|static)
　　show ip route database (|bgp|connected|ospf|rip|static)

◆ show ipv6 route
<説　　明>　IPv6ルーティングテーブルを表示します。
<書　　式>　show ipv6 route (|connected|static)
　　show ipv6 route cache
　　show ipv6 route database (|connected|static)

◆ show ip protocols
<説　　明>　ルーティングプロトコルに関する情報を表示します。
<書　　式>　show ip protocols (|ospf|rip)

◆ show ip access-list
<説　　明>　IPアクセスリストを表示します。
<書　　式>　show ip access-list [IPv4- ACL-NAME]

◆show ip access-list
<説　　明>　IPv4のアクセスリストを表示します。
<書　　式>
ip access-list IPv4-ACL-NAME (permit|deny)
　　src_ip(A.B.C.D|A.B.C.D/M|any|FQDN) dst_ip(A.B.C.D|A.B.C.D/M|any|FQDN)

ip access-list IPv4-ACL-NAME (permit|deny)
　　src_ip(A.B.C.D|A.B.C.D/M|any|FQDN) dst_ip(A.B.C.D|A.B.C.D/M|any|FQDN) <protocol:0-255>

ip access-list IPv4-ACL-NAME (permit|deny)
　　src_ip(A.B.C.D|A.B.C.D/M|any|FQDN) dst_ip(A.B.C.D|A.B.C.D/M|any|FQDN)
　　(icmp|<icmp_type:0-255>)

ip access-list IPv4-ACL-NAME (permit|deny)
　　src_ip(A.B.C.D|A.B.C.D/M|any|FQDN) dst_ip(A.B.C.D|A.B.C.D/M|any|FQDN)
　　(tcp|udp)
　　(tcp|udp) (<sport:1-65535>|any|range <min:1-65535> <max:1-65535>)
　　(<dport:1-65535>|any|range <min:1-65535> <max:1-65535>)

ip access-list IPv4-ACL-NAME (permit|deny)
　　src_ip(A.B.C.D|A.B.C.D/M|any|FQDN) dst_ip(A.B.C.D|A.B.C.D/M|any|FQDN)
　　tcp syn
　　tcp {<sport:1-65535>|any|(range <min:1-65535> <max:1-65535>)}
　　{<dport:1-65535>|any|(range <min:1-65535> <max:1-65535>)} syn

view(exec) mode

◆ show ip default-gateway
<説　　明>　デフォルトゲートウェイを表示します。
<書　　式>　show ip default-gateway

◆ show ip (snat|dnat)
<説　　明>　SNAT | DNATを表示します。
<書　　式>　show ip (snat|dnat) [NAT-RULE-NAME]

◆ show (ip|ipv6) connection
<説　　明>　TCP/UDPポートのlistening状態を表示します。
<書　　式>　show (ip|ipv6) connection

◆ show ip statistics
<説　　明>　プロトコル毎（IP／TCP／UDP／ICMP）の統計情報を表示します。
<書　　式>　show ip statistics

■ show ip conntrack
○ (ip|ipv6) conntrack
<説　　明>　conntrack tableを表示します。
<書　　式>　show (ip|ipv6) conntrack

○ (ip|ipv6) conntrack limit
<説　　明>　session limit機能によってdropされたパケットのカウンタを表示します。
<書　　式>　show (ip|ipv6) conntrack limit

○ (ip|ipv6) conntrack invalid-status-drop
<説　　明>　session invalid-status-drop機能によってdropされたパケットのカウンタを表示します。
<書　　式>　show (ip|ipv6) conntrack invalid-status-drop

◆ show ip spi-filter
<説　　明>　SPI filterを表示します。
<書　　式>　show ip spi-filter

◆ show ip upnp
<説　　明>　UPnP のアクセスリスト（またはNAT）を表示します。
　　アクセスリスト（またはNAT）は、UPnP を設定すると自動的に設定されます。
<書　　式>　show ip upnp (access-list|nat)

view(exec) mode

◆ show ipv6 access-list
<説　　明>　IPv6アクセスリストを表示します。
<書　　式>　show ipv6 access-list [IPv6-ACL-NAME]

◆show ipv6 access-list
<説　　明>　IPv6のアクセスリストを表示します。
<書　　式>　ipv6 access-list IPv6-ACL-NAME (permit|deny) SRC-IPV 6 DST-IPV6
ipv6 access-list IPv6-ACL-NAME (permit|deny) SRC-IPV6 DST-IPV6 PROTOCOL
ipv6 access-list IPv6-ACL-NAME (permit|deny) SRC-IPV6 DST-IPV6 ICMPV6
ipv6 access-list IPv6-ACL-NAME (permit|deny) SRC-IPV6 DST-IPV6 TCP/UDP
ipv6 access-list IPv6-ACL-NAME (permit|deny) SRC-IPV6 DST-IPV6 TCP-OPTIONS
<オプション>

SRC-IPV6	: (X:X::X:X | X:X::X:X/M | any | FQDN)	
DST-IPV6	: (X:X::X:X | X:X::X:X/M | any | FQDN)	
PROTOCOL	: <0-255>	: Protocol number
ICMPV6	: (icmpv6 | icmpv6 <0-255>)	: IPv6 ICMPv6 <IPv6 ICMP type>
TCP/UDP	: (tcp | udp)	
	: (tcp | udp) (<sport:1-65535>|any|range <min:1-65535> <max:1-65535>) (<dport:1-65535>|any|range <min:1-65535> <max:1-65535>)	
TCP-OPTIONS	: tcp syn	: TCP syn packets
	: tcp (<sport:1-65535>|any|range <min:1-65535> <max:1-65535>) (<dport:1-65535>|any|range <min:1-65535> <max:1-65535>) syn	

◆ show ipv6 forwarding
<説　　明>　IPv6フォワーディングのon/offを表示します。
<書　　式>　show ipv6 forwarding

◆ show ipv6 interface
<説　　明>　IPv6インタフェースの状態を表示します。
<書　　式>　show ipv6 interface (|INTERFACE|brief)

◆ show ipv6 default-gateway
<説　　明>　IPv6デフォルトゲートウェイを表示します。
<書　　式>　show ipv6 default-gateway

◆ show ipv6 statistics
<説　　明>　IPv6のネットワークの統計情報を表示します。
<書　　式>　show ipv6 statistics

◆ show ipv6 spi-filter
<説　　明>　IPv6 SPI filterを表示します。
<書　　式>　show ipv6 spi-filter

view(exec) mode

◆ show ipv6 dhcp client pd
＜説　　明＞　ipv6 dhcp-clientのステータスを表示します。
＜書　　式＞　show ipv6 dhcp client pd WORD
＜備　　考＞　WORDには、prefix名を指定します。

◆ show ipv6 ndp proxy
＜説　　明＞　IPv6 NDP proxyのproxyテーブルを表示します。
＜書　　式＞　show ipv6 ndp-proxy interface ethernet <0-XX>

◆ show ipv6 ra proxy
＜説　　明＞　IPv6 RA proxyのprefixを表示します。
＜書　　式＞　show ipv6 ra-proxy interface ethernet <0-XX>

◆show ip web-auth access-list
＜説　　明＞　Web認証フィルタを表示します。
＜書　　式＞　show ip web-auth access-list (|WEBAUTH-ACL-NAME)

◆ show ntp
＜説　　明＞　NTPサーバとの同期状態を表示します。
＜書　　式＞　show ntp

◆ show dns
＜説　　明＞　DNSの設定情報を表示します。
＜書　　式＞　show dns

◆ show dhcp
＜説　　明＞　DHCPサーバのリースアドレス情報を表示します。
＜書　　式＞　show dhcp lease

view(exec) mode

◆ show syslog
<説　　明>　syslogを表示します。
<書　　式>　show syslog (message|bootlog|maillog) (|line:1-99999) (|reverse)
<備　　考>
・通常、syslogは古い情報から新しい情報の順に表示されますが、reverseを指定すると新しい情報から表示します。

<説　　明>　monitorを指定すると、リアルタイムでsyslogを表示することが出来ます。
<書　　式>　show syslog message monitor
<備　　考>
・monitor指定によるsyslogを表示している間は、他のコマンドを実行することは出来ません。また、begin、exclude、includeを指定することは出来ません。

<説　　明>　ディスクイメージ内のユーザ割り当て領域に保存したsyslogを表示します。
<書　　式>　show syslog file FILENAME (|line:1-99999) (|reverse)
<備　　考>
・ファイルパスとファイル名を指定します。
　例）　show syslog file disk0:syslog.log
・syslogをディスクイメージ内のユーザ割り当て領域に保存するには、syslog modeでの設定が必要になります。
　例）　vxr-x86(config)#syslog
　　vxr-x86(config-syslog)#local file disk0:syslog.log

◆ show arp
<説　　明>　ARPテーブルを表示します。
<書　　式>　show arp

◆ show ipv6 neighbors
<説　　明>　IPv6ネイバーを表示します。
<書　　式>　show ipv6 neighbors

◆ show disk0
<説　　明>　ディスクイメージ内のユーザ割り当て領域の情報を表示します。
<書　　式>　show disk0

◆ show uptime
<説　　明>　システムの稼働時間を表示します。
<書　　式>　show uptime

◆ show tech-support
<説　　明>　テクニカルサポート情報を表示します。
<書　　式>　show tech-support

view(exec) mode

◆ show memory
<説　　明>　メモリ使用量を表示します。
<書　　式>　show memory

◆ show process
<説　　明>　アクティブなプロセスに関する情報を表示します。
<書　　式>　show process

◆ show clock
<説　　明>　システムクロックを表示します。
<書　　式>　show clock

◆ show history
<説　　明>　過去に実行した運用コマンドの履歴を表示します。
<書　　式>　show history

◆ show file systems
<説　　明>　ファイルシステムを表示します。
<書　　式>　show file systems

◆ show loadavg
<説　　明>　CPUロードアベレージを表示します。
<書　　式>　show loadavg

◆ show system usb transfer-mode
<説　　明>　USBのデータ転送モードを表示します。
<書　　式>　show system usb transfer-mode

■ show l2tp
○ show l2tp
<説　　明>　L2TPのtunnel/session状態を表示します。
<書　　式>　show l2tp
　　show l2tp tunnel (|<TunnelID:1-65535>)
　　show l2tp session (|<TunnelID:1-65535>)
　　show l2tp session <TunnelID:1-65535> <SessionID:1-65535>

○ show l2tp peer
<説　　明>　該当するtunnel設定で、使用中のaddress pool情報を表示します。
<書　　式>　show l2tp peer <0-1> ip pool

view(exec) mode

■ show l2tpv3

○ show l2tpv3

<説　　明>　L2TPv3の情報を表示します。
<書　　式>　show l2tpv3

○ show l2tpv3 tunnel

<説　　明>　L2TPv3のトンネル情報を表示します。
<書　　式>　show l2tpv3 tunnel (|<TID:1-4294967295>) (|detail)

○ show l2tpv3 session

<説　　明>　L2TPv3のセッション情報を表示します。
<書　　式>　show l2tpv3 session (|<SID:1-4294967295>) (|detail)

○ show l2tpv3 interface

<説　　明>　Xconnectインタフェース情報を表示します。
<書　　式>　show l2tpv3 interface (|INTERFACE) (|detail)

○ show l2tpv3 fdb

<説　　明>　L2TPv3 FDB情報を表示します。
<書　　式>　show l2tpv3 fdb (local|forward|)

○ show l2tpv3 fdb interface

<説　　明>　Xconnectインタフェースの FDB情報を表示します。
<書　　式>　show l2tpv3 fdb interface INTERFACE (local|forward|)

○ show l2tpv3 group

<説　　明>　L2TPv3グループを表示します。
<書　　式>　show l2tpv3 group (<GID:1-65535>|)

○ show l2tpv3 peer

<説　　明>　L2TPv3ピアを表示します。
<書　　式>　show l2tpv3 peer (A.B.C.D|)

○ show l2tpv3 access-list

<説　　明>　L2TPv3のアクセスリストを表示します。
<書　　式>　show l2tpv3 access-list
　　show l2tpv3 access-list interface (|INTERFACE)
　　show l2tpv3 access-list xconnect (|<1-4294967295>)
　　show l2tpv3 access-list (root|layer2|ip|ipv6|arp|vlan|ieee802-3) (|WORD)
　　show l2tpv3 access-list detail (root|layer2|vlan) (|WORD)
　　show l2tpv3 access-list detail root WORD layer2 WORD

view(exec) mode

◆ show interface
＜説　　明＞　インタフェースのステータスと設定情報を表示します。
＜書　　式＞　show interface (|mode|power-save)
　　show interface INTERFACE (|mode|power-save)
　　show interface bridge <0-4095> (|fdb|flows|port-list|statistics)
　　show interface bridge list
　　show interface wlan <0-1> (|all|ssid)
　　show interface tap <0-127> (|vid <1-4094>)
＜備　　考＞　(mode|power-save)はethernet I/Fのみ指定することができます。

◆ clear interface bridge
＜説　　明＞　ブリッジ（仮想スイッチ）インタフェースのFDBをクリアします。
＜書　　式＞　clear interface bridge <0-4095> fdb

◆ show route-map
＜説　　明＞　Route-mapを表示します。
＜書　　式＞　show route-map (|detail) (|WORD)

◆ show class access-list
＜説　　明＞　class access-listを表示します。
＜書　　式＞　show class access-list (|WORD)

◆ show ssh-public-key
＜説　　明＞　Netconf接続のSSH公開鍵を表示します。
＜書　　式＞　show ssh-public-key user netconf

◆ show users
＜説　　明＞　ログインセッションの情報を表示します。
＜書　　式＞　show users

◆ show debugging
＜説　　明＞　デバッグログのステータス(ON/OFF)、およびデバッグタイマーのステータス(設定およびカウントダウンタイマー)を表示します。
＜書　　式＞　show debugging (l2tpv3|netevent|ppp)
　　show debugging timer (|<1-5>)

view(exec) mode

◆ show vrrp

＜説　　明＞　VRRPのステータス情報を表示します。
＜書　　式＞　show vrrp

◆ show ppp

＜説　　明＞　PPPのステータス情報を表示します。
＜書　　式＞　show ppp (|<0-4>)
　　show ppp (|<100-256>)
＜備　　考＞　show ppp <100-256>でPPP(over L2TP LNS)のセッション情報を表示します。

view(exec) mode

◆ show pppoe-bridge
<説　　明>　PPPoE bridgeのステータス情報を表示します。
<書　　式>　show pppoe-bridge

◆ show ipsec
<説　　明>　IPsecの情報を表示します。
<書　　式>　show ipsec ca certificates
　　show ipsec certificates
　　show ipsec crls
　　show ipsec policy
　　show ipsec public-keys
　　show ipsec rsa-pub-key
　　show ipsec sa
　　show ipsec status (|tunnel <1-65535>) (|brief)
　　show ipsec status (version1|version2)
　　show ipsec leases (version1|version2)

◆ show ip rip
<説　　明>　RIPの情報を表示します。
<書　　式>　show ip rip
　　show ip rip interface (|INTERFACE)
　　show ip rip database

◆ show ip ospf
<説　　明>　OSPFの情報を表示します。
<書　　式>　show ip ospf
　　show ip ospf neighbor (|detail)
　　show ip ospf interface (|INTERFACE)
　　show ip ospf database (|external|summary|network|router|asbr-summary)
　　show ip ospf route
　　show ip ospf virtual-links

◆ show ip bgp
<説　　明>　BGPの情報を表示します。
<書　　式>　show ip bgp
　　show ip bgp (A.B.C.D|A.B.C.D/M)
　　show ip bgp neighbors (A.B.C.D|X:X::X:X)
　　show ip bgp neighbors (A.B.C.D|X:X::X:X) (advertised-routes|received-routes|routes)]
　　show ip bgp route-map ROUTE-MAP
　　show ip bgp scan
　　show ip bgp summary
　　show ip bgp regexp LINE　　(BGP AS pathsの正規表現を表示)

view(exec) mode

◆ show bgp ipv6

＜説　　明＞　BGPの情報を表示します。

＜書　　式＞

```
show bgp ipv6 X:X::X:X
show bgp ipv6 X:X::X:X/M
show bgp ipv6 filter-list ACL-NAME
show bgp ipv6 neighbors (A.B.C.D|X:X::X:X)
show bgp ipv6 neighbors (A.B.C.D|X:X::X:X) (advertised-routes|received-routes|routes)]
show bgp ipv6 regexp LINE
show bgp ipv6 route-map ROUTE-MAP
show bgp ipv6 summary
```

◆ clear bgp ipv6

＜説　　明＞

・BGP セッションをリセットします。

・BGPの設定を変更した場合、即時には反映されないため、BGPセッションを一度リセットする必要があります。

- soft out リセット
  BGPネットワークやフィルタリングの変更などの経路情報は、BGPセッションを維持したまま適用することが出来ます。soft outリセットを行うと、設定を内部に反映し、BGP neighborへUPDATEメッセージを送信します。
- soft in リセット
  BGP neighbor へROUTE-REFRESH メッセージを送信し、neighbor へ全てのBGP 経路情報を要求します。ROUTE-REFRESH メッセージを受信した場合は、UPDATE メッセージにより経路情報を送信します。
- hard リセット
  BGPのTCPセッションを一旦切断し、neighbor を再確立します。keepalive やholdtime の設定を変更した場合は、ソフトリセットでは変更が反映されないためハードリセットを行ってください。
  ハードリセットを行う場合は、soft (in|out)を指定しません。

＜書　　式＞　clear bgp ipv6 * soft (in|out)

＜備　　考＞　すべてのneighborとのセッションをリセットします。

＜書　　式＞　clear bgp ipv6 X:X::X:X
　　clear bgp ipv6 X:X::X:X soft (in|out)

＜備　　考＞　Neighbor のIPv6 アドレスを指定して、セッションをリセットします。

view(exec) mode

■ show mobile

＜説　　明＞　3Gデータ通信カードに関する情報を表示します。

○カード情報の表示

＜書　　式＞　show mobile (|<0-1>)

○ ap

＜説　　明＞　APN 情報を表示します。カードによっては、ppp 使用中は取得できません。

＜書　　式＞　show mobile <0-1> ap

○ network-reg-status

＜説　　明＞

・ネットワークへの登録情報を表示します。カードによっては、ppp 使用中は取得できません。

＜書　　式＞　show mobile <0-1> network-reg-status

＜実　行　例＞　vxr-x86#show mobile 0 network-reg-status

Network Area : 3G

○ phone-number

＜説　　明＞　電話番号を表示します。カードによっては、ppp 使用中は取得できません。

＜書　　式＞　show mobile <0-1> phone-number

○ signal-level

＜説　　明＞　電波強度を表示します。カードによっては、ppp 使用中は取得できません。

＜書　　式＞　show mobile <0-1> signal-level

＜実　行　例＞　vxr-x86#show mobile 0 signal-level

Signal Level : 3 [Area: 3G]

view(exec) mode

◆ **show fast-forwarding**

＜説　　明＞　Fast-forwardingの設定情報を表示します。
＜書　　式＞　show fast-forwarding
＜備　　考＞　「Fast-forwarding is on」または「Fast-forwarding is off」が表示されます。

◆ **show fast-forwarding status**

＜説　　明＞　Fast-forwardingされたパケットの情報を表示します。
＜書　　式＞　show fast-forwarding status
＜備　　考＞

・以下に、Fast-forwarding（IP forwarding）の例を示します。

```
vxr-x86#show fast-forwarding status
total forward count 644
3s udp 192.168.0.1:63->192.168.10.1:63 count:9 byte:12564 fw4 natp4 src 192.168.1.254:63 ①
4s udp 192.168.10.1:63->192.168.1.254:63 count:9 byte:12564 natp4 dst 192.168.0.1:63 fw4 ②
```

①、②は、IP forwardingされたエントリーです。

・以下に、Fast-forwarding（IPsec）の例を示します。

```
vxr-x86#show fast-forwarding status
total forward count 661
7s esp 192.168.1.253->192.168.1.254 count:9 byte:12564 ESP_IN spi:$95e97067 fw4          ①
7s udp 192.168.10.1:63->192.168.0.1:63 count:8 byte:11168 fw4                            ②
5s udp 192.168.0.1:63->192.168.10.1:63 count:9 byte:13158 fw4 ESP_OUT spi:$44f8bc92      ③
```

①、②、③はそれぞれ、①ESPヘッダをとるエントリー、②IP forwardingされたエントリー、③ESPヘッダを付けてIP forwardingされたエントリーです。

view(exec) mode

◆ show product
＜説　　明＞　製品に関する情報を表示します。
＜書　　式＞　show product
＜備　　考＞　ベンダー、製品情報、ファームウェアバージョン、シリアル番号、サポートサイト、
サポート情報等が表示されます。

■ show netevent
○ track
＜説　　明＞　Neteventのtrack object(監視対象)のステータスを表示します。
＜書　　式＞　show netevent track (|<object_id:1-255>) (|detail|brief)
＜備　　考＞　Object IDを指定すると、該当するtrack statusを表示します。
briefを指定すると、簡易一覧を表示します。
detailを指定すると、詳細情報を表示します。

○ action
＜説　　明＞　Neteventのtrack object(監視対象)に関連付けられたactionを表示します。
＜書　　式＞　show netevent action (|<object_id:1-255>)
＜備　　考＞　Object IDを指定すると、そのIDに関連付けられたactionを表示します。

◆ show warplink
＜説　　明＞　WarpLink Managerとの通信状態を表示します。
＜書　　式＞　show warplink
＜備　　考＞　詳細は、第31章：WarpLink modeを参照してください。

◆ show monitor-log
＜説　　明＞　Monitor-logを表示します。
＜書　　式＞　show monitor-log (reachability|resource)
＜備　　考＞　詳細は、第34章：Monitor-log modeを参照してください。

◆ show service
＜説　　明＞　サービスの起動状態を表示します。
＜書　　式＞　show service
＜備　　考＞　各サービスの起動状態が、upまたはdownで表示されます。

view(exec) mode

◆ show ngn-sip
<説　　明>　NGN SIPの状態を表示します。
<書　　式>　show ngn-sip

◆ show ip dhcp route
<説　　明>　NGN回線でDHCPv4により取得したstatic routeを表示します。
<書　　式>　show ip dhcp route

◆ clear ngn-sip call
<説　　明>　データコネクト接続中を切断します。
<書　　式>　clear ngn-sip call <1-99999>

◆ clock set
<説　　明>　現在時刻を設定します。
<書　　式>　clock set HH:MM:SS Day Month Year
　　clock set ntp (A.B.C.D|X:X::X:X|FQDN)
<備　　考>　2010年12月31日12時34分56秒に設定する場合は、次のように入力します。
　　clock set 12:34:56 31 12 2010

◆ delete
<説　　明>　ファイルを消去します。
<書　　式>　delete bootlog　　(bootlogの削除)
　　delete dump　　(dumpファイルの削除)
　　delete file disk0:FILENAME
　　(ディスクイメージ内のユーザ割り当て領域からファイルを削除)
　　delete syslog　　(syslogの削除(初期化))
　　delete reachability-log　　(reachabilityログの削除)
　　delete resource-log　　(resourceログの削除)

◆ save config
<説　　明>　設定をフラッシュに保存します。
<書　　式>　save config

◆ dir
<説　　明>　ディスクイメージ内のユーザ割り当て領域に保存されているファイルを全て表示します。
<書　　式>　dir (|disk0)

view(exec) mode

■ copy

○ (bootlog|dump|syslog|reachability-log|resource-log)

＜説　　明＞　bootlog，dump，syslog，reachability-log，resource-logをコピーします。

＜書　　式＞

```
copy (bootlog|dump|syslog|reachability-log|resource-log)
            ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME (|source A.B.C.D|X:X::X:X)
copy (bootlog|dump|syslog|reachability-log|resource-log)
            ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
copy (bootlog|dump|syslog|reachability-log|resource-log) disk0:FILENAME
```

＜備　　考＞

・ソースアドレスを指定することができます。

・SSHを使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合（ssh://user@A.B.C.D/FILENAME）は、22番ポートを使用します（=ssh://user@A.B.C.D:22/FILENAME)。

- IPv4　ssh://user@A.B.C.D:port/FILENAME
- IPv6　ssh://[user@X:X::X:X]:port/FILENAME

○ configのバックアップ

＜説　　明＞　設定ファイルのバックアップ（外部にコピー）をおこないます。

＜書　　式＞

```
copy (config|show-config) ssh://(<user@A.B.C.D|X:X::X:X)>/FILENAME
                                        (|all) (|source A.B.C.D|X:X::X:X)
copy (config|show-config) ftp://<A.B.C.D|X:X::X:X>/FILENAME
                                        (|all) (|source A.B.C.D|X:X::X:X)
copy (config|show-config) disk0:FILENAME (|all)
```

＜備　　考＞

・all指定の場合は、ipsecを含む全てのconfigをtgz形式でコピーします。指定なしの場合は、configのみをxml形式でコピーします。

・設定ファイルをshow config形式でバックアップするには、show-configを指定します。

・ソースアドレスを指定することができます。

・SSHを使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合（ssh://user@A.B.C.D/FILENAME）は、22番ポートを使用します（=ssh://user@A.B.C.D:22/FILENAME)。

- IPv4　ssh://user@A.B.C.D:port/FILENAME
- IPv6　ssh://[user@X:X::X:X]:port/FILENAME

view(exec) mode

○ configの復帰

＜説　　明＞　設定ファイルの復帰をおこないます。

＜書　　式＞

```
copy ssh://user@(A.B.C.D|X:X::X:X)/FILENMAE
            (startup-config|disk0:FILENAME) (rollback|source A.B.C.D|X:X::X:X)
copy ftp://(A.B.C.D|X:X::X:X)/FILENAME
            (startup-config|disk0:FILENAME) (rollback|source A.B.C.D|X:X::X:X)
copy disk0:FILENAME startup-config (rollback|source A.B.C.D|X:X::X:X)
```

＜備　　考＞

・ソースアドレスを指定することができます。

・SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合（ssh://user@A.B.C.D/FILENAME）は、22 番ポートを使用します（=ssh://user@A.B.C.D:22/FILENAME)。

- IPv4　ssh://user@A.B.C.D:port/FILENAME
- IPv6　ssh://[user@X:X::X:X]:port/FILENAME

■ Config Rollback機能

・rollback を指定すると、現在の startup-config を backup します。

・次回の起動時は、復帰させた config で起動し、起動後一定時間（600 秒）内にユーザによる承認が行われない場合、backup した config で再起動する機能です。

・これにより、リモートで config を復帰した場合に、config の間違い等でリモートからの操作が出来なくなることを防ぎます。

・rollback の対象は、startup-config で、保持されるのは 1 世代のみです。

・startup-config 以外（例えば、disk 上の config）で起動している場合、本機能は動作しません。

■ Rollback timer の停止（承認）

・下記のコマンドにて、Rollback timer を停止（承認）することが出来ます（backup の config を削除します)。

- save config
- restart system
- firmware update
- clear rollback
- SMS による clear rooback 指示

■ Rollback の cancel

・Rollback 有効の状態で config を復帰した後、システム再起動を行う前に、cancel rollback を実行することで、rollback を無効にすることが出来ます。

・システム再起動後、rollback timer が起動している状態で、cancel rollback を実行しても、rollbacktimer は停止しません。

view(exec) mode

○ **ssh公開鍵のインポート**

＜説　　明＞　管理サーバ(CMS)との接続に使用するSSH公開鍵をインポートします。

＜書　　式＞

```
copy (ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME)
                        ssh-public-key user netconf |<0-4> (|source A.B.C.D|X:X::X:X)
copy (ftp://<A.B.C.D|X:X::X:X>/FILENAME)
                        ssh-public-key user netconf |<0-4> (|source A.B.C.D|X:X::X:X)
copy disk0:FILENAME ssh-public-key user netconf |<0-4> (|source A.B.C.D|X:X::X:X)
```

＜備　　考＞

・ソースアドレスを指定することができます。

・SSHを使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合（ssh://user@A.B.C.D/FILENAME）は、22番ポートを使用します（=ssh://user@A.B.C.D:22/FILENAME)。

- IPv4　ssh://user@A.B.C.D:port/FILENAME
- IPv6　ssh://[user@X:X::X:X]:port/FILENAME

○ **tech-supportの取得**

＜説　　明＞　tech-supportを取得（外部にコピー）します。

＜書　　式＞

```
copy tech-support ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME (|source A.B.C.D|X:X::X:X)
copy tech-support ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
copy tech-support disk0:FILENAME
```

◆ **firmware update**

＜説　　明＞　ファームウェアをアップデートします。

＜書　　式＞

```
firmware update official (|source A.B.C.D|X:X::X:X)
firmware update ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME (|source A.B.C.D|X:X::X:X)
firmware update ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
firmware update disk0:FILENAME
```

＜備　　考＞

・ソースアドレスを指定することができます。

・SSHを使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合（ssh://user@A.B.C.D/FILENAME）は、22番ポートを使用します（=ssh://user@A.B.C.D:22/FILENAME)。

- IPv4　ssh://user@A.B.C.D:port/FILENAME
- IPv6　ssh://[user@X:X::X:X]:port/FILENAME

・ファームウェア更新後に再起動します。設定を保存していない場合は、問い合わせてからファームウェアの更新を行います。詳細については、「付録D:Firmware update」を参照してください。

◆ **firmware check official**

＜説　　明＞　弊社Webサイトをチェックして、最新ファームウェアの有無を確認します。

＜書　　式＞　firmware check official

view(exec) mode

◆ restart

＜説　　明＞　サービスの再起動を行います。

＜書　　式＞

restart bgp	(BGPサービスを再起動します)
restart ddns	(DDNSサービスを再起動します)
restart dhcp-relay	(DHCPリレーサービスを再起動します)
restart dhcp-server	(DHCPサーバを再起動します)
restart dns	(DNSサービスを再起動します)
restart http-server	(HTTPサーバを再起動します)
restart ipsec	(IPsecサービスを再起動します)
restart l2tp	(L2TPv2サービスを再起動します)
restart l2tpv3	(L2TPv3サービスを再起動します)
restart monitor-log	(Monitor-logサービスを再起動します)
restart netconf-server	(Netconfサーバを再起動します)
restart ntp	(NTPサービスを再起動します)
restart ospf	(OSPFサービスを再起動します)
restart rip	(RIPサービスを再起動します)
restart snmp	(SNMPサービスを再起動します)
restart ssh-server	(SSHサーバを再起動します)
restart syslog	(Syslogサービスを再起動します)
restart system	(本装置を再起動します)
restart telnet-server	(Telnetサーバを再起動します)
restart upnp	(UPnPサービスを再起動します)
restart vrrp	(VRRPサービスを再起動します)
restart warplink	(WarpLinkクライアントを再起動します)
restart ssl-tunnel	(ssl-tunnelを再起動します)
restart lxc	(LXCを再起動します)

◆ restart rollback

＜説　　明＞

・ロールバックタイマが満了する前に、直ちにロールバックさせたい場合、restart rollbackコマンドを実行します。

＜書　　式＞　restart rollback

＜備　　考＞

・ロールバック指定を行い、ロールバックタイマが満了した場合（ロールバックタイマを停止させない場合）、バックアップしたconfigでシステム再起動します。

view(exec) mode

◆ configure
＜説　　明＞　コンフィグレーションモード（global mode）へ移行します。
＜書　　式＞　configure terminal

■ dump
＜説　　明＞
・本装置が送受信したパケットをdumpする機能です。採取したdump情報を、外部記憶装置(USBやCF)に保存したり、SSHを使用して外部サーバに転送することも可能です。
・dump情報はRAM上に保持されます。USERによる削除の指示がない限りmemoryを占有し続けるため、必要のない場合は削除してください。
＜備　　考＞
・本機能を使用する場合は、fast-forwawdingをdisable(no fast-forwarding enable)にしてください。

○ dump
＜書　　式＞　dump interface INTERFACE
＜備　　考＞　INTERFACEは、いずれかを指定します。
bridge <0-4095>
ethernet <0-X> (|vid<vlan_id:1-4094>)
ppp <0-4>
tap <0-127>
tunnel <1-255>
veth <0-1>

○ dump filter
＜書　　式＞　dump interface INTERFACE filter (ssh|telnet|tcp880)

○ dump pcap
＜書　　式＞　dump interface INTERFACE pcap count <1-99999> (size <64-1518>|)
(filter {ssh|telnet|tcp880}|)

view(exec) mode

◆ clear l2tpv3 fdb
<説　　明>　L2TPv3のFDBテーブルをクリアします。
<書　　式>　clear l2tpv3 fdb　　(すべてのFDB情報を削除します)
clear l2tpv3 fdb local ethernet <0-2> (|vid <1-4094>)
clear l2tpv3 fdb forward
clear l2tpv3 fdb forward <gid:1-65535>
clear l2tpv3 fdb forward ethernet <0-2> (|vid <1-4094>)

◆ clear l2tpv3 counter
<説　　明>　L2TPv3のカウンターをクリアします。
<書　　式>　clear l2tpv3 counter ethernet <0-2> (|vid <1-4094>)
clear l2tpv3 counter peer
clear l2tpv3 counter peer A.B.C.D
clear l2tpv3 counter session <session-id:1-4294967295>
clear l2tpv3 counter tunnel <tunnel-id:1-4294967295>

◆ clear l2tpv3 counter access-list
<説　　明>　L2TPv3のアクセスリストカウンターをクリアします。
clear l2tpv3 counter access-list
clear l2tpv3 counter access-list interface (|INTERFACE)
clear l2tpv3 counter access-list xconnect (|<1-4294967295>)
clear l2tpv3 counter access-list
(root|layer2|ip|ipv6|arp|vlan|ieee802-3) (|WORD)
clear l2tpv3 counter access-list detail (root|layer2|vlan) (|WORD)

◆ clear l2tpv3 tunnel
<説　　明>　トンネルIDおよびセッションIDを指定して、L2TPv3トンネルを切断します。
<書　　式>　clear l2tpv3 tunnel <tunnel-id:1-4294967295> <session-id:1-4294967295>

◆ clear l2tpv3 remote-id
<説　　明>　リモートルータIDを指定して、L2TPv3を切断します。
<書　　式>　clear l2tpv3 remote-id <remote-id:A.B.C.D>

◆ clear l2tpv3 group
<説　　明>　グループIDを指定して、L2TPv3を切断します。
<書　　式>　clear l2tpv3 group <group-id:1-65535>

view(exec) mode

■ clear ip bgp

＜説　　明＞

・BGPセッションをリセットします。

・BGPの設定を変更した場合、即時には反映されないため、BGPセッションを一度リセットする必要があります。

- soft outリセット

  BGPネットワークやフィルタリングの変更などの経路情報は、BGPセッションを維持したまま適用することが出来ます。soft outリセットを行うと、設定を内部に反映し、BGP neighborへUPDATEメッセージを送信します。

- soft inリセット

  BGP neighborへROUTE-REFRESHメッセージを送信し、neighborへ全てのBGP経路情報を要求します。ROUTE-REFRESHメッセージを受信した場合は、UPDATEメッセージにより経路情報を送信します。

- hardリセット

  BGPのTCPセッションを一旦切断し、neighborを再確立します。keepaliveやholdtimeの設定を変更した場合は、ソフトリセットでは変更が反映されないためハードリセットを行ってください。
  ハードリセットを行う場合は、soft (in|out)を指定しません。

○ bgp *

＜書　　式＞　clear ip bgp *
　　clear ip bgp * soft (in|out)

＜備　　考＞　すべてのpeerとのセッションをリセットします。

○ bgp <AS:1-65535>

＜書　　式＞　clear ip bgp <AS:1-65535>
　　clear ip bgp <AS:1-65535> soft (in|out)

＜備　　考＞　AS番号を指定して、セッションをリセットします。

○ bgp A.B.C.D

＜書　　式＞　clear ip bgp A.B.C.D
　　clear ip bgp A.B.C.D soft (in|out)

＜備　　考＞　NeighborのIPアドレスを指定して、セッションをリセットします。

view(exec) mode

◆ clear arp
<説　　明>　ARPエントリをクリアします。
<書　　式>　clear arp A.B.C.D

◆ clear ipv6 neighbors
<説　　明>　IPv6ネイバーをクリアします。
<書　　式>　clear ipv6 neighbors X:X::X:X ethernet <0-2>
　　clear ipv6 neighbors X:X::X:X ethernet <0-2> vid <1-4094>
　　clear ipv6 neighbors X:X::X:X ethernet <0-2> vid <1-4094> <id:1-255>

◆ clear ppp
<説　　明>　指定したPPPセッションを切断します。
<書　　式>　clear ppp <0-4>

◆ clear l2tp
<説　　明>　指定したL2TPセッションを切断します。
<書　　式>　clear l2tp

◆ clear ipsec tunnel
<説　　明>　指定したIPsec tunnelを切断します。
<書　　式>　clear ipsec tunnel <tunnel_policy:1-65535>

◆ clear ipsec state
<説　　明>　指定したIPsec stateを削除します。
<書　　式>　clear ipsec state <state_number:1-4294967295>

◆ clear ip route cache
<説　　明>　IPルートキャッシュをクリアします。
<書　　式>　clear ip route cache

◆ clear ip access-list ACL-NAME fqdn
<説　　明>　FQDN形式のaccess-listを再設定します。
<書　　式>　clear ip access-list ACL-NAME fqdn

view(exec) mode

◆ clear ipv6 route cache
<説　　明>　IPv6ルートキャッシュをクリアします。
<書　　式>　clear ipv6 route cache

◆ clear ipv6 access-list ACL-NAME fqdn
<説　　明>　FQDN形式のaccess-listを再設定します。
<書　　式>　clear ipv6 access-list ACL-NAME fqdn

◆ clear ssh-public-key
<説　　明>　SSH公開鍵をクリアします。
<書　　式>　clear ssh-public-key user netconf <0-0>

◆ clear dns cache
<説　　明>　DNS cacheをクリアします。
<書　　式>　clear dns cache

◆ clear mobile <0-2>
<説　　明>　モバイルモジュールを手動リセットする機能です。
<書　　式>　clear mobile <0-2>

◆ clear ppp <0-4> mobile limitation
<説　　明>　mobile制限を解除します。
<書　　式>　clear ppp <0-4> mobile limitation
<備　　考>
・mobile limit (reconnect|time)で設定した再接続時間制限や接続時間制限を解除します（mobile limit (reconnect|time)の設定が削除されるわけではありません)。すぐに再接続したい状況等で使用します。

◆ clear netevent counter track <1-255>
<説　　明>　neteventのカウンタをクリアします。
<書　　式>　clear netevent counter track <object_id:1-255>
<備　　考>
・show netevent track <1-255> detailで表示されるHistory counterがクリアされます。

◆ clear route-map
<説　　明>　route-mapカウンタ(packet/byte数のカウンタ)をクリアします。
<書　　式>　clear route-map <NAME> counter

◆ clear class access-list
<説　　明>　class access-listカウンタ(packet/byte数のカウンタ)をクリアします。
<書　　式>　clear access-list <NAME> counter

view(exec) mode

◆ clear rollback
＜説　　明＞ ロールバックタイマを停止します。
＜書　　式＞ clear rollback

◆ cancel rollback
＜説　　明＞ ロールバックを無効にすることが出来ます。
＜書　　式＞ clear rollback
＜備　　考＞
・Rollback 有効の状態で config を復帰した後、システム再起動を行う前に、cancel rollback を実行することで、rollback を無効にすることが出来ます。
・システム再起動後、rollback timer が起動している状態で、cancel rollback を実行しても、rollback timer は停止しません。

view(exec) mode

■ terminal

○ length

＜説　　明＞　画面に表示する行数を指定します。
＜書　　式＞　terminal length <0-512>
＜初 期 値＞　terminal no length
＜備　　考＞　0を指定した場合は、画面単位での一時停止は行われません。

○ width

＜説　　明＞　画面に表示する列数を指定します。
＜書　　式＞　terminal width <40-180>
＜初 期 値＞　terminal no width (= terminal width 80)

■ connect

○ connect ppp

＜説　　明＞　PPPの接続を開始します。PPPのインタフェース番号を指定します。
＜書　　式＞　connect ppp <0-4>

○ reconnect ppp

＜説　　明＞　PPPの再接続を行います。PPPのインタフェース番号を指定します。
＜書　　式＞　reconnect ppp <0-4>

○ connect l2tp

＜説　　明＞　L2TPの接続を開始します。
＜書　　式＞　connect l2tp

○ connect l2tpv3

＜説　　明＞　L2TPv3の接続を開始します。
＜書　　式＞　connect l2tpv3 ethernet <0-2> (|A.B.C.D)
　　connect l2tpv3 ethernet <0-2> vid <1-4094> (|A.B.C.D)
＜説　　明＞　A.B.C.Dは、Remote Router-IDです。

○ connect ipsec

＜説　　明＞　IPsecの接続を開始します。IPsecのトンネルポリシー番号を指定します。
＜書　　式＞　connect ipsec <1-65535>

◆ disconnect

＜説　　明＞　ログインセッションを切断します。
＜書　　式＞　disconnect console　　(= console CLIからログアウトします。)
　　disconnect vty <VTY line_number:0-10>　(= SSH/Telnetセッションを切断します。)

view(exec) mode

◆ ping

＜説　　明＞　pingを実行します。
＜書　　式＞　ping ip (A.B.C.D | FQDN)
　　ping ipv6 (X:X::X:X | FQDN)
＜備　　考＞　引数を付けずにpingを実行した場合はインタラクティブモードになります。

vxr-x86#ping	入力可能なパラメータ
Protocol [ip]:	ip|ipv6
Target IP address:	A.B.C.D|X:X::X:X|FQDN
Repeat count [5]:	1-2147483647
Datagram size [100]:	36-18024
Interval in seconds [1]:	0-10
Extended commands [n]:	n(pingを実行)|y(インタラクティブモードを継続)
Source address or interface:	A.B.C.D|X:X::X:X|INTERFACE
Type of service [0x0]:	0x00-0xff
Set DF bit in IP header? [no]:	no|yes
Data pattern [0xABCD]:	0x0000-0xffff

◆ traceroute

＜説　　明＞　tracerouteを実行します。
＜書　　式＞　traceroute (icmp|icmpv6) (A.B.C.D|FQDN)
　　traceroute (ip|ipv6) (A.B.C.D|FQDN)
＜備　　考＞　引数を付けずにtracerouteを実行した場合はインタラクティブモードになります。

vxr-x86#traceroute	入力可能なパラメータ
Protocol [ip]:	ip|ipv6
Target IP address:	A.B.C.D|X:X::X:X|FQDN
Source address:	A.B.C.D|X:X::X:X
Numeric display [n]:	n|y
Timeout in seconds [2]:	0-3600
Probe count [3]:	1-65535
Maximum time to live [30]:	1-255
Port Number [33434]:	1025-65535

view(exec) mode

◆ ssh
<説　　明>　SSH接続を開始します。
<書　　式>
```
ssh (ip|ipv6) (A.B.C.D|X:X::X:X|FQDN) user USERNAME [(source A.B.C.D|X:X::X:X)]
ssh (ip|ipv6) (A.B.C.D|X:X::X:X|FQDN) user USERNAME version 1
      [cipher (3des|blowfish|des)] [(source A.B.C.D|X:X::X:X)]
ssh (ip|ipv6) (A.B.C.D|X:X::X:X|FQDN) user USERNAME version 2
      [cipher (3des-cbc|aes128-cbc|aes128-ctr|aes192-cbc
      |aes192-ctr|aes256-cbc|aes256-ctr|arcfour|arcfour128|arcfour256
      |blowfish-cbc|cast128-cbc)] [(source A.B.C.D|X:X::X:X)]
```
<備　　考>　ソースアドレスを指定することができます。

◆ telnet
<説　　明>　Telnet接続を開始します。
<書　　式>
```
telnet (A.B.C.D||X:X:X:X::X|FQDN) (|port PORT) user USER (|source A.B.C.D|X:X::X:X)
```
<備　　考>　ソースアドレスを指定することができます。

◆ logout
<説　　明>　CLIからログアウトします。
<書　　式>　logout

◆ get system statistics cpu
<説　　明>
・指定した間隔と回数で、CPU使用率を取得する機能です。
・コマンドを実行した時刻より、指定した間隔で指定した回数だけ、CPU使用率の計算・出力を行います。
<書　　式>
```
get system statistics cpu (all|total|<0-31>) <interval:1-86400> <count:1-65535>
```
<備　　考>　all:各CPUとトータルのCPU使用率を取得します。
　　total：トータルのCPU使用率を取得します。
　　CPU最大数は、システムに依存します。
<　例　>　実行例を下記に示します。
```
vxr-x86#get system statistics cpu total 1 3
 14:43:40    CPU#      %CPU      %user      %nice    %system      %idle    %iowait
 14:43:41     all      0.00       0.00       0.00       0.00      100.00       0.00
 14:43:42     all      0.00       0.00       0.00       0.00      100.00       0.00
 14:43:43     all      0.00       0.00       0.00       0.00      100.00       0.00
 AVERAGE      all      0.00       0.00       0.00       0.00      100.00       0.00
```

◆ reset
<説　　明>　モバイルモジュールを手動リセットする機能です。
<書　　式>　reset mobile <0-2>

view(exec) mode

■ debug/undebug

○ l2tpv3

<説　　明>　L2TPv3のデバッグログを出力します。
<書　　式>　debug l2tpv3 (|all|error|session|tunnel)
<　No　>　undebug l2tpv3 (|all|error|session|tunnel)　(= デバッグログの出力を停止します。)

○ netevent

<説　　明>　Neteventのデバッグログを出力します。
<書　　式>　debug netevent (|action|all|error|track)
<　No　>　undebug netevent (|action|all|error|track)　(= デバッグログの出力を停止します。)

○ ppp

<説　　明>　PPPのデバッグログを出力します。
<書　　式>　debug ppp
<　No　>　undebug ppp　(= デバッグログの出力を停止します。)

○ timer

<説　　明>　timerがtimeoutすると指定したcommandが実行されます。
<書　　式>　debug timer <1-5> <5-86400> interface ethernet <0-2> (shutdown|no shutdown)
　　debug timer <1-5> <5-86400> interface ppp <0-4> (connect|clear|reconnect)
<　No　>　undebug timer <1-5>　(=指定したIDのデバッグタイマーを解除します。)
<備　　考>

・interface ethernet <0-2> shutdown/no shutdown timerのtimeout時に、configuration modeに入っているUSERがいると実行エラーになります。シスログには、次のように表示されます。

```
cmd-timer: cmd-id 1 start
cmd-timer: cmd-id 1 error(VTY configuration is locked by other vty)
```

・正常に実行された場合のシスログは、次のように表示されます。

```
cmd-timer: cmd-id 1 start
cmd-timer: cmd-id 1 finished
```

view(exec) mode

◆ show version
＜説　　明＞　ファームウェアのバージョンを表示します。
＜書　　式＞　show version
　　show version flash (|<1-2>)

◆ erase flash
＜説　　明＞　フラッシュ上の全設定を消去します。
＜書　　式＞　erase flash

◆ delete flash
＜説　　明＞　ファイル名を指定して、フラッシュ上のファイルを消去します。
＜書　　式＞　delete flash FILENAME

◆ delete bootup-config
＜説　　明＞　bootup-config（起動時に使用する config の情報）を消去します。
＜書　　式＞　delete bootup-config

◆ copy config startup-config
＜説　　明＞　config を startup-config にコピーします。
＜書　　式＞　copy config startup-config (|all)
＜備　　考＞
・all 指定がない場合は、config のみ startup-config にコピーします。
・all 指定の場合は、config/ssh 鍵 /ipsec 証明書の全てを flash にコピーします（save config と同じです)。

◆ show temper
＜説　　明＞　本装置の温度状態および温度を表示します。
＜書　　式＞　show temperature
＜備　　考＞　vxr-x86#show temper
　　degrees: 41.5
　　status : normal

◆ sleep system
＜説　　明＞　sleep 状態へと遷移します。
＜書　　式＞　sleep system
　　sleep system timer <1-31536000>
　　sleep system schedule <NUM>
＜備　　考＞　timer を設定しない場合は、365 日間（31,536,000[sec]）が設定されます。
　　スケジュール機能で resume させる場合は、resume の schedule 番号を指定します。
　　sleep/resume についての詳細は、global mode を参照してください。

view(exec) mode

◆ show ip host

＜説　　明＞　IPアドレスとホスト名の組み合わせを表示します。

＜書　　式＞　show ip host

＜備　　考＞

・IPアドレスとホスト名の組み合わせは、ip host FQDN A.B.C.D（global mode）にて設定します。

view(exec) mode

◆ wol send name

＜説　　明＞　WOL（Wake On LAN：マジックパケット）を送信します。
　　送信するWOLは、あらかじめwol nameコマンド（global mode）で設定しておきます。
＜書　　式＞　wol send name WORD
＜備　　考＞　WORDには、wol nameコマンド（global mode）で設定した名前を指定します。

◆ wol send interface

＜説　　明＞　Ethernetフレームタイプの WOL（Wake On LAN：マジックパケット）を送信します。
＜書　　式＞　wol send interface INTERFACE HH:HH:HH:HH:HH:HH
　　ethernet (|<1-65535> <1-65535>) (|broadcast)
　　wol send interface INTERFACE HH:HH:HH:HH:HH:HH
　　ethernet type <1501-65535> (|<1-65535> <1-65535>) (|broadcast)
＜備　　考＞
・INTERFACEには、Ethernet、VLAN、Bridge（仮想スイッチ）を指定することが出来ます。
・HH:HH:HH:HH:HH:HHには、端末のMACアドレスを指定します。
・typeでは、Ethernet type（default:0x0842(2144)）を指定します。
・送信回数の初期値は1回、送信間隔の初期値は1秒です。
・broadcastを指定した場合、Ethernetヘッダの送信先MACアドレスに、FF:FF:FF:FF:FF:FFをセットします。指定しない場合は、端末のMACアドレスをセットします。

◆ wol send interface

＜説　　明＞　UDPパケットタイプの WOL（Wake On LAN：マジックパケット）を送信します。
＜書　　式＞　wol send ip (A.B.C.D|FQDN) H:H:H:H:H:H (|<1-65535> <1-65535>)
　　wol send ip (A.B.C.D|FQDN) H:H:H:H:H:H port <1-65535> (|<1-65535> <1-65535>)
＜備　　考＞
・送信先アドレスとして、IP アドレス、またはFQDN を指定します。IP アドレスには、端末のIP アドレスやdirected broadcast アドレスを指定します。
・HH:HH:HH:HH:HH:HH には、端末のMAC アドレスを指定します。
・Port には、送信先のUDP port 番号を指定します。初期値は、9（Discard）です。
・送信回数の初期値は1回、送信間隔の初期値は1秒です。
＜備　　考＞
・送信先IPアドレスが、同じネットワーク上にある場合
ユニキャストアドレスにWOLを送信する場合は、スタティックARPの設定を推奨します（sleep状態にある端末は、ARP 要求に応答しないため）。
・送信先IP アドレスが、別のネットワーク上にある場合
ルーティングテーブルに従って、WOLを送信します（通常は、ゲートウェイアドレスに対して、送信します。）

view(exec) mode

◆ show wlan
<説　　明>　無線インタフェースの情報を表示します。
<書　　式>　show wlan ssid WORD
　　show wlan staion ssid WORD
　　show wlan staion wlan <0-1>

◆ search-wifi
<説　　明>　周辺アクセスポイントの電波強度を表示します。
　　電波取得のため、wlan インタフェースは一時的に使用不可になります。
<書　　式>　search-wifi access-point

■ clear wlan deauth
<説　　明>　本装置がAP の場合、deauthentication を送信します(帰属関係を破棄します)。

○ ssid WORD
<説　　明>　SSID 単位で、deauthentication を送信します(帰属関係を破棄します)。
<書　　式>　clear wlan deauth ssid WORD

○ ssid WORD MAC
<説　　明>
・該当するSSID、かつ該当するMAC アドレスに対して、deauthentication を送信します(帰属関係を破棄します)。
<書　　式> clear wlan deauth ssid WORD HH:HH:HH:HH:HH:HH

○ wlan <0-1>
<説　　明> インタフェース単位で、deauthentication を送信します(帰属関係を破棄します)。
<書　　式> clear wlan deauth wlan <0-1>

○ wlan <0-1> MAC
<説　　明>
・該当するインタフェース、かつ該当するMAC アドレスに対して、deauthentication を送信します(帰属関係を破棄します)。
<書　　式> clear wlan deauth wlan <0-1> HH:HH:HH:HH:HH:HH

view(exec) mode

◆ shutdown system
<説　　明>　システムをシャットダウン（停止）します。
<書　　式>　shutdown system

◆ show cpu
<説　　明>　CPUについての情報を表示します。
<書　　式>　show cpu

◆ show config interface
<説　　明>　指定したインタフェースについての設定情報を表示します。
<書　　式>　show config interface ethernet <0-max>
　　show config interface ethernet <0-max> vid <1-4094>
　　show config interface ppp <0-4>
　　show config interface tunnel <0-65535>
　　show config interface loopback <0-9>
　　show config interface tap <0-127> (|vid <1-4094>)
<備　　考>　インタフェース数（max）は、使用する環境に依存します。

◆ connect lxc console
<説　　明>　起動中のLXCに、コンソール接続します。
　　LXCが停止中の場合、接続できません。
<書　　式>　connect lxc console
<備　　考>　アカウント：ubuntu、初期パスワード：ubuntuでログインします。
　　Ctrl+b qで、LXCコンソールをexitできます。

◆ restart lxc
<説　　明>　LXCを再起動します。
<書　　式>　restart lxc

◆ shutdown lxc
<説　　明>　LXCを停止します。
<書　　式>　shutdown lxc

◆ show lxc
<説　　明>　LXCの情報表示を行います。
<書　　式>　show lxc

view(exec) mode

◆ **show openflow interface bridge**

＜説　　明＞　openflow interface bridge（仮想スイッチ）の情報を表示します。

＜書　　式＞　show openflow interface bridge <0-4095>
show openflow interface bridge <0-4095> flows
show openflow interface bridge XX flows (10|11|12|13)
show openflow interface bridge <0-4095> summary

第5章

global mode

global mode

◆ 移行command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#
```

■ show

○ show config

＜説　　明＞　running-config(現在動作中の設定情報)を表示します。
＜書　　式＞　show config (|xml)

○ show startup-config

＜説　　明＞　startup-config(flashに保存されている設定情報)を表示します。
＜書　　式＞　show startup-config xml
＜備　　考＞　startup-configの表示は、XML形式のみ対応しています。

◆ hostname

＜説　　明＞　本装置のホスト名を設定します。
＜書　　式＞　hostname HOSTNAME
＜備　　考＞　設定したホスト名は、次のように表示されます。

```
vxr-x86(config)#hostname VXR01
VXR01(config)#
```

global mode

◆ fast-forwarding

＜説　　明＞　fast forwardingを有効にします.
＜書　　式＞　fast-forwarding enable　　（有効）
＜初 期 値＞　no fast-forwarding enable　（無効）
＜　no　＞　no fast-forwarding enable
＜備　　考＞

・以下のすべての条件を満たすパケットが、fast-forwardingの対象となります。
- Layer4 TCP/UDP/ESP
- Layer3 IPv4
- Layer2 Ethernet(VLAN/PPPoEを含む)

・上記の条件を満たす場合でも、次のパケットはfast-forwardingの対象外です。
- IPフォワーディングしないパケット（本装置自身で処理するパケット）
- Ethernetブロードキャスト/マルチキャストパケット
- IPv4ヘッダが20オクテットではないパケット（オプションには対応しません）
- ステートフルなプロトコルで、セッションコントロールに使用されるパケット（TCP SYNやFIN等）
- アプリケーションで使用されるコントロール用パケット（FTPコントロールやSIPのコントロール）

・また、次の場合もfast-forwardingの対象外です。
- IPフラグメントには対応していません。
- いずれかのインタフェースでQoSを有効にすると、fast-forwardingは自動的に無効になります。
- WiMAXインタフェースを対象とするIPフォワーディング時は、fast-forwardingは無効です。

・fast-forwarding のセッション最大数は、16,384です。
- fast-forwarding のセッション最大数に達している場合は、fast-forwarding セッションを新規作成しません。
- fast-forwarding とL2TPv3 fast-forwarding のセッションは、同一セッションテーブルで管理します。つまり、両方のセッション数の合計が、16,384を超えることはありません。
- L2TPv3 fast-forwarding については、global mode の l2tpv3 fast-forwarding コマンドを参照してください。

global mode

■ ip access-list

Access-List(ACL)によって、IPv4 packetのfilteringを行う条件定義を行います。Filtering時に設定可能なmatch条件とmatch時のactionは、以下の通りです。

○ match条件

IPv4 source address/netmask
IPv4 destination address/netmask
Protocol(既知のprotocol名指定と任意のprotocol番号入力)
Source port(TCP,UDPのみ。範囲指定可)
Destination port(TCP,UDPのみ。範囲指定可)
TCP syn
icmp type/code指定(icmp指定時のみ)
source mac address

○ match時の動作

permit　　許可されたpacketとしてacceptされます。
deny　　許可されていないpacketとしてdropされます。

＜書　　式＞

○ ip/protocol

```
ip access-list ACL-NAME (permit|deny)
      <source:>(any|A.B.C.D/M|A.B.C.D|FQDN)  <destination:>(any|A.B.C.D/M|A.B.C.D|FQDN)
      (|<protocol:0-255>|icmp|tcp|udp) (|mac HH:HH:HH:HH:HH:HH) [log (|WORD)]
```

○ icmp

```
ip access-list ACL-NAME (permit|deny)
      <source:>(any|A.B.C.D/M|A.B.C.D|FQDN)  <destination:>(any|A.B.C.D/M|A.B.C.D|FQDN)
      icmp (|type code) (|mac HH:HH:HH:HH:HH:HH) [log (|WORD)]
```

○ tcp/udp

```
ip access-list ACL-NAME (permit|deny)
      <source:>(any|A.B.C.D/M|A.B.C.D|FQDN)  <destination:>(any|A.B.C.D/M|A.B.C.D|FQDN)
      (tcp|udp) [(<sport:1-65535>|any|range <min:1-65535> <max:1-65535>)
      (<dport:1-65535>|any|range <min:1-65535> <max:1-65535>)] (|mac HH:HH:HH:HH:HH:HH)
      [log (|WORD)]
```

○ TCP option

```
ip access-list ACL-NAME (permit|deny)
      <source:>(any|A.B.C.D/M|A.B.C.D|FQDN) <destination:>(any|A.B.C.D/M|A.B.C.D|FQDN)
      tcp [(<sport:1-65535>|any|range <min:1-65535> <max:1-65535>)
      (<dport:1-65535>|any|range <min:1-65535> <max:1-65535>)] (|syn)
      (|mac HH:HH:HH:HH:HH:HH) [log (|WORD)]
```

○ negate

```
no ip access-list ACL-NAME
```

■ ip access-list（続き）

＜備　　考＞

・IPv4 と IPv6 の ACL は、別 table で管理されるため、ACL-NAME の重複が可能です。
・設定した ACL を有効化するには、ip access-group コマンド(interface/tunnel/ppp mode を参照)で、ACL をインタフェースに適用してください。
・log を指定すると、フィルタログ機能（syslog mode 参照）を有効にします。パケットが当該フィルタにマッチした場合、syslog に出力します。1 秒間に出力可能な log 数の最大値は「10」です。すべての ACL にログを設定すると、システムが高負荷状態になる可能性があるため、ログ出力は最小限にとどめるようにしてください。
・log を指定する場合に、タグを付与することが出来ます。フィルタログ出力時に、タグ情報が表示されます。

global mode

■ ipv6 access-list

Access-List(ACL)によって、IPv6 PacketのFilteringを行う機能です。Filtering時に設定可能なmatch条件とmatch時のactionは、以下の通りです。

○ match条件

IPv6 source address/prefix length
IPv6 destination address/prefix length
Protocol(既知のprotocol名指定と任意のprotocol番号入力)
Source port(TCP,UDPのみ。範囲指定可)
Destination port(TCP,UDPのみ。範囲指定可)
TCP syn
icmpv6 type/code指定(icmpv6指定時のみ)

○ match時の動作

permit　　許可されたpacketとしてacceptされます。
deny　　許可されていないpacketとしてdropされます。

＜書　　式＞

○ ip/protocol

```
ipv6 access-list ACL-NAME (permit|deny)
      <source:>(any|X:X::X:X/M|X:X::X:X|FQDN)  <destination:>(any|X:X::X:X/M|X:X::X:X|FQDN)
      (|<protocol:0-255>|icmpv6|tcp|udp) (|mac HH:HH:HH:HH:HH:HH) [log (|WORD)]
```

○ icmpv6

```
ipv6 access-list ACL-NAME (permit|deny)
      <source:>(any|X:X::X:X/M|X:X::X:X|FQDN) <destination:>(any|X:X::X:X/M|X:X::X:X|FQDN)
      icmpv6 (|type code) (|mac HH:HH:HH:HH:HH:HH) [log (|WORD)]
```

○ tcp/udp

```
ipv6 access-list ACL-NAME (permit|deny)
      <source:>(any|X:X::X:X/M|X:X::X:X|FQDN) <destination:>(any|X:X::X:X/M|X:X::X:X|FQDN)
      (tcp|udp) [(<sport:1-65535>|any|range <min:1-65535> <max:1-65535>)
      (<dport:1-65535>|any|range <min:1-65535> <max:1-65535>)] (|mac HH:HH:HH:HH:HH:HH)
      [log (|WORD)]
```

○ TCP option

```
ipv6 access-list ACL-NAME (permit|deny)
      <source:>(any|X:X::X:X/M|X:X::X:X|FQDN) <destination:>(any|X:X::X:X/M|X:X::X:X|FQDN)
      tcp [(<sport:1-65535>|any|range <min:1-65535> <max:1-65535>)
      (<dport:1-65535>|any|range <min:1-65535> <max:1-65535>)] (|syn)
      (|mac HH:HH:HH:HH:HH:HH) [log (|WORD)]
```

○ negate

```
no ipv6 access-list ACL-NAME
```

■ ipv6 access-list (続き)

＜備　　考＞

・IPv4 と IPv6 の ACL は、別 table で管理されるため、ACL-NAME の重複が可能です。
・設定した ACL を有効化するには、ipv6 access-group コマンド(interface/tunnel/ppp mode を参照)で、ACL をインタフェースに適用してください。
・log を指定すると、フィルタログ機能（syslog mode 参照）を有効にします。パケットが当該フィルタにマッチした場合、syslog に出力します。1 秒間に出力可能な log 数の最大値は「10」です。すべての ACL にログを設定すると、システムが高負荷状態になる可能性があるため、ログ出力は最小限にとどめるようにしてください。
・log を指定する場合に、タグを付与することが出来ます。フィルタログ出力時に、タグ情報が表示されます。

global mode

◆ ip route access-list

＜説　　明＞

route-mapのmatch条件であるmatch ip address設定をフィルタリングする際に使用します。具体的には、BGPのパス属性に関するset条件をフィルタリングする場合に使用します。また、BGPのdistribute-listによるルートフィルタリングにも使用します。

＜書　　式＞　ip route access-list ACL-NAME (permit|deny) A.B.C.D/M (|exact-match)
　　ip route access-list ACL-NAME (permit|deny) any

＜　no　＞　no ip route access-list ACL-NAME (permit|deny) A.B.C.D/M (|exact-match)
　　no ip route access-list ACL-NAME (permit|deny) any

＜備　　考＞

・exact-matchを指定した場合は、prefix長がMのときだけマッチします。exact-matchを指定しない場合は、prefix長がM以上(M～32)のときにマッチします。

・0.0.0.0/0 exact-matchは、default route(0.0.0.0/0)と同義です。0.0.0.0/0(exact-matchなし)は、anyと同義です。

◆ ipv6 route access-list

＜説　　明＞

route-mapのmatch条件であるmatch ipv6 address設定をフィルタリングする際に使用します。具体的には、BGPのパス属性に関するset条件をフィルタリングする場合に使用します。また、BGPのdistribute-listによるルートフィルタリングにも使用します。

＜書　　式＞　ipv6 route access-list ACL-NAME (permit|deny) X:X::X:X/M (|exact-match)
　　ipv6 route access-list ACL-NAME (permit|deny) any

＜　no　＞　no ipv6 route access-list ACL-NAME (permit|deny) X:X::X:X/M (|exact-match)
　　no ipv6 route access-list ACL-NAME (permit|deny) any

＜備　　考＞

・exact-matchを指定した場合は、prefix長がMのときだけマッチします。exact-matchを指定しない場合は、prefix長がM以上(M～128)のときにマッチします。

・::/0 exact-matchは、default routeと同義です。::/0(exact-matchなし)は、anyと同義です。

global mode

■ ip (snat|dnat)

＜説　　明＞　NATルールを追加します。
＜書　　式＞

○ ip

```
ip (snat|dnat) NAT-NAME ip
          <src:>(any|A.B.C.D/M|A.B.C.D) <dst:>(any|A.B.C.D/M|A.B.C.D)
          <to:A.B.C.D> (|to-end:E.F.G.H)
```

○ TCP/IP

```
ip (snat|dnat) NAT-NAME (tcp|udp)
     <src:>(any|A.B.C.D/M|A.B.C.D) (|<sport:1-65535>|any|range <min:1-65535> <max:1-65535>)
     <dst:>(any|A.B.C.D/M|A.B.C.D) (|<dport:1-65535>|any|range <min:1-65535> <max:1-65535>)
     <to:A.B.C.D> [(|to-end:E.F.G.H) (|<port:1-65535>|range <min:1-65535> <max:1-65535>)]
```

○ protocol

```
ip (snat|dnat) NAT-NAME <protocol:0-255>
     <src:>(any|A.B.C.D/M|A.B.C.D) <dst:>(any|A.B.C.D/M|A.B.C.D) <to:A.B.C.D> (|to-end:E.F.G.H)
```

＜備　　考＞　protocol番号でudp/tcp番号指定してもportは指定できません。
　　(文字列としてudp/tcpを指定してください)

○ static

```
ip (snat|dnat) NAT-NAME ip
     <src:>(any|A.B.C.D/M|A.B.C.D) <dst:>(any|A.B.C.D/M|A.B.C.D) static <to:>A.B.C.D/M
```

○ negate

```
no ip (snat|dnat) NAT-NAME
```

＜備　　考＞　NATルール（NAT-NAME全体）を削除します。

```
no ip (snat|dnat) NAT-NAME NAT-RULE
```

＜備　　考＞　NATルールを個別に削除します。
　　下記のように、削除したいNATルールを個別に指定します。
　　no ip snat test ip 192.168.0.0/24 any 1.1.1.1

＜設　定　例＞

○ snatの設定例: Private IPアドレス(192.168.0.0/24)をGlobal IP(1.1.1.1)アドレスに変換します。

```
ip snat test ip 192.168.0.0/24 any 1.1.1.1
```

○ dnatの設定例: 1.1.1.1:80宛てのパケットを192.168.1.1:880に転送します。

```
ip dnat test tcp any any 1.1.1.1 80 192.168.1.1 880
```

○ static snatの設定例:

```
ip snat test ip 192.168.0.0/24 192.168.10.0/24 static 192.168.10.0/24
```

たとえば、192.168.0.245から192.168.10.247への送信パケットは、SNATによりsrc IPが変換(192.168.0.245→192.168.10.245)されます。

global mode

■ system (snat|dnat)

＜説　　明＞　system snat、system dnat を設定します。

＜書　　式＞

○ system (snat|dnat)

```
system snat SNAT-NAME
system dnat DNAT-NAME
```

○ negate

```
no system (snat|dnat)
```

global mode

■ ip web-auth access-list

＜説　　明＞

Web 認証 filter を設定すると、ある特定の host や network、interface について、Web 認証せずに通信することが可能となります。

＜書　　式＞

○ ip/protocol

```
ip web-auth access-list ACL-NAME (permit|deny)
      <source:>(any|A.B.C.D/M|A.B.C.D|FQDN) <destination:>(any|A.B.C.D/M|A.B.C.D|FQDN)
      (|<protocol:0-255>|icmp|tcp|udp) (|mac HH:HH:HH:HH:HH:HH)
```

○ icmp

```
ip web-auth access-list ACL-NAME (permit|deny)
      <source:>(any|A.B.C.D/M|A.B.C.D|FQDN) <destination:>(any|A.B.C.D/M|A.B.C.D|FQDN)
      icmp (|type code) (|mac HH:HH:HH:HH:HH:HH)
```

○ tcp/udp

```
ip web-auth access-list ACL-NAME (permit|deny)
      <source:>(any|A.B.C.D/M|A.B.C.D|FQDN) <destination:>(any|A.B.C.D/M|A.B.C.D|FQDN)
      (tcp|udp) [(<sport:1-65535>|any|range <min:1-65535> <max:1-65535>)
      (<dport:1-65535>|any|range <min:1-65535> <max:1-65535>)] (|mac HH:HH:HH:HH:HH:HH)
```

○ TCP option

```
ip web-auth access-list ACL-NAME (permit|deny)
      <source:>(any|A.B.C.D/M|A.B.C.D|FQDN) <destination:>(any|A.B.C.D/M|A.B.C.D|FQDN)
      tcp [(<sport:1-65535>|any|range <min:1-65535> <max:1-65535>)
      (<dport:1-65535>|any|range <min:1-65535> <max:1-65535>)] (|syn) (|mac HH:HH:HH:HH:HH:HH)
```

○ negate

```
no ip web-auth access-list ACL-NAME
```

＜設　定　例＞

○ Web アクセスを許可: 192.168.0.10 から外部への Web アクセスを、Web 認証なしで許可します。

```
ip web-auth access-list FORWARD-IN permit any 192.168.0.10 tcp 80 any
ip web-auth access-list FORWARD-OUT permit 192.168.0.10 any tcp any 80
```

○ インターフェースへの適用: 上記の Web 認証フィルタを WAN 側インタフェースに適用します。

```
interface ethernet 1
 ip webauth-filter forward-in FORWARD-IN
 ip webauth-filter forward-out FORWARD-OUT
```

global mode

◆pppoe-option sent-padt
<説　　明>　PPPoEオプションを有効化します。
<書　　式>　pppoe-option sent-padt
　　(all|prev-pppoe-session|unknown-ip-packet|unknown-lcp-echo)
<初 期 値>　pppoe-option sent-padt all
<　no　>　no pppoe-option sent-padt
　　(|prev-pppoe-session|unknown-ip-packet|unknown-lcp-echo)

◆pppoe-bridge
<説　　明>　PPPoE bridgeを設定します。
<書　　式>　pppoe-bridge ethernet <0-2> ethernet <0-2>
<初 期 値>　no pppoe-bridge
<　no　>　no pppoe-bridge

◆dhcp-server
<説　　明>　DHCPサーバ機能で、固定IPアドレスを割り当てます。
<書　　式>　dhcp-server bind HH:HH:HH:HH:HH:HH A.B.C.D
<　no　>　no dhcp-server bind HH:HH:HH:HH:HH:HH

■ ssh-server
○ ssh-server enable
<説　　明>　SSHサーバの起動/停止を行います。
<書　　式>　ssh-server enable　　：起動
<初 期 値>　no ssh-server enable
<　no　>　no ssh-server enable　　：停止

○ ssh-server version
<説　　明>　SSHサーバのバージョンを選択します。
<書　　式>　ssh-server version 1|2　　：SSHv1 or SSHv2
　　ssh-server version 1 2　　：SSHv1 and SSHv2
<初 期 値>　ssh-serverversion 1 2
<　no　>　no ssh-server version (=ssh-server version 1 2)

○ ssh-server ciphers
<説　　明>　SSHの暗号化タイプを指定します。
<書　　式>　ssh-server ciphers (aes128-cbc|3des-cbc|blowfish-cbc|cast128-cbc|arcfour128|
　　arcfour256|arcfour|aes192-cbc|aes256-cbc|aes128-ctr|aes192-ctr|aes256-ctr|)
<備　　考>　複数指定可能です。
<　no　>　no ssh-server ciphers

■ ssh-server(続き)

○ ssh-server address-family

<説　　明>　SSHアクセスを許可するアドレスファミリー(IPv4/IPv6)を指定します。
<書　　式>　ssh-server address-family ip　　: IPv4 access only
　　ssh-server address-family ipv6　: IPv6 access only
<初 期 値>　no ssh-server address-family
<　no　>　no ssh-server address-family　　: any

○ ssh-server port

<説　　明>　SSHサーバのポート番号を指定します。ポート番号は2つまで指定することができます。
<書　　式>　ssh-server port (22|512-65535) (22|512-65535)
<初 期 値>　ssh-server port 22
<　no　>　no ssh-server port (=ssh-server port 22)

○ ssh-server authentication

<説　　明>　SSH にてアクセスする場合の認証方法は、plain-text password と RSA public-key をサポートします。
<書　　式>　ssh-server authentication (password|public-key)
<　no　>　no ssh-server authentication (password|public-key)
<備　　考>　Default では、password 認証、RSA 認証(ver1/ver2)共に有効です。

○ ssh-server public-key

<説　　明>　admin ユーザに対して、SSH 接続用公開鍵を設定します(最大 5 つまで設定可能)。
<書　　式>　ssh-server public-key username admin <0-4>
　　ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME (|source A.B.C.D|X:X::X:X)
　　ssh-server public-key username admin <0-4>
　　ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
　　ssh-server public-key username admin <0-4>
　　disk0:FILENAME (|source A.B.C.D|X:X::X:X)
<　no　>　no ssh-server public-key username admin <0-4>
<備　　考>
・ソースアドレスを指定することができます。
・SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合（ssh://user@A.B.C.D/FILENAME）は、22 番ポートを使用します（=ssh://user@A.B.C.D:22/FILENAME)。
- IPv4　ssh://user@A.B.C.D:port/FILENAME
- IPv6　ssh://[user@X:X::X:X]:port/FILENAME

○ssh-server vty authentication

<説　　明>　RSA 認証後に password 認証を行うことができる機能です。このpassword認証時は、IDは問い合わせされません。
<書　　式>　ssh-server vty authentication
<　no　>　no ssh-server vty authentication
<備　　考>　RSA public-key 認証機能使用時(ssh-server authentication public-key)のみ、有効にすることができます。初期値は無効です。

global mode

◆telnet-server enable
<説　　明>　Telnet サーバの起動 / 停止を行います。
<書　　式>　telnet-server enable　　(= 起動)
<初 期 値>　telnet-server enable
<　no　>　no telnet-server enable　　(= 停止)

■ http-server
○ enable
<説　　明>　HTTP サーバの起動 / 停止を行います。
<書　　式>　http-server enable　　(= 起動)
<初 期 値>　http-server enable
<　no　>　no http-server enable　　(= 停止)

○ ip access-filter
<説　　明>　本装置への Web アクセスを制限するための IPv4 ACL を設定します。
<書　　式>　http-server ip access-filter IPv4-ACL-NAME
<備　　考>　source IP のみチェックします。
<　no　>　no http-server ip access-filter

○ ipv6 access-filter
<説　　明>　本装置への Web アクセスを制限するための IPv6 ACL を設定します。
<書　　式>　http-server ipv6 access-filter IPv6-ACL-NAME
<備　　考>　source IP のみチェックします。
<　no　>　no http-server ipv6 access-filter

global mode

■ session

○ session udp timer

<説　　明>　UDPのセッションタイマーを設定します。
<書　　式>　session udp timer <sec:1-8589934>
<初 期 値>　session udp timer 30
<　no　>　no session udp timer(=session udp timer 30)

○ session udp-stream timer

<説　　明>　UDPストリームのセッションタイマーを設定します。
<書　　式>　session udp-stream timer <sec:1-8589934>
<初 期 値>　session udp-stream timer 180
<　no　>　no session udp-stream timer (=session udp-stream timer 180)

○session tcp timer

<説　　明>　TCPのセッションタイマーを設定します。
<書　　式>　session tcp timer <sec:1-8589934>
<初 期 値>　session tcp timer 3600
<　no　>　no session tcp timer (=session tcp timer 3600)

○session tcp time-wait

<説　　明>　TCPセッションのTIME_WAITタイマーを設定します。
<書　　式>　session tcp time-wait <1-85889934>
<初 期 値>　session tcp time-wait 120(sec)
<　no　>　no session tcp time-wait
<備　　考>
・TIME_WAIT状態とは、TCPのアクティブ・クローズ後のタイムアウト待ち状態のことです。
・TIME_WAITタイマーが短い場合、アクティブ・クローズ後に、ネットワーク上の遅延パケットが到着すると、リソース（シーケンス番号やポート番号）が衝突する可能性があります。
・TIME_WAITタイマーが長い場合、TIME_WAIT状態のセッションが、セッションテーブルに多数残留することが考えられます。

○session tcp fin-wait

<説　　明>　TCPセッションのFIN-WAIT状態のタイムアウト値(秒)を設定します。
<書　　式>　session tcp fin-wait <1-8589934>
<初 期 値>　session tcp fin-wait 180
<　no　>　no session tcp fin-wait (=session tcp fin-wait 180)

○session tcp last-ack

<説　　明>　TCPセッションのLAST-ACK状態のタイムアウト値(秒)を設定します。
<書　　式>　session tcp last-ack <1-85889934>
<　no　>　no session tcp last-ack

global mode

■ session (続き)

○session tcp close-wait
<説　　明>　TCPセッションのCLOSE-WAIT状態のタイムアウト値(秒)を設定します。
<書　　式>　session tcp close-wait <1-85889934>
<初 期 値>　session tcp close-wait 360 (=session tcp fin-wait 360)
<　no　>　no session tcp close-wait

○session tcp close
<説　　明>　TCPセッションのCLOSE状態のタイムアウト値(秒)を設定します。
<書　　式>　session tcp close <1-85889934>
<初 期 値>　session tcp close 10
<　no　>　no session tcp close (=session tcp close 10)

○session tcp syn-sent
<説　　明>　TCPセッションのSYN-SENT状態のタイムアウト値(秒)を設定します。
<書　　式>　session tcp syn-sent <1-85889934>
<初 期 値>　session tcp syn-sent 120
<　no　>　no session tcp syn-sent (=session tcp syn-sent 120)

○session tcp syn-recv
<説　　明>　TCPセッションのSYN-RECV状態のタイムアウト値(秒)を設定します。
<書　　式>　session tcp syn-recv <1-85889934>
<初 期 値>　session tcp syn-recv 60
<　no　>　no session tcp syn-recv (=session tcp syn-recv 60)

○ session max
<説　　明>　最大セッション数を設定します。
<書　　式>　session max <4096-65536>
<初 期 値>　session max 32768
<　no　>　no session max (=session max 32768)

○session limit
<説　　明>
・IP address毎にconntrack session数を制限する機能です。一部のUSERにより、conntrack sessionを占有されてしまうような障害を防ぐために使用します。
・この制限は、forwarding処理されるpacketが対象となります。
・0を設定すると、IP address毎のsession数を制限しません。
<書　　式>　session limit <0-65536>
<初 期 値>　session limit 0
<　no　>　no session limit

■ session (続き)

○session tcplimit

<説　　明>　本装置を端点とするTCPコネクションの接続数を制限する機能です。
<書　　式>　session tcp limit (<16-32768>|)
<初 期 値>　session tcp limit 640
<　no　>　no session tcp limit （=無制限）
<備　　考>

・本装置が他の端末にフォワーディングするものについては影響しません。
・IPv4/IPv6それぞれ別にカウントされます。例えば、接続数を16に設定した場合、 IPv4とIPv6のTCPコネクションを、それぞれ16まで接続することができます。
・また、設定変更を行った場合、すでに確立しているコネクションには影響しません。それ以降のコネクションが接続制限の対象になります。

○ session invalid-status-drop enable

<説　　明>

・本装置をpacketが通過すると、conntrack情報が作成されます。通常、statusはNEW state(新規作成)となり、その後双方向で通信が行われるとestablishとなります。
・不正なpacketと判定されるものを受信した際(ex. tcp通信においてsessionがない状態でRST+ackのpacketを受信した場合など)、stateがinvalidとなります。
・本機能は、このようなInvalid stateとなったsessionにmatchするpacketをdropする機能です。Defaultは、無効です。

<書　　式>　session invalid-status-drop enable
<初 期 値>　no session invalid-status-drop enable
<　no　>　no session invalid-status-drop enable
<備　　考>

・あるインタフェースに対してのみ適用するには、本機能は無効に設定して、かつ指定インタフェースでsession invalid-status-drop-interface enableを有効にします。以下は、ppp 0インタフェースに適用する場合の設定例です。

```
vxr-x86(config)#no session invalid-status-drop enable
vxr-x86(config)#interface ppp 0
vxr-x86(config-ppp)#session invalid-status-drop-interface enable
```

○session checksum

<説　　明>

・tcp/udp/icmp packetを転送する際、checksum errorが発生していた場合にNATの対象から外すかどうかを指定する機能です。
・無効な場合、checksum errorが検出されても、NAT(masquerade含む)が適用されます。

<書　　式>　session checksum enable
<初 期 値>　no session checksum enable
<　no　>　no session checksum enable
<備　　考>　Defaultは、無効です。ただし、ver5.6.1以前のversionでは有効となっています。

global mode

■ password

○password

＜説　　明＞　CLIへのログインパスワードを設定します。
＜書　　式＞　password (|hidden) PASSWORD
＜初 期 値＞　password admin
＜　no　＞　no password (= password admin)
＜備　　考 ＞　パスワードは、1-95文字以内で設定してください。
　　使用可能な文字は、英数字および!$#=*+-_.:;(){}[]^~@`<>です。

○gui password

＜説　　明＞　GUIへのログインパスワードを設定します。
＜書　　式＞　gui password (|hidden) PASSWORD
＜初 期 値＞　gui password admin
＜　no　＞　no gui password (= gui password admin)
＜備　　考 ＞　パスワードは、1-95文字以内で設定してください。
　　使用可能な文字は、英数字および!$#=*+-_.:;(){}[]^~@`<>です。

■ CLI

○ console idle-timeout

＜説　　明＞　Consoleのログアウトタイマーを設定します。
＜書　　式＞　console idle-timeout <minutes:0-35791> (|<seconds:0-2147483>)
＜初 期 値＞　console idle-timeout 0 3600
＜　no　＞　no console idle-timeout (=console idle-timeout 0 0)

○ console terminal length

＜説　　明＞　console画面に、一度に表示する行数を指定します。
＜書　　式＞　console terminal length <0-512>
＜初 期 値＞　console terminal length 24
＜　no　＞　no console terminal length (=console terminal length 24)
＜備　　考＞　0を指定した場合は、画面単位での一時停止は行われません。

○ console terminal width

＜説　　明＞　console画面に、一度に表示する列数を指定します。
＜書　　式＞　console terminal width <40-180>
＜初 期 値＞　console terminal width 80
＜　no　＞　no console terminal width (=console terminal width 80)

global mode

■ CLI (続き)

○ vty session-max

＜説　　明＞　vtyの最大セッション数を設定します。
＜書　　式＞　vty session-max <1-10>
＜初 期 値＞　vty session-max 4

○ vty idle-timeout

＜説　　明＞　 vtyのログアウトタイマーを設定します。
＜書　　式＞　vty idle-timeout <minutes:0-35791> (|<seconds:0-2147483>)
＜初 期 値＞　vty idle-timeout 0 600
＜　no　＞　no vty idle-timeout (=vty idle-timeout 0 0)

○ vty terminal length

＜説　　明＞　vtyに、一度に表示する行数を指定します。
＜書　　式＞　vty terminal length <0-512>
＜初 期 値＞　no vty terminal length
＜　no　＞　no vty terminal length
＜備　　考＞　Defaultでは、terminalのサイズに合わせて表示します。
　　0を指定した場合は、画面単位での一時停止は行われません。

○ vty ip access-filter

＜説　　明＞　vtyのIPv4アクセスフィルタを設定します。
＜書　　式＞　vty ip access-filter IPV4-ACL-NAME
＜　no　＞　no vty ip access-filter

○ vty ipv6 access-filter

＜説　　明＞　vtyのIPv6アクセスフィルタを設定します。
＜書　　式＞　vty ipv6 access-filter IPV6-ACL-NAME
＜　no　＞　no vty ipv6 access-filter

global mode

■ l2tp

＜説　　明＞　OCN IPv6サービスに接続する際に使用します。本装置自身から送出するPPPフレームを、L2TPトンネルを使用してLNS側にトンネリングする機能です。

○ udp source-port

＜説　　明＞

・一部の他社製ブロードバンドルータ配下に、本装置が設置されている状況で、L2TPトンネルを確立する場合、src portとしてUDP/1701を使用すると、L2TP/PPPセッションが確立できないという現象が確認されています。その対策として、L2TPで使用するsrc port 番号を変更する機能です。一方、dstポートはUDP/1701(固定)とします。

・なお、L2TPv3をUDP上で使用する場合、L2TPv3とL2TPにそれぞれ異なるport番号を設定してください。

＜書　　式＞　l2tp udp source-port <src_port:1024-65535>

＜初 期 値＞　l2tp udp source-port 40001

○ hostname

＜説　　明＞　L2TPのホスト名を設定します。

＜書　　式＞　l2tp hostname L2TP-HOSTNAME

＜ 備　　考 ＞　省略時は、hostnameコマンドで設定したものを使用します。

＜　 no 　＞　no l2tp hostname

global mode

■ L2TPv3

＜説　　明＞

・本装置にて実装するL2TPv3機能は、LAC-LAC間で確立したL2TPセッションを利用して、Ethernetフレームを透過的に転送することによりEnd-to-EndでのL2サービスを実現させる機能です。RFC3931に準拠しています。

・LAC-LACのみをサポートし、LAC-LNS、およびLNS-LNSモデルのサポートはしません(L2を終端することはできません)。

・L2TPv3パケットのカプセル化の方法としては、L2TPv3 over IP (プロトコル番号115)、およびL2TPv3 over UDPをサポートします。

・L2TP機能と同時に使用する場合は、L2TPv3とL2TPのUDPポート番号を異なる値に設定してください。

・その他の基本仕様については、下記のとおりです。

・L2TP(v2)との互換性はありません。

・L2TPv3 は、IPv4 でトンネルを確立します。IPv6 でのトンネル確立には対応していません。

・トンネリング可能なL2フレームタイプは、Ethernetフレーム(※)および802.1Q VLANのみです。また、Xconnect として指定可能なインタフェースは、Ethernet およびVLAN です。

※Ethernetフレームとは、Ethernet II, IEEE 802.3 Raw, IEEE 802.3 with LLC, IEEE 802.3 with SNAP のことです。

・透過するEthernet フレームサイズは、802.1Q in 802.1Q を考慮し、最大1522 バイト(FCS を除く)です。

・Cookie およびL2 Specific Sub layer には未対応です。

○ hostname

＜説　　明＞　本装置のホスト名を設定します。LCCE(L2TP Control Connection Endpoint)の識別に使用します。

＜書　　式＞　l2tpv3 hostname L2TPv3-HOSTNAME

＜備　　考＞　省略時は、hostnameコマンドで設定したものを使用します。

＜　no　＞　no l2tpv3 hostname

○ router-id

＜説　　明＞　本装置のルータIDを、IPアドレス形式で設定します。LCCEのルータIDの識別に使用します。

＜書　　式＞　l2tpv3 router-id A.B.C.D

＜　no　＞　no l2tpv3 router-id

global mode

○ mac-learning

＜説　　明＞

・L2TPv3 MAC アドレス学習機能の有効 / 無効を設定します。

- 本装置が受信したフレームの MAC アドレスを学習し、不要なトラフィックの転送を抑制する機能です。
- ブロードキャスト、マルチキャストについては、MAC アドレスに関係なく、すべて転送します。

＜書　　式＞　l2tpv3 mac-learning (|always) (|unique)

＜初 期 値＞　l2tpv3 mac-learning enable

＜　no　＞　no l2tpv3 mac-learning enable

＜備　　考＞

・always を指定すると、L2TPv3 MAC Address 学習 Always 機能を有効にします。

-L2TPv3 MAC Advertise Frame 送信機能を有効（mac-advertise enable）にした場合、アクティブセッションが作成されたときに、L2TPv3 MAC Advertise Frame を送信しますが、Xconnect に関連するセッションが 1 つも確立されていない場合は、ローカルテーブルにて MAC アドレスが学習されない為、ローカルテーブルに MAC アドレス情報が存在しません。

-Always を指定すると、セッションが 1 つも確立されていない場合でも、ローカルテーブルに MAC アドレス学習を行います。

- 本機能(always)はデフォルトで無効です。

・unique を指定すると、L2TPv3 MAC Address 学習 unique 機能を有効にします。

- 本機能を有効にするには、l2tpv3 xconnect mode で、次の設定が必要になります。
  vxr-x86(config-l2tpv3-xconnect)#mac-learning unique enable
- ネットワーク構成によっては、ある一つの Xconnect の Local Table、FDB に同じ MAC アドレスが登録されることがあります。本機能を有効にすると、新しく学習した MAC アドレスが、Local Table、FDB のどちらか一方に登録されるため、上記のような状態を回避することが出来ます。
- ある一つの Xconnect で、LoopDetect 機能と共存した場合、LoopDetect の FrameDrop 処理を優先します。つまり、この場合は、MAC アドレス学習 unique 機能は動作しないことになります。
- 本機能(unique)はデフォルトで無効です。

global mode

■ L2TPv3 (続き)

○ mac-aging

＜説　　明＞　本装置が学習したMACアドレスの保持時間を設定します。
＜書　　式＞　l2tpv3 mac-aging <seconds:30-1000>
＜初 期 値＞　l2tpv3 mac-aging 300
＜　no　＞　no l2tpv3 mac-aging (=l2tpv3 mac-aging 300)

○ loop-detect

＜説　　明＞　ループ検出機能を有効にします。
＜書　　式＞　l2tpv3 loop-detect enable
＜初 期 値＞　no l2tpv3 loop-detect enable
＜　no　＞　no l2tpv3 loop-detect enable
＜備　　考＞
フレームの転送がループしてしまうことを防ぐ機能です。この機能が有効になっているときは、以下の2つの場合にフレームの転送を行いません。
・Xconnectインタフェースより受信したフレームの送信元MACアドレスがFDBに存在するとき。
・L2TPセッションより受信したフレームの送信元MACアドレスがローカルMACテーブルに存在するとき。

○ send-known-unicast

＜説　　明＞　L2TPv3のknown unicastフレームを送信します。
＜書　　式＞　l2tpv3 send-known-unicast enable
＜初 期 値＞　no l2tpv3 send-known-unicast enable
＜　no　＞　no l2tpv3 send-known-unicast enable
＜備　　考＞
known unicastフレームとは、MACアドレス学習済みのunicastフレームのことです。この機能を「無効」にしたときは、以下の場合にunicastフレームの転送を行いません。
・Xconnectインタフェースより受信したUnicastフレームの送信先MACアドレスがLocal MACテーブルに存在するとき。

○ udp source-port

＜説　　明＞　L2TPv3 over UDPを使用時のsrc port番号を指定することができます。
＜書　　式＞　l2tpv3 udp source-port <1024-65535>
＜初 期 値＞　l2tpv3 udp source-port 1701
＜　no　＞　no l2tpv3 udp source-port (=l2tpv3 udp source-port 1701)
＜備　　考＞　Src port番号の変更を行った場合、L2TPv3 over UDPを使用しているtunnelでは再接続が発生します。L2TPv3 over IPのトンネルおよびセッションへの影響はありません。

■ L2TPv3（続き）

○ udp path-mtu-discovery

＜説　　明＞　L2TPv3 over UDP使用時に、Path MTU Discovery機能の有効/無効を設定します。
初期値は無効です。

＜書　　式＞　l2tpv3 udp path-mtu-discovery enable

＜初 期 値＞　no l2tpv3 udp path-mtu-discovery enable

＜　no　＞　no l2tpv3 udp path-mtu-discovery enable

＜備　　考＞　本機能を有効にした場合、送信するL2TPv3パケットのDF(Don't Fragment)ビットを1にします。無効にした場合は、DFビットを常に0にします。ただし、カプセル化したフレーム長が送信インタフェースのMTU値を超過する場合は、本設定に関係なくフラグメントされ、DFビットを0にして送信します。

○ path-mtu-discovery

＜説　　明＞　L2TPv3 over IP使用時に、Path MTU Discovery機能の有効/無効を設定します。
初期値は無効です。

＜書　　式＞　l2tpv3 path-mtu-discovery enable

＜初 期 値＞　no l2tpv3 path-mtu-discovery enable

＜　no　＞　no l2tpv3 path-mtu-discovery enable

○ snmp enable

＜説　　明＞　L2TPv3用のSNMPエージェント機能を有効にします。本機能を有効にすると、L2TPv3に関するMIBの取得が可能になります。

＜書　　式＞　l2tpv3 snmp enable

＜初 期 値＞　no l2tpv3 snmp enable

＜　no　＞　no l2tpv3 snmp enable

○ snmp trap

＜説　　明＞　L2TPv3のSNMP trap機能を有効にします。本機能を有効にすると、L2TPv3に関するTrap通知が可能になります。

＜書　　式＞　l2tpv3 snmp trap

＜初 期 値＞　no l2tpv3 snmp trap

＜　no　＞　no l2tpv3 snmp trap

○ tos

＜説　　明＞

・L2TPv3にてトンネリングされるフレームのL3プロトコルがIPまたはIPv6の場合に、IP/IPv6 headerのToS値(IPv6の場合、traffic class)やUSERが指定したToS値をl2tpv3パケットのIP headerのIPv4 ToS field(L2TPv3 session packet)に設定する機能です。Control messageは、0xd0で送られます。

＜書　　式＞　l2tpv3 tos enable

＜初 期 値＞　no l2tpv3 tos enable

＜　no　＞　no l2tpv3 tos enable

＜備　　考＞

・ToS設定機能有効時は、l2tpv3 tunnel tosコマンドを使用して、Control messageのToS値も指定することができます。

global mode

■ L2TPv3（続き）

○ tunnel tos

＜説　　明＞　L2TPv3 ToS設定機能有効時に、Control messageのToS値を指定することが出来ます。
＜書　　式＞　l2tpv3 tunnel tos [|<0-252>]
＜初 期 値＞　l2tpv3 tunnel tos 208 (=l2tpv3 tunnel tos)
＜　no　＞　no l2tpv3 tunnel tos
＜備　　考＞

・L2TPv3 ToS 設定機能の有効 / 無効とコントロールメッセージの ToS 値の関係は、次のとおりです。

L2TPv3のToS設定機能		コントロールメッセージのToS値	
無効	no l2tpv3 tos	固定値	0x0
有効	l2tpv3 tos	初期値 設定範囲	208（0xd0） 0-252（0x0-0xfc）

○ fast-forwarding

＜説　　明＞　L2TPv3にて、fast-forwardingを有効にします。
＜書　　式＞　l2tpv3 fast-forwarding enable
＜初 期 値＞　no l2tpv3 fast-forwarding enable
＜　no　＞　no l2tpv3 fast-forwarding enable
＜備　　考＞

・fast-forwardingの対象となるのは、送信元 / 送信先のMACアドレスがユニキャストのフレームです。
　- MACアドレスがマルチキャスト / ブロードキャストのフレームは、fast-forwardingの対象外です。
　- システムのfast-forwardingとは異なり、プロトコル（IPv4/TCP/UDP等）には依存しません。
・フラグメントされたL2TPv3パケット（再構築を必要とするパケット）を受信した場合は、fast-forwardingの対象外です（システムのfast-forwardingと同様です）。
・フラグメントパケットの送信時（本装置がフラグメントする場合）は、L2TPv3 tunnelingおよびL2TPv3 over IPsec（policy base）に限り、fast-forwardingの対象となります。
　- L2TPv3 over IPsec（route base)は、fast-forwardingの対象外です。
・以下の条件に当てはまる場合に、該当するL2TPv3フレームをfast-forwardingします。
　※ L2TPv3がMACアドレスを保持するテーブルは2種類あり、LAN側がlocal table、WAN側がFDBです。
　- L2TPv3フレーム送信時、受信フレームの送信先MACアドレスがFDBに存在する場合に、上りのfast-forwardingセッションを作成します。
　- L2TPv3フレーム受信時、受信フレームの送信先MACアドレスがlocal tableに存在する場合に、下りのfast-forwardingセッションを作成します。
　- L2TPv3フレーム受信時、受信フレームの送信先MACアドレスがFDBに存在する場合に、(WAN-WAN折り返しの）fast-forwardingセッションを作成します。ただし、同じセッション（グループ）には、折り返しません。
　※ 片方向通信の場合、local tableもしくはFDBに該当MACが存在し、片方向のfast-forwardingセッションを作成しますが、MAC aging-timeのタイムアウトが発生すると、local tableもしくはFDBから該当MACが存在しなくなるため、その後はfast-forwardingの対象外となります。

global mode

■ L2TPv3

○ fast-forwarding（続き）

＜備　　考＞

・fast-forwardingとL2TPv3 fast-forwardingのセッションは、同一セッションテーブルで管理します。つまり、両方のセッション数の合計が、16,384を超えることはありません。

・ fast-forwardingについては、global modeのfast-forwardingコマンドを参照してください。

＜注　　意＞

※本機能を有効にする場合は、次の順に設定してください。

①システムのfast-forwardingを有効にします（defaultは無効です）。

```
vxr-x86(config)# fast-forwarding enable
```

②L2TPv3のMACアドレス学習機能を有効にします（defaultは有効です）。

```
vxr-x86(config)# l2tpv3 mac-learning
```

③L2TPv3のfast-forwardingを有効にします（defaultは無効です）。

```
vxr-x86(config)# l2tpv3 fast-forwarding enable
```

※CLIからの設定で整合性が取れない場合は、本機能を有効にすることが出来ません。show configの結果をコピー＆ペーストするような場合は、設定の順序に気を付けてください。

○システムのfast-forwardingが無効時に、L2TPv3のfast-forwardingを有効にした場合

```
vxr-x86(config)#l2tpv3 fast-forwarding enable
% First configure "fast-forwarding enable" on global mode.
```

○L2TPv3のfast-forwardingが有効時に、L2TPv3のMACアドレス学習機能を無効にした場合

```
vxr-x86(config)#no l2tpv3 mac-learning
% First deconfigure "l2tpv3 fast-forwarding enable" on global mode.
```

global mode

■ L2TPv3

○ fast-forwarding（続き）

＜　例　＞

●PtoP 上り / 下り

VXR_1 で fast-forwarding のエントリーを追加するときのフレームの流れは、次のとおりです。なお、PC_A と PC_B は、同一ネットワーク上に存在します。

```
PC_A ----- VXR_1 =====L2TPv3===== VXR_2 ----- PC_B
```

○ PC_A から PC_B に対して ping を実行します。

① PC_A から ARP REQUEST をブロードキャストで送信します。
VXR_1 は、local table に PC_A の MAC アドレスを登録します。

② PC_B から PC_A に、ARP REPLY を送信します。
VXR_1 は、FDB に、PC_B の MAC アドレスを登録します。
PC_A の MAC アドレスが、local table 上に登録されているので、fast-forwarding のエントリー（下り）を追加します。

③ PC_A から PC_B に、ICMP REQUEST を送信します。
PC_B の MAC アドレスが FDB 上に登録されているので、fast-forwarding のエントリー（上り）を追加します。

④ PC_B から PC_A に、ICMP REPLY を送信します。
Fast-forwarding のエントリーに登録されているので、fast-forwarding します。

⑤ PC_A から PC_B に、ICMP REQUEST を送信します。
Fast-forwarding のエントリーに登録されているので、fast-forwarding します。

●PtoMP 折り返し

VXR_1 で fast-forwarding のエントリーを追加するときのフレームの流れは、次のとおりです。なお、PC_A と PC_B と PC_C は、同一ネットワーク上に存在します。

```
PC_C ----- VXR_1 =====L2TPv3===== VXR_2 ----- PC_A
                    =====L2TPv3===== VXR_3 ----- PC_B
```

○ PC_A から PC_B に対して ping を実行します。

① PC_A から ARP REQUEST をブロードキャストで送信します。
VXR_1 は、VXR_2 向きの FDB に、PC_A の MAC アドレスを登録します。

② PC_B から PC_A に、ARP REPLY を送信します。
VXR_1 は、VXR_3 向きの FDB に、PC_B の MAC アドレスを登録します。
PC_A の MAC アドレスが、VXR_2 向きの FDB 上に登録されているので、fast-forwarding のエントリー（折り返し）を追加します。

③ PC_A から PC_B に、ICMP REQUEST を送信します。
PC_B の MAC アドレスが、VXR_3 向きの FDB 上に登録されているので、fast-forwarding のエントリー（折り返し）を追加します。

④ PC_B から PC_A に、ICMP REPLY を送信します。
Fast-forwarding のエントリーに登録されているので、fast-forwarding します。

⑤ PC_A から PC_B に、ICMP REQUEST を送信します。
Fast-forwarding のエントリーに登録されているので、fast-forwarding します。

global mode

■ IPv4

◆ arp

＜説　　明＞　スタティックARPを設定します。
＜書　　式＞　arp A.B.C.D HH:HH:HH:HH:HH:HH
＜　no　＞　no arp A.B.C.D
＜備　　考＞

- Static ARPで設定されている場合は、Gratuitous ARPでARP情報が書き換わることはありません。
- 1つのHWアドレスを複数のIPv4アドレスに対応づけることは可能ですが、1つのIPv4アドレスに複数のHWアドレスを対応付けることは出来ません。

◆ ip route

＜説　　明＞　IPv4のスタティックルートを設定します。
＜書　　式＞　ip route A.B.C.D/M (<gateway:E.F.G.H>|INTERFACE|null) (tag <1-65535>)
(|<distance:1-255>) (|netevent <trackid:1-255> (active|inactive))
指定可能なINTERFACEは、以下のとおりです。
ethernet <0-2> (|vid <1-4094>) | ppp <0-4> | tunnel <0-255>
＜　no　＞
no ip route (A.B.C.D/M GATEWAY|INTERFACE|null) (|<distance:1-255>) (tag <1-65535>)
＜備　　考＞

- 同じ宛先に対して複数の経路が存在する場合、distance値によって経路の重みづけが行われ、使用する経路が決定されます。同じ宛先に対して複数の経路が選択される場合は、round robinによるバランシングが行われます。
- 255に設定された経路は無効です。
- なお、マルチアクセスネットワーク(ethernetや802.1Q VLAN)に対して、スタティックルートを設定する場合、インタフェース名のみの指定を行うとパケットのフォワーディングが正常にできなくなる(ARP解決を行うために同じLAN内の機器でProxy ARP機能を有効にする必要あり)ことがあります。このため、Point-to-Pointインタフェース以外では、インタフェース名の指定によるスタティックルート設定は推奨しません。
- スタティックルート情報にtagを設定することが出来ます。route-map情報と関連付けることで、RIP/OSPFでtagに基づくスタティックルートの再配信を実行することが出来ます。

＜　null　＞

- nullインタフェースは、実際には存在しないインタフェースで、IPアドレスを割り当てることは出来ません。
- nullインタフェースでは、up/downが発生しないため、（実際のrouteの有無に関係なく）常にrouteを有効にすることが出来ます。したがって、常にルーティングプロトコルで配信されるため、常に本装置経由での通信を行うことが出来ます（他のルータを介した通信を防ぐことが出来ます）。
- このインタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません（dropします）。本装置からパケットの出力を行う場合は、nullインタフェースよりも、distance値を小さく設定するようにしてください。
- ip route/ipv6 routeコマンドで、指定することが出来ます。

global mode

◆ ip icmp-errors-inbound

＜説　　明＞　この機能を有効にすると、ICMP error messageを送信する際、ICMP errorの原因となったpacketを受信したinterfaceのprimary addressで送信されます。
＜書　　式＞　ip icmp-errors-inbound
＜初 期 値＞　no ip icmp-errors-inbound
＜　no　＞　no ip icmp-errors-inbound
＜備　　考＞

- Defaultは、無効です。無効の場合は、routing tableにより決められた出力インタフェースのprimary addressで送信されます。
- ICMP error messageがIPsec化されてしまう場合などに有効にすると、packetを受信したインタフェースから出力することができるようになります。

◆ ip arp-invalid-log

＜説　　明＞　Ethernet/VLAN interfaceにおいて、受信したinterfaceのIPv4 networkと異なるIPv4 addressのarp requestを受信した際に、syslog出力する機能です。初期値は無効です。
＜書　　式＞　ip arp-invalid-log
＜初 期 値＞　no ip arp-invalid-log
＜　no　＞　no ip arp-invalid-log
＜備　　考＞　Invalid arpを受信した際には、下記のようなlogがsyslogに出力されます。なお、この機能を有効にした場合、messageが大量に出力される場合があるため、「Syslog message suppress機能(syslog mode参照)」を有効にすることを推奨します。

```
<< Invalid arp受信 log format >>
Jun 16 18:21:06 vxr-x86 arp_detect: received invalid arp on ethernet0 from 10.10.1.143
      (00:90:fe:12:48:8c) to 10.10.1.110

ethernet0 : 受信したinterface
10.10.1.143 : arp requestのsender IP
00:90:fe:12:48:8c : sender mac address
10.10.1.110 : Target IP address
```

global mode

■ IP martian-log機能

・Source/destination IPアドレス、あるいは、ARP sender IP/target IPが、martianアドレスであるIPv4パケット/ARPパケットを受信した際に、ログを出力します。
・martianパケットの判定は、ルーティングテーブルの探索時に行います。martianパケットであると判断した場合は、ログを出力して、パケット（フレーム）を破棄します。
※ただし、martianパケットであっても、ip martian-log以外のチェックで破棄した場合は、ログを出力しません。
-Target IPが、127.0.0.0/8、マルチキャストアドレス、ブロードキャストアドレスのパケットは、ARP処理時に破棄するため、martian-logは出力しません。
-Source/destination共に、0.0.0.0のパケットは、ルーティングテーブル探索の前に、不正パケットとして破棄します。

□ Martianアドレス判定処理

○ martian source

Sourceアドレス、またはARP sender IPが、不正なアドレスと判断した場合に出力します。なお、martian-log出力時、受信したフレームに、MACヘッダ情報がある場合、MACヘッダの情報も出力します。

・マルチキャストアドレス
・ループバック（127.0.0.1）や0.0.0.0など使用不可のアドレス
・ARPを受信したインタフェースのIPとsender IPが同じアドレス
・受信したIPパケットのsource IPが、本装置のIPと同じアドレス（ループパケット）
ただし、ip nat-loopbackの適用パケット（source/destination IPが同じパケット）を受信した場合は、martian-logは出力せず、転送処理を行います。

○ martian destination

受信したIPパケットのdestination IPが、ループバック（127.0.0.1）や0.0.0.0など使用不可のアドレス

◆ ip martian-log

＜説　　明＞　IP martian-log機能を有効にします。
＜書　　式＞　ip martian-log　　（有効）
＜初 期 値＞　no ip martian-log　　（無効）
＜　no　＞　no ip martian-log
＜備　　考＞
・パケット毎にログを出力すると、システムに非常に負荷がかかり、DoS攻撃etcによってサービス停止状態になる可能性があります。そのため、単位時間当たりに出力可能なログの数を制限しています。
・5秒間に出力可能なログの数は、最大10です（設定の変更は出来ません）。
・出力できなかったログは、その後のログ出力時に、supress message数としてログ出力します。

global mode

◆ip reassemble-output

＜説　　明＞

・インタフェースのMTU（あるいはPMTU）より大きいパケットをIP forwardingする際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。本設定有効時、本装置がリアセンブルしたパケットは、以下のようにフラグメント処理を行います。

- fragmented packet(パケットの断片)がMTUを超える場合、リアセンブルしたパケットを再度MTUサイズにフラグメントして出力します。
- fragmented packet(パケットの断片)がMTUより小さい場合、受信したfragmented packetのサイズで出力します。
- パケット全体のサイズがMTUより小さい場合、リアセンブルしたパケットを出力します。

＜書　　式＞　ip reassemble-output

＜初 期 値＞　ip reassemble-output

＜　no　＞　no ip reassemble-output

＜備　考１＞

・上記の場合（本設定が有効の場合）、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易なIP実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズで本装置　　からパケットを出力します。また、出力時のIPフラグメント処理は、次のようになります。

- fragmented packet(パケットの断片)がMTUを超える場合、受信したfragmented packetをMTUサイズにフラグメントして出力します。
- fragmented packet(パケットの断片)がMTUより小さい場合、受信したfragmented packetのサイズで出力します。
- パケット全体のサイズがMTUより小さい場合、受信したfragmented packetをそのままのサイズで出力します。

・Defaultは、global設定およびinterface設定ともに有効です。Global設定とinterface設定のAND条件により、本機能が有効か無効かを判定します。本設定は、IP forwardingするパケットにのみ影響します。

・受信時のサイズを記載しておくバッファが32 個しかないため、33 個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-output が有効な場合と同様に処理します。

＜備　考２＞

・global modeで「no ip reassemble-output」を設定し、ipsec tunnel interfaceで「no ip fragment-reassembly」を設定した場合には「no ip fragment-reassembly」が優先されます。
この場合、「no ip fragment-reassembly」が設定されたtunnle interfaceで受信したパケットは、reassembleせずに転送しますが、conntrackによるセッション管理の対象から外れるため、conntrackを利用した機能（NAT機能/SPI/sessionコマンドによる各機能）が使用できなくなる他、フィルタリングやpacket coloringの使用にも制限が出ます。

・「no ip reassemble-output」を設定する場合は、全てのtunnel interfaceの「no ip fragment-reassembly」を「ip fragment-reassembly」に設定してから行って下さい。
(no ip fragment-reassemblyが設定されている場合は、Warningが出力されます。)

・ip fragment-reassemblyは、将来的に廃止を予定しているため、なるべくip reassemble-outputを使用するようにしてください。

global mode

■ ip local pool

○ address

＜説　　明＞　IPアドレスプールを設定します。
＜書　　式＞　ip local pool WORD address A.B.C.D (|A.B.C.D)
＜　no　＞　no ip local pool WORD

○ exclude-address

＜説　　明＞　IPアドレスプールの対象外となるIPアドレス（またはIPアドレス範囲）を設定します。
＜書　　式＞　ip local pool WORD exclude-address A.B.C.D (|A.B.C.D)
＜　no　＞

・exclude-addressの全削除　no ip local pool WORD exclude-address
・指定対象のみ削除　no ip local pool WORD exclude-address A.B.C.D (|A.B.C.D)

global mode

■ IPv6

◆ ipv6 forwarding

＜説　　明＞　IPv6パケットのフォワーディングの有効（IPv6ルータとして動作）/無効（ホストとして動作）を設定します。
＜書　　式＞　ipv6 forwarding
＜初 期 値＞　no ipv6 forwarding
＜　no　＞　no ipv6 forwarding
＜備　考1＞　IPv6 forwardingが有効の場合の動作
・Neighbor AdvertisementのIsRouter flagをセットします。
・Router Solicitationは送信しません。
・Redirectsは受信しません（無視します）。
＜備　考2＞　IPv6 forwardingが無効の場合の動作
・Neighbor AdvertisementのIsRouter flagをセットしません。
・必要な場合、Router Solicitationを送信します。
・Redirects受信が有効な場合、redirectsを受け入れることができます。

◆ ipv6 neighbor

＜説　　明＞　ipv6のスタティックネイバーを設定します。
＜書　　式＞　ipv6 neighbor X:X::X:X HH:HH:HH:HH:HH:HH ethernet <0-2> (|vid <1-4094>)
＜　no　＞　no ipv6 neighbor X:X::X:X ethernet <0-2> (|vid <1-4094>)

◆ ipv6 route

＜説　　明＞　ipv6スタティックルートを設定します。
＜書　　式＞　ipv6 route X:X::/M GATEWAY (|<distance:1-255>)
ipv6 route X:X::/M INTERFACE (|<distance:1-255>)
ipv6 route X:X::/M GATEWAY INTERFACE (|<distance:1-255>)
＜　no　＞　no ipv6 route X:X::/M GATEWAY (|<distance:1-255>)
no ipv6 route X:X::/M INTERFACE (|<distance:1-255>)
no ipv6 route X:X::/M GATEWAY INTERFACE (|<distance:1-255>)
＜　null　＞
・nullインタフェースは、実際には存在しないインタフェースで、IPアドレスを割り当てることは出来ません。
・nullインタフェースでは、up/downが発生しないため、（実際のrouteの有無に関係なく）常にrouteを有効にすることが出来ます。したがって、常にルーティングプロトコルで配信されるため、常に本装置経由での通信を行うことが出来ます（他のルータを介した通信を防ぐことが出来ます）。
・このインタフェースを出力インタフェースとして設定した場合、パケットが出力されることはありません（dropします）。本装置からパケットの出力を行う場合は、nullインタフェースよりも、distance値を小さく設定するようにしてください。
・ip route/ipv6 routeコマンドで、指定することが出来ます。

global mode

◆ ipv6 bridge

＜説　　明＞　フレッツドットネットで、ISP(フレッツ網) 側より送信されてくる IPv6 パケットをブリッジする機能です。ブリッジを行うインタフェースは、イーサネットのみ指定することができます。

＜書　　式＞　ipv6 bridge ethernet <0-2> ethernet <0-2>

＜　no　＞　no ipv6 bridge

＜備　　考＞

・IPv6 ブリッジを有効にすると、本装置宛の IPv6 パケットは本装置にて処理されます。

・non-unicast や本装置宛以外の IPv6 パケットはブリッジされます(non-unicast フレームは、本装置で処理され、かつブリッジもされます)。

global mode

■ track

＜説　　明＞

・Netevent の track object を設定します。なお、Netevent の詳細については、「付録 E Netevent 機能」を参照してください。

＜備　　考＞

○ delay/retry

・復旧時(event up と判別した場合)から実際に up 時の action を実行するまでに delay を設定することができます。Delay timer が動作している場合は、track は down state が維持され、この間にも ip reachability check は動作し続けます。

・Delay timer 動作中に event down を(retry 回数)検知した場合、delay timer は cancel されます。

・Delay timer が timeout すると、event up の action が実行されます。このとき、delay timer 中にカウントした ip reachability fail count は 0 にクリアされ、action 実行後に再度 reachability check が開始されます。

○ initial-timeout

・OSPF/BGP4 の neighbor 監視および interface link 監視設定時、初期の track 状態は init です。新規に track が設定されると、現在の状態を取得します。

・neighbor が確立(あるいは interface link up)状態と判断されると track up 状態となります。

・neighbor が確立されていない(あるいは interface link down)状態の場合、すぐに track down 状態とはなりません。この場合は、initial timeout が timeout するか、OSPF/BGP4 機能 / interface 状態監視機能によって down の状態変化通知があったときに、track down として判断し、down action を実行します。

・Initial timeout は、default で無効です。有効時の default の initial timeout 値は 180sec です。なお、initial timeout 値は、10 ～ 3600sec の範囲で設定することが出来ます。

○ interface link 状態監視

＜書　　式＞

```
track <trackid:1-255> interface INTERFACE
track <trackid:1-255> interface INTERFACE initial-timeout (|<10-3600>)
track <trackid:1-255> interface INTERFACE delay <10-3600>
track <trackid:1-255> interface INTERFACE initial-timeout <10-3600> delay <10-3600>
```

＜備　　考＞

・INTERFACE は、(ppp<0-4>|tunnel<0-255>|ethernet<0-2>)から選択します。

< 次ページに続く >

■ track（続き）

○ ping/ping6 による reachability のチェック

＜書　　式＞

```
track <trackid:1-255> (ip|ipv6) reachability (A.B.C.D|FQDN) (|source A.B.C.D|interface IFNAME)
                      (|<interval:10-32767> <retry:0-255>) (|delay <delay:10-3600>)
```

＜備　　考＞

- ip/ipv6 reachability の監視には、icmp/icmpv6 echo-request/reply packet を使用します。
- Interval は、ping を送信してから次の ping を送信するまでの時間です。reply が戻ってきてから次の ping を送信するまでの時間ではありません。
- Interval および retry 回数は、USER が指定することができます。
- Ping の timeout は、10sec です。
- ip reachability に限り、出力 interface を指定することができます。

○ neightbor 監視

＜書　　式＞

```
track <1-255> (ip|ipv6) neighbor (A.B.C.D|FQDN) interface IFNAME
track <1-255> (ip|ipv6) neighbor (A.B.C.D|FQDN) interface IFNAME <10-32767> <0-255>
                                                              (delay <10-3600>|)
track <1-255> (ip|ipv6) neighbor (A.B.C.D|FQDN) interface IFNAME delay <delay:10-3600>
```

＜備　　考＞

- ip/ipv6 neighbor 監視には、arp request/reply, ipv6 neighbor solicitation/advertise を使用します。
- 出力インタフェース、interval、retry 回数を指定することが出来ます。
- 初期値は、interval 60, retry 3 です。
- delay を設定すると、detect up 検出時の recovery action が delay 秒後に実行されます。

○ IKE SA の状態監視

＜書　　式＞　track <trackid:1-255> ipsec isakmp <IKE-POLICY:1-65535>
　　track <trackid:1-255> ipsec isakmp <IKE-POLICY:1-65535> delay <10-3600>

○ OSPF neighbor 監視

＜書　　式＞

```
track <trackid:1-255> ospf neighbor <PEER_RID:A.B.C.D>
track <trackid:1-255> ospf neighbor PEER_RID delay <10-3600>
track <trackid:1-255> ospf neighbor PEER_RID initial-timeout (|<10-3600>)
track <trackid:1-255> ospf neighbor PEER_RID initial-timeout <10-3600> delay <10-3600>
```

＜備　　考＞　指定した router-id との neighbor 確立後から他の state への変化を監視します。

■ track（続き）

○ BGP peer監視

＜書　　式＞

```
track <trackid:1-255> bgp neighbor <PEER_IP:A.B.C.D>
track <trackid:1-255> bgp neighbor PEER_IP delay <10-3600>
track <trackid:1-255> bgp neighbor PEER_IP initial-timeout (|<10-3600>)
track <trackid:1-255> bgp neighbor PEER_IP initial-timeout <10-3600> delay <10-3600>
track <trackid:1-255> bgp neighbor <PEER_IPv6:X:X::X:X>
track <trackid:1-255> bgp neighbor PEER_IPv6 delay <10-3600>
track <trackid:1-255> bgp neighbor PEER_IPv6 initial-timeout (|<10-3600>)
track <trackid:1-255> bgp neighbor PEER_IPv6 initial-timeout <10-3600> delay <10-3600>
```

＜備　　考＞　指定したpeer ipとのneighbor確立後から他のstateへの変化を監視します。

○ VRRPの状態監視

＜書　　式＞　track <trackid:1-255> vrrp ip <vrrpid:1-255> interface ethernet <0-2>

＜　no　＞　no track <trackid:1-255>

＜備　　考＞

・ethernetのみ有効です。

・masterからbackup/initへの変化、またはbackup/initからmasterへの変化を監視します。

○ System resume監視

＜書　　式＞　track <TRACK-ID> system resume

＜備　　考＞

・systemのresume状態を監視します。本trackは、sleep状態からresumeした際に、down状態へと遷移します。すべてのactionを実行した後に、自動的にtrack up状態へと遷移します（track upによるactionは、実行されません）。

・本trackの状態をUIの状態表示以外の他の機能から参照した場合、常にupの状態を返します。

・本trackについては、実行可能なactionが限定されています。下記action以外の動作は、保証していません。

- VRRP priorityを指定値に変更
- IPsec tunnelの確立 / 削除 / 再接続（ISAKMP指定）
- PPPの接続 / 切断 / 再接続
- Tunnelインタフェースのup/down
- L2TPv3 tunnelの接続 / 切断（PPPのインタフェースリンク監視のみ）
- IPsec local policyの変更（IPsec ISAKMP policyにて設定）
- IPsec ISAKMP policyの変更（IPsec tunnel policyにて設定）
- System restart
- Mobile module reset
- BGP advertise-routeの有効 / 無効化（BGP設定）
- Static routeの有効 / 無効化（IP route設定）

global mode

◆ ipsec nat-traversal

＜説　　明＞

・本装置では、NAT-Traversal機能をサポートしているため、NAT装置の配下に本装置が設置されている状況でも、IPsec接続を行うことが出来ます。

・IKEv1では、NAT-Traversal機能の有効/無効を指定することが可能ですが、IKEv2では自動的に有効になり、無効にすることは出来ません。

・NAT-Traversalは、IPv4のみ対応しています。

＜書　　式＞　ipsec nat-traversal enable　　(NAT-Traversal有効)

＜　no　＞　no ipsec nat-traversal enable　　(NAT-Traversal無効)

＜初 期 値＞　no ipsec nat-traversal enable

＜備　　考＞

※Transportモードと NAT-Traversalの併用

NAT環境でTransportモードを利用する場合、接続環境やセキュリティの点で、いくつかプロトコル上の制限事項があります。

・接続時の制限

NAT環境でTransportモードを利用する場合、プロトコル上の制限により、同一NAT装置配下からの接続が出来ない場合があります。

・TCP/UDPチェックサム

TCP/UDPの通信を行う際、クライアント側ではプライベートIPアドレスを利用してチェックサムを計算し、ESP化を行った後に送信します。その後、NAT装置によってソースアドレスが変換されます。本装置がこのパケットを受信した場合、複合化の後にチェックサムのチェックを行いません。本装置が受信したパケットのソースアドレス（グローバルアドレス）と、クライアントが送信したパケットのソースアドレス（プライベートアドレス）が異なるので、チェックサムエラーが発生します。そのため、Transportモード＋NAT-Traversalの環境では、受信したESPパケットのチェックサムはチェックしません。

◆ ipsec path-mtu-discovery

＜説　　明＞　PMTUDを有効にします。

＜書　　式＞　ipsec path-mtu-discovery enable

＜　no　＞　no ipsec path-mtu-discovery enable

＜初 期 値＞　ipsec path-mtu-discovery enable

＜備　　考＞

・IPsecにおいてPMTU discoveryが無効の場合は、DFbitが1でかつtunnel MTUを超えてしまう場合でも、強制的にtunnelingし転送されます。この場合、outerのip headerのDF bitは必ず0が設定されます。

・IPsecにおいてPMTU discoveryを有効にすると、DFbitが1でかつtunnel MTUを超えてしまう場合、fragment neededを送信元に返信し、packetはdropされます。この場合、outerの IP headerのDFbit値は、tunneling packetの値が設定されます。

global mode

◆ ipsec xauth
<説　　明>　IPsec Xauth認証のユーザアカウントを設定します。
<書　　式>　ipsec xauth username USERID password (|hidden) PASSWORD
<　no　>　no ipsec xauth username USERID
<備　考>　パスワードは、1-95文字以内で設定してください。
　　使用可能な文字は、英数字および!$#=*+-_.:;(){}[]^~@`<>です。

◆ ipsec x509 enable
<説　　明>　X.509証明書を使用した認証を有効にします。
<書　　式>　ipsec x509 enable
<　no　>　no ipsec x509 enable
<初 期 値>　no ipsec x509 enable
<備　　考>　IPsecのmainモードで使用することができます。

◆ ipsec x509 validity-period-check
<説　　明>　X.509証明書の有効期間をチェックする機能です。
<書　　式>　ipsec x509 validity-period-check
<　no　>　no ipsec x509 validity-period-check
<初 期 値>　ipsec x509 validity-period-check
<備　　考>
・本機能が有効の場合、現在時刻が証明書の有効期間外であれば、当該証明書を使用することは出来ません。
・本機能が無効の場合、常に証明書の利用が可能となります。また、CRLによる証明書の無効化も行いません。

◆ ipsec x509 ca-certificate
<説　　明>　X.509のCA証明書をインポートします。
<書　　式>
　ipsec x509 ca-certificate NAME ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME
　　(|source A.B.C.D|X:X::X:X)
　ipsec x509 ca-certificate NAME ftp://<A.B.C.D|X:X::X:X>/FILENAME
　　(|source A.B.C.D|X:X::X:X)
<　no　>　no ipsec x509 ca-certificate NAME
<備　　考>
・ソースアドレスを指定することができます。
・SSHを使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合（ssh://user@A.B.C.D/FILENAME）は、22番ポートを使用します（=ssh://user@A.B.C.D:22/FILENAME)。
- IPv4　ssh://user@A.B.C.D:port/FILENAME
- IPv6　ssh://[user@X:X::X:X]:port/FILENAME
・DER(*.der, *.cer)またはPEM(*.pem)フォーマットの証明書をインポートすることができます。ファイルの拡張子は変更しないでください。なお、シングルDESで暗号化された鍵ファイルを使用することは出来ません。

global mode

◆ ipsec x509 certificate

＜説　　明＞　X.509の公開鍵証明書をインポートします。

＜書　　式＞

```
ipsec x509 certificate NAME ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME
                                                    (|source A.B.C.D|X:X::X:X)
ipsec x509 certificate NAME ftp://<A.B.C.D|X:X::X:X>/FILENAME
                                                    (|source A.B.C.D|X:X::X:X)
```

＜　no　＞　no ipsec x509 certificate

＜備　　考＞

・ソースアドレスを指定することができます。

・SSHを使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合（ssh://user@A.B.C.D/FILENAME）は、22番ポートを使用します（=ssh://user@A.B.C.D:22/FILENAME)。

- IPv4　ssh://user@A.B.C.D:port/FILENAME
- IPv6　ssh://[user@X:X::X:X]:port/FILENAME

・DER(*.der, *.cer)またはPEM(*.pem)フォーマットの証明書をインポートすることができます。ファイルの拡張子は変更しないでください。なお、シングルDESで暗号化された鍵ファイルを使用することは出来ません。

◆ ipsec x509 private-key

＜説　　明＞　X.509 の private key を設定します。

＜書　　式＞

```
ipsec x509 private-key NAME key ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME
                                                    (|source A.B.C.D|X:X::X:X)
ipsec x509 private-key NAME key ftp://<A.B.C.D|X:X::X:X>/FILENAME
                                                    (|source A.B.C.D|X:X::X:X)
```

＜　no　＞　no ipsec x509 private-key NAME key

＜備　　考＞

・ソースアドレスを指定することができます。

・SSHを使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合（ssh://user@A.B.C.D/FILENAME）は、22番ポートを使用します（=ssh://user@A.B.C.D:22/FILENAME)。

- IPv4　ssh://user@A.B.C.D:port/FILENAME
- IPv6　ssh://[user@X:X::X:X]:port/FILENAME

◆ ipsec x509 private-key

＜説　　明＞　X.509のパスフレーズを設定します。

＜書　　式＞　ipsec x509 private-key NAME password (hidden|) WORD

＜　no　＞　no ipsec x509 private-key NAME [password]

global mode

◆ ipsec x509 crl

<説　　明>　証明書の失効リストを設定します。

<書　　式>

```
ipsec x509 crl NAME ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME (|source A.B.C.D|X:X::X:X)
ipsec x509 crl NAME ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
```

<　no　>　no ipsec x509 crl NAME

<備　　考>

・ソースアドレスを指定することができます。

・SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合（ssh://user@A.B.C.D/FILENAME）は、22 番ポートを使用します（=ssh://user@A.B.C.D:22/FILENAME)。

- IPv4　ssh://user@A.B.C.D:port/FILENAME
- IPv6　ssh://[user@X:X::X:X]:port/FILENAME

◆ ipsec access-list

<説　　明>　IPsecのアクセスリストを設定します。

<書　　式>

```
ipsec access-list ACL-NAME ip (any|host|A.B.C.D/M any|host|A.B.C.D/M)
ipsec access-list ACL-NAME ipv6 (any|host|X:X::X:X/M any|host|X:X::X:X/M)
```

<　no　>

```
no ipsec access-list ACL-NAME ip (any|host|A.B.C.D/M any|host|A.B.C.D/M)
no ipsec access-list ACL-NAME ipv6 (any|host|X:X::X:X/M any|host|X:X::X:X/M)
no ipsec access-list ACL-NAME
```

<備　　考>

・設定した IPsec access-list は、match address コマンドを使って IPsec tunnel に適用させます。match address コマンドについては、IPsec tunnel policy mode を参照してください。

・一つの access-list に ip と ipv6 のエントリーを各一つずつ登録することができます。また、削除時は、1 つずつ削除することができます。

・IKEv2 では ip と ipv6 の両方のエントリーが有効になりますが、IKEv1 では最初のエントリーのみが有効になります。

・IPsec access-list 内で host rule を設定する場合、以下の制限があります。

・IPv4 host と IPv6 host は同じ扱いとなります(IPv4 になるか IPv6 になるかは、IKE で使用した IP protocol に依存します)。次の設定は、1 つの host host 設定として扱われます。どちらか 1 つを削除しても変更があったとは認識されません。

```
ex)　ipsec access-list test ip host host
　　ipsec access-list test ipv6 host host
```

・host 設定と host 以外の設定を併用することはできません。次の設定では、host host の設定は有効とならず、下記の rule のみが TS(トラフィックセレクタ)として有効になります。

```
ex)　ipsec access-list test ip host host
　　ipsec access-list test ipv6 2001::/64 2002::/64
```

◆ ipsec generate

<説　　明>　RSA signature key を生成します .

<書　　式>　ipsec generate rsa-sig-key <key_length: 512-1024>

<　no　>　no ipsec generate rsa-sig-key

global mode

◆ ipsec eap radius (IKEv2のみ)

＜説　　明＞

・Account 認証を行う RADIUS server の IP address、UDP port 番号、秘密鍵(secret)を設定することができます。UDP port 番号の default は、1812 番です。Web 認証で使用する radius port 番号とは異なる番号を使用してください。

・NAS-identifier Attribute は、USER により任意の文字(32 文字以内)を指定することが可能です。Default は、機種名 -IPsec(ex.NXRG100-IPsec)です。

＜書　　式＞　ipsec eap radius (A.B.C.D|X:X::X:X) password (|hidden) WORD
　　(|port <1-65535>) (|nas-identifier WORD)

＜　no　＞　no ipsec eap radius (|A.B.C.D|X:X::X:X)

＜備　　考＞

・IPsec client からの EAP message を、本装置にて RADIUS message でカプセル化し、RADIUS server へ送信することで認証を行います。

・RADIUS server への認証要求は、最初の timeout は 2 秒、retry 回数は最大 3 回とし、retry 毎に timeout が＋ 1 秒されます。

・設定例は、authentication local/remote(ipsec isakmp policy mode)を参照してください。

◆ ipsec eap identity (IKEv2のみ)

＜説　　明＞　EAP 認証で使用する ID とパスワードを設定します。

＜書　　式＞　ipsec eap identity string WORD password (hidden|) WORD
　　ipsec eap identity key WORD password (hidden|) WORD

＜　no　＞　no ipsec eap identity string WORD
　　no ipsec eap identity key WORD

＜備　　考＞

・設定例は、authentication local/remote(ipsec isakmp policy mode)を参照してください。

・パスワードは、1-95 文字以内で設定してください。使用可能な文字は、英数字および!$#=*+-_.:;() {}[]^~@`<> です。

◆ ipsec pre-share identity (IKEv2のみ)

＜説　　明＞　IKEv2 で、動的拠点毎に異なる PSK を設定することができます。

＜書　　式＞　ipsec pre-share identity fqdn WORD password (|hidden) WORD
　　ipsec pre-share identity user-fqdn WORD password (|hidden) WORD
　　ipsec pre-share identity key WORD password (|hidden) WORD

＜　no　＞　no ipsec pre-share identity fqdn WORD
　　no ipsec pre-share identity user-fqdn WORD
　　no ipsec pre-share identity key WORD

＜備　　考＞

・設定例は、authentication local/remote(ipsec isakmp policy mode)を参照してください。

・パスワードは、1-95 文字以内で設定してください。使用可能な文字は、英数字および!$#=*+-_.:;() {}[]^~@`<> です。

global mode

◆ interface ethernet
<説　　明>　interface mode への遷移、および profile の生成を行います。
<書　　式>　interface ethernet <0-2>
<備　　考>　ethernet interface は削除不可

◆ interface loopback
<説　　明>　interface mode への遷移、および profile の生成を行います。
<書　　式>　interface loopback <0-9>
<　no　>　no interface loopback <0-9>

◆ interface ethernet <0-2> vid <1-4094>
<説　　明>　interface mode への遷移、および profile の生成を行います。
<書　　式>　interface ethernet <0-2> vid <1-4094>
<　no　>　no interface ethernet <0-2> vid <1-4094>

◆ interface tunnel
<説　　明>　interface tunnel mode への遷移、および profile の生成を行います。
<書　　式>　interface tunnel <0-255>
<　no　>　no interface tunnel <0-255>

◆ interface ppp
<説　　明>　interface ppp mode への遷移、および profile の生成を行います。
<書　　式>　interface ppp <0-4>
<　no　>　no interface ppp <0-255>

◆ interface bridge
<説　　明>　interface bridge mode への遷移、および profile の生成を行います。
<書　　式>　interface bridge <0-4095>
<　no　>　no interface bridge <0-4095>

◆ interface wlan
<説　　明>　interface wlan mode への遷移、および profile の生成を行います。
<書　　式>　interface wlan <0-1>
<　no　>　no interface wlan <0-1>

◆ wifi
<説　　明>　wifi mode への遷移、および profile の生成を行います。
<書　　式>　wifi <0-0>
<　no　>　no wifi <0-0>

◆ l2tp
<説　　明>　l2tp mode への遷移、および profile の生成を行います。
<書　　式>　l2tp <0-1>
<　no　>　no l2tp <0-1>

global mode

◆ access-server profile
<説　　明>　access-server profile mode への遷移、および profile の生成を行います。
　　no で、（指定した ID の）プロファイルを削除します。
<書　　式>　access-server profile <0-31>
<　no　>　no access-server profile |<0-31>
<備　　考>　プロファイル数は、機種により異なります。

◆ interface virtual-templare
<説　　明>　interface virtual-template mode への遷移、および profile の生成を行います。
<書　　式>　interface virtual-template <0-0>
　　no で、指定した ID のプロファイルを削除します。
<　no　>　no interface virtual-template <0-0>

◆ l2tpv3 tunnel
<説　　明>　l2tpv3-tunnel mode への遷移、および profile の生成を行います。
　　no で、指定した ID のプロファイルを削除します。
<書　　式>　l2tpv3 tunnel <tunnnel_id:0-4095>
<　no　>　no l2tpv3 tunnel <tunnnel_id:0-4095>

◆ l2tpv3 xconnect
<説　　明>　l2tpv3-xconnect mode への遷移、および profile の生成を行います。
　　no で、指定した ID のプロファイルを削除します。
<書　　式>　l2tpv3 xconnect <xid:1-4294967295>
<　no　>　no l2tpv3 xconnect <xid:1-4294967295>

◆ l2tpv3 group
<説　　明>　l2tpv3-group mode への遷移、および profile の生成を行います。
　　no で、指定した ID のプロファイルを削除します。
<書　　式>　l2tpv3 group <gid:1-8191>
<　no　>　no l2tpv3 group <gid:1-8191>

◆ ntp
<説　　明>　ntp mode への遷移、および profile の生成を行います。
<書　　式>　ntp
<　no　>　no ntp　　(=NTP サービスの停止および profile を削除します。)

◆dns
<説　　明>　dns mode への遷移および profile を生成します。
<書　　式>　dns
<　no　>　no dns　　(=DNS サービスの停止および profile を削除します。)

global mode

◆snmp
<説　　明>　snmp mode への遷移および profile を生成します。
<書　　式>　snmp
<　no　>　no snmp　　(=SNMP サービスの停止および profile を削除します。)

◆syslog
<説　　明>　syslog mode への遷移および profile を生成します。
<書　　式>　syslog
<　no　>　no syslog　(=syslog サービスの停止および profile を削除します。)

◆dhcp-server
<説　　明>　dhcp-server mode への遷移および profile を生成します。
<書　　式>　dhcp-server <1-64>
<　no　>　no dhcp-server(|<1-64>)　　(=DHCP サービスの停止および profile を削除します。)

◆monitor-log
<説　　明>　monitor-log mode への遷移および profile を生成します。
<書　　式>　monitor-log
<　no　>　no monitor-log　(= モニターログサービスの停止および profile を削除します。)

◆track
<説　　明>　extended track (ip|ipv6) reachability mode への遷移および profile を生成します。
<書　　式>　track <2048-4095> (ip|ipv6) reachability
<　no　>　no track <2048-4095>

◆router rip
<説　　明>　RIP mode への遷移および profile を生成します。
<書　　式>　router rip
<　no　>　no router rip　　(=RIP サービスの停止および profile を削除します。)

◆ router ospf
<説　　明>　OSPF mode への遷移および profile を生成します。
<書　　式>　router ospf
<　no　>　no router ospf　(=OSPF サービスの停止および profile を削除します。)

◆ router bgp
<説　　明>　BGP mode への遷移および profile を生成します。
<書　　式>　router bgp
<　no　>　no router bgp　　(=BGP サービスの停止および profile を削除します。)

global mode

◆ interface tap

＜説　　明＞　interface tap mode への遷移および profile を生成します。
　　no で、指定した ID のプロファイルを削除します。
＜書　　式＞　interface tap <0-127>
＜　no　＞　no interface tap <0-127>

◆ ssl tunnel

＜説　　明＞　ssl tunnel mode への遷移および profile を生成します。
　　no で、指定した ID のプロファイルを削除します。
＜書　　式＞　ssl tunnel <0-2>
＜　no　＞　no ssl tunnel |<0-2>

global mode

■ sip-nat

○ enable

<説　　明>　SIP NAT を有効にします。
<書　　式>　sip-nat enable
<初 期 値>　no sip-nat enable
<　no　>　no sip-nat enable

○ port

<説　　明>　任意の UDP ポート番号を宛先とするパケットを SIP-NAT 対象とすることができます。
　　宛先ポート番号は最大 7 つまで指定できます。Default では UDP5060 番のみ有効です。
<書　　式>　sip-nat port .<1-65535>
<初 期 値>　sip-nat port 5060
<　no　>　no sip-nat port

○ port-translate

<説　　明>
・SIP ヘッダの変換範囲を設定します。IP アドレスおよびポート番号を含めた範囲まで変換するか、IP アドレスの部分のみ変換するかを指定することができます。
・Default ではポート番号まで含めた範囲を変換します。
<書　　式>　sip-nat port-translate enable
<初 期 値>　sip-nat port-translate enable
<　no　>　no sip-nat port-translate enable

○ exclude-interface

<説　　明>
・無効化インターフェースとして指定されると、その LAN に対して SIP-NAT は適用されません。指定されたインターフェースへ出力するパケットの SIP ヘッダは、アドレス変換されません。ethernet インターフェースのみ指定可能可能です。
<書　　式>　sip-nat exclude-interface INTERFACE
<初 期 値>　no sip-nat exclude-interface
<　no　>　no sip-nat exclude-interface

global mode

■ CRP

○ udp source port
<説　　明>　CRPのUDPソースポートを設定します。
<書　　式>　crp udp source-port <1024-65535>
<初 期 値>　crp udp source-port 10625
<　no　>　no crp udp source-port

○ hostname
<説　　明>　CRPのホスト名を設定します。
<書　　式>　crp hostname HOSTNAME
<　no　>　no crp hostname

○ customer-id
<説　　明>　CRPのcustomer-idを設定します。
<書　　式>　crp customer-id CUSTOMER-ID
<　no　>　no crp customer-id

○ cpe-id
<説　　明>　CRPのcpe-idを設定します。
<書　　式>　crp cpe-id CPE-ID
<　no　>　no crp cpe-id

○ client
<説　　明>　CRPクライアントを設定します。
<書　　式>　crp client <1-2>
<　no　>　no crp client (<1-2>|)

○ advertise
<説　　明>　CRP広告を設定します。
<書　　式>
　crp advertise (ip|ipv6) interface ppp <0-4> (port <1-65535>|) (secondary|)
　crp advertise (ip|ipv6) interface ethernet <0-3> (port <1-65535>|) (secondary|)
　crp advertise address A.B.C.D (port <1-65535>|)
　crp advertise address X:X::X:X (port <1-65535>|)
　crp advertise nat (port <1-65535>|)
<　no　>　no crp advertise
<備　　考>　interface指定時のみ2つ設定可能（1つはsecondary）です。

global mode

■ netconf-server

管理サーバとの接続に使用します。

○enable

＜説　　明＞　netconfサーバを起動します。
＜書　　式＞　netconf-server enable (tcp|over-ssh)
＜　no　＞　no netconf-server enable

○lock timeout

＜説　　明＞　netconfサーバのロックタイムアウトを設定します。
＜書　　式＞　netconf-server lock timeout <10-3600>
＜　no　＞　no netconf-server lock timeout

○auto-config

＜説　　明＞　auto-configの設定をします。
＜書　　式＞　netconf-server auto-config enable
＜　no　＞　no netconf-server auto-config enable

global mode

■ QoS

＜説　　明＞　QoSの設定をします。

＜書　　式＞

○クラスの作成、変更

```
class policy NAME
```

○クラスの削除

```
no class policy NAME
```

○フィルタの作成

```
class filter <2-254>
```

○フィルタの削除

```
no class filter <2-254>
```

○ Mark値の設定

```
priority-map <1-255> (high|middle|low|normal) ip mark <1-4095>
```

○ TBFの設定

```
pirority-map <1-255> (high|middle|low|normal)
            queue shape <RATE:1-1000000> <BUFFER:1-65535> <LIMIT:1-65535>
```

○ SFQの設定

```
priority-map <1-255> (high|middle|low|normal) queue fair-queue
```

○ FIFOの設定

```
priority-map <1-255> (high|middle|low|normal) queue fifo (limit <1-16384>)
```

○ default classの設定

defaultのclassを設定します。default classとは、どれにも該当しないpacketを割り当てるclassのことです。default classの初期値はnormalです。

```
priority-map <1-255> default (high|middle|normal|low)
```

○ priority-mapの削除

指定したclassのpriority-mapを削除します。

```
no priority-map <1-255> (high|middle|normal|low|)
```

○ default classの初期化

defaultのclassをdefault(normal)に設定します。

```
no priority-map <1-255> default
```

○ Mark設定の削除

指定したclassのMark設定を削除します。

```
no priority-map <1-255> (high|middle|normal|low) ip mark
```

○ default queue(FIFO)に設定

```
no priority-map <1-255> (high|middle|normal|low) queue
```

■ route-map

＜説　　明＞　route-mapを追加します。

＜書　　式＞　route-map NAME (permit|deny) <1-1024>

＜　no　＞　no route-map NAME ： NAMEのroute-mapを削除します。

no route-map NAME (permit|deny) <1-1024> ： 該当のrouet-mapのみ削除します。

global mode

■ class access-list

＜説　　明＞

route-map の match 条件である match ip address 設定をフィルタリングする際に使用します。具体的には、ToS 値や MARK 値を設定する set 条件をフィルタリングする場合に使用します。

○ ip

```
class access-list ACL-NAME ip (|not) <source:>(any|A.B.C.D/M|A.B.C.D)
      <destination:>(any|A.B.C.D/M|A.B.C.D)
```

○ protocol

```
class access-list ACL-NAME ip (|not) <source:>(any|A.B.C.D/M|A.B.C.D)
      <destination:>(any|A.B.C.D/M|A.B.C.D) (|not) (<protocol:0-255>|icmp|tcp|udp)
```

○ icmp

```
class access-list ACL-NAME ip (|not) <source:>(any|A.B.C.D/M|A.B.C.D)
       (|not) <destination:>(any|A.B.C.D/M|A.B.C.D) icmp (|not) type code
```

○ tcp src dst

```
class access-list ACL-NAME ip (|not) <source:>(any|A.B.C.D/M|A.B.C.D)
      (|not) <destination:>(any|A.B.C.D/M|A.B.C.D)
      tcp (|not) (|<sport:1-65535>|any) (|<dport:1-65535>|any)
```

○ tcp src-range dst

```
class access-list ACL-NAME ip (|not) <source:>(any|A.B.C.D/M|A.B.C.D)
       (|not) <destination:>(any|A.B.C.D/M|A.B.C.D)
      tcp (|not) (|range <min:1-65535> <max:1-65535>) (|<dport:1-65535>|any)
```

○ tcp src dst-range

```
class access-list ACL-NAME ip (|not) <source:>(any|A.B.C.D/M|A.B.C.D)
       (|not) <destination:>(any|A.B.C.D/M|A.B.C.D)
      tcp (|not) (|<sport:1-65535>|any) (|range <min:1-65535> <max:1-65535>)
```

○ tcp src-range dst-range

```
class access-list ACL-NAME ip (|not) <source:>(any|A.B.C.D/M|A.B.C.D)
       (|not) <destination:>(any|A.B.C.D/M|A.B.C.D)
      tcp (|not) (|range <min:1-65535> <max:1-65535>) (|range <min:1-65535> <max:1-65535>)
```

○ udp src dst

```
class access-list ACL-NAME ip (|not) <source:>(any|A.B.C.D/M|A.B.C.D)
       (|not) <destination:>(any|A.B.C.D/M|A.B.C.D)
      udp (|not) (|<sport:1-65535>|any) (|<dport:1-65535>|any)
```

○ udp src-range dst

```
class access-list ACL-NAME ip (|not) <source:>(any|A.B.C.D/M|A.B.C.D)
       (|not) <destination:>(any|A.B.C.D/M|A.B.C.D)
      udp (|not) (|range <min:1-65535> <max:1-65535>) (|<dport:1-65535>|any)
```

○ udp src dst-range

```
class access-list ACL-NAME ip (|not) <source:>(any|A.B.C.D/M|A.B.C.D)
       (|not) <destination:>(any|A.B.C.D/M|A.B.C.D)
      udp (|not) (|<sport:1-65535>|any) (|range <min:1-65535> <max:1-65535>)
```

< 次ページに続く >

global mode

■ class access-list(続き)

○ udp src-range dst-range

```
class access-list ACL-NAME ip (|not) <source:>(any|A.B.C.D/M|A.B.C.D)
       (|not) <destination:>(any|A.B.C.D/M|A.B.C.D)
      udp (|not) (|range <min:1-65535> <max:1-65535>) (|range <min:1-65535> <max:1-65535>)
```

○ no (class access-listの削除)

```
no class access-list ACL-NAME ip
```

global mode

■ mobile

○ mobile ppp
<説　　明>　3Gデータ通信カードとPPPインタフェース番号を関連付けます。
<書　　式>　mobile <0-1> ppp <0-4>
<　no　>　no mobile <0-1> ppp

○ mobile error-recovery-restart
<説　　明>　mobile端末との通信に重大な問題が発生する可能性が高いと判断した場合に
　　systemの再起動を行う機能です。Defaultは、無効です。
<書　　式>　mobile error-recovery-restart
<　no　>　no mobile error-recovery-restart

○ mobile error-recovery-reset
<説　　明>　mobile端末との通信に重大な問題が発生する可能性が高いと判断した場合に
　　mobileのresetを行う機能です。Defaultは、無効です。
<書　　式>　mobile error-recovery-reset
<　no　>　no mobile error-recovery-reset
<備　　考>
・Error recoveryまたはnetevent機能によるMobile resetが失敗した場合は、致命的な問題があると判断して、システムを再起動します。

○ mobile termination-recovery
<説　　明>
・Mobileモジュールで PPP接続時、網側から切断された場合に、recovery処理を行う機能です。
・以下の場合に、網側から切断されたと判定します。
　・RAS側からLCP terminate requestを受信した場合
　　本装置側から先にLCP terminate requestを送信している場合は、網側からの切断とは見なしません。
　・CD lostを検知した場合
　　mobile cardの抜去やresetで発生したCD lostは、網側からの切断とは見なしません。
<書　　式>　mobile termination-recovery reset
　　mobile termination-recovery restart
<　no　>　no mobile termination-recovery
<備　　考>　Recoveryとして、mobile resetとsystem restartを指定することが出来ます。
　　Defaultでは、本機能は無効です。

○ mobile frequency-band
<説　　明>　内蔵モジュールの周波数帯を設定します。
<書　　式>　mobile <0-1> frequency-band (auto|lte|wcdma)
<　no　>　no mobile <0-1> frequency-band

■ mobile(続き)

● IP着信機能（対応機種：NXR-G100/F、NXR-G100/N）

網側からのパケットによる着信を契機に、本装置よりPPP接続を開始する機能です。

○ mobile ppp call-accept

＜説　　明＞　call-acceptを指定すると、IP着信モードになります。

＜書　　式＞　mobile 1 ppp <0-4> call-accept

＜　no　＞　no mobile 1 ppp

＜備　　考＞　着信するには、interface ppp modeで、以下の設定が必要です。

ip address A.B.C.D/M

ppp ipcp ip request

また、mobile apnコマンドで、CID（=1に設定）とAPNを設定します。

mobile apn XXXX cid 1 pdp-type (ip|ppp)

● SMS受信機能（対応機種：NXR-G100/N、NXR-G100/S）

SMSにより、本装置に対してPPPの接続や切断などの指示を行う機能です。SMSを受信すると、メッセージ内に含まれるコマンドを実行します。

実行可能なコマンドは、以下のとおりです。

・PPP接続

connect ppp <0-4>　(notify)

notify指定時は、PPP接続完了後に、SMS送信元にSMSメッセージを通知します。

・PPP切断

clear ppp <0-4>

・PPP再接続

reconnect ppp <0-4> (notify)

notify指定時は、PPP再接続完了後に、SMS送信元にSMSメッセージを通知します。

・システムスリープ

sleep system

sleep system timer TIMER

sleep system schedule NUM

● SMS受信許可電話番号指定

○ mobile sms accept

＜説　　明＞　特定の電話番号から送信されたSMSのみを受信可能とする機能です。

許可されていない電話番号から送信されたSMSは破棄します。

＜書　　式＞　mobile 1 sms accept PHONE_NUMBER

＜　no　＞　no mobile 1 sms accept (|PHONE_NUMBER)

＜備　　考＞

・Defaultでは、許可番号が指定されていません。SMS機能を利用する場合は、受信を許可する端末の電話番号を指定します。

global mode

● SMS 認証キー（対応機種：NXR-G100/N、NXR-G100/S）
受信した SMS に含まれる認証キーが、事前に設定した認証キーと一致するかどうかチェックすることで、第三者による不正なコマンドの実行を防ぐ機能です。
SMS 機能を使用する場合は、受信許可電話番号指定に加えて、本認証キーを設定することを推奨します。

○ mobile sms authentication-key
＜書　　式＞　mobile 1 sms authentication-key KEYWORD
＜　no　＞　no mobile 1 mobile 1 sms authentication-key
＜備　　考＞
KEYWORD を設定した場合の動作
- KEYWORD clear ppp X の SMS を受信した場合に、本装置の clear ppp X を実行します。
- KEYWORD reconnect ppp X の SMS を受信した場合に、本装置の reconnect ppp X を実行します。
- KEYWORD sleep system の SMS を受信した場合に、本装置の sleep system を実行します。
- KEYWORD sleep system timer TIMER の SMS を受信した場合に、本装置の sleep system timer TIMER を実行します。
- KEYWORD sleep system schedule SCHED の SMS を受信した場合に、本装置の sleep system schedule SCHED を実行します。
- KEYWORD connect ppp X (notify|)の SMS を受信した場合に、本装置の connect ppp X を実行します。

KEYWORD を設定しない場合の動作
- clear ppp X の SMS を受信した場合に、本装置の clear ppp X を実行します。
- reconnect ppp X の SMS を受信した場合に、本装置の reconnect ppp X を実行します。
- sleep system の SMS を受信した場合に、本装置の sleep system を実行します。
- sleep system timer TIMER の SMS を受信した場合に、本装置の sleep system timer TIMER を実行します。
- sleep system schedule SCHED の SMS を受信した場合に、本装置の sleep system schedule SCHED を実行します。
- connect ppp X (notify|)の SMS を受信した場合に、本装置の connect ppp X を実行します。

global mode

■ system led

＜説　　明＞　STS LED の点灯 / 消灯の条件を、指定することができます。

○ system led status

＜説　　明＞

・指定した PPP、tunnel が、接続時 / 切断状態時に、それぞれ点灯 / 消灯します。

・ngn-sip congestion 指定に、STS1 LED が点滅すると、NGN 網のひかり電話サーバが輻輳していることを示します。点滅中はデータコネクトによる接続は控えるようにしてください。

＜書　　式＞　system led status <2-2> interface tunnel <0-255>
　　system led status <2-2> interface ppp <0-4>
　　system led status <2-2> track (<1-255>|<2048-4095>)
　　system led status <2-2> ngn-sip congestion

＜　no　＞　no system led status <2-2>

＜備　　考＞　STS2 LED は、使用可能な機器のみ対応しています。

◆ as-path

＜説　　明＞　BGP autonomous system path filter を設定します。

＜書　　式＞　ip as-path access-list ACL-NAME (permit|deny) LINE

＜　no　＞　no ip as-path access-list ACL-NAME (permit|deny) LINE
　　no ip as-path access-list ACL-NAME

global mode

■ schedule

＜説　　明＞

設定された日付 / 曜日 / 時刻に、PPP の接続 / 切断 / 再接続などの指定された処理を実行する機能です。

○ PPP の schedule 接続 / 切断 / 再接続

＜説　　明＞

・指定時間に、PPP の接続 / 切断 / 再接続を行います。切断 / 再接続は、PPP の状態に関係なく実施されます。本機能によって切断された場合、手動で切断されたものとみなし、常時接続が設定されていても再接続は行われません。再接続する場合は、USER による指示もしくはスケジュールの設定が必要になります。

＜書　　式＞　日付指定

```
schedule <1-255> HOUR:MIN DAY MONTH interface ppp <0-4> (connect|disconnect|reconnect)
```

＜書　　式＞　曜日指定(DOW: Day Of the Week)

```
schedule <1-255> HOUR:MIN DOW (|DOW) interface ppp <0-4> (connect|disconnect|reconnect)
```

○スケジュールによるデータ通信端末のリセット

＜説　　明＞

・指定時間に、データ通信端末のリセットを行います。PPP が接続状態の場合は、即時実行ではなく PPP 切断後にリセットされます。PPP が接続状態でなければ、すぐにリセットされます。PPP が on-demand でない場合は、PPP が切断されたときに実行されるため、スケジュールで設定した時刻と実際にリセットされた時刻が大きく異なる場合があります。

・また、データ通信端末のリセットには 20-30 秒ほどかかります。データ通信端末のリセットをスケジュール設定する場合は、数時間以上の間隔を空けることを推奨します。

＜書　　式＞　日付指定

```
schedule <1-255> HOUR:MIN DAY MONTH mobile <0-2> clear
```

＜書　　式＞　曜日指定(DOW: Day Of the Week)

```
schedule <1-255> HOUR:MIN DOW (|DOW) mobile <0-2> clear
```

○スケジュールによるシステム再起動

＜説　　明＞　指定時間に、system の再起動を実施します。

＜書　　式＞　日付指定

```
schedule <1-255> HOUR:MIN DAY MON system restart
```

＜書　　式＞　曜日指定(DOW: Day Of the Week)

```
schedule <1-255> HOUR:MIN DOW (|DOW) system restart
```

global mode

○スケジュールによるシスログのローテート
＜説　　明＞
・指定時間に、syslog の rotate を実行します。指定時間に実際に rotate が行われるかどうかの判断は、syslog mode の rotate 設定に依存します。
＜書　　式＞　日付指定
schedule <1-255> HOUR:MIN DAY MON syslog rotate
＜書　　式＞　曜日指定(DOW: Day Of the Week)
schedule <1-255> HOUR:MIN DOW (|DOW) syslog rotate

○スケジュールによるモニターログのローテート
＜説　　明＞
・指定時間に、monitor-log 機能の log 情報の rotate を実行します。指定時間に実際に rotate が行われるかどうかの判断は、monitor-log reachability/resource 設定に依存します。
＜書　　式＞　日付指定
schedule <1-255> HOUR:MIN DAY MON monitor-log reachability rotate
schedule <1-255> HOUR:MIN DAY MON monitor-log resource rotate
＜書　　式＞　曜日指定(DOW: Day Of the Week)
schedule <1-255> HOUR:MIN DOW (|DOW) monitor-log reachability rotate
schedule <1-255> HOUR:MIN DOW (|DOW) monitor-log resource rotate

○スケジュールによる NTP の時刻同期
＜説　　明＞　指定の時刻に、NTP による時刻同期を行います。
＜書　　式＞　日付指定
schedule <1-255> HOUR:MIN DAY MON ntp adjust
＜書　　式＞　曜日指定(DOW: Day Of the Week)
schedule <1-255> HOUR MIN DOW (|DOW) ntp adjust
＜備　　考＞　NTP のスケジュール同期を行うには、NTP サーバの設定（ntp mode）が必要です。

○スケジュールによるファームウェアのチェック
＜説　　明＞
・指定の時刻に、Century Systems HP(official)から最新のファームウェア情報を取得し、更新情報があれば、ユーザに通知します（show version 実行時、あるいは syslog にて通知します)。
・flash 上のファームウェアとバージョンが異なる場合に通知します（ファームウェアが、2 面ある場合は、どちらとも異なる場合に通知します)。
＜書　　式＞　日付指定
schedule <1-255> HOUR:MIN DAY MON firmware check official
＜書　　式＞　曜日指定(DOW: Day Of the Week)
schedule <1-255> HOUR MIN DOW (|DOW) firmware check official
＜備　　考＞　以下に、更新がある場合の show version の出力例を示します。
vxr-x86#show version
Century Systems VXR Series ver 8.0.0E (build 41/11:53 15 06 2015)
Update Available:
  Century Systems VXR Series ver 8.X.X (build 1/23:59 30 06 2015)

global mode

○ファームウェアの更新

＜説　　明＞

・指定時間に、FTP、SSH、またはストレージよりファームウェアのダウンロードを行い、ファームウェアの更新を行います。

＜書　　式＞　日付指定

● Official　schedule <1-255> HOUR:MIN DAY MON firmware update official
(|source A.B.C.D|X:X::X:X) (|hold)

● FTP　schedule <1-255> HOUR:MIN DAY MON firmware update
ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X) (|hold)

● SSH　schedule <1-255> HOUR:MIN DAY MON firmware update
ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME password (|hidden) PASSWORD
(|source A.B.C.D|X:X::X:X) (|hold)

● ストレージ　schedule <1-255> HOUR:MIN DAY MON firmware update
(disk0:FILENAME|disk1:FILENAME) (|hold)

＜書　　式＞　曜日指定(DOW: Day Of the Week)

● Official　schedule <1-255> HOUR:MIN DAY MON firmware update official
(|source A.B.C.D|X:X::X:X) (|hold)

● FTP　schedule <1-255> HOUR:MIN DOW (|DOW) firmware update
ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X) (|hold)

● SSH　schedule <1-255> HOUR MIN DOW (|DOW) firmware update
ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME password (|hidden) PASSWORD
(|source A.B.C.D|X:X::X:X) (|hold)

● ストレージ　schedule <1-255> HOUR:MIN DOW (|DOW) firmware update
disk0:FILENAME (|hold)

＜備　　考＞

・Official を指定した場合、弊社 Web サイトからファームウェアを取得します。

・Official、FTP、SSH では、ソースアドレスを指定することができます。

・SSH を使用する場合は、password を設定してください。

・SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合（ssh://user@A.B.C.D/FILENAME）は、22 番ポートを使用します（=ssh://user@A.B.C.D:22/FILENAME)。

- IPv4　ssh://user@A.B.C.D:port/FILENAME
- IPv6　ssh://[user@X:X::X:X]:port/FILENAME

・hold を指定した場合、ファームウェア更新後の自動再起動を保留します（再起動するまでは、既存のファームウェアで動作します)。

※ hold 指定出来ない機種は、ファームウェア更新後に自動再起動します。

・スケジュールによるファームウェアアップデート実行時、ファームウェアのバージョンチェックを行います。同じバージョンの場合は、ファームウェアの更新を行いません（スケジュール設定が config 上に残っている場合でも、不要なファームウェア更新を回避することが出来ます)。
なお、拡張 flash 管理に対応した機種の場合、起動面と非起動面の両方とファームウェアのバージョンを比較します。いずれかの面と同じであれば、ファームウェアの更新は実行しません。

global mode

○スケジュールによるsystem sleep
＜説　　明＞　指定の時刻に、sleep状態に移行します。
＜書　　式＞　schedule <NUM> HOUR:MIN DAY MON system sleep
　　schedule <NUM> HOUR:MIN DAY MON system sleep timer <1-31536000>
　　schedule <NUM> HOUR:MIN DAY MON system sleep schedule <NUM>
＜備　　考＞　timerを設定しない場合は、365 日間（31,536,000[sec]）が設定されます。
　　スケジュール機能でresumeさせる場合は、resumeのschedule番号を指定します。

○スケジュールによるsystem resume
＜説　　明＞　指定の時刻に、resume（sleep状態から復帰）します。
＜書　　式＞　schedule <NUM> HOUR:MIN DAY MON system resume

○スケジュールによるWOLの送信
＜説　　明＞　指定の時刻に、WOL（Wake On LAN：マジックパケット）を送信します。
＜書　　式＞　schedule <NUM> HOUR:MIN DAY MON wol send name WORD
＜備　　考＞　WORDには、wol nameコマンド（global mode）で設定した名前を指定します。

global mode

○設定の削除

＜書　　式＞　no schedule <1-255>

○日付指定の例

●毎時0分に実行	schedule 1 *:00 * *
●毎日1:20に実行	schedule 1 1:20 1 *
●毎月10日の1:20に実行	schedule 1 1:20 10 *
●毎月10日の毎時20分に実行	schedule 1 *:20 10 *
●1/10の毎時20分に実行	schedule 1 *:20 10 1
●1/10の10:20に実行	schedule 1 10:20 10 1
●1月の毎日10:20に実行	schedule 1 10:20 * 1

○曜日指定の例

●毎週月曜日の毎時10分に実行	schedule 1 *:10 monday
●毎週日曜日の1:10に実行	schedule 1 1:10 sunday
●weekdayの4:10に実行	schedule 1 4:10 monday friday

global mode

◆ system netevent
＜説　　明＞　当該トラックイベントが down した時に、システムの再起動を行います。
＜書　　式＞　system netevent (<1-255>|<2048-4095>) restart
＜　no　＞　no system netevent
＜備　　考＞　イベント up 時は何も実行しません。

■ メール送信機能
＜説　　明＞　イベント発生時に、管理者にメールで通知する機能です。
＜備　　考＞　メール送信機能の詳細は、mail server mode を参照してください。

○ mail server
＜説　　明＞　mail server mode へ移行します。
＜書　　式＞　mail server <0-2>

○ no mail server
＜説　　明＞　メールサーバの設定を一括削除します。
＜書　　式＞　no mail server (|<0-2>)
＜備　　考＞　指定した番号のメールサーバ設定を一括削除します。
　　番号を指定しない場合は、すべてのメールサーバ設定を削除します。

○ mail from
＜説　　明＞　送信元メールアドレスを指定します。
＜書　　式＞　mail from WORD
＜　no　＞　no mail from
＜備　　考＞
・WORD には、送信元メールアドレス（例：centurysys@xxx.isp.ne.jp）を指定します。
・mail send from コマンド（interface ppp/wimax mode）で送信元メールアドレスの指定がない場合は、ここで指定した送信元メールアドレスを使用します。

○ mail to
＜説　　明＞　送信先メールアドレスを指定します。
＜書　　式＞　mail to WORD
＜　no　＞　no mail to
＜備　　考＞
・WORD には、送信先メールアドレス（例：user@centurysys.co.jp）を指定します。
・mail send to コマンド（interface ppp mode）で送信先メールアドレスの指定がない場合は、ここで指定した送信先メールアドレスを使用します。

global mode

◆ system boot flash
<説　　明>　次回起動の際に使用するファームウェアの面を指定します。
<書　　式>　system boot flash <1-2>
<備　　考>　本設定は、config ファイル(xml)には保存されません。

◆ system config flash
<説　　明>　次回起動時に使用するconfig をユーザが指定することが出来ます。
<書　　式>　system config (flash:FILENAME|disk0:FILENAME)
<　no　>　no system config
<初 期 値>　no system config
<備　　考>
・flash:startup.config を指定すると、save config したconfig で起動します。
・ディスクイメージ内のユーザ割り当て領域のconfig から起動するには、disk0:FILENAMEを指定します。
・no system configは、bootup設定を初期化します（startup-configで起動します）。

◆ ppp account username
<説　　明>
・PPPのアカウントを設定します。発信(PPP接続)、および着信（RAS回線着信）に使用します。
<書　　式>　ppp account username USERNAME password (|hidden) PASSWORD
<　no　>　no ppp account username USERNAME
<備　　考>
・パスワードは、1-95 文字以内で設定してください。使用可能な文字は、英数字および!$#=*+-_.:;(){}[]/^~@<>`%?です。
・ppp usernameコマンド（ppp interface mode）で設定したUSERNAME（passwordあり）と重複することはできません。
・パスワードに「?」を入力する場合は、「Ctrl」+「v」を入力してから、「?」を入力してください。

◆ show config ipv6 dhcp-client
<説　　明>　ipv6 dhcp-clientの設定を表示します。
<書　　式>　show config ipv6 dhcp-client (|WORD)
<備　　考>　ipv6 dhcp-client WORDで設定した「WORD」を指定します。

global mode

■ ip policy access-list

＜説　　明＞

・アクセスリストを使って、PBR(Policy Based Routing)を適用するパケットを指定します。
・設定したACLを受信インタフェースに適用するには、ip policy route-mapコマンドを使用します。
　自発パケットに適用するには、ip local policy route-mapコマンドを使用します。
・PBRについては、付録J Policy Based Routingを参照してください。

○ ip

```
ip policy access-list ACL-NAME (|not) source:any|A.B.C.D/M|A.B.C.D
  destination:any|A.B.C.D/M|A.B.C.D (|tos (|not) <0-255>)
```

○ protocol

```
ip policy access-list ACL-NAME (|not) source:any|A.B.C.D/M|A.B.C.D
  destination:any|A.B.C.D/M|A.B.C.D (|not) <protocol:0-255>|icmp|tcp|udp
  (|tos (|not) <0-255>)
```

○ icmp

```
ip policy access-list ACL-NAME (|not) source:any|A.B.C.D/M|A.B.C.D
  (|not) destination:any|A.B.C.D/M|A.B.C.D icmp (|not) type code (|tos (|not) <0-255>)
```

○ tcp src dst

```
ip policy access-list ACL-NAME (|not) source:any|A.B.C.D/M|A.B.C.D
  (|not) destination:any|A.B.C.D/M|A.B.C.D tcp
  (|not) [<sport:1-65535>|any] [<dport:1-65535>|any] (|tos (|not) <0-255>)
```

○ tcp src-range dst

```
ip policy access-list ACL-NAME (|not) source:any|A.B.C.D/M|A.B.C.D
  (|not) destination:any|A.B.C.D/M|A.B.C.D tcp
  (|not) [range <min:1-65535> <max:1-65535>] [<dport:1-65535>|any] (|tos (|not) <0-255>)
```

○ tcp src dst-range

```
ip policy access-list ACL-NAME (|not) source:any|A.B.C.D/M|A.B.C.D
  (|not) destination:any|A.B.C.D/M|A.B.C.D tcp
  (|not) [<sport:1-65535>|any] [range <min:1-65535> <max:1-65535>] (|tos (|not) <0-255>)
```

○ tcp src-range dst-range

```
ip policy access-list ACL-NAME (|not) source:any|A.B.C.D/M|A.B.C.D
  (|not) destination:any|A.B.C.D/M|A.B.C.D tcp
  (|not) [range <min:1-65535> <max:1-65535>] [range <min:1-65535> <max:1-65535>]
  (|tos (|not) <0-255>)
```

< 次ページに続く >

■ ip policy access-list(続き)

○ udp src dst

```
ip policy access-list ACL-NAME (|not) source:any|A.B.C.D/M|A.B.C.D
   (|not) destination:any|A.B.C.D/M|A.B.C.D udp
   (|not) [<sport:1-65535>|any] [<dport:1-65535>|any] (|tos (|not) <0-255>)
```

○ udp src-range dst

```
ip policy access-list ACL-NAME (|not) source:any|A.B.C.D/M|A.B.C.D
   (|not) destination:any|A.B.C.D/M|A.B.C.D udp
   (|not) [<sport:1-65535>|any] [range <min:1-65535> <max:1-65535>] (|tos (|not) <0-255>)
```

○ udp src dst-range

```
ip policy access-list ACL-NAME (|not) source:any|A.B.C.D/M|A.B.C.D
   (|not) destination:any|A.B.C.D/M|A.B.C.D udp
   (|not) [<sport:1-65535>|any] [range <min:1-65535> <max:1-65535>] (|tos (|not) <0-255>)
```

○ udp src dst-range

```
ip policy access-list ACL-NAME (|not) source:any|A.B.C.D/M|A.B.C.D
   (|not) destination:any|A.B.C.D/M|A.B.C.D udp
   (|not) [range <min:1-65535> <max:1-65535>] [range <min:1-65535> <max:1-65535>]
   (|tos (|not) <0-255>)
```

○ negate

```
no ip policy access-list ACL-NAME (|.....)
```

global mode

■ 電源管理機能

消費電力を小さくするための省エネ設定やシステムのsleep/resumeを行う機能です。

■ 電源管理モード設定

◆ **system power-management mode**

＜説　　明＞　電源管理モードとして、balanceモードとm2mモードを設定することが出来ます。
＜書　　式＞　system power-management mode (m2m|balance)
＜初 期 値＞　system power-management mode balance
＜備　　考＞

・balanceモードは、defaultのモードであり、消費電力と性能のバランスを考慮したモードです。
・m2mモードは、消費電力を抑えるために、CPUの動作クロックを低く抑えると共に、Ethernetのリンクスピードを最大100Mbpsに抑えます。発熱量を抑えることによって、通常よりも過酷な利用環境下でも、安定した動作を提供することが可能になります。なお、m2mモードの場合、温度プロテクション機能は動作しません。

※温度プロテクション機能

温度状態がWarning/Criticalの閾値を超えた際に、機器を守るためにCPUの動作クロックを下げる機能です。CPUの動作クロックを下げることで、発熱量が低減するため、周辺温度の降下が期待出来ます。

■ Sleep/Resume機能

・システムをsleep状態に移行させる機能です。sleep状態になると、CPU/Ethernetなどへの電源供給を停止します。
・工場やオフィス等の利用者がいない時間帯（休日や営業時間外）に、sleepモードを使用することで、大幅に消費電力を抑えることが可能になります。
・以下に、sleepへの移行手段、sleep状態からの復帰（resume）の手段を示します。いずれのsleep手段においても、resume時間を指定しない場合は、resumeまでのタイマーとして365日間（31,536,000秒）が設定されます。

○Sleep状態への移行

◆ **system power-management sleep init-button**

＜説　　明＞　INITボタンを3秒間押下した場合、sleep状態へと遷移します。
＜書　　式＞　system power-management sleep init-button
　　system power-management sleep init-button timer <1-31536000>
＜初 期 値＞　system power-management sleep init-button
＜　no　＞　no system power-management sleep init-button
＜備　　考＞

・「no system power-management sleep init-button」設定時、INITボタンを押下しても、sleep状態へと遷移しません。
・timerを設定しない場合は、365日間（31,536,000[sec]）が設定されます。

■ 電源管理機能（続き）

◆ ppp idle-timeout & system sleep

＜説　　明＞ PPP idle-timeoutによる切断時、sleep状態へと遷移します。
＜書　　式＞ ppp idle-timeout <30-86400> system sleep
ppp idle-timeout <30-86400> system sleep timer <1-31536000>
ppp idle-timeout <30-86400> system sleep schedule <NUM>
＜備　　考＞ timerを設定しない場合は、365日間（31,536,000[sec]）が設定されます。
スケジュール機能でresumeさせる場合は、resumeのschedule番号を指定します。

◆ schedule & system sleep

＜説　　明＞ スケジュール機能によって、設定した時刻に、sleep状態へと遷移します。
＜書　　式＞ schedule <NUM> HOUR:MIN DOW (DOW|) system sleep
schedule <NUM> HOUR:MIN DOW (DOW|) system sleep timer <1-31536000>
schedule <NUM> HOUR:MIN DOW (DOW|) system sleep schedule <NUM>
＜備　　考＞ timerを設定しない場合は、365日間（31,536,000[sec]）が設定されます。
スケジュール機能でresumeさせる場合は、resumeのschedule番号を指定します。

◆ sleep system

＜説　　明＞ コマンド実行により、sleep状態へと遷移します。
＜書　　式＞ sleep system
sleep system timer <1-31536000>
sleep system schedule <NUM>
＜備　　考＞ timerを設定しない場合は、365日間（31,536,000[sec]）が設定されます。
スケジュール機能でresumeさせる場合は、resumeのschedule番号を指定します。
＜　mode　＞ view mode

○Resume（Sleep状態からの復帰）

◆ timer

＜説　　明＞ sleep状態へと遷移させる際に、resumeまでのtimer（秒）を設定します。
＜書　　式＞ ppp idle-timeout <30-86400> system sleep timer <1-31536000>
schedule <NUM> HOUR:MIN DOW (DOW|) system sleep timer <1-31536000>
sleep system timer <1-31536000>

◆ schedule

＜説　　明＞ sleep状態へと遷移させる際に、resumeのschedule番号を指定します。
＜書　　式＞ ppp idle-timeout <30-86400> system sleep schedule <NUM>
schedule <NUM> HOUR:MIN DOW (DOW|) system sleep schedule <NUM>
sleep system schedule <NUM>

◆ INITボタン

＜説　　明＞ INITボタンを押下すると、resumeします。
＜書　　式＞ なし

■ 電源管理機能（続き）

◆ Serial

＜説　　明＞ Serial からの入力によって、resume します。
＜書　　式＞ system power-management resume serial <NUM>
＜　no　＞ no system power-management resume serial <NUM>
＜備　　考＞「no system power-management resume serial <NUM>」設定時は、
該当する serial からの入力があっても resume しません。

◆ Wake-up on Ring

＜説　　明＞ 内蔵 mobile モジュールで着信すると、resume します。
＜書　　式＞ system power-management resume mobile <NUM>
＜　no　＞ no system power-management resume mobile <NUM>
＜備　　考＞「no system power-management resume mobile」設定時、
着信を受けても resume しません。

■ 処理の競合

○ Firmware update/System restart
・firmware update 中、または system restart 中は、sleep 指示を受けても、sleep 状態への遷移はしません。
・また、sleep への移行途中で、firmware update や system restart を行うことは出来ません。

○ Sleep/Resume
・sleep 処理中に sleep 指示を受けた場合、後からの sleep 指示をキャンセルします。
・resume 処理中に sleep 指示を受けた場合、resume 処理が完了するまで、最大 60 秒間監視します。
・監視中に resume 処理が完了した場合は、再度 sleep 処理を行います。
・監視中に resume 処理が完了しなかった場合は、sleep 指示をキャンセルします。

○システム起動中
・システム起動中に sleep 指示を受けた場合、システム起動処理終了後に、sleep 処理を実行します。
・複数の sleep 指示を受けた場合、最後の sleep 指示が有効となります。
・システム起動中は、INIT ボタンの押下による sleep 指示は、無視します。
（工場出荷時の設定でシステム起動する場合と、類似の操作になるため。）

global mode

■ WOL（Wake On LAN）パケット送信機能

WOLは、sleep状態にある端末の電源を遠隔で投入するための技術です。

◆ wol name WORD

＜説　　明＞　UIからのコマンド実行、またはschedule設定によって、WOLの送信を行います。
送信タイプとして、Ethernetフレームと UDPパケットを指定することが出来ます。
どちらのタイプでも、送信回数と送信間隔を指定することが可能です。

○ Ethernetフレーム

＜書　　式＞

```
wol name WORD interface INTERFACE
      HH:HH:HH:HH:HH:HH ethernet (|<1-65535> <1-65535>) (|broadcast)
wol name WORD interface INTERFACE
      HH:HH:HH:HH:HH:HH ethernet type <1501-65535> (|<1-65535> <1-65535>) (|broadcast)
```

＜備　　考＞

- WORDには、本設定の名前を入力します。
- INTERFACEには、Ethernet、VLAN、Bridge（仮想スイッチ）を指定することが出来ます。
- HH:HH:HH:HH:HH:HHには、端末のMACアドレスを指定します。
- typeでは、Ethernet type（default:0x0842(2144)）を指定します。
- 送信回数の初期値は1回、送信間隔の初期値は1秒です。
- broadcastを指定した場合、Ethernetヘッダの送信先MACアドレスに、FF:FF:FF:FF:FF:FFをセットします。指定しない場合は、端末のMACアドレスをセットします。

○ UDPパケット

＜書　　式＞

```
wol name WORD ip (A.B.C.D|FQDN) HH:HH:HH:HH:HH:HH (|<1-65535> <1-65535>)
wol name WORD ip (A.B.C.D|FQDN) HH:HH:HH:HH:HH:HH port <1-65535> (|<1-65535> <1-65535>)
```

＜備　　考＞

- WORDには、本設定の名前を入力します。
- 送信先アドレスとして、IPアドレス、またはFQDNを指定します。IPアドレスには、端末のIPアドレスやdirected broadcastアドレスを指定します。
- HH:HH:HH:HH:HH:HHには、端末のMACアドレスを指定します。
- Portには、送信先のUDP port番号を指定します。初期値は、9（Discard）です。
- 送信回数の初期値は1回、送信間隔の初期値は1秒です。

＜備　　考＞

- 送信先IPアドレスが、同じネットワーク上にある場合
  ユニキャストアドレスにWOLを送信する場合は、スタティックARPの設定を推奨します（sleep状態にある端末は、ARP要求に応答しないため）。
- 送信先IPアドレスが、別のネットワーク上にある場合
  ルーティングテーブルに従って、WOLを送信します（通常は、ゲートウェイアドレスに対して、送信します。）

global mode

◆ ip host FQDN

＜説　　明＞　IPアドレスとホスト名の組み合わせを、staticに設定することが出来ます。
＜書　　式＞　ip host FQDN A.B.C.D
＜備　　考＞
・本装置のDNSサービスが有効の場合、外部からの名前解決要求に対して、staticホストエントリー、外部DNSサーバの順に名前解決を行います。
・本装置のDNSサービスが無効の場合、本装置からパケットを送信する場合のみ、staticホストエントリーを参照します。

◆ ipv6 fragment-id

＜説　　明＞　IPv6のfragmentation-idの生成方法を指定することが出来ます。
＜書　　式＞　ipv6 fragment-id random
＜　no　＞　no ipv6 fragment-id
＜初 期 値＞　no ipv6 fragment-id
＜備　　考＞
・Defaultでは、宛先毎に、ランダムに初期値を生成します。以降は、1つずつインクリメントします。
・ramdomを指定すると、毎回ランダムに生成します。

◆ ipsec priority-ignore

＜説　　明＞　Priorityによる IPsec SAの優先度を無効にする機能です。
　　IKEv1で、route based IPsecを利用している場合のみ有効です。
＜書　　式＞　ipsec priority-ignore enable
＜　no　＞　no ipsec priority-ignore enable
＜備　　考＞
・Route based IPsecでは、phase2のIDは、IPsec SAを確立するためのIDとしてのみ使用します。そのため、Priorityによる冗長化etcの機能を利用しない場合は、本機能を有効にすることによって、同じphase2 IDを持つ複数個のIPsec SAを同時に確立することが出来ます。
・Route based IPsec間、またはroute based IPsecとpolicy based IPsec間での重複が可能です。Policy based IPsec間での重複は出来ません。
・本機能は、ISPのVPNサービス等で、phase2のIDをany/anyで指定するような場合に、利用することが出来ます。

global mode

■ Mode-config

リモートVPN clientに対して、内部ネットワーク情報を設定する方法として、mode-configに対応しています。IKEv1/IKEv2のいずれでも使用可能です。

◆ ipsec local pool

＜説　　明＞
・VPN clientに対して、指定したlocal poolから、IP addressを割り当てることが出来ます。
＜書　　式＞　ipsec local pool WORD address A.B.C.D/M
＜　no　＞　no ipsec local pool WORD
＜備　　考＞
・local poolを適用するには、client configurationコマンド（ipsec isakmp policy mode）を使用します。
・VPN clientに割り当てたIPアドレスを確認するには、show ipsec leasesコマンド(view mode)を使用します。

◆ ipsec ike/ike2 client configuration dns-server

＜説　　明＞　VPN clientに対して、指定したDNSを割り当てることが出来ます。
＜書　　式＞　ipsec ike client configuration dns-server A.B.C.D (A.B.C.D|)
　　ipsec ikev2 client configuration dns-server A.B.C.D (A.B.C.D|)
＜　no　＞　no ipsec ike client configuration dns-server
　　no ipsec ikev2 client configuration dns-server
＜備　　考＞
・IKEv1/IKEv2それぞれに対して、primaryとsecondaryの2つを指定することが出来ます。
・システム内で共通の設定です（ISAKMP単位で指定することは出来ません）。

◆ ipsec ike/ike2 client configuration netbios-server

＜説　　明＞　VPN clientに対して、指定したWINS serverを割り当てることが出来ます。
＜書　　式＞　ipsec ike client configuration netbios-server A.B.C.D (A.B.C.D|)
　　ipsec ikev2 client configuration netbios-server A.B.C.D (A.B.C.D|)
＜　no　＞　no ipsec ike client configuration netbios-server
　　no ipsec ikev2 client configuration netbios-server
＜備　　考＞
・IKEv1/IKEv2それぞれに対して、primaryとsecondaryの2つを指定することが出来ます。
・システム内で共通の設定です（ISAKMP単位で指定することは出来ません）。

◆ system usb transfer-mode

＜説　　明＞　USBのデータ転送モードを設定します。
＜書　　式＞　system usb transfer-mode (pio|dma)
＜　no　＞　no system usb transfer-mode
＜備　　考＞　本設定は、save configの対象外です。

global mode

◆ (ip|ipv6) access-list-verdict

＜説　　明＞　Forward フィルタテーブルでの forward in/out の判定処理を指定する機能です。
　　本設定を変更した場合は、システム再起動が必要です。再起動後に有効となります。
＜書　　式＞　(ip|ipv6) access-list-verdict forward (combine|separate)
＜　no　＞　no (ip|ipv6) access-list-verdict forward
＜初 期 値＞　(ip|ipv6) access-list-verdict forward combine
＜備　　考＞

・combile mode（Default：従来通り）
　forward-in で許可されたパケットは、forward-out の判定を行いません。
　forward-in permit にマッチしたパケットは、forward-out deny にマッチする場合でも、許可します。
　SPI 有効時、forward-out permit にマッチしたパケットは、許可します。
・separate mode
　forward-in で許可されたパケットでも、forward-out の判定を行います。
　forward-in permit にマッチしたパケットが、forward-out deny にマッチする場合は、ドロップします。
　SPI 有効時、forward-out permit にマッチしても、SPI でドロップします。
・本機能は、ユーザフィルタリングと SPI フィルタで有効です。他のフィルタリングについては、従来どおりの動作をします（本機能の影響を受けることはありません）。

global mode

■ コンテナ型仮想化

・コンテナ型仮想化技術として、LXC に対応しています。対応するコンテナは、弊社のコンテナです。
また、起動可能なコンテナは、1 つです。
・コンテナと本装置（ホスト）は、veth インタフェース経由で通信することが出来ます。
・veth インタフェースについては、veth interface mode を参照してください。

◆ lxc container

＜説　　明＞　lxc containerを設定します。
　　lxc containerを設定すると、lxcが起動します。
＜書　　式＞　lxc container <1-1>
＜　no　＞　no lxc container
＜備　　考＞
・起動中のLXC にログインするには、connect lxc console コマンド（view mode）を使用します。

第6章

interface mode

interface mode

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#interface ethernet <0-2> [vid <1-4094>]
vxr-x86(config-if)#

vxr-x86(config)#interface loopback <0-9>
vxr-x86(config-loopback)#
```

◆ ip address

```
<説　　明>　インタフェースに IP アドレスを設定します。
<書　　式>　ip address A.B.C.D/M (|secondary)
<　no　 >　no ip address A.B.C.D/M (|secondary)
```

◆ ip address

```
<説　　明>　DHCP により IP アドレスを取得します。
<書　　式>　ip address dhcp (|HOSTNAME)
<　no　 >　no ip address dhcp
```

◆ ipv6 address

```
<説　　明>　インタフェースに IPv6 アドレスを設定します。
<書　　式>　ipv6 address X:X::X:X link-local　: 自動的に設定される LLA を上書きする
            ipv6 address X:X::X:X/M (|eui-64)
                                  : eui-64 指定時は、ipv6-address は prefix 部のみ指定
            ipv6 address autoconfig
<　no　 >　no ipv6 address X:X::X:X link-local
            no ipv6 address X:X::X:X/M (|eui-64)
            no ipv6 address autoconfig
```

interface mode

◆ ipv6 address DHCPv6-PD

<説　　明>　DHCPv6 Prefix Delegationを設定します。
<書　　式>　ipv6 address DHCPv6-PD X:X::X:X/M (|eui-64)
<　no　>　no ipv6 address DHCPv6-PD (|X:X::X:X/M)
<備　　考>

・ipv6-addressは、sub-prefixとhost部を指定することが出来ます。
・DHCPv6-PDは、DHCPv6 PDで受信するprefix部のプロファイル名です。DHCPv6-PDは、DHCPv6パケットを受信するインタフェース(異なるインタフェース)上で、ipv6 dhcp client pdコマンドを使用して設定します。

◆ ipv6 dhcp client

<説　　明>　当該インタフェースに適用するDHCPv6クライアントのプロファイル名を指定します。
<書　　式>　ipv6 dhcp client WORD
<　no　>　no ipv6 dhcp client

◆ ipv6 dhcp client pd

<説　　明>　DHCPv6 PDのprefix部に、プロファイル名を付けます。
<書　　式>　ipv6 dhcp client pd DHCPv6-PD
<　no　>　no ipv6 dhcp client
<備　　考>

・DHCPv6 PDを受信するインタフェース上で設定します。
・受信したDHCPv6 PDを(異なる)インタフェースに対して適用するには、ipv6 address DHCPv6-PDコマンドを使用します。
・ipv6 dhcp client WORDとipv6 dhcpv6 pd DHCPv6-PDは、どちらか一方だけ設定可能です。

◆ ipv6 dhcp server

<説　　明>　当該インタフェース上で、DHCPv6サーバを起動します。
<書　　式>　ipv6 dhcp server WORD
<　No　>　no ipv6 dhcp server
<備　　考>　WORDには、起動するDHCPv6サーバのプロファイル名を指定します。

interface mode

◆ speed

＜説　　明＞　インタフェーススピードとモード(full/half)を設定します。
Default は、auto-negotiation を有効とし、各 ethernet Port に対して設定することができます。

＜書　　式＞　speed (auto|10-full|10-half|100-full|100-half|auto-limit) (|port <1-4>)

＜初 期 値＞　speed auto

＜　no　＞　no speed

＜備　　考＞

・auto-limit を選択すると、auto-negotiation 時に 10/100M のみ advertise します。Gigabit interface を搭載する機種を 1000M(1G)で link させる場合は、auto を選択してください(auto-limit では、1000M link することができません)。

・auto-negotiation 時の優先順位は、次のとおりです。
優先度(高)　1000M > 100M-Full > 100M-Half > 10M-Full > 10M-Half　優先度(低)

・通信モードを auto-negotiation に設定した機器と固定に設定した機器との間で、実際に使用する通信モードおよび通信の可否は次のとおりです。

設定上の通信モード		実際の通信モード	通信の可否
auto	100M-Full	100M-Half	×
auto	100M-Half	100M-Half	○
auto	10M-full	10M-Half	×
auto	10M-Half	10M-Half	○

◆ mdix auto

＜説　　明＞

・相手 port の MDI/MDI-X を自動判別し、接続する機能です。

・通常、MDI と MDI-X で接続する場合は、ストレートケーブルを使用します。一方、MDI と MDI、MDI-X と MDI-X で、接続する場合は、クロスケーブルを使用します。

・auto MDI/MDI-X が有効の場合、ストレート / クロスに関係なく、どちらのケーブルでも接続することが出来ます。

＜書　　式＞　mdix auto

＜初 期 値＞　mdix auto

＜　no　＞　no mdix auto

＜備　　考＞

・auto-negotiation が有効（=speed auto）の場合、auto mdi/mdi-x が常に有効になります。

interface mode

◆ active power save mode

＜説　　明＞　Ethernet または Switching HUB にて使用する PHY によって、波形の振幅を抑えることにより 1 port 当たりの消費電力を削減する機能です（一部機器のみ対応）。
この機能は、default 無効とし、この機能が有効な場合 PHY の消費電力を通常時より 1～2 割ほど抑制することができます。
なお、本機能はすべての環境下で動作するわけではなく、動作するには下記のような条件が必要となります。
・1000M でリンクアップした場合
・Cable 長が 10m 以下の場合

＜書　　式＞　power-save enable (|port <1-4>)

＜初 期 値＞　no power-save enable (|port <1-4>)

＜　no　＞　no power-save enable (|port <1-4>)

＜備　　考＞　port <1-4> は HUB ポートのみ指定可能です。

◆ bandwidth

＜説　　明＞　インタフェースの帯域幅を設定することが出来ます。
bandwidth の最大値は、10Gbps です。

＜書　　式＞　bandwidth <1-10000000000[k/m/g]>

＜　no　＞　no bandwidth

＜備　　考＞　本機能は、OSPF のコスト計算時のみに使用します。
基準となる帯域幅は、auto-cost コマンド(ospf mode)にて設定します。

interface mode

◆ mtu
＜説　　明＞　MTUの値を設定します。
＜書　　式＞　mtu <bytes:68-1500>
＜初 期 値＞　mtu 1500
＜　no　＞　no mtu　(= Set defaults)

◆ ip proxy arp
＜説　　明＞　Proxy ARPを有効にします。
＜書　　式＞　ip proxy-arp
＜初 期 値＞　no ip proxy-arp
＜　no　＞　no ip proxy-arp
＜備　　考＞
・Proxy ARPは、受信したインタフェースとは異なる宛先へのARP requestに対して、代理で応答する機能です。
・forwardingの対象外のアドレス（ブロードキャストアドレスやネットワークアドレス）に対するARP requestには応答しません。

◆ ip local proxy arp
＜説　　明＞　Local proxy ARPを有効にします。
＜書　　式＞　ip local-proxy-arp
＜初 期 値＞　no ip local-proxy-arp
＜　no　＞　no ip local-proxy-arp
＜備　　考＞
・Local proxy ARPは、受信したインタフェースのサブネット宛てのARP requestに対して、代理で応答する機能です。
・Defaultは無効で、Ethernet/VLAN/bridge（仮想スイッチ）インタフェース上で使用することが出来ます。
・forwardingの対象外のアドレス（ブロードキャストアドレスやネットワークアドレス）に対するARP requestには応答しません。
・Local proxy ARPは、直接端末同士が通信できない環境（VLAN環境etc）やブロードキャストが禁止されている環境で利用します。
・local proxy ARPを利用する際は、リダイレクトメッセージが送信されないように、ip send-redirects機能を無効にしておくことを推奨します。
・Local proxy ARPが応答する条件は、次のとおりです。
　sender IPとtarget IPが異なる場合
　target IPが受信インタフェースのネットワークと同じ場合

◆ ip directed-broadcast
＜説　　明＞　Directed Broadcastのフォワーディングを有効にします。
＜書　　式＞　ip directed-broadcast
＜初 期 値＞　no ip directed-broadcast
＜　no　＞　no ip directed-broadcast

interface mode

◆ ip redirects

＜説　　明＞

・ICMP redirect（type=5）とは、同一ネットワーク上に他の最適なルートがあることを通知するためのメッセージです（RFC792）。

・本装置の Send redirect 機能によって、ICMP redirect の送信の有無を切り替えることが出来ます。

＜書　　式＞　ip redirects

＜初 期 値＞　ip redirects　　(有効)

＜　No　＞　no ip redirects　(無効)

＜備　　考＞

・以下に ICMPRedirect の例を示します。ICMP Redirect 受信後の動作は、Host 側の動作に依存するため、常に次のような動作になるというわけではありません。

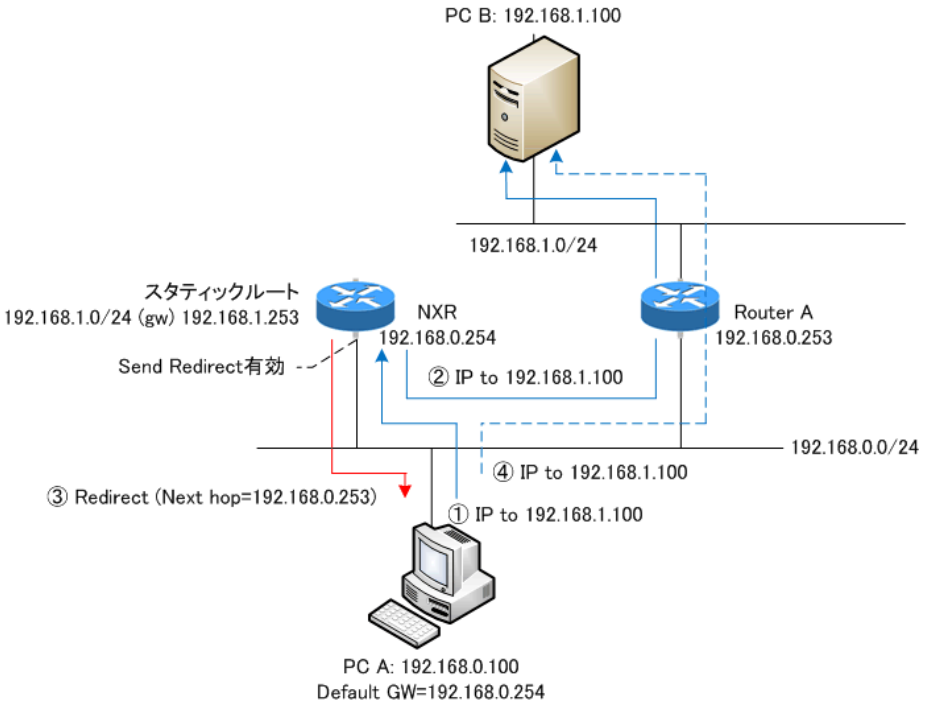
① Host A は、Host B(192.168.1.100)への IPv4 パケットを default gw(VXR)に送信します。

② VXR は、ルーティング情報から、192.168.1.0/24 宛ての next hop は 192.168.1.253 であることを知り、Router A へ転送します。

③ このとき、next hop の Router A は、送信元の Host A と同一ネットワークであるため、Host A に ICMP Redirect を送信します。

④ Host A は、以降の Host B 宛ての IPv4 パケットは、ICMP Redirect で通知された next hop に従って、Router A へ送出します。

・本装置が、ICMP Redirect を受信した場合は、ルーティングキャッシュの更新をしません。ルーティングテーブルに従った forwarding 動作を継続します。



interface mode

◆ ip tcp adjust-mss

＜説　　明＞

・Path MTU Discovery（PMTUD）機能（End-to-end でフラグメントが発生しない最大の MTU を発見すること）によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器（ルータ等）が ICMP fragment needed をフィルタリングしている場合（ブラックホールルータが存在する場合）や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、End-to-end での通信に支障をきたすことになります。このような場合、TCP では　SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

＜書　　式＞　ip tcp adjust-mss (auto|<500-1460:bytes>)

＜初 期 値＞　no ip tcp adjust-mss

＜　No　＞　no ip tcp adjust-mss

＜備　　考＞

・IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。

・本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ユーザが設定する場合は、MSS 値を指定します。元の MSS 値に関係なく指定した値に強制的に変更します。

・UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。

・「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

interface mode

◆ ip mask-reply

＜説　　明＞

・OpenViewなどの監視装置では、監視ネットワーク内の機器に対してICMP address mask request（type=17）を送信することによって機器のインタフェースのネットマスク値を取得します（単純に、死活監視で使用する場合もあります）。

・本装置では、ICMP address mask requestへの応答の有無を設定することが出来ます。

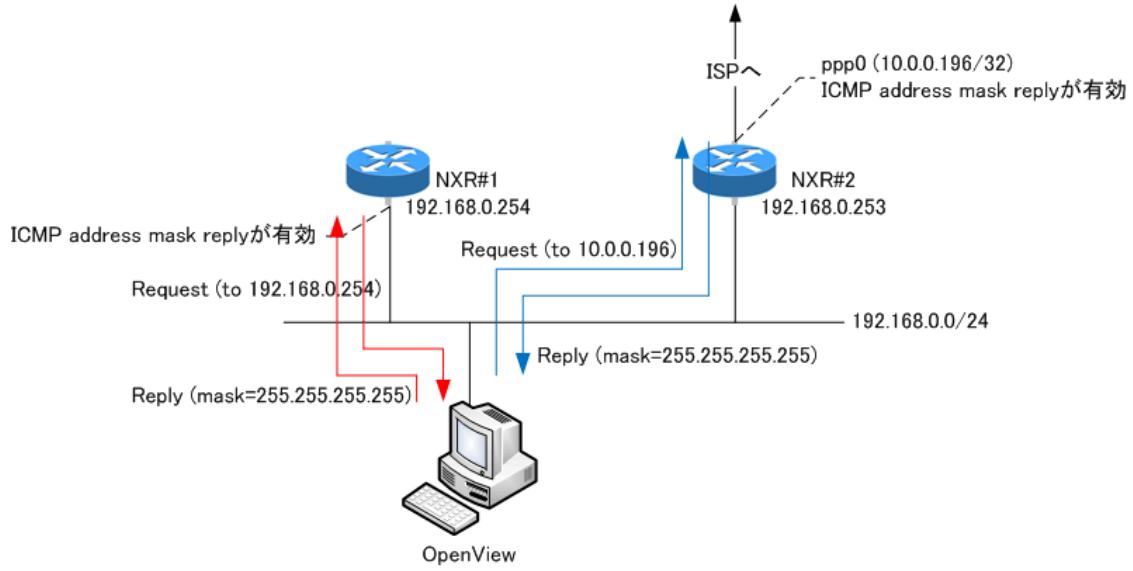
＜書　　式＞　ip mask-reply　（ICMP address mask requestに応答します。）

＜初 期 値＞　no ip mask-reply（ICMP address mask requestに応答しません。）

＜　No　＞　no ip mask-reply

＜備　　考＞

・ICMP address mask request/replyの例を示します。



interface mode

◆ link-check

＜説　　明＞

・Ethernet link 状態の監視を行います。Default は 10[sec]とし、0[sec]を設定した場合 link down を検知しません(常に up の状態です)。Link 状態に変化が発生した場合、以下のような動作が行われます。

・なお、ethernet 上で vlan を作成している場合、ethernet の link up/down に伴い vlan interface の link 状態も up/down へと遷移します。VLAN interface 毎に link 監視を行うことはできません。

upへの遷移	downへの遷移
Connected routeの有効化(RIB/FIBへの追加)	Connected routeの無効化(RIB/FIBから削除)
該当interfaceを出力interfaceとするrouteの有効化	該当interfaceを出力interfaceとするrouteの無効化
Interfaceに割り当てられているIP addressへの通信可	Interfaceに割り当てられているIP addressへの通信不可 (但し、ip/ipv6 access-linkdownが有効な場合、linkdown状態でも通信が可能)
Bind設定されている機能の有効化	Bind設定されている機能の無効化
Network event設定に伴う動作	Network event設定に伴う動作
Router solicitationの送信(IPv6)	-

※ Connected route の有効化 / 無効化は、show ip route database で確認することが出来ます。

・RIB（Routing Information Base）は、経路情報を蓄積するデータベースで、管理者の手動設定による経路や経路制御プロトコルによって学習した経路が、原則としてすべて登録されます。

・FIB（Forwarding Information Base）は、IP パケットの転送判断時に参照するデータベースです。RIB 内に同一宛先への経路が複数存在している場合は、最適経路だけが FIB に登録されます。

＜書　　式＞　link-check (|<0-60sec>)

＜初 期 値＞　link-check 10

＜　no　＞　no link-check (=link-check 0)

＜備　　考＞

・bind 設定されている機能の有効化 / 無効化について

Ethernet interface 上で tunnel interface や PPPoE が確立されていた場合、link down 検知後すぐにこれらの interface が down 状態になることはありません。Tunnel interface や PPP interface の up/down は、それぞれの keepalive 機能に依存します。但し、USER によって bind 設定(該当 interface down を trigger に L2TP tunnel/session を切断するなど)が設定されていた場合は、この限りではありません。

・Switching HUB が装備されている ethernet interface の link 監視について

内部の Switching HUB と接続されている ethernet interface 上で link 監視を行っている場合、switching hub port すべてが link down となった際に ethernet link down となり、1 つでも switching hub port の link が up した際に、ethernet link up 状態へと遷移します。

interface mode

◆ ip access-linkdown

<説　　明>　本機能を有効にすると、link down の状態でも該当 interface の IPv4 address に通信することができます。

<書　　式>　ip access-linkdown

<　no　>　no ip access-linkdown

<備　　考>　Default は、無効(no ip access-linkdown)です。

◆ ipv6 access-linkdown

<説　　明>　本機能を有効にすると、link down の状態でも該当 interface の IPv6 address に通信することができます。

<書　　式>　ipv6 access-linkdown

<　no　>　no ipv6 access-linkdown

<備　　考>　Default は、無効(no ipv6 access-linkdown)です。

◆ ip arp reachable-time

<説　　明>　解決した ARP の有効期間を設定することが出来ます。単位は msec です。

<書　　式>　ip arp reachable-time <30000-3600000>

<初 期 値>　ip arp reachable-time 30000

<　No　>　no ip arp reachable-time

<備　　考>　show arp 実行時に、ステータスが REACHABLE と表示される時間です。
実際の時間は、(0.5 ～ 1.5) × reachable-time の間のランダムな値です。

◆ ip arp queue length

<説　　明>

- Ethernet/Vlan interface 上で、IPv4 通信を行う場合、送信先(nexthop)の mac address の解決を行います。このとき、mac address が解決するまで queueing できるパケット数を指定することができます。
- Queue は、neighbor の entry 毎に作成されます。
- queueing された packet は、address 解決ができると同時に送信が行われます。
- Queue が full の状態で新たに packet が来た場合、queue の先頭から drop されます。

<書　　式>　ip arp queue length <1-1000>

<初 期 値>　no ip arp queue length (=3[packets])

<　no　>　no ip arp queue length

<備　　考>　IPv4 の IPv6 それぞれについて、interface 毎に指定することができます。
IPv6 については、ipv6 nd queue length を参照してください。

◆ ipv6 tcp adjust-mss

<説　　明>　TCP/IPv6 の MSS 値を設定します。

<書　　式>　ipv6 tcp adjust-mss (auto|500-1460)

<初 期 値>　no ipv6 tcp adjust-mss

<　no　>　no ipv6 tcp adjust-mss

interface mode

■ NDP

Ethernet/VLAN/Bridge（仮想スイッチ）インタフェース上で、RA によるアドレス割り当て、または RA 受信が有効になっている場合、当該インタフェースで RA を受信し、IPv6 address prefix や gateway 情報などを取得することが出来ます。
本装置では、以下のパラメータをサポートしています（RA を受信したインタフェースのパラメータとして使用します）。

- prefix information: ipv6 address autoconfig が未設定の場合は、prefix information を無視します。
- router preference: 複数の RA ルータから異なる preference 情報を受信した場合、high>middle>low の順で採用します。
- MTU：複数の RA ルータから異なる値を受信した場合、show ipv6 interface では、大きい方の値を表示します。RA ルータを経由して通信する際は、当該 RA ルータが広告した MTU 値を利用します。なお、RA ルータが広告した MTU 値は、show ipv6 default-gateway にて確認することが出来ます。
- default-gateway: RA パケットのソースアドレス（リンクローカルアドレス）
- preferred lifetime
- valid lifetime
- router lifetime
- hop limit:複数の RA ルータより異なる値を受信した場合、show ipv6 interface では小さいほうの値を表示します。RA ルータを経由して通信する際は、当該 RA ルータが広告した hop-limit 値を利用します。なお、RA ルータが広告した hop-limit 値は、show ipv6 default gateway で確認することが出来ます。
- ns interval: 複数の RA ルータから、異なる値を受信した場合、大きい値を採用します。
- reachable-time: 複数の RA ルータから、異なる値を受信した場合、大きい値を採用します。

※ RA を受信すると、受信した RA の値でユーザ設定値を上書きします。CLI 等から設定変更を行った場合は、ユーザ設定値で RA の値を上書きします。常に新しい設定値を採用します（現在の値は、show ipv6 interface コマンドで確認することが出来ます）。

interface mode

◆ ipv6 nd send-ra
＜説　　明＞　IPv6 RA(Router Advertisement）を送信します。
＜書　　式＞　ipv6 nd send-ra　　(送信)
＜　no　＞　no ipv6 nd send-ra　　(停止)
＜備　　考＞
・RAによるprefix広告は、Ethernet/VLAN/bridge（仮想スイッチ）上にて使用することが出来ます。
・以下のパラメータをユーザ設定値（あるいはシステム固定値）にセットして、RA送信を行います。
-router lifetime: ipv6 nd lifetimeによる設定値
-hop limit: ipv6 hop-limitによる設定値(default:64)
-reachable-time: ipv6 nd reachable-timeによる設定値
-retransmit timer: ipv6 nd ns-intervalによる設定値
RA flags
-default router preference: ipv6 nd router-preferenceによる設定値(default:medium)
-managed-config-flag: ipv6 nd managed-config-flagによる設定値(default:0)
-other-config-flag: ipv6 nd other-config-flagによる設定値(default:0)
※home agent flag, proxy flagはいずれも0をセットします。
※本バージョンでは、DHCPv6 serverをサポートしていないため、O flagまたはM flagが1の場合、別途DHCPv6 serverが必要になります。
Prefix information: ICMPv6 type3（ipv6 nd prefixにより設定します。）
-prefix/prefix length
-preferred lifetime
-valid lifetime
-autonoumous address-configuration flag：ipv6 nd prefix X:X::X:X/M no-autoconfigが設定されている場合は0、未設定は1. default:1
-on-link flag：ipv6 nd prefix X:X::X:X/M off-linkが設定されている場合は0、未設定時は1. default:1。ただし、ipv6 nd prefixで設定したprefixと同じprefixを当該インタフェース上のconnected routeとして保持している場合（IPv6 address設定している場合等）は、本設定に関係なく常に1.
-router address flag：常に0
MTU：iCMPv6 type5
-MTU：インタフェースのMTU値
Source link-layer address: iCMPv6 type1
-link-layer address： ipv6 nd no-advertise-link-addressの有効時、本オプションは広告しません。無効時は、出力インタフェースのlink-layer address(MACアドレス)を設定します。default:無効（本オプションを広告）です。

interface mode

◆ ipv6 nd accept-ra

＜説　　明＞
・本設定(ipv6 address autoconfig設定なし)を有効にすると、RAを受信しても、stateless addressを設定しません。
＜書　　式＞　ipv6 nd accept-ra
＜　no　＞　no ipv6 nd accept-ra
＜備　　考＞
・ipv6 address autoconfig設定時、本設定は必要ありません。
・当該インタフェースに、IPv6アドレスは設定しませんが、RAによって取得したパラメータ（default-gateway, retransmit timer, reachable time, mtu, hop-limit）は使用します。

◆ ipv6 nd prefix

＜説　　明＞　IPv6 RA (Router Advertisement)にて広告するprefixを設定します。
＜書　　式＞　ipv6 nd prefix X:X:X:X::X/M
　　<valid-liftime:0-4294967295> <preferred-lifetime:0-4294967295>
　　(|{off-link|no-autoconfig})
　　ipv6 nd prefix X:X::X:X/M (|{off-link|no-autoconfig})
　　ipv6 nd prefix X:X::X:X/M no-advertise
＜　no　＞　no ipv6 nd prefix (|X:X:X:X::X/M)
＜備　　考＞
・広告するprefixは、当該インタフェースに設定しているIPv6アドレスのprefix（ただし、auto-configurationによるアドレスは除く）、ユーザが設定したprefix、およびDHCPv6-PDによって取得したprefix（VRRPv3の実行中を除く）です。
・インタフェースに設定しているprefix、ユーザ指定によるprefix、DHCPv6-PDによって取得したprefixが同じ場合は、ユーザ指定のprefix設定を使用します。
・valid/preferred lifetimeは、ユーザ指定を除くprefixを広告する場合、固定値（preferred lifetimeは604800sec、valid lifetimeは2592000sec）を使用します。
・一方、ユーザ指定のprefixは、ユーザ設定値を使用します。ユーザ設定値がない場合は、上記の固定値を使用します。
・no-advertiseを指定すると、当該prefixを広告しません（default:1)。
・off-linkを指定すると、当該prefixのon-link flagを0に設定して広告します（default:1)。
・no-autoconfigを指定すると、当該prefixのautonomous address-configuration flagを0に設定して広告します（default:1)。
・RAで広告するprefixに変更があった場合、古いprefixは変更直後の1回のみpreferred lifetimeを0、valid lifetimeを7203に設定してRAを送信します。Preferred lifetimeが0のRAを受信することによって、LAN内のクライアントは、当該IPv6アドレスを使用しなくなります。RAを停止する際は、preferred lifetimeを0にすることに加え、router lifetimeを0にして送信します。

interface mode

◆ ipv6 nd ra-lifetime

<説　　明>　IPv6 RA(Router Advertisement) ライフタイムを設定します。
<書　　式>　ipv6 nd ra-lifetime <0-9000>
<初 期 値>　ipv6 nd ra-lifetime 1800
<　no　>　no ipv6 nd ra-lifetime
<備　　考>　ra-lifetime >= ra-interval max

◆ ipv6 nd ra-interval

<説　　明>　IPv6 RA(Router Advertisement) インターバルを設定します。
<書　　式>　ipv6 nd ra-interval <min:3-1350> <max:4-1800>
<初 期 値>　ipv6 nd ra-interval 200 600
<　no　>　no ipv6 nd ra-interval
<備　　考>

- min < max x 0.75 となるように設定してください。
- VRRPv3 が設定されているインタフェースでは、RA を有効にした場合でも、常に RA 広告するわけではなく、VRRP マスターの場合に限り送信します。また、広告する prefix は、インタフェース上に設定している IPv6 address prefix ではなく、仮想 IPv6 address prefix を広告します。仮想 IPv6 アドレスが未設定の場合は、prefix を広告しません。

■ RS の送信

RA メッセージを要求する際に送信するパケットです。以下のタイミングで、RS を送信します。

- LLA を設定 / 変更した場合
- インタフェースが、administratively down（管理者による shutdown）から up となった場合
- インタフェースのリンク状態が、down から up となった場合

※ RS は、RA 受信が有効でない場合は、送信しません。

■ RS の受信

IPv6 forwarding が有効の場合のみ受信します。RS を受信した場合、RA の送信処理の実行や受信パケットの neighbor 情報の更新に利用します。

◆ ipv6 nd rs-interval

<説　　明>　IPv6 Router Solicitation インターバルを設定します。
<書　　式>　ipv6 nd rs-interval <interval:1-10sec>
<初 期 値>　ipv6 nd rs-interval 1
<　no　>　no ipv6 nd rs-interval　(初期値)

◆ ipv6 nd rs-count

<説　　明>　IPv6 Router Solicitation の送信回数を設定します。
<書　　式>　ipv6 nd rs-count <count:1-2147483647>
<初 期 値>　ipv6 nd rs-count 3
<　no　>　no ipv6 nd rs-count　(初期値)

interface mode

◆ ipv6 nd reachable-time
<説　　明>　隣接ノードの到達性確認間隔を指定します。
<書　　式>　ipv6 nd reachable-time <msec:0-3600000>
<初 期 値>　ipv6 nd reachable-time 30
<　no　>　no ipv6 nd reachable-time　(初期値)

◆ ipv6 nd managed-config-flag
<説　　明>　RA flag(managed-config-flag)を設定することが出来ます。
<書　　式>　ipv6 nd managed-config-flag　　(M flag=1)
<初 期 値>　no ipv6 nd managed-config-flag　(M flag=0)
<　no　>　no ipv6 nd managed-config-flag

◆ ipv6 nd other-config-flag
<説　　明>　RA flag(other-config-flag)を設定することが出来ます。
<書　　式>　ipv6 nd other-config-flag　　(O flag=1)
<初 期 値>　no ipv6 nd other-config-flag　(O flag=0)
<　no　>　no ipv6 nd other-config-flag

◆ ipv6 nd router-preference
<説　　明>　RA flag(router-preference)を設定することが出来ます。
<書　　式>　ipv6 nd router-preference (high|low|medium)
<初 期 値>　ipv6 nd router-preference medium
<　no　>　no ipv6 nd router-preference

◆ ipv6 nd no-advertise-link-address
<説　　明>　Source link-layer address optionの広告（する / しない）を設定します。
<書　　式>　ipv6 nd no-advertise-link-address
<初 期 値>　no ipv6 nd no-advertise-link-address
<　no　>　no ipv6 nd no-advertise-link-address
<備　　考>　有効：source link-layer address optionを送信します。
　　無効：source link-layer address optionを送信しません。

interface mode

■ NDP Proxy

・NDP を受信した際に代理応答する機能です。NTT NGN の IPoE 環境（ひかり電話なし）etc での利用が考えられます。
・各 NDP パケットを受信した場合、NDP Proxy 機能は、次のように動作します。
-**NS パケット**:本バージョンでは、RA Proxy 機能が有効かつ RA で受信した prefix に対する NS に対してのみ代理応答を行い、NA パケットを返します。すべての NS に対して代理応答するわけではありません。RA ルータがダウンした場合（RA Proxy 機能による判定）や、prefix 情報に変更があった場合は、RA を受信していたインタフェース上のすべての NDP proxy エントリを消去します。
-**NA パケット**：NA パケットを受信しても何も行いません。
-**RS パケット**：RS パケットを受信しても何も行いません。
-**RA パケット**：受信した RA パケットに対して代理応答を行うことはありませんが、RA Proxy によって受信した RA 情報を他のインタフェースへ広告することが出来ます。

■ RA Proxy

・RA Proxy：受信した RA パケット内の prefix 情報を、指定したインタフェースに対して代理で送信する機能です。
・prefix 以外の情報は、受信したインタフェースでのみ利用します（他のインタフェースへ送信しません）。
・例えば、NGN IPoE 環境などで RA による prefix 広告を行う場合、RA ルータとユーザ端末間にルータが存在すると、RA パケットがユーザ端末側に届かないため、LAN 側のホスト上で、auto configuration を行うことが出来ません。このような場合に、本機能を利用します。
・IPv6 ブリッジの場合、RA 広告はブリッジしますが、アクセスリストなどは利用できません。RA Proxy の場合は、layer3 フォワーディングのため、アクセスリスト等のルータ機能も利用することが出来ます。
・代理で送信可能な prefix は最大 10 個で、これ以上の prefix 情報は無視します。WAN 側に複数の RA ルータが存在する場合、最初に受信した RA パケットの送信元ルータからの情報のみを使用します。その後、当該ルータからの応答がなくなった場合は、他のルータからの RA パケットを使用します。

◆ ipv6 nd accept-ra proxy

＜説　　明＞　RA Proxy を有効にします。
＜書　　式＞　ipv6 nd accept-ra proxy ethernet <0-X>
　　(|rs-interval <0-604800> rs-count <1-255>)
＜備　　考＞
・RA Proxy 機能は、NDP Proxy 機能の一部ですが、本装置では、NS パケットに対する代理応答の機能を NDP Proxy 機能とし、RA Proxy 機能とは異なる機能として扱います。
・本バージョンでは、NDP Proxy 機能のみを有効にすることは出来ません。RA Proxy 機能と同時に使用します。
・Default では、NDP Proxy および RA Proxy 機能は無効です。

interface mode

◆ ipv6 nd ns-interval

＜説　　明＞　NSの送信間隔を設定します。
＜書　　式＞　ipv6 nd ns-interval <msec:1000-3600000>
＜初 期 値＞　ipv6 nd ns-interval 1000
＜　no　＞　no ipv6 nd ns-interval

◆ ipv6 nd dad attempts

＜説　　明＞　IPv6 DADの送信回数を設定します。
＜書　　式＞　ipv6 nd dad attempts <0-600>
＜初 期 値＞　ipv6 nd dad attempts 1
＜　no　＞　no ipv6 nd dad attempts

◆ ipv6 nd accept-redirects

＜説　　明＞　IPv6 forwardingが無効の場合に、ICMPv6 redirectsを受け入れるかどうかを指定します。
＜書　　式＞　ipv6 nd accept-redirects
＜初 期 値＞　no ipv6 nd accept-redirects
＜備　　考＞　IPv6 forwardingが有効な場合は、この設定に関係なく受信しません。
＜　no　＞　no ipv6 nd accept-redirects

◆ ipv6 nd queue length

＜説　　明＞
・Ethernet/Vlan interface上でIPv6通信を行う場合、近隣探索（Neighbor Discovery）によって送信先(nexthop)のmac addressの解決を行います。このとき、mac addressが解決するまでqueueingできるパケット数を指定することができます。
・Queueは、neighborのentry毎に作成されます。
・queueingされたpacketは、address解決ができると同時に送信が行われます。
・Queueがfullの状態で新たにpacketが来た場合、queueの先頭からdropされます。
＜書　　式＞　ipv6 nd queue length <1-1000>
＜初 期 値＞　no ipv6 nd queue length (= 3[packets])
＜　no　＞　no ipv6 nd queue length
＜備　　考＞　IPv4のIPv6それぞれについて、interface毎に指定することができます。
IPv4については、ip arp queue lengthを参照してください。

◆ ipv6 hop-limit

＜説　　明＞　IPv6 hop-limitを指定することが出来ます。
＜書　　式＞　ipv6 hop-limit <0-255>
＜初 期 値＞　ipv6 hop-limit 64
＜　no　＞　no ipv6 hop-limit
＜備　　考＞
・指定したhop-limitをRAのパラメータ（current-hop-limit）に設定します。
・本機能により、hop-limitを指定した場合、本装置から出力するIPv6パケットのhop-limitには影響しません。
・0を指定した場合、ルータによりhop-limit数を指定しないことを意味します。

interface mode

◆ ip rip receive version
<説　　明>　RIPの受信バージョンを設定します。
<書　　式>　ip rip receive version (1|2) (|1|2)
<初 期 値>　ip rip receive version 2
<備　　考>　version 1, version 2, version 1 & 2の指定が可能
<　no　>　no ip rip receive version

◆ ip rip send version
<説　　明>　RIPの送信バージョンを設定します。
<書　　式>　ip rip send version (1|2) (|1|2)
<初 期 値>　ip rip send version 2
<備　　考>　version 1, version 2, version 1 & 2の指定が可能
<　no　>　no ip rip transmission version

◆ ip rip split-horizon
<説　　明>　スプリットホライズンを設定します。
<書　　式>　ip rip split-horizon (|poisoned)
<初 期 値>　ip rip split-horizon
<　no　>　no ip rip split-horizon

interface mode

◆ ip ospf cost
<説　　明>　OSPFのコスト値を設定します。
<書　　式>　ip ospf cost <1-65535>
<　no　>　no ip ospf cost

◆ ip ospf hello-interval
<説　　明>　Helloインターバルを設定します。
<書　　式>　ip ospf hello-interval <1-65535>
<　no　>　no ip ospf hello-interval

◆ ip ospf dead-interval
<説　　明>　Deadインターバルを設定します。
<書　　式>　ip ospf dead-interval <1-65535>
<　no　>　no ip ospf dead-interval

◆ ip ospf retransmit-interval
<説　　明>　Retransmitインターバルを設定します。
<書　　式>　ip ospf retransmit-interval <1-65535>
<　no　>　no ip ospf retransmit-interval

◆ ip ospf transmit-delay
<説　　明>　Transmit Delayを設定します。
<書　　式>　ip ospf transmit-delay <1-65535>
<　no　>　no ip ospf transmit-delay

◆ ip ospf authentication
<説　　明>　認証を有効にします。
<書　　式>　ip ospf authentication (null|message-digest)
<　no　>　no ip ospf authentication

◆ ip ospf authentication-key
<説　　明>　認証パスワードを設定します。
<書　　式>　ip ospf authentication-key PASSWORD
<　no　>　no ip ospf authentication-key

◆ ip ospf message-digest-key
<説　　明>　MD5パスワードを設定します。
<書　　式>　ip ospf message-digest-key <keyid:1-255> md5 PASSWORD
<　no　>　no ip ospf message-digest-key <keyid:1-255>

interface mode

◆ ip ospf priority

<説　　明>　プライオリティを設定します。
<書　　式>　ip ospf priority <0-255>
<　no　>　no ip ospf priority

◆ ip ospf mtu-ignore

<説　　明>　DBD 内の MTU 値を無視します。
<書　　式>　ip ospf mtu-ignore
<　no　>　no ip ospf mtu-ignore

interface mode

◆ vrrp ip address

＜説　　明＞　VRRPで使用する仮想IPアドレス(VIP)を設定します。
＜書　　式＞　vrrp ip <vrrpid:1-255> address A.B.C.D
＜　no　＞　no vrrp ip <vrripd:1-255> (address A.B.C.D|)

◆ vrrp ip priority

＜説　　明＞　VRRPのプライオリティを設定します。
＜書　　式＞　vrrp ip <vrrpid:1-255> priority <1-254>
＜初 期 値＞　vrrp ip <vrrpid:1-255> priority 100
＜　no　＞　no vrrp ip <vrrpid:1-255> priority
＜備　　考＞
・マスタールータのpriorityを高く、バックアップルータのpriorityを低く設定します。

◆ vrrp ip preempt

＜説　　明＞　Preemptを有効にします。
＜書　　式＞　vrrp ip <vrrpid:1-255> preempt
＜初 期 値＞　vrrp ip <vrrpid:1-255> preempt
＜　no　＞　no vrrp ip <vrrpid:1-255> preempt
＜備　　考＞
・Preemptが有効の場合、priorityのもっとも高いルータが常にマスタールータになります。
・preemptが無効の場合、priorityの高いルータが復旧したとしても、現在マスターになっているルータがそのままマスタールータとして動作を継続します。

interface mode

◆ vrrp ip preempt delay

＜説　　明＞

・Preempt が有効な場合に、バックアップルータが自分より優先度の低い advertise パケットを受信した際に、バックアップからマスターへ切り替わる時間を遅らせることが出来ます。

・preempt delay 時間は、1 ～ 1000(秒)の範囲で指定(秒単位)します。

＜書　　式＞　vrrp ip <vrrpid:1-255> preempt delay <1-1000sec>

＜　no　＞　no vrrp ip <vrrpid:1-255> preempt delay

＜備　　考＞

・Preempt delay が設定されている場合、バックアップルータおよびマスタールータは、以下のとおり動作します（マスタールータへの影響はありません。）。

○ バックアップルータ

- master down timer、あるいは delay timer がタイムアウトすると advertise を送信してマスターへと状態遷移します。
- 自分よりも優先度の高い advertise を受信した場合は、バックアップルータとして動作します(delay timer が動作している場合は停止します)。
- 自分よりも優先度の低い advertise パケットを受信した場合、delay timer が未起動なら delay timer を開始し、master down timer はキャンセルします。また、delay 中に自分より優先度の低い advertise パケットを受信した場合は、無視します(delay timer を継続します)。

○ マスタールータ

- 自分よりも優先度の高い advertise を受信した場合、バックアップルータへと遷移します。
- 自分よりも優先度の低い advertise を受信した場合、advertise を無視します(マスタールータのまま状態遷移しません)。

◆ vrrp ip timers

＜説　　明＞　VRRP の advertise の送信間隔を設定します。

＜書　　式＞　vrrp ip <vrrpid:1-255> timers advertise <1-255sec>

＜初 期 値＞　vrrp ip <vrrpid:1-255> timers advertise 1

＜　no　＞　no vrrp ip <vrripd:1-255> timers advertise

◆ vrrp ip netevent

＜説　　明＞　VRRP tracking を設定します。
　　マスタールータに設定します（バックアップルータには設定しません）。

＜書　　式＞　vrrp ip <vrrpid:1-255> netevent <trackid:1-255> priority <1-254>
　　vrrp ip <vrrpid:1-255> netevent <trackid:2048-4095> priority <1-254>

＜　no　＞　no vrrp ip <vrripd:1-255> netevent

＜備　　考＞

・track event が down したときに、マスタールータの priority を指定値に変更します。ここで指定する priority は、バックアップルータの priority より小さい値を設定します。

・event down 発生時は、priority の大小が逆転するため、マスタールータとバックアップルータが切替ります。

通常	マスタールータのpriority > バックアップルータのpriority
Event down発生時	マスタールータのpriority < バックアップルータのpriority

interface mode

◆ ip access-group

＜説　　明＞

・global mode で設定した ACL をインタフェースに適用することで、パケットフィルタリングを行うことができます。

＜書　　式＞　ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME

＜　No　＞　no ip access-group (in|out|forward-in|forward-out)

＜備　　考＞

・各インタフェースへのパケットフィルタリングの適用箇所(付録の Packet Traveling を参照)は、以下の 4ヶ所です。

- in(local input)　本装置自身で受信して処理するパケットを制限します。
- out(local output) 本装置自身が作成して出力するパケットを制限します。
  トンネリングされたパケットも VXR 自身が作成したパケットとして認識します。
- forward-in　VXR が当該インタフェースで受信して forwarding するパケットを制限します。
- forward-out VXR が受信して当該インタフェースへ forwarding するパケットを制限します。

・mac 指定のある ACL は、out および forward-out に設定することは出来ません。

◆ ipv6 access-group

＜説　　明＞　アクセスグループに IPv6 アクセスリストを追加します。

＜書　　式＞　ipv6 access-group (in|out|forward-in|forward-out) IPV6-ACL-NAME

＜初 期 値＞　設定なし

＜　no　＞　no ipv6 access-group (in|out|forward-in|forward-out)

◆ ip masquerade

＜説　　明＞

・インタフェースよりパケットを出力する際に、パケットの送信元 IPv4 アドレスを出力インタフェースの IPv4 アドレスに自動変換する機能です。

＜書　　式＞　ip masquerade　（有効）

＜初 期 値＞　no ip masquerade（無効）

＜　No　＞　no ip masquerade

＜備　　考＞

・すべてのインタフェース(Ethernet/VLAN/PPP/Tunnel)で設定することが出来ます。

・TCP/UDP/ICMP のみ対応しています。その他のプロトコルに関しては、動作は保証しません。

・IPv6 パケットは、IP マスカレードの対象外です。

・forward out/local output フィルタリング適用後のパケットに、IP マスカレードを適用します。

◆ ip (snat-group|dnat-group)

＜説　　明＞

・global mode で設定した SNAT または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。

・SNAT は、パケットの出力時に適用されます。DNAT は、パケットの入力時に適用されます。

＜書　　式＞　ip (snat-group|dnat-group) NAT-NAME

＜　No　＞　no ip (snat-group|dnat-group)

＜備　　考＞　NAT ルールの設定は、ip snat/ip dnat)コマンド(global mode)で行います。

interface mode

◆ ip webauth-filter

＜説　　明＞
- Web 認証フィルタをインタフェースに適用すると、ある特定のホスト、ネットワークやインタフェースについて、Web 認証せずに通信することが可能となります。
- Web 認証フィルタは、各インタフェースにつき、IN/OUT をそれぞれ一つずつ設定することができます。Default の設定はありません。

＜書　　式＞　ip webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
＜　No　＞　no ip webauth-filter (forward-in|forward-out)
＜備　　考＞
- Web 認証フィルタの設定については、ip web-auth access-list コマンド（global mode）を参照してください。
- Web 認証については、Web Authenticate mode を参照してください。

◆ pppoe-client ppp

＜説　　明＞　PPPoE クライアントを有効にします。
＜書　　式＞　pppoe-client ppp <PPP-INTERFACE-NUMBER:0-4>
＜初 期 値＞　no pppoe-client ppp
＜備　　考＞　複数指定可能。Ethernet interface のみ。
＜　no　＞　no pppoe-client ppp <0-4>

◆ ip spi-filter

＜説　　明＞
- 簡易ファイヤウォールの一つとして、SPI（Stateful Packet Inspection）機能をサポートします。
- パケットに関連するコネクションの状態を見て、当該パケットをドロップするかしないかを決める機能です。

＜書　　式＞　ip spi-filter　（有効）
＜初 期 値＞　no ip spi-filter（無効）
＜　No　＞　no ip spi-filter
＜備　　考＞
- コネクションの状態が、established または related の場合に、パケットの転送を許可します。
  - Established とは、すでに双方向でパケットの通信がありコネクションが確立されている状態です。
  - Related とは、すでに確立しているコネクションがある状態です。FTP のデータ転送等がこれに該当します。
- 新しい接続でありながら、syn ビットの立っていないパケットはドロップします。
- SPI は、forward in および local input の位置で適用されます。ユーザが適用位置を変更することは出来ません。

interface mode

◆ ipv6 spi-filter
＜説　　明＞　IPv6 SPI filterを設定します。
＜書　　式＞　ipv6　spi-filter
＜初 期 値＞　no ipv6 spi-filter
＜　no　＞　no ipv6 spi-filter

◆ ip spi-filter log
◆ ipv6 spi-filter log
＜説　　明＞　フィルタログ機能（syslog mode参照）を有効にします。
　　パケットが、SPIフィルタにマッチした場合、syslogに出力することが出来ます。
＜書　　式＞　ip spi-filter log [limit <0-100>]
　　ipv6 spi-filter log [limit <0-100>]
＜初 期 値＞　ip spi-filter log limit 10
　　ipv6 spi-filter log limit 10
＜　No　＞　no ip spi-filter
　　no ipv6 spi-filter
＜備　　考＞
・limitを指定すると、1秒当たりのログ出力数を制限します。初期値は、10パケット/秒です。
・WAN側からの意図しないパケットが、SPIフィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分に注意してください。

◆ shutdown
＜説　　明＞　インタフェース(ethernet <0-3>)をシャットダウンすることができます。
＜書　　式＞　shutdown
＜初 期 値＞　no shutdown
＜　no　＞　no shutdown

interface mode

◆ ipsec policy

＜説　　明＞　当該インタフェースで使用するIPsecローカルポリシーを設定します。
＜書　　式＞　ipsec policy <local policy:1-255>
＜　No　＞　no ipsec policy (|<local policy:1-255>)
＜備　　考＞
・各インタフェースに、IPsecローカルポリシーを4つまで設定することが出来ます。他のインタフェースで既に設定しているIPsecローカルポリシーは、重複して設定できません。

◆ ipsec policy-ignore

＜説　　明＞
・IPsec policy のチェックを行わないように指定する機能です。IPsec policy としてanyなどを指定したけれども、特定の通信のみIPsec 化したくない場合に、この機能を使用します。
＜書　　式＞ ipsec policy-ignore (|input|output)
＜初　期　値＞ no ipsec policy-ignore（無効）
＜　No　＞ no ipsec policy-ignore
＜備　　考＞
・Inputを指定した場合、inbound policy check を実行しないため、IPsec 化されてくるべきパケットがドロップ されてしまう現象を回避することができます。
・Output を指定した場合、当該インタフェースから出力されるパケットは、IPsec policy をチェックしないため平文で送信されます。

interface mode

■ QoS

＜説　　明＞　QoSの設定をします。

○ HTBの設定

＜書　　式＞　queue policy POLICYNAME bandwidth <1-1000000> (|ifg-pa-fcs)

＜備　　考＞

- HTBを設定するには、class policyコマンドで作成したclass policyを指定します。
- 存在しないclass policyを指定すると、親classのみ設定されます。該当するclass policyを作成したときに、当該HTBが設定されます。
- bandwidthで、class policyの全帯域幅を指定します。
- ifg-pa-fcs(後述)を指定することが出来ます。Defaultは無効です。

○ PQの設定

＜書　　式＞　queue priority-group <PRIORITY-MAP-NUMBER:1-32>

＜備　　考＞

- PQを設定するには、global modeで作成したpriority-mapを指定します。
- 存在しないpriority-mapを指定すると、すべてのパケットをdefault classにマッピングするPQが設定されます。該当するpriority-mapを作成したときに、当該PQが設定されます。
- どのclassにも該当しないパケットは、default classにマッピングされます。

○ SFQの設定

＜書　　式＞　queue fair-queue

○ FIFOの設定

＜書　　式＞　queue fifo (|limit <1-16384>)

＜備　　考＞　limitでFIFOキューの長さを指定することが出来ます。

○ TBF(shaping)の設定

＜書　　式＞

queue shape <RATE:1-1000000> <BUFFER:1-1000000> <LIMIT:1-1000000> (|ifg-pa-fcs)

＜備　　考＞

- <RATE:1-1000000>　Shapingレート(Kbps)を指定します。
- <BUFFER:1-1000000>　Bucketのサイズ(bytes)を指定します。
- <LIMIT:1-1000000>　Tokenが利用可能になるまでにバッファすることが出来るキューの長さ(bytes)を指定します。
- ifg-pa-fcs(後述)を指定することが出来ます。Defaultは無効です。

○ no queue

＜書　　式＞　no queue

＜備　　考＞　上記で設定したqueueを削除して、default queue（pfifo_fast）に設定します。

■ QoS（続き）

○ classify

＜書　　式＞　classify (input|output) route-map ROUTEMAP

＜備　　考＞

・インタフェースにルートマップを適用します。1つのインタフェースに、input と output を別々に設定することが出来ます。

・input で指定したルートマップは、PRE-ROUTING(付録の Packet Traveling を参照)で適用されます。

・output で指定したルートマップは、POST-ROUTING(付録の Packet Traveling を参照)で適用されます。

○ no classify

＜書　　式＞　no classify (|input|output)

＜備　　考＞

・インタフェースに適用したルートマップを削除します。

・「no classify」を実行すると、両方(input と output)を削除します。片方だけを削除する場合は、input または output を指定します。

● ifg-pa-fcs

契約した回線帯域により料金が異なるようなキャリアサービスを利用する場合、ルータでの shaping 時に、FCS や IFG や PA を除いたフレームサイズで rate 計算を行います。この場合、shaping rate としては問題ないようでも、Ethernet フレームとして実際に回線を流れる際は、FCS や IFG や PA が追加されるため、回線側でフレームドロップが発生することがあります。このような場合の対応として、Ethernet インタフェース上での設定に限り、shaping rate の計算時に、IFG(inter-frame-gap の最小サイズ 12 バイトで計算)、FCS(4 バイト)、PA(preamble:8 バイト)をフレームサイズに加えることができます。これにより、回線サービス上での帯域超過によるフレームドロップを回避することが可能となります。Default では、この機能は無効です（IFG、PA、FCS 分のサイズを考慮しません)。

interface mode

◆(ip|ipv6) rebound

＜説　　明＞

・下位ルータから受信したパケットを、受信インタフェースと同一インタフェースから出力(forwarding)した場合、下位ルータから本装置に対して再度パケットが送信されてくるため、下位ルータと本装置の間でTTLが「0」になるまでパケットがループします。

・IP rebound機能を無効にすると、受信インタフェースと送信インタフェースが同一の場合、パケットをドロップし、かつ送信元にdestination unreachableを送信します。

・Defaultは、有効です(受信インタフェースと送信インタフェースが同一でもドロップしません)。

＜書　　式＞　(ip|ipv6) rebound

＜初 期 値＞　(ip|ipv6) rebound

＜　no　＞　no (ip|ipv6) rebound

◆ip reassemble-output

＜説　　明＞

・インタフェースのMTU（あるいはPMTU）より大きいパケットをIP forwardingする際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。本設定有効時、本装置がリアセンブルしたパケットは、以下のようにフラグメント処理を行います。

- fragmented packet(パケットの断片)がMTUを超える場合、リアセンブルしたパケットを再度MTUサイズにフラグメントして出力します。
- fragmented packet(パケットの断片)がMTUより小さい場合、受信したfragmented packetのサイズで出力します。
- パケット全体のサイズがMTUより小さい場合、リアセンブルしたパケットを出力します。

＜書　　式＞　ip reassemble-output

＜初 期 値＞　ip reassemble-output

＜　no　＞　no ip reassemble-output

＜備　　考＞

・上記の場合（本設定が有効の場合)、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易なIP実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズで本装置からパケットを出力します。また、出力時のIPフラグメント処理は、次のようになります。

- fragmented packet(パケットの断片)がMTUを超える場合、受信したfragmented packetをMTUサイズにフラグメントして出力します。
- fragmented packet(パケットの断片)がMTUより小さい場合、受信したfragmented packetのサイズで出力します。
- パケット全体のサイズがMTUより小さい場合、受信したfragmented packetをそのままのサイズで出力します。

・Defaultは、global設定およびinterface設定ともに有効です。Global設定とinterface設定のAND条件により、本機能が有効か無効かを判定します。本設定は、IP forwardingするパケットにのみ影響します。

・受信時のサイズを記載しておくバッファが32 個しかないため、33 個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-output が有効な場合と同様に処理します。

interface mode

◆session invalid-status-drop-interface

＜説　　明＞
・session invalid-status-drop機能(global mode参照)をインタフェース毎に指定することができます。
・本機能は、default で無効です。
＜書　　式＞　session invalid-status-drop-interface enable
＜初 期 値＞　no session invalid-status-drop-interface enable
＜　no　＞　no session invalid-status-drop-interface enable
＜備　　考＞
・あるインタフェースに対してのみ適用したい場合は、global mode で session invalid-status-drop 機能を無効にして、かつ本機能を指定インタフェースで有効にします。以下は、ethernet 0インタフェースに適用する場合の設定例です。
- global mode で、session invalid-status-drop を無効にします。
vxr-x86(config)#no session invalid-status-drop enable
- 指定インタフェースで、本機能を有効にします。
vxr-x86(config)#interface ethernet 0
vxr-x86(config-if)#session invalid-status-drop-interface enable

◆ip dhcp mode ngn

＜説　　明＞　NGN回線でデータコネクトを使用する場合に設定します。
＜書　　式＞　ip dhcp mode ngn
＜　no　＞　no ip dhcp mode
＜備　　考＞　no を設定すると、ip dhcp request classless-static-route も無効になります。

◆ip dhcp request classless-static-route

＜説　　明＞　NGN回線でのデータコネクトとインターネット接続(PPP)を併用する場合に設定します。
＜書　　式＞　ip dhcp request classless-static-route
＜　no　＞　no ip dhcp request classless-static-route
＜備　　考＞
・データコネクトと PPP によるインターネット通信を併用する場合、DHCPv4 の classless-static-route オプション(RFC3442)を使って、NGN 網への static route 情報を取得することにより、データコネクトの通信を NGN 網へルーティングさせることが出来ます。
・取得した static route は、アドレスのリース期間中有効です。

◆l2tpv3 access-group

＜説　　明＞　Xconnect インタフェースでの送受信に対して、l2tpv3 access-list を適用します。
＜書　　式＞　l2tpv3 access-group (in|out) WORD
＜　no　＞　no l2tpv3 access-group (in|out)
＜備　　考＞
・WORD：　root の ACL 名を指定します。
（root の ACL 名は、global mode の l2tpv3 access-list WORD root にて設定します。）
・in:　Xconnect インタフェース→セッション（本装置への入力）方向のフィルタを適用します。
・out:　セッション→ Xconnect インタフェース（本装置からの出力）方向のフィルタを適用します。

interface mode

◆ ip p2p-detection

＜説　　明＞　P2P 検出機能を有効にします（IPv4 のみ対応）。
＜書　　式＞　ip p2p-detection (any|winny|share|bittorrent) {log|deny}
＜　no　＞　no ip p2p-detection
　　no ip p2p-detection (winny|share|bittorrent)
＜備　　考＞
・インターネットに接続しているインタフェース上でのみ有効にすることを推奨します。
・詳細については、「付録 K：P2P 検出機能」を参照してください。

◆ ip arp filter

＜説　　明＞
・異なるインタフェースに割り当てられているアドレスに対する ARP request を受信した際に、ARP reply を返す / 返さない機能です。
＜書　　式＞　ip arp filter
＜初 期 値＞　ip arp filter　　（有効：ARP reply を返さない）
＜　no　＞　no ip arp filter　　（無効：ARP reply を返す）
＜備　　考＞
・ある LAN セグメントに複数の Ethernet インタフェースが接続されている場合は、複数のインタフェースから ARP reply を返さないように、本機能を有効にします。
・一方で、ある LAN 上の端末に対する host route が、別インタフェースになっている場合に、当該 host からの ARP request に対して、ARP reply を返す場合は、本機能を無効にします。
・ARP reply の送信先は、ルート情報によって決まります。

◆ ip arp gratuitous

＜説　　明＞　gratuitous ARP(GARP)を送信する機能です。
＜書　　式＞　ip arp gratuitous <attempts:1-255> <interval:1-3600> <delay:1-600>
　　ip arp gratuitous (= ip arp gratuitous <attempts:1> <interval:1> <delay:5>)
＜初 期 値＞　no ip arp gratuitous　（無効：GARP を送信しない）
＜　no　＞　no ip arp gratuitous
＜備　　考＞
・アドレスの重複を避けたり、ARP テーブルを更新するために、本装置では、下記のタイミングに、GARP (request)を送信します。
　・IP アドレスを追加した場合：追加したアドレスの GARP を送信します。
　・リンクアップした場合：当該インタフェースの全アドレスの GARP を送信します。
　・VRRP マスターに遷移した場合：VIP に対する GARP を送信します。
・GARP 送信機能は、default 無効です。設定により有効にする場合、送信回数、送信間隔(sec)、初期試行までの delay(sec)も同時に指定することが出来ます。
・設定可能なインタフェースは、Ethernet、VLAN、Bridge（仮想スイッチ）です。
・多数の VLAN や Bridge（仮想スイッチ）上で有効にすると、リンクアップ時に大量の GARP を送信するケースがあるため、本機能を有効にする場合は、注意してください。
・DHCP クライアント機能使用時、DHCP によって IP アドレスを取得したタイミングでは、GARP 送信は行いません。しかし、既に IP アドレスを取得した状態で、リンクアップした場合は、GARP を送信します。

interface mode

◆ (ip|ipv6) tcp strip-options

＜説　　明＞

・TCP パケット内のオプションを stip する機能です。

・Fast-forwarding が有効な場合、SACK/timestamp/MD5 については、strip されない場合があります。

＜書　　式＞　(ip|ipv6) tcp strip-options
(all|md5|mss|sack|sack-permitted|timestamp|wscale)

＜初 期 値＞　no (ip|ipv6) tcp strip-options

＜　No　＞　no (ip|ipv6) tcp strip-options

＜備　　考＞　Strip 可能なオプションと監視するパケットの種類は、次のとおりです。

TCPオプション	該当TCPパケット
MSS	SYN/SYN-ACK
Window Scale Option	SYN/SYN-ACK
SACK Permitted	SYN/SYN-ACK
SACK	すべてのTCPパケット
Time Stamp Option	すべてのTCPパケット
MD5 signature Option	すべてのTCPパケット

◆ bridge-group

＜説　　明＞　インタフェースを、bridge-group（仮想スイッチグループ）に参加させます。

＜書　　式＞　bridge-group <0-4095> (port <1-128>|)

＜　No　＞　no bridge-group

＜備　　考＞　bridge-group が未設定（interface bridge が未設定）の場合、join に失敗します。

第7章

interface tunnel mode

interface tunnel mode

◆ 移行command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#interface tunnel <0-255>
vxr-x86(config-tunnel)#
```

◆ description

<説　　明>　インタフェースの説明を記述します。
<書　　式>　description DESCRIPTION
<　no　>　no description (|DESCRIPTION)

◆ ip address

<説　　明>　インタフェースにIPアドレスを付与します。
<書　　式>　ip address A.B.C.D/M (|secondary)
<　no　>　no ip address (|A.B.C.D/M) (|secondary)

◆ ipv6 address

<説　　明>　インタフェースにIPv6アドレスを付与します。
<書　　式>　ipv6 address X:X::X:X/M (|eui-64) : IPv6 address (e.g. 3ffe:506::1/48)
　　ipv6 address X:X::X:X link-local
<　no　>　no ipv6 address X:X::X:X/M (|eui-64)
　　no ipv6 address X:X::X:X link-local

◆ ipv6 address DHCPv6-PD

<説　　明>　DHCPv6 Prefix Delegationを設定します。
<書　　式>　ipv6 address DHCPv6-PD X:X::X:X/M (|eui-64)
<　no　>　no ipv6 address DHCPv6-PD (|X:X::X:X/M)
<備　　考>

・ipv6-addressは、sub-prefixとhost部を指定することが出来ます。
・DHCPv6-PDは、DHCPv6 PDで受信するprefix部のプロファイル名です。DHCPv6-PDは、DHCPv6パケットを受信するインタフェース(異なるインタフェース)上で、ipv6 dhcp client pdコマンドを使用して設定します。

◆ tunnel source

<説　　明>　トンネルのsourceアドレスを設定します。
<書　　式>　tunnel source A.B.C.D

◆ tunnel destination

<説　　明>　トンネルのDestinationアドレスを設定します。
<書　　式>　tunnel destination A.B.C.D

interface tunnel mode

■ tunnel mode

＜説　　明＞
・トンネリング機能として、GRE IP-in-IP、IPsec（over IPv4/IPv6）、6rd の 5 つのモードをサポートしています。
＜初 期 値＞　tunnel mode gre
＜　no　＞　no tunnel mode (= tunnel mode gre)

○ IPinIP
＜説　　明＞
・IPv4 パケットを IPv4 でトンネリングするプロトコルです。IPv6 パケットをトンネリングすることは出来ません。
・プロトコル番号は、4 です。
・IPinIP トンネルインタフェース上では、IPv6 は無効です。
＜書　　式＞　tunnel mode ipip

○ GRE（Generic Routing Encapsulation）
＜説　　明＞
・IPv4 および IPv6 パケットをトンネリングすることが出来ます。Transport 用の IP は、IPv4 のみ対応しています。
・RFC2784 に準拠しています。
・プロトコル番号は、47 です。
・オプション機能として、ID キー、チェックサムの 2 つをサポートしています。シーケンスチェックについては、対応していません。
＜書　　式＞　tunnel mode gre

○ IPsec over IPv4
○ IPsec over IPv6
＜説　　明＞
・Route based IPsec(参照：付録 B)を使用する際は、ipsec ipv4 または ipsec ipv6 を指定します。
＜書　　式＞　tunnel mode ipsec ipv4　　(= IPsec over IPv4)
　　tunnel mode ipsec ipv6　　(= IPsec over IPv6)

○ 6rd（IPv6 Rapid Deployment on IPv4 infractructures）
＜説　　明＞
・IPv6 パケットを IPv4 でトンネリングするためのプロトコルです。
・RFC5569/5969 に準拠しています。
・IPv6 over IPv4 トンネリング上では、IPv4 は無効です。
＜書　　式＞　tunnel mode ipv6ip 6rd
＜備　　考＞
・6rd を使用する場合は、tunnel 6rd prefix、tunnel 6rd ipv4 prefix-length の設定も確認してください。

interface tunnel mode

◆ tunnel key
<説　　明>　送信時、GRE ヘッダに識別子として ID を設定します。GRE の場合のみ有効です。
<書　　式>　tunnel key <0-4294967295>
<初 期 値>　no tunnel key
< no >　no tunnel key
<備　　考>
・受信パケットに key ID がなくても drop しません。しかし、key ID が存在していて ID が一致しない場合は、当該パケットを drop します。

◆ tunnel checksum
<説　　明>　GRE パケット（GRE ヘッダを含む）のチェックサムを計算し、チェックサムフィールドにチェックサム値を設定します。GRE の場合のみ有効です。
<書　　式>　tunnel checksum
<初 期 値>　no tunnel checksum
< no >　no tunnel checksum

interface tunnel mode

◆ tunnel path-mtu-discovery

＜説　　明＞　トンネルインタフェース上でPMTUDを有効にします。
＜書　　式＞　tunnel path-mtu-discovery
＜初 期 値＞　tunnel path-mtu-discovery　　（有効）
＜　no　＞　no tunnel path-mtu-discovery　　（無効）
＜備　　考＞
＜　IPv4　＞
・IPv4パケットをトンネリングする際のPMTU Discoveryの動作について記します。
- 以下は、IP tunnel（tunnel mode ipip|gre）で、fragmentが必要な場合のPMTUDの動作です。
IPsec tunnel（tunnel mode ipsec ipv4）でのPMTUDについては、付録Bを参照してください。
-PMTUDの設定（有効 / 無効）とトンネリングするパケットのDFビットの値（0/1）によって、本装置の処理が異なります。

PMTUD設定	DF bit	本装置の処理
有効	0	fragmentして送信する。 outer IP headerのDFビットは、1を設定する。
	1	fragment neededを送信元に返し、パケットをdropする。
無効	0	fragmentして送信する。 outer IP headerのDFビットは、0を設定する。
	1	強制fragmentして送信する（※）。 outer IP headerのDFビットは、0を設定する。

※tunnel MTUを超えるパケットは、フォワーディング処理の際にPMTUDが作動するため、強制フラグメントを行いません。しかし、トンネルインタフェースへの出力後に、header tax分を加えたパケットの大きさが、tunnelの宛先へのPMTUDを超えている場合は、強制fragmentして送信します。
フォワーディング時にPMTUDの作動を回避するには、tunnelのMTUを1500に設定します。
＜　IPv6　＞
・IPv6の場合、PMTUはdefaultで有効です（無効にすることはできません）。
・MTUとは、PMTUからトンネルヘッダを引いたもの、またはMTU設定値のいずれかの小さい方の値です。
・本装置でトンネリングを行う際に、tunnel header taxによって転送可能な最大パケットサイズが、IPv6の最小MTU（1280バイト）を下回ることも考えられます。このような場合の動作を以下に示します（1280より小さい値を送信元に返しても、送信元ホストは1280より小さいパケットに分割して送信することが出来ないため、通信を行うことが出来ません）。
IPv6 over IPv6 tunneling（RFC2473参照）
・Tunnel MTUがIPv6最小MTU（1280）より大きい場合
パケットを破棄して、送信元ホストへ、ICMPv6 packet too bigメッセージを返信します。
・Tunnel MTUがIPv6最小MTU（1280）より小さい場合（または同じ場合）
パケットを強制的にfragmentして送信します。
IPv6 over IPv4 tunneling（RFC2893参照）
・Tunnel MTUがIPv6最小MTU（1280）より大きい場合
パケットを破棄して、送信元ホストへ、ICMPv6 packet too bigメッセージを返信します。
・Tunnel MTUがIPv6最小MTU（1280）より小さい場合（または同じ場合）
トンネリングパケットがIPv6最小MTUより大きい場合、パケットを破棄し、送信元ホストへIPv6 packet too bigメッセージを返信します。
トンネリングパケットがIPv6最小MTUより小さい場合、トンネルヘッダのDFビットを0に設定した上で、fragmentして送信します。

interface tunnel mode

◆ tunnel ttl

＜説　　明＞　TTLを設定します。
＜書　　式＞　tunnel ttl (<1-255>|inherit)
＜初 期 値＞　tunnel ttl inherit
＜　no　＞　no tunnel ttl　　(= tunnel ttl inherit)
＜備　　考＞

・固定の値（1-255）を設定する場合は、PMTUD （tunnel path-mtu-discovery）を有効にします。
・inheritを設定した場合、GRE/IPIP（tunnel mode gre|ipip）ではTTLをコピーします。IPsec tunnel（tunnel mode ipsec ipv4）でのTTL設定については、付録Bを参照してください。

interface tunnel mode

◆ tunnel tos
<説　　明>
<書　　式>　tunnel tos (<0-252>|inherit)
<初 期 値>　tunnel tos inherit
<　no　>　no tunnel tos　　(= tunnel tos inherit)
<備　　考>
・inherit を指定した場合、IPv4（innner）ヘッダの ToS 値、または tunneling IPv6（inner）ヘッダの traffic-class 値を tunnel IPv4（outer）ヘッダにコピーします。
・ToS 値を指定する場合、0-252 の範囲で指定することが出来ます。
・ECN フィールドの設定は出来ません。ECN field の扱いについては、「付録 B 1.2.4.1 ECN field の扱い」を参照してください。
※ GRE トンネル上で、IPv6 パケットをトンネリングする場合は、inherit を無視し、ToS 値として 0x0 を設定します。

◆ tunnel pre-fragment
<説　　明>　Fragment 処理が必要な場合、先に fragment してから ESP 化します。
　　(複数の ESP packet に分割されます)。
<書　　式>　tunnel pre-fragment
<初 期 値>　no tunnel pre-fragment
<　no　>　no tunnel pre-fragment
<備　　考>　Route based IPsec(参照：付録 B)を使用する際に、IPsec tunnel interface に設定することが出来ます。

◆ tunnel protection ipsec policy
<説　　明>　使用する IPsec tunnel policy を指定します。
<書　　式>　tunnel protection ipsec policy <1-65535>
<　no　>　no tunnel protection
<備　　考>　Route based IPsec(参照：付録 B)を使用する際に設定します。

◆ bandwidth
<説　　明>　インタフェースの帯域幅を設定することが出来ます。
　　bandwidth の最大値は、10Gbps です。
<書　　式>　bandwidth <1-10000000000[k/m/g]>
<　no　>　no bandwidth
<備　　考>　本機能は、OSPF のコスト計算時のみに使用します。
　　基準となる帯域幅は、auto-cost コマンド(ospf mode)にて設定します。

◆ mtu
<説　　明>　トンネルインタフェースの MTU 値を設定します。
<書　　式>　mtu <bytes:68-1500>
<初 期 値>　mtu 1476 (tunnel mode gre の場合)
　　mtu 1480 (tunnel mode ipip の場合)
　　mtu 1500 (tunnel mode ipsec の場合)
<　no　>　no mtu　(= Set defaults)

interface tunnel mode

◆ ip redirects

＜説　　明＞
- ICMP redirect（type=5）とは、同一ネットワーク上に他の最適なルートがあることを通知するためのメッセージです（RFC792）。
- 本装置の Send redirect 機能によって、ICMP redirect の送信の有無を切り替えることが出来ます。

＜書　　式＞　ip redirects
＜初 期 値＞　ip redirects　　(有効)
＜　No　＞　no ip redirects　(無効)
＜備　　考＞
- ICMPRedirect の例は、interface mode の ip redirects を参照して下さい。

◆ ip tcp adjust-mss

＜説　　明＞
- Path MTU Discovery（PMTUD）機能（End-to-end でフラグメントが発生しない最大の MTU を発見すること）によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器（ルータ等）が ICMP fragment needed をフィルタリングしている場合（ブラックホールルータが存在する場合）や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、End-to-end での通信に支障をきたすことになります。このような場合、TCP では　SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

＜書　　式＞　ip tcp adjust-mss (auto|<500-1460:bytes>)
＜初 期 値＞　no ip tcp adjust-mss
＜　No　＞　no ip tcp adjust-mss
＜備　　考＞
- IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。
- 本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。
- ユーザが設定する場合は、MSS 値を指定します。元の MSS 値に関係なく指定した値に強制的に変更します。
- UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。
- 「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

◆ ipv6 tcp adjust-mss

＜説　　明＞　TCP/IPv6 の MSS 値を設定します。
＜書　　式＞　ipv6 tcp adjust-mss (auto|<bytes:500-1440>)
＜初 期 値＞　no ipv6 tcp adjust-mss
＜　no　＞　no ipv6 tcp adjust-mss

interface tunnel mode

◆ ip mask-reply

＜説　　明＞

・OpenView などの監視装置では、監視ネットワーク内の機器に対して ICMP address mask request（type=17）を送信することによって機器のインタフェースのネットマスク値を取得します（単純に、死活監視で使用する場合もあります)。

・本装置では、ICMP address mask request への応答の有無を設定することが出来ます。

＜書　　式＞　ip mask-reply　（ICMP address mask request に応答します。）

＜初 期 値＞　no ip mask-reply（ICMP address mask request に応答しません。）

＜　No　＞　no ip mask-reply

＜備　　考＞

・ICMP address mask request/reply の例は、interface mode の ip mask-reply を参照して下さい。

◆ ip fragment-reassembly

＜説　　明＞

・Pre-fragment されたpacketを受信した場合に、本装置においてreassembleするか、reassembleせずにforwardingするかを設定することができます。defaultは、reassembleします。

・Route based IPsec(参照：付録B)を使用する際に、IPsec tunnel interfaceに設定することができます。

＜書　　式＞　ip fragment-reassembly

＜初 期 値＞　ip fragment-reassembly

＜　no　＞　no ip fragment-reassembly

＜備　　考＞

・global modeで「no ip reassemble-output」を設定し、ipsec tunnel interfaceで「no ip fragment-reassembly」を設定した場合には「no ip fragment-reassembly」が優先されます。
この場合、「no ip fragment-reassembly」が設定されたtunnle interfaceで受信したパケットは、reassembleせずに転送しますが、conntrackによるセッション管理の対象から外れるため、conntrackを利用した機能（NAT機能/SPI/sessionコマンドによる各機能）が使用できなくなる他、フィルタリングやpacket coloringの使用にも制限が出ます。

・「no ip reassemble-output」を設定する場合は、全てのtunnel interfaceの「no ip fragment-reassembly」を「ip fragment-reassembly」に設定してから行って下さい。
(no ip fragment-reassemblyが設定されている場合は、Warningが出力されます。)

・ip fragment-reassemblyは、将来的に廃止を予定しているため、なるべくip reassemble-outputを使用するようにしてください。

◆ ip rip receive version

＜説　　明＞　RIPの受信バージョンを設定します。

＜書　　式＞　ip rip receive version (1|2) (|1|2)

＜備　　考＞　両方指定も可能

＜　no　＞　no ip rip receive version

interface tunnel mode

◆ ip rip send version
＜説　　明＞　RIPの送信バージョンを設定します。
＜書　　式＞　ip rip send version (1|2) (|1|2)
＜備　　考＞　両方指定も可能
＜　no　＞　no ip rip send version

◆ ip rip split-horizon
＜説　　明＞　スプリットホライズンを有効にします。
＜書　　式＞　ip rip split-horizon (|poisoned)
＜初 期 値＞　ip rip split-horizon
＜　no　＞　no ip rip split-horizon

◆ ip access-group
＜説　　明＞
・global mode で設定したACLをインタフェースに適用することで、パケットフィルタリングを行うことができます。
＜書　　式＞　ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
＜　No　＞　no ip access-group (in|out|forward-in|forward-out)
＜備　　考＞
・各インタフェースへのパケットフィルタリングの適用箇所(付録のPacket Travelingを参照)は、以下の4ヶ所です。
- in(local input)　本装置自身で受信して処理するパケットを制限します。
- out(local output) 本装置自身が作成して出力するパケットを制限します。
　トンネリングされたパケットも本装置自身が作成したパケットとして認識します。
- forward-in　本装置が当該インタフェースで受信してforwardingするパケットを制限します。
- forward-out 本装置が受信して当該インタフェースへforwardingするパケットを制限します。
・mac指定のあるACLは、outおよびforward-outに設定することは出来ません。

◆ ipv6 access-group
＜説　　明＞　アドレスグループにIPv6アクセスリストを追加します。
＜書　　式＞　ipv6 access-group (in|out|forward-in|forward-out) IP64-ACL-NAME
＜　no　＞　no ipv6 access-group (in|out|forward-in|forward-out)

◆ ip masquerade
＜説　　明＞　インタフェースよりパケットを出力する際に、パケットの送信元IPv4アドレスを出力インタフェースのIPv4アドレスに自動変換する機能です。
＜書　　式＞　ip masquerade　（有効）
＜初 期 値＞　no ip masquerade（無効）
＜　No　＞　no ip masquerade
＜備　　考＞
・すべてのインタフェース(Ethernet/VLAN/PPP/Tunnel)で設定することが出来ます。
・TCP/UDP/ICMPのみ対応しています。その他のプロトコルに関しては、動作は保証しません。
・IPv6パケットは、IPマスカレードの対象外です。
・forward out/local outputフィルタリング適用後のパケットに、IPマスカレードを適用します。

interface tunnel mode

◆ ip (snat-group|dnat-group)

<説　　明>
・global mode で設定した SNAT または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。
・SNAT は、パケットの出力時に適用されます。DNAT は、パケットの入力時に適用されます。

<書　　式>　ip (snat-group|dnat-group) NAT-NAME
<　No　>　no ip (snat-group|dnat-group)
<備　　考>　NAT ルールの設定は、ip snat/ip dnat)コマンド(global mode)で行います。

◆ ip webauth-filter

<説　　明>
・Web 認証フィルタをインタフェースに適用すると、ある特定のホスト、ネットワークやインタフェースについて、Web 認証せずに通信することが可能となります。
・Web 認証フィルタは、各インタフェースにつき、IN/OUT をそれぞれ一つずつ設定することができます。Default の設定はありません。

<書　　式>　ip webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
<　No　>　no ip webauth-filter (forward-in|forward-out)
<備　　考>
・Web 認証フィルタの設定については、ip web-auth access-list コマンド（global mode）を参照してください。
・Web 認証については、Web Authenticate mode を参照してください。

◆ ip spi-filter

<説　　明>
・簡易ファイヤウォールの一つとして、SPI（Stateful Packet Inspection）機能をサポートします。
・パケットに関連するコネクションの状態を見て、当該パケットをドロップするかしないかを決める機能です。

<書　　式>　ip spi-filter　（有効）
<初 期 値>　no ip spi-filter（無効）
<　No　>　no ip spi-filter
<備　　考>
・コネクションの状態が、established または related の場合に、パケットの転送を許可します。
　・Established とは、すでに双方向でパケットの通信がありコネクションが確立されている状態です。
　・Related とは、すでに確立しているコネクションがある状態です。FTP のデータ転送等がこれに該当します。
・新しい接続でありながら、syn ビットの立っていないパケットはドロップします。
・SPI は、forward in および local input の位置で適用されます。ユーザが適用位置を変更することは出来ません。

◆ ipv6 spi-filter

<説　　明>　IPv6 SPI filter を設定します。
<書　　式>　ipv6 spi-filter
<初 期 値>　no ipv6 spi-filter
<　no　>　no ipv6 spi-filter

interface tunnel mode

◆ ip spi-filter log
◆ ipv6 spi-filter log

＜説　　明＞　フィルタログ機能（syslog mode参照）を有効にします。
　　パケットが、SPIフィルタにマッチした場合、syslogに出力することが出来ます。
＜書　　式＞　ip spi-filter log [limit <0-100>]
　　ipv6 spi-filter log [limit <0-100>]
＜初 期 値＞　ip spi-filter log limit 10
　　ipv6 spi-filter log limit 10
＜　No　＞　no ip spi-filter
　　no ipv6 spi-filter
＜備　　考＞
・limitを指定すると、1秒当たりのログ出力数を制限します。初期値は、10パケット/秒です。
・WAN側からの意図しないパケットが、SPIフィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分に注意してください。

◆ netevent

＜説　　明＞
・トラックイベントの発生時に、当該tunnelをconnect(またはdisconnect)することが出来ます。
＜書　　式＞　netevent <trackid:1-255> (connect|disconnect)
　　netevent <trackid:2048-4095> (connect|disconnect)
＜　no　＞　no netevent

◆ ipv6 nd accept-redirects

＜説　　明＞　IPv6 forwardingが無効の場合に、ICMPv6 redirectsを受け入れるかどうかを指定します。
＜書　　式＞　ipv6 nd accept-redirects
＜初 期 値＞　no ipv6 nd accept-redirects
＜備　　考＞　IPv6 forwardingが有効な場合は、この設定に関係なく受信しません。
＜　no　＞　no ipv6 nd accept-redirects

interface tunnel mode

◆ ipsec policy

＜説　　明＞　当該インタフェースで使用するIPsecローカルポリシーを設定します。
＜書　　式＞　ipsec policy <local policy:1-255>
＜　No　＞　no ipsec policy (|<local policy:1-255>)
＜備　　考＞
・各インタフェースに、IPsecローカルポリシーを4つまで設定することが出来ます。他のインタフェースで既に設定しているIPsecローカルポリシーは、重複して設定できません。

◆ ipsec policy-ignore

＜説　　明＞
・IPsec policy のチェックを行わないように指定する機能です。IPsec policy としてany などを指定したけれども、特定の通信のみIPsec化したくない場合に、この機能を使用します。
＜書　　式＞ ipsec policy-ignore (|input|output)
＜初 期 値＞ no ipsec policy-ignore（無効）
＜　No　＞ no ipsec policy-ignore
＜備　　考＞
・Inputを指定した場合、inbound policy check を実行しないため、IPsec 化されてくるべきパケットがドロップ されてしまう現象を回避することができます。
・Output を指定した場合、当該インタフェースから出力されるパケットは、IPsec policy をチェックしないため平文で送信されます。

interface tunnel mode

■ QoS

＜説　　明＞　QoSの設定をします。

○ HTBの設定

＜書　　式＞　queue policy POLICYNAME bandwidth <1-1000000>

＜備　　考＞

- HTBを設定するには、class policyコマンドで作成したclass policyを指定します。
- 存在しないclass policyを指定すると、親classのみ設定されます。該当するclass policyを作成したときに、当該HTBが設定されます。
- bandwidthで、class policyの全帯域幅を指定します。

○ PQの設定

＜書　　式＞　queue priority-group <PRIORITY-MAP-NUMBER:1-32>

＜備　　考＞

- PQを設定するには、global modeで作成したpriority-mapを指定します。
- 存在しないpriority-mapを指定すると、すべてのパケットをdefault classにマッピングするPQが設定されます。該当するpriority-mapを作成したときに、当該PQが設定されます。
- どのclassにも該当しないパケットは、default classにマッピングされます。

○ SFQの設定

＜書　　式＞　queue fair-queue

○ FIFOの設定

＜書　　式＞　queue fifo (|limit <1-16384>)

＜備　　考＞　limitでFIFOキューの長さを指定することが出来ます。

○ TBF(shaping)の設定

＜書　　式＞

queue shape <RATE:1-1000000> <BUFFER:1-1000000> <LIMIT:1-1000000>

＜備　　考＞

- <RATE:1-1000000>　Shapingレート(Kbps)を指定します。
- <BUFFER:1-1000000>　Bucketのサイズ(bytes)を指定します。
- <LIMIT:1-1000000>　Tokenが利用可能になるまでにバッファすることが出来るキューの長さ(bytes)を指定します。

○ no queue

＜書　　式＞　no queue

＜備　　考＞　上記で設定したqueueを削除して、default queue（pfifo_fast）に設定します。

interface tunnel mode

■ QoS（続き）

○ classify

＜書　　式＞　classify (input|output) route-map ROUTEMAP

＜備　　考＞

・インタフェースにルートマップを適用します。1つのインタフェースに、input と output を別々に設定することが出来ます。

・input で指定したルートマップは、PRE-ROUTING(付録の Packet Traveling を参照)で適用されます。

・output で指定したルートマップは、POST-ROUTING(付録の Packet Traveling を参照)で適用されます。

○ no classify

＜書　　式＞　no classify (|input|output)

＜備　　考＞

・インタフェースに適用したルートマップを削除します。

・「no classify」を実行すると、両方(input と output)を削除します。片方だけを削除する場合は、input または output を指定します。

interface tunnel mode

◆(ip|ipv6) rebound
<説　　明>
・下位ルータから受信したパケットを、受信インタフェースと同一インタフェースから出力(forwarding)した場合、下位ルータから本装置に対して再度パケットが送信されてくるため、下位ルータと本装置の間でTTLが「0」になるまでパケットがループします。
・IP rebound機能を無効にすると、受信インタフェースと送信インタフェースが同一の場合、パケットをドロップし、かつ送信元にdestination unreachableを送信します。
・Defaultは、有効です(受信インタフェースと送信インタフェースが同一でもドロップしません)。
<書　　式>　(ip|ipv6) rebound
<初 期 値>　(ip|ipv6) rebound
<　no　>　no (ip|ipv6) rebound

◆ip reassemble-output
<説　　明>
・インタフェースのMTU（あるいはPMTU）より大きいパケットをIP forwardingする際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。本設定有効時、本装置がリアセンブルしたパケットは、以下のようにフラグメント処理を行います。
- fragmented packet(パケットの断片)がMTUを超える場合、リアセンブルしたパケットを再度MTUサイズにフラグメントして出力します。
- fragmented packet(パケットの断片)がMTUより小さい場合、受信したfragmented packetのサイズで出力します。
- パケット全体のサイズがMTUより小さい場合、リアセンブルしたパケットを出力します。
<書　　式>　ip reassemble-output
<初 期 値>　ip reassemble-output
<　no　>　no ip reassemble-output
<備　　考>
・上記の場合（本設定が有効の場合）、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易なIP実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズで本装置からパケットを出力します。また、出力時のIPフラグメント処理は、次のようになります。
- fragmented packet(パケットの断片)がMTUを超える場合、受信したfragmented packetをMTUサイズにフラグメントして出力します。
- fragmented packet(パケットの断片)がMTUより小さい場合、受信したfragmented packetのサイズで出力します。
- パケット全体のサイズがMTUより小さい場合、受信したfragmented packetをそのままのサイズで出力します。
・Defaultは、global設定およびinterface設定ともに有効です。Global設定とinterface設定のAND条件により、本機能が有効か無効かを判定します。本設定は、IP forwardingするパケットにのみ影響します。
・受信時のサイズを記載しておくバッファが32 個しかないため、33 個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-output が有効な場合と同様に処理します。

interface tunnel mode

◆session invalid-status-drop-interface

＜説　　明＞

・session invalid-status-drop機能(global mode参照)をインタフェース毎に指定することができます。

・本機能は、default で無効です。

＜書　　式＞　session invalid-status-drop-interface enable

＜初 期 値＞　no session invalid-status-drop-interface enable

＜　no　＞　no session invalid-status-drop-interface enable

＜備　　考＞

・あるインタフェースに対してのみ適用したい場合は、global mode で session invalid-status-drop 機能を無効にして、かつ本機能を指定インタフェースで有効にします。以下は、tunnel 0インタフェースに適用する場合の設定例です。

- global mode で、session invalid-status-drop を無効にします。

```
vxr-x86(config)#no session invalid-status-drop enable
```

- 指定インタフェースで、本機能を有効にします。

```
vxr-x86(config)#interface tunnel 0
vxr-x86(config-tunnel)#session invalid-status-drop-interface enable
```

◆ ip p2p-detection

＜説　　明＞　P2P 検出機能を有効にします（IPv4 のみ対応）。

＜書　　式＞　ip p2p-detection (any|winny|share|bittorrent) {log|deny}

＜　no　＞　no ip p2p-detection

　　no ip p2p-detection (winny|share|bittorrent)

＜備　　考＞

・インターネットに接続しているインタフェース上でのみ有効にすることを推奨します。

・詳細については、「付録 K：P2P 検出機能」を参照してください。

interface tunnel mode

◆ tunnel hop-limit
＜説　　明＞　IPv6 hop-limit値を指定します。
＜書　　式＞　tunnel hop-limit <1-255>
＜初 期 値＞　tunnel hop-limit 64
＜　no　＞　no tunnel hop-limit
＜備　　考＞　指定のない場合は、システム初期値(64)を使用します。

◆ tunnel traffic-class
＜説　　明＞　トンネルIPv6ヘッダのトラフィッククラスフィールドに設定する値を指定します。
＜書　　式＞　tunnel traffic-class <0-252>
　　tunnel traffic-class inherit
＜初 期 値＞　tunnel traffic-class inherit
＜　no　＞　no tunnel traffic-class
＜備　　考＞
・inheritを指定した場合、トネリングパケットのヘッダ部のToS値またはトラフィッククラスを、トンネルIPv6ヘッダのトラフィッククラスフィールドにコピーします。
・値を指定する場合、0-252の範囲で指定することが出来ます。ただし、ECNフィールドを設定することはできません。
※ECN field の扱いについては、「付録B 1.2.4.1 ECN field の扱い」を参照してください。

◆ tunnel 6rd prefix
＜説　　明＞　6rdのプレフィクスを指定します。
　　通常、6rdサービスを提供しているサービスプロバイダーから割り当てられます。
＜書　　式＞　tunnel 6rd prefix X:X::/M
＜　no　＞　no tunnel 6rd prefix
＜備　　考＞　6rd作成時に、必ず設定してください。

◆ tunnel 6rdipv4 prefix-length
＜説　　明＞
・RFC5569では、IPv6アドレスに埋め込むIPv4アドレス長は、32ビット固定でしたが、RFC5959では、埋め込むIPv4アドレスの長さを指定することが出来ます。
＜書　　式＞　tunnel 6rd ipv4 prefix-length <0-32>
＜初 期 値＞　tunnel 6rd ipv4 prefix-length 0
＜　no　＞　no tunnel 6rd ipv4 prefix-length
＜備　　考＞
・初期値は、0です（32ビットすべてが埋め込まれます）。
・32-prefix-lenghthの部分がhost部として、IPv6アドレスに埋め込まれます。この長さを変えることにより、ユーザが使用できるネットワークを格段に増やすことが出来るようになります。

interface tunnel mode

◆ (ip|ipv6) tcp strip-options

＜説　　明＞

・TCP パケット内のオプションを stip する機能です。

・Fast-forwarding が有効な場合、SACK/timestamp/MD5 については、strip されない場合があります。

＜書　　式＞　(ip|ipv6) tcp strip-options
(all|md5|mss|sack|sack-permitted|timestamp|wscale)

＜初 期 値＞　no (ip|ipv6) tcp strip-options

＜　No　＞　no (ip|ipv6) tcp strip-options

＜備　　考＞　Strip 可能なオプションと監視するパケットの種類は、次のとおりです。

TCPオプション	該当TCPパケット
MSS	SYN/SYN-ACK
Window Scale Option	SYN/SYN-ACK
SACK Permitted	SYN/SYN-ACK
SACK	すべてのTCPパケット
Time Stamp Option	すべてのTCPパケット
MD5 signature Option	すべてのTCPパケット

第 8 章

interface ppp mode

interface ppp mode

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#interface ppp <0-4>
vxr-x86(config-ppp)#
```

◆ description

＜説　　明＞　interfaceの説明を記述します。
＜書　　式＞　description DESCRIPTION
＜　no　＞　no description (|DESCRIPTION)

◆ ip address

＜説　　明＞　インタフェースにIPアドレスを付与します。
＜書　　式＞　ip address A.B.C.D/M
＜　no　＞　no ip address (|A.B.C.D/M)

◆ ip address

＜説　　明＞　PPP接続のIPアドレスを自動取得に設定します。
＜書　　式＞　ip address negotiated
＜　no　＞　no ip address negotiated

◆ ipv6 address

＜説　　明＞　IPv6アドレスを設定します。
＜書　　式＞　ipv6 address X:X::X:X/M (|eui-64) : IPv6 address (e.g. 3ffe:506::1/48)
＜備　　考＞　eui-64指定時は、ipv6-addressはprefix部のみ指定します。
　　ホスト部は、interface-id設定に依存します。
　　LLAもinterface-id設定によって決定されます。
＜　no　＞　no ipv6 address X:X::X:X/M (|eui-64)

◆ ipv6 address

＜説　　明＞　DHCPv6 PDの設定をします。
＜書　　式＞　ipv6 address DHCPv6PD X:X::X:X/M (|eui-64)　: DHCPv6-PD prefix name
＜備　　考＞
- ipv6-addressは、sub-prefixとhost部を指定可能です。
- PREFIX-NAMEは、dhcpv6 pdで受信するprefixに名前をつけたもので、ipv6 dhcp client pdで設定します。

＜　no　＞　no ipv6 address DHCPv6PD X:X::X:X/M

interface ppp mode

◆ bandwidth
＜説　　明＞　インタフェースの帯域幅を設定することが出来ます。
　　bandwidth の最大値は、10Gbps です。
＜書　　式＞　bandwidth <1-10000000000[k/m/g]>
＜　no　＞　no bandwidth
＜備　　考＞　本機能は、OSPF のコスト計算時のみに使用します。
　　基準となる帯域幅は、auto-cost コマンド(ospf mode)にて設定します。

◆ mtu
＜説　　明＞　MTU の値を設定します。
＜書　　式＞　mtu <bytes:68-1500>
＜初 期 値＞　mtu 1454
＜　no　＞　no mtu　(= Set defaults)

◆ ppp lcp mru
＜説　　明＞　MRU を設定します。
＜書　　式＞　ppp lcp mru <bytes:128-1500>
＜初 期 値＞　ppp lcp mru 1454
＜　no　＞　no ppp lcp mru　(= Set defaults)
＜備　　考＞　IPv6 を使用する場合は、MRU を 1280 以上に設定してください。

◆ ipv6 dhcp client
＜説　　明＞　当該インタフェースに適用する DHCPv6 クライアントのプロファイル名を指定します。
＜書　　式＞　ipv6 dhcp client WORD
＜　no　＞　no ipv6 dhcp client

◆ ipv6 dhcp client pd
＜説　　明＞ DHCPv6 PD の prefix 部に、プロファイル名を付けます。
＜書　　式＞ ipv6 dhcp client pd DHCPv6-PD
＜ no ＞ no ipv6 dhcp client
＜備　　考＞
・DHCPv6 PD を受信するインタフェース上で設定します。
・受信した DHCPv6 PD を(異なる)インタフェースに対して適用するには、ipv6 address DHCPv6-PD コマンドを使用します。
・ipv6 dhcp client WORD と ipv6 dhcpv6 pd DHCPv6-PD は、どちらか一方だけ設定可能です。

interface ppp mode

◆ ip redirects

＜説　　明＞
- ICMP redirect（type=5）とは、同一ネットワーク上に他の最適なルートがあることを通知するためのメッセージです（RFC792）。
- 本装置の Send redirect 機能によって、ICMP redirect の送信の有無を切り替えることが出来ます。

＜書　　式＞　ip redirects
＜初 期 値＞　ip redirects　　(有効)
＜　No　＞　no ip redirects　(無効)
＜備　　考＞
- ICMPRedirect の例は、interface mode の ip redirects を参照して下さい。

◆ ip tcp adjust-mss

＜説　　明＞
- Path MTU Discovery（PMTUD）機能（End-to-end でフラグメントが発生しない最大の MTU を発見すること）によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器（ルータ等）が ICMP fragment needed をフィルタリングしている場合（ブラックホールルータが存在する場合）や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、End-to-end での通信に支障をきたすことになります。このような場合、TCP では SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

＜書　　式＞　ip tcp adjust-mss (auto|<500-1460:bytes>)
＜初 期 値＞　no ip tcp adjust-mss
＜　No　＞　no ip tcp adjust-mss
＜備　　考＞
- IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。
- 本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。
- ユーザが設定する場合は、MSS 値を指定します。元の MSS 値に関係なく指定した値に強制的に変更します。
- UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。
- 「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

◆ ipv6 tcp adjust-mss

＜説　　明＞　TCP/IPv6 の MSS 値を設定します。
＜書　　式＞　ipv6 tcp adjust-mss (auto|<bytes:500-1440>)
＜初 期 値＞　no ipv6 tcp adjust-mss
＜　no　＞　no ipv6 tcp adjust-mss

interface ppp mode

◆ ip mask-reply

＜説　　明＞

・OpenView などの監視装置では、監視ネットワーク内の機器に対して ICMP address mask request（type=17）を送信することによって機器のインタフェースのネットマスク値を取得します（単純に、死活監視で使用する場合もあります）。

・本装置では、ICMP address mask request への応答の有無を設定することが出来ます。

＜書　　式＞　ip mask-reply　（ICMP address mask request に応答します。）

＜初 期 値＞　no ip mask-reply（ICMP address mask request に応答しません。）

＜　No　＞　no ip mask-reply

＜備　　考＞

・ICMP address mask request/reply の例は、interface mode の ip mask-reply を参照して下さい。

◆ ip send-source

＜説　　明＞

・PPP interface に設定されている ip address を source ip とする packet を出力する際、main の routing table で指定された interface ではなく、必ず ip の所有者である ppp interface から出力する機能です。この機能が有効な場合、PPP の IP address を source とする packet で、かつ本装置より出力される packet は、IPsec policy に match しなくなります。

・Local オプションが設定された場合、PPP send-source 機能の対象が、本装置からの自発 packet のみとなります。IP nat-loopback 機能と併用する場合は、本機能を有効にしてください。

＜書　　式＞　ip send-source (|local)

＜初 期 値＞　no ip send-source

＜　no　＞　no ip send-source

＜備　　考＞　Default は、無効です。また、IPv4 のみ対応しています。

interface ppp mode

◆ ip nat-loopback

＜説　　明＞

・1つのglobal IPを使用して複数のWeb/Mail serverなどを公開する際、DNAT機能により内部serverへの転送を行うことがあります。このとき、同じNAT router配下の端末よりglobal IPに対してaccessしても、DNAT変換が行われないため、global IPによるaccessができません。このような場合に、ip nat-loopback機能を使用します。

・この機能が有効な場合、global IPを持たないinterfaceからglobal IPに対してaccessが行われた場合、本装置自身で受信せず、一度main routing tableに従って転送されます（main routingに該当routeが存在しない場合は、強制的にglobal IPが設定されているppp interfaceへと出力されます）。その後、ISP側から戻ってきたpacketをDNATすることで、NAT配下の端末からもglobal IPに対してaccessを行うことができるようになります。

＜書　　式＞　ip nat-loopback

＜初 期 値＞　no ip nat-loopback

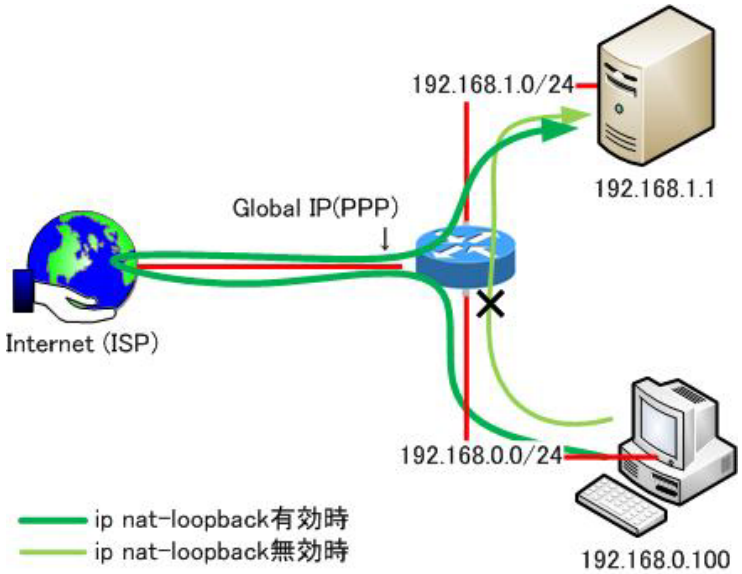
＜　no　＞　no ip nat-loopback

＜備　　考＞

・本機能は、defaultで無効とし、PPP interface上でのみ利用することができます。

・ip nat-loopbackを設定しているinterface上でSPIが有効な場合は、SPIを無効にするか、またはFILTERによって通過させたいpacketを許可してください。

・また、該当のPPP interfaceではNAT(もしくはMasquerade)を設定してください。未設定の場合、PCより公開serverへのaccess時、ISPよりヘアピンされてきたpacketが、LANからのaccess時に作成されたconntrackにmatchしてしまうため、DNATが実行されず公開serverへのaccessができません。



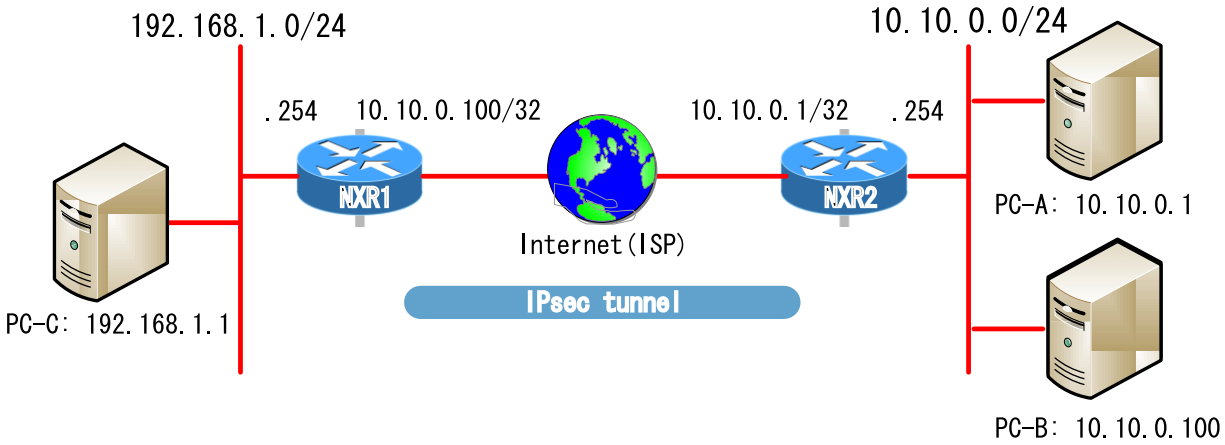
・VXRではGlobal IP(PPP):80に対するaccessがきた場合192.168.1.1にDNATする設定がされています。

・PCよりGlobal IP(PPP):80にaccessします。

interface ppp mode

○ ip nat-loopback による address の重複への対応

ip nat-loopback を利用すると、次のような構成でも通信が可能となります。



・PC-C と PC-A、および PC-C と PC-B の通信が可能です。

・PC-A と PC-B の通信が可能です。

・各 PC と NXR1/NXR2 の WAN IP(NXR1:10.10.0.100/NXR2:10.10.0.1)は、通信することが出来ません。

このように、LAN と WAN で通信範囲が完全に分割される構成になります。

なお、この構成で IPsec トンネルを確立するには、NXR1/NXR2 で ip send-source を設定し、IKE(および ESP)パケットが必ず PPP に出力されるようにします。

また、NXR1/NXR2 の WAN 側 IP へのデフォルトルートの設定や、対向のグローバル IP へのスタティックルートの設定を行うことは出来ません。

interface ppp mode

◆ keepalive lcp-echo

<説　　明>　LCP echo requestによるキープアライブを有効にします。
<書　　式>　keepalive lcp-echo (|<interval:30-600> <failure-count:1-10>)
<初 期 値>　keepalive lcp-echo 30 3
<　no　>　no keepalive lcp-echo
<備　　考>

・lcp-echo request/replyの連続失敗回数が、failure countの設定回数に達すると、PPPを切断します。

◆ keepalive icmp-echo

<説　　明>　ICMP echo requestを有効にします。
<書　　式>　keepalive icmp-echo (|<interval:30-600> <retry:0-10> A.B.C.D)
<初 期 値>　no keepalive icmp-echo
<備　　考>　keepalive icmp-echoは、keepalive icmp-echo 30 2と同じ
<　no　>　no keepalive icmp-echo

◆ ip rip receive version

<説　　明>　RIPの受信バージョンを設定します。
<書　　式>　ip rip receive version (1|2) (|1|2)
<初 期 値>　ip rip receive version 2
<備　　考>　両方指定も可能（ip rip receive version 1 2）
<　no　>　no ip rip receive version

◆ ip rip send version

<説　　明>　RIPの送信バージョンを設定します。
<書　　式>　ip rip send version (1|2) (|1|2)
<初 期 値>　ip rip send version 2
<備　　考>　両方指定も可能（ip rip send version 1 2）
<　no　>　no ip rip send version

◆ ip rip split-horizon

<説　　明>　スプリットホライズンを設定します。
<書　　式>　ip rip split-horizon (|poisoned)
<初 期 値>　ip rip split-horizon
<　no　>　no ip rip split-horizon

interface ppp mode

◆ ip access-group

＜説　　明＞

・global mode で設定した ACL をインタフェースに適用することで、パケットフィルタリングを行うことができます。

＜書　　式＞　ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME

＜　No　＞　no ip access-group (in|out|forward-in|forward-out)

＜備　　考＞

・各インタフェースへのパケットフィルタリングの適用箇所(付録の Packet Traveling を参照)は、以下の 4ヶ所です。

- in(local input)　本装置自身で受信して処理するパケットを制限します。
- out(local output) 本装置自身が作成して出力するパケットを制限します。
  トンネリングされたパケットも VXR 自身が作成したパケットとして認識します。
- forward-in　本装置が当該インタフェースで受信して forwarding するパケットを制限します。
- forward-out 本装置が受信して当該インタフェースへ forwarding するパケットを制限します。

・mac 指定のある ACL は、out および forward-out に設定することは出来ません。

◆ ipv6 access-group

＜説　　明＞　アクセスグループに IPv6 アクセスリストを追加します。

＜書　　式＞　ipv6 access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME

＜初 期 値＞　no ipv6 access-group (in|out|forward-in|forward-out)

＜　no　＞　no ipv6 access-group (in|out|forward-in|forward-out)

◆ ip masquerade

＜説　　明＞

・インタフェースよりパケットを出力する際に、パケットの送信元 IPv4 アドレスを出力インタフェースの IPv4 アドレスに自動変換する機能です。

＜書　　式＞　ip masquerade　（有効）

＜初 期 値＞　no ip masquerade（無効）

＜　No　＞　no ip masquerade

＜備　　考＞

・すべてのインタフェース(Ethernet/VLAN/PPP/Tunnel)で設定することが出来ます。

・TCP/UDP/ICMP のみ対応しています。その他のプロトコルに関しては、動作は保証しません。

・IPv6 パケットは、IP マスカレードの対象外です。

・forward out/local output フィルタリング適用後のパケットに、IP マスカレードを適用します。

◆ ip (snat-group|dnat-group)

＜説　　明＞

・global mode で設定した SNAT または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。

・SNAT は、パケットの出力時に適用されます。DNAT は、パケットの入力時に適用されます。

＜書　　式＞　ip (snat-group|dnat-group) NAT-NAME

＜　No　＞　no ip (snat-group|dnat-group)

＜備　　考＞　NAT ルールの設定は、ip snat/ip dnat)コマンド(global mode)で行います。

interface ppp mode

◆ ip webauth-filter

＜説　　明＞

・Web 認証フィルタをインタフェースに適用すると、ある特定のホスト、ネットワークやインタフェースについて、Web 認証せずに通信することが可能となります。

・Web 認証フィルタは、各インタフェースにつき、IN/OUT をそれぞれ一つずつ設定することができます。Default の設定はありません。

＜書　　式＞　ip webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME

＜　No　＞　no ip webauth-filter (forward-in|forward-out)

＜備　　考＞

・Web 認証フィルタの設定については、ip web-auth access-list コマンド（global mode）を参照してください。

・Web 認証については、Web Authenticate mode を参照してください。

◆ ip spi-filter

＜説　　明＞

・簡易ファイヤウォールの一つとして、SPI（Stateful Packet Inspection）機能をサポートします。

・パケットに関連するコネクションの状態を見て、当該パケットをドロップするかしないかを決める機能です。

＜書　　式＞　ip spi-filter　（有効）

＜初 期 値＞　no ip spi-filter（無効）

＜　No　＞　no ip spi-filter

＜備　　考＞

・コネクションの状態が、established または related の場合に、パケットの転送を許可します。

・Established とは、すでに双方向でパケットの通信がありコネクションが確立されている状態です。

・Related とは、すでに確立しているコネクションがある状態です。FTP のデータ転送等がこれに該当します。

・新しい接続でありながら、syn ビットの立っていないパケットはドロップします。

・SPI は、forward in および local input の位置で適用されます。ユーザが適用位置を変更することは出来ません。

◆ ipv6 spi-filter

＜説　　明＞　IPv6 SPI filter を設定します。

＜書　　式＞　ipv6 spi-filter

＜初 期 値＞　no ipv6 spi-filter

＜　no　＞　no ipv6 spi-filter

interface ppp mode

◆ ip spi-filter log
◆ ipv6 spi-filter log

＜説　　明＞　フィルタログ機能（syslog mode 参照）を有効にします。
　　パケットが、SPI フィルタにマッチした場合、syslog に出力することが出来ます。
＜書　　式＞　ip spi-filter log [limit <0-100>]
　　ipv6 spi-filter log [limit <0-100>]
＜初 期 値＞　ip spi-filter log limit 10
　　ipv6 spi-filter log limit 10
＜　No　＞　no ip spi-filter
　　no ipv6 spi-filter
＜備　　考＞
・limit を指定すると、1 秒当たりのログ出力数を制限します。初期値は、10 パケット / 秒です。
・WAN 側からの意図しないパケットが、SPI フィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分に注意してください。

◆ ppp authentication

＜説　　明＞　PPP の認証プロトコルを設定します。
＜書　　式＞　ppp authentication (chap|pap|auto)
＜初 期 値＞　ppp authentication auto
＜　no　＞　no ppp authentication (= ppp authentication auto)

◆ ppp username

＜説　　明＞　PPP 接続のユーザー ID とパスワードを設定します。
＜書　　式＞　ppp username USERID password (|hidden) PASSWORD
　　ppp username USERID
＜　no　＞　no ppp username
＜備　考＞
・パスワードは、1-95 文字以内で設定してください。使用可能な文字は、英数字および!$#=*+-_.:;(){}[]^~@`<>%?です。
・ppp account コマンド（global mode）で設定した USERID と PASSWORD を使用する場合は、USERID のみを指定します。
・パスワードに「?」を入力する場合は、「Ctrl」+「v」を入力してから、「?」を入力してください。

◆ ppp auto-connect

＜説　　明＞　PPP の自動接続を有効にします。
＜書　　式＞　ppp auto-connect <seconds:10-600>
＜初 期 値＞　ppp auto-connect 60
＜　no　＞　no ppp auto-connect

interface ppp mode

■ NCP

○ppp ncp max-configure

＜説　　明＞　IPCP configuration request の最大再送回数(初期値：10回)を設定します。
　　再送間隔は3秒(固定)です。
＜書　　式＞　ppp ncp max-configure <1-20>
＜初 期 値＞　ppp ncp max-configure 10
＜　no　＞　no ppp ncp max-configure

○ppp ncp max-failure

＜説　　明＞　configuration request 送信 / 受信の最大失敗回数（初期値：5回）を設定します。
＜書　　式＞　ppp ncp max-failure <1-255>
＜初 期 値＞　ppp ncp max-failure 5
＜　no　＞　no ppp ncp max-failure
＜備　　考＞
・再送回数は、timeout によってインクリメントするため、NAK を受信して再度 configuration request を送信するような場合は再送回数としてカウントしません。したがって、configuration request の送信に対して、RAS が NAK を返信し続けると、NCP が終了しないことになります。
・configuration request の送信＋ NAK の受信を max failure 回数繰り返すと、それ以降のパケットをすべて reject し、request に対する応答（情報）はすべて無視します。以降の configuration request パケットには、オプションを含まない形で送信し、応答で受信した情報(IP アドレス)を元に再度 configuration request を送信します。この configuration request に対する ACK 受信によって、IPCP が完了します。
・configuration request の受信＋ NAK による応答の場合、max failure 回数目の configuration request の受信に対して、configuration reject で応答します。

○ppp ncp max-terminate

＜説　　明＞　configuration request 送信 / 受信の最大失敗回数（初期値：5回）を設定します。
＜書　　式＞　ppp ncp max-terminate <1-10>
＜初 期 値＞　ppp ncp max-terminate 2
＜　no　＞　no ppp ncp max-terminate

※上記設定を有効にするには、IPCP/IPv6CP を enable にしてください。

interface ppp mode

◆ ppp ipcp enable
<説　　明>　IPCPを有効にします。
<書　　式>　ppp ipcp enable
<初 期 値>　ppp ipcp enable
<　no　>　no ppp ipcp enable

◆ ppp ipcp dns
<説　　明>　IPCPのDNSオプションを設定します。
<書　　式>　ppp ipcp dns accept
　　ppp ipcp dns reject
　　ppp ipcp dns <primary:A.B.C.D> (|<secondary:A.B.C.D>)
<初 期 値>　ppp ipcp dns accept
<　no　>　no ppp ipcp dns
<備　考>　acceptを指定した場合、プロバイダから自動的に割り当てられるDNSを使用します。
　　rejectを指定した場合、プロバイダから割り当てられるDNSを使用しません。
　　IPアドレスを指定して、DNSを手動で設定することも出来ます。
　　WINSサーバオプションには対応していません。

◆ ppp ipcp ip request
<説　　明>　IPCPでIPアドレスをリクエストします。
<書　　式>　ppp ipcp ip request
<初 期 値>　no ppp ipcp ip request
<　no　>　no ppp ipcp ip request
<備　　考>　ip addressコマンドで指定したIPをIPCPでrequestします。

◆ ppp ipv6cp enable
<説　　明>　IPv6CPを有効にします。
<書　　式>　ppp ipv6cp enable
<初 期 値>　no ppp ipv6cp enable
<　no　>　no ppp ipv6cp enable　（無効）

◆ ppp ipv6cp id
<説　　明>　IPv6CPインタフェースIDを設定します。
<書　　式>　ppp ipv6cp id X:X::X:X
　　ppp ipv6cp id ethernet <0-2>
<初 期 値>　no ppp ipv6cp id
<備　　考>　指定ない場合は、eth0のmacを使用します。この設定によりLLAが決定されます。
<　no　>　no ppp ipv6cp id

interface ppp mode

◆ ppp on-demand
＜説　　明＞　On-demand PPP を設定します。
＜書　　式＞　ppp on-demand
＜　no　＞　no ppp on-demand
＜備　　考＞　Mobile/PPPoE/BRI 使用時に、本機能を有効にすることが出来ます。
　　L2TP、IPv6CP 有効時は、無視されます。

◆ ppp idle-timeout
＜説　　明＞
・idle-timeout で設定した時間内に、IP パケットの送受信がない場合、PPP を切断する（あるいは on-demand 状態へと遷移する）機能です。
・idle-timeout は、PPP 上での IP/IPv6 パケットの送受信のみで更新します。
・LCP echo-request/reply は、idle-timeout の更新対象ではありません。
＜書　　式＞　ppp idle-timeout (<sec:30-86400>|)
＜備　　考＞　ondemand 有効時(l2tp,ipv6cp 時は無視します)、時間指定ない場合は 180sec です。
　　ondemand 無効時でも動作します。
＜　no　＞　no ppp idle-timeout　(ondemand 有効時は、ppp idle-timeout 180)

◆ ppp idle-timeout & system sleep
＜説　　明＞　PPP idle-timeout による PPP 切断時、system sleep 状態に移行します。
＜書　　式＞　ppp idle-timeout <30-86400> system sleep
　　ppp idle-timeout <30-86400> system sleep timer <1-31536000>
　　ppp idle-timeout <30-86400> system sleep schedule <NUM>
＜備　　考＞　timer を設定しない場合は、365 日間（31,536,000[sec]）が設定されます。
　　スケジュール機能で resume させる場合は、resume の schedule 番号を指定します。

◆ netevent
＜説　　明＞
・トラックイベントの発生時に、当該 ppp を connect(または disconnect、あるいは reconnect)することが出来ます。
＜書　　式＞　netevent <trackid:1-255> (connect|disconnect|reconnect)
　　netevent <trackid:2048-4095> (connect|disconnect|reconnect)
＜　no　＞　no netevent

◆ ipv6 nd accept-redirects
＜説　　明＞
・IPv6 forwarding が無効の場合に、ICMPv6 redirects を受け入れるかどうかを指定します。
＜書　　式＞　ipv6 nd accept-redirects
＜初 期 値＞　no ipv6 nd accept-redirects
＜備　　考＞　IPv6 forwarding が有効な場合は、この設定に関係なく受信しません。
＜　no　＞　no ipv6 nd accept-redirects

interface ppp mode

◆ ipsec policy
＜説　　明＞　当該インタフェースで使用するIPsecローカルポリシーを設定します。
＜書　　式＞　ipsec policy <local policy:1-255>
＜　No　＞　no ipsec policy (|<local policy:1-255>)
＜備　　考＞
・各インタフェースに、IPsecローカルポリシーを4つまで設定することが出来ます。他のインタフェースで既に設定しているIPsecローカルポリシーは、重複して設定できません。

◆ ipsec policy-ignore
＜説　　明＞
・IPsec policy のチェックを行わないように指定する機能です。IPsec policy としてany などを指定したけれども、特定の通信のみIPsec 化したくない場合に、この機能を使用します。
＜書　　式＞ ipsec policy-ignore (|input|output)
＜初 期 値＞ no ipsec policy-ignore（無効）
＜　No　＞ no ipsec policy-ignore
＜備　　考＞
・Inputを指定した場合、inbound policy check を実行しないため、IPsec 化されてくるべきパケットがドロップ されてしまう現象を回避することができます。
・Output を指定した場合、当該インタフェースから出力されるパケットは、IPsec policy をチェックしないため平文で送信されます。

◆ ipsec hold-sa
＜説　　明＞
・PPP上でIPsecを利用する場合に、PPP切断と共にIPsec SAを削除するかどうかを指定する機能です。
・PPPのIPが動的に割り当てられる場合、PPPのdownが発生すると、IPsec SAの削除が行われます。このとき、本装置側から切断する場合は、PPP切断前にdelete SA送信を行い、その後PPP切断処理を行います。対向から切断される場合や障害によって切断される場合は、delete SAの送信処理は実行されません。
・一方、PPPのIP addressが固定割り当ての場合は、PPP切断時にIPsec SAを削除しません。しかし、本機能が無効となっている場合は、動的IPの場合と同様、PPP切断と共にIPsec SAの削除を行います。この際、本装置側から切断する場合は、delete SAを送信します。
＜書　　式＞　ipsec hold-sa
＜初 期 値＞　ipsec hold-sa
＜　no　＞　no ipsec hold-sa
＜備　　考＞
・本機能は、defaultで有効です。
・本機能の有効/無効は、固定IPの場合のみ影響します。動的IPの場合は、本機能の有効/無効に関らず、上記の動作となります。

interface ppp mode

■ QoS

＜説　　明＞　QoS の設定をします。

○ HTB の設定

＜書　　式＞　queue policy POLICYNAME bandwidth <1-1000000>

＜備　　考＞

- HTB を設定するには、class policy コマンドで作成した class policy を指定します。
- 存在しない class policy を指定すると、親 class のみ設定されます。該当する class policy を作成したときに、当該 HTB が設定されます。
- bandwidth で、class policy の全帯域幅を指定します。

○ PQ の設定

＜書　　式＞　queue priority-group <PRIORITY-MAP-NUMBER:1-32>

＜備　　考＞

- PQ を設定するには、global mode で作成した priority-map を指定します。
- 存在しない priority-map を指定すると、すべてのパケットを default class にマッピングする PQ が設定されます。該当する priority-map を作成したときに、当該 PQ が設定されます。
- どの class にも該当しないパケットは、default class にマッピングされます。

○ SFQ の設定

＜書　　式＞　queue fair-queue

○ FIFO の設定

＜書　　式＞　queue fifo (|limit <1-16384>)

＜備　　考＞　limit で FIFO キューの長さを指定することが出来ます。

○ TBF(shaping)の設定

＜書　　式＞

queue shape <RATE:1-1000000> <BUFFER:1-1000000> <LIMIT:1-1000000>

＜備　　考＞

- <RATE:1-1000000>　Shaping レート(Kbps)を指定します。
- <BUFFER:1-1000000>　Bucket のサイズ(bytes)を指定します。
- <LIMIT:1-1000000>　Token が利用可能になるまでにバッファすることが出来るキューの長さ(bytes)を指定します。

○ no queue

＜書　　式＞　no queue

＜備　　考＞　上記で設定した queue を削除して、default queue（pfifo_fast）に設定します。

interface ppp mode

■ QoS（続き）

○ classify

＜書　　式＞　classify (input|output) route-map ROUTEMAP

＜備　　考＞

・インタフェースにルートマップを適用します。1 つのインタフェースに、input と output を別々に設定することが出来ます。

・input で指定したルートマップは、PRE-ROUTING(付録の Packet Traveling を参照)で適用されます。

・output で指定したルートマップは、POST-ROUTING(付録の Packet Traveling を参照)で適用されます。

○ no classify

＜書　　式＞　no classify (|input|output)

＜備　　考＞

・インタフェースに適用したルートマップを削除します。

・「no classify」を実行すると、両方(input と output)を削除します。片方だけを削除する場合は、input または output を指定します。

interface ppp mode

■ dialer

＜説　　明＞　ダイヤルアップの設定をします。
＜書　　式＞
○接続先電話番号
　　dial-up string XXXXXXXXXX
○接続先電話番号の削除
　　no dial-up string
○dialup timeout (default:60sec)
　　dial-up timeout <sec:30-300>
○dialup timeoutの初期化
　　no dial-up timeout

■ mobile

＜説　　明＞　3Gデータ通信カードの設定をします。
＜書　　式＞
○APN設定
　　mobile apn XXXX cid XX pdp-type (ip|ppp)
○APN設定の初期化/削除（defaultにもどるか消去されるかは3G端末に依存します）
　　no mobile apn
＜備　　考＞
・NXR-G100/KTで、内蔵LTEモジュールを利用する場合、APN情報を初期化するには、以下のコマンドをすべて実行してください。
　　no mobile apn　　(interface ppp mode)
　　no mobile 1 ppp　　(global mode)
　　clear mobile 1（または、reset mobile 1）(view mode)
※no mobile apn，no mobile 1 pppを実行した後に、mobile error-recovery-resetによるリセットが発生した場合も、APN情報が初期化されます。
○接続時間制限
　　mobile limit time <sec:30-21474836>
○接続時間制限の無効化
　　no mobile limit time
○再接続時間制限
　　mobile limit reconnect <sec:30-86400>
○再接続時間制限の無効化
　　no mobile limit reconnect

interface ppp mode

◆ peer neighbor-route

＜説　　明＞

・IPCPによってpeer ip addressが割り当てられた際に、そのaddressに対するrouteを設定するかどうかを制御します。Defaultは、有効です。

＜書　　式＞　peer neighbor-route

＜初 期 値＞　peer neighbor-route

＜　no　＞　no peer neighbor-route

＜備　　考＞

・PPPにおいてICMP keepaliveが有効で、かつ送信先をpeer ipに設定している場合、本設定を無効にするとpeer ipへ到達できずPPPの切断が発生することが考えられます。したがって、ICMP keepaliveの送信先をpeer ipとしている場合は、本設定を有効のまま使用することを推奨します。

interface ppp mode

◆(ip|ipv6) rebound

＜説　　明＞

・下位ルータから受信したパケットを、受信インタフェースと同一インタフェースから出力(forwarding)した場合、下位ルータから本装置に対して再度パケットが送信されてくるため、下位ルータと本装置の間でTTLが「0」になるまでパケットがループします。

・IP rebound機能を無効にすると、受信インタフェースと送信インタフェースが同一の場合、パケットをドロップし、かつ送信元にdestination unreachableを送信します。

・Defaultは、有効です(受信インタフェースと送信インタフェースが同一でもドロップしません)。

＜書　　式＞　(ip|ipv6) rebound

＜初 期 値＞　(ip|ipv6) rebound

＜　no　＞　no (ip|ipv6) rebound

◆ip reassemble-output

＜説　　明＞

・インタフェースのMTU（あるいはPMTU）より大きいパケットをIP forwardingする際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。本設定有効時、本装置がリアセンブルしたパケットは、以下のようにフラグメント処理を行います。

- fragmented packet(パケットの断片)がMTUを超える場合、リアセンブルしたパケットを再度MTUサイズにフラグメントして出力します。
- fragmented packet(パケットの断片)がMTUより小さい場合、受信したfragmented packetのサイズで出力します。
- パケット全体のサイズがMTUより小さい場合、リアセンブルしたパケットを出力します。

＜書　　式＞　ip reassemble-output

＜初 期 値＞　ip reassemble-output

＜　no　＞　no ip reassemble-output

＜備　　考＞

・上記の場合（本設定が有効の場合）、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易なIP実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズで本装置からパケットを出力します。また、出力時のIPフラグメント処理は、次のようになります。

- fragmented packet(パケットの断片)がMTUを超える場合、受信したfragmented packetをMTUサイズにフラグメントして出力します。
- fragmented packet(パケットの断片)がMTUより小さい場合、受信したfragmented packetのサイズで出力します。
- パケット全体のサイズがMTUより小さい場合、受信したfragmented packetをそのままのサイズで出力します。

・Defaultは、global設定およびinterface設定ともに有効です。Global設定とinterface設定のAND条件により、本機能が有効か無効かを判定します。本設定は、IP forwardingするパケットにのみ影響します。

・受信時のサイズを記載しておくバッファが32個しかないため、33個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-outputが有効な場合と同様に処理します。

interface ppp mode

◆session invalid-status-drop-interface

＜説　　明＞

・session invalid-status-drop機能(global mode参照)をインタフェース毎に指定することができます。

・本機能は、default で無効です。

＜書　　式＞　session invalid-status-drop-interface enable

＜初 期 値＞　no session invalid-status-drop-interface enable

＜　no　＞　no session invalid-status-drop-interface enable

＜備　　考＞

・あるインタフェースに対してのみ適用したい場合は、global mode で session invalid-status-drop 機能を無効にして、かつ本機能を指定インタフェースで有効にします。以下は、ppp 0インタフェースに適用する場合の設定例です。

- global mode で、session invalid-status-drop を無効にします。

```
vxr-x86(config)#no session invalid-status-drop enable
```

- 指定インタフェースで、本機能を有効にします。

```
vxr-x86(config)#interface ppp 0
vxr-x86(config-ppp)#session invalid-status-drop-interface enable
```

■ メールヘッダ部の設定(メール送信機能)

＜説　　明＞
・送信するメールの各ヘッダ部に設定する値を指定します。本設定は、インタフェース毎（PPP <0-4>）に指定することが出来ます。
＜備　　考＞
・メール送信機能の詳細については、mail server mode を参照してください。

○ mail send server
＜説　　明＞　本設定で使用するメールサーバの番号を指定します。
＜書　　式＞　mail send server <0-2>
＜　No　＞　no mail send server
＜備　　考＞　メールサーバの設定については、mail serve mode を参照してください。

○ mail send from
＜説　　明＞　送信元メールアドレスを設定します。
＜書　　式＞　mail send from WORD
＜　No　＞　no mail send from
＜備　　考＞
・WORD には、送信元メールアドレス（例：centurysys@xxx.isp.ne.jp）を指定します。
・mail send from コマンドで送信元メールアドレスを指定しない場合は、mail from コマンド(global mode)で指定した送信元メールアドレスを使用します。

○ mail send to
＜説　　明＞　送信先メールアドレスを設定します。
＜書　　式＞　mail send to WORD
＜　No　＞　no mail send to
＜備　　考＞
・WORD には、送信先メールアドレス（例：user@centurysys.co.jp）を指定します。
・mail send to コマンドで送信先メールアドレスを指定しない場合は、mail to コマンド(global mode)で指定した送信先メールアドレスを使用します。

○ mail send subject
＜説　　明＞　メールの件名を設定します。指定しない場合は、既定のフォーマットを使用します。
＜書　　式＞　mail send subject LINE
＜　No　＞　no mail send subject
＜備　　考＞
・LINE を指定しない場合は、既定のフォーマットを使用します。以下に例を示します。
ppp0 の接続時： ppp0 was connected
ppp0 の切断時： ppp0 was disconnected

○ no mail send
＜説　　明＞　上記の設定を一括削除することができます。
＜書　　式＞　no mail send

interface ppp mode

◆ ip p2p-detection

＜説　　明＞　P2P検出機能を有効にします（IPv4のみ対応）。
＜書　　式＞　ip p2p-detection (any|winny|share|bittorrent) {log|deny}
＜　no　＞　no ip p2p-detection
　　no ip p2p-detection (winny|share|bittorrent)
＜備　　考＞
・インターネットに接続しているインタフェース上でのみ有効にすることを推奨します。
・詳細については、「付録K：P2P検出機能」を参照してください。

◆ pppoe service-name

＜説　　明＞
・ISP名やサービスの品質・分類を表す場合に使用するservice-name tagを指定することが出来ます。
＜書　　式＞　pppoe service-name
＜　no　＞
・Defaultでは、未設定です。未設定の場合、任意のサービスを受け入れることが出来ます。
・設定する場合は、必ずサービスプロバイダーより指定されたservice-nameを設定します。service-nameが不一致の場合、PPPoE接続に失敗します。

◆ (ip|ipv6) tcp strip-options

＜説　　明＞
・TCPパケット内のオプションをstipする機能です。
・Fast-forwardingが有効な場合、SACK/timestamp/MD5については、stripされない場合があります。
＜書　　式＞　(ip|ipv6) tcp strip-options
　　(all|md5|mss|sack|sack-permitted|timestamp|wscale)
＜初　期　値＞　no (ip|ipv6) tcp strip-options
＜　No　＞　no (ip|ipv6) tcp strip-options
＜備　　考＞　Strip可能なオプションと監視するパケットの種類は、次のとおりです。

TCPオプション	該当TCPパケット
MSS	SYN/SYN-ACK
Window Scale Option	SYN/SYN-ACK
SACK Permitted	SYN/SYN-ACK
SACK	すべてのTCPパケット
Time Stamp Option	すべてのTCPパケット
MD5 signature Option	すべてのTCPパケット

第9章

dns mode

dns mode

◆ 移行 command

dns mode に移行します。

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#dns
vxr-x86(dns-config)#
```

◆ service

＜説　　明＞　DNS サービスを有効にします。
＜書　　式＞　service enable

◆ address

＜説　　明＞　DNS サーバの IP アドレスを設定します。
＜書　　式＞　address A.B.C.D
　　address X:X::X:X
＜初 期 値＞　no address
＜備　　考＞　最大 4 つまで設定可能
＜　no　＞　no address (A.B.C.D|X:X::X:X)
＜備　　考＞　no の場合でも、PPP や DHCP で DNS アドレスを取得している場合は、cache/proxy 有効。

◆priority

＜説　　明＞　DNS サーバのプライオリティを設定します。
＜書　　式＞　priority (user|ppp<0-4>|dhcp|dhcpv6) <priority:0-255>
＜初 期 値＞　すべて 20
＜　no　＞　no priority (user|ppp<0-4>|dhcp|dhcpv6)
　　(=no priority (user 20|ppp <0-4> 20|dhcp 20|dhcpv6 20))
＜備　　考＞
・同一 priority の場合の優先度: user > ppp4 > ppp3 > ppp2 > ppp1 > ppp0 > dhcp > dhcpv6
・dhcp6 においては、現在では、dhcp6-pd を使用した DNS server の割り当てをサポートします。
・0 の場合は、当該アドレスを使用しません。

◆ root

＜説　　明＞　root DNS サーバを使用する / しないを設定します。
＜書　　式＞　root enable
＜備　　考＞　設定されている全ての DNS に対して名前解決できなかった場合に、rootDNS に query 転送する
＜　no　＞　no root enable

◆ timeout

＜説　　明＞　DNS のタイムアウト値を設定します。
＜書　　式＞　timeout <seconds:5-30>
＜初 期 値＞　timeout 30
＜　no　＞　no timeout (=timeout 30)

dns mode

◆ limitation enable
＜説　　明＞　DNS サーバ限定機能を有効にします。
＜書　　式＞　limitation enable
＜　no　＞　no limitation enable
＜備　　考＞　enable にした場合、指定 DNS サーバ以外への再帰問い合わせをしません。

◆ zone address
＜説　　明＞　設定された domain の問合せに対して、指定した DNS server への問合せを行います。
＜書　　式＞　zone <1-5> address A.B.C.D
＜　no　＞　no zone <1-5> address (A.B.C.D|)
＜備　　考＞　zone address は、最大 2 つまで設定可能です。
address,domain が各 1 つ以上のときに設定が有効になります。
zone 設定が変更された場合は、exit 時に DNS キャッシュをクリアします。

◆ zone domain
＜説　　明＞　設定された domain の問合せに対して、指定した DNS server への問合せを行います。
＜書　　式＞　zone <1-5> domain WORD
＜　no　＞　no zone <1-5> domain (WORD|)
＜備　　考＞　zone domain は、最大 3 つまで設定可能です。
address,domain が各 1 つ以上のときに設定が有効になります。
先頭の . は設定可能ですが、それ以降は fqdn 形式で設定します。
ホスト名は設定できません。また、最大文字数は 125 文字です。

◆ zone limitation
＜説　　明＞　指定した特定の domain 向けの DNS server に対する問合せで名前解決できない場合、
それ以上は問合せません。
＜書　　式＞　zone <1-5> limitation enable
＜初 期 値＞　zone <1-5> limitation enable
＜　no　＞　no zone <1-5> limitation enable

◆ domain-search
＜説　　明＞　有効にすると、取得したドメインサーチリストに従って、DNS サーバを使用します。
＜書　　式＞　domain-search enable
＜　no　＞　no domain-search enable
＜備　　考＞
・有効の場合、Domain search list で受信した domain を含むアドレスを解決する際、取得した DNS サーバに対して名前解決を試行します。
・無効の場合、Domain search list で受信した domain を含むアドレスを解決する際、priority の優先順位に従って名前解決を試行します。

dns mode

◆ min-ttl
<説　　明>
・Minimum TTLより小さいTTLを持つレコードを受信した場合、Minimum TTLを使用します。
<書　　式>　min-ttl <120-2147483647>
<　No　>　no min-ttl
<初 期 値>　min-ttl 120(sec)

◆ max-ttl
<説　　明>
・Maximum TTLより大きいTTLを持つレコードを受信した場合、Maximum TTLを使用します。
<書　　式>　max-ttl <120-2147483647>
<　No　>　no max-ttl
<初 期 値>　min-ttl 604800(sec)

◆ host-ttl
<説　　明>　ip hostで応答するアドレスのTTLを設定します。
<書　　式>　host-ttl <120-2147483647>
<　No　>　no host-ttl
<初 期 値>　host-ttl 86400

◆ host-ttl
<説　　明>　ip hostで応答するアドレスのTTLを設定します。
<書　　式>　host-ttl <120-2147483647>
<　No　>　no host-ttl
<初 期 値>　host-ttl 86400

◆ edns-query
<説　　明>　EDNS0機能を有効にします。
<書　　式>　edns-query enable　　（有効）
<　No　>　no edns-query enable　（無効）
<初 期 値>　no edns-query enable
<備　　考>
・DNSでは、最大512バイトまでのUDPパケットを送信することが出来ます。しかしながら、このサイズは、IPv4アドレスでの使用を前提としているため、IPv6アドレス使用時は、512バイトを超えることが考えられます。
・EDNS0を有効にすると、DNSサーバへの要求時に、クライアント側で受信可能なUDPパケットの最大データサイズを通知することによって、512バイトを超えるDNSパケットを扱うことが可能になります。

第 10 章

l2tp mode

l2tp mode

■ L2TP（L2TPv2）機能概要

・LAC として、OCN IPv6 サービスに接続する場合や、LNS として call を受けた場合に、PPP フレームを L2TP によってトンネリングし、リモートの IP/IPv6 ネットワークに接続します。
・LAC として動作する場合、ISP 側で用意された LNS へ L2TP トンネル / セッションを確立後、PPP の確立を行います。LNS として動作する場合、LCCE から SCCRQ を受け取ると、L2TP トンネル / セッションを確立後、PPP の確立を行います。LNS モードの場合、本装置から接続を行うことはありません。
・本装置の L2TP（L2TPv2）は、RFC2661 に準拠しています。

◆ 移行 commannd

l2tp mode に移行します。

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#l2tp <0-1>
vxr-x86(config-l2tp)#
```

■ L2TP mode

・L2TP tunnel(peer)設定毎に LAC/LNS のいずれかのモードを指定することが出来ます。Default では LAC として動作します。ただし、対向のアドレスとして any を設定した場合は、強制的に LNS モードとして動作します。

◆ tunnel mode

＜説　　明＞　L2TP トンネルモードの設定を行います。
＜書　　式＞　tunnel mode (lns|lac)
＜初 期 値＞　tunnel mode lac
＜備　　考＞
・ppp account（global mode）設定状態で、LAC モードを指定すると、ppp account が有効になります。
・ppp account 設定状態で LNS モードに変更すると、ppp account が無効になります(ppp は切断されます)。
・virtual-template 設定状態で lac モードに変更すると、virtual-template が無効になります(該当する ppp clone が切断されます)。
・virtual-template 設定状態で lns モードに変更すると、virtual-template が有効になります。

■コントロールメッセージの再送回数とタイムアウト

・コントロールメッセージの再送回数は、5 回（default）です。再送が発生すると、再送毎に再送間隔が 2 倍に増えます。初回のメッセージタイムアウトは 1 秒です。また、最大再送間隔は 8 秒です。
・したがって、コントロールメッセージを送信してから、タイムアウト（down）と判断するまでの時間は、31 秒（＝1＋2＋4＋8＋8＋8）です。なお、再送回数は、1～1000 回の間で変更することができます。

◆ tunnel retransmit

＜説　　明＞
・コントロールメッセージを送信してから、タイムアウトまでのリトライ回数を設定します。
＜書　　式＞　tunnel retransmit retries <max:1-1000>
＜初 期 値＞　tunnel retransmit retries 5
＜　no　＞　no tunnel retransmit retries (=tunnel retransmit retries 5)

l2tp mode

■ L2TP Keepalive (Hello)

・L2TP トンネルの接続性をチェックするために、定期的に keepalive を送信します。送信間隔は 60 秒（default）で、0 ～ 1000 秒の範囲で変更することが出来ます。0 を設定した場合は、hello を送信しません。

・Hello の送信タイマーがタイムアウトする前に、LNS からコントロールメッセージ / データメッセージを受信した場合、本装置内部の hello 送信タイマーを再スケジュールします。したがって、LNS から L2TP パケットを受信している間は、本装置から hello を送信しません。

◆ tunnel hello

＜説　　明＞　Helloインターバルを設定します。
＜書　　式＞　tunnel hello <sec:0-1000>
＜初 期 値＞　tunnel hello 60
＜　no　＞　no tunnel hello
＜備　　考＞　no tunnel hello（=tunnel hello 0）の場合、hello パケットを送出しません。

■ L2TP port number

・一部の他社製ブロードバンドルータの配下に本装置を設置した場合、L2TP トンネルを確立する際に、source port UDP/1701 を使用すると、L2TP/PPP セッションが確立できません。その対策として、L2TP で使用する source port 番号を変更することが出来ます。

・L2TP では、source port として UDP/4001（default）を使用し、destination port として UDP/1701（default）を使用します。source port/destination port 共に、UDP/1024 ～ 65535 の範囲で変更することが出来ます。

・L2TPv3 を UDP 上で使用する場合、L2TPv3 と L2TPv2（本機能)に、それぞれ異なる port 番号を設定してください。

◆ udp source-port

＜説　　明＞　L2TP で使用する UDP の source port 番号を指定します。
＜書　　式＞　l2tp udp source-port <src_port:1024-65535>
＜初 期 値＞　l2tp udp source-port 40001
＜備　　考＞　本機能は、global mode で設定します。

◆ udp port

＜説　　明＞　L2TP で使用する UDP の destination port 番号を指定します。
＜書　　式＞　tunnel udp port <dst_port:1024-65535>
＜　no　＞　no tunnel udp port
＜初 期 値＞　tunnel udp port 1701

l2tp mode

■接続先の指定

・接続先アドレスとして、LAC の場合は IPv4/FQDN を、LNS の場合は any を指定することが出来ます。
・any 指定時は、対向のアドレスを他の機能（本バージョンでは IPsec）から取得し、そのアドレスが L2TP に登録されることで、当該アドレスからの L2TP 接続が可能となります。この場合、L2TP トンネル / セッションの down が発生すると、IPsec に対してトンネルダウンの指示を行います。
・LAC モードで対向アドレスとして FQDN を指定した場合、SCCRQ を送信する毎に、DNS サーバに対して IPv4 アドレスの名前解決を行います。したがって、FQDN を指定した場合、接続中または接続の途中で IPv4 アドレスが変更になっても、L2TP トンネル / セッションの接続先は、すぐには変更されません。再接続時に、新しい IPv4 アドレスに対して接続を試みます。
・IPv6 over PPP を L2TP にてトンネリングすることは可能ですが、転送用プロトコルとして IPv6 を使用することはできません。

◆ tunnel

＜説　　明＞　接続先のアドレスを設定します。

○ address (A.B.C.D|FQDN)

＜書　　式＞　tunnel address (A.B.C.D | FQDN)

○ address any ipsec

＜書　　式＞　tunnel address any ipsec

＜備　　考＞

・any 指定時、bind するプロトコル(ipsec)を指定することが出来ます。IPsec の確立した client からの接続のみを許可します。
・接続タイムアウト
・tunnel address any ipsec を指定した場合、IPsec からのアドレス登録後、300 秒以内に L2TP セッションが確立しなければ、当該アドレスを無効とし、IPsec に対して IPsec tunnel の削除要請を行います。ただし、タイムアウトした場合でも、トンネルが active（再送中）であれば、IPsec tunnel の削除要請は行いません。トンネルが down した際に、IPsec tunnel の削除要請を行います。
・本機能により、IPsec は確立したものの、L2TP のパケットを受信しない場合等に、IPsec SA だけが残ってしまうような状態を防ぐことが出来ます。

l2tp mode

■ LNSとしての動作

□ PPPインタフェースの割り当て

・L2TP LNSとして動作し、クライアントからのL2TPトンネル/セッションの確立を行うことが出来ます。この際に割り当てるPPPインタフェースは、virtual-templateです。特定のPPPインタフェースを固定的に割り当てる動作はサポートしていません。
・Virtual-templateを使用すると、PPPインタフェースのクローンを作成します。このときのPPPインタフェース番号（100～256）は、L2TPサービスが自動的に割り当てます。

◆ tunnel virtual-template
<説　　明>　使用するvirtual-templateを指定します。
<書　　式>　tunnel virtual-template <0-0>
<　no　>　no tunnel virtual-template

□ IPv4アドレスの割り当て

・PPPの確立時に、クライアントからのIPCP addressのrequestに対して、IPv4アドレスを割り当てます。
・L2TPに割り当てられたIP address poolの中から、IPv4アドレスを自動的に割り当てます。access-server profile modeで、ユーザ毎に固定IPの割り当て設定を行っている場合は、当該IPアドレスを割り当てます。
・IPアドレスの自動割り当てを行う際、IP poolのアドレス範囲の中に、PPPユーザ毎に固定的に割り当てるIPアドレスが含まれている場合や、exclude addressが設定されている場合は、該当するIPアドレスを除いて割り当てます。

◆ ip local pool WORD address
<説　　明>　IPアドレスプールを設定します。
<書　　式>　ip local pool WORD address A.B.C.D (|A.B.C.D)
<　no　>　no ip local pool WORD
<備　　考>　本設定は、global modeで行います。

◆ ip local pool WORD exclude-address
<説　　明>　IPアドレスプールの対象外となるIPアドレス（またはIPアドレス範囲）を設定します。
<書　　式>　ip local pool WORD exclude-address A.B.C.D (|A.B.C.D)
<　no　>
・exclude-addressの全削除　no ip local pool WORD exclude-address
・指定対象のみ削除　no ip local pool WORD exclude-address A.B.C.D (|A.B.C.D)
<備　　考>　本設定は、global modeで行います。

◆ peer ip pool
<説　　明>　使用するIP アドレスプールを指定します。
<書　　式>　peer ip pool WORD
<　No　>　no peer ip pool WORD
<備　　考>　本設定は、interface virtual-template modeで行います。

l2tp mode

◆ tunnel hidden
＜説　　明＞　AVP Hidingを有効にします。
＜書　　式＞　tunnel hidden
＜初 期 値＞　no tunnel hidden
＜　no　＞　no tunnel hidden

◆ tunnel password
＜説　　明＞　パスワードを設定します。
＜書　　式＞　tunnel password (|hidden) PASSWORD
＜　no　＞　no tunnel password
＜備　考＞　パスワードは、1-95文字以内で設定してください。
　　使用可能な文字は、英数字および!$#=*+-_.:;(){}[]^~@`<>です。

◆ tunnel ppp
＜説　　明＞　PPPをL2TPでトンネリングします。
＜書　　式＞　tunnel ppp <ppp:0-4>
＜　no　＞　no tunnel ppp
＜備　　考＞　l2tpの再接続、再接続間隔は、pppの設定を使用します。
　　pppとvirtual-templateの設定は排他(どちらかのみ設定可)です。

◆ tunnel authentication callin
＜説　　明＞　tunnel認証の設定を行います。
＜書　　式＞　tunnel authentication callin
＜　no　＞　no tunnel authentication (|callin)

第 11 章

l2tpv3-tunnel mode

第 11 章 l2tpv3-tunnel mode

l2tpv3 tunnel parameters

◆ 移行 commannd
l2tpv3-tunnel mode に移行します。
```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#l2tpv3 tunnel <0-4095>
vxr-x86(config-l2tpv3-tunnel)#
```

◆ description
＜説　　明＞　L2TPv3 トンネルの説明を記述します。
＜書　　式＞　description DESCRIPTION
＜　no　＞　no description

◆ tunnel address
＜説　　明＞　リモード LCCE のトンネルアドレスを設定します。
＜書　　式＞　tunnel address A.B.C.D
　　tunnel address X:X::X:X
　　tunnel address FQDN
　　tunnel address any
　　tunnel address (ip|ipv6) (FQDN|any)
＜備　　考 ＞
・IPv6 アドレスを指定すると、コントロールパケットおよびセッションパケットの転送用プロトコルとして IPv6 を使用します（L2TPv3 over IPv6）。L2TPv3 over IPv6 は、fast-forwarding の対象外です。
・トンネルの接続先として、FQDN を指定することが出来ます。ただし、DNS による名前解決や timeout 待ちで、接続に時間がかかる場合があるため、FQDN の使用には注意が必要です。
・FQDN 指定時は、名前解決を行うプロトコル family（IPv4 または IPv6、あるいは両方のアドレス）を指定することが出来ます。指定のない場合は、IPv6 の名前解決を試行し、失敗した場合に、IPv4 の名前解決を行います。両方の名前解決を行うと時間がかかる場合があるため、そのような場合にはプロトコル family を指定します。
・any 指定時もプロトコル family を指定することが出来ます。any の場合、本装置と対向装置のプロトコル family が一致している場合のみ、接続することが出来ます。

◆ no tunnel address
＜説　　明＞　リモード LCCE のトンネルアドレスを削除します。
＜書　　式＞　no tunnel address

◆ tunnel hostname
＜説　　明＞　リモート LCCE のホスト名を設定します。
＜書　　式＞　tunnel hostname HOSTNAME

◆ tunnel router-id
＜説　　明＞　リモート LCCE のルータ ID を設定します。
＜書　　式＞　tunnel router-id A.B.C.D

l2tpv3 tunnel parameters

◆ tunnel password
<説　　明>　認証や AVP Hiding で使用するパスワードを設定します。
<書　　式>　tunnel password PASSWORD
　　tunnel password hidden PASSWORD
<初 期 値>　no tunnel password
<　no　>　no tunnel password
<備　考 >　パスワードは、1-95 文字以内で設定してください。
　　使用可能な文字は、英数字および!$#=*+-_.:;(){}[]^~@`<> です。

◆ tunnel hidden
<説　　明>　AVP Hiding を設定します。
<書　　式>　tunnel hidden
<　no　>　no tunnel hidden

◆ tunnel protocol
<説　　明>　送信プロトコルを選択します。
<書　　式>　tunnel protocol (ip|udp)
<初 期 値>　tunnel protocol ip
<　no　>　no tunnel protocol (=tunnel protocol ip)

◆ tunnel local hostname
<説　　明>　ローカル LCCE のホスト名を設定します。
<書　　式>　tunnel local hostname HOSTNAME
<初 期 値>　no tunnel local hostname
< To Unset >　no tunnel local hostname

◆ tunnel local router-id
<説　　明>　ローカル LCCE のルータ ID を設定します。
<書　　式>　tunnel local router-id A.B.C.D
<初 期 値>　no tunnel local router-id
<　no　>　no tunnel local router-id

◆ tunnel digest
<説　　明>　メッセージダイジェストを有効にします。
<書　　式>　tunnel digest (md5|sha1)
<初 期 値>　no tunnel digest
<　no　>　no tunnel digest

◆ tunnel hello
<説　　明>　Hello パケットの送信間隔を設定します。
<書　　式>　tunnel hello <0-1000>
<初 期 値>　tunnel hello 60
<　no　>　no tunnel hello （無効）

l2tpv3 tunnel parameters

◆ tunnel vendor
＜説　　明＞　リモート LCCE のベンダー ID を設定します。
＜書　　式＞　tunnel vendor (ietf|century|cisco)
＜初 期 値＞　tunnel vendor ietf
＜　no　＞　no tunnel vendor　　: Set defaults

◆ netevent
＜説　　明＞　イベント検出時にトンネルを切断します。
＜書　　式＞　netevent <trackid:1-255> disconnect
＜初 期 値＞　no netevent
＜備　　考＞　PPP interface の監視のみ対応
＜　no　＞　no netevent

第 12 章

l2tpv3-xconnect mode

l2tpv3 xconnect parameters

◆ 移行 command
vxr-x86#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
vxr-x86(config)#**l2tpv3 xconnect <xid:1-4294967295>**
vxr-x86(config-l2tpv3-xconnect)#

◆ description
<説　　明>　L2TPv3 Xconnect の説明を記述します。
<書　　式>　description DESCRIPTION
<　no　>　no description

■ tunnel
○ tunnel <0-4095>
<説　　明>　Xconnect で使用する L2TPv3 の Tunnel ID を指定します。
<書　　式>　tunnel <tunnel_id:0-4095>

○ tunnel tos
<説　　明>　Xconnect に ToS 値を設定します。
<書　　式>　tunnel tos (<0-252>|inherit)
<初 期 値>　tunnel tos 0
<　no　>　no tunnel tos

◆ xconnect INTERFACE
<説　　明>　Xconnectインタフェースを設定します。
<書　　式>　xconnect ethernet <0-max> (|vid <1-4094>)
　　xconnect bridge <0-4095>
　　xconnect tap <0-127>

◆ xconnect end-id
<説　　明>　リモート LCCE の end id を設定します。
<書　　式>　xconnect end-id <1-4294967295>

◆ vlan-id
<説　　明>　VLAN tag を使用する場合に設定します。
<書　　式>　vlan-id <1-4094>
<　no　>　no vlan-id

◆ retry-interval
<説　　明>　トンネル/セッションが切断したときに自動再接続を開始するまでの間隔を設定します。
<書　　式>　retry-interval <seconds:0-1000>
<初 期 値>　retry-interval 0
<　no　>　no retry-interval (=retry-interval 0)

l2tpv3 xconnect parameters

◆ loop-detect enable
<説　　明>　Loop Detection機能を有効にします。
<書　　式>　loop-detect enable
<初 期 値>　no loop-detect enable
<　no　>　no loop-detect enable

◆ send-known-unicast enable
<説　　明>　Known Unicast送信機能を有効にします。
<書　　式>　send-known-unicast enable
<初 期 値>　no send-known-unicast enable
<　no　>　no send-known-unicast enable

◆ send-circuit-down enable
<説　　明>　Circuit Statusがdownの時に、対向LCCEに対して、Non-Unicast Frameを送信します。
<書　　式>　send-circuit-down enable
<初 期 値>　no send-circuit-down enable
<　no　>　no send-circuit-down enable

◆ split-horizon enable
<説　　明>　Split Horizon機能を有効にします。
<書　　式>　split-horizon enable
<初 期 値>　no split-horizon enable
<　no　>　no split-horizon enable

◆ mac-learning unique enable
<説　　明>　L2TPv3 MACアドレス学習unique機能を有効にします。
<書　　式>　mac-learning unique enable
<初 期 値>　no mac-learning unique enable
<　no　>　no mac-learning unique enable
<備　　考>
・本機能を有効にするには、global modeで、次の設定が必要になります。
vxr-x86(config)#l2tpv3 mac-learning unique
・ネットワーク構成によっては、ある一つのXconnectのLocal Table、FDBに同じMACアドレスが登録されることがあります。本機能を有効にすると、新しく学習したMACアドレスが、Local Table、FDBのどちらか一方に登録されるため、上記のような状態を回避することが出来ます。
・ある一つのXconnectで、LoopDetect機能と共存した場合、LoopDetectのFrameDrop処理を優先します。つまり、この場合は、MACアドレス学習unique機能は動作しないことになります。
・本機能(unique)はデフォルトで無効です。

l2tpv3 xconnect parameters

◆ ip tcp adjust-mss

＜説　　明＞

・Path MTU Discovery（PMTUD）機能（End-to-end でフラグメントが発生しない最大の MTU を発見すること）によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器（ルータ等）が ICMP fragment needed をフィルタリングしている場合（ブラックホールルータが存在する場合）や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、End-to-end での通信に支障をきたすことになります。このような場合、TCP では　SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

＜書　　式＞　ip tcp adjust-mss (auto|<500-1460:bytes>)

＜初 期 値＞　no ip tcp adjust-mss

＜　No　＞　no ip tcp adjust-mss

＜備　　考＞

・IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。

・本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ユーザが設定する場合は、MSS 値を指定します。元の MSS 値に関係なく指定した値に強制的に変更します。

・UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。

・「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

◆ l2tpv3 access-group

＜説　　明＞　L2TPv3 セッションの送信 / 受信に対して、l2tpv3 access-list を適用します。

＜書　　式＞　l2tpv3 access-group (in|out) WORD

＜　no　＞　no l2tpv3 access-group (in|out)

＜備　　考＞

・WORD：　root の ACL 名を指定します。
　（root の ACL 名は、global mode の l2tpv3 access-list WORD root コマンドにて設定）

・in:　受信方向のセッションに対して、フィルタを適用します。

・out:　送信方向のセッションに対して、フィルタを適用します。

第 13 章

l2tpv3-group mode

l2tpv3-group mode

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#l2tpv3 group <gid:1-4095>
vxr-x86(config-l2tpv3-group)#
```

◆ xconnect

＜説　　明＞　使用する Xconnect を指定します。

＜書　　式＞

```
xconnect <primary-xid:1-4294967295> (|<secondary-xid:1-4294967295>) (|hotswap)
```

＜備　　考＞

・hotswap を指定すると、L2TPv3 primary/secondary xconnect hotswap 機能を有効にします。

-hotswap 設定は、config に保存されません。

- 従来、グループ機能を使用している構成において、primary xconnect と secondary xconnect の設定を変更すると、一度、L2TPv3 セッションがダウンします。
本機能は、L2TPv3 セッションをダウンさせずに、primary xconnect と secondary xconnect を切り替える機能です。

-group mode を exit した際、xconnect 以外の設定があった場合は、config の設定変更が発生したと判断して、従来通り L2TPv3 セッションがダウンします。

- なお、本機能の連続での実行を回避するため、l2tpv3 group mode を exit した際は、数秒間コマンドを受け付けない仕様になっています。

```
vxr-x86(config-l2tpv3-group)#xconnect 1 2 hotswap
vxr-x86(config-l2tpv3-group)#exit
 Change primary/secondary xconnect...Please wait.
vxr-x86(config)#
```

◆ preempt enalbe

＜説　　明＞　Group の preempt モードの有効 / 無効を設定します。

＜書　　式＞　preempt enable

＜　no　＞　no preempt enable

◆enforce-secondary-down enable

＜説　　明＞　本機能を有効にすると、Secondary セッションを強制切断します。

＜書　　式＞　enforce-secondary-down enable

＜初 期 値＞　no enforce-secondary-down enable

＜　no　＞　no enforce-secondary-down enable

◆active-hold enable

＜説　　明＞　Group の Active Hold 機能の有効 / 無効を設定します。

＜書　　式＞　active-hold enable

＜初 期 値＞　no active-hold enable

＜　no　＞　no active-hold enable

l2tpv3-group mode

◆mac-advertise enable

＜説　　明＞

・L2TPv3 MAC Advertise Frame送信機能の有効 / 無効を設定します。

- グループ機能を使用している構成で、センター側の配下にあるスイッチのMACテーブルを更新するために、ローカルテーブルに登録されているMACアドレス情報を元に疑似フレームを送信することによって、センターにある端末を発信源とする通信が可能となります。
- この機能はデフォルトで無効です。
- 本機能を使用する場合は、L2TPv3 MAC Address学習Always機能を有効（l2tpv3 mac-learning always）に設定してください。

※本機能を使用する場合は、対向装置も同機能が実装されているファームウェア（v5.15.1以降）を使用することを推奨します。

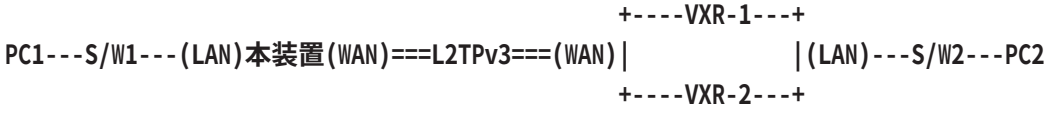
＜書　　式＞　mac-advertise enable

＜初 期 値＞　no mac-advertise enable

＜　no　＞　no mac-advertise enable

＜備　　考＞

・図のような冗長化構成において、拠点側（本装置）でL2TPv3セッションの切替が発生した場合、センター側VXRの配下にあるスイッチ（S/W2）のFDBが更新されるまで、センターにある端末を発信源とする通信を行うことは出来ません。本機能を有効にすることで、このような状況でも、できるだけ早く通信を回復させることが可能になります。



・拠点側にてL2TPv3セッションの切り替えおよび切り戻り等を検知した際、ローカルテーブルで学習したMACアドレス情報を、アクティブセッションを通してセンター側に送信します。1つのMACアドレスにつき1つのL2TPv3 MAC Advertise Frameを作成し、アクティブセッションに送信します。

○ L2TPv3 MAC Advertise Frame送信

①本機能無効（no mac-advertise enable）時は、L2TPv3 MAC Advertise Frameを送信しません。

②本機能有効（mac-advertise enable）時は、次の場合にL2TPv3 MAC Advertise Frameを送信します。

- アクティブセッションの切り替えおよび切り戻りを検知した時
- アクティブセッションが作成されたとき

※ただし、Circuit Down時の送信設定の有効（send-circuit-down enable）/ 無効（no send-circuit-down enable）に関わらず、対向LCCEのCircuit statusがDOWNの場合は、対向LCCEでDropされてしまう為、MAC Advertise Frameを送信しません。対向LCCEからSLI Message(Circuit up)を受信した際は、その時点でアクティブセッションとして選択されているセッションに対して一度もMAC Advertise Frameを送信していない場合に限り、MAC Advertise Frameを送信します。

○ L2TPv3 MAC Advertise Frame受信

①Xconnectで受信時、本機能の有効 / 無効に関わらず、常にDropします。

②L2TPセッションで受信時、本機能の無効 / 有効に関わらず、常に以下の判定を行います。

- データ部にあるXconnectインタフェースのHWアドレスと対向装置のHWアドレスを比較します。

(a)一致した場合は、他拠点にはフレームを転送せず、Xconnectのみにフレームを転送します。

(b)一致しなかった場合は、Dropします。

第 14 章

rip mode

rip mode

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#router rip
vxr-x86(config-router)#
```

◆ network

```
<説　　明>  RIPを有効にするネットワークおよびインタフェースを設定します。
<書　　式>  network A.B.C.D/M      :  IP prefix <network>/<length>, e.g., 35.0.0.0/8
            network ethernet <0-2> (|vid <1-4094>)
            network ppp <0-4>
            network tunnel <0-255>
<    no    >  no network A.B.C.D/M   :  IP prefix <network>/<length>, e.g., 35.0.0.0/8
            no network ethernet <0-2> (|vid <1-4094>)
            no network ppp <0-4>
            no network tunnel <0-255>
```

◆ redistribute

```
<説　　明>  経路の再配信を有効にします。
<書　　式>  redistribute (static|connected|ospf|bgp)
                                        (|metric <metric:0-16>|route-map ACL-NAME)
<    no    >  no redistribute (static|connected|ospf|bgp)
                                        (|metric <metric:0-16>|route-map ACL-NAME)
```

◆ distribute-list

```
<説　　明>  route-map を適用します。
<書　　式>  distribute-list ACL-NAME (in|out) (ethernet <0-4>|ppp <0-4>|tunnel <0-255>)
<    no    >  no distribute-list ACL-NAME distribute-list ACL-NAME (in|out)
            (ethernet <0-4>|ppp <0-4>|tunnel <0-255>)
```

◆ distance

```
<説　　明>  RIP と OSPF を併用していて全く同じ経路を学習した場合に、
            この値の小さい方を経路として採用します。
<書　　式>  distance <1-255>
<    no    >  no distance
```

rip mode

◆ timers basic
＜説　　明＞　RIP タイマーを設定します。
＜書　　式＞　timers basic <update:5-2147483647> <timeout:5-2147483647>
　　<garbage:5-2147483647>
＜初 期 値＞　update: 30sec, timeout: 180sec, garbage: 120sec
＜　no　＞　no timers basic (=timers basic 30 180 120)(= set defaults)

◆ passive-interface
＜説　　明＞　ルーティングアップデートの送信をストップします（受信はします）。
＜書　　式＞　passive-interface ethernet <0-2> (|vid <1-4094>)
　　passive-interface ppp <0-4>
　　passive-interface tunnel <0-255>

＜　no　＞　no passive-interface ethernet <0-2> (|vid <1-4094>)
　　no passive-interface ppp <0-4>
　　no passive-interface tunnel <0-255>

◆ default-information originate
＜説　　明＞　デフォルトルート情報の配信を有効にします。
＜書　　式＞　default-information originate
＜　no　＞　no default-information originate

◆ version
＜説　　明＞　RIP バージョンを設定します。
＜書　　式＞　version <1-2>
＜初 期 値＞　version 2
＜　no　＞　no version (|<1-2>)

第 15 章

ospf mode

ospf mode

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#router ospf
vxr-x86(config-router)#
```

◆ network

```
<説　　明>　OSPF のエリア ID を設定します。
<書　　式>　network A.B.C.D/M area <0-4294967295>   : OSPF area ID as a decimal value
            network A.B.C.D/M area A.B.C.D          : OSPF area ID in IP address format
<　no　 >　no network A.B.C.D/M area <0-4294967295>
            no network A.B.C.D/M area A.B.C.D
```

◆ area default-cost

```
<説　　明>　スタブエリアに対してデフォルトルート情報を送信する際のコスト値を設定します。
<書　　式>　area (<0-4294967295>|A.B.C.D) default-cost <0-16777215>
<　no　 >　no area (<0-4294967295>|A.B.C.D) default-cost
```

◆ area authentication

```
<説　　明>　認証を有効にします。
<書　　式>　area (<0-4294967295>|A.B.C.D) authentication (|message-digest)
<　no　 >　no area (<0-4294967295>|A.B.C.D) authentication
```

◆ area range

```
<説　　明>　経路情報を集約して送信する場合に設定します。
<書　　式>　area (A.B.C.D|<0-4294967295>) range A.B.C.D/M
<　no　 >　no area (A.B.C.D|<0-4294967295>) range A.B.C.D/M
```

◆ area stub

```
<説　　明>　スタブ設定を有効にします。
<書　　式>　area (A.B.C.D|<0-4294967295>) stub
            area (A.B.C.D|<0-4294967295>) stub no-summary
<　no　 >　no area (A.B.C.D|<0-4294967295>) stub
            no area (A.B.C.D|<0-4294967295>) stub no-summary
```

ospf mode

◆ area virtual-link
＜説　　明＞　バーチャルリンクを設定します。
＜書　　式＞　area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
　　area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
　　{authentication (message-digest|null)
　　| authentication-key LINE
　　| dead-interval <1-65535>
　　| hello-interval <1-65535>
　　| message-digest-key <1-255> md5 LINE
　　| retransmit-interval <1-65535>
　　| transmit-delay <1-65535>}
＜　no　＞　no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
　　no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
　　{authentication (message-digest|null)
　　| authentication-key LINE
　　| dead-interval <1-65535>
　　| hello-interval <1-65535>
　　| message-digest-key <1-255> md5 LINE
　　| retransmit-interval <1-65535>
　　| transmit-delay <1-65535>}

◆ redistribute
＜説　　明＞　経路の再配信を設定します。
＜書　　式＞
　redistribute (connected|static|rip|bgp) (|metric<0-16777214>) [|metric-type (1|2)]
　　(|route-map ACL-NAME) (|tag <0-
4294967295>)
＜　no　＞
　redistribute (connected|static|rip|bgp) (|metric<0-16777214>) [|metric-type (1|2)]
　　(|route-map ACL-NAME) (|tag <0-
4294967295>)

◆ distribute-list
＜説　　明＞　route-map を適用します。
＜書　　式＞　distribute-list ACL-NAME (in|out) (ethernet <0-4>|ppp <0-4>|tunnel <0-255>)
＜　no　＞　no distribute-list ACL-NAME distribute-list ACL-NAME (in|out)
　　(ethernet <0-4>|ppp <0-4>|tunnel <0-255>)

◆ distance
＜説　　明＞　OSPF と他のダイナミックルーティング併用時に、同じサブネットを学習した場合、
　　この値の小さい方のダイナミックルートを経路として採用します。
＜書　　式＞　distance <1-255>
　　distance ospf (intra-area <1-255>|inter-area <1-255>|external <1-255>)
＜　no　＞　no distance <1-255>
　　no distance ospf

ospf mode

◆ tiemrs spf
<説　　明>　OSPF SPF timers を設定します。
<書　　式>　timers spf <delay:0-4294967295> <hold_time:0-4294967295>
　　<delay:0-4294967295> : Delay between receiving a change to SPF calculation
　　<hold_time:0-4294967295> : Hold time between consecutive SPF calculations
<　no　>　no timers spf　　: Set defaults

◆ passive-interface
<説　　明>　ルーティングアップデートの送信をストップします（受信はします）。
<書　　式>　passive-interface ethernet <0-2> (|vid <1-4094>)
　　passive-interface ppp <0-4>
　　passive-interface tunnel <0-255>
<　no　>　no passive-interface ethernet <0-2> (|vid <1-4094>)
　　no passive-interface ppp <0-4>
　　no passive-interface tunnel <0-255>

◆ default-information
<説　　明>　デフォルトルートを OSPF で配信します。
<書　　式>
　default-information originate
　　(|metric <0-16777214>) [|metric-type (1|2)] (|always) (|route-map WORD)
<　no　>
　no default-information originate
　　(|metric <0-16777214>) [|metric-type (1|2)] (|always) (|route-map WORD)

◆ auto-cost
<説　　明>　コスト計算時の基準となる帯域値(単位：Mbps)を設定します。
<書　　式>　auto-cost reference-bandwidth <1-4294967>
<　no　>　no auto-cost reference-bandwidth
<備　　考>
・OSPF のコストは、[コスト =100(Mbps) / 帯域幅(Mbps)]によって算出されます。Default の基準帯域幅は、100Mbps です。
・上記の計算式に従うと、100Mbps の回線では「1」、1Gbps の回線でも「1」（小数点以下は切り上げるため、「0.1」ではありません）となり、1Gbps 以上の回線では、正しいコスト計算が出来ません。
・基準帯域幅を変更することによって、ギガビットイーサネットでの回線コストを適切に計算することが出来るようになります。
・インタフェースの帯域幅は、インタフェース毎に bandwidth コマンドで設定します。

◆ router-id
<説　　明>　Router ID を設定します。
<書　　式>　router-id A.B.C.D
<　no　>　no router-id

第 16 章

bgp mode

bgp mode

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#router bgp <1-65535>
vxr-x86(config-router)#
```

◆ network

＜説　　明＞　ネットワークアドレスを設定します。
＜書　　式＞　network A.B.C.D/M (|backdoor)
＜　no　＞　no network A.B.C.D/M (|backdoor)
＜備　　考＞
・特定の BGP 経路を優先経路にしたくない場合、受け取った BGP 経路にローカル BGP の administrative distance 値を設定することで優先順位を下げ、他の経路を優先させることができます。

◆ aggregate-address

＜説　　明＞
・Aggregate 機能を使うと、BGP 経路の集約を行うことが出来る集約経路を構成する経路が、BGP テーブル内に少なくとも一つでも存在する場合に、集約経路を作成し advertise します。
＜書　　式＞　aggregate-address A.B.C.D/M (|summary-only|as-set)
＜　no　＞　no aggregate-address A.B.C.D/M (|summary-only|as-set)
＜備　　考＞
・Aggregate 機能では、集約経路と一緒に集約前の経路も advertise します。集約経路のみ advertise する場合は summary-only 設定を有効にします。
・経路の aggregate 設定を行った場合、AS パス情報が失われます。これによって、同じ AS に新しい経路として受け取られてしまい、ルーティングループを引き起こす可能性があります。As-set 機能を有効にすると、経路集約時に AS セット情報を含む形で広告することが可能になります。なお、この場合の AS セット集合は、順序不同でリストされたものです。

◆ distance

＜説　　明＞　BGP に関する Administrative Distance 値を設定します。
＜書　　式＞　distance bgp <eBPG:1-255> <iBGP:1-255> <local:1-255>
＜　no　＞　no distance bgp
＜備　　考＞　初期値は 20（eBGP)、200（iBPG)、200（local）です。

◆ timers

＜説　　明＞　jitter の範囲を % で指定することができます。
＜書　　式＞　timers bgp jitter <75-100>
＜　no　＞　no timers bgp jitter
＜備　　考＞　Default は、75% です。
本設定で設定した jitter は、keepalive の interval にのみ影響します。keepalive interval については、neighbor の keep alive interval を参照してください。

bgp mode

■ bgp

○ always-compare-med

＜説　　明＞

・通常、異なるASを生成元とする経路については、MED値を比較しませんが、always-compared-med機能を有効にした場合、異なるASを生成元とする経路についてもMED値を比較します。

＜書　　式＞　bgp always-compare-med

＜　no　＞　no bgp always-compare-med

○ bestpath as-path

＜説　　明＞

・通過したAS番号のリストを示す属性がAS-PATH属性です。UPDATE messageがASを通過するたびに、AS-PATHリストの順に追加されます。

・通常、best pathを選択する際、AS-PATHの短いものを優先的に選択します。本機能を設定した場合は、best path選択時に、AS-PATH属性を無視します。

＜書　　式＞　bgp bestpath as-path ignore

＜　no　＞　no bgp bestpath as-path ignore

○ bestpath med

＜説　　明＞　MED値のないprefixに対して、MED最大値の4294967294が割り当てられます。

＜書　　式＞　bgp bestpath med missing-as-worst

＜　no　＞　no bgp bestpath med missing-as-worst

○ local-preference

＜説　　明＞

・ルータ自身に設定される値で、AS内に複数経路を持つような場合、どの経路を優先するかを示す属性がlocal preference属性です。

＜書　　式＞　bgp default local-preference <0-4294967295>

＜　no　＞　no bgp default local-preference

＜備　　考＞　iBGP peer間でのみ交換される値で、値の大きい方が優先されます。
Default値は100です。

○ default-information-check

＜説　　明＞　default route情報を保持している場合にのみ、BGP4にてdefault route情報を広告する機能です。

＜書　　式＞　bgp default-information-check

＜　no　＞　no bgp default-information-check

＜初 期 値＞　no bgp default-information-check

＜備　　考＞　本機能が有効な場合、下記のいずれかの方法によってdefault route情報をBGPへインストールする必要があります。

(1) redistribute設定によりdefault route情報をインストールする。

(2) network設定により0.0.0.0/0をインストールする。

bgp mode

■ bgp （続き）

○ enforce-first-as

＜説　　明＞　UPDATE に含まれる AS シーケンスの中の最初の AS が neighbor の AS でない場合に、notification メッセージを送信して、neighbor とのセッションをクローズします。

＜書　　式＞　bgp enforce-first-as

＜　no　＞　no bgp enforce-first-as

○ network import-check

＜説　　明＞

・BGPでadvertiseされるnetworkは、通常、生成元となるrouterがそのnetworkを知らない場合もadvertiseされます。知らないnetworkをBGPでadvertiseしたくない場合には、import-check機能を有効にすることによって、advertiseされなくなります。

＜書　　式＞　bgp network import-check

＜　no　＞　no bgp network import-check

○ router-id

＜説　　明＞　Router-ID を IP アドレス形式で設定します。

＜書　　式＞　bgp router-id A.B.C.D

＜　no　＞　no bgp router-id

＜備　　考＞

・Router-ID が指定されていない場合、本装置が保持している IPv4 address の中でもっとも大きい IPv4 アドレスを Router-ID として使用します。

○ scan-time

＜説　　明＞　BGP で学習した route の next-hop が到達可能かどうかをスキャンします。

＜書　　式＞　bgp scan-time <0-60>

＜　no　＞　no bgp scan-time

＜備　　考＞　初期値は 5（秒）です。

bgp mode

■ neighbor

○default-originate
＜説　　明＞　デフォルトルートを配信する場合に設定します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) default-originate
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) default-originate

○ distribute-list
＜説　　明＞　peer に送信 / 受信する route update の filtering を行う場合に設定します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) distribute-list ACL-NAME (in|out)
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) distribute-list ACL-NAME (in|out)
＜備　　考＞　Neighbor 毎に IN/OUT それぞれ１つの distribute-list を設定することができます。

○ ebgp-multihop
＜説　　明＞　peer と直接接続されていない場合でも、eBGP Peer を確立することができます。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) ebgp-multihop <1-255>
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) ebgp-multihop <1-255>
＜備　　考＞　到達可能なホップ数を設定します。

○ filter-list
＜説　　明＞　BGP のフィルタを設定します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) filter-list ACL-NAME (in|out)
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) filter-list ACL-NAME (in|out)
＜備　　考＞　global mode で設定した AS-PATH アクセスリストを使用します。

○ next-hop-self
＜説　　明＞　iBGP peerに送信するnexthop情報をpeerのルータとの通信に使用するインタフェースの address に変更します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) next-hop-self
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) next-hop-self

○ remote-as
＜説　　明＞　対向装置の AS 番号を設定します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) remote-as <1-65535>
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) remote-as <1-65535>

○ remove-private-as
＜説　　明＞　Outbound update からプライベート AS を削除します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) remove-private-as
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) remove-private-as

bgp mode

■ neighbor(続き)

○ route-map

＜説　　明＞　Peer に送信 / 受信する route の filtering や属性の操作をすることが出来ます。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) route-map WORD (in|out)
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) route-map WORD (in|out)
＜備　　考＞　neighbor 毎に IN/OUT それぞれ１つの routemap を適用することができます。

○ soft-reconfiguration

＜説　　明＞　Neighbor との BGP session をクリアせずに変更を適用したい場合に使用します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) soft-reconfiguration inbound
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) soft-reconfiguration inbound
＜備　　考＞　BGP の neighbor parameter や routemap の設定を変更した場合、その変更を適用するためには BGP session の clear もしくは、BGP service の再起動が必要となります。

○ keepalive interval & holdtime

＜説　　明＞　keepalive の送信間隔と holdtime を設定します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) timers <keepalive:0-65535><holdtime:0|3-65535>
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) timers
＜初 期 値＞　neighbor (A.B.C.D|X:X::X:X) timers 60 180
＜備　　考＞

- Peer から hold time がタイムアウトする前に、keepalive message か update message を受信しなかった場合、peer との session は close され IDLE 状態へと遷移します。
- Keepalive を 0sec に設定した場合、keepalive message は送信されません。
- Keepalive interval には、jitter が設けられています。USER により jitter 幅の下限を、75-100% の範囲で指定することができます。default では、jitter が 75% に設定されているため、keepalive interval x (75-100)% で interval が決定されます。jitter の設定については、timers bgp jitter を参照してください。

○ connect timer

＜説　　明＞　Connect timer を設定します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) timers connect <0-65535>
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) timers connect
＜初 期 値＞　neighbor (A.B.C.D|X:X::X:X) timers connect 120
＜備　　考＞　0 を設定すると、毎秒 connect しようとします。

○ update-source

＜説　　明＞　BGPパケットのソースアドレスを､指定したインタフェースのIPアドレスに変更します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) update-source
　　(ethernet<0-2>|loopback<0-9>|ppp<0-4>|tunnel<0-255>)
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) update-source

bgp mode

○ advertisement-interval
＜説　　明＞
・BGPの経路テーブルの変化を監視するタイマで、UPDATEメッセージの最小送信間隔になります。常に周期的に動作するタイマで、前回のUPDATE送信から経路情報に変化があった場合や、neighborからROUTE-REFRESHを受信した場合には、タイマ満了時にneighborへUPDATEメッセージを送信します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) advertisement-interval <1-600>
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) advertisement-interval
＜備　　考＞　タイマのデフォルト値は、eBGPが30(秒)、iBGPが5(秒)です。

○ as-origination-interval
＜説　　明＞
・本装置を起源とするBGP経路の変化を監視するタイマです。BGPネットワークの追加やfilterの適用、redistributeルートの変更など、内部のBGP経路情報の変化を周期的に監視します。前回のタイマ満了時からの変化を検出した場合、次のadvertisement-intervalタイマ満了時にUPDATEメッセージでadvertiseします。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) as-origination-interval <1-600>
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) as-origination-interval
＜備　　考＞　タイマのデフォルト値は、15(秒)です。

○ activate
＜説　　明＞
・本機能を有効（activate）にすると、ipv4 neighbor間/ipv6 neighbor間で、ipv4 networkをadvertiseします。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) activate
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) activate

○ interface
＜説　　明＞
・Peerのアドレスとして LLAを指定した場合に、BGPパケットを出力するインタフェースを指定します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) interface IFNAME
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) interface IFNAME
＜備　　考＞
・Ethernet/VLANのみ対応しています。
・update-sourceと併用する場合は、本設定と同じインタフェースの指定を推奨します。異なるインタフェースを指定した場合の動作については、サポートしていません。

bgp mode

◎ UPDATE の送信プロセス

Neighbor への UPDATE メッセージの送信プロセスは、advertisement-interval と as-origination-interval の 2 つのタイマによって支配されます。

- 自身を起源とするルート

as-origination-interval の周期で配信ルート情報を監視します。ルート情報に変化があった場合、UPDATE 送信ルート候補となり、次の advertisement-interval の周期で UPDATE 送信します。

- 他の peer から受信した BGP ルート

他の peer からの UPDATE 受信時に、それ以外の peer への UPDATE 送信ルート候補となり、次の advertisement-interval の周期で UPDATE 送信します。

- soft out リセット実行時

現在保持する全ての BGP ルートが UPDATE 送信ルート候補となり、次の advertisement-interval の周期で UPDATE 送信します。

bgp mode

■ redistribute

○ redistribute (connected|static|rip|ospf)

＜説　　明＞　RIPやOSPFで学習したrouteや、connected route、static routeを
　　BGPで再配信する機能です。Defaultルート情報も再配信されます。
＜書　　式＞　redistribute (connected|static|rip|ospf)
＜　no　＞　no redistribute (connected|static|rip|ospf)

○ redistribute (connected|static|rip|ospf) route-map ABCD

＜説　　明＞　routemap機能を適用することにより、再配信時に特定のprefixのみを配信したり、
　　特定のprefixを拒否したりすることができます。
＜書　　式＞　redistribute (connected|static|rip|ospf) route-map ABCD
＜　no　＞　no redistribute (connected|static|rip|ospf) route-map ABCD

■ netevent

○ advertise-stop

＜説　　明＞
・当該trackがdown状態へと遷移した場合は、network設定によって設定されているBGPルートの配信を停止します。また、当該trackがup状態へと遷移した場合は、BGPルートの配信を再開します。
＜書　　式＞　netevent <1-255> advertise-stop
　　netevent <2048-4095> advertise-stop
＜　no　＞　no netevent
＜備　　考＞
・BGP4のnetwork import-checkが有効な場合、trackがup状態であっても無効なルートは配信しません。

■ default

○ ipv4-unicast

＜説　　明＞　当該neighbor上で、交換するaddress familyのデフォルトをIPv4に設定します。
＜書　　式＞　bgp default ipv4-unicast
＜　no　＞　no bgp default ipv4-unicast

○ local-preference

＜説　　明＞　local preference値を設定します。
　　有効の場合、local-preferenceを、設定値でadvertiseします。
　　無効の場合、local-preferenceを「100」でadvertiseします。
＜書　　式＞　bgp default local-preference <0-4294967295>
＜　no　＞　no bgp default local-preference
＜備　　考＞　local preference値の一番大きいパスを優先します。

bgp mode

◎ BGP recursive route

・BGP で学習した route の nexthop に直接接続できない場合でも、static route によって nexthop への到達が確認できた場合、当該 route は有効になります。static route 以外では、nexthop の解決は行いません。

・recursive static route を設定する場合は、nexthop のみを指定します。出力インタフェースは、nexthop から取得します。インタフェースを指定した場合は、recursive route にはなりません。

・recursive route を、static route の nexthop 解決の route として、使用することは出来ません。

第 17 章

ntp mode

ntp mode

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#ntp
vxr-x86(ntp-config)#
```

◆ service

＜説　　明＞　NTP サービスを有効にします。
＜書　　式＞　service enable　　(有効)
＜　no　＞　no service enable　　(無効)

◆ server

＜説　　明＞　NTP サーバの設定を行います。
＜書　　式＞　server (A.B.C.D|FQDN|X:X::X:X) polling min<4-16> max<5-17>
＜初 期 値＞　no server
＜　no　＞　no server (A.B.C.D|FQDN|X:X::X:X)
＜備　　考＞

・NTP サーバは、2 つまで設定することが出来ます。
・サーバを設定しない場合は、ローカルサーバとして動作します。本装置がローカルサーバとして動作する場合、strantum level は「10」です。
・NTP サーバアドレスは、IPv4/IPv6/FQDN による指定が可能です。
・外部参照する NTP サーバが指定されている場合、時刻同期のために定期的に polling を行います。NTP の通信量を減らすために polling 間隔を大きくしたり、精度を上げるために polling 間隔を小さくしたりすることが出来ます。Polling 間隔の default 値は、最小 6（2 の 6 乗 =64 秒）、最大 10（2 の 10 乗 =1024 秒）です。最小値は、必ず最大値より小さい値になるように設定してください。

◆ timeout

＜説　　明＞　NTP サーバからの応答タイムアウト時間を設定することが出来ます。
＜書　　式＞　timeout <seconds:1-30>
＜初 期 値＞　timeout 30
＜　no　＞　no timeout (=timeout 30)
＜説　　明＞

・NTP サーバからのサンプリングを 4 回行うため、実際のタイムアウト時間は、timeout × 4 秒です。

◆ master

＜説　　明＞　本装置をローカルサーバとして設定した場合の stratum level を設定します。
　　初期値は「10」です。
＜書　　式＞　master　　<1-15>
＜初 期 値＞　master 10
＜　no　＞　no master

第 18 章

SNMP mode

SNMP mode

SNMP(Simple Network Management Protocol)機能

本装置の SNMP 機能は、system の情報を SNMP protocol を使用して取得する機能を有します。また、system にて状態の変化が発生した際に、NMS(SNMP Trap Manager)に trap を送信する機能も有します。なお、SNMP による設定(set)はサポートしていません(read-only です)。

■ SNMP version と access 制御

現在対応している SNMP の version は、v1、v2c です。SNMP Access 制御として、SNMP Server の network と community 名を指定することができます。Network に関しては、IPv4/IPv6 Address を指定することができます。

■ SNMP Trap

本装置内部で発生した状態変化を、指定された NMS に対して SNMP Trap にて通知する機能です。

- Trap version1/version2 に対応しています。また、inform を指定することもできます。Trap の送信先は、IPv4/IPv6 address で指定することが可能です。inform の場合は再送回数 / 再送間隔も指定することができます。
- SNMP trap 用の community 名を SNMP access 用とは別に指定することができます。これらの設定は、Trap の送信先毎に指定することができます。
- Trap は、監視対象の状態変化の通知や USER による設定変更によるイベント発生によって送信されます。Trap は、UDP を使用して送信するため必ず server 側へ届けられる保証はありません。このような場合は、inform を使用することで NMS へ届けられる可能性が高くなります。
- 各 service 状態を定期的に監視する機能は保持していないため、service の突然停止を検出し通知することは出来ません。このような状態を監視する場合は、NMS の機能を利用して周期的に get を行うようにしてください。

■ System Group MIB(MIB-II)設定

本装置では、RFC1213 にて定義されている MIB の内、以下の項目を UI より設定することが出来ます。

- sysContact
- sysName
- sysLocation
- sysDescr

なお、sysObjectID には、century にて定義した機器毎の OID が設定されていて機種の判定をすることができます。

また、sysUpTime アクセス時には、本装置が起動してからの経過時間を返します。(NTP などによる時刻変更の影響は受けません)。

SNMP mode

■ 対応MIB一覧

本装置にて対応するMIBは次のとおりです。

・Standard
RFC1213 (SNMPv2 MIB-II)
RFC2011 (IP-MIB)
RFC2012 (TCP-MIB)
RFC2013 (UDP-MIB)
RFC2863 (IF-MIB)
RFC3411 (SNMP-FRAMEWORK-MIB)
RFC3412 (SNMP-MPD-MIB)
RFC3413 (SNMP-TARGET-MIB: SNMP-NOTIFICATION-MIB: SNMP-PROXY-MIB)
RFC3414 (SNMP-USER-BASED-SM-MIB)
RFC3415 (SNMP-VIEW-BASED-ACM-MIB)
RFC3418 (SNMPv2 MIB)
RFC2465 (IPv6 MIB) ※一部対応

・Private MIB
CS-NXR-PRODUCT-MIB
CS-NXR-L2TPv3-MIB

■ デバイス情報

USBポートに装着したデバイスの情報をSNMPで取得することが出来ます。また、デバイスを装着あるいは取外した場合は、トラップを送信します。

以下に、取得可能な情報やトラップ情報の例を示します。詳細については、CS-NXR-PRODUCT-MIBを参照してください。

○デバイス情報の取得
・USBポートに装着したデバイスの情報をSNMPで取得することが出来ます。未対応のデバイスが装着されている場合は、unknownと表示されます。
・モバイルデータ通信端末では、シグナル状態(up/down)を取得することが出来ます。USBメモリの場合は、シグナル状態はnotSupportとなります。また、モバイルデータ通信端末がPPP接続中の場合は、シグナル状態はnotAccessibleとなります。

○トラップの送信
・USBポートにデバイスを装着または取外した場合に、トラップ(up/down)を送信します。ただし、未対応のデバイスの場合は、トラップを送信しません。
・モバイルデータ通信端末では、シグナル状態が0以下（errorを含む）となった場合にdownトラップを送信します。また、シグナル状態が1以上となった場合にupトラップを送信します。
・モバイルデータ通信端末モジュールをリセットした場合は、down->upのトラップを送信します。

■ SNMP NAT

SNMP PDU部分に含まれるIPアドレス型のNATに対応しています。NATの方法については、RFC2962準拠とし、BASICのみ対応しています。PDU内のIPアドレスのうちNAT対象となったアドレスの先頭1オクテットのみを変換します。

SNMP mode

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#snmp
vxr-x86(snmp-config)#
```

◆security

```
<説　　明>　SNMPマネージャを使いたいネットワーク範囲を指定します。
<書　　式>　security A.B.C.D/M|X:X::X:X/M COMMUNITY
<初 期 値>　no security
<備　　考>　Networkは、3つまで設定することが出来ます。
<　 No　 >　no security (A.B.C.D/M|X:X::X:X/M)
```

◆ syslocation

```
<説　　明>　sysLocationを設定します。
<書　　式>　syslocation LOCATION
<初 期 値>　no syslocation
<　 No　 >　no syslocation
```

◆ syscontact

```
<説　　明>　sysContactを設定します。
<書　　式>　syscontact CONTACT
<初 期 値>　no syscontact
<　 No　 >　no syscontact
```

◆ sysname

```
<説　　明>　sysNameを設定します。
<書　　式>　sysname SYSNAME
<初 期 値>　no sysname  [=機種名(ex. NXR-G100)]
<　 No　 >　no sysname
```

◆ sysdescr

```
<説　　明>　sysDescrを設定します。
<書　　式>　sysdescr DESCRIBE
<初 期 値>　no sysdescr
<　 No　 >　no sysdescr
<備　　考>　初期値は ビルド名です。
            ex. Century Systems VXR Series ver 8.0.0E (build 41/11:53 15 06 2015)
```

SNMP mode

◆ **trap manager**

＜説　　明＞　SNMP の trap manager を設定します。
＜書　　式＞
trap manager (A.B.C.D|X:X::X:X) (|trapcommunity) (|v1|v2)
trap manager (A.B.C.D|X:X::X:X) (|trapcommunity) inform [|(interval <10-1800>)|(retry <0-10>]
＜初 期 値＞　no trap manager
＜　No　＞　no trap manager (|A.B.C.D|X:X::X:X)
＜備　　考＞　3つまで設定することができます。
　　Community 未指定時は "community" を使用します。
　　pdu-type 未指定時は v1 を使用します。

◆ **trap agent**

＜説　　明＞
・TRAP パケット中の Agent Address を、IP アドレスまたはインタフェースにて指定することが出来ます。
＜書　　式＞　trap agent ip A.B.C.D
　　trap agent interface ethernet <0-2>
＜初 期 値＞　no trap agent
＜　No　＞　no trap agent
＜備　　考＞
・インタフェースを指定した場合、当該インタフェースのプライマリー IP アドレスを使用します。
・指定した IP アドレスが、リンクダウン等の理由で使用不可の場合、他のインタフェース（ethernet0 → ethernet1 → ethernet2...）のアドレスを使用します。

◆ **bind address**

＜説　　明＞　TRAP 送信時のソースアドレス（IPv4 アドレスのみ対応）を指定することが出来ます。
＜書　　式＞　bind address A.B.C.D
　　bind address X:X::X:X
＜初 期 値＞　no bind address
＜　No　＞　no bind address
＜備　　考＞
・指定したアドレスを持つインタフェースが、リンクダウンの状態であっても、当該アドレスをソースアドレスとして使用します。
・本設定時に、該当アドレスを保持していない場合は、外部からの SNMP アクセスが出来なくなります。また、その後 IP アドレスを設定しても、自動的に復旧しないため、restart snmp などの操作が必要になります。
・例えば、IPsec policy にマッチせずに、SNMP パケットがドロップされてしまうようなケースで、本設定によるソースアドレスを指定することによって、IPsec tunnel 経由での SNMP 通信が可能になります。

第 19 章

syslog mode

syslog mode

◆ 移行command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#syslog
vxr-x86(syslog-config)#
```

◆ local enable

＜説　　明＞　syslogをローカル出力します。
＜書　　式＞　local enable
＜初 期 値＞　local enable
＜　No　＞　no local enable （ローカル出力しません）

◆ local file

＜説　　明＞　syslogをファイルに出力します。
＜書　　式＞　local file disk0:FILENAME
＜初 期 値＞　no local file
＜　No　＞　no local file
＜備　　考＞　filenameは「disk0:」で始まる任意のファイル名を指定します。

◆ server

＜説　　明＞

- syslogサーバのIPアドレスまたはFQDNを設定します。
- syslogサーバは、5つまで設定することができます。
- syslog送信時の送信元アドレスを設定することができます。
- リモートサーバへsyslogを転送する際のUDP port番号（default:514）を指定することが出来ます。

＜書　　式＞

```
server (A.B.C.D|X:X::X:X|FQDN)
server (A.B.C.D)| X:X::X:X | FQDN) source (A.B.C.D|X:X::X:X)
server (A.B.C.D | X:X::X:X | FQDN) port <1024-65535>
server (A.B.C.D)| X:X::X:X | FQDN) port <1024-65535> source (A.B.C.D|X:X::X:X)
```

＜　No　＞　no server (A.B.C.D|X:X::X:X|FQDN) (= syslogサーバに転送しません)

＜備　　考＞

- syslogサーバへの転送が失敗した場合は、再送キューに蓄積し、60秒後に再送します。以降、60秒毎に再送を試行し、syslogサーバへの転送が成功すると、再送キューをクリアします。
- この場合のタイムスタンプは、サーバへの送信時刻ではなく、最初にsyslogを送信しようとした際の時刻になります。
- 蓄積可能なメッセージキューの長さは、1000件です。

syslog mode

◆ mark

<説　　明>　Syslog markの設定をします。
　　Markの出力間隔を0～10080分の範囲で指定することができます。
　　Defaultは20分毎とし、0を指定した場合、markは出力されません。
<書　　式>　mark <min:0-10080>
<初 期 値>　mark 20
<　No　>　no mark　　(=mark 20)
<備　　考>　mark 0　　(markは出力しません)

◆ priority

<説　　明>　Syslogのプライオリティを設定することができます。
<書　　式>　priority (debug|info|notice)
<初 期 値>　priority info
<　No　>　no priority
<備　　考>　facilityは、指定することができません。

◆ system

<説　　明>
・System Message出力機能とは、Connection tracking数、Load Average、メモリ使用量、温度状態などのシステムの情報を、mark出力時または、一時間毎にsyslog上に出力させる機能です。
・システム内の情報であるため、外部remote serverへ出力することは推奨しません。
<書　　式>　system mark　　: Output messages with mark
　　system hour　　: Output messages hourly
<初 期 値>　no system
<　No　>　no system　　: Systemメッセージ出力しない

◆ suppress

<説　　明>
・同じmessageが繰り返し表示される場合、毎回表示せずに、そのmessageが何回繰り返して出力されたかどうかのみを表示する機能です。
<書　　式>　suppress <10-3600>
<初 期 値>　no suppress
<　No　>　no suppress
<備　　考>
・Suppressする時間を10-3600secの間で指定することができます。
・last messageが繰り返し出力された場合、suppress messageとして表示されます。
・Defaultでは、suppressは無効です。

syslog mode

◆ mail send
<説　　明>　syslogメッセージをメール送信します。
・USERが指定した文字列を含むmessageがsyslogへ出力された場合、設定されたE-mail addressにmailを送信する機能です。この機能により、CLIへのlogin失敗時などの不正アクセスがあった場合に、管理者にmailを送るようなことが可能になります。
・指定した文字列が含まれるかどうかを、60sec毎にcheckし、該当する文字列が存在した場合にmail送信します。なお、mail送信機能については、IPv4/IPv6の両方をサポートします。
<書　　式>　mail send enable
<初 期 値>　no mail send
<　No　>　no mail send

◆ mail to
<説　　明>　送信先メールアドレスを設定します。
<書　　式>　mail to RECEIVER
<初 期 値>　no mail to
<　No　>　no mail to

◆ mail from
<説　　明>　送信元メールアドレスを設定します。
<書　　式>　mail from SENDER
<初 期 値>　no mail from
<　No　>　no mail from

◆ mail subject
<説　　明>　メールの件名を設定します。
<書　　式>　mail subject SUBJECT
<初 期 値>　no mail subject
<　No　>　no mail subject

◆ mail strings
<説　　明>　ここで指定した文字列が含まれるログをメールで送信します。
<書　　式>　mail strings <1-32> STRINGS
<初 期 値>　no mail strings
<備　　考>　メール検索文字列は32行まで設定可
<　No　>　no mail strings <1-32>

◆ mail server authentication
<説　　明>　メールサーバの認証方法を設定します。
<書　　式>　mail server authentication pop-before-smtp　POP before SMTP
　　mail server authentication smtp-auth-login　SMTP authentication (login)
　　mail server authentication smtp-auth-plain　SMTP authentication (plain)
<　No　>　no mail server authentication

syslog mode

◆ mail server address
＜説　　明＞　POP3 サーバのアドレスを設定します。
＜書　　式＞　mail server address A.B.C.D
　　mail server address FQDN

◆ mail server smtp
＜説　　明＞　SMTP サーバのアドレスおよびポート番号を設定します。
＜書　　式＞　mail server smtp address A.B.C.D
　　mail server smtp address FQDN
　　mail server smtp port <1-65535>

◆ mail server username
＜説　　明＞　SMTP サーバのユーザ ID とパスワードを設定します。
＜書　　式＞　mail server username USERNAME password (|hidden) PASSWORD

◆ rotate
＜説　　明＞
○Default の動作では、syslog message の容量が最大許容量の 80% を超えると、後方の 4000 行を残して削除します。システム起動時より、10 分周期で自動的にチェックします。
○上記動作とは別に、syslog rotate 機能を設定することが出来ます。
・Rotate 設定を行うと、syslog のサイズが閾値を超えていた場合に、指定された storage 上に backup を行います（閾値を指定しない場合は、サイズに関係なく backup を行います）。
・Schedule 機能によって rotate の指示を行うため、rotate を有効にし、かつ schedule 機能で実行日時を指定する必要があります。
・Default では、rotate は無効です。
＜書　　式＞
　rotate disk0
　rotate disk0 threshold logsize <kbytes:150-1000>
　rotate disk0 threshold files <files:1-10>
　rotate disk0 threshold logsize <kbytes:150-1000> files <files:1-10>
＜初　期　値＞　no rotate
＜　No　＞　no rotate
＜備　　考＞
・disk0 は、ディスクイメージ内のユーザ割り当て領域です。
・Syslog rotate の閾値はサイズ指定(kbytes)です。また、backup file の数も指定することができます。backup file 数の default 値は、5(files)です。
・なお、backup された syslog message は、gzip にて圧縮されます。また、下記フォーマットの file 名になります。なお、Backup 先に同じ名前の file が存在した場合、上書きされます。
　backup ファイル名の format ： YYYYMMDD_HHMM.log.gz
　2010 年 11 月 2 日 19 時 50 分に取得した backup ファイルの例 ： 20101102_1950.log.gz

syslog mode

◆ auto-rotate

＜説　　明＞

・firmware update や restart によるシステム再起動時に、syslog のバックアップを取得する機能です。

＜書　　式＞　auto-rotate enable

＜初 期 値＞　auto-rotate enable

＜　No　＞　no auto-rotate enable

＜備　　考＞

・syslog メッセージのサイズに関係なく、バックアップを取得します。threshold の logsize は無視しますが、files は指定値に従います。

・Default で、本機能は有効です。ただし、rotate disk0 の設定がない場合、syslog のバックアップは行いません。

・ファイル名は、次のようになります。

backup ファイル名の format ： YYYYMMDD_HHMM_restart.log.gz

2010 年 11 月 2 日 19 時 50 分に取得した backup ファイルの例 ： 20101102_1950_restart.log.gz

syslog mode

■ フィルタログ機能

パケットが、IPv4 ACL、IPv6 ACL、SPI フィルタにマッチした場合、syslog に出力することが出来ます。

□ フィルタログ出力レート制限

・ログ出力有効時、当該フィルタに大量のパケットがマッチすると、ログ出力にシステムリソースを消費してしまい、サービス停止（DoS 攻撃)状態になる可能性が考えられます。
・この対策として、ログ出力のレート（packets/sec）を制限することが出来ます。
・なお、レート制限以下の場合でも、システムの負荷状況等により、ログ出力しない場合があります。また、制限を設けていても、通信環境によっては、ログが大量発生し、ログ容量が大きくなる場合があります。このため、ログの管理には、十分に注意するようにしてください。

● SPI フィルタログ

・1 秒間に出力可能なログ数を設定することが出来ます。Default は「10」です。
・WAN 側からの意図しないパケットが、SPI フィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分な注意が必要です。
・設定については、ip spi-filter log/ipv6 spi-filter log コマンドを参照してください。

●フィルタログ

・1 秒間に出力可能な log 数の最大値は「10」です。
・すべての ACL にログを設定すると、システムが高負荷状態になる可能性があるため、ログ出力は最小限にとどめるようにしてください。
・設定については、ip access-list/ipv6 access-list コマンドを参照してください。

● P2P 検出ログ

・1 秒間に出力可能なログ数の最大値は、winny/share 検出の場合「10」、bittorrent の場合「5」です。

■ net-ratelimit 機能

・システムからログを出力する際、パケット毎にログを出力すると、システムに非常に負荷がかかり、DoS（DDoS）攻撃 etc によってサービス停止状態になる可能性があります。そのため、単位時間当たりに出力可能なログの数を制限しています。
・5 秒間に出力可能なログの数は、最大 10 です（設定の変更は出来ません)。
・出力できなかったログは、その後のログ出力時に、supress message 数としてログ出力します。
・具体的には、以下のログの出力レートを制限します。
  ・ip martian-log 機能によるログの出力
  ・L2TPv3 からのエラーログ（Error:Unknown session SESSION_ID）の出力

第 20 章

dhcp-server mode

dhcp-server mode

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#dhcp-server <1-64>
vxr-x86(dhcps-config)#
```

◆ network

<説　　明>　DHCP サーバを動作させるネットワークを指定します。
<書　　式>　network A.B.C.D/M range <starting IP: E.F.G.H> <ending IP: I.J.K.L>
<　No　>　no network A.B.C.D/M range <starting IP: E.F.G.H> <ending IP: I.J.K.L>
<備　　考>　最大 16 個設定することができます。複数の場合、network を同一にしてください。

◆ lease-time

<説　　明>　IP アドレスのリース時間を設定します。
<書　　式>　lease-time <default:60-15552000> <max:60-15552000>
<初 期 値>　lease-time 21600 43200
<　No　>　no lease-time (=lease-time 21600 43200)

◆ gateway

<説　　明>　DHCP クライアントのデフォルトゲートウェイとなる IP アドレスを指定します。
<書　　式>　gateway A.B.C.D
<初 期 値>　no gateway
<　No　>　no gateway

◆ domain

<説　　明>　DHCP クライアントに割り当てるドメイン名を指定します。
<書　　式>　domain DOMAIN
<初 期 値>　no domain
<　No　>　no domain

◆ dns-server

<説　　明>　DHCP クライアントに割り当てる DNS サーバアドレスを指定します。
<書　　式>　dns-server <primary DNS: A.B.C.D>
　　dns-server <primary DNS: A.B.C.D> <secondary DNS: A.B.C.D>
<初 期 値>　no dns-server
<　No　>　no dns-server
<備　　考>　プライマリー DNS とセカンダリー DNS を設定することが出来ます。

dhcp-server mode

◆ **netbios-server**

＜説　　明＞　NetBIOS サーバの IP アドレスを設定します。
＜書　　式＞　netbios <primary NetBIOS: A.B.C.D>
　　netbios <primary NetBIOS: A.B.C.D> <secondary NetBIOS: A.B.C.D>
＜初 期 値＞　no netbios-server
＜　No　＞　no netbios-server　(= Delete)
＜備　　考＞　プライマリーとセカンダリーを設定することが出来ます。

◆ **netbios-scope-id**

＜説　　明＞　NetBIOS スコープ ID を配布できます。
＜書　　式＞　netbios-scope-id SCOPED-ID
＜初 期 値＞　no netbios-scope-id
＜　No　＞　no netbios-scope-id

◆ **sip-server**

＜説　　明＞　DHCP client からの SIP server 要求に対して、SIP server address を割り当てます。
＜書　　式＞　sip-server A.B.C.D (|A.B.C.D)
　　sip-server FQDN (|FQDN)
＜初 期 値＞　no sip-server
＜　No　＞　no sip-server
＜備　　考＞　IPv4 address または FQDN を最大 2 つまで設定することができます。

◆ **RFC2131 compatibility broadcast bit**

＜説　　明＞
・DHCP server の動作を RFC2131 に準拠させるかどうかを指定する機能です。RFC2131 では broadcast bit が 1 である DHCP packet 受信時、応答の MAC address を broadcast(FF:FF:FF:FF:FF:FF)で送信するべきと記されています。
・このオプションを無効にすると、broadcast bit の値によらず、DHCP packet の応答を常に unicast frame(但し、destination IP address は、オプションが有効な場合と同様 limited broadcast)として送信します。
・このオプションは、default で有効です。
＜書　　式＞　rfc2131-compatibility broadcast-bit enable
＜初 期 値＞　rfc2131-compatibility broadcast-bit enable
＜　No　＞　no rfc2131-compatibility broadcast-bit enable

第 21 章

dhcp-relay mode

dhcp-relay mode

DHCPv4 リレー機能

DHCPv4 リレー機能は、LAN 側より受信したブロードキャスト宛ての DHCP パケットを、PPP やトンネルインタフェースに対してユニキャストパケットとして転送する機能です。リレーの際の出力先インタフェースについては、ルーティングテーブルに依存します。

ユニキャストパケットとして転送する際、DHCP パケットの giaddr フィールドに、DHCP パケットを受信したインタフェースの IPv4 アドレスを設定します。DHCP サーバは、giaddr の情報を元にして、クライアントに割り当てるネットワークのアドレスを決定します。

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#dhcp-relay
vxr-x86(dhcpr-config)#
```

◆ address

＜説　　明＞　BOOTP Request パケットの転送先となる上位 DHCP サーバの IP アドレスを指定します。
＜書　　式＞　address A.B.C.D
＜初 期 値＞　no address
＜　No　＞　no address A.B.C.D
＜備　　考＞　上位 DHCP サーバは、4 つまで設定することができます。

◆ accept

＜説　　明＞
・DHCP サーバ機能と同時に運用する場合を考慮し、クライアントからの BOOTP Request パケットを受信するインタフェースを指定することが出来ます。
＜書　　式＞　accept ethernet <0-2>
＜　No　＞　no accept ethernet <0-2>
＜備　　考＞
・指定外のインタフェースで受信した BOOTP Request パケットは DROP します。
・Ethernet インタフェースのみ指定することが出来ます。指定しない場合は、どの Ethernet インタフェースで受信した場合でもリレーします。

第 22 章

ipsec local policy mode

ipsec local policy mode

◆ 移行command

```
vxr-x86(config)#ipsec local policy <policy:1-255>
vxr-x86(config-ipsec-local)#
```

◆ address

＜説　　明＞　IPsec tunnelのソースIPを指定します。
＜書　　式＞　address ip
　　address ipv6 (|X:X::X:X)
＜備　　考＞
・IPv6アドレスを指定する場合
指定したIPv6アドレスが存在しない（使用できない）場合は、当該IPsec設定は使用できません。
・IPv6アドレスを指定しない場合
（IPsec policy XXでマッピングした）インタフェース上のIPv6アドレスを、本装置が自動的に選択します。

◆ self-identity

＜説　　明＞　本装置のIDを設定します。
＜書　　式＞　self-identity fqdn FQDN　　(例: centurysys.co.jp)
　　self-identity user-fqdn USER@FQDN (例: user@centurysys.co.jp)
　　self-identity dn DN　　(備考を参照してください)
　　self-identity key KEY-ID　　(KEY IDを指定します。)
＜初　期　値＞　no self-identity
＜　No　＞　no self-identity
＜備　　考＞
・DNを指定した場合に使用する文字列の例です。
C=JP,ST=Tokyo,O=century,OU=dev,CN=vxr1.centurysys.co.jp,E=admin@centurysys.co.jp

◆ x509 certificate

＜説　　明＞　X.509証明書を設定します。
＜書　　式＞　x509 certificate CERTIFICATE　　(証明書の設定)
＜　No　＞　no x509 certificate　　(証明書のクリア)

ipsec local policy mode

■動的IPアドレス環境下での接続について

□動的IPアドレスのクライアントからの接続

IKEv1 main モードでは、相手を識別するIDの交換を、phase1の最後に行いますが、情報が暗号化されているため、PSK認証方式利用時には、IDとPSKを結び付けて認証処理を行うことが出来ません。したがって、PSKと相手を結び付けるキーには、IPアドレスを使用します。
しかしながら、リモートアクセスのように接続毎にIPアドレスが変化する環境下では、responder側で事前に相手ID（IPアドレス）とPSKを結び付けることが出来ません。そのため、動的IPアドレスからの接続を受け付けるには、以下のいずれかの方法を用いて設定を行う必要があります。

・Aggressive モードを使用する
・Main モードで、すべての通信相手との間で同一PSKを使用する
（デジタル署名方式では、PSKを検索する必要がないため、上記のような制限はありません。）

※リモートアクセス環境下では、PSK/RSAの認証に加えて、可能な限りxauthの使用を推奨しています。
※ IKEv2では、IDによって対向SGを識別することが出来るため、動的IP環境下であっても、対向毎に異なるPSKを設定してPSK認証を行うことが出来ます。

□動的IPアドレス環境下でのPSK認証による接続

自分が動的IPアドレスの場合、事前にIPアドレスとPSKとの関連付けが出来ないため、IPアドレス以外の識別子をIDとして指定することになります。
しかしながら、IDを設定できない、あるいはIDを設定するとaggressive モードで動作するクライアントが存在するため、相互接続性が悪いという問題が存在します。
この対応として、本装置では、IPアドレスを自分IDとして利用することで、動的IP環境下でのPSK認証を可能にしています（ID（IPアドレス）とPSKの関連付けは、IPアドレスが割り当てられた時点で行います）。
これにより、センター機器が、動的IPであっても、DDNSを利用することで、PSK認証を行うことが出来ます。

第 23 章

ipsec isakmp policy mode

ipsec isakmp policy mode

◆ 移行command
```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#ipsec isakmp policy <policy:1-65535>
vxr-x86(config-ipsec-isakmp)#
```

◆ description
<説　　明>　ISAKMP policyの説明を記述します。
<書　　式>　description DESCRIPTION
<　No　>　no description

◆ version
<説　　明>　IKEのバージョン(IKEv1/IKEv2)を指定します。
<書　　式>　version (1|2)
<初 期 値>　version 1
<備　　考>
・IPsec ISAKMP policy毎に指定することができます(IKEv1とIKEv2を同時に使用することができます)。

■ IKEのパラメータ折衝
□ IKEv1
・本装置がresponderになる場合、本装置の設定には依存せず、initiatorが送ってきたものの中から、transform playloadに設定された順番に、採用可能かどうかを判断して選択します。
・ただし、セキュリティ強度の観点から、暗号化アルゴリズムのプロポーザルとしてDESが指定されてきた場合は、本装置側でも暗号化アルゴリズムとしてDESを設定している場合のみ受け付けます。
□ IKEv2
・本装置がresponderになる場合、設定したtransformセット（暗号化方式やhashアルゴリズム）と一致しない場合は接続を拒否します。

◆ hash
<説　　明>　ハッシュアルゴリズムを設定します。
<書　　式>　hash (md5|sha1|sha256|sha384|sha512)
<初 期 値>　hash sha1

◆ encryption
<説　　明>　暗号化アルゴリズムを設定します。
<書　　式>　encryption (des|3des|aes128|aes192|aes256)
<初 期 値>　encryption aes128

◆ group
<説　　明>　DH (Diffie-Helman) groupを設定します。
<書　　式>　group (1|2|5|14|15|16|17|19|20|21|25|26)
<初 期 値>　group 2

ipsec isakmp policy mode

◆ lifetime
＜説　　明＞
　ISAKMP SAのライフタイム(Hard timer)を設定します。この時間を経過するとSAを削除します。
＜書　　式＞　lifetime <121-86400>
＜初 期 値＞　lifetime 10800　(=3 hours)
＜　No　＞　no lifetime　　(=lifetime 10800)

◆ isakmp-mode
＜説　　明＞　Phase1のネゴシエーションモードを設定します。
＜書　　式＞　isakmp-mode (main|aggressive)

◆ authentication pre-share
＜説　　明＞　PSK認証を使用します。
＜書　　式＞　authentication pre-share KEY

◆ authentication rsa-sig
＜説　　明＞　RSA認証を使用します。
＜書　　式＞　authentication rsa-sig
　　authentication rsa-sig KEY
＜備　　考＞
・次のように、versionコマンドでIKEv2を指定した場合は、raw RSA key情報は無視されます。
```
ipsec isakmp policy 1
 version 2
 authentication rsa-sig AAAAAAAAAAAAAAAAA
```

◆ xauth
＜説　　明＞　xauthを使用します。
＜書　　式＞　xauth mode client USERID
　　xauth mode server
＜　No　＞　no xauth
＜備　　考＞　USERIDは、ipsec xauth(global mode参照)で設定したusernameに一致させます。
　　useridとpasswordは、ipsec xauth(global mode参照)で設定します。

ipsec isakmp policy mode

■ authentication local/remote (IKEv2のみ)

○ local

＜説　　明＞　IKEv2で、自分が使用する認証方式を指定します。

＜書　　式＞　authentication local pre-share WORD
　　authentication local rsa-sig
　　authentication local eap-md5

○ remote

＜説　　明＞　IKEv2で、対向が使用する認証方式を指定します。

＜書　　式＞　authentication remote pre-share (|WORD)
　　authentication remote rsa-sig
　　authentication remote eap-md5
　　authentication remote eap-radius
　　authentication remote eap-mschapv2

＜　No　＞　no authentication remote

＜備　　考＞

・IKEv2では、次の例のように自分が使用する認証方式と対向が使用する認証方式が異なっていても構いません。

```
自分  authentication local eap-md5
      authentication remote rsa-sig
対向  authentication local rsa-sig
      authentication remote eap-md5
```

・pre-shareの設定例1: 1対1接続の場合

```
自分  authentication remote pre-share WORD
      authentication local pre-share WORD
対向  authentication remote pre-share WORD
      authentication local pre-share WORD
```

・pre-shareの設定例2: 1対多接続(対向が動的IPで複数台)の場合

```
自分   ipsec pre-share identity fqdn NXR1 password WORD1
       ipsec pre-share identity fqdn NXR2 password WORD2
       !
       ipsec isakmp policy 1
        authentication remote pre-share
        authentication local pre-share WORD
        remote address ip any
       ・・・省略・・・
       !
対向1 authentication remote pre-share WORD
       authentication local pre-share WORD1
対向2 authentication remote pre-share WORD
       authentication local pre-share WORD2
```

< 次ページに続く >

■ authentication local/remote (続き)

＜備　　考＞

・rsa-sigの設定例 [X.509認証(自分)＋EAP-MD5(対向]

自分

```
ipsec x509 enable
ipsec x509 ca-certificate VXR_CA
ipsec x509 certificate VXR_CERT
ipsec x509 private-key PRIV_KEY key
ipsec x509 private-key PRIV_KEY password PASSPHRASE
ipsec x509 crl VXR_CRL
ipsec eap identity string MYID password PASSWORD
!
ipsec local policy 1
 address ip
 x509 certificate VXR_CERT
・・・省略・・・
!
ipsec isakmp policy 1
 version 2
 authentication remote eap-md5
 authentication local rsa-sig
・・・省略・・・
!
```

対向

```
ipsec x509 ca-certificate VXR_CA
ipsec eap identity string MYID password PASSWORD
!
ipsec isakmp policy 1
 version 2
 authentication remote rsa-sig
 authentication local eap-md5
 eap-identity MYID
 remote identity dn
      C=JP,ST=Tokyo,O=century,OU=dev,CN=vxr1.centurysys.co.jp,E=admin@centurysys.co.jp
・・・省略・・・
!
```

< 次ページに続く >

ipsec isakmp policy mode

■ authentication local/remote (続き)

＜備　　考＞

・eap-md5の設定例

```
自分  ipsec eap identity string MYID password PASSWORD
      !
      ipsec isakmp policy 1
       authentication local eap-md5
       eap-identity MYID
      ・・・省略・・・
      !
対向  ipsec eap identity string MYID password PASSWORD
      !
      ipsec isakmp policy 1
       authentication remote eap-md5
      ・・・省略・・・
      !
```

・eap-radiusの設定例

```
自分  ipsec eap radius A.B.C.D password SECRET
      !
      ipsec isakmp policy 1
       authentication remote eap-radius
      ・・・省略・・・
      !
対向  ipsec eap identity string MYID password PASSWORD
      !
      ipsec isakmp policy 1
       authentication local eap-md5
       eap-identity MYID
      ・・・省略・・・
      !
```

ipsec isakmp policy mode

◆ reauthentication (IKEv2のみ)

＜説　　明＞

・IKEv2では、rekeyのタイミングでreauthを行うかrekeyを行うかを選択することができます。

＜書　　式＞　reauthentication enable

＜初 期 値＞　reauthentication enable

＜　No　＞　no reauthentication enable

＜備　　考＞

・Defaultでは、reauthが有効です。reauth時は、IKE SAのrekey時にCHILD SAの再作成も行われます。reauthを無効にした場合、rekeyが実施されます。

・セキュリティを考慮する場合はreauthを選択するようにしてください。ただし、Security Gatewayに(VXRだけでなく対向装置にも)負荷がかかるため、負荷に配慮する場合はrekeyを選択するようにしてください。

ipsec isakmp policy mode

◆ keepalive

＜説　　明＞　IPsec keepalive(DPD:RFC3706)を設定します。
＜書　　式＞　keepalive periodic (|clear|hold|restart)
　　keepalive <interval:10-3600> <retry:0-60> periodic (|clear|hold|restart)
＜初 期 値＞　keepalive 30 3 periodic restart
＜　No　＞　no keepalive
＜備　考1＞

- DPDは、SG(Security Gateway)のdownやSG間のIP reachability、およびIKE SAの状態監視を目的としています。DPDで、IPsec SAの状態を監視することは出来ません。
- keepaliveが有効でも、SG間でIPsecパケットの通信がある間は、DPDパケットを送信しません。
- no keepaliveを設定すると、DPDパケットを送信しません。ただし、対向SGからのDPDパケットには応答します。
- keepalive 10 3 periodicを設定した場合、10秒間隔で合計4回のR-U-THEREメッセージを送信します。R-U-THERE-ACKメッセージを1回も受信しない場合にエラーと判定します。

＜備　考2＞

- DPDでエラーを検出した場合、IKE/IPsec(CHILD) SAおよびIPsec policyを削除します。その後の動作は、DPDエラー時のアクション設定(clear, hold, restart)に依存します。
  - ○ clear
    SAおよびpolicyの削除後は、ユーザの指示を待ちます。
  - ○ hold
    SAの削除後は、policyのみが有効になります。policyにマッチするパケットを受信するとIKE phase1（version2の場合は、IKE SA INIT）ネゴシエーションを開始します。ただし、ipsec tunnel policyで、negotiation-mode=responderに設定している場合は、IKEネゴシエーションしません。
  - ○ restart
    SAおよびpolicyの削除後に、IKE phase1（version2の場合は、IKE SA INIT）を開始します。ただし、ipsec tunnel policyで、negotiation-mode=responderに設定している場合は、IKEネゴシエーションしません。

＜備　考3＞

- DPDエラーとなったIKEに、backup policyを指定している場合は、backup policyのネゴシエーションを開始します（backup policyを指定していない場合は、backup動作は実施しません）。
- backup policyを指定している場合でも、当該backup policyのnegotiation-modeがresponderの場合は、ネゴシエーションを開始しません。

◆ backup policy

＜説　　明＞　IPsec isakmpのbackup policyを設定します。
＜書　　式＞　backup policy <1-65535>
＜初 期 値＞　no backup policy
＜　No　＞　no backup policy
＜備　　考＞　backup policyは、ISAKMP毎に設定します。

ipsec isakmp policy mode

◆ rekey

＜説　　明＞

・Rekey の soft timer は、margin と increased-ratio により決定されます。
・Margin は、lifetime が切れる何秒前から rekey を実行するかどうかを指定します。
・increased-ratio 値は、margin よりどれぐらい増やすかを % で指定します。

＜書　　式＞　rekey margin <30-360> (increased-ratio <0-100>|)

＜初 期 値＞　no rekey margin

＜備　　考＞

・以下の式によって、Soft timer の最小・最大が決定され、この間でランダムに Soft timer が設定されます。

minimum soft timer = lifetime - margin
maximum soft timer = lifetime - (margin + margin x increased-ratio/100)

・default 値は、margin が 270sec、increased-ratio は 100% です。このため、lifetime から 270 ～ 540sec 前の時間がランダムで設定されます。但し、Responder の場合、soft timer は、margin/2 時間分早く設定されます。これは、initiator 側より rekey を行うようにするためです。
・increased-ratio を 0 に設定すると soft timer が毎回同じ値となります。負荷の分散やセキュリティ的に問題があるため、設定しないことを推奨します。
・negotiation-mode が responder の場合、当該機器からは rekey を実行しません。

◆ remote address

＜説　　明＞　対向の IP/IPv6 アドレス、または FQDN を設定します。

＜書　　式＞　remote address ip (A.B.C.D|any|FQDN)
　　remote address ipv6 (X:X::X:X|any|FQDN)

◆ remote identity

＜説　　明＞　対向の ID を設定します。

＜書　　式＞

remote identity fqdn FQDN	(例: centurysys.co.jp)
remote identity user-fqdn USER@FQDN	(例: user@centurysys.co.jp)
remote identity dn DN	(備考を参照してください)
remote identity key KEY-ID	(KEY ID を指定します。)

＜初 期 値＞　no remote identity

＜　No　＞　no remote identity

＜備　　考＞

・peer identity 未設定時は、IP/IPv6 アドレスを ID として使用します。
・DN を指定する場合の文字列の例です。
　C=JP,ST=Tokyo,O=century,OU=dev,CN=vxr1.centurysys.co.jp,E=admin@centurysys.co.jp
・DN を指定する場合、次のように RDN にて "*" を使用することが出来ます。
　C=JP,ST=Tokyo,CN=*
　ただし、C=JP,ST=Tokyo,CN=*.centurysys.co.jp のように、一部に * を指定することはできません。

ipsec isakmp policy mode

■ FQDN対応（SGが動的IPの場合）

リモートSGが動的IPのため、固定IPを指定出来ない場合は、FQDNを指定します。
（IKEv1のみ対応しています。IKEv2では未対応です。）

○本装置がinitiatorとして動作
対向アドレスがFQDN指定の場合は、DNSによって名前解決を行い、当該IPアドレスに対してIKEパケットを送信します。

○本装置がresponderとして動作
mainモードでPSK認証を行う場合、remote address ip anyを設定します。
※mainモードのPSK認証の際、IPアドレスでPSKの検索を行うためです。対向の設定がFQDN指定だけの場合は、PSKが見付からずに認証エラーとなります。

◎mainモード＋PSK認証におけるresponder側での設定
remote address ip any　（必ず設定します）
remote address ip FQDN　（必要ならば設定します）
※FQDNとanyで、同一PSKを使用するようにしてください。

・Aggressiveモードやmainモードで X.509を使用する場合、あるいは、mainモード（PSK認証）でinitiator動作のみの場合は、FQDN指定だけでも接続可能です。
・いずれの場合においても、ネゴシエーションパケットのsourceアドレスから、逆引き（あるいは正引き）によるFQDNのチェックは行いません。
（逆引きは別のドメイン名が設定されているケースが多く、設定数が多い場合は高負荷になるためです。）

□ FQDN指定の際のID

対向アドレスをFQDN指定する場合、名前解決後のIPアドレスをIDとして認証を行います。
※別途IDを指定している場合は、当該IDを使用します。

□ FQDN指定の制限事項

・Mainモード（PSK認証）で、対向をFQDN指定している場合、対向からのネゴシエーションを受信しても、PSKが見付からないため接続に失敗します（responderとしての動作）。
・Mainモードでは、PSKを検索する段階では、まだIDが分からないため、IPアドレスによる検索を行いますが、対向がFQDN指定の場合は、受信したIKEパケットのsourceアドレスとPSKを関連付ける情報がないため、PSKが見付からず接続に失敗します。
・このような場合に、mainモードで接続するには、対向をFQDNではなく、anyとして指定します。
※mainモードで対向をFQDN指定すると、initiator動作のみ対応することになります。
しかしながら、上記のような制限を抱えたまま、mainモードを使用するよりも、aggressiveモードやX.509認証の使用を推奨します。

ipsec isakmp policy mode

◆ local policy
＜説　　明＞　使用するローカルポリシーを選択します。
＜書　　式＞　local policy <1-255>

◆ local policy (change action)
＜説　　明＞
・IPsec isakmp で使用する local policy の track 状態(up/down)によって、action を実行する機能です。
・この機能により、障害に応じて、1 つの IPsec 設定にて main/backup の構成を取ることができます。
＜書　　式＞
local policy <policy:1-255> netevent <trackid:1-255> change <local_policy:1-255>
local policy <policy:1-255> netevent <trackid:2048-4095> change <local_policy:1-255>
＜備　　考＞
・PSK を使用している場合、変更前の local policy の ID と変更後の local policy の ID は、同じ ID を使用してください。たとえば、下記のような change action を設定する場合は、local policy 1 と local policy 2 の self-identity を同じ ID にしてください。

```
!
ipsec isakmp policy 1
 local policy 1 netevent 1 change 2
!
ipsec local policy 1
 self-identity fqdn myid  ←同じ ID
!
ipsec local policy 2
 self-identity fqdn myid  ←同じ ID
!
```

・action 追加時の動作: track object の状態が down の場合 action が実行されます。
・action 削除時の動作: netevent がない場合と同じ動作が実行されます。Action 復旧処理が行われるわけではありません。

◆ eap-identity
＜説　　明＞　EAP 認証で使用する ID を設定します。
＜書　　式＞　eap-identity (WORD|any)
＜　No　＞　no eap-identity
＜備　　考＞　設定例は、authentication local/remote を参照してください。

◆ netevent
＜説　　明＞　イベント発生時に、IKE 単位で IPsec トンネルの確立、削除を実行します。
＜書　　式＞　netevent <trackid:1-255> (connect|disconnect|reconnect)
netevent <trackid:2048-4095> (connect|disconnect|reconnect)
＜　No　＞　no netevent

ipsec isakmp policy mode

◆ initial-contact-ignore

<説　　明>　initial-contact-ignore が enable の場合、INITIAL_CONTACT を受信しても、
　　既存の SA 削除を実行しません。
<書　　式>　initial-contact-ignore enable
<　No　>　no initial-contact-ignore enable

■ Mode-config

リモート VPN client に対して、内部ネットワーク情報を設定する方法として、mode-config に対応しています。IKEv1/IKEv2 のいずれでも使用可能です。

◆ client configuration mode

<説　　明>
・mode-config によるネットワーク情報割り当て時のモードとして、initiate/respond を指定します。
<書　　式>　client configuration mode (initiate|respond)
<初 期 値>　client configuration mode respond
<　No　>　no client configuration mode
<備　　考>
・initiate を指定した場合、イニシエータとして動作します。
・respond を指定した場合、レスポンダーとして動作します（VPN client からのリクエスト待ち状態となります）。
・IKEv2 の場合、mode 設定に関係なく、常に respond として動作します。

◆ client configuration address-pool

<説　　明>　mode-config で使用する address-pool を指定します。
<書　　式>　client configuration address-pool local WORD
<　No　>　no client configuration address-pool
<備　　考>　address-pool は、ipsec local pool コマンド（global mode）にて設定します。
　　本設定があると、mode-config が有効になります。

第 24 章

ipsec tunnel policy mode

ipsec tunnel policy mode

◆ 移行command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#ipsec tunnel policy <policy:1-65535>
vxr-x86(config-ipsec-tunnel)#
```

◆ description

＜説　　明＞　IPsec tunnel policyの説明を記述します。
＜書　　式＞　description DESCRIPTION
＜　No　＞　no description DESCRIPTION

◆ set transform

＜説　　明＞　transformを設定します。
＜書　　式＞

```
set transform
      (esp-3des|esp-des|esp-aes128|esp-aes192|esp-aes256|esp-null)
      (esp-md5-hmac|esp-sha1-hmac|esp-sha256-hmac|esp-sha384-hmac|esp-sha512-hmac|)
      (esn|)
```

＜初　期　値＞　set transform esp-aes128 esp-sha1-hmac
＜備　　考＞　hashを指定しない場合は、ESPの認証機能は無効となります。
認証機能を無効にした場合は、replay防御window機能も無効になります。
esp-nullを指定した場合は、認証機能は無効にできません。
Defaultでは、ESN（Extended Sequence Number）は無効です。
ESNを有効にする場合は、暗号化方式（およびHash）も指定します。

◆ set pfs

＜説　　明＞　PFSを設定します。
＜書　　式＞　set pfs (|group1|group2|group5|phase1group14|group15|group16|group17
|group19|group20|group21|group25|group26)
＜初　期　値＞　set pfs phase1
・IKEv1の場合、phase1と同じDH groupを使用します。
・IKEv2の場合、PFS機能は無効となります(未指定扱い)。
＜　No　＞　no set pfs （= PFS無効)

◆ set esp-sha256-hmac trunc-length

＜説　　明＞　SHA256-HMACのtruncation lengthを指定します。
＜書　　式＞　set esp-sha256-hmac trunc-length (96|128)
＜　No　＞　no set esp-sha256-hmac trunc-length
＜初　期　値＞　set esp-sha256-hmac trunc-length 128
＜備　　考＞
・SHA256-HMACの認証サイズは、defaultで128bitですが、一部のdraft版対応製品は、96bitで動作するものがあります。
・Android6.xとIPsec接続する場合は、こちらを設定してください。

ipsec tunnel policy mode

◆ set anti-replay-check

＜説　　明＞　replay 防御 window 機能の有効 / 無効を設定します。
＜書　　式＞　set anti-replay-check
＜初 期 値＞　set anti-replay-check
＜　No　＞　no set anti-replay-check

◆ set key-exchange

＜説　　明＞ 使用する ISAKMP ポリシーを指定します。
＜書　　式＞ set key-exchange isakmp <1-65535>

◆ set protocol-mode

＜説　　明＞
・本装置では、tunnel モードと transport モードの両方のモードをサポートします。
・IPv6 利用時は、IPv6 LLA を使用した IPsec tunnel/tranport mode を確立することはできません。
・サポートするトンネリング形式は、IPv4 over IPv4、IPv4 over IPv6、IPv6 over IPv6、IPv6 over IPv4 です。
＜書　　式＞　set protocol-mode (tunnel|tranport)
＜初 期 値＞　set protocol-mode tunnel
＜備　　考＞
※ Transport モードと NAT-Traversal の併用
NAT 環境で Transport モードを利用する場合、接続環境やセキュリティの点で、いくつかプロトコル上の制限事項があります。
・接続時の制限
NAT 環境で Transport モードを利用する場合、プロトコル上の制限により、同一 NAT 装置配下からの接続が出来ない場合があります。
・TCP/UDP チェックサム
TCP/UDP の通信を行う際、クライアント側ではプライベート IP アドレスを利用してチェックサムを計算し、ESP 化を行った後に送信します。その後、NAT 装置によってソースアドレスが変換されます。本装置がこのパケットを受信した場合、複合化の後にチェックサムのチェックを行いません。本装置が受信したパケットのソースアドレス（グローバルアドレス）と、クライアントが送信したパケットのソースアドレス（プライベートアドレス）が異なるので、チェックサムエラーが発生します。そのため、Transport モード＋ NAT-Traversal の環境では、受信した ESP パケットのチェックサムはチェックしません。

ipsec tunnel policy mode

◆ set key-exchange (change action)

＜説　　明＞

・IPsec tunnel で使用する isakmp policy の track 状態(up/down)によって、action を実行します。

・この機能により、障害に応じて、1つの IPsec 設定にて main/backup の構成を取ることができます。

＜書　　式＞

```
set key-exchange isakmp <1-65535> netevent <trackid:1-255> change isakmp <1-65535>
set key-exchange isakmp <1-65535> netevent <trackid:2048-4095> change isakmp <1-65535>
```

＜備　　考＞

・action 追加時の動作: track object の状態が down の場合 action が実行されます。

・action 削除時の動作: netevent がない場合と同じ動作が実行されます。Action 復旧処理が行われるわけではありません。

◆ set sa lifetime

＜説　　明＞

IPsec SA のライフタイム(Hard Timer)を設定します。この時間を経過すると SA が削除されます。

＜書　　式＞　set sa lifetime <121-86400>

＜初 期 値＞　set sa lifetime 3600

＜　No　＞　no set sa lifetime　(= set as lifetime 3600)

◆ negotiation-mode

＜説　　明＞　IPsec policyのネゴシエーションモードを指定します。

＜書　　式＞　negotiation-mode (auto|on-demand|manual|responder)

auto	IPsec service 起動時に negotiation が開始されます。IKEv2 の場合、認証エラーや TS(トラフィックセレクタ)の不一致などのエラーが発生した場合、60sec 後に再度 initiate が開始されます。
manual	IPsec service 起動時に negotiation は開始されず tunnel が追加されるのみです。Backup policy などで使用します。
on-demand	IPsec service 起動時に route のみが設定されます。
responder	IPsec service 起動時の動作は、manual と同様です。但し、常に responder となるため、こちらからいかなる場合(rekey 含む)においても initiate することはありません。

＜初 期 値＞　negotiation-mode auto

ipsec tunnel policy mode

◆ clone

＜説　　明＞

・ある IPsec tunnel policy と同じ policy をもつ ipsec tunnel policy を設定します。

・本機能は、main/backup で同じような設定（IPsec の冗長化を行う際、通常 main/backup では同じ policy を持ちます）を行う手間を省きたい場合に使用します。

・route based IPsec では、1 つの tunnel interface を main/backup で使用することができます。本機能を使用すると、main/backup それぞれの tunnel に対して、同じ static や nat/filter の設定をする必要がなくなり、管理者の負担を軽減することができます。

＜書　　式＞　clone <1-65535>

＜　No　＞　no clone

＜備　　考＞　以下は、本機能により copy されない項目(個別に設定が必要な項目)です。

・tunnel number

・priority

・description

・negotiation-mode

・shutdown

・key-exchange

◆ shutdown

＜説　　明＞　IPsec トンネルポリシーを無効にします。

＜書　　式＞　shutdown

＜　No　＞　no shutdown

◆ set route

＜説　　明＞　Destination Prefixをルーティングテーブルに追加します。

＜書　　式＞　set route

＜　No　＞　no set route　　(= Disable)

◆ set priority

＜説　　明＞　ポリシーのプライオリティを設定します。

＜書　　式＞　set priority <1-255>

＜初 期 値＞　set priority 1

＜　No　＞　no set priority　(初期値)

ipsec tunnel policy mode

■ match

○ address

＜説　　明＞　IPsec tunnel に適用する IPsec ACL を指定します。

＜書　　式＞　match address IPSEC-ACL-NAME (|nat-traversal)

＜備　　考＞　IPsec ACL は、global mode の ipsec access-list コマンドで設定します。

○ protocol

＜説　　明＞　smartphone と L2TPoverIPsec で接続する際に設定します。
　　match address とは、排他設定です。

＜書　　式＞　match protocol l2tp-smartphone (|nat-traversal)

＜備　　考＞

◎L2TP over IPsec (l2tp smartphone mode)

smartphone との間で L2TPv2 over IPsec を確立する際に使用します。本機能を有効にすると、下記の設定が有効になります。

□ IPsec パラメータの自動設定

IPsec 接続を行う際に、下記のパラメータを自動設定します。

・protocol-mode → transport

・negotiation-mode → responder

・IPsec selector → 以下のように自動設定します。また、NAT-Traversal 有効時は、NAT 配下のどのアドレスからの接続も受け付けます。

ID Payload	VXR側	smartphone側
IPv4アドレス	host	host
プロトコル	UDP	UDP
ポート番号	1701	any(どのポートでも受け付ける)

第 25 章

UPnP mode

UPnP mode

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#upnp
vxr-x86(upnp-config)#
```

■ UPnP

○ service

＜説　　明＞　サービスを起動します。
＜書　　式＞　service enable

○ external interface

＜説　　明＞　WAM側インタフェースを設定します。
＜書　　式＞　external interface ethernet <0-2> (|vid <1-4094>)
　　external interface ppp <0-4>
　　external interface bridge <0-4095>

○ external port-reserve

＜説　　明＞　あるWAN ポートについて、ポートマッピングを許可したくない場合は、予約ポート設定を行います（UPnPの割り当てを禁止するポート番号を設定します）。
　　予約ポート番号は、TCP/UDP 共通で単一ポートまたは範囲を指定します。最大64 組まで設定することができます。
＜書　　式＞　external port-reserve <1-65535> (|<1-65535>)
＜　No　＞　no external port-reserve <1-65535> (|<1-65535>)

○ external well-known

＜説　　明＞　well-known port(1-1023)へのUPnPの割り当てを許可します。
＜書　　式＞　external well-known port enable
＜　No　＞　no external well-known port enable

○ listen

＜説　　明＞　LAN配下の機器からのUPnPメッセージをlistenするIPアドレスを設定します。
＜書　　式＞　listen ip A.B.C.D/M
＜　No　＞　no listen ip A.B.C.D/M
＜備　　考＞　最大2つまで設定可能

○ timeout

＜説　　明＞　UPnP機能使用時の無通信切断タイマーを設定します。
＜書　　式＞　timeout <sec:60-21474836>
＜初 期 値＞　no timeout　(= timout 600)

第 26 章

QoS (class-policy) mode

QoS (class-policy) mode

■ QoS

本装置のソフトウェアにてサポートする各 queuing 方式について記します。packet coloring 以外は、すべて egress interface のみで使用することが出来ます。

1. PFIFO(Packet FIFO)

・PFIFO では、輻輳状態になった場合に、すぐにパケットを破棄せず、キューに貯めておきます（キューの最大容量を超えたパケットは破棄します)。パケットが転送可能な状態になると、キューに貯めておいたパケットを（First_In First_Out の）順番に転送します。PFIFO は、優先順位の高いパケットと優先順位の低いパケットを区別しません。

・インタフェースの default queuing 方式は、PFIFO_FAST と呼ばれるもので、IP ヘッダの ToS フィールドの値に応じて受信パケットを 3 つの queue に振り分けて、優先度の高い queue から優先してパケットを出力します。PFIFO_FAST の設定内容をユーザが変更することは出来ません。

2. TBF(Token Bucket Filtering)

Token Bucket Filtering と呼ばれるアルゴリズムで、shaping 機能を提供します。指定したレートで bucket から token を出力し、その token にパケットを格納します。Token がない場合は、パケットを出力しません。

Classless queuing 方式のため、特定のトラフィック class のみに適用させることはできません。特定のトラフィック class に対して shaping を適用する場合は、HTB や PQ のような class full queuing と併用して使用することができます。ただし、HTB には shaping 機能があるため、各 class で TBF を適用すると CPU 使用率の増加や遅延の増大を招く恐れがあります。したがって、HTB との併用は望ましくありません。

キャリアサービスにおいて、契約した回線帯域により料金が異なるようなサービスを使用した場合、ルータで shaping する際に、パケットサイズや FCS や IFG、PA を除いたフレームサイズでレート計算を行ないます。この場合、shaping rate としては問題ないようでも、Ethernet フレームとして実際に回線を流れる際は、FCS や IFG+PA が追加されるため、回線側でフレーム drop が発生することがあります。このような場合の対応として、Ethernet インタフェース上での設定に限り、shaping レートの計算時に、ifg(inter-frame-gap の最小サイズ 12byte で計算)、fcs(4byte)、pa(preamble:8byte)をフレームサイズ に加えることができます。これにより、回線サービス上での帯域超過によるフレーム drop を回避することが可能となります。Default では、IFG、PA、FCS 分のサイズは考慮しません（設定は、interface mode の ifg-pa-fcs を参照してください)。

3. SFQ (Stochastic Fair Queuing)

各パケットをすべて公平に扱う queuing 方式です。Flow 毎に計算されたハッシュ値によって各 bucket にパケットを振り分けます。SFQ には 127 パケットの queue があり、送信(active)となった bucket に対して queue を割り当てます。

Flow は、IP source/destination address、protocol 番号によって区別します(IPv4 の場合)。また、SFQ queue の深さは 127 で、ハッシュテーブルのサイズは 1024 です（ユーザが設定を変更することは出来ません)。

帯域の小さい回線で使用することで、帯域を平等に使用することが出来ます(ある特定の flow のみが帯域を占有することはありません)。しかし、interactive なセッションがある場合は、遅延が大きくなってしまうことがあります。

QoS (class-policy) mode

4. PQ (Priority Queuing)
High/medium/normal/low の 4 つの class の queue を持ちます。
High priority の queue にパケットがある場合は、medium/normal/low の queue からパケットが出力されることはありません。
Class 数は 4 つ(固定)で、class に割り当てる traffic はユーザが指定することが出来ます。各 class の default queuing 方式は、PFIFO です。

5. HTB
Class 分けされたトラフィクに予約帯域を割り当て、クラス毎に設定した重みとパケット長に応じてパケットを出力します。
回線帯域に空きがある場合は、予約帯域以上のトラフィックを送信することが可能で、回線を有効に利用することが出来ます。
各 class の default queuing は、PFIFO です。但し、default class の default queuing は、SFQ です。

5.1 ceil 帯域の割り当て
HTB では、ceil パラメータにより、他の class が帯域を使用していない場合、その帯域を借りることで設定した rate より高い rate で通信することが出来ます。
その際、複数の class のトラフィックが未使用帯域(余剰帯域)を使用する場合の分配方法について記します。

余剰帯域の比率は、class priority が同じ場合は、quantum というパラメータにより決定します。priority が異なる場合は、高優先の class に対して優先的に帯域を割り当てます。quantum 値は、class に割り当てられた rate 設定値から自動的に算出します（ユーザが、設定することは出来ません)。

```
quantum = (rate * 1000/8)/r2q
```

※ r2q は、rate を quantum 値に変換するための係数です。default は、10 です。
Quantum 値の範囲は、1500 ～ 60000 です。そのため、r2q が 10 の場合、rate が 120kbps ～ 4.8Mbps の範囲なら、指定 rate の比率に応じて余剰帯域を割り当てます。一方、rate が 120kbps 以下なら 120kbps と同じ比率、4.8Mbps 以上なら 4.8Mbps と同じ比率で、余剰帯域を割り当てます。
本装置では、class の最高 rate によって r2q の値を変化させます。そのため、設定した class rate によっては、従来の余剰帯域の割り当て比率とは異なる場合があります。
例えば、class の最高 rate を 40Mbps に設定した場合、40Mbps が quantum の最大値(60000)となるように r2q を自動調整します。この場合、余剰比率が rate 比と同じになる minimum rate は

```
r2q = (40000*1000/8)/60000
min rate = 1500 * 8 /1000 * r2q = 1500 * 40000/60000 = 1000 kbps = 1.0 Mbps
```

となります。

5.2 バーストサイズについて
HTB を設定した場合、指定した帯域幅に基づいてバーストサイズを自動的に算出します。また、ceil も指定した場合は、ceil 値に応じて ceil のバーストサイズを別途算出します。

```
burst = bandwidth/HZ +1600
cburst = ceil/HZ + 1600
```

※ NXR-G100 の場合、HZ は 250 です（機器により異なります)。
※ bandwidth/ceil は、設定レートをビットレート(bit rate)からバイトレート(byte rate)に変換した値です。

QoS (class-policy) mode

5.3 class priority機能
HTBで使用する各classにpriorityを設定することが出来ます。priorityの小さいclassをラウンドロビンで優先的に処理します。そのため、VoIPパケットなどの遅延を小さくするには、他のclassより小さいpriorityを設定するようにします。
priorityは、1～7の範囲で指定することが出来ます。指定がない場合は、本装置が4を割り当てます。なお、priorityはleaf classのみで有効です。親class(parent class)で指定したpriorityは無視します。

6. Packet Coloring
ユーザが指定した特定のトラフィックにMARK値(VXR内のみ有効な値)やToS値の設定を行います。ToSとMARKを同時に設定することも出来ます。Packet coloringされた情報により、QoSを適用することができます。
トラフィックの識別、およびMARKやToS値の設定には、route-map設定を利用します。また、Packet coloringの適用箇所やNAT、packet filteringとの適用順番については、付録のPacket Travelingを参照してください。

7. 各classへのトラフィック割り当てについて
PQやHTBのようなclassfullなqueuing方式を使用する際、各classへトラフィックを割り当てる方法として、MARK値とToS値/Precedence値(HTBのみ)による割り当てをサポートします。
MARK値は、VXR内部でのみ使用される値でPacket coloring機能によって設定することができます。
PQの各classへの割り当てはMARKのみで、1つのclassへ割り当て可能な条件は1つだけです。
HTBの各classへの割り当ては、class filterを使用します。Class filter内においては、match条件を複数設定することが出来ます。
複数条件がある場合、その条件に1つでも合致すれば、該当classへトラフィックが割り当てられれます(route-mapの条件とは異なるので注意してください)。

QoS (class-policy) mode

◆ 移行command

```
vxr-x86#
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#class policy NAME
vxr-x86(class-policy-config)#
```

■ class

＜説　　明＞　classを設定します。

＜書　　式＞

○class+child class

```
     class <2-254> bandwidth <1-1000000> (|ceil <1-1000000>) queue policy NAME
     class <2-254> bandwidth percent <1-100> (|ceil <1-100>) queue policy NAME
```

○class+PQ

```
     class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
           queue priority-group <1-255>
     class <2-254> bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>)
           queue priority-group <1-255>
```

○class+fifo

```
     class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
           queue fifo (|limit <1-16384>)
     class <2-254> bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>)
           queue fifo (|limit <1-16384>)
```

○class+sfq

```
     class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>) queue fair-queue
     class <2-254> bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>) queue fair-queue
```

○class+tbf

```
     class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
           queue shape <RATE:1-1000000> <BUFFER:8-1000000> <LIMIT:1-1000000>
     class <2-254> bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>)
           queue shape <RATE:1-1000000> <BUFFER:8-1000000> <LIMIT:1-1000000>
```

○class+default queue (default queue : fifo)

```
     class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
     class <2-254> bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>)
```

○class削除

```
     no class <2-254>
     no class default
```

QoS (class-policy) mode

○class default (policyは選択不可)

```
class default bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
      queue (priority-group|shape|fifo|fair-queue)
class default bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>)
      queue (priority-group|shape|fifo|fair-queue)
```

○default queue (default queue: sfq)

```
class default bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
class default bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>)
```

＜備　　考＞

- bandwidth <1-1000000>を指定した場合、bandwidthおよびceilのレートの単位はkbpsです。
- HTB設定において、bandwidth percent <1-100>を指定した場合、bandwidthおよびceilのレートの単位は%です。パーセンテージは、インタフェースで設定した帯域幅に対する絶対比です。また、この場合は、ceil値もパーセンテージで指定します。
- 下記の例の場合、class 10の帯域幅は、10000kbps × 10% ＝ 1000kbpsになります。

```
!
class policy AAA
 class 10 bandwidth percent 10
!
interface ethernet 1
 queue policy AAA bandwidth 10000
!
```

※小数点以下の端数は、切り捨てます。ただし、1kbpsに満たない場合は、1kbpsとして処理します。

第 27 章

QoS (class-filter) mode

QoS (class-filter) mode

◆ 移行 command

```
vxr-x86#
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#class filter <2-254>
vxr-x86(class-filter-config)#
```

■ match

＜説　　明＞　Mark 値、ToS 値、Precedence を設定します。
＜備　　考＞　複数の match が設定されている場合、or 条件となります。

○ mark

＜書　　式＞　match ip mark <1-4095>
＜　No　＞　no match ip mark <1-4095>

○ tos

＜書　　式＞　match ip tos <0-255>
＜　No　＞　no match ip tos <0-255>

○ precedence

＜書　　式＞　match ip precedence <0-7>
＜　No　＞　no match ip precedence <0-7>

第 28 章

CRP client mode

CRP client mode

管理サーバインタフェース

本装置の設定や状態を管理する管理サーバ（CMS）とのインタフェースについて記します。

■ CMS と VXR 間のインタフェースプロトコル

・CMS との情報のやりとりに netconf(RFC4741)を使用し、netconf の転送用プロトコルとしては、SSH（netconf over SSH:RFC4742）を使用します。
・SSH および netconf は、CMS からセッションを開始します。つまり、VXR がサーバ、CMS がクライアントとして動作します。

■ CMS と VXR 間の SSH 認証

・CMS->VXR 間の SSH 認証は RSA 認証のみであり、ユーザ名は netconf 固定です。CMS の RSA 公開鍵を、VXR へインポートすることで、SSH 認証が可能となります。RSA 公開鍵は、最大 5 つまでインポートすることが出来ます。設定については、SSH 公開鍵のインポート（view mode）を参照してください。
・config 保存時に、インポートした RSA 公開鍵も本装置の flash に保存されます。
・CMS から VXR への SSH 接続は、インタラクティブではないため、公開鍵のパスフレーズは未入力のものを使用してください。

CRP

CRP とは、本装置から管理サーバ（CMS)へ、管理に必要な情報（グローバル IP アドレス等）を登録する際に使用するプロトコルです。CRP は、UDP 上で動作します。また、デフォルトでは 10625 番ポートを使用します。

■ クライアントモード

・CRP が本装置で動作する場合は、クライアントモードで動作します。

■ サーバモード

・クライアントからの情報を待ち受けるモードです。自発的にクライアント側にパケットを送信するようなことは行いません。CRP が管理サーバ（CMS サーバ)上で動作する場合は、サーバモードで動作します。

CRP client mode

◆ 移行command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#crp client <1-2>
```

○server address
＜説　　明＞　CRPサーバ（CMSサーバ）のIPアドレスを設定します。
＜書　　式＞　server address (A.B.C.D|X:X::X:X|FQDN)
＜　No　＞　no server address

○server port
＜説　　明＞　CRPサーバ（CMSサーバ）の待ち受けポート番号を設定します。
＜書　　式＞　server port <udp:1024-65535>
＜初 期 値＞　server port 10625
＜　No　＞　no server port

○username
＜説　　明＞　CRPクライアントのユーザIDとパスワードを設定します。
＜書　　式＞　username WORD password (hidden|) WORD
＜　No　＞　no username

○keepalive
＜説　　明＞　CRPキープアライブの設定を行います。
＜書　　式＞　keepalive (|<300-28800sec>)
＜初 期 値＞　no keepalive
＜　No　＞　no keepalive
＜備　　考＞
・CRPの登録に成功してから、次に再登録を試行するまでの時間を設定します。インターバル未指定時（keepalive）は、「keepalive 3600」と同義です。
・無効（no keepalive）の場合は、CRPの再登録を行いません。ただし、IPアドレスの変化や指定インタフェースのup/down、CPE IDおよびCUSTOMER IDの変更があった場合は、キープアライブが無効でも自動的にCRPの再登録を行います。
・本装置をNAT装置の配下で運用する場合は、必ずキープアライブを有効にしてください。
・本装置がグローバルIPを持つ場合（本装置がNAT装置の配下にない場合）は、キープアライブが無効でも動作しますが、管理サーバの運用上の万一のトラブルを考慮して、keepalive 3600を設定することを推奨します。

第 29 章

route-map mode

route-map mode

Route-map

特定の packet や route などの条件に合うかどうかをチェックし、それに応じた action を実行することができる機能です。

- Packet の coloring や route の属性を変更することができます。Packet coloring で特定の traffic に mark 値(VXR 内のみ有効な値)や ToS 値の設定を行う(tos と mark を同時に設定することも可能)ことによって、QoS を適用することができます。
- Route-map はシーケンス番号をもち、複数の route-map を適用させることができます。
- 同じ名前の route-map が複数存在する場合は、シーケンス番号が小さいものから処理され、最初に match したエントリの action を実行します。
- 1 つの route-map 内に複数の match 条件がある場合は、すべての match 条件に合うと、当該アクションを実行します。一方、一つの match 条件に、複数の条件定義がある場合は、どれか 1 つの条件に match した場合にアクションを実行します。なお、本バージョンでは、1 つの match 条件に複数の条件定義を行うことはできません。

◆ 移行 command

```
vxr-x86#
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#route-map NAME (permit|deny) <1-65535>
vxr-x86(config-route-map)#
```

< 次ページに続く >

route-map mode

■ match

＜説　　明＞　マッチ条件を設定します。
＜備　　考＞　match がない場合は、すべてが set の対象になります。
　　deny で match した場合は、set の対象外になります。
　　各機能でサポートしていない match 条件は無視します。

○ Classify で利用(設定)可能な match 条件
＜説　　明＞　Classify で利用(設定)可能な match 条件は次のとおりです。
　　IP address(class access-list)、tos 値、mark 値(IPv4)、ip precedence
＜書　　式＞　match ip tos <0-255>
　　match ip mark <1-4095>
　　match ip precedence <0-7>
　　match ip address ACL
＜備　　考＞
・同じ route-map シーケンス内で、match 条件として、address と tos/mark/precedence は、AND 設定することが出来ます。
・tos、mark、precedence は、同時に指定することは出来ません（いずれか一つのみ設定可能です）。

○ BGP4 で利用(設定)可能な match 条件
＜説　　明＞　BGP4 で利用(設定)可能な match 条件は、次のとおりです。
　　ip address(ip route access-list のみ)、nexthop address、med、as-path、origin
＜書　　式＞　match ip address ACL-NAME
　　match ipv6 address ACL-NAME
　　match ip next-hop ACL-NAME
　　match ipv6 next-hop X:X::X:X
　　match metric <0-4294967295>
　　match as-path ACL-NAME
　　match origin (egp|igp|incomplete)

○ PBR で利用(設定)可能な match 条件
＜説　　明＞　PBR で利用(設定)可能な match 条件は、次のとおりです。
　　IP address(ip policy access-list)
＜書　　式＞　match ip address ACL

○ RIP/OSPF で利用(設定)可能な match 条件
＜説　　明＞ RIP/OSPF で利用(設定)可能な match 条件は、次のとおりです。
＜書　　式＞ match tag (0-4294967295)

route-map mode

○マッチ条件の削除

＜説　　明＞　設定したマッチ条件を削除します。

＜　No　＞　no match ip [address|tos|mark|precedence|netx-hop (|WORD)]
no match ipv6 address
no match ipv6 next-hop (|X:X::X:X)
no match as-path (|WORD)
no match metric (|<0-4294967295>)
no match origin (|egp|igp|incomplete)
no match tag (|<0-4294967295>)

route-map mode

■ set

＜説　　明＞　QoS（Classify）、BGP4、PBR で使用する属性を設定します。
　　ToS と Mark を同時に設定することが出来ます。
　　各機能でサポートしていない属性の設定は無視します。

○Classify で利用(設定)可能な属性
＜説　　明＞　Classify で利用(設定)可能な属性は、次のとおりです。
　　tos 値、mark 値(IPv4 のみ)
＜書　　式＞　set tos <0-255>
　　set mark <1-4095>

○BGP4 で利用(設定)可能な属性
＜説　　明＞
・BGP4 にて routemap を使用する場合、以下の属性を設定することができます。
aggregator Century、as-path、atomic-aggregate、nexthop、local-preference、med、origin
＜書　　式＞　set aggregator as <1-65535>
　　set as-path prepend <1-65535>
　　set atomic-aggregate
　　set ip next-hop A.B.C.D
　　set ipv6 next-hop (|local) X:X::X:X
　　set local-preference <0-4294967295>
　　set metric <0-4294967295>
　　set origin (egp|igp|incomplete)

○PBR で利用(設定)可能な属性
＜説　　明＞
・PBR にて routemap を使用する場合、ルーティングエントリー作成時に以下の属性を使用します。
ip next-hop、interface
＜書　　式＞　set ip next-hop A.B.C.D
　　set interface INTERFACE
＜備　　考＞
・入力および出力インタフェースとして指定可能なインタフェースは、イーサネット /802.1Q VLAN/ ブリッジ（仮想スイッチ）/ トンネル /PPP です。

○ RIP/OSPF で利用(設定)可能な属性
＜説　　明＞ RIP/OSPF にて、routemap を使用する場合、以下の属性を設定することができます。
＜書　　式＞ set tag (0-4294967295)

route-map mode

■ set(続き)

○セット条件の削除

＜説　　明＞　設定したセット条件を削除します。

＜　No　＞　no set aggregator as (|<1-65535>)
no set as-path prepend (|<1-65535>)
no set atomic-aggregate
no set interface
no set ip netx-hop (|A.B.C.D)
no set ipv6 next-hop (|local) (|X:X::X:X)
no set local preference (|<0-4294967295>)
no set mark <1-4095>
no set metric (|<0-4294967295>)
no set origin (|egp|igp|incomplete)
no set tos <0-252>
no set tag (|<0-4294967295>)

■ class access-list および ip route access-list

class access-list と ip route access-list は、いずれも route-map の match 条件である match ip address 設定をフィルタリングする際に使用します。また、ip route access-list は BGP の distribute-list によるルートフィルタリングにも使用します。

class access-list と ip route access-list は、以下のように使い分けます。なお、設定については global mode の class access-list および ip route access-list を参照してください。

○ class access-list
　ToS 値や MARK 値を設定する set 条件をフィルタリングする場合

○ ip route access-list
　BGP のパス属性に関する set 条件をフィルタリングする場合
　BGP で distribute-list によるルートフィルタリングを行う場合

■ netevent

＜説　　明＞　Netevent で、PBR route の有効化 / 無効化を行うことが出来ます。
＜書　　式＞　netevent (<1-255>|<2048-4095>) (active|inactive)
＜備　　考＞　active　　track down を検出すると、ip route が有効になります。
　　track up を検出すると、ip route が無効になります。
　　inactive　track down を検出すると、ip route が無効になります。
　　track up を検出すると、ip route が有効になります。

第 30 章

Web Authenticate mode

第30章 Web Authentication mode

Web Authentication mode

Web認証機能

Web認証はpacket filterの一種で、認証を通ったUSERのIPv4 addressをsource/destinationに持つ転送のみを通過させる機能です。Web認証によるpacketの判定は、USERが設定したforward(in/out) filter通過後に評価されます。Web認証によって外部との通信が許可されるclient数は、256です。

○ 移行command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#web-authenticate
vxr-x86(config-webauth)#
```

■ 認証方式

対応している認証方式は、HTTP Basic認証です。

○ authenticate basic

＜説　　明＞　Web認証（Basic認証）を行うかどうかを設定します。
＜書　　式＞　authenticate basic (|redirect)
＜　No　＞　no authenticate
＜初 期 値＞　no authenticate
＜備　　考＞

- redirectを指定した場合、Web認証後にURL転送を行うことができます。転送先のURLは、redirect-urlコマンドで指定してください。
- Web認証を有効にする場合は、HTTPサーバを起動してください。(global modeで、http-server enableを設定します。)

■ 認証URL

Basic認証のURLは「http:// 本装置のIP address/login.cgi」です。たとえば、LAN側IPアドレスが192.168.0.254の場合、http://192.168.0.254/login.cgiにアクセスすると、Web認証ダイアログが表示されます。

■ 強制認証

通常、外部に接続したいUSERは、認証URLへのアクセスが必要となります。強制認証機能では、tcp80番への接続を監視し、未認証のUSERからこの接続があった場合に、強制的にWeb認証を行います。Defaultでは本機能は無効です。

○ monitor

＜書　　式＞　monitor port 80 (|redirect)
＜　No　＞　no monitor port
＜初 期 値＞　no monitor port
＜備　　考＞

authenticate basic + monitor port 80
　未認証のPCから外部Webにアクセスすると、Web認証ダイアログが表示されます。
authenticate basic + monitor port 80 redirect
　未認証のPCから外部Webにアクセスすると、Web認証後にredirect-urlに転送されます。
no authenticate + monitor port 80 redirect
　未認証のPCから外部Webにアクセスすると、Web認証なしでredirect-urlへ転送されます。

Web Authentication mode

■ URL 転送

Web 認証後、任意の URL へ転送させることができます。Web 認証は行わず、外部へのアクセスがあった時に、指定した URL へリダイレクトさせるように動作させることも可能です。

○ redirect-url

＜説　　明＞　転送先の URL を指定します。
＜書　　式＞　redirect-url RedirectURL (cf. http://www.centurysys.co.jp)
＜　No　＞　no redirect-url

■ 接続許可時間

Web 認証後に USER が通信可能な時間を、以下の 3 つから選択することができます。

○ close idle-timeout

＜説　　明＞　許可された USER からの無通信状態が一定時間経過すると接続が遮断されます。
　　Timeout は 60-2592000 秒の間で任意の値を設定することができます。
　　Default は 1800 秒です。
＜書　　式＞　close idle-timeout <60-2592000>
＜　No　＞　no close
＜初 期 値＞　close idle-timeout 1800

○ close session-timeout

＜説　　明＞　認証で許可された通信を強制的に切断するまでの時間を設定します。
　　認証してからこの時間が経過すると、通信状態にかかわらず通信を切断します。
　　Timeout は 60-2592000 秒の間で任意の値を設定することができます。
　　Default は 1800 秒です。
＜書　　式＞　close session-timeout <60-2592000>
＜　No　＞　no close
＜初 期 値＞　close idle-timeout 1800

○ close browser-close

＜説　　明＞　認証を受けた Web ブラウザのウィンドウを閉じるまで接続が有効です。Web 認証時の HTML により、ブラウザから 60 秒毎に refresh が行われます。
　　refresh がなくなると接続を遮断します。
＜書　　式＞　close browser-close
＜　No　＞　no close
＜初 期 値＞　close idle-timeout 1800

Web Authentication mode

■ アカウント管理

Basic認証における username、password を本装置上で管理 / 認証する方法(ローカル認証)と、外部の RADIUS server に対して本装置から認証する方法(RADIUS 認証)があります。また、RADIUS 認証に失敗した場合にローカル認証を行うこともできます。

<書　　式>　account authenticate (local|radius|radius-and-local)
<　No　>　no account authenticate
<初 期 値>　account authenticate local

■ ローカル認証

ローカル認証用の username、password を最大 64 組まで設定することができます。

<書　　式>　account username USERNAME password (|hidden) PASSWORD
<　No　>　no account username USERNAME

■ RADUIS 認証

RADIUS 認証は PAP 認証によって行われます。RADIUS server への認証要求は、timeout が 5 秒で、最大 3 回までリトライします。

○ RADUIS サーバ設定

Account 認証を行う RADIUS server の IP address、UDP port 番号、秘密鍵(secret)を設定することができます。UDP port 番号の default は 1645 番です。また、RADIUS server は 2 つまで設定することができます。

<書　　式>
　radius A.B.C.D password (|hidden) PASSWORD (|auth-port <1645|1812|<1024-65535>)
　radius A.B.C.D auth-port (1645|1812|<1024-65535>)
<　No　>　no radius A.B.C.D　(設定を削除します)
　no radius A.B.C.D auth-port (auth-port のみを初期値に戻します)
<初 期 値>　radius A.B.C.D auth-port 1645

○ Attribute 設定

RADIUS server に通知する Attribute のうち、以下の Attribute について任意の値を設定することができます。

<書　　式>　radius attribute nas-ip-address A.B.C.D
　NAS-IP-Address: 通常は本装置の IP アドレスを設定します。
　radius attribute nas-identifier WORD
　NAS-Identifier: 任意の文字列を設定します。半角英数字が使用できます。
<　No　>　no radius attribute (nas-ip-address|nas-identifier)
<備　　考>　RADIUS 認証を使用する場合は、どちらかの Attribute を設定する必要があります。

Web Authentication mode

○ Idle timeoutで使用するAttributeの指定
接続許可時間にidle timeoutを指定している場合は、RADIUS serverからの応答Attributeの値をtimeoutとして使うことができます。
<書　　式>　radius idle-timeout attribute
　　(ascend-idle-limit|ascend-idle-limit-vsa|idle-limit)
　ascend-idle-limit　　Ascend-Idle-Limit(Attribute Type=244)
　ascend-idle-limit-vsa　Ascend-Idle-Limit(Attribute Type=244、VSA Type=26、Vendor-ID=529)
　idle-limit　　Idle-Timeout (Attribute Type=28)
<　No　>　no radius idle-timeout attribute

○ Session timeoutで使用するAttributeの指定
接続許可時間にsession timeoutを指定している場合は、RADIUS serverからの応答Attributeの値をtimeoutとして使うことができます。以下のAttributeから選択してください。
<書　　式>　radius session-timeout attribute
　　(ascend-maximum-time|ascend-maximum-time-vsa|session-timeout)
　session-timeout　　Session-Timeout (Attribute Type=27)
　ascend-maximum-time　Ascend-Maximum-Time(Attribute Type=194)
　ascend-maximum-time-vsa
　　Ascend-Maximum-Time(Attribute Type=194、VSA Type=26、Vendor-ID=529)
<　No　>　no radius session-timeout attribute

○ 全てのradius設定を一括削除
全てのradius設定を一括削除することができます。
<書　　式>　no radius

■ MACアクセスリスト

Web認証機能を有効にすると、外部との通信には認証が必要となりますが、mac access-listで指定したMACアドレスを持つPCについては、認証を必要とせずに通信を許可または拒否することができます。
<書　　式>　mac access-list (permit|deny) HH:HH:HH:HH:HH:HH (|IFNAME)
<　No　>　no mac access-list (permit|deny) HH:HH:HH:HH:HH:HH

■ Web認証フィルタ

Web認証フィルタを設定すると、ある特定のhostやnetwork、interfaceについてWeb認証せずに通信が可能となります。Web認証フィルタの設定条件については、global modeのip web-auth access-listを参照してください。Web認証フィルタは、各interfaceにつき、IN/OUTをそれぞれ一つずつ設定することができます。interfaceへの適用については、interface/tunnel/ppp modeのip webauth-filterを参照してください。

Web Authentication mode

■ 認証ログの出力

認証ログ（login successログ）をsyslogに出力します。

<書　　式>　log enable
<　No　>　no log enable
<初 期 値>　no log enable
<書　　式>

・有効（log enable）時、TCP80監視による認証ログ（login successログ）をsyslogに出力します。
・有効（log enable）時、login.cgi接続による認証ログ（login successログ）をsyslogに出力します。

第 31 章

WarpLink mode

WarpLink mode

WarpLink クライアント機能

WarpLink サービスのクライアントとして機能します。つまり、WarpLink Manager に対して、VXR の機器情報を送信します。

○ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#warplink
vxr-x86(config-warplink)#
```

■ クライアント設定

○　アカウント情報（ユーザ ID、パスワード）の指定

WarpLink Manager に登録してあるユーザ ID、パスワードを指定します。未設定の場合、機器情報は送信されません。

```
<書　　式>　account username USERNAME password (|hidden) PASSWORD
<　No　>　no account username (|USERNAME)
```

○　ダイナミック DNS の有効 / 無効を設定

有効にすると、VXR の WAN 側 IP アドレスを定期的に送信します。デフォルトは無効です。定期送信は 5 分間隔です。

```
<書　　式>　service enable
<　No　>　no service
```

○　統計情報インタフェースの設定

VXR の CPU 使用率、メモリ使用率、トラフィック量を定期的に送信します。ダイナミック DNS が無効の場合は、送信されません。デフォルトは無効です。定期送信は 5 分間隔です。統計情報は、30 秒間隔で取得したデータの 3 分間の平均を 3 日分保持します。

トラフィック量は 2 つまでインターフェース（Ethernet、VLAN、PPP、Tunnel、Bridge（仮想スイッチ）、WLAN）を指定することが出来ます。最大 2 つまで設定可能です。未設定の場合は、統計情報は送信されません。

```
<書　　式>　send-statistics interface INTERFACE
<　No　>　no send-statistics interface (|INTERFACE)
```

○　syslog 情報送信の有効 / 無効を設定

VXR の syslog 情報を定期的に送信します。ダイナミック DNS が無効の場合は、送信されません。デフォルトは無効です。定期送信は 5 分間隔です。syslog 情報は、前回からの差分を最大 100Kbyte まで送信します。

```
<書　　式>　send-syslog enable
<　No　>　no send-syslog
```

WarpLink mode

■ コマンド操作

○ WarpLink クライアントの再起動

WarpLink クライアントを再起動することができます。

＜書　　式＞　restart warplink

＜備　　考＞　view mode で実行します。

○ config 情報の送信

VXR の config 情報をユーザ指定時に送信します。ダイナミック DNS の有効 / 無効とは関係なく送信することができます。

＜書　　式＞　restart warplink send-config

＜備　　考＞　view mode で実行します。

○ WarpLink Manager との通信状態を表示

WarpLink Manager との通信状態を表示します。

＜書　　式＞　show warplink

＜備　　考＞　view mode で実行します。

表示されるステータスおよび意味は下表のとおりです。

項目	ステータス	意味
service	Successed	WarpLink Managerとの通信に成功
	Failed login	アカウントの認証に失敗
	Starting	クライアント起動時に、WarpLink Managerにアクセスできない
	Stopping	クライアント停止時に、WarpLink Managerにアクセスできない
	Failed registraion	WarpLink Managerからのレスポンスが不正
	Status error	WarpLink Managerからのレスポンスが不正

第 32 章

Extended track IP reachability mode

第32章 Extended track IP reachability mode
Netevent拡張機能(ip reachability)

Netevent拡張機能(ip reachability)

Netevent拡張機能を使用することによって、標準のtrackでは指定できないoptionを指定することができます。Netevent機能および拡張track設定についての詳細は、付録E Netevent機能を参照してください。

◆ 移行command

```
vxr-x86#
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#track <2048-4095> ip reachability
vxr-x86(config-ext-track-ipr)#
```

■ destination

```
<説　　明>　ip reachabilityにおけるpingの宛先をIPアドレスまたはFQDNで指定します。
<書　　式>　destination (A.B.C.D|FQDN)
```

■ source

○ interface

```
<説　　明>　ip reachabilityにおけるpingの出力インタフェースを指定することができます。
<書　　式>　source interface ethernet <0-2>
            source interface tunnel <0-255>
            source interface ppp <0-4>
<　No　>　no source
```

○ ip

```
<説　　明>　ip reachabilityにおけるpingの送信元アドレスを指定することができます。
<書　　式>　source ip A.B.C.D
<　No　>　no source
```

■ payload-length

```
<説　　明>
  ・ip reachabilityにおけるping送信時のsize(icmp headerは含まない)を指定することができます。
<書　　式>　payload-length <56-1500>
<初 期 値>　payload-length 56
<　No　>　no payload-length
```

■ transmit

○ interval

<説　　明>　ip reachabilityにおけるpingの送信間隔を指定することができます。
<書　　式>　transmit interval <10-32767> (|variable)
<備　　考>
・variableを指定すると、ping NG発生時にpingの送信間隔を変化させることができます。Defaultは、無効です。

○ retries

<説　　明>　ip reachabilityにおけるpingのretry回数を指定することができます。
<書　　式>　transmit retries <0-255>
<　No　>　no transmit retries

■ recovery

○ count

<説　　明>　指定した回数だけ連続でping OKとなった場合に復旧と判断します。
<書　　式>　recovery count <1-255>
<初 期 値>　recovry count 1
<　No　>　no recovery count

○ delay

<説　　明>
・ip reachability を利用する場合、復旧時(event up と判別した場合)から実際にup 時のactionを実行するまでにdelay を設定することができます。
<書　　式>　recovery delay <10-3600>
<　No　>　no recovery delay
<備　　考>
・Delay timer が動作している場合は、trackはdown state が維持され、この間にもip reachability check は動作し続けます。
・Delay timer動作中にevent downをretry回数検知した場合、delay timerはcancelされます。
・Delay timerがtimeoutすると、event upのactionが実行されます。このとき、delay timer中にカウントしたip reachability fail count は0 にクリアされ、action実行後に再度reachability checkが開始されます。

■ set
○ df-bit
<説　　明>　ip reachabilityにおけるpingパケットにDF bitを設定することができます。
<書　　式>　set df-bit
<初 期 値>　set df-bit
<　No　>　no set df-bit

○ ttl
<説　　明>
・ip reachabilityにおけるpingパケットのTTLを指定します。Defaultは、systemのTTL値(64)をsetします。
<書　　式>　set ttl <1-255>
<初 期 値>　set ttl 64
<　No　>　no set ttl

■ rtt
○ threshold
<説　　明>
・ping requestを送信してから、replyを受信するまでの時間(Round trip time)の閾値を指定します。replyが返信されていても、指定した閾値内にreplyがない状態がrtt delay回数分連続した場合、rtt statusがdownとなります。Defaultでは、RTTの監視は行いません。

○ normal-count
<説　　明>　RTT status upと判断するまでのrtt 正常回数です。Defaultは、3回です。

○ delay-count
<説　　明>　RTT status downと判断するまでの遅延回数です。Defaultは、3回です。

<書　　式>　rtt threshold <1-5000>
　　rtt threshold <1-5000> normal-count <1-255> delay-count <1-255>
<　No　>　no rtt

■ netevent
○ threshold
<説　　明>　monitor-log機能でloggingを行うかどうかを指定します。
<書　　式>　netevent monitor-log-status
<初 期 値>　no netevent monitor-log-status　(無効)
<　No　>　no netevent monitor-log-status

第 33 章

Extended track IPv6 reachability mode

第33章 Extended track IPv6 reachability mode
Netevent拡張機能(ipv6 reachability)

Netevent拡張機能(ipv6 reachability)

Neteventの拡張機能を使用することによって、標準のtrackでは指定できないoptionを指定することができます。Netevent機能および拡張track設定についての詳細は、付録E Netevent機能を参照してください。

◆ 移行command

```
vxr-x86#
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#track <2048-4095> ipv6 reachability
vxr-x86(config-ext-track-ipr)#
```

■ destination

＜説　　明＞　ipv6 reachabilityにおけるping6の宛先をIPv6アドレスまたはFQDNで指定します。
＜書　　式＞　destination (X:X::X:X|FQDN)

■ source

○ interface

＜説　　明＞　ipv6 reachabilityにおけるping6の出力インタフェースを指定することができます。
＜書　　式＞　source interface ethernet <0-2>
　　source interface tunnel <0-255>
　　source interface ppp <0-4>
＜　No　＞　no source

○ ip

＜説　　明＞　ipv6 reachabilityにおけるping6の送信元アドレスを指定することができます。
＜書　　式＞　source ip X:X::X:X
＜　No　＞　no source

■ payload-length

＜説　　明＞
・ipv6 reachabilityにおけるping6送信時のsize(icmpv6 headerは含まない)を指定することができます。
＜書　　式＞　payload-length <56-1500>
＜初 期 値＞　payload-length 56
＜　No　＞　no payload-length

■ transmit

○ interval

<説　　明>　ipv6 reachabilityにおけるping6の送信間隔を指定することができます。
<書　　式>　transmit interval <10-32767> (|variable)
<備　　考>
・variableを指定すると、ping6 NG発生時にping6の送信間隔を変化させることができます。Defaultは、無効です。

○ retries

<説　　明>　ipv6 reachabilityにおけるping6のretry回数を指定することができます。
<書　　式>　transmit retries <0-255>
<　No　>　no transmit retries

■ recovery

○ count

<説　　明>　指定した回数だけ連続でping6 OKとなった場合に復旧と判断します。
<書　　式>　recovery count <1-255>
<初 期 値>　recovry count 1
<　No　>　no recovery count

○ delay

<説　　明>
・ipv6 reachability を利用する場合、復旧時(event up と判別した場合)から実際にup 時のactionを実行するまでにdelay を設定することができます。
<書　　式>　recovery delay <10-3600>
<　No　>　no recovery delay
<備　　考>
・Delay timer が動作している場合は、trackはdown state が維持され、この間にもipv6 reachability check は動作し続けます。
・Delay timer動作中にevent downをretry回数検知した場合、delay timerはcancelされます。
・Delay timerがtimeoutすると、event upのactionが実行されます。このとき、delay timer中にカウントしたipv6 reachability fail count は0 にクリアされ、action実行後に再度reachability checkが開始されます。

■ set
○ hop-limit
<説　　明>
・ipv6 reachabilityにおけるping6パケットのhop limitを指定します。
<書　　式>　set hop-limit <1-255>
<初 期 値>　set hop-limit 64
<　No　>　no set hop-limit

■ rtt
○ threshold
<説　　明>
・ping6 requestを送信してから、replyを受信するまでの時間(Round trip time)の閾値を指定します。replyが返信されていても、指定した閾値内にreplyがない状態がrtt delay回数分連続した場合、rtt statusがdownとなります。Defaultでは、RTTの監視は行いません。

○ normal-count
<説　　明>　RTT status upと判断するまでのrtt 正常回数です。Defaultは、3回です。

○ delay-count
<説　　明>　RTT status downと判断するまでの遅延回数です。Defaultは、3回です。

<書　　式>　rtt threshold <1-5000>
　　rtt threshold <1-5000> normal-count <1-255> delay-count <1-255>
<　No　>　no rtt

■ netevent
○ threshold
<説　　明>　monitor-log機能でloggingを行うかどうかを指定します。
<書　　式>　netevent monitor-log-status
<初 期 値>　no netevent monitor-log-status　(無効)
<　No　>　no netevent monitor-log-status

第 34 章

Monitor-log mode

第 34 章 Monitor-log mode

ログ機能

ログ機能

Neteventip/ipv6 reachability 拡張機能による reachability 監視結果をログファイルとして保存する機能です。

- 揮発性メモリ(内部メモリ)への保存と不揮発性メモリ(USB flash メモリ)へのバックアップを行ないます。
- バックアップしたログ情報は、show monitor-log コマンド(view mode 参照)で CLI 上に表示することが出来ます。また、copy コマンド(view mode 参照)で外部に取り出すことも出来ます。

■ 揮発性メモリ(内部メモリ) への保存

内部メモリへは、reachability 監視ログとリソース監視ログを保存します。

(1) reachability 監視ログ

ログとして出力する情報は次のとおりです。なお、全ての監視結果をログとして出力するわけではありません。疎通結果が Dead/Delay の場合は毎回出力しますが、Alive の場合は他の状態から遷移した時にだけ出力します。

＜出力情報＞

1. TrackID
   Netevent 機能で定義した Track の ID を出力します。
2. 監視時刻
   DateAndTime 形式で出力します(ex. 2010-9-30,9:45:36.0)。
3. 監視先 IPv4 アドレス
4. 監視元 IPv4 アドレス
5. 監視先 IPv6 アドレス
6. 監視元 IPv6 アドレス
7. 空欄
8. 空欄
9. 空欄
10. 疎通結果(数字を出力)
    1: Alive(応答あり /RTT 閾値回復開始時のみ)
    2: Dead(応答なし)
    3: Delay(RTT 閾値超過)
11. ICMP Code/Type
12. 詳細情報(シーケンス番号、NextHop MTU)
13. RTT[msec]
    Trap 通知直前の RTT 取得情報
14 IPv6 ヘッダ送信元アドレス(疎通結果が Dead の場合)
15 IPv4 ヘッダ送信元アドレス(疎通結果が Dead の場合)

＜ 次ページに続く ＞

■ 揮発性メモリ(内部メモリ) への保存（続き）
(2) リソース監視ログ
出力例および出力する情報は次のとおりです。
＜出 力 例＞
2010-10-5,18:15:15.0,0,133052,5
＜出力情報＞
1. 出力時刻
DateAndTime 形式で出力します(ex. 2010-9-30,9:45:36.0)。
2.CPU 使用率
最近 3 分の使用率を 0 ～ 100[%]で出力します。
3. メモリ空き容量[Kbyte]
4. セッション数（Connection Tracking 数）
0～最大セッション数(CLI から設定可能な最大セッション数)の範囲で出力します。

■ 不揮発性メモリ(USB Flash メモリ)へのバックアップ
(1) 定期バックアップ
「内部メモリへの保存」で保存された監視ログについて、最大ファイルサイズ(150 ～ 1000 Kbyte)を閾値として指定することができます。メモリ上のログファイルが監視間隔による判定時に、この条件(最大ファイルサイズ)に達した場合、メモリ上のログファイルを外部 USB Flash メモリへバックアップ（gzip 形式圧縮・移動）します。継続して出力されるログは新たにメモリ上に作成します。
定期バックアップは、スケジュール機能(global mode の schedule コマンドを参照してください)によって実行されます。
reachability 監視およびリソース監視では、監視ログ出力時も閾値チェックを行い、バックアップ条件に達している場合にはバックアップを実行します。

(2) バックアップファイルの管理
定期バックアップのタイミングで、バックアップ対象ファイルを外部 USB Flash メモリに移動します。
USB Flash メモリに既に保存されているログファイル数が、設定した最大ファイル数(1 ～ 10 世代まで)に達している場合は、最も古いファイルを削除してから、バックアップ対象ファイルを USB Flash メモリに移動します。
なお、ファイル名はバックアップ時刻をもとに生成します。同一ファイル名が存在する場合は、新しいファイルで上書きします。

第 34 章 Monitor-log mode

ログ機能

◆ 移行 command

```
vxr-x86#
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#monitor-log
vxr-x86(config-monitor-log)#
```

■ reachability

＜説　　明＞
・ping/ping6 による死活監視、遅延監視の結果を、ログ情報として内部メモリに保存します。

```
＜書　　式＞　reachability disk0 (|threshold logsize <150-1000> files <1-10>)
              reachability disk0 threshold logsize <150-1000>
              reachability disk0 threshold files <1-10>
＜初 期 値＞　no reachability
＜　No　＞　no reachability
```

■ resource

```
＜説　　明＞　本装置のシステムリソース情報を 3 分毎に定期的に監視して結果を出力します。
＜書　　式＞　resource disk0  (|threshold logsize <150-1000> files <1-10>)
              resource disk0 threshold logsize <150-1000>
              resource disk0 threshold files <1-10>
＜初 期 値＞　no resource
＜　No　＞　no resource
```

＜備　　考＞
・定期バックアップの取得先を指定します。disk0 は、ディスクイメージ内のユーザ割り当て領域です。
・logsize については、「定期バックアップ」を参照してください。
・files については、「バックアップファイルの管理」を参照してください。

第 35 章

mail server mode

mail server mode

メール送信機能

＜説　　明＞

・イベント発生時に、管理者にメールで通知する機能です。次のイベント発生時に、メールを送信します。

○ PPP の接続 / 切断

・PPP on-demand 接続が有効な場合、メール送信機能は無効です（動作しません）。

イベント	メールの件名	メールの本文
PPPの接続	ppp0 was connected	IP address is A.B.C.D
PPPの切断	ppp0 was disconnected	IP address is released

※上記は、ppp0 の接続 / 切断時に送信するメールの例です。

mail server mode

○ 移行command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#mail server 0
vxr-x86(config-mail-server)#
```

■ メール送信(SMTP)設定

＜説　　明＞
・SMTPサーバのアドレスおよびポート番号を指定することができます。OP25Bにより、ISPが25番ポートをブロックしている場合は、587番ポートを指定すると接続できるようになります。
・本設定は、メールサーバ毎に行います。

○ server smtp address
＜書　　式＞　server smtp address (A.B.C.D|FQDN)

○ server smtp port
＜書　　式＞　server smtp port <1-65535>
＜　No　＞　no server smtp port
＜初 期 値＞　server smtp port 25 (=no server smtp port)

○ server pop3 address
＜書　　式＞　server pop3 address (A.B.C.D|FQDN)
＜　No　＞　no server pop3 address
＜備　　考＞　認証設定で、POP before SMTPを使用する場合に設定します。

■ 認証設定

○ server authentication
＜説　　明＞
・SMTPサーバよりメール送信するために、以下の3つの認証設定をサポートします。認証なしも指定することが出来ます。
　　POP before SMTP, SMTP-Auth (login) , SMTP-Auth (plain)
＜書　　式＞　server authentication (pop-before-smtp|smtp-auth-login|smtp-auth-plain)
＜　No　＞　no server authentication

○ username
＜説　　明＞　認証設定を有効にした場合は、認証用のIDとパスワードを指定します。
＜書　　式＞　username WORD password (hidden|) WORD
＜　No　＞　no username

mail server mode

■ メールヘッダ部の設定

＜説　　明＞
・送信するメールの各ヘッダ部に設定する値を指定します。
・本設定は、interface ppp mode で、インタフェース毎（ppp <0-4>）に指定することが出来ます。

○ mail send server
＜説　　明＞　使用するメールサーバを番号で指定します。
＜書　　式＞　mail send server <0-2>
＜　No　＞　no mail send server

○ mail send from
＜説　　明＞　送信元メールアドレスを設定します。
＜書　　式＞　mail send from WORD
＜　No　＞　no mail send from
＜備　　考＞
・WORD には、送信元メールアドレス（例：centurysys@xxx.isp.ne.jp）を指定します。
・mail send from コマンド（interface ppp mode）で送信元メールアドレスを指定しない場合は、mail fromコマンド(global mode)で指定した送信元メールアドレスを使用します。

○ mail send to
＜説　　明＞　送信先メールアドレスを設定します。
＜書　　式＞　mail send to WORD
＜　No　＞　no mail send to
＜備　　考＞
・WORD には、送信先メールアドレス（例：user@centurysys.co.jp）を指定します。
・mail send to コマンド（interface ppp mode）で送信先メールアドレスを指定しない場合は、mail toコマンド(global mode)で指定した送信先メールアドレスを使用します。

○ mail send subject
＜説　　明＞　メールの件名を設定します。指定しない場合は、既定のフォーマットを使用します。
＜書　　式＞　mail send subject LINE
＜　No　＞　no mail send subject
＜備　　考＞
・LINE を指定しない場合は、既定のフォーマットを使用します。以下に例を示します。
ppp0 の接続時： ppp0 was connected
ppp0 の切断時： ppp0 was disconnected

○ body
＜説　　明＞
・本文には、既定のフォーマットを使用します。ユーザが指定することは出来ません。
・以下に例を示します。
PPP の接続時： IP address is A.B.C.D
PPP の切断時： IP address is released

第 36 章

interface bridge mode

interface bridge mode

■ OpenFlow

・OpenFlowには、経路制御を行うOpenFlow Controller(OFC)と、データ転送を行うOpenFlow Switch (OFS)があります。OFCとOFSは、OpenFlow protocolによって通信を行います。
・本装置は、OFSとして動作します（OFCの機能はありません）。
・OFCと接続すると、OFCからの制御でデータ転送が行われます。未接続の場合は、通常のスイッチとして動作します（FDBに基づいてデータ転送を行います）。

■ 仮想スイッチ機能

・OpenFlow Controllerからのフォワーディングの制御を行います。Defaultでは、OpenFlow対応スイッチとして動作せず、通常のスイッチングハブとして動作します。OFCと接続すると、OFCからの命令によって処理が行われます。
※仮想スイッチ機能では、Bridge filterは使用できません。

インタフェースを仮想スイッチグループに参加させる場合の制限
インタフェースが以下の状態の場合は、当該インタフェースを仮想スイッチグループに、参加させることは出来ません。仮想スイッチグループに参加させる場合は、以下の設定を削除・変更するようにしてください。

・PPPoEクライアントの設定
・VRRPの設定
・IPsec policyの設定
・L2TPv3 xconnectの設定
VLANインタフェースをxconnectとして使用している場合は、該当する物理インタフェースの指定も出来ません。
・QoSの設定

interface bridge mode

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#interbridge <0-4095>
vxr-x86(config-bridge)#
```

◆ ip address

＜説　　明＞　インタフェースに IP アドレスを設定します。
＜書　　式＞　ip address A.B.C.D/M (|secondary)
＜　no　＞　no ip address A.B.C.D/M (|secondary)

◆ ip address

＜説　　明＞　DHCP により IP アドレスを取得します。
＜書　　式＞　ip address dhcp (|HOSTNAME)
＜　no　＞　no ip address dhcp

◆ ipv6 address

＜説　　明＞　インタフェースに IPv6 アドレスを設定します。
＜書　　式＞

```
ipv6 address X:X::X:X link-local
ipv6 address X:X::X:X/<0-128> (|eui-64)
ipv6 address autoconfig
```

＜　no　＞

```
no ipv6 address X:X::X:X link-local
no ipv6 address X:X::X:X/<0-128> (|eui-64)
no ipv6 address autoconfig
```

＜備　　考＞
・link-local 指定時は、自動的に設定される LLA を上書きします。
・eui-64 指定時は、ipv6-address は prefix 部のみ指定します。

◆ ipv6 address DHCPv6-PD

＜説　　明＞　DHCPv6 Prefix Delegation を設定します。
＜書　　式＞　ipv6 address DHCPv6-PD X:X::X:X/M (|eui-64)
＜　no　＞　no ipv6 address DHCPv6-PD (|X:X::X:X/M)
＜備　　考＞
・ipv6-address は、sub-prefix と host 部を指定することが出来ます。
・DHCPv6-PD は、DHCPv6 PD で受信する prefix 部のプロファイル名です。DHCPv6-PD は、DHCPv6 パケットを受信するインタフェース(異なるインタフェース)上で、ipv6 dhcp client pd コマンドを使用して設定します。

interface bridge mode

◆ mtu
<説　　明>　MTUの値を設定します。
<書　　式>　mtu <bytes:68-1500>
<　no　>　no mtu

◆ ip proxy arp
<説　　明>　Proxy ARPを有効にします。
<書　　式>　ip proxy-arp
<初 期 値>　no ip proxy-arp
<　no　>　no ip proxy-arp

◆ ip directed-broadcast
<説　　明>　Directed Broadcastのフォワーディングを有効にします。
<書　　式>　ip directed-broadcast
<初 期 値>　no ip directed-broadcast
<　no　>　no ip directed-broadcast

interface bridge mode

◆ ip redirects

＜説　　明＞

・ICMP redirect（type=5）とは、同一ネットワーク上に他の最適なルートがあることを通知するためのメッセージです（RFC792）。

・本装置のSend redirect機能によって、ICMP redirectの送信の有無を切り替えることが出来ます。

＜書　　式＞　ip redirects

＜初 期 値＞　ip redirects　　(有効)

＜　No　＞　no ip redirects　(無効)

＜備　　考＞

・以下にICMPRedirectの例を示します。ICMP Redirect受信後の動作は、Host側の動作に依存するため、常に次のような動作になるというわけではありません。

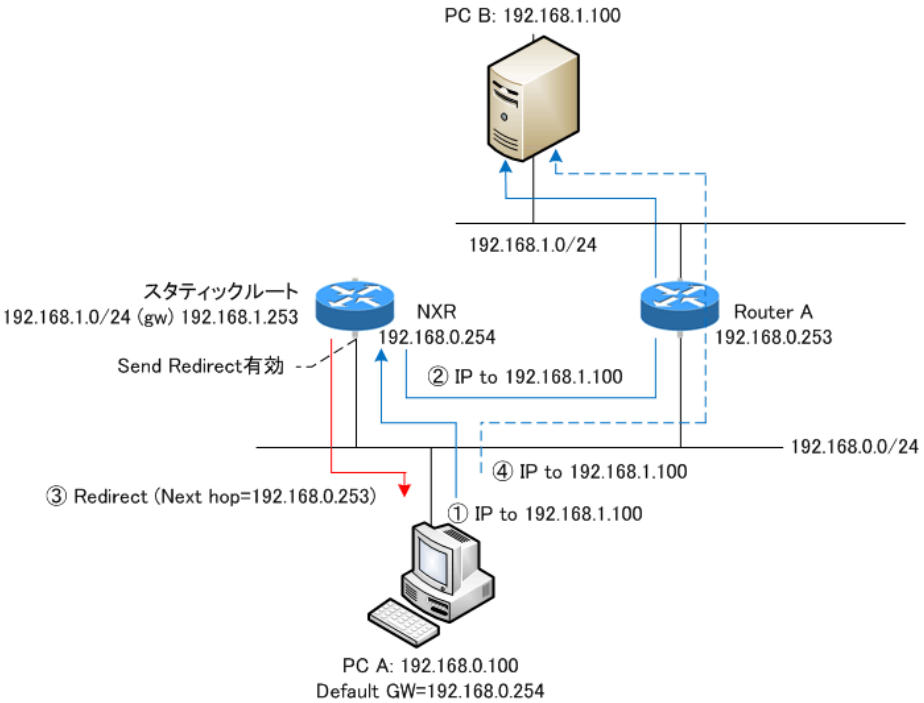
① Host Aは、Host B(192.168.1.100)へのIPv4パケットをdefault gw(VXR)に送信します。

② VXRは、ルーティング情報から、192.168.1.0/24宛てのnext hopは192.168.1.253であることを知り、Router Aへ転送します。

③ このとき、next hopのRouter Aは、送信元のHost Aと同一ネットワークであるため、Host AにICMP Redirectを送信します。

④ Host Aは、以降のHost B宛てのIPv4パケットは、ICMP Redirectで通知されたnext hopに従って、Router Aへ送出します。

・本装置が、ICMP Redirectを受信した場合は、ルーティングキャッシュの更新をしません。ルーティングテーブルに従ったforwarding動作を継続します。



interface bridge mode

◆ ip tcp adjust-mss

＜説　　明＞

・Path MTU Discovery（PMTUD）機能（End-to-end でフラグメントが発生しない最大の MTU を発見すること）によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器（ルータ等）が ICMP fragment needed をフィルタリングしている場合（ブラックホールルータが存在する場合）や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、End-to-end での通信に支障をきたすことになります。このような場合、TCP では　SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

＜書　　式＞　ip tcp adjust-mss (auto|<500-1460:bytes>)

＜初 期 値＞　no ip tcp adjust-mss

＜　No　＞　no ip tcp adjust-mss

＜備　　考＞

・IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。

・本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ユーザが設定する場合は、MSS 値を指定します。元の MSS 値に関係なく指定した値に強制的に変更します。

・UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。

・「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

◆ ipv6 tcp adjust-mss

＜説　　明＞　TCP/IPv6 の MSS 値を設定します。

＜書　　式＞　ipv6 tcp adjust-mss (auto|500-1460)

＜初 期 値＞　no ipv6 tcp adjust-mss

＜　no　＞　no ipv6 tcp adjust-mss

interface bridge mode

◆ ip mask-reply

＜説　　明＞

・OpenView などの監視装置では、監視ネットワーク内の機器に対して ICMP address mask request（type=17）を送信することによって機器のインタフェースのネットマスク値を取得します（単純に、死活監視で使用する場合もあります）。

・本装置では、ICMP address mask request への応答の有無を設定することが出来ます。

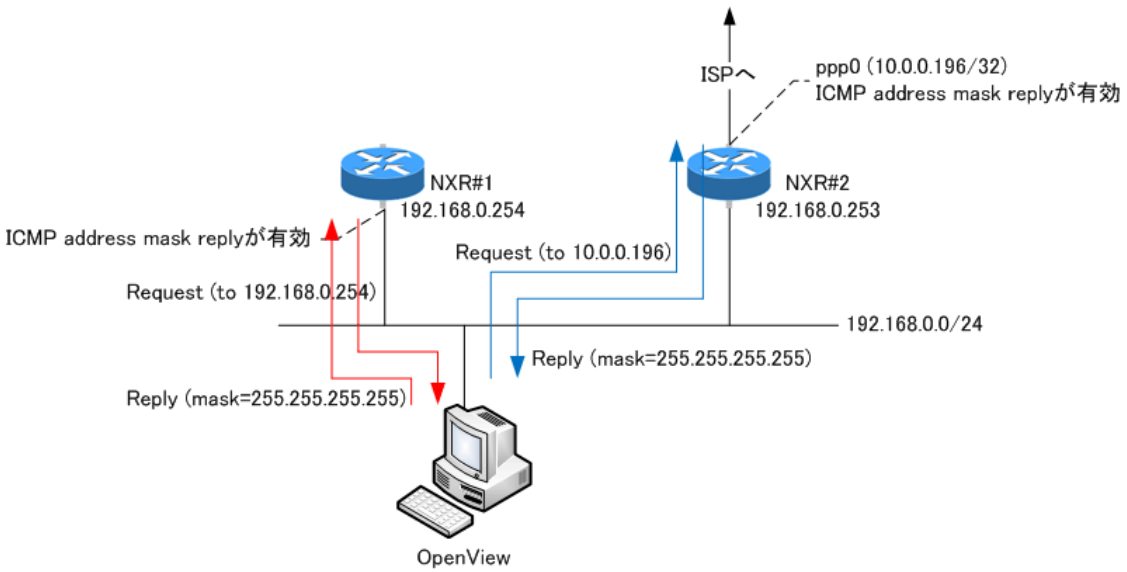
＜書　　式＞　ip mask-reply　（ICMP address mask request に応答します。）

＜初 期 値＞　no ip mask-reply（ICMP address mask request に応答しません。）

＜　No　＞　no ip mask-reply

＜備　　考＞

・ICMP address mask request/reply の例を示します。



interface bridge mode

◆(ip|ipv6) rebound

＜説　　明＞

・下位ルータから受信したパケットを、受信インタフェースと同一インタフェースから出力(forwarding)した場合、下位ルータからVXRに対して再度パケットが送信されてくるため、下位ルータとVXRの間でTTLが「0」になるまでパケットがループします。

・IP rebound機能を無効にすると、受信インタフェースと送信インタフェースが同一の場合、パケットをドロップし、かつ送信元にdestination unreachableを送信します。

・Defaultは、有効です(受信インタフェースと送信インタフェースが同一でもドロップしません)。

＜書　　式＞　(ip|ipv6) rebound

＜初 期 値＞　(ip|ipv6) rebound

＜　no　＞　no (ip|ipv6) rebound

interface bridge mode

◆ ip reassemble-output

＜説　　明＞

・インタフェースのMTU（あるいはPMTU）より大きいパケットをIP forwardingする際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。本設定有効時、VXRがリアセンブルしたパケットは、以下のようにフラグメント処理を行います。

- fragmented packet(パケットの断片)がMTUを超える場合、リアセンブルしたパケットを再度MTUサイズにフラグメントして出力します。
- fragmented packet(パケットの断片)がMTUより小さい場合、受信したfragmented packetのサイズで出力します。
- パケット全体のサイズがMTUより小さい場合、リアセンブルしたパケットを出力します。

＜書　　式＞　ip reassemble-output

＜初 期 値＞　ip reassemble-output

＜　no　＞　no ip reassemble-output

＜備　　考＞

・上記の場合（本設定が有効の場合）、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易なIP実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズでVXRからパケットを出力します。また、出力時のIPフラグメント処理は、次のようになります。

- fragmented packet(パケットの断片)がMTUを超える場合、受信したfragmented packetをMTUサイズにフラグメントして出力します。
- fragmented packet(パケットの断片)がMTUより小さい場合、受信したfragmented packetのサイズで出力します。
- パケット全体のサイズがMTUより小さい場合、受信したfragmented packetをそのままのサイズで出力します。

・Defaultは、global設定およびinterface設定ともに有効です。Global設定とinterface設定のAND条件により、本機能が有効か無効かを判定します。本設定は、IP forwardingするパケットにのみ影響します。

・受信時のサイズを記載しておくバッファが32 個しかないため、33 個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-output が有効な場合と同様に処理します。

interface bridge mode

◆ ip arp reachable-time
<説　　明>　解決したARP の有効期間を設定することが出来ます。
<書　　式>　ip arp reachable-time <30000-3600000>
<初 期 値>　ip arp reachable-time 30000
<　No　>　no ip arp reachable-time
<備　　考>　show arp 実行時に、ステータスがREACHABLE と表示される時間です。
　　実際の時間は、(0.5 ～ 1.5) × reachable-time の間のランダムな値です。

◆ ip arp queue length
<説　　明>
・Ethernet/VLAN インタフェース上で IPv4 通信を行う場合、送信先（あるいは next hop）の MAC アドレスの解決を行う必要があります。この時、MAC アドレスが解決するまで queueing できる数を指定することが出来ます。
<書　　式>　ip arp queue length <1-1000>
<初 期 値>　ip arp queue length 3
<　No　>　no ip arp queue length
<備　　考>
・インタフェース(Ethernet/VLAN/WiMAX)毎に指定することが出来ます。
・Queue は、ネイバーのエントリ毎に作成されます
・この queue に queueing されたパケットは、アドレス解決の完了と同時に送信が行われます。Queue がいっぱいの状態で新たにパケットが来た場合、queue の先頭からドロップします。

◆ ipv6 nd prefix
<説　　明>　IPv6 Routing Prefix Advertisement を設定します。
<書　　式>　ipv6 nd prefix X:X:X:X::X/M
　　(|<valid-lifetime:0-4294967295> <preferred-lifetime:0-4294967295>)
<　no　>　no ipv6 nd prefix X:X:X:X::X/M
　　(|<valid-lifetime:0-4294967295> <preferred-lifetime:0-4294967295>)
<備　　考>　Ethernet/VLAN のみ設定することが出来ます。

◆ ipv6 nd send-ra
<説　　明>　IPv6 RA(Router Advertisement) の送信 / 停止を行います。
<書　　式>　ipv6 nd send-ra　　(RA 送信)
<　no　>　no ipv6 nd send-ra　　(RA 停止)

◆ ipv6 nd ra-lifetime
<説　　明>　IPv6 RA(Router Advertisement) のライフタイムを設定します。
<書　　式>　ipv6 nd ra-lifetime <0-9000>
<初 期 値>　ipv6 nd ra-lifetime 90
<　no　>　no ipv6 nd ra-lifetime
<備　　考>　ra-lifetime >= ra-interval max になるように設定してください。

interface bridge mode

◆ ipv6 nd ra-interval
<説　　明>　RA(Router Advertisement）インターバルを設定します。
<書　　式>　ipv6 nd ra-interval <min:3-6750> <max:4-9000>
<初 期 値>　ipv6 nd ra-interval 10 30
<　no　>　no ipv6 nd ra-interval
<備　　考>　min < max x 0.75になるように設定してください。

◆ ipv6 nd ns-interval
<説　　明>　NS（Neighbor Solicitation）の送信間隔を設定します。
<書　　式>　ipv6 nd ns-interval <msec:1000-3600000>
<初 期 値>　ipv6 nd ns-interval 1000
<　no　>　no ipv6 nd ns-interval （初期値）

◆ ipv6 nd rs-interval
<説　　明>　RS（ Router Solicitation）インターバルを設定します。
<書　　式>　ipv6 nd rs-interval <interval:1-10sec>
<初 期 値>　ipv6 nd rs-interval 1
<　no　>　no ipv6 nd rs-interval （初期値）

◆ ipv6 nd rs-count
<説　　明>　RS（Router Solicitation）の送信回数を設定します。
<書　　式>　ipv6 nd rs-count <count:1-2147483647>
<初 期 値>　ipv6 nd rs-count 3
<　no　>　no ipv6 nd rs-count （初期値）

◆ ipv6 nd reachable-time
<説　　明>
・ルータ広告を受信した端末が,送信時に確認できた隣接ノードの到達性についての情報の有効期間を指定します。
<書　　式>　ipv6 nd reachable-time <msec:0-3600000>
<初 期 値>　ipv6 nd reachable-time 30
<　no　>　no ipv6 nd reachable-time （初期値）
<備　　考>
・この値が大きいと隣接ノードの到達性の問い合わせ回数が減少しますが，端末の所有する到達性情報と実際の到達性が異なる可能性が高くなります。

◆ ipv6 nd dad attempts
<説　　明>　DAD（Duplicate Address Detection）の送信回数を設定します。
<書　　式>　ipv6 nd dad attempts <0-600>
<初 期 値>　ipv6 nd dad attempts 1
<　no　>　no ipv6 nd dad attempts （初期値）

interface bridge mode

◆ ipv6 nd accept-redirects
＜説　　明＞
・IPv6 forwarding が無効の場合に、ICMPv6 redirects を受け入れるかどうかを指定します。
＜書　　式＞　ipv6 nd accept-redirects
＜初 期 値＞　no ipv6 nd accept-redirects
＜　no　＞　no ipv6 nd accept-redirects
＜備　　考＞　IPv6 forwarding が有効な場合は、この設定に関係なく受信しません。

◆ ipv6 nd queue length
＜説　　明＞
・Ethernet/Vlan interface 上で IPv6 通信を行う場合、近隣探索（Neighbor Discovery）によって送信先(nexthop)の mac address の解決を行います。このとき、mac address が解決するまで queueing できるパケット数を指定することができます。
・Queue は、neighbor の entry 毎に作成されます。
・queueing された packet は、address 解決ができると同時に送信が行われます。
・Queue が full の状態で新たに packet が来た場合、queue の先頭から drop されます。
＜書　　式＞　ipv6 nd queue length <1-1000>
＜初 期 値＞　ipv6 nd queue length 3
＜　no　＞　no ipv6 nd queue length
＜備　　考＞　IPv4 の IPv6 それぞれについて、interface 毎に指定することができます。
　　IPv4 については、ip arp queue length を参照してください。

◆ ip access-group
＜説　　明＞
・global mode で設定した ACL をインタフェースに適用することで、パケットフィルタリングを行うことができます。
＜書　　式＞　ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
＜　No　＞　no ip access-group (in|out|forward-in|forward-out)
＜備　　考＞
・各インタフェースへのパケットフィルタリングの適用箇所(付録の Packet Traveling を参照)は、以下の 4ヶ所です。
- in(local input)　VXR 自身で受信して処理するパケットを制限します。
- out(local output) VXR 自身が作成して出力するパケットを制限します。
　　トンネリングされたパケットも VXR 自身が作成したパケットとして認識します。
- forward-in　VXR が当該インタフェースで受信して forwarding するパケットを制限します。
- forward-out VXR が受信して当該インタフェースへ forwarding するパケットを制限します。
・mac 指定のある ACL は、out および forward-out に設定することは出来ません。

◆ ipv6 access-group
＜説　　明＞　アクセスグループに IPv6 アクセスリストを追加します。
＜書　　式＞　ipv6 access-group (in|out|forward-in|forward-out) IPV6-ACL-NAME
＜　no　＞　no ipv6 access-group (in|out|forward-in|forward-out)

interface bridge mode

◆ ip masquerade

＜説　　明＞
・インタフェースよりパケットを出力する際に、パケットの送信元 IPv4 アドレスを出力インタフェースの IPv4 アドレスに自動変換する機能です。
＜書　　式＞　ip masquerade　（有効）
＜初 期 値＞　no ip masquerade（無効）
＜　No　＞　no ip masquerade
＜備　　考＞
・すべてのインタフェース(Ethernet/VLAN/PPP/Tunnel/Bridge（仮想スイッチ))で設定することが出来ます。
・TCP/UDP/ICMP のみ対応しています。その他のプロトコルに関しては、動作は保証しません。
・IPv6 パケットは、IP マスカレードの対象外です。
・forward out/local output フィルタリング適用後のパケットに、IP マスカレードを適用します。

◆ ip (snat-group|dnat-group)

＜説　　明＞
・global mode で設定した SNAT または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。
・SNAT は、パケットの出力時に適用されます。DNAT は、パケットの入力時に適用されます。
＜書　　式＞　ip (snat-group|dnat-group) NAT-NAME
＜　No　＞　no ip (snat-group|dnat-group)
＜備　　考＞　NAT ルールの設定は、ip snat/ip dnat コマンド(global mode)で行います。

◆ ip webauth-filter

＜説　　明＞
・Web 認証フィルタをインタフェースに適用すると、ある特定のホスト、ネットワークやインタフェースについて、Web 認証せずに通信することが可能となります。
・Web 認証フィルタは、各インタフェースにつき、IN/OUT をそれぞれ一つずつ設定することができます。
・Default の設定はありません。
＜書　　式＞　ip webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
＜　No　＞　no ip webauth-filter (forward-in|forward-out)
＜備　　考＞
・Web 認証フィルタの設定については、ip web-auth access-list コマンド（global mode）を参照してください。
・Web 認証については、Web Authenticate mode を参照してください。

◆ pppoe-client ppp

＜説　　明＞　PPPoE クライアントを有効にします。
＜書　　式＞　pppoe-client ppp <0-4>
＜初 期 値＞　no pppoe-client ppp
＜　no　＞　no pppoe-client ppp <0-4>
＜備　　考＞　PPPoE クライアントは、複数指定することが出来ます。

interface bridge mode

◆ ip spi-filter

＜説　　明＞

・簡易ファイヤウォールの一つとして、SPI（Stateful Packet Inspection）機能をサポートします。

・パケットに関連するコネクションの状態を見て、当該パケットをドロップするかしないかを決める機能です。

＜書　　式＞　ip spi-filter　（有効）

＜初 期 値＞　no ip spi-filter（無効）

＜　No　＞　no ip spi-filter

＜備　　考＞

・コネクションの状態が、established または related の場合に、パケットの転送を許可します。

・Established とは、すでに双方向でパケットの通信がありコネクションが確立されている状態です。

・Related とは、すでに確立しているコネクションがある状態です。FTP のデータ転送等がこれに該当します。

・新しい接続でありながら、syn ビットの立っていないパケットはドロップします。

・SPI は、forward in および local input の位置で適用されます。ユーザが適用位置を変更することは出来ません。

◆ ipv6 spi-filter

＜説　　明＞　IPv6 SPI filter を設定します。

＜書　　式＞　ipv6 spi-filter

＜初 期 値＞　no ipv6 spi-filter

＜　no　＞　no ipv6 spi-filter

◆ ip spi-filter log

◆ ipv6 spi-filter log

＜説　　明＞　フィルタログ機能（syslog mode 参照）を有効にします。
パケットが、SPI フィルタにマッチした場合、syslog に出力することが出来ます。

＜書　　式＞　ip spi-filter log [limit <0-100>]
ipv6 spi-filter log [limit <0-100>]

＜初 期 値＞　ip spi-filter log limit 10
ipv6 spi-filter log limit 10

＜　No　＞　no ip spi-filter
no ipv6 spi-filter

＜備　　考＞

・limit を指定すると、1 秒当たりのログ出力数を制限します。初期値は、10 パケット / 秒です。

・WAN 側からの意図しないパケットが、SPI フィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分に注意してください。

interface bridge mode

◆ **shutdown**

＜説　　明＞　インタフェースをシャットダウンすることができます。
＜書　　式＞　shutdown
＜初 期 値＞　no shutdown
＜　no　＞　no shutdown

◆ **ipsec policy**

＜説　　明＞　当該インタフェースで使用するIPsecローカルポリシーを設定します。
＜書　　式＞　ipsec policy <1-255>
＜　No　＞　no ipsec policy (|1-255>)
＜備　　考＞
・各インタフェースに、IPsecローカルポリシーを4つまで設定することが出来ます。他のインタフェースで既に設定しているIPsecローカルポリシーは、重複して設定できません。

◆ **ipsec policy-ignore**

＜説　　明＞
・IPsec policy のチェックを行わないように指定する機能です。IPsec policy としてanyなどを指定したけれども、特定の通信のみIPsec 化したくない場合に、この機能を使用します。
＜書　　式＞　ipsec policy-ignore (|input|output)
＜初 期 値＞　no ipsec policy-ignore （無効）
＜　No　＞　no ipsec policy-ignore
＜備　　考＞
・Inputを指定した場合、inbound policy check を実行しないため、IPsec 化されてくるべきパケットがドロップ されてしまう現象を回避することができます。
・Output を指定した場合、当該インタフェースから出力されるパケットは、IPsec policy をチェックしないため平文で送信されます。

■ **QoS**

＜説　　明＞　QoS（クラス分類）の設定を行います。

○ classify

＜書　　式＞　classify (input|output) route-map ROUTEMAP
＜備　　考＞
・インタフェースにルートマップを適用します。1つのインタフェースに、inputとoutputを別々に設定することが出来ます。
・inputで指定したルートマップは、PRE-ROUTING(付録のPacket Travelingを参照)で適用されます。
・outputで指定したルートマップは、POST-ROUTING(付録のPacket Travelingを参照)で適用されます。

○ no classify

＜書　　式＞　no classify (|input|output)
＜備　　考＞
・インタフェースに適用したルートマップを削除します。
・「no classify」を実行すると、両方(inputとoutput)を削除します。片方だけを削除する場合は、inputまたはoutputを指定します。

interface bridge mode

◆session invalid-status-drop-interface

＜説　　明＞

・session invalid-status-drop機能(global mode参照)をインタフェース毎に指定することができます。

・本機能は、default で無効です。

＜書　　式＞　session invalid-status-drop-interface enable

＜初 期 値＞　no session invalid-status-drop-interface enable

＜　no　＞　no session invalid-status-drop-interface enable

＜備　　考＞

・あるインタフェースに対してのみ適用したい場合は、global mode で session invalid-status-drop 機能を無効にして、かつ本機能を指定インタフェースで有効にします。以下は、ethernet 0 インタフェースに適用する場合の設定例です。

- global mode で、session invalid-status-drop を無効にします。

```
vxr-x86(config)#no session invalid-status-drop enable
```

- 指定インタフェースで、本機能を有効にします。

```
vxr-x86(config)#interface ethernet 0
vxr-x86(config-if)#session invalid-status-drop-interface enable
```

interface bridge mode

◆ ip arp filter

＜説　　明＞
・異なるインタフェースに割り当てられているアドレスに対するARP requestを受信した際に、ARP replyを返す/返さない機能です。
＜書　　式＞　ip arp filter
＜初 期 値＞　ip arp filter　　（有効：ARP replyを返さない）
＜　no　＞　no ip arp filter　　（無効：ARP replyを返す）
＜備　　考＞
・あるLANセグメントに複数のEthernetインタフェースが接続されている場合は、複数のインタフェースからARP replyを返さないように、本機能を有効にします。
・一方で、あるLAN上の端末に対するhost routeが、別インタフェースになっている場合に、当該hostからのARP requestに対して、ARP replyを返す場合は、本機能を無効にします。
・ARP replyの送信先は、ルート情報によって決まります。

◆ ip arp gratuitous

＜説　　明＞　gratuitous ARP(GARP)を送信する機能です。
＜書　　式＞　ip arp gratuitous <attempts:1-255> <interval:1-3600> <delay:1-600>
　　ip arp gratuitous (= ip arp gratuitous <attempts:1> <interval:1> <delay:5>)
＜初 期 値＞　no ip arp gratuitous　（無効：GARPを送信しない）
＜　no　＞　no ip arp gratuitous
＜備　　考＞
・アドレスの重複を避けたり、ARPテーブルを更新するために、本装置では、下記のタイミングに、GARP(request)を送信します。
　・IPアドレスを追加した場合：追加したアドレスのGARPを送信します。
　・リンクアップした場合：当該インタフェースの全アドレスのGARPを送信します。
　・VRRPマスターに遷移した場合：VIPに対するGARPを送信します。
・GARP送信機能は、default無効です。設定により有効にする場合、送信回数、送信間隔(sec)、初期試行までのdelay(sec)も同時に指定することが出来ます。
・設定可能なインタフェースは、Ethernet、VLAN、Bridge（仮想スイッチ）です。
・多数のVLANやBridge（仮想スイッチ）上で有効にすると、リンクアップ時に大量のGARPを送信するケースがあるため、本機能を有効にする場合は、注意してください。
・DHCPクライアント機能使用時、DHCPによってIPアドレスを取得したタイミングでは、GARP送信は行いません。しかし、既にIPアドレスを取得した状態で、リンクアップした場合は、GARPを送信します。

interface bridge mode

◆ **bridge hw-address**

<説　　明>　interface bridge（仮想スイッチ）のHWアドレスを設定します。
<書　　式>　bridge hw-address HH:HH:HH:HH:HH:HH
<　no　>　no bridge hw-address
<備　　考>
・未設定の場合、bridge（仮想スイッチ）に参加しているインタフェースの中で、一番小さいHWアドレスを使用します。
・HWアドレスを、設定することを推奨します。

◆ **bridge mac-aging**

<説　　明>　interface bridge（仮想スイッチ）のmac-agingを設定します。
<書　　式>　bridge mac-aging <15-3600>
<初 期 値>　bridge mac-aging 300
<　no　>　no bridge mac-aging (= bridge mac-aging 300)

◆ **bridge mac-table-size**

<説　　明>　interface bridge（仮想スイッチ）上のmac table size(FDB)を設定します。
<書　　式>　bridge mac-table-size <10-65536>
<　no　>　no bridge mac-table-size

◆ **openflow controller-address**

<説　　明>　接続するopenflow-controllerのIPアドレスを設定します。
<書　　式>　openflow controller-address ip A.B.C.D (port <1-65535>|)
<　no　>　no openflow controller-address　（全てのcontroller-addressを削除します）
　　no openflow controller-address ip A.B.C.D
　　no openflow controller-address ip A.B.C.D port <1-65535>

◆ **openflow datapath-id**

<説　　明>　switchの識別子として、datapath-idを設定することが出来ます。
<書　　式>　openflow datapath-id HEX
<　no　>　no openflow datapath-id
<備　　考>　HEX部は、<1-FFFFFFFFFFFFFFFF>の範囲で設定します。
　　未指定の場合は、システム内部で生成します。

◆ **openflow protocol**

<説　　明>　openflow-controllerへ接続する際のOpenflow　Protocolを指定します。
<書　　式>　openflow protocol {10|11|12|13}
<　no　>　no openflow protocol
<備　　考>　1つ（または複数）のバージョンを指定することが出来ます。
　　未指定の場合は、10(ver1.0)を使用します。
　　OpenFlow Controllerとバージョンを合わせる必要があります。

第 37 章

DDNS mode

DDNS mode

DDNS 機能

DDNS（Dynsmic DNS）とは、動的に変化するグローバル IP アドレスとドメイン名を対応付ける仕組みです。
グローバル IP アドレスの監視を行い、IP アドレスの変更があった場合に、DDNS サービスプロバイダに IP アドレスの変更を通知します。
これにより、動的なグローバル IP アドレス環境においても、固定のドメイン名によるアクセスが可能となります。

■ DDNS サービスプロバイダ

本装置が対応している DDNS サービスプロバイダについて示します。

○有料サービス

有料で DDNS サービスを提供している以下のプロバイダに対応しています。

・どこでもカメラ
  http://www.dococame.net/
・Dyn
  http://dyn.com/

○無料サービス

無料 DDNS サービスと無料ドメイン名を提供している以下のプロバイダに対応しています。

・DtDNS
  http://www.dtdns.com/
・No-IP
  http://www.no-ip.com/

○汎用プロバイダ

上記のプロバイダでは、NAT 環境を考慮して、以下のシーケンスで IP アドレスの変更通知が行われます。
(1)　IP アドレス確認用サーバへ、自身の IP アドレスを問い合わせる。
(2)　DDNS サーバへ、ドメイン名 /IP アドレスを通知する。
また、IP アドレス確認用サーバ、DDNS サーバの URL や HTTP Query は、プロバイダ固有の値を使用します。

汎用プロバイダにおいては、IP アドレス確認用サーバに対して IP アドレスの問い合わせを行わず、指定したインタフェースの IPv4/IPv6 アドレスを直接 DDNS サーバへ通知します。
また、送信先の URL および HTTP Query は、ユーザが指定します。

DDNS mode

■ IPアドレス変更通知

以下に示すタイミングにおいて、DDNS プロバイダに対して IP アドレス変更通知を送信します。
DDNS 機能では、TCP80(HTTP)を利用して、DDNS プロバイダと通信を行います。通知する IP アドレスは、DDNS プロバイダへの問い合わせの際に使用する IP アドレスです。DDNS プロバイダは、本装置からの問い合わせに対して、本装置から受け取った HTTP パケットのソースアドレスを応答として返します。
したがって、バインドインタフェースを設定した場合でも、必ずしも当該インタフェースの IP アドレスが、DDNS プロバイダに登録されるわけではありません。

○サービス起動時

本機能は、必要な configuration が設定された時点で自動的に起動します。この際、指定インタフェースに IP アドレスが割り当てられている場合、IP アドレス変更通知を送信します。

○バインドインタフェース連動

サービス起動時に、インタフェースに対して IP アドレスが割り当てられていなかった場合には
IP アドレスが割り当てられた際に、IP アドレス変更通知を送信します。

○ IP アドレス変更の強制通知

無料 DDNS サービスプロバイダの中には、一定期間 IP アドレス変更通知がない場合、アカウントを削除してしまうものがあります。
そのため、グローバル IP アドレスの有無にかかわらず、上記に示した指定インタフェース連動による IP アドレス変更通知を起点に、ユーザが指定した強制更新間隔毎に IP アドレス変更通知を送信します。
なお、IP アドレスの変更が無いにもかかわらず、短い周期(1 分程度)で IP アドレス変更通知を行うと、アカウントが削除される場合があるので、インターバルの設定には注意するようにしてください。

○再送処理

回線障害等でサービスプロバイダへの接続失敗が発生した場合、IP アドレス変更通知の再送処理を行います。
初回の再送間隔は 10 秒で、再送回数が増える毎に 10 秒ずつ再送間隔が増大します。最大再送間隔は 60 秒です。

■ 状態表示

DDNS サービスには、以下の状態があります（show ddns コマンドで、状態を参照することができます)。

状態表示	説明
Configuration is incomplete	設定項目に不足がある場合
Starting	DDNSサービス開始中
DDNS connect attempt	DDNSプロバイダにアクセス中（接続リトライ中）
Failed login	DDNSプロバイダのアカウント認証に失敗
Succeed	DDNSプロバイダにIPアドレス登録成功

DDNS mode

◆ 移行 command
```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#ddns
vxr-x86(config-ddns)#
```

◆ service enable
```
<説　　明>　DDNSサービスを有効にします。
<書　　式>　service enable　　（有効）
<初 期 値>　no service enable　　（無効）
<　No　 >　no service enable
```

◆ account
```
<説　　明>　DDNSサービスを利用するためのユーザ IDおよびパスワードを設定します。
<書　　式>　account username USERID password (|hidden) PASSWORD
```

◆ bind-interface
```
<説　　明>　バインドインタフェース（接続回線インタフェース）を設定します。
<書　　式>　bind-interface INTERFACE
<備　　考>　本設定のインタフェース回線接続に連動して、IPアドレス変更通知を送信します。
　　INTERFACEには、ethernet，ppp，bridge（仮想スイッチ）を設定することが出来ます。
```

◆ forced-update-interval
```
<説　　明>　IPアドレス変更の強制通知設定を行います。
<書　　式>　forced-update-interval <hour:0-720>
<　No　 >　no forced-update-interval
<初 期 値>　forced-update-interval 0　　（無効）
<備　　考>
```
・グローバル IPアドレス変更の有無にかかわらず、強制的に IPアドレス変更通知を送信する間隔を設定します。

◆ ddns-provider
```
<説　　明>　接続するDDNSサービスプロバイダを指定します。
<書　　式>　ddns-provider (dococame | dtdns | dyndns | no-ip | http client)
<備　　考>　汎用プロバイダを利用する場合は、http clientを指定します。
```

◆ domain-name
```
<説　　明>　IPアドレスを結びつけるドメイン名を指定します。
<書　　式>　domain-name DOMAINNAME
<　No　 >　no domain-name (|DOMAINNAME)
<備　　考>　ドメイン名は、最大5つまで設定することが出来ます。
　　汎用プロバイダを利用する場合は、指定しません。
```

DDNS mode

◆ query
＜説　　明＞　汎用プロバイダを利用する場合に、HTTP Query を指定します。
＜書　　式＞　query WORD
＜備　　考＞
・Query には、以下のマクロ変数を使用することで、動的な値を指定することが出来ます。
　　${SN}：製品のシリアル番号
　　${IP}：bind-interface コマンドで指定したインタフェースの IPv4 アドレス
　　${IPV6}:bind-interface コマンドで指定したインタフェースの IPv6 グローバルアドレス
・大文字、小文字は区別しません。
・なお、マクロ変数に IPv4 アドレス、IPv6 アドレスを指定した場合、指定されたインタフェースに対応するアドレスが付与されていない時は、IP アドレス変更通知を行いません。

◆ url
＜説　　明＞　汎用プロバイダを利用する場合に、DDNS サーバを指定します。
＜書　　式＞　url (ip|ipv6) WROD
＜備　　考＞　送信先 URL（http://）を指定します。

第 38 章

access-server profile mode

access-server profile mode

◆ **移行 command**

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#access-server profile <0-31>
vxr-x86(config-ras)#
```

＜備　　考＞　プロファイル数は、機種により異なります。

◆ **ppp username**

＜説　　明＞　ユーザ名毎に、割り当てる IP アドレスを指定することが出来ます。
＜書　　式＞　ppp username USERID ip A.B.C.D
＜　No　＞　no ppp username
＜備　　考＞　詳細は、「付録 H RAS 機能」を参照してください。

第 39 章

interface virtual-template mode

interface virtual-template mode

■Virtual-template interface

・L2TP LNS機能など、多数の着信（RAS)がある場合、着信の数だけのPPPを設定することは、本装置の管理者にとって大きな負担となります。
・Virtual-templateを使用すると、callを受けた際にPPPのクローンを作成し、本モードの設定内容を当該PPPに適用します。
・Virtual-template interfaceは仮想的なインタフェースであり、実際に作成されるわけではありません。また、PPPクローンのインタフェース番号（ppp <100-256>）は、本装置が自動的に割り当てます。

◆ 移行command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#interface virtual-template <0-0>
vxr-x86(config-if-vt)#
```

◆ description

＜説　　明＞　インタフェースの説明を記述します。
＜書　　式＞　description DESCRIPTION
＜　No　＞　no descritpion
＜備　　考＞　使用可能な文字は、a-z,A-Z,0-9,-_.@です。

◆ ip address

＜説　　明＞　インタフェースにIPアドレスを設定します。
＜書　　式＞　ip address A.B.C.D/32
＜備　　考＞　32ビットマスクのみ指定することが出来ます。

◆ mtu

＜説　　明＞　MTUの値を設定します。
＜書　　式＞　mtu <bytes:68-1500>
＜初 期 値＞　mtu 1454
＜　No　＞　no mtu
＜備　　考＞
・virtual-templateとしての初期値はありません。未設定の場合は、virtual-templateを使用する機能が持つ初期値を使用します。

◆ ppp lcp mru

＜説　　明＞　MRUの値を設定します。
＜書　　式＞　ppp lcp mru <bytes:128-1500>
＜初 期 値＞　ppp lcp mru 1454
＜　No　＞　no ppp lcp mru
＜備　　考＞
・virtual-templateとしての初期値はありません。未設定の場合は、virtual-templateを使用する機能が持つ初期値を使用します。

interface virtual-template mode

◆ ip redirects

＜説　　明＞
- ICMP redirect（type=5）とは、同一ネットワーク上に他の最適なルートがあることを通知するためのメッセージです（RFC792）。
- 本装置の Send redirect 機能によって、ICMP redirect の送信の有無を切り替えることが出来ます。

＜書　　式＞　ip redirects
＜初 期 値＞　ip redirects　　(有効)
＜　No　＞　no ip redirects　(無効)
＜備　　考＞
- ICMPRedirect の例は、interface mode の ip redirects を参照して下さい。

◆ ip tcp adjust-mss

＜説　　明＞
- Path MTU Discovery（PMTUD）機能（End-to-end でフラグメントが発生しない最大の MTU を発見すること）によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器（ルータ等）が ICMP fragment needed をフィルタリングしている場合（ブラックホールルータが存在する場合）や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、End-to-end での通信に支障をきたすことになります。このような場合、TCP では　SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

＜書　　式＞　ip tcp adjust-mss (auto|<500-1460:bytes>)
＜初 期 値＞　no ip tcp adjust-mss
＜　No　＞　no ip tcp adjust-mss
＜備　　考＞
- IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。
- 本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。
- ユーザが設定する場合は、MSS 値を指定します。元の MSS 値に関係なく指定した値に強制的に変更します。
- UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。
- 「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

interface virtual-template mode

◆ ip mask-reply

＜説　　明＞

・OpenView などの監視装置では、監視ネットワーク内の機器に対して ICMP address mask request（type=17）を送信することによって機器のインタフェースのネットマスク値を取得します（単純に、死活監視で使用する場合もあります)。

・本装置では、ICMP address mask request への応答の有無を設定することが出来ます。

＜書　　式＞　ip mask-reply　（ICMP address mask request に応答します。）

＜初 期 値＞　no ip mask-reply（ICMP address mask request に応答しません。）

＜　No　＞　no ip mask-reply

＜備　　考＞

・ICMP address mask request/reply の例は、interface mode の ip mask-reply を参照して下さい。

◆ keepalive lcp-echo

＜説　　明＞　LCP echo requestによるキープアライブを有効にします。

＜書　　式＞　keepalive lcp-echo (|<interval:30-600> <failure-count:1-10>)

＜初 期 値＞　keepalive lcp-echo 30 3

＜　no　＞　no keepalive lcp-echo

＜備　　考＞

・lcp-echo request/reply の連続失敗回数が、failure count の設定回数に達すると、PPP を切断します。

◆ip rebound

＜説　　明＞

・下位ルータから受信したパケットを、受信インタフェースと同一インタフェースから出力(forwarding)した場合、下位ルータからVXRに対して再度パケットが送信されてくるため、下位ルータとVXRの間でTTLが「0」になるまでパケットがループします。

・IP rebound機能を無効にすると、受信インタフェースと送信インタフェースが同一の場合、パケットをドロップし、かつ送信元に destination unreachable を送信します。

・Default は、有効です(受信インタフェースと送信インタフェースが同一でもドロップしません)。

＜書　　式＞　ip rebound

＜初 期 値＞　ip rebound

＜　no　＞　no ip rebound

interface virtual-template mode

◆ip reassemble-output

＜説　　明＞

・インタフェースのMTU（あるいはPMTU）より大きいパケットをIP forwardingする際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。本設定有効時、VXRがリアセンブルしたパケットは、以下のようにフラグメント処理を行います。

- fragmented packet(パケットの断片)がMTUを超える場合、リアセンブルしたパケットを再度MTUサイズにフラグメントして出力します。
- fragmented packet(パケットの断片)がMTUより小さい場合、受信したfragmented packetのサイズで出力します。
- パケット全体のサイズがMTUより小さい場合、リアセンブルしたパケットを出力します。

＜書　　式＞　ip reassemble-output

＜初 期 値＞　ip reassemble-output

＜　no　＞　no ip reassemble-output

＜備　　考＞

・上記の場合（本設定が有効の場合）、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易なIP実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズでVXRからパケットを出力します。また、出力時のIPフラグメント処理は、次のようになります。

- fragmented packet(パケットの断片)がMTUを超える場合、受信したfragmented packetをMTUサイズにフラグメントして出力します。
- fragmented packet(パケットの断片)がMTUより小さい場合、受信したfragmented packetのサイズで出力します。
- パケット全体のサイズがMTUより小さい場合、受信したfragmented packetをそのままのサイズで出力します。

・Defaultは、global設定およびinterface設定ともに有効です。Global設定とinterface設定のAND条件により、本機能が有効か無効かを判定します。本設定は、IP forwardingするパケットにのみ影響します。

・受信時のサイズを記載しておくバッファが32 個しかないため、33 個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-output が有効な場合と同様に処理します。

interface virtual-template mode

◆ ip access-group

＜説　　明＞
・global mode で設定した ACL をインタフェースに適用することで、パケットフィルタリングを行うことができます。
＜書　　式＞　ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
＜　No　＞　no ip access-group (in|out|forward-in|forward-out)
＜備　　考＞
・各インタフェースへのパケットフィルタリングの適用箇所(付録の Packet Traveling を参照)は、以下の 4ヶ所です。
- in(local input)　VXR 自身で受信して処理するパケットを制限します。
- out(local output) VXR 自身が作成して出力するパケットを制限します。
　トンネリングされたパケットも VXR 自身が作成したパケットとして認識します。
- forward-in　VXR が当該インタフェースで受信して forwarding するパケットを制限します。
- forward-out VXR が受信して当該インタフェースへ forwarding するパケットを制限します。

・mac 指定のある ACL は、out および forward-out に設定することは出来ません。

◆ ip (snat-group|dnat-group)

＜説　　明＞
・global mode で設定した SNAT または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。
・SNAT は、パケットの出力時に適用されます。DNAT は、パケットの入力時に適用されます。
＜書　　式＞　ip (snat-group|dnat-group) NAT-NAME
＜　No　＞　no ip (snat-group|dnat-group)
＜備　　考＞　NAT ルールの設定は、ip snat/ip dnat)コマンド(global mode)で行います。

◆ ppp authentication

＜説　　明＞　PPP の認証プロトコルを設定します。
＜書　　式＞　ppp authentication (chap|pap|auto)
＜初 期 値＞　ppp authentication auto
＜　no　＞　no ppp authentication (= ppp authentication auto)

◆ ppp ipcp dns

＜説　　明＞　PPP 接続時に割り当てる DNS を指定します。
＜書　　式＞　ppp ipcp dns <primary:A.B.C.D> (|<secondary:A.B.C.D>)
＜　no　＞　no ppp ipcp dns

interface virtual-template mode

◆ peer ip proxy-arp

＜説　　明＞

・本機能の有効時に、IPCPで割り当てたpeer ipを含むアドレスが設定されているEthernetがある場合、当該インタフェース上でpeer ipに対応するARPを設定します。

＜書　　式＞　peer ip proxy-arp　　（有効）

＜　No　＞　no peer ip proxy-arp　（無効）

＜備　　考＞　Ethernet 0のIPアドレス、MACアドレス、およびpeer IPアドレスが、次の場合

eth0:192.168.0.1/24 mac:00:80:6d:00:00:01

peer ip:192.168.0.200

以下のARPエントリーを登録します。ただし、show arpでは表示されません。

192.168.0.200 00:80:6d:00:00:01

◆ peer ip pool

＜説　　明＞　使用するIPアドレスプールを指定します。

＜書　　式＞　peer ip pool WORD

＜　No　＞　no peer ip pool WORD

＜備　　考＞　IPアドレスプールは、ip local poolコマンド（global mode）で設定します。

◆session invalid-status-drop-interface

＜説　　明＞

・session invalid-status-drop機能(global mode参照)をインタフェース毎に指定することができます。

・本機能は、defaultで無効です。

＜書　　式＞　session invalid-status-drop-interface enable

＜初 期 値＞　no session invalid-status-drop-interface enable

＜　no　＞　no session invalid-status-drop-interface enable

＜備　　考＞

・あるインタフェースに対してのみ適用したい場合は、global modeでsession invalid-status-drop機能を無効にして、かつ本機能を指定インタフェースで有効にします。以下は、ppp 0インタフェースに適用する場合の設定例です。

- global modeで、session invalid-status-dropを無効にします。

```
vxr-x86(config)#no session invalid-status-drop enable
```

- 指定インタフェースで、本機能を有効にします。

```
vxr-x86(config)#interface ppp 0
vxr-x86(config-ppp)#session invalid-status-drop-interface enable
```

interface virtual-template mode

◆ (ip|ipv6) tcp strip-options

＜説　　明＞
- TCP パケット内のオプションを stip する機能です。
- Fast-forwarding が有効な場合、SACK/timestamp/MD5 については、strip されない場合があります。

＜書　　式＞　(ip|ipv6) tcp strip-options
(all|md5|mss|sack|sack-permitted|timestamp|wscale)

＜初 期 値＞　no (ip|ipv6) tcp strip-options

＜　No　＞　no (ip|ipv6) tcp strip-options

＜備　　考＞　Strip 可能なオプションと監視するパケットの種類は、次のとおりです。

TCPオプション	該当TCPパケット
MSS	SYN/SYN-ACK
Window Scale Option	SYN/SYN-ACK
SACK Permitted	SYN/SYN-ACK
SACK	すべてのTCPパケット
Time Stamp Option	すべてのTCPパケット
MD5 signature Option	すべてのTCPパケット

第 40 章

ngn-sip client mode

ngn-sip client mode

■データコネクト

データコネクトを使用する場合に設定します。データコネクトについては、付録 I を参照してください。

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#ngn-sip client <1-4>
vxr-x86(config-ngn-client)#
```

◆ mode tcp ip

＜説　　明＞　TCP アクセスを監視する IP アドレス、および listen port を指定します。
＜書　　式＞　mode tcp ip A.B.C.D port <1-65535>

◆ tel to

＜説　　明＞　TCP アクセス検出時に発呼する電話番号（宛先番号）を指定します。
＜書　　式＞　tel to NUMBER
＜備　　考＞　「0」または「#」で始まる NUMBER を指定します。指定可能な桁数は 5 ～ 32 桁です。

◆ idle-timeout

＜説　　明＞　TCP通信の無通信切断タイマーを設定します。
＜書　　式＞　idle-timeout <10-3600>
＜　No　＞　no idle-timeout (初期値)
＜初 期 値＞　idle-timeout 60
＜備　　考＞

・TCP セッション上のデータ通信状態を定期的に監視し、一定時間の無通信状態を検出すると、自動的にデータコネクト通信を終了します。

第 41 章

ngn-sip server mode

ngn-sip server mode

■データコネクト

データコネクトを使用する場合に設定します。データコネクトについては、付録 I を参照してください。

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#ngn-sip server <1-4>
vxr-x86(config-ngn-server)#
```

◆ mode tcp ip

＜説　　明＞　着信時に TCP を接続させる端末の IP アドレス（宛先 IP アドレス）、
　　および宛先 port 番号を指定します。
＜書　　式＞　mode tcp ip A.B.C.D port <1-65535>

◆ tel to

＜説　　明＞　着信を許可する番号（発信者番号）を指定します。
＜書　　式＞　tel from NUMBER
＜備　　考＞　「0」または「#」で始まる NUMBER を指定します。指定可能な桁数は 5 ～ 32 桁です。

◆ idle-timeout

＜説　　明＞　TCP通信の無通信切断タイマーを設定します。
＜書　　式＞　idle-timeout <10-3600>
＜　No　＞　no idle-timeout (初期値)
＜初 期 値＞　idle-timeout 60
＜備　　考＞

・TCP セッション上のデータ通信状態を定期的に監視し、一定時間の無通信状態を検出すると、自動的にデータコネクト通信を終了します。

第 42 章

ipv6 dhcp-server mode

ipv6 dhcp-server mode

■ DHCPv6 Server

本バージョンでは、DNS servers option のみ対応しています。

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#ipv6 dhcp-server WORD
vxr-x86(config-dhcp6s)#
```

◆ option-send dns-servers address

＜説　　明＞　Reply 送信時に、DNS サーバのアドレスを通知します。
　　任意の DNS サーバ指定、および複数（最大 3 つまで）の DNS サーバ指定が可能です。
＜書　　式＞　option-send dns-servers address (A.B.C.D|X:X::X:X)
＜　No　＞　no option-send dns-servers address (A.B.C.D|X:X::X:X)
＜備　　考＞
・本オプションを設定した場合は、クライアント側の設定（option-request dns-servers）に関係なく DNS アドレスを通知します。

◆ option-send dns-server add ipv6 dhcp-client

＜説　　明＞　DHCPv6 クライアントで取得した DNS サーバを、DHCP サーバで広告します。
　　DHCPv6 クライアントのインタフェースを設定します。
＜書　　式＞　option-send dns-server add ipv6 dhcp-client ethernet <X>
　　option-send dns-server add ipv6 dhcp-client ppp <X>
＜　No　＞　no option-send dns-server add ipv6 dhcp-client
＜備　　考＞
・DHCPv6 クライアントと連携して動作します。本オプションを設定している場合の動作は、次のようになります。
 -DHCPv6 クライアントが DNS サーバ情報を取得している場合、下位からの request に対して、reply に DNS サーバアドレスを付与します。
 -DHCPv6 クライアントが DNS サーバ情報を未取得の場合、下位からの request に対して、reply には DNS サーバアドレスを付与しません。

◆ option-send domain-name

＜説　　明＞　ドメイン名を（最大 3 つまで）設定することが出来ます。
＜書　　式＞　option-send domain-name WORD
＜　No　＞　no option-send domain-name WORD
＜備　　考＞
・本オプションを設定している場合、下位クライアントからの request（オプション：domain search List）に対して、ドメインサーチリストを reply します。

ipv6 dhcp-server mode

◆ option-send domain-name ipv6 add dhcp-client

＜説　　明＞　DHCPv6 クライアントで取得したドメインサーチリストを、DHCP サーバで広告します。
　　DHCPv6 クライアントのインタフェースを設定します。
＜書　　式＞　option-send domain-name add ipv6 dhcp-client ethernet <X>
　　option-send domain-name add ipv6 dhcp-client ppp <X>
＜　No　＞　no option-send domain-name add ipv6 dhcp-client
＜備　　考＞
・DHCPv6 クライアントと連携して動作します。本オプションを設定している場合の動作は、次のようになります。
 -DHCPv6 クライアントがドメインサーチリストを取得している場合、下位からの request に対して、replyにドメインサーチリストを付与します。
 -DHCPv6 クライアントがドメインサーチリストを未取得の場合、下位からの request に対して、replyにドメインサーチリストを付与しません。

◆ rapid-commit enable

＜説　　明＞　rapid-commit を有効にします。
＜書　　式＞　rapid-commit enable
＜　No　＞　no rapid-commit enable
＜備　　考＞
・本設定の有効時、2 つのメッセージ（Solicit/Reply）で、クライアントが情報取得を行うことが出来ます。
・クライアント側も同様に設定します。

第 43 章

ipv6 dhcp-client mode

ipv6 dhcp-client mode

■ DHCPv6 Client

・本装置のDHCPv6クライアントは、DHCPv6サーバに対して、Prefix Delegation(PD)や、DNSサーバなどのアドレスを要求し、情報を受け取ることが出来ます（※DHCPv6サーバよりIPv6アドレスを割り当てるクライアント機能は、本バージョンではサポートしていません）。
・PDを要求した場合、受信したprefixを使用して、本装置のIPv6アドレスを設定したり、LAN配下の端末に対して、RAでprefixを通知したりすることが出来ます。
・DNSサーバetcの情報を取得した場合、他の情報（SNTPサーバアドレス）については、本バージョンでは無視します。
・各オプションへの対応は、以下のとおりです（設定変更可能なオプションのみを記載しています）。
Rapid Commit:有効の場合、2つのメッセージ（通常は4つ）でアドレスを取得します。
Domain Name Servers: 有効にすると、DNSサーバアドレスの通知を要求します。
Domain Search List：有効の場合、ドメインサーチリストの通知を要求します。ドメインサーチリストで、通知されたドメインについて名前解決を行う場合は、DHCP上で取得したDNSサーバアドレスに対してのみクエリを送信し、その他のDNSサーバアドレス（ユーザ設定によるDNSサーバ等）にはクエリを送信しません。
Identity Association for Prefix Delegation(IAPD):IA prefixを要求する際に使用します（IAPDが有効の場合に送信します）。

□ Prefix Delegation機能

・Prefix Delegationは、ユーザサイトに対してprefixを委譲するための仕組みで、LAN側で使用するグローバルprefixをdesignatedルータに対して、通知することが出来ます。※information-onlyと併用することは出来ません。
・Designatedルータは、割り当てられたprefixの中から、ユーザが指定したprefixを、LAN配下のホストに対して、DHCPv6やルータ広告(RA)によって配布します（OCN IPv6サービスやNGNで使用します）。
・PDを受信すると、prefixの中から、ユーザが指定したprefix/lengthを生成し、インタフェースに対してIPv6アドレスを割り当てます(アドレス割り当てが有効な場合)。その後、生成したprefixを本装置配下のIPv6ホストに対して、RAによって広告することも可能です。

□ Information-only機能

・ステートレスDHCPv6で動作するモードです。DHCPv6 information-requestを送信し、DNSサーバやSNTPサーバetcの情報を取得します。
・本バージョンでは、受信した応答のうち、DNSサーバアドレスの情報(option:23)のみを参照し、他の情報（SNTPサーバアドレスetc）については無視します。
・ia-pdを設定している場合は、本機能を有効にすることは出来ません。

□ DHCPv6 client DUID

・DHCPv6でサーバに対して要求を行う際に使用するDUIDのフォーマットについて記します。
・本装置でサポートするDUIDは、RFC3315に準拠したフォーマットで、次の2つをサポートしています
※DUID-ENはサポートしていません。
DUID-LLT: Ethernet/bridge（仮想スイッチ）/VLAN以外で動作する場合に、使用する場合のフォーマットです。リンクレイヤーアドレスには、ethernet 0のHWアドレスを使用します。
DUID-LL: Ethernet/bridge（仮想スイッチ）/VLANで動作する場合に、使用するフォーマットです。

第43章 ipv6 dhcp-client mode

ipv6 dhcp-client mode

◆ **移行command**

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#ipv6 dhcp-client WORD
vxr-x86(config-dhcp6c)#
```

◆ **ia-pd** WORD

＜説　　明＞

・Identity Association for Prefix Delegation(IAPD)を有効にします（当該prefixに名前を付けて、prefixを取得します)。

＜書　　式＞　ia-pd WORD

＜　No　＞　no ia-pd

＜備　　考＞　インタフェース設定のprefix名と同じ名前を設定することは出来ません。
information-onlyが有効の場合は、本機能を設定することは出来ません。

◆ **rapid-commit**

＜説　　明＞　Rapid Commitオプション（初期値：無効）を有効にします。

＜書　　式＞　rapid-commit enable

＜　No　＞　no rapid-commit enable

＜備　　考＞

・有効の場合、2つのメッセージ（Solicit/Reply）でアドレスを取得します。

・無効の場合、通常通り4つのメッセージ（Solicit/Advertise/Request/Reply）でアドレスを取得します。

◆ **option-request dns-servers**

＜説　　明＞　Domain Name Serversオプションを有効にします。
DHCPv6サーバに対して、DNSサーバアドレスの通知を要求します。

＜書　　式＞　option-request dns-servers

＜初 期 値＞　no option-request dns-servers

＜　No　＞　no option-request dns-servers

◆ **option-request domain-name**

＜説　　明＞　Domain Seatch Listオプションを有効にします。
有効の場合、DHCPv6サーバに対してドメインサーチリストの通知を要求します。

＜書　　式＞　option-request domain-name

＜初 期 値＞　no option-request domain-name

＜　No　＞　no option-request dns-servers

ipv6 dhcp-client mode

◆ information-only enable
<説　　明>　information-only機能を有効にします。
<書　　式>　information-only enable
<　No　>　no information-only enable
<備　　考>
・ステートレスDHCPv6で動作するモードです。DHCPv6 information-requestを送信し、DNSサーバやSNTPサーバetcの情報を取得します。
・本バージョンでは、受信した応答のうち、DNSサーバアドレスの情報(option:23)のみを参照し、他の情報（SNTPサーバアドレスetc）については無視します。
・ia-pdを設定している場合は、本機能を有効にすることは出来ません。

□ 関連するコマンド
◇ ipv6 dhcp-client WORD
<説　　明>　ipv6 dhcp-client modeへ移行します。
<書　　式>　ipv6 dhcp-client WORD
<　no　>　no ipv6 dhcp-client WORD　（指定した設定を削除します）
<　mode　>　global mode

◇ show config ipv6 dhcp-client
<説　　明>　ipv6 dhcp-clientの設定を表示します。
<書　　式>　show config ipv6 dhcp-client (|WORD)
<　mode　>　view mode/global mode
<備　　考>　ipv6 dhcp-client WORDで設定した「WORD」を指定します。

◇ show ipv6 dhcp client pd
<説　　明>　ipv6 dhcp-clientのステータスを表示します。
<書　　式>　show ipv6 dhcp client pd WORD
<　mode　>　view mode
<備　　考>　WORDには、prefix名を指定します。

◇ show ipv6 dhcp client dns-servers
<説　　明>　option-request dns-serversで取得したDNSを表示します。
<書　　式>　show ipv6 dhcp client dns-servers WORD
<　mode　>　view mode
<備　　考>　WORDには、profile名（ipv6 dhcp-client WORD）を指定します。

◇ show ipv6 dhcp client domain-name
<説　　明>　option-request domain-nameで取得したdomain名を表示します。
<書　　式>　show ipv6 dhcp client domain-name WORD
<　mode　>　view mode
<備　　考>　WORDには、profile名（ipv6 dhcp-client WORD）を指定します。

第 44 章

l2tpv3 access-list mode

第44章 l2tpv3 access-list mode

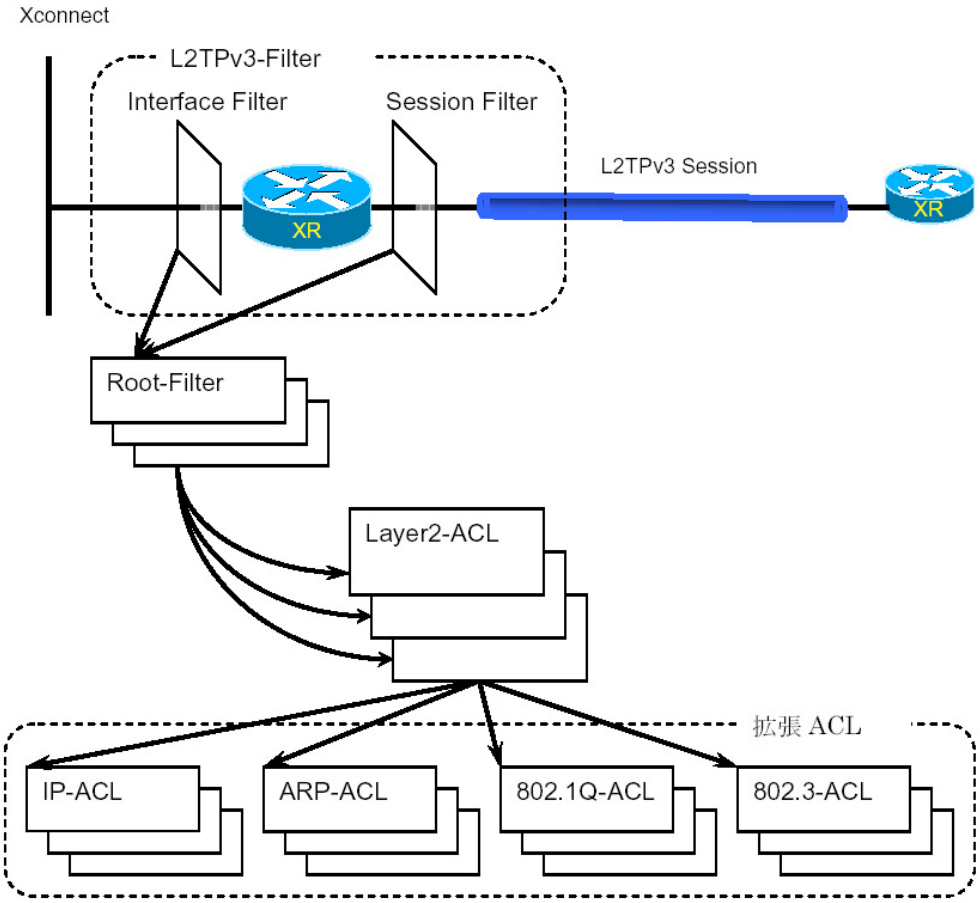
Ⅰ．L2TPv3フィルタリング機能

■ L2TPv3フィルタリング機能

・L2TPv3によりトンネリングされるフレームを、Xconnectインタフェース上、またはセッション上でフィルタリングすることが出来ます。
・フィルタリングの設定は、MACアドレスやIPv4、IPv6、ARP、802.1Q、TCP/UDPなど、レイヤー2からレイヤー4 での詳細な指定が可能です。
※L2TPv3 fast-forwarding機能を利用している場合、fast-forwardingのエントリーに登録済みのセッションに対してL2TPv3フィルタリングを設定しても、当該セッションが（タイムアウト等によって）エントリーから消えるまでは、フィルタリングは適用されません。

■ L2TPv3フィルタ設定概要

L2TPv3フィルタは、以下の要素から構成されています。



○Rootフィルタ
Rootフィルタは、配下にLayer2 ACLを持ち、検索する順に配置します。配下の全てのLayer2 ACLに一致しない場合の動作をdefaultポリシー(deny/permit)とします。

○Layer2 ACL
●Layer2 ACL
Layer2レベルでルールを記述します。配下に、extended ACLを持つことが出来ます。
●extended ACL（拡張ACL）
プロトコル毎に詳細なルールを記述することが出来ます。IP、IPv6、VLAN(IEEE 802.1Q)、ARP、IEEE 802.3の各プロトコルに対応しています。

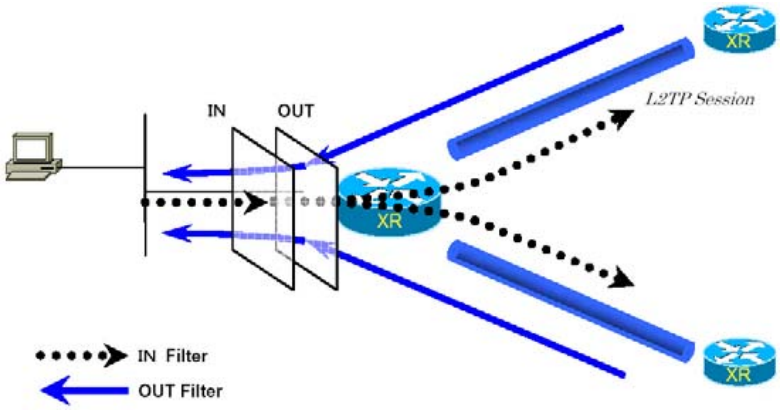
■ L2TPv3フィルタ設定概要(続き)

○L2TPv3フィルタ

Xconnectインタフェース、およびセッションに適用するrootフィルタを設定します。
フィルタリング可能な位置は、以下の4ヶ所です。

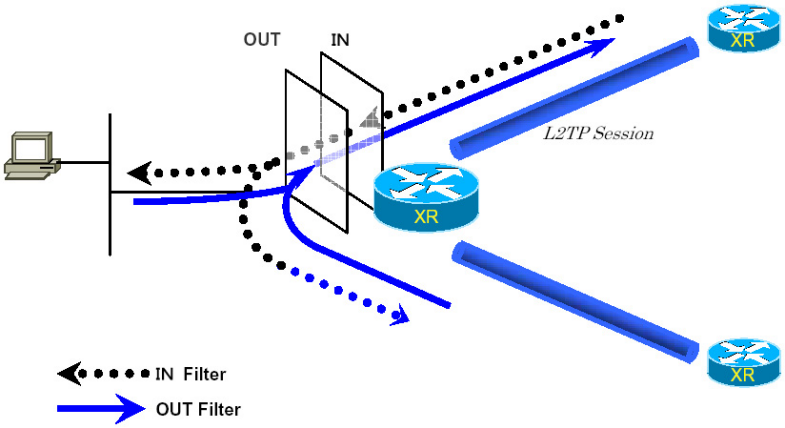
●Xconnectインタフェースで受信する場合
●Xconnectインタフェースへ送信する場合

＜書　　式＞　　l2tpv3 access-group (in|out) WORD
＜　no　＞　　no l2tpv3 access-group (in|out)
＜ mode ＞　　interface mode
＜備　　考＞
・WORD： rootのACL名（l2tpv3 access-list WORD root にて設定します）を指定します。
・in:　Xconnect インタフェース→セッション（本装置への入力）方向のフィルタを適用します。
・out:　セッション→ Xconnect インタフェース（本装置からの出力）方向のフィルタを適用します。



●L2TPv3セッションにより転送される（受信する）場合
●L2TPv3セッションにより転送する（送信する）場合

＜書　　式＞　　l2tpv3 access-group (in|out) WORD
＜　no　＞　　no l2tpv3 access-group (in|out)
＜ mode ＞　　l2tpv3 xconnect mode
＜備　　考＞
・WORD：rootのACL名（l2tpv3 access-list WORD root にて設定します）を指定します。
・in:　受信方向のセッションに対して、フィルタを適用します。
・out:　送信方向のセッションに対して、フィルタを適用します。



第44章 l2tpv3 access-list mode

Ⅰ．L2TPv3フィルタリング機能

■ L2TPv3フィルタの動作（ポリシー）

○deny（破棄）

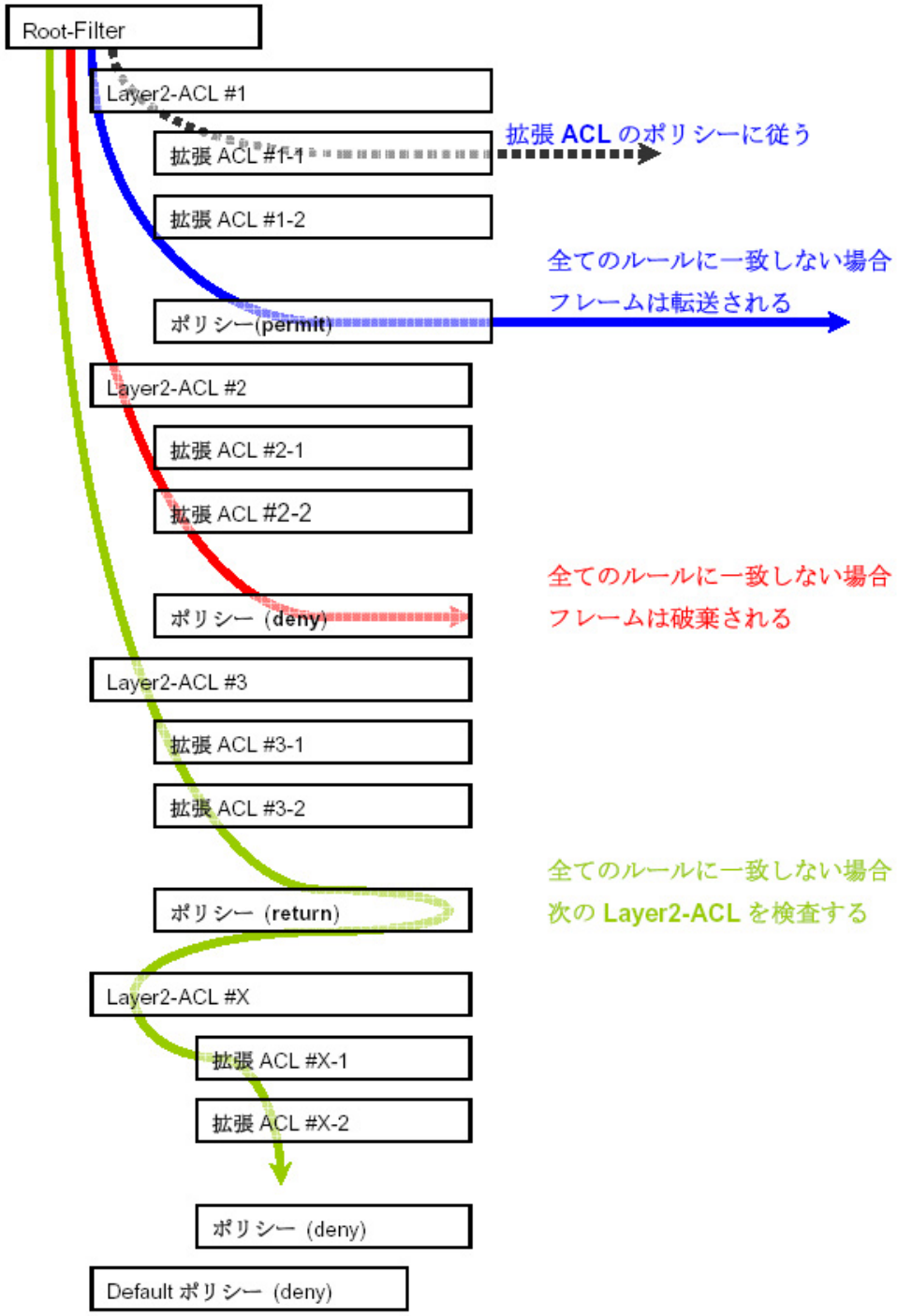
フィルタルールに一致する場合、検索を中止してフレームを転送します。

○permit（許可）

フィルタルールに一致する場合、検索を中止してフレームを破棄します。

○return（復帰）

フィルタルールに一致しない場合、該当layer2 ACLでの検索を中止して、 呼び出し元の次のlayer2 ACLから検索を再開します。



第 44 章 l2tpv3 access-list mode

Ⅰ．L2TPv3 フィルタリング機能

■ L2TPv3 フィルタの評価

root フィルタの配下に設定された layer2 ACL を、上から順に検索し、最初に条件に一致（1st マッチ）する ACL に対して、以下の評価を行います。
すべての layer2 ACL に一致しない場合は、当該 root ACL の default ポリシー（deny/permit）に従います。

● extended ACL がない場合
当該 layer2 ACL のポリシー（deny/permit/return）に従います。

● extended ACL がある場合
Layer2 ACL 配下の extended ACL を、1st マッチにて検索し、以下の評価を行います。
・extended ACL に一致する場合、当該 ACL のポリシー（deny/permit）に従います。
・すべての extended ACL に一致しない場合、当該 layer2 ACL のポリシー(deny/permit/return）に従います。

■ L2TPv3 フィルタの処理順序

・Known Unicast のフレームが、転送禁止状態の場合は、permit 条件に一致しても、フレームを転送しません。
・Circuit Down により転送禁止状態の場合は、permit 条件に一致しても、フレームを転送しません。

■ L2TPv3 フィルタの表示

＜説　　明＞　L2TPv3 アクセスリストを表示します。
＜書　　式＞　show l2tpv3 access-list
　　show l2tpv3 access-list interface (|INTERFACE)
　　show l2tpv3 access-list xconnect (|<1-4294967295>)
　　show l2tpv3 access-list (root|layer2|ip|ipv6|arp|vlan|ieee802-3) (|WORD)
　　show l2tpv3 access-list detail (root|layer2|vlan) (|WORD)
　　show l2tpv3 access-list detail root WORD layer2 WORD
＜　mode　＞　view mode

■ L2TPv3 フィルタのクリア

＜説　　明＞　L2TPv3 アクセスリストのカウンターをクリアします。
＜書　　式＞
　　clear l2tpv3 counter access-list
　　clear l2tpv3 counter access-list interface (|INTERFACE)
　　clear l2tpv3 counter access-list xconnect (|<1-4294967295>)
　　clear l2tpv3 counter access-list (root|layer2|ip|ipv6|arp|vlan|ieee802-3) (|WORD)
　　clear l2tpv3 counter access-list detail (root|layer2|vlan) (|WORD)
＜　mode　＞　view mode

第44章 l2tpv3 access-list mode

II . Root ACL

◆ 移行command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#l2tpv3 access-list WORD root (deny|permit)
vxr-x86(config-l2tpv3-acl)#
```

＜説　　明＞

・Root ACLのACL名(WORD)およびdefaultポリシー(deny|permit)を設定（または指定）して、root ACLのl2tpv3 access-list modeに移行します。

＜備　　考＞

・既に設定済のACLで、deny/permitが異なる場合は、mode移行できません。

・同一ACL名を設定することはできません（root，layer2，extended ip/ipv6/vlan/arp/ieee802-3が異なる場合でも、同じACL名はエラーとして扱います)。

・root ACLの最大設定数は、512個です。

◆ layer2 access-list

＜説　　明＞　当該root ACLの配下に配置するlayer2 ACLを設定します。
　　WORDには、layer2 ACLのACL名を指定します。

＜書　　式＞　layer2 access-list WORD <1-256>

＜　No　＞　no layer2 access-list　　(すべてのACLを削除します)
　　no layer2 access-list WORD　(指定したACLを削除します)

＜備　　考＞　1つのroot配下に、32個までのlayer2 ACLを設定することが出来ます。
　　本装置全体で、設定可能なlayer2 ACLの総数は、4096個です。

第44章 l2tpv3 access-list mode

III . Layer2 ACL

◆ **移行 command**

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#l2tpv3 access-list WORD layer2 (deny|permit|return)
vxr-x86(config-l2tpv3-acl)#
```

＜説　　明＞
・Layer2 ACL の ACL 名(WORD)および default ポリシー(deny|permit|return)を設定（または指定）して、layer2 ACL の l2tpv3 access-list mode に移行します。
＜備　　考＞
・既に設定済の ACL で、deny/permit/return が異なる場合は、mode 移行できません。
・同一 ACL 名を設定することはできません（root，layer2，extended ip/ipv6/vlan/arp/ieee802-3 が異なる場合でも、同じ ACL 名はエラーとして扱います）。
・Layer2 ACL の最大設定数は、128 個です。

◆ **mac source**

＜説　　明＞　マッチ条件に送信元 MAC アドレスを設定します。
＜書　　式＞　mac source HH:HH:HH:HH:HH:HH(/MM:MM:MM:MM:MM:MM)
＜　No　＞　no mac source HH:HH:HH:HH:HH:HH(/MM:MM:MM:MM:MM:MM)
＜備　　考＞
・例えば、ワイルドカードで「00:80:6D:**:**:**」を指定する場合は、次のように設定します。
mac source 00:80:6D:00:00:00/FF:FF:FF:00:00:00

◆ **mac destination**

＜説　　明＞　マッチ条件に送信先 MAC アドレスを設定します。
＜書　　式＞　mac destination HH:HH:HH:HH:HH:HH(/MM:MM:MM:MM:MM:MM)
＜　No　＞　no mac destination HH:HH:HH:HH:HH:HH(/MM:MM:MM:MM:MM:MM)
＜備　　考＞
・例えば、ワイルドカードで「00:80:6D:**:**:**」を指定する場合は、次のように設定します。
mac destination 00:80:6D:00:00:00/FF:FF:FF:00:00:00

◆ **ethernet-type**

＜説　　明＞　ethernet-type と extended ACL を設定します。
WORD には、extended ACL の ACL 名を指定します。
＜書　　式＞　ethernet-type (ip|ipv6|arp|vlan|ieee802-3) (|extended WORD <1-256>)
ethernet-type <1536-65535>
＜　No　＞　no ethernet-type (ip|ipv6|arp|vlan|ieee802-3) extended (|WORD)
(extended のみ削除します。)
no ethernet-type
(ethernet-type とすべての extended を削除します。)
＜備　　考＞　extended ACL は、最大 32 個まで設定することが出来ます。

第44章 l2tpv3 access-list mode

Ⅳ. Extended IP ACL

◆ **移行command**

vxr-x86#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
vxr-x86(config)#**l2tpv3 access-list WORD extended ip (deny|permit)**
vxr-x86(config-l2tpv3-eacl)#
＜説　　明＞
・Extended IP ACLのACL名(WORD)およびdefaultポリシー(deny|permit)を設定（または指定）して、
 extended IP ACLのl2tpv3 access-list modeに移行します。
＜備　　考＞
・既に設定済のACLで、deny/permitが異なる場合は、mode移行できません。
・同一ACL名を設定することはできません（root，layer2，extended ip/ipv6/vlan/arp/ieee802-3が異
  なる場合でも、同じACL名はエラーとして扱います)。
・Extended IP ACLの最大設定数は、128個です。

◆ **source**

＜説　　明＞　マッチ条件に、送信元IPアドレスを設定します。
＜書　　式＞　source (A.B.C.D | A.B.C.D/M)
＜　No　＞　no source

◆ **destination**

＜説　　明＞　マッチ条件に、送信先IPアドレスを設定します。
＜書　　式＞　destination (A.B.C.D | A.B.C.D/M)
＜　No　＞　no destination

◆ **tos**

＜説　　明＞　マッチ条件に、tosを設定します。
＜書　　式＞　tos <0-255>
＜　No　＞　no tos

◆ **protocol**

＜説　　明＞　マッチ条件に、protocolを設定します。
＜書　　式＞　protocol (<0-255> | icmp | tcp | udp)
＜　No　＞　no protocol
＜備　　考＞
・source-port（またはdestination-port）が設定済の場合、protocol <0-255>|icmpは設定出来ません。

◆ source-port
＜説　　明＞　マッチ条件に、source portを設定します。
＜書　　式＞　source-port (<1-65535> | range <1-65535> <1-65535>)
＜　No　＞　no source-port
＜備　　考＞　protocol udp（またはtcp）の場合に、設定することが出来ます。

◆ destination-port
＜説　　明＞　マッチ条件に、destination portを設定します。
＜書　　式＞　destination-port (<1-65535> | range <1-65535> <1-65535>)
＜　No　＞　no destination-port
＜備　　考＞　protocol udp（またはtcp）の場合に、設定することが出来ます。

◆ icmp
＜説　　明＞　マッチ条件に、icmp type/codeを設定します。
＜書　　式＞　icmp <0-255> (|<0-255>)
＜　No　＞　no icmp
＜備　　考＞　protocol icmpを設定済の場合に、設定することが出来ます。

第44章 l2tpv3 access-list mode

V . Extended IPv6 ACL

◆ **移行command**

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#l2tpv3 access-list WORD extended ipv6 (deny|permit)
vxr-x86(config-l2tpv3-eacl)#
```

＜説　　明＞
・Extended IPv6 ACLのACL名(WORD)およびdefaultポリシー(deny|permit)を設定（または指定）して、extended IPv6 ACLのl2tpv3 access-list modeに移行します。
＜備　　考＞
・既に設定済のACLで、deny/permitが異なる場合は、mode移行できません。
・同一ACL名を設定することはできません（root，layer2，extended ip/ipv6/vlan/arp/ieee802-3が異なる場合でも、同じACL名はエラーとして扱います）。
・Extended IPv6 ACLの最大設定数は、128個です。

◆ **source**

＜説　　明＞　マッチ条件に、送信元IPv6アドレスを設定します。
＜書　　式＞　source (X:X::X:X | X:X::X:X/M)
＜　No　＞　no source

◆ **destination**

＜説　　明＞　マッチ条件に、送信先IPv6アドレスを設定します。
＜書　　式＞　destination (X:X::X:X | X:X::X:X/M)
＜　No　＞　no destination

◆ **protocol**

＜説　　明＞　マッチ条件に、protocolを設定します。
＜書　　式＞　protocol　(<0-255> | icmpv6 | tcp | udp)
＜　No　＞　no protocol
＜備　　考＞
・source-port（またはdestination-port）が設定済の場合、protocol <0-255>|icmpv6を設定することは出来ません。

◆ **source-port**

＜説　　明＞　マッチ条件に、source portを設定します。
＜書　　式＞　source-port　(<1-65535> | range <1-65535> <1-65535>)
＜　No　＞　no source-port
＜備　　考＞　protocol udp（またはtcp）の場合に、設定することが出来ます。

◆ **destination-port**

＜説　　明＞　マッチ条件に、destination portを設定します。
＜書　　式＞　destination-port (<1-65535> | range <1-65535> <1-65535>)
＜　No　＞　no destination-port
＜備　　考＞　protocol udp（またはtcp）の場合に、設定することが出来ます。

第44章 l2tpv3 access-list mode

VI . Extended VLAN ACL

◆ 移行 command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#l2tpv3 access-list WORD extended vlan (deny|permit)
vxr-x86(config-l2tpv3-eacl)#
```

＜説　　明＞

・Extended VLAN ACL の ACL 名(WORD)および default ポリシー(deny|permit)を設定（または指定）して、extended VLAN ACL の l2tpv3 access-list mode に移行します。

＜備　　考＞

・既に設定済の ACL で、deny/permit が異なる場合は、mode 移行できません。

・同一 ACL 名を設定することはできません（root，layer2，extended ip/ipv6/vlan/arp/ieee802-3 が異なる場合でも、同じ ACL 名はエラーとして扱います)。

・Extended VLAN ACL の最大設定数は、128 個です。

◆ vlan-id

＜説　　明＞　マッチ条件に、VLAN ID を設定します。

＜書　　式＞　vlan-id <0-4095>

＜　No　＞　no vlan-id

◆ priority

＜説　　明＞　マッチ条件に、priority を設定します。

＜書　　式＞　priority <0-7>

＜　No　＞　no priority

◆ ethernet-type

＜説　　明＞　マッチ条件に、ethernet-type を設定します。

＜書　　式＞　ethernet-type (ip|ipv6|arp) (|extended WORD <1-256>)
　　ethernet-type (vlan|<1536-65535>)

＜　No　＞　no ethernet-type (ip|ipv6|arp) extended (|WORD)
　　(extended のみ削除します。)
　　no ethernet-type
　　(ethernet-type とすべての extended を削除します。)

＜備　　考＞

・extended WORD が設定済の場合は、異なる ethernet-type を設定することは出来ません。

・extended WORD で指定する ACL 名は、l2tpv3 access-list WORD extended の ACL 名です。

・extended ACL の最大設定数は、32 です。

第44章 l2tpv3 access-list mode

Ⅶ. Extended ARP ACL

◆ 移行command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#l2tpv3 access-list WORD extended arp (deny|permit)
vxr-x86(config-l2tpv3-eacl)#
```

＜説　　明＞
・Extended ARP ACLのACL名(WORD)およびdefaultポリシー(deny|permit)を設定（または指定）して、extended ARP ACLのl2tpv3 access-list modeに移行します。
＜備　　考＞
・既に設定済のACLで、deny/permitが異なる場合は、mode移行できません。
・同一ACL名を設定することはできません（root，layer2，extended ip/ipv6/vlan/arp/ieee802-3が異なる場合でも、同じACL名はエラーとして扱います）。
・Extended ARP ACLの最大設定数は、128個です。

◆ opcode

＜説　　明＞　マッチ条件に、opcodeを指定します。
＜書　　式＞　opcode (<0-65535> | request | reply)
＜　No　＞　no opcode

◆ sender-mac

＜説　　明＞　マッチ条件に、送信元MACアドレスを指定します。
＜書　　式＞　sender-mac HH:HH:HH:HH:HH:HH(/MM:MM:MM:MM:MM:MM)
＜　No　＞　no sender-mac
＜備　　考＞
・例えば、ワイルドカードで「00:80:6D:**:**:**」を指定する場合は、次のように設定します。
sender-mac 00:80:6D:00:00:00/FF:FF:FF:00:00:00

◆ target-mac

＜説　　明＞　マッチ条件に、送信先MACアドレスを指定します。
＜書　　式＞　target-mac HH:HH:HH:HH:HH:HH(/MM:MM:MM:MM:MM:MM)
＜　No　＞　no target-mac
＜備　　考＞
・例えば、ワイルドカードで「00:80:6D:**:**:**」を指定する場合は、次のように設定します。
target-mac 00:80:6D:00:00:00/FF:FF:FF:00:00:00

◆ sender-ip

＜説　　明＞　マッチ条件に、送信元IPアドレスを指定します。
＜書　　式＞　sender-ip (A.B.C.D|A.B.C.D/M)
＜　No　＞　no sender-ip

◆ target-ip

＜説　　明＞　マッチ条件に、送信先IPアドレスを指定します。
＜書　　式＞　target-ip (A.B.C.D|A.B.C.D/M)
＜　No　＞　no target-ip

第44章 l2tpv3 access-list mode

Ⅷ. Extended IEEE802.3 ACL

◆ **移行 command**

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#l2tpv3 access-list WORD extended ieee802-3 (deny|permit)
vxr-x86(config-l2tpv3-eacl)#
```

＜説　　明＞

・Extended IEEE802.3 ACL の ACL 名(WORD)および default ポリシー(deny|permit)を設定（または指定）して、extended IEEE802.3 ACL の l2tpv3 access-list mode に移行します。

＜備　　考＞

・既に設定済の ACL で、deny/permit が異なる場合は、mode 移行できません。

・同一 ACL 名を設定することはできません（root，layer2，extended ip/ipv6/vlan/arp/ieee802-3 が異なる場合でも、同じ ACL 名はエラーとして扱います)。

・Extended IEEE802.3 ACL の最大設定数は、128 個です。

◆ **llc-sap**

＜説　　明＞　マッチ条件に、LLC SAP を指定します。

＜書　　式＞　llc-sap <0-255>

＜　No　＞　no llc-sap

＜備　　考＞　snap-type が設定済の場合は、llc-sap を設定することは出来ません。

◆ **snap-type**

＜説　　明＞　マッチ条件に、SNAP タイプを指定します。

＜書　　式＞　snap-type <1536-65535>

＜　No　＞　no snap-type

＜備　　考＞　llc-sap が設定済の場合は、snap-type を設定することは出来ません。

第 45 章

address-family ipv6 mode

第45章 address-family ipv6 mode

address-family ipv6 mode

◆ **移行command**

```
vxr-x86#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
vxr-x86(config)#router bgp <1-65535>
vxr-x86(config-router)#address-family ipv6
vxr-x86(config-router-af)#
```

＜説　　明＞　BGP peerにadvertiseするネットワークを指定します。
＜書　　式＞　network X:X::X:X/M (|backdoor)
＜　No　＞　no network X:X::X:X/M (|backdoor)
＜備　　考＞
・default information(::/0)を指定することも出来ます。
・default-information-checkが無効の場合に、network ::/0とneighbor default-originateを同時に設定すると、複数のdefaultルート情報がインストールされることにより、不要なupdateを送信してしまいます。そのため、両者を同時に設定することは推奨しません。
・特定のBGPルートを優先経路にしたくない場合、受け取ったBGPルートにローカルBGPのadministrative distanceを設定することで、優先順位を下げて、他のルートを優先させることが出来ます。

＜説　　明＞　Address family ondeから、exitします。
＜書　　式＞　exit-address-family
＜備　　考＞　show config形式の設定をcopy & pasteするときに使用するためのコマンドです。
通常設定時は、exitで本モードから抜けます。

＜説　　明＞
・Aggregate機能を使うと、BGPルートの集約を行うことが出来る集約ルートを構成するルートが、BGPテーブル内に少なくとも一つでも存在する場合に、集約ルートを作成しadvertise します。
＜書　　式＞　aggregate-address X:X::X:X/M (|summary-only) (|as-set)
＜備　　考＞
・Aggregate 機能では、集約ルートと一緒に集約前のルートもadvertise します。集約ルートのみadvertiseする場合は、summary-only を設定します。
・ルートのaggregate 設定を行った場合、ASパス情報が失われます。これによって、同じAS に新しいルートとして受け取られてしまい、ルーティングループを引き起こす可能性があります。as-setを設定すると、ルート集約時にAS セット情報を含む形で広告することが可能になります。なお、この場合のAS セット集合は、順序不同でリストされたものです。

address-family ipv6 mode

■ neighbor

○ activate

＜説　　明＞
・本機能を有効（activate）にすると、ipv4 neighbor 間および ipv6 neighbor 間で、ipv6 network を advertise します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) activate　　（有効）
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) activate　　（無効）
＜備　　考＞　activate を最初に設定します。

○ default-originate

＜説　　明＞　default-originate が有効の場合、BGP により default ルートを配信します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) default-originate　　（有効）
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) default-originate　（無効）
＜備　　考＞
・default-originate 無効：default ルートを配信しません。
・default-originate 有効＆ default-import-check 無効：BGP により default ルートを配信します。
・default-originate 有効＆ default-import-check 有効：
default ルートを保持している場合は、default ルートを配信します。
default ルートを保持していない場合は、default ルートを配信しません。

○ distribute-list

＜説　　明＞
・peer に送信、または peer から受信するルート update のフィルタリングを行う場合に設定します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) distribute-list ACL-NAME (in|out)
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) distribute-list ACL-NAME (in|out)
＜備　　考＞　in を指定すると、peer から受信するルート update をフィルタリングします。
out を指定すると、peer へ送信するルート update をフィルタリングします。

○ filter-list

＜説　　明＞　指定した AS にマッチするルート情報をフィルタリングします。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) filter-list ACL-NAME
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) filter-list ACL-NAME
＜備　　考＞　ip as-path access-list で設定した ACL-NAME を指定します。
in を指定すると、受信時にフィルタリングします。
out を指定すると、送信時にフィルタリングします。

○ next-hop-self

＜説　　明＞
・有効の場合、eBGP ルートを iBGP peer へ送信する nexthop 情報を、peer のルータとの通信に使用するインタフェースのアドレスに変更します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) next-hop-self
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) next-hop-self
＜備　　考＞
・無効の場合、iBGP peer へ送信する nexthop 情報を、eBGP から貰った時のまま送信します。

address-family ipv6 mode

○ remove-private-as
＜説　　明＞
・remove-private-as を指定すると、private AS 番号を削除して、経路情報を advertise します。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) remove-private-as
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) remove-private-as

○ route-map
＜説　　明＞
・Peer に送信、または peer から受信するルートのフィルタリング や属性の操作をすることが出来ます。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) route-map WORD (in|out)
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) route-map WORD (in|out)
＜備　　考＞
・WORD には、route-map 名を指定します。
・neighbor 毎に、in/out それぞれ 1 つの route-map を適用することができます。
・設定可能な属性や match 条件については、「第 29 章 route-map mode」を参照してください。

○ soft-reconfiguration
＜説　　明＞
・BGP の neighbor パラメータや route-map の設定を変更した場合、その変更を適用するには、BGP セッションのクリア、もしくは BGP サービスの再起動が必要になります。
・本機能を有効にすることによって、neighbor とのセッションを維持したまま変更を適用することが出来ます（soft clear によって、BGP セッションのクリアを行います）。
＜書　　式＞　neighbor (A.B.C.D|X:X::X:X) soft-reconfiguration inbound
＜　no　＞　no neighbor (A.B.C.D|X:X::X:X) soft-reconfiguration inbound

■ redistribute

○ redistribute (connected|static)
＜説　　明＞　connected route、static route を BGP で再配信する機能です。
　　Default ルート情報も再配信します。
＜書　　式＞　redistribute (connected|static)
＜　no　＞　no redistribute (connected|static)

○ redistribute (connected|static) route-map ABCD
＜説　　明＞　routemap 機能を適用することにより、再配信時に特定の prefix のみを配信したり、特定の prefix を拒否したりすることができます。
＜書　　式＞　redistribute (connected|static) route-map ABCD
＜　no　＞　no redistribute (connected|static) route-map ABCD

第 46 章

interface tap mode

interface tap mode

◆ 移行command

```
vxr-x86#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
wxr250(config)#interface tap <0-127>
wxr250(config-tap)#
```

◆ l2tpv3 access-group

＜説　　明＞　Xconnect インタフェースでの送受信に対して、l2tpv3 access-list を適用します。
＜書　　式＞　l2tpv3 access-group (in|out) WORD
＜　No　＞　no l2tpv3 access-group (in|out)
＜備　　考＞
・WORD： root のACL 名を指定します。
（root のACL 名は、global モードの l2tpv3 access-list WORD root にて設定します。）
・in: Xconnect インタフェース→セッション（本装置への入力）方向のフィルタを適用します。
・out: セッション→ Xconnect インタフェース（本装置からの出力）方向のフィルタを適用します。

◆ bridge-group

＜説　　明＞　インタフェースを bridge-group（仮想スイッチグループ）に参加させます。
＜書　　式＞　bridge-group <0-4095> (port <1-128>|)
＜　No　＞　no bridge-group
＜備　　考＞　bridge-group が未設定（interface bridge が未設定）の場合、join に失敗します。

第 47 章

LXC container mode

LXC container mode

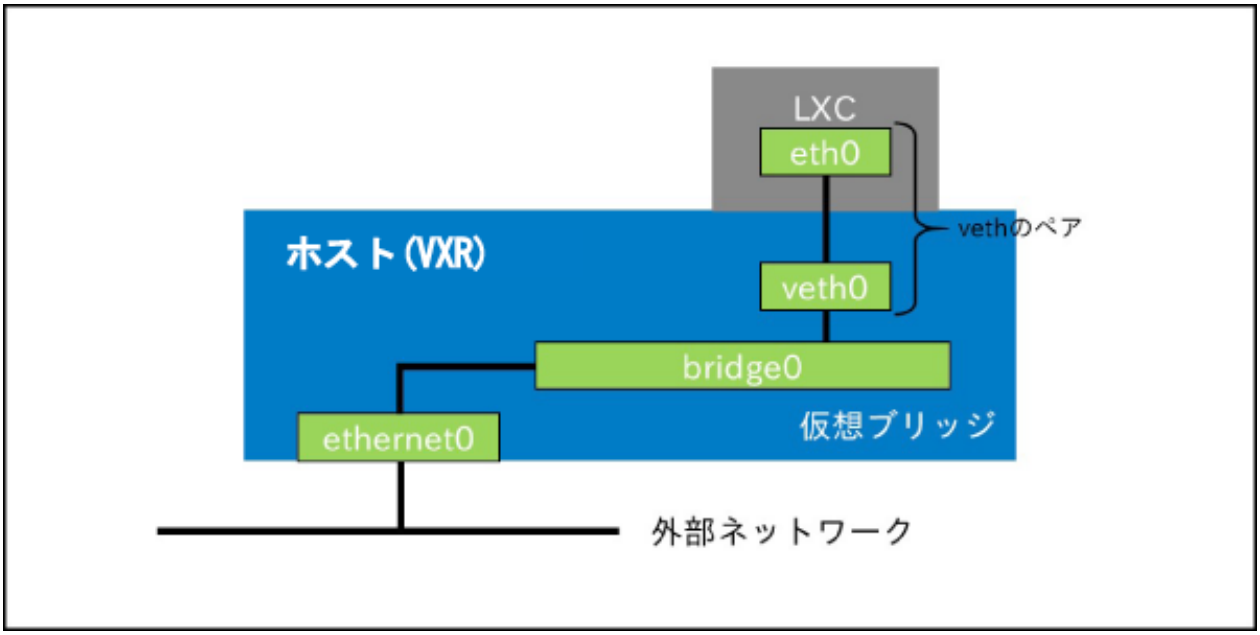
■ コンテナ型仮想化

コンテナ型仮想化（以下LXC）機能は、仮想化技術の一つで、この機能を利用することにより、LXC内に作成したIPソケットアプリケーションから、ルーティングやIPsec VPNなどのルータ機能を利用できるようになります。

・コンテナ型仮想化技術として、LXCに対応しています。コンテナイメージは、弊社HPよりダウンロードしてください。
・起動可能なコンテナは、1つです。
・コンテナと本装置（ホスト）は、vethインタフェース経由で通信することが出来ます。
※LXCを使用した場合の故障、誤動作、不具合等については、当社は一切その責任を負いかねますのであらかじめご了承ください。

■ ネットワーク構成

LXCはホスト（本装置）上のブリッジを介して、外部と通信することが出来ます。仮想インタフェース（veth）を使用して、LXC内部のネットワークと本装置のブリッジを接続します。



LXC container mode

◆ 移行command

```
vxr-x86#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
vxr-x86(config)#lxc container <1-1>
vxr-x86(config-lxc)#
```

■ 本装置の設定例（LXC）

```
vxr-x86#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

・LXCコンテナを設定します。

```
vxr-x86(config)#lxc container 1
vxr-x86(config-lxc)#exit
```

・veth0インタフェースを設定します。

```
vxr-x86(config)#interface veth 0
```

・lxc container 1との仮想ブリッジを設定します。

```
vxr-x86(config-veth)#lxc-link 1
vxr-x86(config-veth)#exit
```

・Bridge0インタフェースのIPアドレスを設定します。

```
vxr-x86(config)#interface bridge 0
vxr-x86(config-bridge)#ip address 192.168.10.1/24
```

・ethernet0とveth0を、bridge-group 0に参加させます。

```
vxr-x86(config)#interface ethernet 0
vxr-x86(config-if)#bridge-group 0 port 1
vxr-x86(config-if)#exit
vxr-x86(config)#interface veth 0
vxr-x86(config-veth)#bridge-group 0 port 2
vxr-x86(config-veth)#exit
vxr-x86(config)#exit
vxr-x86#save config
```

LXC container mode

■ LXC コンソール接続・切断

ここでは、本装置の CLI から LXC のコンソールに接続する方法、および切断方法について説明します。

◆ lxc-link

＜説　　明＞　LXC のコンソールに接続します。
＜書　　式＞　connect lxc console 1
＜　mode　＞　view mode
＜備　　考＞　アカウント：ubuntu、初期パスワード：ubuntu でログインします。
　　Ctrl+b q で、LXC コンソールを exit できます。

■ LXC のネットワーク設定

・LXC の eth0 インタフェースは、ホストの veth0 インタフェースと仮想的にペアリングされています。外部と通信するためには、ホストの bridge0 インタフェースと同じネットワークアドレスを設定します。
・LXC の IP アドレスなどのネットワーク設定は /etc/network/interfaces ファイルを編集して行います。編集には vim(※)等のコマンドを利用することができます。
　※ vim コマンドの利用方法は、下記サイトなどを参考にしてください。
　　https://help.ubuntu.com/community/VimHowto
・LXC には、vimtutor コマンドがインストールされており、このコマンドを実行することで vim の使い方を確認することができます。

＜　例　＞
・以下に、LXC のネットワーク設定例を示します。

```
$sudo vim /etc/network/interfaces
auto lo
iface lo inet loopbackauto eth0
iface eth0 inet static
address 192.168.10.10
netmask 255.255.255.0
network 192.168.10.0
broadcast 192.168.10.255
gateway 192.168.10.1
dns-nameservers 192.168.10.1
```

・IP アドレス設定後は、設定を反映するために以下のコマンドを実行します。

```
$sudo ifdown eth0 && sudo ifup eth0
```

第 48 章

interface veth mode

第 47 章 interface veth mode

interface veth mode

◆ 移行 command

```
nxrg100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
vxr-x86(config)#interface veth <0-0>
vxr-x86(config-veth)#
```

＜説　　明＞

・Virtual ethernet pair(veth) interface は、コンテナ型仮想化との IP 通信を行う際に使用するインタフェースです。
・ホスト側（veth）とコンテナ側で使用するインタフェース（vethX-ct）がそれぞれ作成されます。
1 対 1 で接続されているため、容易に本装置とコンテナ間の通信が可能になっています。
・コンテナに入れられたインタフェース（vethX-ct）は、ホスト側（本装置）で使用することは出来ません。

◆ descripton

＜説　　明＞　インタフェースの説明を記述します。
＜書　　式＞　description DESCRIPTION
＜　No　＞　no description (|DESCRIPTION)

◆ ip address

＜説　　明＞　インタフェースに IP アドレスを付与します。
＜書　　式＞　ip address A.B.C.D/M (|secondary)
＜　No　＞　no ip address (|A.B.C.D/M) (|secondary)

◆ lxc-link

＜説　　明＞　lxc-link の設定を行います。
＜書　　式＞　lxc-link <1-1>
＜　No　＞　no lxc-link
＜備　　考＞　lxc-link 設定後、lxc 内部の eth0 と veth0 間で通信が可能になります。

◆veth hw-address

＜説　　明＞　veth interface の HW address を設定します。
＜書　　式＞　veth hw-address <HH:HH:HH:HH:HH:HH>
＜備　　考＞　hw-address の設定がない場合は、random 値が設定されます。
設定した HW address を削除する場合は、veth interface の削除が必要です。

◆bridge-group

＜説　　明＞　インタフェースを、bridge-group（仮想スイッチグループ）に参加させます。
＜書　　式＞　bridge-group <0-4095> (port <1-128>|)
＜　No　＞　no bridge-group
＜備　　考＞　bridge-group が未設定（interface bridge が未設定）の場合、join に失敗します。

第 49 章

ssl tunnel mode

ssl tunnel mode

■ SSL Tunnel

・SSL（Secure Socket Layer）は、データを暗号化して送受信を可能とするプロトコルです。SSL tunnel を利用することによって、SSL 非対応の既存の TCP 通信を、暗号化（SSL 化）することが出来ます。
・本バージョンでは、SMTP の SSL 化に対応しています。

◆ 移行 command

```
nxrg100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
vxr-x86(config)#ssl tunnel <0-2>
vxr-x86(config-ssl-tunnel)#
```

◆ descripton

＜説　　明＞　インタフェースの説明を記述します。
＜書　　式＞　description DESCRIPTION
＜　No　＞　no description (|DESCRIPTION)

◆ version

＜説　　明＞　バージョンを指定します。
　　Default では、すべてのバージョンに対応します。
＜書　　式＞　version (tlsv10|tlsv11|tlsv12)
＜　No　＞　no version
＜備　　考＞
・対応する SSL/TLS バージョンは、以下のとおりです（SSL v2.0/v3.0 には未対応です。）。

tlsv10	TLS version 1.0
tlsv11	TLS version 1.1
tlsv12	TLS version 1.2

◆ set protocol

＜説　　明＞　プロトコルを指定します。
＜書　　式＞　set protocol smtp
＜　No　＞　no set protocol smtp
＜備　　考＞　本バージョンで指定可能なプロトコルは SMTP です。

◆ remote address

＜説　　明＞　SSL tunnel の接続先(または転送先)アドレス、および TCP ポート番号を指定します。
＜書　　式＞　remote address ip (A.B.C.D|FQDN) port <1-65535>

ssl tunnel mode

◆ listen address

＜説　　明＞

・クライアントの場合、SSL化するパケットを受信するアドレスとポート番号を指定します。

・サーバの場合、SSLパケットの受信アドレスとポート番号を指定します。

＜書　　式＞　listen address ip localhost port <1-65535>

・本バージョンでは、アドレスに、localhostを指定します。

・localhostを指定した場合、以下のTCPポート番号を指定することは出来ません。

9696，4001，4002，2600，3001

付録 A

Packet Traveling

付録 A

Packet Traveling

1. IP filteringの優先順位

INPUT/OUTPUT/FORWARD時のfilteringが適用される順番は、以下のとおりです。IPsec input/output policy checkは、実際にSPD(Security Policy Database)を検索するわけではなく、ESP化されてきたパケット/ESP化するべきパケットの判断のみを行い、この判定にmatchしたパケットが許可されます。

○ INPUT

(1) invalid-status-drop filter
- invalid-status-drop in filter(SYSTEM)
- invalid-status-drop in filter(interface別)

(2) SYSTEM filter
- TCP connection数制限

(3) IPsec input policy check
- IPsec ESP化されてきたものは許可します。

(4) USER input filtering

(5) SPI check

(6) Service用filter(GUIアクセス用filterなど)

○ FORWARD

(1) invalid-status-drop filter
- invalid-status-drop filter(SYSTEM)
- invalid-status-drop forward-in filter(interface別)
- invalid-status-drop forward-out filter(interface別)

(2) SYSTEM filter
- Session limit

(3) IPsec input/output policy check
- IPsec ESP化されてきたものか、outbound policyにmatchするものは許可します。

(4) UPNP filtering

(5) USER forward in/out filtering

(6) SPI(input/forward時のみ)

(7) Web認証用forward in/out filtering

○ OUTPUT

(1) IPsec output policy check

(2) IPsec outbound policyにmatchするものは許可します。

(3) USER output filtering

2. NAT の優先順位

NAT の適用順位は、以下のとおりです。

◯ INPUT

(1) SYSTEM DNAT
(2) UPNP 用 DNAT
(3) USER 設定 DNAT(Static NAT)

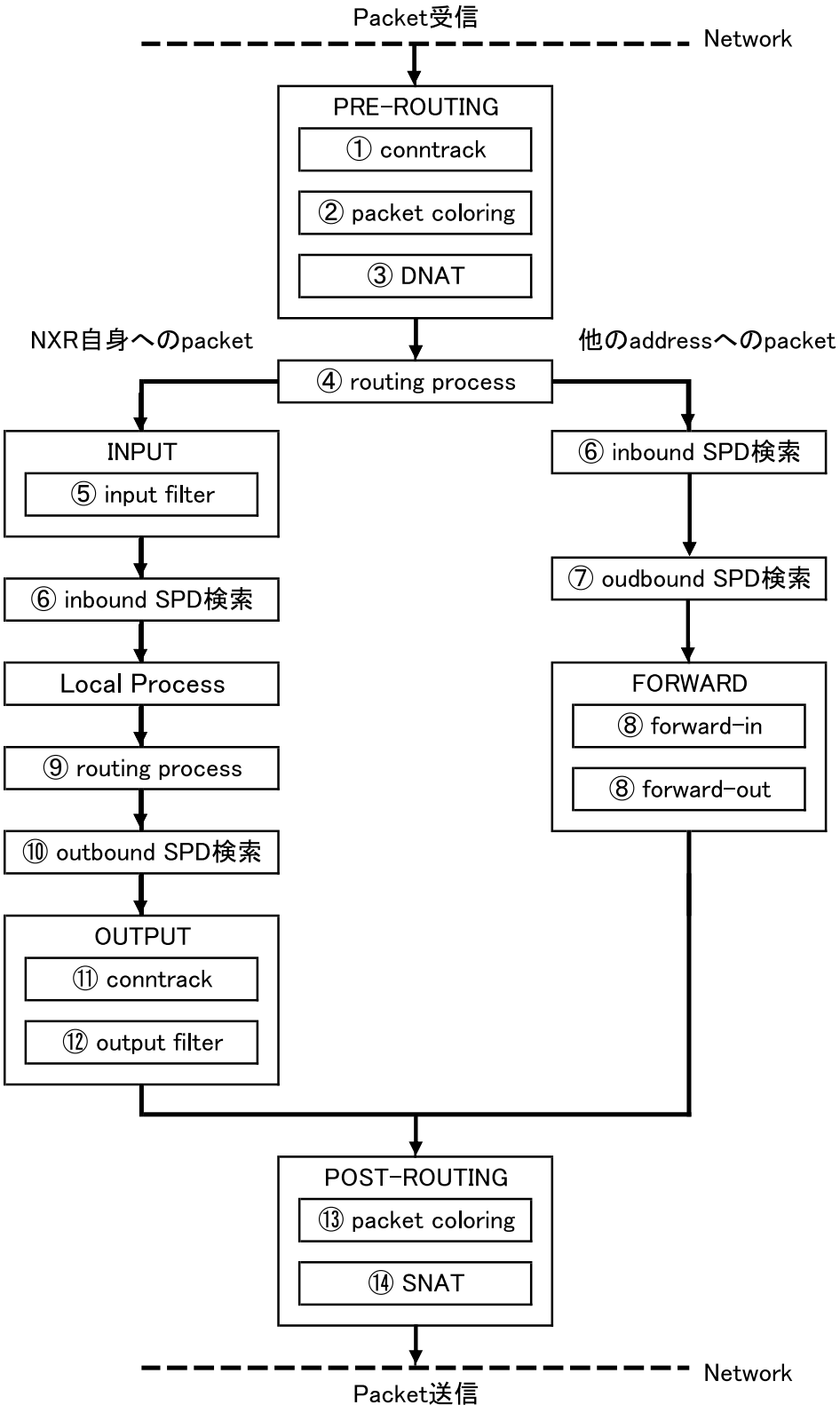
◯ OUTPUT

(1) SYSTEM SNAT
(2) IPsec policy に match したパケットは、以下の NAT はチェックしません。
ただし、IPsec snat-policy が有効の場合は、以下の NAT のチェックを継続します。
(3) USER 設定 SNAT(Static NAT)
(4) IPv4 Masquerade

付録 A
Packet Traveling

3. VXR Packet Traveling

VXR が Packet を受信してから送信するまでに適用される NAT、filtering、packet coloring の順番を下図に示します。



付録 A

Packet Traveling

○ Packet forwarding 時

- Packet 受信 -

① Conntrack
conntrackテーブルをチェックして、テーブルにマッチしないパケットを破棄します。conntrackテーブルは、session コマンド(global mode)を使用して設定します。

② Packet coloring(input)

③ Destination NAT
詳細は、NAT の優先順位(INPUT)を参照してください。

④ Routing Process

⑥ IPsec inbound SPD(※1)検索
ESP 化されてきた packet は、ここで policy check が行われます。ESP 化すべき packet が plain-text で送信されてきた場合は drop されます。但し、ipsec policy-ignore input が有効な場合は、ここでの check は行われません。

⑦ IPsec outbound SPD(※1)検索
ipsec policy-ignore output が設定されている場合は、policy 検索は行われません。

⑧ Packet filtering
詳細は、IP filtering の優先順位(FORWARD)を参照してください。

⑬ Packet coloring(output)

⑭ Source NAT
詳細は、NAT の優先順位(OUTPUT)を参照してください。

- Packet 送信 -

○ Packet 受信時(VXR が宛先)

- Packet 受信 -

① Conntrack
conntrackテーブルをチェックして、テーブルにマッチしないパケットを破棄します。conntrackテーブルは、session コマンド(global mode)を使用して設定します。

② Packet coloring(input)

③ Destination NAT
詳細は、NAT の優先順位(INPUT)を参照してください。

④ Routing Process

⑤ Packet filtering
詳細は、IP filtering の優先順位(INPUT)を参照してください。

⑥ IPsec inbound SPD(※1)検索
ESP 化されてきた packet は、ここで policy check が行われます。ESP 化すべき packet が plain-text で送信されてきた場合は drop されます。但し、ipsec policy-ignore input が有効な場合は、ここでの check は行われません。
--> ESP packet の場合、認証 /decrypt 処理後、①へ戻ります。
--> VXR local process

付録 A

Packet Traveling

○ Packet 送信時（VXR が送信元）

- VXR Local Process が Packet 送出 -

⑨ Routing process

⑩ IPsec outbound SPD(※1)検索

⑪ Conntrack

conntrackテーブルをチェックして、テーブルにマッチしないパケットを破棄します。conntrackテーブルは、session コマンド(global mode)を使用して設定します。

⑫ output filter

詳細は、IP filtering の優先順位(OUTPUT)を参照してください。

⑬ Packet coloring(output)

⑭ Source NAT

詳細は、NAT の優先順位(OUTPUT)を参照してください。

SNAT される場合、この後で再度 IPsec outbound SPD 検索が行われます。但し、ipsec policy-ignore output が設定されている場合は、policy 検索は行われません。 Policy に match した packet は、encrypt 処理を行い、OUTPUT chain --> POST ROUTING を通過し、ESP packet が出力されます。

- Packet 送信 -

(注1)

IPsecを使用するにあたって、どのようなパケットに対してどのようなアクション{discard(パケット廃棄する)、bypass(IPsec 処理を行わない)、apply(IPsec を適用する)}を行うかを定めたルールが SP(Security Policy)で、SP を格納するデータベースが SPD(Security Policy Database)です。

SPD には、inbound SPD と outbound SPD があります。受信パケットの policy check には、inbound SPD が検索されます。送信パケットの policy check には、outbound SPD が検索されます。

付録 B

Policy based IPsec と Route based IPsec

付録 B Policy based IPsec と Route based IPsec

I . Policy based IPsec

1. Policy based IPsec

ここでは、VXR の IPsec が policy base として動作する場合の仕様について記します。Policy base として動作する場合、routing table に関係なく、policy に match する packet はすべて ESP 化されます。IPsec ESP 化される packet に対して、filtering や NAT(SYSTEM NAT を除く)を行うことはできません。

1.1. IPsec policy matching

policy に match しない packet は routing table に従って forwarding されます。policy に match せず、かつ route がない場合は、drop されます。

1.2. ESP 化時の処理

1.2.1. IPv4 DF 付き Packet の ESP 化

IPsec において PMTU discovery が無効となっている場合は、DFbit が 1 でかつ tunnel MTU を超えてしまう場合でも、強制的に tunneling して転送されます。この場合、outer の IP header の DF bit は、必ず 0 が設定されます。
一方、IPsec において PMTU discovery が有効な場合、DFbit が 1 でかつ tunnel MTU を超えると、fragment needed を送信元に返信し、packet は drop されます。このとき、outer の IP header の DF bit 値は、tunneling packet の値が設定されます。

1.2.2. IPv6 Packet の ESP 化

IPv6 の場合も IPv4 と基本的に同様な動作を行います。IPv6 では、中間の router で fragment されないため、PMTU Discovery を使用して fragment が発生しないような packet size を見つけて送信します。この機能は、Default で有効とし、無効にすることはできません。
また、VXR にて tunneling を行う際、tunnel header tax によって転送可能な最大 packet size が、IPv6 の最小 MTU(1280bytes)を下回る場合が考えられます。この場合、1280 より小さい値を送信元に返しても、送信元ノードは 1280 より小さい packet に分割して送信することができないため、通信ができない現象が発生してしまいます。
以下に、tunneling 時に MTU 超えが発生した場合の fragment 動作について記載します。なお、tunnel MTU とは、出力 interface の MTU から tunnel header を引いたものを表します。

1.2.2.1. tunneling 時の fragment 動作

a. IPv6 over IPv6 tunneling (RFC2473 参照)
- tunnel MTU が IPv6 最小 MTU(1280)より大きい場合
  Packet を破棄し、送信元 host へ icmpv6 packet too big message を返信します。
- tunnel MTU が IPv6 最小 MTU(1280)と同じか小さい場合
  強制的に fragment して送信します。

b. IPv6 over IPv4 tunneling (RFC2893 参照)
- tunnel MTU が IPv6 最小 MTU(1280)より大きい場合
  Packet を破棄し、送信元 host へ icmpv6 packet too big message を返信します。
- tunnel MTU が IPv6 最小 MTU(1280)と同じか小さい場合
  tunneling packet が IPv6 最小 MTU より大きい場合、Packet を破棄し、送信元 host へ icmpv6 packet too big message を返信します。
  Tunneling packet が IPv6 最小 MTU より小さい場合、tunnel header の DFbit は必ず 0 に設定され、fragment して送信されます。

1.2.3. Fragment Packet の ESP 化

Fragment packet を ESP 化する場合は、reassemble 後に ESP 化を行います。

1.2.4. ToS 値の設定

Tunneling IP header の ToS field には、tunneling packet の ToS 値(IPv6 の場合は traffic class の値)が設定されます。なお、ECN field の扱いについては、次のとおりです。

1.2.4.1 ECN field の扱い

Tunneling される packet の IPv4 ToS/IPv6 traffic class の ECN field 値によって、tunnel IP header の ECN filed は以下のように設定されます(ECN field については RFC3168 参照)。

- CE の場合
  ECT(0)が設定されます。
- CE でない場合
  ECN field 値がコピーされます。

1.3. IPsec policy ignore 機能

・IPsec policy のチェックを行わないように指定する機能です。IPsec policy として any などを指定したけれども、特定の通信のみ IPsec 化したくない場合に、この機能を使用します。

＜書　　式＞　ipsec policy-ignore (|input|output)
＜初 期 値＞　no ipsec policy-ignore　　（無効）
＜　No　＞　no ipsec policy-ignore
＜備　　考＞
・インタフェース(Ethernet/Tunnel/PPP)毎に設定することができます。
・Input を指定した場合、inbound policy check を実行しないため、IPsec 化されてくるべきパケットがドロップ されてしまう現象を回避することができます。
・Output を指定した場合、当該インタフェースから出力されるパケットは、IPsec policy をチェックしないため平文で送信されます。

付録 B　Policy based IPsec と Route based IPsec

II．Route based IPsec

2. Route based IPsec

Route based IPsec の場合、IPsec mode に設定された tunnel interface に対する route 設定に依って ESP 化するかどうかが決定されます。
出力先 interface が IPsec mode の tunnel interface となっている場合、ESP 化されて出力されます。
そのため、迂回 route の確保や main/backup tunnel の常時確立、IPv6 を IPsec 化する際に any を利用できるなどの利点があります。
※ Transport mode の IPsec では、route based IPsec を利用することはできません（常に policy based IPsec で動作します）。

2.1. IPsec tunnel interface

○ IPsec tunnel interface の設定
IPsec tunnel interface は、GRE や ip-in-ip tunnel と同じように、tunnel interface を使用します。mode を変更することにより、使用する転送用 protocol（IPv4 または IPv6）を変更することができます。
通常の tunnel interface と同じように、tunnel 上で ospf などの routing protocol を利用したり、ip address を設定したり、multicast を送受信することもできます。
＜書　　式＞　tunnel mode (ipip|gre|ipsec ipv4|ipsec ipv6)
＜　No　＞　no tunnel mode
＜備　　考＞　Route based IPsec を使用する際は、ipsec ipv4/ipsec ipv6 を指定します。

IPsec tunnel interface 設定時、以下の option を指定することができます。

○ Path MTU Discovery 機能の有効 / 無効
有効な場合、outer IP header の DF bit は、ipv4 の場合は DF bit がコピーされます。IPv6 の場合は、1 が設定されます。但し、IPv6 を tunneling する場合に MTU 超えが発生したときは強制的に 0 が設定されることがあります。詳細は、「付録 B 1.2.2. IPv6 Packet の ESP 化」を参照してください。
無効な場合、outer header の DF bit は常に 0 が設定されます。Path MTU Discovery の動作は、「付録 B 2.3. IPsec tunnel interface での Path MTU Discovery 動作」を参照してください。
＜書　　式＞　tunnel path-mtu-discovery
＜初 期 値＞　tunnel path-mtu-discovery　（有効）
＜　No　＞　no tunnel path-mtu-discovery

○ ICMP Address Mask Request reply
ICMP address mask request に応答するかどうかを設定します。
＜書　　式＞　ip mask-reply
＜初 期 値＞　no ip mask-reply　　（応答しない）
＜　No　＞　no ip mask-reply

○ ToS 設定(0-252 または inherit) (Default: inherit)
Tunnel IPv4（outer）ヘッダの ToS フィールドに設定する値を指定します。
＜書　　式＞　tunnel tos (<0-252>|inherit)
＜初 期 値＞　tunnel tos inherit
＜　No　＞　no tunnel tos　　(= tunnel tos inherit)
＜備　　考＞
・Tunnel IPv4（outer）ヘッダの ToS フィールドに設定する値を指定します。inherit を指定した場合、IPv4（innner）ヘッダの ToS 値、または tunneling IPv6（inner）ヘッダの traffic-class 値を tunnel IPv4（outer）ヘッダにコピーします。
・ToS 値を指定する場合、0-252 の範囲で指定することが出来ます。
・ECN フィールドの設定は出来ません。ECN field の扱いについては、「付録 B 1.2.4.1 ECN field の扱い」を参照してください。
※ GRE トンネル上で、IPv6 パケットをトンネリングする場合は、inherit を無視し、ToS 値として 0x0 を設定します。

○ TTL 設定
・固定の値（1-255）を設定する場合は、PMTUD を有効にします。
・inherit を設定した場合、GRE/IPIP の場合とは異なり、TTL にシステムの default 値(64)を使用します。
＜書　　式＞　tunnel ttl (<1-255>|inherit)
＜初 期 値＞　tunnel ttl inherit
＜　No　＞　no tunnel ttl　　(= tunnel ttl inherit)

○ protection 設定
使用する IPsec tunnel policy を指定します。
＜書　　式＞　tunnel protection ipsec policy <1-65535>
＜　No　＞　no tunnel protection
＜備　　考＞　Route based IPsec を使用する tunnel に設定します。

○ pre/post-fragment 設定
pre-fragment を指定すると、fragment 処理が必要な場合、先に fragment してから ESP 化します。（複数の ESP packet に分割されます）。詳細は、「付録 B 2.4 Fragment 処理」を参照してください。
＜書　　式＞　tunnel pre-fragment
＜初 期 値＞　no tunnel pre-fragment
＜　No　＞　no tunnel pre-fragment

2.2. Security Policy と IPsec phase2 ID との関係

Route base の場合、policy base の場合と異なり、IPsec phase 2 で negotiation された policy は SP (Security Policy)に登録されません。source/destination address、port/protocol すべてが any として SP に登録され、対応する interface として IPsec tunnel policy に bind された tunnel interface 名が登録されます。そのため、IPsec tunnel interface に送信または IPsec tunnel interface で受信した ESP packet は、すべて policy に match することになります。つまり、IPsec phase2 の ID は、対向 SG と IPsec SA を確立するための識別としてのみ使用されます。

2.3. IPsec tunnel interface での Path MTU Discovery 動作

IPsec tunnel interface における Path MTU Discovery の動作については、tunnel interface の場合の動作と異なり、policy base の場合と同様(「付録 B 1.2. ESP 化時の処理」参照)です。そのため、tunnel interface の MTU を超えている場合でも、Path MTU Discovery 機能を無効にすることにより、強制的に fragment して送信することができます。

2.4. Fragment 処理

Fragment の処理として pre-fragment、post-fragment の 2 つを選択することができます。しかし、pre/post-fragment のどちらを設定しても、実際の処理はインタフェースの MTU 値によって内部的に決まります。

pre/post-fragment 設定は、forwarding するパケットと IPsec インタフェースの MTU 値の大小を判定する際に影響します。pre-fragment 設定の場合は PMTU 値で判定し、post-fragment 設定の場合はインタフェースの MTU 値で判定します。

そのため、post-fragment 設定で、なおかつ MTU が 1500 バイト設定のトンネルでは、PMTU に関係なく 1500 バイト以下のパケットは、ESP 化してから fragment します。

通常、IPsec インタフェースの MTU は 1500 バイトになっているため、forwarding するパケットは、ESP 化を行った後で、当該 ESP パケットが出力インタフェースの MTU 値より大きい場合に fragment(post-fragment)します。このとき、ESP パケットと IP fragment パケットを出力します。

しかし、forwarding するパケットが、IPsec インタフェースの MTU より大きい場合は、IPsec インタフェースの MTU 値に fragment(pre-fragment)した後で、ESP 化します。このとき、複数の ESP パケットを出力します。

なお、デフォルトの動作は、post-fragment です。また、IPv6 パケットをトンネリングする場合は、pre/post-fragment の設定に依存せず、常に post-fragment として動作します。

2.4.1. Pre-fragment

Fragment 処理が必要な場合、fragment を行った後に ESP 化されます。そのため、複数の ESP packet に分割されます。
Pre-fragment は、以下のような場合に利用することが考えられます。

1) Interoperability の確保
Netscreen など一部の機器は、pre-fragment として動作し、HW により暗号化 /fragment/reassemble が行われるため、1500bytes 以上の packet を処理できない場合があります。
例えば 2000bytes の packet を ESP 化した後で fragment して送信すると、Netscreen で reassemble された際に 1500bytes 以上の packet になるため処理ができなくなります。
このような場合に、VXR で pre-fragment 処理して送信すれば、上記のような問題を回避することが可能になります。

2) NAT-traversal
NAT-traversal 環境で post-fragment 処理されると、最初の packet には UDP header が付与されますが、2 番目以降の packet には UDP header が付与されません。この場合、上位の NAT router によっては、2 番目以降の packet を正しく処理できないものがあります。pre-fragment を利用すると、このような問題を回避することが可能です。

3) 負荷の低減
先に述べたように、pre-fragment 処理した場合、複数の ESP packet に分割されます。他社 router では、このような packet を受信した場合、ESP を decrypt した後は packet をそのまま送信して end-point の端末に reassemble の処理をまかせることができます。
しかし、VXR では fragment されてきた packet はすべて reassemble 処理するため、負荷がかかることになります。そのため、特定の構成での利用に限り、reassemble 処理をスルーして負荷を低減することができます。詳細は、「付録 B：2.4.4. IPsec interface で受信した fragment packet の reassemble の回避」を参照してください。

2.4.2. PMTUD 設定と Fragment 設定と DF bit の関係

Fragment が必要なパケットを IPsec 化する場合、pre-fragment(fragment 後に暗号化する方法)と post-fragment(暗号化後に fragment する方法)の二通りの方法があります。
本装置で Pre-fragment をするか、post-fragment をするかは、本装置の PMTUD 設定と fragment 設定、および受信パケット(本装置で暗号化するパケット)の DF bit の値(0/1)の組み合わせによって決まります。
これらの組み合わせと pre-fragment/post-fragment の関係を Table 1 に示します。

Table 1. PMTUD 設定と Fragment 設定と DF bit の値と pre-fragment/post-fragment の関係

PMTUD設定	Fragment設定 pre/post	DF bit	本装置の処理
disable	pre	0	pre-fragment(fragment＋暗号化)
		1	pre-fragment(fragment＋暗号化)
	post	0	post-fragment(暗号化＋fragment)
		1	post-fragment(暗号化＋fragment)
enable	pre	0	pre-fragment(fragment＋暗号化)
		1	パケットをdropして、fragment neededを送信元に返す
	post	0	post-fragment(暗号化＋fragment)
		1	パケットをdropして、fragment neededを送信元に返す

・本装置で post-fragment(暗号化＋ fragment)した場合、対向装置では受信した ESP パケットを reassemble＋複合化の順序で処理します。

・VXR での PMTUD 設定(enable/diable)と Fragment 設定(pre-fragment/post-fragment)は、interface tunnel mode で次のように設定します。

◯ PMTUD 設定

```
< enable >          tunnel path-mtu-discovery
< disable >         no tunnel path-mtu-discovery
```

◯ Fragment 設定

```
< pre-fragment >    tunnel pre-fragment
< post-fragment >   no tunnel pre-fragment
```

2.4.3. IPsec interface で受信した fragment packet の reassemble の回避

Pre-fragment された packet を受信した場合に、VXR において reassemble するか、reassemble せずに forwarding するかを設定することができます。default は、有効です(reassemble します)。また、IPsec tunnel interface 上でのみ利用することができます。

＜書　　式＞　ip fragment-reassembly
＜初 期 値＞　ip fragment-reassembly　　（reassemble する）
＜　No　＞　no ip fragment-reassembly　（reassemble しない）
＜備　考１＞

- reassemble しない場合、fragment されたまま packet の処理を行うため、conntrack による session 管理の対象外となります。そのため、conntrack を利用した機能（NAT、SPI、session command で設定される各機能）との併用については、動作を保証していません。したがって、この機能を無効にする(reassemble しない)場合は、制限事項について理解した上で十分にテストを行ってから使用するようにしてください。

＜制限 事項＞

- 迂回 route から受信した場合に、invalid-status-drop として drop される場合があります。
- filtering や packet coloring 処理においても、protocol や port 番号を指定した処理を行う場合は、fragment された 2 番目以降の packet に情報がないため、2 番目以降の packet の filtering や packet coloring 処理は動作しません。このような場合は、IP header のみ(source/destination address など)で判断するように設定してください。

＜備　考２＞

- global mode で「no ip reassemble-output」を設定し、ipsec tunnel interface で「no ip fragment-reassembly」を設定した場合には「no ip fragment-reassembly」が優先されます。
  この場合、「no ip fragment-reassembly」が設定された tunnle interface で受信したパケットは、reassemble せずに転送しますが、conntrack によるセッション管理の対象から外れるため、conntrack を利用した機能（NAT 機能 /SPI/session コマンドによる各機能）が使用できなくなる他、フィルタリングや packet coloring の使用にも制限が出ます。
- 「no ip reassemble-output」を設定する場合は、全ての tunnel interface の「no ip fragment-reassembly」を「ip fragment-reassembly」に設定してから行って下さい。
  (no ip fragment-reassembly が設定されている場合は、Warning が出力されます。)
- ip fragment-reassembly は、将来的に廃止を予定しているため、なるべく ip reassemble-output を使用するようにしてください。

2.4.4. IPsec policy-ignore 機能

IPsec interface において、policy-ignore 機能を有効にした場合、route は IPsec interface ですが、policy が見つからないため、packet の処理ができずに drop されます。したがって、IPsec interface 上では ipsec policy-ignore 機能は有効にしないでください（「no ipsec policy-ignore（初期値）」にしてください）。

2.4.5. Policy base と Route base IPsec の機能比較

Policy base/Route base それぞれの IPsec で利用可能 / 利用不可な機能の比較を table 2 に示します。

Table 2. Policy/Route base で利用可能な機能の比較

機能名	Policy Based IPsec	Route Based IPsec
set route	○	×
routingによるhandling	×	○
policy-ignore	○	×(無効にしてください)
NAT	△ (SYSTEM NATで一部対応可能)	○
filtering	×	○
routing protocol (OSPF,RIPv1/v2)	×	○
DF bitが1のpacket の強制fragment	○	○
pre/post-fragmentの選択	×(post-fragmentのみ可能)	○
outer headerのカスタマイズ	×	○
IPv6 policy anyの利用	×	○
balancing	×	○(ECMPにより可能) (Equal Cost Multi Path)
QoS	×	○

付録 C

IKEv2 Protocol

付録 C

IKEv2 Protocol

VXR では、IKEv2 をサポートします。IKEv1 と同時利用することも可能です。以下に、IKEv2 の仕様を示します。

1. IKEv1 と IKEv2 の相違点

IKEv1 と IKEv2 の主な相違点は、次のとおりです。

○名称変更

IKEv1	IKEv2
ISAKMP SA	IKE_SA
IPsec SA	CHILD_SA

○ Main/Aggressive/Quick mode の概念の廃止

Main/Aggressive/Quick mode の概念が廃止され、代わりに IKE_SA_INIT、IKE_AUTH、CREATE_CHILD_SA 交換が定義されました。ただし、それぞれが一対一に対応しているわけではありません。

○ Aggressive Mode の廃止

但し、pre-shared-key 方式での ID と暗号鍵の参照方法が変更されたため、通常の IKE_AUTH で動的 address クライアントと接続することができます。

○ lifetime，rekey に関する仕様変更

「4.Rekey」を参照してください。

○ SA の lifetime の negotiation の廃止

IKEv2 では、双方で個別の lifetime を管理するため、対向同士で異なる lifetime の SA を持つ可能性があります。そのため、rekey 時に responder と initiator が入れ替わる可能性があります。

○ IKE_SA と IPSEC_SA の依存関係の変更

IKEv2 では、IKE_SA の lifetime が切れて IKE_SA が無効になった場合、その IKE_SA を使用して作成された CHILD_SA も無効になります。

IKEv1 では、ISAKMP SA と IPsec SA の間に依存関係はなく、ISAKMP SA の lifetime が切れて無効になっても IPsec SA は有効のままです。

○ rekey の際の古い SA と新しい SA との依存関係の変更

IKEv2 では、rekey 時に古い SA の情報を交換し、新しい SA が作成された後に古い SA の削除を行います。

IKEv1 では、rekey 後に古い SA を削除することはありません。古い SA は lifetime が切れることによってのみ削除されます。

付録 C

IKEv2 Protocol

IKEv1 と IKEv2 で利用可能な機能は、下表のとおりです。

機能名	IKEv1	IKEv2
set route	○	△(将来対応予定)
set priority	○	×(対応未定)
ISAKMP backup	○	△(将来対応予定)
XAUTH	○	-
X.509	○	○
PSK	○	○
動的IP時のPSKの利用	△ (main modeでは、すべての通信相手との間で同じPSKを使用)	○
Multiple authentication	-	△(将来対応予定)
EAP-MD5	-	○
EAP-RADIUS	-	○(server側)
IPv6対応	○	○
route based IPsec	○	○
policy based IPsec	○	○
MOBIKE	-	○(将来対応予定)
DPD	○	○
Hold SA	○	○
NAT-Traversal	○	○(常に有効)

2. IKEv2 交換動作

IKEv2 交換動作について、以下に記します。なお、IKE_SA_INIT と IKE_AUTH は必ず連続して行われます。どちらかが単独で行われることはありません。

○ IKE_SA_INIT

IKE_SA で使用するパラメータの negotiation を行い、IKE_SA を作成します。 Request、response の一往復(2 パケット)で完了します。この交換で使用されるパケットは暗号化されません。また、この段階では、対向の認証は行われていません。

○ IKE_AUTH

IKE_SA を用いてパケットを暗号化した上で対向の認証、および CHILD_SA のパラメータの negotiation を行い、CHILD_SA を作成します。Request、response の一往復(2 パケット)で完了します。

○ CREATE_CHILD_SA

IKE_SA_INIT、IKE_AUTH が行われた対向との間に、新たに IKE_SA もしくは CHILD_SA を作成したい場合に行われます。

○ INFORMATIONAL

IKE_SA を用いて通知を行います。そのため、IKE_SA 作成前に INFORMATIONAL を送信することはできません。Request、response の一往復(2 パケット)で完了します。
IKEv1 では、INFORMATIONAL は一方向のみの通知でしたが、IKEv2 では request、response 形式で通知を行います。

付録 C

IKEv2 Protocol

3. サポート機能

下記に IKEv2 で使用可能な認証方式、algorithm、DH group を示します。

・なお、IKEv2 の CHILD_SA において、PFS で使用する DH group として phase1 を指定した場合、未指定扱いとなるため PFS 機能は無効となります。

・CHILD SA にて、NULL 暗号を指定した場合は、認証アルゴリズムを必ず指定してください（NULL 認証不可）。

3.1 IKE SA

(認証方式 /Encryption/Hash algorithm/DH group)

IKE SA にて使用可能な認証方式、Encryption、Hash algorithm、DH group を以下に示します。

認証方式

・Pre-shared-key 方式
・Digital 署名方式 RSA(X.509)
・EAP-MD5
・EAP-Radius

Encryption

・3DES
・DES
・AES128/192/256

Hash algorithm

・MD5
・SHA1
・SHA256/384/512

PRF algorithm

・PRF-HMAC-MD5
・PRF-HMAC-SHA1
・PRF-HMAC-SHA-256
・PRF-HMAC-SHA-384
・PRF-HMAC-SHA-512

PRF は、HASH と同じ algorithm を使用します。

DH group

・DH group1(MODP768)
・DH group2(MODP1024)
・DH group5(MODP1536)
・DH group14(MODP2048)
・DH group15(MODP3072)
・DH group16(MODP4096)
・DH group17(MODP6144)

番号の大きい DH group を使用すると、CPU の処理能力が必要となるため、本装置の処理に影響を与える場合があります。

3.2 CHILD SA

(Encryption/Hash algorithm/DH group)

EAP(CHILD SA)にて使用可能な Encryption、Hash algorithm を以下に示します。

・Encryption alogorithm のみが指定されている場合は、認証機能は無効です。
・NULL 暗号を指定した場合は、認証機能は必須です。

Encryption

・3DES-CBC
・DES-CBC
・AES128/192/256-CBC
・NULL（暗号なし）

Hash algorithm

・HMAC-MD5-96
・HMAC-SHA1-96
・HMAC-SHA256-128
・HMAC-SHA384-192
・HMAC-SHA512-256
・NULL（認証なし）

DH group（PFS 有効時のみ）

・DH group1(MODP768)
・DH group2(MODP1024)
・DH group5(MODP1536)
・DH group14(MODP2048)
・DH group15(MODP3072)
・DH group16(MODP4096)
・DH group17(MODP6144)
・DH group18(MODP8192)

DH group 未指定時、PFS は無効です。

4. EAP-RADIUS 認証

IPsec client からの EAP message を、VXR にて RADIUS message でカプセル化し、RADIUS server へ送信することで認証を行います。
RADIUS server への認証要求は、最初の timeout は 2 秒、retry 回数は最大 3 回とし、retry 毎に timeout が＋1 秒されます。

4.1 RADIUS server 設定

Account 認証を行う RADIUS server の IP address、UDP port 番号、秘密鍵(secret)を設定することができます。
UDP port 番号の default は、1812 番です。Web 認証で使用する radius port 番号とは異なる番号を使用してください。

4.2 NAS-identifier Attribute 設定

USER により任意の文字(32 文字以内)を指定することが可能です。Default は、機種名 -IPsec (ex.NXRG100-IPsec)です。

＜書　　式＞　ipsec eap radius (A.B.C.D|X:X::X:X) password (|hidden) WORD
　　(|port <1-65535>) (|nas-identifier WORD)
＜　no　＞　no ipsec eap radius (|A.B.C.D|X:X::X:X)
＜備　　考＞　global mode で設定します。

付録 C
IKEv2 Protocol

5. Rekey

5.1 IKEv1 の Rekey

・ISAKMP/IPsec SA の lifetime(hard timer)を設定することができます。Default は、ISAKMP SA は 10800[sec]、IPsec SA は 3600[sec]です。この時間を経過すると SA が削除されます。

・Rekey の soft timer は、margin と increased-ratio により決定されます。Margin は、lifetime が切れる何秒前から rekey を実行するかどうかを指定します。increased-ratio 値は、margin よりどれぐらい増やすかを % で指定します。

＜書　　式＞　rekey margin <30-360> (increased-ratio <0-100>|)
＜初 期 値＞　no rekey margin
＜備　　考＞

・ipsec isakmp policy mode で設定します。

・以下の式によって、Soft timer の最小・最大が決定され、この間でランダムに Soft timer が設定されます。

```
minimum soft timer = lifetime - margin
maximum soft timer = lifetime - (margin + margin x increased-ratio/100)
```

・default 値は、margin が 270sec、increased-ratio は 100% です。このため、lifetime から 270 ～ 540sec 前の時間がランダムで設定されます。但し、Responder の場合、soft timer は、margin/2 時間分早く設定されます。これは、initiator 側より rekey を行うようにするためです。

・increased-ratio を 0 に設定すると soft timer が毎回同じ値となります。負荷の分散やセキュリティ的に問題があるため、設定しないことを推奨します。

5.2 IKEv2 の Rekey

IKEv2 では、IKEv1 の Rekey に加え、送信 packet 数が最大 sequence number(4294967295)の 90[%]に達した際に rekey を行います。

付録 D

Firmware update

付録 D

Firmware update

1. Firmware の replace

VXR シリーズでは、CLI または GUI より、firmware 更新の指示を行うことが出来ます。Firmware の転送に使用可能な protocol は、下記のとおりです。

○ HTTP(GUI)

ユーザーズガイド -GUI 編を参照してください。

○ SSH/FTP(CLI)

SSH サーバ /FTP サーバ上にある firmware を取得します。SSH 使用時は、user 名、password、firmware のファイル名(パスを含む)を同時に指定します。FTP は、anonymous による接続のみ対応しています。

＜書　　式＞

```
firmware update ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME (|source A.B.C.D|X:X::X:X) (|no-boot)
firmware update ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X) (|no-boot)
```

＜備　　考＞

- ソースアドレスを指定することができます。
- SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合（ssh://user@A.B.C.D/FILENAME）は、22 番ポートを使用します（=ssh://user@A.B.C.D:22/FILENAME)。
  - IPv4　ssh://user@A.B.C.D:port/FILENAME
  - IPv6　ssh://[user@X:X::X:X]:port/FILENAME
- no-boot を指定すると、現在（再起動前）と同じファームウェアで起動します。

○ copy(CLI)

ディスクイメージ内のユーザ割り当て領域から firmware をコピーします。

＜書　　式＞　firmware update disk0:FILENAME (|no-boot)

＜備　　考＞

- no-boot を指定すると、現在（再起動前）と同じファームウェアで起動します。

付録 D

Firmware update

1.1 Firmware update 中の service の継続

firmware update中もルータとしての処理を行うことが出来ます。
※本装置では、サービスを停止した上でのファームウェア更新は、サポートしていません。

※Firmware updateの実行例を下記に示します。

```
vxr-x86#firmware update disk0:vxr-x86-v600.bin
[============================================================] 100% DECODE
Proceed with update? [(y)es/(r)eserve/(n)o]: b    -----①
Unsaved configuration changes exist. Save Flash? [y/n]: y    -----②

After the firmware is updated, it reboots...

Firmware update is being ex-
ecuted.....................................................
Finished the firmware update, it reboots...                  -----③
```

① Firmare updateを実行するかどうかを確認するメッセージが表示されます。
サービスを継続した状態でファームアップする場合は「y」を入力します。
サービスを継続した状態でファームアップを行い、ファームアップ後に再起動しない場合は[r]を入力します。
ファームアップをキャンセルする場合は「n」を入力します。
② 設定を保存していない場合は、保存するかどうかを問い合わせるメッセージが表示されます。保存する場合は「y」、保存しない場合は「n」を入力します。
③ firmware updateが終了すると、自動的に再起動が行われます。
ただし、「r」を選択した場合、自動再起動は行わず、次回の再起動時に当該ファームウェアで起動します。

※ネットワーク経由(SSHやFTP)でfirmware updateを行った場合、回線状況等によって、ファームウェアの転送に失敗する場合があります。その場合は、回線の状態を確認してから、再度firmware updateを実行するようにしてください。

```
vxr-x86#firmware update ssh://guest@192.168.2.222/vxr-x86-v5138b09.bin
guest@192.168.2.222's password:
[=========================================                    ]  70% DOWNLOAD
% Download failed (255).
```

付録 D
Firmware update

※ファイル転送後3分以内にファームウェアアップデートを実行しない場合(「Proceed with update?」が表示されてから、3分以内に「y」を選択しない場合)、転送したファームウェアを破棄します。この場合は、再度firmware updateを実行してファイル転送から実施するようにしてください。

```
vxr-x86#firmware update ssh://guest@192.168.2.222/vxr-x86-v5138b09.bin
guest@192.168.2.222's password:
[============================================================] 100% DOWNLOAD
Proceed with update? [y/n]: y
% Timed out.
```

1.2 Firmware update中の設定保存 / 復帰

サービスの継続が可能な場合でも、firmware update中は下記の動作を行うことはできません。

・CLI/GUIからの設定の初期化
・CLI/GUI/CMSからの装置の再起動
・CLI/GUI/CMSからのfirmware update
・GUI/CMSからの設定復帰
・CLIからの設定の復帰 / 保存
・GUIからの設定(GUIからの設定時に、必ずflashへの設定保存が行われるため)

1.3 Firmware update終了後の動作

v5.8.1以前のversionでは、firmware update終了後に、自動的に再起動が行われます。

1.4 Firmware update/downdate後の起動

Firmwareの入れ替え作業後、通常startup-configのversionとfirmwareのversionにミスマッチが生じます。このような場合の起動については、次のとおりです。なお、updateおよびdowndateのいずれにおいても、認識できないXML要素名がある場合は無視されます(ログ表示もされません)。

(1) update時

running-configが、新しいfirmware versionに対応したformatに変更され、起動が行われます。
startup-configは、変更されません（以前のversionのままです)。起動後に、USERが(save config等によって)startup-configに書き込まない限り、startup-configのversionが変わることはありません。

(2) downdate時

startup-configとfirmwareのversionが異なる場合、一部のconfigが認識できない可能性があります。この場合、起動時にエラーとなった情報は起動時の情報としてログに残し、認識可能な部分だけを使用して起動します。なお、認識できないXMLタグは、無視されます（ログ表示もされません)。

付録 E

Netevent 機能

付録 E

Netevent 機能

Netevent 機能

USER が指定した監視対象の状態変化を検知した際に、PPP 回線の接続や IPsec SA の確立、VRRP priority の変更などの処理を行うことが出来ます。
Track object を追加した段階では、track の状態は up 状態となり、その後発生した event によって、down(または up)状態へと遷移し、その track に関連づけられた action が実行されます。なお、すでに event down が発生している状態で、新規に監視対象や action を追加した場合、該当する down action が実行されます。

1. 監視対象(track object)の設定

1.1 指定可能な監視対象

指定可能な監視対象は、以下のとおりです。

- interface link 状態監視
  interface の link 状態(up/down)を監視します。Keepalive が無効となっている interface に関しては、link down しないため、keepalive を有効にしてください。但し、PPP や tunnel interface のように interface の作成 / 削除ができるものに関しては、この限りではありません。
- IKE SA 状態監視
  IKE SA の状態(up/down)を監視します。
- ping/ping6 監視
  ping/ping6 による指定 host への ip reachability を監視します。
- VRRP 状態監視
  master から backup/init への変化、または backup/init から master への変化を監視します。
- OSPF neighbor 監視
  指定した router-id との neighbor 確立後から他の state への変化を監視します。
- BGP peer 監視
  指定した peer ip/ipv6 との neighbor 確立後から他の state への変化を監視します。
- System resume 監視
  システムの sleep 状態からの resume を監視します。

1.2 監視対象削除時の動作

監視対象削除時、その track に関連づけられている action の復旧処理が実行されます。
なお、track 設定が無く action のみが設定されている場合、各 action が設定されているモジュール上では、action up の状態として処理されます。例えば、PPP interface 設定で、action として connect を指定している場合、初期の状態では自動接続は行われません(auto-connect が有効な場合でも)。

1.3 ip/ipv6 reachability について

ip/ipv6 reachability の監視には、icmp/icmpv6 echo request/reply packet を使用します。

- Ping の timeout は、10sec です。
- Ping の送信間隔および retry 回数を指定することができます。なお、Ping の送信間隔は、echo request 送信後から次の echo request を送信するまでの時間です。echo reply が戻ってきてから、再度 timer が設定されるわけではありません。
- ip reachability に限り、出力 interface を指定することも可能です。

付録 E

Netevent 機能

1.4 Recovery delay timer 機能

ip/ipv6 reachability、ospf/bgp neighbor、interface link、isakmp を利用する場合、復旧時(event up と判別した場合)から実際に up 時の action を実行するまでに delay を設定することができます。
Delay timer が動作している場合は、track は down state が維持され、この間にも各 check 動作は継続されます。

- Delay timer 動作中に event down を retry 回数検知した場合、delay timer は cancel されます。
- Delay timer が timeout すると、event up の action が実行されます。このとき、ip/ipv6 reachability check の場合は、delay timer 中にカウントした ip reachability fail count は 0 にクリアされ、action 実行後から再度 reachability check が開始されます。

1.5 拡張 track 設定

netevent 拡張機能を使用すれば、標準の track では指定できない下記の option を指定することができます。拡張 track 設定は、ip/ipv6 reachability を使用する場合に有効です。
<拡張 track のみで指定可能な option>

- payload-length
  ping/ping6 送信時の size(icmp header は含まない)を指定することができます。Default は、56byte です。
- 復旧回数
  指定した回数、連続で ping/ping6 OK となった場合に復旧と判断します。Default は、1 です。
- RTT
  ping/ping6 request を送信してから、reply を受信するまでの時間(Round trip time)の閾値を指定します。指定した閾値内に reply がない状態が、rtt delay 回数分連続した場合(reply は返信されている)、rtt status が down となります。Default では、RTT の監視は行われません。
- RTT delay 回数
  RTT status down と判断するまでの遅延回数です。Default は、3 回です。
- RTT normal 回数
  RTT status up と判断するまでの rtt 正常回数です。Default は、3 回です。
- DF
  IPv4 の場合のみ指定することが出来ます。Default で、DF が set されます。
- TTL/hop-limit
  TTL(IPv6:hoplimit)を指定します。Default は、system の TTL 値(64)が set されます。
- monitor-log
  monitor-log 機能で logging を行うかどうかを指定します。Default は、無効です。
- interval variable mode 指定
  ping/ping6 の送信間隔を、ping error 発生時に変化させるかどうかを指定します。Default は、無効です。

付録 E
Netevent 機能

1.5.1 RTT status
RTT の状態を指します。
- RTT が閾値を超えた状態が RTT delay 回数分連続した場合、rtt status が down となり、RTT normal が回数分連続した場合、up 状態へと遷移します。Default は up とし、rtt status の状態変化により action は実行されません。
  - なお、ping が NG となった場合は、rtt の正常 / 異常連続回数は 0 に reset されます。また、track が down になると rtt status は INIT 状態へと遷移します。

1.5.2 Interval variable mode
ip/ipv6 reachability 指定時、常に設定された interval 間隔で監視を行いますが、この mode を有効にすると、track 状態に連動して interval 間隔が変化します。Default は、無効です。
- track up 状態で ping fail を検知すると、interval 間隔が小さくなるため、障害の検出を早く行うことができます。
- 通常時は、interval 間隔を長めに設定することで、ping/ping6 による負荷を軽減することが可能となります。

○ interval の計算方法

Interval の計算方法は次のとおりです。なお、interval の最小値は 10sec のため、下記計算により 10 以下の値となった場合は、10sec 間隔で監視されます。

v_interval = (interval/2^fail_cnt)　(2 のべき乗)

v_interval : 変更後の interval

interval : 設定されている interval

fail_cnt : 連続で ping fail となった回数

○各 track 状態での interval について

track 状態と interval の関係は、次のとおりです。
- track up で ping OK の場合は、interval で監視されます。
- track up 状態で ping fail を検知すると v_interval で監視が行われます。
- track down の場合は、fail_cnt = retry 回数 +1 として計算された v_interval 間隔で監視が行われます。
- delay timer が起動した場合、track up の場合と同様に interval で監視され、Ping fail を検知すると、v_interval で監視が行われます。

1.6 Initial timeout 設定
OSPF/BGP4 の neighbor 監視および interface link 監視設定時、初期の track 状態は init です。新規に track が設定されると、現在の状態を取得します。
- neighbor が確立(あるいは interface link up)状態と判断されると track up 状態となります。
- neighbor が確立されていない(あるいは interface link down)状態の場合、すぐに track down 状態とはなりません。この場合は、initial timeout が timeout するか、OSPF/BGP4 機能 /interface 状態監視機能によって down の状態変化通知があったときに、track down として判断し、down action を実行します。
- Initial timeout は、default で無効です。有効時の default の initial timeout 値は 180sec です。なお、initial timeout 値は、10 ～ 3600sec の範囲で設定することが出来ます。

付録 E

Netevent 機能

1.7 Interface ethernet の初期状態

Ethernet インタフェースの初期状態を track している場合、初期の track の状態(Ethernet インタフェースのリンクの up/down)は、次のとおりです。

・link up 時

すぐに track up 状態となります。

・link down 時

- initial-timeout を設定している場合、initial-timeout がタイムアウトする前に up 通知がない場合は down と判定します。
- initial-timeout が未設定の場合、1 秒後に再度リンク状態を取得して、up でない場合は down と判定します。

付録 E

Netevent 機能

2 actionの設定

2.1 指定可能なaction

指定可能なactionは、次のとおりです。設定の詳細は、当該項目を参照してください。

①VRRP Priorityを指定値に変更することが出来ます。
次のコマンド(interaface mode)で設定します。
vrrp ip <vrrpid:1-255> netevent <trackid:1-255> priority <1-254>

②IPsec tunnelの確立 / 削除 / 再接続(isakmp単位での指定)を行うことが出来ます。
次のコマンド(ipsec isakmp policy mode)で設定します。
netevent <trackid:1-255> (connect|disconnect|reconnect)

③PPPの接続 / 切断を行うことが出来ます。
次のコマンド(interface ppp mode)で設定します。
netevent <trackid:1-255> (connect|disconnect)

④Tunnel interfaceのup/downをすることが出来ます。
次のコマンド(interface tunnel mode)で設定します。
netevent <trackid:1-255> (connect|disconnect)

⑤L2TPv3 tunnelの切断(PPPのinterface link監視のみ対応)を行うことが出来ます。
次のコマンド(l2tpv3 tunnel mode)で設定します。
netevent <trackid:1-255> disconnect

⑥IPsec local policyの変更を行うことが出来ます。
次のコマンド(ipsec isakmp policy mode)で設定します。
local policy <policy:1-255> netevent <trackid:1-255> change <local_policy:1-255>

⑦IPsec isakmp policyの変更を行うことが出来ます。
次のコマンド(ipsec tunnel policy mode)で設定します。
set key-exchange isakmp <1-65535> netevent <trackid:1-255> change isakmp <1-65535>

⑧システムの再起動を行うことが出来ます。
次のコマンド(global mode)で設定します。
system netevent (<1-255>|<2048-4095>) restart

⑨モバイルモジュールのリセットを行うことが出来ます。
次のコマンド(global mode)で設定します。
mobile <0-2> netevent (<1-255>|<2048-4095>) reset

⑩BGP advertise-routeの有効化 / 無効化を行うことが出来ます。
次のコマンド(bgp mode)で設定します。
netevent <trackid:1-255> advertise-stop

⑪IPv4 static routeの有効化 / 無効化を行うことが出来ます。
次のコマンド(global mode)で設定します。
ip route A.B.C.D/M (<gateway:E.F.G.H>|INTERFACE|null) (|<distance:1-255>)
(|netevent <trackid:1-255> (active|inactive))

⑫PBR routeの有効化 / 無効化を行うことが出来ます。
次のコマンド(route-map mode)で設定します。
netevent (<1-255>|<2048-4095>) (active|inactive)

付録 E
Netevent 機能

また、監視対象と event 発生時の動作対象が同じ場合、復旧の動作ができないため、監視対象と event 発生時の動作対象で同じものを設定しないでください。次のように設定した場合、master へ復帰することができなくなります。

```
interface ethernet 0
 ip address 192.168.0.254/24
 vrrp ip 1 address 192.168.0.1
 vrrp ip 1 netevent 1 priority 10
!
track 1 vrrp ip 1 interface ethernet 0
```

付録 E
Netevent 機能

2.2 Reconnect action
ISAKMP policy のみ action として、reconnect を指定することができます。reconnect を指定した場合、event down を detect すると IKE/IPsec SA を削除し、再 negotiation を開始します。event up 時は、何も実行しません。

```
＜書　　式＞　netevent <trackid:1-255> (connect|disconnect|reconnect)
　　　　　　netevent <trackid:2048-4095> (connect|disconnect|reconnect)
＜　no　＞　no netevent
```

2.3 Change action
IPsec isakmp policy の local policy 指定、および IPsec tunnel policy の set key-exchange 指定にて、設定することができる action です。
IPsec isakmp/tunnel で使用する local policy/isakmp policy の track 状態によって変更することができます。この機能により、障害に応じて、1 つの IPsec 設定にて main/backup の構成を取ることができます。なお、IPsec isakmp policy にて local policy の change を行う場合で、かつ PSK を使用する場合は、変更前の ID と変更後の ID は、同じ ID を使用してください。
詳細は、ipsec isakmp policy mode/ipsec tunnel policy mode の「change action」を参照してください。

2.4 Restart action
当該トラックイベントが down した時に、システムの再起動を行います。イベント up 時は何も実行しません。

```
＜書　　式＞　system netevent (<1-255>|<2048-4095>) restart
＜　no　＞　no system netevent
```

2.5 Reset action
当該トラックイベントが down した時に、モバイルモジュールをリセットします。イベント up 時は何も実行しません。

```
＜書　　式＞　mobile <0-2> netevent (<1-255>|<2048-4095>) reset
＜　no　＞　no mobile <0-2> netevent
```

2.6 action 追加時の動作
Action 追加時は、track object の状態が down の場合に action を実行します。

2.7 action 削除時の動作
Action 削除時は、その module において netevent がない場合と同じ動作を実行します。Action 復旧処理を実行するわけではありません。

3 システム起動中に発生した event に対する action の実行
システム起動中に該当する track の状態変化を検知した場合、システム起動処理が完了してから発生した event に伴う action を実行します。

付録 F

VRRP

付録 F

VRRP

本装置でサポートしているVRRP(Virtual Router Redundancy Protocol)について記します。

・VRRP で使用する MAC アドレスは、RFC で定義されている仮想 MAC(00-00-5e-00-01-VRID)のみで、実 MAC を使用した VRRP はサポートしていません。
・VRRP をサポートするインタフェースは、Ethernet インタフェースだけです。

1 VRRPv2

・VRRPv2(RFC3768)をサポートします。
・実 IPv4 アドレスを仮想 IPv4 アドレスとして使用(IP address owner)することはできません。また、仮想 IPv4 アドレスは、実 IPv4 アドレス(セカンダリ IPv4 アドレスを含む)と同じネットワークアドレスを使用してください。

2 VRRP Tracking

・特定の回線や IPsec SA の状態、あるいは特定ホストへの通信状態を監視し、状態が変化した際に VRRP の priority を指定値まで下げ、即座にマスターからバックアップ状態へと遷移する機能です。
・逆に、監視対象となる回線や IPsec SA が正常状態へと遷移した場合は、VRRP priority は元の値へと戻ります。Netevent 機能と連動して動作します。

3. VRRP Event 機能

・VRRP がマスターからバックアップ状態へと変化した際に、PPP 回線の切断や IPsec SA の削除を行います。
・バックアップからマスターへと遷移した場合には、PPP 回線の接続や IPsec SA の確立を行います。
・この機能は、VRRP グループ毎に指定することが可能です。

付録 F

VRRP

4 Preempt 機能

・Preempt 機能によって、バックアップルータがマスタールータへと切り替わる場合の動作を指定することができます。
- Preempt が有効な場合、優先度のもっとも高いルータが、必ずマスタールータになります。
- Preempt が無効な場合、priority の高いルータが復旧したとしても、現在マスターになっているルータがそのままマスタールータとして動作を継続します。

4.1 Preempt delay 機能

・Preempt が有効な場合に、バックアップルータが自分より優先度の低い advertise を受信した際に、バックアップからマスターへ切り替わる時間を遅らせることが出来ます。delay 時間は、1～1000(秒)の範囲で指定(秒単位)します。
・Preempt delay が設定されている場合、バックアップルータおよびマスタールータは、以下のとおり動作します。

○ バックアップルータ
- master down timer、あるいは delay timer がタイムアウトすると advertise を送信してマスターへと状態遷移します。
- 自分よりも優先度の高い advertise を受信した場合は、バックアップルータとして動作します(delay timer が動作している場合は停止します)。
- 自分よりも優先度の低い advertise パケットを受信した場合、delay timer が未起動なら delay timer を開始し、master down timer はキャンセルします。また、delay 中に自分より優先度の低い advertise パケットを受信した場合は、無視します(delay timer を継続します)。

○ マスタールータ
- 自分よりも優先度の高い advertise を受信した場合、バックアップルータへと遷移します。
- 自分よりも優先度の低い advertise を受信した場合、advertise を無視します(マスタールータのまま状態遷移しません)。

付録 G

Configの保存と復帰

付録 G　Configの保存と復帰

Ⅰ．Configの保存

Configの保存

本装置でのconfigは、running-config（現在動作しているconfig）とstartup-config（flashに保存され起動時に使用するconfig）が存在します。ユーザが設定の保存を実行した場合に限り、flashメモリや外部記憶装置に保存します。ただし、GUIから設定変更を行った場合は、設定と同時にflashにも保存します。

・起動中のconfig（running-config）を、flashに保存するにはsaveコマンド（view mode）を使用します。また、外部記憶装置に保存するには、copyコマンド（view mode）を使用します。詳細については、ユーザーズガイドの該当箇所を参照してください。
 - 起動中のconfigをflashに保存する例：　　save config
 - 起動中のconfigをディスクイメージ内のユーザ割り当て領域に保存する例：
　　copy config disk0:config.xml

起動中のconfigを、HTTP（GUIからの実行）やSSH/FTP（CLIからの実行）を使用して、ネットワーク経由で保存することが出来ます。ユーザが設定した情報は、XML形式で保存されます。

・起動中のconfig（running-config）を、SSH/FTPサーバに保存するには、copyコマンド（view mode）を使用します。詳細については、ユーザーズガイドの該当箇所を参照してください。
 - 起動中のconfigをFTPサーバに保存する例：copy config ftp://A.B.C.D/config.xml

■ show-config形式での保存

XML形式での設定のエクスポートに加え、show-config形式（CLIコマンド形式）の設定をエクスポートすることが出来ます。ただし、show config形式で保存したconfigは、ファイルを読み込んで設定の復帰を行うことは出来ないため、本装置の起動後にCLIからログインし、ターミナルソフトなどからコピー＆ペーストで設定の復帰を行います。

・show config形式の設定をエクスポートするには、copyコマンド（view mode）を使用します。詳細については、ユーザーズガイドの該当箇所を参照してください。
 - 外部SSHサーバに保存する例：　copy show-config ssh://user@A.B.C.D/show-config.txt

II．Configの復帰

Configの復帰

Configをflashに保存（復帰）することで、再起動時のconfigとして使用することが出来るようになります。

・起動中のconfig（running-config）をflashに保存（復帰）するには、saveコマンド（view mode）を使用します。外部記憶装置やネットワーク経由でconfigを保存（復帰）するには、copyコマンド（view mode）を使用します。詳細については、ユーザーズガイドの該当箇所を参照してください。

- 起動中のconfigを保存（復帰）する例：save config
- ディスクイメージ内のユーザ割り当て領域からconfigを復帰する例：

```
copy disk0:config.xml startup-config
```

GUIから設定の復帰を行った場合、startup-configを上書きします。再起動時に当該configによってシステムが起動します。

※起動中のconfig（running-config）を、ネットワーク経由で取得したconfigで上書きすることは出来ません。ネットワーク経由で取得したconfigは、flashまたは外部記憶装置（USBメモリ）へ保存します。

※ファームウェアのバージョンとconfigに含まれるファームウェアバージョンが異なる場合は、動作を保証しません。

・CLIよりconfig復帰する際に、config内のバージョンと現在動作しているファームウェアのバージョンが異なる場合は、ユーザにwarningを表示して復帰するかどうかを確認します（config内のバージョンをユーザが書き換えた場合の動作は保証しません）。

```
vxr-x86#copy ssh://guest@192.168.0.1/config.xml startup-config
guest@192.168.0.1's password:
% Version is not same. continue? [y/n]:
```

CLIでのconfig表示は、XML形式およびCLIコマンド形式の2つのタイプの表示が可能です。GUIでは、起動中のconfig情報のみを表示します。

・CLIでconfigを表示するには、showコマンド（view mode）を使用します。詳細については、ユーザーズガイドの該当箇所を参照してください。

-XML形式で表示する例：

```
show config xml
show startup-config xml
```

-CLIコマンド形式で表示する例：

```
show config
```

III. Configの保存形式

Configの保存形式

Configの保存を行った場合に、保存の対象となる情報は、次のとおりです。

- XML config情報
- IPsec X.509の証明書
- SSH公開鍵

XML config情報のみを保存する場合は、text形式で保存することが可能です（config.xml）。
IPsec X.509の証明書については、config保存時にユーザが指定した場合のみ保存対象となります。この場合、XML config情報とX.509の証明書をtar.gz形式で保存します（config.tar.gz）。
・tar.gz形式で保存する場合は、copyコマンド（view mode）でallを指定します。詳細については、ユーザーズガイドの該当箇所を参照してください。
　-tar.gz形式で保存する例： copy config disk0:config.tar.gz all

config.tgzで保存した場合、次のようなファイル名、ディレクトリ構成となります。

- config.xml
- ipsec/privates
  /cacerts
  /certs
  /crls
- ssh/USER名/SSH公開鍵

設定の復帰は、text形式（xml形式のみ）、tar.gz形式（X.509がなくても可）のいずれの形式でも行うことが出来ます。ファイル名については、特に制限はありません。ただし、tar.gz形式で復帰した場合、展開後にconfig.xml（固定のファイル名）がない場合はエラーとなります。

Ⅳ．INITボタン押下による起動時の制限

・INITボタンは、ログイン出来なくなった場合や、configを初期化したい場合、あるいは一時的な設定により動作を確認したい場合etcに使用します。
・ログインが出来なくなった場合やconfigを初期化したい場合は、INITボタンによる起動後に、ログインして、erase flashコマンドで設定を消去します。

※ INITボタンによる起動方法については、「第１章　本装置の概要」→「II各部の名称と機能」の該当項目を参照してください。
※ INITボタンを押下した状態で、本装置を起動した場合の制限は、次の通りです。

■ flashに対するすべての操作の禁止

・save config、boot-configの変更、copy XXXX startup-config、show flashなど、flashに対する操作を行うことは出来ません（※ただし、firmware update、およびerase flashは、実行することが出来ます）。

■ SDカードに対するすべての操作の禁止（※ SDカード内蔵機種のみ）

・SDカード上のファイル表示、config表示、外部からのインポート、外部へのエクスポートなど、SDカードに対する操作を行うことは出来ません（※ただし、SDカードのフォーマットは、実行することが出来ます）。

■ GUIによる設定の禁止

・GUIから設定変更を行うと、必ずflashにconfigを保存します。そのため、INITボタン押下時は、GUIからの設定を行うことは出来ません。

付録 H

RAS 機能

付録 H

RAS 機能

■ RAS 接続機能

・BRI/ シリアル回線および L2TPv2 LNS において、クライアントからの call を受ける機能（Access Server 機能）です（本バージョンでは、BRI/ シリアル回線は未対応です）。
・クライアントに割り当てる IPv4 アドレスをユーザ名や発信回線などの情報を元に、固定で割り当てることが出来ます。IPv6 アドレスの割り当ては、本バージョンでは対応していません。
・なお、プロトコル上、RAS 回線着信時のユーザ名と、発信時に使用する PPP のユーザ名とは、重複しないように設定してください。

■着信回線の設定

□ L2TP LNS での着信

・L2TP LNS 機能による着信では、virtual-template を使用します。設定は、interface virtual-template mode を参照してください。

□ BRI での着信

・本バージョンでは、未対応です。

■着信回線への static route の設定

・着信回線に対して、static route を設定する場合は、以下のいずれかの方法で設定します。

□固定 PPP インタフェースの場合

・着信用に設定したインタフェースに対して、static route を設定します。RAS 着信待機状態で、static route が有効になります。

```
ip route A.B.C.D/M  ppp <0-4>
```

□動的 PPP インタフェースの場合

・接続相手に割り当てる IP アドレスをネクストホップアドレスとして static route を設定します。RAS 着信後、クライアントに IPv4 アドレスを割り当てた際に static route が有効になります。
・virtual-template を利用した着信の場合、PPP インタフェースが固定化されないため、この方法で設定します。

```
ip route A.B.C.D/M  a.b.c.d
```

付録 H

RAS 機能

■ IP アドレスの割り当て

・クライアントに対して割り当てる IPv4 アドレスを指定することが出来ます。IPv6 アドレスの割り当てには対応していません。

□ユーザ名毎に指定

・ユーザ名毎に、割り当てる IPv4 アドレスを指定します。access-server profile mode で、次のように設定します。

```
!
access-server profile 0
 ppp username user01 ip 1.1.1.1
!
```

・IPv4 アドレスの割り当てを行う場合、次のように、Access-server 側の local ip address（virtual-template の IP アドレス）を指定する必要があります。

□着信時の本装置の IP アドレス

・RAS 着信時、interface virtual-template mode で設定した IP アドレスを本装置の IP として使用します。

```
!
interface virtual-template 0
 ip address 10.0.0.1/32
!
```

□着信 PPP での IPsec の利用

・Virtual-template 上では、IPsec を利用することは出来ません。

付録 I

データコネクト

付録 I

データコネクト

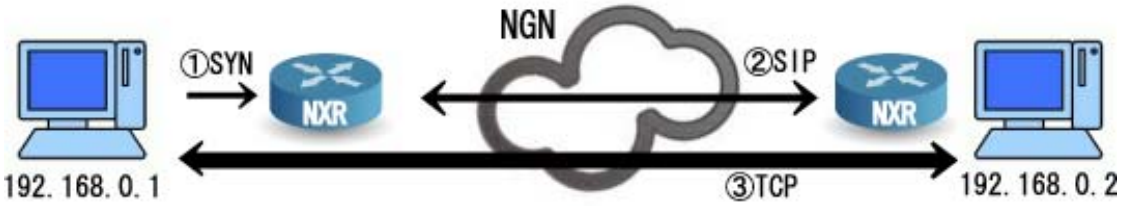
■データコネクト

・データコネクトとは、フレッツ光ネクスト（以下、NGN）の「ひかり電話」を契約している場合に使用することが出来る帯域確保型のデータ通信サービスです。2拠点間での任意のデータ通信をオンデマンドで行うことが出来ます。
・本バージョンでは、TCP モードのデータ通信をサポートしています（VPN モードは未対応です）。

■TCP モードによるデータコネクト接続

□接続の概要

①本装置宛ての TCP SYN パケットを検出します。
②着信先の電話番号宛てに、ひかり電話による呼接続を開始し、2 拠点間で SIP セッションを確立します。
③ SIP セッション上で交換したお互いの WAN アドレスとポート番号を元にして、拠点間での TCP 通信が可能になります。



□ SIPクライアントの設定(ngn-sip client mode)

・TCP アクセスを監視する IP アドレス、および listen port を指定します。
＜書　　式＞ mode tcp ip A.B.C.D port <1-65535>

・TCP アクセス検出時に発呼する電話番号（宛先番号）を指定します。
＜書　　式＞ tel to NUMBER
＜備　　考＞ 「0」または「#」で始まる NUMBER を指定します。指定可能な桁数は 5 ～ 32 桁です。

□ SIPサーバの設定(ngn-sip server mode)

・着信時に TCP を接続させる端末の IP アドレス（宛先 IP アドレス）、および宛先 port 番号を指定します。
＜書　　式＞ mode tcp ip A.B.C.D port <1-65535>

・着信を許可する番号（発信者番号）を指定します。
＜書　　式＞ tel from NUMBER
＜備　　考＞ 「0」または「#」で始まる NUMBER を指定します。指定可能な桁数は 5 ～ 32 桁です。

□ TCP通信の無通信切断タイマー

・TCP セッション上のデータ通信状態を定期的に監視し、一定時間の無通信状態を検出すると、自動的にデータコネクト通信を終了します。
＜書　　式＞ idle-timeout <10-3600>
＜　No　＞ no idle-timeout (初期値)
＜初期値＞ idle-timeout 60
＜ mode ＞ ngn-sip client mode, ngn-sip server mode

付録 I

データコネクト

■ NGN 回線との接続方法

・データコネクトを使用する場合、NGN 回線と VXR は、以下のように接続します。

(LAN)-----VXR-----ONU-----(NGN 回線)

※一体型（ONU ＋ルータ)のひかり電話ルータ(ホームゲートウェイ：HGW）の配下に VXR を配置した場合は、正しく動作しません（将来対応予定)。

(LAN)-----VXR-----[ONU+ ルータ]-----(NGN 回線)

■ NGN 網における WAN アドレス

・NGN 網で使用する WAN アドレス(IPv4)は、DHCPv4 にて取得します。

＜説　　明＞　NGN回線でデータコネクトを使用する場合に設定します。
＜書　　式＞　ip dhcp mode ngn
＜　no　＞　no ip dhcp mode
＜ mode ＞　interface mode
＜備　　考＞　no を設定すると、ip dhcp request classless-static-route も無効になります。

■ Classless-static-route オプションによる route 設定

・データコネクトと PPP によるインターネット通信を併用する場合、DHCPv4 の classless-static-route オプション(RFC3442)を使って、NGN 網への static route 情報を取得することにより、データコネクトの通信を NGN 網へルーティングさせることが出来ます。

＜説　　明＞　NGN回線でのデータコネクトとインターネット接続(PPP)を併用する場合に設定します。
＜書　　式＞　ip dhcp request classless-static-route
＜　no　＞　no ip dhcp request classless-static-route
＜ mode ＞　interface mode
＜備　　考＞　取得した static route は、アドレスのリース期間中有効です。

■データコネクト接続の最大セッション数

・同時に 2 つ以上の SIP セッションを接続することは出来ません。したがって、ひかり電話の「ダブルチャネル / 複数チャネル」サービスには対応していません。
・TCP モードの場合、1 つの TCP コネクションにつき、1 つの SIP セッションが必要になります。したがって、同時に複数の TCP コネクションを使用するようなサービス（HTTP や FTP）は利用できません。

付録 I

データコネクト

■データコネクト接続の帯域制御

□データ通信の帯域

・本バージョンで対応している帯域は、64kbps です。

□データ通信の帯域制御

・設定した帯域幅の情報は、2 つの拠点間で（SIP セッションにより）交換されます。NGN 網では、SIP メッセージ上の帯域幅情報を元に、データ通信のパケットに対してポリシングが行われます。

・帯域幅を超過するデータパケットの送信は、UNI 基準に違反するため、WAN インタフェース上でシェーピング設定することを推奨します。

□データコネクト通信の DSCP

・データコネクトで行われる各種の通信について、WAN インタフェース上で、本装置が次のように DSCP を設定します。

・SIP パケット　　：46

・DHCP パケット　　：46

・データパケット(TCP/ESP)：8

・上記の値を使用して、WAN インタフェース上でシェーピング設定を行うことが出来ます。

■ JATE 発信規制

・同じ接続先に対して、最初の発信から 3 分以内に 2 回連続して失敗すると、3 回目からは発信を行いません。

■網輻輳時の LED 通知

・SIP セッション接続時に、サーバ側から網輻輳を示す応答が返って来る場合があります。輻輳状態を知るには、system led を次のように設定します。

＜書　　式＞　system led status <1-1> ngn-sip congestion

＜　no　＞　no system led status <1-1>

＜ mode ＞　global mode

＜備　　考＞

・ngn-sip congestion 指定に、STS1 LED が点滅すると、NGN 網のひかり電話サーバが輻輳していることを示します。点滅中はデータコネクトによる接続は控えるようにしてください。

■ひかり電話の付加サービス

・データコネクトでは、着信時に、発信者番号による発信者の認証を行うため、発信者番号の通知が必要になります。したがって、着信側としてデータコネクトを利用する場合は、「ナンバーディスプレイサービス」の契約が必要になります。

・その他のひかり電話サービスについては、現在のバージョンでは未対応です。

付録 J

Policy Based Routing(PBR)

付録 J

Policy Based Routing(PBR)

■ Policy Based Routing(PBR)

・通常の宛先アドレスによるルーティングではなく、ユーザ設定によるポリシーを元にパケットのフォワーディング先を決めることが出来る機能です。
・入力および出力インタフェースとして指定可能なインタフェースは、イーサネット /802.1Q VLAN/ ブリッジ（仮想スイッチ）/ トンネル /PPP です。
・PBR は、通常の宛先アドレスによるルーティングより優先されます。
・本バージョンでは、IPv6 PBR はサポートしていません。

・ポリシーとして設定可能な項目は、次のとおりです。マッチ条件の設定には ip policy access-list (global mode)、ルーティングルールの設定には route-map(route-map mode)を使用します。

□マッチ条件

●フォワーディングおよび自発パケットに対して有効な条件
　○送信元 IP アドレス：　src IP アドレスにより出力先を決定します。
　○宛先 IP アドレス：　dst IP アドレスにより出力先を決定します。
　○受信インタフェース：　受信したインタフェースにより出力先を決定します。
　　自発パケットの場合は、自動的に lo を指定します。
●フォワーディングのみ適用可能な条件（自発パケットには適用されません）
　○プロトコル
　○ポート番号（TCP/UDP パケットの場合）
　○ ICMP code/type
　○ ToS 値

□ルーティングルール

　○出力インタフェース
　○ネクストホップ IP アドレス

付録 J

Policy Based Routing(PBR)

◆ ip local policy route-map

＜説　　明＞　自発パケットに、PBR のアクセスリストを適用します。
　　WORD には、適用する ACL 名（ip policy access-list にて設定）を指定します。
＜書　　式＞　ip local policy route-map WORD
＜　mode　＞　global mode
＜備　　考＞
・自発パケットに PBR の ACL を適用した場合、ACL 内の source/destination アドレス情報のみ条件として参照します。その他、プロトコルやポート条件などは無視します。

◆ ip policy route-map

＜説　　明＞　受信インタフェースに、PBR のアクセスリストを適用します。
　　WORD には、適用する ACL 名（ip policy access-list にて設定）を指定します。
＜書　　式＞　ip policy route-map WORD
＜　mode　＞　interface mode
＜備　　考＞
・入力および出力インタフェースとして指定可能なインタフェースは、イーサネット /802.1Q VLAN/ ブリッジ（仮想スイッチ）/ トンネル /PPP です。

◆ show ip policy access-list

＜説　　明＞　PBR のアクセスリストを表示します。
＜書　　式＞　show ip policy access-list (|WORD)
＜　mode　＞　view(exec) mode

◆ show ip policy route-map

＜説　　明＞　適用した PBR のルートマップを表示します。
＜書　　式＞　show ip policy route-map (|WORD)
＜　mode　＞　view(exec) mode

◆ clear ip policy access-list

＜説　　明＞　指定した PBR アクセスリストのカウンターをクリアします。
＜書　　式＞　clear ip policy access-list WORD counter
＜　mode　＞　view(exec) mode

付録 K

P2P 検出機能について

付録 K

P2P 検出機能について

■ P2P 検出機能

・Peer-to-peer（P2P）アプリケーションの通信を検出する機能です。本機能は、IDS（IPS）を利用出来ないような環境で、簡易的に P2P アプリケーションを検出する目的で使用します。
・検出可能な P2P アプリケーションは、次の通りです。
  ・Winny(ver2)
  ・Share(EX2) （※ NT 版は未対応）
  ・BitTorrent

■ P2P 検出時の action

・P2P アプリケーションを検出した場合、当該通信に対して以下の action を指定することが出来ます。
  ・deny　：パケットを破棄します。
  ・log　：以下のようなフォーマットのログを出力します。

```
ulogd[XXX]: p2p-torrent-detect: Message
ulogd[XXX]: p2p-torrent-detect: Message
ulogd[XXX]: p2p-torrent-detect: Message
```

※ Message は、MAC ヘッダ /IP パケットの情報です。

付録 K

P2P 検出機能について

■ 関連するコマンド

◆ ip p2p-detection

＜説　　明＞　P2P 検出機能を有効にします（IPv4 のみ対応）。
＜書　　式＞　ip p2p-detection (any|winny|share|bittorrent) {log|deny}
＜　no　＞　no ip p2p-detection
　　no ip p2p-detection (winny|share|bittorrent)
＜備　　考＞
・any とアプリケーション（winny/share/bittorrent）を同時に指定することは出来ません。
・VT を除く各インタフェースにて設定することが出来ます。
・本機能は、フォワーディングするフレームに対して有効です。ブリッジインタフェースを経由して
　フォワーディングする場合は有効ですが、単純にブリッジするフレームに対しては無効です。

◆ show ip p2p-detection

＜説　　明＞　P2P 検出のカウンタ情報を表示します。
＜書　　式＞　show ip p2p-detection

◆ clear ip p2p-detection counter

＜説　　明＞　P2P 検出のカウンタをクリアします。
＜書　　式＞　clear ip p2p-detection counter

■ 利用時の注意点

・P2P 検出機能を有効にすると、パケットの中身の解析および復号処理を行うため、通信速度に影響を
　及ぼす可能性があります。特に BitTorrent の検出は、影響が大きいと考えられるため、bittorrent
　（または any）を指定する場合は、慎重に行うようにしてください。
・本機能を、送信インタフェースと受信インタフェースの両方で有効にすると、P2P 検出を 2 回行うこ
　とになります。そのため、インターネットに接続しているインタフェース上でのみ有効にすることを
　推奨します。

■ Fast-forwarding 機能との併用

・Fast-forwarding 機能を併用した場合、BitTorrent については、P2P 検出を行うことが出来ない場合
　があります。

付録 L

サポートについて

付録 L

サポートについて

◆今後のお客様サポートおよび製品開発の参考にさせていただくために、ユーザー登録にご協力をお願い致します。 弊社ホームページ内の各製品のサポートページで ”ユーザー登録 ”をクリックすると登録用の画面が開きます。

◆サポートに関する技術的なお問い合わせやご質問は、下記へご連絡ください。

・サポートデスク
e-mail　：support@centurysys.co.jp
電話　：0422-37-8926
FAX　：0422-55-3373
受付時間 ：10:00 ～ 17:00 (土日祝祭日、および弊社の定める休日を除きます)

・ホームページ　http://www.centurysys.co.jp/

◆ご連絡をいただく場合
スムーズなお客様サポートをご提供するために、サポートデスクにご連絡いただく場合は、以下の内容をお知らせいただきますよう、お願いいたします。

・ファームウェアのバージョンと Support ID（※）
・ネットワークの構成(図)
　どのようなネットワークで運用されているかを、差し支えのない範囲でお知らせください。
・不具合の内容または、不具合の再現手順
　何をしたときにどういう問題が発生するのか、できるだけ具体的にお知らせください。
・エラーメッセージ
　エラーメッセージが表示されている場合は、できるだけ正確にお知らせください。
・本装置の設定内容、およびコンピュータの IP 設定
・**可能であれば、「設定のバックアップファイル」をお送りください。**

※弊社サポートデスクへのお問い合わせには、Support ID が必要になります。
・SupportID は、Product License 使用時に、show product コマンドにより取得することが出来ます。

```
vxr-x86#show product
・・・・・・省略・・・・・・
Support ID : 0123456789XXXX
```

・Trial License では、弊社サポートデスクをご利用いただくことは出来ません。

```
vxr-x86#show product
・・・・・・省略・・・・・・
Support ID : n/a
```

◆サポート情報弊社ホームページにて、製品の最新ファームウェア、マニュアル、製品情報を掲載しています。
また製品の FAQ も掲載しておりますので、是非ご覧ください。
下記の FutureNet サポートページから、該当する製品名をクリックしてください。
http://www.centurysys.co.jp/support/index.php

FutureNet VXR-x86シリーズ ユーザーズガイド CLI編 Ver.8.2.0対応版

2016年8月版
発行 センチュリー・システムズ株式会社