# FutureNet NXR シリーズ

# ユーザーズガイド CLI 編

Ver.26.x 対応版／2026 年 11 月更新版

CENTURY SYSTEMS

# 目次


はじめに ..... 4
第1章　本装置の概要 ..... 5
　Ⅰ. 本装置の特長 ..... 6
　Ⅱ. 各部の名称と機能 ..... 7
　　◆ NXR-535 ..... 7
　　◆ NXR-G540 ..... 10
　　◆ NXR-G540/L-CA ..... 15
　　◆ NXR-G540/LW-CA ..... 21
　　◆ NXR-G540/W ..... 21
　Ⅲ. 動作環境 ..... 27
第２章　装置の設置 ..... 28
　Ⅰ. 装置の設置に関する注意点 ..... 29
　Ⅱ. 装置の設置 ..... 30
　　◆ NXR-535 ..... 30
　　◆ NXR-G540 シリーズ ..... 31
第３章　設定方法の概要 ..... 32
　Ⅰ. 本装置へのログイン(CLI) ..... 33
　　◆ Console 接続: NXR-535 ..... 34
　　◆ Console 接続: NXR-G540 シリーズ ..... 35
　　◆ Console 接続: NXR シリーズ共通 ..... 36
　　◆ SSH 接続: NXR シリーズ ..... 38
　Ⅱ. 本装置へのログイン(GUI) ..... 40
　Ⅲ. コマンド実行モード ..... 44
　Ⅳ. コマンド入力時の補助機能 ..... 45
　Ⅴ. 本装置のモード構造 ..... 47
　Ⅵ. パスワード(初期値)の変更 ..... 49
　Ⅶ. SPI フィルタの設定 ..... 50
第４章　view(exec) mode ..... 51
第５章　global mode ..... 96
第６章　interface mode ..... 182
第７章　interface tunnel mode ..... 222
第８章　interface ppp mode ..... 243
第９章　dns mode ..... 271
第10章　l2tp mode ..... 275
第11章　l2tpv3-tunnel mode ..... 281
第12章　l2tpv3-xconnect mode ..... 285
第13章　l2tpv3-group mode ..... 290
第14章　rip mode ..... 293
第15章　ospf mode ..... 296
第16章　bgp mode ..... 301
第17章　ntp mode ..... 311
第18章　SNMP mode ..... 314
第19章　syslog mode ..... 320
第20章　dhcp-server mode ..... 327
第21章　dhcp-relay mode ..... 330
第22章　ipsec local policy mode ..... 332
第23章　ipsec isakmp policy mode ..... 335
第24章　ipsec tunnel policy mode ..... 348
第25章　UPnP mode ..... 354
第26章　QoS (class-policy) mode ..... 356
第27章　QoS (class-filter) mode ..... 363
第28章　CRP client mode ..... 365
第29章　route-map mode ..... 368
第30章　Web Authenticate mode ..... 374
第31章　WarpLink mode ..... 382
第32章　Extended track IP reachability mode ..... 385
第33章　Extended track IPv6 reachability mode ..... 389
第34章　Monitor-log mode ..... 393
第35章　mail server mode ..... 398
第36章　interface bridge mode ..... 402

第37章 DDNS mode ..... 428
第38章 access-server profile mode ..... 433
第39章 interface virtual-template mode ..... 435
第40章 ngn-sip client mode ..... 442
第41章 ngn-sip server mode ..... 444
第42章 ipv6 dhcp-server mode ..... 446
第43章 ipv6 dhcp-client mode ..... 449
第44章 l2tpv3 access-list mode ..... 454
Ⅰ. L2TPv3 フィルタリング機能 ..... 455
Ⅱ. Root ACL ..... 459
Ⅲ. Layer2 ACL ..... 460
Ⅳ. Extended IP ACL ..... 461
Ⅴ. Extended IPv6 ACL ..... 463
Ⅵ. Extended VLAN ACL ..... 464
Ⅶ. Extended ARP ACL ..... 465
Ⅷ. Extended IEEE802.3 ACL ..... 466
第45章 address-family ipv6 mode ..... 467
第46章 terminal-server mode ..... 472
第47章 LXC container mode ..... 475
第48章 interface veth mode ..... 479
第49章 interface tap mode ..... 481
第50章 ssl tunnel mode ..... 485
第51章 Web authentication extension mode ..... 488
第52章 dns-intercept mode ..... 493
第53章 interface MAP mode ..... 497
第54章 interface WWAN mode ..... 506
第55章 Event Notification Service mode ..... 519
第56章 interface wlan mode ..... 522
第57章 wifi mode ..... 550
第58章 management-server mode ..... 555
第59章 Warplink-SPS mode ..... 566
第60章 Speed test mode ..... 569
第61章 DIO mode ..... 571
第62章 interface wireguard mode ..... 574
第63章 Wireguard mode ..... 578
第64章 RIPng mode ..... 580
第65章 OSPFv3 mode ..... 583
付録 A Packet Traveling ..... 587
付録 B Policy based IPsec と Route based IPsec ..... 593
I. Policy based IPsec ..... 594
II. Route based IPsec ..... 597
付録 C IKEv2 Protocol ..... 603
付録 D Firmware update ..... 611
付録 E Netevent 機能 ..... 615
付録 F VRRP ..... 621
付録 G Config の保存と復帰 ..... 624
Ⅰ. Config の保存 ..... 625
Ⅱ. Config の復帰 ..... 626
Ⅲ. Config の保存形式 ..... 627
Ⅳ. INIT ボタン押下による起動時の制限 ..... 628
付録 H 拡張 flash 管理仕様 ..... 629
付録 I RAS 機能 ..... 634
付録 J データコネクト ..... 637
付録 K Policy Based Routing(PBR) ..... 641
付録 L P2P 検出機能について ..... 644
付録 M VLAN ..... 647
Ⅰ. VLAN 仕様 ..... 648
Ⅱ. ポートベース VLAN ..... 650
Ⅲ. マルチプル VLAN ..... 653
Ⅳ. タグ VLAN(VLAN トランク) ..... 656
付録 N サポートについて ..... 659

# はじめに

**◆ ご注意**

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

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

3. 本書の内容の一部または全部を無断で転載、複写することを禁じます。

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

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

**◆ 商標の表示**

- 「FutureNet」はセンチュリー・システムズ株式会社の登録商標です。
- その他の記載されている商品名、会社名は、各社の商標または登録商標です。

# 第1章　本装置の概要

# Ⅰ. 本装置の特長

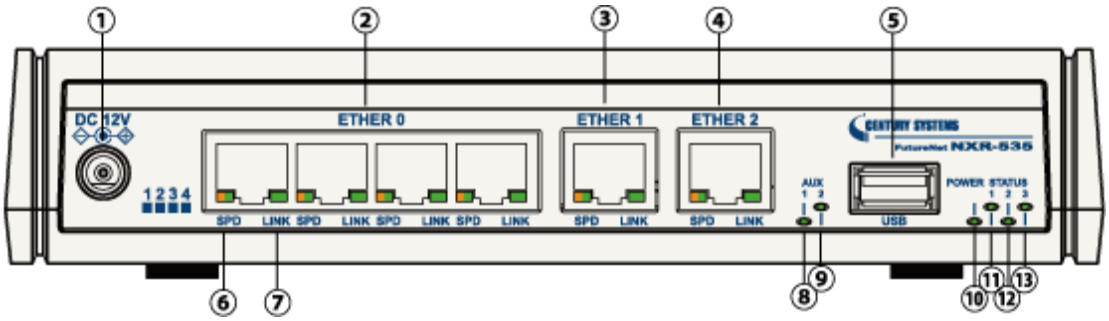
FutureNet NXR シリーズの「製品概要」、「製品の特徴」、「仕様」等については、弊社の Web サイトを参照してください。

- FutureNet NXR-535
  - https://www.centurysys.co.jp/products/router/nxr535.html
- FutureNet NXR-G540
  - https://www.centurysys.co.jp/products/router/nxrg540 s.html

# Ⅱ. 各部の名称と機能

## ◆ NXR-535

### ■ 製品前面




**① DC 12V 電源コネクタ**
製品付属の AC アダプタを接続します。

**② ETHER 0 ポート**
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポートです。主に LAN 側ポートとして使用します。

**③ ETHER 1 ポート**
**④ ETHER 2 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。

**⑤ USB 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。

**⑥ SPD LED**
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　：●

**⑦ LINK LED**
ETHER ポートの LINK 状態を示します。
Link Up 時　：●
Link Down 時　：●

**⑧ AUX 1 LED**
**⑨ AUX 2 LED**
データ通信端末装着時に、電波状況を表示します。

| Signal Level | ：⑧ | ⑨ |
|---|---|---|
| 圏外 | ：● | ● |
| 0-1 | ：● | ● |
| 2 | ：● | ● |
| 3 | ：● | ● |

### ⑩ POWER LED

本装置の電源状態を示します。

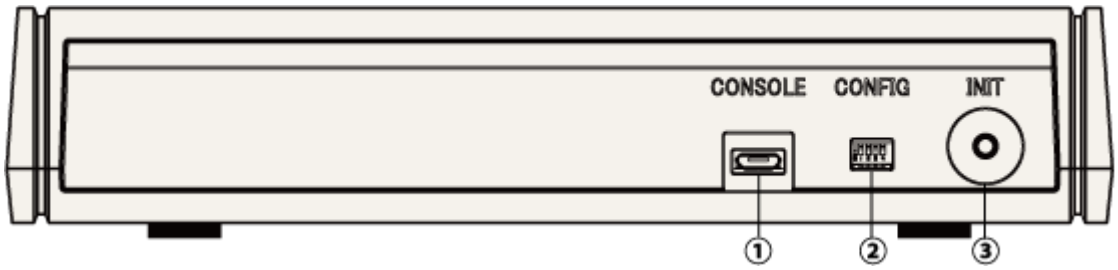
| | |
|---|---|
| 電源投入時 | : 🟡 |
| システム起動中 | : 🟢 |
| システム起動後(ログイン可能状態) | : 🟢 |

### ⑪ STATUS 1 LED
### ⑫ STATUS 2 LED
### ⑬ STATUS 3 LED

本装置のシステムおよび、サービスのステータスを示します。

| システムおよびサービスのステータス | LED の表示<br>⑩⑪⑫⑬ |
|---|---|
| 電源投入時 | :🟢－－－ |
| システム起動中 | :🟢＊－－ |
| システム起動後(ログイン可能状態) | :🟢🟢－－ |
| PPP/Tunnel 等の切断状態(configurable) | :－－●－ |
| PPP/Tunnel 等の接続状態(configurable) | :－－🟢－ |
| SD カード未装着時 | :－－－● |
| SD カード装着時 | :－－－🟢 |
| 温度異常(warning) | :＊－－－ |
| 温度異常(critical) | :🔴－－－ |
| ファームウェア更新中 | :－＊－－ |
| ファームウェア更新失敗 | :－🔴－－ |
| システム異常 | :●🔴🔴－ |
| システム停止(shutdown 状態) | :●＊＊＊ |

■ **製品背面**

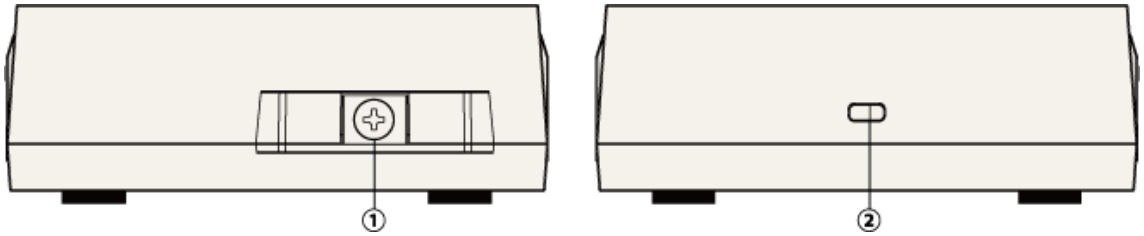



**① CONSOLE**
CLI 接続の際に使用します。
USB ケーブル(USB 2.0 Micro B)を接続します。

**② CONFIG**
すべてのスイッチが、上に位置している状態(上上上上)で使用してください。

**③ INIT**
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、緑点滅(＊)を開始するまで、INIT ボタンを押したままにします。
3. STATUS1 LED が、緑点滅(＊)を開始したら、すみやかに INIT ボタンを放します。本装置が工場出荷状態で起動します。

■ **製品側面**

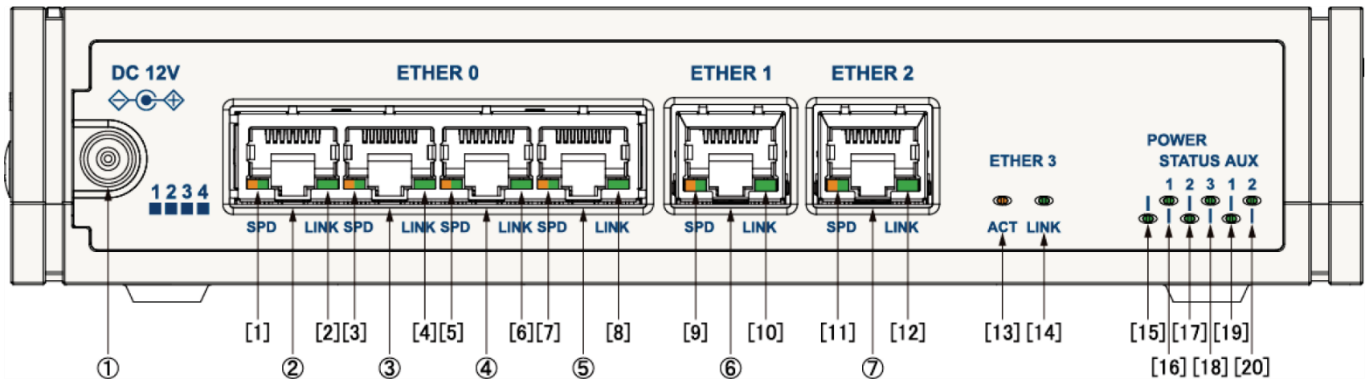



**① FG(アース)端子**
保安用接続端子です。必ずアースを接続してください。

**② セキュリティスロット**
ケンジントンロックに対応しています。

## ◆ NXR-G540

### ■ 製品前面




**① DC 12V 電源ポート**
製品付属の AC アダプタを接続します。

**② ETHER 0 (ETHER 0/0)ポート**
**③ ETHER 0 (ETHER 0/1)ポート**
**④ ETHER 0 (ETHER 0/2)ポート**
**⑤ ETHER 0 (ETHER 0/3)ポート**
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポート(4 ポートハブ)です。

**⑥ ETHER 1 ポート**
**⑦ ETHER 2 ポート**
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポートです。

**[1] SPD LED (ETHER 0/0)**
**[3] SPD LED (ETHER 0/1)**
**[5] SPD LED (ETHER 0/2)**
**[7] SPD LED (ETHER 0/3)**
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 ：●

**[9]　SPD LED (ETHER 1)**
**[11] SPD LED (ETHER 2)**
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 ：●

**[2]　LINK LED (ETHER 0/0)**
**[4]　LINK LED (ETHER 0/1)**
**[6]　LINK LED (ETHER 0/2)**
**[8]　LINK LED (ETHER 0/3)**
**[10] LINK LED (ETHER 1)**
**[12] LINK LED (ETHER 2)**
ETHER ポートの LINK 状態を示します。
　　Link Up 時　　：●
　　Link Down 時　　：●

[13] ACT LED(ETHER 3)
SFP モジュールの着脱状態を表示します。
装着時　：●
未装着時：●

[14] LINK LED(ETHER 3)
SFP ポートのリンク状態を表示します。
Link Up 時　：●
Link Down 時：●

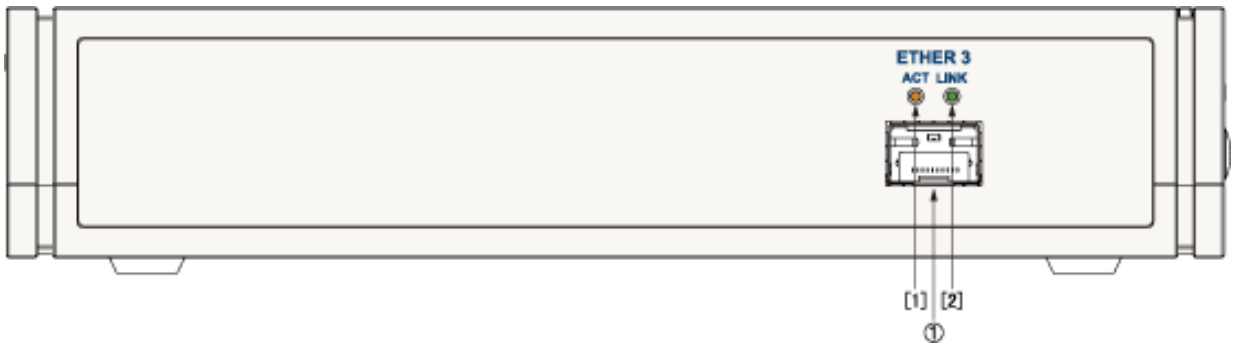
[15] POWER LED
本装置の電源状態を示します。
　電源投入時　　：●
　システム起動中：●
　システム起動後(ログイン可能状態)：●

[16] STATUS 1 LED
[17] STATUS 2 LED
[18] STATUS 3 LED
本装置のシステム、およびサービスのステータスを示します。
システムおよびサービスのステータス :LED の表示

| | | [15] | [16] | [17] | [18] |
|---|---|---|---|---|---|
| 電源投入時 | : | ● | － | － | － |
| システム起動中 | : | ● | ＊ | － | － |
| システム起動後(ログイン可能状態) | : | ● | ● | － | － |
| PPP/Tunnel 等の切断状態(configurable) | : | － | － | ● | － |
| PPP/Tunnel 等の接続状態(configurable) | : | － | － | ● | － |
| 温度異常(warning) | : | ＊ | － | － | － |
| 温度異常(critical) | : | ● | － | － | － |
| ファームウェア更新中 | : | － | ＊ | － | － |
| ファームウェア更新失敗 | : | － | ● | － | － |
| システム異常 | : | ● | ● | ● | － |
| 省電力モード(サスペンド) | : | ● | ＊ | ＊ | ＊ |

[19] AUX 1 LED
[20] AUX 2 LED
指定した ppp/tunnel 等の状態を示します。
　接続状態　：●
　切断状態　：●
設定は、system led aux コマンド(global mode)を参照してください。

■ 製品背面

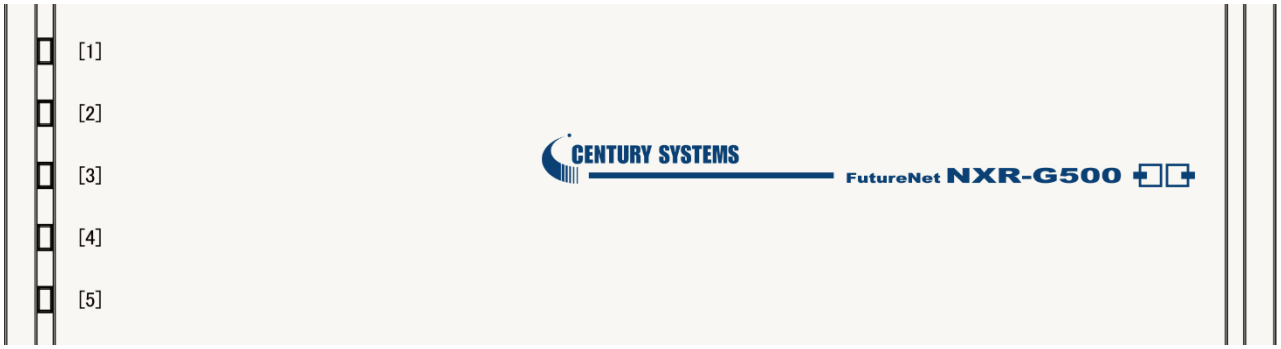



① ETHER 3 ポート(SFP コネクタ)
小型 ONU、1000BASE-SX／1000BASE-LX／1000BASE-T SFP トランシーバに対応した Ethernet ポートです。

[1] ACT LED (ETHER 3)
SFP モジュールの着脱状態を表示します。
装着時　：●
未装着時：●

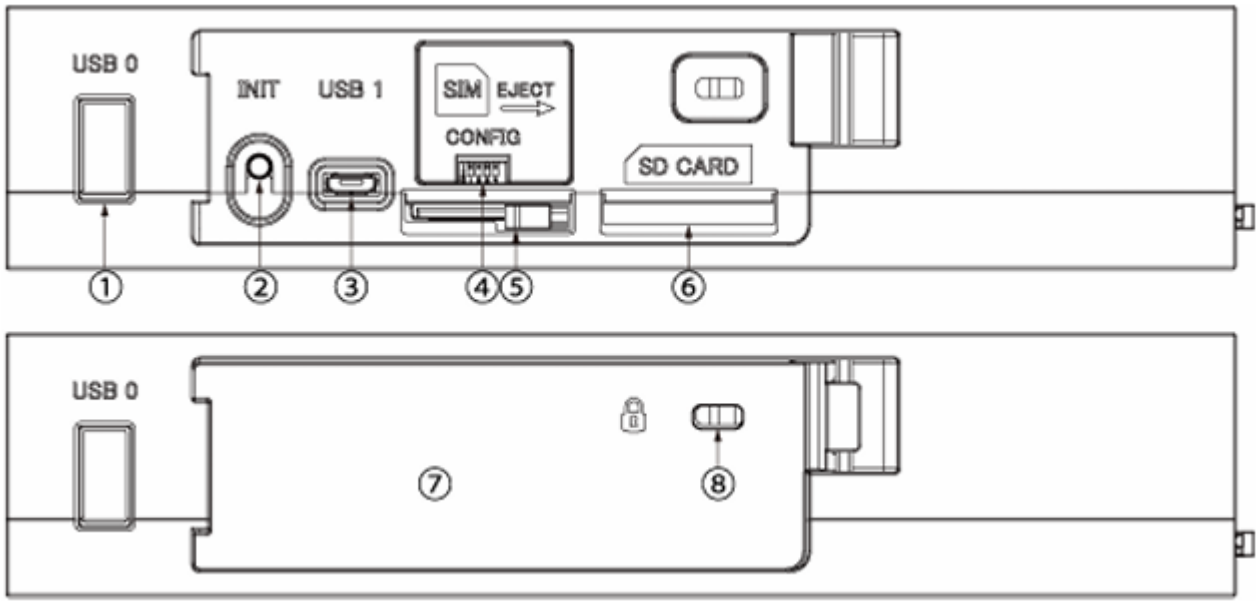
[2] LINK LED(ETHER 3)
SFP ポートのリンク状態を表示します。
Link Up 時　：●
Link Down 時：●

■ 製品上面




[1] -
[2] -
[3] -
[4] -
[5] -
本装置では使用しません。

■ **製品側面**




**① USB 0 ポート**
USB2.0 対応の USB(USB Type-A)ポートです。
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。

**② INIT スイッチ**
本装置を工場出荷時の設定に戻して起動するときに使用します。
1. INIT ボタンを押しながら電源を投入します。
2. STATUS1 LED が、緑点滅(＊)を開始するまで、INIT ボタンを押したままにします。
3. STATUS1 LED が、緑点滅(＊)を開始したら、すみやかに INIT ボタンを放します。本装置が工場出荷状態で起動します。

**③ USB 1 ポート**
コンソールポートです。CLI 接続の際に使用します。
USB ケーブル(USB 2.0 microB)を接続します。

**④ CONFIG スイッチ**
すべてのスイッチが上に位置している状態(上上上上)で使用してください。

**⑤ SIM カードスロット**
5G/LTE SIM カード用スロットです。

**⑥ SD カードスロット**
本装置では使用しません。

**⑦ サイド・カバー**
②～⑥の機能を使用するときに取り外します。

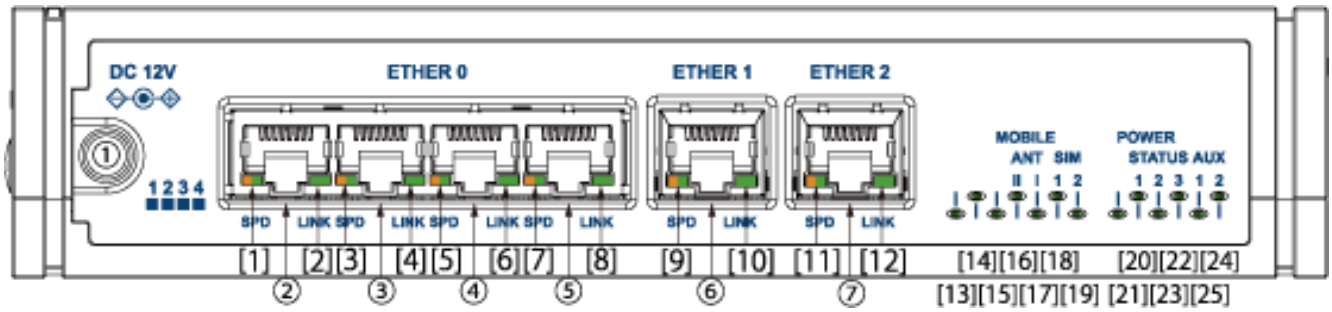
**⑧ セキュリティスロット**
ケンジントンロック(T バーロックタイプ)に対応しています




**① FG(アース)端子**
保安用接続端子です。本機器を使用する場合はアース線を接続します。

## ◆ NXR-G540/L-CA

### ■ 製品前面




**① DC 12V 電源ポート**
製品付属の AC アダプタを接続します。

**② ETHER 0 (ETHER 0/0)ポート**
**③ ETHER 0 (ETHER 0/1)ポート**
**④ ETHER 0 (ETHER 0/2)ポート**
**⑤ ETHER 0 (ETHER 0/3)ポート**
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポート(4 ポートハブ)です。

**⑥ ETHER 1 ポート**
**⑦ ETHER 2 ポート**
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポートです。

**[1] SPD LED (ETHER 0/0)**
**[3] SPD LED (ETHER 0/1)**
**[5] SPD LED (ETHER 0/2)**
**[7] SPD LED (ETHER 0/3)**
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：●

**[9] SPD LED (ETHER 1)**
**[11] SPD LED (ETHER 2)**
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：●

**[2] LINK LED (ETHER 0/0)**
**[4] LINK LED (ETHER 0/1)**
**[6] LINK LED (ETHER 0/2)**
**[8] LINK LED (ETHER 0/3)**
**[10] LINK LED (ETHER 1)**
**[12] LINK LED (ETHER 2)**
ETHER ポートの LINK 状態を示します。
Link Up 時　：●
Link Down 時　：●

**[13] -**
**[14] -**
本装置では使用しません。

**[15] MOBILE LED**
モバイルモジュールのステータスを示します。
モジュール停止　：●
モジュール起動　：●
PPP 接続時　　：●

**[16] MOBILE ANT II LED**
**[17] MOBILE ANT I LED**
モバイルの電波状態を示します。

| | 圏外 | 1 | 2 | 3 |
|---|---|---|---|---|
| [16] | ● | ● | ● | ● |
| [17] | ● | ● | ● | ● |

**[18] MOBILE SIM1 LED**
**[19] MOBILE SIM2 LED**
SIM1, SIM2 の状態を示します。
SIM 装着＋選択中　　：●
SIM 装着＋選択なし　：●
SIM 未装着＋選択中　：＊
SIM 未装着＋選択なし　：●
SIM 装着(異常)　　：●
※選択中とは、当該 SIM が、動作対象となっている状態です。

**[20] POWER LED**
本装置の電源状態を示します。
電源投入時　　：●
システム起動中：●
システム起動後(ログイン可能状態)：●

**[21] STATUS 1 LED**
**[22] STATUS 2 LED**
**[23] STATUS 3 LED**
本装置のシステム、およびサービスのステータスを示します。
**システムおよびサービスのステータス :LED の表示**

| | [20] | [21] | [22] | [23] |
|---|---|---|---|---|
| 電源投入時 | ● | － | － | － |
| システム起動中 | ● | ＊ | － | － |
| システム起動後(ログイン可能状態) | ● | ● | － | － |
| PPP/Tunnel 等の切断状態(configurable) | － | － | ● | － |
| PPP/Tunnel 等の接続状態(configurable) | － | － | ● | － |
| 温度異常(warning) | ＊ | － | － | － |
| 温度異常(critical) | ● | － | － | － |
| ファームウェア更新中 | － | ＊ | － | － |
| ファームウェア更新失敗 | － | ● | － | － |
| システム異常 | ● | ● | ● | － |
| 省電力モード(サスペンド) | ● | ＊ | ＊ | ＊ |

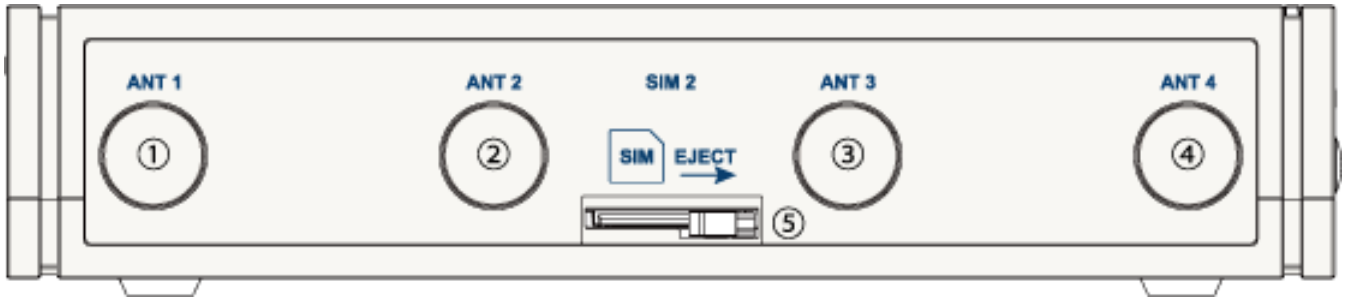
**[24] AUX 1 LED**
**[25] AUX 2 LED**

指定した ppp/tunnel 等の状態を示します。

接続状態　　：●
切断状態　　：●

設定は、system led aux コマンド（global mode）を参照してください。

■ 製品背面




① ANT 1
5G/LTE 用アンテナと接続するためのコネクタ(SMA コネクタ)です。
② ANT 2
本装置では使用しません。
③ ANT 3
本装置では使用しません。
④ ANT 4
5G/LTE 用アンテナと接続するためのコネクタ(SMA コネクタ)です。
⑤ SIM 2
5G/LTE SIM カード用スロットです。

■ 製品上面



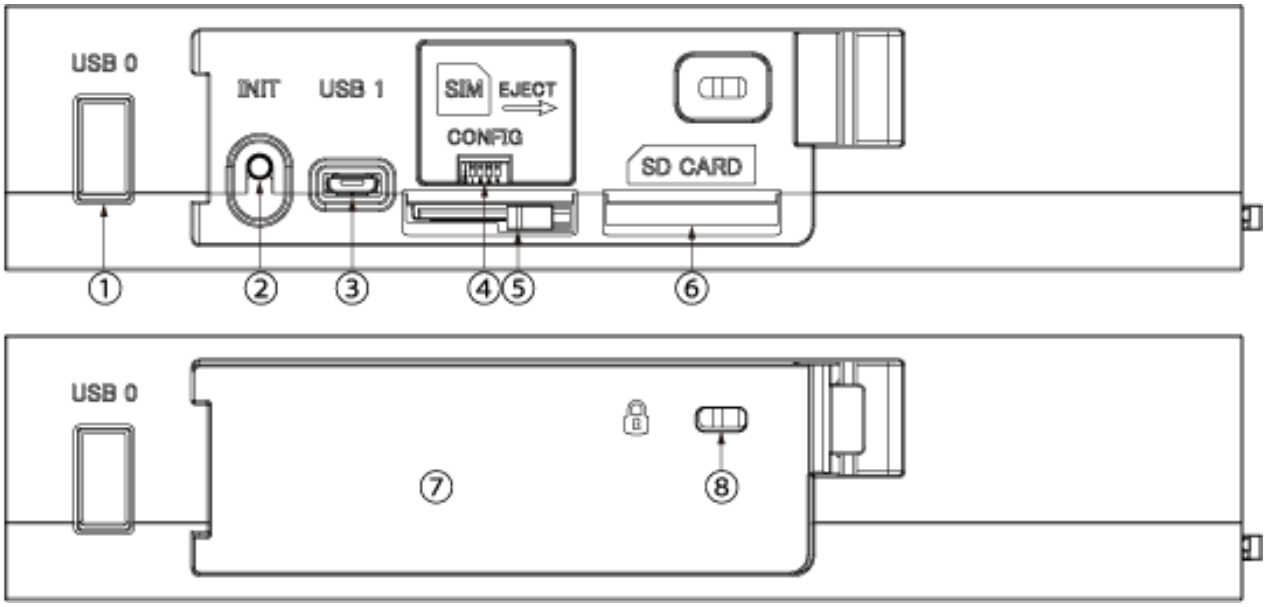

[1] -
[2] -
本装置では使用しません。

[3] MOBILE LED
モバイルモジュールのステータスを示します。
モジュール停止　：●
モジュール起動　：●
PPP 接続時　　：●

[4] ANT II LED
[5] ANT I LED
モバイルの電波状態を示します。

| | 圏外 | 1 | 2 | 3 |
|---|---|---|---|---|
| [4] | ● | ● | ● | ● |
| [5] | ● | ● | ● | ● |

■ **製品側面**




**① USB 0 ポート**
USB2.0 対応の USB(USB Type-A)ポートです。
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。

**② INIT スイッチ**
本装置を工場出荷時の設定に戻して起動するときに使用します。
1. INIT ボタンを押しながら電源を投入します。
2. STATUS1 LED が、緑点滅(＊)を開始するまで、INIT ボタンを押したままにします。
3. STATUS1 LED が、緑点滅(＊)を開始したら、すみやかに INIT ボタンを放します。本装置が工場出荷状態で起動します。

**③ USB 1 ポート**
コンソールポートです。CLI 接続の際に使用します。
USB ケーブル(USB 2.0 microB)を接続します。

**④ CONFIG スイッチ**
すべてのスイッチが上に位置している状態(上上上上)で使用してください。

**⑤ SIM カードスロット(※ NXR-G540W では使用しません)**
5G/LTE SIM カード用スロットです。

**⑥ SD カードスロット**
本装置では使用しません。

**⑦ サイド・カバー**
②～⑥の機能を使用するときに取り外します。

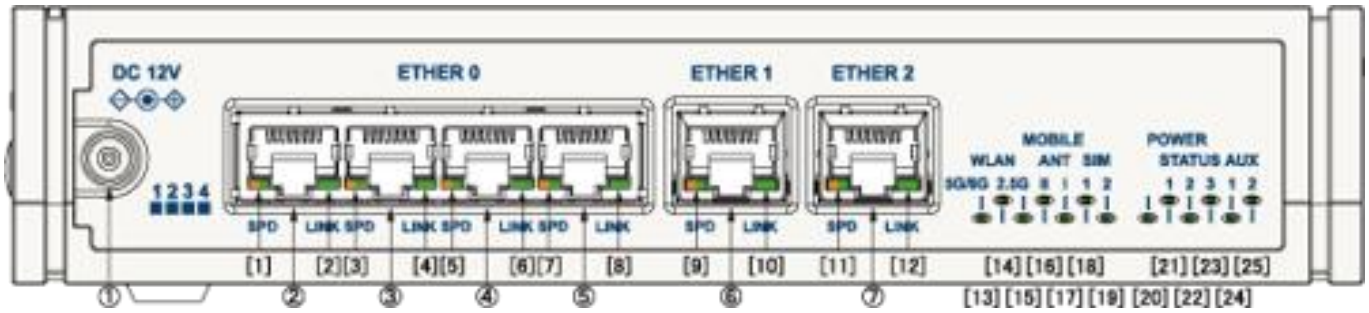
**⑧ セキュリティスロット**
ケンジントンロック(T バーロックタイプ)に対応しています




**① FG(アース)端子**
保安用接続端子です。本機器を使用する場合はアース線を接続します。

## ◆ NXR-G540/LW-CA
## ◆ NXR-G540/W

### ■ 製品前面




**① DC 12V 電源ポート**
製品付属の AC アダプタを接続します。

**② ETHER 0 (ETHER 0/0)ポート**
**③ ETHER 0 (ETHER 0/1)ポート**
**④ ETHER 0 (ETHER 0/2)ポート**
**⑤ ETHER 0 (ETHER 0/3)ポート**
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポート(4 ポートハブ)です。

**⑥ ETHER 1 ポート**
**⑦ ETHER 2 ポート**
10BASE-T/100BASE-TX/1000BASE-T 対応の Ethernet ポートです。

**[1] SPD LED (ETHER 0/0)**
**[3] SPD LED (ETHER 0/1)**
**[5] SPD LED (ETHER 0/2)**
**[7] SPD LED (ETHER 0/3)**
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 ：●

**[9] SPD LED (ETHER 1)**
**[11] SPD LED (ETHER 2)**
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 ：●

**[2] LINK LED (ETHER 0/0)**
**[4] LINK LED (ETHER 0/1)**
**[6] LINK LED (ETHER 0/2)**
**[8] LINK LED (ETHER 0/3)**
**[10] LINK LED (ETHER 1)**
**[12] LINK LED (ETHER 2)**
ETHER ポートの LINK 状態を示します。
　Link Up 時　：●
　Link Down 時　：●

**[13] WLAN 5G/6G･ステータス**
WLAN 5G/6G のステータスを示します。

**[14] WLAN 2.4G･ステータス**
WLAN 2.4G のステータスを示します。

**[15] MOBILE LED(※ NXR-G540W では使用しません)**
モバイルモジュールのステータスを示します。
モジュール停止 ：●
モジュール起動 ：●
PPP 接続　　：●

**[16] MOBILE ANT II LED(※ NXR-G540W では使用しません)**
**[17] MOBILE ANT I LED（※ NXR-G540W では使用しません)**
モバイルの電波状態を示します。

| | 圏外 | 1 | 2 | 3 |
|---|---|---|---|---|
| [16] | ● | ● | ● | ● |
| [17] | ● | ● | ● | ● |

**[18] MOBILE SIM1 LED(※ NXR-G540W では使用しません)**
**[19] MOBILE SIM2 LED(※ NXR-G540W では使用しません)**
SIM1, SIM2 の状態を示します。
SIM 装着+選択中　　：●
SIM 装着+選択なし　：●
SIM 未装着+選択中　：＊
SIM 未装着+選択なし　：●
SIM 装着(異常)　　：●
※選択中とは、当該 SIM が、動作対象となっている状態です。

**[20] POWER LED**
本装置の電源状態を示します。
電源投入時　　：●
システム起動中：●
システム起動後(ログイン可能状態)：●

**[21] STATUS 1 LED**
**[22] STATUS 2 LED**
**[23] STATUS 3 LED**
本装置のシステム、およびサービスのステータスを示します。
**システムおよびサービスのステータス :LED の表示**

| | [20] | [21] | [22] | [23] |
|---|---|---|---|---|
| 電源投入時 | ● | － | － | － |
| システム起動中 | ● | ＊ | － | － |
| システム起動後(ログイン可能状態) | ● | ● | － | － |
| PPP/Tunnel 等の切断状態(configurable) | － | － | ● | － |
| PPP/Tunnel 等の接続状態(configurable) | － | － | ● | － |
| 温度異常(warning) | ＊ | － | － | － |
| 温度異常(critical) | ● | － | － | － |
| ファームウェア更新中 | － | ＊ | － | － |
| ファームウェア更新失敗 | － | ● | － | － |
| システム異常 | ● | ● | ● | － |
| 省電力モード(サスペンド) | ● | ＊ | ＊ | ＊ |

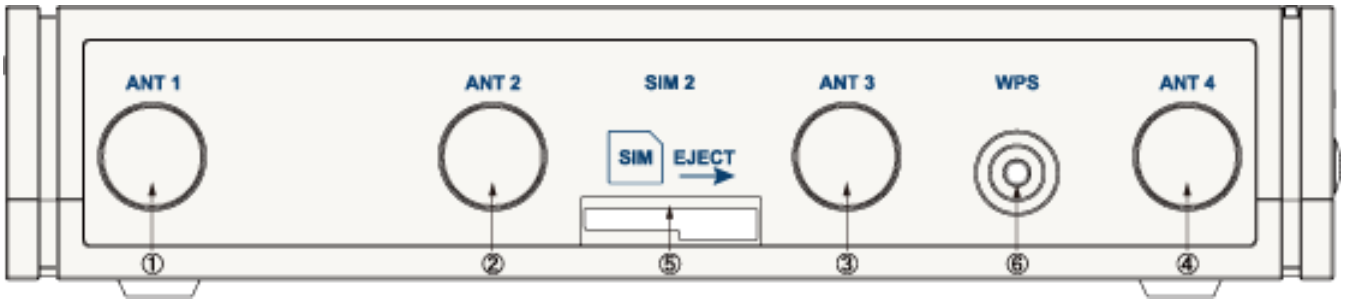
**[24] AUX 1 LED**
**[25] AUX 2 LED**

指定した ppp/tunnel 等の状態を示します。

接続状態　　：●
切断状態　　：●

設定は、system led aux コマンド（global mode）を参照してください。

■ 製品背面




① ANT 1
5G/LTE 用アンテナと接続するためのコネクタ(SMA コネクタ)です。
② ANT 2
本装置では使用しません。
③ ANT 3
本装置では使用しません。
④ ANT 4(※ NXR-G540W では使用しません)
5G/LTE 用アンテナと接続するためのコネクタ(SMA コネクタ)です。
⑤ SIM 2(※ NXR-G540W では使用しません)
5G/LTE SIM カード用スロットです。
⑥ WPS スイッチ
無線 LAN、WPS 機能用スイッチ(プッシュ・タイプ・スイッチ)です。

■ 製品上面




[1] WLAN 5G/6G・ステータス LED
WLAN 5G/6G のステータスを示します。

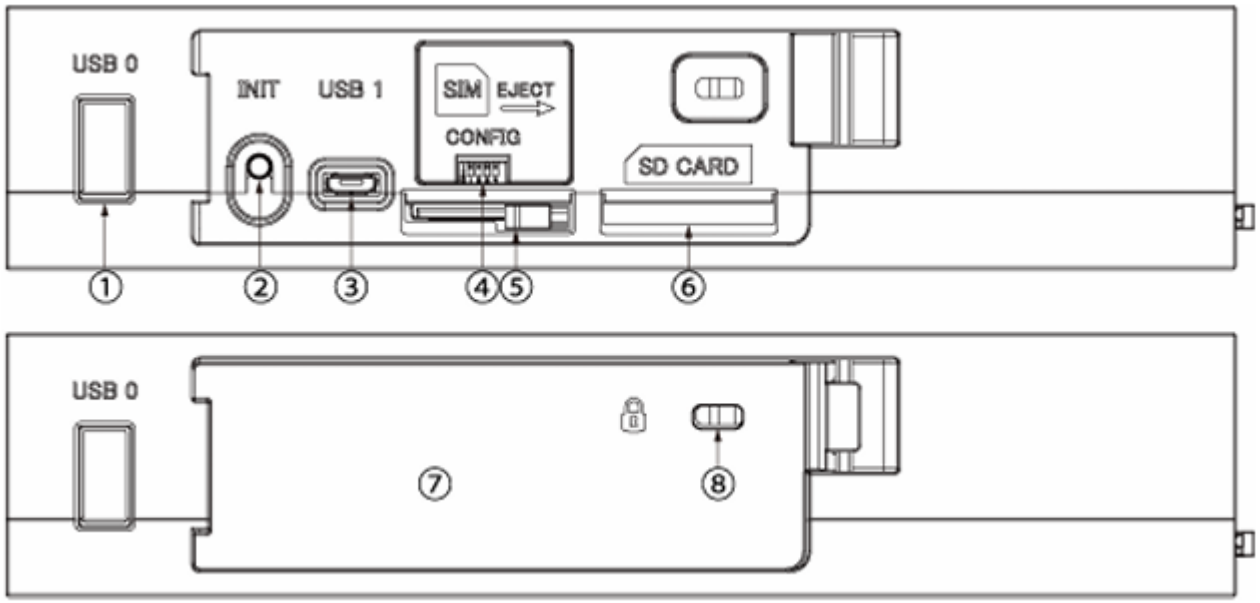
[2] WLAN 2.4G・ステータス LED
WLAN 2.4G のステータスを示します。

[3] MOBILE LED(※ NXR-G540W では使用しません)
モバイルモジュールのステータスを示します。
モジュール停止　：●
モジュール起動　：●
PPP 接続時　　：●

[4] ANT II LED(※ NXR-G540W では使用しません)
[5] ANT I LED (※ NXR-G540W では使用しません)
モバイルの電波状態を示します。

| | 圏外 | 1 | 2 | 3 |
|---|---|---|---|---|
| [4] | ● | ● | ● | ● |
| [5] | ● | ● | ● | ● |

■ **製品側面**




**① USB 0 ポート**
USB2.0 対応の USB(USB Type-A)ポートです。
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。

**② INIT スイッチ**
本装置を工場出荷時の設定に戻して起動するときに使用します。
1. INIT ボタンを押しながら電源を投入します。
2. STATUS1 LED が、緑点滅(＊)を開始するまで、INIT ボタンを押したままにします。
3. STATUS1 LED が、緑点滅(＊)を開始したら、すみやかに INIT ボタンを放します。本装置が工場出荷状態で起動します。

**③ USB 1 ポート**
コンソールポートです。CLI 接続の際に使用します。
USB ケーブル(USB 2.0 microB)を接続します。

**④ CONFIG スイッチ**
すべてのスイッチが上に位置している状態(上上上上)で使用してください。

**⑤ SIM カードスロット(※ NXR-G540W では使用しません)**
5G/LTE SIM カード用スロットです。

**⑥ SD カードスロット**
本装置では使用しません。

**⑦ サイド・カバー**
②～⑥の機能を使用するときに取り外します。

**⑧ セキュリティスロット**
ケンジントンロック(T バーロックタイプ)に対応しています




**① FG(アース)端子**
保安用接続端子です。本機器を使用する場合はアース線を接続します。

# Ⅲ. 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、Microsoft Edge(Windows)で、動作を確認しています。

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

# 第２章　装置の設置

# Ⅰ.装置の設置に関する注意点

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

**注意！**

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

**注意！**

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

**注意！**

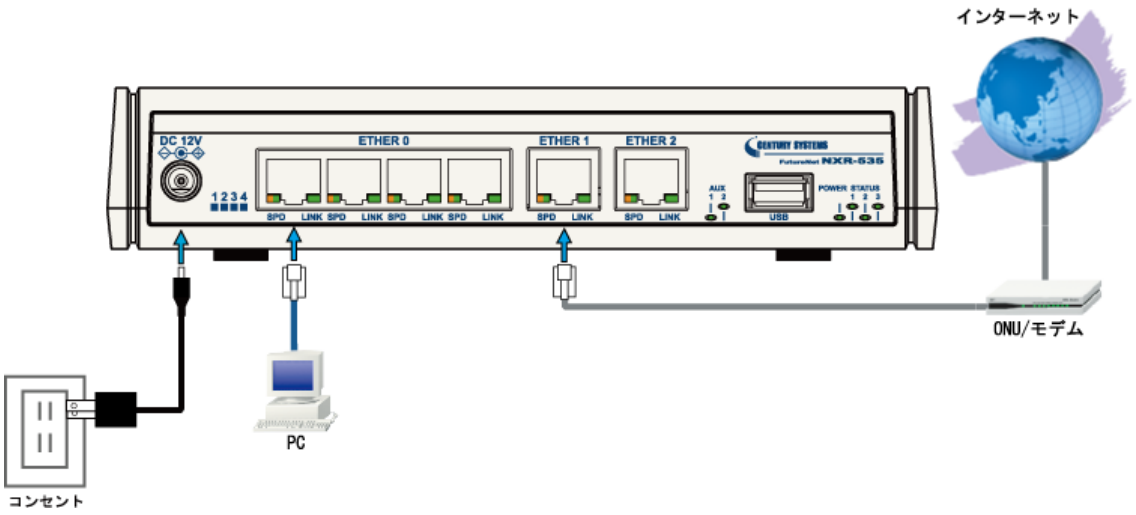
本装置側でも各ポートで ARP table を管理しているため、PC を接続しているポートを変更するとその PC から通信ができなくなる場合があります。このような場合は、本装置側の ARP table が更新されるまで(数秒～数十秒)通信できなくなりますが、故障ではありません。

# Ⅱ. 装置の設置

## ◆ NXR-535

本装置と、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。

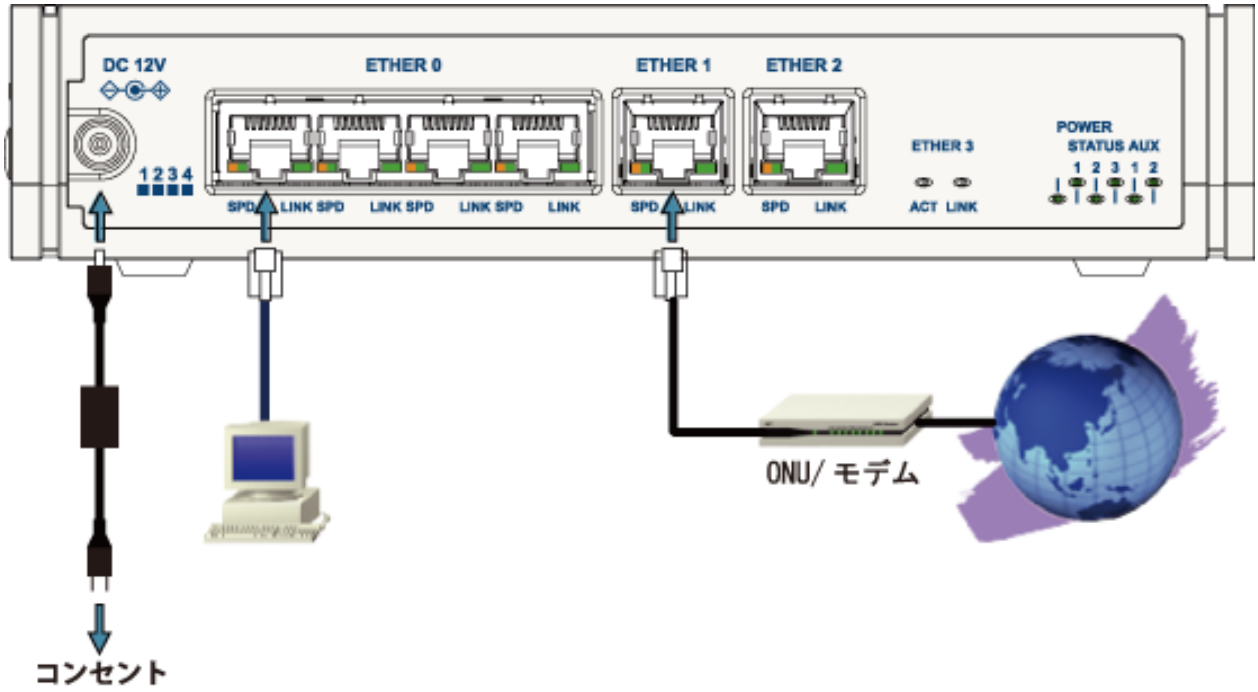
   ※　工場出荷設定状態の場合、ETHER 0 ポートに接続した PC から本装置へログインします。

4. 本装置と AC ケーブル、AC ケーブルとコンセントを接続してください。
5. すべての接続完了後に、各機器に電源を投入してください。

## ◆ NXR-G540 シリーズ

本装置と、PC や ONU/モデムは、以下の手順で接続してください。

接続図 ＜ 例 ＞




1. 本装置および PC や HUB など、接続sるすべての機器の電源が「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 ETHER1 ポートと、ONU/モデムを、LAN ケーブルで接続してください。
3. 本装置の全面にある ETHER0 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、ETHER0 ポートに接続した PC から、本装置へのログインを行います。
4. 本装置と電源アダプタ、電源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。

# 第３章　設定方法の概要

# Ⅰ. 本装置へのログイン（CLI）

**◆はじめに**

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

**◆ CLI への接続方法**

本装置の CLI には、以下の方法で接続できます。

- Console 接続
  PC と本装置の Console ポートを接続します。PC から、console 接続で、本装置の CLI に接続します。

- SSH 接続
  PC と本装置の Ethernet0 ポートを接続します。PC から、SSH で、本装置の CLI に接続します。
  ※ 工場出荷設定では、Ethernet 0 に、IPv4 アドレス（192.168.0.254/24）が設定されています。

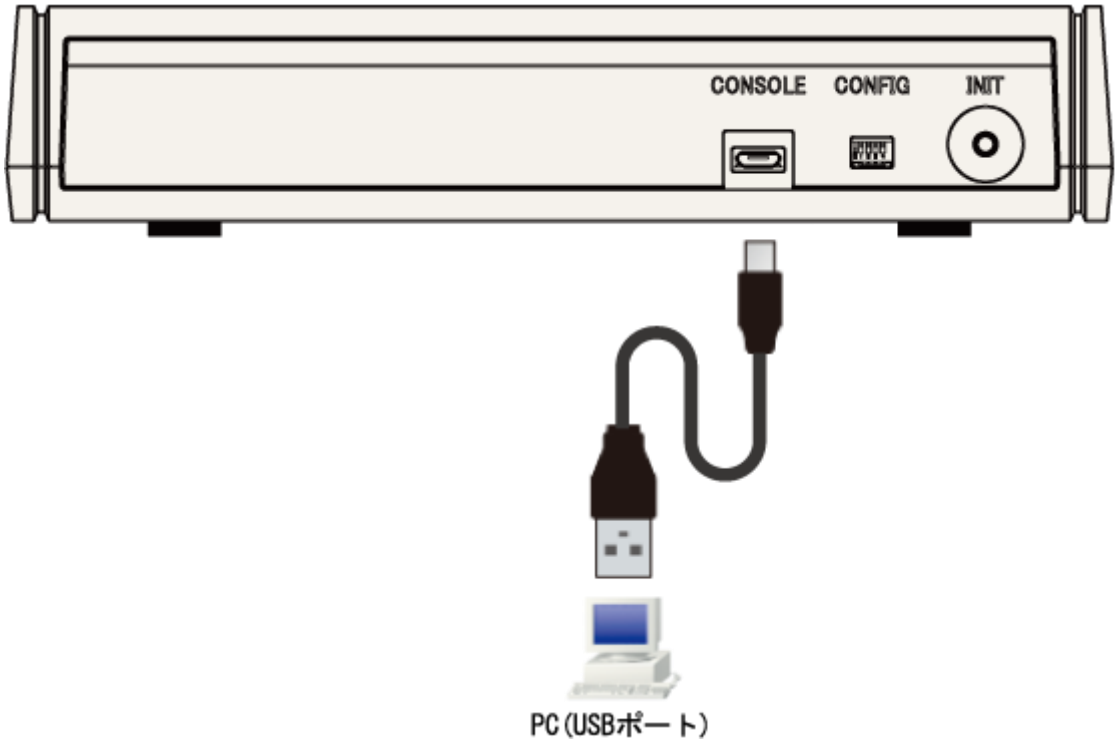
- Telnet 接続
  Telnet 接続には対応していません。

## ◆ Console 接続: NXR-535

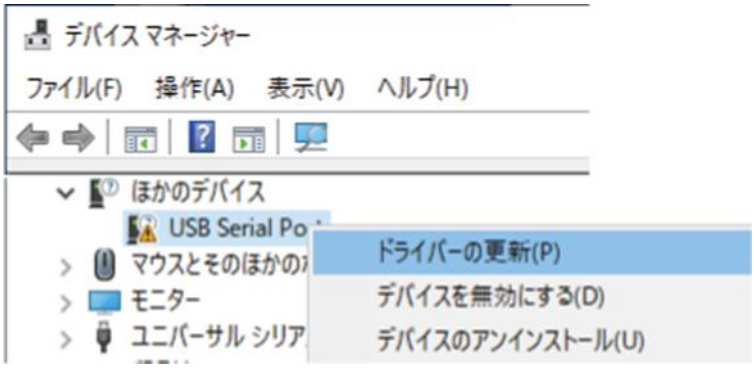
本体側面の CONSOLE ポートを利用して、本装置へログインします。以下の手順で接続します。

1. 本装置と PC を接続します。
   1. 本装置側面の CONSOLE ポートと、USB ケーブルを接続します。
   2. USB ケーブルを、PC の USB ポートに接続してください。
   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。

＜ 接続例 ＞




※ ドライバのインストール(更新)が必要な場合は、手順「3」の後に実施します。
　以下は、PC のデバイスマネージャーからドライバーを更新する例です。




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。

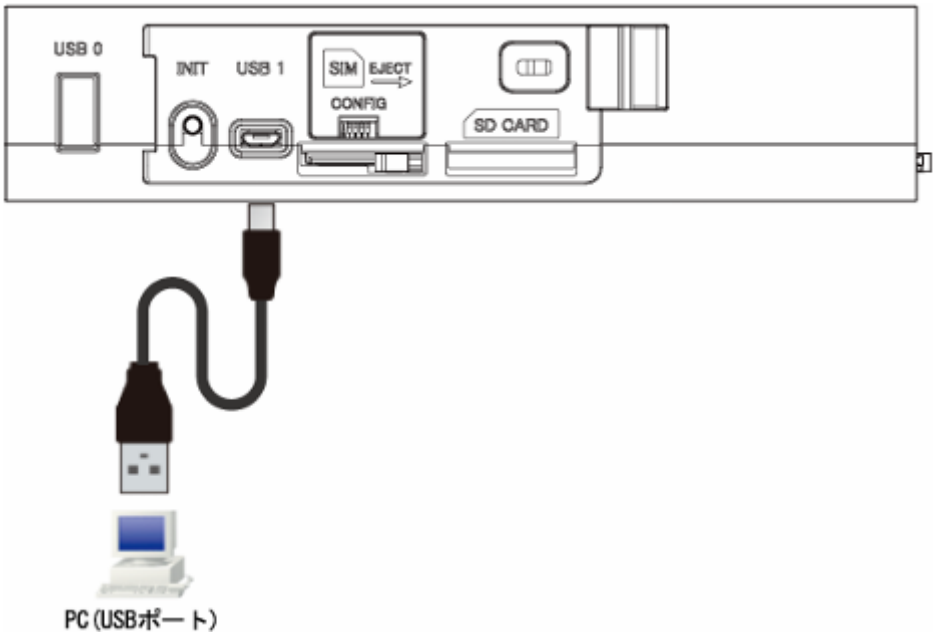
<「Console 接続:NXR シリーズ共通」に続く >

## ◆ Console 接続: NXR-G540 シリーズ

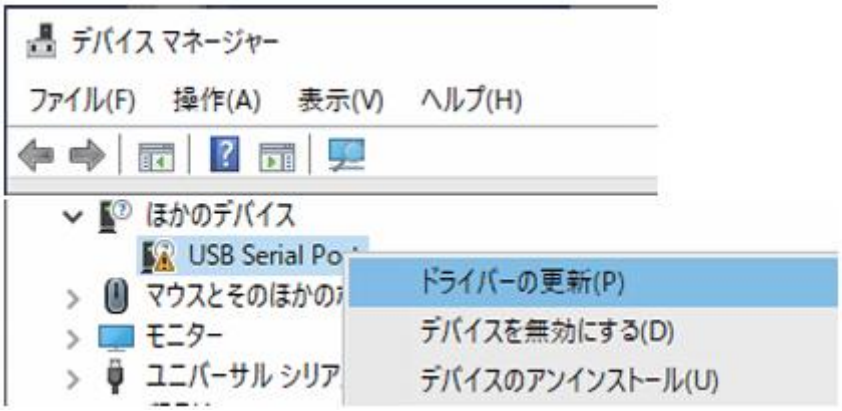
本体前面の CONSOLE ポートを利用して、本装置へログインします。以下の手順で接続します。

1. 本装置と PC を接続します。
   1. 本装置側面の CONSOLE(USB1)ポートと、USB ケーブルを接続します。
   2. USB ケーブルを、PC の USB ポートに接続します。
   3. 本装置と PC の接続完了後に、本装置に電源を投入します。
      本体側面の「POWER LED」が点灯します。

＜ 接続例 ＞




※ ドライバのインストール(更新)が必要な場合は、手順「3」の後に実施します。
以下は、PC のデバイスマネージャーからドライバーを更新する例です。



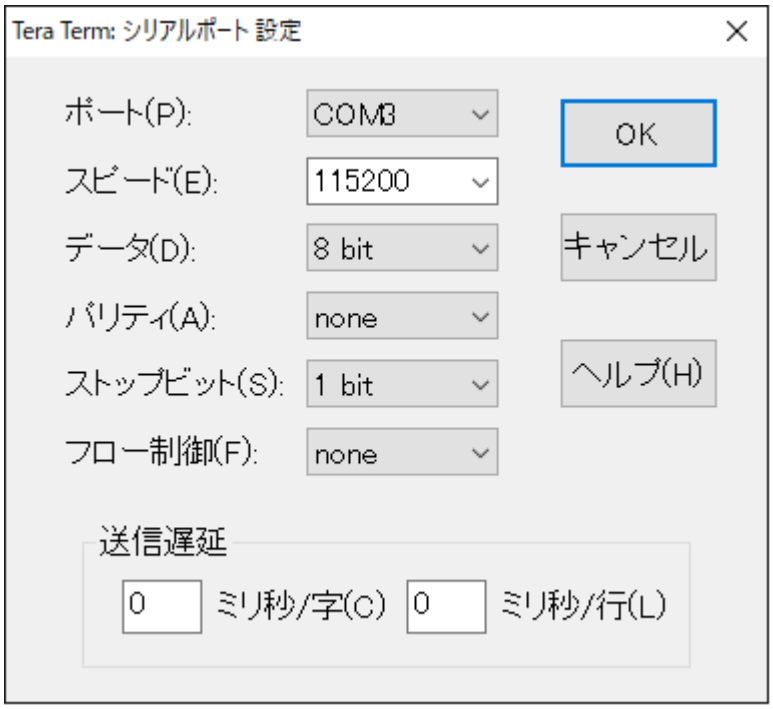

以上で CONSOLE ポートと PC の接続は完了です。続いて、本装置へのログインに移ります。

＜「Console 接続:NXR シリーズ共通」に続く ＞

## ◆ 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. シリアルポート設定は、以下のとおりです。< 設定例(TeraTerm の設定画面)>
※ 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)を入力します。

6. 「You are required to change your password immediately」が表示されるので、
新しいパスワード(8 文字以上)を入力して、パスワードを変更します。

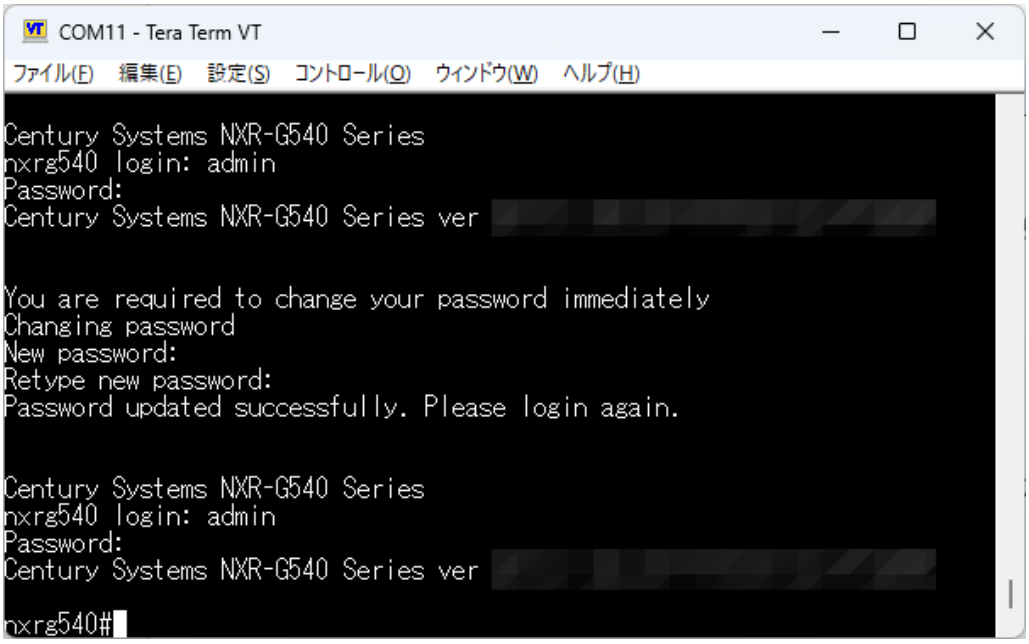
   以下に、パスワードを「$VMZVE6-c9ci」に変更する例を示します。
   New password: $VMZVE6-c9ci
   Retype new password: $VMZVE6-c9ci

7. ユーザ名「admin」、パスワード「新しいパスワード($VMZVE6-c9ci)」を入力すると、
本装置にログインすることが出来ます。

   nxrg540 login: admin
   Password: $VMZVE6-c9ci

以上で、本装置へのログイン(Console 接続)は完了です。

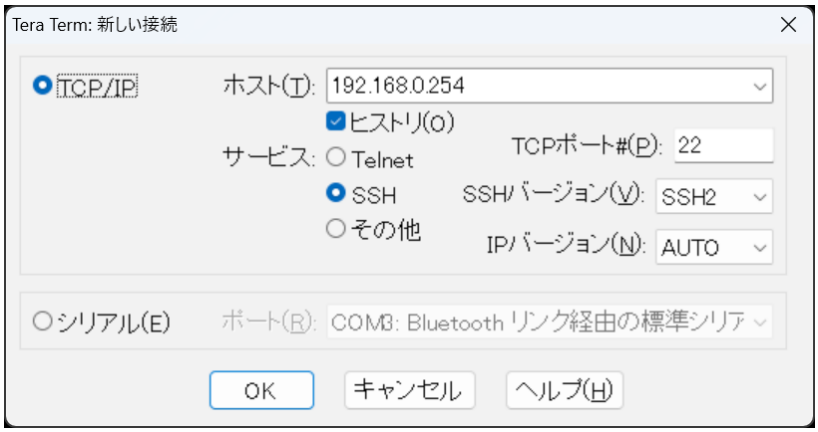
＜ NXR-G540 の例 ＞


COM11 - Tera Term VT
ファイル(F)　編集(E)　設定(S)　コントロール(O)　ウィンドウ(W)　ヘルプ(H)
Century Systems NXR-G540 Series
nxrg540 login: admin
Password:
Century Systems NXR-G540 Series ver
You are required to change your password immediately
Changing password
New password:
Retype new password:
Password updated successfully. Please login again.
Century Systems NXR-G540 Series
nxrg540 login: admin
Password:
Century Systems NXR-G540 Series ver
nxrg540#

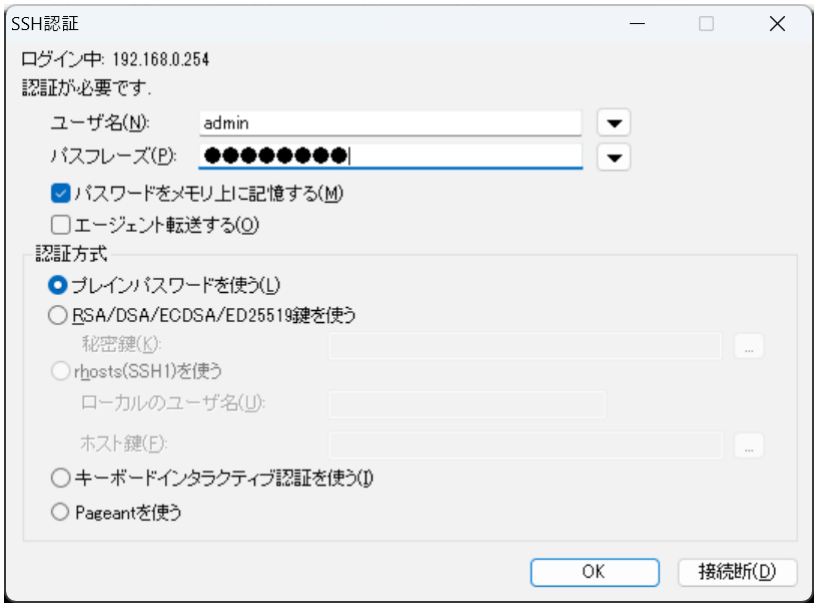
## ◆ SSH 接続: NXR シリーズ

1. PC と本装置の Ethernet 0 ポートを接続します。PC から、SSH で、本装置の CLI に接続します。
   ※工場出荷設定では、Ethernet 0 に、IPv4 アドレス(192.168.0.254/24)が設定されています。

2. SSH 接続を開始します。



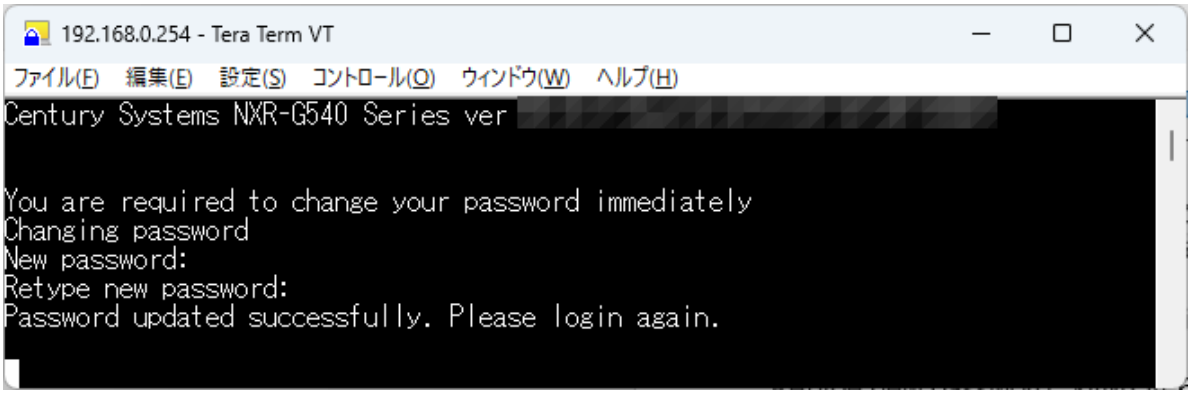

3. ユーザ名、パスワード共に「admin」(工場出荷設定)を入力します。



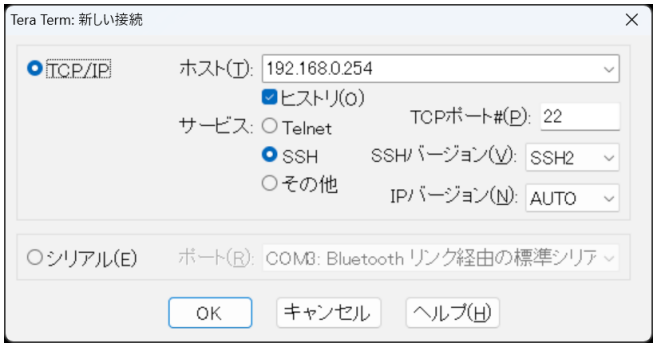

4. 「You are required to change your password immediately」が表示されるので、
   新しいパスワード(8 文字以上)を入力して、パスワードを変更します。

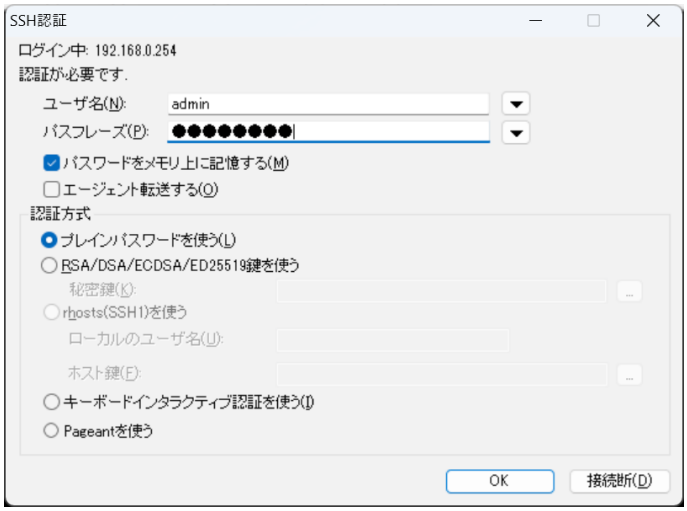
   以下に、パスワードを「$VMZVE6-c9ci」に変更する例を示します。
   New password: $VMZVE6-c9ci
   Retype new password: $VMZVE6-c9ci

＜ NXR-G540 の例 ＞



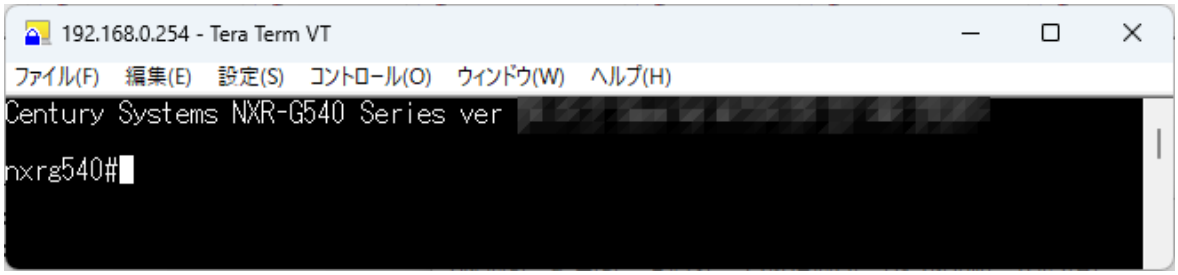

5. SSH 接続が切断されるので、再び SSH 接続を開始します。
ユーザ名「admin」、パスワード「新しいパスワード（$VMZVE6-c9ci）」を入力すると、
本装置にログインすることが出来ます。




以上で、本装置へのログイン(SSH 接続)は完了です。

＜ NXR-G540 の例 ＞



# Ⅱ. 本装置へのログイン(GUI)

◆ **本装置へのログイン(GUI)** ＜ NXR シリーズ ＞

1. PC と本装置の Ethernet 0 ポートを接続します。PC から Web ブラウザで、本装置の GUI に接続します。

2. 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。
   https://192.168.0.254:880/

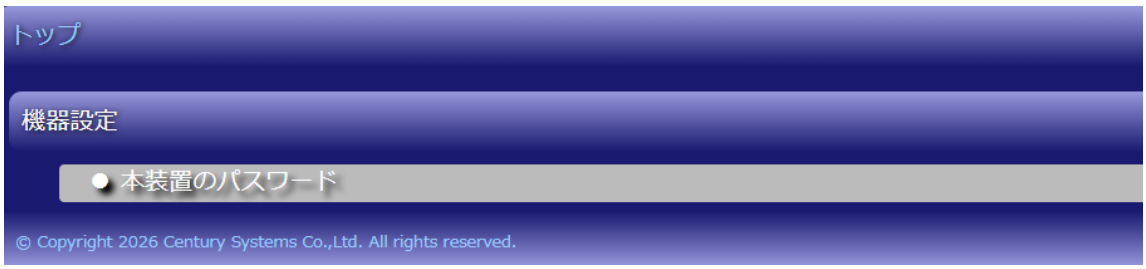
※192.168.0.254 は、Ethernet 0 ポートの IP アドレス(初期値)です。
IP アドレスを変更した場合は、変更後の IP アドレスを指定します。
**ポート番号(880)は変更することができません。**

3. 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)を入力します。

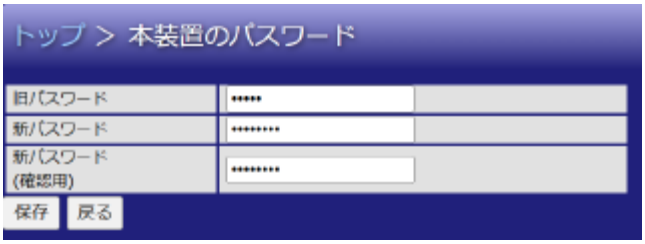



4. パスワード(GUI)が初期値「admin」の場合、パスワードを変更します。

   - パスワード(GUI)が初期値「admin」の場合、ログイン時に以下の画面が表示されます。
     「本装置のパスワード」をクリックして、パスワードを変更します。



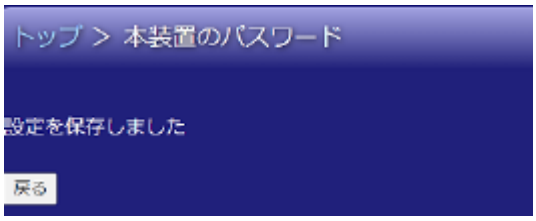

   - 新しいパスワード(8 文字以上)を入力して、パスワードを変更します。
     「旧パスワード」、「新パスワード」、「新パスワード(確認用)」を入力して、「保存」します。




- 認証ダイアログ画面が表示されます。
  ユーザ名「admin」とパスワード(新パスワード)を入力します。

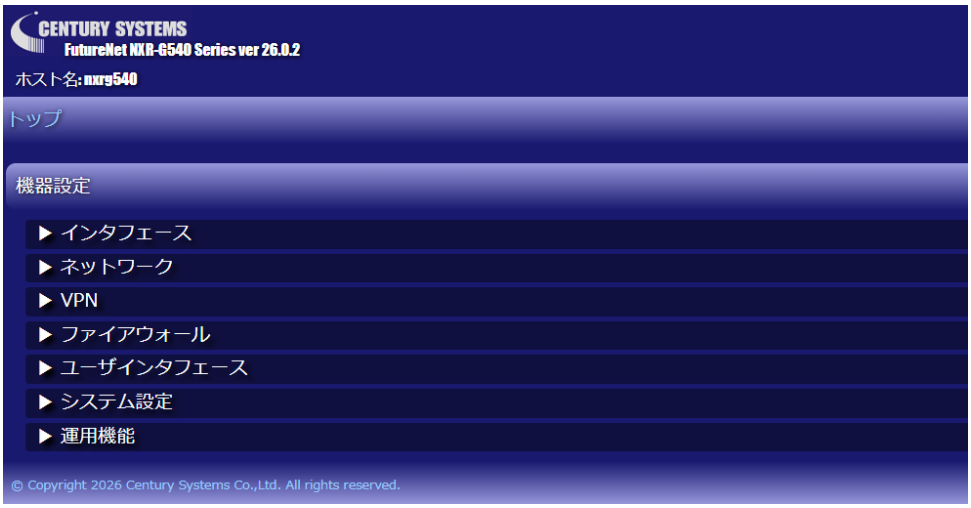



- 以上でパスワードの変更は完了です。




5. 「トップ」をクリックすると、以下の画面が表示されます。以上で本装置へのログイン(GUI)は完了です。

< NXR-G540 の例 >



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/ モバイル
- PPP/ モバイルアカウント
- PPPoE
- モバイル設定

[ネットワーク]
IPv4
- スタティックルート
- 固定 ARP
- NAT

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

DNS
WarpLink
NTP

[VPN]
IPsec
- IPsec トンネル
- IPsec 全体設定
- IPsec 認証設定

L2TPv3
- L2TPv3 接続設定
- L2TPv3 全体設定

[ファイアウォール]
アクセスリスト
- IPv4 アクセスリスト

[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

[システム設定]

システム設定

- 本装置のパスワード
- ホスト名
- 内蔵時計
- セッション数

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

- ファームウェアアップデート
- スケジュール

[運用機能]

ネットワーク診断

- Ping
- Traceroute

パケットダンプ

- パケットダンプ
- パケットダンプ結果表示

ログ情報

- システムログ
- ブートログ

システム情報

- システム情報
- テクニカルサポート
- システムモニター
- 再起動
- インタフェース
- ディスク管理
- サポート情報

# Ⅲ. コマンド実行モード

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

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

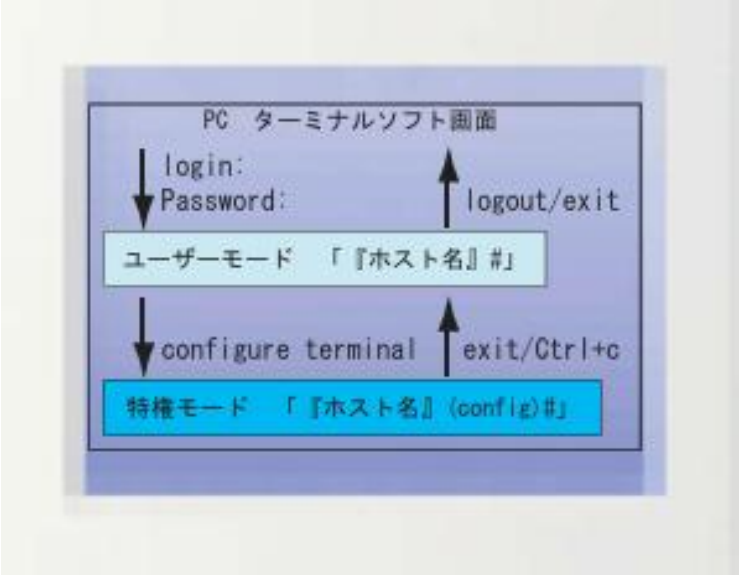
**◆特権モード(CONFIGURATION モード)**
特権モードでは、ユーザモードで実行可能なコマンドに加え、内部システム情報、コンフィグレーション情報を表示するコマンドや、本装置に対して設定をおこなうコマンドの実行が可能になります。
本モードでのプロンプトは、『ホスト名』(config)#」で表示されます。
exit コマンドを入力するか、「Ctrl」+「c」を入力するとユーザーモードに戻ることができます。
更に、各設定の詳細設定をおこなうには、特権モードから各種モードへ移行します。

**<CLI ログアウト時の表示例 >**
nxrg240#exit
Century Systems NXR-G240 Series
nxrg240 login:

**< 特権モードへ移行時の表示例 >**
nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#

**< ユーザーモードへ移行時の表示例>**
nxrg240(config)#exit
nxrg240#

**< モード間の移行 >**



# Ⅳ. コマンド入力時の補助機能

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

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

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

**< スペースの後ろに「?」キー入力時の表示例 >**

```
nxrg240#show ?
      arp              Address Resolution Protocol (ARP)
      bgp              BGP information
      bridge           Bridge information
      class            Show class access-list status
      clock            System Clock
      config           Configurations
      crp              Century Registration Protocol (CRP) informations
--More—
```

**< 直後に「?」キー入力時の表示例 >**

```
nxrg240#?
Exec commands:
      clear            Reset functions
      clock            Adjusting System Clock
      configure        Enter configuration mode
      connect          Attempt connect Functions
      copy             Import or Export files
      debug            Debugging functions (see also 'undebug')
      delete           Delete files
--More--
```

**◆コマンドページャ機能**

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

**◆ grep 機能**

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

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

# V. 本装置のモード構造

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

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

# VI. パスワード(初期値)の変更

不正アクセス防止のために、CLI と GUI のログインパスワードを変更します。
以下に、CLI のパスワードを「$VMZVE6-c9ci」に、GUI のパスワードを「QDEZ/GcQjNFJ」に変更する例を示します。

◆ **設定例**

```
nxr#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr(config)#password $VMZVE6-c9ci
nxr(config)#gui password QDEZ/GcQjNFJ
nxr(config)#exit
nxr#save config
```

◆ **設定例の説明**

global mode に移行します。
　configure terminal
CLI のログインパスワードを変更します。
　password $VMZVE6-c9ci
GUI のログインパスワードを変更します。
　gui password QDEZ/GcQjNFJ
global mode から exit します。
　exit
設定を保存します。
　save config

# Ⅶ. SPI フィルタの設定

WAN からの不正アクセス防止のために、WAN インタフェースで SPI(ステートフルパケットインスペクション)フィルタを有効にします。
以下に、WAN インタフェースが ETHER 1 の例を示します。

**◆ 設定例**

```
nxr#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr(config)#interface ethernet 1
nxr(config-if)#ip spi-filter
nxr(config-if)#exit
nxr(config)#exit
nxr#save config
```

**◆ 設定例の説明**

global mode に移行します。
　configure terminal
インタフェースモードに移行します。
　interface ethernet 1
SPI フィルタを有効にします。
　ip spi-filter
interface mode から exit します。
　exit
global mode から exit します。
　exit
設定を保存します。
　save config

# 第４章　view(exec) mode

## ■ show

### ○ show config

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

### ○ show config interface

<説　　明> インタフェースの設定情報を表示します。
<書　　式> show config interface ethernet <0-3> (|vid <1-4094>)
show config interface ppp <0-4>
show config interface tunnel (|0-511)
show config interface loopback (|0-9)
show config interface bridge <0-4095> (|vid <1-4094>)
show config interface tap <0-127> (|vid <1-4094>)

### ○ show config file

<説　　明> ファイルパスとファイル名を指定して、設定情報を表示します。
<書　　式> show config file FILENAME xml (xml|cmd)
<　　例　　> ・xml 形式で表示します。
show config file disk0:nxr.xml xml
・show config 形式で表示します。
show config file disk0:nxr.xml cmd

### ○ show startup-config

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

### ○ show config section

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

### ○ 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>)
show config ipsec (|local policy <1-255>)
show config ipsec (|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>)
show config l2tpv3 (|tunnel <0-4095>)
show config l2tpv3 (|xconnect <1-4294967295>)

◆ **show config ipv6 dhcp-client**

<説　　明> ipv6 dhcp-client の設定を表示します。

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

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

◆ **show ip route**

<説　　明> ルーティングテーブルを表示します。

<書　　式> show ip route (|bgp|connected|ospf|rip|static)
show ip route database (|bgp|connected|ospf|rip|static)

◆ **show ipv6 route**

<説　　明> IPv6 ルーティングテーブルを表示します。

<書　　式> show ipv6 route (|connected|static)
show ipv6 route cache
show ipv6 route database (|connected|static)

◆ **show ip protocols**

<説　　明> ルーティングプロトコルに関する情報を表示します。

<書　　式> show ip protocols (|ospf|rip)

◆ **show ip access-list**

<説　　明> IP アクセスリストを表示します。

<書　　式> show ip access-list [IPv4- ACL-NAME]

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

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

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

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

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

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

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

◆ **show ipv6 ra proxy**
<説　　明> IPv6 RA proxy の prefix を表示します。
<書　　式> show ipv6 ra-proxy interface ethernet <0-XX>
show ipv6 ra-proxy interface ppp <0-4>

◆ **show ip web-auth access-list**
◆ **show ipv6 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 ipv6 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> syslog を表示します。
<書　　式> show syslog message (|all|backup) (|line:1-99999) (|reverse)
　　show syslog bootlog (|line:1-99999) (|reverse)
　　show syslog maillog (|line:1-99999) (|reverse)
<備　　考> all を指定すると、ログと backup ログを連結して表示します。
　　backup を指定すると、backup ログを表示します。
　　line(表示する行数)を指定することが出来ます。
　　reverse を指定すると、新しい情報→古い情報の順に表示します。

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

<説　　明> 外部ストレージ、または Flash ROM に保存した syslog を表示します。
<書　　式> show syslog file FILENAME (|line:1-99999) (|reverse)
<備　　考> ファイルパスとファイル名を指定します。
　　例) show syslog file disk0:syslog.log
　　show syslog file flash1:20160118_1430.log.gz
　　syslog を外部ストレージに保存するには、syslog mode での設定が必要になります。
　　例) nxrg240(config)#syslog
　　nxrg240(config-syslog)#local file disk0:syslog.log

◆ **show arp**

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

◆ **show ipv6 neighbors**

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

◆ **show (disk0|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

◆ **clear history**
<説　　明> 過去に実行した運用コマンドの履歴を消去します。
<書　　式> clear history

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

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

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

■ **show l2tp**

○ **show l2tp**

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

○ **show l2tp peer**

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

■ **show l2tpv3**

○ **show l2tpv3**

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

○ **show l2tpv3 tunnel**

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

○ **show l2tpv3 session**

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

○ **show l2tpv3 interface**

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

○ **show l2tpv3 fdb**

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

○ **show l2tpv3 fdb interface**

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

○ **show l2tpv3 group**

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

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

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

◆ **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|mdix)
show interface ethernet <0-2> (|mode|mdix|bridge|vid <1-4094>)
show interface wlan <0-1> (|all|ssid)
show interface tap <0-127> (|vid <1-4094>) (|bridge)
show interface bridge (db-brief|list)
show interface bridge <0-4095> (port-list|statistics|fdb|flows|stp|vid <1-4094>)
show interface switchport counter
show interface wireguard <0-31>
<備 考> 指定できるインタフェース番号は、機種によって異なります。

◆ **clear interface bridge**
<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> clear interface bridge <0-4095> fdb

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

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

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

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

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

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

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

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

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

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

◆ **show ip ospf**

<説　　明> OSPF の情報を表示します。

<書　　式> show ip ospf
show ip ospf neighbor (|detail)
show ip ospf interface (|INTERFACE)
show ip ospf database (|external|summary|network|router|asbr-summary)
show ip ospf route
show ip ospf virtual-links

◆ **show ip bgp**

<説　　明> BGP の情報を表示します。

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

◆ **show bgp ipv6**

<説　　明> BGP の情報を表示します。

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

### ◆ clear bgp ipv6

<説　　明>
・ BGP セッションをリセットします。
・ BGP の設定を変更した場合、即時には反映されないため、BGP セッションを一度リセットする必要があります。
  - soft out リセット
  - BGP ネットワークやフィルタリングの変更などの経路情報は、BGP セッションを維持したまま適用することが出来ます。soft out リセットを行うと、設定を内部に反映し、BGP neighbor へ UPDATE メッセージを送信します。
  - soft in リセット
  - BGP neighbor へ ROUTE-REFRESH メッセージを送信し、neighbor へ全ての BGP 経路情報を要求します。ROUTE-REFRESH メッセージを受信した場合は、UPDATE メッセージにより経路情報を送信します。
  - hard リセット
  - BGP の TCP セッションを一旦切断し、neighbor を再確立します。keepalive や holdtime の設定を変更した場合は、ソフトリセットでは変更が反映されないためハードリセットを行ってください。ハードリセットを行う場合は、soft (in|out)を指定しません。

<書　　式> clear bgp ipv6 * soft (in|out)
<備　　考> すべての neighbor とのセッションをリセットします。

<書　　式> clear bgp ipv6 X:X::X:X
　　clear bgp ipv6 X:X::X:X soft (in|out)
<備　　考> Neighbor の IPv6 アドレスを指定して、セッションをリセットします。

### ■ show mobile

<説　　明> モバイルデータ通信端末／内蔵通信モジュールに関する情報を表示します。
　　PPP 使用中は情報を取得できない場合があります。
<書　　式> show mobile (|<0-2>)
<備　　考> show mobile 0　モバイルデータ通信端末に関する情報を表示します。
　　show mobile 1　内蔵通信モジュールに関する情報を表示します。
　　show mobile 2　内蔵通信モジュールに関する情報を表示します。
　　※指定できるモバイルの番号は、機種によって異なります。

○ ap
<説　　明> APN 情報を表示します。
<書　　式> show mobile <0-2> ap

○ network-reg-status
<説　　明> ネットワークへの登録情報を表示します。
<書　　式> show mobile <0-2> network-reg-status
<実 行 例> nxr#show mobile 1 network-reg-status
　　Network Area : LTE

○ phone-number
<説　　明> 電話番号を表示します。
<書　　式> show mobile <0-2> phone-number

○ position
<説　　明> GPS 位置情報(緯度･経度)を表示します。
<書　　式> show mobile <0-2> position
<実 行 例> nxr#show mobile 1 position
Getting positioning information ... Please wait.
Lat : 3X.XXX
Lon : 13Y.YYY

○ signal-info
<説　　明> 電波情報を表示します。
<書　　式> show mobile <0-1> signal-info
<備　　考>
・　表示される項目は、機種(内蔵モジュール)に依存します。

○ signal-level
<説　　明> 電波強度を表示します。
<書　　式> show mobile <0-1> signal-level
<実 行 例> nxr#show mobile 1 signal-level
Signal Level : 2 (RSSI: -85dBm) [Area:LTE]

○ rat
<説　　明> モバイルモジュールの周波数帯の設定を表示します。
<書　　式> show mobile <1> rat

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

### ◆ show fast-forwarding status

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

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

```
nxrg240#show fast-forwarding status
total forward count 644
3s udp 192.168.0.1:63->192.168.10.1:63 count:9 byte:12564 fw4 natp4 src 192.168.1.254:63      ①
4s udp 192.168.10.1:63->192.168.1.254:63 count:9 byte:12564 natp4 dst 192.168.0.1:63 fw4      ②
```

①、②は、IP forwarding されたエントリーです。

・　以下に、Fast-forwarding(IPsec)の例を示します。

```
nxrg240#show fast-forwarding status
total forward count 661
7s esp 192.168.1.253->192.168.1.254 count:9 byte:12564 ESP_IN spi:$95e97067 fw4      ①
7s udp 192.168.10.1:63->192.168.0.1:63 count:8 byte:11168 fw4      ②
5s udp 192.168.0.1:63->192.168.10.1:63 count:9 byte:13158 fw4 ESP_OUT spi:$44f8bc92      ③
```

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

### ◆ show product

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

### ■ show netevent

○ track

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

○ action

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

◆ **show warplink**

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

◆ **show monitor-log**

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

◆ **show service**

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

◆ **show ngn-sip**

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

◆ **show ip dhcp route**

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

◆ **clear ngn-sip call**

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

◆ **clock set**

<説　　明> 現在時刻を設定します。
<書　　式> clock set HH:MM:SS Day Month Year
　　clock set ntp (A.B.C.D|X:X::X:X|FQDN) (timeout <1-30>|)
<備　　考> 2010 年 12 月 31 日 12 時 34 分 56 秒に設定する場合は、次のように入力します。
　　clock set 12:34:56 31 12 2010

### ◆ delete

<説　　明> ファイルを消去します。
<書　　式> delete bootlog　　(bootlog の削除)
delete bootup-config
delete dump　　(dump ファイルの削除)
delete file (disk0:FILENAME|disk1:FILENAME) (disk0=USB0, disk1=USB1)
delete flash FILENAME　　(Flash ROM 上のファイル名を指定して削除)
delete flash1 FILENAME　　(Flash ROM(ログ領域)のファイル名を指定して削除)
delete reachability-log　　(reachability ログの削除)
delete resource-log　　(resource ログの削除)
delete syslog　　(syslog 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)、および Flash ROM 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|flash|flash1)
<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。
Flash ROM(全領域)を指定する場合は、flash を選択します。
Flash ROM(ログ領域)を指定する場合は、flash1 を選択します。

■ **copy**

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

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

<書　　式>

copy (bootlog|dump|syslog|reachability-log|resource-log)
ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME (|source A.B.C.D|X:X::X:X)
copy (bootlog|dump|syslog|reachability-log|resource-log)
ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
copy (bootlog|dump|syslog|reachability-log|resource-log)
http|https://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
copy (bootlog|dump|syslog|reachability-log|resource-log)
(disk0:FILENAME|disk1:FILENAME)
copy (bootlog|dump|syslog|reachability-log|resource-log) zmodem

<備　　考>

・ ソースアドレスを指定することができます。
・ SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
  - IPv4 ssh://user@A.B.C.D:port/FILENAME
  - IPv6 ssh://[user@X:X::X:X]:port/FILENAME
・ https:// の場合、サーバ証明書の validation を行う。https-:// の場合、validation を行わない。
・ URL には、以下のマクロ文字列を使用することが出来ます。これらの文字列は、本装置によって自動的に置換されます。
  ${MODEL}：モデル情報（ex. nxr530）
  ${VER}：バージョン（ex. 21.11.15）
  ${SN}：シリアル番号（ex. 10123456xxx）
  例えば、次のコマンドは、
  copy syslog ftp://a.b.c.d/nxr530/10123456xxx.txt
  以下のように、マクロ文字列を使って、書くことが出来ます。
  copy syslog ftp://a.b.c.d/${MODEL}/${SN}.txt

**○ config のバックアップ**

<説　　明> 設定ファイルのバックアップ(外部にコピー)をおこないます。

<書　　式>

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

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

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

copy (config|show-config) zmodem

<備　　考>

- all 指定の場合は、ipsec を含む全ての config を tgz 形式でコピーします。指定なしの場合は、config のみを xml 形式でコピーします。
- 設定ファイルを show config 形式でバックアップするには、show-config を指定します。
- ソースアドレスを指定することができます。
- SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
  - IPv4 ssh://user@A.B.C.D:port/FILENAME
  - IPv6 ssh://[user@X:X::X:X]:port/FILENAME
- URL には、マクロ文字列を使用することが出来ます。詳細は、■ copy(view mode)を参照してください。

**○ tech-support の取得**

<説　　明> tech-support を取得(外部にコピー)します。

<書　　式>

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

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

copy tech-support disk0:FILENAME|disk1:FILENAME

copy tech-support zmodem

<備　　考>

- URL には、マクロ文字列を使用することが出来ます。詳細は、■ copy(view mode)を参照してください。

**○ century-tech-support の取得**

<説　　明> century-tech-support を取得(外部にコピー)します。

<書　　式>

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

copy century-tech-support ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)

copy century-tech-support disk0:FILENAME|disk1:FILENAME

copy century-tech-support zmodem

<備　　考>

- URL には、マクロ文字列を使用することが出来ます。詳細は、■ copy(view mode)を参照してください。

**○ ssh 公開鍵のインポート**

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

<書　　式>

copy (ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME)
ssh-public-key user netconf |<0-4> (|source A.B.C.D|X:X::X:X)
copy (ftp://<A.B.C.D|X:X::X:X>/FILENAME)
ssh-public-key user netconf |<0-4> (|source A.B.C.D|X:X::X:X)
copy (http|https://<A.B.C.D|X:X::X:X>/FILENAME)
ssh-public-key user netconf |<0-4> (|source A.B.C.D|X:X::X:X)
copy (disk0:FILENAME|disk1:FILENAME)
ssh-public-key user netconf |<0-4> (|source A.B.C.D|X:X::X:X)

<備　　考>

・　ソースアドレスを指定することができます。
・　SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
  - IPv4 ssh://user@A.B.C.D:port/FILENAME
  - IPv6 ssh://[user@X:X::X:X]:port/FILENAME
・　https:// の場合、サーバ証明書の validation を行う。https-:// の場合、validation を行わない。
・　URL には、マクロ文字列を使用することが出来ます。詳細は、■ copy(view mode)を参照してください。

**○ config の復帰**

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

<書　　式>

copy ssh://user@(A.B.C.D|X:X::X:X)/FILENMAE
(startup-config|disk0:FILENAME|disk1:FILENAME) (rollback|source A.B.C.D|X:X::X:X)
copy ftp://(A.B.C.D|X:X::X:X)/FILENAME
(startup-config|disk0:FILENAME|disk1:FILENAME) (rollback|source A.B.C.D|X:X::X:X)
copy http|https://(A.B.C.D|X:X::X:X)/FILENAME
(startup-config|disk0:FILENAME|disk1:FILENAME) (rollback|source A.B.C.D|X:X::X:X)
copy (disk0:FILENAME|disk1:FILENAME)
(startup-config|disk0:FILENAME|disk1:FILENAME) (rollback|source A.B.C.D|X:X::X:X)

<備　　考>

・　disk0 --> disk0、disk1 --> disk1 への copy は不可。disk0 <--> disk1 への copy は可。
・　ソースアドレスを指定することができます。
・　SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
  - IPv4 ssh://user@A.B.C.D:port/FILENAME
  - IPv6 ssh://[user@X:X::X:X]:port/FILENAME
・　https:// の場合、サーバ証明書の validation を行う。https-:// の場合、validation を行わない。

■ **Config Rollback 機能**

- rollback を指定すると、現在の startup-config を backup します。
- 次回の起動時は、復帰させた config で起動し、起動後一定時間(600 秒)内にユーザによる承認が行われない場合、backup した config で再起動する機能です。
- これにより、リモートで config を復帰した場合に、config の間違い等でリモートからの操作が出来なくなることを防ぎます。
- rollback の対象は、startup-config で、保持されるのは 1 世代のみです。
- startup-config 以外(例えば、disk 上の config)で起動している場合、本機能は動作しません。

■ **Rollback timer の停止(承認)**

- 下記のコマンドにて、Rollback timer を停止(承認)することが出来ます(backup の config を削除します)。
  - save config
  - restart system
  - firmware update
  - clear rollback
  - SMS による clear rooback 指示

■ **Rollback の cancel**

- Rollback 有効の状態で config を復帰した後、システム再起動を行う前に、cancel rollback を実行することで、rollback を無効にすることが出来ます。
  システム再起動後、rollback timer が起動している状態で、cancel rollback を実行しても、rollbacktimer は停止しません。

### ◆ firmware update

<説　　明> ファームウェアをアップデートします。

<書　　式>

firmware update official (|source A.B.C.D|X:X::X:X) (|no-boot)
firmware update ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME(|source A.B.C.D|X:X::X:X) (|no-boot)
firmware update ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X) (|no-boot)
firmware update http|https://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X) (|no-boot)
firmware update (disk0:FILENAME|disk1:FILENAME) (|no-boot)
firmware update cms (|source A.B.C.D|X:X::X:X) (|no-boot)

<備　　考>

・　ソースアドレスを指定することができます。
・　no-boot を指定すると、ファームウェアアップデート後に、現在のファームウェアで起動します。
・　SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
  - IPv4 ssh://user@A.B.C.D:port/FILENAME
  - IPv6 ssh://[user@X:X::X:X]:port/FILENAME
・　https:// の場合、サーバ証明書の validation を行う。https-:// の場合、validation を行わない。
・　ファームウェア更新後に再起動します。設定を保存していない場合は、問い合わせてからファームウェアの更新を行います。詳細については、「付録 E:Firmware update」を参照してください。
・　URL には、以下のマクロ文字列を使用することが出来ます。これらの文字列は、本装置によって自動的に置換されます。
  ${MODEL}：モデル情報（ex. nxr530）
  ${VER}：バージョン（ex. 21.11.15）
  ${SN}：シリアル番号（ex. 10123456xxx）
  例えば、次のコマンドは、
  firmware update ftp://a.b.c.d/nxr530/10123456xxx.bin
  以下のように、マクロ文字列を使って、書くことが出来ます。
  firmware update ftp://a.b.c.d/${MODEL}/${SN}.bin

### ◆ firmware list-update

<説　　明> firmware list-update を実行します。

<書　　式> firmware list-update WORD (|source A.B.C.D|X:X::X:X)
　　firmware list-update cms (|source A.B.C.D|X:X::X:X)

<備　　考>

・　list に含まれる version と起動中の version が同じ場合、firmware update を実行しません。
・　list に含まれる version と起動中の version が異なる場合、list で指定された URL から firmware を取得して、firmware update を実行します。
・　URL には、マクロ文字列を使用することが出来ます。詳細は、firmware update(view mode)を参照してください。

◆ **firmware mobile update**

<説　　明> 内蔵モジュールファームウェアをアップデートします。

<書　　式>

firmware mobile 1 update
　　ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME (|source A.B.C.D|X:X::X:X)
firmware mobile 1 update
　　ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
firmware mobile 1 update (disk0:FILENAME|disk1:FILENAME)
firmware mobile 1 update
　　http|https://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
firmware mobile 1 update cms

<備　　考>

・　NXR-G180/L-CA のみ、firmware mobile <1-2> update を使用します。
・　モジュールファームウェア更新後は、自動的にモジュールをリセットします。
・　update 中は該当モジュールに対する操作(connect/disconnect/show mobile/reset mobile)は制限されます。システム再起動、config の保存 / 復帰、system firmware update も制限されます。
・　https:// の場合、サーバ証明書の validation を行う。https-:// の場合、validation を行わない。

### ◆ firmware check official

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

### ◆ restart

<説　　明> サービスの再起動を行います。
<書　　式>

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

### ◆ restart rollback

<説　　明>
・　ロールバックタイマが満了する前に、直ちにロールバックさせたい場合、restart rollback コマンドを実行します。
<書　　式> restart rollback
<備　　考>
・　ロールバック指定を行い、ロールバックタイマが満了した場合(ロールバックタイマを停止させない場合)、バックアップした config でシステム再起動します。

### ◆ configure

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

### ■ dump

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

○ dump
<書　　式> dump interface INTERFACE
<備　　考>
・　INTERFACE には、いずれかを指定します。
bridge<0-4095>|ethernet <0-2>(|vid<1-4094>)|map<0-1>|ppp<0-4|100-256>|tap<0-127>|tunnel<0-255>
※指定できるインタフェース番号は、機種によって異なります。

○ dump filter
<書　　式>
dump interface INTERFACE filter (include|exclude)
{telnet|ip|ipv6|arp|esp|l2tpv3|gre|tcp port <1-65535>|udp port <1-65535>|ipproto <1-255>}
○ dump pcap
<書　　式>
dump interface INTERFACE pcap count <1-99999> (size <64-1518>|) (filter (include|exclude)
{telnet|ip|ipv6|arp|esp|l2tpv3|gre|tcp port <1-65535>|udp port <1-65535>|ipproto <1-255>}|)

### ◆ show dump saved

<説　　明> 保存された dump ファイルを表示します。
<書　　式> show dump saved (|detail)
<備　　考> dump ファイルを削除するには、delete dump(view mode)を実行します。

### ◆ clear l2tpv3 fdb

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

◆ **clear l2tpv3 counter**

<説　　明> L2TPv3 のカウンターをクリアします。

<書　　式> clear l2tpv3 counter ethernet <0-2> (|vid <1-4094>)
clear l2tpv3 counter peer
clear l2tpv3 counter peer A.B.C.D
clear l2tpv3 counter session <session-id:1-4294967295>
clear l2tpv3 counter tunnel <tunnel-id:1-4294967295>

◆ **clear l2tpv3 counter access-list**

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

◆ **clear l2tpv3 tunnel**

<説　　明> トンネル ID およびセッション ID を指定して、L2TPv3 トンネルを切断します。

<書　　式> clear l2tpv3 tunnel <tunnel-id:1-4294967295> <session-id:1-4294967295>

◆ **clear l2tpv3 remote-id**

<説　　明> リモートルータ ID を指定して、L2TPv3 を切断します。

<書　　式> clear l2tpv3 remote-id <remote-id:A.B.C.D>

◆ **clear l2tpv3 group**

<説　　明> グループ ID を指定して、L2TPv3 を切断します。

<書　　式> clear l2tpv3 group <group-id:1-65535>

## ■ clear ip bgp

<説　　明>
・　BGP セッションをリセットします。
・　BGP の設定を変更した場合、即時には反映されないため、BGP セッションを一度リセットする必要があります。
- soft out リセット
BGP ネットワークやフィルタリングの変更などの経路情報は、BGP セッションを維持したまま適用することが出来ます。soft out リセットを行うと、設定を内部に反映し、BGP neighbor へ UPDATE メッセージを送信します。
- soft in リセット
BGP neighbor へ ROUTE-REFRESH メッセージを送信し、neighbor へ全ての BGP 経路情報を要求します。ROUTE-REFRESH メッセージを受信した場合は、UPDATE メッセージにより経路情報を送信します。
- hard リセット
BGP の TCP セッションを一旦切断し、neighbor を再確立します。keepalive や holdtime の設定を変更した場合は、ソフトリセットでは変更が反映されないためハードリセットを行ってください。
ハードリセットを行う場合は、soft (in|out)を指定しません。

○ bgp *
<書　　式> clear ip bgp *
clear ip bgp * soft (in|out)
<備　　考> すべての peer とのセッションをリセットします。

○ bgp <AS:1-65535>
<書　　式> clear ip bgp <AS:1-65535>
clear ip bgp <AS:1-65535> soft (in|out)
<備　　考> AS 番号を指定して、セッションをリセットします。

○ bgp A.B.C.D
<書　　式> clear ip bgp A.B.C.D
clear ip bgp A.B.C.D soft (in|out)
<備　　考> Neighbor の IP アドレスを指定して、セッションをリセットします。

## ◆ clear arp

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

## ◆ clear ipv6 neighbors

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

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

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

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

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

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

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

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

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

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

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

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

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

◆ **clear ppp <0-4> mobile data-usage**
<説　　明> PPP の通信量をクリアします。
<書　　式> clear ppp <0-4> mobile data-usage
<備　　考> 通信量は、以下の場合にクリアします。
・　本コマンド実行時
・　schedule による ppp 通信クリア実行時
・　interface ppp を削除した場合
・　mobile limit data-usage を無効にした場合
・　INIT ボタンで、本装置を工場出荷時の状態で起動した場合

◆ **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

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

### ◆ cancel rollback

<説　　明> ロールバックを無効にすることが出来ます。
<書　　式> clear rollback
<備　　考>

- Rollback 有効の状態で config を復帰した後、システム再起動を行う前に、cancel rollback を実行することで、rollback を無効にすることが出来ます。
- システム再起動後、rollback timer が起動している状態で、cancel rollback を実行しても、rollback timer は停止しません。

## ■ 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 インタフェースの番号を指定して、PPP の接続を開始します。
<書　　式> connect ppp <0-4>

### ○ reconnect ppp

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

### ○ reconnect tunnel

<説　　明> Tunnel インタフェースの番号を指定して、Tunnel の再接続を行います。
<書　　式> reconnect tunnel <0-1023>

### ○ connect l2tp

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

○ **connect l2tpv3**

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

○ **connect ipsec**

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

◆ **disconnect**

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

◆ **format**

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

◆ **eject**

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

◆ 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。

| | |
|---|---|
| nxrg240#ping | 入力可能なパラメータ |
| Protocol [ip]: | ip\|ipv6 |
| Target IP address: | A.B.C.D\|X:X::X:X\|FQDN |
| Repeat count [5]: | 1-2147483647 |
| Datagram size [100]: | 36-18024 |
| Interval in seconds [1]: | 0-10 |
| Extended commands [n]: | n(ping を実行)\|y(インタラクティブモードを継続) |
| Source address or interface: | A.B.C.D\|X:X::X:X\|INTERFACE |
| Type of service [0x0]: | 0x00-0xff |
| Set DF bit in IP header? [no]: | no\|yes |
| Data pattern [0xABCD]: | 0x0000-0xffff |

◆ **traceroute**

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

| | |
|---|---|
| nxrg240#traceroute | 入力可能なパラメータ |
| Protocol [ip]: | ip\|ipv6 |
| Target IP address: | A.B.C.D\|X:X::X:X\|FQDN |
| Source address: | A.B.C.D\|X:X::X:X |
| Numeric display [n]: | n\|y |
| Timeout in seconds [2]: | 0-3600 |
| Probe count [3]: | 1-65535 |
| Maximum time to live [30]: | 1-255 |
| Port Number [33434]: | 1025-65535 |

◆ **ssh**

<説　　明> SSH 接続を開始します。

<書　　式>

ssh (ip|ipv6) (A.B.C.D|X:X::X:X|FQDN) user USERNAME [(source A.B.C.D|X:X::X:X)]
ssh (ip|ipv6) (A.B.C.D|X:X::X:X|FQDN) user USERNAME version 1
[cipher (3des|blowfish|des)] [(source A.B.C.D|X:X::X:X)]
ssh (ip|ipv6) (A.B.C.D|X:X::X:X|FQDN) user USERNAME version 2
[cipher (3des-cbc|aes128-cbc|aes128-ctr|aes192-cbc
|aes192-ctr|aes256-cbc|aes256-ctr|arcfour|arcfour128|arcfour256
|blowfish-cbc|cast128-cbc)] [(source A.B.C.D|X:X::X:X)]

<備　　考> ソースアドレスを指定することができます。

◆ **telnet**

<説　　明> Telnet 接続を開始します。

<書　　式>

telnet (A.B.C.D||X:X:X:X::X|FQDN) (|port PORT) user USER (|source A.B.C.D|X:X::X:X)

<備　　考> ソースアドレスを指定することができます。

◆ **logout**

<説　　明> CLI からログアウトします。

<書　　式> logout

◆ **get system statistics cpu**

<説　　明>

・　指定した間隔と回数で、CPU 使用率を取得する機能です。
・　コマンドを実行した時刻より、指定した間隔で指定した回数だけ、CPU 使用率の計算・出力を行います。
・　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 (0|1|all|total) <interval:1-86400> <count:1-65535>

<　例　>

・　実行例を下記に示します。

nxrg240#get system statistics cpu 1 1 5

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 14:13:53 | CPU# | %CPU | %user | %nice | %system | %idle | %iowait |
| 14:13:54 | 1 | 5.00 | 0.00 | 0.00 | 5.00 | 95.00 | 0.00 |
| 14:13:55 | 1 | 0.00 | 0.00 | 0.00 | 0.00 | 100.00 | 0.00 |
| 14:13:56 | 1 | 5.00 | 0.00 | 0.00 | 5.00 | 95.00 | 0.00 |
| 14:13:57 | 1 | 0.00 | 0.00 | 0.00 | 0.00 | 100.00 | 0.00 |
| 14:13:58 | 1 | 5.00 | 0.00 | 0.00 | 5.00 | 95.00 | 0.00 |
| AVERAGE | 1 | 3.00 | 0.00 | 0.00 | 3.00 | 97.00 | 0.00 |

◆ **reset**

<説　　明> モバイルモジュール／ WiFi モジュールを手動リセットする機能です。
<書　　式> reset mobile <0-1>
　　reset wifi <0>

■ **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 ethernet <0-2> vid <1-4094> (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

◆ **show version**

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

◆ **erase**

<説　　明> Flash ROM 上のファイル、ファームウェア、コンフィグを消去します。
<書　　式> erase firmware
　　erase flash （設定ファイルの保存領域）
　　erase flash1（ログの保存領域）
　　erase startup-config
<備　　考> erase flash で、flash1 上のファイルが削除されることはありません。

◆ **delete flash**

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

◆ **delete bootup-config**

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

◆ **copy config startup-config**

<説　　明> config を startup-config にコピーします。
<書　　式> copy config startup-config (|all)
<備　　考>

- all 指定がない場合は、config のみ startup-config にコピーします。
- all 指定の場合は、config/ssh 鍵 /ipsec 証明書の全てを flash にコピーします（save config と同じです）。

◆ **sleep system**

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

◆ **shutdown system**

<説　　明> shutdown 状態へと遷移します。
<書　　式> shutdown system
　　shutdown system timer <1-31536000>
　　shutdown system schedule <NUM>
<備　　考>
・　shutdown/resume についての詳細は、電源管理機能(global mode)を参照してください。
　< NXR-G050 >
　・ shutdown 状態に移行すると、すべての LED が消灯します。
　・ timer を設定しない場合は、365 日間(31,536,000[sec])が設定されます。
　・ スケジュール機能で resume させる場合は、resume の schedule 番号を指定します。
　・ 手動で resume させる場合は、すべての LED の消灯を確認して(1 分以上経過して)から、電源供給を実施します。または、opt ボタンを押下します。

◆ **show temper**

<説　　明> 本装置の温度状態および温度を表示します。
<書　　式> show temperature
<備　　考> nxrg240#show temper
　　degrees: 41.5
　　status : normal

◆ **show ip host**

<説　　明> IP アドレスとホスト名の組み合わせを表示します。
<書　　式> show ip host
<備　　考>
・　IP アドレスとホスト名の組み合わせは、ip host FQDN A.B.C.D(global mode)にて設定します。

◆ **wol send name**

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

◆ **wol send interface**

<説　　明> Ethernet フレームタイプの WOL(Wake On LAN:マジックパケット)を送信します。
<書　　式> wol send interface INTERFACE HH:HH:HH:HH:HH:HH
ethernet (|<1-65535> <1-65535>) (|broadcast)
wol send interface INTERFACE HH:HH:HH:HH:HH:HH
ethernet type <1501-65535> (|<1-65535> <1-65535>) (|broadcast)
<備　　考>

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

◆ **wol send interface**

<説　　明> UDP パケットタイプの WOL(Wake On LAN:マジックパケット)を送信します。
<書　　式> wol send ip (A.B.C.D|FQDN) H:H:H:H:H:H (|<1-65535> <1-65535>)
wol send ip (A.B.C.D|FQDN) H:H:H:H:H:H port <1-65535> (|<1-65535> <1-65535>)
<備　　考>

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

<備　　考>

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

◆ **show wlan**

<説　　明> 無線インタフェースの情報を表示します。
<書　　式> show wlan ssid WORD
show wlan staion ssid WORD
show wlan staion wlan <0-3>

◆ **search-wifi**

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

■ **clear wlan deauth**

<説　　明> Deauthentication を送信します(帰属関係を破棄します)。

○ ssid WORD

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

○ ssid WORD MAC

<説　　明>

- 該当する SSID、かつ該当する MAC アドレスに対して、deauthentication を送信します(帰属関係を破棄します)。

<書　　式> clear wlan deauth ssid WORD HH:HH:HH:HH:HH:HH

○ wlan <0-3>
<説　　明> インタフェース単位で、deauthentication を送信します(帰属関係を破棄します)。
<書　　式> clear wlan deauth wlan <0-3>

○ wlan <0-3> MAC
<説　　明>
・　該当するインタフェース、かつ該当する MAC アドレスに対して、deauthentication を送信します(帰属関係を破棄します)。
<書　　式> clear wlan deauth wlan <0-3> HH:HH:HH:HH:HH:HH

**◆ connect lxc console**
<説　　明> 起動中の LXC に、コンソール接続します。
　　LXC が停止中の場合、接続できません。
<書　　式> connect lxc console <1-4>
<備　　考> アカウント:ubuntu、初期パスワード:ubuntu でログインします。
　　Ctrl+b q で、LXC コンソールを exit できます。

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

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

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

**◆ show session max**
<説　　明> セッション最大数を表示します。
<書　　式> show session max

**◆ show session count**
<説　　明> 現在のセッション数を表示します。
<書　　式> show session max

**◆ show ip session**
<説　　明> IPv4 のセッション一覧を表示します。
<書　　式> show ip session

**◆ show ipv6 session**
<説　　明> IPv6 のセッション一覧を表示します。
<書　　式> show ipv6 session

**◆ show openflow interface bridge**
<説　　明> openflow interface bridge(仮想スイッチ)の情報を表示します。
<書　　式> show openflow interface bridge <0-4095>
　　show openflow interface bridge <0-4095> flows
　　show openflow interface bridge XX flows (10|11|12|13)
　　show openflow interface bridge <0-4095> summary

◆ **show cpu frequency**

<説　　明> CPU 周波数を表示します。
<書　　式> show cpu frequency

◆ **widestar2 send ppp <0-4> callback**

<説　　明> ワイドスター 2 のパケット着信を許可･禁止します。
<書　　式> widestar2 send ppp <0-4> callback (accept|reject)

■ **flash-initial-config**

・　flash-initial-config から、システム起動することが出来ます。
※詳細は、起動時の config 選択順序(付録 H)を参照してください。

◆ **show flash-initial-config**

<説　　明> flash-initial-config を表示します。
<書　　式> show flash-initial-config xml

◆ **delete flash-initial-config**

<説　　明> flash-initial-config を削除します。
<書　　式> delete flash-initial-config

◆ **copy flash-initial-config**

<説　　明> flash-initial-config を copy(import)します。
<書　　式> copy WORD flash-initial-config
<備　　考>
・　flash-initial-config は、1 つだけです。すでに config が存在する場合、上書き保存します。
・　config の export は出来ません。

◆ **show rollback**

<説　　明> 指定世代へ戻すコマンドリストを確認することが出来ます。
<書　　式> show rollback config (|<1-5>)
<備　　考> 指定世代のコンフィグがない場合は、エラーが表示されます。
<　例　> nxrg260#show rollback config
[Command list]:
==========
interface ethernet 2
ip address 192.168.2.254/24
exit
wifi 1
no txpower
exit

◆ **configure rollback**

<説　　明> 指定した世代まで config を戻すことが出来ます。
<書　　式> configure rollback (|<1-5>)
<備　　考> 指定世代のコンフィグがない場合は、エラーが表示されます。
<　例　> nxrg260#configure rollback 1
Proceed with rollback? [y/n]: y
% Finished a rollback of config.

◆ **copy WORD config**

<説　　明> config(running-config)に、設定を復帰します。
<書　　式> copy WORD config (|source A.B.C.D|X:X::X:X)
　　copy WORD config rollback (restart|revert) (|source A.B.C.D|X:X::X:X)
<備　考 1> rollback restart ロールバック時に、システム再起動します。
　　rollback revert ロールバック時に、システム再起動しません。
<備　考 2> 差分がある場合、command list を確認することが出来ます。

```
nxr#copy disk0:nxr.config config
Found any differences. apply? [y/n/(c)heck]: c
[Command list]:
==========================
interface ethernet 1
  ip address 192.168.1.254/24
  exit
interface ethernet 2
  ip address 192.168.2.254/24
  exit
interface wlan 0
  exit
==========================
apply? [y/n]: y
succeed.
```

◆ **show web-authenticate timer**

<説　　明> Web 認証で認証した端末のタイマー情報を表示します
<書　　式> show web-authenticate timer

◆ **show web-authenticate cert**

<説　　明> Web 認証で設定した証明書ファイルを表示します。
<書　　式> show web-authenticate cert (chain-certificate|certificate|private-key)

◆ **clear web-authenticate timer**

<説　　明> Web 認証で認証した端末を削除します。
<書　　式> clear web-authenticate timer (A.B.C.D|all)

◆ **show mape-rule**

<説　　明> MAP 情報を表示します。
<書　　式> show mape-rule WORD ip address
　　show mape-rule WORD port-set
　　show mape-rule WORD snat (|tcp|udp|icmp)
　　show mape-rule WORD status

◆ **clear mape-rule**
<説　　明> MAP 情報を削除します。
<書　　式> clear mape-rule WORD

◆ **show interface veth**
<説　　明> veth インタフェースの情報を表示します。
<書　　式> show interface veth <0-15>
show interface veth <0-15> bridge
show interface veth <0-15> vid <1-4094>

◆ **get ip route**
<説　　明> 指定した IP アドレスへの経路情報を表示します。
<書　　式> get ip route A.B.C.D
<備　　考> 当該 IP アドレスへの到達性がない場合、エラーメッセージが表示されます。

◆ **create rootfs**
<説　　明> rootfs を作成します。
<書　　式> create rootfs WORD0 extract WORD1
<備　　考>
・　create rootfs diskX:rootfs extract diskY:rootfs.xz で、diskX 上に rootfs を展開することが出来ます。
・　作成した rootfs を lxc に mount するには、mount rootfs コマンド(lxc container モード)を使用します。

◆ **show rest session**
<説　　明> REST-API で使用中のセッション(auth-id)を表示します。
<書　　式> show rest session

◆ **clear rest session**
<説　　明> REST-API の auth-id を削除します。
<書　　式> clear rest session (|WORD)
<備　　考> auth-id を指定した場合、該当する auth-id を削除します。
auth-id を指定しない場合(clear rest session)、すべての auth-id を削除します。

◆ **show ip forbidden-access-wan**
◆ **show ipv6 forbidden-access-wan**
<説　　明>
・　forbidden-access-wan コマンドの状態(パケット数、バイト数、プロトコル、ポート番号)を表示します。
<書　　式> show (ip|ipv6) forbidden-access-wan
<備　　考>
・　WAN(ethernet0 以外のインタフェース)からの接続禁止は、forbidden-access-wan コマンド(global モード)で設定します。

◆ **show ip set**
◆ **show ipv6set**
<説　　明>
・　ipset/ipv6set コマンド(global mode)で設定した IP/IPv6 アドレスのリストを表示します。
<書　　式> show ipset WORD (|file)
　　show ipv6set WORD (|file)

◆ **copy XXXX zmodem**
<説　　明>
・　ZMODEM プロトコルを用いて、本装置から作業用端末に、XXXX(当該情報)を転送(export)します。
<書　　式> copy XXXX zmodem
<備　　考>
・　XXXX には、以下の情報を指定することが出来ます。
bootlog、century-tech-support、config、dump、reachability-log、resource-log、show-config、startup-config、syslog、tech-support、内部・外部ストレージのファイル
・　ZMODEM プロトコルに対応したソフトウェア(Tera Term 等)を、作業用端末で使用します。

◆ **copy zmodem XXXX**
<説　　明>
・　ZMODEM プロトコルを用いて、作業用端末から本装置に、XXXX(当該情報)を転送(import)します。
<書　　式> copy zmodem XXXX
<備　　考>
・　XXXX には、以下の情報を指定することが出来ます。
config、flash-initial-config、startup-config、内部・外部ストレージのファイル

◆ **show dns-intercept**
<説　　明> DNS インターセプトのドメインリスト、およびステータスを表示します。
<書　　式> show dns-intercept domain WORD
　　show dns-intercept status (|<0-3>) (|detail)
<備　　考>
・　WORD には、ip dns-intercept setname WORD(global mode)で指定した、ドメインリスト名を指定します。

◆ **show sip-nat**
<説　　明> SIP NAT 機能の有効 / 無効(on/off)を表示します。
<書　　式> show sip-nat

◆ **show bond**
<説　　明> ボンディングインタフェースのステータスを表示します。
<書　　式> show bond <0-15> (status|lacp)
　　show bond list
<備　　考> 指定できるインタフェース番号は、機種によって異なります。

◆ **reset bond**
<説　　明> ボンディングインタフェースの active member を指定して切り替えます。
<書　　式> reset bond <0-15> active-member ethernet <0-2>

◆ **copy WORD warplink-sps-initial-config**
<説　　明> warplink-sps-initial-config を copy(import)します。
<書　　式> copy WORD warplink-sps-initial-config
<　例　> copy disk0:nxr.xml warplink-sps-initial-config

◆ **delete warplink-sps-initial-config**
<説　　明> warplink-sps-initial-config を削除します。
<書　　式> delete warplink-sps-initial-config

◆ **show warplink-sps-initial-config**
<説　　明> warplink-sps-initial-config を xml 形式で表示します。
<書　　式> show warplink-sps-initial-config xml

◆ **show warplink-sps**
<説　　明> 現在と次回の動作モード、および warplink-sps のステータスを表示します。
<書　　式> show warplink-sps

◆ **copy config cms**
<説　　明> config(xml)を cms にコピーします。
<書　　式> copy config cms WORD
<備　　考> WORD には、コンフィグのラベルを指定します。

◆ **copy show-config cms**
<説　　明> config(show-config)を cms にコピーします。
<書　　式> copy show-config cms WORD
<備　　考> WORD には、コンフィグのラベルを指定します。

◆ **delete cms config**
<説　　明> CMS に保存している本装置のコンフィグを削除します。
<書　　式> delete cms config WORD
<備　　考> WORD には、コンフィグのラベルを指定します。

◆ **reset cms config**
<説　　明> CMS に保存している本装置のコンフィグに「デフォルト指定」を設定します。
<書　　式> reset cms config default WORD
<備　　考> WORD には、コンフィグのラベルを指定します。

◆ clear cms config
<説　　明> CMS に保存している本装置のコンフィグから「デフォルト指定」を解除します。
<書　　式> clear cms config default

◆ show cms config-list
<説　　明> CMS に保存している本装置のコンフィグリストを表示します。
<書　　式> show cms config-list

◆ show ip access-list-dynamic
<説　　明> 動的 IP アクセスリストのステータスを表示します。
<書　　式> show ip access-list-dynamic (|WORD)

◆ show ipv6 access-list-dynamic
<説　　明> 動的 IPv6 アクセスリストのステータスを表示します。
<書　　式> show ipv6 access-list-dynamic (|WORD)

◆ speed-test
<説　　明> speed-test を実行します。
　　指定した宛先からファイルをダウンロードすることで、本装置のスループットを測定します。
<書　　式> speed-test <0-5> start
<備　　考> 指定できる番号は、機種により異なります。
　　設定については、speed test mode を参照してください。

◆ show speed-test
<説　　明> speed-test の結果を表示します。
<書　　式> show speed-test
<備　　考> speed-test の結果は、最大 10 件まで表示されます。
　　10 件を超えた場合、古い結果から削除されます。

◆ delete speed-test
<説　　明> speed-test の結果を削除します。
<書　　式> delete speed-test
<備　　考> 本装置をシステム再起動した場合も、speed-test の結果は削除されます。

◆ show snmp ifindex
<説　　明> 現在の ifindex とインタフェースの対応を表示します。
<書　　式> show snmp ifindex

◆ **show dio**

<説　　明> DI/DO 接点の状態を表示します。
<書　　式> show dio
<備　　考> 対応機種(NXR-G050, NXR-G060)

◆ **dio out**

<説　　明> DO 接点に、ON/OFF を出力します。DO 端子 <0-1> は、機種によって異なります。
<書　　式> dio out <0-1> (on|off)
<備　　考> 以下の例では、DO(0)接点に ON を出力します。
nxr#dio out 0 on

<説　　明> hold で指定した時間(sec)、状態をキープします。
<書　　式> dio out <0-1> (on|off) hold <1-300>
<備　　考> 以下の例では、DO(0)接点に ON を出力して、300 秒間(ON を)継続します。
hold 時間経過後、OFF を出力します。
nxr#dio out 0 on hold 300

◆ **clear ip dns-intercept**

<説　　明> dns-intercept 機能で学習した情報をクリアします。
<書　　式> clear ip dns-intercept setname WORD
clear ip dns-intercept setname WORD A.B.C.D
<備　　考> show ip dns-intercept setname WORD で表示される情報をクリアします。

◆ **show century-tech-suppport**

<説　　明> century-tech-support を表示します。
<書　　式> show century-tech-support
<備　　考> 表示される情報は暗号化されています。

◆ **ssh-server sftp**

<説　　明> SFTP(SSH File Transfer Protocol)を有効にします。
<書　　式> ssh-server sftp enable
<　no　> no ssh-server sftp enable

◆ **show system login history**

<説　　明> 本装置へのログイン履歴を表示します。
<書　　式> show system login history

◆ **reset netevent**

<説　　明> ネットイベントの track(manual)の状態を、手動で設定(up/down)します。
<書　　式> reset netevent track <1-255> (up|down)
reset netevent track <1-255> (up|down) (timer <10-604800>|HH:MM:SS)
<備　　考> timer で時間を設定した場合、指定した時間が経過すると、設定を元に戻します。

# 第 5 章　global mode

◆ **移行 command**

nxrg240#**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#

■ **show**

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

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

◆ **hostname**

<説　　明> 本装置のホスト名を設定します。
<書　　式> hostname HOSTNAME
<備　　考> 設定したホスト名は、次のように表示されます。
nxrg240(config)#hostname NXR01
NXR01(config)#

### ◆ fast-forwarding

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

- 以下のすべての条件を満たすパケットが、fast-forwarding の対象となります。
  - Layer4 TCP/UDP/ESP
  - Layer3 IPv4
  - Layer2 Ethernet（VLAN/PPPoE を含む）
- 上記の条件を満たす場合でも、次のパケットは fast-forwarding の対象外です。
  - IP フォワーディングしないパケット（NXR 自身で処理するパケット）
  - Ethernet ブロードキャスト /マルチキャストパケット
  - IPv4 ヘッダが 20 オクテットではないパケット（オプションには対応しません）
  - ステートフルなプロトコルで、セッションコントロールに使用されるパケット（TCP SYN や FIN 等）
  - アプリケーションで使用されるコントロール用パケット（FTP コントロールや SIP のコントロール）
- また、次の場合も fast-forwarding の対象外です。
  - IP フラグメントには対応していません。
  - いずれかのインタフェースで QoS を有効にすると、fast-forwarding は自動的に無効になります。
- fast-forwarding のセッション最大数:16,384（本書記載の NXR シリーズ）
  - fast-forwarding のセッション最大数に達している場合は、fast-forwarding セッションを新規作成しません。
  - fast-forwarding と L2TPv3 fast-forwarding のセッションは、同一セッションテーブルで管理します。つまり、両方のセッション数の合計が、上記の値を超えることはありません。
  - L2TPv3 fast-forwarding については、global mode の l2tpv3 fast-forwarding コマンドを参照してください。

## ■ ip access-list

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

○ match 条件

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

○ match 時の動作

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

<書　式>

○ ip/protocol

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

○ icmp

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

○ tcp/udp

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

○ TCP option

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

○ No
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 mode を参照）で、ACL をインタフェースに適用してください。
- log を指定すると、フィルタログ機能（syslog mode 参照）を有効にします。パケットが当該フィルタにマッチした場合、syslog に出力します。1 秒間に出力可能な log 数の最大値は「10」です。すべての ACL にログを設定すると、システムが高負荷状態になる可能性があるため、ログ出力は最小限にとどめるようにしてください。

**■ ipset**

<説　　明>
- 多数の IP アドレスを src/dst で指定する場合、個々に ACL を設定すると、管理者の負担増や性能低下を引き起こす可能性があるため、IPset に対応しています。
- 各セットは、IP アドレス（mask あり / なし）、IPv6 アドレス（prefix 長指定あり / なし）をリスト化したものです。
- リスト化したテキストファイルを、機器にインポートすることで利用可能になります。
- 1 つのセット内に、IPv4 と IPv6 は、混在できません。
- 本バージョンでは、ip access-list、ipv6 access-list に対応しています。
- IP セットは、src/dst のいずれかを指定します。

<書　　式> ipset setname XXXX file ssh://a.b.c.d/ipset.txt
ipset setname XXXX file ftp://a.b.c.d/ipset.txt
ipset setname XXXX file http|https://a.b.c.d/ipset.txt
ipset setname XXXX file disk0:ipset.txt
ipset setname XXXX file zmodem
ipset setname XXXX file

<備　　考> ipset の例を以下に示します。

```
192.168.0.0/24
192.168.1.0/24
192.168.2.0/24
172.16.1.0/24
172.16.2.0/24
10.0.0.1/32
```

## ■ ipv6set

<書　式> ipv6set setname XXXX file ssh://a.b.c.d/ipv6set.txt
ipv6set setname XXXX file ftp://a.b.c.d/ipv6set.txt
ipv6set setname XXXX file http|https://a.b.c.d/ipv6set.txt
ipv6set setname XXXX file disk0:ipv6set.txt
ipv6set setname XXXX file zmodem
ipv6set setname XXXX file

## ■ 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|src-set WORD|dynamic WORD
destination:any|X:X::X:X/M|X:X::X:X|FQDN|dst-set WORD|dynamic WORD
[<protocol:0-255>|icmpv6|tcp|udp] [mac HH:HH:HH:HH:HH:HH] [log <WORD|>]

○ icmpv6
ipv6 access-list ACL-NAME permit|deny
source:any|X:X::X:X/M|X:X::X:X|FQDN|src-set WORD|dynamic WORD
destination:any|X:X::X:X/M|X:X::X:X|FQDN|dst-set WORD|dynamic WORD
icmpv6 [type code] [mac HH:HH:HH:HH:HH:HH] [log <WORD|>]

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

○ TCP option

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

○ No

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 mode を参照）で、ACL をインタフェースに適用してください。
・　log を指定すると、フィルタログ機能(syslog mode 参照)を有効にします。パケットが当該フィルタにマッチした場合、syslog に出力します。1 秒間に出力可能な log 数の最大値は「10」です。すべての ACL にログを設定すると、システムが高負荷状態になる可能性があるため、ログ出力は最小限にとどめるようにしてください。

### ◆ ip route access-list

<説　　明>

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

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

<備　　考>

・　exact-match を指定した場合は、prefix 長が M のときだけマッチします。exact-match を指定しない場合は、prefix 長が M 以上(M ～ 32)のときにマッチします。
・　0.0.0.0/0 exact-match は、default route(0.0.0.0/0)と同義です。0.0.0.0/0(exact-match なし)は、any と同義です。

### ◆ ipv6 route access-list

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

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

<備　　考>
- exact-match を指定した場合は、prefix 長が M のときだけマッチします。exact-match を指定しない場合は、prefix 長が M 以上(M ～ 128)のときにマッチします。
- ::/0 exact-match は、default route と同義です。::/0(exact-match なし)は、any と同義です。

### ■ ip (snat|dnat)

<説　　明> NAT ルールを追加します。
<書　　式>
○ ip
ip (snat|dnat) NAT-NAME ip
　　<src:>(any|A.B.C.D/M|A.B.C.D) <dst:>(any|A.B.C.D/M|A.B.C.D)
　　<to:A.B.C.D> (|to-end:E.F.G.H)

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

○ protocol
ip (snat|dnat) NAT-NAME <protocol:0-255>
　<src:>(any|A.B.C.D/M|A.B.C.D) <dst:>(any|A.B.C.D/M|A.B.C.D) <to:A.B.C.D> (|to-end:E.F.G.H)
<備　　考> protocol 番号で udp/tcp 番号指定しても port は指定できません。
　　(文字列として udp/tcp を指定してください)

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

○ negate
no ip (snat|dnat) NAT-NAME
<備　　考> NAT ルール(MAT-NAME 全体)を削除します。
no ip (snat|dnat) NAT-NAME NAT-RULE
<備　　考> NAT ルールを個別に削除します。
　　下記のように、削除したい NAT ルールを個別に削除します。
　　no ip snat test ip 192.168.0.0/24 any 1.1.1.1

<設 定 例>
○ **snat の設定例:** Private IP アドレス(192.168.0.0/24)を Global IP(1.1.1.1)アドレスに変換します。
　　ip snat test ip 192.168.0.0/24 any 1.1.1.1

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

○ **static snat の設定例:**
　　ip snat test ip 192.168.0.0/24 192.168.10.0/24 static 192.168.10.0/24
　　たとえば、192.168.0.245 から 192.168.10.247 への送信パケットは、SNAT により src IP が変換(192.168.0.245 → 192.168.10.245)されます。

■ **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**
■ **ipv6 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, ipv6/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)

ipv6 web-auth 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>|icmp|tcp|udp] [mac HH:HH:HH:HH:HH:HH]

○ icmp, icmpv6

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)

ipv6 web-auth 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
　　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)

ipv6 web-auth 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
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)

ipv6 web-auth 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 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

◆ dhcp-server option-space

<説　　明> option 43 で送信するカプセル化データ(サブオプションの集合)を space 名で定義します。
定義した space は、vendor-specific-information space コマンドで指定します。
<書　　式> dhcp-server option-space WORD
< no > no dhcp-server option-space WORD

○ option

<説　　明> カプセル化データに含めるサブオプションの名前、コード、値を定義します。
<書　　式> option WORD code <1-255> {ip (|A.B.C.D)|text (|WORD)|hex (|HEX)}
< no > no option WORD
<備　　考> option は、dhcp-server option-space 内で設定します。
nxr(config)#dhcp-server option-space WORD
nxr(config-dhcp-space)#

**◆ dhcp-server vendor-class**

<説　　明> クライアントが送信する option 60 (Vendor Class Identifier) の値に応じて、
option-space で定義したカプセル化データの値を変更できます。
<書　　式> dhcp-server vendor-class WORD
< no > no dhcp-server vendor-class WORD
<備　　考> WORD は vendor-class を識別するための名前です。
照合する option 60 の値は identifier で設定します。

○ identifier

<説　　明> 照合する option 60 の値を設定します。
この値と一致した場合に、本 vendor-class の設定が適用されます。
<書　　式> identifier {text WORD|hex HEX}
<備　　考> identifier, option-space, option は、dhcp-server vendor-class 内で設定します。
nxr(config)#dhcp-server vendor-class WORD
nxr(config-dhcp-class)#

○ option-space

<説　　明> 値を変更する対象の space 名を指定します。
<書　　式> option-space WORD

○ option

<説　　明> option-space で定義したサブオプションの値を変更します。
<書　　式> option WORD {ip A.B.C.D|text WORD|hex HEX}
< no > no option WORD
<備　　考> WORD には、option-space で定義したオプション名を指定します。

< 例 >
クライアントの option 60 が ”nxr-530” の場合とそれ以外の場合で、
option 43 のカプセル化データ (client-ip) の値を変える設定例です。

```
!
dhcp-server option-space CENTURY
 option client-ip code 1 ip 192.168.0.1
!
dhcp-server vendor-class nxr-530
```

```
 identifier text nxr-530
 option-space CENTURY
 option client-ip ip 192.168.0.2
!
dhcp-server 1
 vendor-specific-information space CENTURY
!
```

## ■ 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 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|
|aes128-gcm-openssh|aes256-gcm-openssh|chacha20-poly1305-openssh)
<　no　> no ssh-server ciphers
<備　　考> 複数指定可能です。

### ○ ssh-server address-family

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

### ○ ssh-server port

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

### ○ ssh-server authentication

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

**○ ssh-server public-key**

<説　　明> admin ユーザに対して、SSH 接続用公開鍵を設定します(最大 5 つまで設定可能)。
<書　　式> ssh-server public-key username admin <0-4>
ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME (|source A.B.C.D|X:X::X:X)
ssh-server public-key username admin <0-4>
ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
ssh-server public-key username admin <0-4>
http|https://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
ssh-server public-key username admin <0-4>
(disk0:FILENAME|disk1:FILENAME) (|source A.B.C.D|X:X::X:X)
ssh-server public-key username admin <0-4> zmodem
< no > no ssh-server public-key username admin <0-4>
<備　　考>

- ソースアドレスを指定することができます。
- SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
  - IPv4 ssh://user@A.B.C.D:port/FILENAME
  - IPv6 ssh://[user@X:X::X:X]:port/FILENAME
- https:// の場合、サーバ証明書の validation を行う。https-:// の場合、validation を行わない。

**○ 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。

**○ ssh-server key-algorithm**

<説　　明> SSH 鍵のアルゴリズム(SSH RSA/SHA1)を有効にします。
<書　　式> ssh-server key-algorithm ssh-rsa enable
<初 期 値> no ssh-server key-algorithm ssh-rsa enable
< no > no ssh-server key-algorithm ssh-rsa enable

## ■ 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

### ○ timeout

<説　　明> http サーバのタイムアウト値を指定します。
<書　　式> http-server timeout <5-300>
<初 期 値> http-server timeout 300

### ○ max-clients

<説　　明> http サーバの最大接続数を指定します。
<書　　式> http-server max-clients <5-200>
<初 期 値> http-server max-clients 5

### ○ keepalive

<説　　明> http サーバのキープアライブの有効／無効を指定します。
<書　　式> http-server keepalive enable
<初 期 値> http-server keepalive enable
<　no　> no http-server keepalive enable

### ○ keepalive timeout

<説　　明> http サーバのキープアライブのタイムアウト値を指定します。
<書　　式> http-server keepalive timeout <5-60>
<初 期 値> http-server keepalive timeout 15

### ○ keepalive max-requests

<説　　明> http サーバのキープアライブの最大リクエスト数を指定します。
<書　　式> http-server keepalive max-requests <10-100>
<初 期 値> http-server keepalive max-requests 100

### ○ auth-fail-lock

<説　　明> 一定回数ログインに失敗すると、一時的にログイン試行を受け付けなくなります。
<書　　式> http-server auth-fail-lock (account|account-ip|ip)
<初 期 値> http-server auth-fail-lock account
<　no　> no http-server auth-fail-lock

## ■ session

### ○ session udp timer

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

### ○ session udp-stream timer

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

### ○ session tcp timer

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

### ○ session tcp time-wait

<説　　明> TCP セッションの TIME_WAIT タイマー(秒)を設定します。
<書　　式> session tcp time-wait <1-85889934>
<初 期 値> session tcp time-wait 120(sec)
<　no　> no session tcp time-wait
<備　　考>

- TIME_WAIT 状態とは、TCP のアクティブ・クローズ後のタイムアウト待ち状態のことです。
- TIME_WAIT タイマーが短い場合、アクティブ・クローズ後に、ネットワーク上の遅延パケットが到着すると、リソース(シーケンス番号やポート番号)が衝突する可能性があります。
- TIME_WAIT タイマーが長い場合、TIME_WAIT 状態のセッションが、セッションテーブルに多数残留することが考えられます。

### ○ session tcp fin-wait

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

### ○ session tcp last-ack

<説　　明> TCP セッションの LAST-ACK 状態のタイムアウト値(秒)を設定します。
<書　　式> session tcp last-ack <1-85889934>
<初 期 値> session tcp last-ack 160
<　no　> no session tcp last-ack

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

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

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

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

**○ session tcp window-check**
<説　　明> TCP window サイズのチェックを有効にします。
<書　　式> session tcp window-check
<初 期 値> session tcp window-check
<　no　> no session tcp window-check

**○ session max**
<説　　明> 最大セッション数を設定します。
<書　　式> session max <4096-262144>
<初 期 値> session max 131072
<　no　> no session max (=session max 131072)

**○ session limit**

<説　　明>
- IP address 毎に conntrack session 数を制限する機能です。一部の USER により、conntrack session を占有されてしまうような障害を防ぐために使用します。
- この制限は、forwarding 処理される packet が対象となります。
- 0 を設定すると、IP address 毎の session 数を制限しません。

<書　　式> session limit <0-65536>
<初 期 値> session limit 0
<　no　　> no session limit

**○ session 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 (<16-32768>|)
<初 期 値> session tcp limit 640
<　no　　> no session tcp limit (= 無制限)
<備　　考>
- NXR が他の端末にフォワーディングするものについては影響しません。
- IPv4/IPv6 それぞれ別にカウントされます。例えば、接続数を 16 に設定した場合、IPv4 と IPv6 の TCP コネクションを、それぞれ 16 まで接続することができます。
- また、設定変更を行った場合、すでに確立しているコネクションには影響しません。それ以降のコネクションが接続制限の対象になります。

**○ session invalid-status-drop enable**

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

<書　　式> session invalid-status-drop enable
<初 期 値> no session invalid-status-drop enable
<　no　　> no session invalid-status-drop enable
<備　　考>
- あるインタフェースに対してのみ適用するには、本機能は無効に設定して、かつ指定インタフェースで session invalid-status-drop-interface enable を有効にします。以下は、ppp 0 インタフェースに適用する場合の設定例です。

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

**○ session checksum**

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

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

**○ session tcp unacknowledged**

<説　　明> TCP セッションの UNACKNOWLEDGED 状態のタイムアウト値(秒)を設定します。
<書　　式> session tcp unacknowledged <1-85889934>
<初 期 値> session tcp unacknowledged 300
<　no　> no session tcp unacknowledged
<備　　考> ESTABLISHED で UNREPLIED 状態の TCP セッションが対象です。

## ■ 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)

**○ 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>

・ 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 L2TPv3over UDP をサポートします。

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

・ その他の基本仕様については、下記のとおりです。

　・ L2TP(v2)との互換性はありません。

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

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

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

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

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

**○ hostname**

<説　　明> 本装置のホスト名を設定します。LCCE(L2TP Control Connection Endpoint)の識別に使用します。
<書　　式> l2tpv3 hostname L2TPv3-HOSTNAME
<備　　考> 省略時は、hostname コマンドで設定したものを使用します。
<　no　　> no l2tpv3 hostname

**○ router-id**

<説　　明> 本装置のルータ ID を、IP アドレス形式で設定します。LCCE のルータ ID の識別に使用します。
<書　　式> l2tpv3 router-id A.B.C.D
<　no　　> no l2tpv3 router-id

**○ mac-learning**

<説　　明>
・　L2TPv3 MAC アドレス学習機能の有効 /無効を設定します。
　- 本装置が受信したフレームの MAC アドレスを学習し、不要なトラフィックの転送を抑制する機能です。
　- ブロードキャスト、マルチキャストについては、MAC アドレスに関係なく、すべて転送します。
<書　　式> l2tpv3 mac-learning (|always) (|unique)
<初 期 値> l2tpv3 mac-learning enable
<　no　　> no l2tpv3 mac-learning enable
<備　　考>
・ always を指定すると、L2TPv3 MAC Address 学習 Always 機能を有効にします。
　- L2TPv3 MAC Advertise Frame 送信機能を有効(mac-advertise enable)にした場合、アクティブセッションが作成されたときに、L2TPv3 MAC Advertise Frame を送信しますが、Xconnect に関連するセッションが 1 つも確立されていない場合は、ローカルテーブルにて MAC アドレスが学習されない為、ローカルテーブルに MAC アドレス情報が存在しません。
　- Always を指定すると、セッションが 1 つも確立されていない場合でも、ローカルテーブルに MAC アドレス学習を行います。
　- 本機能(always)はデフォルトで無効です。
・ unique を指定すると、L2TPv3 MAC Address 学習 unique 機能を有効にします。
　- 本機能を有効にするには、l2tpv3 xconnect mode で、次の設定が必要になります。
　- nxrg240(config-l2tpv3-xconnect)#mac-learning unique enable
　- ネットワーク構成によっては、ある一つの Xconnect の Local Table、FDB に同じ MAC アドレスが登録されることがあります。本機能を有効にすると、新しく学習した MAC アドレスが、Local Table、FDB のどちらか一方に登録されるため、上記のような状態を回避することが出来ます。
　- ある一つの Xconnect で、LoopDetect 機能と共存した場合、LoopDetect の FrameDrop 処理を優先します。つまり、この場合は、MAC アドレス学習 unique 機能は動作しないことになります。
　- 本機能(unique)はデフォルトで無効です。

**○ mac-aging**

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

**○ loop-detect**

<説　　明> ループ検出機能を有効にします。
<書　　式> l2tpv3 loop-detect enable
<初 期 値> no l2tpv3 loop-detect enable
<　no　> no l2tpv3 loop-detect enable
<備　　考>
フレームの転送がループしてしまうことを防ぐ機能です。この機能が有効になっているときは、以下の 2 つの場合にフレームの転送を行いません。

- Xconnect インタフェースより受信したフレームの送信元 MAC アドレスが FDB に存在するとき。
- L2TP セッションより受信したフレームの送信元 MAC アドレスがローカル MAC テーブルに存在するとき。

**○ send-known-unicast**

<説　　明> L2TPv3 の known unicast フレームを送信します。
<書　　式> l2tpv3 send-known-unicast enable
<初 期 値> no l2tpv3 send-known-unicast enable
<　no　> no l2tpv3 send-known-unicast enable
<備　　考>
known unicast フレームとは、MAC アドレス学習済みの unicast フレームのことです。この機能を「無効」にしたときは、以下の場合に unicast フレームの転送を行いません。

- Xconnect インタフェースより受信した Unicast フレームの送信先 MAC アドレスが Local MAC テーブルに存在するとき。

**○ udp source-port**

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

**○ udp path-mtu-discovery**

<説　　明> L2TPv3 over UDP 使用時に、Path MTU Discovery 機能の有効 / 無効を設定します。
初期値は無効です。
<書　　式> l2tpv3 udp path-mtu-discovery enable
<初 期 値> no l2tpv3 udp path-mtu-discovery enable
<　no　> no l2tpv3 udp path-mtu-discovery enable
<備　　考> 本機能を有効にした場合、送信する L2TPv3 パケットの DF(Don't Fragment)ビットを 1 にします。
無効にした場合は、DF ビットを常に 0 にします。ただし、カプセル化したフレーム長が送信インタフェースの MTU 値を超過する場合は、本設定に関係なくフラグメントされ、DF ビットを 0 にして送信します。

**○ path-mtu-discovery**

<説　　明> L2TPv3 over IP 使用時に、Path MTU Discovery 機能の有効 / 無効を設定します。
初期値は無効です。
<書　　式> l2tpv3 path-mtu-discovery enable
<初 期 値> no l2tpv3 path-mtu-discovery enable
<　no　> no l2tpv3 path-mtu-discovery enable

**○ snmp enable**

<説　　明> L2TPv3 用の SNMP エージェント機能を有効にします。本機能を有効にすると、L2TPv3 に関する MIB の取得が可能になります。
<書　　式> l2tpv3 snmp enable
<初 期 値> no l2tpv3 snmp enable
<　no　> no l2tpv3 snmp enable

**○ snmp trap**

<説　　明> L2TPv3 の SNMP trap 機能を有効にします。本機能を有効にすると、L2TPv3 に関する Trap 通知が可能になります。
<書　　式> l2tpv3 snmp trap
<初 期 値> no l2tpv3 snmp trap
<　no　> no l2tpv3 snmp trap

**○ tos**

<説　　明>

・ L2TPv3 にてトンネリングされるフレームの L3 プロトコルが IP または IPv6 の場合に、IP/IPv6 header の ToS 値(IPv6 の場合、traffic class)や USER が指定した ToS 値を l2tpv3 パケットの IP header の IPv4ToS field(L2TPv3 session packet)に設定する機能です。Control message は、0xd0 で送られます。

<書　　式> l2tpv3 tos enable

<初 期 値> no l2tpv3 tos enable

<　no　　> no l2tpv3 tos enable

<備　　考>

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

**○ tunnel tos**

<説　　明> L2TPv3 ToS 設定機能有効時に、Control message の ToS 値を指定することが出来ます。

<書　　式> l2tpv3 tunnel tos [|<0-252>]

<初 期 値> l2tpv3 tunnel tos 208 (=l2tpv3 tunnel tos)

<　no　　> no l2tpv3 tunnel tos

<備　　考>

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

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

**○ fast-forwarding**

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

・ fast-forwarding の対象となるのは、送信元 / 送信先の MAC アドレスがユニキャストのフレームです。
  - MAC アドレスがマルチキャスト / ブロードキャストのフレームは、fast-forwarding の対象外です。
  - システムの fast-forwarding とは異なり、プロトコル(IPv4/TCP/UDP 等)には依存しません。
・ フラグメントされた L2TPv3 パケット(再構築を必要とするパケット)を受信した場合は、fastforwarding の対象外です(システムの fast-forwarding と同様です)。
・ フラグメントパケットの送信時(本装置がフラグメントする場合)は、L2TPv3 tunneling および L2TPv3 over IPsec(policy base)に限り、fast-forwarding の対象となります。
  - L2TPv3 over IPsec (route base)は、fast-forwarding の対象外です。
・ 以下の条件に当てはまる場合に、該当する L2TPv3 フレームを fast-forwarding します。
  ※ L2TPv3 が MAC アドレスを保持するテーブルは 2 種類あり、LAN 側が local table、WAN 側が FDB です。
  - L2TPv3 フレーム送信時、受信フレームの送信先 MAC アドレスが FDB に存在する場合に、上りの fastforwarding セッションを作成します。
  - L2TPv3 フレーム受信時、受信フレームの送信先 MAC アドレスが local table に存在する場合に、下りの fast-forwarding セッションを作成します。
  - L2TPv3 フレーム受信時、受信フレームの送信先 MAC アドレスが FDB に存在する場合に、(WAN-WAN 折り返しの)fast-forwarding セッションを作成します。ただし、同じセッション(グループ)には、折り返しません。
  ※ 片方向通信の場合、local table もしくは FDB に該当 MAC が存在し、片方向の fast-forwarding セッションを作成しますが、MAC aging-time のタイムアウトが発生すると、local table もしくは FDB から該当 MAC が存在しなくなるため、その後は fast-forwarding の対象外となります。
・ fast-forwarding と L2TPv3 fast-forwarding のセッションは、同一セッションテーブルで管理します。
・ fast-forwarding については、global mode の fast-forwarding コマンドを参照してください。

<注　　意>

※本機能を有効にする場合は、次の順に設定してください。

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

② L2TPv3 の MAC アドレス学習機能を有効にします(default は有効です)。
nxr(config)# l2tpv3 mac-learning

③ L2TPv3 の fast-forwarding を有効にします(default は無効です)。
nxr(config)# l2tpv3 fast-forwarding enable

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

○システムの fast-forwarding が無効時に、L2TPv3 の fast-forwarding を有効にした場合
nxr(config)#l2tpv3 fast-forwarding enable
% First configure "fast-forwarding enable" on global mode.

○L2TPv3 の fast-forwarding が有効時に、L2TPv3 の MAC アドレス学習機能を無効にした場合
nxr(config)#no l2tpv3 mac-learning
% First deconfigure "l2tpv3 fast-forwarding enable" on global mode.

< 例 >

● PtoP 上り / 下り

NXR_1 で fast-forwarding のエントリーを追加するときのフレームの流れは、次のとおりです。なお、PC_A と PC_B は、同一ネットワーク上に存在します。

PC_A ----- NXR_1 =====L2TPv3===== NXR_2 ----- PC_B

○ PC_A から PC_B に対して ping を実行します。

① PC_A から ARP REQUEST をブロードキャストで送信します。
NXR_1 は、local table に PC_A の MAC アドレスを登録します。

② PC_B から PC_A に、ARP REPLY を送信します。
NXR_1 は、FDB に、PC_B の MAC アドレスを登録します。
PC_A の MAC アドレスが、local table 上に登録されているので、fast-forwarding のエントリー(下り)を追加します。

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

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

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

● PtoMP 折り返し

NXR_1 で fast-forwarding のエントリーを追加するときのフレームの流れは、次のとおりです。なお、PC_A と PC_B と PC_C は、同一ネットワーク上に存在します。

PC_C ----- NXR_1 =====L2TPv3===== NXR_2 ----- PC_A
=====L2TPv3===== NXR_3 ----- PC_B

○ PC_A から PC_B に対して ping を実行します。

① PC_A から ARP REQUEST をブロードキャストで送信します。
NXR_1 は、NXR_2 向きの FDB に、PC_A の MAC アドレスを登録します。

② PC_B から PC_A に、ARP REPLY を送信します。
NXR_1 は、NXR_3 向きの FDB に、PC_B の MAC アドレスを登録します。
PC_A の MAC アドレスが、NXR_2 向きの FDB 上に登録されているので、fast-forwarding のエントリー(折り返し)を追加します。

③ PC_A から PC_B に、ICMP REQUEST を送信します。
PC_B の MAC アドレスが、NXR_3 向きの FDB 上に登録されているので、fast-forwarding のエントリー(折り返し)を追加します。

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

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

## ■ IPv4

### ◆ arp

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

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

### ◆ ip route

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

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

<　null　>

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

< dhcp >

- DHCP で取得したゲートウェイ情報を next hop に指定します。

◆ **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 IPv4address の arp request を受信した際に、syslog 出力する機能です。初期値は無効です。
<書　　式> ip arp-invalid-log
<初 期 値> no ip arp-invalid-log
<　no　> no ip arp-invalid-log
<備　　考> Invalid arp を受信した際には、下記のような log が syslog に出力されます。なお、この機能を有効にした場合、message が大量に出力される場合があるため、「Syslog message suppress 機能(syslog mode 参照)」を有効にすることを推奨します。

<< Invalid arp 受信 log format >>
Jun 16 18:21:06 nxrg240 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

■ **IP martian-log 機能**

- Source/destination IP アドレス、あるいは、ARP sender IP/target IP が、martian アドレスである IPv4 パケット /ARP パケットを受信した際に、ログを出力します。
- martian パケットの判定は、ルーティングテーブルの探索時に行います。martian パケットであると判断した場合は、ログを出力して、パケット(フレーム)を破棄します。

※ただし、martian パケットであっても、ip martian-log 以外のチェックで破棄した場合は、ログを出力しません。

- Target IP が、127.0.0.0/8、マルチキャストアドレス、ブロードキャストアドレスのパケットは、ARP 処理時に破棄するため、martian-log は出力しません。
- Source/destination 共に、0.0.0.0 のパケットは、ルーティングテーブル探索の前に、不正パケットとして破棄します。

□ Martian アドレス判定処理

○ martian source

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

- マルチキャストアドレス
- ループバック(127.0.0.1)や 0.0.0.0 など使用不可のアドレス
- ARP を受信したインタフェースの IP と sender IP が同じアドレス
- 受信した IP パケットの source IP が、本装置の IP と同じアドレス(ループパケット)

ただし、ip nat-loopback の適用パケット(source/destination IP が同じパケット)を受信した場合は、martian-log は出力せず、転送処理を行います。

○ martian destination

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

**◆ ip martian-log**

<説　　明> IP martian-log 機能を有効にします。
<書　　式> ip martian-log（有効）
<初 期 値> no ip martian-log（無効）
<　no　> no ip martian-log
<備　　考>

- パケット毎にログを出力すると、システムに非常に負荷がかかり、DoS 攻撃 etc によってサービス停止状態になる可能性があります。そのため、単位時間当たりに出力可能なログの数を制限しています。
- 5 秒間に出力可能なログの数は、最大 10 です(設定の変更は出来ません)。
- 出力できなかったログは、その後のログ出力時に、supress message 数としてログ出力します。

◆ **ip reassemble-output**

<説　　明>

・ インタフェースの MTU(あるいは PMTU)より大きいパケットを IP forwarding する際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。
本設定有効時、NXR がリアセンブルしたパケットは、以下のようにフラグメント処理を行います。
  - fragmented packet(パケットの断片)が MTU を超える場合、リアセンブルしたパケットを再度 MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、リアセンブルしたパケットを出力します。

<書　　式> ip reassemble-output

<初 期 値> ip reassemble-output

<　no　　> no ip reassemble-output

<備　　考1>

・ 上記の場合(本設定が有効の場合)、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易な IP 実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズで NXR からパケットを出力します。また、出力時の IP フラグメント処理は、次のようになります。
  - fragmented packet(パケットの断片)が MTU を超える場合、受信した fragmented packet を MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、受信した fragmented packet をそのままのサイズで出力します。
・ Default は、global 設定および interface 設定ともに有効です。Global 設定と interface 設定の AND 条件により、本機能が有効か無効かを判定します。本設定は、IP forwarding するパケットにのみ影響します。
・ 受信時のサイズを記載しておくバッファが 32 個しかないため、33 個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-output が有効な場合と同様に処理します。

## ■ ip local pool

### ○ address

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

### ○ exclude-address

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

## ■ IPv6

### ◆ ipv6 forwarding

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

### ◆ ipv6 neighbor

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

### ◆ ipv6 route

<説　　明> ipv6 スタティックルートを設定します。
<書　　式> ipv6 route X:X::/M GATEWAY (|<distance:1-255>)
ipv6 route X:X::/M INTERFACE (|<distance:1-255>)
ipv6 route X:X::/M GATEWAY INTERFACE (|<distance:1-255>)
ipv6 route X:X::/M ra INTERFACE (|<distance:1-255>)
ipv6 route X:X::/M dhcp INTERFACE (|<distance:1-255>)
< no > no ipv6 route X:X::/M GATEWAY (|<distance:1-255>)
no ipv6 route X:X::/M INTERFACE (|<distance:1-255>)
no ipv6 route X:X::/M GATEWAY INTERFACE (|<distance:1-255>)
no ipv6 route X:X::/M ra INTERFACE (|<distance:1-255>)
no ipv6 route X:X::/M dhcp INTERFACE (|<distance:1-255>)
< null >

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

< ra >

- RA で取得したゲートウェイ情報を next hop に指定します。

< dhcp >

- DHCPv6 で取得したゲートウェイ情報を next hop に指定します。

### ◆ ipv6 bridge

<説　　明> フレッツドットネットで、ISP(フレッツ網)側より送信されてくる IPv6 パケットをブリッジする機能です。
ブリッジを行うインタフェースは、イーサネットのみ指定することができます。
<書　　式> ipv6 bridge ethernet <0-2> ethernet <0-2>
< no > no ipv6 bridge
<備　　考> IPv6 ブリッジを有効にすると、NXR 宛の IPv6 パケットは NXR にて処理されます。
non-unicast や NXR 宛以外の IPv6 パケットはブリッジされます(non-unicast フレームは、NXR で処理され、かつブリッジもされます)。

### ■ track

<説　　明>

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

<備　　考>

○ delay/retry

- 復旧時(event up と判別した場合)から実際に up 時の action を実行するまでに delay を設定することができます。Delay timer が動作している場合は、track は down state が維持され、この間にも ipreachability 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、downaction を実行します。
- Initial timeout は、default で無効です。有効時の default の initial timeout 値は 180sec です。なお、initial timeout 値は、10 ～ 3600sec の範囲で設定することが出来ます。

○ interface link 状態監視

<書　式>

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

<備　考>

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

○ 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>
　　track <trackid:1-255> bgp neighbor <PEER_IPv6:X:X::X:X>
　　track <trackid:1-255> bgp neighbor PEER_IPv6 delay <10-3600>
　　track <trackid:1-255> bgp neighbor PEER_IPv6 initial-timeout (|<10-3600>)
　　track <trackid:1-255> bgp neighbor PEER_IPv6 initial-timeout <10-3600> delay <10-3600>
<備　　考> 指定した peer ip との neighbor 確立後から他の state への変化を監視します。

○ VRRP の状態監視
<書　　式> track <trackid:1-255> vrrp ip <vrrpid:1-255> interface ethernet <0-2>
<　no　　> no track <trackid:1-255>
<備　　考>
・ ethernet のみ有効です。
・ master から backup/init への変化、または backup/init から master への変化を監視します。

○ ip/ipv6 neighbor 監視
<書　　式>
　　track <1-255> ip neighbor (A.B.C.D|FQDN) interface IFNAME
　　track <1-255> ip neighbor (A.B.C.D|FQDN) interface IFNAME
　　　　<10-32767> <0-255> (delay <10-3600>|)
　　track <1-255> ip neighbor (A.B.C.D|FQDN) interface IFNAME delay <delay:10-3600>
　　track <1-255> ipv6 neighbor (X:X::X:X|FQDN) interface IFNAME
　　track <1-255> ipv6 neighbor (X:X::X:X|FQDN) interface IFNAME
　　　　<10-32767> <0-255> (delay <10-3600>|)
　　track <1-255> ipv6 neighbor (X:X::X:X|FQDN) interface IFNAME delay <delay:10-3600>
<備　　考>
・ 送信間隔、retry 回数、出力インタフェースを設定することが出来ます。

○ manual 監視(自動監視を行いません)
<書　　式> track <1-255> manual
<　no　　> no track <1-255>
<備　　考> 手動のイベントで、デフォルトルートを切り替える設定例です。
nxr(config)# track 1 manual
nxr(config)# ip route 0.0.0.0/0 192.168.0.254 netevent 1 inactive
track 1 を手動で down(障害発生状態)にします(デフォルトルート無効)。
nxr# reset netevent track 1 down
track 1 を手動で up(正常状態)にします(デフォルトルート有効)。
nxr# reset netevent track 1 up

◆ **ipsec nat-traversal**

<説　　明>
- 本装置では、NAT-Traversal 機能をサポートしているため、NAT 装置の配下に本装置が設置されている状況でも、IPsec 接続を行うことが出来ます。
- IKEv1 では、NAT-Traversal 機能の有効 / 無効を指定することが可能ですが、IKEv2 では自動的に有効になり、無効にすることは出来ません。
- NAT-Traversal は、IPv4 のみ対応しています。

<書　　式> ipsec nat-traversal enable　　（NAT-Traversal 有効）
<　no　　> no ipsec nat-traversal enable　（NAT-Traversal 無効）
<初 期 値> no ipsec nat-traversal enable
<備　　考>

※ Transport モードと NAT-Traversal の併用

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

- 接続時の制限

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

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

◆ **ipsec path-mtu-discovery**

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

### ◆ ipsec xauth

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

### ◆ ipsec x509 enable

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

### ◆ ipsec x509 validity-period-check

<説　　明> X.509 証明書の有効期間をチェックする機能です。
<書　　式> ipsec x509 validity-period-check
<　no　　> no ipsec x509 validity-period-check
<初 期 値> ipsec x509 validity-period-check
<備　　考>

- 本機能が有効の場合、現在時刻が証明書の有効期間外であれば、当該証明書を使用することは出来ません。
- 本機能が無効の場合、常に証明書の利用が可能となります。また、CRL による証明書の無効化も行いません。

### ◆ ipsec x509 ca-certificate

<説　　明> X.509 の CA 証明書をインポートします。
<書　　式>
ipsec x509 ca-certificate NAME ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME
　　(|source A.B.C.D|X:X::X:X)
ipsec x509 ca-certificate NAME ftp://<A.B.C.D|X:X::X:X>/FILENAME
　　(|source A.B.C.D|X:X::X:X)
ipsec x509 ca-certificate NAME http|https://<A.B.C.D|X:X::X:X>/FILENAME
　　(|source A.B.C.D|X:X::X:X)
<　no　　> no ipsec x509 ca-certificate NAME
<備　　考>

- ソースアドレスを指定することができます。
- SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
  - IPv4 ssh://user@A.B.C.D:port/FILENAME
  - IPv6 ssh://[user@X:X::X:X]:port/FILENAME
- https:// の場合、サーバ証明書の validation を行う。https-:// の場合、validation を行わない。
- DER(*.der, *.cer)または PEM(*.pem)フォーマットの証明書をインポートすることができます。ファイルの拡張子は変更しないでください。なお、シングル DES で暗号化された鍵ファイルを使用することは出来ません。

◆ **ipsec x509 certificate**

<説　　明> X.509 の公開鍵証明書をインポートします。

<書　　式>

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

(|source A.B.C.D|X:X::X:X)

ipsec x509 certificate NAME ftp://<A.B.C.D|X:X::X:X>/FILENAME

(|source A.B.C.D|X:X::X:X)

ipsec x509 certificate NAME http|https://<A.B.C.D|X:X::X:X>/FILENAME

(|source A.B.C.D|X:X::X:X)

< no > no ipsec x509 certificate

<備　　考>

- ソースアドレスを指定することができます。
- SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
  - IPv4 ssh://user@A.B.C.D:port/FILENAME
  - IPv6 ssh://[user@X:X::X:X]:port/FILENAME
- https:// の場合、サーバ証明書の validation を行う。https-:// の場合、validation を行わない。
- DER(*.der, *.cer)または PEM(*.pem)フォーマットの証明書をインポートすることができます。ファイルの拡張子は変更しないでください。なお、シングル DES で暗号化された鍵ファイルを使用することは出来ません。

◆ **ipsec x509 private-key**

<説　　明> X.509 の private key を設定します。

<書　　式>

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

(|source A.B.C.D|X:X::X:X)

ipsec x509 private-key NAME key ftp://<A.B.C.D|X:X::X:X>/FILENAME

(|source A.B.C.D|X:X::X:X)

ipsec x509 private-key NAME key http|https://<A.B.C.D|X:X::X:X>/FILENAME

(|source A.B.C.D|X:X::X:X)

< no > no ipsec x509 private-key NAME key

<備　　考>

- ソースアドレスを指定することができます。
- SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
  - IPv4 ssh://user@A.B.C.D:port/FILENAME
  - IPv6 ssh://[user@X:X::X:X]:port/FILENAME
- https:// の場合、サーバ証明書の validation を行う。https-:// の場合、validation を行わない。

◆ **ipsec x509 private-key**

<説　　明> X.509 のパスフレーズを設定します。

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

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

### ◆ ipsec x509 crl

<説　　明> 証明書の失効リストを設定します。
<書　　式>
ipsec x509 crl NAME ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME (|source A.B.C.D|X:X::X:X)
ipsec x509 crl NAME ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
ipsec x509 crl NAME http|https://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
< no > no ipsec x509 crl NAME
<備　　考>
・ ソースアドレスを指定することができます。
・ SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
  - IPv4 ssh://user@A.B.C.D:port/FILENAME
  - IPv6 ssh://[user@X:X::X:X]:port/FILENAME
・ https:// の場合、サーバ証明書の validation を行う。https-:// の場合、validation を行わない。

### ◆ ipsec access-list

<説　　明> IPsec のアクセスリストを設定します。
<書　　式> ipsec access-list ACL-NAME ip (any|host|A.B.C.D/M any|host|A.B.C.D/M)
ipsec access-list ACL-NAME ipv6 (any|host|X:X::X:X/M any|host|X:X::X:X/M)
< no > no ipsec access-list ACL-NAME ip (any|host|A.B.C.D/M any|host|A.B.C.D/M)
no ipsec access-list ACL-NAME ipv6 (any|host|X:X::X:X/M any|host|X:X::X:X/M)
no ipsec access-list ACL-NAME
<備　　考>
・ 設定した IPsec access-list は、match address コマンドを使って IPsec tunnel に適用させます。match address コマンドについては、IPsec tunnel policy mode を参照してください。
・ 一つの access-list に ip と ipv6 のエントリーを各一つずつ登録することができます。また、削除時は、1 つずつ削除することができます。
・ IKEv2 では ip と ipv6 の両方のエントリーが有効になりますが、IKEv1 では最初のエントリーのみが有効になります。
・ IPsec access-list 内で host rule を設定する場合、以下の制限があります。
  ・ IPv4 host と IPv6 host は同じ扱いとなります(IPv4 になるか IPv6 になるかは、IKE で使用した IPprotocol 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 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.NXRG240-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 mode)を参照してください。

**◆ ipsec eap identity (IKEv2 のみ)**

<説　　明> EAP 認証で使用する ID とパスワードを設定します。
<書　　式> ipsec eap identity string WORD password (hidden|) WORD
ipsec eap identity key WORD password (hidden|) WORD
< no　> no ipsec eap identity string WORD
no ipsec eap identity key WORD
<備　　考>
- 設定例は、authentication local/remote(ipsec isakmp policy mode)を参照してください。
- パスワードは、1-95 文字以内で設定してください。使用可能な文字は、英数字および!$#=*+-_.:;(){}[]^~@`<>です。

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

<説　　明> IKEv2 で、動的拠点毎に異なる PSK を設定することができます。
<書　　式> ipsec pre-share identity fqdn WORD password (|hidden) WORD
ipsec pre-share identity user-fqdn WORD password (|hidden) WORD
ipsec pre-share identity key WORD password (|hidden) WORD
< no > no ipsec pre-share identity fqdn WORD
no ipsec pre-share identity user-fqdn WORD
no ipsec pre-share identity key WORD
<備　　考>
・ 設定例は、authentication local/remote(ipsec isakmp policy mode)を参照してください。
・ パスワードは、1-95 文字以内で設定してください。使用可能な文字は、英数字および!$#=*+-_.:;(){}[]^~@`<>
です。

◆ **interface ethernet**

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

◆ **interface loopback**

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

◆ **interface ethernet <0-2> vid <1-4094>**

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

◆ **interface tunnel**

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

◆ **interface ppp**

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

◆ **interface bridge**

<説　　明> interface bridge mode への遷移、および profile の生成を行います。
<書　　式> interface bridge <0-4095> (|vid <1-4094>)
< no > no interface bridge <0-4095> (|vid <1-4094>)

◆ **interface wlan**

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

◆ **wifi**

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

◆ **l2tp**

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

◆ **access-server profile**

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

◆ **interface virtual-templare**

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

◆ **l2tpv3 tunnel**

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

◆ **l2tpv3 xconnect**

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

◆ **l2tpv3 group**
<説　　明> l2tpv3-group mode への遷移、および profile の生成を行います。
　　no で、指定した ID のプロファイルを削除します。
<書　　式> l2tpv3 group <gid:1-4095>
<　no　> no l2tpv3 group <gid:1-4095>

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

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

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

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

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

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

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

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

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

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

◆ **terminal-server**
<説　　明> terminal-server mode への遷移および profile を生成します。
<書　　式> terminal-server <0-1>
<　no　　> no terminal-server <0-1> (= 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>
〇クラスの作成、変更
　　class policy NAME
〇クラスの削除
　　no class policy NAME
〇フィルタの作成
　　class filter <2-254>
〇フィルタの削除
　　no class filter <2-254>
○ Mark 値の設定
　　priority-map <1-255> (high|middle|low|normal) ip mark <1-4095>
○ TBF の設定
　　pirority-map <1-255> (high|middle|low|normal)
　　queue shape <RATE:1-1000000> <BUFFER:1-65535> <LIMIT:1-65535>
○ SFQ の設定
　　priority-map <1-255> (high|middle|low|normal) queue fair-queue
○ FIFO の設定
　　priority-map <1-255> (high|middle|low|normal) queue fifo (limit <1-16384>)
○ default class の設定
　　default の class を設定します。default class とは、どれにも該当しない packet を割り当てる class のことです。default class の初期値は normal です。
　　priority-map <1-255> default (high|middle|normal|low)
○ priority-map の削除
　　指定した class の priority-map を削除します。
　　no priority-map <1-255> (high|middle|normal|low|)
○ default class の初期化
　　default の class を default(normal)に設定します。
　　no priority-map <1-255> default
○ Mark 設定の削除
　　指定した class の Mark 設定を削除します。
　　no priority-map <1-255> (high|middle|normal|low) ip mark
○ default queue(FIFO)に設定
　　no priority-map <1-255> (high|middle|normal|low) queue

■ **route-map**

<説　　明> route-map を追加します。
<書　　式> route-map NAME (permit|deny) <1-1024>
<　no　> no route-map NAME : NAME の route-map を削除します。
　　no route-map NAME (permit|deny) <1-1024> : 該当の rouet-map のみ削除します。

## ■ class access-list

<説　　明>

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

○ ip

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

○ protocol

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

○ icmp

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

○ tcp src dst

class access-list ACL-NAME ip (|not) <source:>(any|A.B.C.D/M|A.B.C.D)
(|not) <destination:>(any|A.B.C.D/M|A.B.C.D|dns-set SETNAME)
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|dns-set SETNAME)
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|dns-set SETNAME)
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|dns-set SETNAME)
tcp (|not) (|range <min:1-65535> <max:1-65535>) (|range <min:1-65535> <max:1-655
35>)

○ 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>)

○ 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:1-655
35>)

○ no (class access-list の削除)

no class access-list ACL-NAME ip

## ■ class access-list WORD ipv6

<説　　明>

route-map の match 条件である match ipv6 address 設定をフィルタリングする際に使用します。具体的には、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。

○ ipv6

class access-list ACL-NAME ipv6 (|not) <source:>[any|X:X::X:X/M|X:X::X:X]
<destination:>[any|X:X::X:X/M|X:X::X:X]

○ ipv6 protocol

class access-list ACL-NAME ipv6 (|not) <source:>[any|X:X::X:X/M|X:X::X:X]
<destination:>[any|X:X::X:X/M|X:X::X:X] (|not) <protocol:0-255>|icmpv6|tcp|udp

○ ipv6 icmp

class access-list ACL-NAME ipv6 (|not) <source:>[any|X:X::X:X/M|X:X::X:X]
(|not) <destination:>[any|X:X::X:X/M|X:X::X:X] icmpv6 (|not) type code

○ ipv6 tcp src dst

class access-list ACL-NAME ipv6 (|not) <source:>[any|X:X::X:X/M|X:X::X:X]
(|not) <destination:>[any|X:X::X:X/M|X:X::X:X|]
tcp (|not) [<sport:1-65535>|any] [<dport:1-65535>|any]

○ ipv6 tcp src-range dst

class access-list ACL-NAME ipv6 (|not) <source:>[any|X:X::X:X/M|X:X::X:X]
(|not) <destination:>[any|X:X::X:X/M|X:X::X:X]
tcp (|not) [range <min:1-65535> <max:1-65535>] [<dport:1-65535>|any]

○ ipv6 tcp src dst-range

class access-list ACL-NAME ipv6 (|not) <source:>[any|X:X::X:X/M|X:X::X:X]
(|not) <destination:>[any|X:X::X:X/M|X:X::X:X]
tcp (|not) [<sport:1-65535>|any] [range <min:1-65535> <max:1-65535>]

○ ipv6 tcp src-range dst-range
　　class access-list ACL-NAME ipv6 (|not) <source:>[any|X:X::X:X/M|X:X::X:X]
　　(|not) <destination:>[any|X:X::X:X/M|X:X::X:X]
　　tcp (|not) [range <min:1-65535> <max:1-65535>] [range <min:1-65535> <max:1-65535
　　>]

○ ipv6 udp src dst
　　class access-list ACL-NAME ipv6 (|not) <source:>[any|X:X::X:X/M|X:X::X:X]
　　(|not) <destination:>any|X:X::X:X/M|X:X::X:X
　　udp (|not) [<sport:1-65535>|any] [<dport:1-65535>|any]

○ ipv6 udp src-range dst
　　class access-list ACL-NAME ipv6 (|not) <source:>[any|X:X::X:X/M|X:X::X:X]
　　(|not) <destination:>[any|X:X::X:X/M|X:X::X:X]
　　udp (|not) [range <min:1-65535> <max:1-65535>] [<dport:1-65535>|any]

○ ipv6 udp src dst-range
　　class access-list ACL-NAME ipv6 (|not) <source:>[any|X:X::X:X/M|X:X::X:X]
　　(|not) <destination:>[any|X:X::X:X/M|X:X::X:X]
　　udp (|not) [<sport:1-65535>|any] [range <min:1-65535> <max:1-65535>]

○ ipv6 udp src-range dst-range
　　class access-list ACL-NAME ipv6 (|not) <source:>[any|X:X::X:X/M|X:X::X:X]
　　(|not) <destination:>[any|X:X::X:X/M|X:X::X:X]
　　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 ipv6

## ■ mobile

○ mobile ppp
<説　　明> mobile と PPP インタフェース番号を関連付けます。
<書　　式> mobile <0-1> ppp <0-4>
<　no　　> no mobile <0-1> ppp

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

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

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

○ mobile frequency-band
<説　　明> 内蔵モジュールの周波数帯を設定します。
<書　　式> mobile <0-1> frequency-band (auto|lte|wcdma)
<　no　　> no mobile <0-1> frequency-band
<備　　考> NXR-610X5G は、該当しません。

○ mobile carrier
<説　　明> mobile モジュールの接続先(キャリア)を指定します。
<書　　式> mobile 1 carrier
　　(docomo|kddi|softbank|bwa|rakuten|local-5g|generic|auto) (|mvno)
<　no　　> no mobile <1> carrier
<備　　考> 指定できるキャリアは、機種により異なります。

○ plmn-id
<説　　明> PLMN(Public Land Mobile Network)を設定します。
<書　　式> mobile <1> plmn-id WORD
<　no　　> no mobile <1> plmn-id
<備　　考>
・ WORD には、MCC(Mobile Country Code)と MNC(Mobile Network Code)を組み合わせた 5 桁の番号を設定します。

○ rat
<説　　明> モバイルモジュールの周波数帯を固定することが出来ます。
<書　　式> mobile <1> rat (auto|lte|nr5g|w-cdma)
<初 期 値> mobile <1> rat auto
<　no　　> no mobile <1> rat (＝初期値)

○ nr5g-network-mode
<説　　明> 5G NR(New Radio)接続方式を設定することが出来ます。
<書　　式> mobile <1> nr5g-network-mode (nsa-sa|nsa|sa)
<初 期 値> mobile <1> nr5g-network-mode nsa-sa
<　no　　> no mobile <1> nr5g-network-mode (＝初期値)

○ fix-band
<説　　明> mobile モジュールの周波数帯を固定します。
<書　　式> mobile <1> fix-band (01|03|08|18|19|21|26|28|38|39|40|41|42|43)
<　no　　> no mobile <1> fix-band

○ netevent
<説　　明> Netevent 発生時に、mobile モジュールをリセットします。
<書　　式> mobile <1> netevent (<1-255>|<2048-4095>) reset
<　no　　> no mobile <1> netevent

○ sms accept
<説　　明> SMS の着信許可をする電話番号を指定します。
<書　　式> mobile <1> sms accept PHONE_NUMBER
<　no　　> no mobile <1> sms accept (|PHONE_NUMBER)

○ sms authentication-key
<説　　明> SMS の着信許可をする認証文字列を指定します。
<書　　式> mobile <1> sms authentication-key WORD
<　no　　> no mobile <1> sms authentication-key

○ sms send
<説　　明> SMS の送信先電話番号を設定します。
<書　　式> mobile <1> sms send <0> PHONE_NUMBER
<　no　　> no mobile <1> sms send (|<0>)

○ sms rollback notify sms send
<説　　明> ロールバックタイマに関する通知を SMS で送信するように設定します。
<書　　式> mobile <1> rollback notify sms send <0>
<　no　　> no mobile <1> rollback notify sms send

◆ 以下のコマンドは、Dual SIM 対応機種で、SIM の切り替えを行う場合に使用します。

○ mobile(act) ppp
<説　　明> mobile(act)と PPP インタフェース番号を関連付けます。
<書　　式> mobile 1 ppp <0-4>
<　no　> no mobile 1 ppp
<備　　考> mobile(act)は、SIM1 を利用した回線接続です。

○ mobile(act) carrier
<説　　明> mobile(act)とキャリアを関連付けます。
<書　　式> mobile 1 carrier (docomo|generic|kddi|softbank) (|mvno)
<　no　> no mobile 1 carrier
<備　　考> mobile(act)は、SIM1 を利用した回線接続です。
　　指定できるキャリアは、機種により異なります。

○ mobile(standby) ppp
<説　　明> mobile(standby)と PPP インタフェース番号を関連付けます。
<書　　式> mobile 1 standby ppp <0-4>
<　no　> no mobile 1 standby ppp
<備　　考> mobile(standby)は、SIM2 を利用した回線接続です。

○ mobile(standby) carrier
<説　　明> mobile(standby)とキャリアを関連付けます。
<書　　式> mobile 1 standby carrier (docomo|generic|kddi|softbank) (|mvno)
<　no　> no mobile 1 standby carrier
<備　　考> mobile(standby)は、SIM2 を利用した回線接続です。
　　指定できるキャリアは、機種により異なります。

○ mobile sim netevent change
<説　　明> Netevent による SIM 切り替え(act → standby/standby → act)の設定をします。
<書　　式> mobile 1 sim netevent (<1-255>|<2048-4095>) change
<　no　　> no mobile 1 sim netevent
<備　　考> 指定した track の event down を検知すると、SIM を切り替えます(act → standby)。
指定した track の event up を検知すると、SIM を切り替えます(standby → act)。
track の設定が必要です。

○ mobile sim netevent failover
<説　　明> Netevent による SIM 切り替え(act → standby)の設定をします。
<書　　式> mobile 1 sim netevent (<1-255>|<2048-4095>) failover
<　no　　> no mobile 1 sim netevent
<備　　考> 指定した track の event down を検知すると、SIM を切り替えます(act → standby)。
指定した track の event up を検知しても、何もしません(standby → standby)。
track の設定が必要です。

○ mobile sim change-timer
<説　　明> Standby 回線からの切り戻し(standby → act)の設定をします。
<書　　式> mobile 1 sim change-timer <10-1440>
<　no　　> no mobile 1 sim netevent
<備　　考>
・ act 回線から standby 回線へ切り替わりが発生した場合、指定した時間(分)が経過すると、act 回線への切り戻しを行います(standby → act)。

○ mobile-error-recovery-reset
<説　　明>
・ モバイルのリセットを行う機能です(前述の mobile error-recovery-reset を参照してください)。
・ mobile(standby) ppp, mobile(standby) carrier の設定がある場合、リセットに加えて、SIM 切り替え(act → standby、もしくは standby → act)も行います。
<書　　式> mobile error-recovery-reset
<　no　　> no mobile error-recovery-reset

○ Dual SIM 対応機種で、SIM の切り替えを行う場合の例を示します。

＜　例　＞

・　act 回線として利用する ppp interface と carrier を設定します。SIM1 を使用します。
　　mobile 1 ppp 0　　(1)
　　mobile 1 carrier docomo　　(2)

・　standby 回線として利用する ppp interface と carrier を設定します。SIM2 を使用します。
　　mobile 1 standby ppp 2　　(3)
　　mobile 1 standby carrier kddi mvno　　(4)

・　指定した track の event down を検知すると、SIM の切り替え(act → standby)を実施します。

※ track の設定が必要です。
　　mobile 1 sim netevent 1 change　　(5)

・　act 回線から standby 回線へ切り替わりが発生した場合、指定した時間(分)が経過すると、act 回線への切り戻しを行います。
　　mobile 1 sim change-timer 60　　(6)

・　mobile-error-recovery-reset による SIM 切り替え(act → standby、もしくは standby → act)の設定をします。

※上記(3)(4)の設定が必要です。
　　mobile error-recovery-reset　　(7)

**■ system led**

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

○ system led status

<説　　明>

・　指定した PPP、tunnel が、接続時 / 切断状態時に、それぞれ点灯 / 消灯します。
・　ngn-sip congestion 指定に、STS1 LED が点滅すると、NGN 網のひかり電話サーバが輻輳していることを示します。点滅中はデータコネクトによる接続は控えるようにしてください。

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

＜　no　＞ no system led status <2-2>

<備　　考> STS2 LED は、使用可能な機器のみ対応しています。

**◆ system led config**

<説　　明> STATUS 3 LED の色(点滅)を指定します。

<書　　式> system led config (green|red|orange)

＜　no　＞ no system led config

<備　　考> 対応機種は、NXR-530, NXR-610X です。

### ◆ 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

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

○PPP の schedule 接続/切断/再接続
<説　　明>
・　指定時間に、PPP の接続/切断/再接続を行います。切断/再接続は、PPP の状態に関係なく実施されます。本機能によって切断された場合、手動で切断されたものとみなし、常時接続が設定されていても再接続は行われません。再接続する場合は、USER による指示もしくはスケジュールの設定が必要になります。
<書　　式> 日付指定
schedule <1-255> HOUR:MIN DAY MONTH interface ppp <0-4> (connect|disconnect|reconnect)
<書　　式> 曜日指定(DOW: Day Of the Week)
schedule <1-255> HOUR:MIN DOW (|DOW) interface ppp <0-4> (connect|disconnect|reconnect)

○スケジュールによるデータ通信端末のリセット
<説　　明>
・　指定時間に、データ通信端末のリセットを行います。PPP が接続状態の場合は、即時実行ではなく PPP 切断後にリセットされます。PPP が接続状態でなければ、すぐにリセットされます。PPP が ondemand でない場合は、PPP が切断されたときに実行されるため、スケジュールで設定した時刻と実際にリセットされた時刻が大きく異なる場合があります。
・　また、データ通信端末のリセットには 20-30 秒ほどかかります。データ通信端末のリセットをスケジュール設定する場合は、数時間以上の間隔を空けることを推奨します。
<書　　式> 日付指定
schedule <1-255> HOUR:MIN DAY MONTH mobile <0-2> clear
<書　　式> 曜日指定(DOW: Day Of the Week)
schedule <1-255> HOUR:MIN DOW (|DOW) mobile <0-2> clear

○スケジュールによるシステム再起動
<説　　明> 指定時間に、system の再起動を実施します。
<書　　式> 日付指定
schedule <1-255> HOUR:MIN DAY MON system restart
<書　　式> 曜日指定(DOW: Day Of the Week)
schedule <1-255> HOUR:MIN DOW (|DOW) system restart

○スケジュールによるシスログのローテート

<説　　明>

・ 指定時刻に、syslog の rotate を実行します。指定時刻に実際に rotate が行われるかどうかの判断は、syslog mode の rotate 設定に依存します。

<書　　式> 日付指定

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

<書　　式> 曜日指定(DOW: Day Of the Week)

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

○スケジュールによるモニターログのローテート

<説　　明>

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

<書　　式> 日付指定

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

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

<書　　式> 曜日指定(DOW: Day Of the Week)

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

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

○スケジュールによる NTP の時刻同期

<説　　明> 指定の時刻に、NTP による時刻同期を行います。

<書　　式> 日付指定

schedule <1-255> HOUR:MIN DAY MON ntp adjust

<書　　式> 曜日指定(DOW: Day Of the Week)

schedule <1-255> HOUR MIN DOW (|DOW) ntp adjust

<備　　考> NTP のスケジュール同期を行うには、NTP サーバの設定(ntp mode)が必要です。

○スケジュールによるファームウェアのチェック

<説　　明>

・ 指定の時刻に、Century Systems HP(official)から最新のファームウェア情報を取得し、更新情報があれば、ユーザに通知します(show version 実行時、あるいは syslog にて通知します)。

・ flash 上のファームウェアとバージョンが異なる場合に通知します(ファームウェアが、2 面ある場合は、どちらとも異なる場合に通知します)。

<書　　式> 日付指定

schedule <1-255> HOUR:MIN DAY MON firmware check official

<書　　式> 曜日指定(DOW: Day Of the Week)

schedule <1-255> HOUR MIN DOW (|DOW) firmware check official

<備　　考> 以下に、更新がある場合の show version の出力例を示します。

nxrg240#show version

Century Systems NXR-G240 Series ver 9.0.0 (build 30/17:18 11 11 2016)

Update Available:

Century Systems NXR-G240 Series ver 9.1.0 (build 1/19:38 12 11 2016)

○ファームウェアの更新

<説　　明>

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

<書　　式>

● Official schedule <1-255> HOUR:MIN DAY MON firmware update official
(|source A.B.C.D|X:X::X:X) (|hold) (margin <30-86400>|)

● FTP schedule <1-255> HOUR:MIN DAY MON firmware update
ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
(|hold) (margin <30-86400>|)

● SSH schedule <1-255> HOUR:MIN DAY MON firmware update
ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME password (|hidden) PASSWORD
(|source A.B.C.D|X:X::X:X) (|hold) (margin <30-86400>|)

● HTTP/HTTPS schedule <1-255> HOUR:MIN DAY MON firmware update
http|https://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X)
(|hold) (margin <30-86400>|)

● ストレージ schedule <1-255> HOUR:MIN DAY MON firmware update
(disk0:FILENAME|disk1:FILENAME) (|hold) (margin <30-86400>|)

● CMS schedule <1-255> HOUR:MIN DAY MON firmware update cms
(|source A.B.C.D|X:X::X:X) (|hold) (margin <30-86400>|)

<備　　考>

・ Official を指定した場合、弊社 Web サイトからファームウェアを取得します。
・ Official、FTP、SSH では、ソースアドレスを指定することができます。
・ SSH を使用する場合は、password を設定してください。
・ SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
IPv4　ssh://user@A.B.C.D:port/FILENAME、IPv6　ssh://[user@X:X::X:X]:port/FILENAME
・ https:// の場合、サーバ証明書の validation を行う。https-:// の場合、validation を行わない。
・ hold を指定した場合、ファームウェア更新後の自動再起動を保留します(再起動するまでは、既存のファームウェアで動作します)。
※　hold 指定出来ない機種は、ファームウェア更新後に自動再起動します。
・ スケジュールによるファームウェアアップデート実行時、ファームウェアのバージョンチェックを行います。同じバージョンの場合は、ファームウェアの更新を行いません(スケジュール設定が config 上に残っている場合でも、不要なファームウェア更新を回避することが出来ます)。なお、拡張 flash 管理に対応した機種の場合、起動面と非起動面の両方とファームウェアのバージョンを比較します。いずれかの面と同じであれば、ファームウェアの更新は実行しません。
・ margin 指定した場合、スケジュール時刻から最大で margin 秒後に、firmware update を開始します。
・ URL には、マクロ文字列を使用することが出来ます。詳細は、firmware update(view mode)を参照してください。

○ firmware list-update

<説　　明>

・ 指定時刻に、firmware list-update を実行します。

<書　　式>

schedule <1-255> HOUR:MIN DAY MON firmware list-update URL (hold|) (margin <30-86400>|)
schedule <1-255> HOUR:MIN DAY MON firmware list-update URL source (A.B.C.D|X:X::X:X) (hold|) (margin <30-86400>|)
schedule <1-255> HOUR:MIN DAY MON firmware list-update ssh://URL password (hidden|) WORD (hold|) (margin <30-86400>|)
schedule <1-255> HOUR:MIN DAY MON firmware list-update ssh://URL password (hidden|) WORD source (A.B.C.D|X:X::X:X) (hold|) (margin <30-86400>|)

<備　　考>

・ list に含まれる version と起動中の version が同じ場合、firmware update を実行しません。
・ list に含まれる version と起動中の version が異なる場合、list で指定した URL から firmware を取得して、firmware update を実行します。
・ URL には、以下のいずれかを指定します。
FTP 利用時 (ftp://)、HTTP 利用時 (http://)、HTTPS 利用時 (https://)
HTTPS(no validate)利用時 (https-://)、Storage 利用時 (diskX:)、CMS 利用時 (cms)
・ FTP、SSH では、ソースアドレスを指定することができます。
・ SSH を使用する場合は、password を設定してください。
・ SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
IPv4　ssh://user@A.B.C.D:port/FILENAME、IPv6　ssh://[user@X:X::X:X]:port/FILENAME
・ https:// の場合、サーバ証明書の validation を行う。https-:// の場合、validation を行わない。
・ hold を指定した場合、ファームウェア更新後の自動再起動を保留します(再起動するまでは、既存のファームウェアで動作します)。

※　hold 指定出来ない機種は、ファームウェア更新後に自動再起動します。

・ margin 指定した場合、スケジュール時刻から最大で margin 秒後に、firmware list-update を開始します。
・ URL には、マクロ文字列を使用することが出来ます。詳細は、firmware update(view mode)を参照してください。

○ config copy
<説　　明> 指定時刻に、config copy を実行します。
<書　　式>
schedule <1-255> HOUR:MIN DAY MON config copy URL (startup-config|config|config-and-save)
(margin <30-86400>|)
schedule <1-255> HOUR:MIN DAY MON config copy URL (startup-config|config|config-and-save)
source (A.B.C.D|X:X::X:X) (margin <30-86400>|)
schedule <1-255> HOUR:MIN DAY MON config copy ssh://URL (startup-config|config|config-and-save)
password (hidden|) WORD (margin <30-86400>|)
schedule <1-255> HOUR:MIN DAY MON config copy ssh://URL (startup-config|config|config-and-save)
password (hidden|) WORD source (A.B.C.D|X:X::X:X) (margin <30-86400>|)
<備　　考>
・ config(running-config)指定時
取得した config、あるいは現在の config に configuration-id がない場合でも、config copy を実行します。
・ startup-config 指定時
config copy を実行した場合、システム再起動を行います。
configuration-id が同じ場合、config copy を実行しません。
取得した config あるいは現在の config に、configuration-id がない場合、config copy を実行しません。
・ configuration-id は、system configuration-id コマンドで指定します。
・ URL には、以下のいずれかを指定します。
FTP 利用時 (ftp://)、HTTP 利用時 (http://)、HTTPS 利用時 (https://)
HTTPS(no validate)利用時 (https-://)、Storage 利用時 (diskX:)、CMS 利用時 (cms)
・ FTP、SSH では、ソースアドレスを指定することができます。
・ SSH を使用する場合は、password を設定してください。
・ SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
IPv4　ssh://user@A.B.C.D:port/FILENAME、IPv6　ssh://[user@X:X::X:X]:port/FILENAME
・ https:// の場合、サーバ証明書の validation を行う。https-:// の場合、validation を行わない。
・ margin 指定時、スケジュール時刻から最大で margin 秒後に、config copy を実行します。
・ URL には、マクロ文字列を使用することが出来ます。詳細は、■ copy(view mode)を参照してください。

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

○スケジュールによる通信量クリア
<説　　明> 指定の時刻に、PPP の通信量をクリアします。
<書　　式> schedule <1-255> HOUR:MIN DAY MON interface ppp <0-4> clear data-usage

○スケジュールによるドメインリストの取得・更新
<説　　明> 指定の時刻に、DNS インターセプト機能で利用するドメインリストを取得・更新します。
<書　　式> schedule <1-255> HOUR:MIN DOW (DOW|) dns-intercept ip setname WORD update URL
<備　　考> ドメインリストは、ip dns-intercept setname コマンド(global mode)で設定します。

○スケジュールによるモバイルモジュールの更新
<説　　明> 指定の時刻に、モバイルモジュールを更新します。
<書　　式>
schedule <1-255> HOUR:MIN DOW (DOW|) mobile 1 update cms (margin <30-86400>|)
schedule <1-255> HOUR:MIN DOW (DOW|) mobile 1 update cms source (A.B.C.D|X:X::X:X)
(margin <30-86400>|)

○スケジュールによる拡張情報の送信
<説　　明> 指定の時刻に、CMS へ拡張情報を送信します。
<書　　式>
schedule <1-255> HOUR:MIN DOW (DOW|) system notify cms (margin <30-86400>|)
schedule <1-255> HOUR:MIN DOW (DOW|) system notify cms source (A.B.C.D|X:X::X:X) (margin <30-86400>|)

○スケジュールによる最新 syslog の送信
<説　　明> 指定の時刻に、CMS へ最新 syslog を送信します。
<書　　式>
schedule <1-255> HOUR:MIN DOW (DOW|) syslog copy cms (margin <30-86400>|)
schedule <1-255> HOUR:MIN DOW (DOW|) syslog copy cms source (A.B.C.D|X:X::X:X) (margin <30-86400>|)

○スケジュールによる IPsec の接続 / 切断
<説　　明> 指定の時刻に、IPsec の接続 / 切断を行います。
<書　　式>
schedule <1-255> HOUR:MIN DOW (DOW|) ipsec (isakmp|tunnel) <1-65535> (connect|disconnect)

○スケジュールによる speed-test の実行
<説　　明> 指定の時刻に、speed-test を実行します。
<書　　式> schedule <1-255> HOUR:MIN DAY MON speed-test 0 start (|margin <1-36000>)
schedule <1-255> HOUR:MIN DOW (DOW|) speed-test 0 start (|margin <1-36000>)

○スケジュールによる PoE 給電の実行
<説　　明> 指定の時刻に、PoE 給電を実行(有効／無効)にします。
<書　　式> schedule <1-255> HOUR:MIN DAY MON poe ethernet 0 (enable|disable)
schedule <1-255> HOUR:MIN DOW (DOW|) poe ethernet 0 (enable|disable)
<備　　考> 対応機種は、NXR-G060 です。

○スケジュールによる track のステータス変更
<説　　明> 指定の時刻に、track のステータスを変更(up/down)します。
<書　　式> schedule <1-255> HOUR:MIN DAY MON track <1-255> up/down
schedule <1-255> HOUR:MIN DOW (DOW|) track <1-255> up/down

○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

◆ **system netevent**

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

■ **メール送信機能**

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

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

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

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

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

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

### ◆ system config flash
<説　　明> 次回起動時に使用する config をユーザが指定することが出来ます。
<書　　式> system config (flash:FILENAME|disk0:FILENAME)
<　no　> no system config
<初 期 値> no system config
<備　　考> flash:startup.config を指定すると、save config した config で起動します。
USB メモリ内の config から起動するには、disk0:FILENAME を指定します。
no system config は、bootup 設定を初期化します(startup-config で起動します)。

### ◆ system config factory-initial-config
<説　　明> 次回のシステム再起動時に、工場出荷設定(factory-initial-config)で起動します。
<書　　式> system config factory-initial-config (|one-time)
<　no　> no system config
<備　　考> one-time を指定した場合、一度だけ有効です。

### ◆ system config empty-config
<説　　明> 次回のシステム再起動時に、設定無し(empty-config)で起動します。
<書　　式> system config empty-config one-time (|one-time)
<　no　> no system config
<備　　考> one-time を指定した場合、一度だけ有効です。

### ◆ system boot clear-ppp-data-usage
<書　　式> system boot clear-ppp-data-usage
<初 期 値> system boot clear-ppp-data-usage（=有効）
<　no　> no system boot clear-ppp-data-usage（=無効）
<備　　考>
- 電源断などで、スケジュールによる通信量クリアが行われなかった場合、通信量制限で PPP の接続が出来なくなる場合があります。このような状態を回避するため、初期値では、システム再起動後は、通信量情報を継続して使用しません(通信量 0 として動作します)。
- 本機能を無効にすることで、システム再起動後も通信量情報を継続して使用することが出来ます。

※本機能を無効にした場合、システム再起動後も通信量情報が引き継がれます。そのため、何らかの理由で、スケジュールによる通信量情報のクリアが行われなかった場合は、手動でクリアする必要があります。

### ◆ ppp account username
<説　　明>
・PPP のアカウントを設定します。発信(PPP 接続)、および着信(RAS 回線着信)に使用します。
<書　　式> ppp account username USERNAME password (|hidden) PASSWORD
<　no　> no ppp account username USERNAME
<備　　考>
- USERNAME は、1-63 文字以内で設定してください。
  使用可能な文字は、英数字[a-z,A-Z,0-9]および @-_.%/+$= です。
- PASSWORD は、1-95 文字以内で設定してください。
  使用可能な文字は、英数字および!$#=*+-_.:;(){}[]/^~@<>`%?です。
- ppp username コマンド(ppp interface mode)で設定した USERNAME(password あり)と重複することはできません。
- PASSWORD に「?」を入力する場合は、「Ctrl」+「v」を入力してから、「?」を入力してください。

◆ **show config ipv6 dhcp-client**

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

## ■ ip policy access-list

<説　　明>

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

○ ip

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

○ protocol

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

○ icmp

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

○ tcp src dst

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

○ tcp src-range dst

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

○ tcp src dst-range

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

○ tcp src-range dst-range

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

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

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

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

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

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

**■ 電源管理機能**

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

**■ 電源管理モード設定**

**◆ system power-management mode**

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

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

**※温度プロテクション機能**

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

**■ Sleep/Resume 機能**

- システムを sleep 状態に移行させることができます。また、sleep 状態から復帰(resume)させることができます。sleep 状態になると、CPU/Ethernet などへの電源供給を停止します。
- 工場やオフィス等の利用者がいない時間帯(休日や営業時間外)に、sleep モードを使用することで、大幅に消費電力を抑えることが可能になります。

○ Sleep 状態への移行

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

<説　　明> INIT ボタンを 3 秒間押下した場合、sleep 状態へと遷移します。
<書　　式> system power-management sleep init-button
　　system power-management sleep init-button timer <1-31536000>
　　system power-management sleep init-button schedule <1-255>
<初 期 値> system power-management sleep init-button
<　no　> no system power-management sleep init-button
<備　　考>

・ 「no system power-management sleep init-button」設定時、INIT ボタンを押下しても、sleep 状態へと遷移しません。
・ timer(resume timer)を設定することができます。
　timer を設定しない場合は、365 日間(31,536,000[sec])が設定されます。
・ schedule(resume schedule)を設定することができます。
　schedule の設定例(日時は 12 月 31 日 0 時 30 分)です。
　　system power-management shutdown init-button schedule 1
　　schedule 1 00:30 31 12 system resume
・ sleep 状態で、INIT ボタンを押下すると、resume します。

■ **Shutdown/Resume 機能**

・ システムを shutdown 状態に移行させることができます。また、shutdown 状態から復帰(resume)させることができます。

○ Shutdown 状態への移行

◆ **system power-management shutdown opt-button**

<説　　明> opt ボタンを 3 秒間以上押下した場合、shutdown 状態へと遷移します。
<書　　式> system power-management shutdown opt-button
　　system power-management shutdown opt-button timer <1-31536000>
　　system power-management shutdown opt-button schedule <1-255>
<初 期 値> system power-management shutdown opt-button
<備　　考>

・ timer(resume timer)を設定することができます。
　timer を設定しない場合は、365 日間(31,536,000[sec])が設定されます。
・ schedule(resume schedule)を設定することができます。
　schedule の設定例(日時は 12 月 31 日 0 時 30 分)です。
　　system power-management shutdown opt-button schedule 1
　　schedule 1 00:30 31 12 system resume
・ 手動で resume させる場合は、すべての LED が消灯していることを確認して(1 分以上経過して)から、電源供給を実施します。または、opt ボタンを押下します。

◆ **ppp idle-timeout & system sleep（interface ppp mode）**

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

◆ **schedule & system sleep（global mode）**

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

◆ **sleep system（ sleep system view mode）**

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

○ Resume(Sleep 状態からの復帰)

◆ **timer**

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

◆ **schedule**

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

◆ **INIT ボタン**

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

◆ **schedule & system shutdown（global mode）**

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

◆ **shutdown system（view mode）**

<説　　明> コマンド実行により、shutdown 状態へと遷移します。

<書　　式> shutdown system
　　shutdown system timer <1-31536000>
　　shutdown system schedule <NUM>

<備　　考>

< NXR-G050 >

- shutdown 状態に移行すると、すべての LED が消灯します。
- timer を設定しない場合は、365 日間(31,536,000[sec])が設定されます。
- スケジュール機能で resume させる場合は、resume の schedule 番号を指定します。
- 手動で resume させる場合は、すべての LED の消灯を確認して(1 分以上経過して)から、電源供給を実施します。または、opt ボタンを押下します。

○ Resume(shutdow 状態からの復帰)

◆ **timer**

<説　　明> shutdown 状態へと遷移させる際に、resume までの timer(秒)を設定します。

<書　　式>

schedule <NUM> HOUR:MIN DOW (DOW|) system shutdown timer <1-31536000>　(global mode)
shutdown system timer <1-31536000>　(view mode)

◆ **schedule**

<説　　明> shutdown 状態へと遷移させる際に、resume の schedule 番号を指定します。

<書　　式>

schedule <NUM> HOUR:MIN DOW (DOW|) system shutdown schedule <NUM>　(global mode)
shutdown system schedule <NUM>　(view mode)

◆ **opt ボタン**

<説　　明> opt ボタンを押下すると、resume します。

<書　　式> なし

◆ **Serial**

<説　　明> Serial からの入力によって、resume します。
<書　　式> system power-management resume serial <NUM>
<　no　　> no system power-management resume serial <NUM>
<備　　考>
・ 「no system power-management resume serial <NUM>」設定時は、該当する serial からの入力があっても resume しません。
< NXR-G050 >
・ RS-232 ポートは、未対応です。

**■ 処理の競合**

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

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

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

## ■ WOL(Wake On LAN)パケット送信機能

WOL は、sleep 状態にある端末の電源を遠隔で投入するための技術です。

### ◆ wol name WORD

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

○ Ethernet フレーム

<書　　式>

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

<備　　考>

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

○ UDP パケット

<書　　式>

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

<備　　考>

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

<備　　考>

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

### ◆ ip host FQDN

<説　　明> IP アドレスとホスト名の組み合わせを、static に設定することが出来ます。
<書　　式> ip host FQDN A.B.C.D
< no　> no ip host FQDN
<備　　考>

- 本装置の DNS サービスが有効の場合、外部からの名前解決要求に対して、static ホストエントリー、外部 DNS サーバの順に名前解決を行います。
- 本装置の DNS サービスが無効の場合、本装置からパケットを送信する場合のみ、static ホストエントリーを参照します。

### ◆ ipv6 host FQDN

<説　　明> IPv6 アドレスとホスト名の組み合わせを、static に設定することが出来ます。
<書　　式> ipv6 host FQDN X:X::X:X
< no　> no ipv6 host FQDN

### ◆ ipsec priority-ignore

<説　　明> Priority による IPsec SA の優先度を無効にする機能です。
　　IKEv1 で、route based IPsec を利用している場合のみ有効です。
<書　　式> ipsec priority-ignore enable
< no　> no ipsec priority-ignore enable
<備　　考>

- Route based IPsec では、phase2 の ID は、IPsec SA を確立するための ID としてのみ使用します。そのため、Priority による冗長化 etc の機能を利用しない場合は、本機能を有効にすることによって、同じ phase2 ID を持つ複数個の IPsec SA を同時に確立することが出来ます。
- Route based IPsec 間、または route based IPsec と policy based IPsec 間での重複が可能です。Policy based IPsec 間での重複は出来ません。
- 本機能は、ISP の VPN サービス等で、phase2 の ID を any/any で指定するような場合に、利用することが出来ます。

## ■ Mode-config

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

### ◆ ipsec local pool

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

### ◆ ipsec ike/ike2 client configuration dns-server

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

### ◆ ipsec ike/ike2 client configuration netbios-server

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

### ◆ system usb transfer-mode

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

## ■ コンテナ型仮想化

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

### ◆ lxc container

<説　　明> lxc container を設定します。
　　lxc container を設定すると、lxc が起動します。
<書　　式> lxc container <1-4>
< no > no lxc container
<備　　考>
・ 起動中の LXC にログインするには、connect lxc console コマンド(view mode)を使用します。

### ◆ track mail send server

<説　　明> Track up/down を検出した際、mail にて通知することが出来ます。
<書　　式> track mail send server<0-2>
　　track mail send server<0-2> subject LINE
< no > no track mail send
<初 期 値> no track mail send

### ◆ track snmp trap

<説　　明> Track up/down を検出した際、SNMP trap にて通知することが出来ます。
<書　　式> track snmp trap
< no > no track snmp trap
<初 期 値> no track snmp trap

### ◆ bridge flow-list

<説　　明> ユーザが作成した flow を追加 / 削除することが出来ます。
作成した flow は、ファイルの形で NXR へインストールすることで使用できます。
<書　　式> bridge flow-list WORD file WORD
　　bridge flow-list WORD file
< no > no bridge flow-list WORD
<備　　考>
・ bridge flow-list コマンドで、同じ名前の flow list をインポートした場合、上書きされます。
・ bridge flow-list WORD file は、show config 用のコマンドです。
・ cookie は、指定不可です(cookie を指定した場合、flow を追加することは出来ません)。
・ priority の推奨値は、1024-32768 です。

◆ **ip dns-intercept setname**

<説　　明> DNS インターセプト対象となるドメインリストをインポートします。
<書　　式> ip dns-intercept setname WORD file (URL|) (ms-o365|)
<　no　　> no ip dns-intercept setname WORD
<備　　考>
・ URL 部は、以下のように設定します。
FTP(ftp://)、HTTP(http://)、USB(disk0:)、Microsoft Official HP(ms-o365)
・ 設定したドメインリストをインタフェースに適用するには、ip dns-intercept コマンド(interffacemode)を使用します。

◆ **mape-rule**

<説　　明> MAP-E rule の type を指定します。
<書　　式> mape-rule WORD type jpne auto
mape-rule WORD type ocn auto
<　no　　> no mape-rule WORD
<備　　考>
・ 本バージョンでは、JPNE 社の v6plus サービス、OCN IPoE サービスに対応しています。
・ WORD には、mape-rule 名を設定します。

◆ **ip route mape-rule**

<説　　明> mape-rule の ip route を指定します。
<書　　式> ip route mape-rule WORD (|<1-255>)
<　no　　> no ip route mape-rule WORD (|<1-255>)

◆ **ipv6 route mape-rule**

<説　　明> mape-rule の ipv6 prefix route として、RA/DHCPv6 で取得した gateway に設定します。
<書　　式> ipv6 route mape-rule WORD ra (|<1-255>)
ipv6 route mape-rule WORD dhcp (|<1-255>)
<　no　　> no ipv6 route mape-rule WORD ra (|<1-255>)
no ipv6 route mape-rule WORD dhcp (|<1-255>)

◆ **ip tcp minimum-send-mss**

<説　　明>
・ advertise された MSS 値が本設定より小さい場合、本設定値の segment サイズで送信されます。
<書　　式> ip tcp minimum-send-mss <48-1460>
<　no　　> no ip tcp minimum-send-mss

## ■ REST-API

REST-API 機能を利用することで、HTTP 経由で、本装置上の情報を読み書きすることができます。

### ◆ REST-API の対応機種とバージョン

REST-API には、Version1（REST-APIv1）と Version2（REST-APIv2）があり、利用可能な機能が異なります。

- REST-APIv1 は、一部のメンテナンス操作と設定に対応しています。
  NXR-650,NXR-530,NXR-160/LW,NXR-G180/L-CA,NXR-G110 シリーズ（2020/12 現在）
- REST-APIv2 は、REST-API に対応している全ての機能を利用することが出来ます。
  NXR-650,NXR-530,NXR-160/LW,NXR-G180/L-CA,NXR-G110 シリーズ（2020/12 現在）

### ◆ REST-APIv1 で利用可能な機能

- REST-APIv1 では、以下の操作が可能です。
  Auth-ID 発行等
  機器再起動
  設定の保存
  各種コピー操作
  startup-config の保存・取得
  ファームウェアの更新
  ファームウェアバージョンの取得
  show コマンドの実行
  config の取得
  IPv4 アクセスリスト設定
  IPv4 スタティックルート設定
  IPv4DHCP サーバ設定
  Ethernet インタフェース設定

### ○ rest (http|https) enable

<説　　明> REST-API 機能を有効化します。
<書　　式> rest http enable
　　rest https enable
< no > no rest http enable
　　no rest https enable
<備　　考> http, https のどちらか（または両方）の設定を行います。

### ○ rest (http|https) port

<説　　明> REST-API で使用するポート番号を指定します。
<書　　式> rest http port <1024-65535>
　　rest https port <1024-65535>
< no > no rest http port
　　no rest https port

**○ rest session-max**
<説　　明> REST-API のセッション最大数を指定します。
<書　　式> rest session-max <1-20>
<　no　　> no rest session-max

**○ rest timeout**
<説　　明> REST-API のタイムアウト値(秒)を指定します。
<書　　式> rest timeout <60-3600>
<　no　　> no rest timeout

**○ rest username**
<説　　明> REST-API で使用するユーザ名とパスワードを設定します。
<書　　式> rest username WORD password (hidden|) WORD
<　no　　> no rest username

**○ auth-fail-lock**
<説　　明> 一定回数ログインに失敗すると、一時的にログイン試行を受け付けなくなります。
<書　　式> rest auth-fail-lock (account|account-ip|ip)
<初 期 値> rest auth-fail-lock account
<　no　　> no rest auth-fail-lock

**◆ http-server cert certificate**
<説　　明> PEM 形式のサーバ証明書をインストールします。
<書　　式> http-server cert certificate NAME FILE
<　no　　> no http-server cert certificate NAME

**◆ http-server cert chain-certificate**
<説　　明> PEM 形式のルート(または中間)証明書をインストールします。
<書　　式> http-server cert chain-certificate NAME FILE
<　no　　> no http-server cert chain-certificate NAME

**◆ http-server cert private-key**
<説　　明> PEM 形式の秘密鍵をインストールします
<書　　式> http-server cert private-key NAME key FILE
　　http-server cert private-key NAME password (|hidden) PASSWORD
<　no　　> no http-server cert private-key NAME key
　　no http-server cert private-key NAME password
<備　　考> パスワード付きの秘密鍵を使用する場合は、パスワードを設定します。

◆ **system boot firmware update**

<説　　明> システム起動時に、firmware update を実行します。
<書　　式> system boot firmware update WORD (|password) (|source) (|hold)
　　system boot firmware update official (|source) (|hold)
　　system boot firmware update cms (|source) (|hold)
< no > no system boot firmware
<備　　考>
- 同じバージョンの場合、firmware update を実行しません。
- hold を指定すると、firmware update 後にシステム再起動しません。システム再起動後に、更新されたファームウェアで起動します。
- WORD には、以下のいずれかを指定します。
  ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME、ftp://<A.B.C.D|X:X::X:X>/FILENAME
  http|https://<A.B.C.D|X:X::X:X>/FILENAME、diskX:FILENAME
- URL には、マクロ文字列を使用することが出来ます。詳細は、firmware update(view mode)を参照してください。

◆ **system boot firmware list-update**

<説　　明> システム起動時に、firmware list-update 取得を実行します。
<書　　式> system boot firmware list-update WORD (|password) (|source) (|hold)
　　system boot firmware list-update cms (|source) (|hold)
< no > no system boot firmware
<備　　考>
- list に含まれる version と起動中の version が同じ場合、firmware update を実行しません。
- list に含まれる version と起動中の version が異なる場合、list で指定された URL より firmware を取得して、firmware update を実行します。
- URL には、マクロ文字列を使用することが出来ます。詳細は、firmware update(view mode)を参照してください。

◆ **system boot config copy**

<説　　明> システム起動時に、config copy を実行します。

<書　　式>

system boot config copy WORD (config|config-and-save|startup-config) (|password) (|source)

system boot config copy cms (config|config-and-save|startup-config) (|password) (|source)

< no > no system boot config

<備　　考>

・ config(running-config)指定時
取得した config、あるいは現在の config に configuration-id がない場合でも、config copy を実行します。

・ startup-config 指定時、config copy を実行した場合、システム再起動を行います。
configuration-id が同じ場合 config copy を実行しません。

・ 取得した config、あるいは現在の config に、configuration-id がない場合、config copy を実行しません。

・ configuration-id は、system configuration-id コマンドで指定します。

・ URL には、マクロ文字列を使用することが出来ます。詳細は、■ copy(view mode)を参照してください。

◆ **system configuration-id**

<説　　明> system configuration-id を設定します。

<書　　式> system configuration-id WORD

< no > no system configuration-id

<備　　考> system boot config copy コマンド、schedule xx config copy コマンドで、startup-config を指定する場合に設定します。

◆ **http-server ip forbidden-access-wan**

◆ **http-server ipv6 forbidden-access-wan**

<説　　明> WAN(ethernet0 以外のインタフェース)から、本装置への GUI 接続を禁止します。

<書　　式> http-server (ip|ipv6) forbidden-access-wan

< no > no http-server (ip|ipv6) forbidden-access-wan

<備　　考> 接続禁止ポートは、以下のコマンドで確認することが出来ます。
show (ip|ipv6) forbidden-access-wan

◆ **telnet-server ip forbidden-access-wan**

◆ **telnet-server ipv6 forbidden-access-wan**

<説　　明> WAN(ethernet0 以外のインタフェース)から、本装置への Telnet 接続を禁止します。

<書　　式> telnet-server (ip|ipv6) forbidden-access-wan

< no > no telnet-server (ip|ipv6) forbidden-access-wan

<備　　考> 接続禁止ポートは、以下のコマンドで確認することが出来ます。
show (ip|ipv6) forbidden-access-wan

◆ **ssh-server ip forbidden-access-wan**
◆ **ssh-server ipv6 forbidden-access-wan**

<説　　明> WAN(ethernet0 以外のインタフェース)から、本装置への SSH 接続を禁止します。
<書　　式> ssh-server (ip|ipv6) forbidden-access-wan
<　no　　> no ssh-server (ip|ipv6) forbidden-access-wan
<備　　考> 接続禁止ポートは、以下のコマンドで確認することが出来ます。
　　show (ip|ipv6) forbidden-access-wan

◆ **rest http ip forbidden-access-wan**
◆ **rest http ipv6 forbidden-access-wan**

<説　　明>
・ WAN(ethernet0 以外のインタフェース)から、本装置への REST(HTTP)接続を禁止します。
<書　　式> rest http (ip|ipv6) forbidden-access-wan
<　no　　> no rest http (ip|ipv6) forbidden-access-wan
<備　　考> 接続禁止ポートは、以下のコマンドで確認することが出来ます。
　　show (ip|ipv6) forbidden-access-wan

◆ **rest https ip forbidden-access-wan**
◆ **rest https ipv6 forbidden-access-wan**

<説　　明>
・ WAN(ethernet0 以外のインタフェース)から、本装置への REST(HTTPS)接続を禁止します。
<書　　式> rest https (ip|ipv6) forbidden-access-wan
<　no　　> no rest https (ip|ipv6) forbidden-access-wan
<備　　考> 接続禁止ポートは、以下のコマンドで確認することが出来ます。
　　show (ip|ipv6) forbidden-access-wan

◆ **system event-notify**

<説　　明> システムイベント発生時に、イベントの通知を行います。
<書　　式> system event-notify <0-3> (crit|err|info|warn|)
< no　> no system event-notify
<備　　考>

・ イベント通知の方法(LINE、メール)は、ENS mode で設定します。
・ Priority(infor, warning, error, critical)を指定することが出来ます。指定した priority より低いイベントの場合は、通知しません。

info
システム起動時
温度が normal に遷移した場合
FAN が normal になった場合
CPU LOAD が閾値より低くなった場合
FREE MEMORY が閾値より低くなった場合
SESSION 数が閾値より低くなった場合

warn
温度が閾値(warning)を超えた場合
CPU LOAD が閾値を超えた場合
FREE MEMORY が閾値を超えた場合
SESSION 数が閾値を超えた場合

err
該当イベントはありません。

crit
温度が閾値(critical)を超えた場合
FAN が fault になった場合

## ■ session-helper

<説　　明>

・ 動的ポートの追加セッションが開始されるようなプロトコルについて、接続を許可することができます。以下のプロトコルに対応しています。

○ sip
<書　　式> session helper sip enable
<　no　> no session helper sip enable

○ h323
<書　　式> session helper h323 enable
<　no　> no session helper h323 enable

○ ftp
<書　　式> session helper ftp enable
<　no　> no session helper ftp enable

○ amanda
<書　　式> session helper amanda enable
<　no　> no session helper amanda enable

○ sane
<書　　式> session helper sane enable
<　no　> no session helper sane enable

○ snmp
<書　　式> session helper snmp enable
<　no　> no session helper snmp enable

○ irc
<書　　式> session helper irc enable
<　no　> no session helper irc enable

○ pptp
<書　　式> session helper pptp enable
<　no　> no session helper pptp enable

## ■ system boot cms

○ basic-information
<説　　明> システム起動時に、CMS に basic information を送信します。
<書　　式> system boot cms basic-information
<　no　　> no system boot cms basic-information

○ extra-information
<説　　明> システム起動時に、CMS に extra information を送信します。
<書　　式> system boot cms extra-information
<　no　　> no system boot cms extra-information

## ◆ system clock mobile

<説　　明> 内蔵通信モジュールを利用して、時刻同期を行います。
<書　　式> system clock mobile 1
<　no　　> no system clock
<備　　考> NTP サーバ(ntp mode)を設定している場合、当該コマンドの設定は出来ません。
nxr(config)#system clock mobile 1
% NTP server is already configured

## ◆ ip access-list-dynamic

<説　　明> 動的 IP アクセスリストを設定します。
<書　　式> ip access-list-dynamic NAME PATTERN
ip access-list-dynamic NAME PATTERN A.B.C.D/M
ip access-list-dynamic NAME PATTERN A.B.C.D
<　no　　> no ip access-list-dynamic NAME
<備　　考>

- ethernet1 の IP アドレスを DHCP で取得する場合は、以下の例のように設定します。
  ip access-list-dynamic DHCP_eth1 dhcp@ethernet1
- 設定した ip access-list-dynamic を、ip access-list の destination に適用する例を示します。
  ip access-list eth1_IN permit any dynamic DHCP_eth1 icmp

### ◆ ipv6 access-list-dynamic

<説　　明> 動的 IPv6 アクセスリストを設定します。
<書　　式> ipv6 access-list-dynamic NAME PATTERN
ipv6 access-list-dynamic NAME PATTERN X:X::X:X/M
ipv6 access-list-dynamic NAME PATTERN X:X::X:X
ipv6 access-list-dynamic NAME PATTERN eui-64
ipv6 access-list-dynamic NAME PATTERN mape-rule
< no > no ipv6 access-list-dynamic NAME
<備　　考>
・ ethernet1 の IPv6 アドレスを RA で取得する場合は、以下の例のように設定します。
ipv6 access-list-dynamic RA_eth1 ra-prefix@ethernet1 eui-64
・ 設定した ipv6 access-list-dynamic を、ipv6 access-list の destination に適用する例を示します。
ipv6 access-list eth1_IN permit any dynamic RA_eth1 icmp

### ◆ ip access-list-verdict

<説　　明>
global mode
・ip access-list のルール(permit/deny)が、forward-in と forward-out で異なる場合について、
forwarding のルールを設定します。
<書　　式> ip access-list-verdict forward (combile|separate)
< no > no ip access-list-verdict forward
<備　　考>
・combine: forward-in permit, forward-out deny の両方にマッチする場合、パケットの転送を許可(permit)します。
・separate: forward-in permit, forward-out deny の両方にマッチする場合、パケットの転送を拒否(deny)します。
・combine(SPI 有効時): forward-out permit にマッチする場合、パケットの転送を許可(permit)します。
・separate(SPI 有効時): forward-out permit にマッチする場合、パケットを転送しません。SPI で拒否(deny)します。

### ◆ ipv6 access-list-verdict

<説　　明>
・ip access-list のルール(permit/deny)が、forward-in と forward-out で異なる場合について、forwarding のルールを設定します。
<書　　式> ipv6 access-list-verdict forward (combile|separate)
< no > no ipv6 access-list-verdict forward (combile|separate)
<備　　考>
・combine: forward-in permit, forward-out deny の両方にマッチする場合、パケットの転送を許可(permit)します。
・separate: forward-in permit, forward-out deny の両方にマッチする場合、パケットの転送を拒否(deny)します。
・combine(SPI 有効時): forward-out permit にマッチする場合、パケットの転送を許可(permit)します。
・separate(SPI 有効時): forward-out permit にマッチする場合、パケットを転送しません。SPI で拒否(deny)します。

# 第 6 章　interface mode

◆ 移行 command
nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**interface ethernet <0-2> [vid <1-4094>]**
nxrg240(config-if)#

nxrg240(config)#**interface loopback <0-9>**
nxrg240(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)
　　ip address dhcp (|HOSTNAME)
　　ip address mape-rule WORD
< no > no ip address A.B.C.D/M (|secondary)
　　no ip address dhcp
　　no ip address

**◆ ipv6 address**
<説　　明> インタフェースに IPv6 アドレスを設定します。
<書　　式> ipv6 address X:X::X:X link-local
　　ipv6 address X:X::X:X/M (|eui-64)
　　ipv6 address autoconfig
　　ipv6 address autoconfig interface-id mape-rule WORD
　　ipv6 address NAME1 X:X::X:X/M (|mape-rule NAME2|eui-64)
< no > no ipv6 address X:X::X:X link-local
　　no ipv6 address X:X::X:X/M (|eui-64)
　　no ipv6 address autoconfig
　　no ipv6 address NAME1 (|X:X::X:X/M)
<備　　考>
・ link-local 指定時は、自動的に設定される LLA を上書きします。
・ eui-64 指定時は、ipv6-address は prefix 部のみ指定します。
・ ipv6 address autoconfig/dhcp/DHCPv6-PD/proxyconfig は、一つのインタフェースに対して、どれか一つを設定することが出来ます。
・ NAME1 には、ipv6 プレフィクス名を指定します。NAME2 には、MAP-E ルール名を指定します。以下に設定例(interface mode)を示します。
　　ipv6 address NAME1 ::/64 mape-rule NAME2
　NAME1 の設定例(ipv6 dhcp-client mode)です。
　　ipv6 dhcp-client ipv6dhcpc
　　　ia-pd NAME1
　NAME2 の設定例(global mode)です。
　　mape-rule NAME2 type ocn auto

### ◆ ipv6 address proxyconfig

<説　　明> RA proxy で受信した prefix を使用して、IPv6 アドレスを設定します。
<書　　式> ipv6 address proxyconfig
　　ipv6 address proxyconfig interface-id X:X::X:X
　　ipv6 address proxyconfig interface-id mape-rule WORD
< no　> no ipv6 address proxyconfig
<備　　考>

- ethernet インタフェースに設定することが出来ます。
- ipv6 address (autoconfig|dhcp|DHCPv6-PD|proxyconfig)は、どれか一つを設定することが出来ます。
- 本設定と異なるインタフェースに、RA proxy を設定します。

```
!
interface ethernet 0
  ipv6 address proxyconfig interface-id X:X::X:X
!
interface ethernet 1
  ipv6 nd accept-ra proxy ethernet 0
!
```

### ◆ ipv6 address DHCPv6-PD

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

- ipv6-address は、sub-prefix と host 部を指定することが出来ます。
- DHCPv6-PD は、DHCPv6 PD で受信する prefix 部のプロファイル名です。DHCPv6-PD は、DHCPv6 パケットを受信するインタフェース(異なるインタフェース)上で、ipv6 dhcp client pd コマンドを使用して設定します。
- ipv6 address (autoconfig|dhcp|DHCPv6-PD|proxyconfig)は、どれか一つを設定することが出来ます。

### ◆ ipv6 dhcp client

<説　　明> 当該インタフェースに適用する DHCPv6 クライアントのプロファイル名を指定します。
<書　　式> ipv6 dhcp client WORD
< no　> no ipv6 dhcp client

◆ **ipv6 dhcp client pd**

<説　　明> DHCPv6 PD の prefix 部に、プロファイル名を付けます。
<書　　式> ipv6 dhcp client pd DHCPv6-PD
< no　> no ipv6 dhcp client
<備　　考>
- DHCPv6 PD を受信するインタフェース上で設定します。
- 受信した DHCPv6 PD を(異なる)インタフェースに対して適用するには、ipv6 address DHCPv6-PD コマンドを使用します。
- ipv6 dhcp client WORD と ipv6 dhcpv6 pd DHCPv6-PD は、どちらか一方だけ設定可能です。

◆ **ipv6 dhcp server**

<説　　明> 当該インタフェース上で、DHCPv6 サーバを起動します。
<書　　式> ipv6 dhcp server WORD
< no　> no ipv6 dhcp server
<備　　考> WORD には、起動する DHCPv6 サーバのプロファイル名を指定します。

◆ **ipv6 address dhcp WORD**

<説　　明> 当該インタフェースに適用する DHCPv6 クライアントのプロファイル名を指定します。
<書　　式> ipv6 address dhcp WORD
< no　> no ipv6 address dhcp WORD
<備　　考>
- ipv6 address (autoconfig|dhcp|DHCPv6-PD|proxyconfig)は、どれか一つを設定することが出来ます。

◆ **speed**

<説　　明> インタフェーススピードとモード(full/half)を設定します。
　　Default は、auto-negotiation を有効とし、各 ethernet Port に対して設定することができます。
<書　　式> speed (auto|10-full|10-half|100-full|100-half|auto-limit) (|port <1-4>)
<初 期 値> speed auto
<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、1000Mlink することができません)。
- auto-negotiation 時の優先順位は、次のとおりです。
- 優先度(高) 1000M > 100M-Full > 100M-Half > 10M-Full > 10M-Half 優先度(低)
- 通信モードを auto-negotiation に設定した機器と固定に設定した機器との間で、実際に使用する通信モードおよび通信の可否は次のとおりです。

| 設定上の通信モード | | 実際の通信モード | 通信の可否 |
|---|---|---|---|
| auto | 100M-Full | 100M-Half | × |
| auto | 100M-Half | 100M-Half | ○ |
| auto | 10M-Full | 10M-Half | × |
| auto | 10M-Half | 10M-Half | ○ |

◆ **speed auto-limit (100|1000|2500|5000)**

<説　　明> 10Gbps のインタフェースを搭載するポートで設定することが出来ます。
<書　　式> speed auto-limit (100|1000|2500|5000)
<備　　考>
- 10Gbps のインタフェースで指定できるのは、auto、auto-limit (100|1000|2500|5000)、100M-full です。
- auto-limit 100　　100Mbps までのスピードでリンクすることが出来ます。
- auto-limit 1000　　1000Mbps までのスピードでリンクすることが出来ます。
- auto-limit 2500　　2.5Gbps までのスピードでリンクすることが出来ます。
- auto-limit 5000　　5Gbps までのスピードでリンクすることが出来ます。
- auto-limit　　1000Mbps までのスピードでリンクすることが出来ます。

・ auto　　10Gbps までのスピードでリンクすることが出来ます。

◆ **mdix auto**

<説　　明>

・ 相手 port の MDI/MDI-X を自動判別し、接続する機能です。
・ 通常、MDI と MDI-X で接続する場合は、ストレートケーブルを使用します。一方、MDI と MDI、MDI-X と MDI-X で、接続する場合は、クロスケーブルを使用します。
・ auto MDI/MDI-X が有効の場合、ストレート / クロスに関係なく、どちらのケーブルでも接続することが出来ます。

<書　　式> mdix auto

<初 期 値> mdix auto

<　no　　> no mdix auto

<備　　考>

・ auto-negotiation が有効(speed auto/auto-limit)の場合、(mdix auto/no mdix auto の設定にかかわらず)常に本機能が有効になります。
・ auto-negotiation が無効の場合、mdix auto/no mdix auto の設定に従います。
・ 本機能の状態は、show interface mdix コマンドで確認することが出来ます。
・ 本機能が無効(no mdix auto、かつ speed 固定)の場合、スイッチポートは mdi-x、ルーターポートは mdi として動作します。

◆ **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。

◆ **bandwidth**

<説　　明> インタフェースの帯域幅を設定することが出来ます。
bandwidth の初期値は、10Mbps です。
bandwidth の最大値は、10Gbps です。
<書　　式> bandwidth <1-10000000000[k/m/g]>
<　no　> no bandwidth
<備　　考> 本機能は、OSPF のコスト計算時のみに使用します。
基準となる帯域幅は、auto-cost コマンド(ospf mode)にて設定します。

◆ **mtu**

<説　　明> MTU の値を設定します。
<書　　式> mtu <bytes:68-1500>
<初 期 値> mtu 1500
<　no　> no mtu (= Set defaults)

◆ **ip proxy arp**

<説　　明> Proxy ARP を有効にします。
<書　　式> ip proxy-arp
<初 期 値> no ip proxy-arp
<　no　> no ip proxy-arp
<備　　考>
・ Proxy ARP は、受信したインタフェースとは異なる宛先への ARP request に対して、代理で応答する機能です。
・ forwarding の対象外のアドレス(ブロードキャストアドレスやネットワークアドレス)に対する ARP request には応答しません。

### ◆ ip local proxy arp

<説　　明> Local proxy ARP を有効にします。
<書　　式> ip local-proxy-arp
<初 期 値> no ip local-proxy-arp
<　no　　> no ip local-proxy-arp
<備　　考>

- Local proxy ARP は、受信したインタフェースのサブネット宛ての ARP request に対して、代理で応答する機能です。
- Default は無効で、Ethernet/VLAN/bridge インタフェース上で使用することが出来ます。
- forwarding の対象外のアドレス(ブロードキャストアドレスやネットワークアドレス)に対する ARP request には応答しません。
- Local proxy ARP は、直接端末同士が通信できない環境(VLAN 環境 etc)やブロードキャストが禁止されている環境で利用します。
- local proxy ARP を利用する際は、リダイレクトメッセージが送信されないように、ip send-redirects 機能を無効にしておくことを推奨します。
- Local proxy ARP が応答する条件は、次のとおりです。
  sender IP と target IP が異なる場合
  target IP が受信インタフェースのネットワークと同じ場合

### ◆ ip directed-broadcast

<説　　明> Directed Broadcast のフォワーディングを有効にします。
<書　　式> ip directed-broadcast
<初 期 値> no ip directed-broadcast
<　no　　> no ip directed-broadcast

### ◆ ip redirects

<説　　明>

・ ICMP redirect(type=5)とは、同一ネットワーク上に他の最適なルートがあることを通知するためのメッセージです(RFC792)。

・ 本装置の Send redirect 機能によって、ICMP redirect の送信の有無を切り替えることが出来ます。

<書　　式> ip redirects

<初 期 値> ip redirects　　(有効)

<　no　　> no ip redirects　　(無効)

<備　　考>

・ 以下に ICMPRedirect の例を示します。ICMP Redirect 受信後の動作は、Host 側の動作に依存するため、常に次のような動作になるというわけではありません。

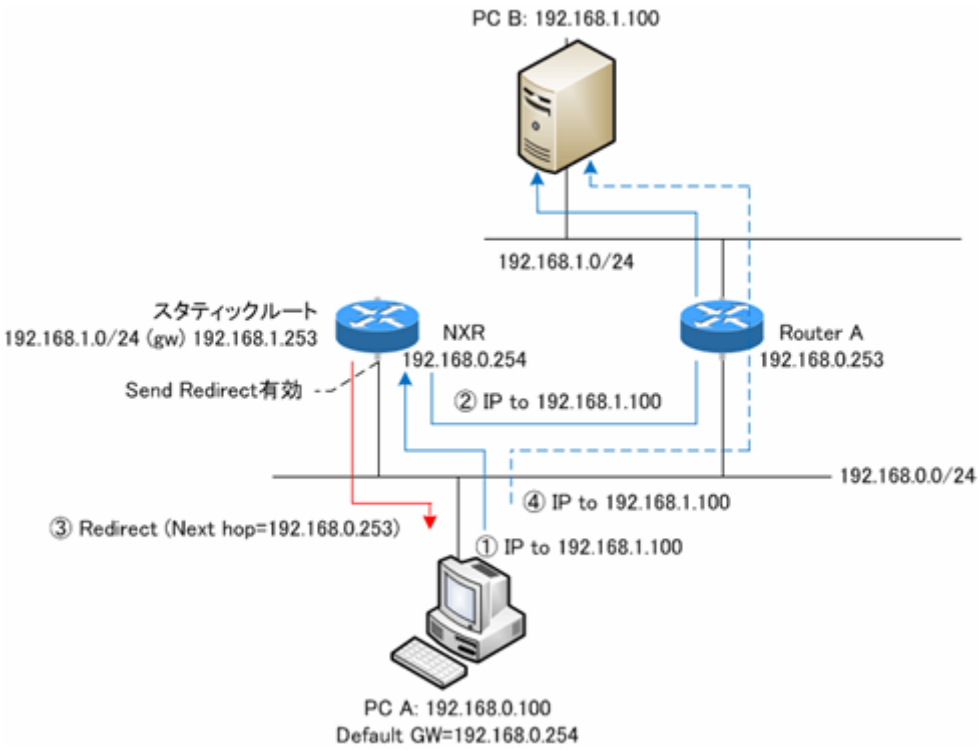
① Host A は、Host B(192.168.1.100)への IPv4 パケットを default gw(NXR)に送信します。

② NXR は、ルーティング情報から、192.168.1.0/24 宛ての next hop は 192.168.1.253 であることを知り、Router A へ転送します。

③ このとき、next hop の Router A は、送信元の Host A と同一ネットワークであるため、Host A に ICMP Redirect を送信します。

④ Host A は、以降の Host B 宛ての IPv4 パケットは、ICMP Redirect で通知された next hop に従って、Router A へ送出します。

・ 本装置が、ICMP Redirect を受信した場合は、ルーティングキャッシュの更新をしません。ルーティングテーブルに従った forwarding 動作を継続します。



### ◆ ip tcp adjust-mss

<説　　明>

・ Path MTU Discovery(PMTUD)機能(End-to-end でフラグメントが発生しない最大の MTU を発見すること)によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器(ルータ等)が ICMP fragment needed をフィルタリングしている場合(ブラックホールルータが存在する場合)や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、Endto-end での通信に支障をきたすことになります。このような場合、TCP では SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

<書　　式> ip tcp adjust-mss (auto|<500-1460:bytes>)

<初 期 値> no ip tcp adjust-mss

<　no　> no ip tcp adjust-mss

<備　　考>

・ IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。

・ 本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ ユーザが設定する場合は、MSS 値を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。

・ 「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

### ◆ ip mask-reply

<説　　明>

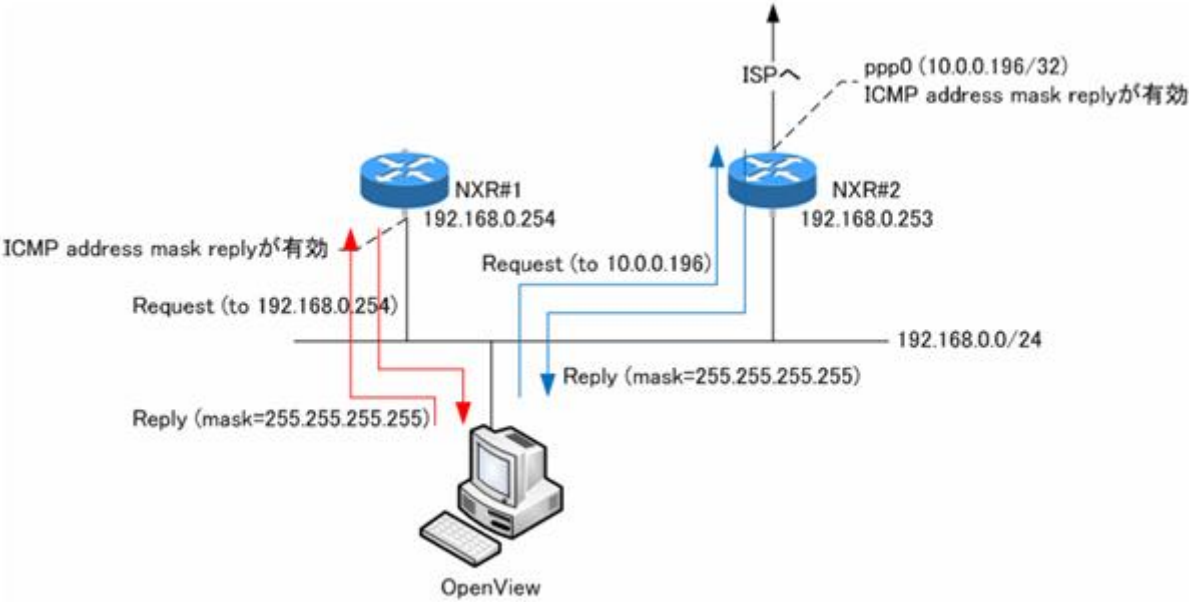
・ OpenView などの監視装置では、監視ネットワーク内の機器に対して ICMP address mask request (type=17)を送信することによって機器のインタフェースのネットマスク値を取得します(単純に、死活監視で使用する場合もあります)。

・ 本装置では、ICMP address mask request への応答の有無を設定することが出来ます。

<書　　式> ip mask-reply　　(ICMP address mask request に応答します。)
<初 期 値> no ip mask-reply　　(ICMP address mask request に応答しません。)
<　no　　> no ip mask-reply

<備　　考>

・ ICMP address mask request/reply の例を示します。



### ◆ link-check

<説　　明>

- Ethernet link 状態の監視を行います。Default は 10[sec]とし、0[sec]を設定した場合 link down を検知しません(常に up の状態です)。Link 状態に変化が発生した場合、以下のような動作が行われます。
- なお、ethernet 上で vlan を作成している場合、ethernet の link up/down に伴い vlan interface の link 状態も up/down へと遷移します。VLAN interface 毎に link 監視を行うことはできません。

| up への遷移 | down への遷移 |
|---|---|
| Connected route の有効化(RIB/FIB への追加) | Connected route の無効化(RIB/FIB から削除) |
| 該当 interface を出力 interface とする route の有効化 | 該当 interface を出力 interface とする route の無効化 |
| Interface に割り当てられている IP address への通信可 | Interface に割り当てられている IP address への通信不可(但し、ip/ipv6 access-linkdown が有効な場合、linkdown 状態でも通信が可能) |
| Bind 設定されている機能の有効化 | Bind 設定されている機能の無効化 |
| Network event 設定に伴う動作 | Network event 設定に伴う動作 |
| Router solicitation の送信(IPv6) | － |

※ Connected route の有効化 / 無効化は、show ip route database で確認することが出来ます。

- RIB(Routing Information Base)は、経路情報を蓄積するデータベースで、管理者の手動設定による経路や経路制御プロトコルによって学習した経路が、原則としてすべて登録されます。
- FIB(Forwarding Information Base)は、IP パケットの転送判断時に参照するデータベースです。RIB 内に同一宛先への経路が複数存在している場合は、最適経路だけが FIB に登録されます。

<書　　式> link-check (|<0-60sec>)
<初 期 値> link-check 10
<　no　　> no link-check (=link-check 0)
<備　　考>

- bind 設定されている機能の有効化 /無効化について
  Ethernet interface 上で tunnel interface や PPPoE が確立されていた場合、link down 検知後すぐにこれらの interface が down 状態になることはありません。Tunnel interface や PPP interface の up/down は、それぞれの keepalive 機能に依存します。但し、USER によって bind 設定(該当 interfacedown を trigger に L2TP tunnel/session を切断するなど)が設定されていた場合は、この限りではありません。
- Switching HUB が装備されている ethernet interface の link 監視について
  内部の Switching HUB と接続されている ethernet interface 上で link 監視を行っている場合、switching hub port すべてが link down となった際に ethernet link down となり、1 つでも switching hub port の link が up した際に、ethernet link up 状態へと遷移します。

◆ **ip access-linkdown**

<説　　明> 本機能を有効にすると、link down の状態でも該当 interface の IPv4 address に通信することができます。
<書　　式> ip access-linkdown
< no　> no ip access-linkdown
<備　　考> Default は、無効(no ip access-linkdown)です。

◆ **ipv6 access-linkdown**

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

◆ **ip arp reachable-time**

<説　　明> 解決した ARP の有効期間を設定することが出来ます。単位は msec です。
<書　　式> ip arp reachable-time <30000-3600000>
<初 期 値> ip arp reachable-time 30000
< no　> no ip arp reachable-time
<備　　考> show arp 実行時に、ステータスが REACHABLE と表示される時間です。
実際の時間は、(0.5 ～ 1.5)× reachable-time の間のランダムな値です。

◆ **ip arp queue length**

<説　　明>
- Ethernet/Vlan interface 上で、IPv4 通信を行う場合、送信先(nexthop)の mac address の解決を行います。このとき、mac address が解決するまで queueing できるパケット数を指定することができます。
- Queue は、neighbor の entry 毎に作成されます。
- queueing された packet は、address 解決ができると同時に送信が行われます。
- Queue が full の状態で新たに packet が来た場合、queue の先頭から drop されます。

<書　　式> ip arp queue length <1-1000>
<初 期 値> no ip arp queue length (=3[packets])
< no　> no ip arp queue length
<備　　考> IPv4 の IPv6 それぞれについて、interface 毎に指定することができます。
IPv6 については、ipv6 nd queue length を参照してください。

◆ **ipv6 tcp adjust-mss**

<説　　明> TCP/IPv6 の MSS 値を設定します。
<書　　式> ipv6 tcp adjust-mss (auto|500-1460)
<初 期 値> no ipv6 tcp adjust-mss
< no　> no ipv6 tcp adjust-mss

■ NDP

Ethernet/VLAN/Bridge インタフェース上で、RA によるアドレス割り当て、または RA 受信が有効になっている場合、当該インタフェースで RA を受信し、IPv6 address prefix や gateway 情報などを取得することが出来ます。
本装置では、以下のパラメータをサポートしています（RA を受信したインタフェースのパラメータとして使用します）。

- prefix information: ipv6 address autoconfig が未設定の場合は、prefix information を無視します。
- router preference: 複数の RA ルータから異なる preference 情報を受信した場合、high>middle>low の順で採用します。
- MTU:複数の RA ルータから異なる値を受信した場合、show ipv6 interface では、大きい方の値を表示します。RA ルータを経由して通信する際は、当該 RA ルータが広告した MTU 値を利用します。なお、RA ルータが広告した MTU 値は、show ipv6 default-gateway にて確認することが出来ます。
- default-gateway: RA パケットのソースアドレス（リンクローカルアドレス）
- preferred lifetime
- valid lifetime
- router lifetime
- hop limit:複数の RA ルータより異なる値を受信した場合、show ipv6 interface では小さいほうの値を表示します。RA ルータを経由して通信する際は、当該 RA ルータが広告した hop-limit 値を利用します。なお、RA ルータが広告した hop-limit 値は、show ipv6 default gateway で確認することが出来ます。
- ns interval: 複数の RA ルータから、異なる値を受信した場合、大きい値を採用します。
- reachable-time: 複数の RA ルータから、異なる値を受信した場合、大きい値を採用します。

※ RA を受信すると、受信した RA の値でユーザ設定値を上書きします。CLI 等から設定変更を行った場合は、ユーザ設定値で RA の値を上書きします。常に新しい設定値を採用します（現在の値は、show ipv6 interface コマンドで確認することが出来ます）。

◆ **ipv6 nd send-ra**

<説　　明> IPv6 RA(Router Advertisement)を送信します。

<書　　式> ipv6 nd send-ra (送信)

<　no　　> no ipv6 nd send-ra (停止)

<備　　考>

・ RA による prefix 広告は、Ethernet/VLAN/bridge 上にて使用することが出来ます。

・ 以下のパラメータをユーザ設定値(あるいはシステム固定値)にセットして、RA 送信を行います。

- router lifetime: ipv6 nd lifetime による設定値
- hop limit: ipv6 hop-limit による設定値(default:64)
- reachable-time: ipv6 nd reachable-time による設定値
- retransmit timer: ipv6 nd ns-interval による設定値

**RA flags**

- default router preference: ipv6 nd router-preference による設定値(default:medium)
- managed-config-flag: ipv6 nd managed-config-flag による設定値(default:0)
- other-config-flag: ipv6 nd other-config-flag による設定値(default:0)

※ home agent flag, proxy flag はいずれも 0 をセットします。

※本バージョンでは、DHCPv6 server をサポートしていないため、O flag または M flag が 1 の場合、別途 DHCPv6 server が必要になります。

**Prefix information: ICMPv6 type3**(ipv6 nd prefix により設定します。)

- prefix/prefix length
- preferred lifetime
- valid lifetime
- autonomous address-configuration flag:ipv6 nd prefix X:X::X:X/M no-autoconfig が設定されている場合は 0、未設定は 1. default:1
- on-link flag:ipv6 nd prefix X:X::X:X/M off-link が設定されている場合は 0、未設定時は 1. default:1。ただし、ipv6 nd prefix で設定した prefix と同じ prefix を当該インタフェース上の connected route として保持している場合(IPv6 address 設定している場合等)は、本設定に関係なく常に 1.
- router address flag:常に 0

**MTU:iCMPv6 type5**

- MTU:インタフェースの MTU 値

**Source link-layer address: iCMPv6 type1**

- -link-layer address: ipv6 nd no-advertise-link-address の有効時、本オプションは広告しません。無効時は、出力インタフェースの link-layer address(MAC アドレス)を設定します。default:無効(本オプションを広告)です。

◆ **ipv6 nd accept-ra**

<説　　明>
- 本設定(ipv6 address autoconfig 設定なし)を有効にすると、RA を受信しても、stateless address を設定しません。

<書　　式> ipv6 nd accept-ra
<　no　> no ipv6 nd accept-ra
<備　　考>
- ipv6 address autoconfig 設定時、本設定は必要ありません。
- 当該インタフェースに、IPv6 アドレスは設定しませんが、RA によって取得したパラメータ(defaultgateway, retransmit timer, reachable time, mtu, hop-limit)は使用します。

◆ **ipv6 nd prefix**

<説　　明> IPv6 RA(Router Advertisement)にて広告する prefix を設定します。
<書　　式> ipv6 nd prefix X:X:X:X::X/M
　　<valid-liftime:0-4294967295> <preferred-lifetime:0-4294967295>
　　(|{off-link|no-autoconfig})
　　ipv6 nd prefix X:X::X:X/M (|{off-link|no-autoconfig})
　　ipv6 nd prefix X:X::X:X/M no-advertise
<　no　> no ipv6 nd prefix (|X:X:X:X::X/M )
<備　　考>
- 広告する prefix は、当該インタフェースに設定している IPv6 アドレスの prefix(ただし、autoconfiguration によるアドレスは除く)、ユーザが設定した prefix、および DHCPv6-PD によって取得した prefix(VRRPv3 の実行中を除く)です。
- インタフェースに設定している prefix、ユーザ指定による prefix、DHCPv6-PD によって取得した prefix が同じ場合は、ユーザ指定の prefix 設定を使用します。
- valid/preferred lifetime は、ユーザ指定を除く prefix を広告する場合、固定値(preferred lifetime は 604800sec、valid lifetime は 2592000sec)を使用します。
- 一方、ユーザ指定の prefix は、ユーザ設定値を使用します。ユーザ設定値がない場合は、上記の固定値を使用します。
- no-advertise を指定すると、当該 prefix を広告しません(default:1)。
- off-link を指定すると、当該 prefix の on-link flag を 0 に設定して広告します(default:1)。
- no-autoconfig を指定すると、当該 prefix の autonomous address-configuration flag を 0 に設定して広告します(default:1)。
- RA で広告する prefix に変更があった場合、古い prefix は変更直後の 1 回のみ preferred lifetime を 0、valid lifetime を 7203 に設定して RA を送信します。Preferred lifetime が 0 の RA を受信することによって、LAN 内のクライアントは、当該 IPv6 アドレスを使用しなくなります。RA を停止する際は、preferred lifetime を 0 にすることに加え、router lifetime を 0 にして送信します。

◆ **ipv6 nd ra-lifetime**

<説　　明> IPv6 RA(Router Advertisement)ライフタイムを設定します。
<書　　式> ipv6 nd ra-lifetime <0-9000>
<初 期 値> ipv6 nd ra-lifetime 1800
<　no　> no ipv6 nd ra-lifetime
<備　　考> ra-lifetime >= ra-interval max

◆ **ipv6 nd ra-interval**

<説　　明> IPv6 RA(Router Advertisement)インターバルを設定します。
<書　　式> ipv6 nd ra-interval <min:3-1350> <max:4-1800>
<初 期 値> ipv6 nd ra-interval 200 600
<　no　> no ipv6 nd ra-interval
<備　　考>

- min < max x 0.75 となるように設定してください。
- VRRPv3 が設定されているインタフェースでは、RA を有効にした場合でも、常に RA 広告するわけではなく、VRRP マスターの場合に限り送信します。また、広告する prefix は、インタフェース上に設定している IPv6 address prefix ではなく、仮想 IPv6 address prefix を広告します。仮想 IPv6 アドレスが未設定の場合は、prefix を広告しません。

■ **RS の送信**

RA メッセージを要求する際に送信するパケットです。以下のタイミングで、RS を送信します。

- LLA を設定 / 変更した場合
- インタフェースが、administratively down(管理者による shutdown)から up となった場合
- インタフェースのリンク状態が、down から up となった場合

※ RS は、RA 受信が有効でない場合は、送信しません。

■ **RS の受信**

IPv6 forwarding が有効の場合のみ受信します。RS を受信した場合、RA の送信処理の実行や受信パケットの neighbor 情報の更新に利用します。

◆ **ipv6 nd rs-interval**

<説　　明> IPv6 Router Solicitation インターバルを設定します。
<書　　式> ipv6 nd rs-interval <interval:1-10sec>
<初 期 値> ipv6 nd rs-interval 1
<　no　> no ipv6 nd rs-interval (初期値)

◆ **ipv6 nd rs-count**

<説　　明> IPv6 Router Solicitation の送信回数を設定します。
<書　　式> ipv6 nd rs-count <count:1-2147483647>
<初 期 値> ipv6 nd rs-count 3
<　no　> no ipv6 nd rs-count (初期値)

◆ **ipv6 nd reachable-time**

<説　　明> 隣接ノードの到達性確認間隔を指定します。
<書　　式> ipv6 nd reachable-time <msec:0-3600000>
<初 期 値> ipv6 nd reachable-time 30
<　no　> no ipv6 nd reachable-time (初期値)

◆ **ipv6 nd managed-config-flag**

<説　　明> RA flag(managed-config-flag)を設定することが出来ます。
<書　　式> ipv6 nd managed-config-flag　　(M flag=1)
<初 期 値> no ipv6 nd managed-config-flag　　(M flag=0)
<　no　> no ipv6 nd managed-config-flag

◆ **ipv6 nd other-config-flag**

<説　　明> RA flag(other-config-flag)を設定することが出来ます。
<書　　式> ipv6 nd other-config-flag　　(O flag=1)
<初 期 値> no ipv6 nd other-config-flag　　(O flag=0)
<　no　> no ipv6 nd other-config-flag

◆ **ipv6 nd router-preference**

<説　　明> RA flag(router-preference)を設定することが出来ます。
<書　　式> ipv6 nd router-preference (high|low|medium)
<初 期 値> ipv6 nd router-preference medium
<　no　> no ipv6 nd router-preference

◆ **ipv6 nd no-advertise-link-address**

<説　　明> Source link-layer address option の広告(する / しない)を設定します。
<書　　式> ipv6 nd no-advertise-link-address
<初 期 値> no ipv6 nd no-advertise-link-address
<　no　> no ipv6 nd no-advertise-link-address
<備　　考> 有効:source link-layer address option を送信します。
　　無効:source link-layer address option を送信しません。

■ NDP Proxy

・ NDP を受信した際に代理応答する機能です。NTT NGN の IPoE 環境(ひかり電話なし)etc での利用が考えられます。
・ 各 NDP パケットを受信した場合、NDP Proxy 機能は、次のように動作します。
- **NS パケット**:本バージョンでは、RA Proxy 機能が有効かつ RA で受信した prefix に対する NS に対してのみ代理応答を行い、NA パケットを返します。すべての NS に対して代理応答するわけではありません。
- RA ルータがダウンした場合(RA Proxy 機能による判定)や、prefix 情報に変更があった場合は、RA を受信していたインタフェース上のすべての NDP proxy エントリを消去します。
- **NA パケット**:NA パケットを受信しても何も行いません。
- **RS パケット**:RS パケットを受信しても何も行いません。
- **RA パケット**:受信した RA パケット パケットに対して代理応答を行うことはありませんが、RA Proxy によって受信した RA 情報を他のインタフェースへ広告することが出来ます。

■ RA Proxy

・ RA Proxy:受信した RA パケット内の prefix 情報を、指定したインタフェースに対して代理で送信する機能です。
・ prefix 以外の情報は、受信したインタフェースでのみ利用します(他のインタフェースへ送信しません)。
・ 例えば、NGN IPoE 環境などで RA による prefix 広告を行う場合、RA ルータとユーザ端末間にルータが存在すると、RA パケットがユーザ端末側に届かないため、LAN 側のホスト上で、auto configuration を行うことが出来ません。このような場合に、本機能を利用します。
・ IPv6 ブリッジの場合、RA 広告はブリッジしますが、アクセスリストなどは利用できません。RA Proxy の場合は、layer3 フォワーディングのため、アクセスリスト等のルータ機能も利用することが出来ます。
・ 代理で送信可能な prefix は最大 10 個で、これ以上の prefix 情報は無視します。WAN 側に複数の RA ルータが存在する場合、最初に受信した RA パケットの送信元ルータからの情報のみを使用します。その後、当該ルータからの応答がなくなった場合は、他のルータからの RA パケットを使用します。

◆ **ipv6 nd accept-ra proxy**

<説　　明> RA Proxy を有効にします。
<書　　式> ipv6 nd accept-ra proxy ethernet <0-X>
　　(|rs-interval <0-604800> rs-count <1-255>)
<備　　考>

・ RA Proxy 機能は、NDP Proxy 機能の一部ですが、本装置では、NS パケットに対する代理応答の機能を NDP Proxy 機能とし、RA Proxy 機能とは異なる機能として扱います。
・ 本バージョンでは、NDP Proxy 機能のみを有効にすることは出来ません。RA Proxy 機能と同時に使用します。
・ Default では、NDP Proxy および RA Proxy 機能は無効です。



### ◆ ipv6 nd ns-interval

<説　　明> NS の送信間隔を設定します。
<書　　式> ipv6 nd ns-interval <msec:1000-3600000>
<初 期 値> ipv6 nd ns-interval 1000
<　no　> no ipv6 nd ns-interval

### ◆ ipv6 nd dad attempts

<説　　明> IPv6 DAD の送信回数を設定します。
<書　　式> ipv6 nd dad attempts <0-600>
<初 期 値> ipv6 nd dad attempts 1
<　no　> no ipv6 nd dad attempts

### ◆ ipv6 nd accept-redirects

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

### ◆ ipv6 nd queue length

<説　　明>
- Ethernet/Vlan interface 上で IPv6 通信を行う場合、近隣探索(Neighbor Discovery)によって送信先(nexthop)の mac address の解決を行います。このとき、mac address が解決するまで queueing できるパケット数を指定することができます。
- Queue は、neighbor の entry 毎に作成されます。
- queueing された packet は、address 解決ができると同時に送信が行われます。
- Queue が full の状態で新たに packet が来た場合、queue の先頭から drop されます。

<書　　式> ipv6 nd queue length <1-1000>
<初 期 値> no ipv6 nd queue length (= 3[packets])
<　no　> no ipv6 nd queue length
<備　　考> IPv4 の IPv6 それぞれについて、interface 毎に指定することができます。
　　IPv4 については、ip arp queue length を参照してください。

### ◆ ipv6 nd ra-dns-server

<説　　明> ルータ広告で送信する DNS サーバを設定します。
<書　　式> ipv6 nd ra-dns-server X:X::X:X
　　ipv6 nd ra-dns-server dhcp-client INTERFACE
<　no　> no ipv6 nd ra-dns-server X:X::X:X
　　no ipv6 nd ra-dns-server dhcp-client
　　no ipv6 nd ra-dns-server

### ◆ ipv6 hop-limit

<説　　明> IPv6 hop-limit を指定することが出来ます。
<書　　式> ipv6 hop-limit <0-255>
<初 期 値> ipv6 hop-limit 64
<　no　> no ipv6 hop-limit
<備　　考>
- 指定した hop-limit を RA のパラメータ(current-hop-limit)に設定します。
- 本機能により、hop-limit を指定した場合、本装置から出力する IPv6 パケットの hop-limit には影響しません。
- 0 を指定した場合、ルータにより hop-limit 数を指定しないことを意味します。

◆ **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 hello-jitter**
<説　　明> Hello インターバルに、揺らぎ(ジッター[%])を持たせます。
<書　　式> ip ospf hello-jitter <1-25>
<　no　> no ip ospf hello-jitter
<備　　考> Hello インターバルをランダムに減少させる最大の割合(パーセンテージ)を指定します。
　　送信タイミングを分散させることで、CPU やネットワークの負荷を平滑化することができます。

◆ **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 で使用する仮想 IP アドレス(VIP)を設定します。
<書　　式> vrrp ip <vrrpid:1-255> address A.B.C.D
<　no　　> no vrrp ip <vrripd:1-255> (address A.B.C.D|)

◆ vrrp ip priority
<説　　明> VRRP のプライオリティを設定します。
<書　　式> vrrp ip <vrrpid:1-255> priority <1-254>
<初 期 値> vrrp ip <vrrpid:1-255> priority 100
<　no　　> no vrrp ip <vrrpid:1-255> priority
<備　　考>
・ マスタールータの priority を高く、バックアップルータの priority を低く設定します。

◆ vrrp ip preempt
<説　　明> Preempt を有効にします。
<書　　式> vrrp ip <vrrpid:1-255> preempt
<初 期 値> vrrp ip <vrrpid:1-255> preempt
<　no　　> no vrrp ip <vrrpid:1-255> preempt
<備　　考>
・ Preempt が有効の場合、priority のもっとも高いルータが常にマスタールータになります。
・ preempt が無効の場合、priority の高いルータが復旧したとしても、現在マスターになっているルータがそのままマスタールータとして動作を継続します。

◆ **vrrp ip preempt delay**

<説　　明>

・ Preempt が有効な場合に、バックアップルータが自分より優先度の低い advertise パケットを受信した際に、バックアップからマスターへ切り替わる時間を遅らせることが出来ます。

・ preempt delay 時間は、1 ～ 1000(秒)の範囲で指定(秒単位)します。

<書　　式> vrrp ip <vrrpid:1-255> preempt delay <1-1000sec>

<　no　　> no vrrp ip <vrrpid:1-255> preempt delay

<備　　考>

・ Preempt delay が設定されている場合、バックアップルータおよびマスタールータは、以下のとおり動作します(マスタールータへの影響はありません。)。

　○ バックアップルータ

　- master down timer、あるいは delay timer がタイムアウトすると advertise を送信してマスターへと状態遷移します。

　- 自分よりも優先度の高い advertise を受信した場合は、バックアップルータとして動作します

　- (delay timer が動作している場合は停止します)。

　- 自分よりも優先度の低い advertise パケットを受信した場合、delay timer が未起動なら delay timer を開始し、master down timer はキャンセルします。また、delay 中に自分より優先度の低い advertise パケットを受信した場合は、無視します(delay timer を継続します)。

　○ マスタールータ

　- 自分よりも優先度の高い advertise を受信した場合、バックアップルータへと遷移します。

　- 自分よりも優先度の低い advertise を受信した場合、advertise を無視します(マスタールータのまま状態遷移しません)。

◆ **vrrp ip timers**

<説　　明> VRRP の advertise の送信間隔を設定します。

<書　　式> vrrp ip <vrrpid:1-255> timers advertise <1-255sec>

<初 期 値> vrrp ip <vrrpid:1-255> timers advertise 1

<　no　　> no vrrp ip <vrripd:1-255> timers advertise

◆ **vrrp ip netevent**

<説　　明> VRRP tracking を設定します。
　　マスタールータに設定します(バックアップルータには設定しません)。
<書　　式> vrrp ip <vrrpid:1-255> netevent <trackid:1-255> priority <1-254>
　　vrrp ip <vrrpid:1-255> netevent <trackid:2048-4095> priority <1-254>
< no > no vrrp ip <vrripd:1-255> netevent
<備　　考>

・ track event が down したときに、マスタールータの priority を指定値に変更します。ここで指定する priority は、バックアップルータの priority より小さい値を設定します。
・ event down 発生時は、priority の大小が逆転するため、マスタールータとバックアップルータが切替ります。

| | |
|---|---|
| 通常 | マスタールータの priority>バックアップルータの priority |
| Event down 発生時 | マスタールータの priority<バックアップルータの priority |

◆ **ip access-group**

<説　　明>
・ global mode で設定した ACL をインタフェースに適用することで、パケットフィルタリングを行うことができます。
<書　　式> ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
< no > no ip access-group (in|out|forward-in|forward-out)
<備　　考>
・ 各インタフェースへのパケットフィルタリングの適用箇所(付録の Packet Traveling を参照)は、以下の 4 ヶ所です。
　- in(local input) NXR 自身で受信して処理するパケットを制限します。
　- out(local output) NXR 自身が作成して出力するパケットを制限します。
　　トンネリングされたパケットも NXR 自身が作成したパケットとして認識します。
　- forward-in NXR が当該インタフェースで受信して forwarding するパケットを制限します。
　- forward-out NXR が受信して当該インタフェースへ forwarding するパケットを制限します。
・ mac 指定のある ACL は、out および forward-out に設定することは出来ません。

◆ **ipv6 access-group**

<説　　明> アクセスグループに IPv6 アクセスリストを追加します。
<書　　式> ipv6 access-group (in|out|forward-in|forward-out) IPV6-ACL-NAME
<初 期 値> 設定なし
< no > no ipv6 access-group (in|out|forward-in|forward-out)

◆ **ip masquerade**

<説　　明>
・ インタフェースよりパケットを出力する際に、パケットの送信元 IPv4 アドレスを出力インタフェースの IPv4 アドレスに自動変換する機能です。
<書　　式> ip masquerade　　(有効)
<初 期 値> no ip masquerade　　(無効)
< no > no ip masquerade
<備　　考>
・ すべてのインタフェース(Ethernet/VLAN/PPP/Tunnel)で設定することが出来ます。
・ TCP/UDP/ICMP のみ対応しています。その他のプロトコルに関しては、動作は保証しません。
・ IPv6 パケットは、IP マスカレードの対象外です。
・ forward out/local output フィルタリング適用後のパケットに、IP マスカレードを適用します。

◆ **ip (snat-group|dnat-group)**

<説　　明>
・ global mode で設定した SNAT または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。
・ SNAT は、パケットの出力時に適用されます。DNAT は、パケットの入力時に適用されます。
<書　　式> ip (snat-group|dnat-group) NAT-NAME
< no > no ip (snat-group|dnat-group)

<備　　考> NAT ルールの設定は、ip snat/ip dnat)コマンド(global mode)で行います。

◆ **ip webauth-filter**
◆ **ipv6 webauth-filter**

<説　　明>
- Web 認証フィルタをインタフェースに適用すると、ある特定のホスト、ネットワークやインタフェースについて、Web 認証せずに通信することが可能となります。
- Web 認証フィルタは、各インタフェースにつき、IN/OUT をそれぞれ一つずつ設定することができます。Default の設定はありません。

<書　　式> ip webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
　　ipv6 webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
< no　> no ip webauth-filter (forward-in|forward-out)
　　no ipv6 webauth-filter (forward-in|forward-out)

<備　　考>
- Web 認証フィルタの設定については、ip web-auth access-list/ipv6 web-auth access-list コマンド(global mode)を参照してください。
- Web 認証については、Web Authenticate mode を参照してください。

◆ **pppoe-client ppp**

<説　　明> PPPoE クライアントを有効にします。
<書　　式> pppoe-client ppp <PPP-INTERFACE-NUMBER:0-4>
<初 期 値> no pppoe-client ppp
<備　　考> 複数指定可能。Ethernet interface のみ。
< no　> no pppoe-client ppp <0-4>

◆ **ip spi-filter**

<説　　明>
- 簡易ファイヤウォールの一つとして、SPI(Stateful Packet Inspection)機能をサポートします。
- パケットに関連するコネクションの状態を見て、当該パケットをドロップするかしないかを決める機能です。

<書　　式> ip spi-filter　　(有効)
<初 期 値> no ip spi-filter　　(無効)
< no　> no ip spi-filter
<備　　考>
- コネクションの状態が、established または related の場合に、パケットの転送を許可します。
- Established とは、すでに双方向でパケットの通信がありコネクションが確立されている状態です。
- Related とは、すでに確立しているコネクションがある状態です。FTP のデータ転送等がこれに該当します。
- 新しい接続でありながら、syn ビットの立っていないパケットはドロップします。
- SPI は、forward in および local input の位置で適用されます。ユーザが適用位置を変更することは出来ません。

◆ **ipv6 spi-filter**
<説　　明> IPv6 SPI filter を設定します。
<書　　式> ipv6 spi-filter
<初 期 値> no ipv6 spi-filter
<　no　　> no ipv6 spi-filter

◆ **ip spi-filter log**
◆ **ipv6 spi-filter log**
<説　　明> フィルタログ機能(syslog mode 参照)を有効にします。
　　パケットが、SPI フィルタにマッチした場合、syslog に出力することが出来ます。
<書　　式> ip spi-filter log [limit <0-100>]
　　ipv6 spi-filter log [limit <0-100>]
<初 期 値> ip spi-filter log limit 10
　　ipv6 spi-filter log limit 10
<　no　　> no ip spi-filter
　　no ipv6 spi-filter
<備　　考>
・ limit を指定すると、1 秒当たりのログ出力数を制限します。初期値は、10 パケット / 秒です。
・ WAN 側からの意図しないパケットが、SPI フィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分に注意してください。

◆ **shutdown**
<説　　明> インタフェース(ethernet <0-3>)をシャットダウンすることができます。
<書　　式> shutdown
<初 期 値> no shutdown
<　no　　> no shutdown

◆ **ipsec policy**
<説　　明> 当該インタフェースで使用する IPsec ローカルポリシーを設定します。
<書　　式> ipsec policy <local policy:1-255>
<　no　　> no ipsec policy (|<local policy:1-255>)
<備　　考>
・ 各インタフェースに、IPsec ローカルポリシーを 4 つまで設定することが出来ます。他のインタフェースで既に設定している IPsec ローカルポリシーは、重複して設定できません。

◆ **ipsec policy-ignore**

<説　　明>

・ IPsec policy のチェックを行わないように指定する機能です。IPsec policy として any などを指定したけれども、特定の通信のみ IPsec 化したくない場合に、この機能を使用します。

<書　　式> ipsec policy-ignore (|input|output)

<初 期 値> no ipsec policy-ignore(無効)

<　no　> no ipsec policy-ignore

<備　　考>

・ Input を指定した場合、inbound policy check を実行しないため、IPsec 化されてくるべきパケットがドロップ されてしまう現象を回避することができます。

・ Output を指定した場合、当該インタフェースから出力されるパケットは、IPsec policy をチェックしないため平文で送信されます。

## ■ QoS

<説　　明> QoS の設定をします。

○ HTB の設定

<書　　式> queue policy POLICYNAME bandwidth <1-1000000> (|ifg-pa-fcs)

<備　　考>

- HTB を設定するには、class policy コマンドで作成した class policy を指定します。
- 存在しない class policy を指定すると、親 class のみ設定されます。該当する class policy を作成したときに、当該 HTB が設定されます。
- bandwidth で、class policy の全帯域幅を指定します。
- ifg-pa-fcs(後述)を指定することが出来ます。Default は無効です。

○ PQ の設定

<書　　式> queue priority-group <PRIORITY-MAP-NUMBER:1-32>

<備　　考>

- PQ を設定するには、global mode で作成した priority-map を指定します。
- 存在しない priority-map を指定すると、すべてのパケットを default class にマッピングする PQ が設定されます。該当する priority-map を作成したときに、当該 PQ が設定されます。
- どの class にも該当しないパケットは、default class にマッピングされます。

○ SFQ の設定

<書　　式> queue fair-queue

○ FIFO の設定

<書　　式> queue fifo (|limit <1-16384>)

<備　　考> limit で FIFO キューの長さを指定することが出来ます。

○ TBF(shaping)の設定

<書　　式>

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

<備　　考>

- <RATE:1-1000000> Shaping レート(Kbps)を指定します。
- <BUFFER:1-1000000> Bucket のサイズ(bytes)を指定します。
- <LIMIT:1-1000000> Token が利用可能になるまでにバッファすることが出来るキューの長さ(bytes)を指定します。
- ifg-pa-fcs(後述)を指定することが出来ます。Default は無効です。

○ no queue

<書　　式> no queue

<備　　考> 上記で設定した queue を削除して、default queue(pfifo_fast)に設定します。

○ classify

<書　　式> classify (input|output) route-map ROUTEMAP

<備　　考>

・ インタフェースにルートマップを適用します。1 つのインタフェースに、input と output を別々に設定することが出来ます。
・ input で指定したルートマップは、PRE-ROUTING(付録の Packet Traveling を参照)で適用されます。
・ output で指定したルートマップは、POST-ROUTING(付録の Packet Traveling を参照)で適用されます。

○ no classify

<書　　式> no classify (|input|output)

<備　　考>

・ インタフェースに適用したルートマップを削除します。
・ 「no classify」を実行すると、両方(input と output)を削除します。片方だけを削除する場合は、input または output を指定します。

● ifg-pa-fcs

契約した回線帯域により料金が異なるようなキャリアサービスを利用する場合、ルータでの shaping 時に、FCS や IFG や PA を除いたフレームサイズで rate 計算を行います。この場合、shaping rate としては問題ないようでも、Ethernet フレームとして実際に回線を流れる際は、FCS や IFG や PA が追加されるため、回線側でフレームドロップが発生することがあります。このような場合の対応として、Ethernet インタフェース上での設定に限り、shaping rate の計算時に、IFG(inter-frame-gap の最小サイズ 12 バイトで計算)、FCS(4 バイト)、PA(preamble:8 バイト)をフレームサイズに加えることができます。これにより、回線サービス上での帯域超過によるフレームドロップを回避することが可能となります。Default では、この機能は無効です(IFG、PA、FCS 分のサイズを考慮しません)。

**◆(ip|ipv6) rebound**

<説　　明>

・ 下位ルータから受信したパケットを、受信インタフェースと同一インタフェースから出力(forwarding)した場合、下位ルータから NXR に対して再度パケットが送信されてくるため、下位ルータと NXR の間で TTL が「0」になるまでパケットがループします。
・ IP rebound 機能を無効にすると、受信インタフェースと送信インタフェースが同一の場合、パケットをドロップし、かつ送信元に destination unreachable を送信します。
・ Default は、有効です(受信インタフェースと送信インタフェースが同一でもドロップしません)。

<書　　式> (ip|ipv6) rebound
<初 期 値> (ip|ipv6) rebound
<　no　　> no (ip|ipv6) rebound

**◆ ip reassemble-output**

<説　　明>

・ インタフェースの MTU(あるいは PMTU)より大きいパケットを IP forwarding する際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。本設定有効時、NXR がリアセンブルしたパケットは、以下のようにフラグメント処理を行います。
  - fragmented packet(パケットの断片)が MTU を超える場合、リアセンブルしたパケットを再度 MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、リアセンブルしたパケットを出力します。

<書　　式> ip reassemble-output
<初 期 値> ip reassemble-output
<　no　　> no ip reassemble-output

<備　　考>

・ 上記の場合(本設定が有効の場合)、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易な IP 実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズで NXR からパケットを出力します。また、出力時の IP フラグメント処理は、次のようになります。
  - fragmented packet(パケットの断片)が MTU を超える場合、受信した fragmented packet を MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、受信した fragmented packet をそのままのサイズで出力します。
・ Default は、global 設定および interface 設定ともに有効です。Global 設定と interface 設定の AND 条件により、本機能が有効か無効かを判定します。本設定は、IP forwarding するパケットにのみ影響します。
・ 受信時のサイズを記載しておくバッファが 32 個しかないため、33 個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-output が有効な場合と同様に処理します。

◆ **session invalid-status-drop-interface**

<説　　明>
- session invalid-status-drop 機能(global mode 参照)をインタフェース毎に指定することができます。
- 本機能は、default で無効です。

<書　　式> session invalid-status-drop-interface enable
<初 期 値> no session invalid-status-drop-interface enable
<　no　　> no session invalid-status-drop-interface enable
<備　　考>
- あるインタフェースに対してのみ適用したい場合は、global mode で session invalid-status-drop 機能を無効にして、かつ本機能を指定インタフェースで有効にします。以下は、ethernet 0 インタフェースに適用する場合の設定例です。
  - global mode で、session invalid-status-drop を無効にします。
    nxrg240(config)#no session invalid-status-drop enable
  - 指定インタフェースで、本機能を有効にします。
    nxrg240(config)#interface ethernet 0
    nxrg240(config-if)#session invalid-status-drop-interface enable

◆ **ip dhcp mode ngn**

<説　　明> NGN 回線でデータコネクトを使用する場合に設定します。
<書　　式> ip dhcp mode ngn
<　no　　> no ip dhcp mode
<備　　考> no を設定すると、ip dhcp request classless-static-route も無効になります。

◆ **ip dhcp request classless-static-route**

<説　　明> NGN 回線でのデータコネクトとインターネット接続(PPP)を併用する場合に設定します。
<書　　式> ip dhcp request classless-static-route
<　no　　> no ip dhcp request classless-static-route
<備　　考>
- データコネクトと PPP によるインターネット通信を併用する場合、DHCPv4 の classless-static-route オプション(RFC3442)を使って、NGN 網への static route 情報を取得することにより、データコネクトの通信を NGN 網へルーティングさせることが出来ます。
- 取得した static route は、アドレスのリース期間中有効です。

◆ **ip dhcp initial-interval**

<説　　明> サーバへの最初のアクセス試行から、次のアクセス試行までの時間を設定します。
<書　　式> ip dhcp initial-interval <1-60>
<　no　　> no ip dhcp initial-interval (= default)
<初 期 値> ip dhcp initial-interval 3

### ◆ ip dhcp retry

<説　　明>
・ クライアントが、DHCP サーバが存在しないという判断をしてから、再び DHCP サーバにアクセスを試行するまでの時間を設定します。
<書　　式> ip dhcp retry <1-3600>
<　no　　> no ip dhcp retry　　（= default）
<初 期 値> ip dhcp initial-interval 300

### ◆ ip dhcp timeout

<説　　明>
・ クライアントがアドレス要求を開始してから、サーバにアクセスすることが出来ないと判断するまでの時間を設定します。
<書　　式> ip dhcp timeout <10-3600>
<　no　　> no ip dhcp timeout　　（= default）
<初 期 値> ip dhcp timeout 60

### ◆ ip dhcp backoff-cutoff

<説　　明>
・ 多数のクライアントが同時に設定しようとした場合に、リクエストがロックしてしまうことがないように、一時退避できる最大時間を決定します。
<書　　式> ip dhcp backoff-cutoff <2-60>
<　no　　> no ip dhcp backoff-cutoff　　（= default）
<初 期 値> ip dhcp backoff-cutoff 15

### ◆ ip p2p-detection

<説　　明> P2P 検出機能を有効にします(IPv4 のみ対応)。
<書　　式> ip p2p-detection (any|winny|share|bittorrent) {log|deny}
<　no　　> no ip p2p-detection
　　no ip p2p-detection (winny|share|bittorrent)
<備　　考>
・ インターネットに接続しているインタフェース上でのみ有効にすることを推奨します。
・ 詳細については、「付録 L:P2P 検出機能」を参照してください。

◆ **ip arp filter**

<説　　明>
- 異なるインタフェースに割り当てられているアドレスに対する ARP request を受信した際に、ARPreply を返す / 返さない機能です。

<書　　式> ip arp filter
<初 期 値> ip arp filter　　(有効:ARP reply を返さない)
<　no　　> no ip arp filter (無効:ARP reply を返す)
<備　　考>
- ある LAN セグメントに複数の Ethernet インタフェースが接続されている場合は、複数のインタフェースから ARP reply を返さないように、本機能を有効にします。
- 一方で、ある LAN 上の端末に対する host route が、別インタフェースになっている場合に、当該 host からの ARP request に対して、ARP reply を返す場合は、本機能を無効にします。
- ARP reply の送信先は、ルート情報によって決まります。

◆ **ip arp gratuitous**

<説　　明> gratuitous ARP(GARP)を送信する機能です。
<書　　式> ip arp gratuitous <attempts:1-255> <interval:1-3600> <delay:1-600>
　　ip arp gratuitous (= ip arp gratuitous <attempts:1> <interval:1> <delay:5>)
<初 期 値> no ip arp gratuitous (無効:GARP を送信しない)
<　no　　> no ip arp gratuitous
<備　　考>
- アドレスの重複を避けたり、ARP テーブルを更新するために、本装置では、下記のタイミングに、GARP (request)を送信します。
- IP アドレスを追加した場合:追加したアドレスの GARP を送信します。
- リンクアップした場合:当該インタフェースの全アドレスの GARP を送信します。
- VRRP マスターに遷移した場合:VIP に対する GARP を送信します。
- GARP 送信機能は、default 無効です。設定により有効にする場合、送信回数、送信間隔(sec)、初期試行までの delay(sec)も同時に指定することが出来ます。
- 設定可能なインタフェースは、Ethernet、VLAN、Bridge です。
- 多数の VLAN や Bridge 上で有効にすると、リンクアップ時に大量の GARP を送信するケースがあるため、本機能を有効にする場合は、注意してください。
- DHCP クライアント機能使用時、DHCP によって IP アドレスを取得したタイミングでは、GARP 送信は行いません。しかし、既に IP アドレスを取得した状態で、リンクアップした場合は、GARP を送信します。

### ◆ bridge-group

<説　　明> インタフェースを bridge-group(仮想スイッチグループ)に参加させます。
<書　　式> bridge-group <0-4095>
　　bridge-group <0-4095> pathcost <0-65535>
　　bridge-group <0-4095> port <1-128>
　　bridge-group <0-4095> priority <0-255>
< no > no bridge-group (|<0-4095>)
　　no bridge-group <0-4095> (pathcost|priority)
<備　　考> bridge-group が未設定(interface bridge が未設定)の場合、join に失敗します。

### ◆ l2tpv3 access-group

<説　　明> Xconnect インタフェースでの送受信に対して、l2tpv3 access-list を適用します。
<書　　式> l2tpv3 access-group (in|out) WORD
< no > no l2tpv3 access-group (in|out)
<備　　考>
・ WORD: root の ACL 名を指定します。
　　(root の ACL 名は、global ノードの l2tpv3 access-list WORD root にて設定します。)
・ in: Xconnect インタフェース→セッション(本装置への入力)方向のフィルタを適用します。
・ out: セッション→ Xconnect インタフェース(本装置からの出力)方向のフィルタを適用します。

### ■ l2tpv3 l2rp

<説　　明> L2TPv3 L2RP(冗長化構成)の設定をします。

○ enable
<説　　明> L2RP を有効にします。
<書　　式> l2tpv3 l2rp <1-255> enable
< no > no l2tpv3 l2rp <1-255> enable

○ type
<説　　明> Master を選択する方法を指定します。
　　Default では、priority の比較によって判定します。
<書　　式> l2tpv3 l2rp <1-255> type (priority|active)
< no > no l2tpv3 l2rp <1-255> type
<初 期 値> l2tpv3 l2rp <1-255> type priority
<備　　考> priority を選択した場合、priority 値の大きい方が、master になります。
　　active を選択した場合、active session 数の多い方が、master になります。

○ priority
<説　　明> Master の選定に使用する priority 値を設定します。
<書　　式> l2tpv3 l2rp <1-255> priority <1-255>
< no > no l2tpv3 l2rp <1-255> priority
<初 期 値> l2tpv3 l2rp <1-255> priority 100

○ preempt
<説　　明> Priority 値の小さいものが master で、大きいものが backup となることを許可するかどうかの設定です。
<書　　式> l2tpv3 l2rp <1-255> preempt
<　no　　> no l2tpv3 l2rp <1-255> preempt
<初 期 値> l2tpv3 l2rp <1-255> preempt
<備　　考>
・ preempt 有効時、Master 選択の判定基準(type で指定した判定方法)に従います。
・ preempt 無効時、priority(または session 数)の大きい LCCE が現れた場合に、backup へと遷移しません。

○ fdb-reset
<書　　式> l2rp <1-255> fdb-reset
<備　　考> スイッチハブ実装の Ethernet ポートのみ有効です。

○ block-reset
<説　　明> 自身のポートのリンク状態を一時的に down させ、配下のスイッチの MAC テーブルをフラッシュします。
<書　　式> l2tpv3 l2rp <1-255> block-reset
<　no　　> no l2tpv3 l2rp <1-255> block-reset
<備　　考>
・ Group blocking 状態に遷移した場合のみ動作します。
・ Group blocking とは、自身で送信した Advertise Frame を受信した場合や、対向 LCCE の Advertise Frame を受信した場合に、Loop が発生していると判断して、Frame の転送を停止している状態です。

○ timers advertise
<説　　明> L2RP Advertise Frame を送信する間隔を指定します。
<書　　式> l2tpv3 l2rp <1-255> timers advertise <1-60>
<　no　　> no l2tpv3 l2rp <1-255> timers advertise
<初 期 値> l2tpv3 l2rp <1-255> timers advertise 1

○ timers delay
<説　　明> L2TP session 確立後、timers delay で指定した時間、Group Blocking 状態となり、Frame の転送を行いません。
<書　　式> l2tpv3 l2rp <l2rpid:1-255> timers delay <0-60>
<　no　　> no l2tpv3 l2rp <1-255> timers delay
<初 期 値> l2tpv3 l2rp <l2rpid:1-255> timers delay 0
<備　　考>
・ L2RP は、主に Loop が発生する環境で使用されます。そのような環境では、L2RP Frame を受信するまで(Loop を検出するまで)の間、Blocking 機能が動作しないので、一時的に Broadcast Storm が発生します。timers delay を設定することで、Broadcast Storm を回避することが出来ます。
・ timers advertise より、長い時間を設定することを推奨します。

○ port-reset
<説　　明>
・ L2TP Group 機能や L2RP 機能により、L2TP session の切替が発生した際、配下スイッチの FDB において、MAC アドレスのエントリーが更新されていないため、最大 5 分間通信できないことがあります。
・ port reset 機能を有効にした場合、master → backup(または、master → init)へ遷移した際に、L2RP インタフェースのリンクを一時的に down させることで、配下スイッチの FDB を flush させます。
<書　　式> l2tpv3 l2rp <l2rpid:1-255> port-reset
<　no　　> no l2tpv3 l2rp <1-255> port-reset
<初 期 値> no l2tpv3 l2rp <1-255> port-reset

◆ **ip dns-intercept**

<説　　明> 当該インタフェースで使用する dns-intercept を指定します。
　　ignore-auto-dns を指定すると、DHCP/IPCP で取得した DNS を使用しません。
<書　　式> ip dns-intercept <0-3> （|ignore-auto-dns）
< no > no ip dns-intercept
<備　　考> DNS インターセプトの設定は、dns-intercept mode で行います。

◆ **event-notify**

<説　　明> インタフェースの link up/down 時に、イベント通知を行います。
<書　　式> event-notify <0-3>
< no > no event-notify
<備　　考> イベント通知の方法(LINE、メール)は、ENS mode で設定します。

◆ **ip multicast-to-unicast**

<説　　明> 有効時、multicast を unicast 変換したパケットを転送します。
<書　　式> ip multicast-to-unicast forwarding （有効）
< no > no ip multicast-to-unicast forwarding（無効）

◆ **cms watch enable**

<説　　明> インタフェースの up/down 時に、インタフェースの監視情報を CMS に送信します。
<書　　式> cms watch enable
< no > no cms watch enable

◆ **poe power-supply enable**

<説　　明> PoE 給電を有効にします。
<書　　式> poe power-supply enable
< no > no poe power-supply enable
<備　　考> 対応機種は、NXR-G060 です。

◆ **poe netevent**

<説　　明> Track の up/down を検出すると、PoE 給電を有効 / 無効にします。
<書　　式> poe netevent <1-255>|<2048-4095> (enable|disable)
　　poe netevent <1-255>|<2048-4095> (enable|disable) timer <1-60>
< no > no poe netevent
<備　　考> 対応機種は、NXR-G060 です。

以下に設定例を示します。

poe netevent 1 enable (timer 60)
　Track 1 の down で、PoE 給電を有効にします。(60 秒後に PoE 給電を無効にします。)
　Track 1 の up で、PoE 給電を無効にします。

poe netevent 1 disable (timer 60)
　Track 1 の down で、PoE 給電を無効にします。(60 秒後に PoE 給電を有効にします。)
　Track 1 の up で、PoE 給電を有効にします。

◆ **ipv6 router rip**
<説　　明> 当該インターフェースで RIPng を有効にします。
　　RIPng パケットの送受信を行い、当該インターフェースのネットワークを広告します。
<書　　式> ipv6 router rip
<　no　> no ipv6 router rip
<備　　考> RIPng の設定は、RIPng mode で設定します。

◆ **ipv6 rip split-horizon**
<説　　明> スプリットホライズンを設定します。
<書　　式> ipv6 rip split-horizon (|poisoned)
<初 期 値> ipv6 rip split-horizon poisoned
<　no　> no ipv6 rip split-horizon
<備　　考>
✓　poisoned を指定しない場合、当該インターフェースから学習した経路を同じインターフェースへ広告しません。
✓　poisoned を指定した場合、当該経路をメトリック 16(到達不能)として広告します(ポイズンリバース)。

◆ **ipv6 router ospf area**
<説　　明> 当該インターフェースで OSPFv3 を有効にし、指定したエリアに所属させます。
　　エリア ID は A.B.C.D 形式、または 10 進数で指定します。
<書　　式> ipv6 router ospf area (A.B.C.D|<0-4294967295>)
<　no　> no ipv6 router ospf area (A.B.C.D|<0-4294967295>)
<備　　考> OSPFv3 の設定は、OSPFv3 mode で設定します。

◆ **ipv6 ospf cost**
<説　　明> 当該インターフェースの OSPFv3 コスト値を設定します。
　　コスト値は最短経路の計算に使用され、値が小さいほど優先されます。
<書　　式> ipv6 ospf cost <1-65535>
<初 期 値> ipv6 ospf cost 10
<　no　> no ipv6 ospf cost

◆ **ipv6 ospf hello-interval**
<説　　明> Hello パケットの送信間隔(秒)を設定します。
　　隣接ルータと同じ値を設定する必要があります。
<書　　式> ipv6 ospf hello-interval <1-65535>
<初 期 値> ipv6 ospf hello-interval 10
<　no　> no ipv6 ospf hello-interval

◆ **ipv6 ospf dead-interval**
<説　　明> ネイバーダウンと判定するまでの時間(秒)を設定します。
　　この時間内に Hello パケットを受信しない場合、ネイバーをダウンとみなします。
　　隣接ルータと同じ値を設定する必要があります。
<書　　式> ipv6 ospf dead-interval <1-65535>
<初 期 値> ipv6 ospf dead-interval 40
<　no　> no ipv6 ospf dead-interval

◆ **ipv6 ospf retransmit-interval**
<説　　明> LSA の再送間隔(秒)を設定します。
　　送信した LSA に対する確認応答を受信できない場合、この間隔で再送します。
<書　　式> ipv6 ospf retransmit-interval <1-65535>
<初 期 値> ipv6 ospf retransmit-interval 5
<　no　> no ipv6 ospf retransmit-interval

◆ **ipv6 ospf transmit-delay**

<説　　明> LSA の送信遅延時間(秒)を設定します。
　　送信する LSA の経過時間(LS age)にこの値を加算します。
<書　　式> ipv6 ospf transmit-delay <1-65535>
<初 期 値> ipv6 ospf transmit-delay 1
<　no　> no ipv6 ospf transmit-delay

◆ **ipv6 ospf priority**

<説　　明> DR/BDR 選出時のプライオリティを設定します。
　　値が大きいほど DR に選出されやすくなります。
　　0 を設定した場合、DR/BDR の選出対象外となります。
<書　　式> ipv6 ospf priority <0-255>
<初 期 値> ipv6 ospf priority 1
<　no　> no ipv6 ospf priority

# 第 7 章　interface tunnel mode

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**interface tunnel <0-255>**
nxrg240(config-tunnel)#

**◆ description**

<説　　明> インタフェースの説明を記述します。
<書　　式> description DESCRIPTION
<　no　> no description (|DESCRIPTION)

**◆ ip address**

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

**◆ ipv6 address**

<説　　明> インタフェースに IPv6 アドレスを付与します。
<書　　式> ipv6 address X:X::X:X/M (|eui-64) : IPv6 address (e.g. 3ffe:506::1/48)
　　ipv6 address X:X::X:X link-local
<　no　> no ipv6 address X:X::X:X/M (|eui-64)
　　no ipv6 address X:X::X:X link-local

**◆ ipv6 address DHCPv6-PD**

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

- ipv6-address は、sub-prefix と host 部を指定することが出来ます。
- DHCPv6-PD は、DHCPv6 PD で受信する prefix 部のプロファイル名です。DHCPv6-PD は、DHCPv6 パケットを受信するインタフェース(異なるインタフェース)上で、ipv6 dhcp client pd コマンドを使用して設定します。

**◆ tunnel source**

<説　　明> トンネルの source アドレス、またはインタフェースを設定します。
<書　　式> tunnel source A.B.C.D|X:X::X:X
　　tunnel source INTERFACE
<備　　考> INTERFACE には、ethernet, bridge, ppp インタフェースを指定することが出来ます。

### ◆ tunnel destination

<説　　明> トンネルの Destination アドレス、または FQDN を設定します。
<書　　式> tunnel destination A.B.C.D|X:X::X:X
　　tunnel destination FQDN

### ■ tunnel mode

<説　　明>
・ トンネリング機能として、GRE IP-in-IP、IPsec(over IPv4/IPv6)、6rd の 5 つのモードをサポートしています。
<初 期 値> tunnel mode gre
<　no　> no tunnel mode (= tunnel mode gre)

○ IPinIP
<説　　明>
・ IP パケット(IPv4/IPv6 パケット)を IP(IPv4/IPv6)でトンネリングするプロトコルです。
<書　　式> tunnel mode ipip|ipipv6|ipv6ip|ipv6ipv6
<備　　考> ipip　　IPv4 over IPv4 tunneling
　　ipipv6　　IPv4 over IPv6 tunneling
　　ipv6ip　　IPv6 over IPv4 tunneling
　　ipv6ipv6　　IPv6 over IPv6 tunneling

○ GRE(Generic Routing Encapsulation)
<説　　明>
・ IPv4 および IPv6 パケットをトンネリングすることが出来ます。Transport 用の IP は、IPv4 のみ対応しています。
・ RFC2784 に準拠しています。
・ プロトコル番号は、47 です。
・ オプション機能として、ID キー、チェックサムの 2 つをサポートしています。シーケンスチェックについては、対応していません。
<書　　式> tunnel mode gre

○ IPsec over IPv4
○ IPsec over IPv6
<説　　明>
・ Route based IPsec(参照:付録 B)を使用する際は、ipsec ipv4 または ipsec ipv6 を指定します。
<書　　式> tunnel mode ipsec ipv4　　(= IPsec over IPv4)
　　tunnel mode ipsec ipv6　　(= IPsec over IPv6)

○ 6rd(IPv6 Rapid Deployment on IPv4 infractructures)

<説　　明>

・ IPv6 パケットを IPv4 でトンネリングするためのプロトコルです。
・ RFC5569/5969 に準拠しています。
・ IPv6 over IPv4 トンネリング上では、IPv4 は無効です。

<書　　式> tunnel mode ipv6ip 6rd

<備　　考>

・ 6rd を使用する場合は、tunnel 6rd prefix、tunnel 6rd ipv4 prefix-length の設定も確認してください。

**◆ tunnel key**

<説　　明> 送信時、GRE ヘッダに識別子として ID を設定します。GRE の場合のみ有効です。
<書　　式> tunnel key <0-4294967295>
<初 期 値> no tunnel key
<　no　> no tunnel key
<備　　考>

・ 受信パケットに key ID がなくても drop しません。しかし、key ID が存在していて ID が一致しない場合は、当該パケットを drop します。

**◆ tunnel checksum**

<説　　明>

・ GRE パケット(GRE ヘッダを含む)のチェックサムを計算し、チェックサムフィールドにチェックサム値を設定します。GRE の場合のみ有効です。

<書　　式> tunnel checksum
<初 期 値> no tunnel checksum
<　no　> no tunnel checksum

**◆ tunnel encap-limit**

<説　　明> 1 つのパケットで許可される入れ子のトンネリングのレベル数を指定します。
<書　　式> tunnel encap-limit <0-255>
<初 期 値> tunnel encap-limit 4
<　no　> no tunnel encap-limit（=無効）
<備　　考> 本設定は、ipv6 トンネルにのみ適用されます。

◆ **tunnel path-mtu-discovery**

<説　　明> トンネルインタフェース上で PMTUD を有効にします。
<書　　式> tunnel path-mtu-discovery
<初 期 値> tunnel path-mtu-discovery　　(有効)
<　no　　> no tunnel path-mtu-discovery　　(無効)
<備　　考>
< IPv4 >
・ IPv4 パケットをトンネリングする際の PMTU Discovery の動作について記します。
  - 以下は、IP tunnel(tunnel mode ipip|gre)で、fragment が必要な場合の PMTUD の動作です。IPsec tunnel(tunnel mode ipsec ipv4)での PMTUD については、付録 B を参照してください。
  - -PMTUD の設定(有効 / 無効)とトンネリングするパケットの DF ビットの値(0/1)によって、本装置の処理が異なります。

| PMTUD 設定 | DF bit | 本装置の処理 |
|---|---|---|
| 有効 | 0 | fragment して送信する。<br>outer IP header の DF ビットは、1 を設定する。 |
| | 1 | fragment needed を送信元に返し、パケットを drop する。 |
| 無効 | 0 | fragment して送信する。<br>outer IP header の DF ビットは、0 を設定する。 |
| | 1 | 強制 fragment して送信する(※)。<br>outer IP header の DF ビットは、0 を設定する。 |

※ tunnel MTU を超えるパケットは、フォワーディング処理の際に PMTUD が作動するため、強制フラグメントを行いません。しかし、トンネルインタフェースへの出力後に、header tax 分を加えたパケットの大きさが、tunnel の宛先への PMTUD を超えている場合は、強制 fragment して送信します。
フォワーディング時に PMTUD の作動を回避するには、tunnel の MTU を 1500 に設定します。

< IPv6 >
・ IPv6 の場合、PMTU は default で有効です(無効にすることはできません)。
・ MTU とは、PMTU からトンネルヘッダを引いたもの、または MTU 設定値のいずれかの小さい方の値です。
・ 本装置でトンネリングを行う際に、tunnel header tax によって転送可能な最大パケットサイズが、
・ IPv6 の最小 MTU(1280 バイト)を下回ることも考えられます。このような場合の動作を以下に示します(1280 より小さい値を送信元に返しても、送信元ホストは 1280 より小さいパケットに分割して送信することが出来ないため、通信を行うことが出来ません)。

**IPv6 over IPv6 tunneling**(RFC2473 参照)
・ Tunnel MTU が IPv6 最小 MTU(1280)より大きい場合
  パケットを破棄して、送信元ホストへ、ICMPv6 packet too big メッセージを返信します。
・ Tunnel MTU が IPv6 最小 MTU(1280)より小さい場合(または同じ場合)
  パケットを強制的に fragment して送信します。

**IPv6 over IPv4 tunneling**(RFC2893 参照)
・ Tunnel MTU が IPv6 最小 MTU(1280)より大きい場合
  パケットを破棄して、送信元ホストへ、ICMPv6 packet too big メッセージを返信します。
・ Tunnel MTU が IPv6 最小 MTU(1280)より小さい場合(または同じ場合)
  トンネリングパケットが IPv6 最小 MTU より大きい場合、パケットを破棄し、送信元ホストへ IPv6packet too big メッセージを返信します。
  トンネリングパケットが IPv6 最小 MTU より小さい場合、トンネルヘッダの DF ビットを 0 に設定した上で、fragment して送信します。

◆ **tunnel ttl**

<説　　明> TTL を設定します。
<書　　式> tunnel ttl (<1-255>|inherit)
<初 期 値> tunnel ttl inherit
<　no　> no tunnel ttl　　(= tunnel ttl inherit)
<備　　考>
- 固定の値(1-255)を設定する場合は、PMTUD (tunnel path-mtu-discovery)を有効にします。
- inherit を設定した場合、GRE/IPIP(tunnel mode gre|ipip)では TTL をコピーします。IPsec tunnel (tunnel mode ipsec ipv4)での TTL 設定については、付録 B を参照してください。

◆ **tunnel tos**

<説　　明> Tunnel IPv4(outer)ヘッダの ToS フィールドに設定する値を指定します。
<書　　式> tunnel tos (<0-252>|inherit)
<初 期 値> tunnel tos inherit
<　no　> no tunnel tos　　(= tunnel tos inherit)
<備　　考>
- inherit を指定した場合、IPv4(innner)ヘッダの ToS 値、または tunneling IPv6(inner)ヘッダの traffic-class 値を tunnel IPv4(outer)ヘッダにコピーします。
- ToS 値を指定する場合、0-252 の範囲で指定することが出来ます。
- ECN フィールドの設定は出来ません。ECN field の扱いについては、「付録 B 1.2.4.1 ECN field の扱い」を参照してください。

※ GRE トンネル上で、IPv6 パケットをトンネリングする場合は、inherit を無視し、ToS 値として 0x0 を設定します。

◆ **tunnel pre-fragment**

<説　　明> Fragment 処理が必要な場合、先に fragment してから ESP 化します。
(複数の ESP packet に分割されます)。
<書　　式> tunnel pre-fragment
<初 期 値> no tunnel pre-fragment
<　no　> no tunnel pre-fragment
<備　　考> Route based IPsec(参照:付録 B)を使用する際に、IPsec tunnel interface に設定することが出来ます。

◆ **tunnel protection ipsec policy**

<説　　明> 使用する IPsec tunnel policy を指定します。
<書　　式> tunnel protection ipsec policy <1-65535>
<　no　> no tunnel protection
<備　　考> Route based IPsec(参照:付録 B)を使用する際に設定します。

◆ **bandwidth**

<説　　明> インタフェースの帯域幅を設定することが出来ます。
bandwidth の初期値は、10Mbps です。
bandwidth の最大値は、10Gbps です。
<書　　式> bandwidth <1-10000000000[k/m/g]>
< no > no bandwidth
<備　　考> 本機能は、OSPF のコスト計算時のみに使用します。
基準となる帯域幅は、auto-cost コマンド（ospf mode）にて設定します。

◆ **mtu**

<説　　明> トンネルインタフェースの MTU 値を設定します。
<書　　式> mtu <bytes:68-1500>
<初 期 値> mtu 1476 (tunnel mode gre の場合)
mtu 1480 (tunnel mode ipip の場合)
mtu 1500 (tunnel mode ipsec の場合)
< no > no mtu (= Set defaults)

◆ **ip redirects**

<説　　明>
・ ICMP redirect(type=5)とは、同一ネットワーク上に他の最適なルートがあることを通知するためのメッセージです(RFC792)。
・ 本装置の Send redirect 機能によって、ICMP redirect の送信の有無を切り替えることが出来ます。
<書　　式> ip redirects
<初 期 値> ip redirects　　(有効)
< no > no ip redirects　　(無効)
<備　　考>
・ ICMPRedirect の例は、interface mode の ip redirects を参照して下さい。

◆ **ip tcp adjust-mss**

<説　　明>

・ Path MTU Discovery(PMTUD)機能(End-to-end でフラグメントが発生しない最大の MTU を発見すること)によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器(ルータ等)が ICMP fragment needed をフィルタリングしている場合(ブラックホールルータが存在する場合)や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、Endto-end での通信に支障をきたすことになります。このような場合、TCP では SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

<書　　式> ip tcp adjust-mss (auto|<500-1460:bytes>)

<初 期 値> no ip tcp adjust-mss

<　no　> no ip tcp adjust-mss

<備　　考>

・ IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。

・ 本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ ユーザが設定する場合は、MSS 値を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。

・ 「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

◆ **ipv6 tcp adjust-mss**

<説　　明> TCP/IPv6 の MSS 値を設定します。

<書　　式> ipv6 tcp adjust-mss (auto|<bytes:500-1440>)

<初 期 値> no ipv6 tcp adjust-mss

<　no　> no ipv6 tcp adjust-mss

◆ **ip mask-reply**

<説　　明>

・ OpenView などの監視装置では、監視ネットワーク内の機器に対して ICMP address mask request (type=17)を送信することによって機器のインタフェースのネットマスク値を取得します(単純に、死活監視で使用する場合もあります)。

・ 本装置では、ICMP address mask request への応答の有無を設定することが出来ます。

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

<初 期 値> no ip mask-reply(ICMP address mask request に応答しません。)

<　no　> no ip mask-reply

<備　　考>

・ ICMP address mask request/reply の例は、interface mode の ip mask-reply を参照して下さい。

◆ **ip 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>
・ global mode で設定した ACL をインタフェースに適用することで、パケットフィルタリングを行うことができます。
<書　　式> ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
<　no　　> no ip access-group (in|out|forward-in|forward-out)
<備　　考>
・ 各インタフェースへのパケットフィルタリングの適用箇所(付録の Packet Traveling を参照)は、以下の 4 ヶ所です。
  - in(local input) NXR 自身で受信して処理するパケットを制限します。
  - out(local output) NXR 自身が作成して出力するパケットを制限します。トンネリングされたパケットも NXR 自身が作成したパケットとして認識します。
  - forward-in NXR が当該インタフェースで受信して forwarding するパケットを制限します。
  - forward-out NXR が受信して当該インタフェースへ forwarding するパケットを制限します。
・ mac 指定のある ACL は、out および forward-out に設定することは出来ません。

◆ **ipv6 access-group**

<説　　明> アドレスグループに IPv6 アクセスリストを追加します。
<書　　式> ipv6 access-group (in|out|forward-in|forward-out) IP64-ACL-NAME
<　no　　> no ipv6 access-group (in|out|forward-in|forward-out)

◆ **ip masquerade**

<説　　明> インタフェースよりパケットを出力する際に、パケットの送信元 IPv4 アドレスを出力インタフェースの IPv4 アドレスに自動変換する機能です。
<書　　式> ip masquerade　　(有効)
<初 期 値> no ip masquerade　　(無効)
<　no　　> no ip masquerade
<備　　考>
- すべてのインタフェース(Ethernet/VLAN/PPP/Tunnel)で設定することが出来ます。
- TCP/UDP/ICMP のみ対応しています。その他のプロトコルに関しては、動作は保証しません。
- IPv6 パケットは、IP マスカレードの対象外です。
- forward out/local output フィルタリング適用後のパケットに、IP マスカレードを適用します。

◆ **ip (snat-group|dnat-group)**

<説　　明>
- global mode で設定した SNAT または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。
- SNAT は、パケットの出力時に適用されます。DNAT は、パケットの入力時に適用されます。

<書　　式> ip (snat-group|dnat-group) NAT-NAME
<　no　　> no ip (snat-group|dnat-group)
<備　　考> NAT ルールの設定は、ip snat/ip dnat)コマンド(global mode)で行います。

◆ **ip webauth-filter**
◆ **ipv6 webauth-filter**

<説　　明>
- Web 認証フィルタをインタフェースに適用すると、ある特定のホスト、ネットワークやインタフェースについて、Web 認証せずに通信することが可能となります。
- Web 認証フィルタは、各インタフェースにつき、IN/OUT をそれぞれ一つずつ設定することができます。Default の設定はありません。

<書　　式> ip webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
　　ipv6 webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
<　no　　> no ip webauth-filter (forward-in|forward-out)
　　no ipv6 webauth-filter (forward-in|forward-out)
<備　　考>
- Web 認証フィルタの設定については、ip web-auth access-list/ipv6 web-auth access-list コマンド(global mode)を参照してください。
- Web 認証については、Web Authenticate mode を参照してください。

◆ **ip spi-filter**

<説　　明>
- 簡易ファイヤウォールの一つとして、SPI(Stateful Packet Inspection)機能をサポートします。
- パケットに関連するコネクションの状態を見て、当該パケットをドロップするかしないかを決める機能です。

<書　　式> ip spi-filter　　(有効)
<初 期 値> no ip spi-filter　　(無効)
<　no　　> no ip spi-filter
<備　　考>
- コネクションの状態が、established または related の場合に、パケットの転送を許可します。
- Established とは、すでに双方向でパケットの通信がありコネクションが確立されている状態です。
- Related とは、すでに確立しているコネクションがある状態です。FTP のデータ転送等がこれに該当します。
- 新しい接続でありながら、syn ビットの立っていないパケットはドロップします。
- SPI は、forward in および local input の位置で適用されます。ユーザが適用位置を変更することは出来ません。

◆ **ipv6 spi-filter**

<説　　明> IPv6 SPI filter を設定します。
<書　　式> ipv6 spi-filter
<初 期 値> no ipv6 spi-filter
<　no　　> no ipv6 spi-filter

◆ **ip spi-filter log**
◆ **ipv6 spi-filter log**

<説　　明> フィルタログ機能(syslog mode 参照)を有効にします。
　　パケットが、SPI フィルタにマッチした場合、syslog に出力することが出来ます。
<書　　式> ip spi-filter log [limit <0-100>]
　　ipv6 spi-filter log [limit <0-100>]
<初 期 値> ip spi-filter log limit 10
　　ipv6 spi-filter log limit 10
<　no　　> no ip spi-filter
　　no ipv6 spi-filter
<備　　考>
- limit を指定すると、1 秒当たりのログ出力数を制限します。初期値は、10 パケット / 秒です。
- WAN 側からの意図しないパケットが、SPI フィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分に注意してください。

◆ **netevent**

<説　　明>
- トラックイベントの発生時に、当該 tunnel を接続／切断／再接続することが出来ます。

<書　　式> netevent <trackid:1-255> (connect|disconnect|reconnect)
　　netevent <trackid:2048-4095> (connect|disconnect|reconnect)
<　no　　> no netevent

◆ **ipv6 nd accept-redirects**

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

◆ **ipsec policy**

<説　　明> 当該インタフェースで使用する IPsec ローカルポリシーを設定します。
<書　　式> ipsec policy <local policy:1-255>
<　no　> no ipsec policy (|<local policy:1-255>)
<備　　考>

・ 各インタフェースに、IPsec ローカルポリシーを 4 つまで設定することが出来ます。他のインタ
・ フェースで既に設定している IPsec ローカルポリシーは、重複して設定できません。

◆ **ipsec policy-ignore**

<説　　明>

・ IPsec policy のチェックを行わないように指定する機能です。IPsec policy として any などを指定したけれども、特定の通信のみ IPsec 化したくない場合に、この機能を使用します。

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

・ Input を指定した場合、inbound policy check を実行しないため、IPsec 化されてくるべきパケットがドロップ されてしまう現象を回避することができます。
・ Output を指定した場合、当該インタフェースから出力されるパケットは、IPsec policy をチェックしないため平文で送信されます。

## ■ QoS

<説　　明> QoS の設定をします。

○ HTB の設定

<書　　式> queue policy POLICYNAME bandwidth <1-1000000>

<備　　考>

- HTB を設定するには、class policy コマンドで作成した class policy を指定します。
- 存在しない class policy を指定すると、親 class のみ設定されます。該当する class policy を作成したときに、当該 HTB が設定されます。
- bandwidth で、class policy の全帯域幅を指定します。

○ PQ の設定

<書　　式> queue priority-group <PRIORITY-MAP-NUMBER:1-32>

<備　　考>

- PQ を設定するには、global mode で作成した priority-map を指定します。
- 存在しない priority-map を指定すると、すべてのパケットを default class にマッピングする PQ が設定されます。該当する priority-map を作成したときに、当該 PQ が設定されます。
- どの class にも該当しないパケットは、default class にマッピングされます。

○ SFQ の設定

<書　　式> queue fair-queue

○ FIFO の設定

<書　　式> queue fifo (|limit <1-16384>)

<備　　考> limit で FIFO キューの長さを指定することが出来ます。

○ TBF(shaping)の設定

<書　　式>

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

<備　　考>

- <RATE:1-1000000>　　Shaping レート(Kbps)を指定します。
- <BUFFER:1-1000000>　　Bucket のサイズ(bytes)を指定します。
- <LIMIT:1-1000000>　　Token が利用可能になるまでにバッファすることが出来るキューの長さ(bytes)を指定します。

○ no queue

<書　　式> no queue

<備　　考> 上記で設定した queue を削除して、default queue(pfifo_fast)に設定します。

○ classify

<書　　式> classify (input|output) route-map ROUTEMAP

<備　　考>

・ インタフェースにルートマップを適用します。1 つのインタフェースに、input と output を別々に設定することが出来ます。
・ input で指定したルートマップは、PRE-ROUTING(付録の Packet Traveling を参照)で適用されます。
・ output で指定したルートマップは、POST-ROUTING(付録の Packet Traveling を参照)で適用されます。

○ no classify

<書　　式> no classify (|input|output)

<備　　考>

・ インタフェースに適用したルートマップを削除します。
・ 「no classify」を実行すると、両方(input と output)を削除します。片方だけを削除する場合は、input または output を指定します。

**◆(ip|ipv6) rebound**

<説　　明>

・ 下位ルータから受信したパケットを、受信インタフェースと同一インタフェースから出力(forwarding)した場合、下位ルータから NXR に対して再度パケットが送信されてくるため、下位ルータと NXR の間で TTL が「0」になるまでパケットがループします。
・ IP rebound 機能を無効にすると、受信インタフェースと送信インタフェースが同一の場合、パケットをドロップし、かつ送信元に destination unreachable を送信します。
・ Default は、有効です(受信インタフェースと送信インタフェースが同一でもドロップしません)。

<書　　式> (ip|ipv6) rebound
<初 期 値> (ip|ipv6) rebound
<　no　　> no (ip|ipv6) rebound

**◆ ip reassemble-output**

<説　　明>

・ インタフェースの MTU(あるいは PMTU)より大きいパケットを IP forwarding する際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。
本設定有効時、NXR がリアセンブルしたパケットは、以下のようにフラグメント処理を行います。
  - fragmented packet(パケットの断片)が MTU を超える場合、リアセンブルしたパケットを再度 MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、リアセンブルしたパケットを出力します。

<書　　式> ip reassemble-output
<初 期 値> ip reassemble-output
<　no　　> no ip reassemble-output

<備　　考>

・ 上記の場合(本設定が有効の場合)、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易な IP 実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズで NXR からパケットを出力します。また、出力時の IP フラグメント処理は、次のようになります。
  - fragmented packet(パケットの断片)が MTU を超える場合、受信した fragmented packet を MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、受信した fragmented packet をそのままのサイズで出力します。
・ Default は、global 設定および interface 設定ともに有効です。Global 設定と interface 設定の AND条件により、本機能が有効か無効かを判定します。本設定は、IP forwarding するパケットにのみ影響します。
・ 受信時のサイズを記載しておくバッファが 32 個しかないため、33 個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-output が有効な場合と同様に処理します。

### ◆ session invalid-status-drop-interface

<説　　明>
- session invalid-status-drop 機能(global mode 参照)をインタフェース毎に指定することができます。
- 本機能は、default で無効です。

<書　　式> session invalid-status-drop-interface enable
<初 期 値> no session invalid-status-drop-interface enable
<　no　　> no session invalid-status-drop-interface enable
<備　　考>
- あるインタフェースに対してのみ適用したい場合は、global mode で session invalid-status-drop 機能を無効にして、かつ本機能を指定インタフェースで有効にします。以下は、tunnel 0 インタフェースに適用する場合の設定例です。
  - global mode で、session invalid-status-drop を無効にします。
    nxrg240(config)#no session invalid-status-drop enable
  - 指定インタフェースで、本機能を有効にします。
    nxrg240(config)#interface tunnel 0
    nxrg240(config-tunnel)#session invalid-status-drop-interface enable

### ◆ ip p2p-detection

<説　　明> P2P 検出機能を有効にします(IPv4 のみ対応)。
<書　　式> ip p2p-detection (any|winny|share|bittorrent) {log|deny}
<　no　　> no ip p2p-detection
no ip p2p-detection (winny|share|bittorrent)
<備　　考>
- インターネットに接続しているインタフェース上でのみ有効にすることを推奨します。
- 詳細については、「付録 L:P2P 検出機能」を参照してください。

◆ **tunnel hop-limit**

<説　　明> IPv6 hop-limit 値を指定します。
<書　　式> tunnel hop-limit <1-255>
<初 期 値> tunnel hop-limit 64
<　no　　> no tunnel hop-limit
<備　　考> 指定のない場合は、システム初期値(64)を使用します。

◆ **tunnel traffic-class**

<説　　明> トンネル IPv6 ヘッダのトラフィッククラスフィールドに設定する値を指定します。
<書　　式> tunnel traffic-class <0-252>
　　tunnel traffic-class inherit
<初 期 値> tunnel traffic-class inherit
<　no　　> no tunnel traffic-class
<備　　考>

・ inherit を指定した場合、トネリングパケットのヘッダ部の ToS 値またはトラフィッククラスを、トンネル IPv6 ヘッダのトラフィッククラスフィールドにコピーします。
・ 値を指定する場合、0-252 の範囲で指定することが出来ます。ただし、ECN フィールドを設定することはできません。

※ ECN field の扱いについては、「付録 B 1.2.4.1 ECN field の扱い」を参照してください。

◆ **tunnel 6rd prefix**

<説　　明> 6rd のプレフィクスを指定します。通常、6rd サービスを提供しているサービスプロバイダーから割り当てられます。
<書　　式> tunnel 6rd prefix X:X::/M
<　no　　> no tunnel 6rd prefix
<備　　考> 6rd 作成時に、必ず設定してください。

◆ **tunnel 6rdipv4 prefix-length**

**<説　　明>**

・ RFC5569 では、IPv6 アドレスに埋め込む IPv4 アドレス長は、32 ビット固定でしたが、RFC5959 では、埋め込む IPv4 アドレスの長さを指定することが出来ます。

<書　　式> tunnel 6rd ipv4 prefix-length <0-32>
<初 期 値> tunnel 6rd ipv4 prefix-length 0
<　no　　> no tunnel 6rd ipv4 prefix-length
<備　　考>

・ 初期値は、0 です(32 ビットすべてが埋め込まれます)。
・ 32-prefix-lenghth の部分が host 部として、IPv6 アドレスに埋め込まれます。この長さを変えることにより、ユーザが使用できるネットワークを格段に増やすことが出来るようになります。

◆ **ip multicast-to-unicast**

<説　　明> 有効時、multicast を unicast 変換したパケットを転送します。
<書　　式> ip multicast-to-unicast forwarding　　（有効）
<　no　> no ip multicast-to-unicast forwarding　　（無効）

◆ **ip dns-intercept**

<説　　明> 当該インタフェースで使用する dns-intercept を指定します。
　　ignore-auto-dns を指定すると、DHCP/IPCP で取得した DNS を使用しません。
<書　　式> ip dns-intercept <0-3> （|ignore-auto-dns）
<　no　> no ip dns-intercept
<備　　考> DNS インターセプトの設定は、dns-intercept mode で行います。

◆ **event-notify**

<説　　明> インタフェースの up/down 時に、イベント通知を行います。
<書　　式> event-notify <0-3>
<　no　> no event-notify
<備　　考> イベント通知の方法(LINE、メール)は、ENS mode で設定します。

◆ **cms watch enable**

<説　　明> インタフェースの up/down 時に、インタフェースの監視情報を CMS に送信します。
<書　　式> cms watch enable
<　no　> no cms watch enable

◆ **ip send-source**

<説　　明>
・ 本機能の有効時、当該インタフェースの IP アドレスをソースアドレスとするパケットは、当該インタフェースから出力します。
・ 本機能の無効時、ルーティングテーブルで指定されたインタフェースから出力します。
・ 本機能の有効時、当該インタフェースから出力するパケットは、ipsec policy にマッチしても暗号化せずに出力します。
<書　　式> ip send-source (|local)
<初 期 値> no ip send-source
<　no　> no ip send-source
<備　　考>
・ ip send-source local を設定した場合、本機能の対象は、NXR からの自発パケットのみです。ip natloopback 機能と併用する場合は、本機能を有効にします。

◆ **ip nat-loopback**

<説　　明>

・ 1 つのグローバル IP を使用して複数の Web/Mail サーバなどを公開する場合、DNAT 機能により内部サーバへの転送を行うことがあります。しかしながら、(下図のような環境で)NAT ルータ配下の端末からグローバル IP にアクセスしても、DNAT 変換が行われないため、公開サーバにアクセスできません。このような場合に、本機能を使用します。

<書　　式> ip nat-loopback

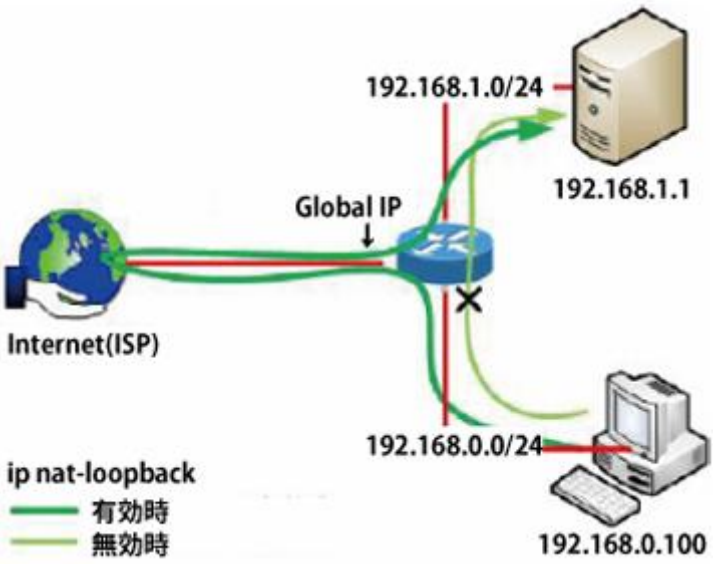
<初 期 値> no ip nat-loopback

<　no　　> no ip nat-loopback

<備　　考>

・ ip nat-loopback を設定しているインタフェース上で SPI を設定している場合は、フィルタを適切に設定して、必要なパケットを許可してください。

・ また、当該インタフェースで、NAT(または ip masquerade)を設定してください。未設定の場合、公開サーバにアクセスできない場合があります。




・ 本装置で DNAT を設定します。
Global IP(当該インタフェース):80 へのアクセスを、192.168.1.1 に変換します。

・ PC より Global IP:80 にアクセスします。

◆ **ipv6 router rip**
<説　　明> 当該インターフェースで RIPng を有効にします。
　　RIPng パケットの送受信を行い、当該インターフェースのネットワークを広告します。
<書　　式> ipv6 router rip
<　no　> no ipv6 router rip
<備　　考> RIPng の設定は、RIPng mode で設定します。

◆ **ipv6 rip split-horizon**
<説　　明> スプリットホライズンを設定します。
<書　　式> ipv6 rip split-horizon (|poisoned)
<初 期 値> ipv6 rip split-horizon poisoned
<　no　> no ipv6 rip split-horizon
<備　　考>
✓　poisoned を指定しない場合、当該インターフェースから学習した経路を同じインターフェースへ広告しません。
✓　poisoned を指定した場合、当該経路をメトリック 16(到達不能)として広告します(ポイズンリバース)。

◆ **ipv6 router ospf area**
<説　　明> 当該インターフェースで OSPFv3 を有効にし、指定したエリアに所属させます。
　　エリア ID は A.B.C.D 形式、または 10 進数で指定します。
<書　　式> ipv6 router ospf area (A.B.C.D|<0-4294967295>)
<　no　> no ipv6 router ospf area (A.B.C.D|<0-4294967295>)
<備　　考> OSPFv3 の設定は、OSPFv3 mode で設定します

◆ **ipv6 ospf cost**
<説　　明> 当該インターフェースの OSPFv3 コスト値を設定します。
　　コスト値は最短経路の計算に使用され、値が小さいほど優先されます。
<書　　式> ipv6 ospf cost <1-65535>
<初 期 値> ipv6 ospf cost 10
<　no　> no ipv6 ospf cost

◆ **ipv6 ospf hello-interval**
<説　　明> Hello パケットの送信間隔(秒)を設定します。
　　隣接ルータと同じ値を設定する必要があります。
<書　　式> ipv6 ospf hello-interval <1-65535>
<初 期 値> ipv6 ospf hello-interval 10
<　no　> no ipv6 ospf hello-interval

◆ **ipv6 ospf dead-interval**
<説　　明> ネイバーダウンと判定するまでの時間(秒)を設定します。
　　この時間内に Hello パケットを受信しない場合、ネイバーをダウンとみなします。
　　隣接ルータと同じ値を設定する必要があります。
<書　　式> ipv6 ospf dead-interval <1-65535>
<初 期 値> ipv6 ospf dead-interval 40
<　no　> no ipv6 ospf dead-interval

◆ **ipv6 ospf retransmit-interval**
<説　　明> LSA の再送間隔(秒)を設定します。
　　送信した LSA に対する確認応答を受信できない場合、この間隔で再送します。
<書　　式> ipv6 ospf retransmit-interval <1-65535>
<初 期 値> ipv6 ospf retransmit-interval 5
<　no　> no ipv6 ospf retransmit-interval

◆ **ipv6 ospf transmit-delay**

<説　　明> LSA の送信遅延時間(秒)を設定します。
　　送信する LSA の経過時間(LS age)にこの値を加算します。
<書　　式> ipv6 ospf transmit-delay <1-65535>
<初 期 値> ipv6 ospf transmit-delay 1
<　no　> no ipv6 ospf transmit-delay

◆ **ipv6 ospf priority**

<説　　明> DR/BDR 選出時のプライオリティを設定します。
　　値が大きいほど DR に選出されやすくなります。
　　0 を設定した場合、DR/BDR の選出対象外となります。
<書　　式> ipv6 ospf priority <0-255>
<初 期 値> ipv6 ospf priority 1
<　no　> no ipv6 ospf priority

# 第 8 章　interface ppp mode

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line.　End with CNTL/Z.
nxrg240(config)#**interface ppp <0-4>**
nxrg240(config-ppp)#

**◆ description**

<説　　明> interface の説明を記述します。
<書　　式> description DESCRIPTION
<　no　> no description (|DESCRIPTION)

**◆ ip address**

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

**◆ ip address**

<説　　明> PPP 接続の IP アドレスを自動取得に設定します。
<書　　式> ip address negotiated
<　no　> no ip address negotiated

**◆ ipv6 address**

<説　　明> IPv6 アドレスを設定します。
<書　　式> ipv6 address X:X::X:X/M (|eui-64) : IPv6 address (e.g. 3ffe:506::1/48)
　　ipv6 address autoconfig
<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)
　　no ipv6 address autoconfig

**◆ ipv6 address**

<説　　明> DHCPv6 PD の設定をします。
<書　　式> ipv6 address DHCPv6PD X:X::X:X/M (|eui-64) : DHCPv6-PD prefix name
<備　　考>

- ipv6-address は、sub-prefix と host 部を指定可能です。
- PREFIX-NAME は、dhcpv6 pd で受信する prefix に名前をつけたもので、ipv6 dhcp client pd で設定します。

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

◆ **ipv6 nd accept-ra**

<説　　明>
- 本設定(ipv6 address autoconfig 設定なし)を有効にすると、RA を受信しても、stateless address を設定しません。

<書　　式> ipv6 nd accept-ra
<　no　　> no ipv6 nd accept-ra
<備　　考>
- ipv6 address autoconfig 設定時、本設定は必要ありません。
- 当該インタフェースに、IPv6 アドレスは設定しませんが、RA によって取得したパラメータ(defaultgateway, retransmit timer, reachable time, mtu, hop-limit)は使用します。

◆ **bandwidth**

<説　　明> インタフェースの帯域幅を設定することが出来ます。
　　bandwidth の初期値は、10Mbps です。
　　bandwidth の最大値は、10Gbps です。
<書　　式> bandwidth <1-10000000000[k/m/g]>
<　no　　> no bandwidth
<備　　考> 本機能は、OSPF のコスト計算時のみに使用します。
　　基準となる帯域幅は、auto-cost コマンド(ospf mode)にて設定します。

◆ **mtu**

<説　　明> MTU の値を設定します。
<書　　式> mtu <bytes:68-1500>
<初 期 値> mtu 1454
<　no　　> no mtu（= Set defaults）

◆ **ppp lcp mru**

<説　　明> MRU を設定します。
<書　　式> ppp lcp mru <bytes:128-1500>
<初 期 値> ppp lcp mru 1454
<　no　　> no ppp lcp mru（= Set defaults）
<備　　考> IPv6 を使用する場合は、MRU を 1280 以上に設定してください。

◆ **ipv6 dhcp client**

<説　　明> 当該インタフェースに適用する DHCPv6 クライアントのプロファイル名を指定します。
<書　　式> ipv6 dhcp client WORD
<　no　　> no ipv6 dhcp client

### ◆ ipv6 dhcp client pd

<説　　明> DHCPv6 PD の prefix 部に、プロファイル名を付けます。
<書　　式> ipv6 dhcp client pd DHCPv6-PD
< no　> no ipv6 dhcp client
<備　　考>
- DHCPv6 PD を受信するインタフェース上で設定します。
- 受信した DHCPv6 PD を(異なる)インタフェースに対して適用するには、ipv6 address DHCPv6-PD コマンドを使用します。
- ipv6 dhcp client WORD と ipv6 dhcpv6 pd DHCPv6-PD は、どちらか一方だけ設定可能です。

### ◆ ip redirects

<説　　明>
- ICMP redirect(type=5)とは、同一ネットワーク上に他の最適なルートがあることを通知するためのメッセージです(RFC792)。
- 本装置の Send redirect 機能によって、ICMP redirect の送信の有無を切り替えることが出来ます。

<書　　式> ip redirects
<初 期 値> ip redirects　　(有効)
< no　> no ip redirects　　(無効)
<備　　考>
- ICMPRedirect の例は、interface mode の ip redirects を参照して下さい。

◆ **ip tcp adjust-mss**

<説　　明>

・ Path MTU Discovery(PMTUD)機能(End-to-end でフラグメントが発生しない最大の MTU を発見すること)によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器(ルータ等)が ICMP fragment needed をフィルタリングしている場合(ブラックホールルータが存在する場合)や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、End-to-end での通信に支障をきたすことになります。このような場合、TCP では SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

<書　　式> ip tcp adjust-mss (auto|<500-1460:bytes>)

<初 期 値> no ip tcp adjust-mss

<　no　　> no ip tcp adjust-mss

<備　　考>

・ IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。

・ 本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ ユーザが設定する場合は、MSS 値を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。

・ 「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

◆ **ipv6 tcp adjust-mss**

<説　　明> TCP/IPv6 の MSS 値を設定します。

<書　　式> ipv6 tcp adjust-mss (auto|<bytes:500-1440>)

<初 期 値> no ipv6 tcp adjust-mss

<　no　　> no ipv6 tcp adjust-mss

◆ **ip mask-reply**

<説　　明>

・ OpenView などの監視装置では、監視ネットワーク内の機器に対して ICMP address mask request (type=17)を送信することによって機器のインタフェースのネットマスク値を取得します(単純に、死活監視で使用する場合もあります)。

・ 本装置では、ICMP address mask request への応答の有無を設定することが出来ます。

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

<初 期 値> no ip mask-reply　　(ICMP address mask request に応答しません。)

<　no　　> no ip mask-reply

<備　　考>

・ ICMP address mask request/reply の例は、interface mode の ip mask-reply を参照して下さい。

◆ **ip send-source**

<説　　明>

- 本機能の有効時、当該インタフェースの IP アドレスをソースアドレスとするパケットは、当該インタフェースから出力します。
- 本機能の無効時、ルーティングテーブルで指定されたインタフェースから出力します。
- 本機能の有効時、当該インタフェースから出力するパケットは、ipsec policy にマッチしても暗号化せずに出力します。

<書　　式> ip send-source (|local)

<初 期 値> no ip send-source

<　no　　> no ip send-source

<備　　考>

- ip send-source local を設定した場合、本機能の対象は、NXR からの自発パケットのみです。ip natloopback 機能と併用する場合は、本機能を有効にします。

### ◆ ip nat-loopback

<説　　明>

・ 1 つのグローバル IP を使用して複数の Web/Mail サーバなどを公開する場合、DNAT 機能により内部サーバへの転送を行うことがあります。しかしながら、(下図のような環境で)NAT ルータ配下の端末からグローバル IP にアクセスしても、DNAT 変換が行われないため、公開サーバにアクセスできません。このような場合に、本機能を使用します。

<書　　式> ip nat-loopback

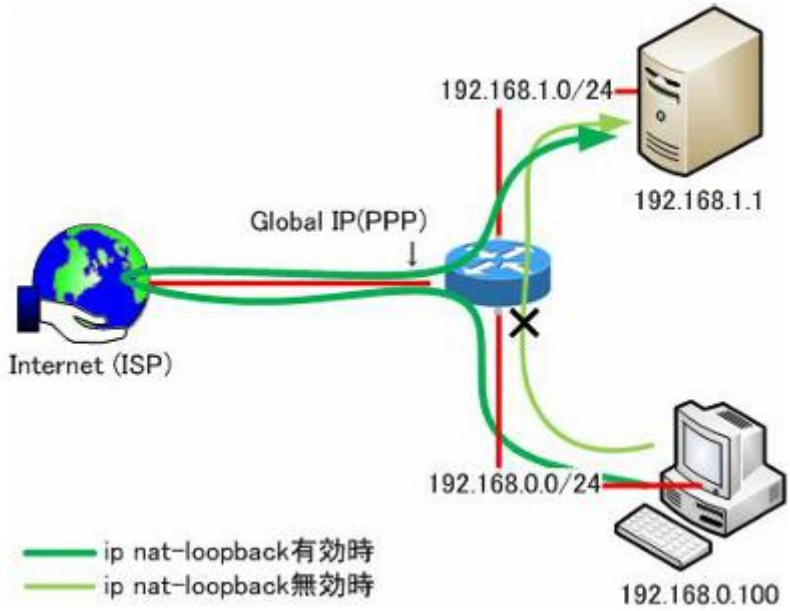
<初 期 値> no ip nat-loopback

<　no　　> no ip nat-loopback

<備　　考>

・ ip nat-loopback を設定しているインタフェース上で SPI を設定している場合は、フィルタを適切に設定して、必要なパケットを許可してください。

・ また、当該インタフェースで、NAT(または ip masquerade)を設定してください。未設定の場合、公開サーバにアクセスできない場合があります。

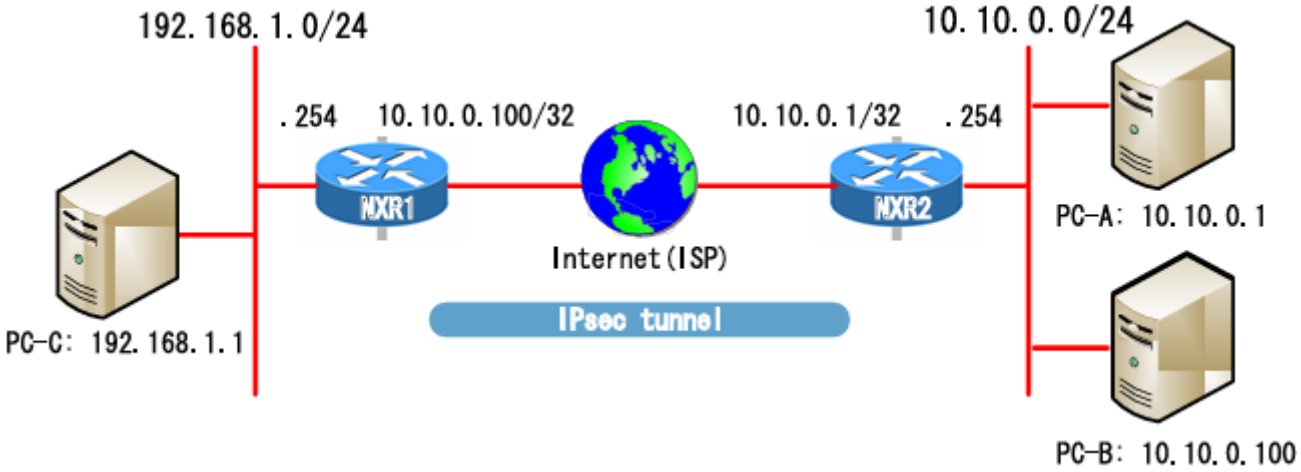



・ 本装置で DNAT を設定します。
Global IP(PPP):80 へのアクセスを、192.168.1.1 に変換します。

・ PC より Global IP:80 にアクセスします。

○ ip nat-loopback による address の重複への対応

ip nat-loopback を利用すると、次のような構成でも通信が可能となります。




- PC-C と PC-A、および PC-C と PC-B の通信が可能です。
- PC-A と PC-B の通信が可能です。
- 各PCとNXR1/NXR2のWAN IP(NXR1:10.10.0.100/NXR2:10.10.0.1)は、通信することが出来ません。

このように、LAN と WAN で通信範囲が完全に分割される構成になります。なお、この構成で IPsec トンネルを確立するには、NXR1/NXR2 で ip send-source を設定し、IKE(および ESP)パケットが必ず PPP に出力されるようにします。また、NXR1/NXR2 の WAN 側 IP へのデフォルトルートの設定や、対向のグローバル IP へのスタティックルートの設定を行うことは出来ません。

◆ **keepalive lcp-echo**

<説　　明> LCP echo request によるキープアライブを有効にします。
<書　　式> keepalive lcp-echo (|<interval:30-600> <failure-count:1-10>)
<初 期 値> keepalive lcp-echo 30 3
<　no　> no keepalive lcp-echo
<備　　考>

・ lcp-echo request/reply の連続失敗回数が、failure count の設定回数に達すると、PPP を切断します。

◆ **keepalive icmp-echo**

<説　　明> ICMP echo request を有効にします。
<書　　式> keepalive icmp-echo (|<interval:30-600> <retry:0-10> A.B.C.D)
<初 期 値> no keepalive icmp-echo
<備　　考> keepalive icmp-echo は、keepalive icmp-echo 30 2 と同じ
<　no　> no keepalive icmp-echo

◆ **ip rip receive version**

<説　　明> RIP の受信バージョンを設定します。
<書　　式> ip rip receive version (1|2) (|1|2)
<初 期 値> ip rip receive version 2
<備　　考> 両方指定も可能(ip rip receive version 1 2)
<　no　> no ip rip receive version

◆ **ip rip send version**

<説　　明> RIP の送信バージョンを設定します。
<書　　式> ip rip send version (1|2) (|1|2)
<初 期 値> ip rip send version 2
<備　　考> 両方指定も可能(ip rip send version 1 2)
<　no　> no ip rip send version

◆ **ip rip split-horizon**

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

◆ **ip access-group**

<説　　明>
・ global mode で設定した ACL をインタフェースに適用することで、パケットフィルタリングを行うことができます。
<書　　式> ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
<　no　> no ip access-group (in|out|forward-in|forward-out)
<備　　考>
・ 各インタフェースへのパケットフィルタリングの適用箇所(付録の Packet Traveling を参照)は、以下の 4 ヶ所です。
  - in(local input) NXR 自身で受信して処理するパケットを制限します。
  - out(local output) NXR 自身が作成して出力するパケットを制限します。
    トンネリングされたパケットも NXR 自身が作成したパケットとして認識します。
  - forward-in NXR が当該インタフェースで受信して forwarding するパケットを制限します。
  - forward-out NXR が受信して当該インタフェースへ forwarding するパケットを制限します。
・ mac 指定のある ACL は、out および forward-out に設定することは出来ません。

◆ **ipv6 access-group**

<説　　明> アクセスグループに IPv6 アクセスリストを追加します。
<書　　式> ipv6 access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
<初 期 値> no ipv6 access-group (in|out|forward-in|forward-out)
<　no　> no ipv6 access-group (in|out|forward-in|forward-out)

◆ **ip masquerade**

<説　　明>
・ インタフェースよりパケットを出力する際に、パケットの送信元 IPv4 アドレスを出力インタフェースの IPv4 アドレスに自動変換する機能です。
<書　　式> ip masquerade　　(有効)
<初 期 値> no ip masquerade　　(無効)
<　no　> no ip masquerade
<備　　考>
・ すべてのインタフェース(Ethernet/VLAN/PPP/Tunnel)で設定することが出来ます。
・ TCP/UDP/ICMP のみ対応しています。その他のプロトコルに関しては、動作は保証しません。
・ IPv6 パケットは、IP マスカレードの対象外です。
・ forward out/local output フィルタリング適用後のパケットに、IP マスカレードを適用します。

◆ **ip (snat-group|dnat-group)**

<説　　明>
・ global mode で設定した SNAT または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。
・ SNAT は、パケットの出力時に適用されます。DNAT は、パケットの入力時に適用されます。
<書　　式> ip (snat-group|dnat-group) NAT-NAME
<　no　> no ip (snat-group|dnat-group)
<備　　考> NAT ルールの設定は、ip snat/ip dnat)コマンド(global mode)で行います。

◆ **ip webauth-filter**
◆ **ipv6 webauth-filter**

<説　　明>
- Web 認証フィルタをインタフェースに適用すると、ある特定のホスト、ネットワークやインタフェースについて、Web 認証せずに通信することが可能となります。
- Web 認証フィルタは、各インタフェースにつき、IN/OUT をそれぞれ一つずつ設定することができます。Default の設定はありません。

<書　　式> ip webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
　　ipv6 webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
< no　> no ip webauth-filter (forward-in|forward-out)
　　no ipv6 webauth-filter (forward-in|forward-out)

<備　　考>
- Web 認証フィルタの設定については、ip web-auth access-list/ipv6 web-auth access-list コマンド(global mode)を参照してください。
- Web 認証については、Web Authenticate mode を参照してください。

◆ **ip spi-filter**

<説　　明>
- 簡易ファイヤウォールの一つとして、SPI(Stateful Packet Inspection)機能をサポートします。
- パケットに関連するコネクションの状態を見て、当該パケットをドロップするかしないかを決める機能です。

<書　　式> ip spi-filter　　(有効)
<初 期 値> no ip spi-filter　　(無効)
< no　> no ip spi-filter

<備　　考>
- コネクションの状態が、established または related の場合に、パケットの転送を許可します。
- Established とは、すでに双方向でパケットの通信がありコネクションが確立されている状態です。
- Related とは、すでに確立しているコネクションがある状態です。FTP のデータ転送等がこれに該当します。
- 新しい接続でありながら、syn ビットの立っていないパケットはドロップします。
- SPI は、forward in および local input の位置で適用されます。ユーザが適用位置を変更することは出来ません。

◆ **ipv6 spi-filter**

<説　　明> IPv6 SPI filter を設定します。
<書　　式> ipv6 spi-filter
<初 期 値> no ipv6 spi-filter
< no　> no ipv6 spi-filter

◆ **ip spi-filter log**

◆ **ipv6 spi-filter log**

<説　　明> フィルタログ機能(syslog mode 参照)を有効にします。
パケットが、SPI フィルタにマッチした場合、syslog に出力することが出来ます。
<書　　式> ip spi-filter log [limit <0-100>]
ipv6 spi-filter log [limit <0-100>]
<初 期 値> ip spi-filter log limit 10
ipv6 spi-filter log limit 10
< no > no ip spi-filter
no ipv6 spi-filter
<備　　考>

- limit を指定すると、1 秒当たりのログ出力数を制限します。初期値は、10 パケット/秒です。
- WAN 側からの意図しないパケットが、SPI フィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分に注意してください。

◆ **ppp authentication**

<説　　明> PPP の認証プロトコルを設定します。
<書　　式> ppp authentication (chap|pap|auto)
<初 期 値> ppp authentication auto
< no > no ppp authentication (= ppp authentication auto)

◆ **ppp username**

<説　　明> PPP 接続のユーザーID とパスワードを設定します。
<書　　式> ppp username USERID password (|hidden) PASSWORD
ppp username USERID
< no > no ppp username
<備　　考 >

- パスワードは、1-95 文字以内で設定してください。使用可能な文字は、英数字および !$#=*+-_.:;(){}[]^~@`<>%?です。
- ppp account コマンド(global ノード)で設定した USERID と PASSWORD を使用する場合は、USERID のみを指定します。
- パスワードに「?」を入力する場合は、「Ctrl」+「v」を入力してから、「?」を入力してください。

◆ **ppp auto-connect**

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

## ■ NCP

### ○ppp ncp max-configure

<説　　明> IPCP configuration request の最大再送回数(初期値:10 回)を設定します。
再送間隔は 3 秒(固定)です。
<書　　式> ppp ncp max-configure <1-20>
<初 期 値> ppp ncp max-configure 10
<　no　> no ppp ncp max-configure

### ○ppp ncp max-failure

<説　　明> configuration request 送信/受信の最大失敗回数(初期値:5 回)を設定します。
<書　　式> ppp ncp max-failure <1-255>
<初 期 値> ppp ncp max-failure 5
<　no　> no ppp ncp max-failure
<備　　考>

- 再送回数は、timeout によってインクリメントするため、NAK を受信して再度 configuration request を送信するような場合は再送回数としてカウントしません。したがって、configuration request の送信に対して、RAS が NAK を返信し続けると、NCP が終了しないことになります。
- configuration request の送信+NAK の受信を max failure 回数繰り返すと、それ以降のパケットをすべて reject し、request に対する応答(情報)はすべて無視します。以降の configuration request パケットには、オプションを含まない形で送信し、応答で受信した情報(IP アドレス)を元に再度 configuration request を送信します。この configuration request に対する ACK 受信によって、IPCP が完了します。
- configuration request の受信+NAK による応答の場合、max failure 回数目の configuration request の受信に対して、configuration reject で応答します。

### ○ppp ncp max-terminate

<説　　明> configuration request 送信/受信の最大失敗回数(初期値:5 回)を設定します。
<書　　式> ppp ncp max-terminate <1-10>
<初 期 値> ppp ncp max-terminate 2
<　no　> no ppp ncp max-terminate

※上記設定を有効にするには、IPCP/IPv6CP を enable にしてください。

◆ **ppp ipcp enable**

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

◆ **ppp ipcp dns**

<説　　明> IPCP の DNS オプションを設定します。
<書　　式> ppp ipcp dns accept
　　ppp ipcp dns reject
　　ppp ipcp dns <primary:A.B.C.D> (|<secondary:A.B.C.D>)
<初 期 値> ppp ipcp dns accept
<　no　　> no ppp ipcp dns
<備　　考> accept を指定した場合、プロバイダから自動的に割り当てられる DNS を使用します。
　　reject を指定した場合、プロバイダから割り当てられる DNS を使用しません。
　　IP アドレスを指定して、DNS を手動で設定することも出来ます。
　　WINS サーバオプションには対応していません。

◆ **ppp ipcp ip request**

<説　　明> IPCP で IP アドレスをリクエストします。
<書　　式> ppp ipcp ip request
<初 期 値> no ppp ipcp ip request
<　no　　> no ppp ipcp ip request
<備　　考> ip address コマンドで指定した IP を IPCP で request します。

◆ **ppp ipv6cp enable**

<説　　明> IPv6CP を有効にします。
<書　　式> ppp ipv6cp enable
<初 期 値> no ppp ipv6cp enable
<　no　　> no ppp ipv6cp enable（無効）

◆ **ppp ipv6cp id**

<説　　明> IPv6CP インタフェース ID を設定します。
<書　　式> ppp ipv6cp id X:X::X:X
　　ppp ipv6cp id ethernet <0-2>
<初 期 値> no ppp ipv6cp id
<備　　考> 指定ない場合は、eth0 の mac を使用します。この設定により LLA が決定されます。
<　no　　> no ppp ipv6cp id

◆ **ppp on-demand**

<説　　明> On-demand PPP を設定します。
<書　　式> ppp on-demand
<　no　　> no ppp on-demand
<備　　考> Mobile/PPPoE/BRI 使用時に、本機能を有効にすることが出来ます。
　　L2TP、IPv6CP 有効時は、無視されます。

◆ **ppp idle-timeout**

<説　　明>
・ idle-timeout で設定した時間内に、IP パケットの送受信がない場合、PPP を切断する(あるいは ondemand 状態へと遷移する)機能です。
・ idle-timeout は、PPP 上での IP/IPv6 パケットの送受信のみで更新します。
・ LCP echo-request/reply は、idle-timeout の更新対象ではありません。

<書　　式> ppp idle-timeout (<sec:30-86400>|)
<備　　考> ondemand 有効時(l2tp,ipv6cp 時は無視します)、時間指定ない場合は 180sec です。
　　ondemand 無効時でも動作します。
<　no　　> no ppp idle-timeout　(ondemand 有効時は、ppp idle-timeout 180)

◆ **ppp idle-timeout & system sleep**

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

◆ **netevent**

<説　　明>
・ トラックイベントの発生時に、当該 ppp を connect(または disconnect、あるいは reconnect)することが出来ます。

<書　　式> netevent <trackid:1-255> (connect|disconnect|reconnect)
　　netevent <trackid:2048-4095> (connect|disconnect|reconnect)
<　no　　> no netevent

◆ **ipv6 nd accept-redirects**

<説　　明>
・ IPv6 forwarding が無効の場合に、ICMPv6 redirects を受け入れるかどうかを指定します。

<書　　式> ipv6 nd accept-redirects
<初 期 値> no ipv6 nd accept-redirects
<備　　考> IPv6 forwarding が有効な場合は、この設定に関係なく受信しません。
<　no　　> no ipv6 nd accept-redirects

◆ **ipsec policy**

<説　　明> 当該インタフェースで使用する IPsec ローカルポリシーを設定します。
<書　　式> ipsec policy <local policy:1-255>
<　no　　> no ipsec policy (|<local policy:1-255>)
<備　　考>
・ 各インタフェースに、IPsec ローカルポリシーを 4 つまで設定することが出来ます。他のインタフェースで既に設定している IPsec ローカルポリシーは、重複して設定できません。

◆ **ipsec policy-ignore**

<説　　明>
・ IPsec policy のチェックを行わないように指定する機能です。IPsec policy として any などを指定したけれども、特定の通信のみ IPsec 化したくない場合に、この機能を使用します。
<書　　式> ipsec policy-ignore (|input|output)
<初 期 値> no ipsec policy-ignore(無効)
<　no　　> no ipsec policy-ignore
<備　　考>
・ Input を指定した場合、inbound policy check を実行しないため、IPsec 化されてくるべきパケットがドロップ されてしまう現象を回避することができます。
・ Output を指定した場合、当該インタフェースから出力されるパケットは、IPsec policy をチェックしないため平文で送信されます。

◆ **ipsec hold-sa**

<説　　明>
・ PPP 上で IPsec を利用する場合に、PPP 切断と共に IPsec SA を削除するかどうかを指定する機能です。
・ PPP の IP が動的に割り当てられる場合、PPP の down が発生すると、IPsec SA の削除が行われます。このとき、NXR 側から切断する場合は、PPP 切断前に delete SA 送信を行い、その後 PPP 切断処理を行います。対向から切断される場合や障害によって切断される場合は、delete SA の送信処理は実行されません。
・ 一方、PPP の IP address が固定割り当ての場合は、PPP 切断時に IPsec SA を削除しません。しかし、本機能が無効となっている場合は、動的 IP の場合と同様、PPP 切断と共に IPsec SA の削除を行います。この際、NXR 側から切断する場合は、delete SA を送信します。
<書　　式> ipsec hold-sa
<初 期 値> ipsec hold-sa
<　no　　> no ipsec hold-sa
<備　　考>
・ 本機能は、default で有効です。
・ 本機能の有効/無効は、固定 IP の場合のみ影響します。動的 IP の場合は、本機能の有効/無効に関らず、上記の動作となります。

■ **QoS**

<説　　明> QoS の設定をします。

○ HTB の設定

<書　　式> queue policy POLICYNAME bandwidth <1-1000000>

<備　　考>

- HTB を設定するには、class policy コマンドで作成した class policy を指定します。
- 存在しない class policy を指定すると、親 class のみ設定されます。該当する class policy を作成したときに、当該 HTB が設定されます。
- bandwidth で、class policy の全帯域幅を指定します。

○ PQ の設定

<書　　式> queue priority-group <PRIORITY-MAP-NUMBER:1-32>

<備　　考>

- PQ を設定するには、global mode で作成した priority-map を指定します。
- 存在しない priority-map を指定すると、すべてのパケットを default class にマッピングする PQ が設定されます。該当する priority-map を作成したときに、当該 PQ が設定されます。
- どの class にも該当しないパケットは、default class にマッピングされます。

○ SFQ の設定

<書　　式> queue fair-queue

○ FIFO の設定

<書　　式> queue fifo (|limit <1-16384>)

<備　　考> limit で FIFO キューの長さを指定することが出来ます。

○ TBF(shaping)の設定

<書　　式>

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

<備　　考>

- <RATE:1-1000000>　　Shaping レート(Kbps)を指定します。
- <BUFFER:1-1000000>　　Bucket のサイズ(bytes)を指定します。
- <LIMIT:1-1000000>　　Token が利用可能になるまでにバッファすることが出来るキューの長さ(bytes)を指定します。

○ no queue

<書　　式> no queue

<備　　考> 上記で設定した queue を削除して、default queue(pfifo_fast)に設定します。

○ classify

<書　　式> classify (input|output) route-map ROUTEMAP

<備　　考>

・ インタフェースにルートマップを適用します。1 つのインタフェースに、input と output を別々に設定することが出来ます。
・ input で指定したルートマップは、PRE-ROUTING(付録の Packet Traveling を参照)で適用されます。
・ output で指定したルートマップは、POST-ROUTING(付録の Packet Traveling を参照)で適用されます。

○ no classify

<書　　式> no classify (|input|output)

<備　　考>

・ インタフェースに適用したルートマップを削除します。
・ 「no classify」を実行すると、両方(input と output)を削除します。片方だけを削除する場合は、input または output を指定します。

■ **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> モバイル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|ipv4v6|ipv6|ppp)

○APN 設定の初期化/削除(default にもどるか消去されるかは、モバイル端末に依存します)

　　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

○通信量制限

PPP(mobile)での通信量が、指定した閾値を超えた場合に、PPP の切断および接続を禁止します。

　　mobile limit data-usage <KiB:1-1073741824>

○通信量制限の無効化

　　no mobile limit data-usage

◆ peer neighbor-route

<説　　明>

・ IPCP によって peer ip address が割り当てられた際に、その address に対する route を設定するかどうかを制御します。Default は、有効です。

<書　　式> peer neighbor-route

<初 期 値> peer neighbor-route

<　no　　> no peer neighbor-route

<備　　考>

・ PPP において ICMP keepalive が有効で、かつ送信先を peer ip に設定している場合、本設定を無効にすると peer ip へ到達できず PPP の切断が発生することが考えられます。したがって、ICMP keepalive の送信先を peer ip としている場合は、本設定を有効のまま使用することを推奨します。

**◆(ip|ipv6)　rebound**

<説　　明>

・ 下位ルータから受信したパケットを、受信インタフェースと同一インタフェースから出力(forwarding)した場合、下位ルータから NXR に対して再度パケットが送信されてくるため、下位ルータと NXR の間で TTL が「0」になるまでパケットがループします。
・ IP rebound 機能を無効にすると、受信インタフェースと送信インタフェースが同一の場合、パケットをドロップし、かつ送信元に destination unreachable を送信します。
・ Default は、有効です(受信インタフェースと送信インタフェースが同一でもドロップしません)。

<書　　式> (ip|ipv6) rebound
<初 期 値> (ip|ipv6) rebound
<　no　　> no (ip|ipv6) rebound

**◆ip reassemble-output**

<説　　明>

・ インタフェースの MTU(あるいは PMTU)より大きいパケットを IP forwarding する際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。本設定有効時、NXR がリアセンブルしたパケットは、以下のようにフラグメント処理を行います。
  - fragmented packet(パケットの断片)が MTU を超える場合、リアセンブルしたパケットを再度 MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、リアセンブルしたパケットを出力します。

<書　　式> ip reassemble-output
<初 期 値> ip reassemble-output
<　no　　> no ip reassemble-output

<備　　考>

・ 上記の場合(本設定が有効の場合)、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易な IP 実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズで NXR からパケットを出力します。また、出力時の IP フラグメント処理は、次のようになります。
  - fragmented packet(パケットの断片)が MTU を超える場合、受信した fragmented packet を MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、受信した fragmented packet をそのままのサイズで出力します。
・ Default は、global 設定および interface 設定ともに有効です。Global 設定と interface 設定の AND 条件により、本機能が有効か無効かを判定します。本設定は、IP forwarding するパケットにのみ影響します。
・ 受信時のサイズを記載しておくバッファが 32 個しかないため、33 個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-output が有効な場合と同様に処理します。

**◆session invalid-status-drop-interface**

<説　　明>

・ session invalid-status-drop 機能(global mode 参照)をインタフェース毎に指定することができます。
・ 本機能は、default で無効です。

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

・ あるインタフェースに対してのみ適用したい場合は、global mode で session invalid-status-drop 機能を無効にして、かつ本機能を指定インタフェースで有効にします。以下は、ppp 0 インタフェースに適用する場合の設定例です。
  - global mode で、session invalid-status-drop を無効にします。
    nxrg240(config)#no session invalid-status-drop enable
  - 指定インタフェースで、本機能を有効にします。
    nxrg240(config)#interface ppp 0
    nxrg240(config-ppp)#session invalid-status-drop-interface enable

**■ メールヘッダ部の設定(メール送信機能)**

<説　　明>
・ 送信するメールの各ヘッダ部に設定する値を指定します。本設定は、インタフェース毎(PPP <0-4>)に指定することが出来ます。

<備　　考>
・ メール送信機能の詳細については、mail server mode を参照してください。

○ mail send server
<説　　明> 本設定で使用するメールサーバの番号を指定します。
<書　　式> mail send server <0-2>
< no > no mail send server
<備　　考> メールサーバの設定については、mail serve mode を参照してください。

○ mail send from
<説　　明> 送信元メールアドレスを設定します。
<書　　式> mail send from WORD
< no > no mail send from
<備　　考>
・ WORD には、送信元メールアドレス(例:centurysys@xxx.isp.ne.jp)を指定します。
・ mail send from コマンドで送信元メールアドレスを指定しない場合は、mail from コマンド(global mode)で指定した送信元メールアドレスを使用します。

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

○ mail send subject
<説　　明> メールの件名を設定します。指定しない場合は、既定のフォーマットを使用します。
<書　　式> mail send subject LINE
< no > no mail send subject
<備　　考>
・ LINE を指定しない場合は、既定のフォーマットを使用します。以下に例を示します。
ppp0 の接続時:ppp0 was connected
ppp0 の切断時:ppp0 was disconnected

○ no mail send
<説　　明> 上記の設定を一括削除することができます。
<書　　式> no mail send

### ◆ ip p2p-detection
<説　　明> P2P 検出機能を有効にします(IPv4 のみ対応)。
<書　　式> ip p2p-detection (any|winny|share|bittorrent) {log|deny}
<　no　> no ip p2p-detection
　　no ip p2p-detection (winny|share|bittorrent)
<備　　考>
・ インターネットに接続しているインタフェース上でのみ有効にすることを推奨します。
・ 詳細については、「付録 L:P2P 検出機能」を参照してください。

### ◆ pppoe service-name
<説　　明>
・ ISP 名やサービスの品質・分類を表す場合に使用する service-name tag を指定することが出来ます。
<書　　式> pppoe service-name
<　no　>
・ Default では、未設定です。未設定の場合、任意のサービスを受け入れることが出来ます。
・ 設定する場合は、必ずサービスプロバイダーより指定された service-name を設定します。service-name が不一致の場合、PPPoE 接続に失敗します。

### ◆ ip dns-intercept
<説　　明> 当該インタフェースで使用する dns-intercept を指定します。
　　ignore-auto-dns を指定すると、DHCP/IPCP で取得した DNS を使用しません。
<書　　式> ip dns-intercept <0-3> （|ignore-auto-dns）
<　no　> no ip dns-intercept
<備　　考> DNS インターセプトの設定は、dns-intercept mode で行います。

### ◆ event-notify
<説　　明> PPP の接続／切断時に、イベント通知を行います。
<書　　式> event-notify <0-3>
<　no　> no event-notify
<備　　考> イベント通知の方法(LINE、メール)は、ENS mode で設定します。

### ◆ cms watch enable
<説　　明> インタフェースの up/down 時に、インタフェースの監視情報を CMS に送信します。
<書　　式> cms watch enable
<　no　> no cms watch enable

◆ **ppp callback accept widestar2**

<説　　明> Widestar2 サービスのパケットを受信して PPPoE 接続することが出来ます。
<書　　式> ppp callback accept widestar2
<　no　　> no ppp callback accept widestar2
<備　　考>

- 既に PPPoE 接続している状態で、Widestar2 サービスのパケットを受信した場合は、以下のようなログを出力します(再接続等は行いません)。
  ws2cd: packet call-in notify message received, but ppp0 is already up.
- widestar2 send ppp <0-4> callback accept(view mode)でパケット着信を許可します。
- widestar2 send ppp <0-4> callback reject(view mode)でパケット着信を禁止します。

◆ **pppoe terminate widestar2**

<説　　明> パケット通信キャンセル通知を設定することが出来ます。
<書　　式> pppoe terminate widestar2
<　no　　> no pppoe terminate
<備　　考>

- PPPoE PADO パケットの受信タイムアウト時、パケット通信キャンセルを通知します。
- Widestar2 と本装置が PPPoE 接続している場合に「圏外→圏内で再接続できない」のような状態を回避することが出来ます。

◆ **ipv6 router rip**
<説　　明> 当該インターフェースで RIPng を有効にします。
　　RIPng パケットの送受信を行い、当該インターフェースのネットワークを広告します。
<書　　式> ipv6 router rip
<　no　> no ipv6 router rip
<備　　考> RIPng の設定は、RIPng mode で設定します。

◆ **ipv6 rip split-horizon**
<説　　明> スプリットホライズンを設定します。
<書　　式> ipv6 rip split-horizon (|poisoned)
<初 期 値> ipv6 rip split-horizon poisoned
<　no　> no ipv6 rip split-horizon
<備　　考>
✓　poisoned を指定しない場合、当該インターフェースから学習した経路を同じインターフェースへ広告しません。
✓　poisoned を指定した場合、当該経路をメトリック 16(到達不能)として広告します(ポイズンリバース)。

◆ **ipv6 router ospf area**
<説　　明> 当該インターフェースで OSPFv3 を有効にし、指定したエリアに所属させます。
　　エリア ID は A.B.C.D 形式、または 10 進数で指定します。
<書　　式> ipv6 router ospf area (A.B.C.D|<0-4294967295>)
<　no　> no ipv6 router ospf area (A.B.C.D|<0-4294967295>)
<備　　考> OSPFv3 の設定は、OSPFv3 mode で設定します。

◆ **ipv6 ospf cost**
<説　　明> 当該インターフェースの OSPFv3 コスト値を設定します。
　　コスト値は最短経路の計算に使用され、値が小さいほど優先されます。
<書　　式> ipv6 ospf cost <1-65535>
<初 期 値> ipv6 ospf cost 10
<　no　> no ipv6 ospf cost

◆ **ipv6 ospf hello-interval**
<説　　明> Hello パケットの送信間隔(秒)を設定します。
　　隣接ルータと同じ値を設定する必要があります。
<書　　式> ipv6 ospf hello-interval <1-65535>
<初 期 値> ipv6 ospf hello-interval 10
<　no　> no ipv6 ospf hello-interval

◆ **ipv6 ospf dead-interval**
<説　　明> ネイバーダウンと判定するまでの時間(秒)を設定します。
　　この時間内に Hello パケットを受信しない場合、ネイバーをダウンとみなします。
　　隣接ルータと同じ値を設定する必要があります。
<書　　式> ipv6 ospf dead-interval <1-65535>
<初 期 値> ipv6 ospf dead-interval 40
<　no　> no ipv6 ospf dead-interval

◆ **ipv6 ospf retransmit-interval**
<説　　明> LSA の再送間隔(秒)を設定します。
　　送信した LSA に対する確認応答を受信できない場合、この間隔で再送します。
<書　　式> ipv6 ospf retransmit-interval <1-65535>
<初 期 値> ipv6 ospf retransmit-interval 5
<　no　> no ipv6 ospf retransmit-interval

◆ **ipv6 ospf transmit-delay**

<説　　明> LSA の送信遅延時間(秒)を設定します。
　　送信する LSA の経過時間(LS age)にこの値を加算します。
<書　　式> ipv6 ospf transmit-delay <1-65535>
<初 期 値> ipv6 ospf transmit-delay 1
<　no　> no ipv6 ospf transmit-delay

◆ **ipv6 ospf priority**

<説　　明> DR/BDR 選出時のプライオリティを設定します。
　　値が大きいほど DR に選出されやすくなります。
　　0 を設定した場合、DR/BDR の選出対象外となります。
<書　　式> ipv6 ospf priority <0-255>
<初 期 値> ipv6 ospf priority 1
<　no　> no ipv6 ospf priority

# 第 9 章　dns mode

### ◆ 移行 command

dns mode に移行します。
nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#dns
nxrg240(dns-config)#

### ◆ service

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

### ◆ address

<説　　明> DNS サーバの IP アドレスを設定します。
<書　　式> address A.B.C.D
　　address X:X::X:X
<初 期 値> no address
<備　　考> 最大 4 つまで設定可能
<　no　　> no address (A.B.C.D|X:X::X:X)
<備　　考> no の場合でも、PPP や DHCP で DNS アドレスを取得している場合は、cache/proxy 有効。

### ◆ priority

<説　　明> DNS サーバのプライオリティを設定します。
<書　　式> priority (user|ppp<0-4>|dhcp|dhcpv6) <priority:0-255>
<初 期 値> すべて 20
<　no　　> no priority (user|ppp<0-4>|dhcp|dhcpv6)
　　(=no priority (user 20|ppp <0-4> 20|dhcp 20|dhcpv6 20))
<備　　考>

- 同一 priority の場合の優先度: user > ppp4 > ppp3 > ppp2 > ppp1 > ppp0 > dhcp > dhcpv6
- dhcp6 においては、現在では、dhcp6-pd を使用した DNS server の割り当てをサポートします。
- 0 の場合は、当該アドレスを使用しません。

### ◆ root

<説　　明> root DNS サーバを使用する /しないを設定します。
<書　　式> root enable
<備　　考> 設定されている全ての DNS に対して名前解決できなかった場合に、rootDNS に query 転送する。
<　no　　> no root enable

### ◆ timeout

<説　　明> DNS のタイムアウト値を設定します。
<書　　式> timeout <seconds:5-30>
<初 期 値> timeout 30
<　no　　> no timeout (=timeout 30)

### ◆ limitation enable

<説　　明> DNS サーバ限定機能を有効にします。
<書　　式> limitation enable
< no > no limitation enable
<備　　考> enable にした場合、指定 DNS サーバ以外への再帰問い合わせをしません。

### ◆ zone address

<説　　明> 設定された domain の問合せに対して、指定した DNS server への問合せを行います。
<書　　式> zone <1-5> address A.B.C.D
< no > no zone <1-5> address（A.B.C.D|）
<備　　考> zone address は、最大 2 つまで設定可能です。
address,domain が各 1 つ以上のときに設定が有効になります。
zone 設定が変更された場合は、exit 時に DNS キャッシュをクリアします。

### ◆ zone domain

<説　　明> 設定された domain の問合せに対して、指定した DNS server への問合せを行います。
<書　　式> zone <1-5> domain WORD
< no > no zone <1-5> domain（WORD|）
<備　　考> zone domain は、最大 3 つまで設定可能です。
address,domain が各 1 つ以上のときに設定が有効になります。
先頭の . は設定可能ですが、それ以降は fqdn 形式で設定します。
ホスト名は設定できません。また、最大文字数は 125 文字です。

### ◆ zone limitation

<説　　明> 指定した特定の domain 向けの DNS server に対する問合せで名前解決できない場合、それ以上は問合せません。
<書　　式> zone <1-5> limitation enable
<初 期 値> zone <1-5> limitation enable
< no > no zone <1-5> limitation enable

### ◆ domain-search

<説　　明> 有効にすると、取得したドメインサーチリストに従って、DNS サーバを使用します。
<書　　式> domain-search enable
< no > no domain-search enable
<備　　考>

- 有効の場合、Domain search list で受信した domain を含むアドレスを解決する際、取得した DNS サーバに対して名前解決を試行します。
- 無効の場合、Domain search list で受信した domain を含むアドレスを解決する際、priority の優先順位に従って名前解決を試行します。

◆ **min-ttl**
<説　　明>
・ Minimum TTL より小さい TTL を持つレコードを受信した場合、Minimum TTL を使用します。
<書　　式> min-ttl <120-2147483647>
<　no　　> no min-ttl
<初 期 値> min-ttl 120(sec)

◆ **max-ttl**
<説　　明>
・ Maximum TTL より大きい TTL を持つレコードを受信した場合、Maximum TTL を使用します。
<書　　式> max-ttl <120-2147483647>
<　no　　> no max-ttl
<初 期 値> min-ttl 604800(sec)

◆ **host-ttl**
<説　　明> ip host で応答するアドレスの TTL を設定します。
<書　　式> host-ttl <120-2147483647>
<　no　　> no host-ttl
<初 期 値> host-ttl 86400

◆ **host-ttl**
<説　　明> ip host で応答するアドレスの TTL を設定します。
<書　　式> host-ttl <120-2147483647>
<　no　　> no host-ttl
<初 期 値> host-ttl 86400

◆ **edns-query**
<説　　明> EDNS0 機能を有効にします。
<書　　式> edns-query enable　　(有効)
<　no　　> no edns-query enable (無効)
<初 期 値> no edns-query enable
<備　　考>
・ DNS では、最大 512 バイトまでの UDP パケットを送信することが出来ます。しかしながら、このサイズは、IPv4 アドレスでの使用を前提としているため、IPv6 アドレス使用時は、512 バイトを超えることが考えられます。
・ EDNS0 を有効にすると、DNS サーバへの要求時に、クライアント側で受信可能な UDP パケットの最大データサイズを通知することによって、512 バイトを超える DNS パケットを扱うことが可能になります。

# 第 10 章　l2tp mode

## ■ L2TP(L2TPv2)機能概要

- LNS として call を受けた場合に、PPP フレームを L2TP によってトンネリングし、リモートの IP/IPv6 ネットワークに接続します。
- LAC として動作する場合、ISP 側で用意された LNS へ L2TP トンネル / セッションを確立後、PPP の確立を行います。LNS として動作する場合、LCCE から SCCRQ を受け取ると、L2TP トンネル / セッションを確立後、PPP の確立を行います。LNS モードの場合、本装置から接続を行うことはありません。
- 本装置の L2TP(L2TPv2)は、RFC2661 に準拠しています。

### ◆ 移行 commannd

l2tp mode に移行します。

```
nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#l2tp <0-1>
nxrg240(config-l2tp)#
```

## ■ L2TP mode

- L2TP tunnel(peer)設定毎に LAC/LNS のいずれかのモードを指定することが出来ます。Default では LAC として動作します。ただし、対向のアドレスとして any を設定した場合は、強制的に LNS モードとして動作します。

### ◆ tunnel mode

<説　　明> L2TP トンネルモードの設定を行います。
<書　　式> tunnel mode (lns|lac)
<初 期 値> tunnel mode lac
<備　　考>

- ppp account(global mode)設定状態で、LAC モードを指定すると、ppp account が有効になります。
- ppp account 設定状態で LNS モードに変更すると、ppp account が無効になります(ppp は切断されます)。
- virtual-template 設定状態で lac モードに変更すると、virtual-template が無効になります(該当する ppp clone が切断されます)。
- virtual-template 設定状態で lns モードに変更すると、virtual-template が有効になります。

## ■コントロールメッセージの再送回数とタイムアウト

- コントロールメッセージの再送回数は、5 回(default)です。再送が発生すると、再送毎に再送間隔が 2 倍に増えます。初回のメッセージタイムアウトは 1 秒です。また、最大再送間隔は 8 秒です。
- したがって、コントロールメッセージを送信してから、タイムアウト(down)と判断するまでの時間は、31 秒(= 1+ 2+ 4+ 8+ 8+ 8)です。なお、再送回数は、1～ 1000 回の間で変更することができます。

### ◆ tunnel retransmit

<説　　明>

- コントロールメッセージを送信してから、タイムアウトまでのリトライ回数を設定します。

<書　　式> tunnel retransmit retries <max:1-1000>
<初 期 値> tunnel retransmit retries 5
<　no　　> no tunnel retransmit retries（=tunnel retransmit retries 5）

## ■ L2TP Keepalive (Hello)

・ L2TP トンネルの接続性をチェックするために、定期的に keepalive を送信します。送信間隔は 60 秒(default)で、0 ～ 1000 秒の範囲で変更することが出来ます。0 を設定した場合は、hello を送信しません。
・ Hello の送信タイマーがタイムアウトする前に、LNS からコントロールメッセージ / データメッセージを受信した場合、本装置内部の hello 送信タイマーを再スケジュールします。したがって、LNS から L2TP パケットを受信している間は、本装置から hello を送信しません。

### ◆ tunnel hello

<説　　明> Hello インターバルを設定します。
<書　　式> tunnel hello <sec:0-1000>
<初 期 値> tunnel hello 60
<　no　> no tunnel hello
<備　　考> no tunnel hello(=tunnel hello 0)の場合、hello パケットを送出しません。

## ■ L2TP port number

・ 一部の他社製ブロードバンドルータの配下に本装置を設置した場合、L2TP トンネルを確立する際に、source port UDP/1701 を使用すると、L2TP/PPP セッションが確立できません。その対策として、L2TP で使用する source port 番号を変更することが出来ます。
・ L2TP では、source port として UDP/4001(default)を使用し、destination port として UDP/1701(default)を使用します。source port/destination port 共に、UDP/1024 ～ 65535 の範囲で変更することが出来ます。
・ L2TPv3 を UDP 上で使用する場合、L2TPv3 と L2TPv2(本機能)に、それぞれ異なる port 番号を設定してください。

### ◆ udp source-port

<説　　明> L2TP で使用する UDP の source port 番号を指定します。
<書　　式> l2tp udp source-port <src_port:1024-65535>
<初 期 値> l2tp udp source-port 40001
<備　　考> 本機能は、global mode で設定します。

### ◆ udp port

<説　　明> L2TP で使用する UDP の destination port 番号を指定します。
<書　　式> tunnel udp port <dst_port:1024-65535>
<　no　> no tunnel udp port
<初 期 値> tunnel udp port 1701

**■接続先の指定**

- 接続先アドレスとして、LAC の場合は IPv4/FQDN を、LNS の場合は any を指定することが出来ます。
- any 指定時は、対向のアドレスを他の機能(本バージョンでは IPsec)から取得し、そのアドレスが L2TP に登録されることで、当該アドレスからの L2TP 接続が可能となります。この場合、L2TP トンネル / セッションの down が発生すると、IPsec に対してトンネルダウンの指示を行います。
- LAC モードで対向アドレスとして FQDN を指定した場合、SCCRQ を送信する毎に、DNS サーバに対して IPv4 アドレスの名前解決を行います。したがって、FQDN を指定した場合、接続中または接続の途中で IPv4 アドレスが変更になっても、L2TP トンネル / セッションの接続先は、すぐには変更されません。再接続時に、新しい IPv4 アドレスに対して接続を試みます。
- IPv6 over PPP を L2TP にてトンネリングすることは可能ですが、転送用プロトコルとして IPv6 を使用することはできません。

**◆ tunnel**

<説　　明> 接続先のアドレスを設定します。

○ address (A.B.C.D|FQDN)

<書　　式> tunnel address (A.B.C.D | FQDN)

○ address any ipsec

<書　　式> tunnel address any ipsec

<備　　考>

- any 指定時、bind するプロトコル(ipsec)を指定することが出来ます。IPsec の確立した client からの接続のみを許可します。
- 接続タイムアウト
  - tunnel address any ipsec を指定した場合、IPsec からのアドレス登録後、300 秒以内に L2TP セッションが確立しなければ、当該アドレスを無効とし、IPsec に対して IPsec tunnel の削除要請を行います。ただし、タイムアウトした場合でも、トンネルが active(再送中)であれば、IPsec tunnel の削除要請は行いません。トンネルが down した際に、IPsec tunnel の削除要請を行います。
  - 本機能により、IPsec は確立したものの、L2TP のパケットを受信しない場合等に、IPsec SA だけが残ってしまうような状態を防ぐことが出来ます。

## ■ LNS としての動作

### □ PPP インタフェースの割り当て

・ L2TP LNS として動作し、クライアントからの L2TP トンネル / セッションの確立を行うことが出来ます。この際に割り当てる PPP インタフェースは、virtual-template です。特定の PPP インタフェースを固定的に割り当てる動作はサポートしていません。
・ Virtual-template を使用すると、PPP インタフェースのクローンを作成します。このときの PPP インタフェース番号(100 ～ 256)は、L2TP サービスが自動的に割り当てます。

#### ◆ tunnel virtual-template

<説　　明> 使用する virtual-template を指定します。
<書　　式> tunnel virtual-template <0-0>
< no > no tunnel virtual-template

### □ IPv4 アドレスの割り当て

・ PPP の確立時に、クライアントからの IPCP address の request に対して、IPv4 アドレスを割り当てます。
・ L2TP に割り当てられた IP address pool の中から、IPv4 アドレスを自動的に割り当てます。accessserver profile mode で、ユーザ毎に固定 IP の割り当て設定を行っている場合は、当該 IP アドレスを割り当てます。
・ IP アドレスの自動割り当てを行う際、IP pool のアドレス範囲の中に、PPP ユーザ毎に固定的に割り当てる IP アドレスが含まれている場合や、exclude address が設定されている場合は、該当する IP アドレスを除いて割り当てます。

#### ◆ ip local pool WORD address

<説　　明> IP アドレスプールを設定します。
<書　　式> ip local pool WORD address A.B.C.D (|A.B.C.D)
< no > no ip local pool WORD
<備　　考> 本設定は、global mode で行います。

#### ◆ ip local pool WORD exclude-address

<説　　明> IP アドレスプールの対象外となる IP アドレス(または IP アドレス範囲)を設定します。
<書　　式> ip local pool WORD exclude-address A.B.C.D (|A.B.C.D)
< no >
・ exclude-address の全削除　　no ip local pool WORD exclude-address
・ 指定対象のみ削除　　no ip local pool WORD exclude-address A.B.C.D (|A.B.C.D)
<備　　考> 本設定は、global mode で行います。

#### ◆ peer ip pool

<説　　明> 使用する IP アドレスプールを指定します。
<書　　式> peer ip pool WORD
< no > no peer ip pool WORD
<備　　考> 本設定は、interface virtual-template mode で行います。

◆ **tunnel hidden**
<説　　明> AVP Hiding を有効にします。
<書　　式> tunnel hidden
<初 期 値> no tunnel hidden
<　no　> no tunnel hidden

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

◆ **tunnel ppp**
<説　　明> PPP を L2TP でトンネリングします。
<書　　式> tunnel ppp <ppp:0-4>
<　no　> no tunnel ppp
<備　　考> l2tp の再接続、再接続間隔は、ppp の設定を使用します。
ppp と virtual-template の設定は排他(どちらかのみ設定可)です。

◆ **tunnel authentication callin**
<説　　明> tunnel 認証の設定を行います。
<書　　式> tunnel authentication callin
<　no　> no tunnel authentication (|callin)

# 第 11 章　l2tpv3-tunnel mode

**◆ 移行 commannd**

l2tpv3-tunnel mode に移行します。

```
nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#l2tpv3 tunnel <0-4095>
nxrg240(config-l2tpv3-tunnel)#
```

**◆ description**

<説　　明> L2TPv3 トンネルの説明を記述します。
<書　　式> description DESCRIPTION
<　no　> no description

**◆ tunnel address**

<説　　明> リモード LCCE のトンネルアドレスを設定します。
<書　　式> tunnel address A.B.C.D
tunnel address X:X::X:X
tunnel address FQDN
tunnel address any
tunnel address (ip|ipv6) (FQDN|any)
<備 考 >

- IPv6 アドレスを指定すると、コントロールパケットおよびセッションパケットの転送用プロトコルとして IPv6 を使用します(L2TPv3 over IPv6)。L2TPv3 over IPv6 は、fast-forwarding の対象外です。
- トンネルの接続先として、FQDN を指定することが出来ます。ただし、DNS による名前解決や timeout 待ちで、接続に時間がかかる場合があるため、FQDN の使用には注意が必要です。
- FQDN 指定時は、名前解決を行うプロトコル family(IPv4 または IPv6、あるいは両方のアドレス)を指定することが出来ます。指定のない場合は、IPv6 の名前解決を試行し、失敗した場合に、IPv4 の名前解決を行います。両方の名前解決を行うと時間がかかる場合があるため、そのような場合にはプロトコル family を指定します。
- any 指定時もプロトコル family を指定することが出来ます。any の場合、本装置と対向装置のプロトコル family が一致している場合のみ、接続することが出来ます。

**◆ no tunnel address**

<説　　明> リモード LCCE のトンネルアドレスを削除します。
<書　　式> no tunnel address

**◆ tunnel hostname**

<説　　明> リモート LCCE のホスト名を設定します。
<書　　式> tunnel hostname HOSTNAME

◆ **tunnel router-id**
<説　　明> リモート LCCE のルータ ID を設定します。
<書　　式> tunnel router-id A.B.C.D

◆ **tunnel password**
<説　　明> 認証や AVP Hiding で使用するパスワードを設定します。
<書　　式> tunnel password PASSWORD
　　tunnel password hidden PASSWORD
<初 期 値> no tunnel password
<　no　> no tunnel password
<備　　考> パスワードは、1-95 文字以内で設定してください。
　　使用可能な文字は、英数字および!$#=*+-_.:;(){}[]^~@`<> です。

◆ **tunnel hidden**
<説　　明> AVP Hiding を設定します。
<書　　式> tunnel hidden
<　no　> no tunnel hidden

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

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

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

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

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

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

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

# 第 12 章　l2tpv3-xconnect mode

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**l2tpv3 xconnect <xid:1-4294967295>**
nxrg240(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|wlan)**

<説　　明> Xconnectインタフェースを設定します。
<書　　式> xconnect ethernet <0-3> (|vid <1-4094>)
　　xconnect wlan <0-1>

◆ **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)

◆ **loop-detect enable**

<説　　明> Loop Detection 機能を有効にします。
<書　　式> loop-detect enable
<初 期 値> no loop-detect enable
<　no　> no loop-detect enable

◆ **send-known-unicast enable**

<説　　明> Known Unicast 送信機能を有効にします。
<書　　式> send-known-unicast enable
<初 期 値> no send-known-unicast enable
<　no　> no send-known-unicast enable

◆ **send-circuit-down enable**

<説　　明> Circuit Status が down の時に、対向 LCCE に対して、Non-Unicast Frame を送信します。
<書　　式> send-circuit-down enable
<初 期 値> no send-circuit-down enable
<　no　> no send-circuit-down enable

◆ **split-horizon enable**

<説　　明> Split Horizon 機能を有効にします。
<書　　式> split-horizon enable
<初 期 値> no split-horizon enable
<　no　> no split-horizon enable

◆ mac-learning unique enable

<説　　明> L2TPv3 MAC アドレス学習 unique 機能を有効にします。
<書　　式> mac-learning unique enable
<初 期 値> no mac-learning unique enable
<　no　> no mac-learning unique enable
<備　　考>

- 本機能を有効にするには、global mode で、次の設定が必要になります。
  nxrg240(config)#l2tpv3 mac-learning unique
- ネットワーク構成によっては、ある一つの Xconnect の Local Table、FDB に同じ MAC アドレスが登録されることがあります。本機能を有効にすると、新しく学習した MAC アドレスが、Local Table、FDB のどちらか一方に登録されるため、上記のような状態を回避することが出来ます。
- ある一つの Xconnect で、LoopDetect 機能と共存した場合、LoopDetect の FrameDrop 処理を優先します。つまり、この場合は、MAC アドレス学習 unique 機能は動作しないことになります。
- 本機能(unique)はデフォルトで無効です。

### ◆ ip tcp adjust-mss

<説　　明>
- Path MTU Discovery(PMTUD)機能(End-to-end でフラグメントが発生しない最大の MTU を発見すること)によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器(ルータ等)が ICMP fragment needed をフィルタリングしている場合(ブラックホールルータが存在する場合)や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、Endto-end での通信に支障をきたすことになります。このような場合、TCP では SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

<書　　式> ip tcp adjust-mss (auto|<500-1460:bytes>)
<初 期 値> no ip tcp adjust-mss
<　no　　> no ip tcp adjust-mss
<備　　考>
- IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。
- 本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。
- ユーザが設定する場合は、MSS 値を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。
- UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。
- 「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

### ◆ ipv6 tcp adjust-mss

<説　　明> IPv6 TCP パケットの MSS 値の書き換えを有効にします。
<書　　式> ipv6 tcp adjust-mss (auto|<500-1440:bytes>)
<初 期 値> no ipv6 tcp adjust-mss
<　no　　> no ipv6 tcp adjust-mss
<備　　考>
- 本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

### ◆ l2tpv3 access-group

<説　　明> L2TPv3 セッションの送信 / 受信に対して、l2tpv3 access-list を適用します。
<書　　式> l2tpv3 access-group (in|out) WORD
<　no　　> no l2tpv3 access-group (in|out)
<備　　考>
- WORD:　root の ACL 名を指定します。
  (root の ACL 名は、global ノードの l2tpv3 access-list WORD root コマンドにて設定)
- ・in:　受信方向のセッションに対して、フィルタを適用します。
- ・out:　送信方向のセッションに対して、フィルタを適用します。

# 第 13 章　l2tpv3-group mode

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**l2tpv3 group <gid:1-4095>**
nxrg240(config-l2tpv3-group)#

◆ **xconnect**

<説　　明> 使用する Xconnect を指定します。
<書　　式>
　　xconnect <primary-xid:1-4294967295> (|<secondary-xid:1-4294967295>) (|hotswap)
<備　　考>
・ hotswap を指定すると、L2TPv3 primary/secondary xconnect hotswap 機能を有効にします。
- -hotswap 設定は、config に保存されません。
- 従来、グループ機能を使用している構成において、primary xconnect と secondary xconnect の設定を変更すると、一度、L2TPv3 セッションがダウンします。
- 本機能は、L2TPv3 セッションをダウンさせずに、primary xconnect と secondary xconnect を切り替える機能です。
- -group mode を exit した際、xconnect 以外の設定があった場合は、config の設定変更が発生したと判断して、従来通り L2TPv3 セッションがダウンします。
- なお、本機能の連続での実行を回避するため、l2tpv3 group mode を exit した際は、数秒間コマンドを受け付けない仕様になっています。

```
nxrg240(config-l2tpv3-group)#xconnect 1 2 hotswap
nxrg240(config-l2tpv3-group)#exit
 Change primary/secondary xconnect...Please wait.
nxrg240(config)#
```

◆ **preempt enalbe**

<説　　明> Group の preempt モードの有効 / 無効を設定します。
<書　　式> preempt enable
<　no　　> no preempt enable

◆ **enforce-secondary-down enable**

<説　　明> 本機能を有効にすると、Secondary セッションを強制切断します。
<書　　式> enforce-secondary-down enable
<初 期 値> no enforce-secondary-down enable
<　no　　> no enforce-secondary-down enable

◆ **active-hold enable**

<説　　明> Group の Active Hold 機能の有効 / 無効を設定します。
<書　　式> active-hold enable
<初 期 値> no active-hold enable
<　no　　> no active-hold enable

◆ **mac-advertise enable**

<説　　明>

・ L2TPv3 MAC Advertise Frame 送信機能の有効 / 無効を設定します。
  - グループ機能を使用している構成で、センター側の配下にあるスイッチの MAC テーブルを更新するために、ローカルテーブルに登録されている MAC アドレス情報を元に疑似フレームを送信することによって、センターにある端末を発信源とする通信が可能となります。
  - この機能はデフォルトで無効です。
  - 本機能を使用する場合は、L2TPv3 MAC Address 学習 Always 機能を有効(l2tpv3 mac-learning always)に設定してください。

※本機能を使用する場合は、対向装置も同機能が実装されているファームウェア(v5.15.1 以降)を使用することを推奨します。

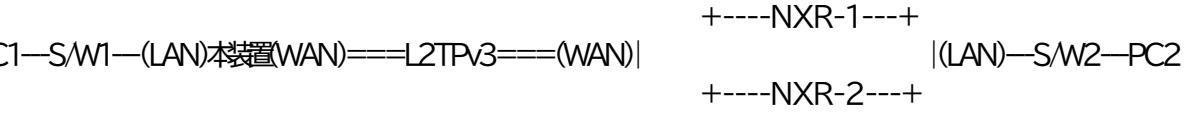
<書　　式> mac-advertise enable

<初 期 値> no mac-advertise enable

<　no　　> no mac-advertise enable

<備　　考>

・ 図のような冗長化構成において、拠点側(本装置)で L2TPv3 セッションの切替が発生した場合、センター側 NXR の配下にあるスイッチ(S/W2)の FDB が更新されるまで、センターにある端末を発信源とする通信を行うことは出来ません。本機能を有効にすることで、このような状況でも、できるだけ早く通信を回復させることが可能になります。




・ 拠点側にて L2TPv3 セッションの切り替えおよび切り戻り等を検知した際、ローカルテーブルで学習した MAC アドレス情報を、アクティブセッションを通してセンター側に送信します。1 つの MAC アドレスにつき 1 つの L2TPv3 MAC Advertise Frame を作成し、アクティブセッションに送信します。

○ L2TPv3 MAC Advertise Frame 送信

① 本機能無効(no mac-advertise enable)時は、L2TPv3 MAC Advertise Frame を送信しません。

② 本機能有効(mac-advertise enable)時は、次の場合に L2TPv3 MAC Advertise Frame を送信します。
  - アクティブセッションの切り替えおよび切り戻りを検知した時
  - アクティブセッションが作成されたとき

※ただし、Circuit Down 時の送信設定の有効(send-circuit-down enable)/ 無効(no send-circuitdown enable)に関わらず、対向 LCCE の Circuit status が DOWN の場合は、対向 LCCE で Drop されてしまう為、MAC Advertise Frame を送信しません。対向 LCCE から SLI Message(Circuit up)を受信した際は、その時点でアクティブセッションとして選択されているセッションに対して一度も MAC Advertise Frame を送信していない場合に限り、MAC Advertise Frame を送信します。

○ L2TPv3 MAC Advertise Frame 受信

① Xconnect で受信時、本機能の有効 / 無効に関わらず、常に Drop します。

② L2TP セッションで受信時、本機能の無効 / 有効に関わらず、常に以下の判定を行います。
  - データ部にある Xconnect インタフェースの HW アドレスと対向装置の HW アドレスを比較します。
    (a)一致した場合は、他拠点にはフレームを転送せず、Xconnect のみにフレームを転送します。
    (b)一致しなかった場合は、Drop します。

# 第 14 章　rip mode

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**router rip**
nxrg240(config-router)#

◆ **network**

<説　　明> RIP を有効にするネットワークおよびインタフェースを設定します。
<書　　式> network A.B.C.D/M : IP prefix <network>/<length>, e.g., 35.0.0.0/8
network ethernet <0-2> (|vid <1-4094>)
network ppp <0-4>
network tunnel <0-255>
< no > no network A.B.C.D/M : IP prefix <network>/<length>, e.g., 35.0.0.0/8
no network ethernet <0-2> (|vid <1-4094>)
no network ppp <0-4>
no network tunnel <0-255>

◆ **redistribute**

<説　　明> 経路の再配信を有効にします。
<書　　式> redistribute (static|connected|ospf|bgp) (|metric <metric:0-16>|route-mapACL-NAME)
< no > no redistribute (static|connected|ospf|bgp) (|metric <metric:0-16>|route-mapACL-NAME)

◆ **distribute-list**

<説　　明> route-map を適用します。
<書　　式> distribute-list ACL-NAME (in|out) (ethernet <0-4>|ppp <0-4>|tunnel <0-255>)
< no > no distribute-list ACL-NAME distribute-list ACL-NAME (in|out) (ethernet<0-4>|ppp <0-4>|tunnel <0-255>)

◆ **distance**

<説　　明> RIP と OSPF を併用していて全く同じ経路を学習した場合に、この値の小さい方を経路として採用します。
<書　　式> distance <1-255>
< no > no distance

◆ **timers basic**

<説　　明> RIP タイマーを設定します。
<書　　式> timers basic <update:5-2147483647> <timeout:5-2147483647><garbage:5-2147483647>
<初 期 値> update: 30sec, timeout: 180sec, garbage: 120sec
< no > no timers basic (=timers basic 30 180 120)(= set defaults)

◆ **passive-interface**

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

◆ **default-information originate**

<説　　明> デフォルトルート情報の配信を有効にします。
<書　　式> default-information originate
< no > no default-information originate

◆ **version**

<説　　明> RIP バージョンを設定します。
<書　　式> version <1-2>
<初 期 値> version 2
< no > no version (|<1-2>)

# 第 15 章　ospf mode

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**router ospf**
nxrg240(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

◆ **area virtual-link**

<説　　明> バーチャルリンクを設定します。
<書　　式> area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
{authentication (message-digest|null)
| authentication-key LINE
| dead-interval <1-65535>
| hello-interval <1-65535>
| message-digest-key <1-255> md5 LINE
| retransmit-interval <1-65535>
| transmit-delay <1-65535>}
< no > no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
{authentication (message-digest|null)
| authentication-key LINE
| dead-interval <1-65535>
| hello-interval <1-65535>
| message-digest-key <1-255> md5 LINE
| retransmit-interval <1-65535>
| transmit-delay <1-65535>}

◆ **redistribute**

<説　　明> 経路の再配信を設定します。
<書　　式>
redistribute (connected|static|rip|bgp)
redistribute (connected|static|rip|bgp) (|metric<0-16777214>) [|metric-type (1|2)
|route-map WORD|tag <0-4294967295>]
< no >
no redistribute (connected|static|rip|bgp)
no redistribute (connected|static|rip|bgp) (|metric<0-16777214>)
[|metric-type (1|2) |route-map WORD|tag <0-4294967295>]

◆ **distribute-list**

<説　　明> route-map を適用します。
<書　　式> distribute-list ACL-NAME out (static|connected|rip|bgp)
< no > no distribute-list ACL-NAME out (static|connected|rip|bgp)

◆ **distance**

<説　　明> OSPF と他のダイナミックルーティング併用時に、同じサブネットを学習した場合、この値の小さい方のダイナミックルートを経路として採用します。

<書　　式> distance <1-255>
distance ospf (intra-area <1-255>|inter-area <1-255>|external <1-255>)

< no > no distance <1-255>
no distance ospf

◆ **tiemrs spf**

<説　　明> OSPF SPF timers を設定します。

<書　　式> timers spf <delay:0-4294967295> <hold_time:0-4294967295>
<delay:0-4294967295> : Delay between receiving a change to SPF calculation
<hold_time:0-4294967295> : Hold time between consecutive SPF calculations

< no > no timers spf : Set defaults

◆ **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)|route-mapACL-NAME|always)

< no >
no default-information originate
no default-information originate (metric <0-16777214> |metric-type (1|2)|route-mapACL-NAME|always)

◆ **auto-cost**

<説　　明> コスト計算時の基準となる帯域値(単位:Mbps)を設定します。
<書　　式> auto-cost reference-bandwidth <1-4294967>
<　no　　> no auto-cost reference-bandwidth
<備　　考>

- OSPF のコストは、[コスト=100(Mbps)/帯域幅(Mbps)]によって算出されます。Default の基準帯域幅は、100Mbps です。
- 上記の計算式に従うと、100Mbps の回線では「1」、1Gbps の回線でも「1」(小数点以下は切り上げるため、「0.1」ではありません)となり、1Gbps 以上の回線では、正しいコスト計算が出来ません。
- 基準帯域幅を変更することによって、ギガビットイーサネットでの回線コストを適切に計算することが出来るようになります。
- インタフェースの帯域幅は、インタフェース毎に bandwidth コマンドで設定します。

◆ **router-id**

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

◆ **max-concurrent-dd**

<説　　明> 同時に DD 交換可能なネイバー数の上限を設定することが出来ます。
<書　　式> max-concurrent-dd <1-65535>
<　no　　> no max-concurrent-dd

# 第 16 章　bgp mode

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**router bgp <1-65535>**
nxrg240(config-router)#

**◆ network**

<説　　明> ネットワークアドレスを設定します。
<書　　式> network A.B.C.D/M (|backdoor)
<　no　　> no network A.B.C.D/M (|backdoor)
<備　　考>
・ 特定の BGP 経路を優先経路にしたくない場合、受け取った BGP 経路にローカル BGP の administrativedistance 値を設定することで優先順位を下げ、他の経路を優先させることができます。

**◆ aggregate-address**

<説　　明>
・ Aggregate 機能を使うと、BGP 経路の集約を行うことが出来る集約経路を構成する経路が、BGP テーブル内に少なくとも一つでも存在する場合に、集約経路を作成し advertise します。
<書　　式> aggregate-address A.B.C.D/M (|summary-only|as-set)
<　no　　> no aggregate-address A.B.C.D/M (|summary-only|as-set)
<備　　考>
・ Aggregate 機能では、集約経路と一緒に集約前の経路も advertise します。集約経路のみ advertise する場合は summary-only 設定を有効にします。
・ 経路の aggregate 設定を行った場合、AS パス情報が失われます。これによって、同じ AS に新しい経路として受け取られてしまい、ルーティングループを引き起こす可能性があります。As-set 機能を有効にすると、経路集約時に AS セット情報を含む形で広告することが可能になります。なお、この場合の AS セット集合は、順序不同でリストされたものです。

**◆ distance**

<説　　明> BGP に関する Administrative Distance 値を設定します。
<書　　式> distance bgp <eBPG:1-255> <iBGP:1-255> <local:1-255>
<　no　　> no distance bgp
<備　　考> 初期値は 20(eBGP)、200(iBPG)、200(local)です。

**◆ timers**

<説　　明> jitter の範囲を % で指定することができます。
<書　　式> timers bgp jitter <75-100>
<　no　　> no timers bgp jitter
<備　　考> Default は、75% です。
本設定で設定した jitter は、keepalive の interval にのみ影響します。keepaliveinterval 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>
・ 通常、異なる AS を生成元とする経路については、MED 値を比較しませんが、always-compared-med 機能を有効にした場合、異なる AS を生成元とする経路についても MED 値を比較します。
<書　　式> bgp always-compare-med
<　no　> no bgp always-compare-med

○ bestpath as-path
<説　　明>
・ 通過した AS 番号のリストを示す属性が AS-PATH 属性です。UPDATE message が AS を通過するたびに、AS-PATH リストの順に追加されます。
・ 通常、best path を選択する際、AS-PATH の短いものを優先的に選択します。本機能を設定した場合は、best path 選択時に、AS-PATH 属性を無視します。
<書　　式> bgp bestpath as-path ignore
<　no　> no bgp bestpath as-path ignore

○ bestpath med
<説　　明> MED 値のない prefix に対して、MED 最大値の 4294967294 が割り当てられます。
<書　　式> bgp bestpath med missing-as-worst
<　no　> no bgp bestpath med missing-as-worst

○ local-preference
<説　　明>
・ ルータ自身に設定される値で、AS 内に複数経路を持つような場合、どの経路を優先するかを示す属性が local preference 属性です。
<書　　式> bgp default local-preference <0-4294967295>
<　no　> no bgp default local-preference
<備　　考> iBGP peer 間でのみ交換される値で、値の大きい方が優先されます。
Default 値は 100 です。

○ default-information-check
<説　　明> default route 情報を保持している場合にのみ、BGP4 にて default route 情報を広告する機能です。
<書　　式> bgp default-information-check
<　no　> no bgp default-information-check
<初 期 値> no bgp default-information-check
<備　　考> 本機能が有効な場合、下記のいずれかの方法によって default route 情報を BGP へインストールする必要があります。
(1) redistribute 設定により default route 情報をインストールする。
(2) network 設定により 0.0.0.0/0 をインストールする。

○ enforce-first-as
<説　　明> UPDATE に含まれる AS シーケンスの中の最初の AS が neighbor の AS でない場合に、notification メッセージを送信して、neighbor とのセッションをクローズします。
<書　　式> bgp enforce-first-as
<　no　> no bgp enforce-first-as

○ network import-check
<説　　明>
・ BGP で advertise される network は、通常、生成元となる router がその network を知らない場合も advertise されます。知らない network を BGP で advertise したくない場合には、import-check 機能を有効にすることによって、advertise されなくなります。
<書　　式> bgp network import-check
<　no　　> no bgp network import-check

○ router-id
<説　　明> Router-ID を IP アドレス形式で設定します。
<書　　式> bgp router-id A.B.C.D
<　no　　> no bgp router-id
<備　　考>
・ Router-ID が指定されていない場合、本装置が保持している IPv4 address の中でもっとも大きい IPv4 アドレスを Router-ID として使用します。

○ scan-time
<説　　明> BGP で学習した route の next-hop が到達可能かどうかをスキャンします。
<書　　式> bgp scan-time <0-60>
<　no　　> no bgp scan-time
<備　　考> 初期値は 60(秒)です。

## ■ neighbor

○ default-originate
<説　　明> デフォルトルートを配信する場合に設定します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) default-originate
<　no　> no neighbor (A.B.C.D|X:X::X:X) default-originate

○ distribute-list
<説　　明> peer に送信 / 受信する route update の filtering を行う場合に設定します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) distribute-list ACL-NAME (in|out)
<　no　> no neighbor (A.B.C.D|X:X::X:X) distribute-list ACL-NAME (in|out)
<備　　考> Neighbor 毎に IN/OUT それぞれ1つの distribute-list を設定することができます。

○ ebgp-multihop
<説　　明> peer と直接接続されていない場合でも、eBGP Peer を確立することができます。
<書　　式> neighbor (A.B.C.D|X:X::X:X) ebgp-multihop <1-255>
<　no　> no neighbor (A.B.C.D|X:X::X:X) ebgp-multihop <1-255>
<備　　考> 到達可能なホップ数を設定します。

○ filter-list
<説　　明> BGP のフィルタを設定します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) filter-list ACL-NAME (in|out)
<　no　> no neighbor (A.B.C.D|X:X::X:X) filter-list ACL-NAME (in|out)
<備　　考> global 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|X:X::X:X) next-hop-self
<　no　> no neighbor (A.B.C.D|X:X::X:X) next-hop-self

○ remote-as
<説　　明> 対向装置の AS 番号を設定します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) remote-as <1-65535>
<　no　> no neighbor (A.B.C.D|X:X::X:X) remote-as <1-65535>

○ remove-private-as
<説　　明> Outbound update からプライベート AS を削除します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) remove-private-as
<　no　> no neighbor (A.B.C.D|X:X::X:X) remove-private-as

○ route-map
<説　　明> Peer に送信 / 受信する route の filtering や属性の操作をすることが出来ます。
<書　　式> neighbor (A.B.C.D|X:X::X:X) route-map WORD (in|out)
<　no　> no neighbor (A.B.C.D|X:X::X:X) route-map WORD (in|out)
<備　　考> neighbor 毎に IN/OUT それぞれ1つの routemap を適用することができます。

○ soft-reconfiguration
<説　　明> Neighbor との BGP session をクリアせずに変更を適用したい場合に使用します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) soft-reconfiguration inbound
<　no　> no neighbor (A.B.C.D|X:X::X:X) soft-reconfiguration inbound
<備　　考> BGP の neighbor parameter や routemap の設定を変更した場合、その変更を適用するためには BGP session の clear もしくは、BGP service の再起動が必要となります。

○ keepalive interval & holdtime
<説　　明> keepalive の送信間隔と holdtime を設定します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) timers <keepalive:0-65535><holdtime:0|3-65535>
<　no　> no neighbor (A.B.C.D|X:X::X:X) timers
<初 期 値> neighbor (A.B.C.D|X:X::X:X) timers 60 180
<備　　考>
・ Peer から hold time がタイムアウトする前に、keepalive message か update message を受信しなかった場合、peer との session は close され IDLE 状態へと遷移します。
・ Keepalive を 0sec に設定した場合、keepalive message は送信されません。
・ Keepalive interval には、jitter が設けられています。USER により jitter 幅の下限を、75-100% の範囲で指定することができます。default では、jitter が 75% に設定されているため、keepaliveinterval x (75-100)% で interval が決定されます。jitter の設定については、timers bgp jitter を参照してください。

○ connect timer
<説　　明> Connect timer を設定します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) timers connect <0-65535>
<　no　> no neighbor (A.B.C.D|X:X::X:X) timers connect
<初 期 値> neighbor (A.B.C.D|X:X::X:X) timers connect 120
<備　　考> 0 を設定すると、毎秒 connect しようとします。

○ update-source
<説　　明> BGP パケットのソースアドレスを、指定したインタフェースの IP アドレスに変更します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) update-source
(ethernet<0-2>|loopback<0-9>|ppp<0-4>|tunnel<0-255>)
<　no　> no neighbor (A.B.C.D|X:X::X:X) update-source

○ advertisement-interval
<説　　明>
・ BGP の経路テーブルの変化を監視するタイマで、UPDATE メッセージの最小送信間隔になります。常に周期的に動作するタイマで、前回の UPDATE 送信から経路情報に変化があった場合や、neighbor から ROUTEREFRESH を受信した場合には、タイマ満了時に neighbor へ UPDATE メッセージを送信します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) advertisement-interval <1-600>
<　no　　> no neighbor (A.B.C.D|X:X::X:X) advertisement-interval
<備　　考> タイマのデフォルト値は、eBGP が 30(秒)、iBGP が 5(秒)です。

○ as-origination-interval
<説　　明>
・ 本装置を起源とする BGP 経路の変化を監視するタイマです。BGP ネットワークの追加や filter の適用、redistribute ルートの変更など、内部の BGP 経路情報の変化を周期的に監視します。前回のタイマ満了時からの変化を検出した場合、次の advertisement-interval タイマ満了時に UPDATE メッセージで advertise します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) as-origination-interval <1-600>
<　no　　> no neighbor (A.B.C.D|X:X::X:X) as-origination-interval
<備　　考> タイマのデフォルト値は、15(秒)です。

○ activate
<説　　明>
・ 本機能を有効(activate)にすると、ipv4 neighbor 間 /ipv6 neighbor 間で、ipv4 network を advertise します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) activate
<　no　　> no neighbor (A.B.C.D|X:X::X:X) activate

○ interface
<説　　明>
・ Peer のアドレスとして LLA を指定した場合に、BGP パケットを出力するインタフェースを指定します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) interface IFNAME
<　no　　> no neighbor (A.B.C.D|X:X::X:X) interface IFNAME
<備　　考>
・ Ethernet/VLAN のみ対応しています。
・ update-source と併用する場合は、本設定と同じインタフェースの指定を推奨します。異なるインタフェースを指定した場合の動作については、サポートしていません。

○ netevent
<説　　明>
・ 当該 track が down 状態へと遷移した場合は、当該 neighbor に関する BGP ルートを無効にします。また、当該 track が up 状態へと遷移した場合は、BGP ルートを有効にします。
<書　　式> neighbor (A.B.C.D|X:X::X:X) netevent <1-255> route-disable
　　neighbor (A.B.C.D|X:X::X:X) netevent <2048-4095> route-disable
<　no　　> no neighbor (A.B.C.D|X:X::X:X) netevent

◎ UPDATE の送信プロセス

Neighbor への UPDATE メッセージの送信プロセスは、advertisement-interval と as-originationinterval の 2 つのタイマによって支配されます。

- 自身を起源とするルート

  as-origination-interval の周期で配信ルート情報を監視します。ルート情報に変化があった場合、UPDATE 送信ルート候補となり、次の advertisement-interval の周期で UPDATE 送信します。

- 他の peer から受信した BGP ルート

  他の peer からの UPDATE 受信時に、それ以外の peer への UPDATE 送信ルート候補となり、次の advertisement-interval の周期で UPDATE 送信します。

- soft out リセット実行時

  現在保持する全ての BGP ルートが UPDATE 送信ルート候補となり、次の advertisement-interval の周期で UPDATE 送信します。

## ■ redistribute

○ redistribute (connected|static|rip|ospf)
<説　　明> RIP や OSPF で学習した route や、connected route、static route を BGP で再配信する機能です。Default ルート情報も再配信されます。
<書　　式> redistribute (connected|static|rip|ospf)
<　no　> no redistribute (connected|static|rip|ospf)

○ redistribute (connected|static|rip|ospf) route-map ABCD
<説　　明> routemap 機能を適用することにより、再配信時に特定の prefix のみを配信したり、特定の prefix を拒否したりすることができます。
<書　　式> redistribute (connected|static|rip|ospf) route-map ABCD
<　no　> no redistribute (connected|static|rip|ospf) route-map ABCD

## ■ netevent

○ advertise-stop
<説　　明>
・ 当該 track が down 状態へと遷移した場合は、network 設定によって設定されている BGP ルートの配信を停止します。また、当該 track が up 状態へと遷移した場合は、BGP ルートの配信を再開します。
<書　　式> netevent <1-255> advertise-stop
netevent <2048-4095> advertise-stop
<　no　> no netevent
<備　　考>
・ BGP4 の network import-check が有効な場合、track が up 状態であっても無効なルートは配信しません。

## ■ default

○ ipv4-unicast
<説　　明> 当該 neighbor 上で、交換する address family のデフォルトを IPv4 に設定します。
<書　　式> bgp default ipv4-unicast
<　no　> no bgp default ipv4-unicast

○ local-preference
<説　　明> local preference 値を設定します。
有効の場合、local-preference を、設定値で advertise します。
無効の場合、local-preference を「100」で advertise します。
<書　　式> bgp default local-preference <0-4294967295>
<　no　> no bgp default local-preference
<備　　考> local preference 値の一番大きいパスを優先します。

◎ BGP recursive route

- BGP で学習した route の nexthop に直接接続できない場合でも、static route によって nexthop への到達が確認できた場合、当該 route は有効になります。static route 以外では、nexthop の解決は行いません。
- recursive static route を設定する場合は、nexthop のみを指定します。出力インタフェースは、nexthop から取得します。インタフェースを指定した場合は、recursive route にはなりません。
- recursive route を、static route の nexthop 解決の route として、使用することは出来ません。

# 第 17 章　ntp mode

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#ntp
nxrg240(ntp-config)#

◆ **service**

<説　　明> NTP サービスを有効にします。
<書　　式> service enable　　（有効）
<　no　　> no service enable　　（無効）

◆ **server**

<説　　明> NTP サーバの設定を行います。
<書　　式> server (A.B.C.D|FQDN|X:X::X:X) polling min<4-16> max<5-17>
<初 期 値> no server
<　no　　> no server (A.B.C.D|FQDN|X:X::X:X)
<備　　考>

- NTP サーバは、2 つまで設定することが出来ます。
- サーバを設定しない場合は、ローカルサーバとして動作します。本装置がローカルサーバとして動作する場合、strantum level は「10」です。
- NTP サーバアドレスは、IPv4/IPv6/FQDN による指定が可能です。
- 外部参照する NTP サーバが指定されている場合、時刻同期のために定期的に polling を行います。NTP の通信量を減らすために polling 間隔を大きくしたり、精度を上げるために polling 間隔を小さくしたりすることが出来ます。Polling 間隔の default 値は、最小 6(2 の 6 乗 =64 秒)、最大 10(2 の 10 乗=1024 秒)です。最小値は、必ず最大値より小さい値になるように設定してください。
- system clock mobile(global mode)を設定している場合、当該コマンドの設定は出来ません。
  nxr(config-ntp)#server A.B.C.D polling 4 17
  % System clock is already configured.

◆ **timeout**

<説　　明> NTP サーバからの応答タイムアウト時間を設定することが出来ます。
<書　　式> timeout <seconds:1-30>
<初 期 値> timeout 30
<　no　　> no timeout (=timeout 30)
<説　　明>

- NTP サーバからのサンプリングを 4 回行うため、実際のタイムアウト時間は、timeout × 4 秒です。

◆ **master**

<説　　明> 本装置をローカルサーバとして設定した場合の stratum level を設定します。
　　初期値は「10」です。
<書　　式> master <1-15>
<初 期 値> master 10
<　no　> no master

◆ **disable**

<説　　明> IPv4 または IPv6 での時刻同期を無効にします。
<書　　式> disable ip|ipv6
<　no　> no disable
<備　　考> ip を指定した場合、本装置は IPv4 NTP サーバ／クライアントとして動作しません。
　　ipv6 を指定した場合、本装置は IPv6 NTP サーバ／クライアントとして動作しません。

# 第 18 章　SNMP mode

## SNMP(Simple Network Management Protocol)機能

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

### ■ SNMP version と access 制御

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

### ■ SNMP Trap

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

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

### ■ System Group MIB(MIB-II)設定

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

- sysContact
- sysName
- sysLocation
- sysDescr

なお、sysObjectID には、century にて定義した機器毎の OID が設定されていて機種の判定をすることができます。また、sysUpTime アクセス時には、本装置が起動してからの経過時間を返します。(NTP などによる時刻変更の影響は受けません)。

**■ 対応 MIB 一覧**

本装置にて対応する MIB は次のとおりです。

・Standard

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

・Private MIB

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

**■ デバイス情報**

USB ポートに装着したデバイスの情報を SNMP で取得することが出来ます。また、デバイスを装着あるいは取外した場合は、トラップを送信します。

以下に、取得可能な情報やトラップ情報の例を示します。詳細については、CS-NXR-PRODUCT-MIB を参照してください。

○デバイス情報の取得

- USB ポートに装着したデバイスの情報を SNMP で取得することが出来ます。未対応のデバイスが装着されている場合は、unknown と表示されます。
- モバイルデータ通信端末では、シグナル状態(up/down)を取得することが出来ます。USB メモリの場合は、シグナル状態は notSupport となります。また、モバイルデータ通信端末が PPP 接続中の場合は、シグナル状態は notAccessible となります。

○トラップの送信

- USB ポートにデバイスを装着または取外した場合に、トラップ(up/down)を送信します。ただし、未対応のデバイスの場合は、トラップを送信しません。
- モバイルデータ通信端末では、シグナル状態が 0 以下(error を含む)となった場合に down トラップを送信します。また、シグナル状態が 1 以上となった場合に up トラップを送信します。
- モバイルデータ通信端末モジュールをリセットした場合は、down->up のトラップを送信します。

**■ SNMP NAT**

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

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#snmp
nxrg240(snmp-config)#

◆ **security**

<説　　明> SNMP マネージャを使いたいネットワーク範囲を指定します。
<書　　式> security A.B.C.D/M|X:X::X:X/M COMMUNITY
<初 期 値> no security
<備　　考> Network は、3 つまで設定することが出来ます。
<　no　> no security (A.B.C.D/M|X:X::X:X/M)

◆ **syslocation**

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

◆ **syscontact**

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

◆ **sysname**

<説　　明> sysName を設定します。
<書　　式> sysname SYSNAME
<初 期 値> no sysname [= 機種名(ex. NXR-G240)]
<　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-G240 Series ver 9.0.0 (build 30/17:18 11 11 2016)

◆ 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) (|port <1-65535>)
　　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。
　　宛先ポート番号を指定することが出来ます。

◆ trap agent

<説　　明>
・ TRAP パケット中の Agent Address を、IP アドレスまたはインタフェースにて指定することが出来ます。
<書　　式> trap agent ip A.B.C.D
　　trap agent interface ethernet <0-2>
<初 期 値> no trap agent
<　no　> no trap agent
<備　　考>
・ インタフェースを指定した場合、当該インタフェースのプライマリー IP アドレスを使用します。
・ 指定した IP アドレスが、リンクダウン等の理由で使用不可の場合、他のインタフェース(ethernet0→ ethernet1 → ethernet2...)のアドレスを使用します。

◆ bind address

<説　　明> TRAP 送信時のソースアドレス(IPv4 アドレスのみ対応)を指定することが出来ます。
<書　　式> bind address A.B.C.D
　　bind address X:X::X:X
<初 期 値> no bind address
<　no　> no bind address
<備　　考>
・ 指定したアドレスを持つインタフェースが、リンクダウンの状態であっても、当該アドレスをソースアドレスとして使用します。
・ 本設定時に、該当アドレスを保持していない場合は、外部からの SNMP アクセスが出来なくなります。また、その後 IP アドレスを設定しても、自動的に復旧しないため、restart snmp などの操作が必要になります。
・ 例えば、IPsec policy にマッチせずに、SNMP パケットがドロップされてしまうようなケースで、本設定によるソースアドレスを指定することによって、IPsec tunnel 経由での SNMP 通信が可能になります。

◆ snmpv3 engine-id
<説　　明> snmpv3 engine-id を設定します。
<書　　式> snmpv3 engine-id WORD
<　no　　> no snmpv3 engine-id

◆ snmpv3 access
<説　　明>
・ ユーザからの SNMPv3 アクセスに、セキュリティ(認証の有無／暗号化の有無)を設定します。
<書　　式> snmpv3 access (noauth|auth|priv) user <1-5>
<　no　　> no snmpv3 snmpv3 access (noauth|auth|priv) user <1-5>
<備　　考> noauth 認証なしユーザから、SNMPv3 アクセスすることが出来ます。
auth 認証あり・暗号化なしユーザから、SNMPv3 アクセスすることが出来ます。
priv 認証あり・暗号化ありユーザから、SNMPv3 アクセスすることが出来ます。

◆ snmpv3 trap
<書　　式> snmpv3 trap host (A.B.C.D|X:X::X:X) (noauth|auth|priv) user <1-5>
<　no　　> no snmpv3 trap host (A.B.C.D|X:X::X:X)
<備　　考> trap noauth 認証なしユーザで、SNMPv3 trap を送信します。
trap auth 認証あり・暗号化なしユーザで、SNMPv3 trap を送信します。
trap priv 認証あり・暗号化ありユーザで、SNMPv3 trap を送信します。

◆ snmpv3 usm
<説　　明> user mode に移行します。
<書　　式> snmpv3 usm user <1-5>
<備　　考> nxr160(config-snmp)#snmpv3 usm user 1
nxr160(config-snmpv3-user)#

◆ name
<説　　明> (user mode で)user name を設定します。
<書　　式>　name WORD

◆ auth
<説　　明> (user mode で)認証方式およびパスワードを設定します。
<書　　式> auth (md5|sha) password (|hidden) WORD
auth (md5|sha) password encrypted WORD
<　no　　> no auth

◆ priv
<説　　明> (user mode で)暗号化方式およびパスワードを設定します。
<書　　式> priv (des|aes) (|password (|hidden) WORD)
priv (des|aes) (|password encrypted WORD)
<　no　　> no priv

◆ ifindex persist
<説　　明> 本機能を有効にすることで、ifindex を固定することが出来ます。
<書　　式> ifindex persist
<　no　　> no ifindex persist
<初 期 値> no ifindex persist

# 第 19 章　syslog mode

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**syslog**
nxrg240(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。
- syslog サーバは、5 つまで設定することができます。
- syslog 送信時の送信元アドレスを設定することができます。
- リモートサーバへ syslog を転送する際の UDP port 番号(default:514)を指定することが出来ます。

<書　　式>
server (A.B.C.D|X:X::X:X|FQDN)
server (A.B.C.D)| X:X::X:X | FQDN) source (A.B.C.D|X:X::X:X)
server (A.B.C.D | X:X::X:X | FQDN) port <1024-65535>
server (A.B.C.D)| X:X::X:X | FQDN) port <1024-65535> source (A.B.C.D|X:X::X:X)

<　no　　> no server (A.B.C.D|X:X::X:X|FQDN) (= syslog サーバに転送しません)
<備　　考>
- syslog サーバへの転送が失敗した場合は、再送キューに蓄積し、60 秒後に再送します。以降、60 秒毎に再送を試行し、syslog サーバへの転送が成功すると、再送キューをクリアします。
- この場合のタイムスタンプは、サーバへの送信時刻ではなく、最初に syslog を送信しようとした際の時刻になります。
- 蓄積可能なメッセージキューの長さは、1000 件です。

◆ **mark**

<説　　明> Syslog mark の設定をします。
　　Mark の出力間隔を 0 ～ 10080 分の範囲で指定することができます。
　　Default は 20 分毎とし、0 を指定した場合、mark は出力されません。
<書　　式> mark <min:0-10080>
<初 期 値> mark 20
<　no　> no mark (=mark 20)
<備　　考> mark 0 (mark は出力しません)

◆ **priority**

<説　　明> Syslog のプライオリティを設定することができます。
<書　　式> priority (debug|info|notice)
<初 期 値> priority info
<　no　> no priority
<備　　考> facility は、指定することができません。

◆ **system**

<説　　明>
- System Message 出力機能とは、Connection tracking 数、Load Average、メモリ使用量、温度状態などのシステムの情報を、mark 出力時または、一定時間毎に syslog 上に出力させる機能です。
- システム内の情報であるため、外部 remote server へ出力することは推奨しません。

<書　　式> system 5min　: 5 分毎にメッセージを出力します。
　　system 30min : 30 分毎にメッセージを出力します。
　　system hour　: 1 時間毎にメッセージを出力します。
　　system mark : Output messages with mark
<初 期 値> no system
<　no　> no system : System メッセージ出力しない

◆ **suppress**

<説　　明>
- 同じ message が繰り返し表示される場合、毎回表示せずに、その message が何回繰り返して出力されたかどうかのみを表示する機能です。

<書　　式> suppress <10-3600>
<初 期 値> no suppress
<　no　> no suppress
<備　　考>
- Suppress する時間を 10-3600sec の間で指定することができます。
- last message が繰り返し出力された場合、suppress message として表示されます。
- Default では、suppress は無効です。

◆ **mail send**

<説　　明> syslog メッセージをメール送信します。

・ USER が指定した文字列を含む message が syslog へ出力された場合、設定された E-mail address に mail を送信する機能です。この機能により、CLI への login 失敗時などの不正アクセスがあった場合に、管理者に mail を送るようなことが可能になります。

・ 指定した文字列が含まれるかどうかを、60sec 毎に check し、該当する文字列が存在した場合に mail 送信します。なお、mail 送信機能については、IPv4/IPv6 の両方をサポートします。

<書　　式> mail send enable
<初 期 値> no mail send
<　no　> no mail send

◆ **mail to**

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

◆ **mail from**

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

◆ **mail subject**

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

◆ **mail strings**

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

◆ **mail server authentication**

<説　　明> メールサーバの認証方法を設定します。
<書　　式> mail server authentication pop-before-smtp POP before SMTP
　　mail server authentication smtp-auth-login SMTP authentication (login)
　　mail server authentication smtp-auth-plain SMTP authentication (plain)
<　no　> no mail server authentication

◆ **mail server address**

<説　　明> POP3 サーバのアドレスを設定します。
<書　　式> mail server address A.B.C.D
　　mail server address FQDN

◆ **mail server smtp**

<説　　明> SMTP サーバのアドレスおよびポート番号を設定します。
<書　　式> mail server smtp address A.B.C.D
　　mail server smtp address FQDN
　　mail server smtp port <1-65535>

◆ **mail server username**

<説　　明> SMTP サーバのユーザ ID とパスワードを設定します。
<書　　式> mail server username USERNAME password (|hidden) PASSWORD

◆ **rotate**

<説　　明>
○ Default の動作では、syslog message の容量が最大許容量の 80% を超えると、後方の 4000 行を残して削除します。システム起動時より、10 分周期で自動的にチェックします。
○ 上記動作とは別に、syslog rotate 機能を設定することが出来ます。
・ Rotate 設定を行うと、syslog のサイズが閾値を超えていた場合に、指定された storage 上に backup を行います(閾値を指定しない場合は、サイズに関係なく backup を行います)。
・ Schedule 機能によって rotate の指示を行うため、rotate を有効にし、かつ schedule 機能で実行日時を指定する必要があります。
・ Default では、rotate は無効です。

<書　　式>
　rotate (disk0|disk1|flash1|cms)
　rotate (disk0|disk1|flash1|cms) threshold logsize <kbytes:150-4000>
　rotate (disk0|disk1|flash1|cms) threshold files <files:1-32>
　rotate (disk0|disk1|flash1|cms) threshold logsize <kbytes:150-4000> files <files:1-32>
<初 期 値> no rotate
<　no　> no rotate
<備　　考>
・ USB0 に接続された USB Flash メモリを指定する場合は、disk0 を選択します。USB1 に接続された USBFlash メモリを指定する場合は、disk1 を選択します。内蔵 Flash を指定する場合は、flash1 を指定します。
・ 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。backup file 数の default 値は、5(files)です。
・ なお、backup された syslog message は、gzip にて圧縮されます。また、下記フォーマットの file 名になります。なお、Backup 先に同じ名前の file が存在した場合、上書きされます。
・ backup ファイル名の format：YYYYMMDD_HHMM.log.gz
・ 2010 年 11 月 2 日 19 時 50 分に取得した backup ファイルの例：20101102_1950.log.gz
・ cms を指定した場合、rotate した syslog を CMS に送信します。

◆ **auto-rotate**

<説　　明>
・ firmware update や restart によるシステム再起動時に、syslog のバックアップを取得する機能です。
<書　　式> auto-rotate enable
<初 期 値> auto-rotate enable
<　no　　> no auto-rotate enable
<備　　考>
・ syslog メッセージのサイズに関係なく、バックアップを取得します。threshold の logsize は無視しますが、files は指定値に従います。
・ Default で、本機能は有効です。ただし、rotate（disk0|disk1）の設定がない場合、syslog のバックアップは行いません。
・ ファイル名は、次のようになります。
　backup ファイル名の format : YYYYMMDD_HHMM_restart.log.gz
　2010 年 11 月 2 日 19 時 50 分に取得した backup ファイルの例 : 20101102_1950_restart.log.gz

**■ フィルタログ機能**

パケットが、IPv4 ACL、IPv6 ACL、SPI フィルタにマッチした場合、syslog に出力することが出来ます。

**□ フィルタログ出力レート制限**

・ ログ出力有効時、当該フィルタに大量のパケットがマッチすると、ログ出力にシステムリソースを消費してしまい、サービス停止(DoS 攻撃)状態になる可能性が考えられます。
・ この対策として、ログ出力のレート(packets/sec)を制限することが出来ます。
・ なお、レート制限以下の場合でも、システムの負荷状況等により、ログ出力しない場合があります。
また、制限を設けていても、通信環境によっては、ログが大量発生し、ログ容量が大きくなる場合があります。このため、ログの管理には、十分に注意するようにしてください。

● SPI フィルタログ

・ 1 秒間に出力可能なログ数を設定することが出来ます。Default は「10」です。
・ WAN 側からの意図しないパケットが、SPI フィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分な注意が必要です。
・ 設定については、ip spi-filter log/ipv6 spi-filter log コマンドを参照してください。

●フィルタログ

・ 1 秒間に出力可能な log 数の最大値は「10」です。
・ すべての ACL にログを設定すると、システムが高負荷状態になる可能性があるため、ログ出力は最小限にとどめるようにしてください。
・ 設定については、ip access-list/ipv6 access-list コマンドを参照してください。

● P2P 検出ログ

・ 1 秒間に出力可能なログ数の最大値は、winny/share 検出の場合「10」、bittorrent の場合「5」です。

■ **net-ratelimit 機能**

- システムからログを出力する際、パケット毎にログを出力すると、システムに非常に負荷がかかり、DoS（DDoS）攻撃 etc によってサービス停止状態になる可能性があります。そのため、単位時間当たりに出力可能なログの数を制限しています。
  - 5 秒間に出力可能なログの数は、最大 10 です（設定の変更は出来ません）。
  - 出力できなかったログは、その後のログ出力時に、supress message 数としてログ出力します。
  - 具体的には、以下のログの出力レートを制限します。
    - ip martian-log 機能によるログの出力
    - L2TPv3 からのエラーログ（Error:Unknown session SESSION_ID）の出力

# 第 20 章　dhcp-server mode

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**dhcp-server <1-64>**
nxrg240(dhcps-config)#

◆ **network**

<説　　明> DHCP サーバを動作させるネットワークを指定します。
<書　　式> network A.B.C.D/M range <starting IP: E.F.G.H> <ending IP: I.J.K.L>
<　no　　> no network A.B.C.D/M range <starting IP: E.F.G.H> <ending IP: I.J.K.L>
<備　　考> 最大 16 個設定することができます。複数の場合、network を同一にしてください。

◆ **lease-time**

<説　　明> IP アドレスのリース時間を設定します。
<書　　式> lease-time <default:60-15552000> <max:60-15552000>
<初 期 値> lease-time 21600 43200
<　no　　> no lease-time (=lease-time 21600 43200)

◆ **gateway**

<説　　明> DHCP クライアントのデフォルトゲートウェイとなる IP アドレスを指定します。
<書　　式> gateway A.B.C.D
<初 期 値> no gateway
<　no　　> no gateway

◆ **domain**

<説　　明> DHCP クライアントに割り当てるドメイン名を指定します。
<書　　式> domain DOMAIN
<初 期 値> no domain
<　no　　> no domain

◆ **dns-server**

<説　　明> DHCP クライアントに割り当てる DNS サーバアドレスを指定します。
<書　　式> dns-server <primary DNS: A.B.C.D>
　　dns-server <primary DNS: A.B.C.D> <secondary DNS: A.B.C.D>
<初 期 値> no dns-server
<　no　　> no dns-server
<備　　考> プライマリー DNS とセカンダリー DNS を設定することが出来ます。

◆ **netbios-server**
<説　　明> NetBIOS サーバの IP アドレスを設定します。
<書　　式> netbios <primary NetBIOS: A.B.C.D>
　　netbios <primary NetBIOS: A.B.C.D> <secondary NetBIOS: A.B.C.D>
<初 期 値> no netbios-server
<　no　> no netbios-server（= Delete）
<備　　考> プライマリーとセカンダリーを設定することが出来ます。

◆ **netbios-scope-id**
<説　　明> NetBIOS スコープ ID を配布できます。
<書　　式> netbios-scope-id SCOPED-ID
<初 期 値> no netbios-scope-id
<　no　> no netbios-scope-id

◆ **sip-server**
<説　　明> DHCP client からの SIP server 要求に対して、SIP server address を割り当てます。
<書　　式> sip-server A.B.C.D (|A.B.C.D)
　　sip-server FQDN (|FQDN)
<初 期 値> no sip-server
<　no　> no sip-server
<備　　考> IPv4 address または FQDN を最大 2 つまで設定することができます。

◆ **RFC2131 compatibility broadcast bit**
<説　　明>
・ DHCP server の動作を RFC2131 に準拠させるかどうかを指定する機能です。RFC2131 では broadcast bit が 1 である DHCP packet 受信時、応答の MAC address を broadcast(FF:FF:FF:FF:FF:FF)で送信するべきと記されています。
・ このオプションを無効にすると、broadcast bit の値によらず、DHCP packet の応答を常に unicast frame(但し、destination IP address は、オプションが有効な場合と同様 limited broadcast)として送信します。
・ このオプションは、default で有効です。
<書　　式> rfc2131-compatibility broadcast-bit enable
<初 期 値> rfc2131-compatibility broadcast-bit enable
<　no　> no rfc2131-compatibility broadcast-bit enable

◆ **vendor-specific-information**
<説　　明> option 43 (Vendor-Specific Information) を要求したクライアントに対し、
　　ここで設定した値を option 43 として返送します。
<書　　式> vendor-specific-information {text WORD|hex HEX|ip A.B.C.D|space WORD}
<　no　> no vendor-specific-information
<備　　考> space: dhcp-server option-space で定義した space 名を指定します。
　　クライアントが option 60 を送信している場合は、その値に応じて
　　dhcp-server vendor-class の設定が適用されます。

◆ **vendor-class-identifier**
<説　　明> DHCP サーバが送信する option 60 (Vendor Class Identifier) の値を設定します。
<書　　式> vendor-class-identifier {text WORD|hex HEX}
<　no　> no vendor-class-identifier
<備　　考> クライアントの option 60 による振り分けには、
　　dhcp-server vendor-class の identifier を使用します。

# 第 21 章　dhcp-relay mode

**DHCPv4 リレー機能**

DHCPv4 リレー機能は、LAN 側より受信したブロードキャスト宛ての DHCP パケットを、PPP やトンネルインタフェースに対してユニキャストパケットとして転送する機能です。リレーの際の出力先インタフェースについては、ルーティングテーブルに依存します。

ユニキャストパケットとして転送する際、DHCP パケットの giaddr フィールドに、DHCP パケットを受信したインタフェースの IPv4 アドレスを設定します。DHCP サーバは、giaddr の情報を元にして、クライアントに割り当てるネットワークのアドレスを決定します。

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**dhcp-relay**
nxrg240(dhcpr-config)#

**◆ address**

<説　　明> BOOTP Request パケットの転送先となる上位 DHCP サーバの IP アドレスを指定します。
<書　　式> address A.B.C.D
<初 期 値> no address
<　no　　> no address A.B.C.D
<備　　考> 上位 DHCP サーバは、4 つまで設定することができます。

**◆ accept**

<説　　明>
- DHCP サーバ機能と同時に運用する場合を考慮し、クライアントからの BOOTP Request パケットを受信するインタフェースを指定することが出来ます。

<書　　式> accept ethernet <0-2>
<　no　　> no accept ethernet <0-2>
<備　　考>
- 指定外のインタフェースで受信した BOOTP Request パケットは DROP します。
- Ethernet インタフェースのみ指定することが出来ます。指定しない場合は、どの Ethernet インタフェースで受信した場合でもリレーします。

# 第 22 章　ipsec local policy mode

### ◆ 移行 command

nxrg240(config)#ipsec local policy <policy:1-255>
nxrg240(config-ipsec-local)#

### ◆ address

<説　　明> IPsec tunnel のソース IP を指定します。
<書　　式> address ip (|A.B.C.D)
　　address ipv6 (|X:X::X:X)
<備　　考>
・ IPv6 アドレスを指定する場合
　指定した IPv6 アドレスが存在しない(使用できない)場合は、当該 IPsec 設定は使用できません。
・ IPv6 アドレスを指定しない場合
　(IPsec policy XX でマッピングした)インタフェース上の IPv6 アドレスを、本装置が自動的に選択します。

### ◆ self-identity

<説　　明> 本装置の ID を設定します。
<書　　式> self-identity fqdn FQDN　　(例: centurysys.co.jp)
　　self-identity user-fqdn USER@FQDN　　(例: user@centurysys.co.jp)
　　self-identity dn DN　　(備考を参照してください)
　　self-identity key KEY-ID　　(KEY ID を指定します。)
<初 期 値> no self-identity
<　no　> no self-identity
<備　　考>
・ DN を指定した場合に使用する文字列の例です。
　C=JP,ST=Tokyo,O=century,OU=dev,CN=nxr1.centurysys.co.jp,E=admin@centurysys.co.jp

### ◆ x509 certificate

<説　　明> X.509 証明書を設定します。
<書　　式> x509 certificate CERTIFICATE　　(証明書の設定)
<　no　> no x509 certificate　　(証明書のクリア)

**■動的 IP アドレス環境下での接続について**

**□動的 IP アドレスのクライアントからの接続**

IKEv1 main モードでは、相手を識別する ID の交換を、phase1 の最後に行いますが、情報が暗号化されているため、PSK 認証方式利用時には、ID と PSK を結び付けて認証処理を行うことが出来ません。したがって、PSK と相手を結び付けるキーには、IP アドレスを使用します。

しかしながら、リモートアクセスのように接続毎に IP アドレスが変化する環境下では、responder 側で事前に相手 ID（IP アドレス）と PSK を結び付けることが出来ません。そのため、動的 IP アドレスからの接続を受け付けるには、以下のいずれかの方法を用いて設定を行う必要があります。

- Aggressive モードを使用する
- Main モードで、すべての通信相手との間で同一 PSK を使用する

（デジタル署名方式では、PSK を検索する必要がないため、上記のような制限はありません。）

※リモートアクセス環境下では、PSK/RSA の認証に加えて、可能な限り xauth の使用を推奨しています。

※ IKEv2 では、ID によって対向 SG を識別することが出来るため、動的 IP 環境下であっても、対向毎に異なる PSK を設定して PSK 認証を行うことが出来ます。

**□動的 IP アドレス環境下での PSK 認証による接続**

自分が動的 IP アドレスの場合、事前に IP アドレスと PSK との関連付けが出来ないため、IP アドレス以外の識別子を ID として指定することになります。しかしながら、ID を設定できない、あるいは ID を設定すると aggressive モードで動作するクライアントが存在するため、相互接続性が悪いという問題が存在します。

この対応として、本装置では、IP アドレスを自分 ID として利用することで、動的 IP 環境下での PSK 認証を可能にしています（ID(IP アドレス)と PSK の関連付けは、IP アドレスが割り当てられた時点で行います）。

これにより、センター機器が、動的 IP であっても、DDNS を利用することで、PSK 認証を行うことが出来ます。

# 第 23 章　ipsec isakmp policy mode

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**ipsec isakmp policy <policy:1-65535>**
nxrg240(config-ipsec-isakmp)#

◆ **description**

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

◆ **version**

<説　　明> IKE のバージョン(IKEv1/IKEv2)を指定します。
<書　　式> version (1|2)
<初 期 値> version 1
<備　　考>
・ IPsec ISAKMP policy 毎に指定することができます(IKEv1 と IKEv2 を同時に使用することができます)。

■ **IKE のパラメータ折衝**

□ IKEv1
・ 本装置が responder になる場合、本装置の設定には依存せず、initiator が送ってきたものの中から、transform playload に設定された順番に、採用可能かどうかを判断して選択します。
・ ただし、セキュリティ強度の観点から、暗号化アルゴリズムのプロポーザルとして DES が指定されてきた場合は、本装置側でも暗号化アルゴリズムとして DES を設定している場合のみ受け付けます。

□ IKEv2
・ 本装置が responder になる場合、設定した transform セット(暗号化方式や hash アルゴリズム)と一致しない場合は接続を拒否します。

◆ **hash**

<説　　明> ハッシュアルゴリズムを設定します。
<書　　式> hash (md5|sha1|sha256|sha384|sha512)
<初 期 値> hash sha1

◆ **encryption**

<説　　明> 暗号化アルゴリズムを設定します。
<書　　式> encryption (aes128|aes192|aes256|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|18|19|20|21|25|26)
<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 を削除します。
<書　　式> lifetime <121-86400>
<初 期 値> lifetime 10800 (=3 hours)
<　no　> no lifetime (=lifetime 10800)

◆ **isakmp-mode**

<説　　明> Phase1 のネゴシエーションモードを設定します。
<書　　式> isakmp-mode (main|aggressive)

◆ **authentication pre-share**

<説　　明> PSK 認証を使用します。
<書　　式> authentication pre-share KEY
<備　　考>
・ KEY は、1-128 文字以内で設定してください。
使用可能な文字は、英数字[a-z,A-Z,0-9]および!$#&=*+-_.:;(){}[]/^~@`<> です。

◆ **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 AAAAAAAAAAAAAAAAAA
```

◆ **xauth**

<説　　明> xauth を使用します。
<書　　式> xauth mode client USERID
xauth mode server
< no > no xauth
<備　　考> USERID は、ipsec xauth(global mode 参照)で設定した username に一致させます。
userid と password は、ipsec xauth(global mode 参照)で設定します。

■ **authentication local/remote (IKEv2 のみ)**

○ local

<説　　明> IKEv2 で、自分が使用する認証方式を指定します。

<書　　式> authentication local pre-share WORD
authentication local rsa-sig
authentication local eap-md5

○ remote

<説　　明> IKEv2 で、対向が使用する認証方式を指定します。

<書　　式> authentication remote pre-share (|WORD)
authentication remote rsa-sig
authentication remote eap-md5
authentication remote eap-radius
authentication remote eap-mschapv2

< no > no authentication remote

<備　　考>

・ IKEv2 では、次の例のように自分が使用する認証方式と対向が使用する認証方式が異なっていても構いません。
自分 authentication local eap-md5
authentication remote rsa-sig
対向 authentication local rsa-sig
authentication remote eap-md5

・ pre-share の設定例 1: 1 対 1 接続の場合
自分 authentication remote pre-share WORD
authentication local pre-share WORD
対向 authentication remote pre-share WORD
authentication local pre-share WORD

・ pre-share の設定例 2: 1 対多接続(対向が動的 IP で複数台)の場合
自分 ipsec pre-share identity fqdn NXR1 password WORD1
ipsec pre-share identity fqdn NXR2 password WORD2
!
ipsec isakmp policy 1
authentication remote pre-share
authentication local pre-share WORD
remote address ip any
…省略…
!
対向 1 authentication remote pre-share WORD
authentication local pre-share WORD1
対向 2 authentication remote pre-share WORD
authentication local pre-share WORD2

・ 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…
!
```

・ 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…
!
```

◆ **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。

◆ **keepalive**

<説　　明> IPsec keepalive(DPD:RFC3706)を設定します。
<書　　式> keepalive periodic (|clear|hold|restart)
　　keepalive <interval:10-3600> <retry:0-60> periodic (|clear|hold|restart)
<初 期 値> keepalive 30 3 periodic restart
<　no　> no keepalive
<備　考 1>

- DPD は、SG(Security Gateway)の down や SG 間の IP reachability、および IKE SA の状態監視を目的としています。DPD で、IPsec SA の状態を監視することは出来ません。
- keepalive が有効でも、SG 間で IPsec パケットの通信がある間は、DPD パケットを送信しません。
- no keepalive を設定すると、DPD パケットを送信しません。ただし、対向 SG からの DPD パケットには応答します。
- keepalive 10 3 periodic を設定した場合、10 秒間隔で合計 4 回の R-U-THERE メッセージを送信します。R-U-THERE-ACK メッセージを 1 回も受信しない場合にエラーと判定します。

<備　考 2>

- DPD でエラーを検出した場合、IKE/IPsec(CHILD) SA および IPsec policy を削除します。その後の動作は、DPD エラー時のアクション設定(clear, hold, restart)に依存します。
  - ○ clear
    SA および policy の削除後は、ユーザの指示を待ちます。
  - ○ hold
    SA の削除後は、policy のみが有効になります。policy にマッチするパケットを受信すると IKEphase1 (version2 の場合は、IKE SA INIT)ネゴシエーションを開始します。ただし、ipsec tunnel policy で、negotiation-mode=responder に設定している場合は、IKE ネゴシエーションしません。
  - ○ restart
    SA および policy の削除後に、IKE phase1(version2 の場合は、IKE SA INIT)を開始します。ただし、ipsec tunnel policy で、negotiation-mode=responder に設定している場合は、IKE ネゴシエーションしません。

<備　考 3>

- DPD エラーとなった IKE に、backup policy を指定している場合は、backup policy のネゴシエーションを開始します(backup policy を指定していない場合は、backup 動作は実施しません)。
- backup policy を指定している場合でも、当該 backup policy の negotiation-mode が responder の場合は、ネゴシエーションを開始しません。

◆ **backup policy**

<説　　明> IPsec isakmp の backup policy を設定します。
<書　　式> backup policy <1-65535>
<初 期 値> no backup policy
<　no　> no backup policy
<備　　考> backup policy は、ISAKMP 毎に設定します。

◆ **rekey**

<説　　明>
- Rekey の soft timer は、margin と increased-ratio により決定されます。
- Margin は、lifetime が切れる何秒前から rekey を実行するかどうかを指定します。
- increased-ratio 値は、margin よりどれぐらい増やすかを % で指定します。

<書　　式> rekey margin <30-360> (increased-ratio <0-100>|)
<初 期 値> no rekey margin
<備　　考>
- 以下の式によって、Soft timer の最小・最大が決定され、この間でランダムに Soft timer が設定されます。
  minimum soft timer = lifetime - margin
  maximum soft timer = lifetime - (margin + margin x increased-ratio/100)
- default 値は、margin が 270sec、increased-ratio は 100% です。このため、lifetime から 270 ～ 540sec 前の時間がランダムで設定されます。但し、Responder の場合、soft timer は、margin/2 時間分早く設定されます。これは、initiator 側より rekey を行うようにするためです。
- increased-ratio を 0 に設定すると soft timer が毎回同じ値となります。負荷の分散やセキュリティ的に問題があるため、設定しないことを推奨します。
- negotiation-mode が responder の場合、当該機器からは rekey を実行しません。

◆ **remote address**

<説　　明> 対向の IP/IPv6 アドレス、または FQDN を設定します。
<書　　式> remote address ip (A.B.C.D|any|FQDN)
　　remote address ipv6 (X:X::X:X|any|FQDN)

◆ **remote identity**

<説　　明> 対向の ID を設定します。
<書　　式> remote identity fqdn FQDN (例: centurysys.co.jp)
　　remote identity user-fqdn USER@FQDN (例: user@centurysys.co.jp)
　　remote identity dn DN (備考を参照してください)
　　remote identity key KEY-ID (KEY ID を指定します。)
<初 期 値> no remote identity
<　no　> no remote identity
<備　　考>
- peer identity 未設定時は、IP/IPv6 アドレスを ID として使用します。
- DN を指定する場合の文字列の例です。
  C=JP,ST=Tokyo,O=century,OU=dev,CN=nxr1.centurysys.co.jp,E=admin@centurysys.co.jp
- DN を指定する場合、次のように RDN にて ”*” を使用することが出来ます。
  C=JP,ST=Tokyo,CN=*
- ただし、C=JP,ST=Tokyo,CN=*.centurysys.co.jp のように、一部に * を指定することはできません。

**■ FQDN 対応(SG が動的 IP の場合)**

リモート SG が動的 IP のため、固定 IP を指定出来ない場合は、FQDN を指定します。
(IKEv1 のみ対応しています。IKEv2 では未対応です。)

○本装置が initiator として動作
対向アドレスが FQDN 指定の場合は、DNS によって名前解決を行い、当該 IP アドレスに対して IKE パケットを送信します。

○本装置が responder として動作
main モードで PSK 認証を行う場合、remote address ip any を設定します。
※ main モードの PSK 認証の際、IP アドレスで PSK の検索を行うためです。対向の設定が FQDN 指定だけの場合は、PSK が見付からずに認証エラーとなります。

◎ main モード＋ PSK 認証における responder 側での設定
remote address ip any (必ず設定します)
remote address ip FQDN (必要ならば設定します)
※ FQDN と any で、同一 PSK を使用するようにしてください。

- Aggressive モードや main モードで X.509 を使用する場合、あるいは、main モード(PSK 認証)で initiator 動作のみの場合は、FQDN 指定だけでも接続可能です。
- いずれの場合においても、ネゴシエーションパケットの source アドレスから、逆引き(あるいは正引き)による FQDN のチェックは行いません。
  (逆引きは別のドメイン名が設定されているケースが多く、設定数が多い場合は高負荷になるためです。)

**□ FQDN 指定の際の ID**

対向アドレスを FQDN 指定する場合、名前解決後の IP アドレスを ID として認証を行います。
※別途 ID を指定している場合は、当該 ID を使用します。

**□ FQDN 指定の制限事項**

- Main モード(PSK 認証)で、対向を FQDN 指定している場合、対向からのネゴシエーションを受信しても、PSK が見付からないため接続に失敗します(responder としての動作)。
- Main モードでは、PSK を検索する段階では、まだ ID が分からないため、IP アドレスによる検索を行いますが、対向が FQDN 指定の場合は、受信した IKE パケットの source アドレスと PSK を関連付ける情報がないため、PSK が見付からず接続に失敗します。
- このような場合に、main モードで接続するには、対向を FQDN ではなく、any として指定します。
  ※ main モードで対向を FQDN 指定すると、initiator 動作のみ対応することになります。
  しかしながら、上記のような制限を抱えたまま、main モードを使用するよりも、aggressive モードや X.509 認証の使用を推奨します。

### ◆ local policy

<説　　明> 使用するローカルポリシーを選択します。
<書　　式> local policy <1-255>

### ◆ local policy (change action)

<説　　明>
・ IPsec isakmp で使用する local policy の track 状態(up/down)によって、action を実行する機能です。
・ この機能により、障害に応じて、1 つの IPsec 設定にて main/backup の構成を取ることができます。
<書　　式>
local policy <policy:1-255> netevent <trackid:1-255> change <local policy:1-255>
local policy <policy:1-255> netevent <trackid:2048-4095> change <local policy:1-255>
<備　　考>
・ PSK を使用している場合、変更前の local policy の ID と変更後の local policy の ID は、同じ ID を使用してください。たとえば、下記のような change action を設定する場合は、local policy 1 と local policy 2 の self-identity を同じ ID にしてください。

```
!
ipsec isakmp policy 1
 local policy 1 netevent 1 change 2
!
ipsec local policy 1
 self-identity fqdn myid  ←同じ ID
!
ipsec local policy 2
 self-identity fqdn myid  ←同じ ID
!
```

・ action 追加時の動作: track object の状態が down の場合 action が実行されます。
・ action 削除時の動作: netevent がない場合と同じ動作が実行されます。Action 復旧処理が行われるわけではありません。

### ◆ eap-identity

<説　　明> EAP 認証で使用する ID を設定します。
<書　　式> eap-identity (WORD|any)
<　no　　> no eap-identity
<備　　考> 設定例は、authentication local/remote を参照してください。

### ◆ netevent

<説　　明> イベント発生時に、IKE 単位で IPsec トンネルの確立、削除を実行します。
<書　　式> netevent <trackid:1-255> (connect|disconnect|reconnect)
netevent <trackid:2048-4095> (connect|disconnect|reconnect)
<　no　　> no netevent

◆ initial-contact-ignore
<説　　明> initial-contact-ignore が enable の場合、INITIAL_CONTACT を受信しても、
　　既存の SA 削除を実行しません。
<書　　式> initial-contact-ignore enable
<　no　> no initial-contact-ignore enable

◆ force-encapsulation
<説　　明>
・ 本機能を有効にすると、NAT 環境下以外でも、IKE/ESP パケットを UDP encapsulation します。
・ IKEv2 で使用することが出来ます。
<書　　式> force-encapsulation enable
<初 期 値> no force-encapsulation enable
<　no　> no force-encapsulation enable

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

◆ client configuration mode
<説　　明>
・ mode-config によるネットワーク情報割り当て時のモードとして、initiate/respond を指定します。
<書　　式> client configuration mode (initiate|respond)
<初 期 値> client configuration mode respond
<　no　> no client configuration mode
<備　　考>
・ initiate を指定した場合、イニシエータとして動作します。
・ respond を指定した場合、レスポンダーとして動作します(VPN client からのリクエスト待ち状態となります)。
・ IKEv2 の場合、mode 設定に関係なく、常に respond として動作します。

◆ client configuration address-pool
<説　　明> mode-config で使用する address-pool を指定します。
<書　　式> client configuration address-pool local WORD
<　no　> no client configuration address-pool
<備　　考> address-pool は、ipsec local pool コマンド(global mode)にて設定します。
　　本設定があると、mode-config が有効になります。

◆ remote udp port
<説　　明> IKE パケットの宛先 UDP ポート番号を指定することが出来ます。
<書　　式> remote udp port <1-65535>
<初 期 値> remote udp port 500
<　no　> no remote udp port <1-65535>

◆ udp port
<説　　明> IKEv2 パケットの送信 UDP ポート番号を指定することが出来ます。
<書　　式> udp port 4500
<初 期 値> udp port 500
<　no　> no udp port
<備　　考> 現状、指定可能な port 番号は、4500 です。

# 第 24 章　ipsec tunnel policy mode

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**ipsec tunnel policy <policy:1-65535>**
nxrg240(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> ESP の暗号化アルゴリズムと認証アルゴリズムを指定します。
<書　　式>
　　set transform
　　(esp-3des|esp-des|esp-null|
　　esp-aes128|esp-aes128-ctr|esp-aes128-gcm-16|
　　esp-aes192|esp-aes192-ctr|esp-aes192-gcm-16|
　　esp-aes256|esp-aes256-ctr|esp-aes256-gcm-16)
　　(esn|esp-aesxcbc|esp-md5-hmac|
　　esp-sha1-hmac|esp-sha256-hmac|esp-sha384-hmac|esp-sha512-hmac)
<初 期 値> set transform esp-aes128 esp-sha1-hmac
<備　　考> hash を指定しない場合は、ESP の認証機能は無効となります。
　　認証機能を無効にした場合は、replay 防御 window 機能も無効になります。
　　esp-null を指定した場合は、認証機能は無効にできません。
　　Default では、ESN(Extended Sequence Number)は無効です。
　　ESN を有効にする場合は、暗号化方式(および Hash)も指定します。

**◆ set pfs**

<説　　明> PFS を設定します。
<書　　式> set pfs
　　(|group1|group2|group5|phase1|group14|group15|group16|group17
　　|group18|group19|group20|group21|group25|group26)
<初 期 値> set pfs phase1
　　・ IKEv1 の場合、phase1 と同じ DH group を使用します。
　　・ IKEv2 の場合、PFS 機能は無効となります(未指定扱い)。
<　no　> no set pfs (= PFS 無効)

◆ **set anti-replay-check**

<説　　明> replay 防御 window 機能の有効 / 無効を設定します。
<書　　式> set anti-replay-check
<初 期 値> set anti-replay-check
<　no　　> no set anti-replay-check

◆ **set key-exchange**

<説　　明> 使用する ISAKMP ポリシーを指定します。
<書　　式> set key-exchange isakmp <1-65535>

◆ **set protocol-mode**

<説　　明>
・ 本装置では、tunnel モードと transport モードの両方のモードをサポートします。
・ IPv6 利用時は、IPv6 LLA を使用した IPsec tunnel/tranport mode を確立することはできません。
・ サポートするトンネリング形式は、IPv4 over IPv4、IPv4 over IPv6、IPv6 over IPv6、IPv6 over IPv4 です。

<書　　式> set protocol-mode (tunnel|tranport)
<初 期 値> set protocol-mode tunnel
<備　　考>

※ Transport モードと NAT-Traversal の併用

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

・ 接続時の制限

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

・ TCP/UDP チェックサム

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

◆ **set esp-sha256-hmac trunc-length**

<説　　明> SHA256-HMAC の認証サイズを設定します。
<書　　式> set esp-sha256-hmac trunc-length (96|128)
<　no　　> no set esp-sha256-hmac trunc-length
<初 期 値> set esp-sha256-hmac trunc-length 128
<備　　考> 本設定は、IKEv1 利用時のみ適用されます。初期値は「128」です。
　　Android6 以降の製品と接続する場合に「trunc-length 96」を指定します。

◆ **set key-exchange (change action)**

<説　　明>

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

<書　　式>

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

<備　　考>

・ action 追加時の動作: track object の状態が down の場合 action が実行されます。
・ action 削除時の動作: netevent がない場合と同じ動作が実行されます。Action 復旧処理が行われるわけではありません。

◆ **set sa lifetime**

<説　　明>

IPsec SA のライフタイム(Hard Timer)を設定します。この時間を経過すると SA が削除されます。

<書　　式> set sa lifetime <121-86400>
<初 期 値> set sa lifetime 3600
<　no　　> no set sa lifetime　　(= set as lifetime 3600)

◆ **negotiation-mode**

<説　　明> IPsec policy のネゴシエーションモードを指定します。
<書　　式> negotiation-mode (auto|on-demand|manual|responder)

| | |
|---|---|
| auto | IPsec service 起動時に negotiation が開始されます。IKEv2 の場合、認証エラーや TS(トラフィックセレクタ)の不一致などのエラーが発生した場合、60sec 後に再度 initiate が開始されます。 |
| manual | IPsec service 起動時に negotiation は開始されず tunnel が追加されるのみです。Backup policy などで使用します。 |
| on-demand | IPsec service 起動時に route のみが設定されます。 |
| responder | IPsec service 起動時の動作は、manual と同様です。但し、常に responder となるため、こちらからいかなる場合(rekey 含む)においても initiate することはありません。 |

<初 期 値> negotiation-mode auto

◆ **clone**

<説　　明>
- ある IPsec tunnel policy と同じ policy をもつ ipsec tunnel policy を設定します。
- 本機能は、main/backup で同じような設定(IPsec の冗長化を行う際、通常 main/backup では同じ policy を持ちます)を行う手間を省きたい場合に使用します。
- route based IPsec では、1 つの tunnel interface を main/backup で使用することができます。本機能を使用すると、main/backup それぞれの tunnel に対して、同じ static や nat/filter の設定をする必要がなくなり、管理者の負担を軽減することができます。

<書　　式> clone <1-65535>
<　no　　> no clone
<備　　考> 以下は、本機能により copy されない項目(個別に設定が必要な項目)です。
- tunnel number
- priority
- description
- negotiation-mode
- shutdown
- key-exchange

◆ **shutdown**

<説　　明> IPsec トンネルポリシーを無効にします。
<書　　式> shutdown
<　no　　> no shutdown

◆ **set route**

<説　　明> Destination Prefix をルーティングテーブルに追加します。
<書　　式> set route
<　no　　> no set route　　（= Disable）

◆ **set priority**

<説　　明> ポリシーのプライオリティを設定します。
<書　　式> set priority <1-255>
<初 期 値> set priority 1
<　no　　> no set priority　　（初期値）

## ■ match

### ○ address

<説　　明> IPsec tunnel に適用する IPsec ACL を指定します。
<書　　式> match address IPSEC-ACL-NAME (|nat-traversal)
<備　　考> IPsec ACL は、global mode の ipsec access-list コマンドで設定します。

### ○ protocol

<説　　明> smartphone と L2TPoverIPsec で接続する際に設定します。
　　match address とは、排他設定です。
<書　　式> match protocol l2tp-smartphone (|nat-traversal)
<備　　考>

◎ L2TP over IPsec (l2tp smartphone mode)
smartphone との間で L2TPv2 over IPsec を確立する際に使用します。本機能を有効にすると、下記の設定が有効になります。

□ IPsec パラメータの自動設定
IPsec 接続を行う際に、下記のパラメータを自動設定します。

- protocol-mode → transport
- negotiation-mode → responder
- IPsec selector → 以下のように自動設定します。また、NAT-Traversal 有効時は、NAT 配下のどのアドレスからの接続も受け付けます。

| ID PayLoad | NXR 側 | smartphone 側 |
|---|---|---|
| IPv4 アドレス | host | host |
| プロトコル | UDP | UDP |
| ポート番号 | 1701 | any(どのポートでも受け付ける) |

# 第 25 章　UPnP mode

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**upnp**
nxrg240(upnp-config)#

■ **UPnP**

○ service
<説　　明> サービスを起動します。
<書　　式> service enable

○ external interface
<説　　明> WAM 側インタフェースを設定します。
INTERFACE は ethernet, vlan, ppp, bridge 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 interface bridge <0-4095>

○ external port-reserve
<説　　明> ある WAN ポートについて、ポートマッピングを許可したくない場合は、予約ポート設定を行います(UPnP の割り当てを禁止するポート番号を設定します)。
予約ポート番号は、TCP/UDP 共通で単一ポートまたは範囲を指定します。最大 64 組まで設定することができます。
<書　　式> external port-reserve <1-65535> (|<1-65535>)
<　no　> no external port-reserve <1-65535> (|<1-65535>)

○ external well-known
<説　　明> well-known port(1-1023)への UPnP の割り当てを許可します。
<書　　式> external well-known port enable
<　no　> no external well-known port enable

○ listen
<説　　明> LAN 配下の機器からの UPnP メッセージを listen する IP アドレスを設定します。
<書　　式> listen ip A.B.C.D/M
<　no　> no listen ip A.B.C.D/M
<備　　考> 最大 2 つまで設定可能

○ timeout
<説　　明> UPnP 機能使用時の無通信切断タイマーを設定します。
<書　　式> timeout <sec:60-21474836>
<初 期 値> no timeout　　(= timout 600)

# 第 26 章　QoS (class-policy) mode

## ■ QoS

本装置のソフトウェアにてサポートする各 queuing 方式について記します。packet coloring 以外は、すべて egress interface のみで使用することが出来ます。

1. PFIFO(Packet FIFO)

・ PFIFO では、輻輳状態になった場合に、すぐにパケットを破棄せず、キューに貯めておきます(キューの最大容量を超えたパケットは破棄します)。パケットが転送可能な状態になると、キューに貯めておいたパケットを(First_In First_Out の)順番に転送します。PFIFO は、優先順位の高いパケットと優先順位の低いパケットを区別しません。

・ インタフェースの default queuing 方式は、PFIFO_FAST と呼ばれるもので、IP ヘッダの ToS フィールドの値に応じて受信パケットを 3 つの queue に振り分けて、優先度の高い queue から優先してパケットを出力します。PFIFO_FAST の設定内容をユーザが変更することは出来ません。

2. TBF(Token Bucket Filtering)

Token Bucket Filtering と呼ばれるアルゴリズムで、shaping 機能を提供します。指定したレートで bucket から token を出力し、その token にパケットを格納します。Token がない場合は、パケットを出力しません。

Classless queuing 方式のため、特定のトラフィック class のみに適用させることはできません。特定のトラフィック class に対して shaping を適用する場合は、HTB や PQ のような class full queuing と併用して使用することができます。ただし、HTB には shaping 機能があるため、各 class で TBF を適用すると CPU 使用率の増加や遅延の増大を招く恐れがあります。したがって、HTB との併用は望ましくありません。

キャリアサービスにおいて、契約した回線帯域により料金が異なるようなサービスを使用した場合、ルータで shaping する際に、パケットサイズや FCS や IFG、PA を除いたフレームサイズでレート計算を行ないます。この場合、shaping rate としては問題ないようでも、Ethernet フレームとして実際に回線を流れる際は、FCS や IFG+PA が追加されるため、回線側でフレーム drop が発生することがあります。
このような場合の対応として、Ethernet インタフェース上での設定に限り、shaping レートの計算時に、ifg(inter-frame-gap の最小サイズ 12byte で計算)、fcs(4byte)、pa(preamble:8byte)をフレームサイズ に加えることができます。これにより、回線サービス上での帯域超過によるフレーム drop を回避することが可能となります。Default では、IFG、PA、FCS 分のサイズは考慮しません(設定は、interfacemode の ifg-pa-fcs を参照してください)。

3. SFQ (Stochastic Fair Queuing)

各パケットをすべて公平に扱う queuing 方式です。Flow 毎に計算されたハッシュ値によって各 bucket にパケットを振り分けます。SFQ には 127 パケットの queue があり、送信(active)となった bucket に対して queue を割り当てます。

Flow は、IP source/destination address、protocol 番号によって区別します(IPv4 の場合)。また、SFQqueue の深さは 127 で、ハッシュテーブルのサイズは 1024 です(ユーザが設定を変更することは出来ません)。

帯域の小さい回線で使用することで、帯域を平等に使用することが出来ます(ある特定の flow のみが帯域を占有することはありません)。しかし、interactive なセッションがある場合は、遅延が大きくなってしまうことがあります。

4. PQ (Priority Queuing)

High/medium/normal/low の 4 つの class の queue を持ちます。

High priority の queue にパケットがある場合は、medium/normal/low の queue からパケットが出力されることはありません。

Class 数は 4 つ(固定)で、class に割り当てる traffic はユーザが指定することが出来ます。各 class の default queuing 方式は、PFIFO です。

5. HTB

Class 分けされたトラフィクに予約帯域を割り当て、クラス毎に設定した重みとパケット長に応じてパケットを出力します。

回線帯域に空きがある場合は、予約帯域以上のトラフィックを送信することが可能で、回線を有効に利用することが出来ます。

各 class の default queuing は、PFIFO です。但し、default class の default queuing は、SFQ です。

## 5.1. ceil 帯域の割り当て

HTB では、ceil パラメータにより、他の class が帯域を使用していない場合、その帯域を借りることで設定した rate より高い rate で通信することが出来ます。
その際、複数の class のトラフィックが未使用帯域(余剰帯域)を使用する場合の分配方法について記します。

余剰帯域の比率は、class priority が同じ場合は、quantum というパラメータにより決定します。priority が異なる場合は、高優先の class に対して優先的に帯域を割り当てます。quantum 値は、class に割り当てられた rate 設定値から自動的に算出します(ユーザが、設定することは出来ません)。

quantum = (rate * 1000/8)/r2q

※ r2q は、rate を quantum 値に変換するための係数です。default は、10 です。

Quantum 値の範囲は、1500 ～ 60000 です。そのため、r2q が 10 の場合、rate が 120kbps ～ 4.8Mbps の範囲なら、指定 rate の比率に応じて余剰帯域を割り当てます。一方、rate が 120kbps 以下なら 120kbps と同じ比率、4.8Mbps 以上なら 4.8Mbps と同じ比率で、余剰帯域を割り当てます。
本装置では、class の最高 rate によって r2q の値を変化させます。そのため、設定した class rate によっては、従来の余剰帯域の割り当て比率とは異なる場合があります。
例えば、class の最高 rate を 40Mbps に設定した場合、40Mbps が quantum の最大値(60000)となるように r2q を自動調整します。この場合、余剰比率が rate 比と同じになる minimum rate は

r2q = (40000*1000/8)/60000

min rate = 1500 * 8 /1000 * r2q = 1500 * 40000/60000 = 1000 kbps = 1.0 Mbps

となります。

## 5.2. バーストサイズについて

HTB を設定した場合、指定した帯域幅に基づいてバーストサイズを自動的に算出します。また、ceil も指定した場合は、ceil 値に応じて ceil のバーストサイズを別途算出します。

burst = bandwidth/HZ +1600

cburst = ceil/HZ + 1600

※ NXR-G240 の場合、HZ は 250 です(機器により異なります)。

※ bandwidth/ceil は、設定レートをビットレート(bit rate)からバイトレート(byte rate)に変換した値です。

## 5.3. class priority 機能

HTB で使用する各 class に priority を設定することが出来ます。priority の小さい class をラウンドロビンで優先的に処理します。そのため、VoIP パケットなどの遅延を小さくするには、他の class より小さい priority を設定するようにします。
priority は、1 ～ 7 の範囲で指定することが出来ます。指定がない場合は、本装置が 4 を割り当てます。
なお、priority は leaf class のみで有効です。親 class(parent class)で指定した priority は無視します。

6.　Packet Coloring

ユーザが指定した特定のトラフィックに MARK 値(NXR 内のみ有効な値)や ToS 値の設定を行います。ToS と MARK を同時に設定することも出来ます。Packet coloring された情報により、QoS を適用することができます。トラフィックの識別、および MARK や ToS 値の設定には、route-map 設定を利用します。また、Packet coloring の適用箇所や NAT、packet filtering との適用順番については、付録の Packet Traveling を参照してください。

7.　各 class へのトラフィック割り当てについて

PQ や HTB のような classfull な queuing 方式を使用する際、各 class へトラフィックを割り当てる方法として、MARK 値と ToS 値 /Precedence 値(HTB のみ)による割り当てをサポートします。MARK 値は、NXR 内部でのみ使用される値で Packet coloring 機能によって設定することができます。PQ の各 class への割り当ては MARK のみで、1 つの class へ割り当て可能な条件は 1 つだけです。HTB の各 class への割り当ては、class filter を使用します。Class filter 内においては、match 条件を複数設定することが出来ます。複数条件がある場合、その条件に 1 つでも合致すれば、該当 class へトラフィックが割り当てられれます
(route-map の条件とは異なるので注意してください)。

**◆ 移行 command**

nxrg240#
nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**class policy NAME**
nxrg240(class-policy-config)#

**■ class**

<説　　明> class を設定します。
<書　　式>

○ class+child class
　class <2-254> bandwidth <1-1000000> (|ceil <1-1000000>) queue policy NAME
　class <2-254> bandwidth percent <1-100> (|ceil <1-100>) queue policy NAME

○ class+PQ
　class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
　　queue priority-group <1-255>
　class <2-254> bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>)
　　queue priority-group <1-255>

○ class+fifo
　class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
　　queue fifo (|limit <1-16384>)
　class <2-254> bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>)
　　queue fifo (|limit <1-16384>)

○ class+sfq
　class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>) queue fair-queue
　class <2-254> bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>) queue fair-queue

○ class+tbf
　class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
　　queue shape <RATE:1-1000000> <BUFFER:8-1000000> <LIMIT:1-1000000>
　class <2-254> bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>)
　　queue shape <RATE:1-1000000> <BUFFER:8-1000000> <LIMIT:1-1000000>

○ class+default queue (default queue : fifo)
　class <2-254> bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
　class <2-254> bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>)

○ class 削除
　no class <2-254>
　no class default

○ class default (policy は選択不可)

class default bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
queue (priority-group|shape|fifo|fair-queue)
class default bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>)
queue (priority-group|shape|fifo|fair-queue)

○ default queue (default queue: sfq)

class default bandwidth <1-1000000> (|priority <0-7>) (|ceil <1-1000000>)
class default bandwidth percent <1-100> (|priority <0-7>) (|ceil <1-100>)

<備　考>

- bandwidth <1-1000000> を指定した場合、bandwidth および ceil のレートの単位は kbps です。
- HTB 設定において、bandwidth percent <1-100> を指定した場合、bandwidth および ceil のレートの単位は % です。パーセンテージは、インタフェースで設定した帯域幅に対する絶対比です。また、この場合は、ceil 値もパーセンテージで指定します。
- 下記の例の場合、class 10 の帯域幅は、10000kbps × 10% ＝ 1000kbps になります。

```
!
class policy AAA
 class 10 bandwidth percent 10
!
interface ethernet 1
 queue policy AAA bandwidth 10000
!
```

※小数点以下の端数は、切り捨てます。ただし、1kbps に満たない場合は、1kbps として処理します。

# 第 27 章　QoS (class-filter) mode

**◆ 移行 command**

nxrg240#
nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**class filter <2-254>**
nxrg240(class-filter-config)#

**■ match**

<説　　明> Mark 値、ToS 値、Precedence を設定します。
<備　　考> 複数の match が設定されている場合、or 条件となります。

○ mark
<書　　式> match ip mark <1-4095>
<　no　　> no match ip mark <1-4095>

○ tos
<書　　式> match ip tos <0-255>
<　no　　> no match ip tos <0-255>

○ precedence
<書　　式> match ip precedence <0-7>
<　no　　> no match ip precedence <0-7>

# 第 28 章　CRP client mode

**管理サーバインタフェース**

本装置の設定や状態を管理する管理サーバ(CMS)とのインタフェースについて記します。

**■ CMS と NXR 間のインタフェースプロトコル**

- CMS との情報のやりとりに netconf(RFC4741)を使用し、netconf の転送用プロトコルとしては、SSH (netconf over SSH:RFC4742)を使用します。
- SSH および netconf は、CMS からセッションを開始します。つまり、NXR がサーバ、CMS がクライアントとして動作します。

**■ CMS と NXR 間の SSH 認証**

- CMS->NXR 間の SSH 認証は RSA 認証のみであり、ユーザ名は netconf 固定です。CMS の RSA 公開鍵を、NXR へインポートすることで、SSH 認証が可能となります。RSA 公開鍵は、最大 5 つまでインポートすることが出来ます。設定については、SSH 公開鍵のインポート(view mode)を参照してください。
- config 保存時に、インポートした RSA 公開鍵も本装置の flash に保存されます。
- CMS から NXR への SSH 接続は、インタラクティブではないため、公開鍵のパスフレーズは未入力のものを使用してください。

**CRP**

CRP とは、本装置から管理サーバ(CMS)へ、管理に必要な情報(グローバル IP アドレス等)を登録する際に使用するプロトコルです。CRP は、UDP 上で動作します。また、デフォルトでは 10625 番ポートを使用します。

**■ クライアントモード**

- CRP が本装置で動作する場合は、クライアントモードで動作します。

**■ サーバモード**

- クライアントからの情報を待ち受けるモードです。自発的にクライアント側にパケットを送信するようなことは行いません。CRP が管理サーバ(CMS サーバ)上で動作する場合は、サーバモードで動作します。

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**crp client <1-2>**

○ server address
<説　　明> CRP サーバ(CMS サーバ)の IP アドレスを設定します。
<書　　式> server address (A.B.C.D|X:X::X:X|FQDN)
<　no　> no server address

○ server port
<説　　明> CRP サーバ(CMS サーバ)の待ち受けポート番号を設定します。
<書　　式> server port <udp:1024-65535>
<初 期 値> server port 10625
<　no　> no server port

○ username
<説　　明> CRP クライアントのユーザ ID とパスワードを設定します。
<書　　式> username WORD password (hidden|) WORD
<　no　> no username

○ keepalive
<説　　明> CRP キープアライブの設定を行います。
<書　　式> keepalive (|<300-28800sec>)
<初 期 値> no keepalive
<　no　> no keepalive
<備　　考>

- CRP の登録に成功してから、次に再登録を試行するまでの時間を設定します。インターバル未指定時(keepalive)は、「keepalive 3600」と同義です。
- 無効(no keepalive)の場合は、CRP の再登録を行いません。ただし、IP アドレスの変化や指定インタフェースの up/down、CPE ID および CUSTOMER ID の変更があった場合は、キープアライブが無効でも自動的に CRP の再登録を行います。
- 本装置を NAT 装置の配下で運用する場合は、必ずキープアライブを有効にしてください。
- 本装置がグローバル IP を持つ場合(本装置が NAT 装置の配下にない場合)は、キープアライブが無効でも動作しますが、管理サーバの運用上の万一のトラブルを考慮して、keepalive 3600 を設定することを推奨します。

# 第 29 章　route-map mode

**Route-map**

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、すべての match 条件に合うと、当該アクションを実行します。一方、一つの match 条件に、複数の条件定義がある場合は、どれか 1 つの条件に match した場合にアクションを実行します。なお、本バージョンでは、1 つの match 条件に複数の条件定義を行うことはできません。

**◆ 移行 command**

nxrg240#
nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**route-map NAME (permit|deny) <1-65535>**
nxrg240(config-route-map)#

**■ match**

<説　　明> マッチ条件を設定します。
<備　　考> match がない場合は、すべてが set の対象になります。
deny で match した場合は、set の対象外になります。
各機能でサポートしていない match 条件は無視します。

○ Classify で利用(設定)可能な match 条件
<説　　明>
・ Classify で利用(設定)可能な match 条件は次のとおりです。
・ ip/ipv6 address(class access-list)、ip/ipv6 tos 値、ip/ipv6 mark 値、ip precedence
<書　　式> match ip|ipv6 address ACL
　　match ip|ipv6 tos <0-255>
　　match ip|ipv6 mark <1-4095>
　　match ip precedence <0-7>
<備　　考>
・ 同じ route-map シーケンス内で、match 条件として、ip tos と ip precedence は、同時に指定できません。

○ BGP4 で利用(設定)可能な match 条件
<説　　明>
・ BGP4 で利用(設定)可能な match 条件は、次のとおりです。
・ ip/ipv6 address(ip route access-list のみ)、ip/ipv6 nexthop address、med、as-path、rigin
<書　　式> match ip|ipv6 address ACL-NAME
　　match ip|ipv6 next-hop ACL-NAME
　　match metric <0-4294967295>
　　match as-path ACL-NAME
　　match origin (egp|igp|incomplete)

○ PBR で利用(設定)可能な match 条件
<説　　明> PBR で利用(設定)可能な match 条件は、次のとおりです。
　　IP address(ip policy access-list)
<書　　式> match ip address ACL

○ RIP/OSPF で利用(設定)可能な match 条件

<説　　明> RIP/OSPF で利用(設定)可能な match 条件は、次のとおりです。

<書　　式> match tag (0-4294967295)

○マッチ条件の削除

<説　　明> 設定したマッチ条件を削除します。

<　no　> no match ip [address|tos|mark|precedence|netx-hop(|WORD)]
no match ipv6 [address|tos|mark|next-hop(|WORD]
no match as-path (|WORD)
no match metric (|<0-4294967295>)
no match origin (|egp|igp|incomplete)
no match tag (|<0-4294967295>)

■ **set**

<説　　明> QoS(Classify)、BGP4、PBR で使用する属性を設定します。
ToS と Mark を同時に設定することが出来ます。
各機能でサポートしていない属性の設定は無視します。

○ Classify で利用(設定)可能な属性

<説　　明> Classify で利用(設定)可能な属性は、次のとおりです。
tos 値、mark 値、DSCP 値、ttl 値

<書　　式> set tos <0-255>
set mark <1-4095>
set dscp <0-63>
set ttl (|decr|incr) <1-255>

○ BGP4 で利用(設定)可能な属性

<説　　明>

・ BGP4 にて routemap を使用する場合、以下の属性を設定することができます。
aggregator、as-path、atomic-aggregate、ip nexthop、local-preference、med、origin、ipv6 next hop(local/global)

<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)
set ipv6 next-hop (|local) X:X::X:X

○ PBR で利用(設定)可能な属性

<説　　明>

・ PBR にて routemap を使用する場合、ルーティングエントリー作成時に以下の属性を使用します。
ip next-hop、interface

<書　　式> set ip next-hop A.B.C.D
set interface INTERFACE

<備　　考>

・ 入力および出力インタフェースとして指定可能なインタフェースは、イーサネット /802.1Q VLAN/ ブリッジ(仮想スイッチ)/ トンネル /PPP です。

○ RIP/OSPF で利用(設定)可能な属性

<説　　明> RIP/OSPF にて、routemap を使用する場合、以下の属性を設定することができます。

<書　　式> set tag (0-4294967295)

○セット条件の削除
<説　　明> 設定したセット条件を削除します。
<　no　　> no set aggregator as (|<1-65535>)
no set as-path prepend (|<1-65535>)
no set atomic-aggregate
no set interface
no set ip netx-hop (|A.B.C.D)
no set ipv6 next-hop (|local) (|X:X::X:X)
no set local preference (|<0-4294967295>)
no set mark <1-4095>
no set metric (|<0-4294967295>)
no set origin (|egp|igp|incomplete)
no set tos <0-252>
no set tag (|<0-4294967295>)
no set ttl (|decr|incr) <1-255>

**■ 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 distributelist によるルートフィルタリングにも使用します。

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

○　class access-list
ToS 値や MARK 値を設定する set 条件をフィルタリングする場合

○　ip route access-list
BGP のパス属性に関する set 条件をフィルタリングする場合
BGP で distribute-list によるルートフィルタリングを行う場合

**■ netevent**
<説　　明> Netevent で、PBR route の有効化 / 無効化を行うことが出来ます。
<書　　式> netevent (<1-255>|<2048-4095>) (active|inactive)
<備　　考> active　track down を検出すると、ip route が有効になります。
track up を検出すると、ip route が無効になります。
inactive track down を検出すると、ip route が無効になります。
track up を検出すると、ip route が有効になります。

# 第 30 章　Web Authenticate mode

**Web 認証機能**

Web 認証は packet filter の一種で、認証を通った USER の IP 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 認証による認証可能ホスト数は 1024 です。

**○ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**web-authenticate**
nxrg240(config-webauth)#

**■ 認証方式**

HTTP Basic 認証、外部サーバ連携に対応しています。

○ authenticate
<説　　明> 認証方式を設定します。
<書　　式> authenticate basic (|redirect)
　　authenticate post-ext-html (|redirect)
　　authenticate post-ext-XML (|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。
- 認証を有効にする場合は、HTTP サーバを起動してください。(global mode で、http-server enable を設定します。)
- 外部サーバ連携では、外部サーバから、POST(XML または HTML 形式)による認証データの受信(および認証)を行い、指定した IP アドレスのアクセスを許可することが出来ます。
  (※詳細は、Web authentication extension モードを参照してください。)

**■ 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、外部に接続したいユーザは、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、未認証のユーザ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)
　　monitor port 80 443 (|redirect)
<　no　> no monitor port
<初 期 値> no monitor port
<備　　考>
・ HTTP(TCP 80)と HTTPS(TCP 443)の接続を監視することが出来ます(※ TCP 443 のみを監視することは出来ません)。
　authenticate basic + monitor port 80
　authenticate basic + monitor port 80 443
　　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
　authenticate basic + monitor port 80 443 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
　no authenticate + monitor port 80 443 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。

○ https enable
<説　　明>
・ monitor port 80 443 (|redirect)を設定する場合、本機能(https enable)を有効にします。
<書　　式> https enable
<　no　> no https enable

**■ 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 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。

<書　　式> close session-timeout <60-2592000>

< no > no close

○ 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>
close idle-timeout <60-2592000> 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

■ アカウント管理

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

<書　　式> account authenticate (local|radius|radius-and-local)
<　no　> no account authenticate
<初 期 値> account authenticate local

**■ ローカル認証**

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

<書　　式> account username USERNAME password (|hidden) PASSWORD
<　no　> no account username USERNAME

**■ RADUIS 認証**

RADIUS 認証は PAP 認証によって行われます。RADIUS server への認証要求は、timeout が 5 秒で、最大３回までリトライします。

○ RADUIS サーバ設定

Account 認証を行う RADIUS server の IP address、UDP port 番号、秘密鍵(secret)を設定することができます。UDP port 番号の default は 1645 番です。また、RADIUS server は 2 つまで設定することができます。

<書　　式>
radius (A.B.C.D|X:X::X:X) password (|hidden) PASSWORD (|auth-port <1645|1812|<1024-65535>)
radius (A.B.C.D|X:X::X:X) auth-port (1645|1812|<1024-65535>)
<　no　>
　no radius (A.B.C.D|X:X::X:X) (設定を削除します)
　no radius (A.B.C.D|X:X::X:X) auth-port (auth-port のみを初期値(1645)に戻します)

○ 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

○ 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-ipv6-address X:X::X:X
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
no radius attribute nas-ipv6-address
no radius attribute 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。

○ Session timeout で使用する Attribute の指定

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

<書　　式>
radius session-timeout attribute
(ascend-maximum-time|ascend-maximum-time-vsa|session-timeout)
session-timeout Session-Timeout (Attribute Type=27)
ascend-maximum-time Ascend-Maximum-Time(Attribute Type=194)
ascend-maximum-time-vsa
Ascend-Maximum-Time(Attribute Type=194、VSA Type=26、Vendor-ID=529)

< no > no radius session-timeout attribute

○ 全ての radius 設定を一括削除

全ての radius 設定を一括削除することができます。

<書　　式> no radius

**■ MAC アクセスリスト**

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

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

**■ Web 認証フィルタ**

Web 認証フィルタを設定すると、ある特定の host や network、interface について Web 認証せずに通信が可能となります。Web 認証フィルタの設定条件については、global mode の ip web-auth access-list を参照してください。Web 認証フィルタは、各 interface につき、IN/OUT をそれぞれ一つずつ設定することができます。interface への適用については、ip webauth-filter/ipv6 webauth-filter コマンド(interface/tunnel/ppp/bridge/WWAN mode)を参照してください。

**■ 認証ログの出力**

認証ログ(login success ログ)を syslog に出力します。

<書　　式> log enable
<　no　> no log enable
<初 期 値> no log enable
<備　　考>
- 有効(log enable)時、TCP 80(TCP 443)監視による認証ログ(login success ログ)を syslog に出力します。
- 有効(log enable)時、login.cgi 接続による認証ログ(login success ログ)を syslog に出力します。

**■ 認証 URL 設定**

アクセスする認証 URL を設定することが出来ます。http:// 本装置の IP アドレス / 設定値でアクセスすることが出来ます。

<書　　式> access-path WORD
<　no　> no access-path WORD
<備　　考>
- 本装置の IP アドレスが 192.168.0.254 で、access-path WORD の場合、http://192.168.0.254/WORD でアクセスすることが出来ます。
- 設定値がディレクトリ指定(設定値の終わりが「/」)の場合、そのディレクトリ以降は任意の文字列として扱います。
- 認証 URL を設定した場合でも、元の認証 URL(http:// 本装置の IP アドレス /login.cgi)は有効です (無効にすることは出来ません)。

**■ WISPr 対応**

設定した URL に対して、認証前の端末からのアクセスが行われた場合、HTTP 200 OK を返します。

<書　　式> wispr-success-url WORD (|reply no-content)
<　no　　> no wispr-success-url
<備　　考>
・ WORD には、URL を設定します(例: http://www.centurysys.co.jp)。
・ 設定値がディレクトリ指定(設定値の終わりが「/」)の場合、そのディレクトリ以降は任意の文字列として扱います。
・ 16 個まで設定することが出来ます。

**■ 証明書**

証明書、中間証明書、秘密鍵を設定することが出来ます。未設定の場合は、初期証明書を使用します。
※証明書の設定が正しくない場合、HTTP サービスが起動しないことがあります。

<説　　明> 証明書を設定します。
<書　　式> cert certificate NAME WORD (source A.B.C.D|X:X::X:X)
<　no　　> no cert certificatge NAME

<説　　明> 中間証明書を設定します。
<書　　式> cert chain-certificate NAME WORD (source A.B.C.D|X:X::X:X)
<　no　　> no cert chain-certificatge NAME

<説　　明> 本装置の秘密鍵を設定します。
<書　　式> cert private-key NAME key WORD (source A.B.C.D|X:X::X:X)
<　no　　> no cert private-key NAME key

<説　　明> パスフレーズを設定します。
<書　　式> cert private-key NAME password (|hidden) WORD
<　no　　> no cert private-key NAME password

# 第 31 章　WarpLink mode

**WarpLink クライアント機能**

WarpLink サービスのクライアントとして機能します。つまり、WarpLink Manager に対して、NXR の機器情報を送信します。

**○ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**warplink**
nxrg240(config-warplink)#

**■ クライアント設定**

○ アカウント情報(ユーザ ID、パスワード)の指定

WarpLink Manager に登録してあるユーザ ID、パスワードを指定します。未設定の場合、機器情報は送信されません。
<書　　式> account username USERNAME password (|hidden) PASSWORD
<　no　> no account username (|USERNAME)

○ ダイナミック DNS の有効 / 無効を設定

有効にすると、NXR の WAN 側 IP アドレスを定期的に送信します。デフォルトは無効です。定期送信は 5 分間隔です。
<書　　式> service enable
<　no　> no service

○ 統計情報インタフェースの設定

NXR の CPU 使用率、メモリ使用率、トラフィック量を定期的に送信します。ダイナミック DNS が無効の場合は、送信されません。デフォルトは無効です。定期送信は 5 分間隔です。統計情報は、30 秒間隔で取得したデータの 3 分間の平均を 3 日分保持します。
トラフィック量は 2 つまでインターフェース(Ethernet、VLAN、PPP、Tunnel、Bridge, WLAN)を指定することが出来ます。最大 2 つまで設定可能です。未設定の場合は、統計情報は送信されません。
<書　　式> send-statistics interface INTERFACE
<　no　> no send-statistics interface (|INTERFACE)

○ syslog 情報送信の有効 / 無効を設定

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 mode 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 mode で実行します。

○ WarpLink Manager との通信状態を表示

WarpLink Manager との通信状態を表示します。

<書　　式> show warplink

<備　　考> view mode で実行します。

表示されるステータスおよび意味は下表のとおりです。

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

# 第 32 章　Extended track IP reachability mode

**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**

nxrg240#
nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**track <2048-4095> ip reachability**
nxrg240(config-ext-track-ipr)#

**■ destination**

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

**■ source**

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

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

**■ payload-length**

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

■ **transmit**

○ interval

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

<書　　式> transmit interval <10-32767> (|variable)

<備　　考>

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

○ retries

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

<書　　式> transmit retries <0-255>

<　no　> no transmit retries

■ recovery

○ count

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

<書　　式> recovery count <1-255>

<初 期 値> recovry count 1

<　no　> no recovery count

○ delay

<説　　明>

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

<書　　式> recovery delay <10-3600>

<　no　> no recovery delay

<備　　考>

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

■ set

○ df-bit

<説　　明> ip reachability における ping パケットに DF bit を設定することができます。
<書　　式> set df-bit
<初 期 値> set df-bit
<　no　> no set df-bit

○ ttl

<説　　明>
・ ip reachability における ping パケットの TTL を指定します。Default は、system の TTL 値(64)を set します。
<書　　式> set ttl <1-255>
<初 期 値> set ttl 64
<　no　> no set ttl

■ rtt

○ threshold

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

○ normal-count

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

○ delay-count

<説　　明> RTT status down と判断するまでの遅延回数です。Default は、3 回です。
<書　　式> rtt threshold <1-5000>
　　rtt threshold <1-5000> normal-count <1-255> delay-count <1-255>
<　no　> no rtt

■ netevent

○ threshold

<説　　明> monitor-log 機能で logging を行うかどうかを指定します。
<書　　式> netevent monitor-log-status
<初 期 値> no netevent monitor-log-status　　（無効）
<　no　> no netevent monitor-log-status

# 第 33 章　Extended track IPv6 reachability mode

**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**

nxrg240#
nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**track <2048-4095> ipv6 reachability**
nxrg240(config-ext-track-ipr)#

**■ destination**

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

**■ source**

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

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

**■ payload-length**

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

■ **transmit**

○ interval

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

<書　　式> transmit interval <10-32767> (|variable)

<備　　考>

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

○ retries

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

<書　　式> transmit retries <0-255>

<　no　> no transmit retries

■ **recovery**

○ count

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

<書　　式> recovery count <1-255>

<初 期 値> recovry count 1

<　no　> no recovery count

○ delay

<説　　明>

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

<書　　式> recovery delay <10-3600>

<　no　> no recovery delay

<備　　考>

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

■ **set**

○ hop-limit

<説　　明>

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

<書　　式> set hop-limit <1-255>

<初 期 値> set hop-limit 64

<　no　> no set hop-limit

■ **rtt**

○ threshold

<説　　明>

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

○ normal-count

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

○ delay-count

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

<書　　式> rtt threshold <1-5000>

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

<　no　> no rtt

■ **netevent**

○ threshold

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

<書　　式> netevent monitor-log-status

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

<　no　> no netevent monitor-log-status

# 第 34 章　Monitor-log mode

**ログ機能**

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

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

**■ 揮発性メモリ(内部メモリ)への保存**

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

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

< 出力情報 >

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

(2) リソース監視ログ

出力例および出力する情報は次のとおりです。

< 出 力 例 >

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

< 出力情報 >

1. 出力時刻
   DateAndTime 形式で出力します(ex. 2010-9-30,9:45:36.0)。
2. CPU 使用率
   最近 3 分の使用率を 0 ～ 100[%]で出力します。
3. メモリ空き容量[Kbyte]
4. セッション数(Connection Tracking 数)
   0～最大セッション数(CLI から設定可能な最大セッション数)の範囲で出力します。

**■ 不揮発性メモリ(USB Flash メモリ)へのバックアップ**

(1) 定期バックアップ

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

定期バックアップは、スケジュール機能(global mode の schedule コマンドを参照してください)によって実行されます。reachability 監視およびリソース監視では、監視ログ出力時も閾値チェックを行い、バックアップ条件に達している場合にはバックアップを実行します。

(2) バックアップファイルの管理

定期バックアップのタイミングで、バックアップ対象ファイルを外部 USB Flash メモリに移動します。

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

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

**◆ 移行 command**

nxrg240#
nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**monitor-log**
nxrg240(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 <1-32>)
reachability (disk0|disk1) threshold logsize <150-1000>
reachability (disk0|disk1) threshold files <1-32>
<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 <1-32>)
resource (disk0|disk1) threshold logsize <150-1000>
resource (disk0|disk1) threshold files <1-32>
<初 期 値> no resource
< no > no resource

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

# 第 35 章　mail server mode

**メール送信機能**

<説　　明>

・　イベント発生時に、管理者にメールで通知する機能です。次のイベント発生時に、メールを送信します。

○ PPP の接続 / 切断

・　PPP on-demand 接続が有効な場合、メール送信機能は無効です(動作しません)。

| イベント | メールの件名 | メール本文 |
|---|---|---|
| PPP の接続 | ppp0 was connected | IP address is A.B.C.D |
| PPP の切断 | ppp0 was disconnected | IP address is released |

※上記は、ppp0 の接続 / 切断時に送信するメールの例です。

**○ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#mail server 0
nxrg240(config-mail-server)#

**■ メール送信(SMTP)設定**

<説　　明>
- SMTP サーバのアドレスおよびポート番号を指定することができます。OP25B により、ISP が 25 番ポートをブロックしている場合は、587 番ポートを指定すると接続できるようになります。
- 本設定は、メールサーバ毎に行います。

○ server smtp address
<書　　式> server smtp address (A.B.C.D|FQDN)

○ server smtp port
<書　　式> server smtp port <1-65535>
<　no　　> no server smtp port
<初 期 値> server smtp port 25 (=no server smtp port)

○ server pop3 address
<書　　式> server pop3 address (A.B.C.D|FQDN)
<　no　　> no server pop3 address
<備　　考> 認証設定で、POP before SMTP を使用する場合に設定します。

**■ 認証設定**

○ server authentication
<説　　明>
- SMTP サーバよりメール送信するために、以下の 3 つの認証設定をサポートします。認証なしも指定することが出来ます。
  POP before SMTP, SMTP-Auth(login), SMTP-Auth(plain)

<書　　式> server authentication (pop-before-smtp|smtp-auth-login|smtp-auth-plain)
<　no　　> no server authentication

○ username
<説　　明> 認証設定を有効にした場合は、認証用の ID とパスワードを指定します。
<書　　式> username WORD password (hidden|) WORD
<　no　　> no username

**■ メールヘッダ部の設定**

<説　　明>
- 送信するメールの各ヘッダ部に設定する値を指定します。
- 本設定は、interface ppp mode で、インタフェース毎(ppp <0-4>)に指定することが出来ます。

○ mail send server
<説　　明> 使用するメールサーバを番号で指定します。
<書　　式> mail send server <0-2>
<　no　> no mail send server

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

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

○ mail send subject
<説　　明> メールの件名を設定します。指定しない場合は、既定のフォーマットを使用します。
<書　　式> mail send subject LINE
<　no　> no mail send subject
<備　　考>
- LINE を指定しない場合は、既定のフォーマットを使用します。以下に例を示します。
  ppp0 の接続時: ppp0 was connected
  ppp0 の切断時: ppp0 was disconnected

○ body
<説　　明>
- 本文には、既定のフォーマットを使用します。ユーザが指定することは出来ません。
- 以下に例を示します。
  PPP の接続時: IP address is A.B.C.D
  PPP の切断時: IP address is released

# 第 36 章　interface bridge mode

■ **OpenFlow**

- OpenFlow には、経路制御を行う OpenFlow Controller(OFC)と、データ転送を行う OpenFlow Switch(OFS)があります。OFC と OFS は、OpenFlow protocol によって通信を行います。
- 本装置は、OFS として動作します(OFC の機能はありません)。
- OFC と接続すると、OFC からの制御でデータ転送が行われます。未接続の場合は、通常のスイッチとして動作します(FDB に基づいてデータ転送を行います)。

■ **仮想スイッチ機能**

- OpenFlow Controller からのフォワーディングの制御を行います。Default では、OpenFlow 対応スイッチとして動作せず、通常のスイッチングハブとして動作します。OFC と接続すると、OFC からの命令によって処理が行われます。

※仮想スイッチ機能では、Bridge filter は使用できません。

インタフェースを仮想スイッチグループに参加させる場合の制限インタフェースが以下の状態の場合は、当該インタフェースを仮想スイッチグループに、参加させることは出来ません。仮想スイッチグループに参加させる場合は、以下の設定を削除･変更するようにしてください。

- PPPoE クライアントの設定
- VRRP の設定
- IPsec policy の設定
- L2TPv3 xconnect の設定
  VLAN インタフェースを xconnect として使用している場合は、該当する物理インタフェースの指定も出来ません。
- QoS の設定

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**interbridge <0-4095>**
nxrg240(config-bridge)#

**◆ ip address**

<説　　明> インタフェースに IP アドレスを設定します。
<書　　式> ip address A.B.C.D/M (|secondary)
<　no　> no ip address A.B.C.D/M (|secondary)
<備　　考> Bridge port 有効の場合に設定することが出来ます。

**◆ 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
<備　　考> Bridge port 有効の場合に設定することが出来ます。

**◆ ipv6 address**

<説　　明> インタフェースに IPv6 アドレスを設定します。
<書　　式>
　ipv6 address X:X::X:X link-local
　ipv6 address X:X::X:X/<0-128> (|eui-64)
　ipv6 address autoconfig
　ipv6 address autoconfig interface-id (X:X::X:X|mape-rule WORD)
<　no　>
　no ipv6 address X:X::X:X link-local
　no ipv6 address X:X::X:X/<0-128> (|eui-64)
　no ipv6 address autoconfig
<備　　考>
・ link-local 指定時は、自動的に設定される LLA を上書きします。
・ eui-64 指定時は、ipv6-address は prefix 部のみ指定します。

**◆ ipv6 address DHCPv6-PD**

<説　　明> DHCPv6 Prefix Delegation を設定します。
<書　　式> ipv6 address DHCPv6-PD X:X::X:X/M (|eui-64)
<　no　> no ipv6 address DHCPv6-PD (|X:X::X:X/M)
<備　　考>
・ ipv6-address は、sub-prefix と host 部を指定することが出来ます。
・ DHCPv6-PD は、DHCPv6 PD で受信する prefix 部のプロファイル名です。DHCPv6-PD は、DHCPv6 パケットを受信するインタフェース(異なるインタフェース)上で、ipv6 dhcp client pd コマンドを使用して設定します。

◆ **ipv6 dhcp client**

<説　　明> 当該インタフェースに適用する DHCPv6 クライアントのプロファイル名を指定します。
<書　　式> ipv6 dhcp client WORD
<　no　> no ipv6 dhcp client

◆ **ipv6 dhcp client pd**

<説　　明> DHCPv6 PD の prefix 部に、プロファイル名を付けます。
<書　　式> ipv6 dhcp client pd DHCPv6-PD
<　no　> no ipv6 dhcp client
<備　　考>

- DHCPv6 PD を受信するインタフェース上で設定します。
- 受信した DHCPv6 PD を(異なる)インタフェースに対して適用するには、ipv6 address DHCPv6-PD コマンドを使用します。
- ipv6 dhcp client WORD と ipv6 dhcpv6 pd DHCPv6-PD は、どちらか一方だけ設定可能です。

◆ **ipv6 address dhcp WORD**

<説　　明> 当該インタフェースに適用する DHCPv6 クライアントのプロファイル名を指定します。
<書　　式> ipv6 address dhcp WORD
<　no　> no ipv6 address dhcp WORD

## ■ bridge stp

- Bridge インタフェースは、STP(Spanning Tree Protocol IEEE802.1D)の機能を保有します。本機能を有効にすると、BPDU(Bridge Protocol Data Unit)の送受信による Spanning Tree のトポロジ変更が行われ、他のブリッジとの冗長リンクを構成する場合に、ブリッジループによるブロードキャストストームを防ぐことが出来ます。
- STP は、default 無効です。
- RSTP/MSTP は、未サポートです。

○ enable
<説　　明> Bridge インタフェースの STP を有効にすることができます。
<書　　式> bridge stp enable
<初 期 値> no bridge stp enable
<　no　> no bridge stp enable
<備　　考> no bridge stp enable のとき、forward delay は 0.00 になります。

○ priority
<説　　明> Bridge インタフェースの priority を設定することができます。
<書　　式> bridge priority <0-65535>
<初 期 値> no bridge priority 32768
<　no　> no bridge priority (= 初期値)

○ hello-time
<説　　明> Bridge インタフェースの helllo-time を設定することができます。
<書　　式> bridge hello-time <1-10>
<初 期 値> bridge hello-time 2
<　no　> no bridge hello-time (= 初期値)

○ forward-delay
<説　　明> Bridge インタフェースの forward-delay を設定することができます。
<書　　式> bridge forwaed-delay <4-30>
<初 期 値> bridge forwaed-delay 15
<　no　> no bridge forward-dely (= 初期値)
<備　　考> no bridge enable のとき、設定は可能ですが、設定の反映は行いません。

○ forward-delay
<説　　明> Bridge インタフェースの max-age を設定することができます。
<書　　式> bridge max-age <6-40>
<初 期 値> bridge max-age 20
<　no　> no bridge max-age

◆ **mtu**

<説　　明> MTU の値を設定します。
<書　　式> mtu <bytes:68-1500>
<　no　　> no mtu
<備　　考>

- bridge port の MTU よい大きい値を設定することはできません(例えば、ethernet 0 の MTU が 1400 の場合に、1400 より大きい値を設定することはできません)。
- interface bridge mode への移行時に、bridge port が無効の場合、設定だけ行います(設定の反映は exit 時に行います)。
- interface bridge mode への移行時に、bridge port が有効の場合、設定および設定の反映を行います。

◆ **ip proxy arp**

<説　　明> Proxy ARP を有効にします。
<書　　式> ip proxy-arp
<初 期 値> no ip proxy-arp
<　no　　> no ip proxy-arp

◆ **ip directed-broadcast**

<説　　明> Directed Broadcast のフォワーディングを有効にします。
<書　　式> ip directed-broadcast
<初 期 値> no ip directed-broadcast
<　no　　> no ip directed-broadcast

◆ **ip redirects**

<説　　明>

・ ICMP redirect(type=5)とは、同一ネットワーク上に他の最適なルートがあることを通知するためのメッセージです(RFC792)。

・ 本装置の Send redirect 機能によって、ICMP redirect の送信の有無を切り替えることが出来ます。

<書　　式> ip redirects

<初 期 値> ip redirects　　(有効)

< no > no ip redirects　　(無効)

<備　　考>

・ 以下に ICMPRedirect の例を示します。ICMP Redirect 受信後の動作は、Host 側の動作に依存するため、常に次のような動作になるというわけではありません。

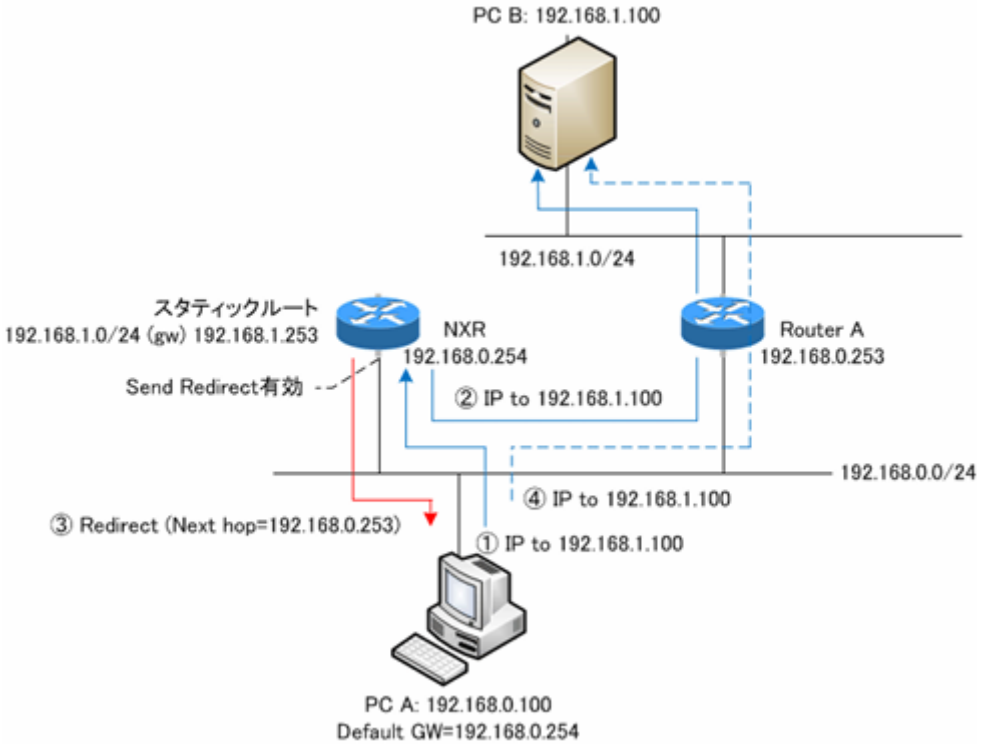
① Host A は、Host B(192.168.1.100)への IPv4 パケットを default gw(NXR)に送信します。

② NXR は、ルーティング情報から、192.168.1.0/24 宛ての next hop は 192.168.1.253 であることを知り、Router A へ転送します。

③ このとき、next hop の Router A は、送信元の Host A と同一ネットワークであるため、Host A に ICMP Redirect を送信します。

④ Host A は、以降の Host B 宛ての IPv4 パケットは、ICMP Redirect で通知された next hop に従って、Router A へ送出します。

・ 本装置が、ICMP Redirect を受信した場合は、ルーティングキャッシュの更新をしません。ルーティングテーブルに従った forwarding 動作を継続します。



◆ **ip tcp adjust-mss**

<説　　明>

・ Path MTU Discovery(PMTUD)機能(End-to-end でフラグメントが発生しない最大の MTU を発見すること)によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器(ルータ等)が ICMP fragment needed をフィルタリングしている場合(ブラックホールルータが存在する場合)や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、Endto-end での通信に支障をきたすことになります。このような場合、TCP では SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

<書　　式> ip tcp adjust-mss (auto|<500-1460:bytes>)

<初 期 値> no ip tcp adjust-mss

<　no　> no ip tcp adjust-mss

<備　　考>

・ IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。

・ 本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ ユーザが設定する場合は、MSS 値を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。

・ 「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

◆ **ipv6 tcp adjust-mss**

<説　　明> TCP/IPv6 の MSS 値を設定します。

<書　　式> ipv6 tcp adjust-mss (auto|500-1460)

<初 期 値> no ipv6 tcp adjust-mss

<　no　> no ipv6 tcp adjust-mss

◆ **ip mask-reply**

<説　　明>

・ OpenView などの監視装置では、監視ネットワーク内の機器に対して ICMP address mask request (type=17)を送信することによって機器のインタフェースのネットマスク値を取得します(単純に、死活監視で使用する場合もあります)。

・ 本装置では、ICMP address mask request への応答の有無を設定することが出来ます。

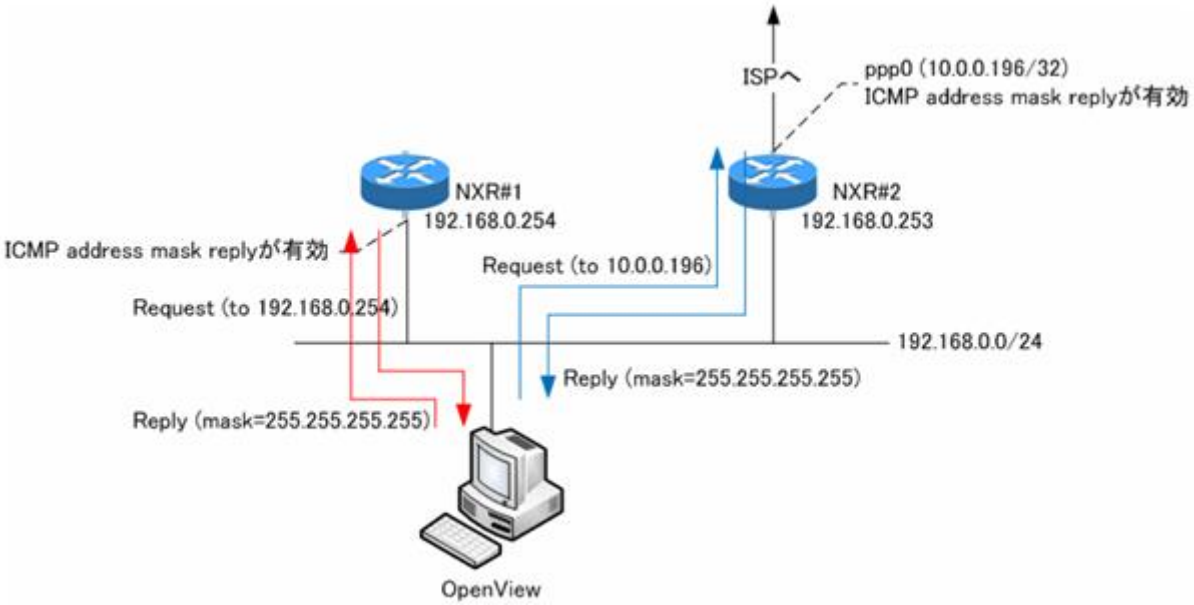
<書　　式> ip mask-reply (ICMP address mask request に応答します。)

<初 期 値> no ip mask-reply(ICMP address mask request に応答しません。)

<　no　> no ip mask-reply

<備　　考>

・ ICMP address mask request/reply の例を示します。



**◆ (ip|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 IPv4 address に通信することができます。
<書　　式> (ip|ipv6) access-linkdown
<　no　　> no (ip|ipv6) access-linkdown
<初 期 値> no (ip|ipv6) access-linkdown　　(無効)

**◆(ip|ipv6) rebound**

<説　　明>

- 下位ルータから受信したパケットを、受信インタフェースと同一インタフェースから出力(forwarding)した場合、下位ルータから NXR に対して再度パケットが送信されてくるため、下位ルータと NXR の間で TTL が「0」になるまでパケットがループします。
- IP rebound 機能を無効にすると、受信インタフェースと送信インタフェースが同一の場合、パケットをドロップし、かつ送信元に destination unreachable を送信します。
- Default は、有効です(受信インタフェースと送信インタフェースが同一でもドロップしません)。

<書　　式> (ip|ipv6) rebound
<初 期 値> (ip|ipv6) rebound
<　no　　> no (ip|ipv6) rebound

◆ **ip reassemble-output**

<説　　明>

・ インタフェースの MTU(あるいは PMTU)より大きいパケットを IP forwarding する際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。
本設定有効時、NXR がリアセンブルしたパケットは、以下のようにフラグメント処理を行います。
  - fragmented packet(パケットの断片)が MTU を超える場合、リアセンブルしたパケットを再度 MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、リアセンブルしたパケットを出力します。

<書　　式> ip reassemble-output

<初 期 値> ip reassemble-output

<　no　　> no ip reassemble-output

<備　　考>

・ 上記の場合(本設定が有効の場合)、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易な IP 実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズで NXR からパケットを出力します。また、出力時の IP フラグメント処理は、次のようになります。
  - fragmented packet(パケットの断片)が MTU を超える場合、受信した fragmented packet を MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、受信した fragmented packet をそのままのサイズで出力します。
・ Default は、global 設定および interface 設定ともに有効です。Global 設定と interface 設定の AND 条件により、本機能が有効か無効かを判定します。本設定は、IP forwarding するパケットにのみ影響します。
・ 受信時のサイズを記載しておくバッファが 32 個しかないため、33 個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-output が有効な場合と同様に処理します。

◆ **ip arp reachable-time**

<説　　明> 解決した ARP の有効期間を設定することが出来ます。
<書　　式> ip arp reachable-time <30000-3600000>
<初 期 値> ip arp reachable-time 30000
<　no　　> no ip arp reachable-time
<備　　考> show arp 実行時に、ステータスが REACHABLE と表示される時間です。
　　実際の時間は、(0.5 ～ 1.5)× reachable-time の間のランダムな値です。

◆ **ip arp queue length**

<説　　明>
・ Ethernet/VLAN インタフェース上で IPv4 通信を行う場合、送信先(あるいは next hop)の MAC アドレスの解決を行う必要があります。この時、MAC アドレスが解決するまで queueing できる数を指定することが出来ます。
<書　　式> ip arp queue length <1-1000>
<初 期 値> ip arp queue length 3
<　no　　> no ip arp queue length
<備　　考>
・ インタフェース(Ethernet/VLAN)毎に指定することが出来ます。
・ Queue は、ネイバーのエントリ毎に作成されます
・ この queue に queueing されたパケットは、アドレス解決の完了と同時に送信が行われます。Queue がいっぱいの状態で新たにパケットが来た場合、queue の先頭からドロップします。

◆ **ipv6 nd prefix**

<説　　明> IPv6 Routing Prefix Advertisement を設定します。
<書　　式> ipv6 nd prefix X:X:X:X::X/M
　　(|<valid-lifetime:0-4294967295> <preferred-lifetime:0-4294967295>)
<　no　　> no ipv6 nd prefix X:X:X:X::X/M
　　(|<valid-lifetime:0-4294967295> <preferred-lifetime:0-4294967295>)
<備　　考> Ethernet/VLAN のみ設定することが出来ます。

◆ **ipv6 nd send-ra**

<説　　明> IPv6 RA(Router Advertisement)の送信 / 停止を行います。
<書　　式> ipv6 nd send-ra　　( RA 送信)
<　no　　> no ipv6 nd send-ra　　( RA 停止)

◆ **ipv6 nd ra-lifetime**

<説　　明> IPv6 RA(Router Advertisement)のライフタイムを設定します。
<書　　式> ipv6 nd ra-lifetime <0-9000>
<初 期 値> ipv6 nd ra-lifetime 90
<　no　　> no ipv6 nd ra-lifetime
<備　　考> ra-lifetime >= ra-interval max になるように設定してください。

◆ **ipv6 nd ra-interval**

<説　　明> RA(Router Advertisement)インターバルを設定します。
<書　　式> ipv6 nd ra-interval <min:3-6750> <max:4-9000>
<初 期 値> ipv6 nd ra-interval 10 30
<　no　　> no ipv6 nd ra-interval
<備　　考> min < max x 0.75 になるように設定してください。

◆ **ipv6 nd ns-interval**

<説　　明> NS(Neighbor Solicitation)の送信間隔を設定します。
<書　　式> ipv6 nd ns-interval <msec:1000-3600000>
<初 期 値> ipv6 nd ns-interval 1000
<　no　　> no ipv6 nd ns-interval　　(初期値)

◆ **ipv6 nd rs-interval**

<説　　明> RS( Router Solicitation)インターバルを設定します。
<書　　式> ipv6 nd rs-interval <interval:1-10sec>
<初 期 値> ipv6 nd rs-interval 1
<　no　　> no ipv6 nd rs-interval　　(初期値)

◆ **ipv6 nd rs-count**

<説　　明> RS(Router Solicitation)の送信回数を設定します。
<書　　式> ipv6 nd rs-count <count:1-2147483647>
<初 期 値> ipv6 nd rs-count 3
<　no　　> no ipv6 nd rs-count　　(初期値)

◆ **ipv6 nd reachable-time**

<説　　明>
・ ルータ広告を受信した端末が, 送信時に確認できた隣接ノードの到達性についての情報の有効期間を指定します。
<書　　式> ipv6 nd reachable-time <msec:0-3600000>
<初 期 値> ipv6 nd reachable-time 30
<　no　　> no ipv6 nd reachable-time　　(初期値)
<備　　考>
・ この値が大きいと隣接ノードの到達性の問い合わせ回数が減少しますが, 端末の所有する到達性情報と実際の到達性が異なる可能性が高くなります。

◆ **ipv6 nd dad attempts**

<説　　明> DAD(Duplicate Address Detection)の送信回数を設定します。
<書　　式> ipv6 nd dad attempts <0-600>
<初 期 値> ipv6 nd dad attempts 1
<　no　　> no ipv6 nd dad attempts　　(初期値)

### ◆ ipv6 nd accept-redirects

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

### ◆ ipv6 nd queue length

<説　　明>
・ Ethernet/Vlan interface 上で IPv6 通信を行う場合、近隣探索(Neighbor Discovery)によって送信先(nexthop)の mac address の解決を行います。このとき、mac address が解決するまで queueing できるパケット数を指定することができます。
・ Queue は、neighbor の entry 毎に作成されます。
・ queueing された packet は、address 解決ができると同時に送信が行われます。
・ Queue が full の状態で新たに packet が来た場合、queue の先頭から drop されます。
<書　　式> ipv6 nd queue length <1-1000>
<初 期 値> ipv6 nd queue length 3
<　no　　> no ipv6 nd queue length
<備　　考> IPv4 の IPv6 それぞれについて、interface 毎に指定することができます。
　　IPv4 については、ip arp queue length を参照してください。

### ◆ ip access-group

<説　　明>
・ global mode で設定した ACL をインタフェースに適用することで、パケットフィルタリングを行うことができます。
<書　　式> ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
<　no　　> no ip access-group (in|out|forward-in|forward-out)
<備　　考>
・ 各インタフェースへのパケットフィルタリングの適用箇所(付録の Packet Traveling を参照)は、以下の 4 ヶ所です。
  - in(local input) NXR 自身で受信して処理するパケットを制限します。
  - out(local output) NXR 自身が作成して出力するパケットを制限します。
  - トンネリングされたパケットも NXR 自身が作成したパケットとして認識します。
  - forward-in NXR が当該インタフェースで受信して forwarding するパケットを制限します。
  - forward-out NXR が受信して当該インタフェースへ forwarding するパケットを制限します。
・ mac 指定のある ACL は、out および forward-out に設定することは出来ません。

### ◆ ipv6 access-group

<説　　明> アクセスグループに IPv6 アクセスリストを追加します。
<書　　式> ipv6 access-group (in|out|forward-in|forward-out) IPV6-ACL-NAME
<　no　　> no ipv6 access-group (in|out|forward-in|forward-out)

◆ **ip masquerade**

<説　　明>
- インタフェースよりパケットを出力する際に、パケットの送信元 IPv4 アドレスを出力インタフェースの IPv4 アドレスに自動変換する機能です。

<書　　式> ip masquerade　　(有効)
<初 期 値> no ip masquerade　　(無効)
<　no　　> no ip masquerade
<備　　考>
- すべてのインタフェース(Ethernet/VLAN/PPP/Tunnel/Bridge)で設定することが出来ます。
- TCP/UDP/ICMP のみ対応しています。その他のプロトコルに関しては、動作は保証しません。
- IPv6 パケットは、IP マスカレードの対象外です。
- forward out/local output フィルタリング適用後のパケットに、IP マスカレードを適用します。

◆ **ip (snat-group|dnat-group)**

<説　　明>
- global mode で設定した SNAT または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。
- SNAT は、パケットの出力時に適用されます。DNAT は、パケットの入力時に適用されます。

<書　　式> ip (snat-group|dnat-group) NAT-NAME
<　no　　> no ip (snat-group|dnat-group)
<備　　考> NAT ルールの設定は、ip snat/ip dnat コマンド(global mode)で行います。

◆ **ip webauth-filter**

◆ **ipv6 webauth-filter**

<説　　明>
- Web 認証フィルタをインタフェースに適用すると、ある特定のホスト、ネットワークやインタフェースについて、Web 認証せずに通信することが可能となります。
- Web 認証フィルタは、各インタフェースにつき、IN/OUT をそれぞれ一つずつ設定することができます。
  Default の設定はありません。

<書　　式> ip webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
　　ipv6 webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
<　no　　> no ip webauth-filter (forward-in|forward-out)
　　no ipv6 webauth-filter (forward-in|forward-out)
<備　　考>
- Web 認証フィルタの設定については、ip web-auth access-list/ipv6 web-auth access-list コマンド(global mode)を参照してください。
- Web 認証については、Web Authenticate mode を参照してください。

◆ **pppoe-client ppp**

<説　　明> PPPoE クライアントを有効にします。
<書　　式> pppoe-client ppp <0-4>
<初 期 値> no pppoe-client ppp
<　no　　> no pppoe-client ppp <0-4>
<備　　考> PPPoE クライアントは、複数指定することが出来ます。

◆ **ip spi-filter**

<説　　明>
・ 簡易ファイヤウォールの一つとして、SPI(Stateful Packet Inspection)機能をサポートします。
・ パケットに関連するコネクションの状態を見て、当該パケットをドロップするかしないかを決める機能です。
<書　　式> ip spi-filter　　(有効)
<初 期 値> no ip spi-filter　　(無効)
<　no　　> no ip spi-filter
<備　　考>
・ コネクションの状態が、established または related の場合に、パケットの転送を許可します。
・ Established とは、すでに双方向でパケットの通信がありコネクションが確立されている状態です。
・ Related とは、すでに確立しているコネクションがある状態です。FTP のデータ転送等がこれに該当します。
・ 新しい接続でありながら、syn ビットの立っていないパケットはドロップします。
・ SPI は、forward in および local input の位置で適用されます。ユーザが適用位置を変更することは出来ません。

◆ **ipv6 spi-filter**

<説　　明> IPv6 SPI filter を設定します。
<書　　式> ipv6 spi-filter
<初 期 値> no ipv6 spi-filter
<　no　　> no ipv6 spi-filter

◆ **ip spi-filter log**
◆ **ipv6 spi-filter log**

<説　　明> フィルタログ機能(syslog mode 参照)を有効にします。
　　パケットが、SPI フィルタにマッチした場合、syslog に出力することが出来ます。
<書　　式> ip spi-filter log [limit <0-100>]
　　ipv6 spi-filter log [limit <0-100>]
<初 期 値> ip spi-filter log limit 10
　　ipv6 spi-filter log limit 10
<　no　　> no ip spi-filter
　　no ipv6 spi-filter
<備　　考>
・ limit を指定すると、1 秒当たりのログ出力数を制限します。初期値は、10 パケット / 秒です。
・ WAN 側からの意図しないパケットが、SPI フィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分に注意してください。

◆ **shutdown**

<説　　明> インタフェースをシャットダウンすることができます。
<書　　式> shutdown
<初 期 値> no shutdown
<　no　> no shutdown

◆ **ipsec policy**

<説　　明> 当該インタフェースで使用する IPsec ローカルポリシーを設定します。
<書　　式> ipsec policy <1-255>
<　no　> no ipsec policy (|1-255>)
<備　　考>

・ 各インタフェースに、IPsec ローカルポリシーを 4 つまで設定することが出来ます。他のインタフェースで既に設定している IPsec ローカルポリシーは、重複して設定できません。

◆ **ipsec policy-ignore**

<説　　明>

・ IPsec policy のチェックを行わないように指定する機能です。IPsec policy として any などを指定したけれども、特定の通信のみ IPsec 化したくない場合に、この機能を使用します。

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

・ Input を指定した場合、inbound policy check を実行しないため、IPsec 化されてくるべきパケットがドロップ されてしまう現象を回避することができます。
・ Output を指定した場合、当該インタフェースから出力されるパケットは、IPsec policy をチェックしないため平文で送信されます。

## ■ QoS

<説　　明> QoS(クラス分類)の設定を行います。

○ classify

<書　　式> classify (input|output) route-map ROUTEMAP

<備　　考>

・ インタフェースにルートマップを適用します。1 つのインタフェースに、input と output を別々に設定することが出来ます。
・ input で指定したルートマップは、PRE-ROUTING(付録の Packet Traveling を参照)で適用されます。
・ output で指定したルートマップは、POST-ROUTING(付録の Packet Traveling を参照)で適用されます。

○ no classify

<書　　式> no classify (|input|output)

<備　　考>

・ インタフェースに適用したルートマップを削除します。
・ 「no classify」を実行すると、両方(input と output)を削除します。片方だけを削除する場合は、input または output を指定します。

## ◆ session invalid-status-drop-interface

<説　　明>

・ session invalid-status-drop 機能(global mode 参照)をインタフェース毎に指定することができます。
・ 本機能は、default で無効です。

<書　　式> session invalid-status-drop-interface enable

<初 期 値> no session invalid-status-drop-interface enable

<　no　　> no session invalid-status-drop-interface enable

<備　　考>

・ あるインタフェースに対してのみ適用したい場合は、global mode で session invalid-status-drop 機能を無効にして、かつ本機能を指定インタフェースで有効にします。以下は、bridge 0 インタフェースに適用する場合の設定例です。
  - global mode で、session invalid-status-drop を無効にします。
    nxrg240(config)#no session invalid-status-drop enable
  - 指定インタフェースで、本機能を有効にします。
    nxrg240(config)#interface bridge 0
    nxrg240(config-bridge)#session invalid-status-drop-interface enable

### ◆ ip arp filter

<説　　明>
- 異なるインタフェースに割り当てられているアドレスに対する ARP request を受信した際に、ARPreply を返す / 返さない機能です。

<書　　式> ip arp filter
<初 期 値> ip arp filter　　(有効:ARP reply を返さない)
<　no　　> no ip arp filter　　(無効:ARP reply を返す)
<備　　考>
- ある LAN セグメントに複数の Ethernet インタフェースが接続されている場合は、複数のインタフェースから ARP reply を返さないように、本機能を有効にします。
- 一方で、ある LAN 上の端末に対する host route が、別インタフェースになっている場合に、当該 host からの ARP request に対して、ARP reply を返す場合は、本機能を無効にします。
- ARP reply の送信先は、ルート情報によって決まります。

### ◆ ip arp gratuitous

<説　　明> gratuitous ARP(GARP)を送信する機能です。
<書　　式> ip arp gratuitous <attempts:1-255> <interval:1-3600> <delay:1-600>
　　ip arp gratuitous (= ip arp gratuitous <attempts:1> <interval:1> <delay:5>)
<初 期 値> no ip arp gratuitous (無効:GARP を送信しない)
<　no　　> no ip arp gratuitous
<備　　考>
- アドレスの重複を避けたり、ARP テーブルを更新するために、本装置では、下記のタイミングに、GARP(request)を送信します。
- IP アドレスを追加した場合:追加したアドレスの GARP を送信します。
- リンクアップした場合:当該インタフェースの全アドレスの GARP を送信します。
- VRRP マスターに遷移した場合:VIP に対する GARP を送信します。
- GARP 送信機能は、default 無効です。設定により有効にする場合、送信回数、送信間隔(sec)、初期試行までの delay(sec)も同時に指定することが出来ます。
- 設定可能なインタフェースは、Ethernet、VLAN、Bridge です。
- 多数の VLAN や Bridge 上で有効にすると、リンクアップ時に大量の GARP を送信するケースがあるため、本機能を有効にする場合は、注意してください。
- DHCP クライアント機能使用時、DHCP によって IP アドレスを取得したタイミングでは、GARP 送信は行いません。しかし、既に IP アドレスを取得した状態で、リンクアップした場合は、GARP を送信します。

### ◆ bridge hw-address

<説　　明> interface bridge(仮想スイッチ)の HW アドレスを設定します。
<書　　式> bridge hw-address HH:HH:HH:HH:HH:HH
< no > no bridge hw-address
<備　　考>
・ 未設定の場合、bridge(仮想スイッチ)に参加しているインタフェースの中で、一番小さい HW アドレスを使用します。
・ HW アドレスを、設定することを推奨します。

### ◆ bridge mac-aging

<説　　明> interface bridge(仮想スイッチ)の mac-aging を設定します。
<書　　式> bridge mac-aging <15-3600>
<初 期 値> bridge mac-aging 300
< no > no bridge mac-aging (= bridge mac-aging 300)

### ◆ bridge mac-table-size

<説　　明> interface bridge(仮想スイッチ)上の mac table size(FDB)を設定します。
<書　　式> bridge mac-table-size <10-65536>
< no > no bridge mac-table-size

### ◆ bridge multicast-snooping enable

<説　　明> multicast snooping の有効／無効を設定します。
<書　　式> bridge multicast-snooping enable
<初 期 値> no bridge multicast-snooping enable
< no > no bridge multicast-snooping enable

## ■ bridge stp

○ bridge stp enable
<説　　明> STP(Spanning Tree Protocol)を有効にします。
<書　　式> bridge stp enable
<初 期 値> no bridge stp enable
<　no　> no bridge stp enable
<備　　考> STP が有効でない場合、以下の STP パラメータの設定は出来ません。

○ bridge forward-delay
<説　　明> bridge forward-delay を設定します。
<書　　式> bridge forward-delay <4-30>
<初 期 値> bridge dorward-delay 15
<　no　> no bridge forward-delay (= default)

○ bridge hello-time
<説　　明> bridge hello-time を設定します。
<書　　式> bridge hello-time <1-10>
<初 期 値> bridge hello-time 2
<　no　> no bridge hello-time (= default)

○ bridge max-age
<説　　明> bridge max-age を設定します。
<書　　式> bridge max-age <6-40>
<初 期 値> bridge dorward-delay 20
<　no　> no bridge forward-delay (= default)

○ bridge priority
<説　　明> bridge priority を設定します。
<書　　式> bridge priority <0-65535>
<初 期 値> bridge priority 32768
<　no　> no bridge priority (= default)

○ bridge set-flow
<説　　明> bridge set-flow で、指定した FLOW が追加されます。
<書　　式> bridge set-flow WORD
<　no　> no bridge set-flow

◆ **openflow controller-address**

<説　　明> 接続する openflow-controller の IP アドレスを設定します。
<書　　式> openflow controller-address ip A.B.C.D (port <1-65535>|)
< no　> no openflow controller-address (全ての controller-address を削除します)
no openflow controller-address ip A.B.C.D
no openflow controller-address ip A.B.C.D port <1-65535>

◆ **openflow datapath-id**

<説　　明> switch の識別子として、datapath-id を設定することが出来ます。
<書　　式> openflow datapath-id HEX
< no　> no openflow datapath-id
<備　　考> HEX 部は、<1-FFFFFFFFFFFFFFFF> の範囲で設定します。
未指定の場合は、システム内部で生成します。

◆ **openflow protocol**

<説　　明> openflow-controller へ接続する際の Openflow Protocol を指定します。
<書　　式> openflow protocol {10|11|12|13|14|15}
< no　> no openflow protocol
<備　　考> 1 つ(または複数)のバージョンを指定することが出来ます。
未指定の場合は、10(ver1.0)を使用します。
OpenFlow Controller とバージョンを合わせる必要があります。

◆ **l2tpv3 access-group**

<説　　明> Bridge インタフェースでの送受信に対して、l2tpv3 access-list を適用します。
<書　　式> l2tpv3 access-group (in|out) WORD
< no　> no l2tpv3 access-group (in|out)
<備　　考>

- WORD: root の ACL 名を指定します。
  (root の ACL 名は、global ノードの l2tpv3 access-list WORD root にて設定します。)
- in: Xconnect インタフェース→セッション(本装置への入力)方向のフィルタを適用します。
- out: セッション→ Xconnect インタフェース(本装置からの出力)方向のフィルタを適用します。

■ l2tpv3 l2rp
<説　　明> L2TPv3 L2RP(冗長化構成)の設定をします。

○ enable
<説　　明> L2RP を有効にします。
<書　　式> l2tpv3 l2rp <1-255> enable
<　no　> no l2tpv3 l2rp <1-255> enable

○ type
<説　　明> Master を選択する方法を指定します。
　　Default では、priority の比較によって判定します。
<書　　式> l2tpv3 l2rp <1-255> type (priority|active)
<　no　> no l2tpv3 l2rp <1-255> type
<初 期 値> l2tpv3 l2rp <1-255> type priority
<備　　考> priority を選択した場合、priority 値の大きい方が、master になります。
　　active を選択した場合、active session 数の多い方が、master になります。

○ priority
<説　　明> Master の選定に使用する priority 値を設定します。
<書　　式> l2tpv3 l2rp <1-255> priority <1-255>
<　no　> no l2tpv3 l2rp <1-255> priority
<初 期 値> l2tpv3 l2rp <1-255> priority 100

○ preempt
<説　　明> Priority 値の小さいものが master で、大きいものが backup となることを許可するかどうかの設定です。
<書　　式> l2tpv3 l2rp <1-255> preempt
<　no　> no l2tpv3 l2rp <1-255> preempt
<初 期 値> l2tpv3 l2rp <1-255> preempt
<備　　考>
・ preempt 有効時、Master 選択の判定基準(type で指定した判定方法)に従います。
・ preempt 無効時、priority(または session 数)の大きい LCCE が現れた場合に、backup へと遷移しません。

○ block-reset
<説　　明> 自身のポートのリンク状態を一時的に down させ、配下のスイッチの MAC テーブルをフラッシュします。
<書　　式> l2tpv3 l2rp <1-255> block-reset
<　no　　> no l2tpv3 l2rp <1-255> block-reset
<備　　考>
・ Group blocking 状態に遷移した場合のみ動作します。
・ Group blocking とは、自身で送信した Advertise Frame を受信した場合や、対向 LCCE の AdvertiseFrame を受信した場合に、Loop が発生していると判断して、Frame の転送を停止している状態です。

○ timers advertise
<説　　明> L2RP Advertise Frame を送信する間隔を指定します。
<書　　式> l2tpv3 l2rp <1-255> timers advertise <1-60>
<　no　　> no l2tpv3 l2rp <1-255> timers advertise
<初 期 値> l2tpv3 l2rp <1-255> timers advertise 1

○ timers delay
<説　　明> L2TP session 確立後、timers delay で指定した時間、Group Blocking 状態となり、Frame の転送を行いません。
<書　　式> l2tpv3 l2rp <l2rpid:1-255> timers delay <0-60>
<　no　　> no l2tpv3 l2rp <1-255> timers delay
<初 期 値> l2tpv3 l2rp <l2rpid:1-255> timers delay 0
<備　　考>
・ L2RP は、主に Loop が発生する環境で使用されます。そのような環境では、L2RP Frame を受信するまで(Loop を検出するまで)の間、Blocking 機能が動作しないので、一時的に Broadcast Storm が発生します。timers delay を設定することで、Broadcast Storm を回避することが出来ます。
・ timers advertise より、長い時間を設定することを推奨します。

○ port-reset
<説　　明>
・ L2TP Group 機能や L2RP 機能により、L2TP session の切替が発生した際、配下スイッチの FDB において、MAC アドレスのエントリーが更新されていないため、最大 5 分間通信できないことがあります。
・ port reset 機能を有効にした場合、master → backup(または、master → init)へ遷移した際に、L2RP インタフェースのリンクを一時的に down させることで、配下スイッチの FDB を flush させます。
<書　　式> l2tpv3 l2rp <l2rpid:1-255> port-reset
<　no　　> no l2tpv3 l2rp <1-255> port-reset
<初 期 値> no l2tpv3 l2rp <1-255> port-reset

### ◆ ip multicast-to-unicast

<説　　明> 有効時、multicast を unicast 変換したパケットを転送します。
<書　　式> ip multicast-to-unicast forwarding　　(有効)
<　no　　> no ip multicast-to-unicast forwarding　　(無効)

### ◆ bridge bpdu-forwarding

<説　　明> 有効時、BPDU などのフレームを転送します。
<書　　式> bridge bpdu-forwarding enable　　(有効)
<　no　　> no bridge bpdu-forwarding enable　　(無効)

### ◆ bond

<説　　明> bond mode へ移行します。
<書　　式> bond <0-1>
<　no　　> no bond <0-1>

### ◆ bonding mode

複数のインタフェースを束ねて、1 つのインタフェースとして利用することができます。
<説　　明> ボンディングモードを設定します。
<書　　式> bonding mode (active-backup|balance-slb|balance-tcp)
<　no　　> no bonding mode
<備　　考>

・ active-backup 通常時 / 障害発生時で、インタフェース(active/backup)を切り替えます。
　balance-slb 送信元の MAC アドレスに基づいて、ロードバランシングを実行します。
　balance-tcp レイヤー 2 とレイヤー 4 のデータを考慮して、ロードバランシングを実行します。
・ インタフェース(ethernet 1, 2)に、本機能を適用する設定例を示します。

```
!
interface bridge 0
  ip address 192.168.10.1/24
  bond 0
    bonding mode active-backup
    exit-bond
!
interface ethernet 1
  bonding-group 0
!
interface ethernet 2
  bonding-group 0
!
```

## ■ lacp

LACP(Link Aggregation Control Protocol)の設定を行います。

○ mode
<説　　明> LACP のモード(active/passive)を指定します。
<書　　式> lacp mode (active|passive)
<　no　> no lacp mode

○ system-id
<説　　明> LACP システム ID(MAC アドレス)を設定します。
<書　　式> lacp system-id HH:HH:HH:HH:HH:HH
<　no　> no lacp system-id

○ system-priority
<説　　明> LACP システム優先度を設定します。値が小さいほど優先度は高くなります。
<書　　式> lacp system-priority <1-65535>
<　no　> no lacp system-priority

○ time
<説　　明> LACP フレームの送信間隔(slow[30 秒]/fast[1 秒)を指定します。
<書　　式> lacp time (slow|fast)
<　no　> no lacp time

○ fallback-active-backup
<説　　明>
・ 対向スイッチと LACP によるネゴシエーションができない場合に、active-backup にフォールバックします。
<書　　式> lacp fallback-active-backup
<　no　> no lacp fallback-active-backup

# 第 37 章　DDNS mode

# 第 37 章　DDNS mode

**DDNS 機能**

DDNS(Dynsmic DNS)とは、動的に変化するグローバル IP アドレスとドメイン名を対応付ける仕組みです。
グローバル IP アドレスの監視を行い、IP アドレスの変更があった場合に、DDNS サービスプロバイダに IP アドレスの変更を通知します。
これにより、動的なグローバル IP アドレス環境においても、固定のドメイン名によるアクセスが可能となります。

## ■ DDNS サービスプロバイダ

本装置が対応している DDNS サービスプロバイダについて示します。

### ○ 有料サービス

有料で DDNS サービスを提供している以下のプロバイダに対応しています。

- どこでもカメラ
  http://www.dococame.net/
- Dyn
  http://dyn.com/

### ○ 無料サービス

無料 DDNS サービスと無料ドメイン名を提供している以下のプロバイダに対応しています。

- DtDNS
  http://www.dtdns.com/
- No-IP
  http://www.no-ip.com/

### ○ 汎用プロバイダ

上記のプロバイダでは、NAT 環境を考慮して、以下のシーケンスで IP アドレスの変更通知が行われます。
（1）IP アドレス確認用サーバへ、自身の IP アドレスを問い合わせる。
（2）DDNS サーバへ、ドメイン名 /IP アドレスを通知する。
また、IP アドレス確認用サーバ、DDNS サーバの URL や HTTP Query は、プロバイダ固有の値を使用します。

汎用プロバイダにおいては、IP アドレス確認用サーバに対して IP アドレスの問い合わせを行わず、指定したインタフェースの IPv4/IPv6 アドレスを直接 DDNS サーバへ通知します。
また、送信先の URL および HTTP Query は、ユーザが指定します。

**■ IP アドレス変更通知**

以下に示すタイミングにおいて、DDNS プロバイダに対して IP アドレス変更通知を送信します。
DDNS 機能では、TCP80(HTTP)を利用して、DDNS プロバイダと通信を行います。通知する IP アドレスは、DDNS プロバイダへの問い合わせの際に使用する IP アドレスです。DDNS プロバイダは、本装置からの問い合わせに対して、本装置から受け取った HTTP パケットのソースアドレスを応答として返します。
したがって、バインドインタフェースを設定した場合でも、必ずしも当該インタフェースの IP アドレスが、DDNS プロバイダに登録されるわけではありません。

○ サービス起動時
本機能は、必要な configuration が設定された時点で自動的に起動します。この際、指定インタフェースに IP アドレスが割り当てられている場合、IP アドレス変更通知を送信します。

○ バインドインタフェース連動
サービス起動時に、インタフェースに対して IP アドレスが割り当てられていなかった場合には IP アドレスが割り当てられた際に、IP アドレス変更通知を送信します。

○ IP アドレス変更の強制通知
無料 DDNS サービスプロバイダの中には、一定期間 IP アドレス変更通知がない場合、アカウントを削除してしまうものがあります。
そのため、グローバル IP アドレスの有無にかかわらず、上記に示した指定インタフェース連動による IP アドレス変更通知を起点に、ユーザが指定した強制更新間隔毎に IP アドレス変更通知を送信します。
なお、IP アドレスの変更が無いにもかかわらず、短い周期(1 分程度)で IP アドレス変更通知を行うと、アカウントが削除される場合があるので、インターバルの設定には注意するようにしてください。

○ 再送処理
回線障害等でサービスプロバイダへの接続失敗が発生した場合、IP アドレス変更通知の再送処理を行います。
初回の再送間隔は 10 秒で、再送回数が増える毎に 10 秒ずつ再送間隔が増大します。最大再送間隔は 60 秒です。

**■ 状態表示**

DDNS サービスには、以下の状態があります(show ddns コマンドで、状態を参照することができます)。

| 状態表示 | 説明 |
|---|---|
| Configuration is incomplete | 設定項目に不足がある場合 |
| Starting | DDNS サービス開始中 |
| DDNS connect attempt | DDNS プロバイダにアクセス中(接続リトライ中) |
| Failed login | DDNS プロバイダのアカウント認証に失敗 |
| Succeed | DDNS プロバイダに IP アドレス登録成功 |

### ◆ 移行 command

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#ddns
nxrg240(config-ddns)#

### ◆ service enable

<説　　明> DDNS サービスを有効にします。
<書　　式> service enable　　(有効)
<初 期 値> no service enable　　(無効)
<　No　　> no service enable

### ◆ account

<説　　明> DDNS サービスを利用するためのユーザ ID およびパスワードを設定します。
<書　　式> account username USERID password (|hidden) PASSWORD

### ◆ bind-interface

<説　　明> バインドインタフェース(接続回線インタフェース)を設定します。
<書　　式> bind-interface INTERFACE
<備　　考> 本設定のインタフェース回線接続に連動して、IP アドレス変更通知を送信します。
　　INTERFACE には、ethernet, ppp, bridge を設定することが出来ます。

### ◆ forced-update-interval

<説　　明>
・ グローバル IP アドレス変更の有無にかかわらず、強制的に IP アドレス変更通知を送信する間隔を設定します。
<書　　式> forced-update-interval <hour:0-720>
　　forced-update-interval <0-43200> minutes
<　No　　> no forced-update-interval
<初 期 値> forced-update-interval 0　　(無効)

### ◆ ddns-provider

<説　　明> 接続する DDNS サービスプロバイダを指定します。
<書　　式> ddns-provider (dococame | dtdns | dyndns | no-ip | http client | ocn-ipoe)
<備　　考> 汎用プロバイダを利用する場合は、http client を指定します。

### ◆ domain-name

<説　　明> IP アドレスを結びつけるドメイン名を指定します。
<書　　式> domain-name DOMAINNAME
<　No　　> no domain-name (|DOMAINNAME)
<備　　考> ドメイン名は、最大 5 つまで設定することが出来ます。
　　汎用プロバイダを利用する場合は、指定しません。

◆ **query**

<説　　明> 汎用プロバイダを利用する場合に、HTTP Query を指定します。
<書　　式> query WORD
<備　　考>

・ Query には、以下のマクロ変数を使用することで、動的な値を指定することが出来ます。
　　${SN}:製品のシリアル番号
　　${IP}:bind-interface コマンドで指定したインタフェースの IPv4 アドレス
　　${IPV6}:bind-interface コマンドで指定したインタフェースの IPv6 グローバルアドレス
・ 大文字、小文字は区別しません。
・ なお、マクロ変数に IPv4 アドレス、IPv6 アドレスを指定した場合、指定されたインタフェースに対応するアドレスが付与されていない時は、IP アドレス変更通知を行いません。

◆ **url**

<説　　明> 汎用プロバイダを利用する場合に、DDNS サーバを指定します。
<書　　式> url (ip|ipv6) WROD
<備　　考> 送信先 URL(http://)を指定します。

# 第 38 章　access-server profile mode

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**access-server profile <0-31>**
nxrg240(config-ras)#
<備　　考> プロファイル数は、機種により異なります。

◆ **ppp username**

<説　　明> ユーザ名毎に、割り当てる IP アドレスを指定することが出来ます。
<書　　式> ppp username USERID ip A.B.C.D
<　No　　> no ppp username
<備　　考> 詳細は、「付録 l RAS 機能」を参照してください。

# 第 39 章　interface virtual-template mode

## ■ Virtual-template interface

- L2TP LNS 機能など、多数の着信(RAS)がある場合、着信の数だけの PPP を設定することは、本装置の管理者にとって大きな負担となります。
- Virtual-template を使用すると、call を受けた際に PPP のクローンを作成し、本ノードの設定内容を当該 PPP に適用します。
- Virtual-template interface は仮想的なインタフェースであり、実際に作成されるわけではありません。また、PPP クローンのインタフェース番号(ppp <100-256>)は、本装置が自動的に割り当てます。

### ◆ 移行 command

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**interface virtual-template <0-0>**
nxrg240(config-if-vt)#

### ◆ description

<説　　明> インタフェースの説明を記述します。
<書　　式> description DESCRIPTION
<　no　　> no descritpion
<備　　考> 使用可能な文字は、a-z,A-Z,0-9,-_.@ です。

### ◆ ip address

<説　　明> インタフェースに IP アドレスを設定します。
<書　　式> ip address A.B.C.D/32
<備　　考> 32 ビットマスクのみ指定することが出来ます。

### ◆ mtu

<説　　明> MTU の値を設定します。
<書　　式> mtu <bytes:68-1500>
<初 期 値> mtu 1454
<　no　　> no mtu
<備　　考>

- virtual-template としての初期値はありません。未設定の場合は、virtual-template を使用する機能が持つ初期値を使用します。

### ◆ ppp lcp mru

<説　　明> MRU の値を設定します。
<書　　式> ppp lcp mru <bytes:128-1500>
<初 期 値> ppp lcp mru 1454
<　no　　> no ppp lcp mru
<備　　考>

- virtual-template としての初期値はありません。未設定の場合は、virtual-template を使用する機能が持つ初期値を使用します。

### ◆ ip redirects

<説　　明>
- ICMP redirect(type=5)とは、同一ネットワーク上に他の最適なルートがあることを通知するためのメッセージです(RFC792)。
- 本装置の Send redirect 機能によって、ICMP redirect の送信の有無を切り替えることが出来ます。

<書　　式> ip redirects
<初 期 値> ip redirects　　(有効)
<　no　　> no ip redirects　　(無効)
<備　　考>
- ICMPRedirect の例は、interface mode の ip redirects を参照して下さい。

### ◆ ip tcp adjust-mss

<説　　明>
- Path MTU Discovery(PMTUD)機能(End-to-end でフラグメントが発生しない最大の MTU を発見すること)によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器(ルータ等)が ICMP fragment needed をフィルタリングしている場合(ブラックホールルータが存在する場合)や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、Endto-end での通信に支障をきたすことになります。このような場合、TCP では SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

<書　　式> ip tcp adjust-mss (auto|<500-1460:bytes>)
<初 期 値> no ip tcp adjust-mss
<　no　　> no ip tcp adjust-mss
<備　　考>
- IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。
- 本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。
- ユーザが設定する場合は、MSS 値を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。
- UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。
- 「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

◆ **ip mask-reply**

<説　　明>
- OpenView などの監視装置では、監視ネットワーク内の機器に対して ICMP address mask request (type=17)を送信することによって機器のインタフェースのネットマスク値を取得します(単純に、死活監視で使用する場合もあります)。
- 本装置では、ICMP address mask request への応答の有無を設定することが出来ます。

<書　　式> ip mask-reply　　(ICMP address mask request に応答します。)
<初 期 値> no ip mask-reply　　(ICMP address mask request に応答しません。)
<　no　　> no ip mask-reply
<備　　考>
- ICMP address mask request/reply の例は、interface mode の ip mask-reply を参照して下さい。

◆ **keepalive lcp-echo**

<説　　明> LCP echo request によるキープアライブを有効にします。
<書　　式> keepalive lcp-echo (|<interval:30-600> <failure-count:1-10>)
<初 期 値> keepalive lcp-echo 30 3
<　no　　> no keepalive lcp-echo
<備　　考>
- lcp-echo request/reply の連続失敗回数が、failure count の設定回数に達すると、PPP を切断します。

◆ **ip rebound**

<説　　明>
- 下位ルータから受信したパケットを、受信インタフェースと同一インタフェースから出力(forwarding)した場合、下位ルータから NXR に対して再度パケットが送信されてくるため、下位ルータと NXR の間で TTL が「0」になるまでパケットがループします。
- IP rebound 機能を無効にすると、受信インタフェースと送信インタフェースが同一の場合、パケットをドロップし、かつ送信元に destination unreachable を送信します。
- Default は、有効です(受信インタフェースと送信インタフェースが同一でもドロップしません)。

<書　　式> ip rebound
<初 期 値> ip rebound
<　no　　> no ip rebound

◆ **ip reassemble-output**

<説　　明>

・ インタフェースの MTU(あるいは PMTU)より大きいパケットを IP forwarding する際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。

・ 本設定有効時、NXR がリアセンブルしたパケットは、以下のようにフラグメント処理を行います。
  - fragmented packet(パケットの断片)が MTU を超える場合、リアセンブルしたパケットを再度 MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、リアセンブルしたパケットを出力します。

<書　　式> ip reassemble-output

<初 期 値> ip reassemble-output

<　no　　> no ip reassemble-output

<備　　考>

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

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

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

◆ **ip access-group**

<説　　明>
- global mode で設定した ACL をインタフェースに適用することで、パケットフィルタリングを行うことができます。

<書　　式> ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
<　no　> no ip access-group (in|out|forward-in|forward-out)
<備　　考>
- 各インタフェースへのパケットフィルタリングの適用箇所(付録の Packet Traveling を参照)は、以下の 4 ヶ所です。
  - in(local input) NXR 自身で受信して処理するパケットを制限します。
  - out(local output) NXR 自身が作成して出力するパケットを制限します。
    トンネリングされたパケットも NXR 自身が作成したパケットとして認識します。
  - forward-in NXR が当該インタフェースで受信して forwarding するパケットを制限します。
  - forward-out NXR が受信して当該インタフェースへ forwarding するパケットを制限します。
- mac 指定のある ACL は、out および forward-out に設定することは出来ません。

◆ **ip (snat-group|dnat-group)**

<説　　明>
- global mode で設定した SNAT または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。
- SNAT は、パケットの出力時に適用されます。DNAT は、パケットの入力時に適用されます。

<書　　式> ip (snat-group|dnat-group) NAT-NAME
<　no　> no ip (snat-group|dnat-group)
<備　　考> NAT ルールの設定は、ip snat/ip dnat)コマンド(global mode)で行います。

◆ **ppp authentication**

<説　　明> PPP の認証プロトコルを設定します。
<書　　式> ppp authentication (chap|pap|auto)
<初 期 値> ppp authentication auto
<　no　> no ppp authentication (= ppp authentication auto)

◆ **ppp ipcp dns**

<説　　明> PPP 接続時に割り当てる DNS を指定します。
<書　　式> ppp ipcp dns <primary:A.B.C.D> (|<secondary:A.B.C.D>)
<　no　> no ppp ipcp dns

◆ **peer ip proxy-arp**

<説　　明>
- 本機能の有効時に、IPCP で割り当てた peer ip を含むアドレスが設定されている Ethernet がある場合、当該インタフェース上で peer ip に対応する ARP を設定します。

<書　　式> peer ip proxy-arp　　(有効)
<　no　　> no peer ip proxy-arp　　(無効)
<備　　考> Ethernet 0 の IP アドレス、MAC アドレス、および peer IP アドレスが、次の場合
eth0:192.168.0.1/24 mac:00:80:6d:00:00:01
peer ip:192.168.0.200
以下の ARP エントリーを登録します。ただし、show arp では表示されません。
192.168.0.200 00:80:6d:00:00:01

◆ **peer ip pool**

<説　　明> 使用する IP アドレスプールを指定します。
<書　　式> peer ip pool WORD
<　no　　> no peer ip pool WORD
<備　　考> IP アドレスプールは、ip local pool コマンド(global mode)で設定します。

◆ **session invalid-status-drop-interface**

<説　　明>
- session invalid-status-drop 機能(global mode 参照)をインタフェース毎に指定することができます。
- 本機能は、default で無効です。

<書　　式> session invalid-status-drop-interface enable
<初 期 値> no session invalid-status-drop-interface enable
<　no　　> no session invalid-status-drop-interface enable
<備　　考>
- あるインタフェースに対してのみ適用したい場合は、global mode で session invalid-status-drop 機能を無効にして、かつ本機能を指定インタフェースで有効にします。以下は、virtual-template 0 インタフェースに適用する場合の設定例です。
  - global mode で、session invalid-status-drop を無効にします。
  nxrg240(config)#no session invalid-status-drop enable
  - 指定インタフェースで、本機能を有効にします。
  nxrg240(config)#interface virtual-template 0
  nxrg240(config-if-vt)#session invalid-status-drop-interface enable

◆ **ip multicast-to-unicast**

<説　　明> 有効時、multicast を unicast 変換したパケットを転送します。
<書　　式> ip multicast-to-unicast forwarding　　(有効)
<　no　　> no ip multicast-to-unicast forwarding　　(無効)

# 第 40 章　ngn-sip client mode

**■データコネクト**

データコネクトを使用する場合に設定します。データコネクトについては、付録 M を参照してください。

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
**nxrg240(config)#ngn-sip client <1-4>**
nxrg240(config-ngn-client)#

**◆ mode tcp ip**

<説　　明> TCP アクセスを監視する IP アドレス、および listen port を指定します。
<書　　式> mode tcp ip A.B.C.D port <1-65535>

**◆ tel to**

<説　　明> TCP アクセス検出時に発呼する電話番号(宛先番号)を指定します。
<書　　式> tel to NUMBER
<備　　考> 「0」または「#」で始まる NUMBER を指定します。指定可能な桁数は 5 ～ 32 桁です。

**◆ idle-timeout**

<説　　明> TCP 通信の無通信切断タイマーを設定します。
<書　　式> idle-timeout <10-3600>
<　no　　> no idle-timeout (初期値)
<初 期 値> idle-timeout 60
<備　　考>

・ TCP セッション上のデータ通信状態を定期的に監視し、一定時間の無通信状態を検出すると、自動的にデータコネクト通信を終了します。

# 第 41 章　ngn-sip server mode

**■データコネクト**

データコネクトを使用する場合に設定します。データコネクトについては、付録 M を参照してください。

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
**nxrg240(config)#ngn-sip server <1-4>**
nxrg240(config-ngn-server)#

**◆ mode tcp ip**

<説　　明> 着信時に TCP を接続させる端末の IP アドレス(宛先 IP アドレス)、および宛先 port 番号を指定します。
<書　　式> mode tcp ip A.B.C.D port <1-65535>

**◆ tel to**

<説　　明> 着信を許可する番号(発信者番号)を指定します。
<書　　式> tel from NUMBER
<備　　考> 「0」または「#」で始まる NUMBER を指定します。指定可能な桁数は 5 ～ 32 桁です。

**◆ idle-timeout**

<説　　明> TCP 通信の無通信切断タイマーを設定します。
<書　　式> idle-timeout <10-3600>
<　no　　> no idle-timeout (初期値)
<初 期 値> idle-timeout 60
<備　　考>

・ TCP セッション上のデータ通信状態を定期的に監視し、一定時間の無通信状態を検出すると、自動的にデータコネクト通信を終了します。

# 第 42 章　ipv6 dhcp-server mode

## ■ DHCPv6 Server

本バージョンでは、DNS servers option のみ対応しています。

### ◆ 移行 command

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**ipv6 dhcp-server WORD**
nxrg240(config-dhcp6s)#

### ◆ option-send dns-servers address

<説　　明> Reply 送信時に、DNS サーバのアドレスを通知します。
　　任意の DNS サーバ指定、および複数(最大 3 つまで)の DNS サーバ指定が可能です。
<書　　式> option-send dns-servers address (A.B.C.D|X:X::X:X)
< no > no option-send dns-servers address (A.B.C.D|X:X::X:X)
<備　　考>

・ 本オプションを設定した場合は、クライアント側の設定(option-request dns-servers)に関係なく DNS アドレスを通知します。

### ◆ option-send dns-servers add ipv6 dhcp-client

<説　　明> DHCPv6 クライアントで取得した DNS サーバを、DHCP サーバで広告します。
　　DHCPv6 クライアントのインタフェースを設定します。
<書　　式> option-send dns-servers add ipv6 dhcp-client ethernet X
　　option-send dns-servers add ipv6 dhcp-client ppp X
< no > no option-send dns-servers add ipv6 dhcp-client
<備　　考>

・ DHCPv6 クライアントと連携して動作します。本オプションを設定している場合の動作は、次のようになります。
  - DHCPv6 クライアントが DNS サーバ情報を取得している場合、下位からの request に対して、reply に DNS サーバアドレスを付与します。
  - DHCPv6 クライアントが DNS サーバ情報を未取得の場合、下位からの request に対して、reply には DNS サーバアドレスを付与しません。

### ◆ option-send domain-name

<説　　明> ドメイン名を(最大 3 つまで)設定することが出来ます。
<書　　式> option-send domain-name WORD
< no > no option-send domain-name WORD
<備　　考>

・ 本オプションを設定している場合、下位クライアントからの request(オプション:domain search List)に対して、ドメインサーチリストを reply します。

◆ **option-send domain-name add dhcp-client**

<説　　明> DHCPv6 クライアントで取得したドメインサーチリストを、DHCP サーバで広告します。
DHCPv6 クライアントのインタフェースを設定します。

<書　　式> option-send domain-name add ipv6 dhcp-client ethernet X
option-send domain-name add ipv6 dhcp-client ppp X

<　no　> no option-send domain-name add ipv6 dhcp-client

<備　　考>

・ DHCPv6 クライアントと連携して動作します。本オプションを設定している場合の動作は、次のようになります。
  - DHCPv6 クライアントがドメインサーチリストを取得している場合、下位からの request に対して、reply にドメインサーチリストを付与します。
  - DHCPv6 クライアントがドメインサーチリストを未取得の場合、下位からの request に対して、reply にドメインサーチリストを付与しません。

◆ **rapid-commit enable**

<説　　明> rapid-commit を有効にします。

<書　　式> rapid-commit enable

<　no　> no rapid-commit enable

<備　　考>

・ 本設定の有効時、2 つのメッセージ(Solicit/Reply)で、クライアントが情報取得を行うことが出来ます。
・ クライアント側も同様に設定します。

# 第 43 章　ipv6 dhcp-client mode

## ■ DHCPv6 Client

・ 本装置の DHCPv6 クライアントは、DHCPv6 サーバに対して、Prefix Delegation(PD)や、DNS サーバなどのアドレスを要求し、情報を受け取ることが出来ます(※ DHCPv6 サーバより IPv6 アドレスを割り当てるクライアント機能は、本バージョンではサポートしていません)。
・ PD を要求した場合、受信した prefix を使用して、本装置の IPv6 アドレスを設定したり、LAN 配下の端末に対して、RA で prefix を通知したりすることが出来ます。
・ DNS サーバ etc の情報を取得した場合、他の情報(SNTP サーバアドレス)については、本バージョンでは無視します。
・ 各オプションへの対応は、以下のとおりです(設定変更可能なオプションのみを記載しています)。
**Rapid Commit**: Rapid Commit 有効の場合、2 つのメッセージ(通常は 4 つ)でアドレスを取得します。
**Domain Name Servers**: Domain Name Servers 有効にすると、DNS サーバアドレスの通知を要求します。
**Domain Search List**: Domain Search List 有効の場合、ドメインサーチリストの通知を要求します。ドメインサーチリストで、通知されたドメインについて名前解決を行う場合は、DHCP 上で取得した DNS サーバアドレスに対してのみクエリを送信し、その他の DNS サーバアドレス(ユーザ設定による DNS サーバ等)にはクエリを送信しません。
**Identity Association for Prefix Delegation(IAPD)**:IA prefix を要求する際に使用します(IAPD が有効の場合に送信します)。

### □ Prefix Delegation 機能

・ Prefix Delegation は、ユーザサイトに対して prefix を委譲するための仕組みで、LAN 側で使用するグローバル prefix を designated ルータに対して、通知することが出来ます。※ information-only と併用することは出来ません。
・ Designated ルータは、割り当てられた prefix の中から、ユーザが指定した prefix を、LAN 配下のホストに対して、DHCPv6 やルータ広告(RA)によって配布します。
・ PD を受信すると、prefix の中から、ユーザが指定した prefix/length を生成し、インタフェースに対して IPv6 アドレスを割り当てます(アドレス割り当てが有効な場合)。その後、生成した prefix を本装置配下の IPv6 ホストに対して、RA によって広告することも可能です。

### □ Information-only 機能

・ ステートレス DHCPv6 で動作するモードです。DHCPv6 information-request を送信し、DNS サーバや SNTP サーバ etc の情報を取得します。
・ 本バージョンでは、受信した応答のうち、DNS サーバアドレスの情報(option:23)のみを参照し、他の情報(SNTP サーバアドレス etc)については無視します。
・ ia-pd を設定している場合は、本機能を有効にすることは出来ません。

### □ DHCPv6 client DUID

・ DHCPv6 でサーバに対して要求を行う際に使用する DUID のフォーマットについて記します。
・ 本装置でサポートする DUID は、RFC3315 に準拠したフォーマットで、次の 2 つをサポートしています。
※ DUID-EN はサポートしていません。
**DUID-LLT**: Ethernet/bridge/VLAN 以外で動作する場合に、使用する場合のフォーマットです。リンクレイヤーアドレスには、ethernet 0 の HW アドレスを使用します。
**DUID-LL**: Ethernet/bridge/VLAN で動作する場合に、使用するフォーマットです。

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**ipv6 dhcp-client WORD**
nxrg240(config-dhcp6c)#

**◆ ia-pd WORD**

<説　　明>
・ Identity Association for Prefix Delegation(IAPD)を有効にします(当該 prefix に名前を付けて、prefix を取得します)。
<書　　式> ia-pd WORD
<　no　　> no ia-pd
<備　　考> インタフェース設定の prefix 名と同じ名前を設定することは出来ません。
information-only が有効の場合は、本機能を設定することは出来ません。

**◆ ia-na enable**

<説　　明> IA_NA(Identity Association for Non-temporary Addresses)を有効にします。
<書　　式> ia-na enable
<　no　　> no ia-na enable
<備　　考> information-only が有効の場合は、本機能を設定することは出来ません。
ia-pd WORD を設定すると、ia-na は無効になります。

**◆ rapid-commit**

<説　　明> Rapid Commit オプション(初期値:無効)を有効にします。
<書　　式> rapid-commit enable
<　no　　> no rapid-commit enable
<備　　考>
・ 有効の場合、2 つのメッセージ(Solicit/Reply)でアドレスを取得します。
・ 無効の場合、通常通り 4 つのメッセージ(Solicit/Advertise/Request/Reply)でアドレスを取得します。

**◆ option-request dns-servers**

<説　　明> Domain Name Servers オプションを有効にします。
DHCPv6 サーバに対して、DNS サーバアドレスの通知を要求します。
<書　　式> option-request dns-servers
<初 期 値> no option-request dns-servers
<　no　　> no option-request dns-servers

◆ **option-request domain-name**

<説　　明> Domain Seatch List オプションを有効にします。
　　有効の場合、DHCPv6 サーバに対してドメインサーチリストの通知を要求します。
<書　　式> option-request domain-name
<初 期 値> no option-request domain-name
<　no　> no option-request dns-servers

◆ **information-only enable**

<説　　明> information-only 機能を有効にします。
<書　　式> information-only enable
<　no　> no information-only enable
<備　　考>

- ステートレス DHCPv6 で動作するモードです。DHCPv6 information-request を送信し、DNS サーバや SNTP サーバ etc の情報を取得します。
- 本バージョンでは、受信した応答のうち、DNS サーバアドレスの情報(option:23)のみを参照し、他の情報(SNTP サーバアドレス etc)については無視します。
- ia-pd を設定している場合は、本機能を有効にすることは出来ません。

**□ 関連するコマンド**

**◇ ipv6 dhcp-client WORD**

<説　　明> ipv6 dhcp-client mode へ移行します。
<書　　式> ipv6 dhcp-client WORD
< no > no ipv6 dhcp-client WORD（指定した設定を削除します）
< mode > global mode

**◇ show config ipv6 dhcp-client**

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

**◇ show ipv6 dhcp client pd**

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

**◇ show ipv6 dhcp client dns-servers**

<説　　明> option-request dns-servers で取得した DNS を表示します。
<書　　式> show ipv6 dhcp client dns-servers WORD
< mode > view mode
<備　　考> WORD には、profile 名(ipv6 dhcp-client WORD)を指定します。

**◇ show ipv6 dhcp client domain-name**

<説　　明> option-request domain-name で取得した domain 名を表示します。
<書　　式> show ipv6 dhcp client domain-name WORD
< mode > view mode
<備　　考> WORD には、profile 名(ipv6 dhcp-client WORD)を指定します。

# 第 44 章　l2tpv3 access-list mode

# Ⅰ．L2TPv3 フィルタリング機能

## ■ L2TPv3 フィルタリング機能

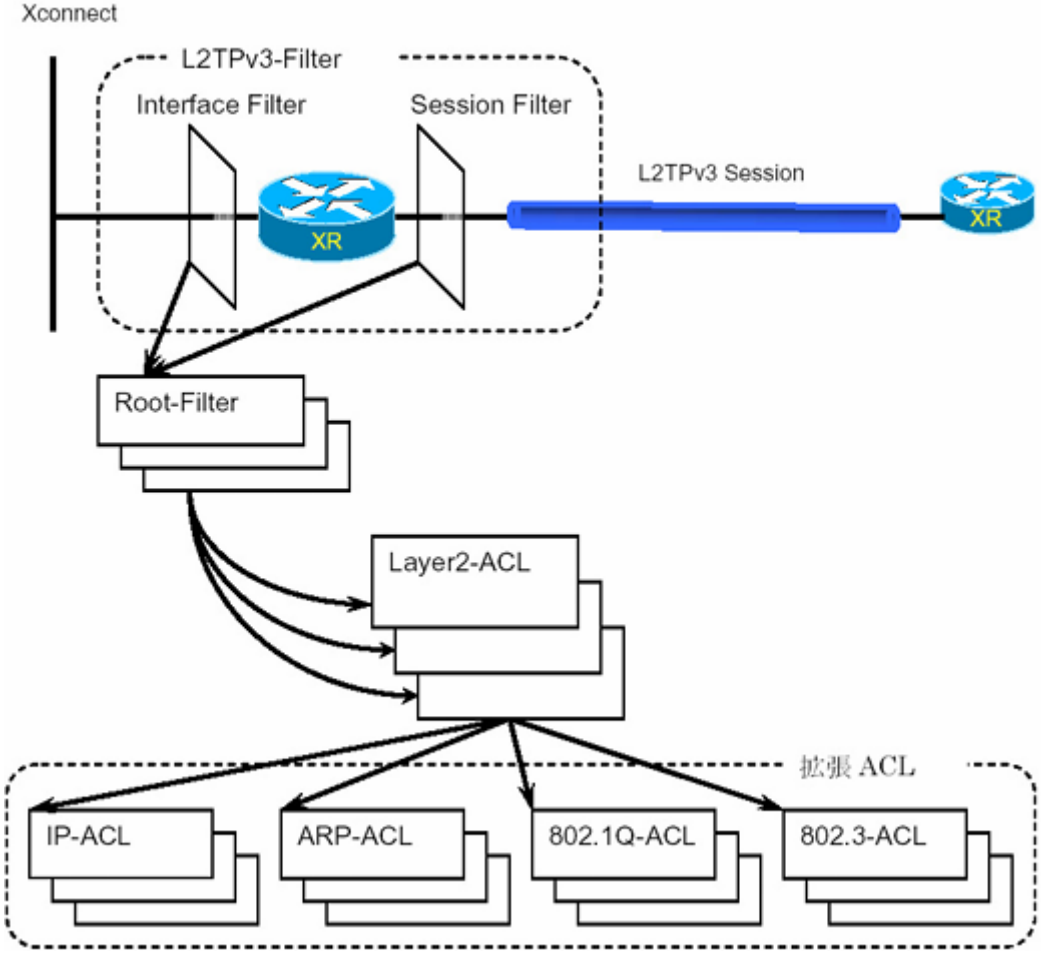
・ L2TPv3 によりトンネリングされるフレームを、Xconnect インタフェース上、またはセッション上でフィルタリングすることが出来ます。

・ フィルタリングの設定は、MAC アドレスや IPv4、IPv6、ARP、802.1Q、TCP/UDP など、レイヤー 2 からレイヤー 4 での詳細な指定が可能です。

※ L2TPv3 fast-forwarding 機能を利用している場合、fast-forwarding のエントリーに登録済みのセッションに対して L2TPv3 フィルタリングを設定しても、当該セッションが(タイムアウト等によって)エントリーから消えるまでは、フィルタリングは適用されません。

## ■ L2TPv3 フィルタ設定概要

L2TPv3 フィルタは、以下の要素から構成されています。




○ Root フィルタ

Root フィルタは、配下に Layer2 ACL を持ち、検索する順に配置します。配下の全ての Layer2 ACL に一致しない場合の動作を default ポリシー(deny/permit)とします。

○ Layer2 ACL

● Layer2 ACL

Layer2 レベルでルールを記述します。配下に、extended ACL を持つことが出来ます。

● extended ACL(拡張 ACL)

プロトコル毎に詳細なルールを記述することが出来ます。IP、IPv6、VLAN(IEEE 802.1Q)、ARP、IEEE 802.3 の各プロトコルに対応しています。

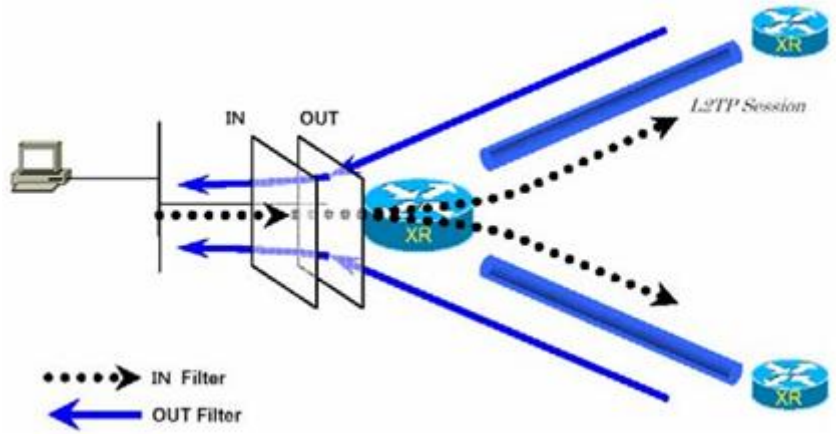
○ L2TPv3 フィルタ

Xconnect インタフェース、およびセッションに適用する root フィルタを設定します。
フィルタリング可能な位置は、以下の 4 ヶ所です。

● Xconnect インタフェースで受信する場合
● Xconnect インタフェースへ送信する場合

<書　　式> l2tpv3 access-group (in|out) WORD
< no > no l2tpv3 access-group (in|out)
< mode > interface mode
<備　　考>

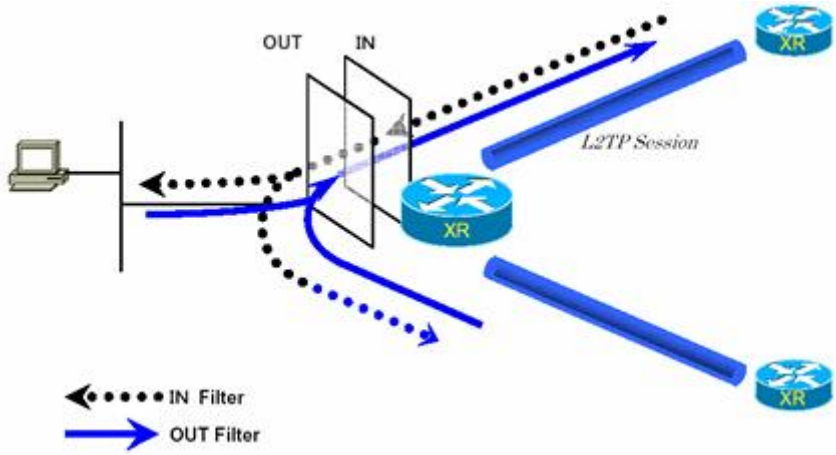
・ WORD: root の ACL 名(l2tpv3 access-list WORD root にて設定します)を指定します。
・ in: Xconnect インタフェース→セッション(本装置への入力)方向のフィルタを適用します。
・ out: セッション→ Xconnect インタフェース(本装置からの出力)方向のフィルタを適用します。




● L2TPv3 セッションにより転送される(受信する)場合
● L2TPv3 セッションにより転送する(送信する)場合

<書　　式> l2tpv3 access-group (in|out) WORD
< no > no l2tpv3 access-group (in|out)
< mode > l2tpv3 xconnect mode
<備　　考>

・ WORD: root の ACL 名(l2tpv3 access-list WORD root にて設定します)を指定します。
・ in: 受信方向のセッションに対して、フィルタを適用します。
・ out: 送信方向のセッションに対して、フィルタを適用します。

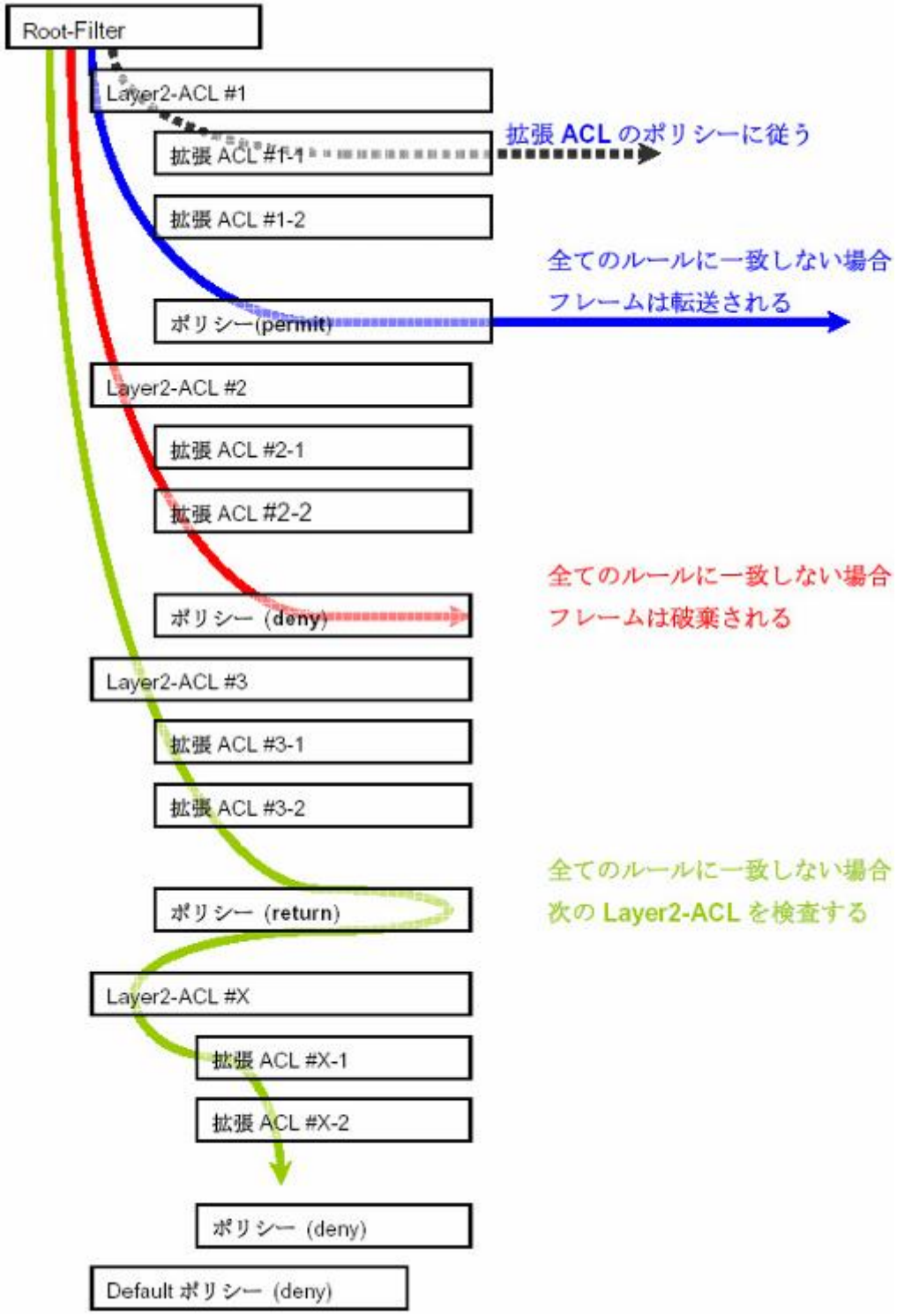


■ **L2TPv3 フィルタの動作(ポリシー)**

○ permit(許可)
フィルタルールに一致する場合、検索を中止してフレームを転送します。

○ deny(破棄)
フィルタルールに一致する場合、検索を中止してフレームを破棄します。

○ return(復帰)
フィルタルールに一致しない場合、該当 layer2 ACL での検索を中止して、呼び出し元の次の layer2ACL から検索を再開します。



**■ L2TPv3 フィルタの評価**

root フィルタの配下に設定された layer2 ACL を、上から順に検索し、最初に条件に一致(1st マッチ)する ACL に対して、以下の評価を行います。

すべての layer2 ACL に一致しない場合は、当該 root ACL の default ポリシー(deny/permit)に従います。

● extended ACL がない場合

当該 layer2 ACL のポリシー(deny/permit/return)に従います。

● extended ACL がある場合

Layer2 ACL 配下の extended ACL を、1st マッチにて検索し、以下の評価を行います。

- extended ACL に一致する場合、当該 ACL のポリシー(deny/permit)に従います。
- すべての extended ACL に一致しない場合、当該 layer2 ACL のポリシー(deny/permit/return)に従います。

**■ L2TPv3 フィルタの処理順序**

- Known Unicast のフレームが、転送禁止状態の場合は、permit 条件に一致しても、フレームを転送しません。
- Circuit Down により転送禁止状態の場合は、permit 条件に一致しても、フレームを転送しません。

**■ L2TPv3 フィルタの表示**

<説　　明> L2TPv3 アクセスリストを表示します。

<書　　式> show l2tpv3 access-list
show l2tpv3 access-list interface (|INTERFACE)
show l2tpv3 access-list xconnect (|<1-4294967295>)
show l2tpv3 access-list (root|layer2|ip|ipv6|arp|vlan|ieee802-3) (|WORD)
show l2tpv3 access-list detail (root|layer2|vlan) (|WORD)
show l2tpv3 access-list detail root WORD layer2 WORD

< mode > view mode

**■ L2TPv3 フィルタのクリア**

<説　　明> L2TPv3 アクセスリストのカウンターをクリアします。

<書　　式>
clear l2tpv3 counter access-list
clear l2tpv3 counter access-list interface (|INTERFACE )
clear l2tpv3 counter access-list xconnect (|<1-4294967295>)
clear l2tpv3 counter access-list (root|layer2|ip|ipv6|arp|vlan|ieee802-3) (|WORD)
clear l2tpv3 counter access-list detail (root|layer2|vlan) (|WORD)

< mode > view mode

# Ⅱ. Root ACL

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**l2tpv3 access-list WORD root (deny|permit)**
nxrg240(config-l2tpv3-acl)#

<説　　明>
- Root ACL の ACL 名(WORD)および default ポリシー(deny|permit)を設定(または指定)して、root ACL の l2tpv3 access-list mode に移行します。

<備　　考>
- 既に設定済の ACL で、deny/permit が異なる場合は、mode 移行できません。
- 同一 ACL 名を設定することはできません(root, layer2, extended ip/ipv6/vlan/arp/ieee802-3 が異なる場合でも、同じ ACL 名はエラーとして扱います)。
- root ACL の最大設定数は、512 個です。

**◆ layer2 access-list**

<説　　明> 当該 root ACL の配下に配置する layer2 ACL を設定します。
　　WORD には、layer2 ACL の ACL 名を指定します。
<書　　式> layer2 access-list WORD <1-256>
<　no　　> no layer2 access-list (すべての ACL を削除します)
　　no layer2 access-list WORD (指定した ACL を削除します)
<備　　考> 1 つの root 配下に、32 個までの layer2 ACL を設定することが出来ます。
　　本装置全体で、設定可能な layer2 ACL の総数は、4096 個です。

# Ⅲ. Layer2 ACL

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**l2tpv3 access-list WORD layer2 (deny|permit|return)**
nxrg240(config-l2tpv3-acl)#
<説　　明>
・ Layer2 ACL の ACL 名(WORD)および default ポリシー(deny|permit|return)を設定(または指定)して、layer2 ACL の l2tpv3 access-list mode に移行します。
<備　　考>
・ 既に設定済の ACL で、deny/permit/return が異なる場合は、mode 移行できません。
・ 同一 ACL 名を設定することはできません(root, layer2, extended ip/ipv6/vlan/arp/ieee802-3 が異なる場合でも、同じ ACL 名はエラーとして扱います)。
・ Layer2 ACL の最大設定数は、128 個です。

**◆ mac source**

<説　　明> マッチ条件に送信元 MAC アドレスを設定します。
<書　　式> mac source HH:HH:HH:HH:HH:HH(/MM:MM:MM:MM:MM:MM)
<　no　> no mac source HH:HH:HH:HH:HH:HH(/MM:MM:MM:MM:MM:MM)
<備　　考>
・ 例えば、ワイルドカードで「00:80:6D:**:**:**」を指定する場合は、次のように設定します。
mac source 00:80:6D:00:00:00/FF:FF:FF:00:00:00

**◆ mac destination**

<説　　明> マッチ条件に送信先 MAC アドレスを設定します。
<書　　式> mac destination HH:HH:HH:HH:HH:HH(/MM:MM:MM:MM:MM:MM)
<　no　> no mac destination HH:HH:HH:HH:HH:HH(/MM:MM:MM:MM:MM:MM)
<備　　考>
・ 例えば、ワイルドカードで「00:80:6D:**:**:**」を指定する場合は、次のように設定します。
mac destination 00:80:6D:00:00:00/FF:FF:FF:00:00:00

**◆ ethernet-type**

<説　　明> ethernet-type と extended ACL を設定します。
WORD には、extended ACL の ACL 名を指定します。
<書　　式> ethernet-type (ip|ipv6|arp|vlan|ieee802-3) (|extended WORD <1-256>)
ethernet-type <1536-65535>
<　no　> no ethernet-type (ip|ipv6|arp|vlan|ieee802-3) extended (|WORD)
(extended のみ削除します。)
no ethernet-type
(ethernet-type とすべての extended を削除します。)
<備　　考> extended ACL は、最大 32 個まで設定することが出来ます。

# Ⅳ. Extended IP ACL

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**l2tpv3 access-list WORD extended ip (deny|permit)**
nxrg240(config-l2tpv3-eacl)#

<説　　明>
- Extended IP ACL の ACL 名(WORD)および default ポリシー(deny|permit)を設定(または指定)して、extended IP ACL の l2tpv3 access-list mode に移行します。

<備　　考>
- 既に設定済の ACL で、deny/permit が異なる場合は、mode 移行できません。
- 同一 ACL 名を設定することはできません(root, layer2, extended ip/ipv6/vlan/arp/ieee802-3 が異なる場合でも、同じ ACL 名はエラーとして扱います)。
- Extended IP ACL の最大設定数は、128 個です。

**◆ source**

<説　　明> マッチ条件に、送信元 IP アドレスを設定します。
<書　　式> source (A.B.C.D | A.B.C.D/M)
<　no　> no source

**◆ destination**

<説　　明> マッチ条件に、送信先 IP アドレスを設定します。
<書　　式> destination (A.B.C.D | A.B.C.D/M)
<　no　> no destination

**◆ tos**

<説　　明> マッチ条件に、tos を設定します。
<書　　式> tos <0-255>
<　no　> no tos

**◆ protocol**

<説　　明> マッチ条件に、protocol を設定します。
<書　　式> protocol (<0-255> | icmp | tcp | udp)
<　no　> no protocol
<備　　考>
- source-port(または destination-port)が設定済の場合、protocol <0-255>|icmp は設定出来ません。

◆ **source-port**

<説　　明> マッチ条件に、source port を設定します。
<書　　式> source-port (<1-65535> | range <1-65535> <1-65535>)
<　no　　> no source-port
<備　　考> protocol udp(または tcp)の場合に、設定することが出来ます。

◆ **destination-port**

<説　　明> マッチ条件に、destination port を設定します。
<書　　式> destination-port (<1-65535> | range <1-65535> <1-65535>)
<　no　　> no destination-port
<備　　考> protocol udp(または tcp)の場合に、設定することが出来ます。

◆ **icmp**

<説　　明> マッチ条件に、icmp type/code を設定します。
<書　　式> icmp <0-255> (|<0-255>)
<　no　　> no icmp
<備　　考> protocol icmp を設定済の場合に、設定することが出来ます。

# V．Extended IPv6 ACL

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**l2tpv3 access-list WORD extended ipv6 (deny|permit)**
nxrg240(config-l2tpv3-eacl)#

<説　　明>
- Extended IPv6 ACL の ACL 名(WORD)および default ポリシー(deny|permit)を設定(または指定)して、extended IPv6 ACL の l2tpv3 access-list mode に移行します。

<備　　考>
- 既に設定済の ACL で、deny/permit が異なる場合は、mode 移行できません。
- 同一 ACL 名を設定することはできません(root, layer2, extended ip/ipv6/vlan/arp/ieee802-3 が異なる場合でも、同じ ACL 名はエラーとして扱います)。
- Extended IPv6 ACL の最大設定数は、128 個です。

**◆ source**

<説　　明> マッチ条件に、送信元 IPv6 アドレスを設定します。
<書　　式> source (X:X::X:X | X:X::X:X/M)
<　no　> no source

**◆ destination**

<説　　明> マッチ条件に、送信先 IPv6 アドレスを設定します。
<書　　式> destination (X:X::X:X | X:X::X:X/M)
<　no　> no destination

**◆ protocol**

<説　　明> マッチ条件に、protocol を設定します。
<書　　式> protocol (<0-255> | icmpv6 | tcp | udp)
<　no　> no protocol
<備　　考>
- source-port(または destination-port)が設定済の場合、protocol <0-255>|icmpv6 を設定することは出来ません。

**◆ source-port**

<説　　明> マッチ条件に、source port を設定します。
<書　　式> source-port (<1-65535> | range <1-65535> <1-65535>)
<　no　> no source-port
<備　　考> protocol udp(または tcp)の場合に、設定することが出来ます。

**◆ destination-port**

<説　　明> マッチ条件に、destination port を設定します。
<書　　式> destination-port (<1-65535> | range <1-65535> <1-65535>)
<　no　> no destination-port
<備　　考> protocol udp(または tcp)の場合に、設定することが出来ます。

# VI. Extended VLAN ACL

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**l2tpv3 access-list WORD extended vlan (deny|permit)**
nxrg240(config-l2tpv3-eacl)#

<説　　明>
- Extended VLAN ACL の ACL 名(WORD)および default ポリシー(deny|permit)を設定(または指定)して、extended VLAN ACL の l2tpv3 access-list mode に移行します。

<備　　考>
- 既に設定済の ACL で、deny/permit が異なる場合は、mode 移行できません。
- 同一 ACL 名を設定することはできません(root, layer2, extended ip/ipv6/vlan/arp/ieee802-3 が異なる場合でも、同じ ACL 名はエラーとして扱います)。
- Extended VLAN ACL の最大設定数は、128 個です。

**◆ vlan-id**

<説　　明> マッチ条件に、VLAN ID を設定します。
<書　　式> vlan-id <0-4095>
<　no　　> no vlan-id

**◆ priority**

<説　　明> マッチ条件に、priority を設定します。
<書　　式> priority <0-7>
<　no　　> no priority

**◆ ethernet-type**

<説　　明> マッチ条件に、ethernet-type を設定します。
<書　　式> ethernet-type (ip|ipv6|arp) (|extended WORD <1-256>)
　　ethernet-type (vlan|<1536-65535>)
<　no　　> no ethernet-type (ip|ipv6|arp) extended (|WORD)
　　(extended のみ削除します。)
　　no ethernet-type
　　(ethernet-type とすべての extended を削除します。)

<備　　考>
- extended WORD が設定済の場合は、異なる ethernet-type を設定することは出来ません。
- extended WORD で指定する ACL 名は、l2tpv3 access-list WORD extended の ACL 名です。
- extended ACL の最大設定数は、32 です。

# Ⅶ. Extended ARP ACL

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**l2tpv3 access-list WORD extended arp (deny|permit)**
nxrg240(config-l2tpv3-eacl)#

<説　　明>
- Extended ARP ACL の ACL 名(WORD)および default ポリシー(deny|permit)を設定(または指定)して、extended ARP ACL の l2tpv3 access-list mode に移行します。

<備　　考>
- 既に設定済の ACL で、deny/permit が異なる場合は、mode 移行できません。
- 同一 ACL 名を設定することはできません(root, layer2, extended ip/ipv6/vlan/arp/ieee802-3 が異なる場合でも、同じ ACL 名はエラーとして扱います)。
- Extended ARP ACL の最大設定数は、128 個です。

◆ **opcode**

<説　　明> マッチ条件に、opcode を指定します。
<書　　式> opcode (<0-65535> | request | reply)
<　no　> no opcode

◆ **sender-mac**

<説　　明> マッチ条件に、送信元 MAC アドレスを指定します。
<書　　式> sender-mac HH:HH:HH:HH:HH:HH(/MM:MM:MM:MM:MM:MM)
<　no　> no sender-mac
<備　　考>
- 例えば、ワイルドカードで「00:80:6D:**:**:**」を指定する場合は、次のように設定します。
  sender-mac 00:80:6D:00:00:00/FF:FF:FF:00:00:00

◆ **target-mac**

<説　　明> マッチ条件に、送信先 MAC アドレスを指定します。
<書　　式> target-mac HH:HH:HH:HH:HH:HH(/MM:MM:MM:MM:MM:MM)
<　no　> no target-mac
<備　　考>
- 例えば、ワイルドカードで「00:80:6D:**:**:**」を指定する場合は、次のように設定します。
  target-mac 00:80:6D:00:00:00/FF:FF:FF:00:00:00

◆ **sender-ip**

<説　　明> マッチ条件に、送信元 IP アドレスを指定します。
<書　　式> sender-ip (A.B.C.D|A.B.C.D/M)
<　no　> no sender-ip

◆ **target-ip**

<説　　明> マッチ条件に、送信先 IP アドレスを指定します。
<書　　式> target-ip (A.B.C.D|A.B.C.D/M)
<　no　> no target-ip

# Ⅷ. Extended IEEE802.3 ACL

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**l2tpv3 access-list WORD extended ieee802-3 (deny|permit)**
nxrg240(config-l2tpv3-eacl)#

<説　　明>

・ Extended IEEE802.3 ACL の ACL 名(WORD)および default ポリシー(deny|permit)を設定(または指定)して、extended IEEE802.3 ACL の l2tpv3 access-list mode に移行します。

<備　　考>

・ 既に設定済の ACL で、deny/permit が異なる場合は、mode 移行できません。
・ 同一 ACL 名を設定することはできません(root, layer2, extended ip/ipv6/vlan/arp/ieee802-3 が異なる場合でも、同じ ACL 名はエラーとして扱います)。
・ Extended IEEE802.3 ACL の最大設定数は、128 個です。

**◆ llc-sap**

<説　　明> マッチ条件に、LLC SAP を指定します。
<書　　式> llc-sap <0-255>
<　no　　> no llc-sap
<備　　考> snap-type が設定済の場合は、llc-sap を設定することは出来ません。

**◆ snap-type**

<説　　明> マッチ条件に、SNAP タイプを指定します。
<書　　式> snap-type <1536-65535>
<　no　　> no snap-type
<備　　考> llc-sap が設定済の場合は、snap-type を設定することは出来ません。

# 第 45 章　address-family ipv6 mode

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**router bgp <1-65535>**
nxrg240(config-router)#**address-family ipv6**
nxrg240(config-router-af)#

<説　　明> BGP peer に advertise するネットワークを指定します。
<書　　式> network X:X::X:X/M (|backdoor)
<　no　　> no network X:X::X:X/M (|backdoor)
<備　　考>
- default information(::/0)を指定することも出来ます。
- default-information-check が無効の場合に、network ::/0 と neighbor default-originate を同時に設定すると、複数の default ルート情報がインストールされることにより、不要な update を送信してしまいます。そのため、両者を同時に設定することは推奨しません。
- 特定の BGP ルートを優先経路にしたくない場合、受け取った BGP ルートにローカル BGP の administrative distance を設定することで、優先順位を下げて、他のルートを優先させることが出来ます。

<説　　明> Address family onde から、exit します。
<書　　式> exit-address-family
<備　　考> show config 形式の設定を copy & paste するときに使用するためのコマンドです。
通常設定時は、exit で本ノードから抜けます。

<説　　明>
- Aggregate 機能を使うと、BGP ルートの集約を行うことが出来る集約ルートを構成するルートが、BGP テーブル内に少なくとも一つでも存在する場合に、集約ルートを作成し advertise します。

<書　　式> aggregate-address X:X::X:X/M (|summary-only) (|as-set)
<備　　考>
- Aggregate 機能では、集約ルートと一緒に集約前のルートも advertise します。集約ルートのみ advertise する場合は、summary-only を設定します。
- ルートの aggregate 設定を行った場合、AS パス情報が失われます。これによって、同じ AS に新しいルートとして受け取られてしまい、ルーティングループを引き起こす可能性があります。as-set を設定すると、ルート集約時に AS セット情報を含む形で広告することが可能になります。なお、この場合の AS セット集合は、順序不同でリストされたものです。

## ■ neighbor

○ activate

<説　　明>

・ 本機能を有効(activate)にすると、ipv4 neighbor 間および ipv6 neighbor 間で、ipv6 network を advertise します。

<書　　式> neighbor (A.B.C.D|X:X::X:X) activate　　(有効)

< no　> no neighbor (A.B.C.D|X:X::X:X) activate　　(無効)

<備　　考> activate を最初に設定します。

○ default-originate

<説　　明> default-originate が有効の場合、BGP により default ルートを配信します。

<書　　式> neighbor (A.B.C.D|X:X::X:X) default-originate　　(有効)

< no　> no neighbor (A.B.C.D|X:X::X:X) default-originate　　(無効)

<備　　考>

・ default-originate 無効:default ルートを配信しません。

・ default-originate 有効& default-import-check 無効:BGP により default ルートを配信します。

・ default-originate 有効& default-import-check 有効:
default ルートを保持している場合は、default ルートを配信します。
default ルートを保持していない場合は、default ルートを配信しません。

○ distribute-list

<説　　明>

・ peer に送信、または peer から受信するルート update のフィルタリングを行う場合に設定します。

<書　　式> neighbor (A.B.C.D|X:X::X:X) distribute-list ACL-NAME (in|out)

< no　> no neighbor (A.B.C.D|X:X::X:X) distribute-list ACL-NAME (in|out)

<備　　考> in を指定すると、peer から受信するルート update をフィルタリングします。
out を指定すると、peer へ送信するルート update をフィルタリングします。

○ filter-list

<説　　明> 指定した AS にマッチするルート情報をフィルタリングします。

<書　　式> neighbor (A.B.C.D|X:X::X:X) filter-list ACL-NAME

< no　> no neighbor (A.B.C.D|X:X::X:X) filter-list ACL-NAME

<備　　考> ip as-path access-list で設定した ACL-NAME を指定します。
in を指定すると、受信時にフィルタリングします。
out を指定すると、送信時にフィルタリングします。

○ next-hop-self
<説　　明>
・ 有効の場合、eBGP ルートを iBGP peer へ送信する nexthop 情報を、peer のルータとの通信に使用するインタフェースのアドレスに変更します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) next-hop-self
<　no　> no neighbor (A.B.C.D|X:X::X:X) next-hop-self
<備　　考>
・ 無効の場合、iBGP peer へ送信する nexthop 情報を、eBGP から貰った時のまま送信します。

○ remove-private-as
<説　　明>
・ remove-private-as を指定すると、private AS 番号を削除して、経路情報を advertise します。
<書　　式> neighbor (A.B.C.D|X:X::X:X) remove-private-as
<　no　> no neighbor (A.B.C.D|X:X::X:X) remove-private-as

○ route-map
<説　　明>
・ Peer に送信、または peer から受信するルートのフィルタリング や属性の操作をすることが出来ます。
<書　　式> neighbor (A.B.C.D|X:X::X:X) route-map WORD (in|out)
<　no　> no neighbor (A.B.C.D|X:X::X:X) route-map WORD (in|out)
<備　　考>
・ WORD には、route-map 名を指定します。
・ neighbor 毎に、in/out それぞれ 1 つの route-map を適用することができます。
・ 設定可能な属性や match 条件については、「第 29 章 route-map mode」を参照してください。

○ soft-reconfiguration
<説　　明>
・ BGP の neighbor パラメータや route-map の設定を変更した場合、その変更を適用するには、BGP セッションのクリア、もしくは BGP サービスの再起動が必要になります。
・ 本機能を有効にすることによって、neighbor とのセッションを維持したまま変更を適用することが出来ます(soft clear によって、BGP セッションのクリアを行います)。
<書　　式> neighbor (A.B.C.D|X:X::X:X) soft-reconfiguration inbound
<　no　> no neighbor (A.B.C.D|X:X::X:X) soft-reconfiguration inbound

■ **redistribute**

○ redistribute (connected|static)

<説　　明> connected route、static route を BGP で再配信する機能です。
Default ルート情報も再配信します。

<書　　式> redistribute (connected|static)

<　no　> no redistribute (connected|static)

○ redistribute (connected|static) route-map ABCD

<説　　明> routemap 機能を適用することにより、再配信時に特定の prefix のみを配信したり、特定の prefix を拒否したりすることができます。

<書　　式> redistribute (connected|static) route-map ABCD

<　no　> no redistribute (connected|static) route-map ABCD

# 第 46 章　terminal-server mode

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**terminal-server <0-1>**
nxrg240(config-ts)#

<説　　明>

・ Terminal-server 機能は、本装置のシリアルポート、または USB ポート(と USB シリアルコンバーター)に接続されたシリアル機器に TCP/IP(Telnet)で接続する機能です。

<備　　考>

・ Terminal-server の接続先シリアルポートとして、RS-232C、RJ-45、USB シリアルを指定することが出来ます。
・ CLI コンソールとシリアル通信用ポートを DIP SW で切り替える機器の場合、CLI コンソールで使用していないポートを、(terminal-server の接続先シリアルポートとして)自動的に使用します。
・ 設定番号は、シリアルポートから、USB0、USB1 と割り当てます。
terminal-server 0 シリアルポート(RS-232C/RJ-45:DIP-SW に依存)
terminal-server 1 USB0

◆ **baud-rate**

<説　　明> ボーレートを設定します。
<書　　式> baud-rate (300|600|1200|2400|4800|9600|19200|38400|57600|115200)

◆ **data-bits**

<説　　明> データビット(7 ビット、または 8 ビット)を設定します。
<書　　式> data-bits (7|8)

◆ **parity**

<説　　明> パリティを設定します。
<書　　式> parity (even|none|odd)
<備　　考> even(偶数)、odd(奇数)、none(なし)を指定します。

◆ **stop-bits**

<説　　明> ストップビット(1 ビット、または 2 ビット)を設定します。
<書　　式> stop-bits (1|2)

◆ **flow-control**

<説　　明> フロー制御を設定します。
<書　　式> flow-control (rtscts|xon-xoff|none)
< no > no flow-control (= flow-control none)
<備　　考>
・ XON/XOFF(ソフトウェア制御)、RTS/CTS(ハードウェア制御)、None(なし)を指定します。
・ XON/XOFF と RTS/CTS を同時に指定することも出来ます。

◆ **transport**

<説　　明> Telnet、または Raw を指定します。
<書　　式> transport (raw|telnet)

◆ **port**

<説　　明> Telnet クライアントから接続する際のポート番号を指定することが出来ます。
<書　　式> port <1024-65535>
<備　　考> 他の設定と重複しないように設定します。

◆ **idle-timeout**

<説　　明> 無通信切断タイマーを設定します。
<書　　式> idle-timeout <0-604800>
< no > no idle-timeout (=idle-timeout 0)
<備　　考> no を指定すると、idle-timeout が無効になります。

◆ **listen**

<説　　明> Telnet クライアントから接続可能な IP アドレスを指定することが出来ます。
指定がない場合、すべてのアドレスで接続を受け付けます。
<書　　式> listen address (A.B.C.D|X:X::X:X)
< no > no listen address
<備　　考>
・ listen address として指定した IP アドレスが、up/down する場合、設定した IP アドレスが追加 / 削除されても、自動的に listen 状態が無効 / 有効になるわけではありません。
・ そのため、IP アドレスの状態が変化した場合には、ユーザによる terminal-server の再起動が必要になります。
・ したがって、listen address を設定する場合、IP アドレスの up/down が発生しないように、loopback インタフェースに割り当てた IP アドレスなどを指定するようにします。

# 第 47 章　LXC container mode

**■ コンテナ型仮想化**

・ コンテナ型仮想化技術として、LXC に対応しています。対応するコンテナは、Debian/Ubuntu です。rootfs は、弊社から提供していません。

**◆コンテナ保存 disk の条件**

① コンテナで使用する rootfs は、USB や SD などのストレージ上に保存します。1 つの disk ストレージ上に、複数の rootfs を置き、それぞれ起動することが可能です。ただし、複数の rootfs を、一つのストレージ上に置く場合は、それぞれ異なるディレクトリに、rootfs を配置します。

② 保存領域は、ext4/vfat で、フォーマットします。

**◆ disk ストレージの eject/inject 時の動作**

・ LXC 起動中に、disk ストレージの eject を実行した場合、LXC を停止後、アンマウントします。

・ disk 挿入時、あるいは inject 実行時、disk ストレージは自動的にマウントされますが、LXC は自動起動しません。手動で LXC を起動してください(restart lxc)。

**◆コンテナとの通信**

・ コンソールに接続したい場合は、lxc console を使用します。LXC を最初に起動した際は、IP 通信が出来ないため、console を利用して各種設定を行います。

・ コンテナと NXR(host)は、veth interface 経由で、通信することが出来ます。

**◆ LXC の停止**

・ LXC が起動している状態で、LXC コンテナが置かれている disk ストレージを抜去する場合は、必ず shutdown コマンドで、LXC を停止させます。または、eject diskX を実行します。

・ システム再起動時は、LXC は自動的に停止します。

**◆ 移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**lxc container <1-4>**
nxrg240(config-lxc)#

**◆ mount rootfs**

<説　　明> rootfs をマウントします。
<書　　式> mount rootfs WORD
<備　　考> WORD には、ディスク名とディレクトリパス(例 disk1:/root)を入力します。

**◆ serial**

<説　　明>
・ 本装置の RS-232C や USB-Serial を LXC に割り当てることで、LXC のアプリから Serial にアクセスすることが出来ます。
<書　　式> serial <1-4>
< no　> no serial |<1-4>
<備　　考>
・ LXC に Serial を割り当てた場合、当該 Serial ポートは、NXR からアクセスすることが出来なくなります。

**■ 本装置の設定例(LXC)**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

・ LXC コンテナを設定します。
nxrg240(config)# lxc container 1
nxrg240(config-lxc)# exit

・ インタフェース bridge 1 の IP アドレスを設定します。
nxrg240(config)# interface bridge 1
nxrg240(config-bridge)# ip address 192.168.20.1/24
nxrg240(config-bridge)# exit

・ ブリッジ対象のインタフェース内で、ブリッジグループを設定します。
nxrg240(config)# interface ethernet 0
nxrg240(config-if)# bridge-group 1 port 1
nxrg240(config-if)# exit

・ veth1 インタフェースを設定します。
nxrg240(config)# interface veth 1

・ ブリッジ対象のインタフェース内で、ブリッジグループを設定します。
nxrg240(config-veth)# bridge-group 1 port 2
nxrg240(config-veth)# no ip address

・ lxc container 1 との仮想ブリッジを設定します。
nxrg240(config-veth)# lxc-link 1
nxrg240(config-veth)# exit
nxrg240(config)# exit
nxrg240(config)# save config

**■ LXC コンソール接続**

ここでは、本装置の CLI から LXC のコンソールに接続する方法について説明します。

**◆ lxc-link**

<説　　明> LXC のコンソールに接続します。
<書　　式> connect lxc console <1-4>
< mode > view mode

# 第 48 章　interface veth mode

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**interface veth <0-15>**
nxrg240(config-veth)#
<説　　明>

- Virtual ethernet pair(veth) interface は、コンテナ型仮想化との IP 通信を行う際に使用するインタフェースです。
- ホスト側(veth)とコンテナ側で使用するインタフェース(vethX-ct)がそれぞれ作成されます。
  1 対 1 で接続されているため、容易に本装置とコンテナ間の通信が可能になっています。
- コンテナに入れられたインタフェース(vethX-ct)は、ホスト側(本装置)で使用することは出来ません。

◆ **descripton**

<説　　明> インタフェースの説明を記述します。
<書　　式> description DESCRIPTION
<　no　　> no description (|DESCRIPTION)

◆ **ip address**

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

◆ **lxc-link**

<説　　明> lxc-link の設定を行います。
<書　　式> lxc-link <1-4>
<　no　　> no lxc-link
<備　　考> lxc-link 設定後、lxc 内部の eth0 と veth0 間で通信が可能になります。

◆ **veth hw-address**

<説　　明> veth interface の HW address を設定します。
<書　　式> veth hw-address <HH:HH:HH:HH:HH:HH>
<備　　考> hw-address の設定がない場合は、random 値が設定されます。
　　設定した HW address を削除する場合は、veth interface の削除が必要です。

◆ **bridge group**

<説　　明> bridge group を設定します。
<書　　式> bridge group <0-4095>

# 第 49 章　interface tap mode

◆ **移行 command**

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#interface tap <0-127>
nxrg240(config-tap)#

◆ **l2tpv3 access-group**

<説　　明> Xconnect インタフェースでの送受信に対して、l2tpv3 access-list を適用します。
<書　　式> l2tpv3 access-group (in|out) WORD
<　no　> no l2tpv3 access-group (in|out)
<備　　考>
- WORD: root の ACL 名を指定します。
  (root の ACL 名は、global モードの l2tpv3 access-list WORD root にて設定します。)
- in: Xconnect インタフェース→セッション(本装置への入力)方向のフィルタを適用します。
- out: セッション→ Xconnect インタフェース(本装置からの出力)方向のフィルタを適用します。

◆ **bridge-group**

<説　　明> インタフェースを bridge-group(仮想スイッチグループ)に参加させます。
<書　　式> bridge-group <0-4095>
bridge-group <0-4095> pathcost <0-65535>
bridge-group <0-4095> port <1-128>
bridge-group <0-4095> priority <0-255>
<　no　> no bridge-group (|<0-4095>)
no bridge-group <0-4095> (pathcost|priority)
<備　　考> bridge-group が未設定(interface bridge が未設定)の場合、join に失敗します。

■ l2tpv3 l2rp
<説　　明> L2TPv3 L2RP(冗長化構成)の設定をします。

○ enable
<説　　明> L2RP を有効にします。
<書　　式> l2tpv3 l2rp <1-255> enable
<　no　> no l2tpv3 l2rp <1-255> enable

○ type
<説　　明> Master を選択する方法を指定します。
　　Default では、priority の比較によって判定します。
<書　　式> l2tpv3 l2rp <1-255> type (priority|active)
<　no　> no l2tpv3 l2rp <1-255> type
<初 期 値> l2tpv3 l2rp <1-255> type priority
<備　　考> priority を選択した場合、priority 値の大きい方が、master になります。
　　active を選択した場合、active session 数の多い方が、master になります。

○ priority
<説　　明> Master の選定に使用する priority 値を設定します。
<書　　式> l2tpv3 l2rp <1-255> priority <1-255>
<　no　> no l2tpv3 l2rp <1-255> priority
<初 期 値> l2tpv3 l2rp <1-255> priority 100

○ preempt
<説　　明> Priority 値の小さいものが master で、大きいものが backup となることを許可するかどうかの設定です。
<書　　式> l2tpv3 l2rp <1-255> preempt
<　no　> no l2tpv3 l2rp <1-255> preempt
<初 期 値> l2tpv3 l2rp <1-255> preempt
<備　　考>
・ preempt 有効時、Master 選択の判定基準(type で指定した判定方法)に従います。
・ preempt 無効時、priority(または session 数)の大きい LCCE が現れた場合に、backup へと遷移しません。

○ block-reset
<説　　明> 自身のポートのリンク状態を一時的に down させ、配下のスイッチの MAC テーブルをフラッシュします。
<書　　式> l2tpv3 l2rp <1-255> block-reset
<　no　　> no l2tpv3 l2rp <1-255> block-reset
<備　　考>
・ Group blocking 状態に遷移した場合のみ動作します。
・ Group blocking とは、自身で送信した Advertise Frame を受信した場合や、対向 LCCE の Advertise Frame を受信した場合に、Loop が発生していると判断して、Frame の転送を停止している状態です。

○ timers advertise
<説　　明> L2RP Advertise Frame を送信する間隔を指定します。
<書　　式> l2tpv3 l2rp <1-255> timers advertise <1-60>
<　no　　> no l2tpv3 l2rp <1-255> timers advertise
<初 期 値> l2tpv3 l2rp <1-255> timers advertise 1

○ timers delay
<説　　明> L2TP session 確立後、timers delay で指定した時間、Group Blocking 状態となり、Frame の転送を行いません。
<書　　式> l2tpv3 l2rp <l2rpid:1-255> timers delay <0-60>
<　no　　> no l2tpv3 l2rp <1-255> timers delay
<初 期 値> l2tpv3 l2rp <l2rpid:1-255> timers delay 0
<備　　考>
・ L2RP は、主に Loop が発生する環境で使用されます。そのような環境では、L2RP Frame を受信するまで(Loop を検出するまで)の間、Blocking 機能が動作しないので、一時的に Broadcast Storm が発生します。timers delay を設定することで、Broadcast Storm を回避することが出来ます。
・ timers advertise より、長い時間を設定することを推奨します。

○ port-reset
<説　　明>
・ L2TP Group 機能や L2RP 機能により、L2TP session の切替が発生した際、配下スイッチの FDB において、MAC アドレスのエントリーが更新されていないため、最大 5 分間通信できないことがあります。
・ port reset 機能を有効にした場合、master → backup(または、master → init)へ遷移した際に、L2RP インタフェースのリンクを一時的に down させることで、配下スイッチの FDB を flush させます。
<書　　式> l2tpv3 l2rp <l2rpid:1-255> port-reset
<　no　　> no l2tpv3 l2rp <1-255> port-reset
<初 期 値> no l2tpv3 l2rp <1-255> port-reset

# 第 50 章　ssl tunnel mode

## ■ SSL Tunnel

・ SSL(Secure Socket Layer)は、データを暗号化して送受信を可能とするプロトコルです。SSL
・ tunnel を利用することによって、SSL 非対応の既存の TCP 通信を、暗号化(SSL 化)することが出来ます。
・ 本バージョンでは、SMTP の SSL 化に対応しています。

### ◆ 移行 command

nxrg240#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#ssl tunnel <0-2>
nxrg240(config-ssl-tunnel)#

### ◆ descripton

<説　　明> インタフェースの説明を記述します。
<書　　式> description DESCRIPTION
<　no　　> no description (|DESCRIPTION)

### ◆ version

<説　　明> バージョンを指定します。
　　Default では、すべてのバージョンに対応します。
<書　　式> version (tlsv10|tlsv11|tlsv12)
<　no　　> no version
<備　　考>
・ 対応する SSL/TLS バージョンは、以下のとおりです(SSL v2.0/v3.0 には未対応です。)。
　　tlsv10 TLS version 1.0
　　tlsv11 TLS version 1.1
　　tlsv12 TLS version 1.2

### ◆ set protocol

<説　　明> プロトコルを指定します。
<書　　式> set protocol smtp
<　no　　> no set protocol smtp
<備　　考> 本バージョンで指定可能なプロトコルは SMTP です。

### ◆ remote address

<説　　明> SSL tunnel の接続先(または転送先)アドレス、および TCP ポート番号を指定します。
<書　　式> remote address ip (A.B.C.D|FQDN) port <1-65535>

◆ **listen address**

<説　　明>

・ クライアントの場合、SSL 化するパケットを受信するアドレスとポート番号を指定します。
・ サーバの場合、SSL パケットの受信アドレスとポート番号を指定します。

<書　　式> listen address ip localhost port <1-65535>

・ 本バージョンでは、アドレスに、localhost を指定します。
・ localhost を指定した場合、以下の TCP ポート番号を指定することは出来ません。
9696, 4001, 4002, 2600, 3001

# 第 51 章　Web authentication extension mode

**外部サーバ連携機能**

web-authenticate mode で、authenticate post-ext-html を設定することで、外部 WEB サーバ連携機能(post でのアクセス)が有効になります。

### ◆ 移行 command

wxr250#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
wxr250(config)#**web-auth-extension <1-16>**
wxr250(config-webauth-ext)#

### ■ ネットワーク設定

<説　　明> post 認証を行う端末のネットワークアドレス範囲を指定します。
<書　　式> network (A.B.C.D/M|X:X::X:X/M)
< no > no network
<備　　考>

- 外部サーバ連携機能の有効時は、端末からのアクセスに対して、web-auth-extension <1-16> の番号順にネットワーク設定(network A.B.C.D/M|X:X::X:X/M)を検索し、該当する web-auth-extension の設定で動作します。
- 該当するネットワーク設定が存在しない場合、認証エラーのリザルト画面が表示されます。
- 該当するネットワーク設定が複数存在する場合は、web-auth-extension の番号の小さい設定で動作します。

### ◆ account authenticate

<説　　明> RADIUS 認証を行う場合に設定します。
<書　　式> account authenticate (none|radius|disable)
< no > no account authenticate
<初 期 値> account authenticate none
<備　　考>

- radius を指定すると、post アクセスで渡されるユーザ ID とパスワードのデータを元に、該当ネットワークの radius server にアクセスして認証を行います。
- none を指定すると、認証を行いません(認証 OK として動作します)。また、POST データ(ユーザ ID、パスワード)に関するチェックも行いません。
- disable を指定すると、認証 NG として動作します。
- web-authenticate mode で、log enable を設定すると、認証時のログを syslog に出力します。

◆ **radius server**

<説　　明> RADIUS サーバの設定を行います。
<書　　式>
radius (A.B.C.D|X:X::X:X) password (|hidden) PASSWORD (|auth-port <1645|1812|<1024-65535>)
radius (A.B.C.D|X:X::X:X) auth-port (1645|1812|<1024-65535>)
<　no　>
　no radius (A.B.C.D|X:X::X:X) (設定を削除します)
　no radius (A.B.C.D|X:X::X:X) auth-port (auth-port のみを初期値(1645)に戻します)
<備　　考>
・ RADIUS サーバは、2 つまで設定することが出来ます。
・ RADIUS サーバへのアクセスタイムアウトは 5 秒で、リトライは 2 回行います(タイムアウト値および、リトライ回数を変更することは出来ません)。

◆ **radius attribute**

<説　　明> 送信アトリビュートの設定を行います。
<書　　式> radius attribute nas-identifier WORD
　　radius attribute nas-ip-address A.B.C.D
　　radius attribute nas-ipv6-address X:X::X:X
　　radius attribute chap-password
<　no　> no radius-attribute
<備　　考>
・ RADIUS サーバへの送信アトリビュートは、上記アトリビュート(NAS-IP-Address, NAS-Identifier)および、User-Name, User-Password, Login-IP-Host(端末の IP アドレス)、Message-Authenticator です。
・ chap-password を設定した場合は、User-Password の代わりに、CHAP-Password を使用します。

◆ **radius idle-timeout attribute**

<説　　明> 受信時に適応する timeout 値のアトリビュート指定を行います。
<書　　式> radius idle-timeout attribute
　　(ascend-idle-limit|ascend-idle-limit-vsa|idle-limit)
<　no　> no radius idle-timeout attribute
<備　　考> web-authenticate mode で、close 設定を行ってください。

◆ **radius session-timeout attribute**

<説　　明> session-timeout 値に使用する attribute の設定を行います。
<書　　式> radius session-timeout attribute
　　(ascend-maximum-time|ascend-maximum-time-vsa|session-timeout)
<　no　> no radius session-timeout attribute

◆ **no radius**

<説　　明> すべての RADIUS 設定を削除します。
<書　　式> no radius

◆ **access-url**

<説　　明> 指定ネットワーク内に対して、転送先 URL を指定します。
<書　　式> access-url URL
<　no　　> no access-url
<初 期 値> no access-url
<備　　考>
・ URL は、http://www.centurysys.co.jp、または https://www.centurysys.co.jp のように記載します。
・ access-url は、Web 認証が未認証の端末でもアクセス可能な URL を指定します。
・ access-url 設定が無い場合は、認証エラーのリザルト画面が表示されます。

◆ **redirect-url**

<説　　明> 指定ネットワーク内に対して、認証 OK の場合の転送先 URL を指定します。
<書　　式> redirect-url URL
<　no　　> no redirect-url
<初 期 値> no redirect-url
<備　　考>
・ URL は、http://www.centurysys.co.jp、または https://www.centurysys.co.jp のように記載します。
・ redirect-url 設定が無い場合は、認証エラーのリザルト画面が表示されます。

◆ **failure-url**

<説　　明> 指定ネットワーク内に対して、認証エラーの場合の転送先 URL を指定します。
<書　　式> failure-url URL
<　no　　> no failure-url
<初 期 値> no failure-url
<備　　考>
・ URL は、http://www.centurysys.co.jp、または https://www.centurysys.co.jp のように記載します。
・ failure-url は、Web 認証が未認証の端末でもアクセス可能な URL を指定します。
・ failure-url 設定が無い場合は、認証エラーのリザルト画面が表示されます。

◆ **receive option permit-source**

<説　　明> POST で受信した source_address が、設定したネットワークアドレスの範囲内の場合、POST で指定されたアドレスで WEB 認証動作が行われます。
<書　　式> receive option permit-source A.B.C.D/M
<　no　> no receive-option permit-source
<初 期 値> no receive-option permit-source
<備　　考>
・ 0.0.0.0/0 を指定した場合、POST で指定されたすべてのアドレスで、WEB 認証動作が行われます。
・ 設定が無い場合、POST で source_address の指定を行っても無視されます(アクセスしたアドレスで動作します)。

◆ **receive-option password-key**

<説　　明> POST で受信した password_key が一致した場合、POST での設定を受け付け、POST で指定されたアドレスで WEB 認証動作が行われます。
<書　　式> receive option password-key (|hidden) PASSWORD)
<　no　> no receive-option password-key
<初 期 値> no receive-option password-key
<備　　考>
・ 設定が無い場合、POST で password_key の有無にかかわらず、POST での設定を受け付けます。

◆ **receive-option idle-timeout**

<説　　明> POST からの idle_timeout の設定を受け付け、その値で WEB 認証動作を行います。
<書　　式> receive-option idle-timeout
<　no　> no receive-option idle-timeout
<初 期 値> no receive-option idle-timeout
<備　　考>
・ 設定がない場合、POST からの idle_timeout の設定は無視されます。

◆ **receive-option session-timeout**

<説　　明> POST からの session_timeout の設定を受け付け、その値で WEB 認証動作を行います。
<書　　式> receive-option session-timeout
<　no　> no receive-option session-timeout
<初 期 値> no receive-option session-timeout
<備　　考>
・ 設定がない場合、POST からの session_timeout の設定は無視されます。

# 第 52 章　dns-intercept mode

## ■ DNS インターセプト機能

DNS インターセプト機能は、特定ドメインに関する DNS 名前解決の際に、本装置を通過、または本装置で受信する DNS レスポンスパケットをインターセプトし、A レコードの IPv4 アドレスとドメインの対応付けを学習する機能です。学習した情報は、PBR の条件として利用することが出来ます。

### ◆ DNS アドレスの指定

本装置を送信元とする DNS パケット、または本装置を経由する DNS パケットのうち、監視対象となる DNS レスポンスパケットの送信元 IPv4 アドレス(通常は DNS のアドレス)、および UDP ポート番号を指定します。

### ◆ドメインリストのインポート

インターセプトするドメインのリストを、外部サーバからインポートすることが出来ます。
プレインテキスト、または xml 形式のファイルに対応しています。

- プレインテキストの場合、各ドメインを IPv4 アドレスと FQDN で指定することが出来ます。
- XML の場合、Microsoft 社が提供するドメインリストファイルに対応しています。

※ ip dns-intercept setname コマンド(global mode)を使用します。

### ◆スケジュールによるドメインリストの取得

ドメインリストは、スケジュール機能により、定期的に取得・更新することが可能です。
※ schedule コマンド(global mode)を使用します。

**◆ 移行 command**

nxrg260#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg240(config)#**dns-intercept <0-3>**
nxrg240(config-dns-intercept)#

特定ドメインに関する DNS 名前解決の際に、本装置を通過、または本装置が受信する DNS レスポンスパケットをインターセプトし、その A レコードの IPv4 アドレスとドメインの対応付けを学習する機能です。
学習した情報は、本装置を通過するパケットの match 条件リスト(dns-set)として指定することで、PBR の条件として使用することが出来ます。

○ address
<説　　明>
・ 監視対象となる DNS レスポンスパケットの送信元 IPv4 アドレス(通常は DNS のアドレス)を指定します。
<書　　式> address A.B.C.D
<　no　　> no address
<備　　考> 最大 4 つまで指定することが出来ます。

○ listen udp local-port
<説　　明> UDP のローカルポート番号を指定します。
<書　　式> listen udp local-port <49152-65535>
<　no　　> no listen udp local-port
<初 期 値> listen udp local-port 50053

○ listen udp src-port
<説　　明> UDP のソースポート番号を指定します。
<書　　式> listen udp src-port <1-65535>
<　no　　> no listen udp src-port
<初 期 値> listen udp src-port 53

○ match ip setname
<説　　明>
・ インターセプトするドメインを外部サーバから、plain テキスト、または xml 形式のファイルによって取り込むことが出来ます。
<書　　式> match ip setname WORD
<　no　　> no match ip setname WORD
<備　　考>
・ 最大 8 つまで設定することが出来ます。
・ ドメインリストが plain テキストの場合、IPv4 アドレス形式と FQDN 形式による指定が可能です。
・ ドメインリストが xml 形式の場合、マイクロソフト社が提供するドメインリストファイルに対応しています(本バージョンでは、ドメインリスト内の office365 の情報のみ使用します)。

○ min-ttl
<説　　明>
・ 通常、各エントリーの生存時間として、DNS レスポンスパケット内の TTL を利用しますが、ユーザが TTL の最大値／最小値を設定することも出来ます。
<書　　式> min-ttl <120-4294967>
<初 期 値> 無し
<　no　> no min-ttl

○ max-ttl
<説　　明>
・ 通常、各エントリーの生存時間として、DNS レスポンスパケット内の TTL を利用しますが、ユーザが TTL の最大値／最小値を設定することも出来ます。
<書　　式> max-ttl <120-4294967>
<初 期 値> 無し
<　no　> no max-ttl

○ignore-auto-dns
<説　　明> 本機能を有効にすると、DHCP/IPCP で取得した DNS を使用しません。
<書　　式> ignore-auto-dns enable
<　no　> no ignore-auto-dns enable
<備　　考>
・dns-intercept mode で設定した場合、すべてのインタフェースで、本機能が有効になります。
!
 dns-intercept 0
 ignore-auto-dns enable（有効）
!
 interface tunnel 0
 ip dns-intercept 0（有効）
!
 interface tunnel 1
 ip dns-intercept 0（有効）
!
・dns-intercept mode で設定しない場合、設定したインタフェースだけで、本機能が有効になります。
!
 dns-intercept 2
 no ignore-auto-dns enable（無効）
!
 interface tunnel 2
 ip dns-intercept 2 ignore-auto-dns（有効）
!
 interface tunnel 3
 ip dns-intercept 2（無効）
!

◆ margin-ttl
<説　　明> TTL margin を設定することが出来ます。
<書　　式> margin-ttl <0-604800>
<初 期 値> margin-ttl 10
<　no　> no margin-ttl

# 第 53 章　interface MAP mode

◆ **移行 command**

nxrg260#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg260(config)#**interface map <0-1>**
nxrg260(config-map)#

◆ **description**

<説　　明> インタフェースの説明を記述します。
<書　　式> description DESCRIPTION
<　no　> no descritpion

◆ **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
　　ip address mape-rule
<　no　> no ip address (|A.B.C.D/M)
<備　　考>
・ 手動による固定割り当て、および MAP-E rule により取得したアドレス割り当てに対応しています。

◆ **tunnel mode ipipv6 mape-rule**

<説　　明> MAP-E rule 名を指定します。
<書　　式> tunnel mode ipipv6 mape-rule WORD
<備　　考> WORD には、MAP-E rule 名を指定します。
　　MAP-E rule 名は、mape-rule コマンド(global mode)で指定します。

◆ **tunnel hop-limit**

<説　　明> hop-limit 値を指定することが出来ます。
<書　　式> tunnel hop-limit <1-255>
<初 期 値> tunnel hop-limit 64
<　no　> no tunnel hop-limit
<備　　考> 指定した hop-limit 値は、ipv6 ヘッダ部に設定されます。

◆ **tunnel traffic-class**

<説　　明> トンネル IPv6 ヘッダのトラフィッククラスフィールドに設定する値を指定します。
<書　　式> tunnel traffic-class <0-252>
　　tunnel traffic-class inherit
<初 期 値> tunnel traffic-class inherit
<　no　> no tunnel traffic-class
<備　　考>
・ inherit を指定した場合、トネリングパケットのヘッダ部の ToS 値またはトラフィッククラスを、トンネル IPv6 ヘッダのトラフィッククラスフィールドにコピーします。
・ 値を指定する場合、0-252 の範囲で指定することが出来ます。ただし、ECN フィールドを設定することはできません。
※ ECN field の扱いについては、「付録 B 1.2.4.1 ECN field の扱い」を参照してください。

◆ **tunnel encap-limit**

<説　　明> 1 つのパケットで許可される入れ子のトンネリングのレベル数を指定します。
<書　　式> tunnel encap-limit <0-255>
<初 期 値> tunnel encap-limit 4
<　no　> no tunnel encap-limit （=無効）
<備　　考> 本設定は、ipv6 トンネルにのみ適用されます。

◆ **bandwidth**

<説　　明> インタフェースの帯域幅を設定することが出来ます。
　　bandwidth の初期値は、10Mbps です。
　　bandwidth の最大値は、10Gbps です。
<書　　式> bandwidth <1-10000000000[k/m/g]>
<　no　> no bandwidth
<備　　考> 本機能は、OSPF のコスト計算時のみに使用します。
　　基準となる帯域幅は、auto-cost コマンド（ospf mode）にて設定します。

◆ **mtu**

<説　　明> MTU の値を設定します。
<書　　式> mtu <bytes:68-1500>
<初 期 値> mtu 1500
<　no　> no mtu （= mtu 1500）

◆ **ip rebound**

<説　　明>

- 下位ルータから受信したパケットを、受信インタフェースと同一インタフェースから出力（forwarding）した場合、下位ルータから NXR に対して再度パケットが送信されてくるため、下位ルータと NXR の間で TTL が「0」になるまでパケットがループします。
- IP rebound 機能を無効にすると、受信インタフェースと送信インタフェースが同一の場合、パケットをドロップし、かつ送信元に destination unreachable を送信します。
- Default は、有効です（受信インタフェースと送信インタフェースが同一でもドロップしません）。

<書　　式> ip rebound
<初 期 値> ip rebound
<　no　> no ip rebound

### ◆ ip tcp adjust-mss

<説　　明>

・ Path MTU Discovery(PMTUD)機能(End-to-end でフラグメントが発生しない最大の MTU を発見すること)によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器(ルータ等)が ICMP fragment needed をフィルタリングしている場合(ブラックホールルータが存在する場合)や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、Endtoend での通信に支障をきたすことになります。このような場合、TCP では SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

<書　　式> ip tcp adjust-mss (auto|<500-1460:bytes>)

<初 期 値> no ip tcp adjust-mss

<　no　> no ip tcp adjust-mss

<備　　考>

・ IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。

・ suto を指定すると、本装置が自動で MSS 値を設定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ ユーザが設定する場合は、MSS 値を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。

・ 「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

### ◆ ip mask-reply

<説　　明>

・ OpenView などの監視装置では、監視ネットワーク内の機器に対して ICMP address mask request (type=17)を送信することによって機器のインタフェースのネットマスク値を取得します(単純に、死活監視で使用する場合もあります)。

・ 本装置では、ICMP address mask request への応答の有無を設定することが出来ます。

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

<初 期 値> no ip mask-reply(ICMP address mask request に応答しません。)

<　no　> no ip mask-reply

<備　　考>

・ ICMP address mask request/reply の例は、interface mode の ip mask-reply を参照して下さい。

### ◆ ip reassemble-output

<説　　明>

・ インタフェースの MTU(あるいは PMTU)より大きいパケットを IP forwarding する際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。本設定有効時、NXR がリアセンブルしたパケットは、以下のようにフラグメント処理を行います。
  - fragmented packet(パケットの断片)が MTU を超える場合、リアセンブルしたパケットを再度 MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、リアセンブルしたパケットを出力します。

<書　　式> ip reassemble-output

<初 期 値> ip reassemble-output

<　no　　> no ip reassemble-output

<備　　考>

・ 上記の場合(本設定が有効の場合)、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易な IP 実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズで NXR からパケットを出力します。また、出力時の IP フラグメント処理は、次のようになります。
  - fragmented packet(パケットの断片)が MTU を超える場合、受信した fragmented packet を MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、受信した fragmented packet をそのままのサイズで出力します。
・ Default は、global 設定および interface 設定ともに有効です。Global 設定と interface 設定の AND 条件により、本機能が有効か無効かを判定します。本設定は、IP forwarding するパケットにのみ影響します。
・ 受信時のサイズを記載しておくバッファが 32 個しかないため、33 個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-output が有効な場合と同様に処理します。

◆ **ip access-group**

<説　　明>
・ global mode で設定した ACL をインタフェースに適用することで、パケットフィルタリングを行うことができます。
<書　　式> ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
<　no　> no ip access-group (in|out|forward-in|forward-out)
<備　　考>
・ 各インタフェースへのパケットフィルタリングの適用箇所(付録の Packet Traveling を参照)は、以下の 4 ヶ所です。
  - in(local input) NXR 自身で受信して処理するパケットを制限します。
  - out(local output) NXR 自身が作成して出力するパケットを制限します。
    トンネリングされたパケットも NXR 自身が作成したパケットとして認識します。
  - forward-in NXR が当該インタフェースで受信して forwarding するパケットを制限します。
  - forward-out NXR が受信して当該インタフェースへ forwarding するパケットを制限します。
・ mac 指定のある ACL は、out および forward-out に設定することは出来ません。

◆ **ip masquerade**

<説　　明>
・ インタフェースよりパケットを出力する際に、パケットの送信元 IPv4 アドレスを出力インタフェースの IPv4 アドレスに自動変換する機能です。
<書　　式> ip masquerade（有効）
<初 期 値> no ip masquerade(無効)
<　no　> no ip masquerade
<備　　考>
・ TCP/UDP/ICMP のみ対応しています。その他のプロトコルに関しては、動作保証はありません。
・ IPv6 パケットは、IP マスカレードの対象外です。
・ forward out/local output フィルタリング適用後のパケットに、IP マスカレードを適用します。

◆ ip (snat-group|dnat-group)

<説　　明>
・ global mode で設定した SNAT または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。
・ SNAT は、パケットの出力時に適用されます。DNAT は、パケットの入力時に適用されます。
<書　　式> ip (snat-group|dnat-group) NAT-NAME
<　no　> no ip (snat-group|dnat-group)
<備　　考> NAT ルールの設定は、ip snat/ip dnat)コマンド(global mode)で行います。

### ◆ ip spi-filter

<説　　明>
- 簡易ファイヤウォールの一つとして、SPI(Stateful Packet Inspection)機能をサポートします。
- パケットに関連するコネクションの状態を見て、当該パケットをドロップするかしないかを決める機能です。

<書　　式> ip spi-filter (有効)
<初 期 値> no ip spi-filter(無効)
<　no　　> no ip spi-filter
<備　　考>
- コネクションの状態が、established または related の場合に、パケットの転送を許可します。
- Established とは、すでに双方向でパケットの通信がありコネクションが確立されている状態です。
- Related とは、すでに確立しているコネクションがある状態です。FTP のデータ転送等がこれに該当します。
- 新しい接続でありながら、syn ビットの立っていないパケットはドロップします。
- SPI は、forward in および local input の位置で適用されます。ユーザが適用位置を変更することは出来ません。

### ◆ netevent

<説　　明>
- トラックイベントの発生時に、当該 tunnel を接続／切断／再接続することが出来ます。

<書　　式> netevent <trackid:1-255> (connect|disconnect|reconnect)
　　netevent <trackid:2048-4095> (connect|disconnect|reconnect)
<　no　　> no netevent

### ◆ ipsec policy

<説　　明> 当該インタフェースで使用する IPsec ローカルポリシーを設定します。
<書　　式> ipsec policy <local policy:1-255>
<　no　　> no ipsec policy (|<local policy:1-255>)
<備　　考>
- 各インタフェースに、IPsec ローカルポリシーを 4 つまで設定することが出来ます。他のインタフェースで既に設定している IPsec ローカルポリシーは、重複して設定できません。

### ◆ ipsec policy-ignore

<説　　明>
- IPsec policy のチェックを行わないように指定する機能です。IPsec policy として any などを指定したけれども、特定の通信のみ IPsec 化したくない場合に、この機能を使用します。

<書　　式> ipsec policy-ignore (input|output)
<初 期 値> no ipsec policy-ignore(無効)
<　no　　> no ipsec policy-ignore
<備　　考>
- Input を指定した場合、inbound policy check を実行しないため、IPsec 化されてくるべきパケットがドロップ されてしまう現象を回避することができます。
- Output を指定した場合、当該インタフェースから出力されるパケットは、IPsec policy をチェックしないため平文で送信されます。

◆ **QoS**

○ classify

<書　　式> classify (input|output) route-map ROUTEMAP

<備　　考>

・ インタフェースにルートマップを適用します。1 つのインタフェースに、input と output を別々に設定することが出来ます。

・ input で指定したルートマップは、PRE-ROUTING(付録の Packet Traveling を参照)で適用されます。

・ output で指定したルートマップは、POST-ROUTING(付録の Packet Traveling を参照)で適用されます。

○ no classify

<書　　式> no classify (|input|output)

<備　　考>

・ インタフェースに適用したルートマップを削除します。

◆ **session invalid-status-drop-interface**

<説　　明>

・ session invalid-status-drop 機能(global mode 参照)をインタフェース毎に指定することができます。

・ 本機能は、default で無効です。

<書　　式> session invalid-status-drop-interface enable

<初 期 値> no session invalid-status-drop-interface enable

<　no　> no session invalid-status-drop-interface enable

<備　　考>

・ あるインタフェースに対してのみ適用したい場合は、global mode で session invalid-status-drop 機能を無効にして、かつ本機能を指定インタフェースで有効にします。以下は、map 0 インタフェースに適用する場合の設定例です。

- global mode で、session invalid-status-drop を無効にします。
  nxrg260(config)#no session invalid-status-drop enable
- 指定インタフェースで、本機能を有効にします。
  nxrg260(config)#interface map 0
  nxrg260(config-map)#session invalid-status-drop-interface enable

◆ **ip multicast-to-unicast**

<説　　明> 有効時、multicast を unicast 変換したパケットを転送します。

<書　　式> ip multicast-to-unicast forwarding　　(有効)

<　no　> no ip multicast-to-unicast forwarding　　(無効)

◆ **cms watch enable**

<説　　明> インタフェースの up/down 時に、インタフェースの監視情報を CMS に送信します。

<書　　式> cms watch enable

<　no　> no cms watch enable

### ◆ ip send-source

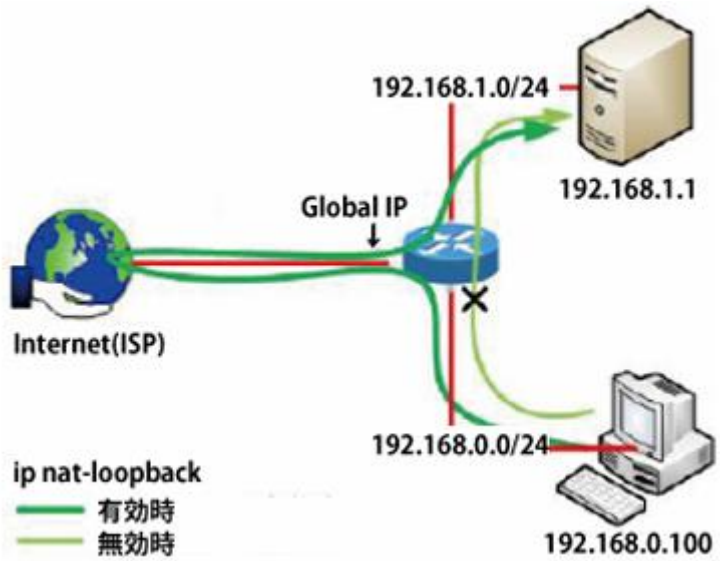
<説　　明>
- 本機能の有効時、当該インタフェースの IP アドレスをソースアドレスとするパケットは、当該インタフェースから出力します。
- 本機能の無効時、ルーティングテーブルで指定されたインタフェースから出力します。
- 本機能の有効時、当該インタフェースから出力するパケットは、ipsec policy にマッチしても暗号化せずに出力します。

<書　　式> ip send-source (|local)
<初 期 値> no ip send-source
<　no　　> no ip send-source
<備　　考>
- ip send-source local を設定した場合、本機能の対象は、NXR からの自発パケットのみです。ip natloopback 機能と併用する場合は、本機能を有効にします。

### ◆ ip nat-loopback

<説　　明>
- 1 つのグローバル IP を使用して複数の Web/Mail サーバなどを公開する場合、DNAT 機能により内部サーバへの転送を行うことがあります。しかしながら、(下図のような環境で)NAT ルータ配下の端末からグローバル IP にアクセスしても、DNAT 変換が行われないため、公開サーバにアクセスできません。このような場合に、本機能を使用します。

<書　　式> ip nat-loopback
<初 期 値> no ip nat-loopback
<　no　　> no ip nat-loopback
<備　　考>
- ip nat-loopback を設定しているインタフェース上で SPI を設定している場合は、フィルタを適切に設定して、必要なパケットを許可してください。
- また、当該インタフェースで、NAT(または ip masquerade)を設定してください。未設定の場合、公開サーバにアクセスできない場合があります。




- 本装置で DNAT を設定します。
  Global IP(当該インタフェース):80 へのアクセスを、192.168.1.1 に変換します。
- PC より Global IP:80 にアクセスします。

# 第 54 章　interface WWAN mode

■ 本機能は、QMI 対応モバイルモジュールを搭載した機種にて動作します。

**◆ 移行 command**

nxrg180#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg180(config)#**interface wwan <0-0>**
nxrg180(config-wwan)#

**◆ mobile apn**

<説　　明> APN を設定します。
<書　　式> mobile apn XXXX cid XX pdp-type (ip|ipv6|ppp)
<　no　> no mobile apn

**◆ wwan authentication**

<説　　明> WWAN の認証プロトコルを設定します。
<書　　式> wwan authentication (chap|pap)
<　no　> no wwan authentication

**◆ wwan username**

<説　　明> WWAN 接続のユーザー ID とパスワードを設定します。
<書　　式> wwan username USERID password (|hidden) PASSWORD
<　no　> no wwan 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。
・パスワードに「?」を入力する場合は、「Ctrl」+「v」を入力してから、「?」を入力してください。

**◆ wwan auto-connect**

<説　　明> WWAN の自動接続を有効にします。
<書　　式> wwan auto-connect
<　no　> no wwan auto-connect

**◆ wwan area-check**

<説　　明> WWAN 接続後、60 秒周期で指定回数まで、WCDMA の状態が続くことを監視します。
　　回数を超えると module のリセットを実施し、切替を試みます。
<書　　式> wwan area-check <1-1440>
<　no　> no wwan area-check

◆ **description**

<説　　明> インタフェースの説明を記述します。
<書　　式> description DESCRIPTION
<　no　　> no descritpion

◆ **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（= mtu 1500）

◆ **ip tcp adjust-mss**

<説　　明>

- Path MTU Discovery(PMTUD)機能(End-to-end でフラグメントが発生しない最大の MTU を発見すること)によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器(ルータ等)が ICMP fragment needed をフィルタリングしている場合(ブラックホールルータが存在する場合)や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、End-toend での通信に支障をきたすことになります。このような場合、TCP では SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

<書　　式> ip tcp adjust-mss (auto|<500-1460:bytes>)
<初 期 値> no ip tcp adjust-mss
<　no　　> no ip tcp adjust-mss
<備　　考>

- IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。
- suto を指定すると、本装置が自動で MSS 値を設定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。
- ユーザが設定する場合は、MSS 値を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。
- UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。
- 「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

◆ **ip reassemble-output**

<説　　明>

・ インタフェースの MTU(あるいは PMTU)より大きいパケットを IP forwarding する際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。
本設定有効時、本装置がリアセンブルしたパケットは、以下のようにフラグメント処理を行います。
  - fragmented packet(パケットの断片)が MTU を超える場合、リアセンブルしたパケットを再度 MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、リアセンブルしたパケットを出力します。

<書　　式> ip reassemble-output

<初 期 値> ip reassemble-output

<　no　　> no ip reassemble-output

<備　　考>

・ 上記の場合(本設定が有効の場合)、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易な IP 実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズで本装置からパケットを出力します。また、出力時の IP フラグメント処理は、次のようになります。
  - fragmented packet(パケットの断片)が MTU を超える場合、受信した fragmented packet を MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、受信した fragmented packet をそのままのサイズで出力します。
・ Default は、global 設定および interface 設定ともに有効です。Global 設定と interface 設定の AND条件により、本機能が有効か無効かを判定します。本設定は、IP forwarding するパケットにのみ影響します。
・ 受信時のサイズを記載しておくバッファが 32 個しかないため、33 個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-output が有効な場合と同様に処理します。

◆ **ip access-group**

<説　　明>
- global mode で設定した ACL をインタフェースに適用することで、パケットフィルタリングを行うことができます。

<書　　式> ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
<　no　> no ip access-group (in|out|forward-in|forward-out)
<備　　考>
- 各インタフェースへのパケットフィルタリングの適用箇所(付録の Packet Traveling を参照)は、以下の 4 ヶ所です。
  - in(local input) NXR 自身で受信して処理するパケットを制限します。
  - out(local output) NXR 自身が作成して出力するパケットを制限します。
    トンネリングされたパケットも NXR 自身が作成したパケットとして認識します。
  - forward-in NXR が当該インタフェースで受信して forwarding するパケットを制限します。
  - forward-out NXR が受信して当該インタフェースへ forwarding するパケットを制限します。
- mac 指定のある ACL は、out および forward-out に設定することは出来ません。

◆ **ip masquerade**

<説　　明>
- インタフェースよりパケットを出力する際に、パケットの送信元 IPv4 アドレスを出力インタフェースの IPv4 アドレスに自動変換する機能です。

<書　　式> ip masquerade（有効）
<初 期 値> no ip masquerade(無効)
<　no　> no ip masquerade
<備　　考>
- すべてのインタフェース(Ethernet/VLAN/PPP/Tunnel)で設定することが出来ます。
- TCP/UDP/ICMP のみ対応しています。その他のプロトコルに関しては、動作は保証しません。
- IPv6 パケットは、IP マスカレードの対象外です。
- forward out/local output フィルタリング適用後のパケットに、IP マスカレードを適用します。

◆ **ip (snat-group|dnat-group)**

<説　　明>
- global mode で設定した SNAT または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。
- SNAT はパケットの出力時に適用されます。DNAT はパケットの入力時に適用されます。

<書　　式> ip (snat-group|dnat-group) NAT-NAME
<　no　> no ip (snat-group|dnat-group)
<備　　考> NAT ルールの設定は、ip snat/ip dnat)コマンド(global mode)で行います。

◆ **ip webauth-filter**

◆ **ipv6 webauth-filter**

<説　　明>

・ Web 認証フィルタをインタフェースに適用すると、ある特定のホスト、ネットワークやインタフェースについて、Web 認証せずに通信することが可能となります。

・ Web 認証フィルタは、各インタフェースにつき、IN/OUT をそれぞれ一つずつ設定することができます。Default の設定はありません。

<書　　式> ip webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
ipv6 webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME

< no > no ip webauth-filter (forward-in|forward-out)
no ipv6 webauth-filter (forward-in|forward-out)

<備　　考>

➢ Web 認証フィルタの設定については、ip web-auth access-list/ipv6 web-auth access-list コマンド (global mode)を参照してください。

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

◆ **ip spi-filter**

<説　　明>

・ 簡易ファイヤウォールの一つとして、SPI(Stateful Packet Inspection)機能をサポートします。

・ パケットに関連するコネクションの状態を見て、当該パケットをドロップするかしないかを決める機能です。

<書　　式> ip spi-filter (有効)
<初 期 値> no ip spi-filter(無効)
< no > no ip spi-filter

<備　　考>

・ コネクションの状態が、established または related の場合に、パケットの転送を許可します。

・ Established とは、すでに双方向でパケットの通信がありコネクションが確立されている状態です。

・ Related とは、すでに確立しているコネクションがある状態です。FTP のデータ転送等がこれに該当します。

・ 新しい接続でありながら、syn ビットの立っていないパケットはドロップします。

・ SPI は、forward in および local input の位置で適用されます。ユーザが適用位置を変更することは出来ません。

◆ **netevent**

<説　　明>

・トラックイベントの発生時に、当該 tunnel を接続／切断／再接続することが出来ます。

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

< no > no netevent

◆ **ipsec policy**

<説　　明> 当該インタフェースで使用する IPsec ローカルポリシーを設定します。

<書　　式> ipsec policy <local policy:1-255>

< no > no ipsec policy (|<local policy:1-255>)

<備　　考>

・ 各インタフェースに、IPsec ローカルポリシーを 4 つまで設定することが出来ます。他のインタフェースで既に設定している IPsec ローカルポリシーは、重複して設定できません。

### ◆ ipsec policy-ignore

<説　　明>
- IPsec policy のチェックを行わないように指定する機能です。IPsec policy として any などを指定したけれども、特定の通信のみ IPsec 化したくない場合に、この機能を使用します。

<書　　式> ipsec policy-ignore (|input|output)
<初 期 値> no ipsec policy-ignore(無効)
<　no　> no ipsec policy-ignore
<備　　考>
- Input を指定した場合、inbound policy check を実行しないため、IPsec 化されてくるべきパケットがドロップされてしまう現象を回避することができます。
- Output を指定した場合、当該インタフェースから出力されるパケットは、IPsec policy をチェックしないため平文で送信されます。

### ◆ ipsec hold-sa

<説　　明>
- PPP 上で IPsec を利用する場合に、PPP 切断と共に IPsec SA を削除するかどうかを指定する機能です。
- PPP の IP が動的に割り当てられる場合、PPP の down が発生すると、IPsec SA の削除が行われます。
- このとき、NXR 側から切断する場合は、PPP 切断前に delete SA 送信を行い、その後 PPP 切断処理を行います。対向から切断される場合や障害によって切断される場合は、delete SA の送信処理は実行されません。
- 一方、PPP の IP address が固定割り当ての場合は、PPP 切断時に IPsec SA を削除しません。しかし、本機能が無効となっている場合は、動的 IP の場合と同様、PPP 切断と共に IPsec SA の削除を行います。
- この際、NXR 側から切断する場合は、delete SA を送信します。

<書　　式> ipsec hold-sa
<初 期 値> ipsec hold-sa
<　no　> no ipsec hold-sa
<備　　考>
- 本機能は、default で有効です。
- 本機能の有効／無効は、固定 IP の場合のみ影響します。動的 IP の場合は、本機能の有効 / 無効に関らず、上記の動作となります。

### ◆ session invalid-status-drop-interface

<説　　明>
- session invalid-status-drop 機能(global mode 参照)をインタフェース毎に指定することができます。
- 本機能は、default で無効です。

<書　　式> session invalid-status-drop-interface enable
<初 期 値> no session invalid-status-drop-interface enable
<　no　> no session invalid-status-drop-interface enable
<備　　考>
- あるインタフェースに対してのみ適用したい場合は、global mode で session invalid-status-drop 機能を無効にして、かつ本機能を指定インタフェースで有効にします。以下は、wwan 0 インタフェースに適用する場合の設定例です。
  - global mode で、session invalid-status-drop を無効にします。
    nxrg240(config)#no session invalid-status-drop enable
  - 指定インタフェースで、本機能を有効にします。
    nxrg240(config)#interface wwan 0
    nxrg240(config-wwan)#session invalid-status-drop-interface enable

**■ メールヘッダ部の設定(メール送信機能)**

<説　　明>
・ 送信するメールの各ヘッダ部に設定する値を指定します。
<備　　考>
・ メール送信機能の詳細については、mail server mode を参照してください。

○ mail send server
<説　　明> 本設定で使用するメールサーバの番号を指定します。
<書　　式> mail send server <0-2>
<　no　> no mail send server
<備　　考> メールサーバの設定については、mail serve mode を参照してください。

○ mail send from
<説　　明> 送信元メールアドレスを設定します。
<書　　式> mail send from WORD
<　no　> no mail send from
<備　　考>
・ WORD には、送信元メールアドレス(例:centurysys@xxx.isp.ne.jp)を指定します。
・ mail send from コマンドで送信元メールアドレスを指定しない場合は、mail from コマンド(global mode)で指定した送信元メールアドレスを使用します。

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

○ mail send subject
<説　　明> メールの件名を設定します。指定しない場合は、既定のフォーマットを使用します。
<書　　式> mail send subject LINE
<　no　> no mail send subject

○ no mail send
<説　　明> 上記の設定を一括削除することができます。
<書　　式> no mail send

◆ ip policy route-map
<説　　明> 受信インタフェースに、PBR のアクセスリストを適用します。
　　WORD には、適用する ACL 名(ip policy access-list にて設定)を指定します。
<書　　式> ip policy route-map WORD
<　no　> ip policy route-map

**◆ ip p2p-detection**
<説　　明> P2P 検出機能を有効にします(IPv4 のみ対応)。
<書　　式> ip p2p-detection (any|winny|share|bittorrent) {log|deny}
<　no　> no ip p2p-detection
　　no ip p2p-detection (winny|share|bittorrent)
<備　　考>
・ インターネットに接続しているインタフェース上でのみ有効にすることを推奨します。
・ 詳細については、「付録 L:P2P 検出機能」を参照してください。

◆ **bandwidth**

<説　　明> インタフェースの帯域幅を設定することが出来ます。
　　bandwidth の初期値は、10Mbps です。
　　bandwidth の最大値は、10Gbps です。
<書　　式> bandwidth <1-10000000000[k/m/g]>
<　no　> no bandwidth
<備　　考> 本機能は、OSPF のコスト計算時のみに使用します。
　　基準となる帯域幅は、auto-cost コマンド（ospf mode）にて設定します。

◆ **event-notify**

<説　　明> WWAN の接続／切断時に、イベント通知を行います。
<書　　式> event-notify <0-3>
<　no　> no event-notify
<備　　考> イベント通知の方法(LINE、メール)は、ENS mode で設定します。

◆ **ip multicast-to-unicast**

<説　　明> 有効時、multicast を unicast 変換したパケットを転送します。
<書　　式> ip multicast-to-unicast forwarding　　（有効）
<　no　> no ip multicast-to-unicast forwarding　　（無効）

◆ **cms watch enable**

<説　　明> インタフェースの up/down 時に、インタフェースの監視情報を CMS に送信します。
<書　　式> cms watch enable
<　no　> no cms watch enable

### ◆ 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 autoconfig
<　no　　> no ipv6 address autoconfig

### ◆ ipv6 dhcp client

<説　　明> 当該インタフェースに適用する DHCPv6 クライアントのプロファイル名を指定します。
<書　　式> ipv6 dhcp client WORD
<　no　　> no ipv6 dhcp client

### ◆ ipv6 tcp adjust-mss

<説　　明> TCP/IPv6 の MSS 値を設定します。
<書　　式> ipv6 tcp adjust-mss (auto|500-1460)
<初 期 値> no ipv6 tcp adjust-mss
<　no　　> no ipv6 tcp adjust-mss

### ◆ 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)

### ◆ ipv6 nd accept-ra

<説　　明>
・ 本設定(ipv6 address autoconfig 設定なし)を有効にすると、RA を受信しても、stateless address を設定しません。
<書　　式> ipv6 nd accept-ra
<　no　　> no ipv6 nd accept-ra
<備　　考>
・ ipv6 address autoconfig 設定時、本設定は必要ありません。
・ 当該インタフェースに、IPv6 アドレスは設定しませんが、RA によって取得したパラメータ (defaultgateway, retransmit timer, reachable time, mtu, hop-limit)は使用します。

### ◆ ipv6 nd accept-ra proxy

<説　　明> RA Proxy を有効にします。
<書　　式>
ipv6 nd accept-ra proxy ethernet <0-X>
ipv6 nd accept-ra proxy ethernet <0-X> (|rs-interval <0-604800> rs-count <1-255>)
<備　　考>

- RA Proxy 機能は、NDP Proxy 機能の一部ですが、本装置では、NS パケットに対する代理応答の機能を NDP Proxy 機能とし、RA Proxy 機能とは異なる機能として扱います。
- 本バージョンでは、NDP Proxy 機能のみを有効にすることは出来ません。RA Proxy 機能と同時に使用します。
- Default では、NDP Proxy および RA Proxy 機能は無効です。




### ◆ ipv6 nd rs-interval

<説　　明> RS( Router Solicitation)インターバルを設定します。
<書　　式> ipv6 nd rs-interval <1-10>
<初 期 値> ipv6 nd rs-interval 1
<　no　　> no ipv6 nd rs-interval（初期値）

### ◆ ipv6 nd rs-count

<説　　明> RS(Router Solicitation)の送信回数を設定します。
<書　　式> ipv6 nd rs-count <1-2147483647>
<初 期 値> ipv6 nd rs-count 3
<　no　　> no ipv6 nd rs-count（初期値）

### ◆ 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 webauth-filter**

<説　　明>
- Web 認証フィルタをインタフェースに適用すると、ある特定のホスト、ネットワークやインタフェースについて、Web 認証せずに通信することが可能となります。
- Web 認証フィルタは、各インタフェースにつき、IN/OUT をそれぞれ一つずつ設定することができます。Default の設定はありません。

<書　　式> ipv6 webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
<　no　> no ipv6 webauth-filter (forward-in|forward-out)
<備　　考>
- Web 認証フィルタの設定については、ipv6 web-auth access-list コマンド(global mode)を参照してください。
- Web 認証については、Web Authenticate mode を参照してください。

◆ **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

◆ **ipv6 spi-filter log**

<説　　明> フィルタログ機能(syslog mode 参照)を有効にします。
　　パケットが、SPI フィルタにマッチした場合、syslog に出力することが出来ます。
<書　　式> ipv6 spi-filter log [limit <0-100>]
<初 期 値> ipv6 spi-filter log limit 10
<　no　> no ipv6 spi-filter
<備　　考>
- limit を指定すると、1 秒当たりのログ出力数を制限します。初期値は、10 パケット / 秒です。
- WAN 側からの意図しないパケットが、SPI フィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分に注意してください。

# 第 55 章　Event Notification Service mode

◆ **移行 command**

nxrg110#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxrg110(config)#ens <0-3>
nxrg110(config-ens)#

以下のイベント発生時に、LINE またはメールによる通知を行います。

- Ethernet のリンクアップ／リンクダウン
  詳細は、interface mode(event-notify)を参照してください。
- PPP の接続／切断
  詳細は、interface ppp mode(event-notify)を参照してください。
- WWAN の接続／切断
  詳細は、interface WWAN mode(event-notify)を参照してください。
- システムイベント
  詳細は、global mode(system event-notify)を参照してください。

◆ **line**

<説　　明> イベント発生時、line notify による通知を行います。
<書　　式> line WORD authorization bearer token (hidden|) WORD
<　no　> no line WORD

■ **mail send**

<説　　明> イベント発生時、メールを送信による通知を行います。

○ **mail send server**

<説　　明> 本設定で使用するメールサーバの番号を指定します。
<書　　式> mail send server <0-2>
<　no　> no mail send server
<備　　考> メールサーバの設定については、mail serve mode を参照してください。

○ **mail send from**

<説　　明> 送信元メールアドレスを設定します。
<書　　式> mail send from WORD
<　no　> no mail send from
<備　　考>

- WORD には、送信元メールアドレス(例:sender@xxx.isp.ne.jp)を指定します。
- mail send from コマンドで送信元メールアドレスを指定しない場合は、mail from コマンド(global mode)で指定した送信元メールアドレスを使用します。

**○ mail send to**

<説　　明> 送信先メールアドレスを設定します。
<書　　式> mail send to WORD
< no　> no mail send to
<備　　考>
・ WORD には、送信先メールアドレス(例:user@xxx.isp.co.jp)を指定します。
・ mail send to コマンドで送信先メールアドレスを指定しない場合は、mail to コマンド(global mode)で指定した送信先メールアドレスを使用します。

**○ mail send subject**

<説　　明> メールの件名を設定します。指定しない場合は、既定のフォーマットを使用します。
<書　　式> mail send subject LINE
< no　> no mail send subject
<備　　考>
・ LINE を指定しない場合は、既定のフォーマットを使用します。以下に例を示します。
・ ppp0 の接続時: ppp0 was connected
・ ppp0 の切断時: ppp0 was disconnected

**○ no mail send**

<説　　明> 上記の設定を一括削除することができます。
<書　　式> no mail send

# 第 56 章　interface wlan mode

## ■ WLAN

### □用語

本書で使用する無線に関する用語を記します。

**モジュール**
本装置は、1 つの無線モジュール(wifi0)を内蔵しています。

**AP(Access Point)**
無線 LAN で端末間を接続する電波中継器(アクセスポイント)です。

**STA(STAtion)**
無線 LAN 端末(ステーション)を指します。

**SSID(Service Set Identifier)**
アクセスポイントの識別子です。

**ESSID(Extended Service Set Identifier)**
複数の AP を設置したネットワークでも使用できるように、ネットワーク識別子を拡張したものです。
(本書では、SSID と同義です。)

**BSSID(Basic Service Set Identifier)**
無線 LAN におけるネットワーク識別子の一つです。

**チャネル**
使用する周波数帯域です。

**Beacon**
無線 LAN の通信の可否を伝える信号です。AP は Beacon を一定間隔で送信し、STA はこれを受信して AP を発見し、通信を開始します。

**TIM(Traffic Indication Message)**
AP から STA に送信される Beacon の一部です。パワーセーブ中の STA 向けデータの有無を通知します。

**DTIM(Delivery TIM)**
マルチキャスト /ブロードキャストデータがあることを通知する TIM です。

**VAP(Virtual Access Point)**
1 台の AP を仮想的な複数の AP として動作させる機能です。

**ANY 接続**
STA 側で接続先 AP の SSID を指定しない場合に、電波状態が最良の AP に接続する方法です。

**DFS(Dynamic Frequency Selection)**
無線 LAN の通信が、気象レーダー等に影響を与えないように、AP 側が使用周波数帯を変更する機能です。

**GI(Guard Interval)**
マルチパスによる前後の信号の重なりを避けるため、シンボル間に設ける付加時間です。short(400ns)と long(800ns)があります。

**HT / VHT / HE**
IEEE 802.11n(HT)、802.11ac(VHT)、802.11ax(HE)での 1 チャネルあたりの帯域幅の呼称です。例:HT40 は 802.11n の 40MHz、HE160 は 802.11ax の 160MHz を指します。

**WPA3-SAE**
パスワード(パスフレーズ)を用いる WPA3 のパーソナル認証方式です。

**WPA3-OWE(Enhanced Open)**
パスワードなしで接続でき、通信を暗号化する方式です。

**PMF(Protected Management Frames)**
切断要求などの管理フレームを保護する機能です(IEEE 802.11w)。

**BSS Color**
IEEE 802.11ax で、近隣の BSS からの電波を識別するための番号です。

**TWT(Target Wake Time)**
IEEE 802.11ax で、STA の送受信タイミングを AP と取り決め、STA の消費電力を抑える機能です。

**□無線 LAN アクセスポイント機能**
本装置は、無線 LAN アクセスポイント(AP)として利用可能な無線モジュール(wifi0)を内蔵しています。本装置は、無線 LAN ステーション(STA)として動作することは出来ません。
※ wifi については、wifi mode を参照してください。

**□ VAP(仮想 AP)機能**
VAP とは、一台の AP を仮想的な複数の AP として動作させる機能です。

**□無線 LAN インタフェース**
無線 LAN インタフェースは、VAP 毎に作成される論理インタフェースです。VAP 毎のインタフェース設定は、wlan interface に対して行います。

**◆ 移行 command**
nxr#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr(config)#**interface wlan <0-2>**
nxr(config-wlan)#
< no > no interface wlan <0-2>
<備　考>
- wlan0-2 は、wifi0 に割り当てられます。
- 設定は、exit 時に反映されます。認証の設定が不完全な場合は、wlan を有効にしません。
- bridge-group のポートとして使用している wlan インタフェースは、削除することが出来ません。

**□マルチプル BSSID**
最大３つまでの VAP(wifi0: wlan0-2)を作成することが出来ます。これにより、複数の SSID でアクセスすることが出来るようになります。また、VLAN 機能との組み合わせで、複数のネットワークを収容することが出来ます。
VAP 毎に、以下の項目について設定することが出来ます。

| 設定項目 | |
|---|---|
| VAP の有効/無効 | DTIM |
| SSID | 無通信監視 |
| 認証方式 | RADIUS 認証 / アカウンティング |
| ANY 接続拒否 | PMF |
| ステルス機能(SSID 非通知) | WPS |
| MAC アドレスフィルタリング | 接続台数制限 |
| プライバシープロテクション | |

◆ **wlan ssid WORD**

<説　　明> SSID を設定します。
<書　　式> wlan ssid WORD
<備　　考>
- 1-32 文字の文字列を指定します。
- 使用可能な文字は、英数字および !$#&=*+-_.:;(){}[]/^~@`< です。
- 「-」「--」のみの文字列は指定できません。
- 他の wlan インタフェースと同じ SSID は設定できません。

**□ ANY 接続拒否機能**

VAP 毎の ANY 接続を拒否する機能です。本機能とステルス機能の設定は連動し、ステルス機能を有効にすると ANY 接続拒否も有効になります。
受信したプローブ要求の SSID 状態と本機能の設定状況により以下の動作を行います。

| ANY 接続拒否設定 | 受信したプローブ要求の SSID | プローブ送信応答の有無 |
|---|---|---|
| 有効 | ブロードキャスト SSID | 送信しない |
| | 指定した SSID に一致 | 送信する |
| | 指定した SSID に不一致 | 送信しない |
| 無効 | ブロードキャスト SSID | 送信する |
| | 指定した SSID に一致 | 送信する |
| | 指定した SSID に不一致 | 送信しない |

**□ ステルス機能**

・ Beacon 信号に SSID を含めないことで、VAP 毎に SSID を隠蔽することが出来ます。本機能は、ANY 接続拒否機能と連動して動作します。

◆ **wlan guest-mode enable**

<説　　明> ゲストモードの有効 / 無効(ステルス機能の無効 / 有効)を設定します。
<書　　式> wlan guest-mode enable　　(SSID を隠蔽しません)
<　no　　> no wlan guest-mode enable　　(SSID を隠蔽します)
<初 期 値> wlan guest-mode enable

**□ MAC アドレスフィルタ機能**

VAP 毎に、STA の MAC アドレスによる接続制限を行う機能です。

・　「MAC アドレスリストに含まれる STA のみ接続許可」または「MAC アドレスリストに含まれる STA のみ接続禁止」とするデフォルト動作を、VAP 毎に定義することが出来ます。

・　最大登録数は、VAP 毎に 32 個です。MAC アドレスのマスク指定は出来ません。

| MAC アドレスフィルタ | MAC アドレスリスト | 接続条件 |
|---|---|---|
| 無効(disable) | – | 許可 |
| リストに含む STA のみ接続許可(permit) | STA の MAC を含む | 許可 |
| リストに含む STA のみ接続許可(permit) | STA の MAC を含まない | 拒否 |
| リストに含む STA のみ接続禁止(deny) | STA の MAC を含む | 拒否 |
| リストに含む STA のみ接続禁止(deny) | STA の MAC を含まない | 許可 |

**◆ wlan mac access-list permission**

<説　　明> MAC アドレスフィルタのデフォルト動作(permit / deny / disable)を設定します。
<書　　式> wlan mac access-list permission (permit|deny|disable)
<　no　> no wlan mac access-list permission　　(= 初期値)
<初 期 値> wlan mac access-list permission disable

**◆ wlan mac access-list address**

<説　　明> MAC アドレスリストに、MAC アドレスを登録します。
<書　　式> wlan mac access-list address HH:HH:HH:HH:HH:HH
<　no　> no wlan mac access-list address (|HH:HH:HH:HH:HH:HH)
<備　　考> 最大 32 個まで登録することが出来ます。MAC アドレスを省略して no を実行すると、すべて削除します。

**□ プライバシープロテクション**

access-point-bridge を有効にすると、STA 同士の通信が可能となります。無効にした場合、STA 同士の通信は出来ません。

**◆ wlan access-point-bridge enable**

<説　　明> プライバシープロテクション(プライバシーセパレータ)の有効 / 無効を設定します。
<書　　式> wlan access-point-bridge enable　　(STA 間の通信が可能)
<　no　> no wlan access-point-bridge enable　(STA 間の通信を遮断)
<初 期 値> wlan access-point-bridge enable

**□ 接続台数制限**

VAP 毎に、IEEE 802.11 接続できる STA の台数を制限することが出来ます。

**◆ wlan max-associations**

<説　　明> 接続台数制限を設定します。
<書　　式> wlan max-associations <1-64>
<　no　> no wlan max-associations　　(=初期値)
<初 期 値> wlan max-associations 16
<備　　考> 接続できる STA の台数は、wifi 全体(wlan0-2 の合計)で最大 64 台です。

**□ DTIM**

**◆ wlan beacon dtim-period**

<説　　明> VAP 毎に、beacon の DTIM 値を設定します。
<書　　式> wlan beacon dtim-period <1-255>
<　no　> no wlan beacon dtim-period (= 初期値)
<初 期 値> wlan beacon dtim-period 1

**□暗号化方式･セキュリティ**

VAP 毎に、以下の認証･暗号化方式を設定することが出来ます。

| 認証方式 | 暗号化方式 | 必要な設定 |
|---|---|---|
| WPA3-OWE | - | なし(初期値) |
| WPA-PSK | AES | wlan wpa-psk password |
| WPA2-PSK | AES | wlan wpa-psk password |
| WPA-PSK/WPA2-PSK (mixed mode) | AES | wlan wpa-psk password |
| WPA3-SAE | AES | wlan wpa-psk password |
| WPA3-SAE transition (WPA2-PSK/WPA3-SAE) | AES | wlan wpa-psk password |
| WPA-EAP | AES | wlan radius authentication |
| WPA2-EAP | AES | wlan radius authentication |
| WPA-EAP/WPA2-EAP (mixed mode) | AES | wlan radius authentication |
| WPA3-EAP | AES / AES(192bit) | wlan radius authentication |
| WPA3-EAP transition | AES | wlan radius authentication |
| | | |

<備　　考>

wifi mode で、mode 11ax 6ghz を設定している場合、使用できる認証方式は WPA3-OWE、WPA3-SAE、WPA3-EAP のみです。

◆ **wlan authenticate**
<説　　明> WLAN の認証設定を行います。
<初 期 値> wlan authenticate wpa3-owe

○ wpa3-owe
<書　　式> wlan authenticate wpa3-owe
<備　　考> パスワードの設定は不要です。

○ wpa-psk / wpa2-psk / wpa-mixed-psk
<書　　式> wlan authenticate (wpa-psk|wpa2-psk|wpa-mixed-psk) aes
<備　　考> wlan wpa-psk password の設定が必要です。

○ wpa3-sae / wpa3-sae-transition
<書　　式> wlan authenticate (wpa3-sae|wpa3-sae-transition) aes
<備　　考> wlan wpa-psk password の設定が必要です。

○ wpa-eap / wpa2-eap / wpa-mixed-eap / wpa3-eap-transition
<書　　式> wlan authenticate (wpa-eap|wpa2-eap|wpa-mixed-eap|wpa3-eap-transition) aes
<備　　考> wlan radius authentication の設定が必要です。

○ wpa3-eap
<書　　式> wlan authenticate wpa3-eap (aes|aes-192bit)
<備　　考> wlan radius authentication の設定が必要です。

○ no wlan authenticate
<書　　式> no wlan authenticate
<備　　考> 認証方式を初期値(wpa3-owe)に戻します。

◆ **wlan wpa-psk password**
<説　　明> PSK / SAE 系の認証方式で使用するパスワードを設定します。
<書　　式> wlan wpa-psk password (|hidden) WORD
　　wlan wpa-psk password encrypted WORD
<　no　> no wlan wpa-psk password
<備　　考>
・ 設定可能な長さは、認証方式によって異なります。
・ hidden を指定した場合は、パスワードを暗号化します。encrypted は、暗号化済みの文字列を入力する場合に指定します。

| 認証方式 | パスワード長 |
|---|---|
| wpa-psk / wpa2-psk / wpa-mixed-psk | ASCII 8-63 文字、または HEX 64 文字 |
| wpa3-sae-transition | ASCII 8-63 文字 |
| wpa3-sae | ASCII 8-128 文字 |

◆ **wlan wpa-psk rekey gtk**
<説　　明> GTK の rekey 間隔(秒)を設定します。
<書　　式> wlan wpa-psk rekey gtk <60-86400>
<　no　> no wlan wpa-psk rekey gtk(= 初期値)
<初 期 値> wlan wpa-psk rekey gtk 600

◆ **wlan wpa-psk rekey gtk-strict enable**

<説　　明> GTK strict を有効にします。
<書　　式> wlan wpa-psk rekey gtk-strict enable(有効)
<　no　> no wlan wpa-psk rekey gtk-strict enable(無効)
<初 期 値> wlan wpa-psk rekey gtk-strict enable

◆ **wlan wpa-psk rekey gmk**

<説　　明> GMK の rekey 間隔(秒)を設定します。
<書　　式> wlan wpa-psk rekey gmk <60-86400>
<　no　> no wlan wpa-psk rekey gmk(= 初期値)
<初 期 値> wlan wpa-psk rekey gmk 86400

◆ **wlan wpa-psk rekey ptk**

<説　　明> PTK の rekey 間隔(秒)を設定します。
<書　　式> wlan wpa-psk rekey ptk <60-86400>
<　no　> no wlan wpa-psk rekey ptk(= 初期値)
<初 期 値> wlan wpa-psk rekey ptk 600

◆ **wlan pmf**

<説　　明> PMF(Protected Management Frames)を設定します。
<書　　式> wlan pmf (disable|optional|required)
<　no　> no wlan pmf(= 初期値)
<初 期 値> wlan pmf disable
<備　　考> optional:PMF 対応の STA とは PMF を使用します。required:PMF 非対応の STA は接続できません。WPA3 では、本設定は無効(required 固定)です。

**□ RADIUS 連携**

- AP は、STA(Supplicant)と RADIUS サーバ間に位置する Authenticator として動作します。
- 認証・アカウンティングを行う RADIUS サーバとして、各々 2 台(Primary / Secondary)まで、IPv4 アドレス形式で指定することが出来ます(wlan インタフェース毎に指定します)。
- Primary から応答がない場合は最大 2 回までリトライを行い(1 回目は 3 秒後、2 回目は 6 秒後)、すべてのリトライに失敗すると Secondary へ接続します。
- Secondary への接続後、wlan radius dead-interval で指定した時間が経過するまでは Secondary を使用し、経過後に Primary へ接続します。
- 認証後のアクションは特にありません。

**□ RADIUS アカウンティング**

RADIUS サーバ宛に、以下の内容のフレーム(UDP 1813 ポート / ポート指定可能)を送信する機能です。NAS-IP-Address および NAS-Identifier を指定することが出来ます。

| Accounting start/stop 時 | | |
|---|---|---|
| 属性名 | start 時 | stop 時 |
| Acct-Session-Id | セッション ID | セッション ID |
| Acct-Status-Type | start(1) | stop(2) |
| Acct-Authentic | RADIUS(1) | RADIUS(1) |
| User-Name | 暗号なしの場合:BSSID<br>暗号ありの場合:ユーザ ID | 同左 |
| NAS-IP-Address | 本装置の IP アドレス<br>(wlan interface で設定した場合は、その IP アドレス) | 同左 |
| NAS-Identifier | wlan interface で設定した場合は、<br>その NAS-Identifier | 同左 |
| Called-Station-Id | AP の BSSID、及び SSID | 同左 |
| Calling-Station-Id | STA の MAC アドレス | 同左 |
| NAS-Port-Type | Wireless-802.11(19) | 同左 |
| Acct-Session-Time | - | 接続時間(秒) |
| Event-Timestamp | - | 現在時刻 |
| Acct-Terminate-Cause | - | 終了理由 |

| Accounting On / Off 時 | | |
|---|---|---|
| 属性名 | On 時 | Off 時 |
| Acct-Status-Type | Accounting-On(7) | Accounting-Off(8) |
| Acct-Authentic | RADIUS(1) | RADIUS(1) |
| NAS-IP-Address | 本装置の IP アドレス<br>(wlan interface で設定した場合は、その IP アドレス) | 同左 |
| NAS-Identifier | wlan interface で設定した場合は、<br>その NAS-Identifier | 同左 |
| Called-Station-Id | AP の BSSID、及び SSID | 同左 |
| Acct-Terminate-Cause | – | 終了理由 |

◆ **wlan radius authentication**

○ wlan radius authentication
<説　　明> RADIUS 認証サーバの IP アドレス、パスワード、ポート番号を設定します。
<書　　式>
wlan radius authentication A.B.C.D password (|hidden) WORD
(|port (1645|1812|<1024-65535>))
wlan radius authentication A.B.C.D password encrypted WORD
(|port (1645|1812|<1024-65535>))
<備　　考>
・port を省略した場合は、1812 を使用します。
・パスワードは、5-95 文字で設定します。
・hidden を指定した場合は、パスワードを暗号化します。
・サーバは、2 つまで設定することが出来ます。

○ no wlan radius authentication
<書　　式> no wlan radius authentication A.B.C.D
<備　　考> 認証方式が EAP 系の場合、削除することは出来ません。

◆ **wlan radius accounting**

○ wlan radius accounting
<説　　明> RADIUS アカウンティングサーバの IP アドレス、パスワード、ポート番号を設定します。
<書　　式>
wlan radius accounting A.B.C.D password (|hidden) WORD (|port (1646|1813|<1024-65535>))
wlan radius accounting A.B.C.D password encrypted WORD (|port (1646|1813|<1024-65535>))
<備 考>
・port を省略した場合は、1813 を使用します。
・パスワードは、5-95 文字で設定します。
・hidden を指定した場合は、パスワードを暗号化します。
・サーバは、2 つまで設定することが出来ます。

○ no wlan radius accounting
<書　　式> no wlan radius accounting A.B.C.D

◆ **wlan radius attribute nas-ip-address**

<説　　明> NAS-IP-Address を設定します。
<書　　式> wlan radius attribute nas-ip-address A.B.C.D
<　no　> no wlan radius attribute nas-ip-address

◆ **wlan radius attribute nas-identifier**

<説　　明> NAS-Identifier を設定します。
<書　　式> wlan radius attribute nas-identifier WORD
<　no　> no wlan radius attribute nas-identifier

◆ **wlan radius dead-interval**

<説　　明> RADIUS サーバの切り戻し時間(秒)を設定します。
<書　　式> wlan radius dead-interval <60-86400>
<　no　> no wlan radius dead-interval(= 初期値)
<初 期 値> wlan radius dead-interval 600

**□ 無通信監視**

**◆ wlan inactive-timeout**

<説　　明> 無通信監視時間(秒)を設定します。無通信状態が設定時間続いた STA を切断します。
<書　　式> wlan inactive-timeout (disable|<60-3600>)
<　no　> no wlan inactive-timeout(= 初期値)
<初 期 値> wlan inactive-timeout 600
<備　　考> disable を指定すると、無通信監視を行いません。

**□ WPS**

**◆ wlan wps information-element enable**

<説　　明> Beacon 等に WPS の情報要素を含めます。
<書　　式> wlan wps information-element enable
<　no　> no wlan wps information-element enable
<初 期 値> no wlan wps information-element enable
<備　考>
・本設定は、1 つの wlan インタフェースにのみ設定することが出来ます。
・WPS による接続は、認証方式が wpa2-psk の wlan で使用できます。

【WPS スイッチによる接続手順】
1. 本装置の WPS スイッチを約 10 秒間長押しします(接続待機状態になります)。
2. 接続したい機器の WPS ボタンを押します。
※ 2 分間接続リクエストがない場合、自動的にタイムアウトします。

**□ 利用するネットワーク環境・構成等について**

◇ VLAN 対応
タグ VLAN で分離されている有線ネットワークと、マルチプル BSSID によってグループ分けされた無線ネットワーク(VAP)との連携は、無線 LAN インタフェースと VLAN インタフェースを同じ bridge-group に参加させることで実現します(AP と STA の間はタグなしフレームで通信します)。

◇ カントリーコード
カントリーコードは、固定値(JP)です。

◇ その他
無線 LAN インタフェースや bridge インタフェースを L2TPv3 の xconnect インタフェースとする場合は、fast-forwarding の対象外です。

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

◆ **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 WORD X:X::X:X/M (|eui-64)
ipv6 address X:X::X:X link-local
ipv6 address X:X::X:X/<0-128> (|eui-64)
<　no　> no ipv6 address X:X::X:X link-local
no ipv6 address X:X::X:X/<0-128> (|eui-64)
no ipv6 address WORD (|X:X::X:X/M)
<備　　考> link-local 指定時、自動設定の LLA を、指定した IPv6 アドレスで上書きします。
eui-64 指定時、IPv6 アドレスは prefix 部のみ指定します。

◆ **mtu**
<説　　明> MTU の値を設定します。
<書　　式> mtu <bytes:256-1500>
<初 期 値> mtu 1500
<　no　> no mtu　　(= mtu 1500)

◆ **ipv6 dhcp server**
<説　　明> 当該インタフェース上で、DHCPv6 サーバを起動します。
<書　　式> ipv6 dhcp server WORD
<　no　> no ipv6 dhcp server
< mode > interface mode
<備　　考> WORD には、起動する DHCPv6 サーバのプロファイル名を指定します。

◆ **ip proxy-arp**
<説　　明> Proxy ARP を有効にします。
<書　　式> ip proxy-arp
<初 期 値> no ip proxy-arp
<　no　> no ip proxy-arp
<備　　考>
・ Proxy ARP は、受信したインタフェースとは異なる宛先への ARP request に対して、代理で応答する機能です。
・ forwarding の対象外のアドレス(ブロードキャストアドレスやネットワークアドレス)に対する ARP request には応答しません。

◆ **ip directed-broadcast**
<説　　明> Directed Broadcast のフォワーディングを有効にします。
<書　　式> ip directed-broadcast
<初 期 値> no ip directed-broadcast
<　no　> no ip directed-broadcast

### ◆ ip redirects

<説　　明>

・ ICMP redirect(type=5)とは、同一ネットワーク上に他の最適なルートがあることを通知するためのメッセージです(RFC792)。

・ 本装置の Send redirect 機能によって、ICMP redirect の送信の有無を切り替えることが出来ます。

<書　　式> ip redirects

<初 期 値> ip redirects　　(有効)

<　no　　> no ip redirects　　(無効)

<備　　考>

・ 以下に ICMPRedirect の例を示します。ICMP Redirect 受信後の動作は、Host 側の動作に依存するため、常に次のような動作になるというわけではありません。

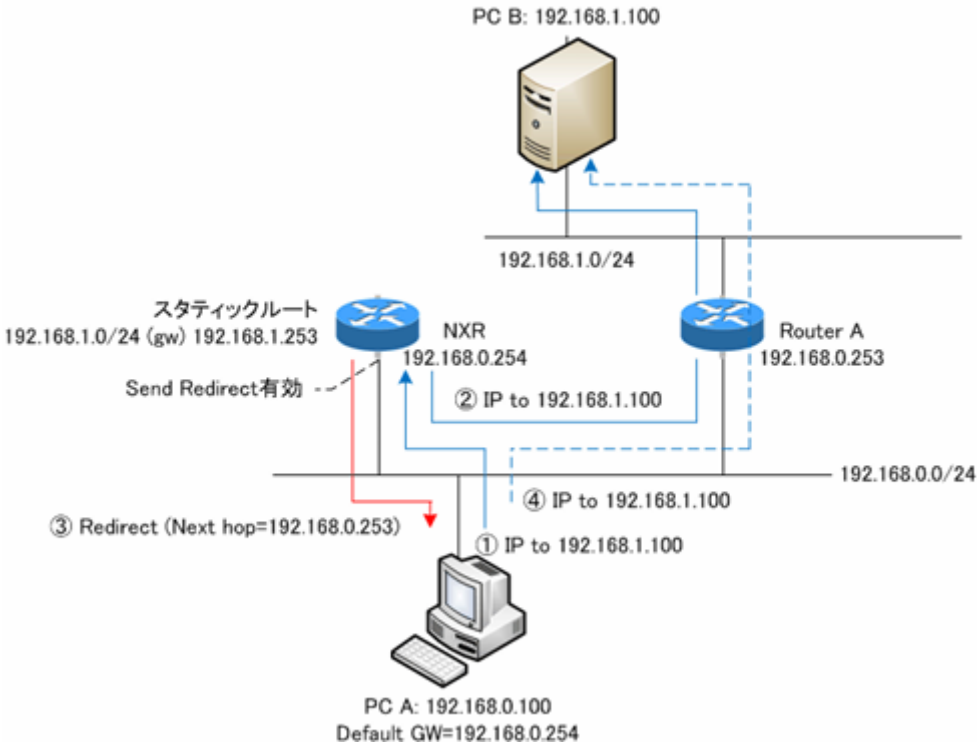
① Host A は、Host B(192.168.1.100)への IPv4 パケットを default gw(NXR)に送信します。

② NXR は、ルーティング情報から、192.168.1.0/24 宛ての next hop は 192.168.1.253 であることを知り、Router A へ転送します。

③ このとき、next hop の Router A は、送信元の Host A と同一ネットワークであるため、Host A に ICMP Redirect を送信します。

④ Host A は、以降の Host B 宛ての IPv4 パケットは、ICMP Redirect で通知された next hop に従って、Router A へ送出します。

・ 本装置が、ICMP Redirect を受信した場合は、ルーティングキャッシュの更新をしません。ルーティングテーブルに従った forwarding 動作を継続します。



◆ **ip tcp adjust-mss**

<説　　明>

・ Path MTU Discovery(PMTUD)機能(End-to-end でフラグメントが発生しない最大の MTU を発見すること)によって、フラグメントなしでパケットの送信を行うことが可能になります。しかし、通信の途中に存在する IPv4 機器(ルータ等)が ICMP fragment needed をフィルタリングしている場合(ブラックホールルータが存在する場合)や PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、Endto-end での通信に支障をきたすことになります。このような場合、TCP では SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

<書　　式> ip tcp adjust-mss (auto|<500-1460>)

<初 期 値> no ip tcp adjust-mss

<　no　> no ip tcp adjust-mss

<備　　考>

・ IPv4 パケット内のプロトコルが TCP の場合に有効な機能です。TCP オプションフィールドがない場合は、オプションフィールドを付与した上で MSS 値を設定します。

・ 本装置が自動で MSS 値を設定する場合は、auto を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ ユーザが設定する場合は、MSS 値を指定します。元の MSS 値が変更後の MSS 値より小さい場合は、値を書き換えません。

・ UDP、ICMP やその他のプロトコルでは、送信するアプリケーション側で DF ビットを 0 にしたり、パケットサイズを細かくして送ったりすることで対処するようにしてください。

・ 「no ip tcp adjust-mss」を設定すると、TCP MSS 調整機能が無効になります。

◆ **ipv6 tcp adjust-mss**

<説　　明> TCP/IPv6 の MSS 値を設定します。

<書　　式> ipv6 tcp adjust-mss (auto|<500-1440>)

<初 期 値> no ipv6 tcp adjust-mss

<　no　> no ipv6 tcp adjust-mss

◆ **ip mask-reply**

<説　　明>

・ OpenView などの監視装置では、監視ネットワーク内の機器に対して ICMP address mask request (type=17)を送信することによって機器のインタフェースのネットマスク値を取得します(単純に、死活監視で使用する場合もあります)。

・ 本装置では、ICMP address mask request への応答の有無を設定することが出来ます。

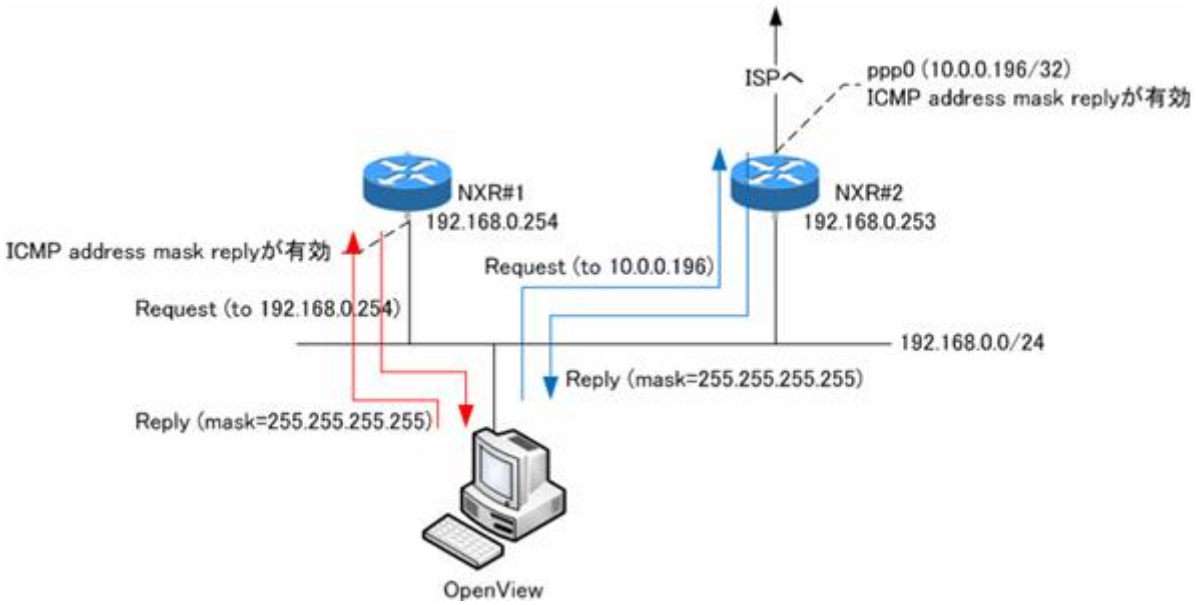
<書　　式> ip mask-reply　　(ICMP address mask request に応答します。)

<初 期 値> no ip mask-reply　　(ICMP address mask request に応答しません。)

< no > no ip mask-reply

<備　　考>

・ ICMP address mask request/reply の例を示します。



◆ **(ip|ipv6) rebound**

<説　　明>

・ 下位ルータから受信したパケットを、受信インタフェースと同一インタフェースから出力(forwarding)した場合、下位ルータから本装置に対して再度パケットが送信されてくるため、下位ルータと本装置の間で TTL が「0」になるまでパケットがループします。
・ IP rebound 機能を無効にすると、受信インタフェースと送信インタフェースが同一の場合、パケットをドロップし、かつ送信元に destination unreachable を送信します。
・ Default は、有効です(受信インタフェースと送信インタフェースが同一でもドロップしません)。

<書　　式> (ip|ipv6) rebound
<初 期 値> (ip|ipv6) rebound
<　no　　> no (ip|ipv6) rebound

◆ **ip reassemble-output**

<説　　明>

・ インタフェースの MTU(あるいは PMTU)より大きいパケットを IP forwarding する際、フラグメントが許可されているか、または強制フラグメントが有効であれば、パケットをフラグメントして出力します。
  本設定有効時、本装置がリアセンブルしたパケットは、以下のようにフラグメント処理を行います。
  - fragmented packet(パケットの断片)が MTU を超える場合、リアセンブルしたパケットを再度 MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、リアセンブルしたパケットを出力します。

<書　　式> ip reassemble-output
<初 期 値> ip reassemble-output
<　no　　> no ip reassemble-output

<備　　考>

・ 上記の場合(本設定が有効の場合)、送信元ホストが出力したパケットのサイズと宛先ホストが受信したパケットのサイズが異なることがあります。このような状況下では、簡易な IP 実装を行っているホストで通信障害になることを確認しています。これを回避するには、本設定を出力インタフェース上で無効にします。本設定が無効の場合、ホストから出力されたサイズと同じサイズで本装置からパケットを出力します。また、出力時の IP フラグメント処理は、次のようになります。
  - fragmented packet(パケットの断片)が MTU を超える場合、受信した fragmented packet を MTU サイズにフラグメントして出力します。
  - fragmented packet(パケットの断片)が MTU より小さい場合、受信した fragmented packet のサイズで出力します。
  - パケット全体のサイズが MTU より小さい場合、受信した fragmented packet をそのままのサイズで出力します。
・ Default は、global 設定および interface 設定ともに有効です。Global 設定と interface 設定の AND条件により、本機能が有効か無効かを判定します。本設定は、IP forwarding するパケットにのみ影響します。
・ 受信時のサイズを記載しておくバッファが 32 個しかないため、33 個以上にフラグメントされているパケットは、本機能を無効にした場合でも、ip reassemble-output が有効な場合と同様に処理します。

◆ **ip arp reachable-time**

<説　　明> 解決した ARP の有効期間を設定することが出来ます。
<書　　式> ip arp reachable-time <30000-3600000>
<初 期 値> ip arp reachable-time 30000
<　no　　> no ip arp reachable-time
<備　　考> show arp 実行時に、ステータスが REACHABLE と表示される時間です。
実際の時間は、(0.5 ～ 1.5)× reachable-time の間のランダムな値です。

◆ **ip arp queue length**

<説　　明>
- Ethernet/Vlan interface 上で、IPv4 通信を行う場合、送信先(nexthop)の mac address の解決を行います。このとき、mac address が解決するまで queueing できるパケット数を指定することができます。
- Queue は、neighbor の entry 毎に作成します。
- queueing 状態の packet は、address 解決ができると同時に送信します。
- Queue が full の状態で新たに packet が来た場合、queue の先頭から drop します。

<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 と 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 send-ra**

<説　　明> IPv6 RA(Router Advertisement)を送信します。
<書　　式> ipv6 nd send-ra　　(送信)
<　no　　> no ipv6 nd send-ra　　(停止)
<備　　考>

・ RA による prefix 広告は、Ethernet/VLAN/bridge/WLAN 上にて使用することが出来ます。
・ 以下のパラメータをユーザ設定値(あるいはシステム固定値)にセットして、RA 送信を行います。
  - router lifetime: ipv6 nd ra-lifetime による設定値
  - hop limit: ipv6 hop-limit による設定値(default:64)
  - reachable-time: ipv6 nd reachable-time による設定値
  - retransmit timer: ipv6 nd ns-interval による設定値

**RA flags**

  - default router preference: ipv6 nd router-preference による設定値(default:medium)
  - managed-config-flag: ipv6 nd managed-config-flag による設定値(default:0)
  - other-config-flag: ipv6 nd other-config-flag による設定値(default:0)

※ home agent flag, proxy flag はいずれも 0 をセットします。

**Prefix information: ICMPv6 type3**(ipv6 nd prefix により設定します。)

  - prefix/prefix length
  - preferred lifetime
  - valid lifetime
  - autonomous address-configuration flag:ipv6 nd prefix X:X::X:X/M no-autoconfig が設定されている場合は 0、未設定は 1. default:1
  - on-link flag:ipv6 nd prefix X:X::X:X/M off-link が設定されている場合は 0、未設定時は 1. default:1。ただし、ipv6 nd prefix で設定した prefix と同じ prefix を当該インタフェース上の connected route として保持している場合(IPv6 address 設定している場合等)は、本設定に関係なく常に 1.
  - router address flag:常に 0

**MTU:ICMPv6 type5**

  - MTU:インタフェースの MTU 値

**Source link-layer address: ICMPv6 type1**

  - link-layer address: ipv6 nd no-advertise-link-address の有効時、本オプションは広告しません。無効時は、出力インタフェースの link-layer address(MAC アドレス)を設定します。default:無効(本オプションを広告)です。

◆ **ipv6 nd prefix**

<説　　明> IPv6 RA(Router Advertisement)にて広告する prefix を設定します。
<書　　式> ipv6 nd prefix X:X::X:X/M
　　<valid-lifetime:0-4294967295> <preferred-lifetime:0-4294967295>
　　(|{off-link|no-autoconfig})
　　ipv6 nd prefix X:X::X:X/M (|{off-link|no-autoconfig})
　　ipv6 nd prefix X:X::X:X/M no-advertise
< no > no ipv6 nd prefix (|X:X::X:X/M )
<備　　考>

- 広告する prefix は、当該インタフェースに設定している IPv6 アドレスの prefix（ただし、autoconfiguration によるアドレスは除く）、ユーザが設定した prefix、および DHCPv6-PD によって取得した prefix(VRRPv3 の実行中を除く)です。
- インタフェースに設定している prefix、ユーザ指定による prefix、DHCPv6-PD によって取得した prefix が同じ場合は、ユーザ指定の prefix 設定を使用します。
- valid/preferred lifetime は、ユーザ指定を除く prefix を広告する場合、固定値(preferred lifetime は 604800sec、valid lifetime は 2592000sec)を使用します。
- 一方、ユーザ指定の prefix は、ユーザ設定値を使用します。ユーザ設定値がない場合は、上記の固定値を使用します。
- no-advertise を指定すると、当該 prefix を広告しません(default:1)。
- off-link を指定すると、当該 prefix の on-link flag を 0 に設定して広告します(default:1)。
- no-autoconfig を指定すると、当該 prefix の autonomous address-configuration flag を 0 に設定して広告します(default:1)。
- RA で広告する prefix に変更があった場合、古い prefix は変更直後の 1 回のみ preferred lifetime を 0、valid lifetime を 7203 に設定して RA を送信します。Preferred lifetime が 0 の RA を受信することによって、LAN 内のクライアントは、当該 IPv6 アドレスを使用しなくなります。RA を停止する際は、preferred lifetime を 0 にすることに加え、router lifetime を 0 にして送信します。

◆ **ipv6 nd ra-lifetime**

<説　　明> IPv6 RA(Router Advertisement)ライフタイムを設定します。
<書　　式> ipv6 nd ra-lifetime <0-9000>
<初 期 値> ipv6 nd ra-lifetime 1800
< no > no ipv6 nd ra-lifetime
<備　　考> ra-lifetime >= ra-interval max

◆ **ipv6 nd ra-interval**

<説　　明> IPv6 RA(Router Advertisement)インターバルを設定します。
<書　　式> ipv6 nd ra-interval <min:3-1350> <max:4-1800>
<初 期 値> ipv6 nd ra-interval 200 600
<　no　　> no ipv6 nd ra-interval
<備　　考>

- min < max x 0.75 となるように設定してください。
- VRRPv3 が設定されているインタフェースでは、RA を有効にした場合でも、常に RA 広告するわけではなく、VRRP マスターの場合に限り送信します。また、広告する prefix は、インタフェース上に設定している IPv6 address prefix ではなく、仮想 IPv6 address prefix を広告します。仮想 IPv6 アドレスが未設定の場合は、prefix を広告しません。

◆ **ipv6 nd managed-config-flag**

<説　　明> RA flag(managed-config-flag)を設定することが出来ます。
<書　　式> ipv6 nd managed-config-flag (M flag=1)
<初 期 値> no ipv6 nd managed-config-flag (M flag=0)
<　no　　> no ipv6 nd managed-config-flag

◆ **ipv6 nd other-config-flag**

<説　　明> RA flag(other-config-flag)を設定することが出来ます。
<書　　式> ipv6 nd other-config-flag (O flag=1)
<初 期 値> no ipv6 nd other-config-flag (O flag=0)
<　no　　> no ipv6 nd other-config-flag

◆ **ipv6 nd router-preference**

<説　　明> RA flag(router-preference)を設定することが出来ます。
<書　　式> ipv6 nd router-preference (high|low|medium)
<初 期 値> ipv6 nd router-preference medium
<　no　　> no ipv6 nd router-preference

◆ **ipv6 nd no-advertise-link-address**

<説　　明> Source link-layer address option の広告(する / しない)を設定します。
<書　　式> ipv6 nd no-advertise-link-address
<初 期 値> no ipv6 nd no-advertise-link-address
<　no　　> no ipv6 nd no-advertise-link-address
<備　　考> 有効:source link-layer address option を送信しません。
　　無効:source link-layer address option を送信します。

◆ **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 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 30000
<　no　> no ipv6 nd reachable-time　　（初期値）

◆ **ipv6 nd rs-interval**
<説　　明> IPv6 Router Solicitation インターバルを設定します。
<書　　式> ipv6 nd rs-interval <interval:1-10sec>
<初 期 値> ipv6 nd rs-interval 1
<　no　> no ipv6 nd rs-interval　　（初期値）

◆ **ipv6 nd rs-count**
<説　　明> IPv6 Router Solicitation の送信回数を設定します。
<書　　式> ipv6 nd rs-count <count:1-2147483647>
<初 期 値> ipv6 nd rs-count 3
<　no　> no ipv6 nd rs-count　　（初期値）

◆ **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 と 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。

## ■ RIP

### ◆ 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 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 poisoned
<　no　> no ip rip split-horizon

## ■ OSPF

### ◆ 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

### ◆ ip access-group

<説　　明>
・ global mode で設定した ACL をインタフェースに適用することで、パケットフィルタリングを行うことができます。
<書　　式> ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
<　no　　> no ip access-group (in|out|forward-in|forward-out)
<備　　考>
・ 各インタフェースへのパケットフィルタリングの適用箇所(付録の Packet Traveling を参照)は、以下の 4 ヶ所です。
  - in(local input) 本装置自身で受信して処理するパケットを制限します。
  - out(local output) 本装置自身が作成して出力するパケットを制限します。
  - トンネリングされたパケットも本装置自身が作成したパケットとして認識します。
  - forward-in 本装置が当該インタフェースで受信して forwarding するパケットを制限します。
  - forward-out 本装置が受信して当該インタフェースへ forwarding するパケットを制限します。
・ mac 指定のある ACL は、out および forward-out に設定することは出来ません。

### ◆ ipv6 access-group

<説　　明> アクセスグループに IPv6 アクセスリストを追加します。
<書　　式> ipv6 access-group (in|out|forward-in|forward-out) IPV6-ACL-NAME
<初 期 値> 設定なし
<　no　　> no ipv6 access-group (in|out|forward-in|forward-out)

### ◆ ip masquerade

<説　　明>
・ インタフェースよりパケットを出力する際に、パケットの送信元 IPv4 アドレスを出力インタフェースの IPv4 アドレスに自動変換する機能です。
<書　　式> ip masquerade　　(有効)
<初 期 値> no ip masquerade　　(無効)
<　no　　> no ip masquerade
<備　　考>
・ すべてのインタフェース(Ethernet/VLAN/PPP/Tunnel/WLAN)で設定することが出来ます。
・ TCP/UDP/ICMP のみ対応しています。その他のプロトコルに関しては、動作は保証しません。
・ IPv6 パケットは、IP マスカレードの対象外です。
・ forward out/local output フィルタリング適用後のパケットに、IP マスカレードを適用します。

### ◆ ip (snat-group|dnat-group)

<説　　明>
・ global mode で設定した SNAT または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。
・ SNAT は、パケットの出力時に適用されます。DNAT は、パケットの入力時に適用されます。
<書　　式> ip (snat-group|dnat-group) NAT-NAME
<　no　　> no ip (snat-group|dnat-group)
<備　　考> NAT ルールの設定は、ip snat/ip dnat コマンド(global mode)で行います。

◆ **ip webauth-filter**

<説　　明>
- Web 認証フィルタをインタフェースに適用すると、ある特定のホスト、ネットワークやインタフェースについて、Web 認証せずに通信することが可能となります。
- Web 認証フィルタは、各インタフェースにつき、IN/OUT をそれぞれ一つずつ設定することができます。Default の設定はありません。

<書　　式> ip webauth-filter (forward-in|forward-out) WEBAUTH-ACL-NAME
<　no　> no ip webauth-filter (forward-in|forward-out)
<備　　考>
- Web 認証フィルタの設定については、ip web-auth access-list コマンド(global mode)を参照してください。
- Web 認証については、Web Authenticate mode を参照してください。

◆ **l2tpv3 access-group**

<説　　明> Xconnect インタフェースでの送受信に対して、l2tpv3 access-list を適用します。
<書　　式> l2tpv3 access-group (in|out) WORD
<　no　> no l2tpv3 access-group (in|out)
<備　　考>
- WORD:　root の ACL 名を指定します。
  (root の ACL 名は、global ノードの l2tpv3 access-list WORD root にて設定します。)
- in:　Xconnect インタフェース→セッション(本装置への入力)方向のフィルタを適用します。
- out:　セッション→ Xconnect インタフェース(本装置からの出力)方向のフィルタを適用します。

◆ **ip spi-filter**

<説　　明>
- 簡易ファイヤウォールの一つとして、SPI(Stateful Packet Inspection)機能をサポートします。
- パケットに関連するコネクションの状態を見て、当該パケットをドロップするかしないかを決める機能です。

<書　　式> ip spi-filter　　(有効)
<初 期 値> no ip spi-filter　　(無効)
<　no　> no ip spi-filter
<備　　考>
- コネクションの状態が、established または related の場合に、パケットの転送を許可します。
- Established とは、すでに双方向でパケットの通信がありコネクションが確立されている状態です。
- Related とは、すでに確立しているコネクションがある状態です。FTP のデータ転送等がこれに該当します。
- 新しい接続でありながら、syn ビットの立っていないパケットはドロップします。
- SPI は、forward in および local input の位置で適用されます。ユーザが適用位置を変更することは出来ません。

◆ **ipv6 spi-filter**

<説　　明> IPv6 SPI filter を設定します。
<書　　式> ipv6 spi-filter
<初 期 値> no ipv6 spi-filter
<　no　> no ipv6 spi-filter

◆ **shutdown**

<説　　明> 当該インタフェースをシャットダウンすることができます。
<書　　式> shutdown
<初 期 値> no shutdown
<　no　> no shutdown

◆ **QoS**

○ classify

<書　　式> classify (input|output) route-map ROUTEMAP

<備　　考>

・ インタフェースにルートマップを適用します。1 つのインタフェースに、input と output を別々に設定することが出来ます。
・ input で指定したルートマップは、PRE-ROUTING(付録の Packet Traveling を参照)で適用されます。
・ output で指定したルートマップは、POST-ROUTING(付録の Packet Traveling を参照)で適用されます。

○ no classify

<書　　式> no classify (|input|output)

<備　　考>

・ インタフェースに適用したルートマップを削除します。
・ 「no classify」を実行すると、両方(input と output)を削除します。片方だけを削除する場合は、input または output を指定します。

◆ **session invalid-status-drop-interface**

<説　　明>

・ session invalid-status-drop 機能(global mode 参照)をインタフェース毎に指定することができます。
・ 本機能は、default で無効です。

<書　　式> session invalid-status-drop-interface enable

<初 期 値> no session invalid-status-drop-interface enable

<　no　> no session invalid-status-drop-interface enable

<備　　考>

・ あるインタフェースに対してのみ適用したい場合は、global mode で session invalid-status-drop 機能を無効にして、かつ本機能を指定インタフェースで有効にします。以下は、wlan0 インタフェースに適用する場合の設定例です。
  - global mode で、session invalid-status-drop を無効にします。
    nxr(config)#no session invalid-status-drop enable
  - 指定インタフェースで、本機能を有効にします。
    nxr(config)#interface wlan 0
    nxr(config-wlan)#session invalid-status-drop-interface enable

◆ **ip policy route-map**

<説　　明> 受信インタフェースに、PBR の route-map を適用します。
　　WORD には、適用する route-map 名を指定します。

<書　　式> ip policy route-map WORD

<　no　> no ip policy route-map

◆ **bridge-group**

<説　　明> インタフェースを bridge-group(仮想スイッチグループ)に参加させます。

<書　　式> bridge-group <0-4095>
　　bridge-group <0-4095> pathcost <0-65535>
　　bridge-group <0-4095> port <1-128>
　　bridge-group <0-4095> priority <0-255>

<　no　> no bridge-group
　　no bridge-group <0-4095> (pathcost|priority)

<備　　考> bridge-group が未設定(interface bridge が未設定)の場合、join に失敗します。

◆ **(ip|ipv6) tcp strip-options**
<説　　明> 指定した TCP オプションを、NOP に置き換えます。
<書　　式>
(ip|ipv6) tcp strip-options {wscale|mss|sack-permitted|sack|timestamp|md5}
(ip|ipv6) tcp strip-options all
<初 期 値> no (ip|ipv6) tcp strip-options
<　no　> no (ip|ipv6) tcp strip-options
<備　　考>
・ 複数のオプションを同時に指定することが出来ます。all を指定すると、すべてのオプションを対象にします。

# 第 57 章　wifi mode

**□ 無線 LAN アクセスポイント機能**

本装置は、無線 LAN アクセスポイント(AP)として利用可能な無線モジュールを 1 つ(wifi0)内蔵しています。無線方式、帯域幅、チャネル、送信出力などを設定することが出来ます。

**■ 6GHz 帯 無線 LAN 機能のご利用について**

本製品の 6GHz 帯無線 LAN 機能をご利用いただくにあたり、以下の点にご注意ください。

1. 標準設定（屋内利用）

本製品の 6GHz 帯機能は、工場出荷時の標準設定で屋内利用（LPI モード）に最適化されています。電波法の規定により、この設定（LPI モード）でのアクセスポイントとしての利用は屋内に限定されています。

2. 限定的な屋外利用（VLP モード）の設定

本製品は、設定を変更して送信出力を抑制することで、限定的に屋外で利用すること（VLP モード）が可能です。屋外で利用する場合は、必ず以下の手順で VLP モード（送信電力 14dBm EIRP 以下）に設定してください。

【設定手順】wifi mode で、送信出力（txpower）を 4 に設定します。

<設定コマンド例>

```
nxr#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr(config)#wifi 0
nxr(config-wifi)#txpower 4
nxr(config-wifi)#exit
nxr(config)#exit
nxr#save config
succeed.
```

【ご注意(免責事項)】

- VLP モードは LPI モードに比べ送信出力が大幅に低いため、通信距離が著しく短くなります（数メートル～数十メートル程度)。
- VLP モードの設定および屋外での利用は、お客様自身の責任において行ってください。
- 適切な設定(txpower 4)を行わずに屋外で利用した場合、電波法に抵触する恐れがあります。
- mode か channel-width を変更すると、txpower が max に戻ります。再度、VLP モードの設定を行うようにしてください。

**◆ 移行 command**

```
nxr#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr(config)#wifi 0
nxr(config-wifi)#
<   no    > no wifi 0
```

<備　　考>

- wifi 0 は、wlan 0-2 に対応しています。※ wlan については、interface wlan mode を参照してください。
- 設定は、exit 時に無線モジュールへ反映されます。
- 無線モジュールの復旧処理中は、移行することが出来ません。

**○ 無線方式**
IEEE 802.11 に準拠した、以下の無線方式を設定することが出来ます。

| 識別名 | 無線通信規格 | 周波数帯 |
|---|---|---|
| 11b | IEEE 802.11b | 2.4GHz |
| 11g | IEEE 802.11g | 2.4GHz |
| 11ng | IEEE 802.11n | 2.4GHz |
| 11a | IEEE 802.11a | 5GHz |
| 11na | IEEE 802.11n | 5GHz |
| 11ac | IEEE 802.11ac | 5GHz |
| 11ax 24ghz | IEEE 802.11ax | 2.4GHz |
| 11ax 5ghz | IEEE 802.11ax | 5GHz |
| 11ax 6ghz | IEEE 802.11ax | 6GHz |

**◆ mode**
<説　　明> 無線方式を設定します。
<書　　式>
mode (11b|11g|11ng|11a|11na|11ac)
mode 11ax (6ghz|5ghz|24ghz)
<初 期 値> 未設定
<備　　考>
・channel-width、guard-interval、channel、txpower を設定する前に、mode を設定してください。
・mode を変更すると、channel-width、guard-interval、channel、txpower を初期値に戻します。
・mode の no 形式はありません。

**◆ channel-width**
<説　　明> 1 チャネルあたりの帯域幅を設定します。
<書　　式> channel-width (20mhz|40mhz|80mhz|160mhz)
<　 no　 > no channel-width(= 初期値)
<初 期 値> channel-width 20mhz
<備　　考>
・mode が 11b / 11g / 11a の場合は、設定することが出来ません(20MHz 固定)。
・mode が 11ng / 11na の場合は、20mhz / 40mhz のみ設定することが出来ます。
・mode が 11ax 24ghz の場合は、20mhz / 40mhz を設定してください。
・channel-width を変更すると、guard-interval、channel、txpower を初期値に戻します。

**◆ guard-interval**
<説　　明> ガードインターバルを設定します(short:400ns、long:800ns)。
<書　　式> guard-interval (short|long)
<　 no　 > no guard-interval(= 初期値)
<初 期 値> guard-interval long
<備　　考> mode が 11ng / 11na / 11ac の場合のみ設定することが出来ます。

○ チャネル

チャネル設定

設定できるチャネルは、mode と channel-width の組み合わせで決まります。

| mode | channel-width | チャネル(番号指定) | チャネル(自動) |
|---|---|---|---|
| 11b / 11g | 20MHz 固定 | 1-13 | auto, auto-1-6-11, auto-2-7-12, auto-3-8-13 |
| 11ng / 11ax 24ghz | 20mhz | 1-13 | auto, auto-1-6-11, auto-2-7-12, auto-3-8-13 |
| 11ng / 11ax 24ghz | 40mhz | 1-9 | auto, auto-1-6-11, auto-2-7-12, auto-3-8-13 |
| 11a | 20MHz 固定 | 36-64, 100-144(4ch 間隔) | auto, auto-w52, auto-w53, auto-w56 |
| 11na / 11ac / 11ax 5ghz | 20mhz | 36-64, 100-144(4ch 間隔) | auto, auto-w52, auto-w53, auto-w56 |
| 11na / 11ac / 11ax 5ghz | 40mhz | 36, 44, 52, 60, 100, 108, 116, 124, 132, 140 | auto, auto-w52, auto-w53, auto-w56 |
| 11ac / 11ax 5ghz | 80mhz | 36, 44, 52, 60, 100, 108, 116, 124, 132, 140 | auto, auto-w52, auto-w53, auto-w56 |
| 11ac | 160mhz | 100, 108, 116, 124 | auto, auto-w56 |
| 11ax 5ghz | 160mhz | 100, 108, 116, 124 | auto, auto-w52, auto-w53, auto-w56 |
| 11ax 6ghz | 20mhz | 1-93(4ch 間隔:1, 5, 9 … 93) | auto |
| 11ax 6ghz | 40mhz | 3-91(8ch 間隔:3, 11, 19 … 91) | auto |
| 11ax 6ghz | 80mhz | 7, 23, 39, 55, 71, 87 | auto |
| 11ax 6ghz | 160mhz | 15, 47, 79 | auto |

チャネル自動設定

周囲の AP から送信される Beacon の電波強度を測定し、最も干渉が少ないと判断したチャネルを選択する機能です。
auto 以外を指定すると、選択の候補を限定することが出来ます。

| 指定 | 選択の候補 |
|---|---|
| auto | 設定可能なすべてのチャネル |
| auto-1-6-11 / auto-2-7-12 / auto-3-8-13 | 2.4GHz の 1･6･11 / 2･7･12 / 3･8･13 ch |
| auto-w52 | W52(36-48 ch) |
| auto-w53 | W53(52-64 ch) |
| auto-w56 | W56(100-144 ch) |

◆ **channel**
<説　　明> チャネルを設定します。
<書　　式>
channel (auto|auto-1-6-11|auto-2-7-12|auto-3-8-13|auto-w52|auto-w53|auto-w56|<1-144>)
<　no　> no channel(= 初期値)
<初 期 値> channel auto
<備　　考> mode が未設定の場合は、設定することが出来ません。設定可能な値は、上表を参照してください。

◆ **txpower**
<説　　明> 送信出力を設定します。
<書　　式> txpower (max|<1-21>)
<　no　> no txpower(= 初期値)
<初 期 値> txpower max
<備　　考>
・mode が未設定の場合は、設定することが出来ません。
・設定可能な最大値は周波数帯によって異なります(2.4GHz:21、5GHz:18、6GHz:15)。

□ **Beacon 送信間隔設定**
◆ beacon period
<説　　明> Beacon の送信間隔を設定します。
<書　　式> beacon period <40-2000>
<　no　> no beacon period(= 初期値)
<初 期 値> beacon period 100
<備　　考> 単位は TU(1TU = 1,024$\mu$sec)です。

◆ **rts-threshold**
<説　　明> RTS/CTS を使用するフレームサイズの閾値(Byte)を設定します。設定値を超えるフレームの送信前に RTS/CTS を行います。
<書　　式> rts-threshold <256-2345>
<　no　> no rts-threshold
<初 期 値> no rts-threshold(RTS/CTS 無効)

◆ **bss-color**
<説　　明> IEEE 802.11ax の BSS Color を設定します。
<書　　式> bss-color (auto|<1-63>)
<　no　> no bss-color(= 初期値)
<初 期 値> bss-color auto
<備　　考> mode 11ax の場合に設定できます。

◆ **twt enable**
<説　　明> TWT(Target Wake Time)を有効にします。
<書　　式> twt enable
<　no　> no twt enable
<初 期 値> no twt enable
<備　　考> mode 11ax の場合に設定できます。

# 第 58 章　management-server mode

◆ **移行 command**

nxr160#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr160(config)#management-server
nxr160(config-cms)#

◆ **tenant-code**

<説　　明> テナントコードを設定します。
<書　　式> tenant-code WORD
<備　　考> CMS 側のテナントコードと一致するように設定します。

◆ **node-code**

<説　　明> ノードコード(機器コード)を設定します。
<書　　式> node-code WORD
<　no　　> no node-code
<備　　考> CMS 側の機器コードと一致するように設定します。

◆ **default authorization**

<説　　明> CMS に HTTP アクセス(HTTPS アクセス)する際の認証情報を設定します。
<書　　式> default authorization WORD bearer token TOKEN
　　default authorization WORD none
<　no　　> no default authorization
<備　　考> WORD は認証対象パスです。以下のように設定します。
　　CMS の設定で HTTPS の認証が「必要」な場合
　　default authorization https://A.B.C.D bearer token TOKEN
　　または、default authorization / token TOKEN
　　※ TOKEN は、CMS で表示されているトークンを設定します。
　　CMS の設定で HTTPS の認証が「不要」な場合
　　default authorization https://A.B.C.D none
　　または、default authorization / none

◆ **http access-interval**

<説　　明> CMS に HTTP アクセスするインターバル(秒)を設定します。
<書　　式> http access-interval <600-2678400>
<　no　　> no http access-interval

### ◆ firmware update url

<説　　明> ファームウェアアップデート時の参照先 URL を指定します。
　　（当該 URL のファームウェアにアップデートします。）
<書　　式> firmware update url auto　　（自動 URL）
　　firmware update url WORD
<　no　　> no firmware update url　　（ファームウェアアップデート無効）
<初 期 値> firmware update url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL には以下のマクロ文字列が使用できます。これらの文字列は、本装置によって自動的に置換されます。
　- ${SERVER}　　:server アドレスに置換
　- ${VER}　　:バージョン名に置換（例: 21.12.0）
　- ${MODEL}　　:機種名に置換（例:nxr530, vxrx64）
　- ${SN}　　:機器のシリアル番号に置換

※ ${SERVER}は、以下の例のように、server 設定(後述)している場合のみ有効です。

```
!
 management-server
  tenant-code century
  node-code nxr001
  .....
  server 192.168.XXX.XXX
   exit-server
!
```

### ◆ firmware update authentication

<説　　明> ファームウェアアップデート時の認証について設定します。
<書　　式> firmware update authentication default　　（初期値）
　　default authorization の設定に従います。
　　firmware update authentication bearer token WORD
　　指定したトークンで認証します。WORD には、トークンを指定します。
<　no　　> no firmware update authentication　　（認証不要）

### ◆ firmware list-update url

<説　　明> firmware list-update 時の参照先 URL を指定します。
<書　　式> firmware list-update url auto　　（自動 URL）
　　firmware list-update url WORD
<　no　　> no firmware list-update url　　（firmware list-update 無効）
<初 期 値> firmware list-update url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL にはマクロ文字列が使用できます。詳細は、firmware update url コマンドを参照してください。

◆ **firmware list-update authentication**

<説　　明> firmware list-update 時の認証について設定します。
<書　　式> firmware list-update authorization default　　（初期値）
　　default authorization の設定に従います。
　　firmware list-update authorization bearer token WORD
　　指定したトークンで認証します。WORD には、トークンを指定します。
< no > no firmware list-update authorizatoin　　（認証不要）

◆ **mobile update url**

<説　　明> モバイルモジュールアップデート時の参照先 URL を指定します。
<書　　式> mobile <0-1> update url auto　　（自動 URL）
　　mobile <0-1> update url WORD
< no > no mobile <0-1> update url　　（モバイルモジュールアップデート無効）
<初 期 値> mobile <0-1> update url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL にはマクロ文字列が使用できます。詳細は、firmware update url コマンドを参照してください。

◆ **mobile update authentication**

<説　　明> モバイルモジュールアップデート時の認証について設定します。
<書　　式> mobile <0-1> update authorization default　　（初期値）
　　default authorization の設定に従います。
　　mobile <0-1> update authorization bearer token WORD
　　指定したトークンで認証します。WORD には、トークンを指定します。
< no > no mobile <0-1> update authorizatoin　　（認証不要）

◆ **firmware list-update url**

<説　　明> firmware list-update 時の参照先 URL を指定します。
<書　　式> firmware list-update url auto　　（自動 URL）
　　firmware list-update url WORD
< no > no firmware list-update url　　（firmware list-update 無効）
<初 期 値> firmware list-update url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL にはマクロ文字列が使用できます。詳細は、firmware update url コマンドを参照してください。

◆ **firmware list-update authentication**

<説　　明> firmware list-update 時の認証について設定します。
<書　　式> firmware list-update authorization default　　（初期値）
　　default authorization の設定に従います。
　　firmware list-update authorization bearer token WORD
　　指定したトークンで認証します。WORD には、トークンを指定します。
< no > no firmware list-update authorizatoin　　（認証不要）

◆ **information basic url**

<説　　明> information basic の送信先 URL を指定します。
<書　　式> information basic url auto　　（自動 URL）
　　information basic url WORD
< no > no information basic url　　（information basic の送信無効）
<初 期 値> information basic url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL にはマクロ文字列が使用できます。詳細は、firmware update url コマンドを参照してください。

◆ **information basic authentication**

<説　　明> information basic 送信時の認証について設定します。
<書　　式> information basic authentication default　　（初期値）
　　default authorization の設定に従います。
　　information basic authentication bearer token WORD
　　指定したトークンで認証します。WORD には、トークンを指定します。
< no > no information basic authentication　　（認証不要）

◆ **information extra url**

<説　　明> information extra の送信先 URL を指定します。
<書　　式> information extra url auto　　（自動 URL）
　　information extra url WORD
< no > no information extra url　　（information extra の送信無効）
<初 期 値> information extra url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL にはマクロ文字列が使用できます。詳細は、firmware update url コマンドを参照してください。

◆ **information extra authentication**

<説　　明> information extra 送信時の認証について設定します。
<書　　式> information extra authentication default　　（初期値）
　　default authorization の設定に従います。
　　information extra authentication bearer token WORD
　　指定したトークンで認証します。WORD には、トークンを指定します。
< no > no information extra authentication　　（認証不要）

◆ **information watch url**

<説　　明> information watch の送信先 URL を指定します。
<書　　式> information watch url auto　　（自動 URL）
　　information watch url WORD
< no > no information watch url　　（information watch の送信無効）
<初 期 値> information watch url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL にはマクロ文字列が使用できます。詳細は、firmware update url コマンドを参照してください。

◆ **information watch authentication**

<説　　明> information watch 送信時の認証について設定します。
<書　　式> information watch authentication default　　（初期値）
　　default authorization の設定に従います。
　　information watch authentication bearer token WORD
　　指定したトークンで認証します。WORD には、トークンを指定します。
< no > no information watch authentication　　（認証不要）

◆ **syslog latest url**

<説　　明> syslog latest の送信先 URL を指定します。
<書　　式> syslog latest url auto　　（自動 URL）
　　syslog latest url WORD
< no > no syslog latest url　　（syslog latest の送信無効）
<初 期 値> syslog latest url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL にはマクロ文字列が使用できます。詳細は、firmware update url コマンドを参照してください。

◆ syslog latest authentication
<説　　明> syslog latest 送信時の認証について設定します。
<書　　式> syslog latest authentication default　　（初期値）
　　default authorization の設定に従います。
　　syslog latest authentication bearer token WORD
　　指定したトークンで認証します。WORD には、トークンを指定します。
< no > no syslog latest authentication　　（認証不要）

**◆ syslog archived url**
<説　　明> syslog archived の送信先 URL を指定します。
<書　　式> syslog archived url auto　　（自動 URL）
　　syslog archived url WORD
< no > no syslog archived url　　（syslog archived の送信無効）
<初 期 値> syslog archived url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL にはマクロ文字列が使用できます。詳細は、firmware update url コマンドを参照してください。

**◆ syslog archived authentication**
<説　　明> syslog archived 送信時の認証について設定します。
<書　　式> syslog archived authentication default　　（初期値）
　　default authorization の設定に従います。
　　syslog archived authentication bearer token WORD
　　指定したトークンで認証します。WORD には、トークンを指定します。
< no > no syslog archived authentication　　（認証不要）

**◆ import config url**
<説　　明> import config の参照先 URL を指定します。
<書　　式> import config url auto　　（自動 URL）
　　import config url WORD
< no > no import config url　　（import config 無効）
<初 期 値> import config url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL にはマクロ文字列が使用できます。詳細は、firmware update url コマンドを参照してください。

◆ **import config authentication**

<説　　明> import config 時の認証について設定します。
<書　　式> import config authentication default　　（初期値）
　　default authorization の設定に従います。
　　import config authentication bearer token WORD
　　指定したトークンで認証します。WORD には、トークンを指定します。
< no > no import config authentication　　（認証不要）

◆ **export config default url**

<説　　明> export config default の参照先 URL を指定します。
<書　　式> export config default url auto　　（自動 URL）
　　export config default url WORD
< no > no export config default url　　（export config default 無効）
<初 期 値> export config default url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL にはマクロ文字列が使用できます。詳細は、firmware update url コマンドを参照してください。

◆ **export config default authentication**

<説　　明> export config default 時の認証について設定します。
<書　　式> export config default authentication default　　（初期値）
　　default authorization の設定に従います。
　　export config default authentication bearer token WORD
　　指定したトークンで認証します。WORD には、トークンを指定します。
< no > no export config default authentication　　（認証不要）

◆ **export config file url**

<説　　明> export config file の参照先 URL を指定します。
<書　　式> export config file url auto　　（自動 URL）
　　export config file url WORD
< no > no export config file url　　（export config file 無効）
<初 期 値> export config file url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL にはマクロ文字列が使用できます。詳細は、firmware update url コマンドを参照してください。

◆ **export config file authentication**

<説　　明> export config file 時の認証について設定します。
<書　　式> export config file authentication default　　（初期値）
　　default authorization の設定に従います。
　　export config file authentication bearer token WORD
　　指定したトークンで認証します。WORD には、トークンを指定します。
< no > no export config file authentication　　（認証不要）

◆ **export config list url**

<説　　明> export config list の参照先 URL を指定します。
<書　　式> export config list url auto　　（自動 URL）
　　export config list url WORD
< no > no export config list url　　（export config list 無効）
<初 期 値> export config list url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL にはマクロ文字列が使用できます。詳細は、firmware update url コマンドを参照してください。

◆ **export config list authentication**

<説　　明> export config list 時の認証について設定します。
<書　　式> export config list authentication default　　（初期値）
　　default authorization の設定に従います。
　　export config list authentication bearer token WORD
　　指定したトークンで認証します。WORD には、トークンを指定します。
< no > no export config list authentication　　（認証不要）

◆ **export config upload url**

<説　　明> export config upload の参照先 URL を指定します。
<書　　式> export config upload url auto　　（自動 URL）
　　export config upload url WORD
< no > no export config upload url　　（export config upload 無効）
<初 期 値> export config upload url auto
<備　　考>
・ WORD には、URL(例 https://a.b.c.d/path)を指定します。
・ URL にはマクロ文字列が使用できます。詳細は、firmware update url コマンドを参照してください。

◆ **export config upload authentication**

<説　　明> export config upload 時の認証について設定します。
<書　　式> export config upload authentication default　　（初期値）
default authorization の設定に従います。
export config upload authentication bearer token WORD
指定したトークンで認証します。WORD には、トークンを指定します。
< no > no export config upload authentication　　（認証不要）

◆ **server**

<説　　明> CMS server mode に移行します。
<書　　式> server (A.B.C.D|X:X::X:X|FQDN)
< no > no server
<備　　考> CMS の IP アドレス(IPv6 アドレス、または FQDN)を指定します。
nxr(config-cms)#server 192.168.0.1
nxr(config-cms-server)#

◆ **port**

<説　　明> サーバのポート番号を指定します。
<書　　式> port <443|1024-65535>
< no > no port (= port 443)

◆ **cert**

<説　　明> サーバ証明書(CMS 側で使用しているサーバ証明書)を指定します。
<書　　式> cert NAME
< no > no cert
<備　　考>
・ http-server cert certificate NAME FILE コマンド(global mode)で、サーバ証明書(CMS 側で使用しているサーバ証明書)を、事前にインポートしておきます。

◆ **verify-peer**

<説　　明> サーバ証明書(CMS 側で使用しているサーバ証明書)を検証します。
<書　　式> verify-peer enable
< no > no verify-peer enable

◆ **ca-certificate file**

<説　　明> CA 証明書(CMS 側で使用している CA 証明書)を指定します。
<書　　式> ca-certificate file NAME
< no > no ca-certificate file NAME
<備　　考>
・ http-server cert chain-certificate コマンド(global mode)で、CA 証明書(CMS 側で使用している CA 証明書)を、事前にインポートしておきます。

◆ **ca-certificate enable**

<説　　明> CA 証明書を有効化します。
<書　　式> ca-certificate enable
<　no　　> no ca-certificate enable

◆ **ca-certificate verify-host**

<説　　明> CA 証明書(CMS 側で使用している CA 証明書)を検証します。
<書　　式> ca-certificate verify-host
<　no　　> no ca-certificate verify-host

◆ **exit-server**

<説　　明> CMS server mode から exit します。
<書　　式> exit-server
<備　　考> nxr(config-cms-server)#exit-server
　　nxr(config-cms)#

# 第 59 章　Warplink-SPS mode

**■ 製品情報**

Warplink-SPS については、こちらを参照してください。
https://www.centurysys.co.jp/products/service/warplink_sps.html

**◆ 本装置のモード**(CLI 本装置のモード モード / ゼロコンフィグモード)

本装置の通常モードは、CLI モード(コマンドラインモード)ですが、Warplink-SPS では、ゼロコンフィグモードを使用します。
本装置の CONFIG(DIP スイッチ)と INIT ボタンを操作することで、CLI モードから、ゼロコンフィグモードへの切り替えを行います。

**○ モードの切り替え**

(1) CONFIG(DIP スイッチ)を、10*0(下上 * 上)に設定します。
　STATUS1 LED が、次回システム起動時のモードを表示します。
(2) INIT ボタンを押下する毎に、モードが切り替わります。

| STATUS1 LED | 次回の起動モード |
|---|---|
| 緑点滅(＊) | CLI モード |
| 緑赤点滅(＊＊) | ゼロコンフィグモード |
| 消灯(●) | モード変更なし |

(3) CONFIG(DIP スイッチ)を 00*0(上上 * 上)に戻します。STATUS1 LED が点灯(●)します。
(4) 本装置をシステム再起動します(restart system)。
(5) (1)～(4)を、30 秒以内に実行します。

**○ 動作中のモード**

動作中のモード(システム起動後の現在のモード)は、STATUS1 LED で確認することが出来ます。

| STATUS1 LED | 動作中のモード |
|---|---|
| 緑点灯(●) | CLI モード |
| 緑赤点滅(＊＊) | ゼロコンフィグモード |

**◆ 本装置の動作**(ゼロコンフィグモード)

(1) 本装置を、ゼロコンフィグモードでシステム起動します。
　システム起動時の config は、warplink-sps-initial-config を使用します。
(2) システム起動後、本装置が Warplink-SPS サーバに接続して、config を取得します。
　取得した config を、running-config として使用します。

◆ **移行 command**

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

◆ **service**

<説　　明> サービスを起動します。
<書　　式> service enable
<　no　> no service enable

◆ **statistics traffic**

<説　　明> インタフェースの統計情報を Warplink-SPS サーバに送信する機能です。
　　統計情報を送信するインタフェースを設定します。
<書　　式> statistics traffic <0-7>
　　interface bridge <0-4095>|ethernet <0-2>|ppp <0-4>|tunnel <0-255>
<　no　> no statistics traffic |<0-7>
<備　　考> 指定できるインタフェース番号は、機種によって異なります。

関連するコマンドを以下に示します(本書の view mode を参照してください)。
copy WORD warplink-sps-initial-config
delete warplink-sps-initial-config
show warplink-sps-initial-config
show warplink-sps

# 第 60 章　Speed test mode

◆ **移行 command**

nxr#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr(config)#speed-test <0-5>
nxr(config-speed-test)#
※指定できるな番号は、機種により異なります。

◆ **method**

<説　　明> 測定方法として、fileload を指定することが出来ます。
<書　　式> method fileload

◆ **fileload**

<説　　明> ダウンロード／アップロードするファイルを URL で指定します。
<書　　式> fileload down ip WORD
　　fileload up ip WORD
<備　　考> WORD には、URL(http://, https://)を指定します。
　　例: http://192.168.0.100/filename.dat(ファイル形式は任意)

◆ **send-result**

<説　　明> 結果を送信する際のファイル形式を指定します。
<書　　式> send-result (text|json) WORD (|source A.B.C.D)
　　send-result (text|json) WORD password (|hidden) PASSWORD (|source A.B.C.D)
< no > send-result
<備　　考> WORD には、URL(http://, https://)を指定します。
　　HTTP サーバ(server.py)に、json 形式で結果を送信する例を示します。
　　send-result json http://192.168.0.249:3333/server.py source 192.168.0.254

◆ **target-interface**

<説　　明> インタフェースを指定することが出来ます。
<書　　式> target-interface ethernet <0-4>
　　target-interface map <0-1>
　　target-interface ppp <0-4>
　　target-interface tunnel <0-1023>
　　target-interface wwan <0-0>
< no > no target-interface
<備　　考> 指定できるインタフェース(および番号)は、機種により異なります。

関連するコマンドを以下に示します(本書の view mode を参照してください)。
speed-test
show speed-test
delete speed-test

# 第 61 章　DIO mode

**◆ 移行 command**

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

**◆ input debounce**

<説　　明> DI 端子の debounce 時間(msec)を設定します。
<書　　式> input <0-3> debounce <0-5000>
<　no　　> no input <0-3> debounce
<備　　考> 端子数 <0-3> は、機種によって異なります。

**◆ input detection**

<説　　明> DI 端子の状態監視を設定します。
<書　　式> input <0-3> detection (on|off)
<　no　　> no input <0-3> detection (on|off)
<備　　考> 以下は、DI(0)の off → on の状態変化を監視する例です。
　　input 0 detection on

<説　　明>
・ DI 端子の状態変化を検知した場合に、event-notify 機能と連携して、メールを送信することが出来ます。
<書　　式> input <0-3> detection (on|off) event-notify <0-1> boby MESSAGE
<備　　考>
・ MESSAGE には、メール本文を指定します。
　メール本文に %D を指定すると、現在日付を挿入することが出来ます。
　メール本体に %T を指定すると、現在時刻を挿入することが出来ます。
・ 以下は、DI(0)の on → off を検知した場合に、メール送信する例です。
　input 0 detection off event-notify 0 body ”MailTest %D-%T”
　　メール本文は、以下のようになります。
　　MailTest 2024/07/16-16:13:17

◆ **output hold**

<説　　明> DO 端子制御(on|off)の継続時間(sec)を設定します。
<書　　式> output <0-1> hold <1-300>
< no > no output <0-1> hold
<備　　考> 端子数 <0-1> は、機種によって異なります。

◆ **output initial**

<説　　明> 本装置起動時の DO 端子制御(on|off)を設定します。
<書　　式> output <0-1> initial (on|off)
< no > no output <0-1> initial

◆ **output netevent**

<説　　明> netevent 発生時、DO 端子制御(on|off)を行う設定です。
<書　　式> output <0-1> netevent <1-255>|<2048-4095> (on|off)
< no > no output <0-1> netevent
<備　　考> 以下の例では、track 1 の down で、DO(0)に、on を出力します。
(track 1 の up で、DO(0)に、off を出力します。)
output 0 netevent 1 on

# 第 62 章　interface wireguard mode

◆ **移行 command**

nxr#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr(config)#interface wireguard <0-31>
nxr(config-if-wg)#

◆ **description**

<説　　明> 当該インタフェースの説明を記述します。
<書　　式> description LINE
<　no　> no description

◆ wireguard port

<説　　明> 本装置のポート番号を設定します。
<書　　式> wireguard port <1024-65535>
　　wireguard port any
<　no　> no wireguard port

◆ **wireguard private-key**

<説　　明> 本装置の private-key(秘密鍵)を設定します。
<書　　式> wireguard private-key WORD

◆ **wireguard public-key**

<説　　明> 本装置の public-key(公開鍵)を設定します。
<書　　式> wireguard public-key WORD

◆ **wireguard remote-peer-id**

<説　　明> リモートピア(対向装置)の ID を指定します。
<書　　式> wireguard remote-peer-id <0-31>

◆ **mtu**

<説　　明> MTU の値を設定します。
<書　　式> mtu <256-1500>
<初 期 値> mtu 1420
<　no　> no mtu (初期値)
<備　　考> 1280 未満に設定すると、当該インタフェースの IPv6 は無効になります。

◆ **shutdown**

<説　　明> 当該インタフェースをシャットダウンします。
<書　　式> shutdown
<初 期 値> no shutdown
<　no　> no shutdown

### ◆ 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 masquerade

<説　　明>
・ インタフェースよりパケットを出力する際に、パケットの送信元 IPv4 アドレスを出力インタフェースの IPv4 アドレスに自動変換する機能です。
<書　　式> ip masquerade　　(有効)
<初 期 値> no ip masquerade　　(無効)
<　no　> no ip masquerade

### ◆ ip access-group

<説　　明>
・ global mode で設定した ACL をインタフェースに適用することで、パケットフィルタリングを行うことができます。
<書　　式> ip access-group (in|out|forward-in|forward-out) IPV4-ACL-NAME
<　no　> no ip access-group (in|out|forward-in|forward-out)

### ◆ ip (snat-group|dnat-group)

<説　　明>
・ global mode で設定した SNAT、または DNAT ルールをインタフェースに適用することで、Static NAT を動作させることが出来ます。
・ SNAT は、パケットの出力時に適用されます。DNAT は、パケットの入力時に適用されます。
<書　　式> ip (snat-group|dnat-group) NAT-NAME
<　no　> no ip (snat-group|dnat-group)
<備　　考> NAT ルールの設定は、ip snat/ip dnat)コマンド(global mode)で行います。

### ◆ ip spi-filter

<説　　明>
・ 簡易ファイヤウォールの一つとして、SPI(Stateful Packet Inspection)機能をサポートします。
・ パケットに関連するコネクションの状態を見て、当該パケットをドロップする(または、しない)を決める機能です。
<書　　式> ip spi-filter　　(有効)
<初 期 値> no ip spi-filter　　(無効)
<　no　> no ip spi-filter

### ◆ ip spi-filter log

<説　　明> フィルタログ機能(syslog mode 参照)を有効にします。
　　パケットが、SPI フィルタにマッチした場合、syslog に出力することが出来ます。
<書　　式> ip spi-filter log [limit <0-100>]
<初 期 値> ip spi-filter log limit 10
<　no　　> no ip spi-filter
<備　　考>

- limit を指定すると、1 秒当たりのログ出力数を制限します。初期値は、10 パケット / 秒です。
- WAN 側からの意図しないパケットが、SPI フィルタに大量にマッチする可能性があるため、ログ数を増やす場合は、十分に注意してください。

### ◆ ip tcp adjust-mss

<説　　明>

- Path MTU Discovery(PMTUD)機能(End-to-end でフラグメントが発生しない最大の MTU を発見すること)によって、フラグメントなしでパケットの送信を行うことが可能になります。
- しかし、通信の途中に存在する IPv4 機器(ルータ等)が、ICMP fragment needed をフィルタリングている場合(ブラックホールルータが存在する場合)や、PMTUD 機能をサポートしない機器が存在する場合は、PMTUD 機能が適切に動作しなくなるため、MTU 超えが発生したルータ上でパケットがドロップされて、End-to-end での通信に支障をきたすことになります。
- このような場合、TCP では SYN/SYN-ACK パケットの MSS フィールド値を調整することによって、サイズの大きい TCP パケットでもフラグメントなしで転送することが可能になるため、スループットの低下を抑制することが出来ます。

<書　　式> ip tcp adjust-mss (auto|<500-1460>)
<初 期 値> no ip tcp adjust-mss
<　no　　> no ip tcp adjust-mss

# 第 63 章　Wireguard mode

◆ **移行 command**

nxr#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr(config)#wireguard peer <0-31>
nxr(config-wg-peer)#

◆ **description**

<説　　明> 本モードの説明を記述します。
<書　　式> description LINE
<　no　> no description

◆ **server address**

<説　　明> サーバ(対向装置)のアドレス、およびポート番号を設定します。
<書　　式> server address A.B.C.D (|port <1024-65535>)
　　server address X:X::X:X (|port <1024-65535>)
　　server address ip FQDN (|port <1024-65535>)
　　server address ipv6 FQDN (|port <1024-65535>)
<　no　> no server address
<備　　考> ポート番号の初期値は、51820 です。

◆ **network**

<説　　明> サーバ(対向装置)のネットワークを設定します。
<書　　式> network A.B.C.D/M
　　network X:X::X:X/M
<　no　> no network A.B.C.D/M
　　no network X:X::X:X/M

◆ **public-key**

<説　　明> サーバ(対向装置)の public key(公開鍵)を設定します。
<書　　式> public-key WORD
<　no　> no public-key

◆ **keepalive**

<説　　明> キープアライブの間隔(秒)を設定します。
<書　　式> keepalive <1-65535>
<　no　> no keepalive

# 第 64 章　RIPng mode

◆ 移行 command
nxr#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr(config)#router ipv6 rip
nxr(config-router)#

◆ redistribute
<説　　明> 他のプロトコル等(OSPF、BGP、static、connectedなど)で取得したIPv6の経路情報を、他のRIPngルーターへ広告します。
<書　　式> redistribute (static|connected|ospf|bgp) (|metric <0-16>) (|route-map WORD)
<　no　> no redistribute (static|connected|ospf|bgp) (|metric <0-16>) (|route-map WORD)
<備　　考> RIPng において、metric 16 は「到達不能(インフィニティ)」を意味します。

◆ default-information
<説　　明> 本装置が「デフォルトルート(::/0)」を生成し、隣接する他の RIPng ルーターに対して広告します。
<書　　式> default-information originate
<　no　> no default-information originate

◆ default-metric
<説　　明> 他のルーティングプロトコルや経路から、ルートを再配送(redistribute)して取り込む際、デフォルトのメトリック値(初期値)を一括で指定します。
<書　　式> default-metric <1-16>
<初 期 値> default-metric 1
<　no　> no default-metric (|<1-16>)

◆ aggregate-address
<説　　明> 複数の連続する細かい IPv6 ネットワーク(個別ルート)を、1 つの大きなネットワーク(集約ルート)にまとめて周囲のルーターに広告します。
<書　　式> aggregate-address X:X::X:X/M
<　no　> no aggregate-address X:X::X:X/M

◆ distribute-list
<説　　明> access-list による RIPng の経路フィルタを設定することが出来ます。
<書　　式> distribute-list ACL-NAME (in|out) (IFNAME|)
<　no　> no distribute-list ACL-NAME (in|out) (IFNAME|)
<備　　考> 指定した経路情報のみ送信する場合は、以下のように設定します。
nxr(config)#ipv6 route access-list ACL permit X:X::X:X/M
nxr(config)#router ipv6 rip
nxr(config-router)#redistribute static
nxr(config-router)#distribute-list ACL out

◆ route-map
<説　　明> route-map による RIPng の経路フィルタを設定することが出来ます。
<書　　式> route-map WORD (in|out) IFNAME
<　no　> no route-map WORD (in|out) IFNAME
<備　　考> WORD には、適用する route-map 名を設定します。

◆ offset-list
<説　　明> 本装置が送受信するルーティング情報(経路情報)のメトリック値を加算(プラス)して調整します。
<書　　式> offset-list WORD (in|out) <0-16> (IFNAME|)
<　no　> no offset-list WORD (in|out) <0-16> (IFNAME|)

### ◆ timers basic

<説　　明> 経路情報の更新や維持、削除を管理する 3 つの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> timers basic 30 180 120
<　no　> no timers basic
<備　　考>
update: ルーティング情報を周囲のルーターに送信する間隔(秒)です。
timeout: 受信した経路情報が「無効(ダウンした可能性がある)」と判断されるまでの時間(秒)です。
garbage: 無効になった経路情報が、ルーティングテーブルから「完全に削除」されるまでの猶予時間(秒)です。

### ◆ passive-interface

<説　　明> 指定したインターフェースで、RIPng の受信のみを行います(RIPng の送信は行いません)。
<書　　式> passive-interface IFNAME
<　no　> no passive-interface IFNAME

### ◆ neighbor

<説　　明> RIPng のルーティング情報を、特定の相手に「ユニキャスト」で送信します。
<書　　式> neighbor X:X::X:X IFNAME
<　no　> no neighbor X:X::X:X IFNAME
<備　　考> リンクローカルアドレスを指定します。

関連するコマンドを以下に示します。
(本書の interface mode/interface tunnel mode/interface ppp mode を参照してください。)
ipv6 router rip
ipv6 rip split-horizon

# 第 65 章　OSPFv3 mode

◆ **移行 command**

nxr#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr(config)#router ipv6 ospf
nxr(config-router)#

◆ **router-id**

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

◆ **default-cost**

<説　　明> 指定したスタブエリアへ、ABR が広告するデフォルトルート(::/0)のコスト値を設定します。
<書　　式> area (A.B.C.D|<0-4294967295>) default-cost <0-16777215>
<　no　　> no area (A.B.C.D|<0-4294967295>) default-cost
<備　　考>
area: 対象となるスタブエリアの ID を、A.B.C.D 形式または 10 進数で指定します。
default-cost: デフォルトルートのコスト値を指定します。
本設定は、スタブエリアに接続する ABR でのみ有効です。

◆ **range**

<説　　明> エリア内の複数の IPv6 ルートを、1 つの大きな集約ルートに集約します。
<書　　式> area (A.B.C.D|<0-4294967295>) range X:X::X:X/M (|advertise|not-advertise)
<　no　　> no area (A.B.C.D|<0-4294967295>) range X:X::X:X/M
<備　　考>
area: 集約したい元々のルートが所属している「ソースエリア(送信元エリア)の ID」を指定します。
range: 集約した後の「新しい IPv6 アドレスとプレフィックス長(/M)」を指定します。
advertise: 集約したルートを他のエリアへ広告します

◆ **stub**

<説　　明> 指定したエリアをスタブエリアに設定します。
<書　　式> area (A.B.C.D|<0-4294967295>) stub
<　no　　> no area (A.B.C.D|<0-4294967295>) stub
<備　　考>
area: スタブエリアに設定するエリアの ID を指定します。
スタブエリアでは外部ルート(AS-External-LSA)の流入をブロックし、代わりに ABR がデフォルトルート(::/0)を広告します。
エリア内の全ルーターで本設定を行う必要があります。設定が一致しない場合、ネイバーは確立しません。
バックボーンエリア(エリア 0)はスタブエリアに設定できません。

◆ **stub no-summary**

<説　　明> 指定したエリアを完全スタブエリアに設定します。
<書　　式> area (A.B.C.D|<0-4294967295>) stub no-summary
<　no　　> no area (A.B.C.D|<0-4294967295>) stub no-summary
<備　　考>
area: 完全スタブエリアに設定するエリアの ID を指定します。
外部ルート(AS-External-LSA)に加え、他エリアからのルート(Inter-Area-Prefix-LSA)の流入もブロックし、代わりにデフォルトルート(::/0)のみを広告します。
no-summary は ABR でのみ設定します。エリア内の ABR 以外のルーターには、area stub を設定してください。

**◆ virtual-link**

<説　　明> 指定した Transit エリア(通過エリア)を経由して、隔離されたエリアとバックボーンエリア(Area 0)の間に仮想的なリンク(トンネル)を確立します。
<書　　式> area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
< no > no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
<備　　考>

- ✓ area: 仮想リンクを通過させる「Transit エリア(通過エリア)の ID」を指定します。スタブエリアを Transit エリアに指定することはできません。
- ✓ 末尾の A.B.C.D: 対向(トンネルの反対側)にあるルーターの router-id を指定します(IPv6 アドレスではない点に注意が必要です)。
- ✓ 設定の対称性: リンクの両端となる 2 台のルーター(ABR)の双方で、お互いのルーターID を指し合うように設定する必要があります。

**◆ virtual-link (タイマー・パラメーター調整)**

<説　　明> 仮想的に確立したバーチャルリンク上でやり取りされる、Hello パケットの送信間隔や障害検知タイマーなどの各種パラメーターをカスタマイズします。
<書　　式> area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
{dead-interval <1-65535>|hello-interval <1-65535>
|retransmit-interval <1-65535>|transmit-delay <1-65535>}
< no > no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D
{dead-interval|hello-interval|retransmit-interval|transmit-delay}
<備　　考>
各タイマーの役割は以下の通りです。hello-interval と dead-interval は両端で一致させる必要があります。

- ✓ hello-interval: バーチャルリンク上で Hello パケットを送信する間隔(秒)を指定します。
- ✓ dead-interval: 隣接ルーターがダウンしたとみなすまでの無通信時間(秒)を指定します(通常は hello-interval の 4 倍)。
- ✓ retransmit-interval: LSA(リンク状態広告)の送信後、相手からの確認応答(Ack)がない場合に再送するまでの待ち時間(秒)を指定します。
- ✓ transmit-delay: LSA を送信する際に、LSA のエージ(LS Age)に加算する遅延時間(秒)を指定します。

**◆ redistribute**

<説　　明> 他のルーティングソース(直接接続された経路や静的経路など)から取得した IPv6 ルートを、OSPFv3 のルートとして変換し、ネットワーク全体へ広告します。
<書　　式> redistribute (connected|static|rip|bgp)
< no > no redistribute (connected|static|rip|bgp)

**◆ redistribute (メトリック・メトリックタイプ指定)**

<説　　明> 他のルーティングソースから IPv6 ルートを取り込む(再配分する)際、OSPFv3 内での初期コスト値(メトリック)や、経路計算時のコスト加算方法(メトリックタイプ)を明示的に指定します。
<書　　式> redistribute (connected|static|rip|bgp) {metric <0-16777214>|metric-type (1|2)}
< no > no redistribute (connected|static|rip|bgp)
<備　　考>
metric : OSPFv3 に注入する際の初期コスト値を指定します。
metric-type : 外部ルートのコスト計算方法を「1」か「2」で指定します(初期値は「2」)。

**◆ passive-interface**

<説　　明> 指定したインターフェースでの OSPFv3 パケット(Hello 等)の送受信を停止し、ネイバー関係の確立を無効化します。
<書　　式> passive-interface INTERFACE
< no > no passive-interface INTERFACE

◆ **default-metric**

<説　　明> ルート再配分(redistribute)を行う際、個別のコスト値(メトリック)が指定されていない外部ルートに一括で適用されるデフォルトの初期コスト値を設定します。
<書　　式> default-metric <1-16777214>
<　no　> no default-metric [<1-16777214>]

◆ **max-concurrent-dd**

<説　　明> OSPFv3 のネイバー(隣接ルーター)との間で、同時に行うことができるデータベース記述パケット(DD パケット)交換処理の最大数を指定します。
<書　　式> max-concurrent-dd <1-65535>
<　no　> no max-concurrent-dd [<1-65535>]

関連するコマンドを以下に示します。
(本書の interface mode/interface tunnel mode/interface ppp mode を参照してください。)
ipv6 router ospf area
ipv6 ospf cost
ipv6 ospf hello-interval
ipv6 ospf dead-interval
ipv6 ospf retransmit-interval
ipv6 ospf transmit-delay
ipv6 ospf priority

# 付録 A　Packet Traveling

**1. IP filtering の優先順位**

INPUT/OUTPUT/FORWARD 時の filtering が適用される順番は、以下のとおりです。IPsec input/output policy check は、実際に SPD(Security Policy Database)を検索するわけではなく、ESP 化されてきたパケット / ESP 化するべきパケットの判断のみを行い、この判定に match したパケットが許可されます。

○ INPUT
(1) invalid-status-drop filter
・ invalid-status-drop in filter(SYSTEM)
・ invalid-status-drop in filter(interface 別)
(2) SYSTEM filter
・ TCP connection 数制限
(3) IPsec input policy check
・ IPsec ESP 化されてきたものは許可します。
(4) USER input filtering
(5) SPI check
(6) Service 用 filter(GUI アクセス用 filter など)

○ FORWARD
(1) invalid-status-drop filter
・ invalid-status-drop filter(SYSTEM)
・ invalid-status-drop forward-in filter(interface 別)
・ invalid-status-drop forward-out filter(interface 別)
(2) SYSTEM filter
・ Session limit
(3) IPsec input/output policy check
・ IPsec ESP 化されてきたものか、outbound policy に match するものは許可します。
(4) UPNP filtering
(5) USER forward in/out filtering
(6) SPI(input/forward 時のみ)
(7) Web 認証用 forward in/out filtering

○ OUTPUT
(1) IPsec output policy check
(2) IPsec outbound policy に match するものは許可します。
(3) USER output filtering

**2. NAT の優先順位**

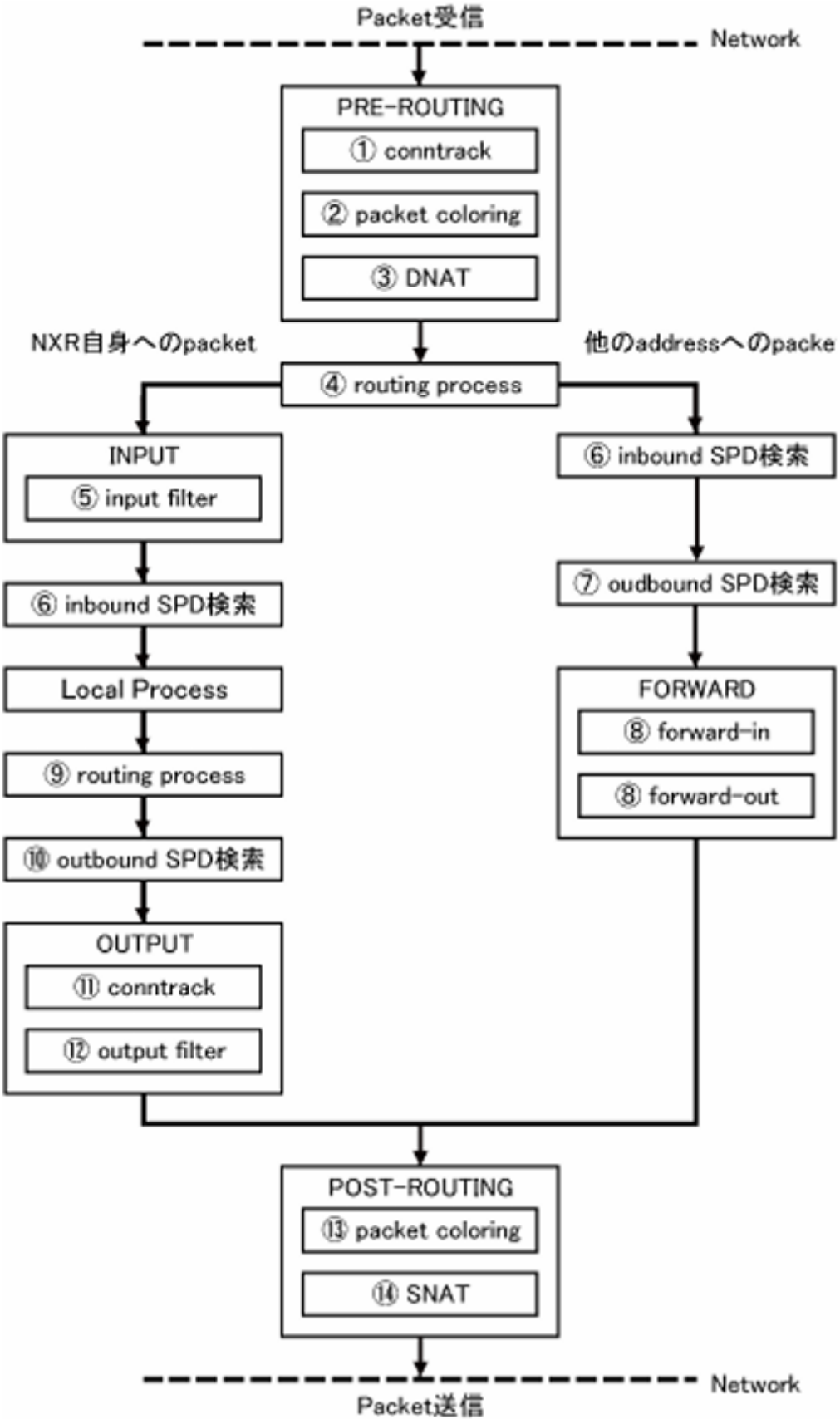
NAT の適用順位は、以下のとおりです。

○ INPUT
（1）SYSTEM DNAT
（2）UPNP 用 DNAT
（3）USER 設定 DNAT(Static NAT)

○ OUTPUT
（1）SYSTEM SNAT
（2）IPsec policy に match したパケットは、以下の NAT はチェックしません。
　　ただし、IPsec policy ignore 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

### 3. NXR Packet Traveling

NXR が Packet を受信してから送信するまでに適用される NAT、filtering、packet coloring の順番を下図に示します。



# 付録 A　Packet Traveling

○ Packet forwarding 時

- Packet 受信 -

① Conntrack
conntrack テーブルをチェックして、テーブルにマッチしないパケットを破棄します。conntrack テーブルは、session コマンド(global mode)を使用して設定します。

② Packet coloring(input)

③ Destination NAT
詳細は、NAT の優先順位(INPUT)を参照してください。

④ Routing Process

⑥ IPsec inbound SPD(※ 1)検索
ESP 化されてきた packet は、ここで policy check が行われます。ESP 化すべき packet が plain-text で送信されてきた場合は drop されます。但し、ipsec policy-ignore input が有効な場合は、ここでの check は行われません。

⑦ IPsec outbound SPD(※ 1)検索
ipsec policy-ignore output が設定されている場合は、policy 検索は行われません。

⑧ Packet filtering
詳細は、IP filtering の優先順位(FORWARD)を参照してください。

⑬ Packet coloring(output)

⑭ Source NAT
詳細は、NAT の優先順位(OUTPUT)を参照してください。

- Packet 送信 -

○ Packet 受信時(NXR が宛先)

- Packet 受信 -

① Conntrack
conntrack テーブルをチェックして、テーブルにマッチしないパケットを破棄します。conntrack テーブルは、session コマンド(global mode)を使用して設定します。

② Packet coloring(input)

③ Destination NAT
詳細は、NAT の優先順位(INPUT)を参照してください。

④ Routing Process

⑤ Packet filtering
詳細は、IP filtering の優先順位(INPUT)を参照してください。

⑥ IPsec inbound SPD(※ 1)検索
ESP 化されてきた packet は、ここで policy check が行われます。ESP 化すべき packet が plain-text で送信されてきた場合は drop されます。但し、ipsec policy-ignore input が有効な場合は、ここでの check は行われません。
--> ESP packet の場合、認証 /decrypt 処理後、①へ戻ります。
--> NXR local process

○ Packet 送信時(NXR が送信元)

- NXR Local Process が Packet 送出 -

⑨ Routing process

⑩ IPsec outbound SPD(※ 1)検索

⑪ Conntrack

conntrack テーブルをチェックして、テーブルにマッチしないパケットを破棄します。conntrack テーブルは、session コマンド(global mode)を使用して設定します。

⑫ output filter

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

⑬ Packet coloring(output)

⑭ Source NAT

詳細は、NAT の優先順位(OUTPUT)を参照してください。

SNAT される場合、この後で再度 IPsec outbound SPD 検索が行われます。但し、ipsec policy-ignore output が設定されている場合は、policy 検索は行われません。 Policy に match した packet は、encrypt 処理を行い、OUTPUT chain --> POST ROUTING を通過し、ESP packet が出力されます。

- Packet 送信 -

(注 1)

IPsec を使用するにあたって、どのようなパケットに対してどのようなアクション{discard(パケット廃棄する)、bypass(IPsec 処理を行わない)、apply(IPsec を適用する)}を行うかを定めたルールが SP(Security Policy)で、SP を格納するデータベースが SPD(Security Policy Database)です。

SPD には、inbound SPD と outbound SPD があります。受信パケットの policy check には、inbound SPD が検索されます。送信パケットの policy check には、outbound SPD が検索されます。

# 付録 B　Policy based IPsec と Route based IPsec

# I. Policy based IPsec

## 1. Policy based IPsec

ここでは、NXR の IPsec が policy base として動作する場合の仕様について記します。Policy base として動作する場合、routing table に関係なく、policy に match する packet はすべて ESP 化されます。
IPsec ESP 化される packet に対して、filtering や NAT(SYSTEM NAT を除く)を行うことはできません。

### 1.1. IPsec policy matching

policy に match しない packet は routing table に従って forwarding されます。policy に match せず、かつ route がない場合は、drop されます。

### 1.2. ESP 化時の処理

#### 1.2.1 IPv4 DF 付き Packet の ESP 化

IPsec において PMTU discovery が無効となっている場合は、DFbit が 1 でかつ tunnel MTU を超えてしまう場合でも、強制的に tunneling して転送されます。この場合、outer の IP header の DF bit は、必ず 0 が設定されます。
一方、IPsec において PMTU discovery が有効な場合、DFbit が 1 でかつ tunnel MTU を超えると、fragment needed を送信元に返信し、packet は drop されます。このとき、outer の IP header の DF bit 値は、tunneling packet の値が設定されます。

#### 1.2.2 IPv6 Packet の ESP 化

IPv6 の場合も IPv4 と基本的に同様な動作を行います。IPv6 では、中間の router で fragment されないため、PMTU Discovery を使用して fragment が発生しないような packet size を見つけて送信します。この機能は、Default で有効とし、無効にすることはできません。
また、NXR にて tunneling を行う際、tunnel header tax によって転送可能な最大 packet size が、IPv6 の最小 MTU(1280bytes)を下回る場合が考えられます。この場合、1280 より小さい値を送信元に返しても、送信元ノードは 1280 より小さい packet に分割して送信することができないため、通信ができない現象が発生してしまいます。
以下に、tunneling 時に MTU 超えが発生した場合の fragment 動作について記載します。なお、tunnelMTU とは、出力 interface の MTU から tunnel header を引いたものを表します。

#### 1.2.2.1. tunneling 時の fragment 動作

a. IPv6 over IPv6 tunneling (RFC2473 参照)

- tunnel MTU が IPv6 最小 MTU(1280)より大きい場合
  Packet を破棄し、送信元 host へ icmpv6 packet too big message を返信します。
- tunnel MTU が IPv6 最小 MTU(1280)と同じか小さい場合
  強制的に fragment して送信します。

b. IPv6 over IPv4 tunneling (RFC2893 参照)

- tunnel MTU が IPv6 最小 MTU(1280)より大きい場合
  Packet を破棄し、送信元 host へ icmpv6 packet too big message を返信します。
- tunnel MTU が IPv6 最小 MTU(1280)と同じか小さい場合
  tunneling packet が IPv6 最小 MTU より大きい場合、Packet を破棄し、送信元 host へ icmpv6 packet too big message を返信します。
  Tunneling packet が IPv6 最小 MTU より小さい場合、tunnel header の DFbit は必ず 0 に設定され、fragment して送信されます。

### 1.2.3 Fragment Packet の ESP 化

Fragment packet を ESP 化する場合は、reassemble 後に ESP 化を行います。

### 1.2.4 ToS 値の設定

Tunneling IP header の ToS field には、tunneling packet の ToS 値(IPv6 の場合は traffic class の値)が設定されます。なお、ECN field の扱いについては、次のとおりです。

#### 1.2.4.1. ECN field の扱い

Tunneling される packet の IPv4 ToS/IPv6 traffic class の ECN field 値によって、tunnel IP header の ECN filed は以下のように設定されます(ECN field については RFC3168 参照)。

- CE の場合
  ECT(0)が設定されます。
- CE でない場合
  ECN field 値がコピーされます。

### 1.3. IPsec policy ignore 機能

・ IPsec policy のチェックを行わないように指定する機能です。IPsec policy として any などを指定したけれども、特定の通信のみ IPsec 化したくない場合に、この機能を使用します。

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

・ インタフェース(Ethernet/Tunnel/PPP)毎に設定することができます。
・ Input を指定した場合、inbound policy check を実行しないため、IPsec 化されてくるべきパケットがドロップ されてしまう現象を回避することができます。
・ Output を指定した場合、当該インタフェースから出力されるパケットは、IPsec policy をチェックしないため平文で送信されます。

# II. Route based IPsec

## 2.　Route based IPsec

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

### 2.1.　IPsec tunnel interface

○ IPsec tunnel interface の設定
IPsec tunnel interface は、GRE や ip-in-ip tunnel と同じように、tunnel interface を使用します。
mode を変更することにより、使用する転送用 protocol(IPv4 または IPv6)を変更することができます。
通常の tunnel interface と同じように、tunnel 上で ospf などの routing protocol を利用したり、ip address を設定したり、multicast を送受信することもできます。
<書　　式> tunnel mode (ipip|gre|ipsec ipv4|ipsec ipv6)
<　no　> no tunnel mode
<備　　考> Route based IPsec を使用する際は、ipsec ipv4/ipsec ipv6 を指定します。

IPsec tunnel interface 設定時、以下の option を指定することができます。

○ Path MTU Discovery 機能の有効 / 無効

有効な場合、outer IP header の DF bit は、ipv4 の場合は DF bit がコピーされます。IPv6 の場合は、1 が設定されます。但し、IPv6 を tunneling する場合に MTU 超えが発生したときは強制的に 0 が設定されることがあります。詳細は、「付録 B 1.2.2. IPv6 Packet の ESP 化」を参照してください。

無効な場合、outer header の DF bit は常に 0 が設定されます。Path MTU Discovery の動作は、「付録 B 2.3. IPsec tunnel interface での Path MTU Discovery 動作」を参照してください。

<書　　式> tunnel path-mtu-discovery
<初 期 値> tunnel path-mtu-discovery　　（有効）
<　no　　> no tunnel path-mtu-discovery

○ ICMP Address Mask Request reply

ICMP address mask request に応答するかどうかを設定します。

<書　　式> ip mask-reply
<初 期 値> no ip mask-reply　　（応答しない）
<　no　　> no ip mask-reply

○ ToS 設定(0-252 または inherit) (Default: inherit)

Tunnel IPv4(outer)ヘッダの ToS フィールドに設定する値を指定します。

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

- Tunnel IPv4(outer)ヘッダの ToS フィールドに設定する値を指定します。inherit を指定した場合、IPv4(innner)ヘッダの ToS 値、または tunneling IPv6(inner)ヘッダの traffic-class 値を tunnel IPv4(outer)ヘッダにコピーします。
- ToS 値を指定する場合、0-252 の範囲で指定することが出来ます。
- ECN フィールドの設定は出来ません。ECN field の扱いについては、「付録 B 1.2.4.1 ECN field の扱い」を参照してください。

※ GRE トンネル上で、IPv6 パケットをトンネリングする場合は、inherit を無視し、ToS 値として 0x0 を設定します。

○ TTL 設定

- 固定の値(1-255)を設定する場合は、PMTUD を有効にします。
- inherit を設定した場合、GRE/IPIP の場合とは異なり、TTL にシステムの default 値(64)を使用します。

<書　　式> tunnel ttl (<1-255>|inherit)
<初 期 値> tunnel ttl inherit
<　no　　> no tunnel ttl (= tunnel ttl inherit)

○ protection 設定
使用する IPsec tunnel policy を指定します。
<書　　式> tunnel protection ipsec policy <1-65535>
<　no　　> no tunnel protection
<備　　考> Route based IPsec を使用する tunnel に設定します。

○ pre/post-fragment 設定
pre-fragment を指定すると、fragment 処理が必要な場合、先に fragment してから ESP 化します。(複数の ESP packet に分割されます)。詳細は、「付録 B 2.4 Fragment 処理」を参照してください。
<書　　式> tunnel pre-fragment
<初 期 値> no tunnel pre-fragment
<　no　　> no tunnel pre-fragment

### 2.2. Security Policy と IPsec phase2 ID との関係

Route base の場合、policy base の場合と異なり、IPsec phase 2 で negotiation された policy は SP(Security Policy)に登録されません。source/destination address、port/protocol すべてが any として SP に登録され、対応する interface として IPsec tunnel policy に bind された tunnel interface 名が登録されます。そのため、IPsec tunnel interface に送信または IPsec tunnel interface で受信した ESP packet は、すべて policy に match することになります。つまり、IPsec phase2 の ID は、対向 SG と IPsec SA を確立するための識別としてのみ使用されます。

### 2.3. IPsec tunnel interface での Path MTU Discovery 動作

IPsec tunnel interface における Path MTU Discovery の動作については、tunnel interface の場合の動作と異なり、policy base の場合と同様(「付録 B 1.2. ESP 化時の処理」参照)です。そのため、tunnel interface の MTU を超えている場合でも、Path MTU Discovery 機能を無効にすることにより、強制的に fragmentして送信することができます。

## 2.4. Fragment 処理

Fragment の処理として pre-fragment、post-fragment の 2 つを選択することができます。しかし、pre/post-fragment のどちらを設定しても、実際の処理はインタフェースの MTU 値によって内部的に決まります。

pre/post-fragment 設定は、forwarding するパケットと IPsec インタフェースの MTU 値の大小を判定する際に影響します。pre-fragment 設定の場合は PMTU 値で判定し、post-fragment 設定の場合はインタフェースの MTU 値で判定します。

そのため、post-fragment 設定で、なおかつ MTU が 1500 バイト設定のトンネルでは、PMTU に関係なく 1500 バイト以下のパケットは、ESP 化してから fragment します。

通常、IPsec インタフェースの MTU は 1500 バイトになっているため、forwarding するパケットは、ESP 化を行った後で、当該 ESP パケットが出力インタフェースの MTU 値より大きい場合に fragment(postfragment)します。このとき、ESP パケットと IP fragment パケットを出力します。

しかし、forwarding するパケットが、IPsec インタフェースの MTU より大きい場合は、IPsec インタフェースの MTU 値に fragment(pre-fragment)した後で、ESP 化します。このとき、複数の ESP パケットを出力します。

なお、デフォルトの動作は、post-fragment です。また、IPv6 パケットをトンネリングする場合は、pre/post-fragment の設定に依存せず、常に post-fragment として動作します。

### 2.4.1　Pre-fragment

Fragment 処理が必要な場合、fragment を行った後に ESP 化されます。そのため、複数の ESP packet に分割されます。
Pre-fragment は、以下のような場合に利用することが考えられます。

1)　Interoperability の確保
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、reassemble された際に 1500bytes 以上の packet になって処理できない場合があります。
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。

### 2.4.2　PMTUD 設定と Fragment 設定と DF bit の関係

Fragment が必要なパケットを IPsec 化する場合、pre-fragment(fragment 後に暗号化する方法)と postfragment(暗号化後に fragment する方法)の二通りの方法があります。
本装置で Pre-fragment をするか、post-fragment をするかは、本装置の PMTUD 設定と fragment 設定、および受信パケット(本装置で暗号化するパケット)の DF bit の値(0/1)の組み合わせによって決まります。
これらの組み合わせと pre-fragment/post-fragment の関係を Table 1 に示します。

Table 1. PMTUD 設定と Fragment 設定と DF bit の値と pre-fragment/post-fragment の関係

| PMTUD 設定 | Fragment 設定 pre/post | DF bit | 本装置の処理 |
|---|---|---|---|
| disable | pre | 0 | pre-fragment(fragment+暗号化) |
| | | 1 | pre-fragment(fragment+暗号化) |
| | post | 0 | post-fragment(暗号化+fragment) |
| | | 1 | post-fragment(暗号化+fragment) |
| enable | pre | 0 | pre-fragment(fragment+暗号化) |
| | | 1 | パケットを drop して、fragment needed を送信元に返す |
| | post | 0 | post-fragment(暗号化+fragment) |
| | | 1 | パケットを drop して、fragment needed を送信元に返す |

・ 本装置で post-fragment(暗号化＋ fragment)した場合、対向装置では受信した ESP パケットを reassemble+複合化の順序で処理します。

・ NXR での PMTUD 設定(enable/diable)と Fragment 設定(pre-fragment/post-fragment)は、interface tunnel mode で次のように設定します。

○ PMTUD 設定
＜ enable ＞　　tunnel path-mtu-discovery
＜ disable ＞　　no tunnel path-mtu-discovery
○ Fragment 設定
＜ pre-fragment ＞　　tunnel pre-fragment
＜ post-fragment ＞　　no tunnel pre-fragment

### 2.4.3　IPsec 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)。

### 2.4.4　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 | △<br>(SYSTEM NAT で一部対応可能) | ○ |
| filtering | × | ○ |
| routing protocol<br>(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 C　IKEv2 Protocol

# 付録 C　IKEv2 Protocol

NXR では、IKEv2 をサポートします。IKEv1 と同時利用することも可能です。以下に、IKEv2 の仕様を示します。

## 1.　IKEv1 と IKEv2 の相違点

IKEv1 と IKEv2 の主な相違点は、次のとおりです。

○ 名称変更

| IKEv1 | IKEv2 |
|---|---|
| ISAKMP SA | IKE_SA |
| IPsec SA | CHILD_SA |

○ Main/Aggressive/Quick mode の概念の廃止

Main/Aggressive/Quick mode の概念が廃止され、代わりに IKE_SA_INIT、IKE_AUTH、CREATE_CHILD_SA 交換が定義されました。ただし、それぞれが一対一に対応しているわけではありません。

○ Aggressive Mode の廃止

但し、pre-shared-key 方式での ID と暗号鍵の参照方法が変更されたため、通常の IKE_AUTH で動的 address クライアントと接続することができます。

○ lifetime, rekey に関する仕様変更

「4.Rekey」を参照してください。

○ SA の lifetime の negotiation の廃止

IKEv2 では、双方で個別の lifetime を管理するため、対向同士で異なる lifetime の SA を持つ可能性があります。そのため、rekey 時に responder と initiator が入れ替わる可能性があります。

○ IKE_SA と IPSEC_SA の依存関係の変更

IKEv2 では、IKE_SA の lifetime が切れて IKE_SA が無効になった場合、その IKE_SA を使用して作成された CHILD_SA も無効になります。

IKEv1 では、ISAKMP SA と IPsec SA の間に依存関係はなく、ISAKMP SA の lifetime が切れて無効になっても IPsec SA は有効のままです。

○ rekey の際の古い SA と新しい SA との依存関係の変更

IKEv2 では、rekey 時に古い SA の情報を交換し、新しい SA が作成された後に古い SA の削除を行います。

IKEv1 では、rekey 後に古い SA を削除することはありません。古い SA は lifetime が切れることによってのみ削除されます。

# 付録 C　IKEv2 Protocol

IKEv1 と IKEv2 で利用可能な機能は、下表のとおりです。

| 機能名 | IKEv1 | IKEv2 |
|---|---|---|
| set route | ○ | △(将来対応予定) |
| set priority | ○ | ×(対応予定 |
| ISAKMP backup | ○ | △(将来対応予定) |
| XAUTH | ○ | - |
| X.509 | ○ | ○ |
| PSK | ○ | ○ |
| 動的 IP 時の PSK の利用 | △<br>(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。

## 3.　サポート機能

下記に IKEv2 で使用可能な認証方式、algorithm、DH group を示します。

- なお、IKEv2 の CHILD_SA において、PFS で使用する DH group として phase1 を指定した場合、未指定扱いとなるため PFS 機能は無効となります。
- CHILD SA にて、NULL 暗号を指定した場合は、認証アルゴリズムを必ず指定してください(NULL 認証不可)。

### 3.1　IKE SA

**(認証方式 /Encryption/Hash algorithm/DH group)**

IKE SA にて使用可能な認証方式、Encryption、Hash algorithm、DH group を以下に示します。

**認証方式**

- Pre-shared-key 方式
- Digital 署名方式 RSA(X.509)
- EAP-MD5
- EAP-Radius

**Encryption**

- 3DES
- DES
- AES128/192/256

**Hash algorithm**

- MD5
- SHA1
- SHA256/384/512

**PRF algorithm**

- PRF-HMAC-MD5
- PRF-HMAC-SHA1
- PRF-HMAC-SHA-256
- PRF-HMAC-SHA-384
- PRF-HMAC-SHA-512

PRF は、HASH と同じ algorithm を使用します。

**DH group**

- DH group1(MODP768)
- DH group2(MODP1024)
- DH group5(MODP1536)
- DH group14(MODP2048)
- DH group15(MODP3072)
- DH group16(MODP4096)
- DH group17(MODP6144)

番号の大きい DH group を使用すると、CPU の処理能力が必要となるため、本装置の処理に影響を与える場合があります。

### 3.2　CHILD SA (Encryption/Hash algorithm/DH group)

EAP(CHILD SA)にて使用可能な Encryption、Hash algorithm を以下に示します。

- Encryption alogorithm のみが指定されている場合は、認証機能は無効です。
- NULL 暗号を指定した場合は、認証機能は必須です。

**Encryption**

- 3DES-CBC
- DES-CBC
- AES128/192/256-CBC
- NULL(暗号なし)

**Hash algorithm**

- HMAC-MD5-96
- HMAC-SHA1-96
- HMAC-SHA256-128
- HMAC-SHA384-192
- HMAC-SHA512-256
- NULL(認証なし)

**DH group( DH group PFS 有効時のみ)**

- DH group1(MODP768)
- DH group2(MODP1024)
- DH group5(MODP1536)
- DH group14(MODP2048)
- DH group15(MODP3072)
- DH group16(MODP4096)
- DH group17(MODP6144)
- DH group18(MODP8192)

DH group 未指定時、PFS は無効です。

## 4.　EAP-RADIUS 認証

IPsec client からの EAP message を、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。

### 4.1　RADIUS server 設定

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

### 4.2　NAS-identifier Attribute 設定

USER により任意の文字(32 文字以内)を指定することが可能です。Default は、機種名 -IPsec(ex.NXRG240-IPsec)です。

<書　　式> ipsec eap radius (A.B.C.D|X:X::X:X) password (|hidden) WORD
　　(|port <1-65535>) (|nas-identifier WORD)
<　no　> no ipsec eap radius (|A.B.C.D|X:X::X:X)
<備　　考> global mode で設定します。

## 5. Rekey

### 5.1 IKEv1 の Rekey

・ ISAKMP/IPsec SA の lifetime(hard timer)を設定することができます。Default は、ISAKMP SA は 10800[sec]、IPsec SA は 3600[sec]です。この時間を経過すると SA が削除されます。
・ Rekey の soft timer は、margin と increased-ratio により決定されます。Margin は、lifetime が切れる何秒前から rekey を実行するかどうかを指定します。increased-ratio 値は、margin よりどれぐらい増やすかを %で指定します。

<書　　式> rekey margin <30-360> (increased-ratio <0-100>|)
<初 期 値> no rekey margin
<備　　考>

・ ipsec isakmp policy mode で設定します。
・ 以下の式によって、Soft timer の最小・最大が決定され、この間でランダムに Soft timer が設定されます。
　　minimum soft timer = lifetime - margin
　　maximum soft timer = lifetime - (margin + margin x increased-ratio/100)
・ default 値は、margin が 270sec、increased-ratio は 100% です。このため、lifetime から 270 ～ 540sec 前の時間がランダムで設定されます。但し、Responder の場合、soft timer は、margin/2 時間分早く設定されます。これは、initiator 側より rekey を行うようにするためです。
・ increased-ratio を 0 に設定すると soft timer が毎回同じ値となります。負荷の分散やセキュリティ的に問題があるため、設定しないことを推奨します。

### 5.2 IKEv2 の Rekey

IKEv2 では、IKEv1 の Rekey に加え、送信 packet 数が最大 sequence number(4294967295)の 90[%]に達した際に rekey を行います。

# 付録 D　Firmware update

# 付録 D　Firmware update

## 1. Firmware の replace

NXR シリーズでは、CLI または GUI より、firmware 更新の指示を行うことが出来ます。Firmware の転送に使用可能な protocol は、下記のとおりです。

○ HTTP(GUI)

ユーザーズガイド -GUI 編を参照してください。

○ SSH/FTP(CLI)

SSH サーバ /FTP サーバ上にある firmware を取得します。SSH 使用時は、user 名、password、firmware のファイル名(パスを含む)を同時に指定します。FTP は、anonymous による接続のみ対応しています。

<書　　式>

firmware update ssh://<user@(A.B.C.D|X:X::X:X)>/FILENAME (|source A.B.C.D|X:X::X:X) (|no-boot)

firmware update ftp://<A.B.C.D|X:X::X:X>/FILENAME (|source A.B.C.D|X:X::X:X) (|no-boot)

<備　　考>

- ソースアドレスを指定することができます。
- SSH を使用する場合、次の書式でポート番号を指定することができます。ポート番号を指定しない場合(ssh://user@A.B.C.D/FILENAME)は、22 番ポートを使用します(=ssh://user@A.B.C.D:22/FILENAME)。
  - IPv4 ssh://user@A.B.C.D:port/FILENAME
  - IPv6 ssh://[user@X:X::X:X]:port/FILENAME
- no-boot を指定すると、現在(再起動前)と同じファームウェアで起動します。

○ copy(CLI)

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) (|no-boot)

<備　　考>

- no-boot を指定すると、現在(再起動前)と同じファームウェアで起動します。

# 付録 D　Firmware update

## 1.1 Firmware update 中の service の継続

firmware update 中もルータとしての処理を行うことが出来ます。
※本装置では、サービスを停止した上でのファームウェア更新は、サポートしていません。

※ Firmware update の実行例を下記に示します。

```
nxrg240#firmware update disk0:nxrg240-v900.bin
[==========================================] 100% DECODE
Proceed with update? [(y)es/(r)eserve/(n)o]: b ----- ①
Unsaved configuration changes exist. Save Flash? [y/n]: y ----- ②
After the firmware is updated, it reboots...
Firmware update is being
executed.....
Finished the firmware update, it reboots... ----- ③
```

① Firmare update を実行するかどうかを確認するメッセージが表示されます。
サービスを継続した状態でファームアップする場合は「y」を入力します。
サービスを継続した状態でファームアップを行い、ファームアップ後に再起動しない場合は[r]を入力します。
ファームアップをキャンセルする場合は「n」を入力します。

② 設定を保存していない場合は、保存するかどうかを問い合わせるメッセージが表示されます。保存する場合は「y」、保存しない場合は「n」を入力します。

③ firmware update が終了すると、自動的に再起動が行われます。
ただし、「r」を選択した場合、自動再起動は行わず、次回の再起動時に当該ファームウェアで起動します。

※ネットワーク経由(SSH や FTP)で firmware update を行った場合、回線状況等によって、ファームウェアの転送に失敗する場合があります。その場合は、回線の状態を確認してから、再度 firmware update を実行するようにしてください。

```
nxrg240#firmware update ssh://guest@192.168.2.222/nxrg240-v900b30.bin
guest@192.168.2.222's password:
[==========================================] 70% DOWNLOAD
% Download failed (255).
```

※ファイル転送後 3 分以内にファームウェアアップデートを実行しない場合(「Proceed with update?」が表示されてから、3 分以内に「y」を選択しない場合)、転送したファームウェアを破棄します。この場合は、再度 firmware update を実行してファイル転送から実施するようにしてください。

```
nxrg240#firmware update ssh://guest@192.168.2.222/nxrg240-v900b30.bin
guest@192.168.2.222's password:
[==========================================] 100% DOWNLOAD
Proceed with update? [y/n]: y
% Timed out.
```

### 1.2 Firmware update 中の設定保存 / 復帰

サービスの継続が可能な場合でも、firmware update 中は下記の動作を行うことはできません。

- CLI/GUI からの設定の初期化
- CLI/GUI/CMS からの装置の再起動
- CLI/GUI/CMS からの firmware update
- GUI/CMS からの設定復帰
- CLI からの設定の復帰 / 保存
- GUI からの設定(GUI からの設定時に、必ず flash への設定保存が行われるため)

### 1.3 Firmware update 終了後の動作

v5.8.1 以前の version では、firmware update 終了後に、自動的に再起動が行われます。

### 1.4 Firmware update/downdate 後の起動

Firmware の入れ替え作業後、通常 startup-config の version と firmware の version にミスマッチが生じます。このような場合の起動については、次のとおりです。なお、update および downdate のいずれにおいても、認識できない XML 要素名がある場合は無視されます(ログ表示もされません)。

(1) update 時

running-config が、新しい firmware version に対応した format に変更され、起動が行われます。
startup-config は、変更されません(以前の version のままです)。起動後に、USER が(save config 等によって)startup-config に書き込まない限り、startup-config の version が変わることはありません。

(2) downdate 時

startup-config と firmware の version が異なる場合、一部の config が認識できない可能性があります。
この場合、起動時にエラーとなった情報は起動時の情報としてログに残し、認識可能な部分だけを使用して起動します。なお、認識できない XML タグは、無視されます(ログ表示もされません)。

# 付録 E　Netevent 機能

**Netevent 機能**

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

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

## 1.　監視対象(track object)の設定

### 1.1　指定可能な監視対象

指定可能な監視対象は、以下のとおりです。

- interface link 状態監視
  interface の link 状態(up/down)を監視します。Keepalive が無効となっている interface に関しては、link down しないため、keepalive を有効にしてください。但し、PPP や tunnel interface のように interface の作成 / 削除ができるものに関しては、この限りではありません。
- IKE SA 状態監視
  IKE SA の状態(up/down)を監視します。
- ping/ping6 監視
  ping/ping6 による指定 host への ip reachability を監視します。
- VRRP 状態監視
  master から backup/init への変化、または backup/init から master への変化を監視します。
- OSPF neighbor 監視
  指定した router-id との neighbor 確立後から他の state への変化を監視します。
- BGP peer 監視
  指定した peer ip/ipv6 との neighbor 確立後から他の state への変化を監視します。
- IP/IPv6 neighbor 監視
  IP/IPv6 neighbor 監視には、ARP request、IPv6 neighbor solicitation を使用します。

### 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出来ます。Default で、DF が set されます。
- TTL/hop-limit
  TTL(IPv6:hoplimit)を指定します。Default は、system の TTL 値(64)が set されます。
- monitor-log
  monitor-log 機能で logging を行うかどうかを指定します。Default は、無効です。
- interval variable mode 指定
  ping/ping6 の送信間隔を、ping error 発生時に変化させるかどうかを指定します。Default は、無効です。

### 1.5.1　RTT status

RTT の状態を指します。

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

### 1.5.2　Interval variable mode

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

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

○ interval の計算方法

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

v_interval = (interval/2^fail_cnt)（2 のべき乗）
v_interval : 変更後の interval
interval : 設定されている interval
fail_cnt : 連続で ping fail となった回数

○ 各 track 状態での interval について

track 状態と interval の関係は、次のとおりです。

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

## 1.6　Initial timeout 設定

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

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

## 1.7　Interface ethernet の初期状態

Ethernet インタフェースの初期状態を track している場合、初期の track の状態(Ethernet インタフェースのリンクの up/down)は、次のとおりです。

- link up 時
  すぐに track up 状態となります。
- link down 時
  - initial-timeout を設定している場合、initial-timeout がタイムアウトする前に up 通知がない場合は down と判定します。
  - initial-timeout が未設定の場合、1 秒後に再度リンク状態を取得して、up でない場合は down と判定します。

## 2.　action の設定

### 2.1　指定可能な action

指定可能な action は、次のとおりです。設定の詳細は、当該項目を参照してください。

① VRRP Priority を指定値に変更することが出来ます。
次のコマンド（interaface mode）で設定します。
vrrp ip <vrrpid:1-255> netevent <trackid:1-255> priority <1-254>

② IPsec tunnel の確立 / 削除 / 再接続(isakmp 単位での指定)を行うことが出来ます。
次のコマンド（ipsec isakmp policy mode）で設定します。
netevent <trackid:1-255> (connect|disconnect|reconnect)

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

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

⑤ L2TPv3 tunnel の切断(PPP の interface link 監視のみ対応)を行うことが出来ます。
次のコマンド（l2tpv3 tunnel mode）で設定します。
netevent <trackid:1-255> disconnect

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

⑦ IPsec isakmp policy の変更を行うことが出来ます。
次のコマンド(ipsec tunnel policy mode)で設定します。
set key-exchange isakmp <1-65535> netevent <trackid:1-255> change isakmp <1-65535>

⑧ システムの再起動を行うことが出来ます。
次のコマンド（global mode）で設定します。
system netevent (<1-255>|<2048-4095>) restart

⑨ モバイルモジュールのリセットを行うことが出来ます。
次のコマンド（global mode）で設定します。
mobile <0-2> netevent (<1-255>|<2048-4095>) reset

⑩ BGP advertise-route の有効化 / 無効化を行うことが出来ます。
次のコマンド（bgp mode）で設定します。
netevent <trackid:1-255> advertise-stop

⑪ IPv4 static route の有効化 / 無効化を行うことが出来ます。
次のコマンド（global mode）で設定します。
ip route A.B.C.D/M (<gateway:E.F.G.H>|INTERFACE|null) (|<distance:1-255>)
(|netevent <trackid:1-255> (active|inactive))

⑫ PBR route の有効化 / 無効化を行うことが出来ます。
次のコマンド（route-map mode）で設定します。
netevent (<1-255>|<2048-4095>) (active|inactive)

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

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

### 2.2　Reconnect action

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

<書　　式> netevent <trackid:1-255> (connect|disconnect|reconnect)
　　netevent <trackid:2048-4095> (connect|disconnect|reconnect)
<　no　> no netevent

### 2.3　Change action

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

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

詳細は、ipsec isakmp policy mode/ipsec tunnel policy mode の「change action」を参照してください。

### 2.4　Restart action

当該トラックイベントが down した時に、システムの再起動を行います。イベント up 時は何も実行しません。

<書　　式> system netevent (<1-255>|<2048-4095>) restart
<　no　> no system netevent

### 2.5　Reset action

当該トラックイベントが down した時に、モバイルモジュールをリセットします。イベント up 時は何も実行しません。

<書　　式> mobile <0-2> netevent (<1-255>|<2048-4095>) reset
<　no　> no mobile <0-2> netevent

### 2.6　action 追加時の動作

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

### 2.7　action 削除時の動作

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

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

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

# 付録 F　VRRP

# 付録 F　VRRP

本装置でサポートしている VRRP(Virtual Router Redundancy Protocol)について記します。

- VRRP で使用する MAC アドレスは、RFC で定義されている仮想 MAC(00-00-5e-00-01-VRID)のみで、実 MAC を使用した VRRP はサポートしていません。したがって、NXR と XR 間で VRRP を使用する場合は、XR で仮想 MAC を使用してください。
- VRRP をサポートするインタフェースは、Ethernet インタフェースだけです。

## 1 VRRPv2

- VRRPv2(RFC3768)をサポートします。
- 実 IPv4 アドレスを仮想 IPv4 アドレスとして使用(IP address owner)することはできません。また、仮想 IPv4 アドレスは、実 IPv4 アドレス(セカンダリ IPv4 アドレスを含む)と同じネットワークアドレスを使用してください。

## 2 VRRP Tracking

- 特定の回線や IPsec SA の状態、あるいは特定ホストへの通信状態を監視し、状態が変化した際に VRRP の priority を指定値まで下げ、即座にマスターからバックアップ状態へと遷移する機能です。
- 逆に、監視対象となる回線や IPsec SA が正常状態へと遷移した場合は、VRRP priority は元の値へと戻ります。Netevent 機能と連動して動作します。

## 3 VRRP Event 機能

- VRRP がマスターからバックアップ状態へと変化した際に、PPP 回線の切断や IPsec SA の削除を行います。
- バックアップからマスターへと遷移した場合には、PPP 回線の接続や IPsec SA の確立を行います。
- この機能は、VRRP グループ毎に指定することが可能です。

## 4 Preempt 機能

・ Preempt 機能によって、バックアップルータがマスタールータへと切り替わる場合の動作を指定することができます。
  - Preempt が有効な場合、優先度のもっとも高いルータが、必ずマスタールータになります。
  - Preempt が無効な場合、priority の高いルータが復旧したとしても、現在マスターになっているルータがそのままマスタールータとして動作を継続します。

### 4.1 Preempt delay 機能

・ Preempt が有効な場合に、バックアップルータが自分より優先度の低い advertise を受信した際に、バックアップからマスターへ切り替わる時間を遅らせることが出来ます。delay 時間は、1 ～ 1000(秒)の範囲で指定(秒単位)します。
・ Preempt delay が設定されている場合、バックアップルータおよびマスタールータは、以下のとおり動作します。

○ バックアップルータ
  - master down timer、あるいは delay timer がタイムアウトすると advertise を送信してマスターへと状態遷移します。
  - 自分よりも優先度の高い advertise を受信した場合は、バックアップルータとして動作します(delay timer が動作している場合は停止します)。
  - 自分よりも優先度の低い advertise パケットを受信した場合、delay timer が未起動なら delay timer を開始し、master down timer はキャンセルします。また、delay 中に自分より優先度の低い advertise パケットを受信した場合は、無視します(delay timer を継続します)。

○ マスタールータ
  - 自分よりも優先度の高い advertise を受信した場合、バックアップルータへと遷移します。
  - 自分よりも優先度の低い advertise を受信した場合、advertise を無視します(マスタールータのまま状態遷移しません)。

# 付録 G　Config の保存と復帰

# Ⅰ. Config の保存

**Config の保存**

本装置での config は、running-config(現在動作している config)と startup-config(flash に保存され起動時に使用する config)が存在します。ユーザが設定の保存を実行した場合に限り、flash メモリや外部記憶装置に保存します。ただし、GUI から設定変更を行った場合は、設定と同時に flash にも保存します。

- 起動中の config(running-config)を、flash に保存するには save コマンド(view mode)を使用します。また、外部記憶装置に保存するには、copy コマンド(view mode)を使用します。詳細については、ユーザーズガイドの該当箇所を参照してください。
  - 起動中の config を flash に保存する例: save config
  - 起動中の config を外部記憶装置に保存する例:copy config disk0:config.xml

起動中の config を、HTTP(GUI からの実行)や SSH/FTP(CLI からの実行)を使用して、ネットワーク経由で保存することが出来ます。ユーザが設定した情報は、XML 形式で保存されます。

- 起動中の config(running-config)を、SSH/FTP サーバに保存するには、copy コマンド(view mode)を使用します。詳細については、ユーザーズガイドの該当箇所を参照してください。
  - 起動中の config を FTP サーバに保存する例:copy config ftp://A.B.C.D/config.xml

**■　show-config 形式での保存**

XML 形式での設定のエクスポートに加え、show-config 形式(CLI コマンド形式)の設定をエクスポートすることが出来ます。ただし、show config 形式で保存した config は、ファイルを読み込んで設定の復帰を行うことは出来ないため、本装置の起動後に CLI からログインし、ターミナルソフトなどからコピー&ペーストで設定の復帰を行います。

- show config 形式の設定をエクスポートするには、copy コマンド(view mode)を使用します。詳細については、ユーザーズガイドの該当箇所を参照してください。
  - 外部 SSH サーバに保存する例: copy show-config ssh://user@A.B.C.D/show-config.txt

# Ⅱ. Config の復帰

**Config の復帰**

Config を flash に保存(復帰)することで、再起動時の config として使用することが出来るようになります。

・ 起動中の config(running-config)を flash に保存(復帰)するには、save コマンド(view mode)を使用します。外部記憶装置やネットワーク経由で config を保存(復帰)するには、copy コマンド(view mode)を使用します。詳細については、ユーザーズガイドの該当箇所を参照してください。
  - 起動中の config を保存(復帰)する例: save config
  - 外部記憶装置から config を復帰する例: copy disk0:config.xml startup-config

GUI から設定の復帰を行った場合、startup-config を上書きします。再起動時に当該 config によってシステムが起動します。

※ 起動中の config(running-config)を、ネットワーク経由で取得した config で上書きすることは出来ません。ネットワーク経由で取得した config は、flash または外部記憶装置(USB メモリ)へ保存します。

※ ファームウェアのバージョンと config に含まれるファームウェアバージョンが異なる場合は、動作を保証しません。

・ CLI より config 復帰する際に、config 内のバージョンと現在動作しているファームウェアのバージョンが異なる場合は、ユーザに warning を表示して復帰するかどうかを確認します(config 内のバージョンをユーザが書き換えた場合の動作は保証しません)。

```
nxrg240#copy ssh://guest@192.168.0.1/config.xml startup-config
guest@192.168.0.1's password:
% Version is not same. continue? [y/n]:
```

CLI での config 表示は、XML 形式および CLI コマンド形式の 2 つのタイプの表示が可能です。GUI では、起動中の config 情報のみを表示します。

・ CLI で config を表示するには、show コマンド(view mode)を使用します。詳細については、ユーザーズガイドの該当箇所を参照してください。
  - XML 形式で表示する例: show config xml
    show startup-config xml
  - CLI コマンド形式で表示する例: show config

# Ⅲ. Config の保存形式

**Config の保存形式**

Config の保存を行った場合に、保存の対象となる情報は、次のとおりです。

- XML config 情報
- IPsec X.509 の証明書
- SSH 公開鍵

XML config 情報のみを保存する場合は、text 形式で保存することが可能です(config.xml)。
IPsec X.509 の証明書については、config 保存時にユーザが指定した場合のみ保存対象となります。この場合、XML config 情報と X.509 の証明書を tar.gz 形式で保存します(config.tar.gz)。

- tar.gz 形式で保存する場合は、copy コマンド(view mode)で all を指定します。詳細については、ユーザーズガイドの該当箇所を参照してください。
  - tar.gz 形式で保存する例: copy config disk0:config.tar.gz all

config.tgz で保存した場合、次のようなファイル名、ディレクトリ構成となります。

- config.xml
- ipsec/privates
  - /cacerts
  - /certs
  - /crls
- ssh/USER 名 /SSH 公開鍵

設定の復帰は、text 形式(xml 形式のみ)、tar.gz 形式(X.509 がなくても可)のいずれの形式でも行うことが出来ます。ファイル名については、特に制限はありません。ただし、tar.gz 形式で復帰した場合、展開後に config.xml(固定のファイル名)がない場合はエラーとなります。

# Ⅳ. INIT ボタン押下による起動時の制限

・ INIT ボタンは、ログイン出来なくなった場合や、config を初期化したい場合、あるいは一時的な設定により動作を確認したい場合 etc に使用します。
・ ログインが出来なくなった場合や config を初期化したい場合は、INIT ボタンによる起動後に、ログインして、erase flash コマンドで設定を消去します。

※ INIT ボタンによる起動方法については、「第1章 本装置の概要」→「Ⅱ各部の名称と機能」の該当項目を参照してください。
※ INIT ボタンを押下した状態で、本装置を起動した場合の制限は、次の通りです。

■ **flash に対するすべての操作の禁止**
・ save config、boot-config の変更、copy XXXX startup-config、show flash など、flash に対する操作を行うことは出来ません(※ただし、firmware update、および erase flash は、実行することが出来ます)。

■ **SD カードに対するすべての操作の禁止(※ SD カード内蔵機種のみ)**
・ SD カード上のファイル表示、config 表示、外部からのインポート、外部へのエクスポートなど、SD カードに対する操作を行うことは出来ません(※ただし、SD カードのフォーマットは、実行することが出来ます)。

■ **GUI による設定の禁止**
・ GUI から設定変更を行うと、必ず flash に config を保存します。そのため、INIT ボタン押下時は、GUI からの設定を行うことは出来ません。

# 付録 H　拡張 flash 管理仕様

# 付録 H　拡張 flash 管理仕様

本装置の拡張 flash 管理仕様について記します。

本装置では、通常起動用のファームウェアを、flash 1 および flash 2 にそれぞれ一つずつ(合計二つ)持つことが出来ます。

## 1.　ファームウェアの更新

ファームウェアの更新は、従来と同じコマンドを使用します。GUI/CLI/スケジュールから実行することが出来ます。

```
nxrg240#firmware update disk0:nxrg240-v900.bin
[==========================================] 100% DECODE
Proceed with update? [(y)es/(r)eserve/(n)o]:
```

[(y)es/(r)eserve/(n)o]の 3 つから選択することが出来ます(reserve 指定は、CLI のみ)。

## 2.　起動ファームウェアの選択

### 2.1　ファームウェア更新時の動作

firmware update を実行した場合、次回の起動はファームウェア更新を行った面から起動します。ただし、CLI からの firmware update 実行時に、no-boot オプションを指定することで、更新した面から起動しないようにすることも可能です。

<書　　式> firmware update disk0:nxrg240-v900.bin no-boot
<ノ ー ド ＞ view mode
<備　　考> no-boot オプションは、CLI のみ対応しています。

### 2.2　ユーザによる指定

次回起動の際に使用するファームウェアの面を指定します。本設定は、config ファイル(xml)には保存されません。

<書　　式> system boot flash <1-2>
<ノ ー ド ＞ global mode

## 3. 起動 config

### 3.1 ユーザによる起動 config 指定

<説　　明> 次回起動時に使用する config をユーザが指定することが出来ます。
<書　　式> system config flash:FILENAME
<ノ ー ド > global mode
<備　　考> flash:startup.config を指定すると、save config した config で起動します。

<説　　明> USB メモリ内の config から起動します。
<書　　式> system config disk0:FILENAME
<ノ ー ド > global mode

<説　　明> bootup 設定を初期化します(startup-config で起動します)。
<書　　式> no system config
<ノ ー ド > global mode

### 3.2 起動時の config 選択順序

起動時に使用する config の優先順位は次のとおりです。
① ユーザ指定の config(system config コマンドで指定)
② show config 形式で保存された config
CMS サーバから、show config 形式の config を NXR にリストアする場合に該当します。
③ startup-config
save config で保存したもので、通常、起動時に使用します。
④ Flash memory 上の initial-config 領域に保存された initial-config(flash-initial-config)
⑤ 内蔵 SD に保存された initial-config(対象機種のみ)
⑥ 外付け SD カードに保存された initial-config (対象機器のみ)
⑦ 外付け USB メモリに保存された initial-config
⑧ initial-config(工場出荷設定)
※ INIT ボタン押下状態で起動した場合は、⑧で起動します。

### 3.3 config の形式と起動方法

起動時に使用する config ファイルの形式が tgz の場合と xml の場合で、起動方法が異なります。
① boot-config で指定された config ファイルが tgz の場合
・ tgz 内の config.xml をリストアして起動します。
・ tgz 内の ipsec/ssh 公開鍵を展開して使用します。

② boot-config で指定された config ファイルが xml の場合
・ xml ファイルをリストアして起動します。
・ ipsec および ssh 公開鍵は、flash 上のファイル(flash/.ssh および flash/.ipsec)を使用します。

なお、flash 内の構成は、次のとおりです(dir flash コマンドでは表示されません)。

| | |
|---|---|
| flash/.ipsec | -> ipsec 用証明書ファイル領域 |
| flash/.ssh | -> ユーザの ssh 公開鍵ファイル領域 |
| flash/.ssh_host | -> NXR 自身の ssh 秘密鍵 |

## 4. ファームウェアおよび config の管理(保存 / 削除)

### 4.1 ファームウェア管理(view/exec mode)

<説　明> 起動中のファームウェアバージョンを表示します。
<書　式> show version

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

<説　明> flash 上のファームウェアを消去します。
<書　式> erase firmware flash <1-2>

### 4.2 config 管理

<説　明> flash 上の config ファイルを表示します。
<書　式> dir flash

<説　明> flash 上の config を XML 形式で表示します。
<書　式> show flash FILENAME xml
　　show startup-config xml

<説　明> flash 上に startup-config として保存します。
<書　式> save config

<説　明> config を flash 上に保存(XML のみ保存)します。
<書　式> copy config flash:startup-config
<備　考> save config と同じです。ただし、ipsec/ssh 公開鍵は保存しません。
　　src/dst が同じ場合はエラーとなります。また、同じ disk 上に copy することはできません。

<説　明> config を WORD 指定した場所に別名で保存(XML のみ保存)します。
<書　式> copy config WORD
<備　考> すでに file が存在する場合は、「overwrite ?」と問い合わせます。
　　ipsec/ssh 公開鍵は保存しません。
　　src/dst が同じ場合はエラーとなります。また、同じ disk 上に copy することはできません。

<説　明> all オプションを指定して、config を flash 上に保存します。
<書　式> copy config flash:startup-config all
　　copy config startup-config all
<備　考> save config all と同じです。ipsec/ssh 公開鍵も保存されます。

<説　明> WORD 指定した場所に、xml の config と ipsec/ssh 公開鍵を tgz 化して保存します。
<書　式> copy config WORD all
<備　考> すでに file が存在する場合は、「overwrite ?」と問い合わせます。

<説　　明> startup-config(xml)を WORD で指定した場所に export します。
<書　　式> copy flash:startup-config WORD
　　copy startup-config WORD

<説　　明> GUI から config を保存した場合は、すべて startup-config に保存されます。
<書　　式> なし(GUI 操作)

<説　　明> flash 上の config を削除します。
<書　　式> delete flash FILENAME
<備　　考> FILENAME で startup-config を指定した場合は、erase startup-config と同じです。

<説　　明> bootup 設定を初期化します。
<書　　式> delete bootup-config

<説　　明> startup-config を削除します。
<書　　式> erase startup-config

<説　　明> flash 上の config(bootup-config 含む)をすべて削除します。
<書　　式> erase flash

<説　　明> tgz 形式(FILENAME の拡張子が tgz)の config を import します。
<書　　式> copy WORD flash:FILENAME
<備　　考>
① dst ファイル =flash/startup-config の場合
・ tgz ファイルの中の config.xml　　->　flash/startup-config
・ tgz ファイルの中の ipsec/ssh 公開鍵　　->　flash/.ssh/*, flash/.ipsec/*
② それ以外
・ flash/xxxxx として tgz ファイルのまま import します。

<説　　明> tgz 形式以外の config を import します。
<書　　式> copy WORD flash:FILENAME
<備　　考> flash/XXXX に import します。

※ config の名称は、下記のとおりです。
・ config: 現在起動している config(running-config)です。save config 実行時に保存されます。
・ SD-initial-config: SD 内に保存された initial-config(起動 config)です(内蔵 SD 搭載機種のみ)。
・ initial-config: Firmware 内部の初期 config です。ethernet 0 インタフェースの IP アドレスとして 192.168.0.254/24 が設定されています。
・ CMS-show-config: CMS からインポートした show config 形式の config です。CMS 以外からインポートすることは出来ません。
・ startup-config: 起動時に使用する config です。flash 上に存在します。
・ bootup-config: 起動時に使用する config 情報が記載されている config です。flash 上にのみ存在します。
・ system-config: 起動時に使用した config です。起動直後であれば、system-config と runningconfig は同じです。

# 付録 Ⅰ　RAS 機能

## ■ RAS 接続機能

・ BRI/ シリアル回線および L2TPv2 LNS において、クライアントからの call を受ける機能(Access Server 機能)です(本バージョンでは、BRI/ シリアル回線は未対応です)。
・ クライアントに割り当てる IPv4 アドレスをユーザ名や発信回線などの情報を元に、固定で割り当てることが出来ます。IPv6 アドレスの割り当ては、本バージョンでは対応していません。
・ なお、プロトコル上、RAS 回線着信時のユーザ名と、発信時に使用する PPP のユーザ名とは、重複しないように設定してください。

## ■ 着信回線の設定

### □ L2TP LNS での着信

・ L2TP LNS 機能による着信では、virtual-template を使用します。設定は、interface virtualtemplate mode を参照してください。

### □ BRI での着信

・ 本バージョンでは、未対応です。

## ■ 着信回線への static route の設定

・ 着信回線に対して、static route を設定する場合は、以下のいずれかの方法で設定します。

### □ 固定 PPP インタフェースの場合

・ 着信用に設定したインタフェースに対して、static route を設定します。RAS 着信待機状態で、static route が有効になります。

ip route A.B.C.D/M ppp <0-4>

### □ 動的 PPP インタフェースの場合

・ 接続相手に割り当てる IP アドレスをネクストホップアドレスとして static route を設定します。
RAS 着信後、クライアントに IPv4 アドレスを割り当てた際に static route が有効になります。
・ virtual-template を利用した着信の場合、PPP インタフェースが固定化されないため、この方法で設定します。

ip route A.B.C.D/M a.b.c.d

## ■ IP アドレスの割り当て

・ クライアントに対して割り当てる IPv4 アドレスを指定することが出来ます。IPv6 アドレスの割り当てには対応していません。

### □ ユーザ名毎に指定

・ ユーザ名毎に、割り当てる IPv4 アドレスを指定します。access-server profile mode で、次のように設定します。

```
!
access-server profile 0
 ppp username user01 ip 1.1.1.1
!
```

・ IPv4 アドレスの割り当てを行う場合、次のように、Access-server 側の local ip address (virtual-template の IP アドレス)を指定する必要があります。

### □ 着信時の本装置の IP アドレス

・ RAS 着信時、interface virtual-template mode で設定した IP アドレスを本装置の IP として使用します。

```
!
interface virtual-template 0
 ip address 10.0.0.1/32
!
```

### □ 着信 PPP での IPsec の利用

・ Virtual-template 上では、IPsec を利用することは出来ません。

# 付録 J　データコネクト

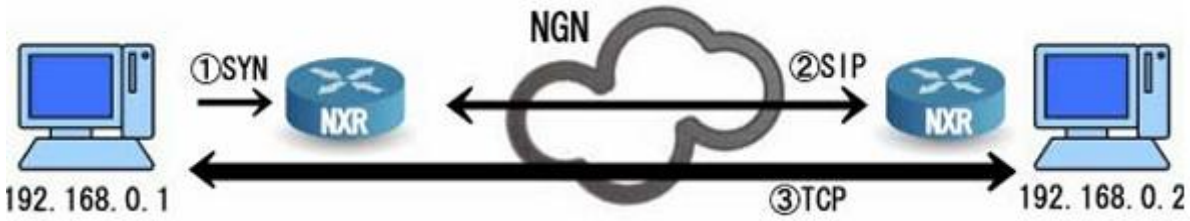
## ■ データコネクト

・ データコネクトとは、フレッツ光ネクスト(以下、NGN)の「ひかり電話」を契約している場合に使用することが出来る帯域確保型のデータ通信サービスです。2 拠点間での任意のデータ通信をオンデマンドで行うことが出来ます。
・ 本バージョンでは、TCP モードのデータ通信をサポートしています(VPN モードは未対応です)。

## ■ TCP モードによるデータコネクト接続

### □ 接続の概要

① 本装置宛ての TCP SYN パケットを検出します。
② 着信先の電話番号宛てに、ひかり電話による呼接続を開始し、2 拠点間で SIP セッションを確立します。
③ SIP セッション上で交換したお互いの WAN アドレスとポート番号を元にして、拠点間での TCP 通信が可能になります。




### □ SIP クライアントの設定(ngn-sip client mode)

・ TCP アクセスを監視する IP アドレス、および listen port を指定します。
<書　　式> mode tcp ip A.B.C.D port <1-65535>

・ TCP アクセス検出時に発呼する電話番号(宛先番号)を指定します。
<書　　式> tel to NUMBER
<備　　考> 「0」または「#」で始まる NUMBER を指定します。指定可能な桁数は 5 ～ 32 桁です。

### □ SIP サーバの設定(ngn-sip server mode)

・ 着信時に TCP を接続させる端末の IP アドレス(宛先 IP アドレス)、および宛先 port 番号を指定します。
<書　　式> mode tcp ip A.B.C.D port <1-65535>

・ 着信を許可する番号(発信者番号)を指定します。
<書　　式> tel from NUMBER
<備　　考> 「0」または「#」で始まる NUMBER を指定します。指定可能な桁数は 5 ～ 32 桁です。

### □ TCP 通信の無通信切断タイマー

・ TCP セッション上のデータ通信状態を定期的に監視し、一定時間の無通信状態を検出すると、自動的にデータコネクト通信を終了します。
<書　　式> idle-timeout <10-3600>
< no　> no idle-timeout (初期値)
<初 期 値> idle-timeout 60
< mode > ngn-sip client mode, ngn-sip server mode

## ■ NGN 回線との接続方法

・ データコネクトを使用する場合、NGN 回線と NXR は、以下のように接続します。

（LAN)-----NXR-----ONU-----(NGN 回線)

※ 一体型(ONU +ルータ)のひかり電話ルータ(ホームゲートウェイ:HGW)の配下に NXR を配置した場合は、正しく動作しません(将来対応予定)。

（LAN)-----NXR-----[ONU+ ルータ]-----(NGN 回線)

## ■ NGN 網における WAN アドレス

・ NGN 網で使用する WAN アドレス(IPv4)は、DHCPv4 にて取得します。

<説　　明> NGN 回線でデータコネクトを使用する場合に設定します。
<書　　式> ip dhcp mode ngn
< no　> no ip dhcp mode
< mode > interface mode
<備　　考> no を設定すると、ip dhcp request classless-static-route も無効になります。

## ■ Classless-static-route オプションによる route 設定

・ データコネクトと PPP によるインターネット通信を併用する場合、DHCPv4 の classless-staticroute オプション(RFC3442)を使って、NGN 網への static route 情報を取得することにより、データコネクトの通信を NGN 網へルーティングさせることが出来ます。

<説　　明> NGN 回線でのデータコネクトとインターネット接続(PPP)を併用する場合に設定します。
<書　　式> ip dhcp request classless-static-route
< no　> no ip dhcp request classless-static-route
< mode > interface mode
<備　　考> 取得した static route は、アドレスのリース期間中有効です。

## ■ データコネクト接続の最大セッション数

・ 同時に 2 つ以上の SIP セッションを接続することは出来ません。したがって、ひかり電話の「ダブルチャネル / 複数チャネル」サービスには対応していません。

・ TCP モードの場合、1 つの TCP コネクションにつき、1 つの SIP セッションが必要になります。したがって、同時に複数の TCP コネクションを使用するようなサービス(HTTP や FTP)は利用できません。

## ■ データコネクト接続の帯域制御

### □ データ通信の帯域

・ 本バージョンで対応している帯域は、64kbps です。

### □ データ通信の帯域制御

・ 設定した帯域幅の情報は、2 つの拠点間で(SIP セッションにより)交換されます。NGN 網では、SIP メッセージ上の帯域幅情報を元に、データ通信のパケットに対してポリシングが行われます。
・ 帯域幅を超過するデータパケットの送信は、UNI 基準に違反するため、WAN インタフェース上でシェーピング設定することを推奨します。

### □ データコネクト通信の DSCP

・ データコネクトで行われる各種の通信について、WAN インタフェース上で、本装置が次のように DSCP を設定します。
・ SIP パケット　　:46
・ DHCP パケット　　:46
・ データパケット(TCP/ESP)　　:8
・ 上記の値を使用して、WAN インタフェース上でシェーピング設定を行うことが出来ます。

## ■ JATE 発信規制

・ 同じ接続先に対して、最初の発信から 3 分以内に 2 回連続して失敗すると、3 回目からは発信を行いません。

## ■ 網輻輳時の LED 通知

・ SIP セッション接続時に、サーバ側から網輻輳を示す応答が返って来る場合があります。輻輳状態を知るには、system led を次のように設定します。

<書　　式> system led status <1-1> ngn-sip congestion
<　no　　> no system led status <1-1>
< mode > global mode
<備　　考>

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

## ■ ひかり電話の付加サービス

・ データコネクトでは、着信時に、発信者番号による発信者の認証を行うため、発信者番号の通知が必要になります。したがって、着信側としてデータコネクトを利用する場合は、「ナンバーディスプレイサービス」の契約が必要になります。
・ その他のひかり電話サービスについては、現在のバージョンでは未対応です。

# 付録 K　Policy Based Routing(PBR)

## ■ Policy Based Routing(PBR)

- 通常の宛先アドレスによるルーティングではなく、ユーザ設定によるポリシーを元にパケットのフォワーディング先を決めることが出来る機能です。
- 入力および出力インタフェースとして指定可能なインタフェースは、イーサネット /802.1Q VLAN/ ブリッジ / トンネル /PPP です。
- PBR は、通常の宛先アドレスによるルーティングより優先されます。
- 本バージョンでは、IPv6 PBR はサポートしていません。

- ポリシーとして設定可能な項目は、次のとおりです。マッチ条件の設定には ip policy access-list(global mode)、ルーティングルールの設定には route-map(route-map mode)を使用します。

### □ マッチ条件

● フォワーディングおよび自発パケットに対して有効な条件
- ○ 送信元 IP アドレス: src IP アドレスにより出力先を決定します。
- ○ 宛先 IP アドレス: dst IP アドレスにより出力先を決定します。
- ○ 受信インタフェース: 受信したインタフェースにより出力先を決定します。
  自発パケットの場合は、自動的に lo を指定します。

● フォワーディングのみ適用可能な条件(自発パケットには適用されません)
- ○ プロトコル
- ○ ポート番号(TCP/UDP パケットの場合)
- ○ ICMP code/type
- ○ ToS 値

### □ ルーティングルール

- ○ 出力インタフェース
- ○ ネクストホップ IP アドレス

◆ **ip local policy route-map**

<説　　明> 自発パケットに、PBR のアクセスリストを適用します。
　　WORD には、適用する ACL 名(ip policy access-list にて設定)を指定します。
<書　　式> ip local policy route-map WORD
< mode > global mode
<備　　考>
・ 自発パケットに PBR の ACL を適用した場合、ACL 内の source/destination アドレス情報のみ条件として参照します。その他、プロトコルやポート条件などは無視します。

◆ **ip policy route-map**

<説　　明> 受信インタフェースに、PBR のアクセスリストを適用します。
　　WORD には、適用する ACL 名(ip policy access-list にて設定)を指定します。
<書　　式> ip policy route-map WORD
< mode > interface mode
<備　　考>
・ 入力および出力インタフェースとして指定可能なインタフェースは、イーサネット /802.1Q VLAN/ ブリッジ / トンネル /PPP です。

◆ **show ip policy access-list**

<説　　明> PBR のアクセスリストを表示します。
<書　　式> show ip policy access-list (|WORD)
< mode > view(exec) mode

◆ **show ip policy route-map**

<説　　明> 適用した PBR のルートマップを表示します。
<書　　式> show ip policy route-map (|WORD)
< mode > view(exec) mode

◆ **clear ip policy access-list**

<説　　明> 指定した PBR アクセスリストのカウンターをクリアします。
<書　　式> clear ip policy access-list WORD counter
< mode > view(exec) mode

# 付録 L　P2P 検出機能について

付録 L　P2P 検出機能について

## ■ P2P 検出機能

・ Peer-to-peer(P2P)アプリケーションの通信を検出する機能です。本機能は、IDS(IPS)を利用出来ないような環境で、簡易的に P2P アプリケーションを検出する目的で使用します。
・ 検出可能な P2P アプリケーションは、次の通りです。
・ Winny(ver2)
・ Share(EX2)（※ NT 版は未対応）
・ BitTorrent

## ■ P2P 検出時の action

・ P2P アプリケーションを検出した場合、当該通信に対して以下の action を指定することが出来ます。
・ deny　　:パケットを破棄します。
・ log　　:以下のようなフォーマットのログを出力します。

```
ulogd[XXX]: p2p-torrent-detect: Message
ulogd[XXX]: p2p-torrent-detect: Message
ulogd[XXX]: p2p-torrent-detect: Message
```

※　Message は、MAC ヘッダ /IP パケットの情報です。

## ■ 関連するコマンド

### ◆ ip p2p-detection

<説　　明> P2P 検出機能を有効にします(IPv4 のみ対応)。
<書　　式> ip p2p-detection (any|winny|share|bittorrent) {log|deny}
< no　> no ip p2p-detection
　　no ip p2p-detection (winny|share|bittorrent)
<備　　考>

- any とアプリケーション(winny/share/bittorrent)を同時に指定することは出来ません。
- VT を除く各インタフェースにて設定することが出来ます。
- 本機能は、フォワーディングするフレームに対して有効です。ブリッジインタフェースを経由してフォワーディングする場合は有効ですが、単純にブリッジするフレームに対しては無効です。

### ◆ show ip p2p-detection

<説　　明> P2P 検出のカウンタ情報を表示します。
<書　　式> show ip p2p-detection

### ◆ clear ip p2p-detection counter

<説　　明> P2P 検出のカウンタをクリアします。
<書　　式> clear ip p2p-detection counter

## ■ 利用時の注意点

- P2P 検出機能を有効にすると、パケットの中身の解析および復号処理を行うため、通信速度に影響を及ぼす可能性があります。特に BitTorrent の検出は、影響が大きいと考えられるため、bittorrent(または any)を指定する場合は、慎重に行うようにしてください。
  - 本機能を、送信インタフェースと受信インタフェースの両方で有効にすると、P2P 検出を 2 回行うことになります。そのため、インターネットに接続しているインタフェース上でのみ有効にすることを推奨します。

## ■ Fast-forwarding 機能との併用

- Fast-forwarding 機能を併用した場合、BitTorrent については、P2P 検出を行うことが出来ない場合があります。

# 付録 M　VLAN

# Ⅰ. VLAN 仕様

**スイッチポート搭載機種の VLAN 仕様**

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

**■　デフォルト VLAN ID(PVID)**

<説　　明> ポート毎に、デフォルト VLAN ID(PVID)を指定することができます。
- ここで指定した PVID は、トランク接続で付加する IEEE802.1Q タグ(VLAN タグ)の VLAN ID として使用されます。
- システムのデフォルト状態では、全てのポートは PVID=1 の VLAN に所属します。

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

**■　アクセスリンク／トランクリンク**

<説　　明>
ポート毎に、アクセスリンクとして使用するか、またはトランクリンクとして使用するかを設定します。
- ポートをアクセスリンクとして指定すると、そのポートが所属する VLAN トラフィックのみを転送することができます。転送するフレームに、VLAN タグを付加しません。システムのデフォルト状態では、全てのポートはアクセスリンクとして設定されています。
- ポートをトランクリンクとして指定すると、複数の VLAN トラフィックを転送することができます。転送するフレームには、フレームを受信したアクセスリンクの PVID を VLAN ID とする VLAN タグを付加します。タグ無しフレームは破棄します。

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

**■　VLAN データベース**

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

**■　VLAN ID とタグの有無**

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

■　**VLAN データベースの情報表示**

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

■　**スイッチポートの情報表示**

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

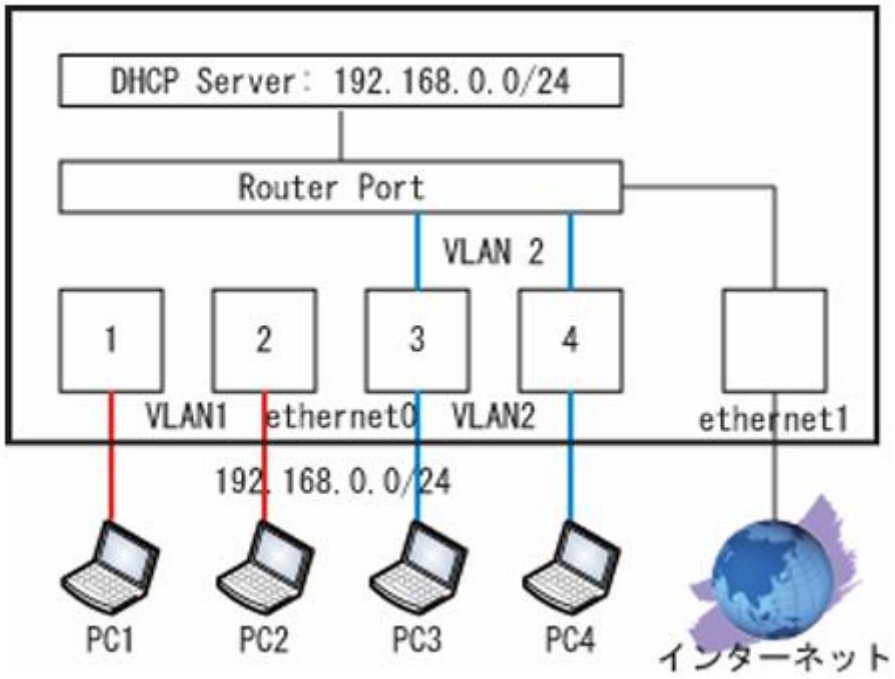
# Ⅱ. ポートベース VLAN

**ポートベース VLAN**

ポートベース VLAN の例を示します。

■ **ネットワーク構成**

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



■　**設定（抜粋）**

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

■　情報表示

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

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

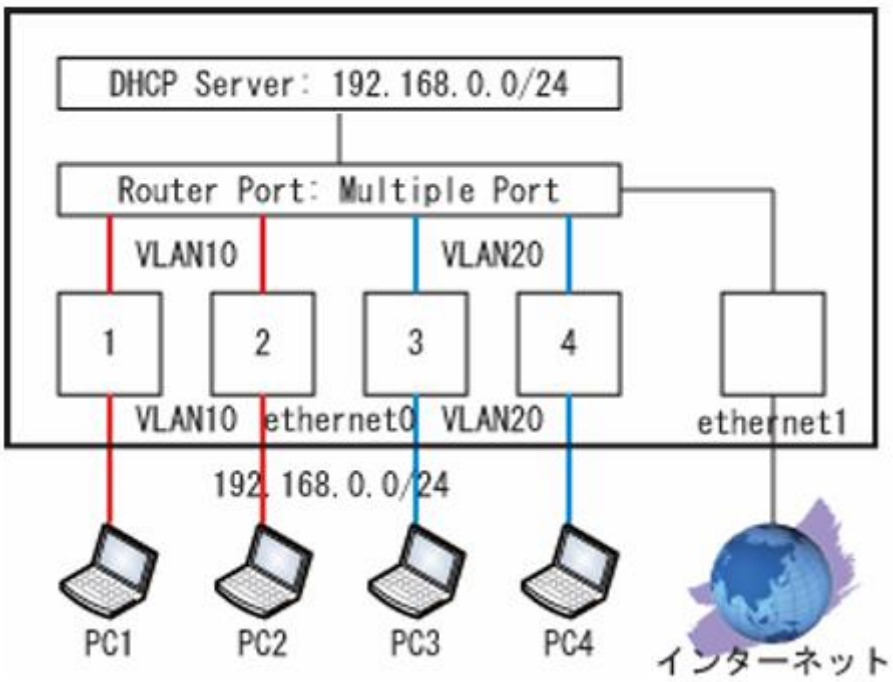
# Ⅲ. マルチプル VLAN

**マルチプル VLAN**

マルチプル VLAN の例を示します。

■ **ネットワーク構成**

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



■　設定（抜粋）

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

■　情報表示

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

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

# Ⅳ. タグ VLAN(VLAN トランク)

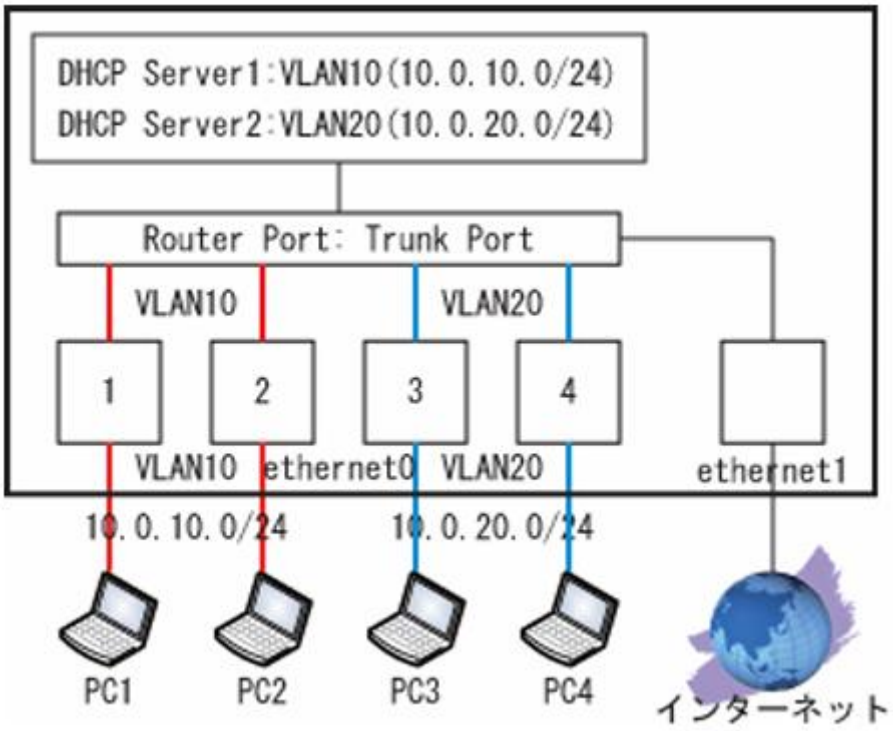
**タグ VLAN(VLAN トランク)**

タグ VLAN(VLAN トランク)の例を示します。

■　ネットワーク構成

・ VLAN10(Port1 と Port2)、VLAN20(Port3 と Port4)、および VLAN1[Router Port(Trunk Port)]からなる構成例です。

・ アクセスリンクとトランクリンクを保有します。アクセスリンクから受信したフレームは、PVID を VLAN ID とする VLAN タグを付加してトランクリンクから転送します。



■　設定（抜粋）

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

■　情報表示

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

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

# 付録 N　サポートについて

# 付録 N　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　　：0422-37-8112
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 https://www.centurysys.co.jp/

◆　故障と思われる場合は

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

◆　ご連絡をいただく前に

スムーズなお客様サポートをご提供するために、サポートデスクにご連絡いただく場合は以下の内容をお知らせいただきますよう、お願いいたします。

・　ファームウェアのバージョンと MAC アドレス
・　ネットワークの構成(図)
　どのようなネットワークで運用されているかを、差し支えのない範囲でお知らせください。
・　不具合の内容または、不具合の再現手順
　何をしたときにどういう問題が発生するのか、できるだけ具体的にお知らせください。
・　エラーメッセージ
　エラーメッセージが表示されている場合は、できるだけ正確にお知らせください。
・　本装置の設定内容、およびコンピュータの IP 設定
・　**可能であれば、「設定のバックアップファイル」をお送りください。**

◆サポート情報

弊社ホームページにて、製品の最新ファームウェア、マニュアル、製品情報を掲載しています。
また製品の FAQ も掲載しておりますので、是非ご覧ください。
下記の FutureNet サポートページから、該当する製品名をクリックしてください。
https://www.centurysys.co.jp/support/index.php

◆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。

本製品にはフラッシュ、電池、FAN 等「有寿命部品」が含まれる場合があります。
本製品の保守、保証期間内においても部品寿命に至った場合、保守、保証の対象外となります。

FutureNet NXR シリーズ ユーザーズガイド CLI 編 Ver.26.x 対応版

2026 年 11 月更新版

発行 センチュリー・システムズ株式会社

COPYRIGHT (C) 2009-2026 CENTURY SYSTEMS CO., LTD. ALL RIGHTS RESERVED.