FutureNet NXRシリーズ
ユーザーズガイド CLI編

Ver.5.16.1 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。

□ UQ WiMAX は、UQ コミュニケーションズ株式会社の商標または登録商標です。

□ 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。

パッケージの内容物の確認

本製品のパッケージには以下のものが同梱されております。
本製品をお使いいただく前に、内容物がすべて揃っているかご確認ください。

万が一不足がありましたら、お買い上げいただいた店舗または弊社サポートデスクまで
ご連絡ください。

＜FutureNet NXRシリーズ 梱包物＞

梱包物	NXR-120/C	NXR-125/CX	NXR-130/C	NXR-155/C-WM	NXR-1200
本体	1台				
はじめにお読みください	1部				
安全にお使いいただくために	1部				
ご注意	1部				
保証書	1部				
LANケーブル(ストレート)	1本				―
RJ-45/D-sub9ピン変換アダプタ(クロス)	1個				―
ACアダプタ/電源コード	1個				1本
ゴム足	4個				―
接続用ケーブル類の固定方法	1部	―			
ケーブル固定部品	1個	―			
ケーブル固定用クリップ	―	1個	―	1個	―
ケーブル固定用ネジ	―	1個	―	1個	―
CARD部分を塞ぐシール	―	1枚	―		
アンテナ(SWiM WA0003)	―			1組	―
WiMAX MACアドレスのシール	―			1枚	―
ラックマウント用レール	―				1式
ラックマウントガイド	―				1部

※「ゴム足」は、必要に応じて、本体底面の四隅に貼ってください。

第1章

本装置の概要

Ⅰ．本装置の特長

FutureNet NXR シリーズの「製品概要」、「製品の特徴」、「仕様」、「利用例」、「オプション」等については、弊社の Web サイトを参照してください。

◆ FutureNet NXR-120/C
http://www.centurysys.co.jp/router/nxr120c.html

◆ FutureNet NXR-125/CX
http://www.centurysys.co.jp/router/nxr125cx.html

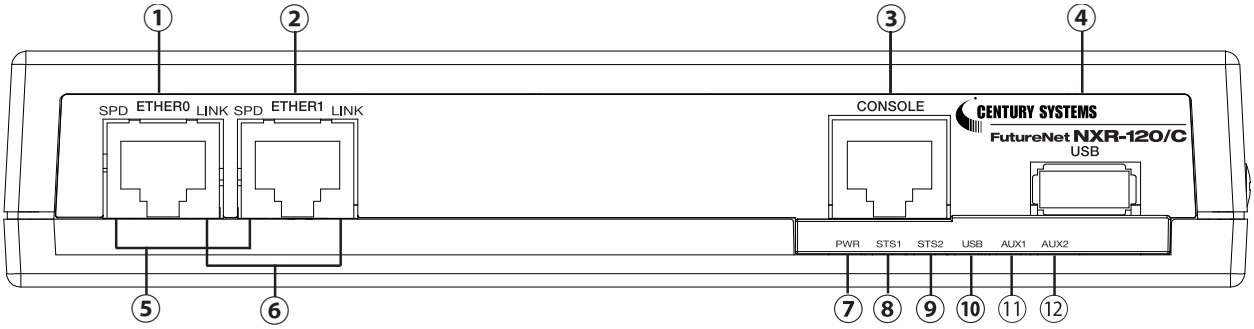
◆ FutureNet NXR-130/C
http://www.centurysys.co.jp/router/nxr130c.html

◆ FutureNet NXR-155/C-WM
http://www.centurysys.co.jp/router/nxr155cwm.html

◆ FutureNet NXR-1200
http://www.centurysys.co.jp/router/nxr1200.html

Ⅱ．各部の名称と機能（NXR-120/C）

◆製品前面



① ETHER 0ポート
主にLAN側ポートとして使用します。

② ETHER 1ポート
主にWAN側ポートとして使用します。

③ CONSOLEポート
CLI接続の場合に使用します。
Ethernet規格のLANケーブルを接続します。

④ USBポート
USB Flash メモリ、またはUSB タイプのデータ通信モジュールを挿入します。

⑤ SPD LED(緑 / 橙)
ETHERNET ポートの接続速度を示します。
10BASE-T モードで接続時 ：
100BASE-TX モードで接続時 ：
1000BASE-T モードで接続時 ：

⑥ LINK LED(緑)
ETHER ポートの状態を示します。
Link Down時 ：
Link UP時 ：
データ通信時 ：

⑦ PWR LED(青)
本装置の電源状態を示します。
電源投入時 ：

⑧ STS1 LED(赤)
本装置のシステム起動時のステータスを示します。
システム起動中 ：
システム起動完了状態 ：
ファームウェアのアップデート作業中：

⑨ STS2 LED(緑)
本装置のシステムおよび、サービス起動時のステータスを示します。
システム起動中 ：
サービス起動中 ：
サービス起動完了状態 ：

ステータスLED が以下の状態になると、本装置へのアクセスが可能になります。
STS1 LED ：
STS2 LED ：

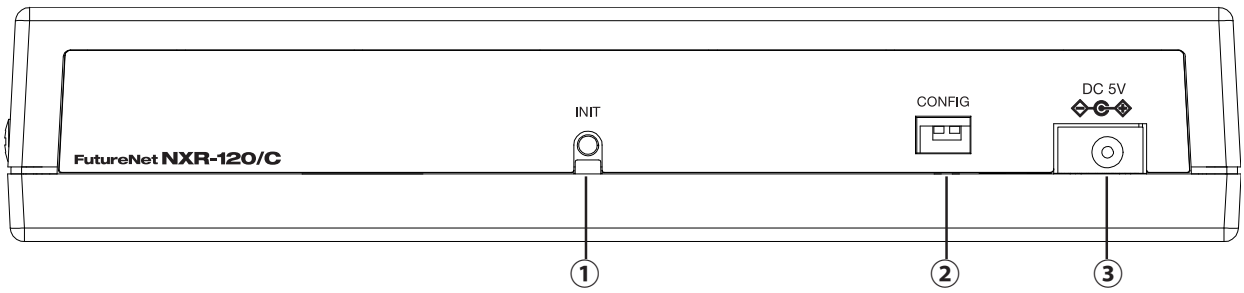
⑩ USB LED(緑)
USB ステータスを示します。
USB デバイス装着時 ：
USB デバイス未装着時 ：

⑪ AUX1 LED(緑)
⑫ AUX2 LED(緑)
データ通信端末装着時に、電波状況を表示します。
電波状況の取得周期の設定等については、第6章 global node の system led を参照してください。

	AUX1	AUX2
データ通信端末未装着時 ：		
圏外（および unknown） ：		
圏内 Signal Level 1 ：		
Signal Level 2 ：		
Signal Level 3 ：		

Ⅱ．各部の名称と機能（NXR-120/C）

◆製品背面



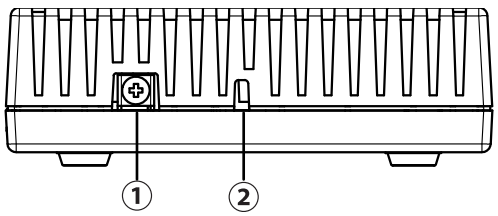
① INIT ボタン
本装置を工場出荷時の設定に戻して起動するときに使用します。

1. INITボタンを押しながら電源を投入します。
2. STS1 LEDが下記の状態になるまで、INITボタンを押したままにしておきます。
   点灯→消灯→点灯
3. STS1 LEDが再度点灯したら、INITボタンを放します。STS1 LEDが消灯し、本装置が工場出荷設定で起動します。

② CONFIG
本製品では使用しません。両方のスイッチが下に位置している状態で使用してください。

③ DC 5V 電源コネクタ
製品付属のACアダプタを接続します。

◆製品側面

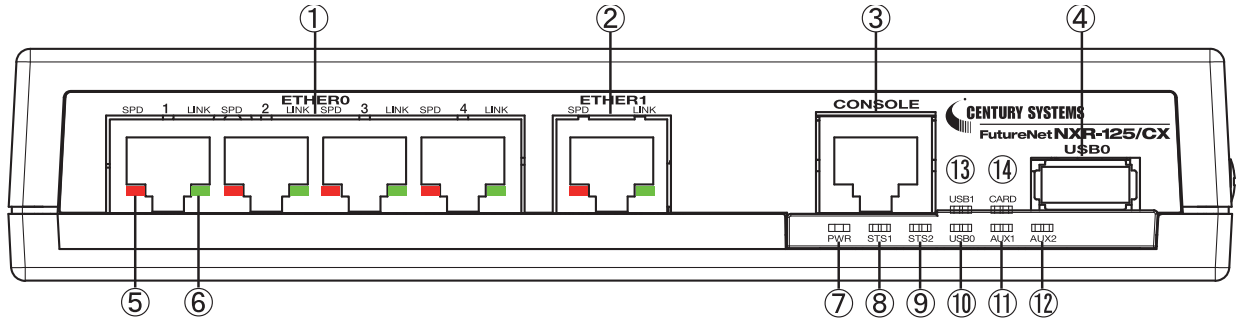


① FG端子
保安用接続端子です。
必ずアース線を接続してください。

② セキュリティスロット
ケンジントンロックに対応しています。

III．各部の名称と機能（NXR-125/CX）

◆製品前面



① ETHER 0ポート

10BASE-T/100BASE-TX/1000BASE-T対応の4ポートハブです。主にLAN側ポートとして使用します。

② ETHER 1ポート

10BASE-T/100BASE-TX/1000BASE-T対応のEthernetポートです。主にWAN側ポートとして使用します。

③ CONSOLEポート

CLI接続の際に使用します。
Ethernet規格のLANケーブルを接続します。

④ USB0ポート

USB Flashメモリ、またはUSBタイプのデータ通信端末を挿入します。

⑤ SPD LED(赤/緑)

ETHERポートの接続速度を示します。

10BASE-T モードで接続時 ：■
100BASE-TX モードで接続時：■
1000BASE-T モードで接続時：■

⑥ LINK LED(緑)

ETHERポートのリンク状態を示します。

Link Down時 ：■
Link UP時 ：■

⑦ PWR LED(青)

本装置の電源状態を示します。

電源ON時 ：■

⑧ STS1 LED(赤/緑)

本装置のシステム起動時のステータスを示します。

電源ON時 ：■
システム起動中 ：■
ファームウェア更新中：■

指定したPPPまたはtunnelの状態を示します（設定は、第6章 global nodeの system ledを参照）。

接続時 ：■
切断状態時 ：■

⑨ STS2 LED(緑)

本装置のシステムおよび、サービス起動時のステータスを示します。

電源ON時 ：■
システム起動中 ：■
システム起動後(ログイン可能状態) ：■

⑩ USB0 LED(緑)

USB デバイス0のステータスを示します。

USBデバイス0の接続時 ：■
USBデバイス0の未接続時：■

⑪ AUX1 LED(緑)/⑫ AUX2 LED(緑)

データ通信端末装着時に、電波状況を表示します（設定は、第6章 global nodeの system ledを参照）。

	AUX1	AUX2
データ通信端末未装着時 ：	■	■
圏外 （およびunknown） ：	■	■
圏内 Signal Level 0-1 ：	■	■
Signal Level 2 ：	■	■
Signal Level 3 ：	■	■

指定したPPPまたはtunnelの状態を示します。

接続時 ：■
切断状態時 ：■

⑬ USB1 LED(緑)

USB デバイス1のステータスを示します。

USBデバイス1の接続時 ：■
USBデバイス1の未接続時：■

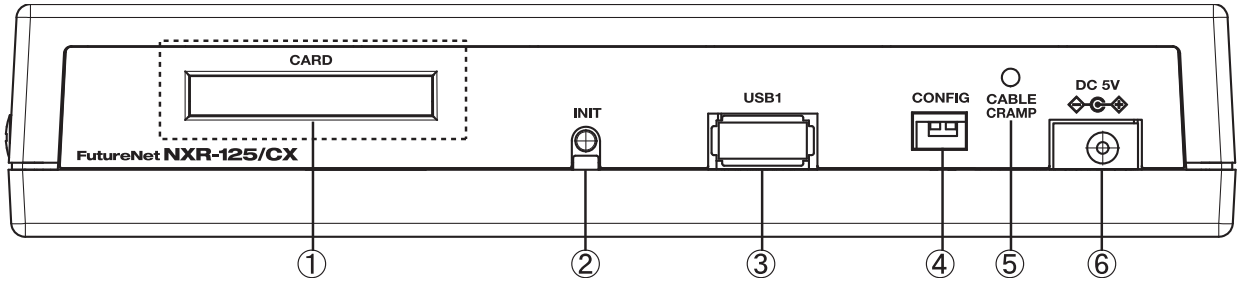
⑭ CARD LED

カードのステータスを表示します。

カードの接続時 ：■
カードの未接続時 ：■

III．各部の名称と機能（NXR-125/CX）

◆製品背面



① CARD スロット
対応するカードを接続します。
カードを使用しない場合は、異物や埃の混入を防ぐために、同梱のシールを図の点線枠の部分に貼って、CARD スロットを塞いでください。

② INIT ボタン
本装置を工場出荷時の設定に戻して起動するときに使用します。

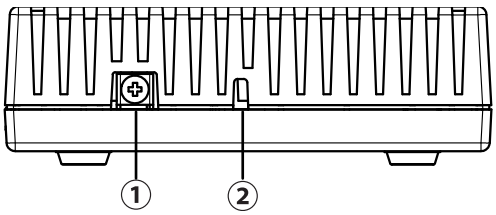
③ USB1 ポート
USB Flash メモリ、または USB タイプのデータ通信端末を挿入します。

④ CONFIG
本製品では使用しません。両方のスイッチが下に位置している状態で使用してください。

⑤ CABLE CRAMP
AC アダプタのケーブルが不意に引っ張られても、DC プラグが抜けないようにすることが出来ます。
クリップでケーブルを挟み、クリップと本装置をネジで固定します。

⑥ DC 5V 電源コネクタ
製品付属の AC アダプタを接続します。

◆製品側面

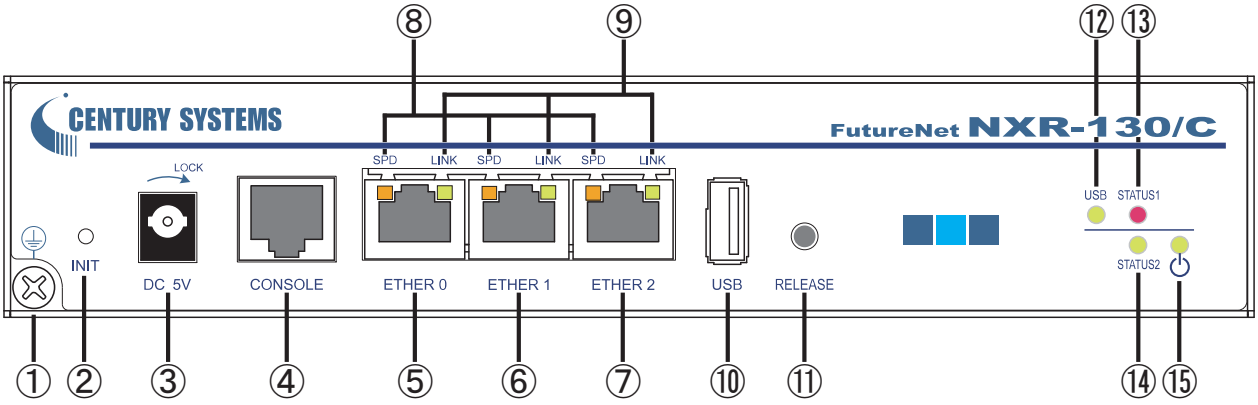


① FG(アース) 端子
保安用接続端子です。
必ずアース線を接続してください。

② セキュリティスロット
ケンジントンロックに対応しています。

Ⅳ．各部の名称と機能（NXR-130/C:ISDN ポートなし）

◆製品前面



① FG(アース）端子
保安用接続端子です。
必ずアース線を接続してください。

② INITボタン
本装置を工場出荷時の設定に戻して起動するときに使用します。

1. Initボタンを押しながら電源を投入します。
2. STATUS1 LEDが下記の状態になるまで、Initボタンを押したままにしておきます。
   点灯→消灯→点灯
3. STATUS1 LEDが再度点灯したら、Initボタンを放します。STATUS1 LEDが消灯し、本装置が工場出荷設定で起動します。

③ DC5V電源コネクタ（ロック機構付き）
製品付属のACアダプタを接続します。
電源コネクタの溝に、DCプラグのツメを合わせて、右に回してください。電源コードがロックされます。
電源コードを外す時は、DCプラグ部分を持って左に戻してから抜いてください。

本装置をご使用の際は必ず、電源コードをロックしてご使用ください。

④ CONSOLEポート
CLI接続の場合に使用します。
Ethernet規格のLANケーブルを接続します。

⑤ ETHER 0ポート
主にLAN側ポートとして使用します。

⑥ ETHER 1ポート
主にWAN側ポートとして使用します。

⑦ ETHER 2ポート
主にDMZポートとして使用します。

本装置の各ETHERポートは、全てGigabit Ethernetに対応しています。別セグメントを接続するポートとして使用可能です。
また、ポートはAutoMDI/MDI-X対応です。
Ethernet規格のLANケーブルを接続してください。

⑧ SPEED LED（緑/橙）
ETHERNETポートの接続速度を表示します。

10BASE-Tモードで接続時　：
100BASE-TXモードで接続時　：
1000BASE-Tモードで接続時　：

⑨ LINK/ACT LED（緑）
ETHERNETポートの接続状態を表示します。

Link Down時　：
Link UP時　：
データ通信時　：

⑩ USBポート
USB Flash メモリ、またはUSB タイプのデータ通信モジュールを挿入します。

Ⅳ．各部の名称と機能（NXR-130/C:ISDN ポートなし）

⑪ RELEASE ボタン

USB flash メモリを取り外すときに使用します。
本装置から USB flash メモリを取り外すときは、
以下の手順で操作してください。

1. RELEASE ボタンの長押し(約 3 秒)
2. USB LED の消灯を確認
3. USB flash メモリの取り外し

⑫ USB LED（緑）

USB ステータスを表示します。

USB デバイス装着時　：●
USB デバイス未装着時　：●

⑬ STATUS1 LED（赤）

本装置のシステム起動時のステータスを表示します。

システム起動中　：●
システム起動完了状態　：●
ファームウェアのアップデート作業中：☀

これら以外の状態で、STATUS1 が点滅している時はシステム異常が起きておりますので、弊社までご連絡ください。

⑭ STATUS2 LED（緑）

本装置のシステムおよび、サービス起動時のステータスを表示します。

システム起動中　：●
サービス起動中　：☀
サービス起動完了状態　：●

STATUS LED が以下の状態になると、本装置へのアクセスが可能になります。

STATUS1 LED　：●
STATUS2 LED　：●

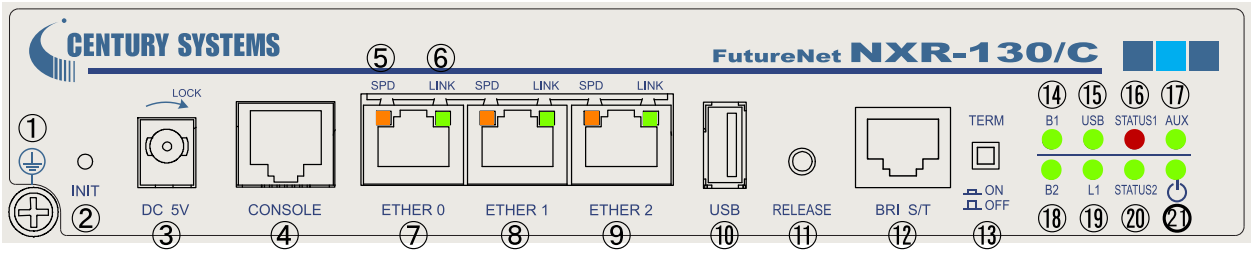
⑮ POWER LED（緑）

本装置の電源状態を表示します。

電源投入時　：●

Ｖ．各部の名称と機能（NXR-130/C:ISDN ポートあり）

◆製品前面



① FG(アース）端子
保安用接続端子です。
必ずアース線を接続してください。

② INITボタン
本装置を工場出荷時の設定に戻して起動するときに使用します。

1. Initボタンを押しながら電源を投入します。
2. STATUS1 LEDが下記の状態になるまで、Initボタンを押したままにしておきます。
   点灯→消灯→点灯
3. STATUS1 LEDが再度点灯したら、Initボタンを放します。STATUS1 LEDが消灯し、本装置が工場出荷設定で起動します。

③ DC5V電源コネクタ（ロック機構付き）
製品付属のACアダプタを接続します。
電源コネクタの溝に、DCプラグのツメを合わせて、右に回してください。電源コードがロックされます。
電源コードを外す時は、DCプラグ部分を持って左に戻してから抜いてください。

本装置をご使用の際は必ず、電源コードをロックしてご使用ください。

④ CONSOLEポート
CLI接続の場合に使用します。
Ethernet規格のLANケーブルを接続します。

⑤ SPD LED（■/■）
ETHERNETポートの接続速度を表示します。
10BASE-Tモードで接続時　：　■
100BASE-TXモードで接続時　：　■
1000BASE-Tモードで接続時　：　■

⑥ LINK LED（緑）
ETHERNETポートの接続状態を表示します。
Link Down時　：　■
Link UP時　：　■
データ通信時　：　■/■(点滅)

⑦ ETHER 0ポート
主にLAN側ポートとして使用します。

⑧ ETHER 1ポート
主にWAN側ポートとして使用します。

⑨ ETHER 2ポート
主にDMZポートとして使用します。

本装置の各ETHERポートは、全てGigabit Ethernetに対応しています。別セグメントを接続するポートとして使用可能です。
また、ポートはAutoMDI/MDI-X対応です。
Ethernet規格のLANケーブルを接続してください。

Ｖ．各部の名称と機能（NXR-130/C:ISDN ポートあり）

⑩ USB ポート
USB Flash メモリ、または USB タイプのデータ通信モジュールを挿入します。

⑪ RELEASE ボタン
USB flash メモリを取り外すときに使用します。
本装置から USB flash メモリを取り外すときは、以下の手順で操作してください。

1. RELEASE ボタンの長押し(約３秒)
2. USB LED の消灯を確認
3. USB flash メモリの取り外し

⑫ ISDN BRI S/T 点(RJ-45)
このポートと外部 DSU を ISDN ケーブルで接続します。

⑬ S/T 点終端抵抗 ON/OFF スイッチ
「ISDN S/T 点ポート」接続時の終端抵抗の ON/OFF を切り替えます。
外部 DSU を接続している場合は、本装置を含めていずれか１つの機器の終端抵抗を ON にしてください。

⑭ B1 LED（●）
⑱ B2 LED（●）
「B1」および「B2」は、本装置の BRI ポートを使って回線接続しているときに点灯します。
回線接続していないときは消灯しています。

⑮ USB LED（●）
USB ステータスを表示します。

USB flash メモリ装着時	：	●
USB flash メモリ未装着時	：	●

⑯ STATUS1 LED（●）
本装置のシステム起動時のステータスを表示します。

システム起動中	：	●
システム起動完了状態	：	●
ファームウェアのアップデート作業中	：	● / ●(点滅)

これら以外の状態で、STATUS1 が点滅している時はシステム異常が起きていますので、弊社までご連絡ください。

⑰ AUX LED（●）
本装置では使用しません。

⑲ L1 LED（●）
本装置の ISDN BRI S/T 点ポートがリンクアップしているときに点灯します。

⑳ STATUS2 LED（●）
本装置のシステムおよび、サービス起動時のステータスを表示します。

システム起動中	：	●
サービス起動中	：	● / ●(点滅)
サービス起動完了状態	：	●

STATUS LED が以下の状態になると、本装置へのアクセスが可能になります。

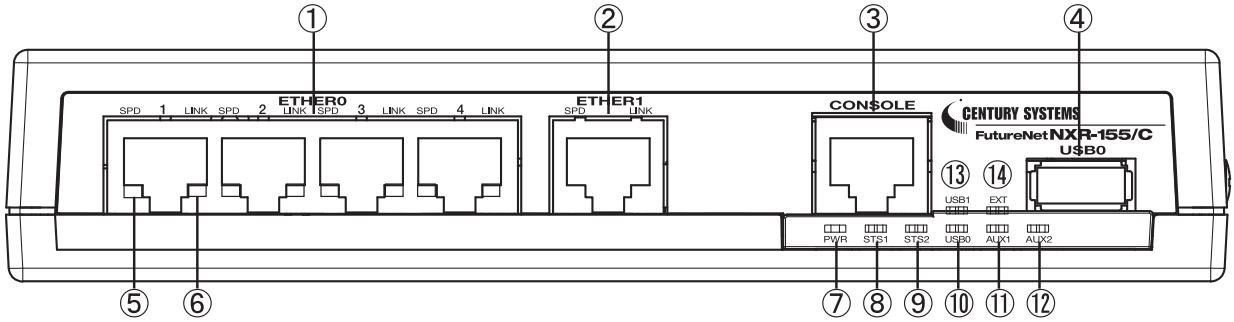
STATUS1 LED	：	●
STATUS2 LED	：	●

㉑ POWER LED（●）
本装置の電源状態を表示します。

電源投入時	：	●

VI．各部の名称と機能（NXR-155/C-WM）

◆製品前面



① ETHER 0 ポート
10BASE-T/100BASE-TX/1000BASE-T 対応の 4 ポートハブです。主に LAN 側ポートとして使用します。

② ETHER 1 ポート
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポートです。主に WAN 側ポートとして使用します。

③ CONSOLE ポート
CLI 接続の際に使用します。
Ethernet 規格の LAN ケーブルを接続します。

④ USB0 ポート
USB Flash メモリ、または USB タイプのデータ通信端末を挿入します。

⑤ SPD LED(赤 / 緑)
ETHER ポートの接続速度を示します。
10BASE-T モードで接続時 ：■
100BASE-TX モードで接続時: ■
1000BASE-T モードで接続時: ■

⑥ LINK LED(緑)
ETHER ポートのリンク状態を示します。
Link Down 時 ： ■
Link UP 時 ： ■

⑦ PWR LED(青)
本装置の電源状態を示します。
電源 ON 時 ： ■

⑧ STS1 LED(赤 / 緑)
本装置のシステム起動時のステータスを示します。
電源 ON 時 ： ■
システム起動中 ： ■
ファームウェア更新中：＊(点滅)
指定した PPP または tunnel の状態を示します（設定は、第 6 章 global node の system led を参照)。
接続時 ： ■
切断状態時 ： ■

⑨ STS2 LED(緑)
本装置のシステムおよび、サービス起動時のステータスを示します。
電源 ON 時 ： ■
システム起動中 ： ＊（点滅）
システム起動後(ログイン可能状態)
： ■

⑩ USB0 LED(緑)
USB デバイス 0 のステータスを示します。
USB デバイス 0 の接続時 ： ■
USB デバイス 0 の未接続時： ■

⑪ AUX1 LED(緑)/ ⑫ AUX2 LED(緑)
データ通信端末装着時に、電波状況を表示します（設定は、第 6 章 global node の system led を参照)。

	AUX1	AUX2
データ通信端末未装着時 ：	■	■
圏外 （および unknown） ：	■	■
圏内 Signal Level 0-1 ：	■	■
Signal Level 2 ：	■	■
Signal Level 3 ：	■	■

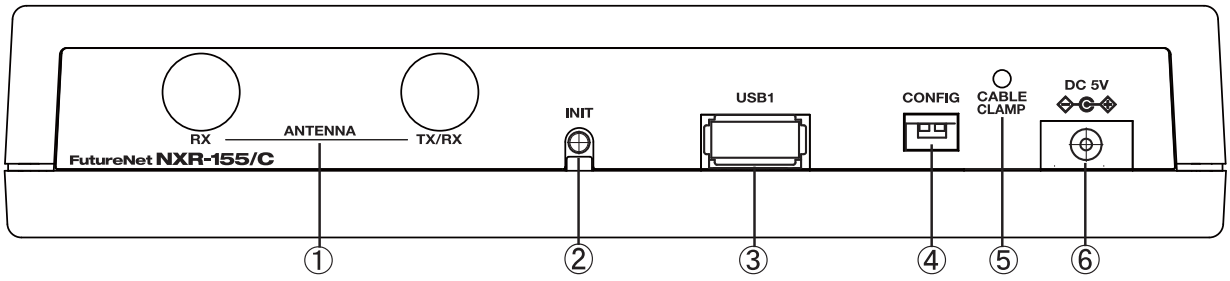
指定した PPP または tunnel の状態を示します。
接続時 ： ■
切断状態時 ： ■

⑬ USB1 LED(緑)
USB デバイス 1 のステータスを示します。
USB デバイス 1 の接続時 ： ■
USB デバイス 1 の未接続時： ■

⑭ EXT LED
内蔵通信モジュールのステータスを表示します。
通常動作時 ： ■
異常発生時やリセット時 ： ■

Ⅵ．各部の名称と機能（NXR-155/C-WM）

◆製品背面



① ANTENNA RX，ANTENNA TX/RX
対応するアンテナを装着します。

② INIT ボタン
本装置を工場出荷時の設定に戻して起動するときに使用します。

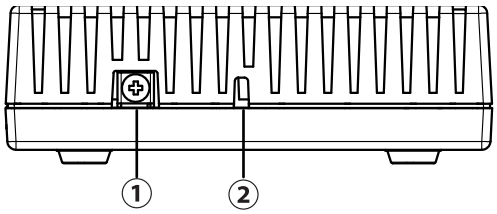
③ USB1 ポート
USB Flash メモリ、または USB タイプのデータ通信端末を挿入します。

④ CONFIG
本製品では使用しません。両方のスイッチが下に位置している状態で使用してください。

⑤ CABLE CRAMP
AC アダプタのケーブルが不意に引っ張られても、DC プラグが抜けないようにすることが出来ます。
クリップでケーブルを挟み、クリップと本装置をネジで固定します。

⑥ DC 5V 電源コネクタ
製品付属の AC アダプタを接続します。

◆製品側面

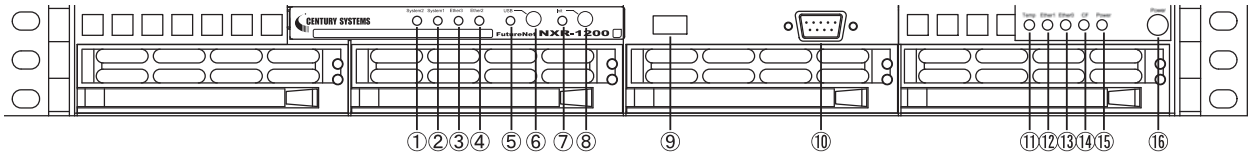


① FG(アース）端子
保安用接続端子です。
必ずアース線を接続してください。

② セキュリティスロット
ケンジントンロックに対応しています。

Ⅶ．各部の名称と機能（NXR-1200）

◆製品前面



ランプ表示 凡例

消灯時 ： ●、点灯時 ： ●、点滅時 ： ＊

① SYSTEM 2 LED(●)

システムの起動状態を示します。

システム起動中 ： ＊

システム起動後(ログイン可能状態) ： ●

② SYSTEM 1 LED(●)

使用しません。

③ Ether 3 LED(●)、④ Ether 2 LED(●)
⑫ Ether 1 LED(●)、⑬ Ether 0 LED(●)

各 Ether ポートの状態を示します。

Link UP ： ●

Link DOWN ： ●

データ通信中 ： ＊

⑤ USB Status LED(●)

USB フラッシュメモリの接続状態を表示します。

接続時 ： ● → ＊ → ●

動作状態 ： ●

「USB スイッチ」による取り外し操作時

： ● → ＊ → ●

⑥ USB スイッチ

本装置から、USB フラッシュメモリを取り外すときに使用します。以下の手順で操作してください。

1．USB スイッチの長押し(約 3 秒)
2．USB LED の消灯を確認
3．USB フラッシュメモリの取り外し

⑦ Init Status LED(●)

起動状態を表示します。

起動中 ： ＊

「Init スイッチ」で初期設定にて起動中 ： ●

起動完了時 ： ●

⑧ Init スイッチ

本装置を工場出荷時の設定に戻して起動するときに使用します。

1. Init スイッチを押しながら電源を投入します。
2. Init Status LED が下記の状態になるまで、Init スイッチを押したままにしておきます。
   点灯→消灯→点灯
3. Init Status LED が再度点灯したら、Init スイッチを放します。Init Status LED が消灯し、本装置が工場出荷設定で起動します。

⑨ USB インタフェース

オプションの USB フラッシュメモリを接続します。センチュリー・システムズがサポートする USB フラッシュメモリを使用してください。

⑩ RS-232 ポート(D-Sub 9 ピン)

本装置に CLI 接続するためのコンソールポートです。

⑪ Temp LED(●)

温度状態を表示します。

本装置の内部温度が一定以上になった時 ： ●

⑭ CF LED(●)

搭載している CF カードの使用状態を表示します。

CF へのアクセス時 ： ●

⑮ Power LED(●)

電源の状態を表示します。

電源が投入されている状態 ： ●

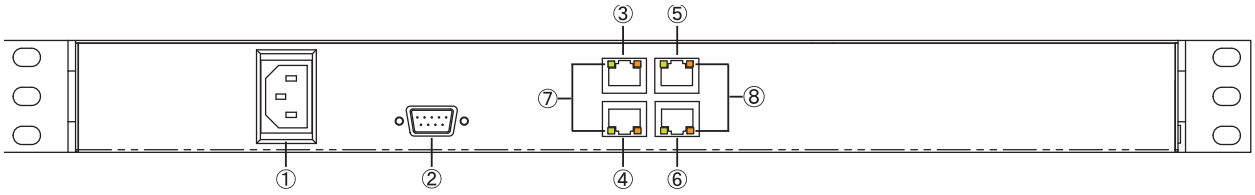
⑯ Power スイッチ

本装置の停止中にスイッチを押すと、本装置が起動します。

本装置の稼働中にスイッチを短押（１秒程度）すると、正常終了します。

Ⅶ．各部の名称と機能（NXR-1200）

◆製品背面



① 電源ケーブル差し込み口
付属の電源ケーブルを差し込んでください。

② RS-232 ポート(D-Sub 9 ピン)
使用しません。

③ Ether0 ポート(RJ-45)
④ Ether1 ポート(RJ-45)
⑤ Ether2 ポート(RJ-45)
⑥ Ether3 ポート(RJ-45)
Ethernet 規格の LAN ケーブルを接続します。ポートは AutoMDI/MDI-X 対応です。

⑦ LINK ランプ（●）
Ether ポートのリンク状態を表示します。
Link DOWN ： ●
Link UP ： ●
データ送受信時 ： ＊

⑧ 速度表示ランプ（● / ●）
Ethernet の接続速度を表示します。
10Base-T モード ： ●
100Base-TX モード ： ●
1000Base-T モード ： ●

Ⅷ．動作環境

本製品をお使いいただくには、以下の環境を満たしている必要があります。

◆ハードウェア環境

・本製品に接続するコンピュータの全てに、LAN インタフェースがインストールされていること。

・ADSL モデム /CATV モデム /ONU に、10BASE-T、100BASE-TX または 1000BASE-T のインターフェースが搭載されていること。

・本製品と全てのコンピュータを接続するためのハブやスイッチングハブが用意されていること。

・本製品と全てのコンピュータを接続するために必要な種類のネットワークケーブルが用意されていること。

◆ソフトウェア環境

・TCP/IP を利用できる OS がインストールされていること。

・GUI で本装置にログインする場合は、接続されている全てのコンピュータの中で少なくとも 1 台に、ブラウザがインストールされていること。弊社では Internet Explorer 8 で動作確認を行っています。

なおサポートにつきましては、本製品固有の設定項目と本製品の設定に関係する OS 上の設定に限らせていただきます。
OS 上の一般的な設定やパソコンにインストールされた LAN ボード / カードの設定、各種アプリケーションの固有の設定等のお問い合わせについてはサポート対象外とさせていただきますので、あらかじめご了承ください。

第2章

装置の設置

Ⅰ．装置の設置に関する注意点

本装置の各設置方法について説明します。
下記は設置に関する注意点です。よくご確認いただいてから設置してください。

注意！

本装置は直射日光が当たるところや、温度の高いところには設置しないようにしてください。
内部温度が上がり、動作が不安定になる場合があります。

注意！

ACアダプタのプラグを本体に差し込んだ後にACアダプタのケーブルを左右および上下に引っ張らず、緩みがある状態にしてください。
抜き差しもケーブルを引っ張らず、コネクタを持って行ってください。
また、ACアダプタのケーブルを足などで引っ掛けてプラグ部に異常な力が掛からないように配線にご注意ください。

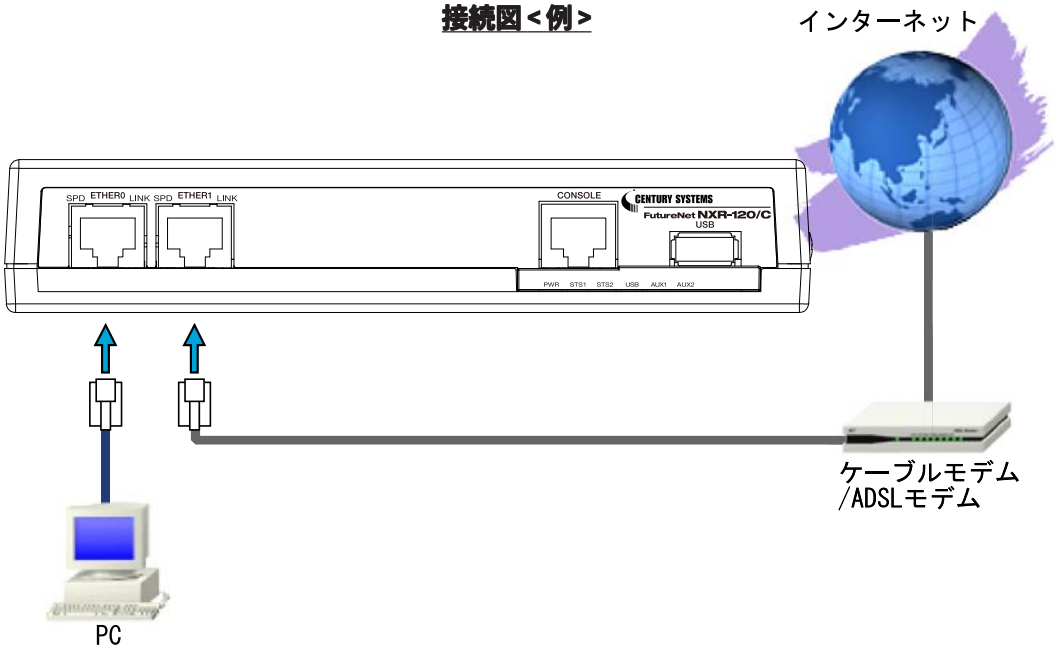
注意！

本装置側でも各ポートでARP tableを管理しているため、PCを接続しているポートを変更するとそのPCから通信ができなくなる場合があります。このような場合は、本装置側のARP tableが更新されるまで(数秒～数十秒)通信できなくなりますが、故障ではありません。

Ⅱ．装置の設置（NXR-120/C）

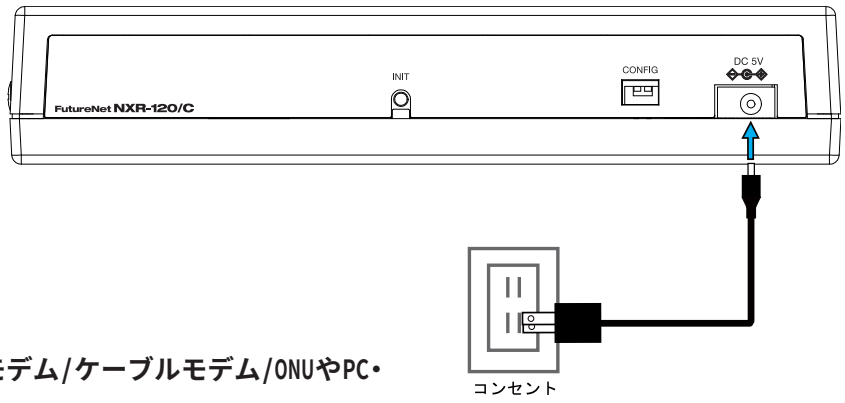
NXR-120/C と PC や xDSL モデム / ケーブルモデム /ONU は、以下の手順で接続してください。

接続図＜例＞



◆ 前面

◆ 背面



1 本装置とxDSLモデム/ケーブルモデム/ONUやPC・HUBなど、接続する全ての機器の電源が‘OFF’になっていることを確認してください。

2 本装置の前面にある ETHER 1 ポートと、xDSL/ケーブルモデムや ONU を、LAN ケーブルで接続してください。

3 本装置の前面にある ETHER 0 ポートと PC を LAN ケーブルで接続してください。

※ 工場出荷設定状態の場合、本装置へのログインは、ETHER 0ポートに接続したPCからおこないます。

4 本装置と AC アダプタ、AC アダプタとコンセントを接続してください。

5 全ての接続が完了しましたら、各機器の電源を投入してください。

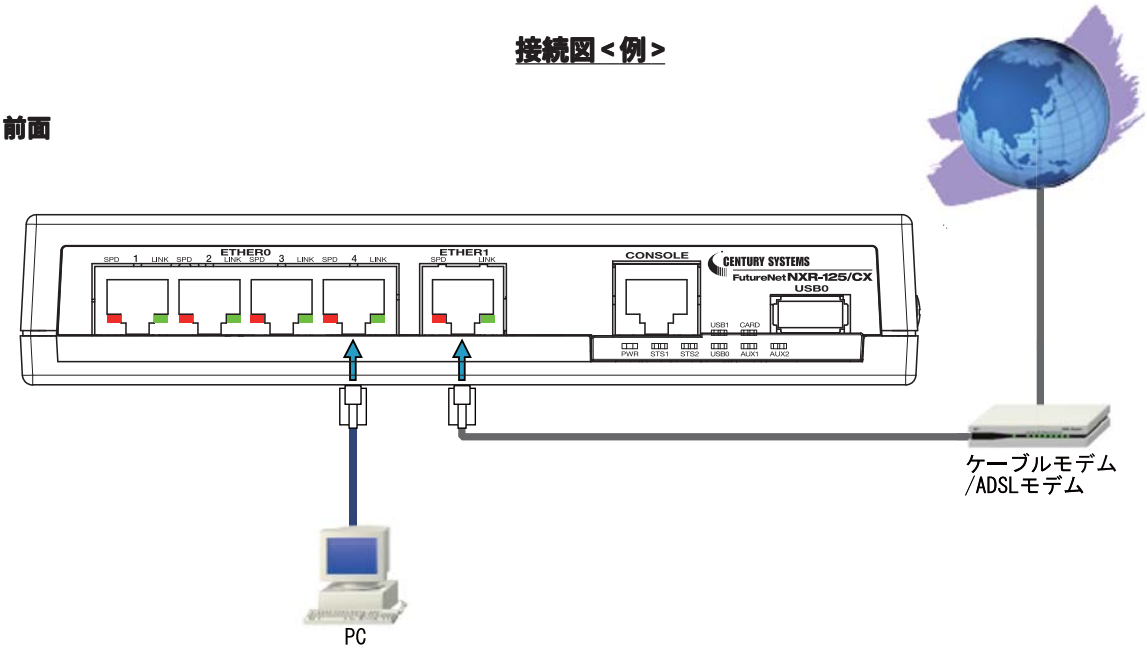
本装置の全ての Ethernet ポートは、AutoMDI/MDI-X 対応です。

III．装置の設置（NXR-125/CX）

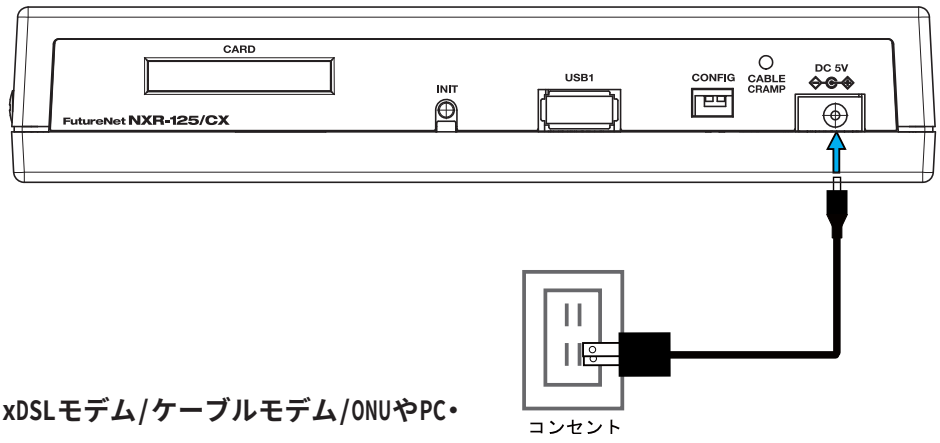
NXR-125/CX と PC や xDSL モデム / ケーブルモデム /ONU は、以下の手順で接続してください。

接続図＜例＞

◆ 前面



◆ 背面



1 本装置とxDSLモデム/ケーブルモデム/ONUやPC・HUBなど、接続する全ての機器の電源が‘OFF’になっていることを確認してください。

2 本装置の前面にある ETHER 1 ポートと、ADSL モデム / ケーブルモデム /ONU を、LAN ケーブルで接続してください。

3 本装置の前面にある ETHER 0 ポートと、HUB や PC を LAN ケーブルで接続してください。

※ 工場出荷設定状態の場合、本装置へのログインは、ETHER 0ポートに接続したPCからおこないます。

4 本装置と AC アダプタ、AC アダプタとコンセントを接続してください。

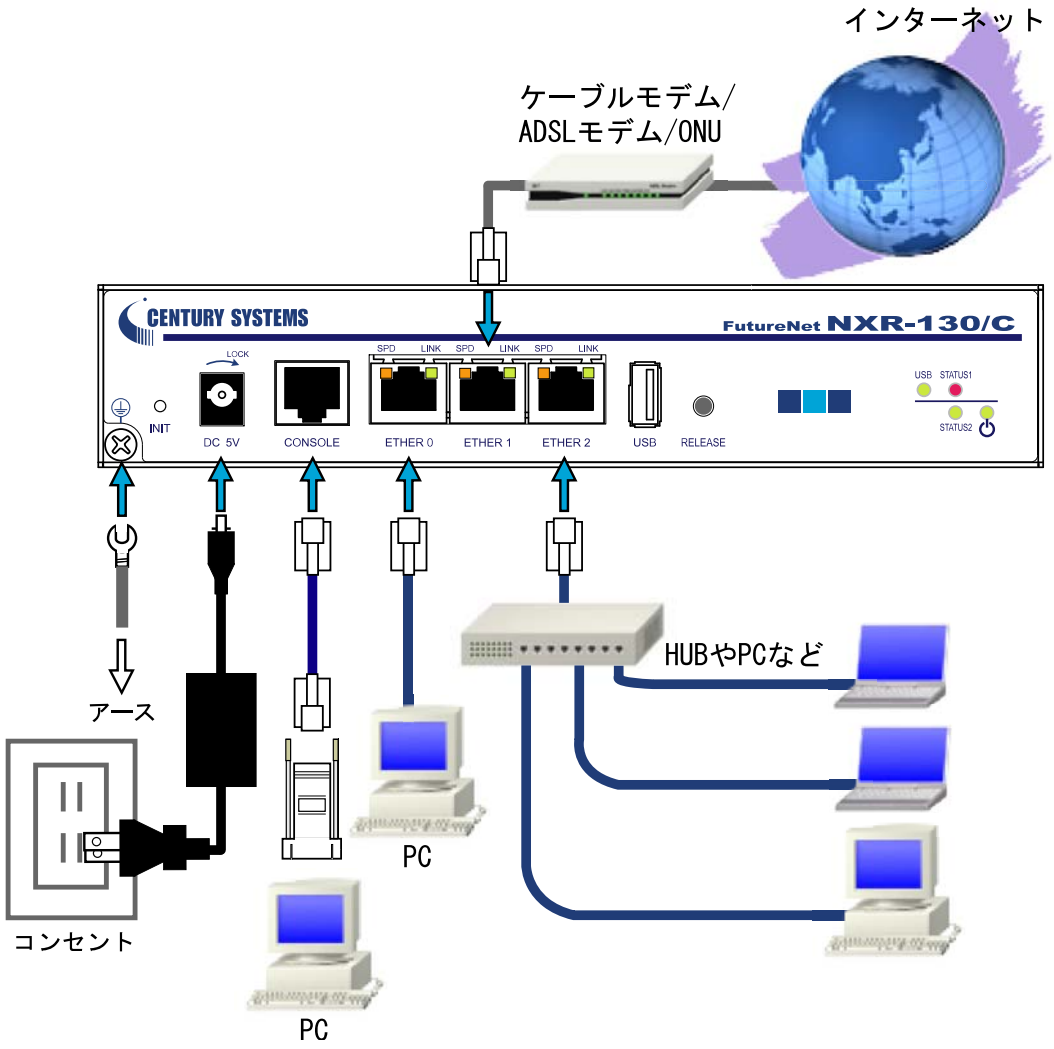
5 全ての接続が完了しましたら、各機器の電源を投入してください。

本装置の全ての Ethernet ポートは、AutoMDI/MDI-X 対応です。

Ⅳ．装置の設置（NXR-130/C）

NXR-130/C と PC や xDSL モデム / ケーブルモデム /ONU は、以下の手順で接続してください。

接続図＜例＞



1 本装置とxDSLモデム/ケーブルモデム/ONUやPC・HUBなど、接続する全ての機器の電源が“OFF”になっていることを確認してください。

2 本装置の前面にある ETHER 1 ポートと、xDSL モデム / ケーブルモデム /ONU を、LAN ケーブルで接続してください。

3 本装置の前面にある ETHER 0 ポート、ETHER 2 ポートと、PC を LAN ケーブルで接続してください。

※ 工場出荷設定状態の場合、本装置へのログインは、ETHER 0ポートに接続したPCからおこないます。

4 本装置と AC アダプタ、AC アダプタとコンセントを接続してください。

5 全ての接続が完了しましたら、各機器の電源を投入してください。

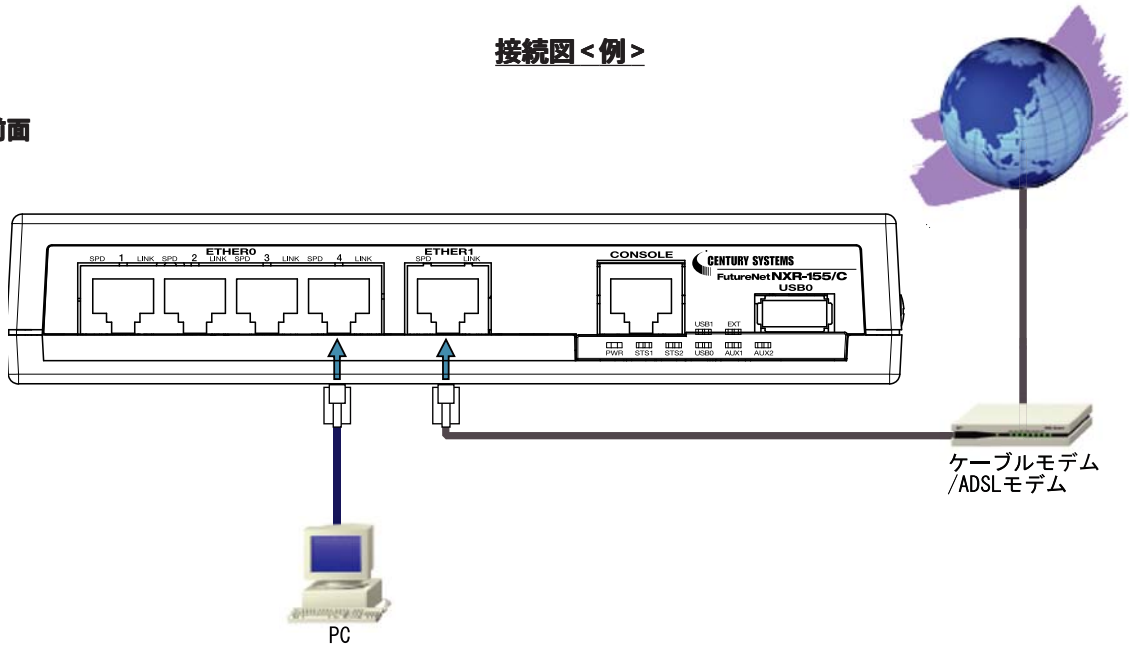
本装置の全ての Ethernet ポートは、AutoMDI/MDI-X 対応です。

Ⅴ．装置の設置（NXR-155/C-WM）

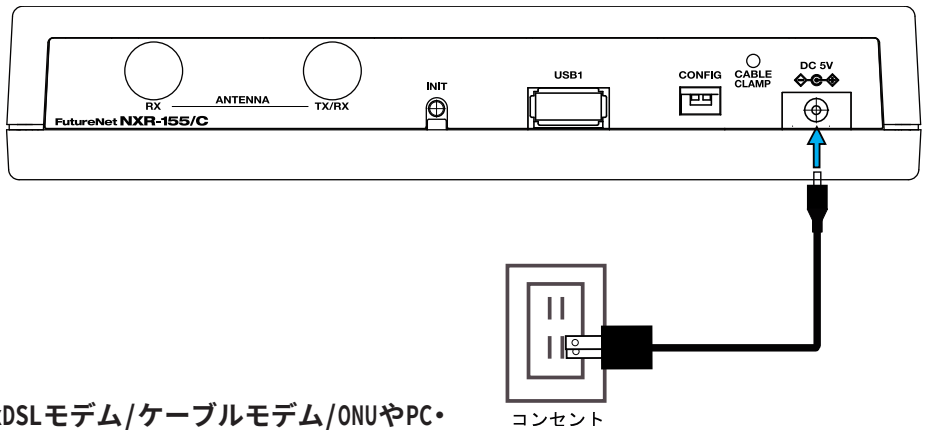
NXR-155/C-WM と PC や xDSL モデム / ケーブルモデム /ONU は、以下の手順で接続してください。

接続図＜例＞

◆ 前面



◆ 背面



1 本装置とxDSLモデム/ケーブルモデム/ONUやPC・HUBなど、接続する全ての機器の電源が“OFF”になっていることを確認してください。

2 本装置の前面にある ETHER 1 ポートと、ADSL モデム / ケーブルモデム /ONU を、LAN ケーブルで接続してください。

3 本装置の前面にある ETHER 0 ポートと、HUB や PC を LAN ケーブルで接続してください。

※ 工場出荷設定状態の場合、本装置へのログインは、ETHER 0ポートに接続したPCからおこないます。

4 本装置とACアダプタ、ACアダプタとコンセントを接続してください。

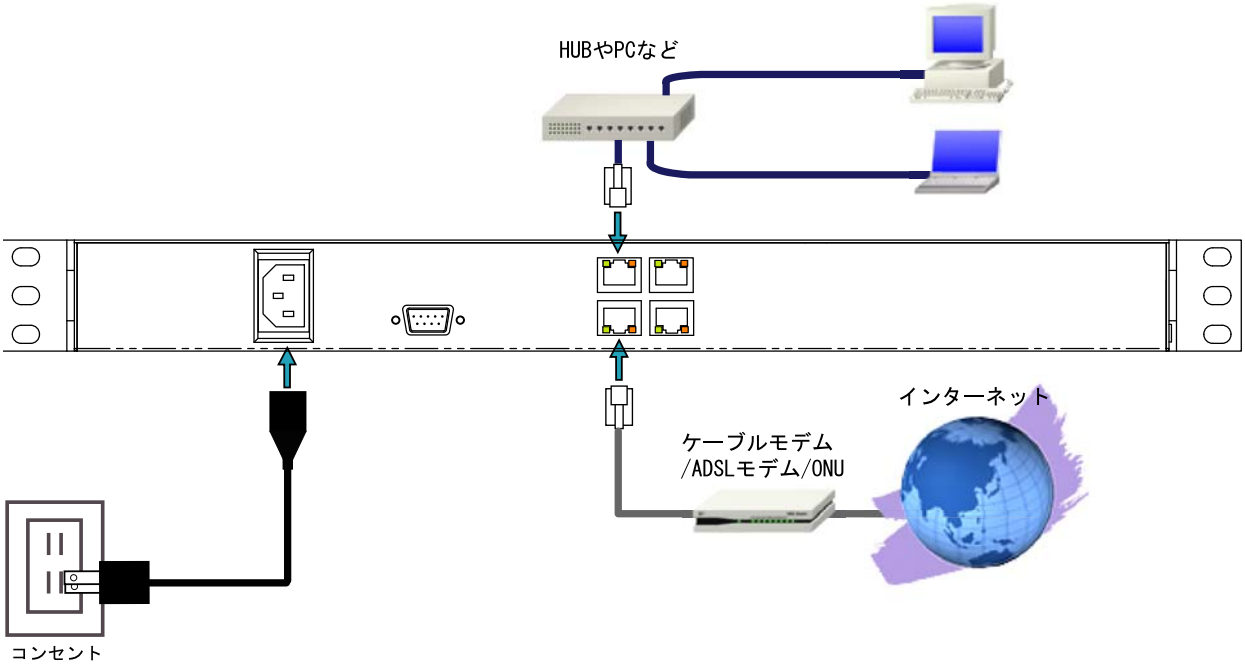
5 全ての接続が完了しましたら、各機器の電源を投入してください。

本装置の全ての Ethernet ポートは、AutoMDI/MDI-X 対応です。

Ⅵ．装置の設置（NXR-1200）

NXR-1200 と、PC や ADSL モデム / ケーブルモデム /ONU は、以下の手順で接続してください。

接続図＜例＞



1 本装置と ADSL モデム / ケーブルモデム /ONU や PC・HUB など、接続する全ての機器の電源が“ OFF ”になっていることを確認してください。

2 本装置の前面にある Ether 1 ポートと、ADSL モデム / ケーブルモデム /ONU を、LAN ケーブルで接続してください。

3 本装置の前面にある Ether 0 ポートと、HUB や PC を LAN ケーブルで接続してください。

※ 工場出荷設定状態の場合、本装置へのログインは、Ether 0 ポートに接続した PC からおこないます。

本装置の全 Ethernet ポートは Gigabit Ethernet、AutoMDI/MDI-X に対応しています。

4 本装置と電源コード、電源コードとコンセントを接続してください。

5 全ての接続が完了しましたら、各機器の電源を投入してください。NXR-1200 の本体前面にある Power スイッチを押すと、本装置が起動します。

第3章

設定方法の概要

第３章 設定方法の概要

Ⅰ．本装置へのログイン(CLI)

◆はじめに

本章では、FutureNet NXR シリーズに搭載された Command Line Interface(以下、CLI)について説明しています。

◆CLI のアクセス方法

本装置の CLI へのアクセスは、以下の方法で接続できます。

・Console 接続
　本装置の Console(RS-232C)ポートと接続した PC からアクセスします。

・Telnet 接続
　本装置の Ethernet0 ポートと接続した PC から IPv4 を用いてアクセスします。
　※ 工場出荷設定では、Ethernet 0 に IPv4 アドレス(192.168.0.254)が設定されています。

・SSH 接続
　※ SSH 接続時の認証方法は、plain-text password と RSA public-key をサポートしています。

本装置の工場出荷設定状態時は、Console か、IPv4 使用した Telnet での CLI へのアクセスが可能です。

Ⅰ．本装置へのログイン(CLI)

◆本装置へのログイン(Console 接続:NXR-120/C)

Console ポートを利用して、NXR-120/C へログインします。以下の手順で接続します。

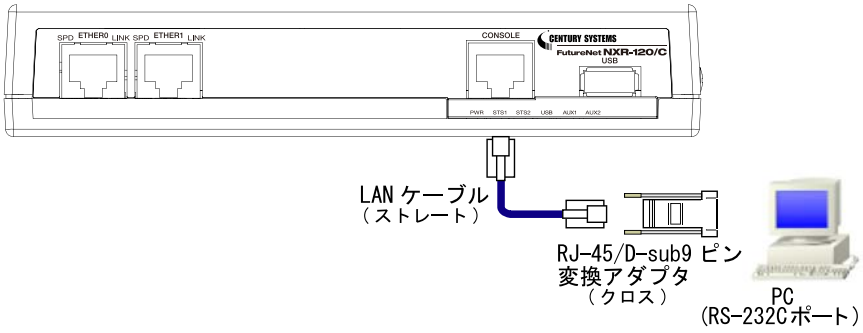
1. NXR-120/C と PC を接続します。

1．本装置前面の Console ポートと、変換アダプタを、LAN ケーブルで接続します。接続に使用する以下の部品は、製品に付属されています。

・LAN ケーブル(ストレート)
・RJ-45/D-sub9 ピン変換アダプタ(クロス)

2．変換アダプタのコネクタを、PC の RS-232C ポートに接続してください。

<接続例: NXR-120/C>



3．全ての接続が完了しましたら、本装置に電源を投入してください。本体前面の「PWR LED」が点灯します。

以上で Console ポートと PC の接続は完了です。続いて、本装置へのログインに移ります。

< 本装置へのログイン(Console 接続:NXR シリーズ共通)に続く >

Ⅰ．本装置へのログイン(CLI)

◆本装置へのログイン(Console 接続:NXR-125/CX)

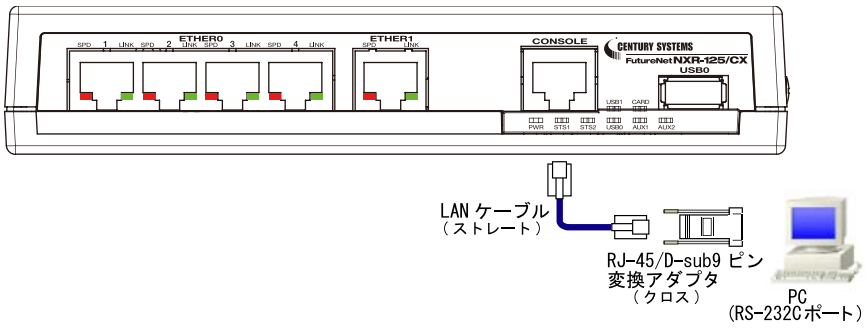
Console ポートを利用して、NXR-125/CX へログインします。以下の手順で接続します。

1’．NXR-125/CX と PC を接続します。

1．本装置前面の Console ポートと、変換アダプタを、LAN ケーブルで接続します。接続に使用する以下の部品は、製品に付属されています。
- LAN ケーブル(ストレート)
- RJ-45/D-sub9 ピン変換アダプタ(クロス)

2．変換アダプタのコネクタを、PC の RS-232C ポートに接続してください。

<接続例：NXR-125/CX>



3．全ての接続が完了しましたら、本装置に電源を投入してください。本体前面の「PWR LED」が点灯します。

以上で Console ポートと PC の接続は完了です。続いて、本装置へのログインに移ります。

< 本装置へのログイン(Console 接続:NXR シリーズ共通)に続く >

Ⅰ．本装置へのログイン(CLI)

◆本装置へのログイン(Console 接続:NXR-130/C)

Console ポートを利用して、NXR-130/C へログインします。以下の手順で接続します。

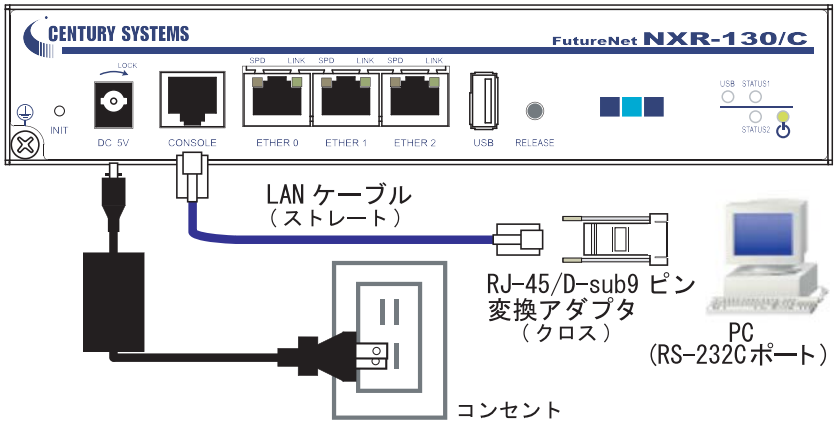
1’’. NXR-130/C と PC を接続します。

1．本装置前面の Console ポートと、変換アダプタを、LAN ケーブルで接続します。接続に使用する以下の部品は、製品に付属されています。

- LAN ケーブル(ストレート)
- RJ-45/D-sub9 ピン変換アダプタ(クロス)

2．変換アダプタのコネクタを、PC の RS-232C ポートに接続してください。

<接続例: NXR-130/C>



3．全ての接続が完了しましたら、本装置に電源を投入してください。本体前面の「POWER LED」が点灯します。

以上で Console ポートと PC の接続は完了です。続いて、本装置へのログインに移ります。

< 本装置へのログイン(Console 接続:NXR シリーズ共通)に続く >

Ⅰ．本装置へのログイン(CLI)

◆本装置へのログイン(Console 接続:NXR-155/C-WM)

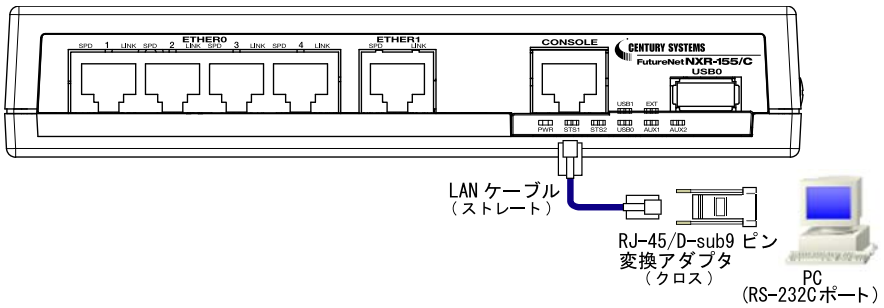
Console ポートを利用して、NXR-155/C-WM へログインします。以下の手順で接続します。

1．．．．NXR-155/C-WM と PC を接続します。

1. 本装置前面の Console ポートと、変換アダプタを、LAN ケーブルで接続します。接続に使用する以下の部品は、製品に付属されています。
   - LAN ケーブル(ストレート)
   - RJ-45/D-sub9 ピン変換アダプタ(クロス)

2. 変換アダプタのコネクタを、PC の RS-232C ポートに接続してください。

<接続例：NXR-155/C-WM>



3. 全ての接続が完了しましたら、本装置に電源を投入してください。本体前面の「POWER LED」が点灯します。

以上で Console ポートと PC の接続は完了です。続いて、本装置へのログインに移ります。

< 本装置へのログイン(Console 接続:NXR シリーズ共通)に続く >

Ⅰ．本装置へのログイン(CLI)

◆本装置へのログイン(Console 接続:NXR-1200)

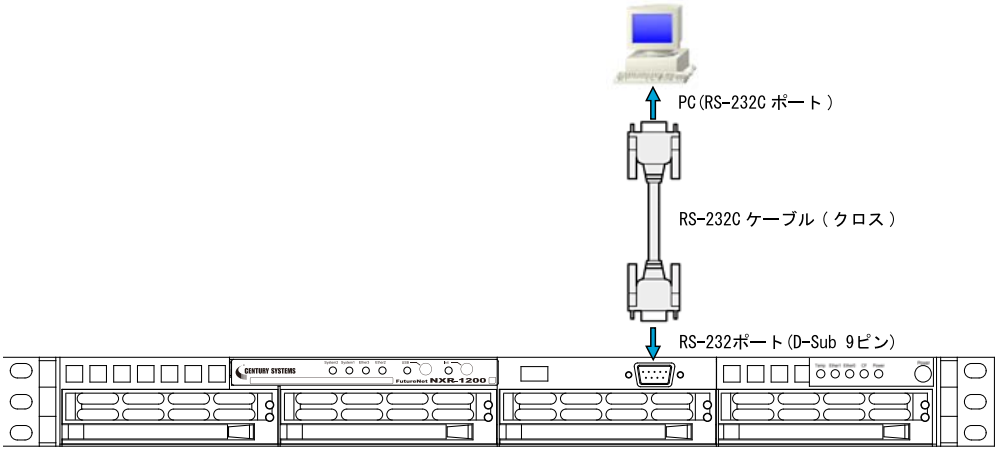
本体前面の RS-232 ポートを利用して、NXR-1200 へログインします。以下の手順で接続します。

1 ’’’’．NXR-1200 と PC を接続します。

1．本装置前面の RS-232 ポートと、RS-232C ケーブル(クロス)を接続します。

2．RS-232C ケーブルを、PC の RS-232C ポートに接続してください。

<接続例：NXR-1200>



3．全ての接続が完了しましたら、本装置に電源を投入してください。本体前面の「Power LED」が点灯します。

以上で Console ポートと PC の接続は完了です。続いて、本装置へのログインに移ります。

< 本装置へのログイン(Console 接続:NXR シリーズ共通)に続く >

Ⅰ．本装置へのログイン(CLI)

◆本装置へのログイン(Console 接続:NXR シリーズ共通)

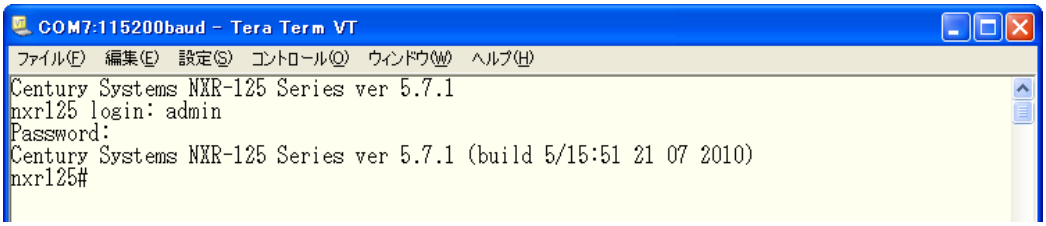
2．本装置を接続した PC で、設定用のターミナルソフト(TeraTerm 等)を起動します。

3．接続条件設定は以下のように設定します。< 設定例(TeraTerm での接続設定画面)>

※ 設定方法については、ご使用の各ターミナルソフトの説明書をご覧ください。

4．「Return」キーまたは「Enter」キーを押すと、ログイン画面が表示されます。

5．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。

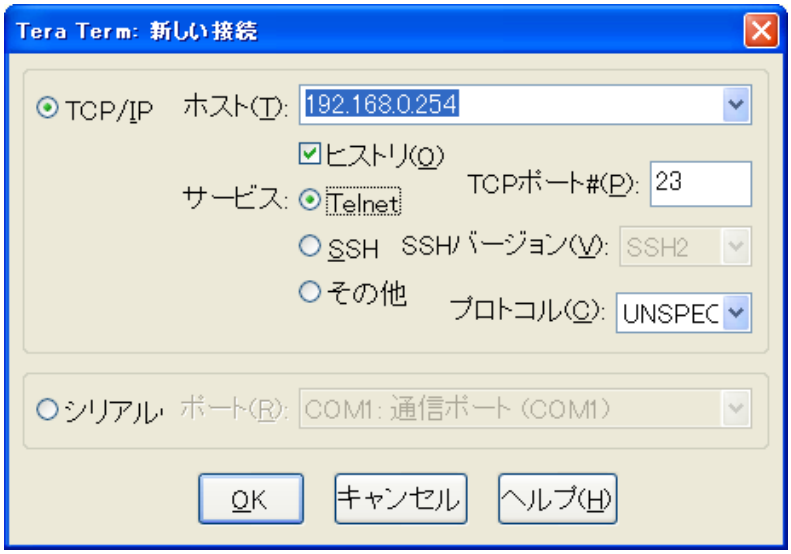


以上で本装置へのログイン(Console接続)は完了です。

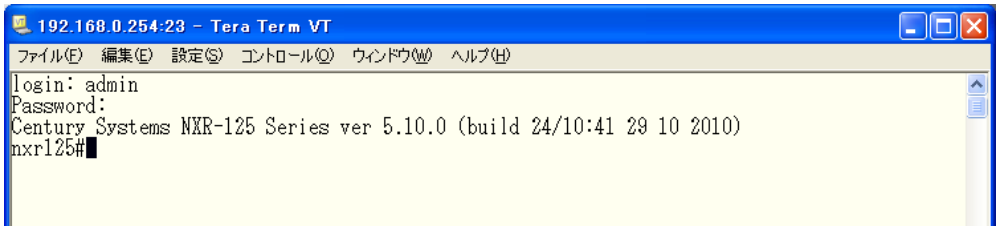
Ⅱ．本装置へのログイン(CLI)

◆本装置へのログイン(Telnet 接続)

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。

Ⅱ．本装置へのログイン(GUI)

◆本装置へのログイン（GUI）

1 .Web ブラウザを起動します。

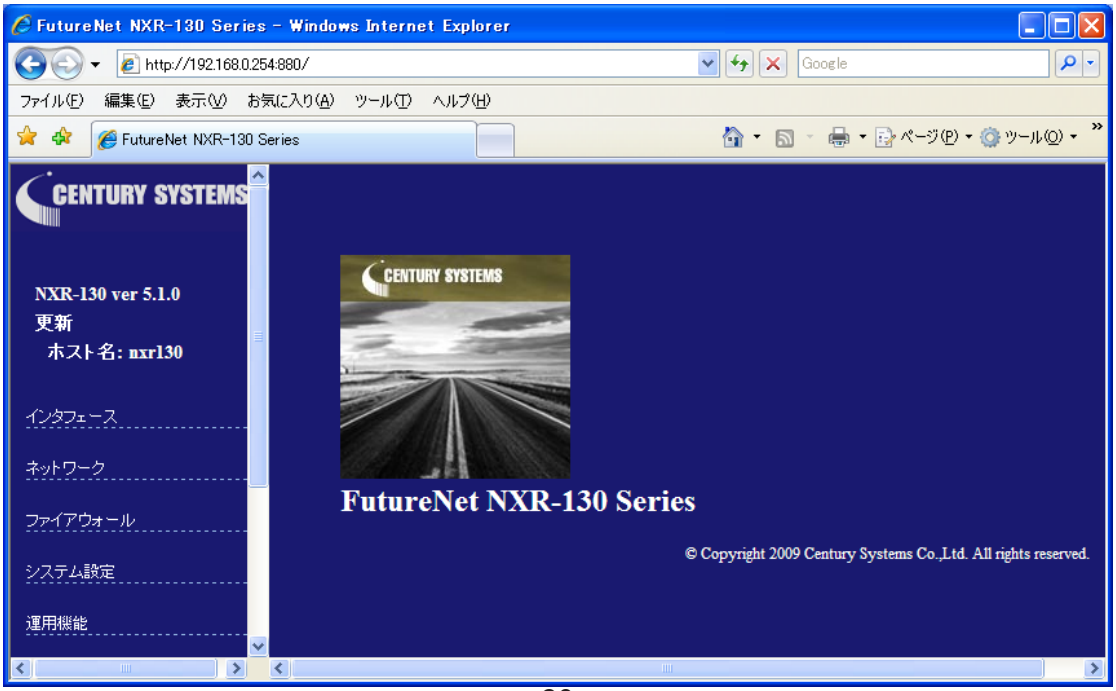
ブラウザのアドレス欄に、以下の IP アドレスとポート番号を入力してください。

http://192.168.0.254:880/

※ 192.168.0.254 は、Ethernet 0 ポートの工場出荷時の IP アドレスです。アドレスを変更した場合は、そのアドレスを指定してください。**設定画面のポート番号 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」（工場出荷設定）を入力してログインします。

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。



II．本装置へのログイン(GUI)

本装置の GUI で設定可能な項目の一覧です。

[インタフェース]
Ethernet I/F
　・Ethernet
PPP I/F
　・PPP アカウント
　・PPPoE

[ネットワーク]
IPv4
　・スタティックルート
　・固定 ARP
DHCP
　・DHCP ネットワーク
　・DHCP ホスト
　・DHCP リレー
DNS
WarpLink
NTP

[ユーザインタフェース]
SSH
　・SSH サービス
　・SSH 鍵（netconf）
NETCONF
　・NETCONF
CRP
　・CRP グローバル
　・CRP クライアント

[ファイアウォール]
アクセスリスト
　・IPv4 アクセスリスト

[システム設定]
・本装置のパスワード
・ホスト名
ログ
　・システムログ
　・ログメール
設定情報
　・設定の保存
　・設定の復帰
　・設定のリセット
ファームウェア
　・アップデート
・内蔵時計
・再起動

[運用機能]
ネットワーク診断
　・Ping
　・Traceroute
パケットダンプ
　・実行
　・結果表示
ログ情報
　・システムログ
システム情報
　・システム情報
　・システムモニター
・サポート情報

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。

＜CLIログアウト時の表示例＞

```
nxr130#exit

Century Systems NXR-130 Series ver 5.1.0
nxr130 login:
```

＜特権モードへ移行時の表示例＞

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#
```

◆特権モード(CONFIGURATIONモード)

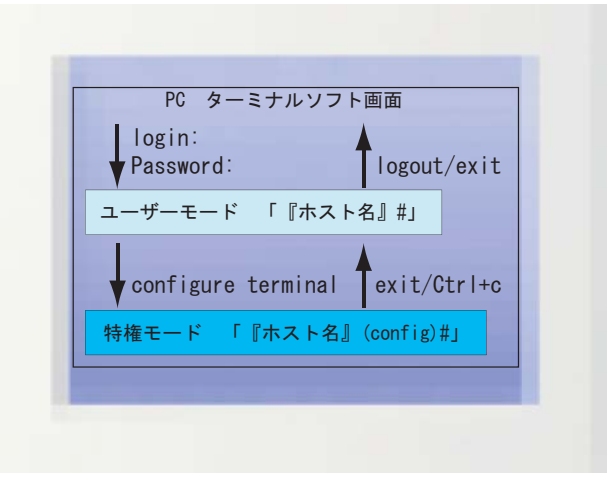
特権モードでは、ユーザモードで実行可能なコマンドに加え、内部システム情報、
コンフィグレーション情報を表示するコマンドや、本装置に対して設定をおこなうコマンドの実行が可能になります。
本モードでのプロンプトは、「『ホスト名』(config)#」で表示されます。
“exit”コマンドを入力するか、「Ctrl」+「c」を入力するとユーザーモードに戻ることができます。

＜ユーザーモードへ移行時の表示例＞

```
nxr130(config)#exit
nxr130#
```

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。

＜モード間の移行＞



各モード間の移行をまとめると次のようになります。

本書では、ホスト名を『nxr130』として説明します。

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＞

```
nxr130#show ?
  arp               Address Resolution Protocol (ARP)
  clock             System Clock
  config            Configurations
  dhcp              Dynamic Host Configuration Protocol (DHCP)
  disk0             External Storage information
  dns               Domain Name System (DNS)
  fast-forwarding   Fast-forwarding
--More--
```

＜直後に「?」キー入力時の表示例＞

```
nxr130#show?
  show  Show running system information
```

◆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。

第4章

本装置のノード構造

ノード構造について

本装置のノード構造は以下ようになっています。
各設定方法について、本書では上記の各ノード毎に説明します。

```
view node
    |----  global node
                |-----  interface node
                |-----  interface tunnel node
                |-----  interface ppp node
                |-----  dns node
                |-----  l2tp node
                |-----  l2tpv3-tunnel node
                |-----  l2tpv3-xconnect node
                |-----  l2tpv3-group node
                |-----  rip node
                |-----  ospf node
                |-----  bgp node
                |-----  ntp node
                |-----  snmp node
                |-----  syslog node
                |-----  dhcp-server node
                |-----  dhcp-relay node
                |-----  ipsec local policy node
                |-----  ipsec isakmp policy node
                |-----  ipsec tunnel policy node
                |-----  QoS (class-policy node)
                |-----  QoS (class-filter node)
                |-----  crp client node
                |-----  route-map node
                |-----  Web Authenticate node
                |-----  WarpLink node
                |-----  Extended track IP reachability node
                |-----  Extended track IPv6 reachability node
                |-----  Monitor-log node
```

<本装置ノード構造図>

第5章

view(exec) node

view(exec) node

■ 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 flash-config

＜説　　明＞　flash-config(flashに保存されている設定情報)を表示します。
＜書　　式＞　show flash-config xml
＜備　　考＞　flash-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)

○ show config ipsec

＜説　　明＞　IPsecの設定情報を表示します。Policy ID/Tunnel IDを指定することによって、
　　特定のPolicy/Tunnel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 <1-65535>|local policy <1-255>|tunnel <1-65535>)

○ show config l2tpv3

＜説　　明＞　L2TPv3の設定情報を表示します。Group ID/Tunnel ID/Xconnect IDを指定することによって、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 <1-4095>|tunnel <0-4095>|xconnect <1-4294967295>)

◆ 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 cashe
　　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)

view(exec) node

◆ 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 DST-IP
　　ip access-list IPv4-ACL-NAME (permit|deny) SRC-IP DST-IP PROTOCOL
　　ip access-list IPv4-ACL-NAME (permit|deny) SRC-IP DST-IP ICMP
　　ip access-list IPv4-ACL-NAME (permit|deny) SRC-IP DST-IP TCP/UDP
　　ip access-list IPv4-ACL-NAME (permit|deny) SRC-IP DST-IP TCP-OPTIONS
＜オプション＞

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>	: Protocol number
ICMP	: icmp | icmp <0-255>	: ICMP <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 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

view(exec) node

■ 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)

◆ 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]

view(exec) node

◆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

view(exec) node

◆ 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

◆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

◆ show syslog
<説　　明>　シスログを表示します。
<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されます。

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

view(exec) node

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

◆ show (disk0|disk1)
<説　　明>　外部ストレージ情報を表示します。
<書　　式>　show (disk0|disk1)

◆ 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

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

view(exec) node

◆ show l2tp
<説　　明>　L2TPトンネルステータスを表示します。
<書　　式>　show l2tp (tunnel|session)

◆ 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:1-4095>|)

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

view(exec) node

◆ 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)
＜備　　考＞　(mode|power-save)はethernet I/Fのみ指定することができます。

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

◆ 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>)

◆ show vrrp
＜説　　明＞　VRRPの情報を表示します。
＜書　　式＞　show vrrp

◆ show ppp
＜説　　明＞　PPPの情報を表示します。
＜書　　式＞　show ppp (<0-4>|)

◆ show pppoe-bridge
＜説　　明＞　PPPoE bridgeの状態を表示します。
＜書　　式＞　show pppoe-bridge

view(exec) node

◆ show ipsec

＜説　　明＞　IPsecの情報を表示します。

＜書　　式＞　show ipsec ca certificates　: Display IPsec CA certificates
show ipsec certificates　: Display IPsec certificates
show ipsec crls　: Display IPsec crls
show ipsec policy　: Display IPsec policy
show ipsec public-keys　: Display IPsec public-keys
show ipsec rsa-pub-key　: Display IPsec RSA public key
show ipsec sa　: Display IPsec Security Associations
show ipsec status (|tunnel <1-65535>) (|brief)
show ipsec status (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 (advertised-routes|received-routes|routes)]
show ip bgp route-map ROUTE-MAP
show ip bgp scan
show ip bgp summary

view(exec) node

■ 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>)

○APN情報の表示(カードによってはppp使用中は取得不可)
＜書　　式＞　show mobile <0-1> ap

○電話番号の表示(カードによってはppp使用中は取得不可)
＜書　　式＞　show mobile <0-1> phone-number

○電波強度の表示(カードによってはppp使用中は取得不可)
＜書　　式＞　show mobile <0-1> signal-level

◆ 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。

```
nxr155#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。

```
nxr155#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) node

◆ 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32章：WarpLink nodeを参照してください。

view(exec) node

◆ 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35章：Monitor-log node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。

◆ show wimax
<説　　明>　WiMAXの状態を表示します。
<書　　式>　show wimax (|<0-0>)

◆ clock set
<説　　明>　現在時刻を設定します。
<書　　式>　clock set HH:MM:SS Day Month Year
<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

◆ erase flash-config
<説　　明>　フラッシュ上の設定を消去します（初期設定に戻します）。
<書　　式>　erase flash-config
<備　　考>　flash-configを消去した後、本装置を再起動します。

◆ 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|disk1:FILENAME)　(disk0=USB0, disk1=USB1)
　　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>
・外部記憶装置(USB0, USB1)に保存されているファイルを全て表示します。
<書　　式>　dir (|disk0|disk1)
<備　　考>　USB0に接続されたUSB Flashメモリを指定する場合は、disk0を選択します。
　　USB1に接続されたUSB Flashメモリを指定する場合は、disk1を選択します。

view(exec) node

■ 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|disk1: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|disk1:FILENAME) (|all)
```

＜備　　考＞

・allを指定の場合は、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) node

○ configの復帰

＜説　　明＞　設定ファイルの復帰(local flashまたはUSB/CFへの保存)をおこないます。

＜書　　式＞

```
copy ssh://user@(A.B.C.D|X:X::X:X)/FILENMAE
            (flash-config|disk0:FILENAME|disk1:FILENAME) (|source A.B.C.D|X:X::X:X)
copy ftp://(A.B.C.D|X:X::X:X)/FILENAME
            (flash-config|disk0:FILENAME|disk1:FILENAME) (|source A.B.C.D|X:X::X:X)
copy (disk0:FILENAME|disk1:FILENAME)
                  (flash-config|disk0:FILENAME|disk1:FILENAME)
```

＜備　　考＞

- disk0 --> disk0、disk1 --> disk1へのcopyは不可。disk0 <--> disk1へのcopyは可。
- 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|disk1: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

view(exec) node

◆ **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 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|disk1: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E:Firmware update」を参照してください。

◆ **restart**

＜説　　明＞　サービスを再起動します。

＜書　　式＞

```
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 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 waplink send-config (WarpLink Managerに本装置のconfigを送信します)
```

◆ **configure**

＜説　　明＞　コンフィグレーションモードへ移行します。

＜書　　式＞　configure terminal

view(exec) node

■ dump

＜説　　明＞　NXR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。
なお、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。
[ethernet <0-2> (|vid<vlan_id:1-4094>) | ppp <0-4> | tunnel <1-255>]

○ 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}|)

◆ 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>

view(exec) node

◆ 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>

■ 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) node

◆ 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 wimax
<説　　明>　WiMAX接続を切断します。
<書　　式>　clear wimax <0-0>

◆ 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) node

◆ 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) node

■ 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>

○ connect wimax

<説　　明>　WiMAXの接続を開始します。
<書　　式>　connect wimax <0-0>

◆ 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) node

◆ format
<説　　明>　外部ストレージをフォーマットします。
<書　　式>　format (disk0|disk1)

◆ eject
<説　　明>　外部ストレージをアンマウントします。
<書　　式>　eject (disk0|disk1)

◆ inject
<説　　明>　外部ストレージをマウントします。
<書　　式>　eject (disk0|disk1)

◆ 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。

nxr120#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。

nxr120#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) node

◆ 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)　[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>
・CPU使用率を指定した間隔と回数で取得する機能です。
・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。
・終了時には、取得したCPU使用率の平均値を出力して終了します。
<書　　式>　get system statistics cpu <interval(sec):1-86400> <count(回):1-65535>
<　例　>　実行例を下記に示します。

```
nxr120#get system statistics cpu 1 5
 14:20:02       %CPU      %user      %nice    %system      %idle    %iowait
 14:20:03      22.00      17.00       0.00       5.00      78.00       0.00
 14:20:04      23.00      11.00       0.00      11.00      77.00       0.00
 14:20:05     100.00      65.00       0.00      35.00       0.00       0.00
 14:20:06       4.95       3.96       0.00       0.00      95.05       0.00
 14:20:07       0.00       0.00       0.00       0.00     100.00       0.00
 AVERAGE       29.99      19.39       0.00      10.20      70.01       0.00
```

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

view(exec) node

■ 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
```

第6章

global node

global node

◆ 移行command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(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 flash-config

＜説　　明＞　flash-config(flashに保存されている設定情報)を表示します。

＜書　　式＞　show flash-config xml

＜備　　考＞　flash-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。

```
nxr130(config)#hostname NXR01
NXR01(config)#
```

global node

◆ 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（NXR 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 および L2TPv3 fast-forwarding のセッション最大数は、次のとおりです。

—	NXR-120	NXR-125	NXR-130	NXR-155	NXR-1200
fast-forwarding	16,383				65,533
L2TPv3 fast-forwarding	16,192				62,462

  - 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、16,383（NXR-1200 の場合は、65,533）を超えることはありません。
  - L2TPv3 fast-forwarding については、global node の l2tpv3 fast-forwarding コマンドを参照してください。

global node

■ 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)
```

○ 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)
```

○ 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)
```

○ 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)
```

○ negate

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

＜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 node を参照)で、ACL をインタフェースに適用してください。

global node

■ 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)
```

○ 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)
```

○ 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)
```

○ 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)
```

○ negate

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

＜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 nodeを参照)で、ACLをインタフェースに適用してください。

global node

◆ 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。

global node

■ 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)
```

＜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
```

○ dsnat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 node

■ 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 node

■ 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 node

◆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|disk1: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 node

◆ 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 node

■ 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> (NXR-120/C、NXR-125/CX、NXR-130/C)
　　session udp timer <sec:1-2147483> (NXR-1200)
＜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> (NXR-120/C、NXR-125/CX、NXR-130/C)
　　session udp-stream timer <sec:1-2147483> (NXR-1200)
＜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> (NXR-120/C、NXR-125/CX、NXR-130/C)
　　session tcp timer <sec:1-2147483> (NXR-1200)
＜初 期 値＞　session tcp timer 3600
＜　no　＞　no session tcp timer (=session tcp timer 3600)

○ session max

＜説　　明＞　最大セッション数を設定します。
＜書　　式＞　session max <4096-32768>　(NXR-120/C、NXR-125/CX、NXR-130/C)
　　session max <4096-65536>　(NXR-1200)
＜初 期 値＞　session max 4096　(NXR-120/C、NXR-125/CX、NXR-130/C)
　　session max 32768　(NXR-1200)
＜　no　＞　no session max (=初期値に戻す)

○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。
＜書　　式＞　session limit <0-32768>　(NXR-120/C、NXR-125/CX、NXR-130/C)
　　session limit <0-65536>　(NXR-1200)
＜初 期 値＞　session limit 0
＜　no　＞　no session limit
＜備　　考＞　0を設定すると、IP address毎のsession数を制限しません。

■ session (続き)

○session tcplimit

＜説　　明＞　NXR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 (<16-16384>|)　(NXR-120/C、NXR-125/CX、NXR-130/C)
　　session tcp limit (<16-32768>|)　(NXR-1200)

＜初 期 値＞　session tcp limit 640　(NXR-120/C、NXR-125/CX、NXR-130/C)
　　session tcp limit 1024　(NXR-1200)

＜　no　＞　no session tcp limit （=無制限）

＜備　　考＞

・NXR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＞　NXR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。
　　しかし、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。

```
nxr125(config)#no session invalid-status-drop enable
nxr125(config)#interface ppp 0
nxr125(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。
　　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。

＜書　　式＞　session checksum enable

＜初 期 値＞　no session checksum enable

＜　no　＞　no session checksum enable

global node

■ 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 node

■ 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 node

■ l2tp

＜説　　明＞　OCN IPv6サービスに接続する際に使用します。NXR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NXR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 node

■ L2TPv3

＜説　　明＞

・NXR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 node

○ 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)

＜初 期 値＞　l2tpv3 mac-learning

＜　no　＞　no l2tpv3 mac-learning

＜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。

global node

■ 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
<初 期 値>　no l2tpv3 loop-detect
<　no　>　no l2tpv3 loop-detect
<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
<初 期 値>　no l2tpv3 send-known-unicast
<　no　>　no l2tpv3 send-known-unicast
<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

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

＜　no　＞　no l2tpv3 udp path-mtu-discovery

＜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

＜初 期 値＞　no l2tpv3 path-mtu-discovery

＜　no　＞　no l2tpv3 path-mtu-discovery

○ 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

＜初 期 値＞　no l2tpv3 tos

＜　no　＞　no l2tpv3 tos

＜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。

■ 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 node

■ L2TPv3

○ fast-forwarding（続き）

＜備　　考＞

・fast-forwarding および L2TPv3 fast-forwarding のセッション最大数は、次のとおりです。

—	NXR-120	NXR-125	NXR-130	NXR-155	NXR-1200
fast-forwarding	16,383				65,533
L2TPv3 fast-forwarding	16,192				62,462

- L2TPv3 fast-forwarding のセッション最大数に達している場合は、L2TPv3 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、16,383（NXR-1200 の場合は、65,533）を超えることはありません。
- fast-forwarding については、global node の fast-forwarding コマンドを参照してください。

＜注　　意＞

※本機能（L2TPv3 の fast-forwarding）は、v5.11.1 以降のファームウェアでサポートしています。但し、v5.12.0 では未サポートです。

※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）。

```
nxr120(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）。

```
nxr120(config)# l2tpv3 mac-learning
```

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

```
nxr120(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

```
nxr120(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

```
nxr120(config)#no l2tpv3 mac-learning
% First deconfigure "l2tpv3 fast-forwarding enable" on global mode.
```

global node

■ L2TPv3

○ fast-forwarding（続き）

＜　例　＞

● PtoP 上り / 下り

NXR_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 ----- NXR_1 =====L2TPv3===== NXR_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。
NXR_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。
NXR_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

NXR_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 ----- NXR_1 =====L2TPv3===== NXR_2 ----- PC_A
                 =====L2TPv3===== NXR_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。
NXR_1 は、NXR_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。
NXR_1 は、NXR_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、NXR_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、NXR_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 node

■ 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|INTERFACE|null) (|<distance:1-255>)
＜パラメータ＞　A.B.C.D/M　：ネットワークアドレス/プレフィクス (e.g. 10.0.0.0/8)
　　GATEWAY　：E.F.G.H　ゲートウェイのIPv4アドレス
　　INTERFACE　：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>)
＜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。

◆ 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。

global node

◆ 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 node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 nxr120 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 node

◆ 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、NXR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NXR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 node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 node

■ 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がセットされます。
・Router Solicitationは送信されません。
・RAは受信しません（無視します）。
・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はセットされません。
・必要な場合、Router Solicitationが送信されます。
・RA受信が有効な場合、RAによるauto-configurationが可能になります。
・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>)
＜パラメータ＞　X:X::/M　　: IPv6 destination prefix (e.g. 3ffe:506::/32)
GATEWAY　　: X:X::X:X　IPv6 gateway address
INTERFACE　: ethernet <0-2> (|vid <1-4094>) | ppp <0-4> | tunnel <0-255>
＜　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>)

◆ 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、NXR宛のIPv6パケットはNXRにて処理されます。
non-unicastやNXR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、NXRで処理され、かつブリッジもされます)。

global node

■ 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 F 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。

○ 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。

○ 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>
```

＜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。

global node

◆ ipsec nat-traversal
<説　　明>　NATトラバーサルを有効にします。
<書　　式>　ipsec nat-traversal enable
<　no　>　no ipsec nat-traversal enable
<初 期 値>　no ipsec nat-traversal enable
<備　　考>　IPv4のみ対応しています。
　　IKEv2では自動的に有効になります（無効にすることはできません）。

◆ 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 node

◆ 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

global node

◆ 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]

◆ 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 node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

global node

◆ 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

◆ 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 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 node

◆ 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.NXR120-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、NXR 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 node)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 node)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 node)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 node

◆ interface ethernet
<説　　明>　interface nodeへの遷移およびprofileを削除・生成します。
<書　　式>　interface ethernet <0-2>
<備　　考>　ethernet interfaceは削除不可

◆ interface loopback
<説　　明>　interface nodeへの遷移およびprofileを削除・生成します。
<書　　式>　interface loopback <0-9>
<　no　>　no interface loopback <0-9>

◆ interface ethernet <0-2> vid <1-4094>
<説　　明>　interface nodeへの遷移およびprofileを削除・生成します。
<書　　式>　interface ethernet <0-2> vid <1-4094>
<　no　>　no interface ethernet <0-2> vid <1-4094>

◆ interface tunnel
<説　　明>　interface tunnel nodeへの遷移およびprofileを削除・生成します。
<書　　式>　interface tunnel <0-255>
<　no　>　no interface tunnel <0-255>

◆ interface ppp
<説　　明>　interface ppp nodeへの遷移およびprofileを削除・生成します。
<書　　式>　interface ppp <0-4>
<　no　>　no interface ppp <0-255>

◆ l2tp
<説　　明>　l2tp nodeへの遷移およびprofileを削除・生成します。
<書　　式>　l2tp <0>
<　no　>　no l2tp <0>

◆ l2tpv3 tunnel
<説　　明>　l2tpv3-tunnel nodeへの遷移およびプロファイルを生成します。
　　noで、指定したIDのプロファイルを削除します。
<書　　式>　l2tpv3 tunnel <tunnnel_id:0-4095>
<　no　>　no l2tpv3 tunnel <tunnnel_id:0-4095>

◆ l2tpv3 xconnect
<説　　明>　l2tpv3-xconnect nodeへの遷移およびプロファイルを生成します。
　　noで、指定したIDのプロファイルを削除します。
<書　　式>　l2tpv3 xconnect <xid:1-4294967295>
<　no　>　no l2tpv3 xconnect <xid:1-4294967295>

global node

◆ l2tpv3 group
<説　　明>　l2tpv3-group nodeへの遷移およびプロファイルを生成します。
　　noで、指定したIDのプロファイルを削除します。
<書　　式>　l2tpv3 group <gid:1-4095>
<　no　>　no l2tpv3 group <gid:1-4095>

◆ ntp
<説　　明>　ntp nodeへの遷移およびprofileを生成します。
<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 node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。)

◆snmp
<説　　明>　snmp node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 node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 nodeへの遷移およびprofileを生成します。
<書　　式>　dhcp-server <1-5>
<　no　>　no dhcp-server(|<1-5>) (=DHCPサービスの停止およびprofileを削除します。)

◆monitor-log
<説　　明>　monitor-log node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 node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>

global node

◆router rip
<説　　明>　RIP node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 node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。)

■ 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 node

■ 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 node

■ 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 node

■ 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 node

■ 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 >

■ 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
```

■ mobile

○ mobile

＜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

global node

■ system led

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

○ system led ext

＜説　　明＞

・ユーザが指定した周期で、データ通信モジュール、またはWiMAXモジュールの電波状態をチェックし、結果をAUX LED 1，2の点灯 / 消灯で表示します。

＜書　　式＞　system led ext 0 signal-level mobile <0-0> (|interval <0-60>)
　　system led ext 0 signal-level wimax <0-0> (|interval <0-60>)

＜　no　＞　no system led ext 0

＜初 期 値＞　system led ext 0 signal-level mobile 0 interval 5

＜備　　考＞　Intervalが0の場合は、定期チェックは行われません。
　　なお、電波状態が取得できなかった場合等については、LEDの消灯を行います。
　　PPP接続中に本機能が有効になった場合は、PPP接続前の状態がLEDに反映されます。

○ system led aux

＜説　　明＞

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

＜書　　式＞　system led aux <1-2> interface tunnel <0-255>
　　system led aux <1-2> interface ppp <0-4>
　　system led aux <1-2> interface wimax <0-0>
　　system led aux <1-2> track (<1-255>|<2048-4095>)

＜　no　＞　no system led aux <1-2>

＜備　　考＞　EXT0とAUX1/2の設定は、排他制御です。つまり、EXT0が有効であれば、AUX1/2の設定はできません。また、AUX1/2の設定が行われると、EXT0の設定は無効となります。

○ system led status

＜説　　明＞

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

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

＜　no　＞　no system led status <1-1>

＜備　　考＞　STS1 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 node

■ 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)
```

○データ通信端末の schedule 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
```

○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 node 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
```

global node

○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

○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

○ SNMP notify の送信
＜説　　明＞　指定時間に、SNMP notify(trap)を送信します。
＜書　　式＞　日付指定
schedule <1-255> HOUR:MIN DAY MON snmp extension-mib WORD notify (|<0-3600>)
＜書　　式＞　曜日指定(DOW: Day Of the Week)
schedule <1-255> HOUR:MIN DOW (|DOW) snmp extension-mib WORD notify (|<0-3600>)
＜備　　考＞
・サーバ側の負担軽減のために、0～3600 秒の間で margin を設定することができます。margin が設定されている場合、margin * (0-100)% のランダムな時間後に notify を送信します。

global node

○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

● 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)

● 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|disk1:FILENAME) (|hold)

＜備　　考＞

・FTP および 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
・NXR-125 では、バックグラウンドでファームウェアの更新を行います。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)。

global node

○WiMAXのスケジュール接続 / 切断 / 再接続

＜説　　明＞

・指定の時刻に、WiMAXの接続 / 切断 / 再接続を行います。切断、再接続は、WiMAXの状態に関係なく実行します。

・スケジュールによる切断は、手動による切断と同じように扱うため、常時接続の設定をしていても再接続を行いません。スケジュールによる切断後に再接続を行うには、ユーザによる接続の指示、またはスケジュールによる接続の設定を行ってください。

＜書　　式＞　日付指定

```
schedule <1-255> HOUR:MIN DAY MON interface wimax <0-0> (connect|disconnect|reconnect)
```

＜書　　式＞　曜日指定(DOW: Day Of the Week)

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

○WiMAXのスケジュールリセット

＜説　　明＞

・指定の時刻にWiMAXモジュールをリセットします。リセットを実行する際、WiMAXが接続中であれば、WiMAXを切断してからリセットを実行します。リセット後にWiMAXを再認識すると、自動接続が許可される状況（neteventなどの状況に依存します）であれば、WiMAXの接続を行います。

＜書　　式＞　日付指定

```
schedule <1-255> HOUR:MIN DAY MON wimax <0-0> clear
```

＜書　　式＞　曜日指定(DOW: Day Of the Week)

```
schedule <1-255> HOUR MIN DOW (|DOW) wimax <0-0> clear
```

○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 node

■ WiMAX

○ error-recovery

＜説　　明＞

・WiMAXモジュールの異常を自動検出して、管理者が操作しなくても自動的に通信を復帰させることを試みる機能です。

・復旧が必要と判断される状態を検出した場合は、WiMAXモジュールのリセットやシステムの再起動を実行することにより異常状態からの復旧を試みます。

＜書　　式＞　wimax error-recovery (restart|reset)

＜　no　＞　no wimax error-recovery

＜初 期 値＞　no wimax error-recovery

＜備　　考＞

・エラーの検出には、ステータスチェックとコネクトチェックがあります。

● ステータスチェック

60秒周期でステータスチェックを行い、3回連続で下記のエラーを検出した場合にerror-recovery処理を実行します。本機能を無効にした場合や、WiMAXモジュールのリセット中は、監視機能を停止します。

・WiMAXモジュールのステータス状態を取得できない場合

・IPアドレスは設定されているが、ss statusが、DeviceNotFoundYetの場合

● コネクトチェック

接続の試行から開始します。60秒周期で動作します。下記に示す動作を3回連続で検出するとerror-recovery処理を実行します。また、600秒経過後に接続が完了しない場合にも、error-recovery処理を実行します。その後、接続完了やエラー回復処理を実行すると停止します。

・WiMAXモジュールのステータス状態を取得できない場合

・ss statusがConnectedではなく、antenna levelが1より小さい場合

○ netevent

＜説　　明＞

・当該トラックイベントがdownした時に、WiMAXまたはモバイルモジュールをリセットします。

＜書　　式＞　wimax <0-0> netevent (<1-255>|<2048-4095>) reset

　　mobile <0-2> netevent (<1-255>|<2048-4095>) reset

＜　no　＞　no wimax <0-0> netevent

＜備　　考＞　イベントup時は何も実行しません。

◆ 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。

global node

■ 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 node を参照してください。

○ mail server
＜説　　明＞　mail server node 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 node）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/wimax node）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。

第7章

interface node

interface node

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#interface ethernet <0-2> [vid <1-4094>]
nxr130(config-if)#

nxr130(config)#interface loopback <0-9>
nxr130(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          : ipv6 forwarding が有効のときは設定不可
<　no　>　no ipv6 address X:X::X:X link-local
            no ipv6 address X:X::X:X/M (|eui-64)
            no ipv6 address autoconfig
```

◆ ipv6 address

```
<説　　明>　DHCPv6 Prefix Delegation を設定します。
<書　　式>　ipv6 address DHCPv6-PD X:X::X:X/M (|eui-64)
<備　　考>　ipv6-address は、sub-prefix と host 部を指定可能
            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 で設定される
<　no　>　no ipv6 address DHCPv6-PD (|X:X::X:X/M)
                                        :DHCPv6 packet は、別 interface から受信
```

interface node

◆ 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。またSW HUB portをもつ機種の場合は、switched port毎に通信モードを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)。

・port <1-4>はHUBポートのみ指定することが出来ます。

・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	○

◆ 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。

interface node

◆ 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

◆ 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 node

◆ 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。

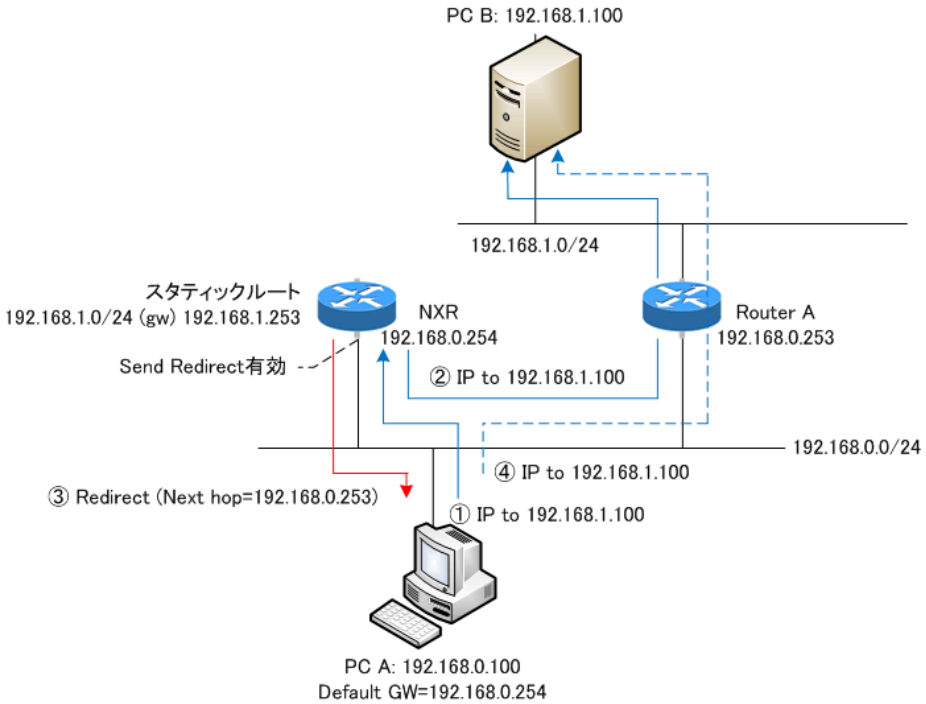
① Host A は、Host B(192.168.1.100)への IPv4 パケットを default gw(NXR)に送信します。

② NXR 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 node

◆ 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 node

◆ 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。

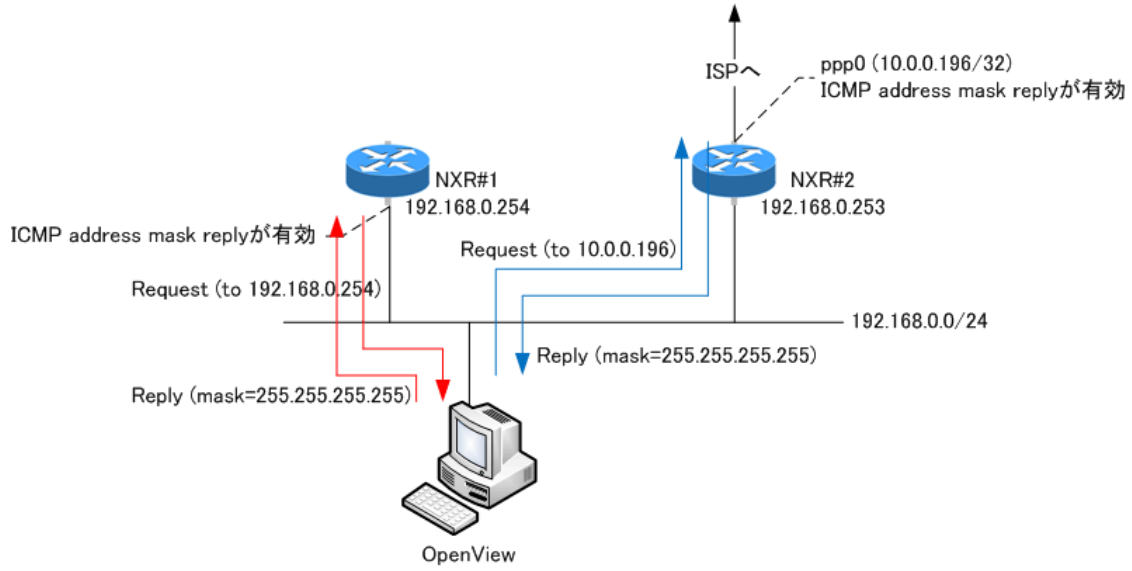
＜書　　式＞　ip mask-reply　（ICMP address mask request に応答します。）

＜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 node

◆ 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 node

◆ 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。

<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 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>)

<備　　考>　Ethernet/VLAN のみ設定可能

<　no　>　no ipv6 nd prefix X:X:X:X::X/M
(|<valid-lifetime:0-4294967295> <preferred-lifetime:0-4294967295>)

interface node

◆ ipv6 tcp adjust-mss
<説　　明>　IPv6 MSSを自動設定します。
<書　　式>　ipv6 tcp adjust-mss (auto|500-1460)
<初 期 値>　no ipv6 tcp adjust-mss
<　no　>　no ipv6 tcp adjust-mss

◆ ipv6 nd send-ra
<説　　明>　IPv6 RA(Router Advertisement) を送信します。
<書　　式>　ipv6 nd send-ra　　(= RA送信開始)
<　no　>　no ipv6 nd send-ra　　(= RA送信停止)

◆ 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 90
<　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:3-6750> <max:4-9000>
<初 期 値>　ipv6 nd ra-interval 10 30
<備　　考>　min < max x 0.75
<　no　>　no ipv6 nd ra-interval

◆ 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　　: Set defaults

◆ 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　　: Set defaults

◆ 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　　: Set defaults

interface node

◆ 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。

◆ 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

interface node

◆ 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

◆ 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

interface node

◆ 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>

◆ 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

◆ 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 node

◆ 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 node

◆ ip access-group

<説　　明>
・global node 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)　NXR 自身で受信して処理するパケットを制限します。
- out(local output) NXR 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 NXR 自身が作成したパケットとして認識します。
- forward-in　NXR 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 NXR 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/WiMAX)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 node 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 node)で行います。

interface node

◆ 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 node）を参照してください。

・Web 認証については、Web Authenticate node 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 node

◆ 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

◆ 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

◆ shutdown port (NXR-125およびNXR-155のみ)
<説　　明>　スイッチポート(ethernet 0)をポート単位でシャットダウンすることができます。
　　デフォルトでは、すべてのスイッチポートが有効（no shutdown）です。
<書　　式>　shutdown port <1-4>
<　　no　　>　no shutdown port <1-4>

◆ 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2つまで設定することが出来ます。IPv4とIPv6に、それぞれ1つずつのIPsecローカルポリシー の割り当てを想定しています。

◆ 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 node

■ 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 node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。

interface node

■ 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/WiMAX 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 node

◆(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NXR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NXR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、NXR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NXR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 node

◆session invalid-status-drop-interface

＜説　　明＞

・session invalid-status-drop機能(global node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 node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 nodeで、session invalid-status-dropを無効にします。

```
nxr125(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。

```
nxr125(config)#interface ethernet 0
nxr125(config-if)#session invalid-status-drop-interface enable
```

第 8 章

interface tunnel node

interface tunnel node

◆ 移行command
```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#interface tunnel <0-255>
nxr130(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
```
<説　　明>　DHCPv6 PDの設定をします。
・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prefixeに名前をつけたもので、ipv6 dhcp client pdで設定します。
<書　　式>　ipv6 address DHCPv6-PD X:X::X:X/M (|eui-64)
<　no　 >　no ipv6 address DHCPv6-PD X:X::X:X/M
```

◆ 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
```

◆ tunnel mode
```
<説　　明>　トンネルモードを選択します（IP over IP/GRE/IPsec IPv4)。
<書　　式>　tunnel mode (ipip|gre|ipsec ipv4)
<初 期 値>　tunnel mode gre
<　no　 >　no tunnel mode (= tunnel mode gre)
<備　　考>　Route based IPsec(参照：付録C)を使用する際は、ipsec ipv4を指定します。
```

interface tunnel node

◆ 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

◆ 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 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 C 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。

interface tunnel node

◆ 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Cを参照してください。

◆ tunnel tos
<説　　明>
指定したToS 値をtunnel IP Header に設定します。inherit に設定した場合、tunneling IPv4 headerのToS 値をtunnel IP header にコピーします。ToS 値指定の場合、ECN field を設定することはできません。また、IPv6 packet をtunneling する場合は、inherit 設定は無視されて、ToS は0x0 が設定されます。ECN field の扱いについては、「付録C 1.2.4.1 ECN field の扱い」を参照してください。
<書　　式>　tunnel tos (<0-252>|inherit)
<初 期 値>　tunnel tos inherit
<　no　>　no tunnel tos　　(= tunnel tos inherit)

◆ 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C)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C)を使用する際に設定します。

◆ 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 node

◆ 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 node 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＞　IPv6 MSS を有効にします。
＜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 node

◆ 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 node 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、NXR 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C)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 node 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 node

◆ 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 node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)　NXR自身で受信して処理するパケットを制限します。
- out(local output) NXR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NXR自身が作成したパケットとして認識します。
- forward-in　NXR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 NXR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/WiMAX)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 node

◆ ip (snat-group|dnat-group)

＜説　　明＞
- global node 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 node)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 node）を参照してください。
- Web 認証については、Web Authenticate node 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 node

◆ **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

◆ **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 2 つまで設定することが出来ます。IPv4 と IPv6 に、それぞれ 1 つずつの IPsec ローカルポリシー の割り当てを想定しています。

◆ **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 node

■ 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 node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 node

■ 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 node

◆(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NXR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NXR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、NXR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NXR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 node

◆session invalid-status-drop-interface

＜説　　明＞

・session invalid-status-drop機能(global node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 node 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 node で、session invalid-status-drop を無効にします。

```
nxr125(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。

```
nxr125(config)#interface tunnel 0
nxr125(config-tunnel)#session invalid-status-drop-interface enable
```

第9章

interface ppp node

interface ppp node

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#interface ppp <0-4>
nxr130(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 (|secondary)
<　no　 >　no ip address (|A.B.C.D/M) (|secondary)
```

◆ 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で設定されます。

```
<　no　 >　no ipv6 address DHCPv6PD X:X::X:X/M
```

◆ 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)
```

interface ppp node

◆ 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 pd
<説　　明>　DHCPv6 PDを有効にします。
<書　　式>　ipv6 dhcp client pd DHCPv6-PREFIXNAME
<初 期 値>　no ipv6 dhcp client pd
<備　　考>　DHCPv6 PDを受信するinterfaceに対して設定します。
<　no　>　no ipv6 dhcp client pd

◆ 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 nodeのip redirectsを参照して下さい。

interface ppp node

◆ 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＞　IPv6 MSS を自動設定します。

＜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 node

◆ 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 node 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 NXR 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、NXR 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 node

◆ 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、NXR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

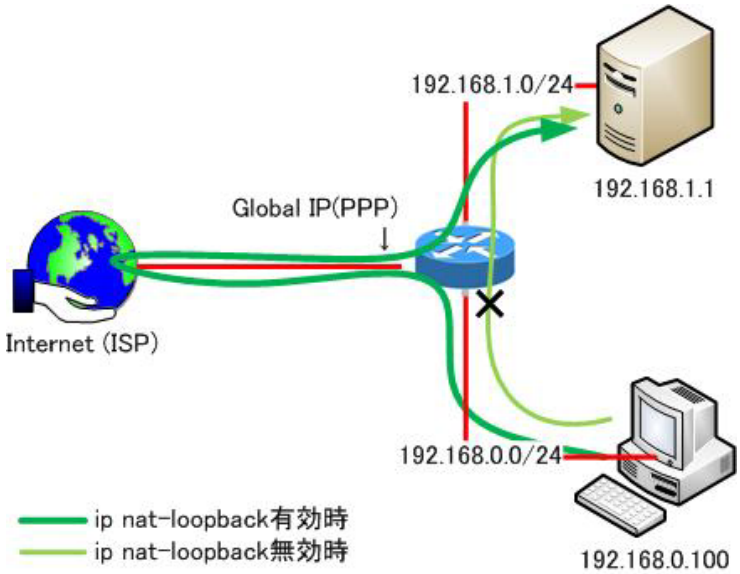
＜　no　＞　no ip nat-loopback

＜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。



・NXR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 node

○ip nat-loopback設定時のルーティングテーブルの設定と参照条件

ip nat-loopback設定時、PPPのインタフェース番号に従ってpolicy based routingを設定します。
各ルーティングテーブルを参照する条件は、以下のとおりです。

※ PPPインタフェースをppp(n)と表記します（nは0～4のいずれか)。また、m=nx4とします。

※ 下記(2)および(4)の場合、ppp(n)のIPアドレスを送信先とするパケットはppp(n)に出力するような経路が、該当のルーティングテーブルに設定されています。

(1) rule number m
　送信先IPアドレスが、ppp(n)のIPアドレスで、かつppp(n)以外から受信した場合に参照します。

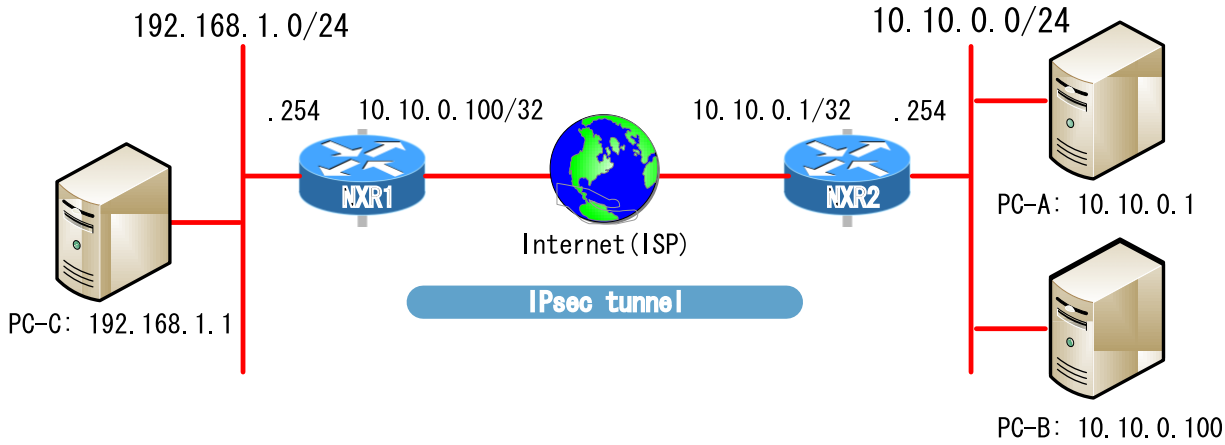
(2) rule number m+1
　送信元/送信先IPアドレスが、共にppp(n)のIPアドレスの場合に参照します。

(3) rule number m+2
　NXRを送信元とするパケットで、送信先がppp(n)のIPアドレスに等しい場合に参照します。

(4) rule number m+3
　ppp(n)以外から受信した場合に参照します。

○ 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 node

◆ keepalive lcp-echo
<説　　明>　LCP echo request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

◆ 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 node

◆ ip access-group

＜説　　明＞

・global node 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)　NXR 自身で受信して処理するパケットを制限します。
- out(local output) NXR 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 NXR 自身が作成したパケットとして認識します。
- forward-in　NXR 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 NXR 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/WiMAX)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 node 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 node)で行います。

interface ppp node

◆ 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 node）を参照してください。
- Web 認証については、Web Authenticate node 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

◆ 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)

interface ppp node

◆ ppp username
<説　　明>　PPP接続のUser IDをパスワードを設定します。
<書　　式>　ppp username USERID password (|hidden) PASSWORD
<　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 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

◆ 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>　DNSオプションを設定します。
<書　　式>　ppp ipcp dns accept　　: Accept any non zero DNS address
　　ppp ipcp dns reject　　: Reject negotiations with the peer
　　ppp ipcp dns <primary:A.B.C.D> (|<secondary:A.B.C.D>)　　: 手動割り当て
<初 期 値>　ppp ipcp dns accept
<　no　>　no ppp ipcp dns

◆ 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 commandで設定されたIPをIPCPでrequestする

◆ 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　　: Disable IPv6CP

interface ppp node

◆ 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 を使用する。この設定により LLA が決定される。
<　no　>　no ppp ipv6cp id

◆ ppp on-demand
<説　　明>　On-demand PPP を設定します。
<書　　式>　ppp on-demand
<備　　考>　現状 mobile 時のみ対応(l2tp,ipv6cp 有効時は無視される)
<　no　>　no ppp on-demand

◆ ppp idle-timeout
<説　　明>　On-demand PPP の idle timer を設定します。
<書　　式>　ppp idle-timeout (<sec:30-86400>|)
<備　　考>　ondemand 有効時のみ(l2tp,ipv6cp 時は無視される)
　　時間指定ないときは 180sec
<　no　>　no ppp idle-timeout
<備　　考>　ondemand 有効のときは default 180sec に戻る

◆ 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)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 ppp node

◆ 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2つまで設定することが出来ます。IPv4とIPv6に、それぞれ1つずつのIPsecローカルポリシー の割り当てを想定しています。

◆ 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、NXR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、NXR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 node

■ 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 node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 node

■ 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 node

■ 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
○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

◆ 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 node

◆(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NXR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NXR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、NXR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NXR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 node

◆session invalid-status-drop-interface

＜説　　明＞

・session invalid-status-drop機能(global node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 node 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 node で、session invalid-status-drop を無効にします。

```
nxr125(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。

```
nxr125(config)#interface ppp 0
nxr125(config-ppp)#session invalid-status-drop-interface enable
```

interface ppp node

■ 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 node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 node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 node)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 node)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

第 10 章

dns node

dns node

◆ 移行 command

dns node に移行します。

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#dns
nxr130(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 dhcp <priority:0-255>
　　priority ppp <interface:0-4> <priority:0-255>
　　priority user <priority:0-255>
＜初 期 値＞　すべて 20
＜備　　考＞　同一 priority の場合の優先度: user > ppp4 > ppp3 > ppp2 > ppp1 > ppp0 > dhcp
　　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
＜　no　＞　no priority (dhcp | ppp <interface:0-4> | user)
　　(=no priority (dhcp 20 | ppp <interface:0-4> 20 | user 20))

◆ 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)

第 10 章 dns node

dns node

◆ 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

第 11 章

l2tp node

l2tp node

◆ 移行 commannd
l2tp node に移行します。
```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#l2tp 0
nxr130(config-l2tp)#
```

◆ tunnel
＜説　　明＞　L2TP の tunnel address を指定します。
＜書　　式＞　tunnel address (A.B.C.D | FQDN)

◆ 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　　: Set defaults

◆ tunnel retransmit
＜説　　明＞　切断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)

◆ tunnel hello
＜説　　明＞　Helloインターバルを設定します。
＜書　　式＞　tunnel hello <seconds:0-1000>
＜初 期 値＞　tunnel hello 60
＜　no　＞　no tunnel hello　　: Disable

◆ 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 をトネリングします。
＜書　　式＞　tunnel ppp <interface:0-4>
＜備　　考＞　l2tp の再接続、再接続間隔は、ppp の設定を使用する

第 12 章

l2tpv3-tunnel node

第 12 章 l2tpv3-tunnel node

l2tpv3 tunnel parameters

◆ **移行 commannd**

l2tpv3-tunnel node に移行します。

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#l2tpv3 tunnel <0-4095>
nxr130(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

◆ **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
＜備　　考＞　dynamic address 使用時

◆ **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
＜備　　考＞　必須

◆ **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
＜備　　考＞　必須

◆ **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

l2tpv3 tunnel parameters

◆ 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　　: Disable

◆ 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 13 章

l2tpv3-xconnect node

l2tpv3 xconnect parameters

◆ 移行 command
nxr130#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr130(config)#**l2tpv3 xconnect <xid:1-4294967295>**
nxr130(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 ethernet
＜説　　明＞　Xconnectインタフェースを設定します。
＜書　　式＞　xconnect ethernet <0-2> (|vid <1-4094>)

◆ 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

◆ 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 nodeのip mask-replyを参照してください。

◆ 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

第 14 章

l2tpv3-group node

l2tpv3-group node

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#l2tpv3 group <gid:1-4095>
nxr130(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>)

◆ 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 node

◆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。

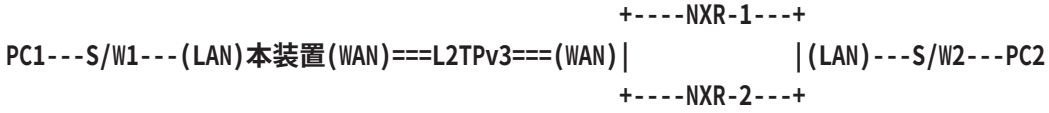
＜書　　式＞　mac-advertise enable

＜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NXR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 15 章

rip node

rip node

◆ 移行command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#router rip
nxr130(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>)
<    no    >　no redistribute (static|connected|ospf|bgp) (|metric <metric:0-16>)
```

◆ 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
```

◆ 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)
```

rip node

◆ 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 16 章

ospf node

ospf node

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#router ospf
nxr130(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 node

◆ 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)
redistribute (connected|static|rip|bgp) (|metric<0-16777214>) [|metric-type (1|2)]
```

＜　no　＞

```
no redistribute (connected|static|rip|bgp)
no redistribute (connected|static|rip|bgp) (|metric) (|metric-type)
```

◆ 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 node

◆ 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
　default-information originate (|metric <0-16777214>) [|metric-type (1|2)] (|always)
<　no　>
　no default-information originate
　no default-information originate (|metric<0-16777214>)[metric-type(1|2)] (|always)

◆ 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 17 章

bgp node

bgp node

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#router bgp <1-65535>
nxr130(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 node

■ 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 node

■ 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 node

■ 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 default-originate
＜　no　＞　no neighbor A.B.C.D 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 distribute-list ACL-NAME (in|out)
＜　no　＞　no neighbor A.B.C.D 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 ebgp-multihop <1-255>
＜　no　＞　no neighbor A.B.C.D 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 filter-list ACL-NAME (in|out)
＜　no　＞　no neighbor A.B.C.D filter-list ACL-NAME (in|out)
＜備　　考＞　global ノードで設定した 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 next-hop-self
＜　no　＞　no neighbor A.B.C.D 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 remote-as <1-65535>
＜　no　＞　no neighbor A.B.C.D 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 remove-private-as
＜　no　＞　no neighbor A.B.C.D remove-private-as

bgp node

■ 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 route-map WORD (in|out)
<　no　>　no neighbor A.B.C.D 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 soft-reconfiguration inbound
<　no　>　no neighbor A.B.C.D 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 timers <keepalive:0-65535><holdtime:0|3-65535>
<　no　>　no neighbor A.B.C.D timers
<初 期 値>　neighbor A.B.C.D 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 timers connect <0-65535>
<　no　>　no neighbor A.B.C.D timers connect
<初 期 値>　neighbor A.B.C.D 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 update-source
　　(ethernet<0-2>|loopback<0-9>|ppp<0-4>|tunnel<0-255>)
<　no　>　no neighbor A.B.C.D update-source

bgp node

○ 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 advertisement-interval <1-600>

＜　no　＞　no neighbor A.B.C.D 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 as-origination-interval <1-600>

＜　no　＞　no neighbor A.B.C.D as-origination-interval

＜備　　考＞　タイマのデフォルト値は、15(秒)です。

◎ 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 node

■ 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。

第 18 章

ntp node

ntp node

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#ntp
nxr130(ntp-config)#
```

◆ service

＜説　　明＞　NTPサービスを有効にします。
＜書　　式＞　service enable

◆server

＜説　　明＞　NTPサーバの設定をします。
＜書　　式＞　server (A.B.C.D|FQDN|X:X::X:X) polling min max
＜初 期 値＞　no server
＜備　　考＞　2つまで設定可能。
　　serverを設定しない場合は、自身がmasterとなる。
　　serverをsetした場合はmaster設定は無効となる。
＜　no　＞　no server (A.B.C.D|FQDN|X:X::X:X) : Delete

◆ timeout

＜説　　明＞　同期時刻タイムアウト時間を設定します。
＜書　　式＞　timeout <seconds:1-30>
＜初 期 値＞　timeout 30
＜　no　＞　no timeout (=timeout 30)

第 19 章

SNMP node

SNMP node

SNMP(Simple Network Management Protocol)機能

NXR 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 node

■ 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/ExpressCard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。

■ WiMAX情報

WiMAXモジュール対応機器の場合、RSSI/CINR、SS/CUステータスをMIBで取得することが出来ます。
WiMAXモジュールに対応していない機器の場合は、未対応状態を返信します。

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。
※WiMAXモジュールは、NXR-155/C-WMのみ対応しています。また、NXR-1200は、モバイルデータ通信端末に対応していません。

○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およびWiMAXモジュールでは、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およびWiMAXモジュールでは、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およびWiMAX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 node

■ 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 node

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#snmp
nxr130(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-130)]
<　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 NXR-130 Series ver 5.1.0 (build 50/15:44 22 04 2009)

SNMP node

◆ 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＞　SNMP の trap agent を設定します。
＜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＞　TRAP パケット中の "Agent Address" を指定することが出来ます。

◆ bind address
＜説　　明＞　SNMP の bind address を設定します。
＜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＞　TRAP 送信時の source ip もこの bind address となります。
　　未設定(no bind address)の場合は 0.0.0.0 で listen します。

第 20 章

syslog node

syslog node

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#syslog
nxr130(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|disk1:FILENAME)
＜初 期 値＞　no local file
＜　No　＞　no local file
＜備　　考＞　filename は「disk0:」または「disk1:」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。
＜書　　式＞　server (A.B.C.D|X:X::X:X|FQDN) (|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。

◆ mark

＜説　　明＞　Syslog mark の設定をします。
・Mark の出力間隔を 0 ～ 99min 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。
・なお、mark を syslog へ出力する場合は、syslog の出力 level を debug/info のいずれかに設定してください。
＜書　　式＞　mark <min:0-99>
＜初 期 値＞　mark 20
＜備　　考＞　mark 0　　(Disable にします)
＜　No　＞　no mark　　(=mark 20)

◆ 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。

syslog node

◆ system

<説　　明>
・System Message 出力機能とは、Connection tracking 数、Load Average、メモリ使用量などの system 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。
・System 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。

◆ 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

syslog node

◆ 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
<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

◆ mail server
<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
<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
<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

syslog node

◆ 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。

・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）。rotate チェックの日時は、schedule コマンドで指定します。

＜書　　式＞

```
rotate (disk0|disk1)
rotate (disk0|disk1) threshold logsize <kbytes:150-1000>
rotate (disk0|disk1) threshold files <files:1-10>
rotate (disk0|disk1) threshold logsize <kbytes:150-1000> files <files:1-10>
```

＜初　期　値＞　no rotate

＜　No　＞　no rotate

＜備　　考＞

・USB0 に接続された USB Flash メモリを指定する場合は、disk0 を選択します。USB1 に接続された USB Flash メモリを指定する場合は、disk1 を選択します。

・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。

・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

第 21 章

dhcp-server node

第 21 章 dhcp-server node

dhcp-server node

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#dhcp-server <1-64>
nxr130(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:1-4294967295> <max:1-4294967295>
＜初 期 値＞　lease-time 21600 43200
＜　No　＞　no lease-time　　: Unset DHCP lease time

◆ 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 GATEWAY
＜初 期 値＞　no gateway
＜　No　＞　no gateway　　: Delete

◆ 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　　: Unconfigure

◆ 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
＜備　　考＞　2 つまで設定可能
＜　No　＞　no dns-server　　: Delete

dhcp-server node

◆ **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
＜備　　考＞　2 つまで設定可能
＜　No　＞　no netbios-server　(= Delete)

◆ **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 22 章

dhcp-relay node

dhcp-relay node

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

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#dhcp-relay
nxr130(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 23 章

ipsec local policy node

ipsec local policy node

◆ 移行command
nxr130(config)#**ipsec local policy <policy:1-255>**
nxr130(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

◆ 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=nxr1.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
＜　No　＞　no x509 certificate　　: Unset X.509

第 24 章

ipsec isakmp policy node

ipsec isakmp policy node

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#ipsec isakmp policy <policy:1-65535>
nxr130(config-ipsec-isakmp)#
```

◆ description

＜説　　明＞　ISAKMP policy の説明を記述します。
＜書　　式＞　description DESCRIPTION
＜　No　＞　no description

◆ 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 node 参照)で設定した username に一致させます。
　　userid と password は、ipsec xauth(global node 参照)で設定します。

ipsec isakmp policy node

■ 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

＜　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 ＞

ipsec isakmp policy node

■ 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 NXR_CA
ipsec x509 certificate NXR_CERT
ipsec x509 private-key PRIV_KEY key
ipsec x509 private-key PRIV_KEY password PASSPHRASE
ipsec x509 crl NXR_CRL
ipsec eap identity string MYID password PASSWORD
!
ipsec local policy 1
 address ip
 x509 certificate NXR_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 NXR_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=nxr1.centurysys.co.jp,E=admin@centurysys.co.jp
・・・省略・・・
!
```

< 次ページに続く >

ipsec isakmp policy node

■ 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 node

◆ 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(NXR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 node

◆ 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 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。

＜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。

◆ hash

＜説　　明＞　ハッシュアルゴリズムを設定します。
＜書　　式＞　hash (md5|sha|sha256|sha384|sha512)
＜初 期 値＞　hash sha

ipsec isakmp policy node

◆ encryption
＜説　　明＞　暗号化アルゴリズムを設定します。
＜書　　式＞　encryption (aes128|des|3des)
＜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)
＜初 期 値＞　group 2

◆ 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が削除されます。
＜書　　式＞　lifetime <1081-86400>
＜初 期 値＞　lifetime 10800　(=3 hours)
＜　No　＞　no lifetime　(= lifetime 10800)

◆ 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。

◆ isakmp-mode
＜説　　明＞　Phase 1のネゴーシエーションモードを設定します。
＜書　　式＞　isakmp-mode (main|aggressive)

ipsec isakmp policy node

◆ **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)。

◆ **remote address**

＜説　　明＞　対向のIPアドレスを設定します。
＜書　　式＞　remote address ip (A.B.C.D|any)
　　remote address ipv6 (X:X::X:X|any)

◆ **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=nxr1.centurysys.co.jp,E=admin@centurysys.co.jp

◆ **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>

ipsec isakmp policy node

◆ 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

第 25 章

ipsec tunnel policy node

第25章 ipsec tunnel policy node

ipsec tunnel policy node

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#ipsec tunnel policy <policy:1-65535>
nxr130(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-sha1-hmac|esp-md5-hmac|esp-sha256-hmac|esp-sha384-hmac|esp-sha512-hmac|)
＜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。

◆ set pfs

＜説　　明＞　PFSを設定します。
＜書　　式＞　set pfs (|group1|group2|group5|phase1|group14|group15|group16|group17)
＜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 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>

ipsec tunnel policy node

◆ 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 <1081-86400>

＜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

第25章 ipsec tunnel policy node

ipsec tunnel policy node

◆ 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

◆ match address
＜説　　明＞　IPsec tunnel に適用する IPsec の access-list を設定します。
＜書　　式＞　match address IPSEC-ACL-NAME
match address IPSEC-ACL-NAME nat-traversal
＜備　　考＞　IPsec access-list は、global node で設定します。

◆ 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)

第 26 章

UPnP node

第 26 章 UPnP node

UPnP node

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#upnp
nxr130(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。
　　INTERFACE はethernet, vlan, ppp を指定することができます。
＜書　　式＞　external interface ethernet <0-2> (|vid <1-4094>)
　　external interface ppp <0-4>

○ 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 27 章

QoS (class-policy) node

QoS (class-policy) node

■ 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。
また、いずれかのインタフェースで QoS 機能が有効になった場合、fast-forwarding 機能は、自動的に無効になります。

1. PFIFO(Packet FIFO)
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 node 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) node

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 わ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-120 および NXR-125 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) node

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(NXR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(HTBのみ)による割り当てをサポートします。
MARK値は、NXR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) node

◆ 移行 command

```
nxr130#
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#class policy NAME
nxr130(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+PQ

```
     class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
          queue priority-group <1-32>
```

○ class+fifo

```
     class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
          queue fifo (|limit <1-16384>)
```

○ class+sfq

```
     class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>) queue fair-queue
```

○ class+tbf

```
     class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
          queue shape <RATE:1-1000000> <BUFFER:1-1000000> <LIMIT:1-1000000>
```

○ class+default queue (default queue : fifo)

```
     class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
```

○ class 削除

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

○ 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)
```

○ default queue (default queue: sfq)

```
     class default bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
```

＜備　　考＞　bandwidth および ceil のレートの単位は、kbps です。

第 28 章

QoS (class-filter) node

QoS (class-filter) node

◆ 移行 command

```
nxr130#
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#class filter <2-254>
nxr130(class-filter-config)#
```

■ match

＜説　　明＞　Mark 値、ToS 値を設定します。
＜書　　式＞　match ip mark <1-4095>
　　match ip tos <0-255>
＜備　　考＞　複数の match が設定されている場合、or 条件となります。
＜　No　＞　no match ip mark <1-4095>
　　no match ip tos <0-255>

第 29 章

CRP client node

CRP client node

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 NXR 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、NXR がサーバ、CMS がクライアントとして動作します。

■ CMS と NXR 間の SSH 認証

・CMS->NXR 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、NXR 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 node）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 NXR 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 node

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(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 30 章

route-map node

route-map node

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(NXR 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、いずれかの match 条件にマッチすると該当するアクションが実行されます。なお、NXR 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

```
nxr130#
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#route-map NAME (permit|deny) <1-65535>
nxr130(config-route-map)#
```

< 次ページに続く >

route-map node

■ match

＜説　　明＞　マッチ条件を設定します。

○ QoS で利用(設定)可能な match 条件

＜説　　明＞　QoS 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)

＜書　　式＞　match ip tos <0-255>
match ip mark <1-4095>
match ip address ACL

○ QoS 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
match ip next-hop ACL-NAME
match metric <0-4294967295>
match as-path ACL-NAME
match origin (egp|igp|incomplete)

＜　No　＞　設定したマッチ条件を削除します
no match ip [address|tos|mark|netx-hop (|WORD)]
no match as-path (|WORD)
no match metric (|<0-4294967295>)
no match origin (|egp|igp|incomplete)

＜備　　考＞　ToS と Mark を同時に設定することは出来ません。
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 条件は無視されます。

route-map node

■ set

＜説　　明＞　QoS、BGP4で使用する属性を設定します。

○QoSで利用(設定)可能な属性

＜説　　明＞　QoS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attribute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 local-preference <0-4294967295>
　　set metric <0-4294967295>
　　set origin (egp|igp|incomplete)

＜備　　考＞　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されます。

■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 node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

第 31 章

Web Authenticate node

第31章 Web Authentication node

Web Authentication node

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**

```
nxr120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr120(config)#web-authenticate
nxr120(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 node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 node

■ 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 node

■ 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 node

○ 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 node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 nodeのip webauth-filterを参照してください。

第 32 章

WarpLink node

WarpLink node

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、NXR の機器情報を送信します。

○ 移行 command

```
nxr120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr120(config)#warplink
nxr120(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、NXR 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

NXR 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、WiMAX）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

NXR 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 node

■ 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 nodeで実行します。

○ config情報の送信

NXR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 node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 node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 33 章

Extended track IP reachability node

第33章 Extended track IP reachability node
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F Netevent機能を参照してください。

◆ 移行command

```
nxr125#
nxr125#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr125(config)#track <2048-4095> ip reachability
nxr125(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>
　　source interface wimax <0-0>
＜　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。

第33章 Extended track IP reachability node
Netevent拡張機能(ip reachability)

■ **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 34 章

Extended track IPv6 reachability node

第34章 Extended track IPv6 reachability node
Netevent 拡張機能(ipv6 reachability)

Netevent 拡張機能(ipv6 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 F Netevent 機能を参照してください。

◆ 移行 command

```
nxr125#
nxr125#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr125(config)#track <2048-4095> ipv6 reachability
nxr125(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。

第34章 Extended track IPv6 reachability node
Netevent 拡張機能(ipv6 reachability)

■ **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 35 章

Monitor-log node

第35章 Monitor-log node

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 node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 node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 node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35章 Monitor-log node
ログ機能

◆ 移行command

```
nxr125#
nxr125#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr125(config)#monitor-log
nxr125(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|disk1) (|threshold logsize <150-1000> files <1-10>)
              reachability (disk0|disk1) threshold logsize <150-1000>
              reachability (disk0|disk1) 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|disk1) (|threshold logsize <150-1000> files <1-10>)
              resource (disk0|disk1) threshold logsize <150-1000>
              resource (disk0|disk1) 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(disk0|disk1から)選択します。USB0に接続されたUSB Flashメモリを指定する場合は、disk0を選択します。USB1に接続されたUSB Flashメモリを指定する場合は、disk1を選択します。
・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 36 章

interface WiMAX node

interface WiMAX node

■ UQ WiMAX対応

NXR-155-/C-WMは、UQ WiMAX に対応した通信モジュールを搭載しています。

※ UQ WiMAX を利用するには、別途契約が必要です。UQ WiMAX 契約時に、WiMAX MAC アドレスの情報が必要となります。WiMAX MAC アドレスは、同梱のシールまたは製品裏面のラベルに記載されています。

※ この製品は、UQ WiMAXネットワーク環境でご使用になれますが、本製品の品質等に関してUQコミュニケーションズ株式会社が何ら保証するものではありません。

※ WiMAX モジュールおよびアンテナは、住友電工ネットワークスの製品です。

■ WiMAXインタフェース

- WiMAX（Worldwide Interoperability for Microwave Access）を使用して通信するインタフェースです。本装置で利用可能なWiMAXサービスは、UQ WiMAXサービスのみです。
- Ethernetのように L2 ARPを利用します。
- IPv4のみ使用可能です。IPv6には対応していません。
- IPv4アドレスは、DHCPv4クライアント機能によって取得します。このとき、ネットワークマスクが32ビットのIPアドレスが割り当てられるため、Ethernetのように ARPを利用しますが、point-to-pointインタフェースとして設定されます。
- 本インタフェースは、リンクダウンすることがありません。そのため、WiMAXインタフェースに対してDHCPによってIPv4アドレスが割り当てられているかどうかで、切断 / 接続を判断します。
- WiMAXの接続 / 切断時に、SNMPのインタフェースリンク up/downを送出します。WiMAXモジュールの抜き差しを行うと、インタフェース admin up/downを送出します。モジュールのリセット等により、突然WiMAXがdownした場合は、リンクダウントラップが送出されないことがあります。
- 本インタフェースを対象とするパケットフォワーディング時、fast-forwarding機能は動作しません。

○WiMAXインタフェースの設定例

以下に、WiMAXインタフェースの設定例を示します（設定はお客様の環境に合わせて変更してください）。

```
!
interface wimax 0
 ip address dhcp              ①DHCPクライアントでIPアドレスを取得します。
 ip masquerade                ②IPマスカレードを設定します。
!
ip route 0.0.0.0/0 wimax 0    ③WiMAXインタフェースをデフォルトゲートウェイに設定します。
!
```

interface WiMAX node

○ 移行command

```
nxr155#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr155(config)#interface wimax 0
nxr155(config-wimax)#
```

◆ 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。

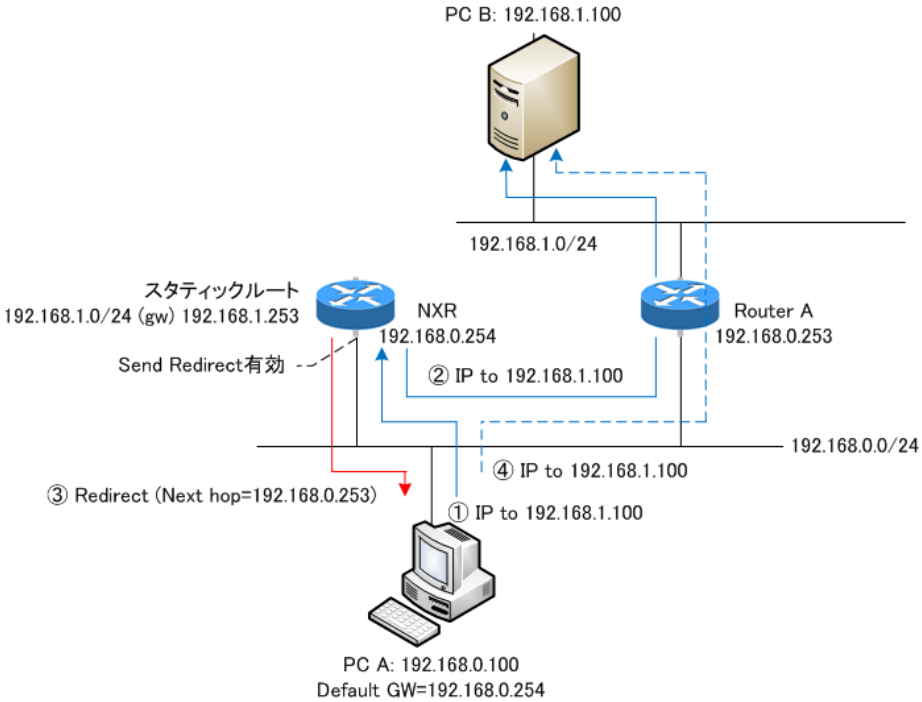
① Host Aは、Host B(192.168.1.100)へのIPv4パケットをdefault gw(NXR)に送信します。

② NXR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 WiMAX node

◆ 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 WiMAX node

◆ 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。

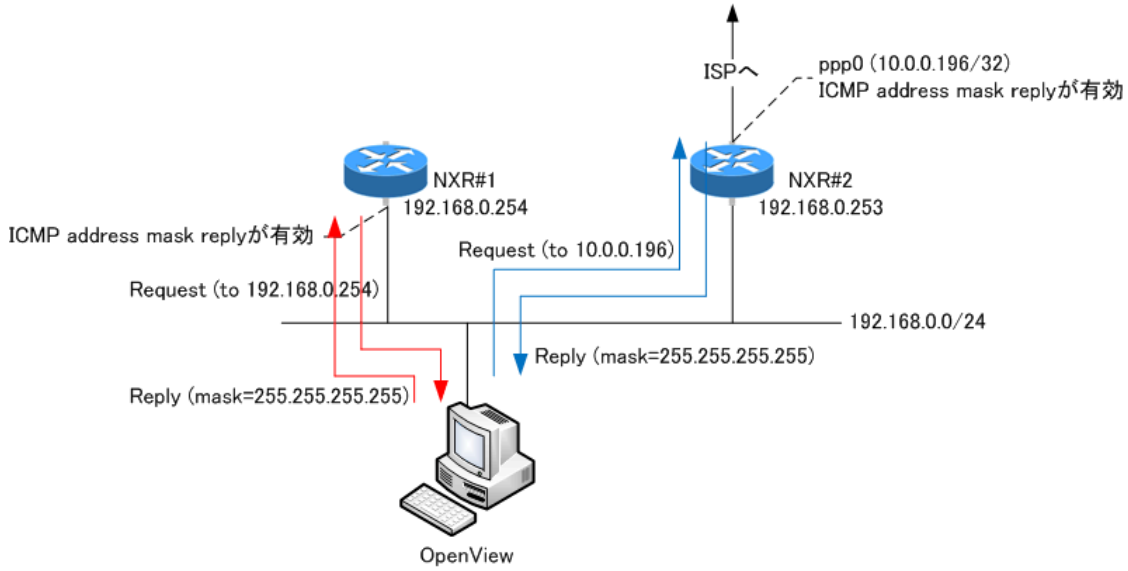
＜書　　式＞　ip mask-reply　（ICMP address mask requestに応答します。）

＜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 WiMAX node

◆ 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/WiMAX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。

◆ ip access-group

＜説　　明＞
・global node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)　NXR自身で受信して処理するパケットを制限します。
- out(local output) NXR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NXR自身が作成したパケットとして認識します。
- forward-in　NXR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 NXR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。

interface WiMAX node

◆ 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/WiMAX)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 node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 node)で行います。

◆ 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 WiMAX node

◆ session invalid-status-drop-interface

＜説　　明＞

・session invalid-status-drop 機能(global node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 node 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、wimax 0 インタフェースに適用する場合の設定例です。

- global node で、session invalid-status-drop を無効にします。

```
nxr155(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。

```
nxr155(config)#interface wimax 0
nxr155(config-wimax)#session invalid-status-drop-interface enable
```

◆ netevent

＜説　　明＞

・トラックイベントの発生時に、当該WiMAX をconnect(またはdisconnect)することが出来ます。

＜書　　式＞　netevent <trackid:1-255>|<trackid:2048-4095> (connect|disconnect)

＜　No　＞　no netevent

◆ 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 node）を参照してください。

・Web認証については、Web Authenticate nodeを参照してください。

interface WiMAX node

◆ 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2つまで設定することが出来ます。IPv4とIPv6に、それぞれ1つずつのIPsecローカルポリシー の割り当てを想定しています。

◆ 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 WiMAX node

■ 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 node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。

interface WiMAX node

■ 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/WiMAX 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 WiMAX node

■ 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(wimax <0-0>)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 node 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 node 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 node)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 node)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。
wimax0 の接続時：　wimax0 was connected
wimax0 の切断時：　wimax0 was disconnected

第 37 章

mail server node

mail server node

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。

○ WiMAX の接続 / 切断

イベント	メールの件名	メールの本文
WiMAXの接続	wimax0 was connected	IP address is A.B.C.D
WiMAXの切断	wimax0 was disconnected	wimax0 was disconnected
DHCPのアドレスリリース時	wimax0 was disconnected	IP address is released

※上記は、wimax0 の接続 / 切断時に送信するメールの例です。

第37章 mail server node

mail server node

○ 移行command

```
nxr155#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr155(config)#mail server 0
nxr155(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 node

■ 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 node または interface wimax node で、インタフェース毎（ppp <0-4>, wimax <0-0>）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/wimax node）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 node)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/wimax node）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 node)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

付録 A

設定事例

付録 A

Ⅰ．インタフェースの設定例

工場出荷状態では、ETHER 1 に IP アドレスが付いていません。ここでは、ETHER 1 に IP アドレスを付与する手順について説明します。

1. Console(または Telnet)で、本装置にログインします。

```
Century Systems NXR-130 Series ver 5.1.0
nxr130 login: admin
Password:
Century Systems NXR-130 Series ver 5.1.0 (build 47/17:36 03 04 2009)
nxr130#
```

2. “configure terminal”コマンドで、CONFIGURATION モードに移行します。

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#
```

3. “interface ethernet 1”コマンドで、interface node に移行します。

```
nxr130(config)#interface ethernet 1
nxr130(config-if)#
```

4. IP アドレス（およびその他）の設定をします。

```
nxr130(config-if)# description ETHER 1              ←インタフェース名の設定（任意）
nxr130(config-if)#ip address 192.168.1.254/24
```

5. “exit”コマンドを 2 回実行して、view node に移行します。

```
nxr130(config-if)#exit
nxr130(config)#exit
nxr130#
```

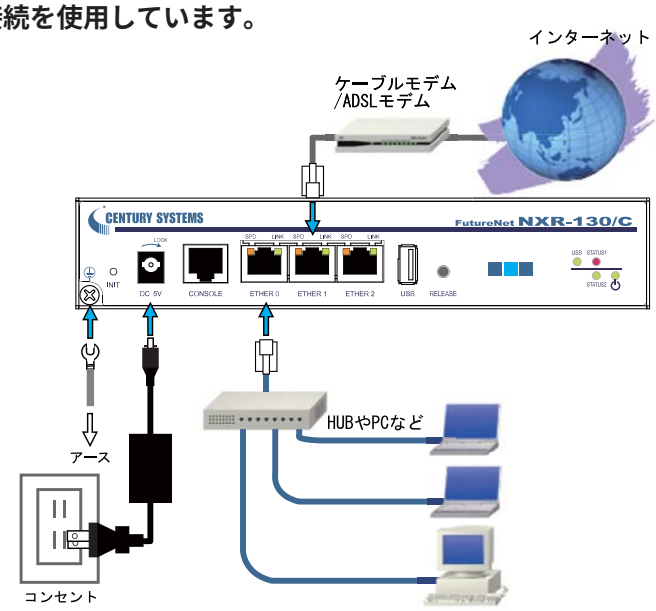
6. “show config”コマンドで、設定を確認します。

```
nxr130#show config
!
!  ・・・前後の設定表示は省略・・・
!
interface ethernet 1
 description ETHER 1
 ip address 192.168.1.254/24
!
!  ・・・前後の設定表示は省略・・・
!
```

付録 A

II．PPPoE の設定例

PPPoE を使用してインターネットに接続する基本的な設定例を記載します。この例では、OCN IPv6 および、IPv4 の B フレッツ接続を使用しています。




```
nxr130#show config
!
! Century Systems NXR-130 ver 5.1.1 (build XX/11:43 07 05 2009)
!
hostname nxr130                          ←ホスト名の設定
!
!
ipv6 forwarding                          ← IPv6 フォワーディングを有効に設定
fast-forwarding enable                   ←ファストフォワーディングを有効に設定（任意）
!
!
l2tp 0                                   ← OCN IPv6 の接続は L2TP トンネルを使用
 tunnel address XXXXXXXXX.ocn.ne.jp      ← OCN IPv6 の接続先を指定（XXXX は伏せ字）
 tunnel ppp 0                            ← PPP over L2TP の設定
!
interface ppp 0
 description OCNv6                       ← PPP 0 の接続名を OCNv6 に設定
 no ip address
 ipv6 dhcp client pd AAA                 ← DHCPv6-PD（prefix delegation）の設定
 mtu 1390                                ← PPP インタフェースの MTU を設定。
                                           OCN IPv6 のデフォルト値は 1390 バイト。
 ipv6 tcp adjust-mss auto                ← IPv6 の TCP MSS を auto(自動調整)に設定
 ipv6 access-group in dhcpv6             ←入力フィルタで DHCPv6 パケットを許可（詳細は後述）
 ipv6 spi-filter                         ← IPv6 の SPI フィルタを設定
 ppp username XXXXXX password hidden XXXXXXX ← PPP 接続のアカウント（ID とパスワード）を設定
 no ppp ipcp enable                      ← IPCP を無効に設定
 ppp ipv6cp enable                       ← IPv6CP を有効に設定
```

付録 A

II．PPPoE の設定例

```
!
interface ppp 1
 description B-flets_XXX                ←PPP1 は B フレッツ
 ip address negotiated                  ←動的 IP を使用
 no ip redirects                        ←ICMP リダイレクトを無効に設定
 ip tcp adjust-mss auto                 ←TCP MSS を auto(自動調整)に設定
 ip access-group in upnp                ←入力フィルタで UPnP パケットを破棄（詳細は後述）
 ip access-group forward-in upnp        ←転送フィルタで UPnP パケットを破棄（詳細は後述）
 ip access-group forward-out private    ←転送フィルタで private ネットワーク宛のパケットを破棄
                                          （詳細は後述）
 ip masquerade                          ←ppp1 インタフェースで IP マスカレードを有効に設定
 ip spi-filter                          ←ppp1 インタフェースで SPI を有効に設定
 ppp username XXXXXX password hidden XXXXXX   ←PPP 接続のアカウント（ID とパスワード）を設定
!
interface ethernet 0
 ip address 192.168.XXX.XXX/24          ←ethernet 0 インタフェースに IP アドレスを設定
 ip access-group in netbios             ←入力フィルタで NetBIOS パケットを破棄（詳細は後述）
 ip access-group forward-in netbios     ←転送フィルタで NetBIOS パケットを破棄（詳細は後述）
 ipv6 address AAA ::254/64              ←DHCPv6-PD で取得したプレフィクス＋下位アドレス（254）
 ipv6 nd send-ra                        ←RA（Router advertisement）を送信する
!
interface ethernet 1
 no ip address                              ←ethernet 1 インタフェースの IP アドレスを無効化
 ip access-group in upnp                    ←入力フィルタで UPnP パケットを破棄（詳細は後述）
 ip access-group forward-in upnp            ←転送フィルタで UPnP パケットを破棄（詳細は後述）
 pppoe-client ppp 1                         ←pppoe クライアントを実行（ppp1）。
!
interface ethernet 2
 shutdown                                   ←ethernet 2 は、ここでは使用しないので無効化
 no ip address
!
dns
 service enable                             ←DNS サービスを有効に設定
 address XXX.XXX.XXX.XXX                    ←DNS サーバを指定
 address XXX.XXX.XXX.XXX
!
syslog
 local enable                               ←syslog のローカル出力を有効に設定
!
snmp
 security 192.168.XXX.XXX/24                ←SNMP マネージャのネットワーク範囲を指定
 syslocation XXX                            ←sysLocation の設定
 syscontact XXXXXX                          ←sysContact の設定
 sysname nxr130                             ←sysName の設定
```

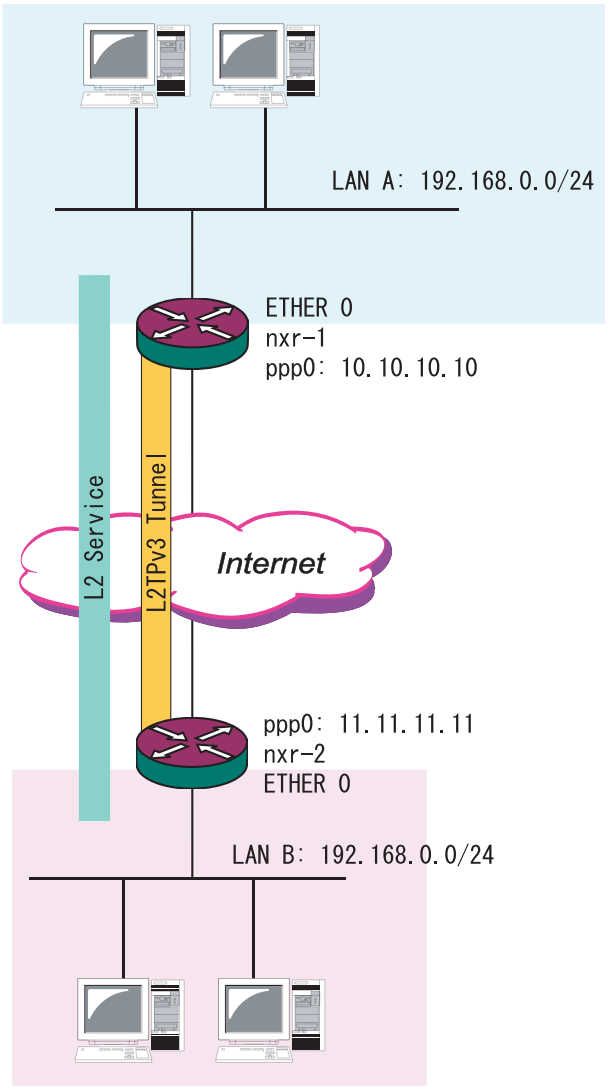
付録 A

II．PPPoE の設定例

```
!
!
!
ip route 0.0.0.0/0 ppp 1                        ← IPv4 のデフォルトルートを ppp1 に設定
ip route 192.168.110.0/24 192.168.XXX.XXX       ←その他のスタティックルートの設定
ip route 192.168.120.0/24 192.168.XXX.XXX
ip route 192.168.130.0/24 192.168.XXX.XXX
ip route 192.168.140.0/24 192.168.XXX.XXX
ip route 192.168.150.0/24 192.168.XXX.XXX
!
ipv6 route ::/0 ppp 0                           ← IPv6 のデフォルトルートを ppp0 に設定
!
ip access-list netbios deny any any tcp any range 137 139       ← NetBIOS のパケットを破棄
ip access-list netbios deny any any udp any range 137 139
ip access-list netbios deny any any tcp 137 any
ip access-list netbios deny any any udp 137 any
ip access-list private deny any 192.168.0.0/16  ←プライベートネットワーク宛のパケットを破棄
ip access-list private deny any 172.16.0.0/12
ip access-list private deny any 10.0.0.0/8
ip access-list upnp deny any any udp any 1900       ← UPnP のパケットを破棄
ip access-list upnp deny any any tcp any 5000
ip access-list upnp deny any any tcp any 2869
!
ipv6 access-list dhcpv6 permit any any udp range 546 547 range 546 547
                                                    ← DHCPv6 のパケットを許可
!
```

III．L2TPv3 の設定例

2 拠点間で L2TPv3 トンネルを構築し、End to End で Ethernet フレームを透過的に転送する設定例です。

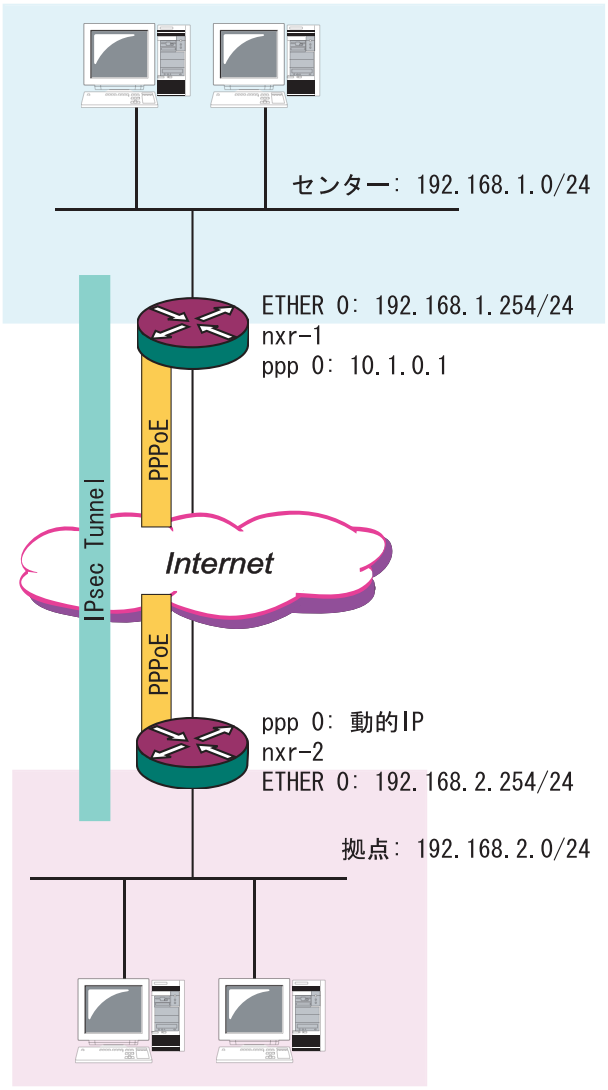



```
< nxr1 の設定 >
!
l2tpv3 hostname nxr1   ←本装置のホスト名
l2tpv3 router-id 192.168.200.254
                       ←本装置の ID
!
l2tpv3 tunnel 1
 description nxr1-nxr2
 tunnel address 11.11.11.11
          ←対向 LCCE の WAN 側 IP アドレス
 tunnel hostname nxr2  ←対向 LCCE のホスト名
 tunnel router-id 192.168.200.253
                       ←対向 LCCE の ID
!
l2tpv3 xconnect 1
 description nxr1-nxr2
 tunnel 1
 xconnect ethernet 0
          ←L2 フレーム受信インタフェース
 xconnect end-id 1
          ←対向 LCCE の end-id と一致させます
!

 < nxr2 の設定 >
!
l2tpv3 hostname nxr2
l2tpv3 router-id 192.168.200.253
!
l2tpv3 tunnel 1
 description nxr2-nxr1
 tunnel address 10.10.10.10
 tunnel hostname nxr1
 tunnel router-id 192.168.200.254
!
l2tpv3 xconnect 1
 description nxr2-nxr1
 tunnel 1
 xconnect ethernet 0
 xconnect end-id 1
!
```

IV. IPsec の設定例

センター・拠点間で IPsec トンネルを 1 対 1 で構築する場合の設定例です。



<接続条件>

- センター側・拠点側ともに PPPoE 接続とします。
- ただし、センター側は固定アドレス、拠点側は動的アドレスとします。
- IPsec 接続の再接続性を高めるため、IPsec キープアライブを設定します。
- IP アドレス、ネットワークアドレスは、左図のとおりです。
- 拠点が動的 IP アドレスのため、aggressive モードで接続します。
- PSK 共有鍵を用い、鍵は ”centurysys” とします。

<次ページに続く>

Ⅳ．IPsec の設定例

```
< nxr-1 の設定 >
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description to nxr2
 authentication pre-share centurysys
                  ←PSK を ” centurysys ” に設定
 keepalive periodic clear
      ←キープアライブの設定（失敗時に SA を削除）
 hash sha1
 encryption aes128
 group 14
 isakmp-mode aggressive       ←aggressive モード
 remote address ip any        ←拠点は動的 IP
 remote identity fqdn nxr2.desu
                        ←拠点の ID を設定(FQDN)
 local policy 1
!
!
ipsec tunnel policy 1
 description to nxr2
 negotiation-mode manual
           ←センター側はイニシエートしない。
 set transform esp-aes128 esp-sha1-hmac
 set key-exchange isakmp 1
           ←使用する ISAKMP ポリシー番号を指定
 match address nxr2
      ← IPsec アクセスリスト ” nxr2 ” を指定（後述）

!
!
interface ppp 0
 description test
 ip address 10.1.0.1/32       ←固定 IP アドレス
 ip tcp adjust-mss auto
 ip access-group in in-ppp0
 ip masquerade
 ip spi-filter
 ppp authentication pap
 ppp username user001@xxx.com password user001
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.1.254/24
                          ←LAN 側の IP アドレス
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
interface ethernet 2
 no ip address
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list in-ppp0 permit any any 50
                          ←ESP を許可
ip access-list in-ppp0 permit any any udp
any 500
                          ←ISAKMP を許可
ip access-list in-ppp0 permit any any icmp
!
ipsec access-list nxr2 ip 192.168.1.0/24
192.168.2.0/24
                  ←srcIP dstIP の場合に暗号化
!
```

IV. IPsecの設定例

< nxr-2の設定 >

```
!
ipsec local policy 1
 address ip
 self-identity fqdn nxr2.desu
                        ←センターのID(FQDN)
!
!
ipsec isakmp policy 1
 description to nxr1
 authentication pre-share centurysys
 keepalive 10 3 periodic
 hash sha1
 encryption aes128
 group 14
 isakmp-mode aggressive
 remote address ip 10.1.0.1
                  ←センターのWAN側IPアドレス
 local policy 1
!
!
ipsec tunnel policy 1
 description to nxr1
 set transform esp-aes128 esp-sha1-hmac
 set key-exchange isakmp 1
 match address nxr1
!
!
interface ppp 0
 description test
 ip address negotiated
 ip tcp adjust-mss auto
 ip access-group in in-ppp0
 ip masquerade
 ip spi-filter
 ppp authentication pap
 ppp username user002@xxx.com password user002
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.2.254/24
                          ←LAN側のIPアドレス
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
interface ethernet 2
 no ip address
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list in-ppp0 permit any any icmp
ip access-list in-ppp0 permit 10.0.0.1 any 50
ip access-list in-ppp0 permit 10.0.0.1 any
udp any 500
!
ipsec access-list nxr1 ip 192.168.2.0/24
192.168.1.0/24
                    ←srcIP dstIPの場合に暗号化
!
```

付録 A

V．モバイル接続の設定例

NXR シリーズが現在対応している、もしくは対応を予定しているモバイルデータ通信端末は、弊社の Web サイトを参照してください。

http://www.centurysys.co.jp/router/list_mobiledata.html

モバイルデータ通信端末を使用してインターネットに接続する基本的な設定例を記載します。この例では、通信事業者としてイーモバイルを使用しています。

1．はじめに、モバイルデータ通信端末を装着します。show mobile 0 ap を実行して、”APN: emb.ne.jp ” の CID と PDP Type を確認します。下記の例では、”APN: emb.ne.jp ” の CID は 1、PDP Type は IP です。

```
nxr120#show mobile 0 ap
CID      : 1
PDP Type : IP
APN      : emb.ne.jp

CID      : 2
PDP Type : PPP
APN      : rtc.data

CID      : 3
PDP Type : IP
APN      : 3g.commu
```

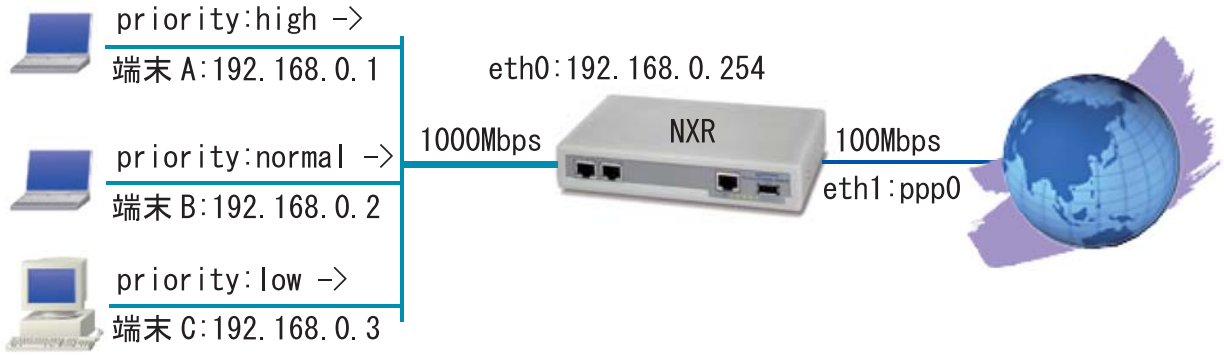
2．続いて、取得した CID と PDP Type を元に、モバイル接続の設定を行います。

```
nxr120#show config
・・・途中省略・・・
!
interface ppp 0
 description 3G
 ip address negotiated
 no ip redirects
 ip tcp adjust-mss auto
 ip masquerade
 ppp username em password em            ←ユーザ ID とパスワードを設定
 dial-up string *99***1#                ←cid が 1 なので、末尾を 1# に設定
 mobile apn emb.ne.jp cid 1 pdp-type ip ←cid は 1、pdp-type は IP
・・・途中省略・・・
!
mobile 0 ppp 0                          ←モバイル接続に ppp 0 を使用
!
ip route 0.0.0.0/0 ppp 0                ← IPv4 のデフォルトルートを ppp0 に設定
end
```

付録 A

VI. QoSの設定例

QoS(PQ)の設定例を示します。
端末A、端末B、端末C(LAN:1000Mbps)からWAN:100Mbpsにudpデータを送信する際に、優先制御(PQ)が行われます。例えば、各端末からの送信レートが40Mbpsの場合、ppp0を通過するトラフィックは、A:40Mbps、B:40Mbps、C:20Mbpsになります(実際のスループットは、WAN回線の実効速度に依存します)。




```
!
priority-map 1 high ip mark 1
                      ← Mark値の設定をします。
priority-map 1 low ip mark 3
      ← 1:high, 3:low, その他:default(normal)
!
interface ppp 0
 description pppoe
 ip address negotiated
 ip tcp adjust-mss auto
 ip masquerade
 ppp username XXXX password YYYY
 queue priority-group 1
                          ← PQの設定をします。
!
interface ethernet 0
 ip address 192.168.0.254/24
 classify input route-map RMAP1
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
route-map RMAP1 permit 1
 match ip address list1
       ← マッチ条件の設定をします。(ACL:list1)
 set mark 1
               ← Mark値を設定します。(1:high)
!
route-map RMAP1 permit 2
         ← マッチ条件の設定をします。(ACL:list2)
 match ip address list2
      ←default class(normal)に割り当てられます。
 set mark 2
!
route-map RMAP1 permit 3
 match ip address list3
         ← マッチ条件の設定をします。(ACL:list3)
 set mark 3
                    ← Mark値を設定します。(3:low)
!
!
!     QoSのアクセスリストを設定します。
class access-list list1 ip 192.168.0.1 any udp
class access-list list2 ip 192.168.0.2 any udp
class access-list list3 ip 192.168.0.3 any udp
!
end
```

付録 B

Packet Traveling

付録 B

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

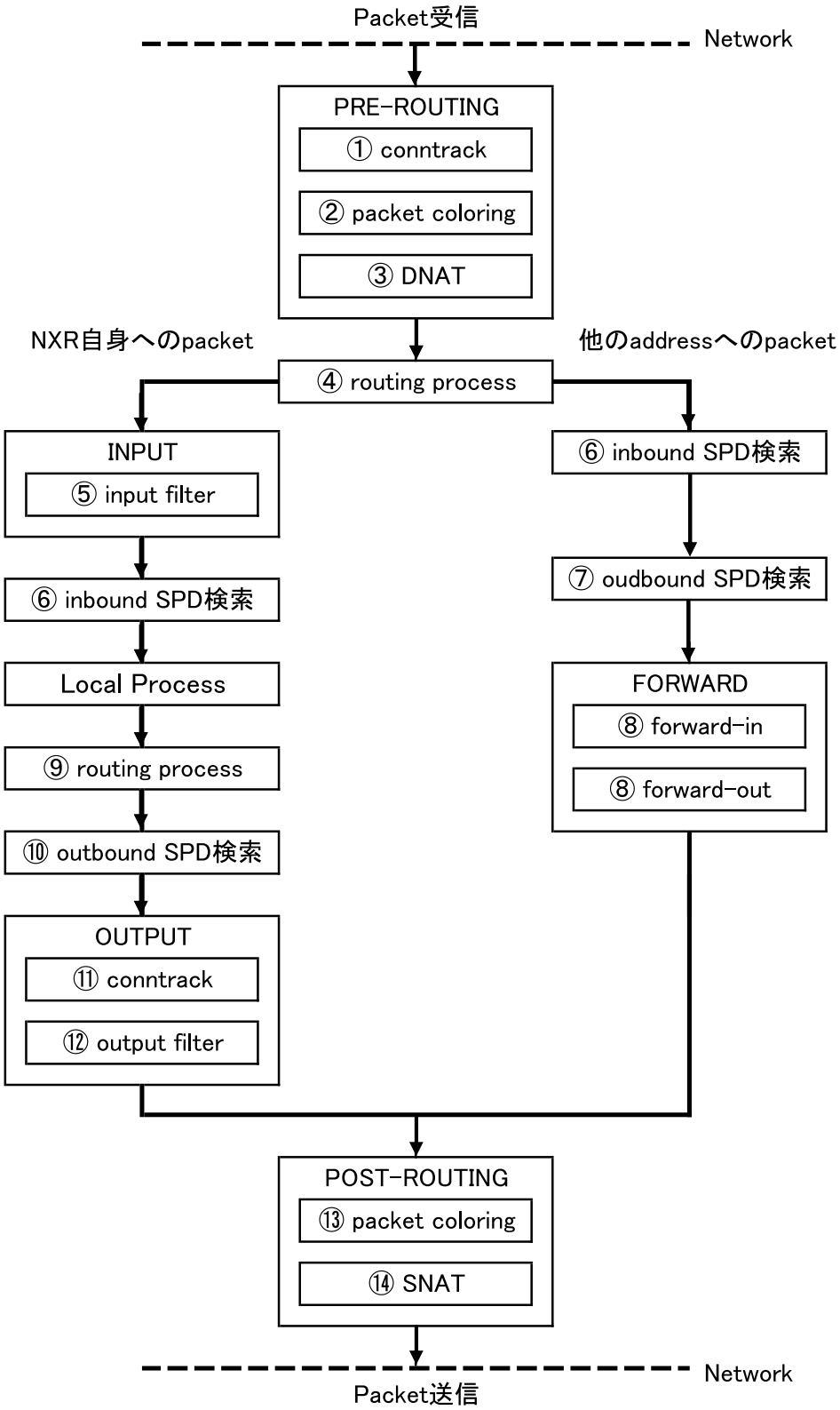
(1) SYSTEM SNAT
(2) IPsec policy に match したパケットは、以下の NAT はチェックしません。
ただし、IPsec snat-policy が有効の場合は、以下の NAT のチェックを継続します。
(3) USER 設定 SNAT(Static NAT)
(4) IPv4 Masquerade

付録 B

Packet Traveling

3. NXR Packet Traveling

NXR 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 B

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 node)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(NXR 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 node)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。
--> NXR local process

付録 B

Packet Traveling

○ Packet 送信時（NXR が送信元）

- NXR 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 node)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 C

Policy based IPsec と Route based IPsec

付録 C　Policy based IPsec と Route based IPsec

Ⅰ. Policy based IPsec

1. Policy based IPsec

ここでは、NXR 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、NXR 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/WiMAX)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。

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。

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 protocol を変更することができます。現状、transport 用の IP としては、IPv4のみ対応しています。
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)
<　No　>　no tunnel mode
<備　　考>　Route based IPsec を使用する際は、ipsec ipv4 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 C 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 C 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)
指定した ToS 値を tunnel IP Header に設定します。inherit に設定した場合、tunneling IPv4 header の ToS 値を tunnel IP header にコピーします。ToS 値指定の場合、ECN field を設定することはできません。また、IPv6 packet を tunneling する場合は、inherit 設定は無視されて、ToS は 0x0 が設定される。
ECN field の扱いについては、「付録 C 1.2.4.1 ECN field の扱い」を参照してください。

```
<書　　式>　tunnel tos (<0-252>|inherit)
<初 期 値>　tunnel tos inherit
<　No　>　no tunnel tos　　(= tunnel tos inherit)
```

○ 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 C 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 C 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。Default の動作は、post-fragment です。

2.4.1. Post-fragment

Fragment 処理が必要な場合、ESP 化した後に fragment が行われます。そのため、ESP packet と ip fragment packet に分割されます。

2.4.2. 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出来ます。

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、NXR 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、NXR 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 C：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。

2.4.3. 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。

・NXR での PMTUD 設定(enable/diable)と Fragment 設定(pre-fragment/post-fragment)は、interface tunnel node 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
```

2.4.4. 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、NXR 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 node 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。

付録 C Policy based IPsec と Route based IPsec

II. Route based IPsec

2.4.5. 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）。

2.4.6. 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 D

IKEv2 Protocol

付録 D

IKEv2 Protocol

NXR 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 D

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 D

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。

認証方式	Pre-shared key方式
	Digital署名方式 RSA(X.509)
	EAP-MD5
	EAP-RADIUS
Encryption Algorithm	3DES-CBC
	DES-CBC
	AES128/192/256-CBC
	NULL
Hash Algorithm	HMAC-MD5-96
	HMAC-SHA1-96
	HMAC-SHA256-128
	HMAC-SHA384-192
	HMAC-SHA512-256
	NULL(認証なし) ※CHILD_SA時のみ
PRF Algorithm (Hashと同じAlgorithmを使用)	PRF-HMAC-MD5
	PRF-HMAC-SHA1
	PRF-HMAC-SHA-256
	PRF-HMAC-SHA-384
	PRF-HMAC-SHA512
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 Group未指定(PFSは無効)

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。

付録 D

IKEv2 Protocol

3. EAP-RADIUS 認証

IPsec client からの EAP message を、NXR 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。

3.1 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。

3.2 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.NXR120-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 node で設定します。
```

付録 D

IKEv2 Protocol

4. Rekey

4.1 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 node 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。

4.1 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 E

Firmware update

付録 E

Firmware update

1. Firmware の replace

NXR 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)
firmware update ftp://<A.B.C.D|X:X::X:X>/FILENAME (|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

○ copy(CLI)

ストレージデバイスから firmware をコピーします。

＜書　　式＞　firmware update (disk0:FILENAME|disk1:FILENAME)

付録 E

Firmware update

1.1 Firmware update 中の service の継続

NXR-125、NXR-130(ISDN ポートありの機種のみ)、および NXR-155 では、firmware update 中もルータとしての処理を行うことが出来ます。サービスの継続を行うか停止するかをユーザが選択することができます。
上記以外の NXR シリーズでは、すべてのサービスおよびパケット処理を停止します。

Firmware update の実行例を下記に示します。

```
nxr125#firmware update disk0:nxr125-v581.bin
[============================================================] 100% DECODE
Proceed with update? [(y)es/(b)ackgroud/(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 executed.............................................
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。サービスを停止する場合は「y」、サービスを継続する場合は「b」、firmware update をキャンセルする場合は「n」を入力します。
※本装置の負荷が高い状態で、サービスを継続したままファームアップを行うと、ファームアップに時間がかかる場合があります。その場合は、サービスを停止してファームアップを行うようにしてください。
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。

付録 E

Firmware update

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 F

Netevent 機能

付録 F

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 との neighbor 確立後から他の state への変化を監視します。

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 F
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 F
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 F

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 F

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 node)で設定します。
vrrp ip <vrrpid:1-255> netevent <trackid:1-255> priority <1-254>

② IPsec 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 node)で設定します。
netevent <trackid:1-255> (connect|disconnect|reconnect)

③ PPP の接続 / 切断を行うことが出来ます。
次のコマンド(interface ppp node)で設定します。
netevent <trackid:1-255> (connect|disconnect)

④ Tunnel interface の up/down をすることが出来ます。
次のコマンド(interface tunnel node)で設定します。
netevent <trackid:1-255> (connect|disconnect)

⑤ L2TPv3 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 node)で設定します。
netevent <trackid:1-255> disconnect

⑥ IPsec local policy の変更を行うことが出来ます。
次のコマンド(ipsec isakmp policy node)で設定します。
local policy <policy:1-255> netevent <trackid:1-255> change <local_policy:1-255>

⑦ IPsec isakmp policy の変更を行うことが出来ます。
次のコマンド(ipsec tunnel policy node)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 node)で設定します。
system netevent (<1-255>|<2048-4095>) restart

⑨WiMAX 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 node)で設定します。
wimax <0-0> netevent (<1-255>|<2048-4095>) reset

⑩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 node)で設定します。
mobile <0-2> netevent (<1-255>|<2048-4095>) reset

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
```

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 node/ipsec tunnel policy node 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、WiMAX または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＞　wimax <0-0> netevent (<1-255>|<2048-4095>) reset
　　　　　　　mobile <0-2> netevent (<1-255>|<2048-4095>) reset
＜　no　＞　no wimax <0-0> 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 G

VRRP

付録 G

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。したがって、NXR と XR 間で VRRP を使用する場合は、XR で仮想 MAC を使用してください。
・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。

1.1 セカンダリアドレスとの併用

・VRRP パケットを送出する際の送信元 IPv4 アドレスには、プライマリの IPv4 アドレスを使用します。セカンダリアドレスは使用できません。

1.2 ルーティングプロトコルとの併用(RIP と VRRP の併用)

・RIP が動作している状態で VRRP マスターとなっている場合、仮想 IP アドレスを RIP パケットの送信元アドレスとして使用することは出来ません。

1.3 Proxy ARP の使用について

・VRRP が動作しているインタフェース上では、proxy ARP 機能は無効になります。

1.4 ICMP redirect について

・VRRP が動作しているインタフェース上では、ICMP redirect は送信しません。

1.5 ARP Request に対する応答

・仮想 IPv4 アドレスに対する ARP Request に対しては、仮想 MAC で応答を返します。一方、実 IPv4 アドレスに対する ARP Request の場合は、実 MAC にて応答します。

付録 G

VRRP

1.6 仮想 IP アドレスに対する通信

・VRRP マスターの状態になると、VRRP インタフェースに仮想 IP アドレス(VIP)が設定されます。送信元アドレスが VIP で、送信先アドレスが VIP の属するネットワークの場合、VRRP インタフェースから出力するように policy routing table が設定されます。
・そのため、仮想 IP アドレスから送信する場合、送信元 MAC アドレスとして必ず仮想 MAC アドレスを使用します。VRRP インタフェースから出力されるため、Ethernet に設定したフィルタや経路設定は適用されません。

1.6.1 VRRP インタフェース

・VRRP インタフェース(およびインタフェース番号)は、本装置が VRRP インスタンス毎に自動的に生成します。ユーザは、VRRP インタフェースに対して、フィルタやルート設定などを行うことは出来ません。
・VRRP インタフェースは、次に示す設定値を Ethernet インタフェースから引き継ぎます。したがって、VRRP グループが属する Ethernet インタフェースで、arp queue length を 100 に設定すると、VRRP インタフェースの arp queue length も 100 に設定されます。

```
ip icmp mask-reply
ip arp queue length
ip arp reachable-time
```

付録 G

VRRP

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。

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 H

VLAN

付録 H （スイッチポート搭載機種のみ）

Ⅰ．VLAN 仕様

スイッチポート搭載機種の VLAN 仕様

スイッチポートを搭載する NXR（NXR125 および NXR-155 のみ）の VLAN 仕様について記します。使用可能なポートは Ether0 のポート 1～4、およびルータポート(CPU)です。

■ デフォルト VLAN ID(PVID)

＜説　　明＞　ポート毎に、デフォルト VLAN ID(PVID)を指定することができます。

・ここで指定した PVID は、トランク接続で付加する IEEE802.1Q タグ(VLAN タグ)の VLAN ID として使用されます。

・システムのデフォルト状態では、全てのポートは PVID=1 の VLAN に所属します。

＜書　　式＞　switchport (<1-4>|router) default-vlan-id <1-4094>
＜初 期 値＞　switchport (<1-4>|router) default-vlan-id 1
＜　no　＞　no switchport (<1-4>|router) default-vlan-id
＜備　　考＞　インタフェースノード（interface ethernet 0）にて設定します。

■ アクセスリンク／トランクリンク

＜説　　明＞

ポート毎に、アクセスリンクとして使用するか、またはトランクリンクとして使用するかを設定します。

・ポートをアクセスリンクとして指定すると、そのポートが所属する VLAN トラフィックのみを転送することができます。転送するフレームに、VLAN タグを付加しません。システムのデフォルト状態では、全てのポートはアクセスリンクとして設定されています。

・ポートをトランクリンクとして指定すると、複数の VLAN トラフィックを転送することができます。転送するフレームには、フレームを受信したアクセスリンクの PVID を VLAN ID とする VLAN タグを付加します。タグ無しフレームは破棄します。

＜書　　式＞　switchport (<1-4>|router) link (access|trunk)
＜初 期 値＞　switchport (<1-4>|router) link access
＜　no　＞　no switchport (<1-4>|router) link
＜備　　考＞　インタフェースノード（interface ethernet 0）にて設定します。

■ VLAN データベース

＜説　　明＞　スイッチポートで使用する VLAN ID を設定します。
＜書　　式＞　vlan-database vid <1-4094>
＜初 期 値＞　no vlan-database
＜　no　＞　no vlan-database (|vid <1-4094>)
＜備　　考＞　インタフェースノード（interface ethernet 0）にて設定します。

■ VLAN ID とタグの有無

＜説　　明＞　スイッチポート毎に、有効な VLAN ID とタグの有無(tagged/untagged)を設定します。
＜書　　式＞　switchport (<1-4>|router) vlan <1-4094> (tagged|untagged)
＜初 期 値＞　switchport (<1-4>|router) vlan 1 untagged
＜　no　＞　no switchport (<1-4>|router) vlan (|(1-4094)>
＜備　　考＞　インタフェースノード（interface ethernet 0）にて設定します。

付録 H （スイッチポート搭載機種のみ）

Ⅰ．VLAN 仕様

■ VLAN データベースの情報表示

＜説　　明＞　VLAN ID 毎に、tagged/untagged の情報および所属するポート番号を表示します。
＜書　　式＞　show interface vlan-database
＜備　　考＞　view node にて実行することができます。

■ スイッチポートの情報表示

＜説　　明＞
・スイッチポートのポート毎に、デフォルト VLAN ID とアクセスリンク / トランクリンクの情報を表示します。
＜書　　式＞　show interface switchport
＜備　　考＞　view node にて実行することができます。

付録 H （スイッチポート搭載機種のみ）

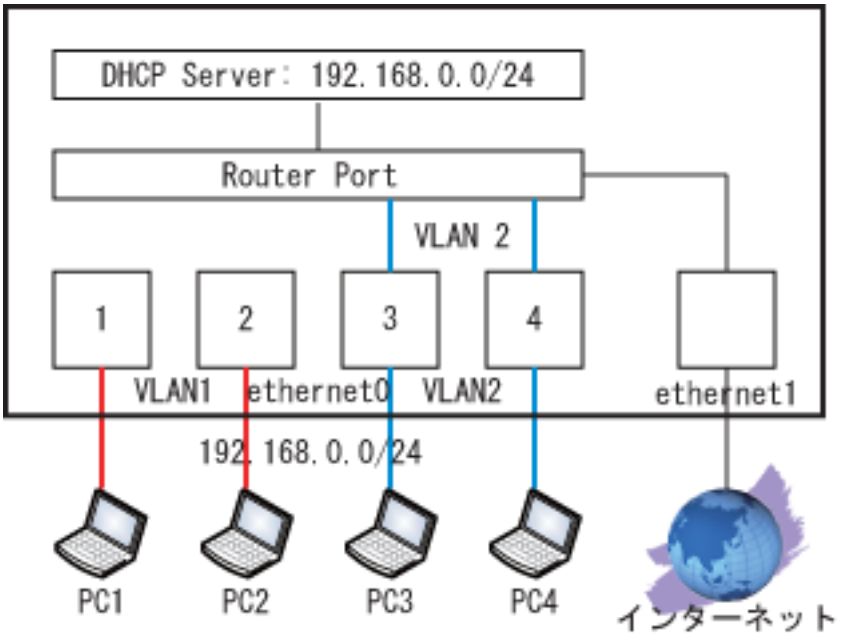
II．ポートベース VLAN

ポートベース VLAN

ポートベース VLAN の例を示します。

■ ネットワーク構成

・VLAN1(Port1 と Port2)および VLAN2(Port3 と Port4)の 2 つの VLAN からなる構成例です。
・同一 VLAN 内での通信は可能ですが、異なる VLAN 間での通信は不可です。PC1 と PC2 は通信可能ですが、PC1 と PC3 は通信不可です。
・PC3 と PC4 はインターネットに接続できますが、PC1 と PC2 はインターネットに接続できません。
・PC3 と PC4 は DHCP Client です。この構成では、PC1 と PC2 は内部 DHCP サーバからアドレスを取得することは出来ません。(VLAN1 は、Router Port(CPU)と通信できないため、孤立したネットワークです)。



付録 H （スイッチポート搭載機種のみ）

II．ポートベース VLAN

■ 設定（抜粋）

```
interface ethernet 0
 ip address 192.168.0.125/24
 switchport 3 default-vlan-id 2
 no switchport 3 vlan 1
 switchport 3 vlan 2 untagged
 switchport 4 default-vlan-id 2
 no switchport 4 vlan 1
 switchport 4 vlan 2 untagged
 switchport router default-vlan-id 2
 no switchport router vlan 1
 switchport router vlan 2 untagged
 vlan-database vid 1
 vlan-database vid 2
!
interface ethernet 1
ip address 172.16.77.125/24
ip masquerade
!
dns
service enable
address 172.16.77.64
!
dhcp-server 1
network 192.168.0.0/24 range 192.168.0.1 192.168.0.10
gateway 192.168.0.125
dns-server 192.168.0.125
!
ip route 0.0.0.0/0 172.16.77.64
```

■ 情報表示

```
nxr125#show interface vlan-database
ethernet0
    VLAN ID 1
        Untagged:port1,port2
        Tagged:n/a
    VLAN ID 2
        Untagged:port3,port4,router
        Tagged:n/a

nxr125#show interface switchport
ethernet0
        port1  Default VLAN ID:1    Access link
        port2  Default VLAN ID:1    Access link
        port3  Default VLAN ID:2    Access link
        port4  Default VLAN ID:2    Access link
        router Default VLAN ID:2    Access link
```

付録 H （スイッチポート搭載機種のみ）

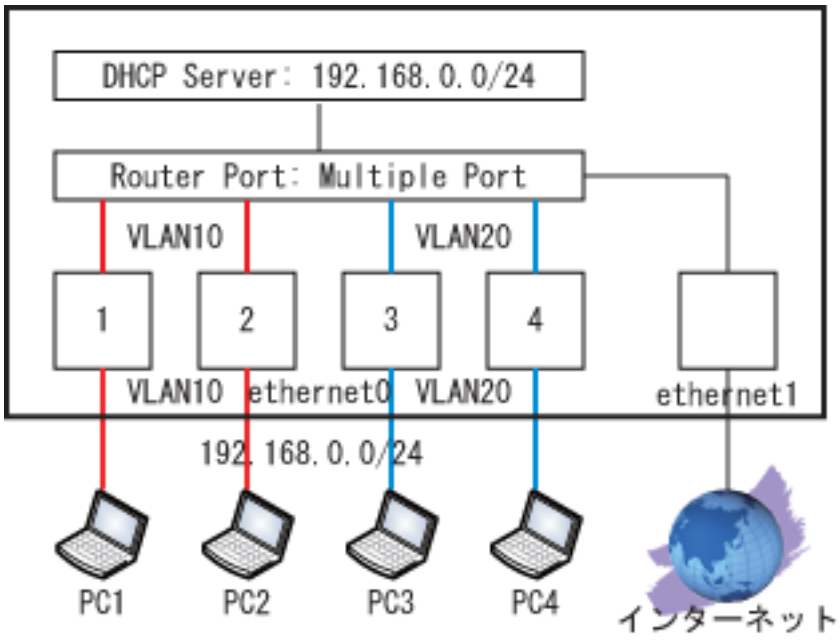
III．マルチプル VLAN

マルチプル VLAN

マルチプル VLAN の例を示します。

■ ネットワーク構成

・複数の VLAN から接続できるポート（マルチプルポート）からなる構成例です。
VLAN1(Port1，Port2，Port3，Port4，Router Port)、VLAN10(Port1 と Port2)、VLAN20(Port3 と Port4)、および Multiple Port(Router Port)を持ちます。
・VLAN10 および VLAN20 は、同一 VLAN 内での通信は可能ですが、異なる VLAN 間での通信は不可です。
PC1 と PC2 は通信可能ですが、PC1 と PC3 は通信不可です。
・PC1～PC4 は DHCP Client です。内部 DHCP サーバでは VLAN10 と VLAN20 のサブネットを分けることはできません。サブネットを分ける場合はスイッチポートに外部 DHCP サーバを接続します。



付録 H （スイッチポート搭載機種のみ）

III．マルチプル VLAN

■ 設定（抜粋）

```
interface ethernet 0
 ip address 192.168.0.125/24
 switchport 1 default-vlan-id 10
 switchport 1 vlan 10 untagged
 switchport 2 default-vlan-id 10
 switchport 2 vlan 10 untagged
 switchport 3 default-vlan-id 20
 switchport 3 vlan 20 untagged
 switchport 4 default-vlan-id 20
 switchport 4 vlan 20 untagged
 switchport router vlan 10 untagged
 switchport router vlan 20 untagged
 vlan-database vid 1
 vlan-database vid 10
 vlan-database vid 20
!
interface ethernet 1
 ip address 172.16.77.125/24
 ip masquerade
!
dns
 service enable
 address 172.16.77.64
!
dhcp-server 1
 network 192.168.0.0/24 range 192.168.0.1 192.168.0.10
 gateway 192.168.0.125
 dns-server 192.168.0.125
!
ip route 0.0.0.0/0 172.16.77.64
```

■ 情報表示

```
nxr125#show interface vlan-database
ethernet0
    VLAN ID 1
        Untagged:port1,port2,port3,port4,router
        Tagged:n/a
    VLAN ID 10
        Untagged:port1,port2,router
        Tagged:n/a
    VLAN ID 20
        Untagged:port3,port4,router
        Tagged:n/a

nxr125#show interface switchport
ethernet0
        port1  Default VLAN ID:10   Access link
        port2  Default VLAN ID:10   Access link
        port3  Default VLAN ID:20   Access link
        port4  Default VLAN ID:20   Access link
        router Default VLAN ID:1    Access link
```

付録 H （スイッチポート搭載機種のみ）

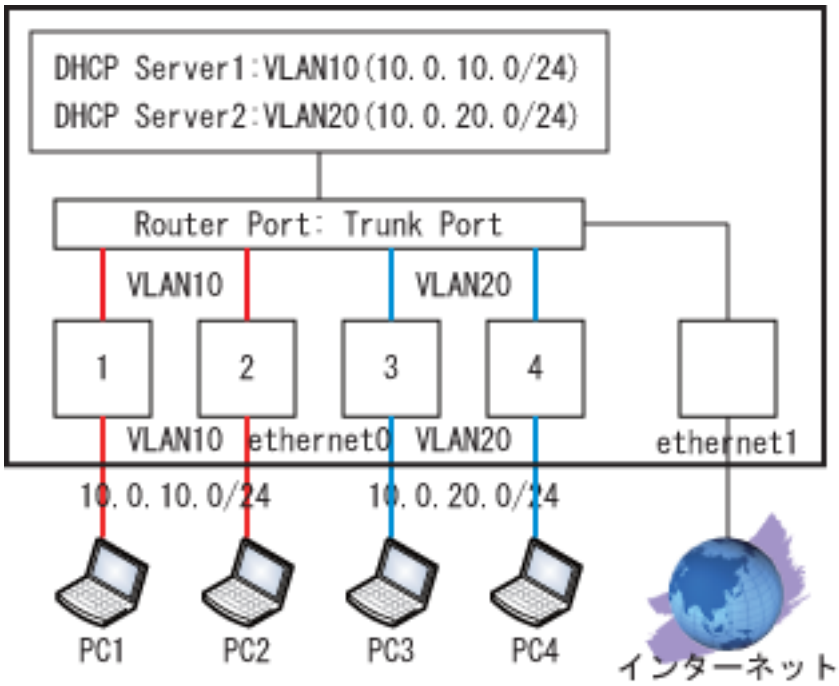
IV．タグ VLAN(VLAN トランク)

タグ VLAN(VLAN トランク)

タグ VLAN(VLAN トランク)の例を示します。

■ ネットワーク構成

・VLAN10(Port1 と Port2)、VLAN20(Port3 と Port4)、および VLAN1[Router Port(Trunk Port)]からなる構成例です。
・アクセスリンクとトランクリンクを保有します。アクセスリンクから受信したフレームは、PVID を VLAN ID とする VLAN タグを付加してトランクリンクから転送します。



付録 H （スイッチポート搭載機種のみ）

Ⅳ．タグ VLAN(VLAN トランク)

■ 設定（抜粋）

```
interface ethernet 0
 ip address 192.168.0.125/24
 switchport 1 default-vlan-id 10
 no switchport 1 vlan 1
 switchport 1 vlan 10 untagged
 switchport 2 default-vlan-id 10
 no switchport 2 vlan 1
 switchport 2 vlan 10 untagged
 switchport 3 default-vlan-id 20
 no switchport 3 vlan 1
 switchport 3 vlan 20 untagged
 switchport 4 default-vlan-id 20
 no switchport 4 vlan 1
 switchport 4 vlan 20 untagged
 switchport router link trunk
 switchport router vlan 10 tagged
 switchport router vlan 20 tagged
 vlan-database vid 1
 vlan-database vid 10
 vlan-database vid 20
!
interface ethernet 0 vid 10
 ip address 10.0.10.125/24
 ip access-group forward-in VLAN10
!
interface ethernet 0 vid 20
 ip address 10.0.20.125/24
 ip access-group forward-in VLAN20
!
interface ethernet 1
 ip address 172.16.77.125/24
 ip masquerade
!
dns
 service enable
 address 172.16.77.64
!
dhcp-server 1
 network 10.0.10.0/24 range 10.0.10.1 10.0.10.10
 gateway 10.0.10.125
 dns-server 10.0.10.125
!
dhcp-server 2
 network 10.0.20.0/24 range 10.0.20.1 10.0.20.10
 gateway 10.0.20.125
 dns-server 10.0.20.125
!
ip route 0.0.0.0/0 172.16.77.64
!
ip access-list VLAN10 deny any 10.0.20.0/24
ip access-list VLAN20 deny any 10.0.10.0/24
!
```

■ 情報表示

```
nxr125#show interface vlan-database
ethernet0
    VLAN ID 1
        Untagged:router
        Tagged:n/a
    VLAN ID 10
        Untagged:port1,port2
        Tagged:router
    VLAN ID 20
        Untagged:port3,port4
        Tagged:router

nxr125#show interface switchport
ethernet0
        port1  Default VLAN ID:10   Access link
        port2  Default VLAN ID:10   Access link
        port3  Default VLAN ID:20   Access link
        port4  Default VLAN ID:20   Access link
        router Default VLAN ID:1    Trunk link
```

付録 I

Configの保存と復帰

付録 I　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flash-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 node）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 node）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を外部記憶装置に保存する例：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 node）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 node）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 node）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 node）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
- 外部記憶装置からconfigを復帰する例： copy disk0:config.xml flash-config

GUIから設定の復帰を行った場合、flash-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）。

```
nxr130#copy ssh://guest@192.168.0.1/config.xml flash-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 node）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 flash-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 node）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。

付録 J

サポートについて

付録 I

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/

◆故障と思われる場合は

製品の不良や故障と思われる場合でも、必ず事前に弊社までご連絡ください。
事前のご連絡なしに弊社までご送付いただきましてもサポートをお受けすることはできません。

◆ご連絡をいただく前に

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 MAC アドレス
・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。**

◆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/

◆製品の保証について

本製品の保証期間は、ご購入から販売終了後 5 年間までです。
（但し、AC アダプタ及び添付品の保証期間はご購入から 1 年間とします。）
保証期間内でも、保証書に販売店印のないもの(弊社より直接販売したものは除く)、また保証の範囲外の故障については有償修理となりますのでご了承ください。
保証規定については、同梱の保証書をご覧ください。

FutureNet NXR シリーズ ユーザーズガイド CLI 編 Ver.5.16.1 対応版

2011 年 09 月版
発行 センチュリー・システムズ株式会社