FutureNet NXR-120/C
NXR-125/CX
NXR-130/C

ユーザーズガイド　CLI 編

NXR-120/C　v5.9.0 対応版
NXR-125/CX　v5.8.1 対応版
NXR-130/C　v5.5.5 対応版

CENTURY SYSTEMS

目次

はじめに

◆ご注意

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

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

3 本書の内容の一部または全部を無断で転載、複写することを禁じます。

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

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

◆商標の表示

□「FutureNet」はセンチュリー・システムズ株式会社の登録商標です。

その他、本書で使用する各会社名、製品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
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、1m）	1本		
RJ-45/D-sub9ピン変換アダプタ（クロス）	1個		
ACアダプタ	1個		
ゴム足 （必要に応じて本体底面の四隅に貼ってください）	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	―
ケーブル固定用ネジ	―	1個	―
CARD部分を塞ぐシール	―	1枚	―

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。

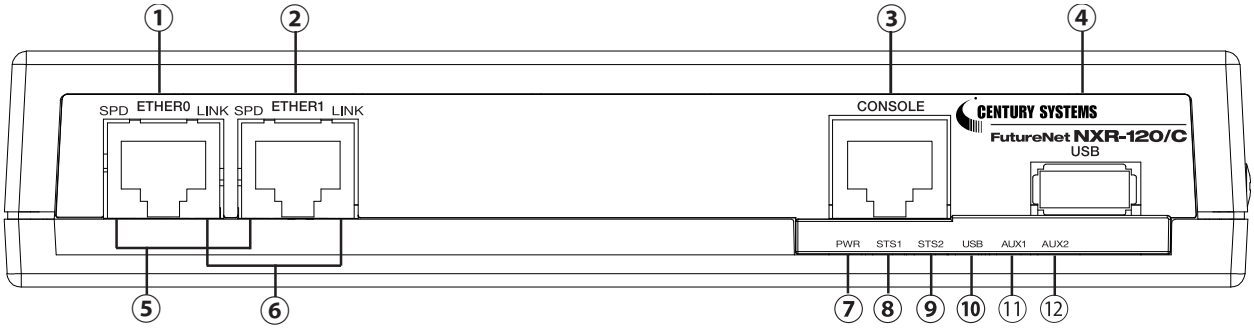
◆ FutureNet NXR-120/C
http://www.centurysys.co.jp/router/nxr120c.html

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

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

II．各部の名称と機能（NXR-120/C）

◆製品前面（NXR-120/C）



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 ：

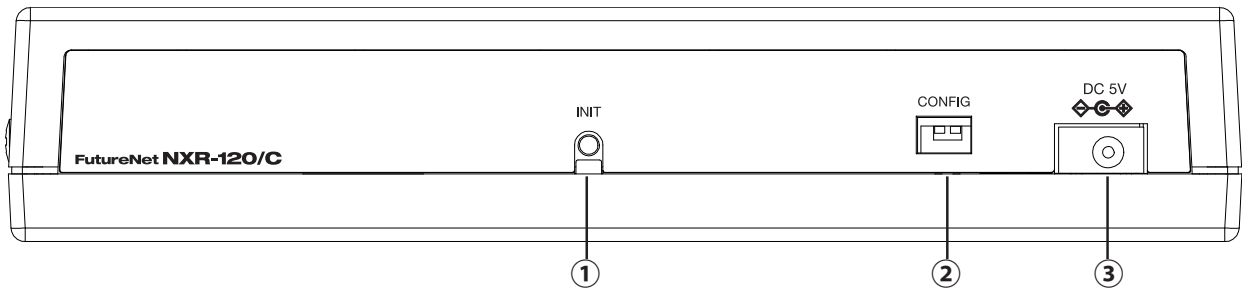
⑩ USB LED(緑)
USB ステータスを示します。
USB デバイス装着時 ：
USB デバイス未装着時 ：

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（NXR-120/C）



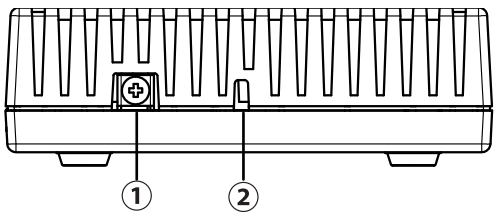
① INIT ボタン
本装置を工場出荷時の設定に戻して起動するときに使用します。

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（NXR-120/C）

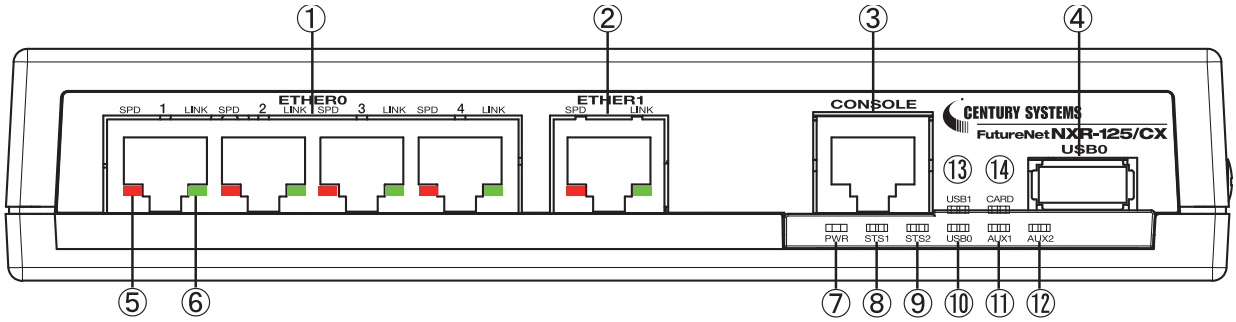


① FG端子
保安用接続端子です。
必ずアース線を接続してください。

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（NXR-125/CX）



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 ：	■	■

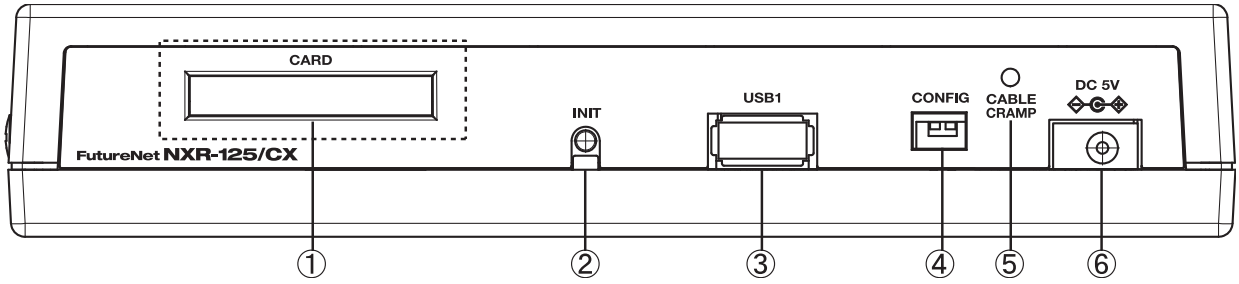
指定した PPP または tunnel の状態を示します。
接続時 ： ■
切断状態時 ： ■

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（NXR-125/CX）



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。

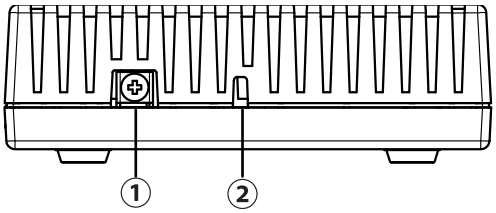
③ USB1 ポート
USB Flash メモリ、または USB タイプのデータ通信端末を挿入します。

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（NXR-125/CX）

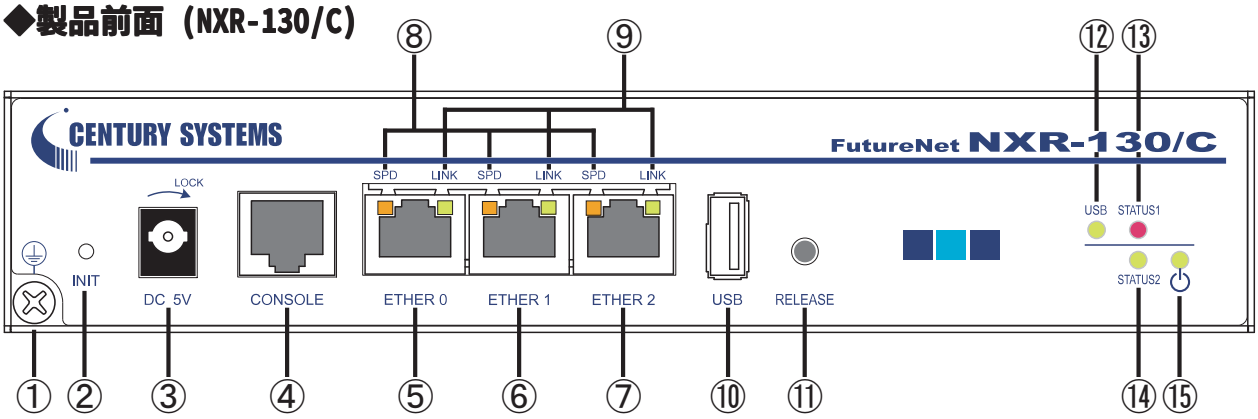


① FG(アース）端子
保安用接続端子です。
必ずアース線を接続してください。

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）

◆製品前面（NXR-130/C）



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）

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．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。

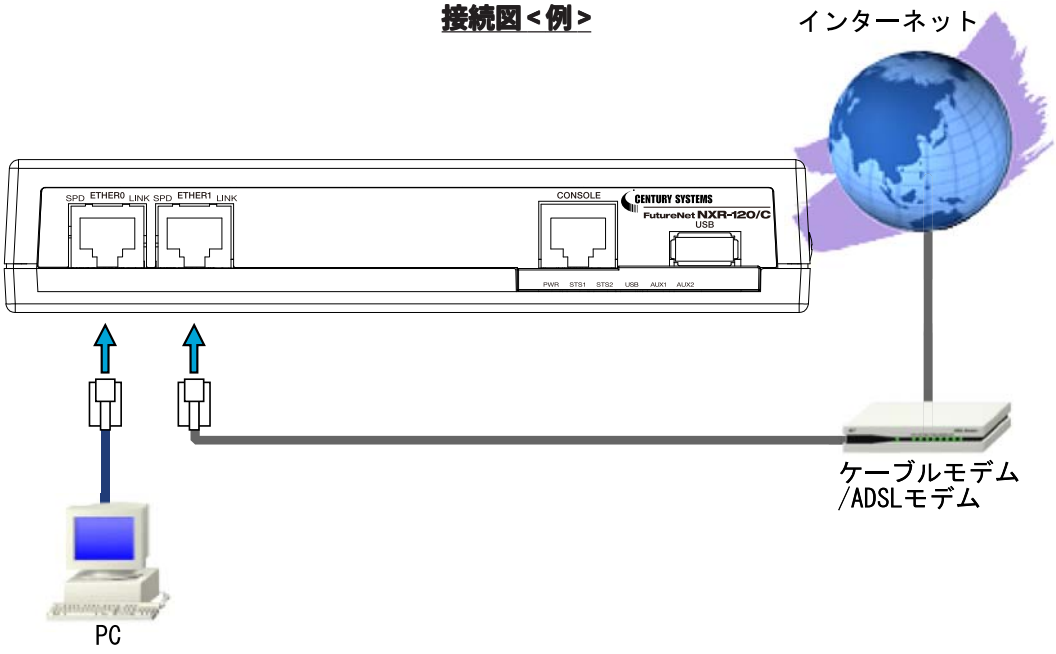
注意！

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）

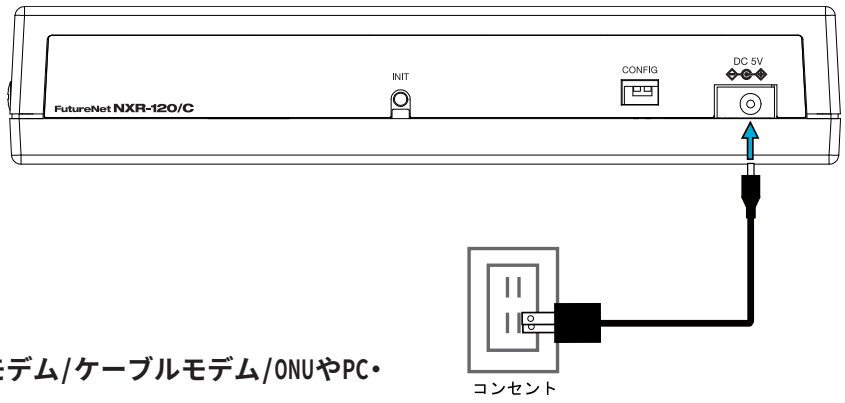
NXR-120/C と PC や xDSL モデム / ケーブルモデム /ONU は、以下の手順で接続してください。

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。**

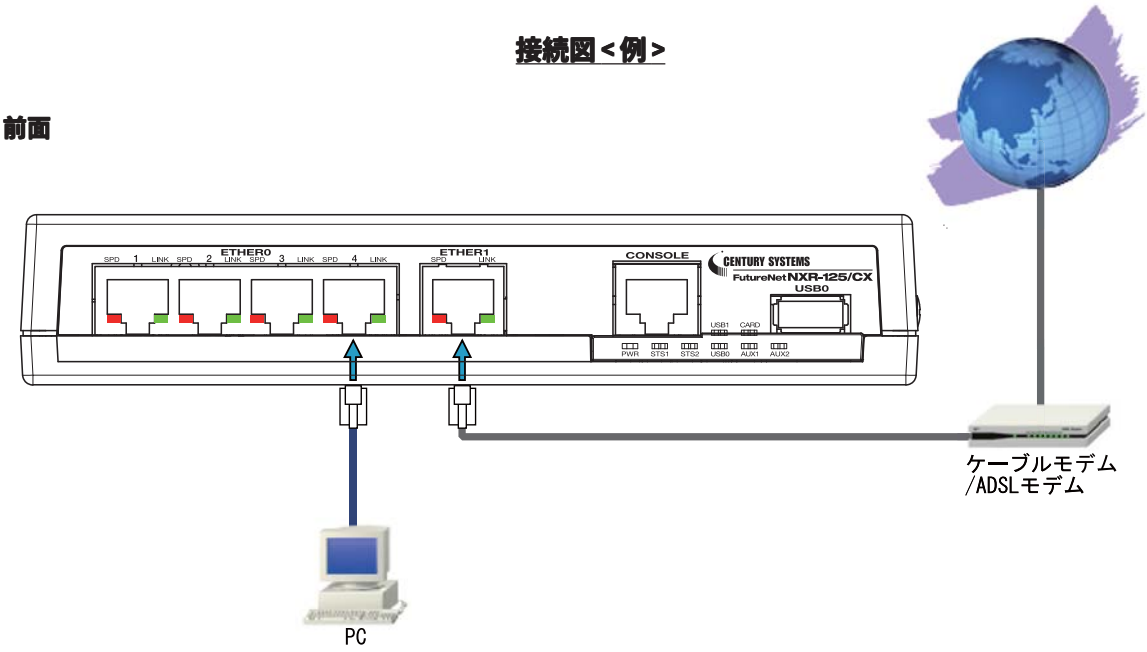
本装置の全ての Ethernet ポートは、AutoMDI/MDI-X対応です。

III．装置の設置（NXR-125/CX）

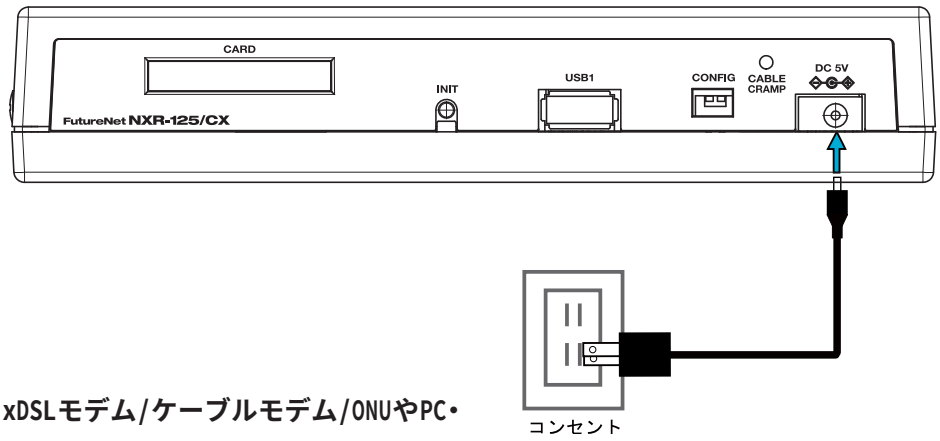
NXR-125/CX と PC や xDSL モデム / ケーブルモデム /ONU は、以下の手順で接続してください。

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。

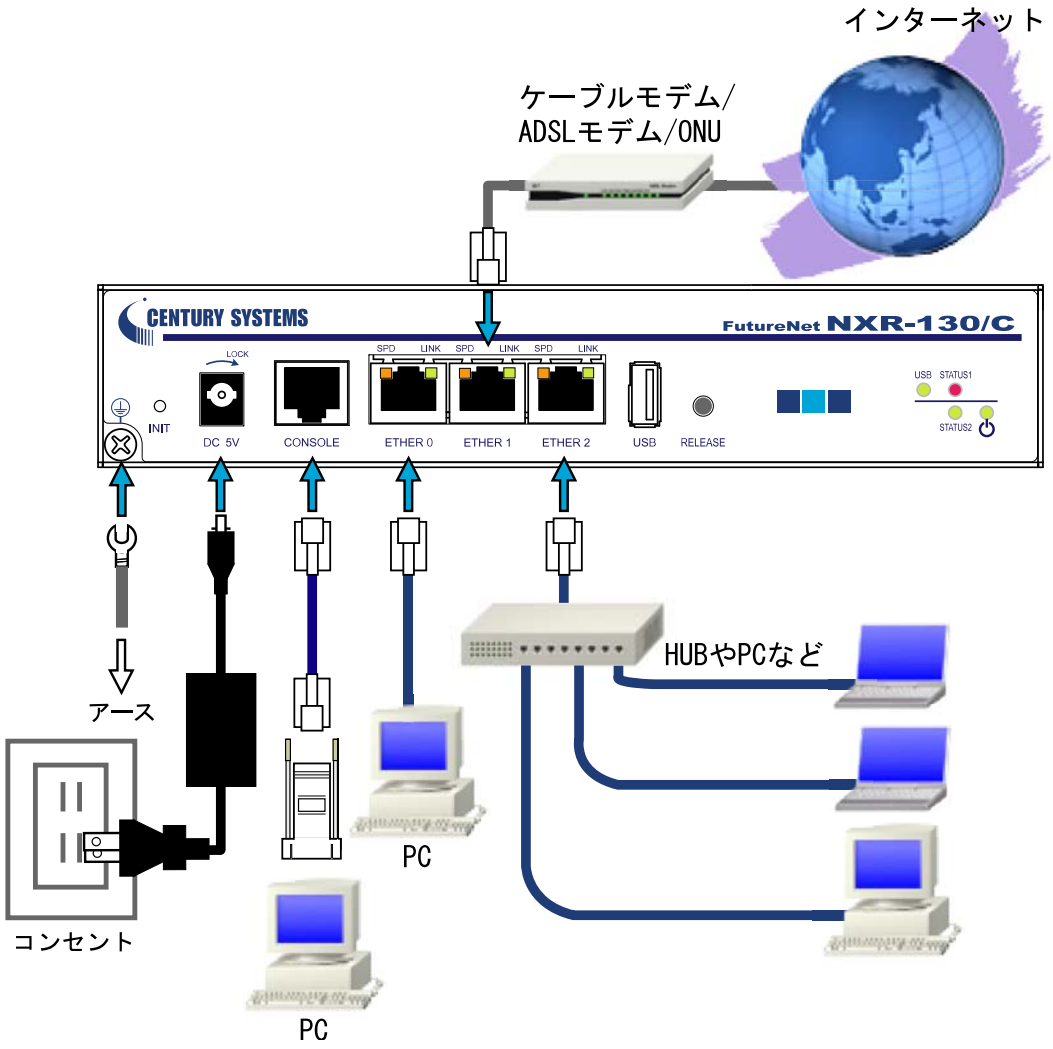
5 全ての接続が完了しましたら、各機器の電源を投入してください。

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。

第3章

設定方法の概要

Ⅰ．CLI の接続方法

◆はじめに

ユーザーズガイド CLI 編は、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 ETHER 0 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、ETHER 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 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。

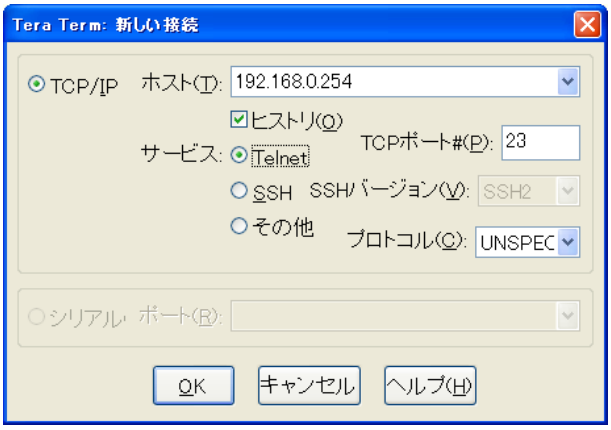
◆本装置へのログイン（TELNET の場合）

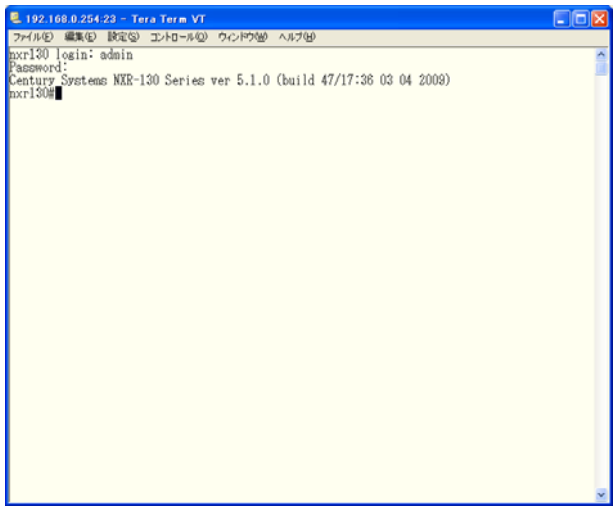
1．TELNET 接続を開始すると、ログイン画面が表示されます。

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は完了です。

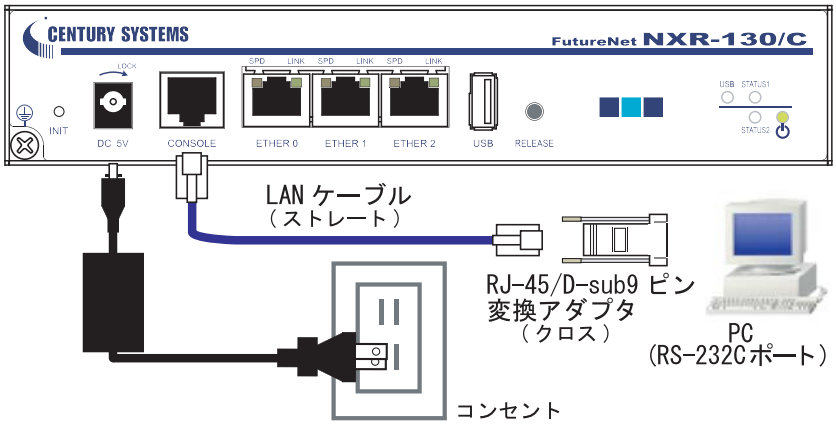
＜画面は TeraTerm による Telnet のログイン画面です＞





Ⅰ．CLI の接続方法

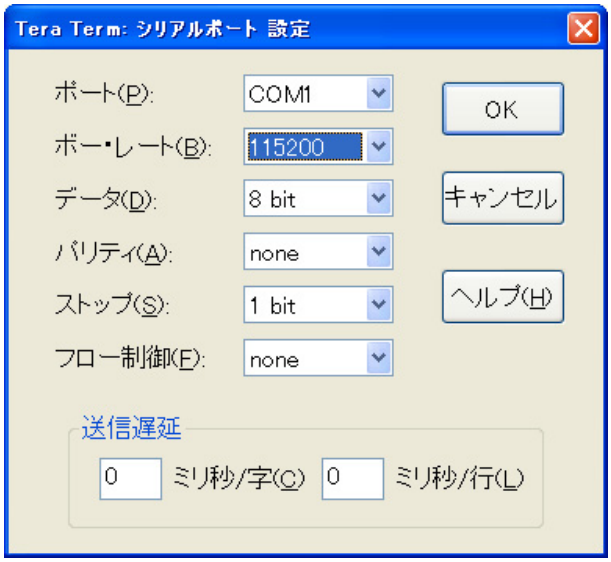
◆本装置へのログイン（CONSOLE の場合）



1．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。

2．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。



3．「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。

4．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は完了です。

II．GUI の接続方法

◆本装置へのログイン（GUI の場合）

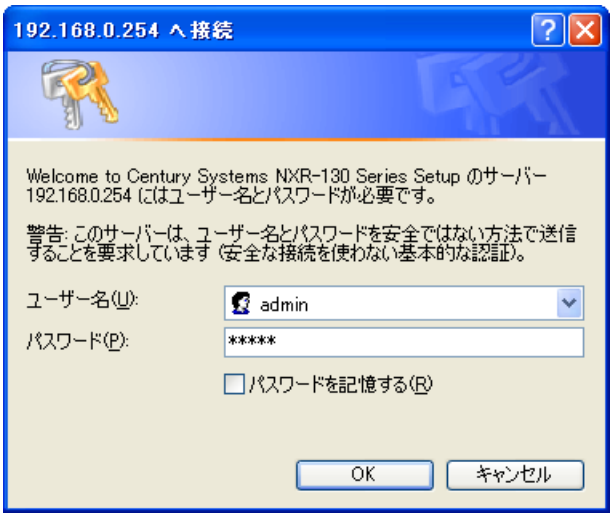
1 .Web ブラウザを起動します。

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。

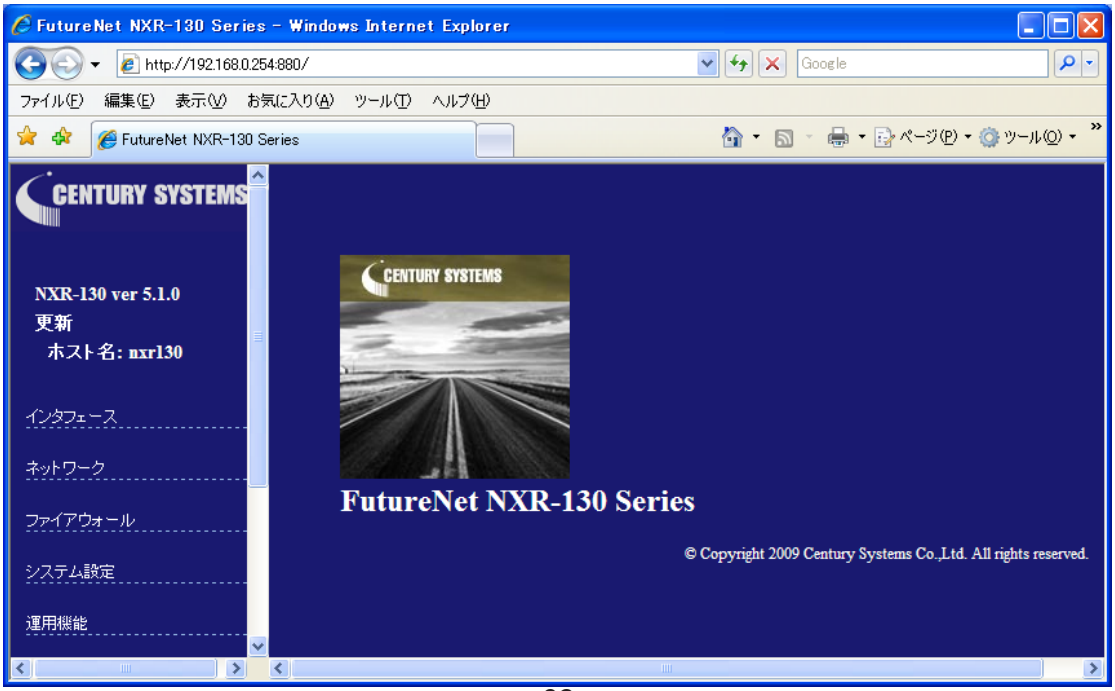
http://192.168.0.254:880/

※ 192.168.0.254 は、ETHER 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．GUI の接続方法

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
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)

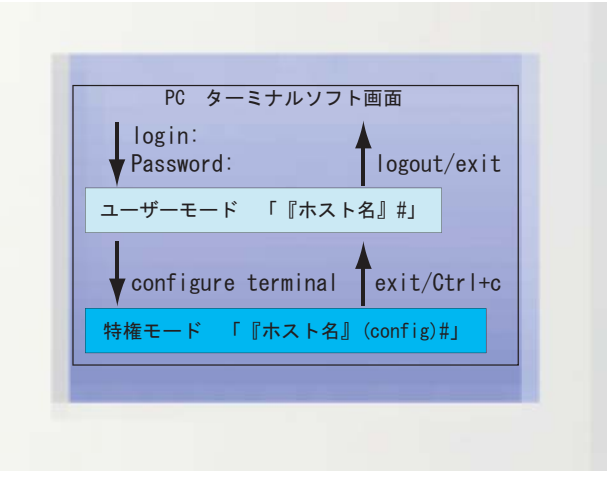
特権モードでは、ユーザモードで実行可能なコマンドに加え、内部システム情報、
コンフィグレーション情報を表示するコマンドや、本装置に対して設定をおこなうコマンドの実行が可能になります。
本モードでのプロンプトは、「『ホスト名』(config)#」で表示されます。
“ exit ” コマンドを入力するか、「Ctrl」+「c」を入力するとユーザーモードに戻ることができます。

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。

＜ユーザーモードへ移行時の表示例＞

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

＜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
```

<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 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

◆ 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)

view(exec) node

◆ 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

■ 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

view(exec) node

◆ show fast-forwarding
＜説　　明＞　ファストフォワーディングの情報を表示します。
＜書　　式＞　show fast-forwarding

◆ 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。

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

view(exec) node

◆ clock set
<説　　明>　時刻設定をします。
<書　　式>　clock set HH:MM:SS Day Month Year
<オプション>　HH　　: hour
　　MM　　: minutes
　　SS　　: seconds
　　Day (1-31)　　: Day of month
　　Month (1-12)　　: Month of year
　　Year (2007-2037)　: Year

◆ 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　　: Configurations on Flash ROM
<備　　考>　flash-configを消去した後、NXRを再起動します。

◆ delete
<説　　明>　ファイルを消去します。
<書　　式>　delete bootlog
　　delete dump　　: dumpファイルの削除
　　delete file (disk0:FILENAME|disk1:FILENAME)
　　delete syslog　　: syslogの削除(初期化)

◆ 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>　USB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)

view(exec) node

■ copy

○ (bootlog|dump|syslog)

＜説　　明＞　bootlog，dump，syslogを外部にコピーします。

＜書　　式＞

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

○ configのバックアップ

＜説　　明＞　設定ファイルのバックアップをおこないます。

＜書　　式＞

```
copy config ssh://<user@A.B.C.D>/FILENAME (|all) (|source A.B.C.D|X:X::X:X)
copy config ftp://<A.B.C.D>/FILENAME (|all) (|source A.B.C.D|X:X::X:X)
copy config (disk0:FILENAME|disk1:FILENAME) (|all)
```

＜備　　考＞　設定ファイルをバックアップ（外部にコピー）します。
all指定の場合は、ipsecを含む全てのconfigをtgz形式でコピーします。
指定なしの場合は、configのみをxml形式でコピーします。
ソースアドレスを指定することができます。

○ 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公開鍵のインポート

＜説　　明＞　SSH公開鍵をインポートします。

＜書　　式＞

```
copy (ssh://<user@A.B.C.D>/FILENAME) ssh-public-key user netconf (source A.B.C.D|X:X::X:X)
copy (ftp://<A.B.C.D>/FILENAME) ssh-public-key user netconf (source A.B.C.D|X:X::X:X)
copy (disk0:FILENAME|disk1:FILENAME) ssh-public-key user netconf (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。

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

・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　　: Dynamic Host Configuration Protocol (DHCP) Relay
　　restart dhcp-server　　: Dynamic Host Configuration Protocol (DHCP) Server
　　restart dns　　: Domain Name Service (DNS)
　　restart http-server　　: HTTP (Hyper Text Transfer Protocol) Server
　　restart ipsec　　: IP security service (IPsec)
　　restart l2tp　　: Layer Two Tunneling Protocol version2 (L2TPv2)
　　restart l2tpv3　　: Layer Two Tunneling Protocol version3 (L2TPv3)
　　restart ntp　　: Network Time Protocol (NTP)
　　restart ospf　　: Open Shortest Path First (OSPF)
　　restart rip　　: Routing Information Protocol (RIP)
　　restart snmp　　: Simple Network Management Protocol (SNMP)
　　restart ssh-serve　　: Secure SHell Server
　　restart syslog　　: Syslog
　　restart system　　: System restart
　　restart telnet-server　: Telnet Server
　　restart vrrp　　: Enable Virtual Router Redundancy Protocol (VRRP) for IP
　　restart warplink　　: WarpLinkクライアントを再起動します。
　　restart waplink send-config　: WarpLink ManagerにNXR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>
clear l2tpv3 counter ethernet <0-2> vid <1-4094>
clear l2tpv3 counter peer
clear l2tpv3 counter peer A.B.C.D
clear l2tpv3 counter session <session-id:1-4294967295>
clear l2tpv3 counter tunnel <tunnel-id:1-4294967295>

◆ clear l2tpv3 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>

view(exec) node

◆ 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 arp
<説　　明>　ARP エントリをクリアします。
<書　　式>　clear arp A.B.C.D　　: A.B.C.D IP address of the ARP cache entry

◆ 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>　PPP を切断します。
<書　　式>　clear ppp <0-4>

◆ clear l2tp
<説　　明>　L2TP を切断します。
<書　　式>　clear l2tp

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

◆ clear ipsec state
<説　　明>　IPsec state をクリアします。
<書　　式>　clear ipsec state <state_number:1-4294967295>

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

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

view(exec) 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 <0-1>
<説　　明>　USBモバイルをリセットします。
<書　　式>　clear mobile <0-1>

◆ 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

◆ terminal
<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。

view(exec) node

■ connect

○ connect ppp

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

○ reconnect ppp

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

○ connect l2tp

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

○ connect l2tpv3

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

○ connect ipsec

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

◆ disconnect

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

◆ 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)

view(exec) node

◆ 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)
　　ping (ipv6 X:X::X:X | FQDN) ethernet <0-2>

＜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
　　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>　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
```

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。

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)
icmp type/code指定(icmp指定時のみ)
source/destination mac address
type/length(Ethernet Header)

○ 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>/FILENAME (|source A.B.C.D|X:X::X:X)
　　ssh-server public-key username admin <0-4>
　　ftp://<A.B.C.D>/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>

○ 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>
<初 期 値>　session udp timer 30
<　 no　 >　no session udp timer(=session udp timer 30)

○ session udp-stream timer

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

○session tcp timer

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

○ session max

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

○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>
<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 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 (<16-8192>|)
<初 期 値>　session tcp limit 640
<　 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。

global node

■ session (続き)

○ 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、有効です。

＜書　　式＞　session invalid-status-drop enable

＜初 期 値＞　session invalid-status-drop enable

＜　no　＞　no session invalid-status-drop 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

◆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

＜備　考＞　「passwordなし」は設定不可

＜　no　＞　no password (= password admin)

◆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

＜備　考＞　「passwordなし」は設定不可

＜　no　＞　no gui password (= gui password admin)

global node

■ 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。

○ 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。
  - 転送用のプロトコルとしては、IPv4のみ対応し、IPv6は未対応です。
  - 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。
  - 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。HWに依存するため、1522バイトのフレームの送受信を保証するものではありません。
  - 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

○ mac-learning

＜説　　明＞　MACアドレス学習機能を有効にします。
＜書　　式＞　l2tpv3 mac-learning
＜初 期 値＞　l2tpv3 mac-learning
＜　no　＞　no l2tpv3 mac-learning
＜備　　考＞　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、すべて転送されます。

■ 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。

○ 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。

○ 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。

global node

■ L2TPv3（続き）

○ 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

global node

◆ **hostname**

＜説　　明＞　ホスト名を設定します。
＜書　　式＞　hostname HOSTNAME

◆ **fast-forwarding enable**

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

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

■ 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＞　ネットワークイベントを設定します。

○ interface link状態監視

＜書　　式＞

```
track <trackid:1-255> interface (ethernet <0-2> | ppp <0-4>| tunnel <0-255>)
```

＜備　　考＞

○ 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。
・ip/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。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。

○ IKE SA の状態監視

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

○ 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)

＜書　　式＞　track <trackid:1-255> ospf neighbor <PEER_RID:A.B.C.D>

○ 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)

＜書　　式＞　track <trackid:1-255> bgp neighbor <PEER_IP:A.B.C.D>

○ VRRP の状態監視(master から backup/init への変化または backup/init から master への変化)

＜書　　式＞　track <trackid:1-255> vrrp ip <vrrpid:1-255> interface ethernet <0-2>
＜備　　考＞　ethernet のみ有効
＜　no　＞　no track <trackid:1-255>

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
<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
<備　　考>　IPsecのmainモードで使用することができます。

◆ 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>/FILENAME (|source A.B.C.D|X:X::X:X)
　ipsec x509 ca-certificate NAME ftp://<A.B.C.D>/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。
・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 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>/FILENAME (|source A.B.C.D|X:X::X:X)
　ipsec x509 certificate NAME ftp://<A.B.C.D>/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。
・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>/FILENAME (|source A.B.C.D|X:X::X:X)
ipsec x509 private-key NAME key ftp://<A.B.C.D>/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。

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

◆ 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

◆ ipsec generate
<説　　明>　RSA signature keyを生成します.
<書　　式>　ipsec generate rsa-sig-key <key_length: 512-1024>
<　no　>　no ipsec generate rsa-sig-key

global node

◆ 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

◆ 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。

◆ 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。

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。)

◆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。)

◆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。)

global node

■ 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＞　USERが指定した周期で、データ通信端末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>|)
＜　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またはtunnel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>
＜　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またはtunnel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>
＜　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 / 再接続など指定された処理を実行する機能です。

○ PPP の接続 / 切断 / 再接続

＜説　　明＞

指定された時間に、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
```

○データ通信端末のリセット

＜説　　明＞

指定された時間に、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> MIN HOUR DOW (DOW|) mobile <0-2> 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
```

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。

◆ 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。

◆ 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リダイレクトを有効にします。
<書　　式>　ip redirects
<初 期 値>　ip redirects
<　no　>　no ip redirects

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

◆ 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

◆ ip mask-reply
<説　　明>　ICMP Address Mask Requestに応答します。
<書　　式>　ip mask-reply
<初 期 値>　no ip mask-reply
<　no　>　no ip mask-reply

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(routing protocolによる配信可)	Connected routeの無効化 (routing protocolによる配信停止。FIB上は存在)
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)	-

＜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。

◆ 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。

interface node

◆ 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＞　no ip arp reachable-time (=30000[msec])

＜　no　＞　no ip arp reachable-time

＜備　　考＞　show arp 実行時に、Status が REACHABLE と表示される時間です。実際の時間は、0.5 x reachable-time ～ 1.5 x 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>)

◆ 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)

interface node

◆ 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

◆ 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

interface node

◆ 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

◆ ip rip send version

<説　　明>　RIPの送信バージョンを設定します。
<書　　式>　ip rip send version (1|2) (|1|2)
<初 期 値>　ip rip send version 2
<備　　考>　version 1, version 2, version 1 & 2の指定が可能
<　no　>　no ip rip transmission version

◆ ip rip split-horizon

<説　　明>　スプリットホライズンを設定します。
<書　　式>　ip rip split-horizon (|poisoned)
<初 期 値>　ip rip split-horizon
<　no　>　no ip rip split-horizon

interface node

◆ ip ospf cost
<説　　明>　OSPFのコスト値を設定します。
<書　　式>　ip ospf cost <1-65535>
<　no　>　no ip ospf cost

◆ ip ospf hello-interval
<説　　明>　Helloインターバルを設定します。
<書　　式>　ip ospf hello-interval <1-65535>
<　no　>　no ip ospf hello-interval

◆ ip ospf dead-interval
<説　　明>　Deadインターバルを設定します。
<書　　式>　ip ospf dead-interval <1-65535>
<　no　>　no ip ospf dead-interval

◆ ip ospf retransmit-interval
<説　　明>　Retransmitインターバルを設定します。
<書　　式>　ip ospf retransmit-interval <1-65535>
<　no　>　no ip ospf retransmit-interval

◆ ip ospf transmit-delay
<説　　明>　Transmit Delayを設定します。
<書　　式>　ip ospf transmit-delay <1-65535>
<　no　>　no ip ospf transmit-delay

◆ ip ospf authentication
<説　　明>　認証を有効にします。
<書　　式>　ip ospf authentication (null|message-digest)
<　no　>　no ip ospf authentication

◆ ip ospf authentication-key
<説　　明>　認証パスワードを設定します。
<書　　式>　ip ospf authentication-key PASSWORD
<　no　>　no ip ospf authentication-key

◆ ip ospf message-digest-key
<説　　明>　MD5パスワードを設定します。
<書　　式>　ip ospf message-digest-key <keyid:1-255> md5 PASSWORD
<　no　>　no ip ospf message-digest-key <keyid:1-255>

◆ 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

interface node

◆ 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IPアドレスを設定します。
<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グループ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

◆ 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

◆ vrrp ip preempt delay
<説　　明>　マスタールータへの自動切り戻し抑止時間を設定します。
<書　　式>　vrrp ip <vrrpid:1-255> preempt delay <1-1000sec>
<　no　>　no vrrp ip <vrrpid:1-255> preempt delay

◆ vrrp ip timers
<説　　明>　VRRPのインターバルタイマーを設定します。
<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>　ネットワークイベントでのVRRP監視を設定します。
<書　　式>　vrrp ip <vrrpid:1-255> netevent <trackid:1-255> priority <1-254>
<　no　>　no vrrp ip <vrripd:1-255> netevent

◆ ip access-group
<説　　明>　アクセスグループにIPv4アクセスリストを追加します。
<書　　式>　ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
<初 期 値>　設定なし
<　no　>　no ip access-group (in|out|forward-in|forward-out)

interface node

◆ 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＞　ip マスカレードを有効にします。
＜書　　式＞　ip masquerade
＜　no　＞　no ip masquerade

◆ ip (snat-group|dnat-group)
＜説　　明＞　SNAT|DNAT を有効にします。
＜書　　式＞　ip (snat-group|dnat-group) NAT-NAME
＜　no　＞　no ip (snat-group|dnat-group)

◆ ip webauth-filter
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。Web 認証 filter 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。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 filter については、global node の ip web-auth access-list を参照してください。
　Web 認証については、Web Authenticate node を参照してください。

interface node

◆ 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>　SPI filterを設定します。
<書　　式>　ip spi-filter
<初 期 値>　no ip spi-filter
<　no　>　no ip spi-filter

◆ 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>　インタフェースを無効にします。
<書　　式>　shutdown
<初 期 値>　no shutdown
<　no　>　no shutdown

◆ ipsec policy
<説　　明>　IPsecのローカルポリシーを設定します。
<書　　式>　ipsec policy <1-255>
<　no　>　no ipsec policy (|<local policy:1-255>)
<備　　考>　2つまで設定可能(ipv4用1、ipv6用1の割り当てを想定)
　　ethernet、vlanのみ指定可能

◆ ipsec policy-ignore
<説　　明>　IPsec policyのcheckを行わないように指定する機能です。Interface毎に設定することができます。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
<　no　>　no ipsec policy-ignore
<備　　考>　Defaultは、無効です。また、input/outputに設定を行うことができます。
　　Input側で有効となった場合、inbound policy checkが行われなくなり、IPsec化されてくるべきpacketがdropされてしまう現象を回避することができます。
　　Outputで有効とした場合、そのinterfaceを出力とするpacketは、IPsec policyのcheckがされず、平文で送信されます。

interface node

■ QoS

＜説　　明＞　QoSの設定をします。

＜書　　式＞

○ HTBの設定

```
queue policy POLICYNAME bandwidth <1-1000000>
```

○ PQの設定

```
queue priority-group <PRIORITY-MAP-NUMBER:1-255>
```

○ SFQの設定

```
queue fair-queue
```

○ FIFOの設定

```
queue fifo (limit <1-16384>|)
```

○ TBFの設定

```
queue shape <RATE:1-1000000> <BUFFER:1-1000000> <LIMIT:1-1000000> (|ifg-pa-fcs)
```

○ default queueに設定（default queueはpfifo_fastです。）

```
no queue
```

○ classify

```
classify (input|output) route-map ROUTEMAP
input : PREROUTING, output : POSTROUTING
```

○ no classify

```
no classify (input|output|)
```

＜備　　考＞　ifg-pa-fcsについて

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、routerでshapingする際に、packet sizeやFCSやIFG、PAを除いたframe sizeでrate計算が行われます。この場合、shaping rateとしては問題ないようでも、ethernet frame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frame 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 interface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12byteで計算)、fcs(4byte)、pa(preamble:8byte)をframe size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frame dropを回避することが可能となります。Defaultでは、IFG、PA、FCS分のsizeは考慮されません。

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。
<書　　式>　ipv6 address DHCPv6PD X:X::X:X/M (|eui-64)　: DHCPv6-PD prefix name
<　no　>　no ipv6 address DHCPv6PD X:X::X:X/M
<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
```

◆ 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)
<　no　>　no tunnel mode
<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>　IDキーを設定します。
<書　　式>　tunnel key <0-4294967295>
<初 期 値>　no tunnel key
<備　　考>　GREの場合のみ
<　no　>　no tunnel key　　: Disable

◆ tunnel checksum
<説　　明>　チェックサム機能を有効にします。
<書　　式>　tunnel checksum
<初 期 値>　no tunnel checksum
<備　　考>　GREの場合のみ
<　no　>　no tunnel checksum　　: Disable

◆ tunnel path-mtu-discovery
<説　　明>　トンネルにPMTUDを有効にします。
<書　　式>　tunnel path-mtu-discovery
<初 期 値>　tunnel path-mtu-discovery
<　no　>　no tunnel path-mtu-discovery　　: Disable

◆ 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　　: Set defaults

◆ tunnel tos
<説　　明>　TOS値を設定します。
<書　　式>　tunnel tos (<0-252>|inherit)
<初 期 値>　tunnel tos inherit
<　no　>　no tunnel tos　　: Set defaults

◆ 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。

interface tunnel node

◆ 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>　MTUの値を設定します。
<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)

◆ ip redirects
<説　　明>　ICMP Redirect を有効にします。
<書　　式>　ip redirects
<　no　>　no ip redirects

◆ ip tcp adjust-mss
<説　　明>　MSSを有効にします。
<書　　式>　ip tcp adjust-mss (auto|<bytes:500-1460>)
<初 期 値>　no ip tcp adjust-mss
<　no　>　no ip tcp adjust-mss

◆ 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

◆ ip mask-reply
<説　　明>　ICMP Mask Replyを有効にします。
<書　　式>　ip mask-reply
<　no　>　no ip mask-reply

◆ ip fragment-reassembly
<説　　明>　Pre-fragmentされたpacketを受信した場合に、NXRでreassembleせずにforwardingする機能です。defaultは無効です（reassembleします）。
<書　　式>　ip fragment-reassembly
<初 期 値>　ip fragment-reassembly
<　no　>　no ip fragment-reassembly
<備　　考>　Route based IPsec(参照：付録C)を使用する際に、IPsec tunnel interfaceに設定することができます。

interface tunnel node

◆ 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

◆ 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>　アドレスグループにIPv4アクセスリストを追加します。
<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)

◆ 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>　ip masqueradeを有効にします。
<書　　式>　ip masquerade
<初 期 値>　no ip masquerade

◆ ip snat-group|dnat-group
<説　　明>　source/destination NATを設定します。
<書　　式>　ip (snat-group|dnat-group) NAT-NAME
<　no　>　no ip (snat-group|dnat-group)

interface tunnel node

◆ ip webauth-filter

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。Web認証filter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。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filterについては、global nodeのip web-auth access-listを参照してください。
　Web認証については、Web Authenticate nodeを参照してください。

◆ ip spi-filter

<説　　明>　SPI filterを設定します。
<書　　式>　ip spi-filter
<初 期 値>　no ip spi-filter
<　no　>　no ip spi-filter

◆ 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

◆ netevent

<説　　明>　neteventを設定します。
<書　　式>　netevent <trackid:1-255> (connect|disconnect)
<　no　>　no netevent
<備　　考>　connect|disconnect はtrack event がdown したときの動作定義です。

◆ ipv6 nd accept-redirects

<説　　明>　IPv6 forwardingが無効の場合に、ICMPv6 redirectsを受け入れるかどうかを指定します。
<書　　式>　ipv6 nd accept-redirects
<初 期 値>　no ipv6 nd accept-redirects
<備　　考>　IPv6 forwardingが有効な場合は、この設定に関係なく受信しません。
<　no　>　no ipv6 nd accept-redirects

interface tunnel node

◆ ipsec policy
＜説　　明＞　IPsecローカルポリシーを設定します。
＜書　　式＞　ipsec policy <local policy:1-255>
＜備　　考＞　2つまで設定可能(ipv4用1、ipv6用1の割り当てを想定)
＜　no　＞　no ipsec policy (|<local policy:1-255>)

◆ ipsec policy-ignore
＜説　　明＞　IPsec policyのcheckを行わないように指定する機能です。Interface毎に設定することができます。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
＜　no　＞　no ipsec policy-ignore
＜備　　考＞　Defaultは、無効です。また、input/outputに設定を行うことができます。
Input側で有効となった場合、inbound policy checkが行われなくなり、IPsec化されてくるべきpacketがdropされてしまう現象を回避することができます。
Outputで有効とした場合、そのinterfaceを出力とするpacketは、IPsec policyのcheckがされず、平文で送信されます。

■ QoS
＜説　　明＞　QoSの設定をします。
＜書　　式＞
○HTBの設定
　queue policy POLICYNAME bandwidth <1-1000000>
○PQの設定
　queue priority-group <PRIORITY-MAP-NUMBER:1-255>
○SFQの設定
　queue fair-queue
○FIFOの設定
　queue fifo (limit <1-16384>|)
○TBFの設定
　queue shape <RATE:1-1000000> <BUFFER:1-1000000> <LIMIT:1-1000000>
○default queueに設定
default queueはpfifo_fastです。
　no queue
○classify
　classify (input|output) route-map ROUTEMAP
　input: PREROUTING, output: POSTROUTING
○no classify
　no classify (input|output|)

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 messagesを有効にします。
<書　　式>　ip redirects
<初 期 値>　no ip redirects　(無効)
<　no　>　no ip redirects

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

◆ 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

◆ ip mask-reply
<説　　明>　ICMP Mask Replyを有効にします。
<書　　式>　ip mask-reply
<初 期 値>　no ip mask-reply　(無効)
<　no　>　no ip mask-reply

interface ppp node

◆ 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

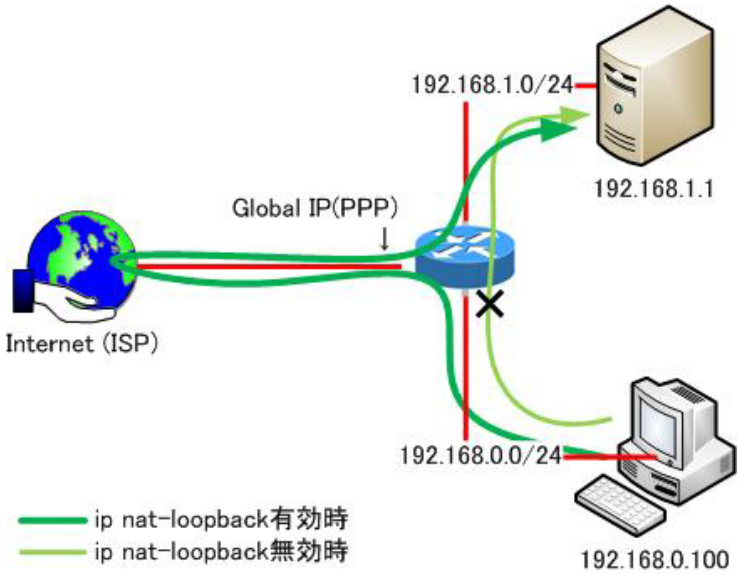
＜　no　＞　no ip nat-loopback

＜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

◆ 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

◆ ip access-group
<説　　明>　アクセスグループにIPv4アクセスリストを追加します。
<書　　式>　ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
<オプション>　　in　　: Apply the access-list to in-forwarding packets
　　out　　: Apply the access-list to out-forwarding packets
　　forward-in : Apply the access-list to incoming packets
　　forward-out: Apply the access-list to outgoing packets
<初 期 値>　no ip access-group (in|out|forward-in|forward-out)
<　no　>　no ip access-group (in|out|forward-in|forward-out)

interface ppp node

◆ 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>　IP masqueradeを有効にします。
<書　　式>　ip masquerade
<初 期 値>　no ip masquerade
<　no　>　no ip masquerade

◆ ip (snat-group|dnat-group)
<説　　明>　source/destination NATルールを設定します。
<書　　式>　ip (snat-group|dnat-group) NAT-NAME
<　no　>　no ip (snat-group|dnat-group)

◆ ip webauth-filter
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。Web認証filter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。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filterについては、global nodeのip web-auth access-listを参照してください。
　Web認証については、Web Authenticate nodeを参照してください。

◆ ip spi-filter
<説　　明>　SPI filterを設定します。
<書　　式>　ip spi-filter
<初 期 値>　no ip spi-filter
<　no　>　no ip spi-filter

◆ 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

◆ 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

interface ppp node

◆ netevent
<説　　明>　netevent を設定します。
<書　　式>　netevent <trackid:1-255> (connect|disconnect)
<　no　>　no netevent
<備　　考>　connect|disconnect は track event が down したときの動作定義です。

◆ 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>　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>　2 つまで設定可能(ipv4 用 1 つ、ipv6 用 1 つを想定)

◆ ipsec policy-ignore
<説　　明>
・IPsec policy の check を行わないように指定する機能です。Interface 毎に設定することができます。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
<　no　>　no ipsec policy-ignore
<備　　考>
・Default は、無効です。また、input/output に設定を行うことができます。
・Input 側で有効となった場合、inbound policy check が行われなくなり、IPsec 化されてくるべき packet が drop されてしまう現象を回避することができます。
・Output で有効とした場合、その interface を出力とする packet は、IPsec policy の check がされず、平文で送信されます。

interface ppp node

◆ 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。

■ QoS

＜説　　明＞　QoSの設定をします。

＜書　　式＞

○HTBの設定

```
queue policy POLICYNAME bandwidth <1-1000000>
```

○PQの設定

```
queue priority-group <PRIORITY-MAP-NUMBER:1-255>
```

○SFQの設定

```
queue fair-queue
```

○FIFOの設定

```
queue fifo (limit <1-16384>|)
```

○TBFの設定

```
queue shape <RATE:1-1000000> <BUFFER:1-1000000> <LIMIT:1-1000000>
```

○default queueに設定

default queueはpfifo_fastです。

```
no queue
```

○classify

```
classify (input|output) route-map ROUTEMAP
input: PREROUTING, output: POSTROUTING
```

○no classify

```
no classify (input|output|)
```

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

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)

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

◆ 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

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

◆ 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

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 tcp adjust-mss
<説　　明>　MSS値を調整します。
<書　　式>　ip tcp adjust-mss (auto|<bytes:500-1460>)
<初 期 値>　no ip tcp adjust-mss
<　no　>　no ip tcp adjust-mss　　: Set defaults

◆ 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 モードを有効にします。
＜書　　式＞　preempt enable
＜　no　＞　no preempt enable

◆enforce-secondary-down enable

＜説　　明＞　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 機能を有効にします。
＜書　　式＞　active-hold enable
＜初 期 値＞　no active-hold enable
＜　no　＞　no active-hold enable

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>}

◆ area 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

◆ 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

ospf 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

<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＞　Backdoor 機能を使用すると、受け取った BGP 経路の優先順位を下げて他のルートを優先させることができます。

◆ aggregate-address

＜説　　明＞　アグリゲートアドレスを設定します。
＜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＞　BGP route の集約を行うことができる場合に、集約 route を作成します。
集約 route のみを advertise する場合は、summary-only 設定を有効にします。

◆ distance

＜説　　明＞　eBGP ルートの administrative distance 値を設定します。
＜書　　式＞　distance bgp <1-255>
＜　no　＞　no distance bgp
＜備　　考＞　初期値は 20 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>　異なる AS を生成元とするルートの MED 値の比較を行います。
<書　　式>　bgp always-compare-med
<　no　>　no bgp always-compare-med

○ bestpath as-path
<説　　明>　BGP の最適パス決定プロセスにおいて、AS PATH が最短であるルートを優先するというプロセスを省略します。
<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>　Local Preference 値のデフォルト値を変更します。
<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。

○ 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

bgp node

■ bgp （続き）

○ 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 される。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、XROS が保持している IPv4 address の中でもっとも大きい IPv4 address が Router-ID として使用されます。

○ 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
＜　no　＞　no neighbor A.B.C.D filter-list ACL-NAME
＜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

■ 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

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

◆ 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>　3 つまで Network 設定可能。
<　 No　 >　no security (A.B.C.D/M|X:X::X:X/M)　　: Delete
```

◆ syslocation

```
<説　　明>　sysLocation を設定します。
<書　　式>　syslocation LOCATION
<初 期 値>　no syslocation
<　 No　 >　no syslocation　　: Negate
```

◆ syscontact

```
<説　　明>　sysContact を設定します。
<書　　式>　syscontact CONTACT
<初 期 値>　no syscontact
<　 No　 >　no syscontact　　: Negate
```

◆ sysname

```
<説　　明>　sysName を設定します。
<書　　式>　sysname SYSNAME
<初 期 値>　no sysname
<　 No　 >　no sysname　　: Negate
```

◆ sysdescr

```
<説　　明>　sysDescr を設定します。
<書　　式>　sysdescr DESCRIBE
<初 期 値>　no sysdescr
<　 No　 >　no sysdescr　　: Negate
```

◆ 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)
<初 期 値>　no trap manager
<備　　考>　3 つまで設定可能
　　Community 未指定時は "community"
<　 No　 >　no trap manager (|A.B.C.D|X:X::X:X)
```

第19章 snmp node

snmp node

◆ 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
＜備　　考＞　TRAP パケット中の "Agent Address" を指定できる
＜　No　＞　no trap agent　　: Delete

◆ 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
＜備　　考＞　SNMP の listen アドレスを指定。TRAP 送信時の source ip もこの bind address となる。
　　未設定の場合は 0.0.0.0 で listen する。
＜　No　＞　no bind address　　: 自動選択(0.0.0.0 で lilsten)

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　　　　: ローカル出力しない
```

◆ 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。
<書　　式>　mark <0-99min>
<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します。
<書　　式>　priority (debug|info|notice)
<初 期 値>　priority info
<　No　 >　no priority
```

◆ system
```
<説　　明>　syslogシステムメッセージの設定をします。
<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
```

syslog node

◆ 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。
<書　　式>　mail send enable
<初 期 値>　no mail send
<　No　>　no mail send

◆ mail to
<説　　明>　送信先メールアドレスを設定します。
<書　　式>　mail to RECEIVER
<初 期 値>　no mail to
<　No　>　no mail to

◆ mail from
<説　　明>　送信元メールアドレスを設定します。
<書　　式>　mail from SENDER
<初 期 値>　no mail from
<　No　>　no mail from

◆ mail subject
<説　　明>　メールの件名を設定します。
<書　　式>　mail subject SUBJECT
<初 期 値>　no mail subject
<　No　>　no mail subject

◆ mail strings
<説　　明>　ここで指定した文字列が含まれるログをメールで送信します。
<書　　式>　mail strings <1-32> STRINGS
<初 期 値>　no mail strings
<備　　考>　メール検索文字列は 32 行まで設定可
<　No　>　no mail strings <1-32>

syslog node

◆ 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

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 <1-5>
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

◆ 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＞　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＞　4つまで設定することができます。

◆ accept

＜説　　明＞　DHCP クライアントからの DHCP パケットを受信するインターフェースを 設定します。
＜書　　式＞　accept ethernet <0-2>
＜　No　＞　no accept ethernet <0-2>

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＞　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＞
・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

◆ keepalive
<説　　明>　キープアライブの設定をします。
<書　　式>　keepalive periodic
　　keepalive periodic (clear|hold|restart)
　　keepalive <interval:10-3600> <retry:0-60> periodic
　　keepalive <interval:10-3600> <retry:0-60> periodic (clear|hold|restart)
<オプション>
　clear　　: keepalive失敗時、SAを削除する。
　hold　　: keepalive失敗時、SAを削除する。IPsec policyはon-demandモードに移行。
　restart　: keepalive失敗時、SAを削除する。IKEネゴシエーションを開始する。
<　No　>　no keepalive　　: Unset keepalive

◆ 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

◆ 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

◆ 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)

ipsec isakmp policy node

◆ 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)

◆ 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)

ipsec isakmp policy node

◆ 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>

◆ 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 <local_policy:1-255> netevent <trackid:1-255> 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。

ipsec isakmp policy node

◆ 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)
＜　No　＞　no netevent

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>

＜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

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

◆ 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> (ceil <1-1000000>|) queue priority-group <1-32>
```

○class+fifo

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

○class+sfq

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

○class+tbf

```
      class <2-254> bandwidth <1-1000000> (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> (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> (ceil <1-1000000>|)
            queue (priority-group|shape|fifo|fair-queue)
```

○default queue (default queue: sfq)

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

＜備　　考＞　bandwidth/ceil,RATE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

◆ 移行 command

```
nxr130#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr130(config)#crp client <1-2>
```

■ server configuration

○ server address

```
<説　　明>　CRPサーバの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 : CRPサーバのアドレスを削除します。
```

○ server port

```
<説　　明>　CRPサーバのポート番号を設定します。
<書　　式>　server port <udp:1024-65535>
<　No　>　no server port : ポート番号の設定を削除します。
```

○ 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 : ユーザIDを削除します。
```

○ keepalive

```
<説　　明>　キープアライブの設定をします。
<書　　式>　keepalive (<300-28800sec>|)
<備　　考>　インターバル未指定時は「keepalive 3600」と同義です。
<　No　>　no keepalive : キープアライブを無効にします。
```

第 30 章

route-map node

第 30 章 route-map node

route-map node

◆ 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)#
```

■ match

＜説　　明＞　マッチ条件を設定します。

＜書　　式＞　match as-path ACL-NAME
match ip address ACL
match ip tos <0-255>
match ip next-hop ACL-NAME
match ip mark <1-4095>
match metric <0-4294967295>
match origin (egp|igp|incomplete)

＜　No　＞　no match ip (address|tos|mark) :　設定したマッチ条件を削除します。

＜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。

■ set

＜説　　明＞　Mark 値、ToS 値を設定します。

＜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 mark <1-4095>
set metric <0-4294967295>
set origin (egp|igp|incomplete)
set tos <0-255>

route-map node

■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

Web Authenticate 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 Authenticate 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 Authenticate 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)
　　radius A.B.C.D auth-port (1645|1812|<1024-65535>)
<　No　>　no radius A.B.C.D
<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 Authenticate 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）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

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#
```

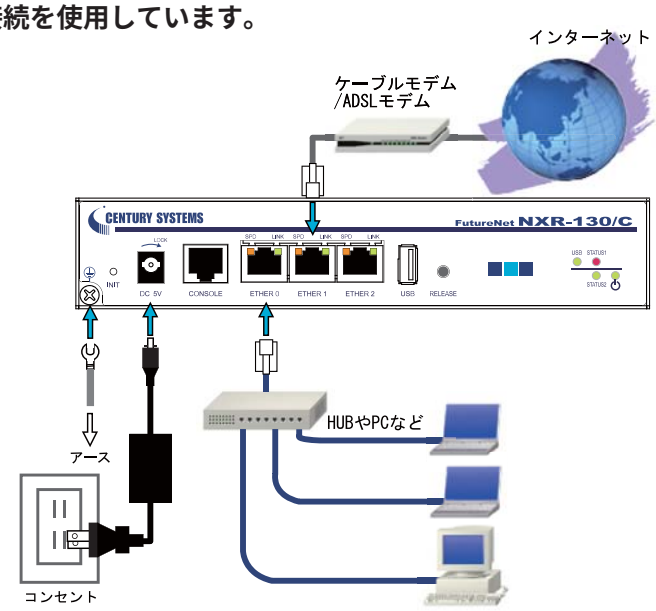
6. “ show config ”コマンドで、設定を確認します。

```
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
```

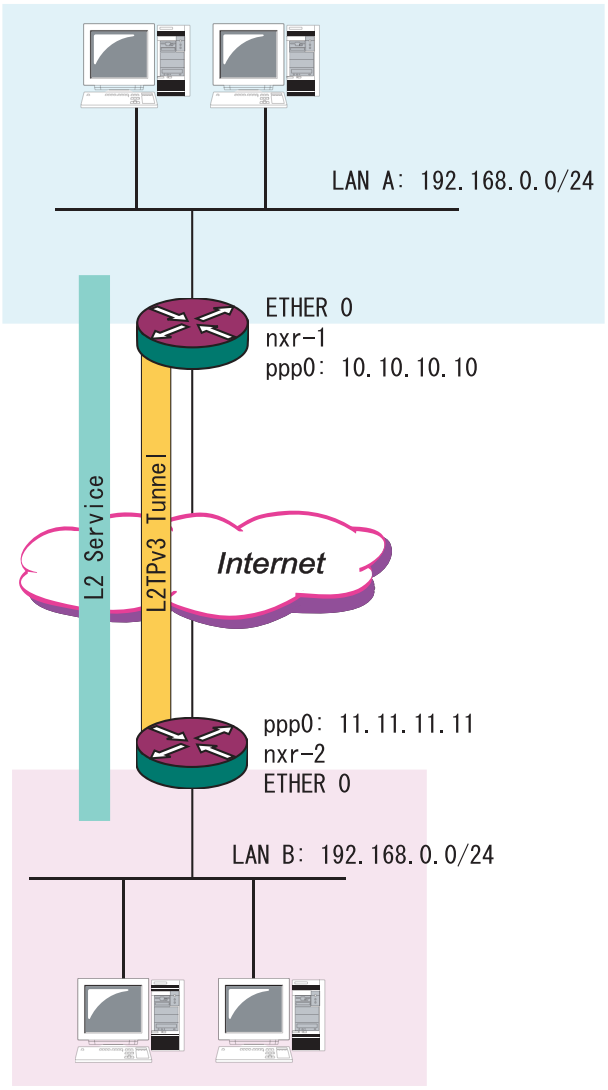
付録 A

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。

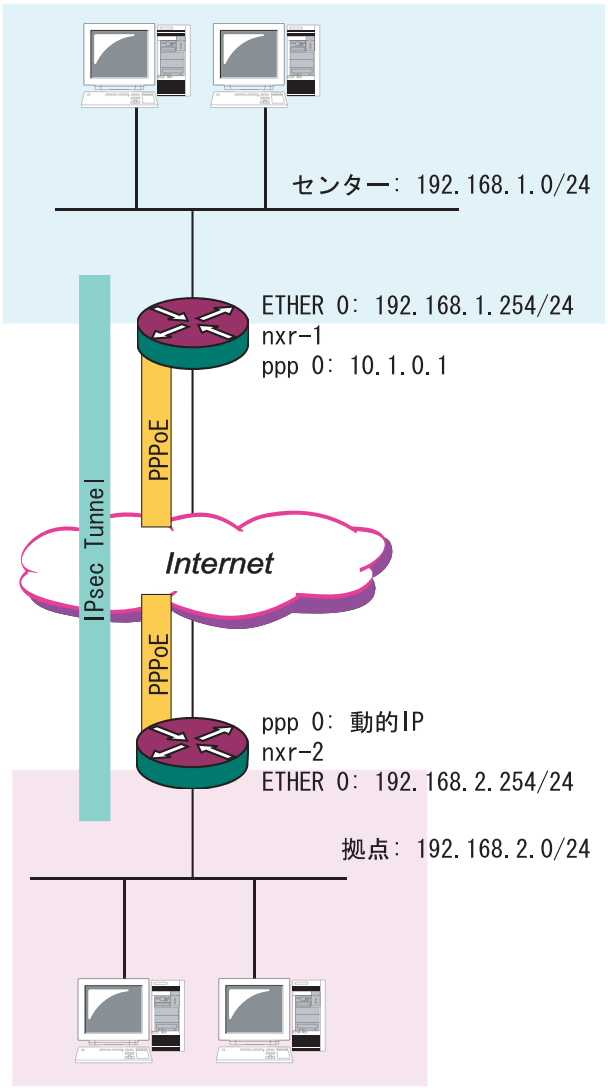



```
< nxr1 の設定 >
!
l2tpv3 hostname nxr1   ←本装置のホスト名
l2tpv3 router-id 192.168.200.254
                       ←本装置の ID
!
l2tpv3 tunnel 1
 description nxr1-nxr2
 tunnel address 11.11.11.11
          ←対向 LCCE の WAN 側 IP アドレス
 tunnel hostname nxr2  ←対向 LCCE のホスト名
 tunnel router-id 192.168.200.253
                       ←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
```

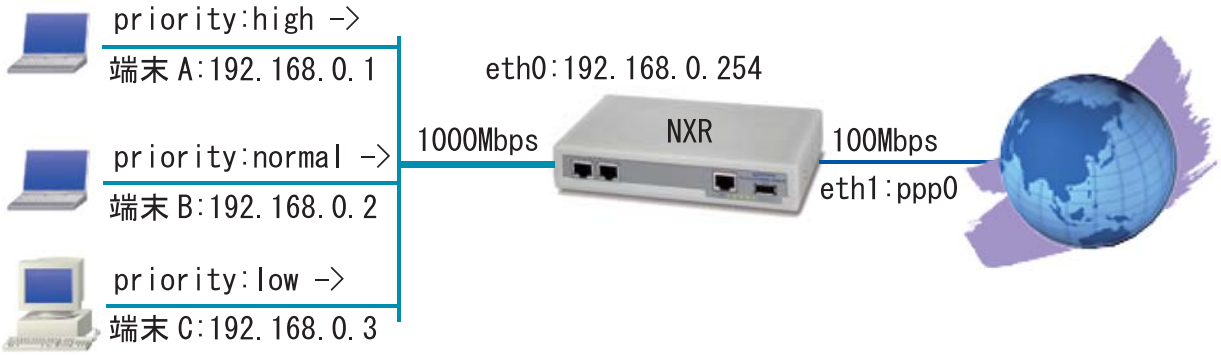
2．続いて、取得した CID と PDP Type を元に、モバイル接続の設定を行います。

```
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) SYSTEM filter
    TCP connection数制限
(2) IPsec input policy check
    IPsec ESP化されてきたものは許可します。
(3) USER input filtering
(4) SPI check
(5) Service用filter(GUIアクセス用filterなど)

○ FORWARD

(1) SYSTEM filter
    Session limit
(2) 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。
(3) UPNP filtering
(4) USER forward in/out filtering
(5) SPI(input/forward時のみ)

○ 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)

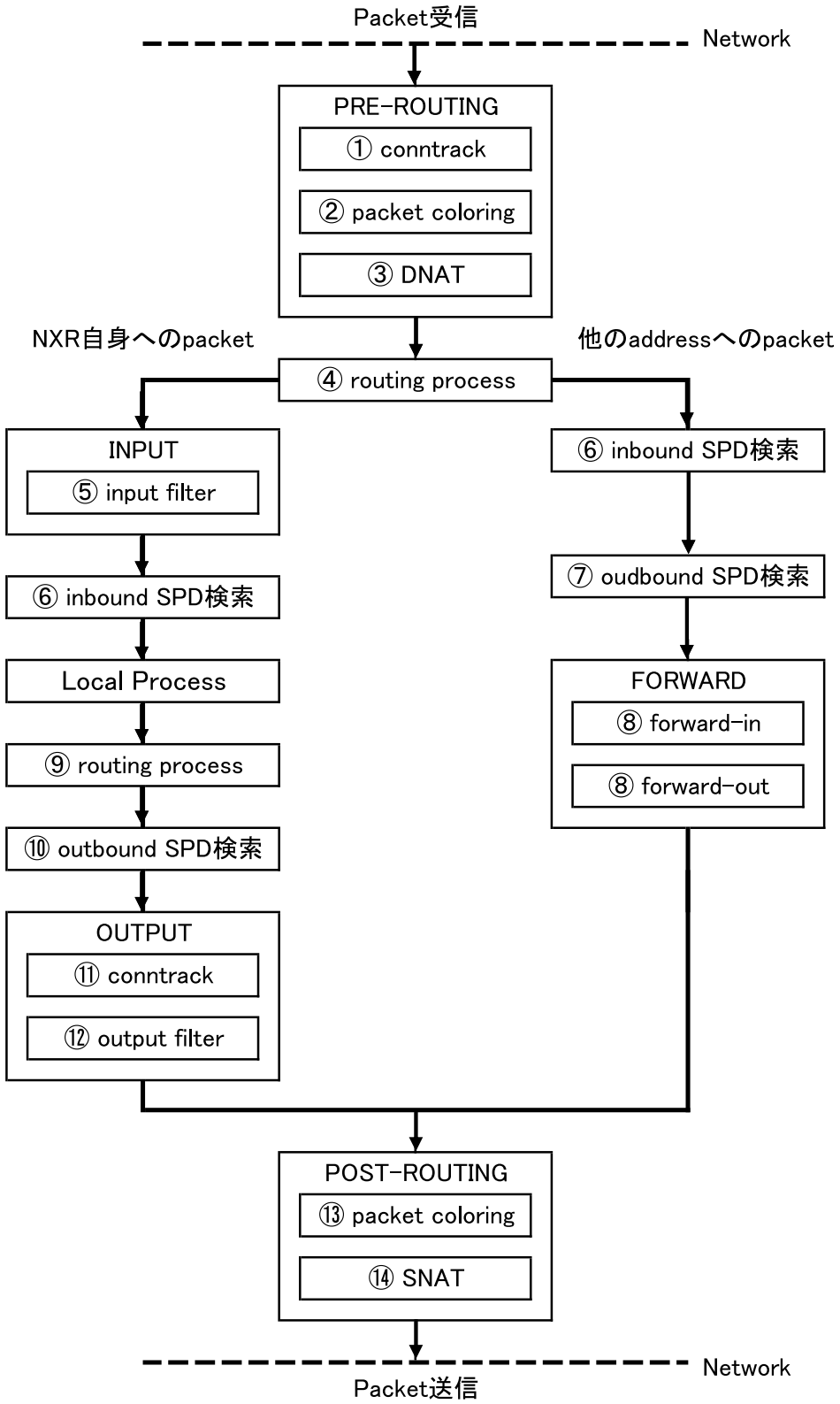
○ OUTPUT

(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

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 check を行わないように指定する機能です。Interface 毎に設定することができます。Default は無効で、input/output に設定を行うことができます。この機能は、IPsec policy として any などを指定した際に、特定の通信のみ IPsec 化したくない場合に使用します。
Input 側で有効となった場合、inbound policy check が行われなくなり、IPsec 化されてくるべき packet が drop されてしまう現象を回避することができます。
Output で有効とした場合、その interface を出力とする packet は、IPsec policy の check がされず、平文で送信されます。

```
<書　　式>　ipsec policy-ignore (input|output|)
<初 期 値>　no ipsec policy-ignore　　(無効)
<　No　 >　no ipsec policy-ignore
```

付録 C　Policy based IPsec と Route based IPsec

II．Route based IPsec

2. Route based IPsec

Route based IPsec の場合、IPsec mode に設定された tunnel interface に対する route 設定に依って ESP化するかどうかが決定されます。
出力先 interface が IPsec mode の tunnel interface となっている場合、ESP 化されて出力されます。
そのため、迂回 route の確保や main/backup tunnel の常時確立、IPv6 を IPsec 化する際に any を利用できるなどの利点があります。

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
0 以外の固定の値を設定する場合は、PMTUD は無効にする必要があります。0 を設定した場合、SYSTEM の default の TTL(64)が設定されます。
<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 せずに forwarding する機能です。IPsec tunnel interface 上でのみ利用することができ、default の設定は無効です。
この機能を有効とした場合、reassemble されないため、該当 packet への NAT/filter 処理が適用されなくなります(制限事項)。したがって、この機能を有効にする場合は、end-point の端末が LAN 側に存在するような構成に限定するようにしてください。

＜書　　式＞　ip fragment-reassembly
＜初 期 値＞　ip fragment-reassembly　　（reassemble する）
＜　No　＞　no ip fragment-reassembly　（reassemble しない）

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。

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。

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

○ 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)

1.1 Firmware update 中の service の継続

NXR-125 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 USER が選択することができます。
NXR-125 以外の NXR シリーズでは、すべてのサービスおよび packet 処理が停止されます。

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。
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

サポートについて

付録 F

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-120/C　ユーザーズガイド CLI編 v5.9.0対応版
FutureNet NXR-125/CX ユーザーズガイド CLI編 v5.8.1対応版
FutureNet NXR-130/C　ユーザーズガイド CLI編 v5.5.5対応版

2010年10月版
発行 センチュリー・システムズ株式会社