

FutureNet NXR-120/C
NXR-125/CX
NXR-130/C
NXR-1200

ユーザーズガイド CLI 編	NXR-120/C	v5.9.0 対応版
	NXR-125/CX	v5.10.0 対応版
	NXR-130/C	v5.5.5 対応版
	NXR-1200	v5.8.2 対応版

目次

はじめに	5
パッケージの内容物の確認	6
第1章 本装置の概要	7
. 本装置の特長	8
. 各部の名称と機能 (NXR-120/C)	9
. 各部の名称と機能 (NXR-125/CX)	11
. 各部の名称と機能 (NXR-130/C)	13
. 各部の名称と機能 (NXR-1200)	15
. 動作環境	17
第2章 装置の設置	18
. 装置の設置に関する注意点	19
. 装置の設置 (NXR-120/C)	20
. 装置の設置 (NXR-125/CX)	21
. 装置の設置 (NXR-130/C)	22
. 装置の設置 (NXR-1200)	23
第3章 設定方法の概要	24
. 本装置へのログイン (CLI)	25
. 本装置へのログイン (Console 接続: NXR-120/C)	26
. 本装置へのログイン (Console 接続: NXR-125/CX)	27
. 本装置へのログイン (Console 接続: NXR-130/C)	28
. 本装置へのログイン (Console 接続: NXR-1200)	29
. 本装置へのログイン (Console 接続: NXR シリーズ共通)	30
. 本装置へのログイン (Telnet 接続)	31
. 本装置へのログイン (GUI)	32
. コマンド実行モード	34
. コマンド入力時の補助機能	35
第4章 本装置のノード構造	36
. ノード構造について	37
第5章 view(exec) node	38
. view(exec) node	39
第6章 global node	59
. global node	60
第7章 interface node	99
. interface node	100
第8章 interface tunnel node	112
. interface tunnel node	113
第9章 interface ppp node	119
. interface ppp node	120
第10章 dns node	131
. dns node	132
第11章 l2tp node	134
. l2tp node	135
第12章 l2tpv3-tunnel node	136
. l2tpv3 tunnel parameters	137
第13章 l2tpv3-xconnect node	139
. l2tpv3 xconnect parameters	140

第14章	l2tpv3-group node	142
	l2tpv3-group node	143
第15章	rip node	144
	rip node	145
第16章	ospf node	147
	ospf node	148
第17章	bgp node	151
	bgp node	152
第18章	ntp node	158
	ntp node	159
第19章	SNMP node	160
	SNMP node	161
第20章	syslog node	165
	syslog node	166
第21章	dhcp-server node	170
	dhcp-server node	171
第22章	dhcp-relay node	173
	dhcp-relay node	174
第23章	ipsec local policy node	175
	ipsec local policy node	176
第24章	ipsec isakmp policy node	177
	ipsec isakmp policy node	178
第25章	ipsec tunnel policy node	187
	ipsec tunnel policy node	188
第26章	UPnP node	191
	UPnP node	192
第27章	QoS (class-policy) node	193
	QoS (class-policy) node	194
第28章	QoS (class-filter) node	195
	QoS (class-filter) node	196
第29章	CRP client node	197
	CRP client node	198
第30章	route-map node	199
	route-map node	200
第31章	Web Authenticate node	203
	Web Authentication node	204
第32章	WarpLink node	208
	WarpLink node	209
第33章	Extended track IP reachability node	211
	Netevent 拡張機能(ip reachability)	212
第34章	Extended track IPv6 reachability node	215
	Netevent 拡張機能(ipv6 reachability)	216
第35章	Monitor-log node	219
	ログ機能	220

付録 A 設定事例	223
. インタフェースの設定例	224
. PPPoE の設定例	225
. L2TPv3 の設定例	228
. IPsec の設定例	229
. モバイル接続の設定例	232
. QoS の設定例	233
付録 B Packet Traveling	234
Packet Traveling	235
付録 C Policy based IPsec と Route based IPsec	239
. Policy based IPsec	240
. Route based IPsec	242
付録 D IKEv2 Protocol	248
IKEv2 Protocol	249
付録 E Firmware update	255
Firmware update	256
付録 F Netevent 機能	258
Netevent 機能	259
付録 G サポートについて	263
サポートについて	264

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粹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

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>

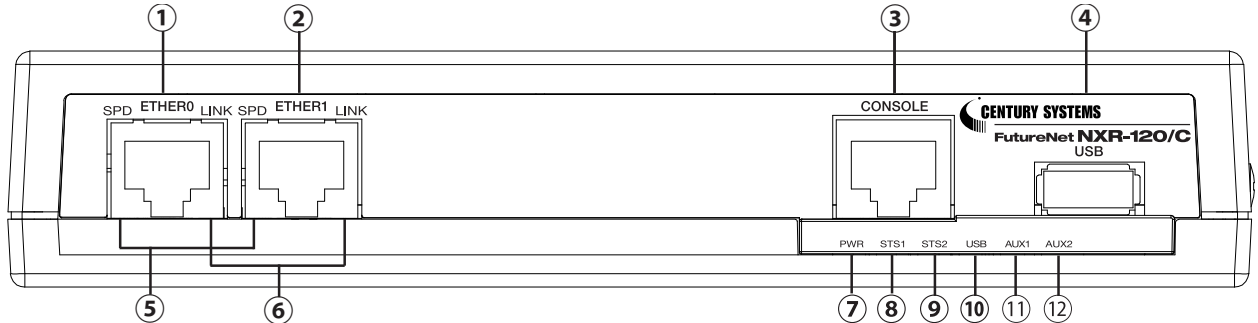
FutureNet NXR-130/C

<http://www.centurysys.co.jp/router/nxr130c.html>

第1章 本装置の概要

. 各部の名称と機能 (NXR-120/C)

製品前面 (NXR-120/C)



ETHER 0 ポート

主に LAN 側ポートとして使用します。

ETHER 1 ポート

主に WAN 側ポートとして使用します。

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。

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。

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	: ■

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	: ■

PWR LED(青)

本装置の電源状態を示します。

電源投入時	: ■
-------	-----

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	: ■

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	: ■

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	: ■

AUX1 LED(緑)

AUX2 LED(緑)

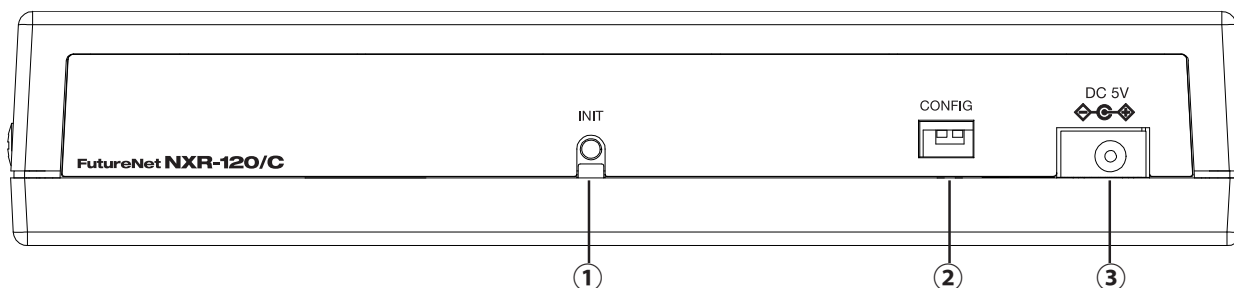
データ通信端末装着時に、電波状況を表示します。
電波状況の取得周期の設定等については、第6章 global node の system led を参照してください。

	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	: ■	: ■

第1章 本装置の概要

各部の名称と機能 (NXR-120/C)

製品背面 (NXR-120/C)



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ボタンを押しただ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。

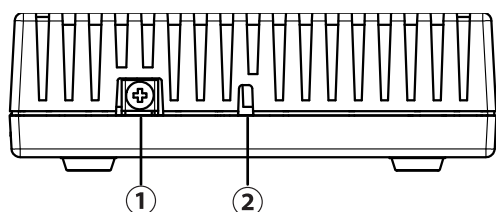
CONFIG

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。

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)



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。

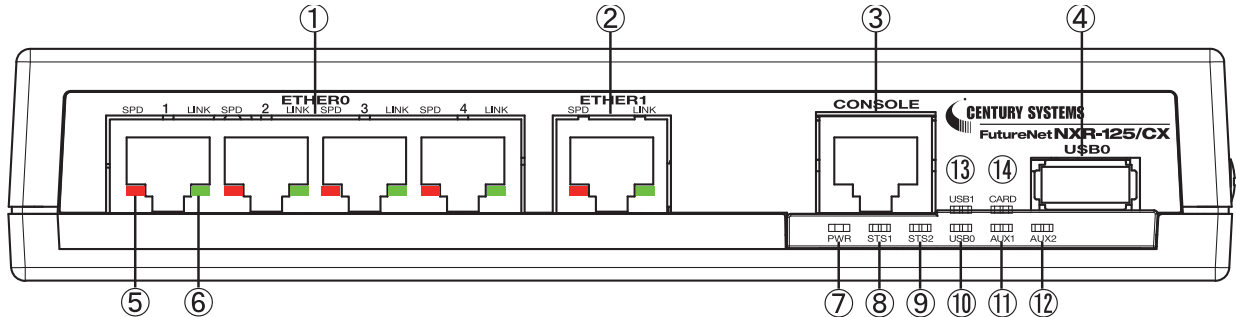
セキュリティスロット

ケンジントンロックに対応しています。

第1章 本装置の概要

. 各部の名称と機能 (NXR-125/CX)

製品前面 (NXR-125/CX)



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。

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。

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。

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。

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:

LINK LED(緑)

ETHER ポートのリンク状態を示します。
Link Down 時 :
Link UP 時 :

PWR LED(青)

本装置の電源状態を示します。
電源 ON 時 :

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 :

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):
:

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 :

AUX1 LED(緑)/ AUX2 LED(緑)

データ通信端末未装着時に、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 :

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 :

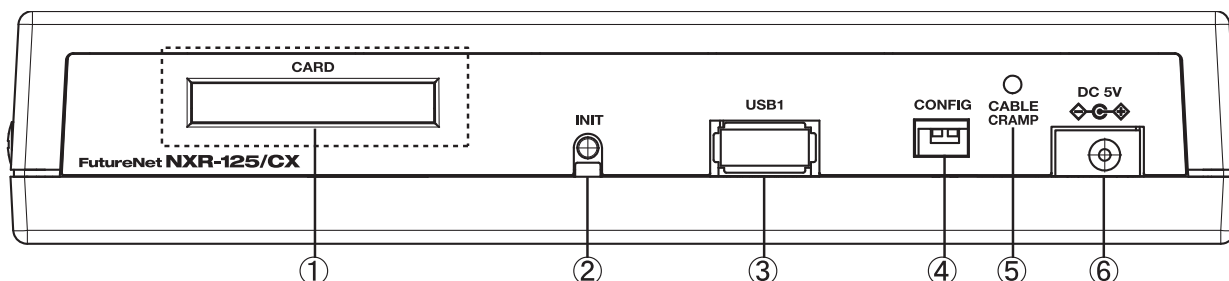
CARD LED

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 :

第1章 本装置の概要

各部の名称と機能 (NXR-125/CX)

製品背面 (NXR-125/CX)



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。

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。

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。

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。

CABLE CRAMP

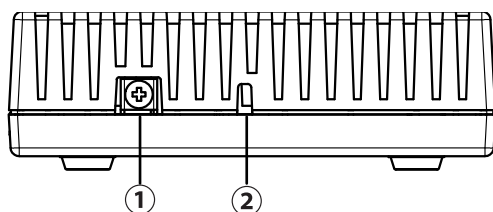
AC アダプタのケーブルが不意に引っ張られても、DC プラグが抜けないようにすることが出来ます。
クリップでケーブルを挟み、クリップと本装置をネジで固定します。



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)



FG(アース) 端子

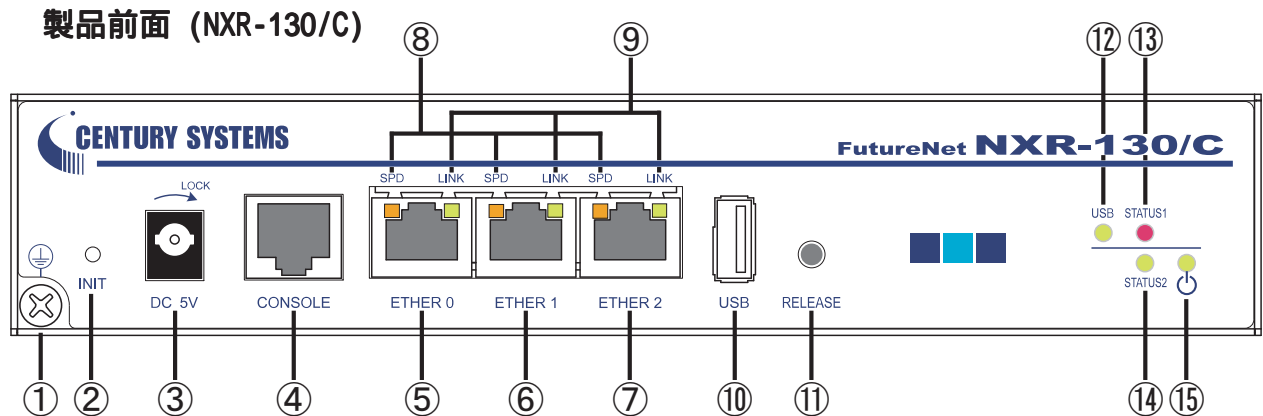
保安用接続端子です。
必ずアース線を接続してください。

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。

第1章 本装置の概要

各部の名称と機能 (NXR-130/C)



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。

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。

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。

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。

ETHER 0 ポート

主に LAN 側ポートとして使用します。

ETHER 1 ポート

主に WAN 側ポートとして使用します。

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。

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 : ■

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 : ■

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。

第1章 本装置の概要

各部の名称と機能 (NXR-130/C)

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

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 : ●

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。

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 : ●

POWER LED (緑)

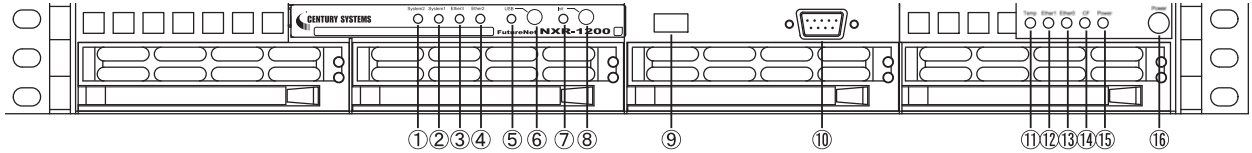
本装置の電源状態を表示します。

- 電源投入時 : ●

第1章 本装置の概要

各部の名称と機能 (NXR-1200)

製品前面 (NXR-1200)



ランプ表示 凡例

消灯時 : 、点灯時 : 、点滅時 : *

SYSTEM 2 LED ()

システムの起動状態を示します。

システム起動中 : *

システム起動後 (ログイン可能状態) :

SYSTEM 1 LED ()

使用しません。

Ether 3 LED ()、 Ether 2 LED ()

Ether 1 LED ()、 Ether 0 LED ()

各 Ether ポートの状態を示します。

Link UP :

Link DOWN :

データ通信中 : *

USB Status LED ()

USBフラッシュメモリの接続状態を表示します。

接続時 : *

動作状態 :

「USBスイッチ」による取り外し操作時

: *

USBスイッチ

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

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

Init Status LED ()

起動状態を表示します。

起動中 : *

「Initスイッチ」で初期設定にて起動中 :

起動完了時 :

Initスイッチ

本装置を工場出荷時の設定に戻して起動するときを使用します。

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

USBインタフェース

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

RS-232ポート (D-Sub 9ピン)

本装置にCLI接続するためのコンソールポートです。

Temp LED ()

温度状態を表示します。

本装置の内部温度が一定以上になった時 :

CF LED ()

搭載しているCFカードの使用状態を表示します。

CFへのアクセス時 :

Power LED ()

電源の状態を表示します。

電源が投入されている状態 :

Powerスイッチ

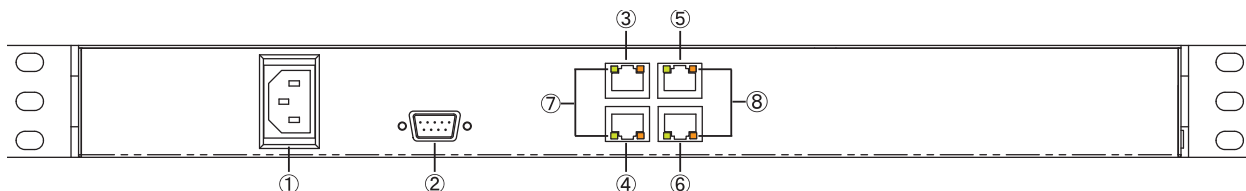
本装置の停止中にスイッチを押すと、本装置が起動します。

本装置の稼働中にスイッチを短時間押しすると、正常終了します。また4秒以上スイッチを押すと、強制終了します。

第1章 本装置の概要

. 各部の名称と機能 (NXR-1200)

製品背面 (NXR-1200)



電源ケーブル差し込み口

付属の電源ケーブルを差し込んでください。

RS-232 ポート (D-Sub 9 ピン)

使用しません。

Ether0 ポート (RJ-45)

Ether1 ポート (RJ-45)

Ether2 ポート (RJ-45)

Ether3 ポート (RJ-45)

Ethernet 規格の LAN ケーブルを接続します。ポートは AutoMDI / MDI-X 対応です。

LINK ランプ ()

Ether ポートのリンク状態を表示します。

Link DOWN :
Link UP :
データ送受信時 : *

速度表示ランプ (/)

Ethernet の接続速度を表示します。

10Base-T モード :
100Base-TX モード :
1000Base-T モード :

・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

第2章 装置の設置

・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！

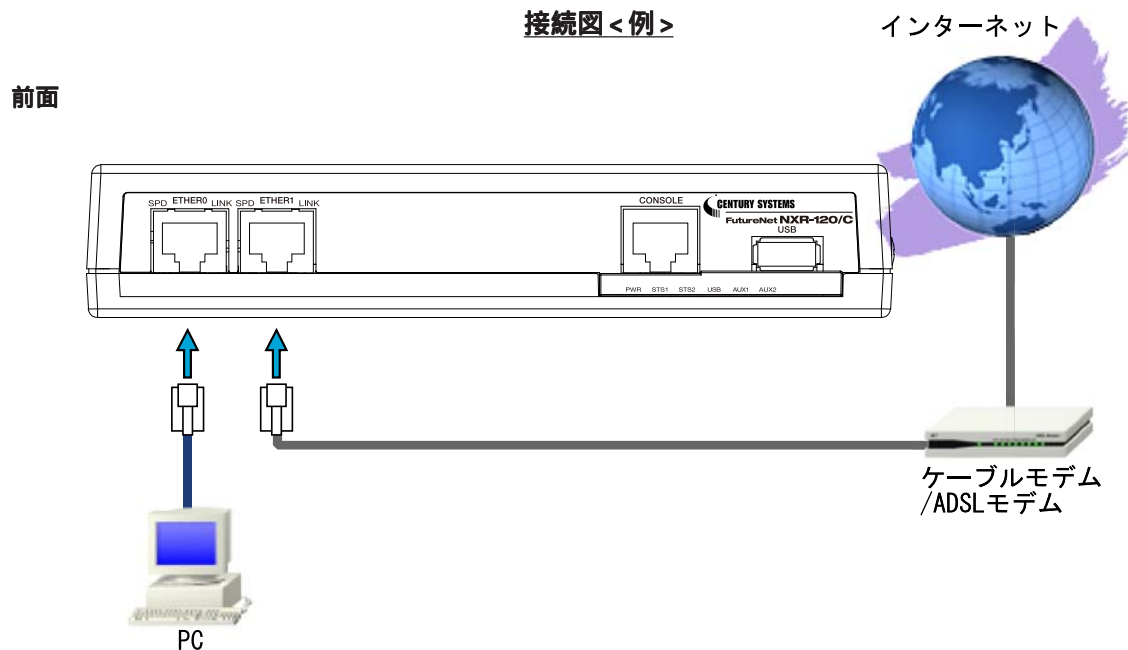
本装置側でも各ポートでARP tableを管理しているため、PCを接続しているポートを変更するとそのPC
から通信ができなくなる場合があります。このような場合は、本装置側のARP tableが更新されるまで
(数秒～数十秒)通信できなくなりますが、故障ではありません。

第2章 装置の設置

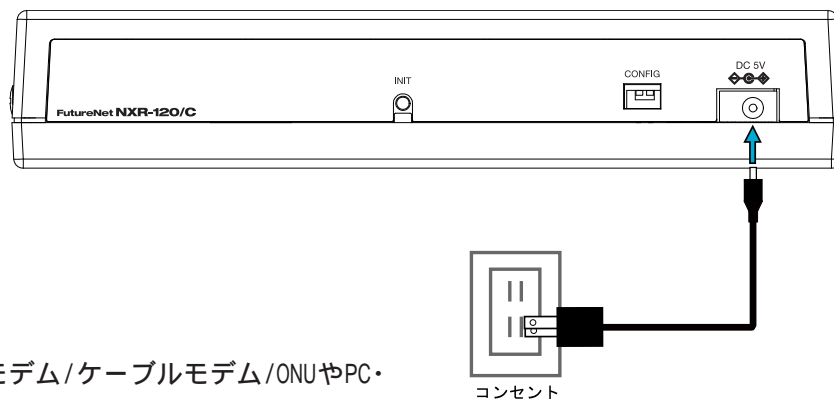
．装置の設置（NXR-120/C）

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>



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。

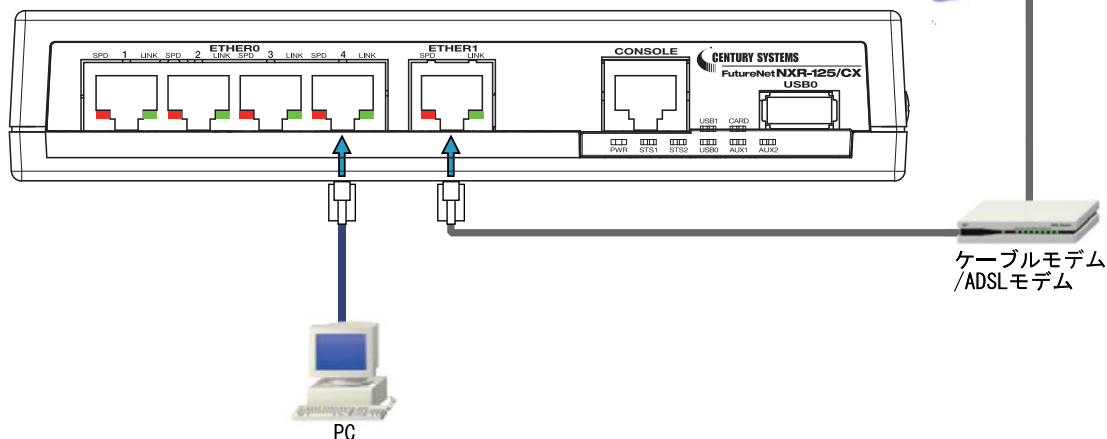
第2章 装置の設置

・装置の設置 (NXR-125/CX)

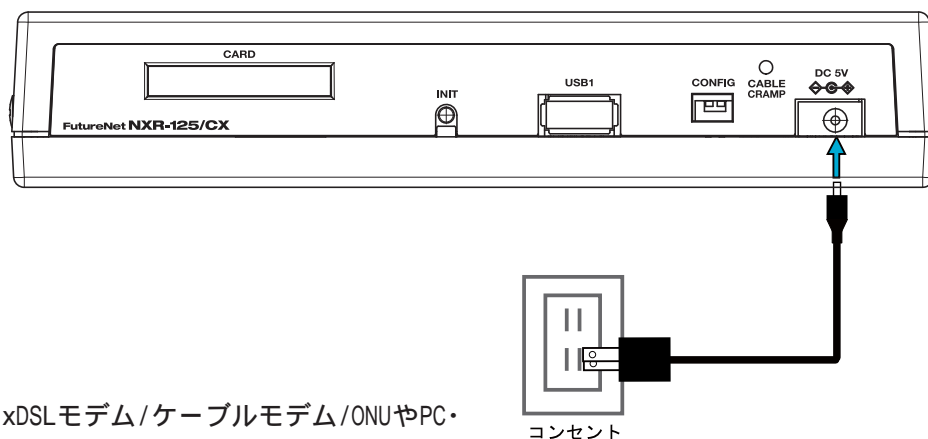
NXR-125/CX と PC や xDSL モデム / ケーブルモデム / ONU は、以下の手順で接続してください。

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。

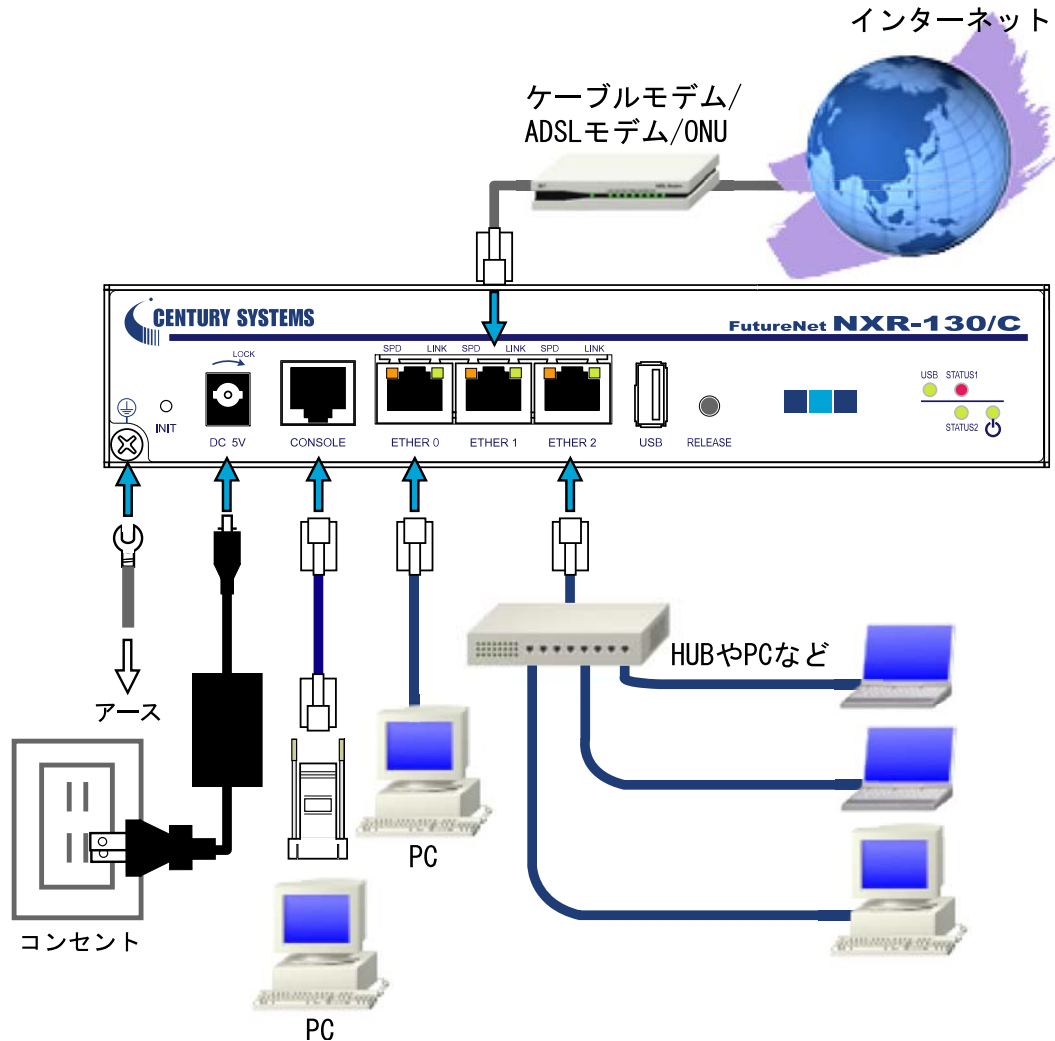
本装置の全てのEthernetポートは、AutoMDI/MDI-X対応です。

第2章 装置の設置

1. 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。

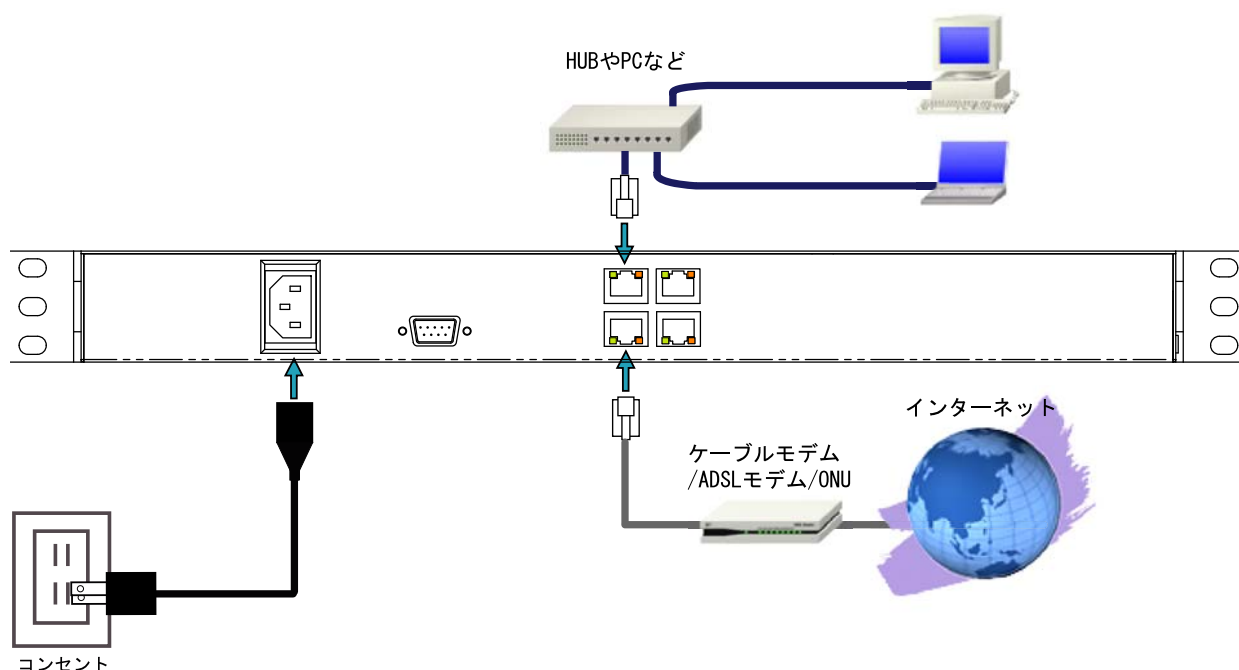
本装置の全てのEthernetポートは、AutoMDI/MDI-X対応です。

第2章 装置の設置

1. 装置の設置 (NXR-1200)

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

接続図<例>



- 1 本装置と ADSL モデム / ケーブルモデム / ONU や PC ・ HUB など、接続する全ての機器の電源が “ OFF ” になっていることを確認してください。
 - 2 本装置の前面にある Ether 1 ポートと、ADSL モデム / ケーブルモデム / ONU を、LAN ケーブルで接続してください。
 - 3 本装置の前面にある Ether 0 ポートと、HUB や PC を LAN ケーブルで接続してください。
工場出荷設定状態の場合、本装置へのログインは、Ether 0 ポートに接続した PC からおこないます。
- 本装置の全 Ethernet ポートは Gigabit Ethernet、AutoMDI/MDI-X に対応しています。**
- 4 本装置と電源コード、電源コードとコンセントを接続してください。
 - 5 全ての接続が完了しましたら、各機器の電源を投入してください。NXR-1200 の本体前面にある Power スイッチを押すと、本装置が起動します。

第3章

設定方法の概要

はじめに

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

CLI のアクセス方法

本装置の CLI へのアクセスは、以下の方法で接続できます。

- ・ Console 接続
本装置の Console(RS-232C)ポートと接続した PC からアクセスします。
- ・ Telnet 接続
本装置の Ethernet0 ポートと接続した PC から IPv4 を用いてアクセスします。
工場出荷設定では、Ethernet 0 に IPv4 アドレス(192.168.0.254)が設定されています。
- ・ SSH 接続
SSH 接続時の認証方法は、plain-text password 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。

第3章 設定方法の概要

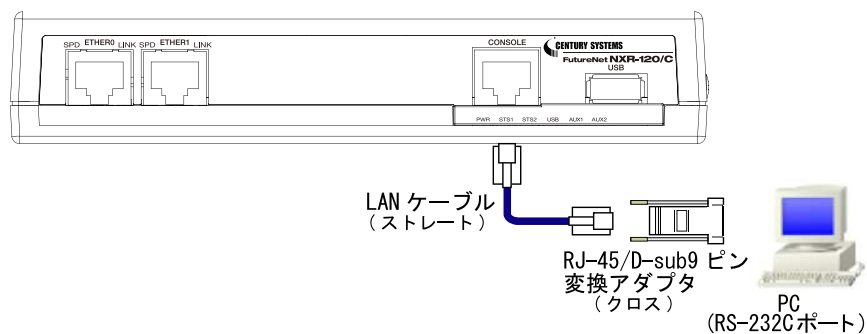
・本装置へのログイン(CLI)

本装置へのログイン(Console接続:NXR-120/C)

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

1. NXR-120/CとPCを接続します。
 1. 本装置前面のConsoleポートと、変換アダプタを、LANケーブルで接続します。接続に使用する以下の部品は、製品に付属されています。
 - ・LANケーブル(ストレート)
 - ・RJ-45/D-sub9ピン変換アダプタ(クロス)
 2. 変換アダプタのコネクタを、PCのRS-232Cポートに接続してください。

<接続例: NXR-120/C>



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

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

< 本装置へのログイン(Console接続:NXRシリーズ共通)に続く >

第3章 設定方法の概要

1. 本装置へのログイン(CLI)

本装置へのログイン(Console接続:NXR-125/CX)

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

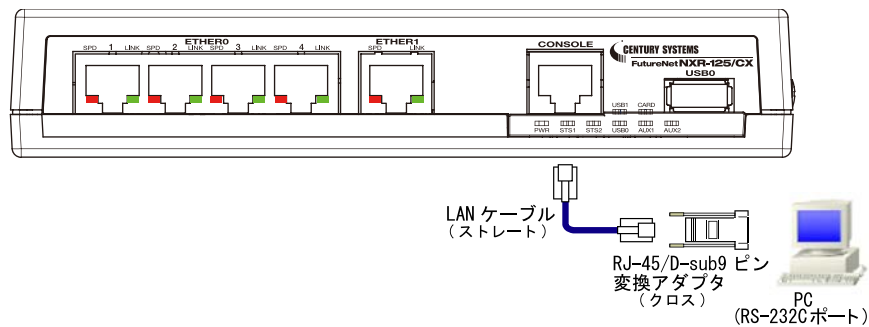
1. NXR-125/CXとPCを接続します。

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

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

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

<接続例: NXR-125/CX>



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

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

< 本装置へのログイン(Console接続:NXRシリーズ共通)に続く >

第3章 設定方法の概要

. 本装置へのログイン(CLI)

本装置へのログイン(Console接続:NXR-130/C)

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

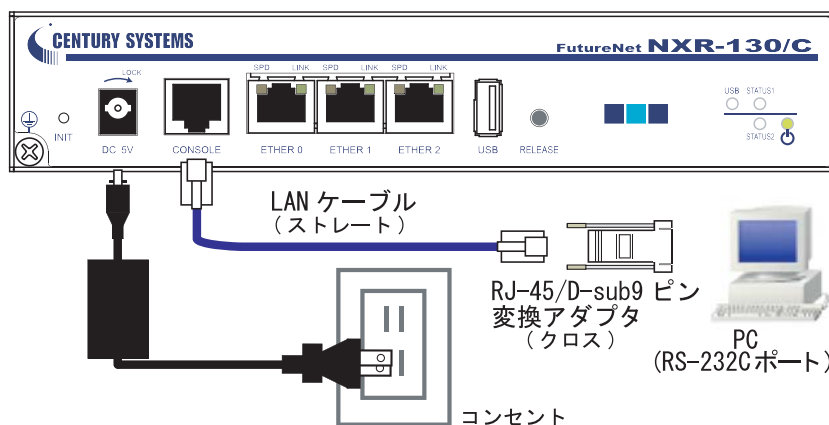
1. NXR-130/CとPCを接続します。

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

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

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

<接続例: NXR-130/C>



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

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

< 本装置へのログイン(Console接続:NXRシリーズ共通)に続く >

第3章 設定方法の概要

・本装置へのログイン(CLI)

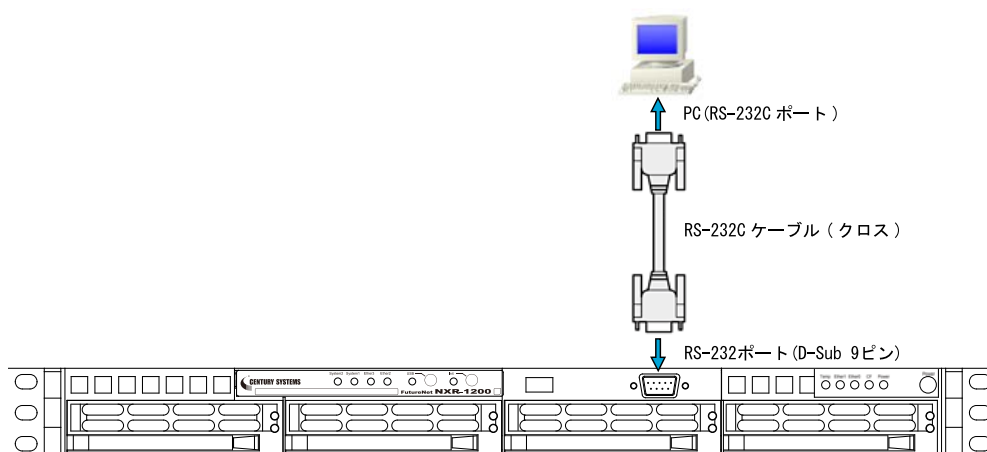
本装置へのログイン(Console接続:NXR-1200)

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

1. NXR-1200とPCを接続します。

1. 本装置前面のRS-232ポートと、RS-232Cケーブル(クロス)を接続します。
2. RS-232Cケーブルを、PCのRS-232Cポートに接続してください。

<接続例: NXR-1200>



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

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

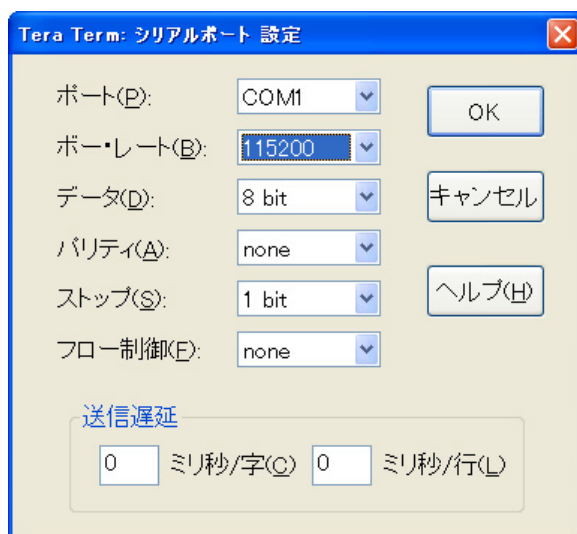
< 本装置へのログイン(Console接続:NXRシリーズ共通)に続く >

第3章 設定方法の概要

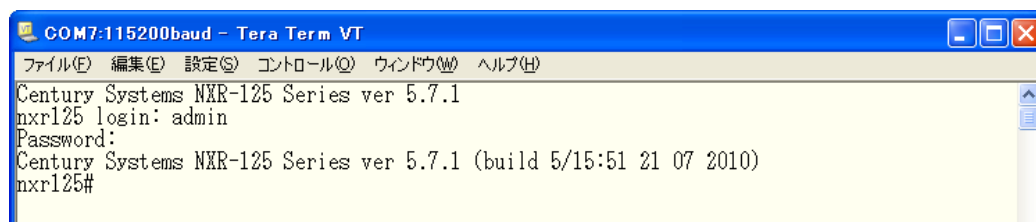
・本装置へのログイン(CLI)

本装置へのログイン(Console接続:NXRシリーズ共通)

2. 本装置を接続したPCで、設定用のターミナルソフト(TeraTerm等)を起動します。
3. 接続条件設定は以下のように設定します。<設定例(TeraTermでの接続設定画面)>
設定方法については、ご使用の各ターミナルソフトの説明書をご覧ください。



4. 「Return」キーまたは「Enter」キーを押すと、ログイン画面が表示されます。
5. ユーザ名、パスワード共に「admin」(工場出荷設定)を入力してログインします。



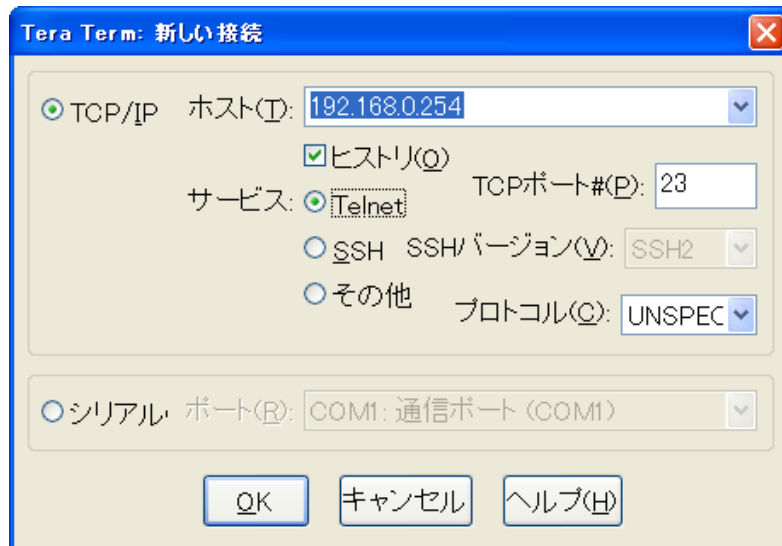
以上で本装置へのログイン(Console接続)は完了です。

第3章 設定方法の概要

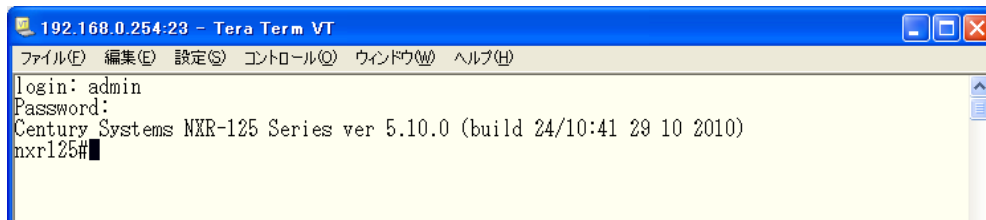
3.1 本装置へのログイン(CLI)

3.1.1 本装置へのログイン(Telnet 接続)

1. Telnet 接続を開始すると、ログイン画面が表示されます。



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



以上で、本装置へのログイン(Telnet 接続)は完了です。

第3章 設定方法の概要

. 本装置へのログイン(GUI)

本装置へのログイン (GUI)

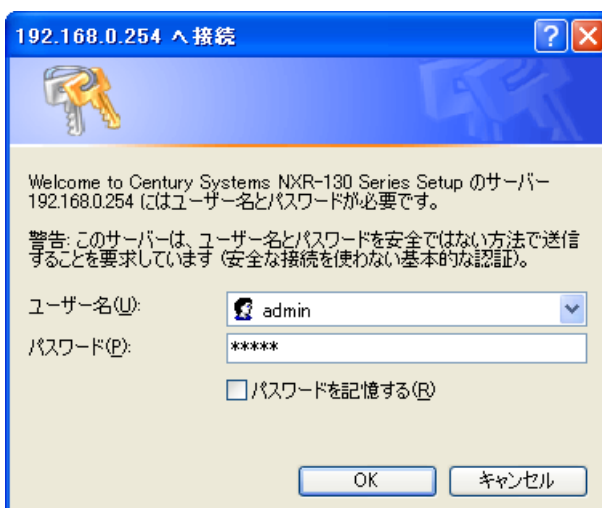
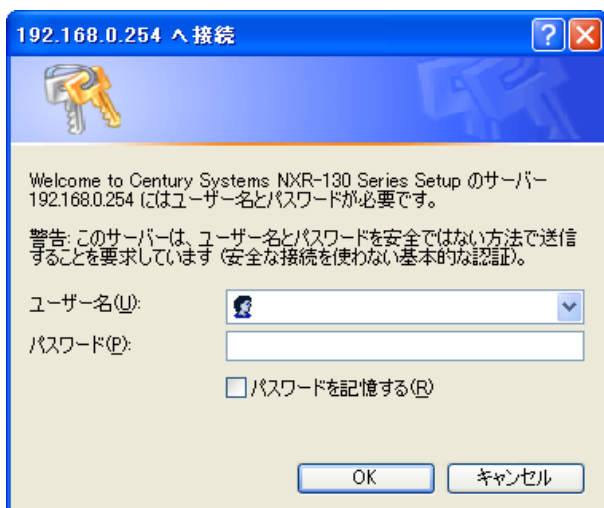
1 .Web ブラウザを起動します。

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

http://192.168.0.254:880/

192.168.0.254 は、Ethernet 0 ポートの工場出荷時の IP アドレスです。アドレスを変更した場合は、そのアドレスを指定してください。**設定画面のポート番号 880 は変更することができません。**

2 . 認証ダイアログ画面が表示されます。ユーザ名、パスワード共に「admin」(工場出荷設定)を入力してログインします。



3 . 下記のような画面が表示されます。以上で本装置へのログインは完了です。



第3章 設定方法の概要

・本装置へのログイン(GUI)

本装置のGUIで設定可能な項目の一覧です。

[インタフェース]

Ethernet I/F

- ・Ethernet

PPP I/F

- ・PPP アカウント
- ・PPPoE

[ネットワーク]

IPv4

- ・スタティックルート
- ・固定ARP

DHCP

- ・DHCP ネットワーク
- ・DHCP ホスト
- ・DHCP リレー

DNS

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

第3章 設定方法の概要

3. コマンド実行モード

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

ユーザーモード(VIEWモード)

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

特権モード(CONFIGURATIONモード)

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

更に、各設定の詳細設定をおこなうには、特権モードから各種モードへ移行します。

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「nrx130」として説明します。

<CLI ログアウト時の表示例>

```
nrx130#exit
Century Systems NXR-130 Series ver 5.1.0
nrx130 login: █
```

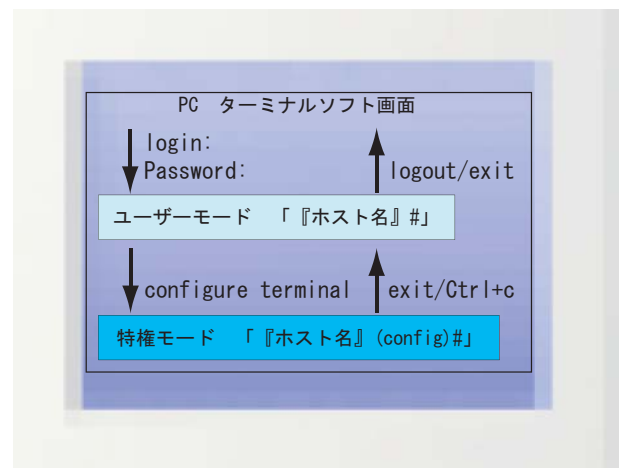
<特権モードへ移行時の表示例>

```
nrx130#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx130(config)#
```

<ユーザーモードへ移行時の表示例>

```
nrx130(config)#exit
nrx130#
```

<モード間の移行>



第3章 設定方法の概要

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、行送りに表示する機能です。“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

第4章 本装置のノード構造

ノード構造について

本装置のノード構造は以下ようになっています。

各設定方法について、本書では上記の各ノード毎に説明します。

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

<本装置ノード構造図>

第 5 章

`view(exec) node`

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 cache
 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)

第5章 view(exec) node

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

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]

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

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

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|)

show interface

- < 説 明 > インタフェースのステータスと設定情報を表示します。
- < 書 式 > show interface (|mode|power-save)
show interface INTERFACE (|mode|power-save)
- < 備 考 > (mode|power-save)はethernet I/Fのみ指定することができます。

show route-map

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

show class access-list

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

show ssh-public-key

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

show users

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

show debugging

- < 説 明 > デバッグログのステータス(ON/OFF)、およびデバッグタイマーのステータス(設定およびカウントダウンタイマー)を表示します。
- < 書 式 > show debugging (|2tpv3|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)

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

第5章 view(exec) node

view(exec) node

show mobile

<説明> 3Gデータ通信カードに関する情報を表示します。

カード情報の表示

<書式> show mobile (|<0-1>)

APN情報の表示(カードによってはppp使用中は取得不可)

<書式> show mobile <0-1> ap

電話番号の表示(カードによってはppp使用中は取得不可)

<書式> show mobile <0-1> phone-number

電波強度の表示(カードによってはppp使用中は取得不可)

<書式> show mobile <0-1> signal-level

show fast-forwarding

<説明> 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 monitor-log

- < 説 明 > Monitor-log を表示します。
< 書 式 > show monitor-log (reachability|resource)
< 備 考 > 詳細は、第35章 : Monitor-log node を参照してください。

show service

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

clock set

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

erase flash-config

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

delete

- < 説 明 > ファイルを消去します。
< 書 式 > delete bootlog (boot log の削除)
delete dump (dump ファイルの削除)
delete file (disk0:FILENAME|disk1:FILENAME) (disk0=USB0, disk1=USB1)
delete syslog (syslog の削除 (初期化))
delete reachability-log (reachability ログの削除)
delete resource-log (resource ログの削除)

save config

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

dir

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

view(exec) node

copy

(boot log|dump|syslog|reachability-log|resource-log)

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

<書式>

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

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

```
copy (boot log|dump|syslog|reachability-log|resource-log)
      (disk0:FILENAME|disk1:FILENAME)
```

<備考> ソースアドレスを指定することができます。

configのバックアップ

<説明> 設定ファイルのバックアップ(外部にコピー)をおこないます。

<書式>

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

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

```
copy (config|show-config) (disk0:FILENAME|disk1:FILENAME) (|all)
```

<備考>

- ・all 指定の場合は、ipsecを含む全てのconfigをtgz形式でコピーします。指定なしの場合は、configのみをxml形式でコピーします。
- ・設定ファイルをshow config形式でバックアップするには、show-configを指定します。
- ・ソースアドレスを指定することができます。

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)/FILENAME
      (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、問い合わせしてからファームウェアの更新を行います。詳細については、「付録E:Firmware update」を参照してください。

restart

- <説明> サービスを再起動します。
- <書式> `restart dhcp-relay` (DHCP リレーサービスを再起動します)
`restart dhcp-server` (DHCP サーバを再起動します)
`restart dns` (DNS サービスを再起動します)
`restart http-server` (HTTP サーバを再起動します)
`restart ipsec` (IPsec サービスを再起動します)
`restart l2tp` (L2TPv2 サービスを再起動します)
`restart l2tpv3` (L2TPv3 サービスを再起動します)
`restart monitor-log` (Monitor-log サービスを再起動します)
`restart netconf-server` (Netconf サーバを再起動します)
`restart ntp` (NTP サービスを再起動します)
`restart ospf` (OSPF サービスを再起動します)
`restart rip` (RIP サービスを再起動します)
`restart snmp` (SNMP サービスを再起動します)
`restart ssh-server` (SSH サーバを再起動します)
`restart syslog` (Syslog サービスを再起動します)
`restart system` (本装置を再起動します)
`restart telnet-server` (Telnet サーバを再起動します)
`restart vrrp` (VRRP サービスを再起動します)
`restart warplink` : (WarpLink クライアントを再起動します)
`restart waplink send-config` (WarpLink Manager に本装置の config を送信します)

configure

- <説明> コンフィグレーションモードへ移行します。
- <書式> `configure terminal`

第5章 view(exec) node

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-forwarding を disable (no fast-forwarding enable) にしてください。

dump

- < 書 式 > dump interface INTERFACE
- < 備 考 > INTERFACE は、いずれかを指定します。
[ethernet <0-2> (|vid<vlan_id:1-4094>) | ppp <0-4> | tunnel <1-255>]

dump filter

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

dump pcap

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

clear l2tpv3 fdb

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

clear l2tpv3 counter

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

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

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

clear class access-list

<説明> class access-list カウンタ (packet/byte数のカウンタ) をクリアします。

<書式> clear access-list <NAME> counter

terminal

length

- <説明> 画面に表示する行数を指定します。
<書式> terminal length <0-512>
<初期値> terminal no length
<備考> 0を指定した場合は、画面単位での一時停止は行われません。

width

- <説明> 画面に表示する列数を指定します。
<書式> terminal width <40-180>
<初期値> terminal no width (= terminal width 80)

connect**connect ppp**

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

reconnect ppp

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

connect l2tp

- <説明> L2TPの接続を開始します。
<書式> connect l2tp

connect l2tpv3

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

connect ipsec

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

disconnect

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

第5章 view(exec) node

view(exec) node

format

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

eject

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

inject

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

ping

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

	入力可能なパラメータ
nrx120#ping	
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

tracert

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

	入力可能なパラメータ
nrx120#tracert	
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

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|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。

```
nrx120#get system statistics cpu 1 5
```

時刻	%CPU	%user	%nice	%system	%idle	%iowait
14:20:02						
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

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。

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。

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。62

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。

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。

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)
```

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
```

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-server version 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。

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

session**session udp timer**

- <説明> UDPのセッションタイマーを設定します。
- <書式> session udp timer <sec:1-8589934> (NXR-120/C、NXR-125/CX、NXR-130/C)
 session udp timer <sec:1-2147483> (NXR-1200)
- <初期値> session udp timer 30
- <no> no session udp timer(=session udp timer 30)

session udp-stream timer

- <説明> UDPストリームのセッションタイマーを設定します。
- <書式> session udp-stream timer <sec:1-8589934> (NXR-120/C、NXR-125/CX、NXR-130/C)
 session udp-stream timer <sec:1-2147483> (NXR-1200)
- <初期値> session udp-stream timer 180
- <no> no session udp-stream timer (=session udp-stream timer 180)

session tcp timer

- <説明> TCPのセッションタイマーを設定します。
- <書式> session tcp timer <sec:1-8589934> (NXR-120/C、NXR-125/CX、NXR-130/C)
 session tcp timer <sec:1-2147483> (NXR-1200)
- <初期値> session tcp timer 3600
- <no> no session tcp timer (=session tcp timer 3600)

session max

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

session limit

- <説明> IP address 毎に conntrack session 数を制限する機能です。一部のUSERにより、conntrack sessionを占有されてしまうような障害を防ぐために使用します。この制限は、forwarding 処理される packet が対象となります。
- <書式> session limit <0-32768> (NXR-120/C、NXR-125/CX、NXR-130/C)
 session limit <0-65536> (NXR-1200)
- <初期値> session limit 0
- <no> no session limit
- <備考> 0を設定すると、IP address 毎の session 数を制限しません。

session (続き)**session tcp limit**

- < 説明 > NXRを端点とするTCPコネクションの接続数を制限する機能です。
- < 書式 > session tcp limit (<16-16384>|) (NXR-120/C、NXR-125/CX、NXR-130/C)
 session tcp limit (<16-32768>|) (NXR-1200)
- < 初期値 > session tcp limit 640 (NXR-120/C、NXR-125/CX、NXR-130/C)
 session tcp limit 1024 (NXR-1200)
- < no > no session tcp limit (=無制限)
- < 備考 >
- ・NXRが他の端末にフォワーディングするものについては影響しません。
 - ・IPv4/IPv6それぞれ別にカウントされます。例えば、接続数を16に設定した場合、IPv4とIPv6のTCPコネクションを、それぞれ16まで接続することができます。
 - ・また、設定変更を行った場合、すでに確立しているコネクションには影響しません。それ以降のコネクションが接続制限の対象になります。

session invalid-status-drop enable

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

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

gui password

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

CLI**console idle-timeout**

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

console terminal length

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

console terminal width

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

CLI (続き)

vty session-max

- <説明> vtyの最大セッション数を設定します。
- <書式> vty session-max <1-10>
- <初期値> vty session-max 4

vty idle-timeout

- <説明> vtyのログアウトタイマーを設定します。
- <書式> vty idle-timeout <minutes:0-35791> (|<seconds:0-2147483>)
- <初期値> vty idle-timeout 0 600
- <no > no vty idle-timeout (=vty idle-timeout 0 0)

vty terminal length

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

vty ip access-filter

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

vty ipv6 access-filter

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

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

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。

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

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

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 アドレスに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、インタフェース名だけ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。

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
```


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ず (non-unicast フレームは、NXR で処理され、かつブリッジもされず)。

track

< 説明 >

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

< 備考 >

delay/retry

- ・ 復旧時(event up と判別した場合)から実際に up 時の action を実行するまでに delay を設定することができます。Delay timer が動作している場合は、track は down state が維持され、この間にも ip reachability check は動作し続けます。
 - ・ Delay timer 動作中に event down を (retry 回数) 検知した場合、delay timer は cancel されます。
 - ・ Delay timer が timeout すると、event up の action が実行されます。このとき、delay timer 中にカウントした ip reachability fail count は 0 にクリアされ、action 実行後に再度 reachability check が開始されます。

initial-timeout

- ・ OSPF/BGP4 の neighbor 監視および interface link 監視設定時、初期の track 状態は init です。新規に track が設定されると、現在の状態を取得します。
 - ・ neighbor が確立(あるいは interface link up)状態と判断されると track up 状態となります。
 - ・ neighbor が確立されていない(あるいは interface link down)状態の場合、すぐに track down 状態とはなりません。この場合は、initial timeout が timeout するか、OSPF/BGP4 機能 / interface 状態監視機能によって down の状態変化通知があったときに、track down として判断し、down action を実行します。
 - ・ Initial timeout は、default で無効です。有効時の default の initial timeout 値は 180sec です。なお、initial timeout 値は、10 ~ 3600sec の範囲で設定することができます。

interface link 状態監視

< 書式 >

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

< 備考 >

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

< 次ページに続く >

track (続き)

ping/ping6による reachability のチェック

<書 式>

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

<備 考>

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

IKE SA の状態監視

<書 式>

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

OSPF neighbor 監視

<書 式>

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

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

BGP peer 監視

<書 式>

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

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

VRRP の状態監視

<書 式>

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

< no > no track <trackid:1-255>

<備 考>

- ethernet のみ有効です。
- master から backup/init への変化、または backup/init から master への変化を監視します。

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)
ipsec x509 ca-certificate NAME ftp://<A.B.C.D>/FILENAME (|source A.B.C.D|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。ファイルの拡張子を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)
ipsec x509 certificate NAME ftp://<A.B.C.D>/FILENAME (|source A.B.C.D|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。ファイルの拡張子を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)
ipsec x509 private-key NAME key ftp://<A.B.C.D>/FILENAME (|source A.B.C.D|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。

**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、一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

**ipsec xauth**

- < 説明 > IPsec Xauth 認証のユーザアカウントを設定します。
- < 書式 > ipsec xauth username USERID password (|hidden) PASSWORD
- < no > no ipsec xauth username USERID
- < 備考 > パスワードは、1-95文字以内で設定してください。  
使用可能な文字は、英数字および!\$#=%+~@`<> です。

**ipsec path-mtu-discovery**

- < 説明 > PMTUD を有効にします。
- < 書式 > ipsec path-mtu-discovery enable
- < no > no ipsec path-mtu-discovery enable
- < 初期値 > ipsec path-mtu-discovery enable
- < 備考 >
- ・ IPsec において PMTU discovery が無効の場合は、DFbit が 1 でかつ tunnel MTU を超えてしまう場合でも、強制的に tunneling し転送されます。この場合、outer の ip header の DF bit は必ず 0 が設定されます。
  - ・ IPsec において PMTU discovery を有効にすると、DFbit が 1 でかつ tunnel MTU を超えてしまう場合、fragment needed を送信元に返信し、packet は drop されます。この場合、outer の IP header の DFbit 値は、tunneling packet の値が設定されます。

**ipsec eap radius (IKEv2のみ)**

< 説明 >

- ・ Account 認証を行う RADIUS server の IP address、UDP port 番号、秘密鍵(secret)を設定することができます。UDP port 番号の default は、1812 番です。Web 認証で使用する radius port 番号とは異なる番号を使用してください。
- ・ NAS-identifier Attribute は、USER により任意の文字(32 文字以内)を指定することが可能です。Default は、機種名 -IPsec(ex.NXR120-IPsec)です。

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

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

< 備考 >

- ・ IPsec client からの EAP message を、NXR にて RADIUS message でカプセル化し、RADIUS server へ送信することで認証を行います。
- ・ RADIUS server への認証要求は、最初の timeout は 2 秒、retry 回数は最大 3 回とし、retry 毎に timeout が + 1 秒されます。
- ・ 設定例は、authentication local/remote(ipsec isakmp policy node)を参照してください。

**ipsec eap identity (IKEv2のみ)**

< 説明 > EAP 認証で使用する ID とパスワードを設定します。

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

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

< 備考 >

- ・ 設定例は、authentication local/remote(ipsec isakmp policy node)を参照してください。
- ・ パスワードは、1-95 文字以内で設定してください。使用可能な文字は、英数字および!\$#="+-\_.:;(){}[]^~@`<> です。

**ipsec pre-share identity (IKEv2のみ)**

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

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

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

< 備考 >

- ・ 設定例は、authentication local/remote(ipsec isakmp policy node)を参照してください。
- ・ パスワードは、1-95 文字以内で設定してください。使用可能な文字は、英数字および!\$#="+-\_.:;(){}[]^~@`<> です。

**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 <tunnel\_id:0-4095>
- <no> no l2tpv3 tunnel <tunnel\_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>



**l2tpv3 group**

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

**ntp**

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

**dns**

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

**snmp**

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

**syslog**

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

**dhcp-server**

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

**monitor-log**

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

**track**

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

**router rip**

- <説明> RIP nodeへの遷移およびprofileを生成します。
- <書式> router rip
- <no> no router rip (=RIPサービスの停止およびprofileを削除します。)

**router ospf**

- <説明> OSPF nodeへの遷移およびprofileを生成します。
- <書式> router ospf
- <no> no router ospf (=OSPFサービスの停止およびprofileを削除します。)

**sip-nat**

## enable

- <説明> SIP NAT を有効にします。
- <書式> sip-nat enable
- <初期値> no sip-nat enable
- <no> no sip-nat enable

## port

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

## port-translate

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

## exclude-interface

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

## 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。

**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

**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

```
priority-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 route-map のみ削除します。

**class access-list**

&lt;説明&gt;

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>)
```

&lt; 次ページに続く &gt;

**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
```

**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>

system led aux <1-2> track (<1-255>|<2048-4095>)

< no > no system led aux <1-2>

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

**system led status**

< 説 明 > 指定した PPP 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>

system led status <1-1> track (<1-255>|<2048-4095>)

< no > no system led status <1-1>

< 備 考 > STS1 LED は、使用可能な機器のみ対応しています。

**as-path**

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

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

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

no ip as-path access-list ACL-NAME



**schedule**

&lt; 説明 &gt;

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 schedule 接続 / 切断 / 再接続

&lt; 説明 &gt;

- ・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。

&lt; 書式 &gt; 日付指定

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

&lt; 書式 &gt; 曜日指定(DOW: day of the week)

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

データ通信端末の schedule リセット

&lt; 説明 &gt;

- ・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。

&lt; 書式 &gt; 日付指定

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

&lt; 書式 &gt; 曜日指定(DOW: day of the week)

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

シスログのローテート

&lt; 説明 &gt;

- ・指定された時間に、syslog の rotate を実行します。指定時間に実際に rotate が行われるかどうかの判断は、syslog node の rotate 設定に依存します。

&lt; 書式 &gt; 日付指定

```
schedule <1-255> HOUR:MIN DAY MON syslog rotate
```

&lt; 書式 &gt; 曜日指定(DOW: day of the week)

```
schedule <1-255> HOUR:MIN DOW (|DOW) syslog rotate
```

## モニターログのローテート

<説明>

指定された時間に、monitor-log 機能の log 情報の rotate を実行します。指定時間に実際に rotate が行われるかどうかの判断は、monitor-log reachability/resource 設定に依存します。

<書式> 日付指定

```
schedule <1-255> HOUR:MIN DAY MON monitor-log reachability rotate
schedule <1-255> HOUR:MIN DAY MON monitor-log resource rotate
```

<書式> 曜日指定 (DOW: day of the week)

```
schedule <1-255> HOUR:MIN DOW (|DOW) monitor-log reachability rotate
schedule <1-255> HOUR:MIN DOW (|DOW) monitor-log resource rotate
```

## システム再起動

<説明> 指定された時間に、system の再起動を実施します。

<書式> 日付指定

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

<書式> 曜日指定 (DOW: day of the week)

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

## 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

**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

**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できます。

**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のフォー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

**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

**link-check**

&lt; 説明 &gt;

・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)                 | -                                                                                             |

&lt; 書式 &gt; link-check (|&lt;0-60sec&gt;)

&lt; 初期値 &gt; link-check 10

&lt; no &gt; no link-check (=link-check 0)

&lt; 備考 &gt;

・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。

&lt; 書式 &gt; ip access-linkdown

&lt; no &gt; no ip access-linkdown

&lt; 備考 &gt; Default は、無効(no ip access-linkdown)です。

**ipv6 access-linkdown**

- < 説 明 > 本機能を有効にすると、link downの状態でも該当 interface の IPv6 address に通信することができます。
- < 書 式 > ipv6 access-linkdown
- < no > no ipv6 access-linkdown
- < 備 考 > Default は、無効(no ipv6 access-linkdown)です。

**ip arp reachable-time**

- < 説 明 > 解決した ARP の有効期間を設定することができます。
- < 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(next hop)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)



**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

**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

**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

**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 <vrrpid:1-255> (address A.B.C.D|)

**vrrp ip priority**

- <説 明> VRRPのプライオリティを設定します。
- <書 式> vrrp ip <vrrpid:1-255> priority <1-254>
- <初 期 値> vrrp ip <vrrpid:1-255> priority 100
- < no > no vrrp ip <vrrpid:1-255> priority

**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 <vrrpid: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>  
vrrp ip <vrrpid:1-255> netevent <trackid:2048-4095> priority <1-254>
- < no > no vrrp ip <vrrpid:1-255> netevent
- <備 考> track event がdownしたときに、VRRPのpriorityを変更します。

**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)

**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。

#### 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。

**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

```
nrx130#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
nrx130(config)#interface tunnel <0-255>
```

```
nrx130(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においてreassembleするか、reassembleせずにforwardingするかを設定することができます。defaultは、reassembleします。
- <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) IPv6-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)

netevent <trackid:2048-4095> (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

## 第8章 interface tunnel node

### 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

## 第9章 interface ppp node

### interface ppp node

#### 移行 command

```
nrx130#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
nrx130(config)#interface ppp <0-4>
```

```
nrx130(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)



**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

#### 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。

**ip nat-loopback**

&lt;説明&gt;

- ・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を行うことができますようになります。

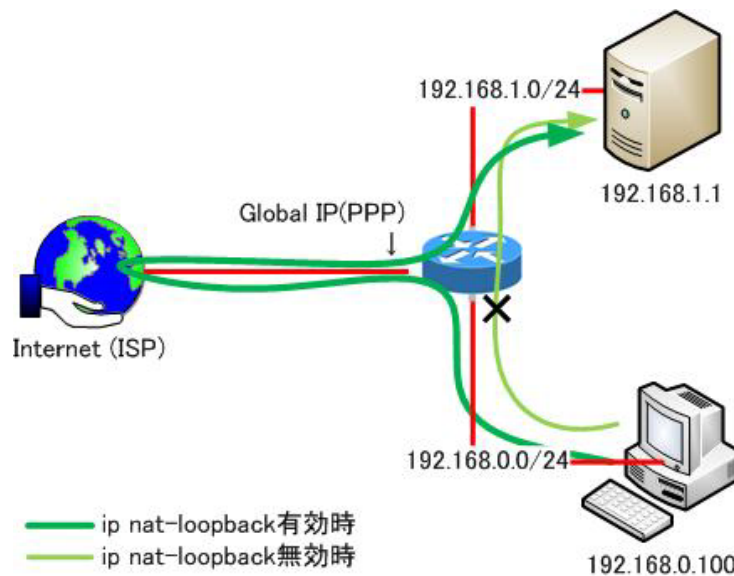
&lt;書式&gt; ip nat-loopback

&lt;初期値&gt; no ip nat-loopback

&lt;no&gt; no ip nat-loopback

&lt;備考&gt;

- ・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contrack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。

**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)

**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)

**ppp username**

- < 説 明 > PPP 接続の User ID をパスワードを設定します。
- < 書 式 > ppp username USERID password (|hidden) PASSWORD
- < no > no ppp username
- < 備 考 > パスワードは、1-95 文字以内で設定してください。  
使用可能な文字は、英数字および!\$#=\*+-.\_:();(){}[]^~@` <> です。

**ppp auto-connect**

- < 説 明 > PPP の自動接続を有効にします。
- < 書 式 > ppp auto-connect <seconds:10-600>
- < 初 期 値 > ppp auto-connect 60
- < no > no ppp auto-connect

**ppp ipcp enable**

- < 説 明 > IPCP を有効にします。
- < 書 式 > ppp ipcp enable
- < 初 期 値 > ppp ipcp enable
- < no > no ppp ipcp enable

**ppp ipcp dns**

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

**ppp ipcp ip request**

- < 説 明 > IPCP で IP アドレスをリクエストします。
- < 書 式 > ppp ipcp ip request
- < 初 期 値 > no ppp ipcp ip request
- < no > no ppp ipcp ip request
- < 備 考 > ip address command で設定された IP を IPCP で request する

**ppp ipv6cp enable**

- < 説 明 > IPv6CP を有効にします。
- < 書 式 > ppp ipv6cp enable
- < 初 期 値 > no ppp ipv6cp enable
- < no > no ppp ipv6cp enable : Disable IPv6CP

#### ppp ipv6cp id

- <説明> IPv6CP インタフェース ID を設定します。
- <書式> ppp ipv6cp id X:X::X:X  
ppp ipv6cp id ethernet <0-2>
- <初期値> no ppp ipv6cp id
- <備考> 指定ない場合は、eth0 の mac を使用する。この設定により LLA が決定される。
- <no> no ppp ipv6cp id

#### ppp on-demand

- <説明> On-demand PPP を設定します。
- <書式> ppp on-demand
- <備考> 現状 mobile 時のみ対応 (l2tp, ipv6cp 有効時は無視される)
- <no> no ppp on-demand

#### ppp idle-timeout

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

**netevent**

- <説明> netevent を設定します。
- <書式> netevent <trackid:1-255> (connect|disconnect)  
netevent <trackid:2048-4095> (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。



**ipsec hold-sa**

## &lt; 説 明 &gt;

- ・ 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

## &lt; 備 考 &gt;

- ・ 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。

## &lt; 書 式 &gt;

## 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|)

#### 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

**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)

**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 command**

l2tp node に移行します。

```
nxr130#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
nxr130(config)#l2tp 0
```

```
nxr130(config-l2tp)#
```

**tunnel**

<説明> L2TP の tunnel address を指定します。

<書式> tunnel address (A.B.C.D | FQDN)

**tunnel hidden**

<説明> AVP Hiding を有効にします。

<書式> tunnel hidden

<初期値> no tunnel hidden

<no> no tunnel hidden : Set defaults

**tunnel retransmit**

<説明> 切断までのリトライ回数を設定します。

<書式> tunnel retransmit retries <max:1-1000>

<初期値> tunnel retransmit retries 5

<no> no tunnel retransmit retries (=tunnel retransmit retries 5)

**tunnel hello**

<説明> Hello インターバルを設定します。

<書式> tunnel hello <seconds:0-1000>

<初期値> tunnel hello 60

<no> no tunnel hello : Disable

**tunnel password**

<説明> パスワードを設定します。

<書式> tunnel password ([hidden) PASSWORD

<no> no tunnel password

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

**tunnel ppp**

<説明> PPP をトネリングします。

<書式> tunnel ppp <interface:0-4>

<備考> l2tp の再接続、再接続間隔は、ppp の設定を使用する

# 第 12 章

---

---

l2tpv3-tunnel node



## l2tpv3 tunnel parameters

### 移行 command

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> リモード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> リモードLCCEのルータIDを設定します。

<書 式> tunnel router-id A.B.C.D

<備 考> 必須

### tunnel password

<説 明> 認証やAVP Hidingで使用するパスワードを設定します。

<書 式> tunnel password PASSWORD

tunnel password hidden PASSWORD

<初 期 値> no tunnel password

< no > no tunnel password

<備 考> パスワードは、1-95文字以内で設定してください。

使用可能な文字は、英数字および!\$#=\*+\_-.:;(){}[]^~@` <> です。

### tunnel hidden

<説 明> AVP Hidingを設定します。

<書 式> tunnel hidden

< no > no tunnel hidden

## 第12章 l2tpv3-tunnel node

### l2tpv3 tunnel parameters

#### tunnel protocol

- < 説 明 > 送信プロトコルを選択します。
- < 書 式 > tunnel protocol (ip|udp)
- < 初 期 値 > tunnel protocol ip
- < no > no tunnel protocol (=tunnel protocol ip)

#### tunnel local hostname

- < 説 明 > ローカル LCCE のホスト名を設定します。
- < 書 式 > tunnel local hostname HOSTNAME
- < 初 期 値 > no tunnel local hostname
- < To Unset > no tunnel local hostname

#### tunnel local router-id

- < 説 明 > ローカル LCCE のルータ ID を設定します。
- < 書 式 > tunnel local router-id A.B.C.D
- < 初 期 値 > no tunnel local router-id
- < no > no tunnel local router-id

#### tunnel digest

- < 説 明 > メッセージダイジェストを有効にします。
- < 書 式 > tunnel digest (md5|sha1)
- < 初 期 値 > no tunnel digest
- < no > no tunnel digest

#### tunnel hello

- < 説 明 > Helloパケットの送信間隔を設定します。
- < 書 式 > tunnel hello <0-1000>
- < 初 期 値 > tunnel hello 60
- < no > no tunnel hello : Disable

#### tunnel vendor

- < 説 明 > リモート LCCE のベンダー ID を設定します。
- < 書 式 > tunnel vendor (ietf|century|cisco)
- < 初 期 値 > tunnel vendor ietf
- < no > no tunnel vendor : Set defaults

#### netevent

- < 説 明 > イベント検出時にトンネルを切断します。
- < 書 式 > netevent <trackid:1-255> disconnect
- < 初 期 値 > no netevent
- < 備 考 > PPP interface の監視のみ対応
- < no > no netevent

# 第 13 章

---

---

l2tpv3-xconnect node

### l2tpv3 xconnect parameters

#### 移行 command

```
nrx130#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx130(config)#l2tpv3 xconnect <xid:1-4294967295>
nrx130(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)

### I2tpv3 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 enable

<説 明> Group の preempt モードを有効にします。  
<書 式> preempt enable  
< 初 期 値 > 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**

```
nrx130#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
nrx130(config)#router rip
```

```
nrx130(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)

#### 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

**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

**timers spf**

- < 説 明 > OSPF SPF timers を設定します。
- < 書 式 > timers spf <delay:0-4294967295> <hold\_time:0-4294967295>  
 <delay:0-4294967295> : Delay between receiving a change to SPF calculation  
 <hold\_time:0-4294967295> : Hold time between consecutive SPF calculations
- < no > no timers spf : Set defaults

**passive-interface**

- < 説 明 > ルーティングアップデートの送信をストップします(受信はします)。  
< 書 式 > passive-interface ethernet <0-2> (|vid <1-4094>)  
passive-interface ppp <0-4>  
passive-interface tunnel <0-255>  
< no > no passive-interface ethernet <0-2> (|vid <1-4094>)  
no passive-interface ppp <0-4>  
no passive-interface tunnel <0-255>

**default-information**

- < 説 明 > デフォルトルートをOSPFで配信します。  
< 書 式 > default-information originate  
default-information originate (|metric <0-16777214>) [|metric-type (1|2)] (|always)  
< no > no default-information originate  
no default-information originate (|metric<0-16777214>)[metric-type(1|2)] (|always)

**router-id**

- < 説 明 > Router IDを設定します。  
< 書 式 > router-id A.B.C.D  
< no > no router-id

# 第 17 章

---

---

bgp node

**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**

## 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 ヘ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 ( 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。

**neighbor**

## default-originate

- < 説 明 > デフォルトルートを送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

**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 &amp; 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

**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

**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(Simple Network Management Protocol)機能

NXRのSNMP機能は、systemの情報をSNMP protocolを使用して取得する機能を有します。また、systemにて状態の変化が発生した際に、NMS(SNMP Trap Manager)にtrapを送信する機能も有します。なお、SNMPによる設定(set)はサポートしていません(read-onlyです)。

### SNMP version と access 制御

現在対応しているSNMPのversionは、v1、v2cです。SNMP Access制御として、SNMP Serverのnetworkとcommunity名を指定することができます。Networkに関しては、IPv4/IPv6 Addressを指定することができます。

### SNMP Trap

本装置内部で発生した状態変化を、指定されたNMSに対してSNMP Trapにて通知する機能です。

- Trap version1/version2に対応しています。また、informを指定することもできます。Trapの送信先は、IPv4/IPv6 addressで指定することが可能です。informの場合は再送回数 / 再送間隔も指定することができます。
- SNMP trap用のcommunity名をSNMP access用とは別に指定することができます。これらの設定は、Trapの送信先毎に指定することができます。
- Trapは、監視対象の状態変化の通知やUSERによる設定変更によるイベント発生によって送信されません。Trapは、UDPを使用して送信するため必ずserver側へ届けられる保証はありません。このような場合は、informを使用することでNMSへ届けられる可能性が高くなります。
- 各service状態を定期的に監視する機能は保持していないため、serviceの突然停止を検出し通知することは出来ません。このような状態を監視する場合は、NMSの機能を利用して周期的にgetを行うようにしてください。

### System Group MIB(MIB-II)設定

本装置では、RFC1213にて定義されているMIBの内、以下の項目をUIより設定することが出来ます。

- sysContact
- sysName
- sysLocation
- sysDescr

なお、sysObjectIDには、centuryにて定義した機器毎のOIDが設定されていて機種判定をすることができます。

また、sysUpTimeアクセス時には、本装置が起動してからの経過時間を返します。(ntpなどによる時刻変更の影響は受けません)。

#### 対応 MIB 一覧

本装置にて対応する MIB は次のとおりです。

##### ・ Standard

- RFC1213 (SNMPv2 MIB-II)
- RFC2011 (IP-MIB)
- RFC2012 (TCP-MIB)
- RFC2013 (UDP-MIB)
- RFC2863 (IF-MIB)
- RFC3411 (SNMP-FRAMEWORK-MIB)
- RFC3412 (SNMP-MPD-MIB)
- RFC3413 (SNMP-TARGET-MIB: SNMP-NOTIFICATION-MIB: SNMP-PROXY-MIB)
- RFC3414 (SNMP-USER-BASED-SM-MIB)
- RFC3415 (SNMP-VIEW-BASED-ACM-MIB)
- RFC3418 (SNMPv2 MIB)
- RFC2465 (IPv6 MIB) 一部対応

##### ・ Private MIB

- CS-NXR-PRODUCT-MIB
- CS-NXR-L2TPv3-MIB

#### SNMP NAT

SNMP PDU 部分に含まれる IP アドレス型の NAT に対応しています。NAT の方法については、RFC2962 準拠とし、BASIC のみ対応しています。PDU 内の IP アドレスのうち NAT 対象となったアドレスの先頭 1 オクテットのみを変換します。

**移行 command**

```

nrx130#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx130(config)#snmp
nrx130(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/M COMMUNITY

< 初期値 > no security

< 備考 > Network は、3 つまで設定することができます。

< No > no security (A.B.C.D/M|X::X::X/M)

**syslocation**

< 説明 > sysLocation を設定します。

< 書式 > syslocation LOCATION

< 初期値 > no syslocation

< No > no syslocation

**syscontact**

< 説明 > sysContact を設定します。

< 書式 > syscontact CONTACT

< 初期値 > no syscontact

< No > no syscontact

**sysname**

< 説明 > sysName を設定します。

< 書式 > sysname SYSNAME

< 初期値 > no sysname [= 機種名(ex. NXR-130)]

< No > no sysname

**sysdescr**

< 説明 > sysDescr を設定します。

< 書式 > sysdescr DESCRIBE

< 初期値 > no sysdescr

< No > no sysdescr

< 備考 > 初期値は ビルド名です。  
ex. Century Systems NXR-130 Series ver 5.1.0 (build 50/15:44 22 04 2009)

**trap manager**

<説明> SNMPのtrap managerを設定します。

<書式>

```
trap manager (A.B.C.D|X:X::X:X) (|trapcommunity) (|v1|v2)
```

```
trap manager (A.B.C.D|X:X::X:X) (|trapcommunity) inform [(interval <10-1800>)|(retry <0-10>)]
```

<初期値> no trap manager

<No> no trap manager (|A.B.C.D|X:X::X:X)

<備考> 3つまで設定することができます。

Community未指定時は"community"を使用します。

pdu-type未指定時はv1を使用します。

**trap agent**

<説明> SNMPのtrap agentを設定します。

<書式> trap agent ip A.B.C.D

```
trap agent interface ethernet <0-2>
```

<初期値> no trap agent

<No> no trap agent

<備考> TRAPパケット中の"Agent Address"を指定することが出来ます。

**bind address**

<説明> SNMPのbind addressを設定します。

<書式> bind address A.B.C.D

```
bind address X:X::X:X
```

<初期値> no bind address

<No> no bind address

<備考> TRAP送信時のsource ipもこのbind addressとなります。

未設定(no bind address)の場合は0.0.0.0でlistenします。

# 第 20 章

---

---

syslog node

**移行 command**

```

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

```

**local enable**

<説 明> syslogをローカル出力します。

<書 式> local enable

<初 期 値> local enable

< No > no local enable (ローカル出力しません)

**local file**

<説 明> syslogをファイルに出力します。

<書 式> local file (disk0:FILENAME|disk1:FILENAME)

<初 期 値> no local file

< No > no local file

<備 考> filenameは「disk0:」または「disk1:」で始まる任意のファイル名を指定します。

**server**

<説 明> syslogサーバのIPアドレスまたはFQDNを設定します。

<書 式> server (A.B.C.D|X:X::X:X|FQDN) (|source A.B.C.D|X:X::X:X)

< No > no server (A.B.C.D|X:X::X:X|FQDN) (= syslogサーバに転送しません)

<備 考> syslog送信時の送信元アドレスを設定することができます。

**mark**

<説 明> Syslog markの設定をします。

- ・Markの出力間隔を0～99minの範囲で指定することができます。Defaultは20分毎とし、0を指定した場合、markは出力されません。
- ・なお、markをsyslogへ出力する場合は、syslogの出力levelをdebug/infoのいずれかに設定してください。

<書 式> mark <min:0-99>

<初 期 値> mark 20

<備 考> mark 0 (Disableにします)

< No > no mark (=mark 20)

**priority**

<説 明> Syslogのプライオリティを設定することができます。

<書 式> priority (debug|info|notice)

<初 期 値> priority info

< No > no priority

<備 考> facilityは、指定することができません。

**system**

&lt; 説明 &gt;

- ・ System Message 出力機能とは、Connection tracking 数、Load Average、メモリ使用量などの system の情報を、mark 出力時または、一時間毎に syslog 上に出力させる機能です。
- ・ System 内の情報であるため、外部 remote server へ出力することは推奨しません。

< 書式 >    system mark                    : Output messages with mark  
                  system hour                : Output messages hourly

&lt; 初期値 &gt;    no system

&lt; No &gt;        no system                    : System メッセージ出力しない

**suppress**

&lt; 説明 &gt;

- ・ 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のみを表示する機能です。

&lt; 書式 &gt;    suppress &lt;10-3600&gt;

&lt; 初期値 &gt;    no suppress

&lt; No &gt;        no suppress

&lt; 備考 &gt;

- ・ 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**

&lt; 説明 &gt;    syslog メッセージをメール送信します。

- ・ USER が指定した文字列を含む message が syslog へ出力された場合、設定された E-mail address に mail を送信する機能です。この機能により、CLI への login 失敗時などの不正アクセスがあった場合に、管理者に mail を送るようなことが可能になります。
- ・ 指定した文字列が含まれるかどうかを、60sec 毎に check し、該当する文字列が存在した場合に mail 送信します。なお、mail 送信機能については、IPv4/IPv6 の両方をサポートします。

&lt; 書式 &gt;    mail send enable

&lt; 初期値 &gt;    no mail send

&lt; No &gt;        no mail send

**mail to**

&lt; 説明 &gt;    送信先メールアドレスを設定します。

&lt; 書式 &gt;    mail to RECEIVER

&lt; 初期値 &gt;    no mail to

&lt; No &gt;        no mail to

**mail from**

&lt; 説明 &gt;    送信元メールアドレスを設定します。

&lt; 書式 &gt;    mail from SENDER

&lt; 初期値 &gt;    no mail from

&lt; No &gt;        no mail from

**mail subject**

- < 説明 > メール の 件名 を 設定 し ます。
- < 書 式 > mail subject SUBJECT
- < 初 期 値 > no mail subject
- < No > no mail subject

**mail strings**

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

**mail server**

- < 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



**rotate**

## &lt; 説明 &gt;

- ・ Default の動作では、syslog message の容量が最大許容量の 80% を超えると、後方の 4000 行を残して削除します。システム起動時より、10 分周期で自動的にチェックします。
- ・ rotate 設定を行うと、syslog のサイズが閾値を超えていた場合に指定された storage 上に backup を行います ( 閾値を指定しない場合は、サイズに関係なく backup を行います )。rotate チェックの日時は、schedule コマンドで指定します。

## &lt; 書式 &gt;

```
rotate (disk0|disk1)
```

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

```
rotate (disk0|disk1) threshold files <files:1-10>
```

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

< 初期値 > no rotate

< No > no rotate

## &lt; 備考 &gt;

- ・ USB0 に接続された USB Flash メモリを指定する場合は、disk0 を選択します。USB1 に接続された USB Flash メモリを指定する場合は、disk1 を選択します。
- ・ Syslog rotate の閾値はサイズ指定(kbytes)です。また、backup file の数も指定することができます。
- ・ なお、backup された syslog message は、gzip にて圧縮されます。また、下記フォーマットの file 名になります。なお、Backup 先に同じ名前の file が存在した場合、上書きされます。

backup ファイル名の format : YYYYMMDD\_HHMM.log.gz

2010 年 11 月 2 日 19 時 50 分に取得した backup ファイルの例 : 20101102\_1950.log.gz

# 第 21 章

---

---

dhcp-server node

**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

**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 SCOPEID
- < 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

#### 移行 command

```
nrx130#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx130(config)#dhcp-relay
nrx130(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

## 第23章 ipsec local policy node

### ipsec local policy node

#### 移行 command

```
nrx130(config)#ipsec local policy <policy:1-255>
nrx130(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=nrx1.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

## 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 AAAAAAAAAAAAAAAAAAAAA
```

#### 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。

**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 >

## 第24章 ipsec isakmp policy node

### 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 >

## 第24章 ipsec isakmp policy node

### 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 . . .
!
```

## 第 24 章 ipsec isakmp policy node

### ipsec isakmp policy node

#### reauthentication (IKEv2のみ)

< 説 明 >

- ・IKEv2では、rekeyのタイミングでreauthを行うかrekeyを行うかを選択することができます。

< 書 式 > reauthentication enable

< 初 期 値 > reauthentication enable

< No > no reauthentication enable

< 備 考 >

- ・Defaultでは、reauthが有効です。reauth時は、IKE SAのrekey時にCHILD SAの再作成も行われます。reauthを無効にした場合、rekeyが実施されます。
- ・セキュリティを考慮する場合はreauthを選択するようにしてください。ただし、Security Gatewayに(NXRだけでなく対向装置にも)負荷がかかるため、負荷に配慮する場合はrekeyを選択するようにしてください。

## 第 24 章 ipsec isakmp policy node

### 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)

## 第 24 章 ipsec isakmp policy node

### 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 よりどれくらい増やすかを % 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。

$$\text{minimum soft timer} = \text{lifetime} - \text{margin}$$
$$\text{maximum soft timer} = \text{lifetime} - (\text{margin} + \text{margin} \times \text{increased-ratio}/100)$$

- ・ 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)



## 第 24 章 ipsec isakmp policy node

### 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 <policy:1-255> netevent <trackid:1-255> change <local_policy:1-255>
local policy <policy:1-255> netevent <trackid:2048-4095> change <local_policy:1-255>
```
- < 備 考 >
- ・ PSK を使用している場合、変更前の local policy の ID と変更後の local policy の ID は、同じ ID を使用してください。たとえば、下記のような change action を設定する場合は、local policy 1 と local policy 2 の self-identity を同じ ID にしてください。
- ```
!
ipsec isakmp policy 1
 local policy 1 netevent 1 change 2
!
ipsec local policy 1
 self-identity fqdn myid 同じ ID
!
ipsec local policy 2
 self-identity fqdn myid 同じ ID
!
```
- ・ action 追加時の動作: track object の状態が down の場合 action が実行されます。
  - ・ action 削除時の動作: netevent がない場合と同じ動作が実行されます。Action 復旧処理が行われるわけではありません。

## 第 24 章 ipsec isakmp policy node

### 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)  
netevent <trackid:2048-4095> (connect|disconnect|reconnect)
- < No > no netevent

# 第 25 章

---

---

ipsec tunnel policy node

## 第25章 ipsec tunnel policy node

### ipsec tunnel policy node

#### 移行 command

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

#### description

<説明> IPsec tunnel policyの説明を記述します。  
<書式> description DESCRIPTION  
<No> no description DESCRIPTION

#### set transform

<説明> transformを設定します。  
<書式>  
set transform (esp-3des|esp-des|esp-aes128|esp-aes192|esp-aes256|esp-null)  
(esp-sha1-hmac|esp-md5-hmac|esp-sha256-hmac|esp-sha384-hmac|esp-sha512-hmac|)  
<初期値> set transform esp-aes128 esp-sha1-hmac  
<備考> HASHを指定しない場合は、ESPの認証機能は無効となります。  
認証機能は無効にした場合は、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>

## 第25章 ipsec tunnel policy node

### ipsec tunnel policy node

#### set key-exchange (change action)

< 説 明 >

- ・ IPsec tunnel で使用する isakmp policy の track 状態(up/down)によって、action を実行します。
- ・ この機能により、障害に応じて、1つの IPsec 設定にて main/backup の構成を取ることができます。

< 書 式 >

```
set key-exchange isakmp <1-65535> netevent <trackid:1-255> change isakmp <1-65535>
set key-exchange isakmp <1-65535> netevent <trackid:2048-4095> change isakmp <1-65535>
```

< 備 考 >

- ・ action 追加時の動作: track object の状態が down の場合 action が実行されます。
- ・ action 削除時の動作: netevent がい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

## 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 > WAN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 (= timeout 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 fifo (|limit <1-16384>)
```

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><br>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><br>no match ip tos <0-255> |

# 第 29 章

---

---

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

## Route-map

特定の packet や route などの条件に合うかどうかをチェックし、それに応じた action を実行することができる機能です。

- Packet の coloring や route の属性を変更することができます。Packet coloring で特定の traffic に mark 値(NXR 内のみ有効な値)や ToS 値の設定を行う(tos と mark を同時に設定することも可能)ことによって、QoS を適用することができます。
- Route-map はシーケンス番号をもち、複数の route-map を適用させることができます。
- 同じ名前の route-map が複数存在する場合は、シーケンス番号が小さいものから処理され、最初に match したエントリの action を実行します。
- 1 つの route-map 内に複数の match 条件がある場合は、いずれかの match 条件にマッチすると該当するアクションが実行されます。なお、NXR では、1 つの match 条件に複数の条件定義を行うことはできません。

### 移行 command

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

< 次ページに続く >



**match**

< 説 明 > マッチ条件を設定します。

QoS で利用(設定)可能な match 条件

< 説 明 > QoS で利用(設定)可能な match 条件は次のとおりです。  
IP address(class access-list)、tos 値、mark 値(IPv4)

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

QoS で利用(設定)可能な match 条件

< 説 明 > BGP4 で利用(設定)可能な match 条件は、次のとおりです。  
ip address(ip route access-list のみ)、nexthop address、med、as-path、origin

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

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

< 備 考 > ToS と Mark を同時に設定することは出来ません。  
match がない場合は、すべてが set の対象になります。  
deny で match した場合は、set の対象外になります。  
各機能でサポートしていない match 条件は無視されます。

#### set

<説明> QoS、BGP4 で使用する属性を設定します。

#### QoS で利用(設定)可能な属性

<説明> QoS で利用(設定)可能な属性は、次のとおりです。

tos 値、mark 値(IPv4 のみ)

<書式> set tos <0-255>  
set mark <1-4095>

#### BGP4 で利用(設定)可能な属性

<説明>

・BGP4 にて routemap を使用する場合、以下の attribute を設定することができます。

aggregator Century、as-path、atomic-aggregate、nexthop、local-preference、med、origin

<書式> set aggregator as <1-65535>  
set as-path prepend <1-65535>  
set atomic-aggregate  
set ip next-hop A.B.C.D  
set local-preference <0-4294967295>  
set metric <0-4294967295>  
set origin (egp|igp|incomplete)

<備考> ToS と Mark を同時に設定することが出来ます。  
各機能でサポートしていない属性の設定は無視されます。

#### class access-list および ip route access-list

class access-list と ip route access-list は、いずれも route-map の match 条件である match ip address 設定をフィルタリングする際に使用します。また、ip route access-list は BGP の distribute-list によるルートフィルタリングにも使用します。

class access-list と ip route access-list は、以下のように使い分けます。なお、設定については global node の class access-list および ip route access-list を参照してください。

#### class access-list

ToS 値や MARK 値を設定する set 条件をフィルタリングする場合

#### ip route access-list

BGP のパス属性に関する set 条件をフィルタリングする場合

BGP で distribute-list によるルートフィルタリングを行う場合

# 第 31 章

---

---

Web Authenticate node

#### 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。

#### 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

## 第31章 Web Authentication node

### Web Authentication node

#### アカウント管理

Basic 認証における username、password を本装置上で管理 / 認証する方法(ローカル認証)と、外部の RADIUS server に対して本装置から認証する方法(RADIUS 認証)があります。また、RADIUS 認証に失敗した場合にローカル認証を行うこともできます。

<書式> account authenticate (local|radius|radius-and-local)  
< No > no account authenticate  
<初期値> account authenticate local

#### ローカル認証

ローカル認証用の username、password を最大 64 組まで設定することができます。

<書式> account username USERNAME password (|hidden) PASSWORD  
< No > no account username USERNAME

#### RADIUS 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。

#### RADIUS 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。

## 第31章 Web Authentication node

### Web Authentication node

#### Idle timeout で使用する Attribute の指定

接続許可時間に idle timeout を指定している場合は、RADIUS server からの応答 Attribute の値を timeout として使うことができます。

```
< 書 式 > radius idle-timeout attribute
 (ascend-idle-limit|ascend-idle-limit-vsa|idle-limit)
ascend-idle-limit Ascend-Idle-Limit(Attribute Type=244)
ascend-idle-limit-vsa Ascend-Idle-Limit(Attribute Type=244、VSA Type=26、Vendor-ID=529)
idle-limit Idle-Timeout (Attribute Type=28)
< No > no radius idle-timeout attribute
```

#### Session timeout で使用する Attribute の指定

接続許可時間に session timeout を指定している場合は、RADIUS server からの応答 Attribute の値を timeout として使うことができます。以下の Attribute から選択してください。

```
< 書 式 > radius session-timeout attribute
 (ascend-maximum-time|ascend-maximum-time-vsa|session-timeout)
session-timeout Session-Timeout (Attribute Type=27)
ascend-maximum-time Ascend-Maximum-Time(Attribute Type=194)
ascend-maximum-time-vsa
 Ascend-Maximum-Time(Attribute Type=194、VSA Type=26、Vendor-ID=529)
< No > no radius session-timeout attribute
```

#### 全ての radius 設定を一括削除

全ての radius 設定を一括削除することができます。

```
< 書 式 > no radius
```

#### MAC アクセスリスト

Web 認証機能を有効にすると、外部との通信には認証が必要となりますが、mac access-list で指定した MAC アドレスを持つ PC については、認証を必要とせずに通信を許可または拒否することができます。

```
< 書 式 > mac access-list (permit|deny) HH:HH:HH:HH:HH:HH (|IFNAME)
< No > no mac access-list (permit|deny) HH:HH:HH:HH:HH:HH
```

#### Web 認証フィルタ

Web 認証フィルタを設定すると、ある特定の host や network、interface について Web 認証せずに通信が可能となります。Web 認証フィルタの設定条件については、global node の ip web-auth access-list を参照してください。Web 認証フィルタは、各 interface につき、IN/OUT をそれぞれ一つずつ設定することができます。interface への適用については、interface/tunnel/ppp node の ip webauth-filter を参照してください。

# 第 32 章

---

---

WarpLink node



## WarpLink 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
```

**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 | Succesed           | WarpLink Managerとの通信に成功              |
|         | Failed login       | アカウントの認証に失敗                          |
|         | Starting           | クライアント起動時に、WarpLink Managerにアクセスできない |
|         | Stopping           | クライアント停止時に、WarpLink Managerにアクセスできない |
|         | Failed registraion | WarpLink Managerからのレスポンスが不正          |
|         | Status error       | WarpLink Managerからのレスポンスが不正          |

# 第 33 章

---

---

Extended track IP reachability node

### Netevent 拡張機能(ip reachability)

#### Netevent 拡張機能(ip reachability)

Netevent 拡張機能を使用することによって、標準の track では指定できない option を指定することができます。Netevent 機能および拡張 track 設定についての詳細は、付録 F Netevent 機能を参照してください。

#### 移行 command

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

#### destination

< 説 明 > ip reachability における ping の宛先を IP アドレスまたは FQDN で指定します。  
< 書 式 > destination (A.B.C.D|FQDN)

#### source

##### interface

< 説 明 > ip reachability における ping の出力インタフェースを指定することができます。  
< 書 式 > source interface ethernet <0-2>  
source interface tunnel <0-255>  
source interface ppp <0-4>  
< No > no source

##### ip

< 説 明 > ip reachability における ping の送信元アドレスを指定することができます。  
< 書 式 > source ip A.B.C.D  
< No > no source

#### payload-length

< 説 明 >  
・ ip reachability における ping 送信時の size (icmp header は含まない) を指定することができます。  
< 書 式 > payload-length <56-1500>  
< 初 期 値 > payload-length 56  
< No > no payload-length

## 第33章 Extended track IP reachability node

### Netevent 拡張機能(ip reachability)

#### transmit

##### interval

<説明> ip reachabilityにおけるpingの送信間隔を指定することができます。

<書式> transmit interval <10-32767> (|variable)

<備考>

- ・variableを指定すると、ping NG発生時にpingの送信間隔を変化させることができます。Defaultは、無効です。

##### retries

<説明> ip reachabilityにおけるpingのretry回数を指定することができます。

<書式> transmit retries <0-255>

< No > no transmit retries

#### recovery

##### count

<説明> 指定した回数だけ連続でping OK となった場合に復旧と判断します。

<書式> recovery count <1-255>

<初期値> recovery count 1

< No > no recovery count

##### delay

<説明>

- ・ip reachability を利用する場合、復旧時(event up と判別した場合)から実際にup 時の action を実行するまでにdelay を設定することができます。

<書式> recovery delay <10-3600>

< No > no recovery delay

<備考>

- ・Delay timer が動作している場合は、trackはdown state が維持され、この間にもip reachability check は動作し続けます。
- ・Delay timer 動作中にevent downをretry回数検知した場合、delay timer はcancel されます。
- ・Delay timer がtimeoutすると、event upのactionが実行されます。このとき、delay timer中にカウントしたip reachability fail count は0にクリアされ、action実行後に再度reachability checkが開始されます。

## 第33章 Extended track IP reachability node

### Netevent 拡張機能(ip reachability)

#### set

##### df-bit

- <説明> ip reachabilityにおけるpingパケットにDF bitを設定することができます。
- <書式> set df-bit
- <初期値> set df-bit
- <No> no set df-bit

##### tll

- <説明>
- ・ip reachabilityにおけるpingパケットのTTLを指定します。Defaultは、systemのTTL値(64)をsetします。
- <書式> set tll <1-255>
- <初期値> set tll 64
- <No> no set tll

#### rtt

##### threshold

- <説明>
- ・ping requestを送信してから、replyを受信するまでの時間(Round trip time)の閾値を指定します。replyが返信されていても、指定した閾値内にreplyがない状態がrtt delay回数分連続した場合、rtt statusがdownとなります。Defaultでは、RTTの監視は行いません。

##### normal-count

- <説明> RTT status upと判断するまでのrtt正常回数です。Defaultは、3回です。

##### delay-count

- <説明> RTT status downと判断するまでの遅延回数です。Defaultは、3回です。

- <書式> rtt threshold <1-5000>  
rtt threshold <1-5000> normal-count <1-255> delay-count <1-255>
- <No> no rtt

#### netevent

##### threshold

- <説明> monitor-log機能でloggingを行うかどうかを指定します。
- <書式> netevent monitor-log-status
- <初期値> no netevent monitor-log-status (無効)
- <No> no netevent monitor-log-status

# 第 34 章

---

---

Extended track IPv6 reachability node

### Netevent 拡張機能(ipv6 reachability)

#### Netevent 拡張機能(ipv6 reachability)

Netevent 拡張機能を使用することによって、標準の track では指定できない option を指定することができます。Netevent 機能および拡張 track 設定についての詳細は、付録 F Netevent 機能を参照してください。

#### 移行 command

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

#### destination

< 説明 > ipv6 reachability における ping6 の宛先を IPv6 アドレスまたは FQDN で指定します。  
< 書 式 > destination (X:X::X:X|FQDN)

#### source

##### interface

< 説明 > ipv6 reachability における ping6 の出力インタフェースを指定することができます。  
< 書 式 > source interface ethernet <0-2>  
source interface tunnel <0-255>  
source interface ppp <0-4>  
< No > no source

##### ip

< 説明 > ipv6 reachability における ping6 の送信元アドレスを指定することができます。  
< 書 式 > source ip X:X::X:X  
< No > no source

#### payload-length

< 説明 >  
・ ipv6 reachability における ping6 送信時の size (icmpv6 header は含まない) を指定することができます。  
< 書 式 > payload-length <56-1500>  
< 初 期 値 > payload-length 56  
< No > no payload-length



## 第34章 Extended track IPv6 reachability node

### Netevent 拡張機能 (ipv6 reachability)

#### transmit

##### interval

<説明> ipv6 reachabilityにおけるping6の送信間隔を指定することができます。

<書式> transmit interval <10-32767> (|variable)

<備考>

- ・variableを指定すると、ping6 NG発生時にping6の送信間隔を変化させることができます。Defaultは、無効です。

##### retries

<説明> ipv6 reachabilityにおけるping6のretry回数を指定することができます。

<書式> transmit retries <0-255>

<No> no transmit retries

#### recovery

##### count

<説明> 指定した回数だけ連続でping6 OKとなった場合に復旧と判断します。

<書式> recovery count <1-255>

<初期値> recovery count 1

<No> no recovery count

##### delay

<説明>

- ・ipv6 reachability を利用する場合、復旧時(event up と判別した場合)から実際にup時のactionを実行するまでにdelayを設定することができます。

<書式> recovery delay <10-3600>

<No> no recovery delay

<備考>

- ・Delay timer が動作している場合は、trackはdown state が維持され、この間にも ipv6 reachability check は動作し続けます。
- ・Delay timer 動作中に event down を retry 回数検知した場合、delay timer はcancel されます。
- ・Delay timer がtimeoutすると、event upのactionが実行されます。このとき、delay timer中にカウントした ipv6 reachability fail count は0にクリアされ、action実行後に再度 reachability check が開始されます。

## 第 34 章 Extended track IPv6 reachability node

### Netevent 拡張機能(ipv6 reachability)

#### set

hop-limit

<説 明>

・ipv6 reachabilityにおけるping6パケットのhop limitを指定します。

<書 式> set hop-limit <1-255>

<初 期 値> set hop-limit 64

< No > no set hop-limit

#### rtt

threshold

<説 明>

・ping6 requestを送信してから、replyを受信するまでの時間(Round trip time)の閾値を指定します。replyが返信されていても、指定した閾値内にreplyがない状態がrtt delay回数分連続した場合、rtt statusがdownとなります。Defaultでは、RTTの監視は行いません。

normal-count

<説 明> RTT status upと判断するまでのrtt 正常回数です。Defaultは、3回です。

delay-count

<説 明> RTT status downと判断するまでの遅延回数です。Defaultは、3回です。

<書 式> rtt threshold <1-5000>

rtt threshold <1-5000> normal-count <1-255> delay-count <1-255>

< No > no rtt

#### netevent

threshold

<説 明> monitor-log機能でloggingを行うかどうかを指定します。

<書 式> netevent monitor-log-status

<初 期 値> no netevent monitor-log-status (無効)

< No > no netevent monitor-log-status

# 第 35 章

---

---

Monitor-log node

## ログ機能

Neteventip/ipv6 reachability 拡張機能による reachability 監視結果をログファイルとして保存する機能です。

- ・揮発性メモリ(内部メモリ)への保存と不揮発性メモリ(USB flashメモリ)へのバックアップを行いません。
- ・バックアップしたログ情報は、show monitor-log コマンド(view node 参照)でCLI 上に表示することができます。また、copy コマンド(view node 参照)で外部に取り出すことも出来ます。

### 揮発性メモリ(内部メモリ)への保存

内部メモリへは、reachability 監視ログとリソース監視ログを保存します。

#### (1) reachability 監視ログ

ログとして出力する情報は次のとおりです。なお、全ての監視結果をログとして出力するわけではありません。疎通結果が Dead/Delay の場合は毎回出力しますが、Alive の場合は他の状態から遷移した時にだけ出力します。

< 出力情報 >

- 1.TrackID  
Netevent 機能で定義した Track の ID を出力します。
2. 監視時刻  
DateAndTime 形式で出力します(ex. 2010-9-30,9:45:36.0)。
3. 監視先 IPv4 アドレス
4. 監視元 IPv4 アドレス
5. 監視先 IPv6 アドレス
6. 監視元 IPv6 アドレス
7. 空欄
8. 空欄
9. 空欄
10. 疎通結果(数字を出力)
  - 1: Alive(応答あり /RTT 閾値回復開始時のみ)
  - 2: Dead(応答なし)
  - 3: Delay(RTT 閾値超過)
11. ICMP Code/Type
12. 詳細情報(シーケンス番号、NextHop MTU)
- 13.RTT[msec]  
Trap 通知直前の RTT 取得情報
- 14 IPv6 ヘッダ送信元アドレス(疎通結果が Dead の場合)
- 15 IPv4 ヘッダ送信元アドレス(疎通結果が Dead の場合)

< 次ページに続く >

#### 揮発性メモリ(内部メモリ)への保存 (続き)

##### (2) リソース監視ログ

出力例および出力する情報は次のとおりです。

<出力例>

```
2010-10-5,18:15:15.0,0,133052,5
```

<出力情報>

##### 1. 出力時刻

DateAndTime形式で出力します(ex. 2010-9-30,9:45:36.0)。

##### 2. CPU使用率

最近3分の使用率を0～100[%]で出力します。

##### 3. メモリ空き容量[Kbyte]

##### 4. セッション数 (Connection Tracking 数)

0～最大セッション数(CLIから設定可能な最大セッション数)の範囲で出力します。

#### 不揮発性メモリ(USB Flashメモリ)へのバックアップ

##### (1) 定期バックアップ

「内部メモリへの保存」で保存された監視ログについて、最大ファイルサイズ(150～1000 Kbyte)を閾値として指定することができます。メモリ上のログファイルが監視間隔による判定時に、この条件(最大ファイルサイズ)に達した場合、メモリ上のログファイルを外部USB Flashメモリへバックアップ(gzip形式圧縮・移動)します。継続して出力されるログは新たにメモリ上に作成します。

定期バックアップは、スケジュール機能(global nodeのscheduleコマンドを参照してください)によって実行されます。

reachability監視およびリソース監視では、監視ログ出力時も閾値チェックを行い、バックアップ条件に達している場合にはバックアップを実行します。

##### (2) バックアップファイルの管理

定期バックアップのタイミングで、バックアップ対象ファイルを外部USB Flashメモリに移動します。USB Flashメモリに既に保存されているログファイル数が、設定した最大ファイル数(1～10世代まで)に達している場合は、最も古いファイルを削除してから、バックアップ対象ファイルをUSB Flashメモリに移動します。

なお、ファイル名はバックアップ時刻をもとに生成します。同一ファイル名が存在する場合は、新しいファイルで上書きします。

**移行 command**

```

nrx125#
nrx125#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nrx125(config)#monitor-log
nrx125(config-monitor-log)#

```

**reachability**

< 説 明 >

- ・ ping/ping6 による死活監視、遅延監視の結果を、ログ情報として内部メモリに保存します。

< 書 式 > reachability (disk0|disk1) (|threshold logsize <150-1000> files <1-10>)  
 reachability (disk0|disk1) threshold logsize <150-1000>  
 reachability (disk0|disk1) threshold files <1-10>

< 初 期 値 > no reachability

< No > no reachability

**resource**

< 説 明 > 本装置のシステムリソース情報を3分毎に定期的に監視して結果を出力します。

< 書 式 > resource (disk0|disk1) (|threshold logsize <150-1000> files <1-10>)  
 resource (disk0|disk1) threshold logsize <150-1000>  
 resource (disk0|disk1) threshold files <1-10>

< 初 期 値 > no resource

< No > no resource

< 備 考 >

- ・ 定期バックアップの取得先を(disk0|disk1 から)選択します。USB0 に接続された USB Flash メモリを指定する場合は、disk0 を選択します。USB1 に接続された USB Flash メモリを指定する場合は、disk1 を選択します。
- ・ logsize については、「定期バックアップ」を参照してください。
- ・ files については、「バックアップファイルの管理」を参照してください。

# 付録 A

---

---

設定事例

## . 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
```

```
!
```

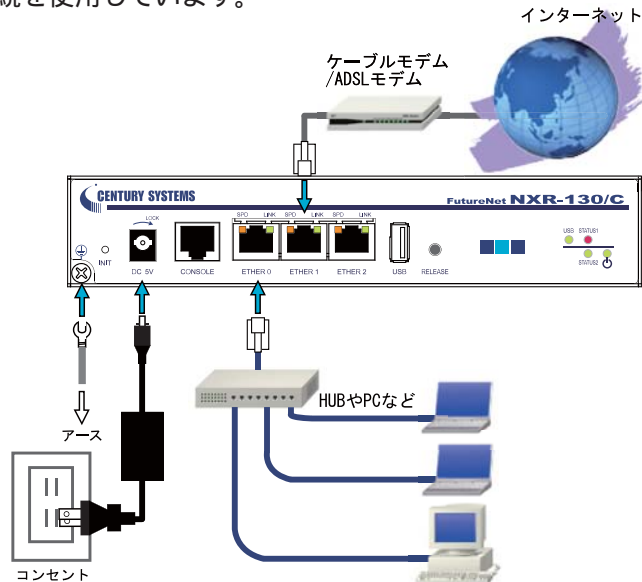
```
! ... 前後の設定表示は省略 ...
```

```
!
```



## . 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 XXXXXXXX.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
```

PPP 0 の接続名を OCNv6 に設定

```
description OCNv6
```

```
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 XXXXXX
```

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

## . 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)

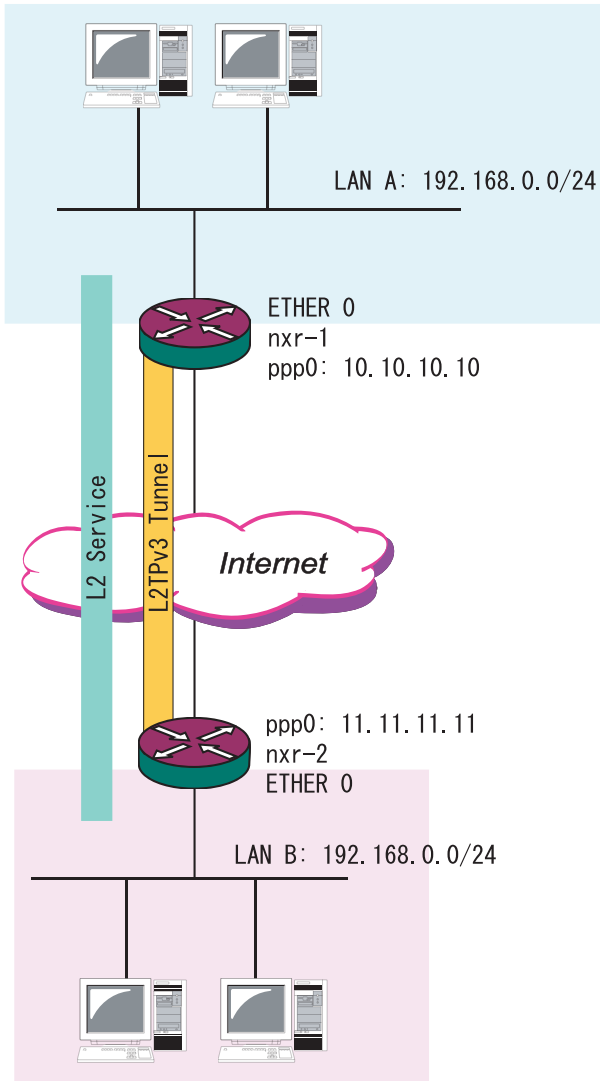
ip masquerade ppp1 インタフェースで IP マスカレードを有効に設定
ip spi-filter ppp1 インタフェースで SPI を有効に設定
ppp username XXXXXX password hidden XXXXXX PPP 接続のアカウント (ID とパスワード) を設定
!
interface ethernet 0
ip address 192.168.XXX.XXX/24 ethernet 0 インタフェースに IP アドレスを設定
ip access-group in netbios 入力フィルタで NetBIOS パケットを破棄(詳細は後述)
ip access-group 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

```

```
!
!
!
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 DHCPv6 のパケットを許可
!
!
```

## . 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 >

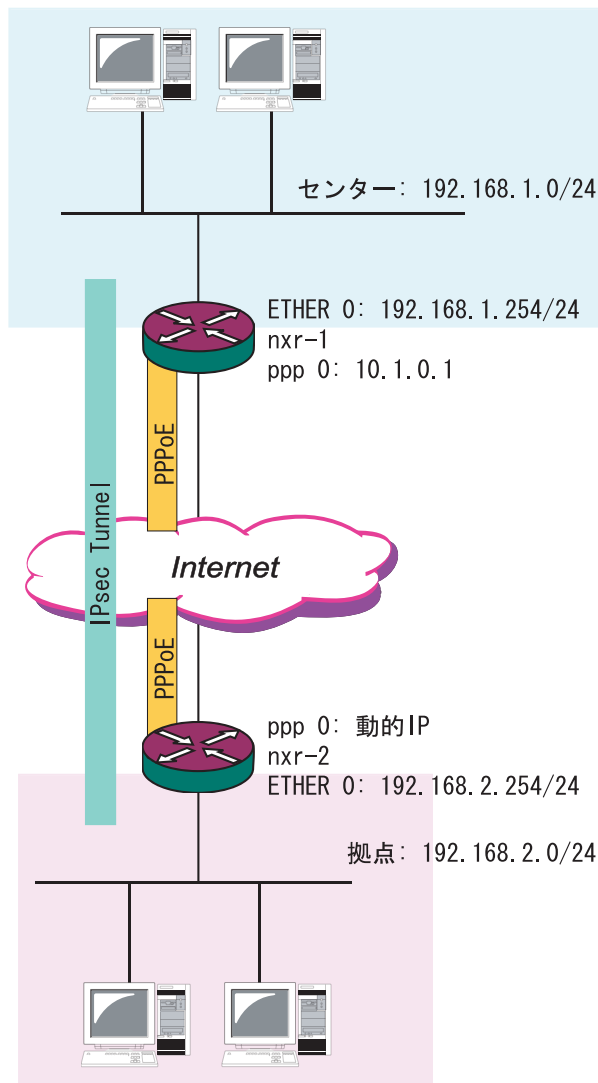
```
!
l2tpv3 hostname nxr1 本装置のホスト名
l2tpv3 router-id 192.168.200.254
 本装置の ID
!
l2tpv3 tunnel 1
description nxr1-nxr2
tunnel address 11.11.11.11
 対向 LCCE の WAN 側 IP アドレス
tunnel hostname nxr2 対向 LCCE のホスト名
tunnel router-id 192.168.200.253
 対向 LCCE の ID
!
l2tpv3 xconnect 1
description nxr1-nxr2
tunnel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

## . 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 >

## . IPsec の設定例

&lt; nxr-1 の設定 &gt;

```

!
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
!
!

```

## . IPsec の設定例

&lt; nxr-2 の設定 &gt;

```

!
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
!
!

```

## . 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](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
```

```
dial-up string *99***1#
```

```
mobile apn emb.ne.jp cid 1 pdp-type ip
```

```
...途中省略...
```

```
!
```

```
mobile 0 ppp 0
```

```
!
```

```
ip route 0.0.0.0/0 ppp 0
```

```
end
```

ユーザIDとパスワードを設定

cidが1なので、末尾を1#に設定

cidは1、pdp-typeはIP

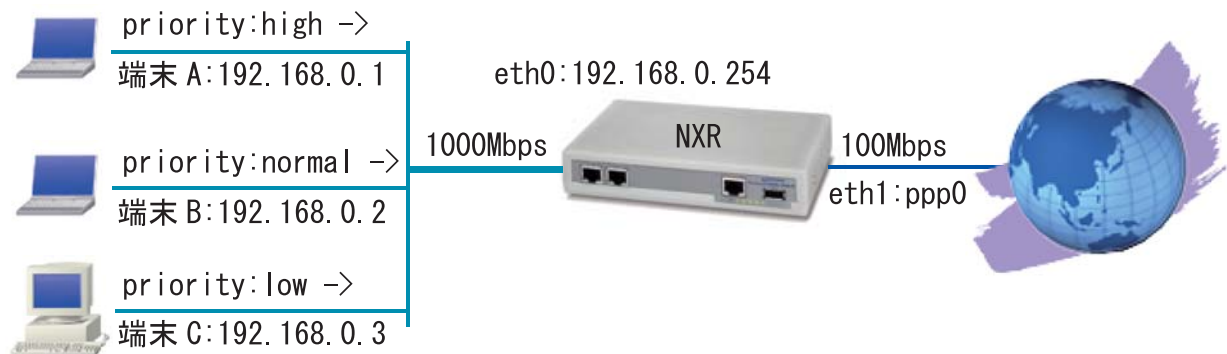
モバイル接続に ppp 0 を使用

IPv4のデフォルトルートを ppp0 に設定



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
 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)
!
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

## 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)

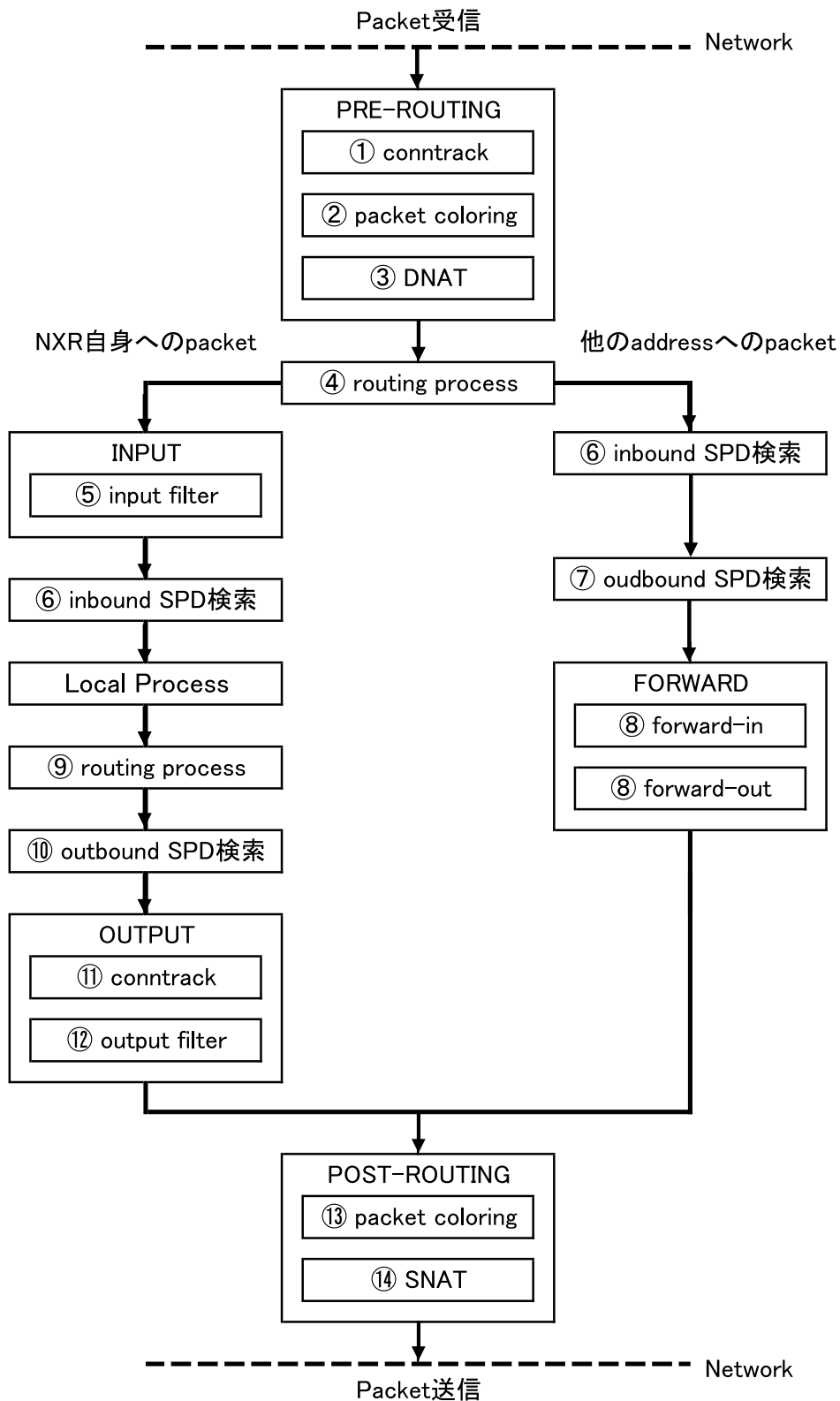
### OUTPUT

- (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。



## Packet forwarding 時

## - Packet 受信 -

## Contrack

contrack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。contrackテーブルは、session コマンド(global node)を使用して設定します。

## Packet coloring(input)

## Destination NAT

詳細は、NATの優先順位(INPUT)を参照してください。

## Routing Process

## 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されません。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。

## 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。

## Packet filtering

詳細は、IP filteringの優先順位(FORWARD)を参照してください。

## Packet coloring(output)

## 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 -

## Contrack

contrack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。contrackテーブルは、session コマンド(global node)を使用して設定します。

## Packet coloring(input)

## Destination NAT

詳細は、NATの優先順位(INPUT)を参照してください。

## Routing Process

## Packet filtering

詳細は、IP filteringの優先順位(INPUT)を参照してください。

## 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されません。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、 へ戻ります。

--> NXR local process

## Packet 送信時 (NXR が送信元)

- NXR Local Process が Packet 送出 -

Routing process

IPsec outbound SPD (注1) 検索

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。

output filter

詳細は、IP filtering の優先順位 (OUTPUT) を参照してください。

Packet coloring (output)

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

#### 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 (1280 bytes) 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 field 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
```

## 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)

## 付録 C Policy based IPsec と Route based IPsec

### . Route based IPsec

#### 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できます。

##### 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、負荷がかかることとなります。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<br>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/disable) と Fragment 設定 (pre-fragment/post-fragment) は、interface tunnel node で次のように設定します。

PMTUD 設定

< enable > tunnel path-mtu-discovery

< disable > no tunnel path-mtu-discovery

Fragment 設定

< pre-fragment > tunnel pre-fragment

< post-fragment > no tunnel pre-fragment

#### 2.4.4. IPsec interface で受信した fragment packet の reassemble の回避

Pre-fragment された packet を受信した場合に、NXR において reassemble するか、reassemble せずに forwarding するかを設定することができます。default は、有効です (reassemble します)。また、IPsec tunnel interface 上でのみ利用することができます。

<書式> ip fragment-reassembly

<初期値> ip fragment-reassembly (reassemble する)

<No> no ip fragment-reassembly (reassemble しない)

<備考>

- ・ reassemble しない場合、fragment されたまま packet の処理を行うため、conntrack による session 管理の対象外となります。そのため、conntrack を利用した機能 (NAT、SPI、session command で設定される各機能) との併用については、動作を保証していません。したがって、この機能を無効にする (reassemble しない) 場合は、制限事項について理解した上で十分にテストを行ってから使用するよう にしてください。

<制限事項>

- ・ 迂回 route から受信した場合に、invalid-status-drop として drop される場合があります。
- ・ filtering や packet coloring 処理においても、protocol や port 番号を指定した処理を行う場合は、fragment された 2 番目以降の packet に情報がいないため、2 番目以降の packet の filtering や packet coloring 処理は動作しません。このような場合は、IP header のみ (source/destination address など) で判断するように設定してください。

## 付録 C Policy based IPsec と Route based IPsec

### . Route based IPsec

#### 2.4.5. IPsec policy-ignore 機能

IPsec interface において、policy-ignore 機能を有効にした場合、route は IPsec interface ですが、policy が見つからないため、packet の処理ができずに drop されます。したがって、IPsec interface 上では ipsec policy-ignore 機能は有効にしないでください（「no ipsec policy-ignore (初期値)」にしてください）。

#### 2.4.6. Policy base と Route base IPsec の機能比較

Policy base/Route base それぞれの IPsec で利用可能 / 利用不可な機能の比較を table 2 に示します。

Table 2. Policy/Route base で利用可能な機能の比較

| 機能名                               | Policy Based IPsec    | Route Based IPsec                      |
|-----------------------------------|-----------------------|----------------------------------------|
| set route                         |                       | ×                                      |
| routingによるhandling                | ×                     |                                        |
| policy-ignore                     |                       | × (無効にしてください)                          |
| NAT                               | (SYSTEM NATで一部対応可能)   |                                        |
| filtering                         | ×                     |                                        |
| routing protocol (OSPF, RIPv1/v2) | ×                     |                                        |
| DF bitが1のpacketの強制fragment        |                       |                                        |
| pre/post-fragmentの選択              | × (post-fragmentのみ可能) |                                        |
| outer headerのカスタマイズ               | ×                     |                                        |
| IPv6 policy anyの利用                | ×                     |                                        |
| balancing                         | ×                     | (ECMPにより可能)<br>(Equal Cost Multi Path) |
| QoS                               | ×                     |                                        |

# 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、それぞれが一對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 が切れることによりのみ削除されます。

## 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。

## 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<br>(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 よりどれくらい増やすかを % 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。

$$\text{minimum soft timer} = \text{lifetime} - \text{margin}$$
$$\text{maximum soft timer} = \text{lifetime} - (\text{margin} + \text{margin} \times \text{increased-ratio}/100)$$

- 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

## 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できます。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できます。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)ackground/(n)o]: b -----
Unsaved configuration changes exist. Save Flash? [y/n]: y -----
```

After the firmware is updated, it reboots...

```
Firmware update is being executed.....
Finished the firmware update, it reboots... -----
```

Firmware 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。

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。

firmware update が終了すると、自動的に再起動が行われます。



### 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起動します。なお、認識できない XML タグは、無視されます (ログ表示もされません)。

# 付録 F

---

---

Netevent 機能

## Netevent 機能

USER が指定した監視対象の状態変化を検知した際に、PPP 回線の接続や IPsec SA の確立、VRRP priority の変更などの処理を行うことが出来ます。

Track object を追加した段階では、track の状態は up 状態となり、その後発生した event によって、down (または up) 状態へと遷移し、その track に関連づけられた action が実行されます。なお、すでに event down が発生している状態で、新規に監視対象や action を追加した場合、該当する down action が実行されます。

### 1. 監視対象(track object)の設定

#### 1.1 指定可能な監視対象

指定可能な監視対象は、以下のとおりです。

- interface link 状態監視  
interface の link 状態(up/down)を監視します。Keepalive が無効となっている interface に関しては、link down しないため、keepalive を有効にしてください。但し、PPP や tunnel interface のように interface の作成 / 削除ができるものに関しては、この限りではありません。
- IKE SA 状態監視  
IKE SA の状態(up/down)を監視します。
- ping/ping6 監視  
ping/ping6 による指定 host への ip reachability を監視します。
- VRRP 状態監視  
master から backup/init への変化、または backup/init から master への変化を監視します。
- OSPF neighbor 監視  
指定した router-id との neighbor 確立後から他の state への変化を監視します。
- BGP peer 監視  
指定した peer ip との neighbor 確立後から他の state への変化を監視します。

#### 1.2 監視対象削除時の動作

監視対象削除時、その track に関連づけられている action の復旧処理が実行されます。

なお、track 設定が無く action のみが設定されている場合、各 action が設定されているモジュール上では、action up の状態として処理されます。例えば、PPP interface 設定で、action として connect を指定している場合、初期の状態では自動接続は行われません(auto-connect が有効な場合でも)。

#### 1.3 ip/ipv6 reachability について

ip/ipv6 reachability の監視には、icmp/icmpv6 echo request/reply packet を使用します。

- Ping の timeout は、10sec です。
- Ping の送信間隔および retry 回数を指定することができます。なお、Ping の送信間隔は、echo request 送信後から次の echo request を送信するまでの時間です。echo reply が戻ってきてから、再度 timer が設定されるわけではありません。
- ip reachability に限り、出力 interface を指定することも可能です。

#### 1.4 Recovery delay timer 機能

ip/ipv6 reachability、ospf/bgp neighbor、interface link、isakmp を利用する場合、復旧時(event up と判別した場合)から実際に up 時の action を実行するまでに delay を設定することができます。Delay timer が動作している場合は、track は down state が維持され、この間にも各 check 動作は継続されます。

- Delay timer 動作中に event down を retry 回数検知した場合、delay timer は cancel されます。
- Delay timer が timeout すると、event up の action が実行されます。このとき、ip/ipv6 reachability check の場合は、delay timer 中にカウントした ip reachability fail count は 0 にクリアされ、action 実行後から再度 reachability check が開始されます。

#### 1.5 拡張 track 設定

netevent 拡張機能を使用すれば、標準の track では指定できない下記の option を指定することができます。拡張 track 設定は、ip/ipv6 reachability を使用する場合に有効です。

< 拡張 track のみで指定可能な option >

- payload-length  
ping/ping6 送信時の size (icmp header は含まない) を指定することができます。Default は、56byte です。
- 復旧回数  
指定した回数、連続で ping/ping6 OK となった場合に復旧と判断します。Default は、1 です。
- RTT  
ping/ping6 request を送信してから、reply を受信するまでの時間 (Round trip time) の閾値を指定します。指定した閾値内に reply がない状態が、rtt delay 回数分連続した場合 (reply は返信されている)、rtt status が down となります。Default では、RTT の監視は行われません。
- RTT delay 回数  
RTT status down と判断するまでの遅延回数です。Default は、3 回です。
- RTT normal 回数  
RTT status up と判断するまでの rtt 正常回数です。Default は、3 回です。
- DF  
IPv4 の場合のみ指定することができます。Default で、DF が set されます。
- TTL/hop-limit  
TTL (IPv6:hoplimit) を指定します。Default は、system の TTL 値 (64) が set されます。
- monitor-log  
monitor-log 機能で logging を行うかどうかを指定します。Default は、無効です。
- interval variable mode 指定  
ping/ping6 の送信間隔を、ping error 発生時に変化させるかどうかを指定します。Default は、無効です。

### 1.5.1 RTT status

RTTの状態を指します。

- ・RTTが閾値を超えた状態がRTT delay回数分連続した場合、rtt statusがdownとなり、RTT normalが回数分連続した場合、up状態へと遷移します。Defaultはupとし、rtt statusの状態変化によりactionは実行されません。
- ・なお、pingがNGとなった場合は、rttの正常/異常連続回数は0にresetされます。また、trackがdownになるとrtt statusはINIT状態へと遷移します。

### 1.5.2 Interval variable mode

ip/ipv6 reachability 指定時、常に設定された interval 間隔で監視を行いますが、この mode を有効にすると、track 状態に連動して interval 間隔が変化します。Default は、無効です。

- ・track up 状態で ping fail を検知すると、interval 間隔が小さくなるため、障害の検出を早く行うことができます。
- ・通常時は、interval 間隔を長めに設定することで、ping/ping6 による負荷を軽減することが可能となります。

interval の計算方法

Interval の計算方法は次のとおりです。なお、interval の最小値は 10sec のため、下記計算により 10 以下の値となった場合は、10sec 間隔で監視されます。

$$v\_interval = (interval / 2^{fail\_cnt}) \quad (2 \text{ のべき乗})$$

v\_interval : 変更後の interval

interval : 設定されている interval

fail\_cnt : 連続で ping fail となった回数

各 track 状態での interval について

track 状態と interval の関係は、次のとおりです。

- ・track up で ping OK の場合は、interval で監視されます。
- ・track up 状態で ping fail を検知すると v\_interval で監視が行われます。
- ・track down の場合は、fail\_cnt = retry 回数 + 1 として計算された v\_interval 間隔で監視が行われます。
- ・delay timer が起動した場合、track up の場合と同様に interval で監視され、Ping fail を検知すると、v\_interval で監視が行われます。

### 1.6 Initial timeout 設定

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

- ・neighbor が確立(あるいは interface link up)状態と判断されると track up 状態となります。
- ・neighbor が確立されていない(あるいは interface link down)状態の場合、すぐに track down 状態とはなりません。この場合は、initial timeout が timeout するか、OSPF/BGP4 機能 / interface 状態監視機能によって down の状態変化通知があったときに、track down として判断し、down action を実行します。
- ・Initial timeout は、default で無効です。有効時の default の initial timeout 値は 180sec です。なお、initial timeout 値は、10 ~ 3600sec の範囲で設定することが出来ます。

## 2 actionの設定

### 2.1 指定可能な action

指定可能な action は、次のとおりです。

- ・ VRRP Priority を指定値に変更
- ・ IPsec tunnel の確立 / 削除 / 再接続 (isakmp 単位での指定)
- ・ PPP の接続 / 切断
- ・ Tunnel interface の up/down
- ・ L2TPv3 tunnel の接続 / 切断 (PPP の interface link 監視のみ対応)
- ・ IPsec local policy の変更 (IPsec isakmp policy にて設定)
- ・ IPsec isakmp policy の変更 (IPsec tunnel policy にて設定)

また、監視対象と event 発生時の動作対象が同じ場合、復旧の動作ができないため、監視対象と event 発生時の動作対象で同じものを設定しないでください。次のように設定した場合、master へ復帰することができなくなります。

```
interface ethernet 0
 ip address 192.168.0.254/24
 vrrp ip 1 address 192.168.0.1
 vrrp ip 1 netevent 1 priority 10
 !
 track 1 vrrp ip 1 interface ethernet 0
```

### 2.2 Reconnect action

ISAKMP policy のみ action として、reconnect を指定することができます。reconnect を指定した場合、event down を detect すると IKE/IPsec SA を削除し、再 negotiation を開始します。event up 時は、何も実行しません。

### 2.3 Change action

IPsec isakmp policy の local policy 指定、および IPsec tunnel policy の set key-exchange 指定にて、設定することができる action です。

IPsec isakmp/tunnel で使用する local policy/isakmp policy の track 状態によって変更することができます。この機能により、障害に応じて、1 つの IPsec 設定にて main/backup の構成を取ることができます。なお、IPsec isakmp policy にて local policy の change を行う場合で、かつ PSK を使用する場合は、変更前の ID と変更後の ID は、同じ ID を使用してください。

### 2.4 action 追加時の動作

Action 追加時は、track object の状態が down の場合に action を実行します。

### 2.5 action 削除時の動作

Action 削除時は、その module において netevent がない場合と同じ動作を実行します。Action 復旧処理を実行するわけではありません。

## 3 システム起動中に発生した event に対する action の実行

システム起動中に該当する track の状態変化を検知した場合、システム起動処理が完了してから発生した event に伴う action を実行します。

# 付録 G

---

---

サポートについて

## 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/CX 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 v5.10.0 対応版  
FutureNet NXR-130/CX ユーザーズガイド CLI 編 v5.5.5 対応版  
FutureNet NXR-1200 ユーザーズガイド CLI 編 v5.8.2 対応版

---

2010年11月版

発行 センチュリー・システムズ株式会社

Copyright (c) 2009-2010 Century Systems Co., Ltd. All rights reserved.

---