ギガビットイーサネット対応 IPsec 集線ルータ

コマンドリファレンス

FITELnet F2200

（設定コマンド編）

古河電工

目次

コマンドリファレンスについて 7
コマンド形式の見方 7
使用可能文字について 7
コマンドの基本操作 8
各設定モードへの移行コマンド 10
BVI インタフェース設定モード 10
LAN インタフェース設定モード 11
PPPoE インタフェース設定モード 12
EWAN インタフェース設定モード 13
モデムインタフェース設定モード 14
ダイヤラーインタフェース設定モード 15
USB Ethernet インタフェース設定モード 16
ループバックインタフェース設定モード 17
RIP サービス設定モード 18
OSPF サービス設定モード 19
BGP サービス設定モード 20
アドレスファミリー設定モード 21
RIPng サービス設定モード 22
Route-MAP 設定モード 23
DHCP サーバ設定モード 25
IPv6 アドレスプール設定モード 27
DHCPv6 クライアントプロファイル設定モード 28
key-chain モード 29
イベントクラス設定モード 30
イベントアクション設定モード 31
イベントマップ設定モード 32
ICMP クラス設定モード 33
Watch クラス設定モード 34
クラスマップ設定モード 35
アクションマップ設定モード 36
ポリシーマップ設定モード 37
IPsec インタフェース設定モード 38
VLAN インタフェース設定モード 39
トンネルインタフェース設定モード 40
電子証明書（自身の ID）設定モード 41
グループ鍵 IPsec 設定モード 42
IKEv2 ポリシー設定モード 43
IKE ポリシー設定モード 44
VPN セレクタ設定モード 45
IPsec 各種設定モード 46
IPsec ログモード 47
Ethernet 設定モード 48
L2TP-PPP テンプレート設定モード 49
L2TP プロファイル設定モード 50
L2TP Pseudowire 設定モード 51
CLIENT-データベース設定モード 52

HTTP クライアント設定モード 53
Radius サーバ設定モード 54
sFlow profile 設定モード 55

PPPoE 機能 56

PPPoE を使用するための設定 56

DHCP クライアント機能 69

DHCP クライアントとして使用するための設定 69

DHCPv6 機能 74

DHCPv6 サーバ機能を使用するための設定 74
DHCPv6 クライアント機能を使用するための設定 90

IPv6 ルーティングの設定 103

IPv6 アドレスについて 103
Router Advertisement (RA) について 106
IPv6 アドレス設定 110
ICMPv6 に関する設定 114
RIPng 132
フィルタリングの設定 143
スタティックルーティングの設定 157
MTU 長の設定 159
ポリシールーティング 162
ドメインルーティングの設定 177
マルチキャストの設定 180
ECMP の設定 194

IPv4 ルーティングの設定 195

IP アドレスの設定 195
RIP に関する設定 200
OSPF に関する設定 231
フィルタリングの設定 280
スタティックルーティングの設定 294
ルートマップの設定 297
リゾルバの設定 315
MTU 長 323
TCP MSS 325
ProxyARP の設定 327
ARP 制御の設定 328
ダイレクトブロードキャストの設定 334
ICMP 制御の設定 335
ポリシールーティング 338
ドメインルーティングの設定 350
マルチキャストの設定 353
リミテッドブロードキャストの設定 370
ECMP の設定 371

BGP に関する設定 372

BGP4 について 372
BGP4 の設定 373

BGP4+の設定 427
MP-BGP の設定 442

IPsec 機能の設定 446

IPsec 基本コマンド 446
Phase1 ポリシーの設定 449
Phase2 ポリシーの設定 486
Mode-config の設定 508
トンネルルート機能の設定 516
SA-UP ルート機能の設定 520
拡張認証の設定 521
電子証明書に関する設定 525
IPsec のログ情報に関する設定 533
IPsec の各種設定 536
IPsec 基本コマンド(IKEv2) 557
IKE-SA の設定（IKEv2） 559
CHILD SA の設定（IKEv2） 575
拡張認証の設定（IKEv2） 598
電子証明書に関する設定（IKEv2） 600
IPsec のログ情報に関する設定（IKEv2） 605
IPsec の各種設定（IKEv2） 607
グループ鍵 IPsec 機能の設定 617

IP in IP 機能 639

IP in IP 機能 639

Layer2 中継機能 645

EtherIP/L2TPv2/L2TPv3 共通コマンド 645
EtherIP/L2TPv3 共通コマンド 647
L2TPv2/L2TPv3 共通コマンド 658
L2TPv2 関連コマンド 666
L2TPv3 関連コマンド 679

NAT 機能 688

NAT 機能 688

DHCP サーバ機能 715

DHCP サーバ機能 715

DHCP リレーエージェント機能 727

DHCP リレーエージェント機能 727

簡易 DNS 機能 730

簡易 DNS 機能の設定 730
ドメイン名による DNS 振り分け 738
ホスト名称と DNS IP アドレスの登録 739

ダイナミック DNS 機能 740

サーバ機能 740
クライアント機能(ダイナミック DNS 動作の設定) 744
クライアント機能（HTTP クライアントに関する設定） 746

簡易ファイアウォール機能 753
外部からの接続制御機能 753
IP パケットフィルタリング機能 756
MAC アドレスフィルタリング機能 761
サービス制限機能 778
冗長機能 783
VRRP 機能について 783
イベント-アクション機能 796
イベントクラス 796
宛先到達確認 815
アクション 825
マッピング 849
QoS/CoS 機能 851
クラスマップの定義 851
アクションマップの定義 862
ポリシーマップの定義 880
ポリシーマップの適用とキューの定義 883
L2 QoS 機能 893
L2 QoS 機能 893
UPnP 機能 899
UPnP 機能 899
モデム接続機能 902
モデム接続機能 902
障害監視／通知機能 945
SNMP エージェント機能 945
SYSLOGD への障害通知機能 952
電子メールによる障害通知機能 972
自律監視機能 977
FAN 制御機能 986
NTP 機能 987
SNTP クライアント機能 987
NTP サーバ機能 993
SSH サーバ機能 995
SSH サーバ機能 995
Ethernet 機能 1001
Ethernet 機能 1001
VLAN 機能 1014
VLAN 機能 1014
アクセスリスト 1023

アクセスリスト 1023
ループバックインタフェースの設定 1040
ループバックインタフェースの設定 1040
sFlow Agent 機能 1043
sFlow Agent 機能 1043
その他の機能 1051
CLI の表示に関する機能 1051
高速化キャッシュ機能 1055
設定内容の削除方法 1058

コマンドリファレンスについて

このマニュアルでは、FITELnet F2200 を設定する各種コマンドを説明したものです。
FITELnet F2200 の設定コマンドは、コンソールの基本設定モードで設定します。

コマンド形式の見方

コマンド形式で使用される記号の意味は以下の通りです。

記号	意味
{ }	{ } 内の項目は省略できません。
[ ]	[ ] 内のパラメータは省略可能です。
< >	< >内の内容にそった任意の値を入力して下さい。
|	| で区切られたパラメータのうち、どれか1つを選択して下さい。
,	, で区切られた項目は複数の選択が可能です。

使用可能文字について

FITELnet F2200 の文字列を入力するコマンドについては、以下の文字を使用することができます。
※ASCII コードで、00～1F までは、コントロールキャラクタになりますので、表示されていません。

表は ASCII コード　文字 の順で書かれています。

	21 !	22 ″	23 #	24 $	25 %	26 &	27 ’
28 (	29)	2A *	2B +	2C ,	2D −	2E .	2F /
30 0	31 1	32 2	33 3	34 4	35 5	36 6	37 7
38 8	39 9	3A :	3B ;	3C <	3D =	3E >	
40 @	41 A	42 B	43 C	44 D	45 E	46 F	47 G
48 H	49 I	4A J	4B K	4C L	4D M	4E N	4F O
50 P	51 Q	52 R	53 S	54 T	55 U	56 V	57 W
58 X	59 Y	5A Z	5B [	5C ¥	5D]	5E ^	5F _
60 `	61 a	62 b	63 c	64 d	65 e	66 f	67 g
68 h	69 i	6A j	6B k	6C l	6D m	6E n	6F o
70 p	71 q	72 r	73 s	74 t	75 u	76 v	77 w
78 x	79 y	7A z	7B {	7C |	7D }	7E ~	

コマンドの基本操作

FITELnet F2200 は、コマンドを入力しても機能設定を行うことができます。設定する場合は、ターミナルソフトを使って設定を行います。ターミナルソフトの使用方法は、パソコンや各ターミナルソフトの取扱説明書などを参照してください。

コマンド操作の手順

1. FITELnet F2200 とパソコンの COM ポートを、コンソールケーブルを使用して接続します。
↓
2. パソコンを起動します。
↓
3. パソコンでハイパーターミナル※を起動します。
↓
4. 装置の電源を入れます。
↓
5. ハイパーターミナルの画面に「Login:」と表示されます。
工場出荷状態ではログイン ID が設定されていないので、表示されず手順7の表示になります。
↓
6. 設定されているログイン ID を入力します。
↓
7. ハイパーターミナルの画面に「Enter pasword:」と表示されます。
↓
8. ログインパスワードを入力します。
工場出荷状態ではログインパスワードが設定されていないので、
「Enter キー」のみを押下します。
↓
9. プロンプトが表示され、コマンド入力待ち状態になります。

※：ハイパーターミナルの COM ポートのプロパティは、以下のように設定してください。

ビット/秒	9600(固定)
データビット	8
パリティ	なし
ストップビット	1
フロー制御	Xon/Xoff

特権ユーザモードへの移行

１．ログイン状態のプロンプトで、"enable"と入力します。
↓
２．パスワードの問い合わせがありますので、enable パスワードを入力します。
工場出荷状態では enable パスワードが設定されていないので、
「Enter キー」のみを押下します。
↓
３．特権ユーザモードへの移行が完了しました。
特権ユーザモードからユーザモードに戻る場合は、"exit"コマンドを
実行します。

基本設定ユーザモードへの移行

１．特権ユーザモードの状態で"configure terminal"と入力します。
↓
２．基本設定モードへの移行が完了しました。
基本設定モードから、特権ユーザモードに戻る場合は
"end"コマンドを実行します。

各設定モードへの移行コマンド

BVI インタフェース設定モード

interface bvi

BVI インタフェース設定モードに移行します。

設定例１　BVI インタフェース設定モードに移行します

```
Router(config)#interface bvi 1
Router(config-if bvi 1)#
```

コマンド書式

interface bvi <BVI インタフェース番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BVI インタフェース番号	BVI インタフェース番号を指定します。	1～100	省略不可

設定モード

基本設定モード

LAN インタフェース設定モード

interface lan

LAN インタフェース設定モードに移行します。

設定例 1　LAN インタフェース設定モードに移行する

```
Router(config)#interface lan 1
Router(config-if lan 1)#
```

コマンド書式

```
interface lan 1
```

パラメータ

パラメータはありません。

設定モード

基本設定モード

PPPoE インタフェース設定モード

interface pppoe

PPPoE インタフェース設定モードに移行します。
本装置は、24 の PPPoE インタフェースを持つことができます。
PPPoE インタフェース設定モードに移行する際は、PPPoE インタフェースの番号(1～24)を指定します。

設定例 1　PPPoE インタフェース設定モードに移行する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#
```

コマンド書式

interface pppoe <PPPoE 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
PPPoE 番号	PPPoE ポートの番号を指定します。	1～24	省略不可

設定モード

基本設定モード

EWAN インタフェース設定モード

interface ewan

EWAN インタフェース設定モードに移行します。

設定例１　EWAN インタフェース設定モードに移行する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#
```

コマンド書式

interface ewan <EWAN 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
EWAN 番号	EWAN ポートの番号を指定します。	1～2	省略不可

設定モード

基本設定モード

モデムインタフェース設定モード

interface modem

モデムインタフェース設定モードに移行します。

設定例１　モデムインタフェース設定モードに移行する

```
Router(config)#interface modem 1
Router(config-if modem 1)#
```

コマンド書式

```
interface modem 1
```

パラメータ

パラメータはありません。

設定モード

基本設定モード

ダイヤラーインタフェース設定モード

interface dialer

dialer インタフェース設定モードに移行します。

設定例１　ダイヤラーインタフェース設定モードに移行する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#
```

コマンド書式

interface dialer〈接続相手シーケンス番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
接続相手シーケンス番号	接続相手を識別する番号	1～20	省略不可

設定モード

基本設定モード

USB Ethernet インタフェース設定モード

interface usb-ethernet

USB Ethernet インタフェース設定モードに移行します。

設定例　USB Ethernet インタフェース設定モードに移行する

```
Router(config)#interface usb-ethernet 1
Router(config-if usb-ethernet 1)#
```

コマンド書式

interface usb-ethernet <USB ポート番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
USB ポート番号	USB ポートの番号を指定します。	1～2	省略不可

設定モード

基本設定モード

ループバックインタフェース設定モード

interface loopback

ループバックインタフェース設定モードに移行します。

設定例１　ループバックインタフェース設定モードに移行する

```
Router(config)#interface loopback 1
Router(config-if loopback 1)#
```

コマンド書式

interface loopback <ループバックインタフェース番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ループバックインタフェース番号	ループバックインタフェース番号を指定します。	1～100	省略不可

設定モード

基本設定モード

RIP サービス設定モード

router rip

RIP サービス設定モードに移行します。

設定例 1　RIP サービス設定モードに移行する

```
Router(config)# router rip
Router(config-rip)#
```

コマンド書式

router rip

パラメータ

パラメータはありません。

この設定を行わない場合

RIP を使用できません。

設定モード

基本設定モード

OSPF サービス設定モード

router ospf

OSPF サービス設定モードへ移行します。

設定例 1　OSPF サービス設定モードへ移行する

```
Router(config)#router ospf
Router(config-ospf)#
```

コマンド書式

```
router ospf
```

パラメータ

パラメータはありません。

この設定を行わない場合

OSPF を使用することができません。

設定モード

基本設定モード

BGP サービス設定モード

router bgp

BGP サービス設定モードに移行します。(AS 番号を指定)
BGP サービス設定モードでは、E-BGP/I-BGP のピアのアドレスや、各種アトリビュート情報を設定します。
有効になる最大ピア数は、500 ピアです。

設定例 1　BGP サービス設定モードに移行する（自 AS 番号=64512）

```
Router (config)# router bgp 64512
Router (config-bgp)#
```

コマンド書式

router bgp <自 AS 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
自 AS 番号	自装置側の AS 番号を指定します。	1～65535	省略不可

この設定を行わない場合

BGP を使用できません。

設定モード

基本設定モード

AS 番号

Autonomous System(自律システム)の番号のことです。

現在のインターネットを含めた TCP/IP のネットワークシステムは、AS が、互いに相互接続して、大規模なネットワークを形成しています。AS を識別するためには、AS 番号があり、1～65535 の範囲で割り振られています。このうち、1～64511 はグローバル AS 番号と呼ばれ、IANA(Internet Assigned Numbers Authority:IP アドレスやドメイン名等の割り当てを司る組織)からプロバイダ等で使用するよう予約されています。それに対し 64512～65535 はプライベート AS 番号と呼ばれ、IP-VPN 網やインターネットに接続する場合に使用する AS 番号とされています。
現在の IP-VPN サービスでは、ユーザ側のネットワークを BGP で受け渡す方法がとられています。
IP-VPN サービスを契約し、BGP での経路制御を要望すると、IP-VPN サービスより AS 番号が割り当てられます(通常はプライベート AS 番号)。その AS 番号を利用して、IP-VPN サービスの PE (Provider Edge)と接続し、IP-VPN を利用したダイナミックルーティングを実現しています。

アドレスファミリー設定モード

address-family ipv6 unicast

IPv6 アドレス交換を行うためのアドレスファミリー設定モードに移行します。
router bgp <AS 番号> の設定がない場合は、本設定を行なっても BGP は使用できません。

設定例 1　アドレスファミリー設定モードに移行する

```
Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)#
```

コマンド書式

```
address-family ipv6 unicast
```

パラメータ

パラメータはありません。

この設定を行わない場合

BGP で IPv6 ユニキャストの経路交換を行いません。

設定モード

基本設定モード

RIPng サービス設定モード

router ripng

RIPng サービス設定モードへ移行します。
RIPng の各種設定を行ないます。

設定例 1　RIPng サービス設定モードに移行する

```
Router(config)# router ripng
Router(config-ripng)#
```

コマンド書式

```
router ripng
```

パラメータ

パラメータはありません。

この設定を行わない場合

RIPng を使用できません。

設定モード

基本設定モード

Route-MAP 設定モード

route-map

Route-map 設定モードに移行します。
Route-MAP とは、ルート情報の送受信条件や送受信先を詳細に規定しておくものです。
ルート情報の送受信条件や送受信対象を"match "で特定し、送受信するルート情報を"set "で編集します。

設定例 1　Route-map 名=map1 の Route-map 設定モードに移行する

```
Router(config)# route-map map1 permit 1
Router(config-rmap map1 permit 1)#
```

コマンド書式

route-map 〈Route-map 名〉〈属性〉〈シーケンス番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Route-map 名	各種ルーティングプロトコルで、Route-map を指定する場合の名称になります。	–	省略不可
属性	このルートマップが許可する属性(permit)なのか、許可しない属性(deny)なのかを指定します。	permit deny	省略不可
シーケンス番号	同じルートマップ名で、複数の操作を行なう場合に、複数の属性を指定します。 ここにつける番号が、シーケンス番号です。	1～65535	省略不可

この設定を行わない場合

詳細な経路の制御を使用できない場合があります。

Route-map 詳細

Route-map の詳細について説明します。
Route-map は、ルーティングプロトコルの、各種パラメータの操作・経路情報のフィルタリングのために使用します。

例 1　BGP で広告する場合は、メトリック（MED 値）を 5 としたい

本装置では、何も指定しない場合は MED のアトリビュートを付加せずに BGP のアップデート情報を通知しますが、Route-map を利用することにより、MED アトリビュートをつけて BGP のアップデートを通知することができます。

設定モード

基本設定モード

DHCP サーバ設定モード

ip dhcp pool

DHCP サーバ設定モードに移行します。
本装置を DHCP サーバとして使用する場合には設定が必要です。

DHCP サーバ機能と、DHCP リレーエージェント機能は共存できません。両方の設定がされている場合は、DHCP リレーエージェント機能が採用されます。

設定例　LAN インタフェースで DHCP サーバ機能を使用するために、DHCP サーバ設定モードに移行する

```
Router(config)#ip dhcp pool lan 1
Router(config-dhcp-pool)#
```

コマンド書式

ip dhcp pool 〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	DHCP サーバ機能を使用するインタフェースを指定します。	lan 1 ewan 1～2 vlanif 1～150	省略不可

この設定を行わない場合

DHCP サーバ機能を使用できません。

DHCP サーバ機能とは？

DHCP サーバ機能とは、DHCP(Dynamic Host Configuration Protocol)を使用して、LAN 上の端末(PC)に IP アドレスなどの情報を割り当てる機能です。
DHCP サーバ機能では、以下の情報を通知することができます。
・IP アドレス／サブネットマスク
・DNS サーバの IP アドレス
・デフォルトゲートウェイの IP アドレス
・ドメイン名
DHCP リレーエージェント機能もサポートしています。DHCP リレーエージェント機能は、自身がサーバになるのではなく、外部の DHCP サーバに問い合わせしなおす機能です。双方の設定がされている場合、DHCP リレーエージェント機能が有効になります。

設定モード

基本設定モード

IPv6 アドレスプール設定モード

address-pool ipv6

IPv6 のアドレスプールを指定するために、IPv6 アドレスプール設定モードに移行します。
複数設定がある場合は、プール名で sort して、一番先頭のアドレスプールのみ有効になります。

設定例 1　IPv6 アドレスプール設定モードに移行する

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)#
```

コマンド書式

address-pool ipv6 <アドレスプール名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスプール名	アドレスプール名称を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

IPv6 アドレスプールの設定が行えません。

設定モード

基本設定モード

DHCPv6 クライアントプロファイル設定モード

ipv6 dhcp client-profile

DHCPv6 クライアントとして動作する際の各種パラメータの設定を行う、DHCPv6 クライアントプロファイル設定モードに移行するためのコマンドです。

設定例 1　DHCPv6 クライアントプロファイル設定モードに移行する

```
Router(config)#ipv6 dhcp client-profile dhcpv6
Router(config-ipv6-dhcp-client-prof)#
```

コマンド書式

ipv6 dhcp client-profile <クライアントプロファイル名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クライアントプロファイル名	設定を行う DHCPv6 クライアントプロファイル名を指定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

DHCPv6 クライアントを使用することができません。

設定モード

基本設定モード

key-chain モード

key chain

RIP2 の認証を有効にするための key-chain モードに移行します。
key-chain の設定は、キー名称を指定して行ないます。key-chain モードで、キーの情報を設定し、各インタフェースの RIP2 に関する設定で、使用するキー名称を指定します。

```
Router(config)# key chain key1
Router(config-keychain)#
```

キー名称

設定例 1　キー名称が"key1"である key-chain モードに移行する

```
Router(config)# key chain key1
Router(config-keychain)#
```

コマンド書式

key chain <キー名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キー名称	RIP2 で参照するキー(パスワード)の名称インタフェース設定モードで参照する名称なので、わかりやすい名前にしてください。	-	省略不可

RIP2 の認証について

RIP2 では、認証キーによる認証を行い、信用できるルータからのルーティング情報であるかどうかを制御することができます。
この認証キーが異なる RIP2 の情報は、ルーティングテーブルに登録しません。

実際の RIP2 に付加される認証の情報には、以下の 2 種類があります。
・simple password （設定されたテキストの情報）
・MD5 digest （設定されたテキストから MD5 で計算されたデータ）
本装置で、RIP2 の認証を使用する場合は、RIP2 を使用するインタフェースのインタフェース設定モードの"ip rip authentication"コマンドで、key-chain で設定するキー名称を指定する形で設定します。

```
Router(config-if lan 1)#ip rip authentication key-chain key1
```

キー名称

設定モード

基本設定モード

イベントクラス設定モード

event-class

イベントクラス設定モードに移行します。

設定例１　イベントクラス設定モードに移行する

```
Router(config)#event-class 1
Router(config-event-class 1)
```

コマンド書式

event-class〈イベントクラス番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
イベントクラス番号	イベントクラス番号を指定します。	1～2000	省略不可

設定モード

基本設定モード

イベントアクション設定モード

event-action

イベントアクション設定モードに移行します。

設定例１　イベントアクション設定モードに移行する

```
Router(config)#event-action 1
Router(config-event-action 1)
```

コマンド書式

event-action 〈イベントアクション番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
イベント アクション番号	イベントアクション番号を指定します。	1～2000	省略不可

設定モード

基本設定モード

イベントマップ設定モード

event-map

イベントマップ設定モードに移行します。

設定例１　イベントマップ設定モードに移行する

```
Router(config)#event-map
Router(config-event-map)#
```

コマンド書式

event-map

パラメータ

パラメータはありません。

設定モード

基本設定モード

ICMP クラス設定モード

icmp-class

ICMP クラス設定モードに移行します。

設定例１　ICMP クラス設定モードに移行する

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)#
```

コマンド書式

icmp-class <ICMP クラス番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ICMP クラス番号	ICMP クラス番号を指定します。	1～2000	省略不可

設定モード

基本設定モード

Watch クラス設定モード

watch-class

Watch クラス設定モードに移行します。

設定例１　Watch クラス設定モードに移行する

```
Router(config)#watch-class 1
Router(config-watch-class 1)#
```

コマンド書式

watch-class <Watch クラス番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Watch クラス番号	Watch クラス番号を指定します。	1～16	省略不可

設定モード

基本設定モード

クラスマップ設定モード

class-map

クラスマップ設定モードに移行し、トラフィックを分類するクラシファイアを定義します。
クラスマップ設定モードでは、match ip もしくは、match ipv6 コマンドによってトラフィックの分類条件が設定されます。
複数の条件が設定された場合、match-any の有無によって、複数の条件が OR 条件となるか、AND 条件となるかが指定されます。
IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合は、指定された条件は無視されるのではなく、不成立と判定されます。

設定例１　クラスマップ設定モードへ移行する

```
Router(config)#class-map video-class
Router(config-class-map)#
```

コマンド書式

class-map〈クラスマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クラスマップ名	クラスマップ名称を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップ名によるトラフィックの分類を行いません。

設定モード

基本設定モード

アクションマップ設定モード

action-map

アクションマップ設定モードに移行し、トラフィックに対するアクションを定義します。
実行場所によってサポートされないアクションや、IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合、指定されたアクションは無視されます。

設定例１　アクションマップ設定モードへ移行する

```
Router(config)#action-map stream-action
Router(config-action-map)#
```

コマンド書式

action-map 〈アクションマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクションマップ名	アクションマップ名を設定します	16 文字以内の文字列	省略不可

この設定を行わない場合

アクションは定義されません。

設定モード

基本設定モード

ポリシーマップ設定モード

policy-map

ポリシーマップ設定モードに移行し、クラスマップによって分類したトラフィックに対して、どのような制御を行なうかを定義します。
ここで指定したポリシーマップを有効にするには、各インタフェース設定モードで、"service-policy input/output"コマンドで登録します。
また、自局送信をポリシールーティングする場合は、"service-policy local"コマンドで登録します。

設定例１　ポリシーマップ設定モードへ移行する

```
Router(config)#policy-map stream-service
Router(config-policy-map)#
```

コマンド書式

policy-map <policy-map-name>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
policy-map-name	policy-map-name を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

ポリシーマップの設定を行うことができません。

設定モード

基本設定モード

IPsec インタフェース設定モード

interface ipsecif

IPsec インタフェース設定モードに移行します。

設定例 1　IPsec インタフェース設定モードに移行します

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#
```

コマンド書式

interface ipsecif < IPsec インタフェース番号 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPsec インタフェース番号	IPsec インタフェース番号を指定します。	1～2000	省略不可

設定モード

基本設定モード

VLAN インタフェース設定モード

interface vlanif

VLAN インタフェースを登録するために、VLAN インタフェース設定モードに移行します。
VLAN インタフェースでは、属するブリッジグループや、使用する VLAN-TAG 値等の設定を行います。

設定例 1　VLAN インタフェース設定モードへ移行する

```
Router(config)#interface vlanif 1
Router(config-if vlanif 1)
```

コマンド書式

interface vlanif <VLAN インタフェース番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VLAN インタフェース番号	VLAN インタフェース番号を指定します。	1～150	省略不可

設定モード

基本設定モード

トンネルインタフェース設定モード

interface tunnel

トンネルインタフェース設定モードに移行します。
トンネルインタフェースモードで設定できるコマンドについては、こちらを参照してください。

設定例１　トンネルインタフェース設定モードに移行する

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#
```

コマンド書式

interface tunnel〈トンネルインタフェース番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
トンネルインタフェース番号	トンネルインタフェース番号を指定します。	1～2000	省略不可

設定モード

基本設定モード

電子証明書（自身の ID）設定モード

crypto ca identity

証明書のリクエストを作成する上で、自身の情報を設定する必要があります。
本コマンドでは、証明書のリクエストを作成する上での、自身の情報を設定するために、電子証明書（自身の ID）設定モードに移行します。

IKEv1/IKEv2 共通コマンド

設定例 1　電子証明書（自身の ID）設定モードに移行する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#
```

コマンド書式

```
crypto ca identity
```

パラメータ

パラメータはありません。

設定モード

基本設定モード

グループ鍵 IPsec 設定モード

crypto ipsec group-security policy

マルチポイント SA サーバ機能に関する設定をおこなうために、グループ鍵 IPsec 設定モードに移行します。

設定例 1　グループ鍵 IPsec 設定モードへ移行する

```
Router(config)#crypto ipsec group-security policy MPSA1
Router(config-gr-sec)#
```

コマンド書式

crypto ipsec group-security policy <マルチポイント SA ポリシー名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
マルチポイント SA ポリシー名称	マルチポイント SA ポリシー名称を設定します。	最大 64 文字の英数字	省略不可

この設定を行わない場合

マルチポイント SA サーバ機能を使用できません。

設定モード

基本設定モード

IKEv2 ポリシー設定モード

crypto ikev2 policy

Internet Key Exchange ポリシー(VPN ピアとの IKE SA 用のポリシー)のエントリを設定するために、IKEv2 ポリシー設定モードに移行します。

設定例１　IKEv2 ポリシー（ポリシー番号：１）設定モードに移行します

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#
```

コマンド書式

crypto ikev2 policy <policy 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
policy 番号	IKEv2 ポリシーの番号を指定します。	1～2000	省略不可

設定モード

基本設定モード

IKE ポリシー設定モード

crypto isakmp policy

Internet Key Exchange ポリシー(VPN ピアとのフェーズ 1 ネゴシエーション用のポリシー)のエントリを設定するために、IKE ポリシー設定モードに移行します。

設定例１　IKE ポリシー（ポリシー番号：１）設定モードに移行する

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#
```

コマンド書式

crypto isakmp policy <policy 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
policy 番号	IKE ポリシーの番号を指定します。 この数字の小さいポリシーを優先的に使用します。	1～2000	省略不可

設定モード

基本設定モード

VPN セレクタ設定モード

crypto map

VPN ピアとのセレクタ情報のエントリを設定する為に、VPN セレクタ設定モードに移行します。
設定の際は、セレクタ名称、シーケンス番号を指定します。

IKEv1/IKEv2 共通コマンド

設定例 1　VPN セレクタ設定モード（セレクタ名称：Tokyo）に移行する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#
```

コマンド書式

crypto map〈セレクタ名称〉〈シーケンス番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セレクタ名称	VPN セレクタの名称を指定します。 PPPoE インタフェース設定モード/EWAN インタフェース設定モード等で、適用する VPN セレクタを指定しますので、わかりやすい名称にしてください。	最大 16 文字の英数字	省略不可
シーケンス番号	シーケンス番号を指定します。 既に使用したシーケンス番号と同じ番号を重複して使用すると以前設定した内容を上書きします。	1～4000	省略不可

設定モード

基本設定モード

IPsec 各種設定モード

crypto security-association

IPsec 機能全般の、各種タイマ値等を設定するために、IPsec 各種設定モードに移行します。

IKEv1/IKEv2 共通コマンド

設定例 1　IPsec 各種設定モードに移行する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#
```

コマンド書式

crypto security-association

パラメータ

パラメータはありません。

設定モード

基本設定モード

IPsec ログモード

crypto ipsec-log

"SPI no match"、"block type discard"ログ出力の抑制および、vpnlog 詳細ログ出力を制御するために IPsec ログモードに移行します。

設定例 1　IPsec ログモードに移行する

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#
```

コマンド書式

```
crypto ipsec-log
```

パラメータ

パラメータはありません

設定モード

基本設定モード

Ethernet 設定モード

line

Ethernet インタフェースについて、速度/デュプレックス/SFP/MDI/MDI-X の設定を行なう Ethernet 設定モードに移行するためのコマンドです。

設定例 1　EWAN#1 ポートの設定を行なうモードに移行する

```
Router(config)# line ewan 1
Router(config line ewan 1)#
```

コマンド書式

line〈物理インタフェース〉

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
物理 インタフェース	設定を行なう物理インタフェースを選択します。		lan ewan 1 ewan 2	省略不可
	lan	LAN インタフェース (SW-HUB 8 ポート)		
	ewan 1	EWAN#1 ポート		
	ewan 2	EWAN#2 ポート		

設定モード

基本設定モード

L2TP-PPP テンプレート設定モード

l2tp-ppp-template

L2TP-PPP テンプレート設定モードに移行します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　L2TP-PPP テンプレート設定モードに移行する (L2TP-PPP テンプレート名：ppp-A)

```
Router(config)#l2tp-ppp-template ppp-A
Router(config-l2tp-ppp-tmp)#
```

コマンド書式

l2tp-ppp-template <L2TP-PPP テンプレート名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
L2TP-PPP テンプレート名	L2TP-PPP テンプレート名を指定します。	最大 16 文字の英数字	省略不可

設定モード

基本設定モード

L2TP プロファイル設定モード

l2tp profile

L2TP プロファイル設定モードへ移行します。

設定例　L2TP プロファイル設定モードへ移行する

```
Router(config)#l2tp profile 1
Router(config-l2tp-profile 1)#
```

コマンド書式

l2tp profile <L2TP プロファイル ID>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
L2TP プロファイル ID	L2TP プロファイル ID を指定します。 ここで指定した L2TP プロファイル ID は、L2TP Pseudowire 設定モードの tunnel mode l2tp で指定する番号に対応します。	1～2000	省略不可

この設定を行わない場合

L2TP 機能を使用できません。

設定モード

基本設定モード

L2TP Pseudowire 設定モード

l2tp pseudowire

L2TP Pseudowire 設定モードへ移行します。

設定例　L2TP Pseudowire 設定モードへ移行する

```
Router(config)#l2tp pseudowire 1
Router(config-l2tp-pseudowire 1)#
```

コマンド書式

l2tp pseudowire <L2TP Pseudowire ID>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
L2TP Pseudowire ID	L2TP Pseudowire ID を指定します。 ここで指定した L2TP Pseudowire ID は、トンネルインタフェース設定モードの tunnel mode l2tp で指定する番号に対応します。 ただし、複数の tunnel mode l2tpv3 から1つの L2TP Pseudowire ID への紐付けはできません。	1～2000	省略不可

この設定を行わない場合

L2TP 機能を使用できません。

設定モード

基本設定モード

CLIENT-データベース設定モード

aaa local group

認証(L2TP/PPP による認証) を行うデータベースを登録するために、CLIENT-データベース設定モードに移行します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　CLIENT- データベース設定モードに移行する(認証グループ名 : local-A)

```
Router(config)#aaa local group local-A
Router(config-lg-user)#
```

コマンド書式

aaa local group <認証グループ名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
認証グループ名	認証グループ名を指定します。	最大 16 文字の英数字	省略不可

設定モード

基本設定モード

HTTP クライアント設定モード

http-client

HTTP クライアント設定モードに移行するためのコマンドです。

設定例１　HTTP クライアント設定モードに移行する

```
Router(config)# http-client 1
Router(http-client 1)#
```

コマンド書式

http-client 〈HTTP クライアント番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
HTTP クライアント番号	設定を行なう HTTP クライアント番号を選択します。	1～16	省略不可

設定モード

基本設定モード

Radius サーバ設定モード

aaa group server radius エラー! ブックマークが定義されていません。

Radius サーバ設定モードに移行するためのコマンドです。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　Radius サーバ設定モードに移行する

```
Router(config)#aaa group server radius Radius-A
Router(config-sg-radius)#
```

コマンド書式

aaa group server radius <Radius サーバグループ名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Radius サーバグループ名	Radius サーバグループの名称を指定します。	最大 16 文字の英数字	省略不可

設定モード

基本設定モード

sFlow profile 設定モード

sflow profile エラー! ブックマークが定義されていません。

sFlow Agent の設定をするために、sFlow profile 設定モードに移行します。

refresh コマンド後に有効になるコマンドです。

V01.03(00)以降サポート

設定例 1　sflow profile サーバ設定モードに移行する

```
Router(config)#sflow profile 1
Router(config-sflow-prof)#
```

コマンド書式

sflow profile <sflow profile 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
sflow profile 番号	sflow profile 番号を指定します。	1～1	省略不可

設定モード

基本設定モード

PPPoE 機能

PPPoE を使用するための設定

pppoe account

プロバイダから指定されたユーザ ID とパスワードを設定します。

設定例 1　ユーザ ID に f2200@xxxxx.ne.jp, パスワードに f2200pass を設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe account f2200@xxxxx.ne.jp f2200pass
```

コマンド書式

pppoe account <ユーザ ID> <パスワード> [{secret | private}[encrypted]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ユーザ ID	プロバイダから指定された、ユーザ ID を設定します。	127 文字以内の文字列	省略不可
パスワード	プロバイダから指定された、パスワードを設定します。	32 文字以内の文字列	省略不可
secret | private	パスワードを暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。※1 secret：暗号化する際に共有暗号鍵を使用する private：暗号化する際に装置固有暗号鍵を使用する	secret private	パスワードを暗号化しません
encrypted	パスワードを暗号化処理するかどうかを設定します。このオプションを付加することにより、パスワードは暗号化済みと判定されます。※2 secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。	encrypted	パスワードを暗号化データとして扱いません

※1 このオプションは、設定するとすぐに有効となり、パスワードが暗号化されて表示され encrypted オプションが自動的に付加されます。
※2 パスワードが既に暗号化済みの場合は、このオプションを指定する必要があります。

この設定を行わない場合

プロバイダに接続することができません。

設定モード

PPPoE インタフェース設定モード

pppoe auth-accept

PPP の認証プロトコル(CHAP or PAP)を指定します。
通常は、プロバイダとのネゴシエーションにより決定します。プロバイダとのネゴシエーションの結果に従う場合は"auto"を指定します。
プロバイダから、認証プロトコルの指示がある場合は、認証プロトコルを指定してください。

設定例１　PPP の認証プロトコルを自動（ネゴシエーションに従う）とする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe auth-accept auto
```

設定例２　PPP の認証プロトコルを PAP 固定とする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe auth-accept pap
```

コマンド書式

pppoe auth-accept 〈認証プロトコル〉

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
認証プロトコル	認証プロトコル(CHAP or PAP)を設定します。		auto chap pap	省略不可
	auto	CHAP または PAP を自動で選択します。		
	chap	CHAP 固定とします。		
	pap	PAP 固定とします。		

この設定を行わない場合

auto で動作します。

設定モード

PPPoE インタフェース設定モード

pppoe interface

PPPoE インタフェースがパケット送受信で使用する物理インタフェースを指定します。
本装置は、24 の PPPoE インタフェースを持つことができます。

設定例 1　PPPoE 6 を EWAN 2 で使用する

```
Router(config)#interface pppoe 6
Router(config-if pppoe 1)#pppoe interface ewan 2
```

コマンド書式

pppoe interface〈物理インタフェース〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
物理 インタフェース	PPPoE インタフェースが使用する物理インタフェースを指定します。 none を指定した PPPoE インタフェースは使用できません。	lan 1 ewan 1～2 vlanif 1～150 none	省略不可

この設定を行わない場合

pppoe 1～4 は ewan 1、pppoe 5 は ewan 2 が指定されます。
pppoe 6～24 は使用できません。

設定モード

PPPoE インタフェース設定モード

pppoe ncp

PPPoE 接続時に使用する NCP を設定します。ipcp のときは IPCP を、ipv6cp のときは IPv6CP を、both のときはその両方を使用します。

設定例 1　NCP に IPCP のみを接続する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe ncp ipcp
```

コマンド書式

pppoe ncp〈中継プロトコル〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
中継プロトコル	PPP 上を中継するプロトコル(IPv4, IPv6)を指定します。 ipcp　IPv4 を中継します。 ipv6cp　IPv6 を中継します。 both　IPv4、IPv6 の双方を中継します。	ipcp ipv6cp both	省略不可

この設定を行わない場合

IPCP を使用します。

NCP とは？

NCP(Network Control Protocol)とは、PPP のオプションで、PPP を接続する両者で通信するプロトコルを規定するためにネゴシエーションするプロトコルです。
PPP は、まず LCP(Link Control Protocol)により、この PPP をどのように使用するかのネゴシエーションを行い、LCP のネゴシエーションが終了した後、どのようなプロトコルを通すかのネゴシエーション(NCP)を行ないます。

IPv4 を通すために行なう NCP を IPCP、IPv6 を通すために行なう NCP を IPv6CP といいます。
例えば、PPP を確立する相手に対して、IPCP のリクエストを送信し、確立可能のレスポンス(ACK)を受信した場合に、PPP 上で IPv4 の通信が可能になります。
ここでの設定は、PPP 上で IPv4/IPv6 のどちら(あるいは両方)の通信を行ないたいかを設定します。

設定モード

PPPoE インタフェース設定モード

pppoe server

PPPoE 接続相手の名称を設定します。この設定は、わかりやすい名称を設定してください。
PPPoE を使用する場合は、この設定が必須になります。

設定例１　接続する相手名称を”A-Provider”に設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe server A-Provider
```

コマンド書式

pppoe server〈接続相手名称〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
接続相手名称	PPPoE 接続相手の名称を設定します。	20 文字以内の文字列	省略不可

この設定を行わない場合

PPPoE が使用できません。

この設定は何に使われるのか？

接続相手の設定を見分けるための名称です。プロバイダに接続するためのパラメータではありません。本装置では、同時に 24 セッションの PPPoE を設定できますので、わかりやすいように名称をつける目的の設定です。

設定モード

PPPoE インタフェース設定モード

pppoe service

サービス名称を設定します。通常は設定の必要はありません。
プロバイダより、サービス名を指定された場合のみ設定が必要です。

設定例 1　サービス名称として xxxxx. ne. jp を設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe service xxxxx.ne.jp
```

コマンド書式

pppoe service〈サービス名称〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
サービス名称	サービス名称を設定します。	20 文字以内の文字列	省略不可

この設定を行わない場合

設定なしとなります。

設定モード

PPPoE インタフェース設定モード

pppoe type

PPP の IP 制御プロトコルで IP アドレスのリクエストをするかしないかを設定します。
端末型接続の場合は host と設定し、IP8/IP16 のように LAN 型接続の場合は lan と設定します。

設定例 1　PPPoE を LAN 型で接続する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe type lan
```

コマンド書式

pppoe type〈接続タイプ〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
接続タイプ	PPPoE の接続タイプを指定します。	host lan	省略不可

この設定を行わない場合

host として動作します。

「端末型」「LAN 型」とは？

「端末型」は、IP アドレスが1つだけ割り当てられる形態、「LAN 型」は、IP アドレスが複数割り当てられる形態を表します。

設定モード

PPPoE インタフェース設定モード

ip address

PPPoE インタフェースの IP アドレスとサブネットマスクを指定します。
PPP で、アドレスを割り当てられるケースでは、設定の必要はありません。プロバイダより、設定するアドレスを指定された場合に設定してください。

設定例 1　PPPoE 1 の IP アドレスを 158.xxx.xxx.1 に設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip address 158.xxx.xxx.1
```

コマンド書式

ip address <IP アドレス> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	インタフェースに割り当てる IP アドレスを設定します。	IPv4 アドレス形式	省略不可

設定モード

PPPoE インタフェース設定モード

ip name-server

プロバイダから書面で通知されている場合に、プロバイダから通知された DNS サーバの IP アドレスを入力します。書面での通知がない場合は、設定しなくてかまいません。

設定例 1　プロバイダから DNS サーバの IP アドレスとして、プライマリ DNS サーバ：158.xxx.xxx.1、セカンダリ DNS サーバ：158.xxx.xxx.2 が通知された

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip name-server 158.xxx.xxx.1 158.xxx.xxx.2
```

コマンド書式

ip name-server <DNS アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DNS アドレス	プロバイダから通知された DNS サーバのアドレスを設定します。	IPv4 アドレス形式	省略不可

※ DNS アドレスの優先度は、入力した順に2つまで有効になります。すでに、2つ入力されている状態で3つ目以降を入力しても設定上無効となります。

この設定を行わない場合

PPP で学習できない場合は、リゾルバ・簡易 DNS 機能を使用できません。ただし、基本設定モードの ip name-server, proxydns default name-server コマンドが設定されている場合は、そちらの情報を使用します。

また、PPP で学習できた場合は、学習した DNS サーバの IP アドレスを利用します。

DNS サーバとは？

DNS は Domain Name System の略で、ホスト名から IP アドレス（またはその逆）を探し出すシステムのことです。

このシステムのために、ホスト名と IP アドレスの組み合わせデータベースが存在し、そのデータベースをもつホストのことを、DNS サーバといいます。

DNS サーバは、世界中のホストと IP アドレスの組み合わせデータベースを持っているわけではなく、自分の属するドメインの組み合わせのみを保有し、わからないホスト名のリクエストを受けた場合は、他の DNS サーバに問い合わせるという仕組みを持っています。

設定モード

PPPoE インタフェース設定モード

ip mtu

PPPoE インタフェースの MTU 長を指定します。
フレッツ ADSL または B フレッツを介して PPPoE を接続する場合は、MTU 長を 1454byte より大きくすると、通信できなくなる場合がありますので注意してください。

refresh コマンド後に有効になるコマンドです。

設定例 1　PPPoE1 の MTU 長を 1400byte にする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip mtu 1400
```

コマンド書式

ip mtu <MTU 長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MTU 長	MTU 長を指定します。	578～1492	省略不可

この設定を行わない場合

PPPoE インタフェースでは 1454byte となります。通常は変更の必要はありません。

MTU 長とは？

MTU とは（Max Transfer Unit）の略で、MTU 長とは、通常、1 パケットで運ぶことができる IP パケット（IP ヘッダ＋IP ペイロード）の長さをいいます。
フレッツ ADSL、B フレッツと接続する場合、必ず経由する IP ネットワークの MTU 値が 1454byte になっています。したがって PPPoE をフレッツ ADSL や B フレッツを介して接続する場合は、この設定を 1454 以下に設定してください。

設定モード

PPPoE インタフェース設定モード

ipv6 mtu

PPPoE インタフェースの MTU 長を指定します。
フレッツ ADSL または B フレッツを介して PPPoE を接続する場合は、MTU 長を 1454byte より大きくすると、通信できなくなる場合がありますので注意してください。

refresh コマンド後に有効になるコマンドです。

設定例 1　PPPoE1 の MTU 長を 1400byte にする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ipv6 mtu 1400
```

コマンド書式

ipv6 mtu <MTU 長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MTU 長	MTU 長を指定します。	1280～1492	省略不可

この設定を行わない場合

PPPoE インタフェースでは 1454byte となります。通常は変更の必要はありません。

MTU 長とは？

MTU とは（Max Transfer Unit）の略で、MTU 長とは、通常、1 パケットで運ぶことができる IP パケット（IP ヘッダ＋IP ペイロード）の長さをいいます。
フレッツ ADSL、B フレッツと接続する場合、必ず経由する IP ネットワークの MTU 値が 1454byte になっています。したがって PPPoE をフレッツ ADSL や B フレッツを介して接続する場合は、この設定を 1454 以下に設定してください。

設定モード

PPPoE インタフェース設定モード

mss

インタフェースの MSS 値を指定します。
本装置では、TCP ヘッダオプションに含まれる MSS 値を適切な値に書き換えることができます。
パケットに書かれている値と設定値を比較して小さい方の値にします。

refresh コマンド後に有効になるコマンドです。

設定例 1　LAN の MSS 値を 1300byte にする

```
Router(config)#mss lan 1 1300
```

コマンド書式

mss {<インタフェース名>|ipsec}　<MSS 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	インタフェースを指定します。	lan 1 ewan 1～2 pppoe 1～24 ipsecif 1～2000 vlanif 1～150 tunnel 1～2000 usb-ethernet 1～2	省略不可
ipsec	ポリシーベース IPsec の場合に指定します。	ipsec	省略不可
MSS 値	MSS 値を指定します。 off を指定した場合は、MSS 値を変更しません。 ipseif の場合は、VPN セレクタの MSS 値を指定します。※1	216※3～1460※2 off	省略不可

※1 IPsec interface 以外に提供される VPN セレクタの MSS 値の指定となります。
※2 次の設定値の上限は、ipsec 1420、tunnel 1440、usb-ethernet 1440、pppoe 1452 となります。
※3 設定値の下限の 216 は V01.04(00)以降サポート

この設定を行わない場合

各インタフェースからパケットを送出する際に、下記の値とパケットに書かれている値を比較して小さい方の値にします。通常は変更の必要はありません。

LAN interface：MTU 長 −40
EWAN interface：MTU 長 −40
PPPoE interface：MTU 長 −40
IPsec interface：MTU 長 −40
IPsec VPN selector：（送信 IF の MTU ）−113
Tunnel interface：MTU 長 −40
VLANIF interface：MTU 長 −40
USB Ethernet interface：MTU 長 −40

MSS 長とは？

MSS (Maximum Segment Size)とは、TCP で一度に伝送できるデータの最大量。
最大セグメントサイズ。

設定モード

基本設定モード

DHCP クライアント機能

DHCP クライアントとして使用するための設定

dhcp-client retries infinitely

本設定により、DHCP クライアント動作においてアドレスが取得できるまでアドレス取得動作を継続します。

refresh コマンド後に有効になるコマンドです。

設定例 1　アドレスが取得できるまで取得動作を継続する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#dhcp-client retries infinitely
```

コマンド書式

```
dhcp-client retries infinitely
```

パラメータ

パラメータはありません。

この設定を行わない場合

DHCPDISCOVER を 2 回リトライしても DHCPOFFER が得られない場合、アドレス取得動作を打ち切ります。

設定モード

EWAN インタフェース設定モード
USB Ethernet インタフェース設定モード

ip address dhcp

EWAN、USB Ethernet インタフェースで、DHCP クライアント機能を使用する場合に指定します。ADSL モデムで PPP を終端し EWAN 側に DHCP でアドレスを通知するようなケースや、CATV インターネット等 DHCP でアドレスを割り当てるプロバイダに契約している場合等は、このモードで使用することがあります。加入しているインターネットサービスに確認してください。

このモードの場合、DHCP サーバから「クライアント ID」もしくは「ホスト名」の指定を指示される場合があります。この場合は、コマンドのオプションとして指示された内容を設定してください。

設定例 1　EWAN インタフェースで DHCP クライアント機能を使用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip address dhcp
```

コマンド書式

```
ip address dhcp { client-id [{ ascii | hex} < クライアント ID >] [[type < タ
                イプ >] [hostname < ホスト名 >] | [hostname < ホスト名 >] ]
                |hostname< ホスト名 >}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
{ ascii | hex} クライアント ID	クライアント ID を ASCII または、hex で指定します。 ascii：最大 63 文字(ASCII) hex：最大 126 桁(16 進数)	ascii hex	クライアント ID を付けない
タイプ	クライアント ID のタイプを指定します。	0～255	クライアント ID が ASCII の場合：0 クライアント ID が hex の場合：1
ホスト名	ホスト名を指定します。	最大 63 文字	ホスト名を付けない

この設定を行わない場合

DHCP クライアント機能を使用できません。

DHCP クライアント機能とは？

DHCP プロトコルを利用して、IP アドレス等の情報を割り当ててもらい、その内容にしたがって IP 通信を行なう機能を、DHCP クライアント機能といいます。

本装置は、LAN インタフェースで DHCP サーバ機能または DHCP リレーエージェント機能が使用でき、EWAN、USB Ethernet インタフェースで DHCP クライアント機能を使用できます。

設定モード

EWAN インタフェース設定モード
USB Ethernet インタフェース設定モード

ip mtu

EWAN、USB Ethernet インタフェースの MTU 長を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　EWAN の MTU 長を 1400byte にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip mtu 1400
```

コマンド書式

ip mtu <MTU 長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MTU 長	MTU 長を指定します。	256～1500	省略不可

この設定を行わない場合

各インタフェースにより以下のようになります。通常は変更の必要はありません。

EWAN：1454
USB Ethernet：1500

MTU 長とは？

MTU とは（Max Transfer Unit）の略で、MTU 長とは、通常、1 パケットで運ぶことができる IP パケット（IP ヘッダ＋IP ペイロード）の長さをいいます。
標準的な Ethernet では、MTU 長は 1500byte です。

設定モード

EWAN インタフェース設定モード
USB Ethernet インタフェース設定モード

ipv6 mtu

EWAN インタフェースの MTU 長を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　EWAN の MTU 長を 1400byte にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 mtu 1400
```

コマンド書式

ipv6 mtu <MTU 長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MTU 長	MTU 長を指定します。	1280～1500	省略不可

この設定を行わない場合

1454byte となります。通常は変更の必要はありません。

MTU 長とは？

MTU とは（Max Transfer Unit）の略で、MTU 長とは、通常、1 パケットで運ぶことができる IP パケット（IP ヘッダ＋IP ペイロード）の長さをいいます。
標準的な Ethernet では、MTU 長は 1500byte です。

設定モード

EWAN インタフェース設定モード

DHCPv6 機能

DHCPv6 サーバ機能を使用するための設定

address-pool

アドレスプールの設定を行います。

refresh コマンド後に有効になるコマンドです。

設定例 1　アドレスプールを有効にする

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)# address-pool enable
```

コマンド書式

address-pool 〈アドレスプール設定〉

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>アドレスプール設定</td><td>アドレスプールを有効にするか無効にするかを指定します。<table><tr><td>enable</td><td>アドレスプールを有効とする。</td></tr><tr><td>disable</td><td>アドレスプールを無効とする。
アドレスの払い出しは行わないが、プールの登録は可能です。</td></tr></table></td><td>enable
disable</td><td>省略不可</td></tr>
</table>

※ enable から disable に変更した場合は、すでに払い出しているアドレスを回収します。

この設定を行わない場合

アドレスプールは使用不可となります。

設定モード

IPv6 アドレスプール設定モード

allocate address

払い出しアドレスブロックを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　払い出しアドレスブロックを 2001:db8::1/32 とする

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)# allocate address 2001:db8::1/32
```

コマンド書式

allocate address〈アドレスブロック〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスブロック	払い出しアドレスブロックを指定します。	IPv6 アドレス形式	省略不可

この設定を行わない場合

固定払い出しブロックはありません。

設定モード

IPv6 アドレスプール設定モード

allocate prefix-length

アドレスを払い出す際のプレフィックス長を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　プレフィックス長を 64 とする

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)# allocate prefix-length 64
```

コマンド書式

allocate prefix-length <プレフィックス長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プレフィックス長	アドレスを払い出す際のプレフィックス長を指定します。	1～128	省略不可

この設定を行わない場合

アドレスの払い出しを行いません。
ただし、プールの登録は可能です。

設定モード

IPv6 アドレスプール設定モード

allocate retention-time

アドレスの払い出しを行った後、そのアドレスが払い戻された場合の、該当プレフィックスの払い出し抑制期間を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　アドレス払い出し抑制期間を 2400 秒とする

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)# allocate retention-time
```

コマンド書式

allocate retention-time 〈抑制期間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
抑制期間	アドレスの払い出しを行った後、そのアドレスが払い戻された場合の、該当プレフィックスの払い出し抑制期間(単位:秒)を指定します。	0～2147483647	省略不可

この設定を行わない場合

アドレス払い出し抑制期間は、3600 秒になります。

設定モード

IPv6 アドレスプール設定モード

description

アドレスプールの Description を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　Description を prefix-list_ipv6 とする

```
Router(config)#address-pool ipv6 1
Router(config-if dialer 1)#description prefix-list_ipv6
```

コマンド書式

description <文字列>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
文字列	コメントを入力します。	50 文字までの 半角英数字、記号	省略不可

設定モード

IPv6 アドレスプール設定モード

dns-server

ORO にて OPTION_DNS_SERVERS を要求された場合に通知する DNS サーバアドレスを設定します。
::0/0 を指定した場合は、DHCPv6 を送信するインタフェースのリンクローカルアドレスを通知します。

refresh コマンド後に有効になるコマンドです。

設定例 1　DNS サーバアドレス 2001:db8::1 を登録する

```
Router(config)#ipv6 dhcp server-profile sprof
Router(config-ipv6-dhcp-server-prof)#dns-server 2001:db8::1
```

コマンド書式

dns-server 〈プライマリ DNS アドレス〉 ［セカンダリ DNS アドレス］

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プライマリ DNS アドレス	DHCP で通知するプライマリ DNS サーバの IP アドレス	IPv6 アドレス形式	省略不可
セカンダリ DNS アドレス	DHCP で通知するセカンダリ DNS サーバの IP アドレス	IPv6 アドレス形式	セカンダリ DNS を使用しない

この設定を行わない場合

OPTION_DNS_SERVERS を通知しません。

設定モード

DHCPv6 サーバプロファイル設定モード

dns-server forward dhcp-client

DHCPv6 クライアントで取得した DNS サーバの情報をリレーする場合に設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　EWAN 1 で取得した DNS サーバの情報をリレーする

```
Router(config)#ipv6 dhcp server-profile sprof
Router(config-ipv6-dhcp-server-prof)#dns-server forward dhcp-client ewan 1
```

コマンド書式

dns-server forward dhcp-client <インタフェース名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	DHCPv6 クライアント動作インタフェースを指定します。	lan 1 ewan 1～2 pppoe 1～24 vlanif 1～150	省略不可

この設定を行わない場合

DNS サーバの情報をリレーできません。

設定モード

DHCPv6 サーバプロファイル設定モード

domain-search-list fixed

OPTION_DOMAIN_LIST にて通知するドメイン名を設定します。
DHCPv6 クライアントからの要求がなくても、本コマンドが設定されている場合は、OPTION_DOMAIN_LIST を通知します。

refresh コマンド後に有効になるコマンドです。

設定例１　OPTION_DOMAIN_LIST にて通知するドメイン名を fitelnet.co.jp とする

```
Router(config)#ipv6 dhcp server-profile sprof
Router(config-ipv6-dhcp-server-prof)#domain-search-list fixed fitelnet.co.jp
```

コマンド書式

domain-search-list fixed〈ドメイン名〉[ドメイン名]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ドメイン名	OPTION_DOMAIN_LIST にて通知するドメイン名を指定します。 ドメイン名は、2つまで登録可能です。	63 文字以内の文字列	省略不可※

※ 2つ目は省略可能です。

この設定を行わない場合

OPTION_DOMAIN_LIST を通知しません。

設定モード

DHCPv6 サーバプロファイル設定モード

domain-search-list forward dhcp-client

DHCPv6 クライアントで取得した OPTION_DOMAIN_LIST の情報をリレーする場合に設定します。リレーできる情報は、最大 128 バイトになります。

refresh コマンド後に有効になるコマンドです。

設定例 1　情報を取得した DHCPv6 クライアント動作インタフェースを EWAN 1 とする

```
Router(config)#ipv6 dhcp server-profile sprof
Router(config-ipv6-dhcp-server-prof)#domain-search-list forward dhcp-client ewan 1
```

コマンド書式

domain-search-list forward dhcp-client <インタフェース名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	OPTION_DOMAIN_LIST の情報をリレーする場合の、情報を取得した DHCPv6 クライアント動作インタフェースを指定します。	lan 1～1 ewan 1～2 vlanif 1～150	省略不可

この設定を行わない場合

OPTION_DOMAIN_LIST を通知しません。

設定モード

DHCPv6 サーバプロファイル設定モード

ipv6 dhcp server

DHCPv6 サーバを動作させるインタフェースで、DHCPv6 サーバプロファイルを指定します。
DHCPv6 サーバプロファイルに関しては、ipv6 dhcp server-profile で設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　DHCPv6 サーバプロファイル：Profile1 を指定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 dhcp server Profile1
```

コマンド書式

ipv6 dhcp server〈サーバプロファイル名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
サーバプロファイル名	DHCPv6 サーバプロファイル名を指定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

DHCPv6 サーバ機能を使用できません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 dhcp server-profile

DHCPv6 サーバとして動作する際の各種パラメータの設定を行う、DHCPv6 サーバプロファイル設定モードに移行するためのコマンドです。

設定例 1　DHCPv6 サーバプロファイル設定モードに移行する

```
Router(config)#ipv6 dhcp server-profile sprof
Router(config-ipv6-dhcp-server-prof)#
```

コマンド書式

ipv6 dhcp server-profile <サーバプロファイル名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
サーバプロファイル名	設定を行う DHCPv6 サーバプロファイル名を指定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

DHCPv6 サーバを使用することができません。

設定モード

基本設定モード

logging enable

DHCPv6 クライアントからの要求を受信した際に、ログ(slog)を出力するかどうかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　DHCPv6 クライアントから要求を受信した際に slog を出力する

```
Router(config)#ipv6 dhcp server-profile sprof
Router(config-ipv6-dhcp-server-prof)#logging enable
```

コマンド書式

logging enable

パラメータ

パラメータはありません。

この設定を行わない場合

要求を受信してもログを出力しません。

設定モード

DHCPv6 サーバプロファイル設定モード

option hex

任意の DHCP オプションを通知する場合に設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　オプションコードを 100、オプションパラメータを 0x1234567890 とする

```
Router(config)#ipv6 dhcp server-profile sprof
Router(config-ipv6-dhcp-server-prof)#option 100 hex 0x1234567890
```

コマンド書式

option〈オプションコード〉hex〈オプションパラメータ〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
オプションコード	DHCP オプションコードを指定します。	1～254	省略不可
オプションパラメータ	オプションパラメータを 16 進数で指定します。	最大 127byte までの 16 進数	省略不可

※ 4 エントリ以上指定した場合は、オプションコードの小さい順に 4 エントリが有効になります。

この設定を行わない場合

他コマンドで設定したオプション以外は通知しません。

設定モード

DHCPv6 サーバプロファイル設定モード

option forward dhcp-client

DHCPv6 クライアントで取得した DHCP オプション情報をリレーする場合に設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　オプションコードを 100 として、EWAN1 で取得したオプション情報をリレーする

```
Router(config)#ipv6 dhcp server-profile sprof
Router(config-ipv6-dhcp-server-prof)#option 100 forward dhcp-client ewan1
```

コマンド書式

option 〈オプションコード〉 forward dhcp-client 〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
オプションコード	DHCP オプションコードを指定します。	1～254	省略不可
インタフェース名	DHCPv6 クライアント動作インタフェースを指定します。	lan 1 ewan 1～2 pppoe 1～24 vlanif 1～150	省略不可

※ 4 エントリ以上指定した場合は、オプションコードの小さい順に 4 エントリが有効になります。

この設定を行わない場合

DHCP オプション情報をリレーしません。

設定モード

DHCPv6 サーバプロファイル設定モード

pooled-route

アドレスプールに静的および動的に登録されたプレフィックス情報をあて先とする経路情報を登録します。

refresh コマンド後に有効になるコマンドです。

設定例 1　宛先プレフィックスを 2001:db8::1 とする

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)# pooled-route 2001:db8::1
```

コマンド書式

```
pooled-route {<宛先プレフィックス> | <インタフェース名※1>|
              connected <インタフェース名※2>} [メトリック値]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先プレフィックス	宛先プレフィックスを指定します。	IPv6 アドレス形式	省略不可
インタフェース名※1	宛先へ到達するためのインタフェースを指定します。	lan 1～1 ewan 1～2 pppoe 1～24 tunnel 1～2000 vlanif 1～150	省略不可
インタフェース名※2	宛先を IPsecIF、Null インタフェースの connected として扱う場合に指定します。	ipsecif 1～2000 null 0	省略不可
メトリック値	メトリック値を指定します。	1～255	210

この設定を行わない場合

経路登録を行いません。

設定モード

IPv6 アドレスプール設定モード

prefix-delegation address-pool

IA_PD オプションの要求があった場合に、プレフィックス情報を通知する場合に設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　アドレスプール名 XX から取得したプレフィックス情報を通知する

```
Router(config)#ipv6 dhcp server-profile sprof
Router(config-ipv6-dhcp-server-prof)#prefix-delegation address-pool XX
```

コマンド書式

prefix-delegation address-pool 〈アドレスプール名〉 [T1 値] [T2 値]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスプール名	通知するプレフィックス情報を取得するアドレスプール名を指定します。	16 文字以内の文字列	省略不可
T1 値	プレフィックスを与えられたサーバに再接続するまでの時間(単位:秒)を指定します。	1～4294967295	Preferred Lifetime 値の 0.5 倍
T2 値	任意のサーバに再接続するまでの時間(単位:秒)を指定します。	1～4294967295	Preferred Lifetime 値の 0.8 倍

この設定を行わない場合

IA_PD オプションを通知しません。

設定モード

DHCPv6 サーバプロファイル設定モード

DHCPv6 クライアント機能を使用するための設定

address-pool

アドレスプールの設定を行います。

refresh コマンド後に有効になるコマンドです。

設定例 1　アドレスプールを有効にする

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)# address-pool enable
```

コマンド書式

address-pool 〈アドレスプール設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスプール設定	アドレスプールを有効にするか無効にするかを指定します。 enable：アドレスプールを有効とする。 disable：アドレスプールを無効とする。アドレスの払い出しは行わないが、プールの登録は可能です。	enable disable	省略不可

※ enable から disable に変更した場合は、すでに払い出しているアドレスを回収します。

この設定を行わない場合

アドレスプールは使用不可となります。

設定モード

IPv6 アドレスプール設定モード

allocate address

払い出しアドレスブロックを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　払い出しアドレスブロックを 2001:db8::1/32 とする

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)# allocate address 2001:db8::1/32
```

コマンド書式

allocate address〈アドレスブロック〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスブロック	払い出しアドレスブロックを指定します。	IPv6 アドレス形式	省略不可

この設定を行わない場合

固定払い出しブロックはありません。

設定モード

IPv6 アドレスプール設定モード

allocate prefix-length

アドレスを払い出す際のプレフィックス長を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　プレフィックス長を 64 とする

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)# allocate prefix-length 64
```

コマンド書式

allocate prefix-length <プレフィックス長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プレフィックス長	アドレスを払い出す際のプレフィックス長を指定します。	1～128	省略不可

この設定を行わない場合

アドレスの払い出しを行いません。
ただし、プールの登録は可能です。

設定モード

IPv6 アドレスプール設定モード

allocate retention-time

アドレスの払い出しを行った後、そのアドレスが払い戻された場合の、該当プレフィックスの払い出し抑制期間を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　アドレス払い出し抑制期間を 2400 秒とする

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)# allocate retention-time
```

コマンド書式

allocate retention-time 〈抑制期間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
抑制期間	アドレスの払い出しを行った後、そのアドレスが払い戻された場合の、該当プレフィックスの払い出し抑制期間(単位:秒)を指定します。	0～2147483647	省略不可

この設定を行わない場合

アドレス払い出し抑制期間は、3600 秒になります。

設定モード

IPv6 アドレスプール設定モード

description

アドレスプールの Description を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　Description を prefix-list_ipv6 とする

```
Router(config)#address-pool ipv6 1
Router(config-if dialer 1)#description prefix-list_ipv6
```

コマンド書式

description <文字列>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
文字列	コメントを入力します。	50 文字までの 半角英数字、記号	省略不可

設定モード

IPv6 アドレスプール設定モード

address-pool ipv6

IPv6 のアドレスプールを指定するために、IPv6 アドレスプール設定モードに移行します。
複数設定がある場合は、プール名で sort して、一番先頭のアドレスプールのみ有効になります。

設定例 1　IPv6 アドレスプール設定モードに移行する

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)#
```

コマンド書式

address-pool ipv6 〈アドレスプール名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスプール名	アドレスプール名称を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

IPv6 アドレスプールの設定が行えません。

設定モード

基本設定モード

ipv6 address address-pool

アドレスプールから、/64 を切り出して、インタフェースのアドレスとして割り当てます。
アドレスプールに割り当て可能な/64 がない場合は、割り当てません(ログは出力しない)。
アドレスの割り当てが可能になったタイミングで、アドレスを割り当てます。
また、使用しているアドレスが使用禁止となった場合(例:DHCP クライアントの RENEW で異なるプレフィックスが割り当てられた等)は、アドレスを解放します。
RA により配布しているプレフィックスが使用禁止になった場合は、Valid/Preferred Lifetime を 0 とする RA を送信します。

refresh コマンド後に有効になるコマンドです。

設定例 1　アドレスプール名 (DHCPv6) からアドレスを割り当てる

```
Router(config)#interface lan 1
Router(config-if lan 1)# ipv6 address address-pool DHCPv6 prefix-length 64
```

コマンド書式

```
ipv6 address address-pool <アドレスプール名> prefix-length <プレフィックス長>
                          [interface-id <インタフェース ID>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスプール名	/64 を切り出して割り当てるアドレスプール名を指定します。	16 文字以内の文字列	省略不可
プレフィックス長	プレフィックス長を指定します。	64	省略不可
インタフェース ID	割当先のインタフェースのアドレスを指定します。	IPv6 アドレス形式	省略不可

この設定を行わない場合

インタフェースのアドレスとして、アドレスプールを利用しません。

設定モード

LAN インタフェース設定モード
WAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 dhcp client

DHCPv6 クライアント機能を指定した DHCPv6 クライアントプロファイル設定で動作させます。
DHCPv6 を動作させるインタフェースは、1 インタフェースのみになります。

refresh コマンド後に有効になるコマンドです。

設定例 1　DHCPv6 クライアントプロファイル名称を DHCPv6_1 とする

```
Router(config)#interface lan 1
Router(config-if lan 1)# ipv6 dhcp client DHCPv6_1
```

コマンド書式

ipv6 dhcp client <プロファイル名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プロファイル名	指定したインタフェースで DHCPv6 機能を動作させる場合の、クライアントプロファイル名を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

指定しているインタフェースでは、DHCPv6 クライアントが動作しません。

設定モード

LAN インタフェース設定モード
WAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード

ipv6 dhcp client-profile

DHCPv6 クライアントとして動作する際の各種パラメータの設定を行う、DHCPv6 クライアントプロファイル設定モードに移行するためのコマンドです。

設定例 1　DHCPv6 クライアントプロファイル設定モードに移行する

```
Router(config)#ipv6 dhcp client-profile dhcpv6
Router(config-ipv6-dhcp-client-prof)#
```

コマンド書式

ipv6 dhcp client-profile <クライアントプロファイル名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クライアントプロファイル名	設定を行う DHCPv6 クライアントプロファイル名を指定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

DHCPv6 クライアントを使用することができません。

設定モード

基本設定モード

option-request dns-servers

OPTION_DNS_SERVERS を要求する場合設定し、取得した DNS サーバのアドレス情報は ProxyDNS で使用します。
本コマンドが設定されている場合は、OPTION_ORO に OPTION_DNS_SERVERS をつけて SOLICIT メッセージもしくは、INFORMATION-REQUEST メッセージを送信します。
option-request prefix-delegation コマンドが設定されている場合は、SOLICIT メッセージを送信し、設定されていない場合は、INFORMATION-REQUEST メッセージを送信します。

refresh コマンド後に有効になるコマンドです。

設定例１　オプション DNS サーバを要求する

```
Router(config)#ipv6 dhcp client-profile dhcpv6
Router(config-ipv6-dhcp-client-prof)# option-request dns-servers
```

コマンド書式

```
option-request dns-servers
```

パラメータ

パラメータはありません。

この設定を行わない場合

DNS サーバアドレスを要求しません。

設定モード

DHCPv6 クライアントプロファイル設定モード

option-request prefix-delegation

Prefix Delegation を要求する場合に指定します。
割り当てられた情報は、address-pool で指定する名称のプールに prefix-length/offset で切り出した分を保管し、他目的(他 IF での DHCP サーバ機能等)に利用できることができます。
本コマンドが設定されている場合は、OPTION_IA_PD をつけて SOLICIT メッセージを送信します。

refresh コマンド後に有効になるコマンドです。

設定例 1　通知されたプレフィックス値を保管する address-pool 名称を DHCPv6_1 とする

```
Router(config)#ipv6 dhcp client-profile dhcpv6
Router(config-ipv6-dhcp-client-prof)# option-request prefix-delegation delegates address-pool
DHCPv6_1 prefix-length 64
```

コマンド書式

```
option-request prefix-delegation delegates address-pool <アドレスプール名>
  prefix-length <プレフィックス値> offset <オフセット値>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスプール名	通知されたプレフィックス値を保管するアドレスプール名称を設定します。	16 文字以内の文字列	省略不可
プレフィックス値	プレフィックス値を指定します。	1～128	省略不可
オフセット値	切り出す際のオフセット値を指定します。	0～2147483647	省略不可

prefix-length と offset による切り出し方

例 1)

prefix-length 52 offset 1 と設定しているケースで、3ffe:1:1::/51 を受けた場合

3ffe:1:1::/51	
3ffe:1:1::/52	3ffe:1:1:10::/52
↑ offset 0	↑ offset 1

例 2)

prefix-length 52 offset 1 と設定しているケースで、3ffe:1:1::/50 を受けた場合

3ffe:1:1::/50			
3ffe:1:1::/52	3ffe:1:1:10::/52	3ffe:1:1:20::/52	3ffe:1:1:30::/52
↑ offset 0	↑ offset 1	↑ offset 2	↑ offset 3

この設定を行わない場合

Prefix Delegation を要求しません。

設定モード

DHCPv6 クライアントプロファイル設定モード

pooled-route

アドレスプールに静的および動的に登録されたプレフィックス情報をあて先とする経路情報を登録します。

refresh コマンド後に有効になるコマンドです。

設定例 1　宛先プレフィックスを 2001:db8::1 とする

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)# pooled-route 2001:db8::1
```

コマンド書式

```
pooled-route {<宛先プレフィックス> | <インタフェース名※1>|
              connected <インタフェース名※2>} [メトリック値]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先プレフィックス	宛先プレフィックスを指定します。	IPv6 アドレス形式	省略不可
インタフェース名※1	宛先へ到達するためのインタフェースを指定します。	lan 1～1 ewan 1～2 pppoe 1～24 tunnel 1～2000 vlanif 1～150	省略不可
インタフェース名※2	宛先を IPsecIF、Null インタフェースの connected として扱う場合に指定します。	ipsecif 1～2000 null 0	省略不可
メトリック値	メトリック値を指定します。	1～255	210

この設定を行わない場合

経路登録を行いません。

設定モード

IPv6 アドレスプール設定モード

IPv6 ルーティングの設定

IPv6 アドレスについて

IPv6 アドレスの基本的な仕様について説明します。

現在インターネットをはじめ、ネットワーク分野で広く利用されている IPv4 の次期バージョンにあたる IP プロトコルです。IPv4 と比較して 128 ビッ トの広大なアドレス空間を持つもつところです。さらに、ネットワークの自動設定やセキュリティといった技術を標準で実装しているという特徴も持っていま す。
IPv6 アドレスは、プレフィックスと呼ばれるネットワークを規定する番号と、インタフェース ID と呼ばれるホストを規定する番号で構成されます。
IPv6 ネットワークでは、プレフィックスが 64bit／インタフェース ID が 64bit の、128bit のアドレスを使用します。

IPv6 アドレスの種類

IPv6 アドレスには、以下の３種類があります。

ユニキャストアドレス	特定のノードの IPv6 アドレス
マルチキャストアドレス	グループの中のみんなを意味するアドレス。グループ全員に配信される。 IPv4 のブロードキャストもしくはマルチキャストのようなもの
エニーキャストアドレス	グループのうちの誰かを意味するアドレス。グループのうち最も近くにいるノードとなる。 IPv4 ではこれに該当するアドレスはない。

さらにユニキャストアドレスは、使用する用途により、以下の 3 種類があります。

グローバルアドレス	インターネット等、パブリックネットワークに接続できるアドレス体系
リンクローカルアドレス	同一サブネット内の通信のみに使用されるアドレス体系
サイトローカルアドレス	サイト内の通信で使用されるアドレス体系。IPv4 のローカルアドレスのようなもの

プレフィックス

プレフィックスは、各アドレス体系により異なります。

グローバルアドレスの場合

グローバルアドレスのプレフィックスは、通常 IPv6 ルータから広告される ICMPv6 の RA（Router Advertisement）をノードが受信し、取得します。

RA でプレフィックスを広告する際、同時に、以下の情報も広告されます。
・LINK 上に存在するプレフィックスかどうか
・このプレフィックスをノードが使用しても良いか
・このプレフィックスの使用が可能な時間（Valid Lifetime）
・このプレフィックスを率先して使用しても良い時間（Prefferd Lifetime）

各ノードは、この情報に基づいて、自身のインタフェースのアドレスのプレフィックスを定義することができます。
この方式を、Stateless Address Autoconfiguration ということが多いです。

リンクローカルアドレスの場合

リンクローカルアドレスのプレフィックスは、fe80::/64 であることが規定されています。

サイトローカルアドレスの場合

サイトローカルアドレスは、各サイトで一意となるプレフィックス値を各ノードに設定します。サイトローカルアドレスは、fec0:で始まるプレフィックスであることが規定されています。

マルチキャストアドレスの場合

マルチキャストアドレスの場合、プレフィックスは ff02::/64 となります。下位の 64bit で、グループを表しています。

例）
ff02::1：全ての IPv6 ノード
ff02::2：全ての IPv6 ルータ
ff02::9：RIPng
ff02::1:ｆｆXX:XXXX：要請ノードマルチキャストアドレス　（XXXXXX は、MAC アドレスを解決したい IPv6 アドレスの下位３バイト）

エニーキャストアドレスの場合

エニーキャストアドレスの場合、プレフィックスはユニキャスト宛と同様で、ホスト ID 部が機能を示す ID となります。

インターフェース ID

ホストを規定する番号がインタフェース ID です。
通常の IPv6 ノードは、インタフェース ID を、そのインタフェースのデータリンクアドレス（通常 MAC アドレス）から計算された値を使用します。この計算の方式には、EUI-64 形式が利用されます。EUI-64 形式は、以下のルールで決定されます。
　－MAC アドレス 6 バイトの、上位 3 バイトと下位 3 バイトをわけ、間に"fffe"を入れる
　－上位 1 バイト目の下位 2 ビット目を"1"にする。

例えば、MAC アドレスが"0080.bdcf.f100"だった場合、上位 3 バイト（"0080bd"）と下位 3 バイト（"cff100"）の間 に"fffe"を入れた"0080bdfffecff100"の上位 1 バイト目の下位 2 ビット目を"1"にした、"0280bdfffecff100"が このインタフェースのインタフェース ID となります。

IPv6 アドレスの決定

プレフィックスとインタフェース ID が決まると、IPv6 アドレスが決定します。
例えば、ルータ以外のノードが、RA によりプレフィックス 2002:901::/64 を受信し、インタフェース ID を EUI-64 形式で"0280bdfffecff100"と決まった場合、このインタフェースの IPv6 アドレスは
　2002:901::280:bdff:fecf:f100
となります。

したがって、このインタフェースのリンクローカルアドレスは、
　fe80::280:bdff:fecf:f100
となります。

グローバルアドレスに関する注意事項

IPv4 と異なり、IPv6 アドレスは、インタフェースに複数のアドレスを割り当てることができます。
RA で通知された各グローバルプレフィックスには、「使用可能時間（Valid Lifetime）」と「使用が望ましい時間（Prefferd Lifetime）」が指定されています。
通常は、「使用が望ましい時間」＜「使用可能時間」となっており、【使用が望ましい状態】から「使用が望ましい時間」経過すると【使用可能状態】となり、「使用可能時間」が経過すると【使用不可能状態】となります。

インタフェースに複数の IPv6 グローバルアドレスが割り振られており、それぞれ【使用が望ましい状態】【使用可能状態】【使用不可能状態】であった場合は、【使用が望ましい状態】の IPv6 アドレスが、送信元アドレスとして採用されます。
ただし、TCP 等セッションが解放される前に、【使用が望ましい状態】→【使用可能状態】になった場合は、このアドレスを継続して採用します。

Router Advertisement (RA) について

IPv6 ルータが、グローバルアドレスのプレフィックス等の情報を ICMPv6 で広告します。この情報のことを、Router Advertisement (RA) といいます。

RA では、以下の情報を広告します。
- current hop limit
- M フラグ (Managed Flag)
- O フラグ (Other Flag)
- ルータライフタイム
- Reachable タイム
- Retransmission タイム
- MTU 長

また、通知するプレフィックスごとに、以下の情報があります。
- On-link フラグ
- AutoConfig フラグ
- Valid ライフタイム
- Prefferd ライフタイム
- プレフィックス

以下、各情報に関する説明です。

current hop limit

この RA を使用するノードが送信する IPv6 パケットの、IPv6 ヘッダ中にある Hop limit に入れる値を通知します。
Hop limit は、そのパケットが到達可能なホップ数です。

例えば、Hop limit に"100"が設定されているパケットは、送信元のノードから、100Hop の宛先までは到達できますが、それより先のネットワークには到達できないことを意味します。

このように、ノードが通信できるホップ数を、ルータで管理することができます。
本装置では、"ipv6 hop-limit"コマンドで設定できます。

M フラグ（Managed Flag）

この RA を使用するノードが、Stateless Address Autoconfiguration を使用して IPv6 アドレスを割り当てるか、DHCPv6 などを利用して、Stateful なアドレス割り当てを行なうかを規定するフラグです。

M フラグに"0"が設定されている RA の場合は、Stateless Address Autoconfiguration の使用が認められます。
M フラグに"1"が設定されている RA の場合は、Stateless Address Autoconfiguration のほかに、Stateful なプロトコル（DHCPv6 等）を利用して、IPv6 アドレスを割り当てる必要があります。

本装置では、各インタフェース毎に M フラグをセットするかどうかを指定できます。
各インタフェース設定モードで、"ipv6 nd managed-config-flag"コマンドで設定できます。
"ipv6 nd managed-config-flag"を指定した場合は M フラグを"1"にセット、工場出荷時または"no ipv6 nd managed-config-flag"を指定した場合は M フラグを"0"にセットして、RA を通知します。

O フラグ（Other Flag）

この RA を使用するノードが、アドレス以外の情報を自動設定、ステートフルなプロトコルを利用して取得すべきかどうかを規定するフラグです。

O フラグに"0"が設定されている場合は、ステートフルなプロトコルを受け付けることができません。
O フラグに" 1 " が設定されている場合は、ステートフルなプロトコルを利用して、アドレス以外の情報を自動設定で取得します。

本装置では、各インタフェース毎に O フラグをセットするかどうかを指定できます。
各インタフェース設定モードで、"ipv6 nd other-config-flag"コマンドで設定できます。
"ipv6 nd other-config-flag"を指定した場合は O フラグを"1"にセット、工場出荷時または"no ipv6 nd other-config-flag"を指定した場合は O フラグを"0"にセットして、RA を通知します。

ルータライフタイム

この RA を送信したルータをデフォルトルートとして使用できる時間を規定しています。

本装置では、各インタフェース毎にルータライフタイムを設定できます。
各インタフェース設定モードで、"ipv6 nd ra-lifetime"コマンドで設定できます。（単位：秒）
工場出荷時または"no ipv6 nd ra-lifetime"を指定した場合は、1800 秒（30 分）として、RA を通知します。
なお、0 を指定した場合は、このルータがデフォルトルータとはなり得ないことを表します。

Reachable タイム

アドレス解決（Neighbor Solicitation）を行なう間隔を規定しています。
本装置では、"ipv6 nd reachable-time"コマンドで設定することができます。
工場出荷時または"no ipv6 nd reachable-time"を指定した場合は、30000m 秒（＝30 秒）となります。

Retransmission タイム

このRAを受信したノードが、MACアドレス解決のためにNeighbor Solicitation（NS）パケットを送信した時に、応答がない等の理由で再送が必要になった場合に、Retransmissionタイムとして通知された時間の間隔で再送を行ないます。

本装置では、各インタフェース毎にRetransmissionタイムを設定できます。
各インタフェース設定モードで、"ipv6 nd ns-interval"コマンドで設定できます。（単位：ミリ秒）
工場出荷時または"no ipv6 nd ns-interval"を指定した場合は、1秒（1000ミリ秒）として、RAを通知します。

なお、この設定は、本装置自身がNSを送信する状況で、再送が必要になった場合は、この設定に従います。

MTU 長

このRAを受信したノードが、受信したインタフェースに対して送信するパケットのMTU長を規定します。

本装置では、"ipv6 mtu"コマンドで設定できます。
工場出荷時または"no ipv6 mtu"を指定した場合は、MTUを1500とします。
本装置は、MTU長に1500以外が設定された場合のみ、RAのオプションとしてMTU長を通知します。

On-link フラグ

該当プレフィックスが、受信したインタフェースと同一リンク上に存在するかどうかのフラグです。

同一リンク上のプレフィックスの場合は"1"、同一リンク上にないプレフィックスの場合は"0"がセットされます。

RAを受信したノードが、Stateless Address Autoconfigurationを使用する場合、On-linkフラグが"1"にセットされたプレフィックスについては、自身のインタフェースアドレスとして割り当てることができます。

本装置では、設定でインタフェースに割り当てたアドレスのプレフィックスをRAで広告する場合は、On-linkに"1"をセットして広告します。また、PD（Prefix Delegation）で、インターネットプロバイダから割り当てられたプレフィックスをLANインタフェースに広告する場合も、On-linkに"1"をセットして広告します。

上記２形態とは異なり、通知するプレフィックスをスタティックで登録することもできます（ipv6 nd prefix-advertisementコマンド）。この場合は、指定したプレフィックスがリンク上に存在するかどうかを指定します。

Auto Config フラグ

このRAを受信したノードが、Stateless Address Autoconfigurationを使用する場合、このプレフィックスをインタフェースのIPv6アドレスのプレフィックスとして使用しても良いかどうかのフラグです。

使用しても良い場合は"1"、使用してはいけない場合は"2"がセットされます。

本装置では、設定でインタフェースに割り当てたアドレスのプレフィックスをRAで広告する場合は、Auto Configに"1"をセットして広告します。また、PD（Prefix Delegation)で、インターネットプロバイダから割り当てられたプレフィックスをLANインタフェースに広告する場合も、Auto Configに"1"をセットして広告します。

上記２形態とは異なり、通知するプレフィックスをスタティックで登録することもできます（ipv6 nd prefix-advertisementコマンド）。この場合は、指定したプレフィックスがインタフェースアドレスのプレフィックスとして使用可能どうかを指定します。

Validライフタイム

該当プレフィックスの使用可能期間を規定します。

RAで通知されるプレフィックスを使用する場合は、【使用が望ましい状態】と【使用可能状態】が存在します。

本装置では、設定でインタフェースに割り当てたアドレスのプレフィックスをRAで広告する場合は、2592000秒（720時間）で広告します。また、PD（Prefix Delegation)で、インターネットプロバイダから割り当てられたプレフィックスをLANインタフェースに広告する場合も、2592000秒（720時間）で広告します。

上記２形態とは異なり、通知するプレフィックスをスタティックで登録することもできます（ipv6 nd prefix-advertisement コマンド）。この場合は、Valid ライフタイムを指定します。

Prefferdライフタイム

該当プレフィックスの「使用が望ましい期間」を規定します。

RAで通知されるプレフィックスを使用する場合は、【使用が望ましい状態】と【使用可能状態】が存在します。

本装置では、設定でインタフェースに割り当てたアドレスのプレフィックスをRAで広告する場合は、604800秒（168時間）で広告します。また、PD（Prefix Delegation)で、インターネットプロバイダから割り当てられたプレフィックスをLANインタフェースに広告する場合も、604800秒（168時間）で広告します。

上記２形態とは異なり、通知するプレフィックスをスタティックで登録することもできます（ipv6 nd prefix-advertisemente コマンド）。この場合は、Prefferd ライフタイムを指定します。

IPv6 アドレス設定

ipv6 address

インタフェースの IPv6 アドレス(グローバル・リンクローカル)を指定します。
リンクローカルアドレスを指定しなかった場合は、EUI-64 形式のリンクローカルアドレスが自動で設定されます。
本装置では、1つのインタフェースに4つのグローバルアドレスを指定することができます。

設定例１　プレフィックス：2001:db8::/32　EUI-64 形式で指定する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 address 2001:db8::/32 eui-64
```

設定例２　リンクローカルアドレスを、2001:db8::1 に設定する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 address 2001:db8::1 link-local
```

コマンド書式

ipv6 address { <IPv6 アドレス> link-local | <IPv6 プレフィックス> [eui-64] }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPv6 アドレス	IPv6 リンクローカルアドレスを指定します。	IPv6 アドレス形式	省略不可
link-local	リンクローカルアドレスである場合に指定します。	link-local	省略不可
IPv6 プレフィックス	IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可
eui-64	EUI-64 方式でグローバルアドレスを設定する場合に指定します。	eui-64	省略した場合はグローバルアドレスとして使用しません。RA で広告するプレフィックスにのみ使用します。

最大エントリ数:256 エントリ(装置全体)

この設定を行わない場合

インタフェースに IPv6 アドレスが割り当てられません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ipv6 address autoconfig

インタフェースで Stateless Address Autoconfiguration を使用し、IPv6 アドレスを自動設定します。
本設定を行う場合は、ipv6 nd receive-ra コマンドの設定が必要です。

設定例 1　RA を受信するインタフェースを EWAN1 とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# ipv6 address autoconfig
```

コマンド書式

ipv6 address autoconfig [interface-id <インタフェース ID>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース ID	Stateless Address Autoconfiguration において使用するインタフェース ID を指定します。	64 ビット /xxxx:xxxx:xxxx:xxxx 型式	EUI-64 型式

この設定を行わない場合

Stateless Address Autoconfiguration によるアドレス自動割り当てを行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 enable

インタフェースにグローバルアドレスを割り当てず（ipv6 address コマンドを使用しない）、リンクローカルアドレスのみで IPv6 通信を行なう（同一リンク内のみの通信）場合に指定します。

設定例 1　LAN インタフェースを、リンクローカルアドレスのみで使用する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 enable
```

コマンド書式

```
ipv6 enable
```

パラメータ

パラメータはありません。

この設定を行わない場合

ipv6 address コマンドで、IPv6 アドレスを明示的に設定しない場合、リンクローカルアドレスが割り当てられません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ICMPv6 に関する設定

ipv6 address autoconfig

インタフェースで Stateless Address Autoconfiguration を使用し、IPv6 アドレスを自動設定します。
本設定を行う場合は、ipv6 nd receive-ra コマンドの設定が必要です。

設定例 1　RA を受信するインタフェースを EWAN1 とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# ipv6 address autoconfig
```

コマンド書式

ipv6 address autoconfig [interface-id <インタフェース ID>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース ID	Stateless Address Autoconfiguration において使用するインタフェース ID を指定します。	64 ビット /xxxx:xxxx:xxxx:xxxx 型式	EUI-64 型式

この設定を行わない場合

Stateless Address Autoconfiguration によるアドレス自動割り当てを行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 hop-limit

Hop limit とは、そのパケットが到達可能なホップ数です。例えば、Hop limit に"100"が設定されているパケットは、送信元のノードから、100Hop の宛先までは到達できますが、それより先のネットワークには到達できないことを意味します。

本装置では、自身から送信する IPv6 パケットの Hop limit 値、および本装置が RA を送信する場合に、RA の"current hop limit"に入れる値を設定できます。RA を受信したノードは、"current hop limit"の値を、送信する IPv6 パケットの、IPv6 ヘッダ中にある Hop limit に入れます。

設定例１　RA の current hop limit 値を、100 とする

```
Router(config)#ipv6 hop-limit 100
```

コマンド書式

ipv6 hop-limit <最大ホップ数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
最大ホップ数	自身または RA で通知する hop-limit 値を設定します。	1～255	省略不可

この設定を行わない場合

本装置自身が送信するパケットの Hop limit 値は 64、RA で送信する current hop limit は 0(ルータは規定しない)となります。

設定モード

基本設定モード

ipv6 hoplimit-receive-enable

受信した RA で指定されている CurHopLimit 値を有効とする場合に指定します。
有効とした場合、受信した RA に規定されている CurHopLimit 値をホップリミット値として使用します。
本設定を行う場合は、ipv6 nd receive-ra コマンドの設定が必要です。

設定例 1　EWAN1 インタフェースから受信した RA に規定されている CurHopLimit 値をホップリミット値とする

```
Router(config)#interface ewan 1
Router(config config-if ewan 1)# ipv6 hoplimit-receive-enable
```

コマンド書式

ipv6 hoplimit-receive-enable

パラメータ

パラメータはありません。

この設定を行わない場合

ipv6 hop-limit コマンドの設定に従います。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 icmp error-ratelimit

本装置が、ICMP を使ってエラーを送信する際の、1 秒間に送信する最大送信パケット数を設定します。1 秒間に送信するパケット数が規定数を超過した場合に、次の 1 秒まで送信を抑止します。
0 を指定した場合、ICMP エラーメッセージおよび REDIRECT メッセージは送信されません。
エラーパケットにより、データ通信のための帯域が減ってしまうのを防ぐ機能です。

refresh コマンド後に有効になるコマンドです。

設定例 1　エラーパケットを、最大 300 パケット/秒とする

```
Router(config)#ipv6 icmp error-ratelimit 300
```

コマンド書式

ipv6 icmp error-ratelimit {パケット数/秒 | unlimit}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
パケット数/秒	IPv6 ICMP でエラーを送信する際の 1 秒間に送信する最大送信パケット数	0～2147483647	省略不可
unlimit	ICMP エラーメッセージおよび REDIRECT メッセージのレート制限を行いません。	unlimit	省略不可

この設定を行わない場合

100 パケット/秒が設定されます。

IPv6 での ICMP エラーパケットの種類

IPv6 での ICMP エラーパケットには、以下の種類があります。

Type	内容
1	受信したパケットの宛先への中継ができない
2	パケット長が MTU 長より大きいため、転送できない
3	ホップ数が制限を越えたため、転送できない
4	IPv6 ヘッダ（拡張ヘッダを含む）が異常、もしくは未知
137	中継先を別のルータに変更したことを通知

設定モード

基本設定モード

ipv6 nd managed-config-flag

本装置から RA（Router Advertisement）を送信する際に、M フラグを"1"とするかどうかを設定します。このコマンドを指定した場合は、M フラグを"1"として RA を送信します。
M フラグが"1"になっている RA を受信したノードは、Stateless Auto Configuration ではなく、DHCPv6 などのアドレス自動設定（Stateful Auto Configuration）を行なう必要があります。

設定例 1　M フラグをつける

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd managed-config-flag
```

コマンド書式

```
ipv6 nd managed-config-flag
```

パラメータ

パラメータはありません。

この設定を行わない場合

M フラグを"0"として RA を送信しています。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 nd ns-interval

本装置が、RA を送信する際に、Retrans Timer 値として通知する値を設定します。
この RA を受信したノードは、NS(Neighbor Solicitation)を再送する際、ここで指定した間隔で送信します。
また、本装置が NS を再送する際も、この値を使用します。

設定例 1　NS の再送間隔を 10 秒（10000m 秒）とする

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd ns-interval 10000
```

コマンド書式

ipv6 nd ns-interval <RA で通知する NS の再送間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
RA で通知する NS の再送間隔	RA で通知する NS の定期送信間隔および、本装置が再送信する際の送信間隔(単位:m 秒)	1000～3600000	省略不可

この設定を行わない場合

RA では 0(未指定)を通知し、本装置は 1 秒(1000m 秒)で動作します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 nd other-config-flag

本装置から RA（Router Advertisement）を送信する際に、O フラグを"1"とするかどうかを設定します。このコマンドを指定した場合は、O フラグを"1"として RA を送信します。
O フラグが"1"になっている RA を受信したノードは、アドレス以外の情報を自動設定するために、ステートフルなプロトコルを使用する必要があります。

設定例 1　0 フラグをつける

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd other-config-flag
```

コマンド書式

```
ipv6 nd other-config-flag
```

パラメータ

パラメータはありません。

この設定を行わない場合

O フラグを"0"として RA を送信しています。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 nd prefix-advertisement

RA で通知するプレフィックスを設定します。この設定がない場合は、LAN インタフェースに割り当てられたプレフィックスを通知します。

このコマンドで通知するプレフィックスを指定する場合は、プレフィックス値のほかに、「Valid Lifetime」「Prefferd Lifetime」「onlink フラグ」「Autoconfig フラグ」も指定します。

Valid Lifetime	このプレフィックスをノードが使用する場合に、使用可能な時間(秒)
Prefferd Lifetime	このプレフィックスをノードが使用する場合に、正当な使用が問題ない時間(秒)
onlink フラグ	同一リンク上に存在することを表すフラグ
Autoconfig フラグ	このプレフィックスをノードが受信した場合に、Stateless Auto Configuration でアドレスを使用してよいかどうかを表すフラグ

設定例 1　RA で通知するプレフィックスを"2001:db8::/32"に設定（Valid Lifetime:500 秒、Prefferd Lifetime:400 秒、Autoconfig フラグあり）する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd prefix-advertisement 2001:db8::/32 500 400 autoconfig
```

コマンド書式

ipv6 nd prefix-advertisement <IPv6 プレフィックス> <Valid Lifetime> <Prefferd Lifetime> [onlink] [autoconfig]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPv6 プレフィックス	RA で通知する IPv6 プレフィックスを設定します。	IPv6 プレフィックス形式	省略不可
Valid Lifetime	Valid Lifetime 値(単位:秒)を設定します。	0～4294967295	省略不可
Prefferd Lifetime	Prefferd Lifetime 値(単位:秒)を設定します。	0～4294967295	省略不可
onlink	Onlink フラグを立てる場合に指定します。	onlink	Onlink フラグを立てない
autoconfig	Autoconfig フラグを立てる場合に指定します。	autoconfig	Autoconfig フラグを立てない

この設定を行わない場合

ipv6 address コマンドで指定したプレフィックス値を RA で通知します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 nd ra-interval

本装置から RA を定期送信する際の、送信間隔を設定します。

設定例 1　RA を 30 秒おきに送信する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd ra-interval 30
```

コマンド書式

ipv6 nd ra-interval <RA の送信間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
RA の送信間隔	RA を定期送信する際の送信間隔(単位:秒)	3～1800	省略不可

この設定を行わない場合

200 秒間隔で RA を送信します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 nd ra-lifetime

本装置が送信する RA のルータライフタイム値を設定します。lifetime 値は、RA を受信したノードが、RA の送信元ルータをデフォルトルータとして使用できる時間(秒)です。

設定例 1　RA の lifetime を 3000 秒とする

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd ra-lifetime 3000
```

コマンド書式

ipv6 nd ra-lifetime <ルータライフタイム値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ルータライフタイム値	RA で公開するルータライフタイム値(単位:秒)	0～9000	省略不可

この設定を行わない場合

1800 秒となります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 nd reachable-time

本装置が送信する RA の reachable time 値を設定します。

設定例 1　reachable time 値を 15000 に設定する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd reachable-time 15000
```

コマンド書式

ipv6 nd reachable-time <Reachable Time 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Reachable Time 値	Reachable Time 値を指定します（単位：m 秒）	0-3600000	省略不可

この設定を行わない場合

30000m 秒となります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 nd receive-ra

本コマンドを指定することにより、RA を受信するインタフェースとします。
同じインタフェースで、ipv6 nd send-ra が設定されている場合はログを出力し、RA の送信／受信の動作を行ないません。

設定例 1　RA を受信するインタフェースを EWAN1 とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# ipv6 nd receive-ra
```

コマンド書式

ipv6 nd receive-ra [prefix-delegation <インタフェース名>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
prefix-delegation	受信したプレフィックス情報を他のインタフェースで利用する場合に設定します。	prefix-delegation	受信したプレフィックス情報を受信したインタフェースで利用します。
インタフェース名	プレフィックス情報を利用するインタフェースを指定します。	lan 1 ewan 1～2 vlanif 1～150	省略不可

この設定を行わない場合

RA を受信しても無視します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 nd rs-delay

インタフェースが UP して最初の RS 送信までの遅延時間と次回以降の送信間隔を設定します。
ipv6 nd rs-times コマンドで指定した回数まで、設定した送信間隔で RS を送信します。
本コマンドは、ipv6 nd receive-ra コマンドが設定されている場合のみ有効となります。

設定例 1　最初に RS を送信するまでの遅延時間を 5 秒、その後 30 秒おきに送信する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd rs-delay 5 30
```

コマンド書式

ipv6 nd rs-delay <RS 初回送信遅延時間> <RS 送信間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
RS 初回送信遅延時間	インタフェースが UP して最初の RS 送信までの遅延時間(単位:秒)を指定します。	0～3600	省略不可
RS 送信間隔	初回送信以降の RS 送信間隔(単位:秒)を指定します。	4～3600	省略不可

この設定を行わない場合

最初に RS を送信するまでの遅延時間 0 秒、次回以降は 4 秒おきに送信します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 nd rs-times

RS 送信開始後、RA が受信出来ない場合の RS 送信回数を指定します。
ipv6 nd rs-delay コマンドで指定した間隔で、指定した送信回数分 RS を送信します。
本コマンドは、ipv6 nd receive-ra コマンドが設定されている場合のみ有効となります。

設定例 1　RS の送信回数を 10 回にとする

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd rs-times 10
```

コマンド書式

ipv6 nd rs-times <RS 送信回数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
RS 送信回数	RS 送信開始後、RA が受信出来ない場合の RS 送信回数を指定します。	0※～65535	省略不可

※ RS 送信回数を 0 秒に設定した場合は、RA が受信できるまで RS を送信し続けます。

この設定を行わない場合

RS の送信回数は 3 回になります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 nd send-ra

本装置から RA を送信するかどうかを設定します。
ipv6 nd prefix-advertisement の設定がある場合は、指定されたプレフィックス情報を通知します。
ipv6 nd prefix-advertisement の設定がない場合は、ipv6 address コマンドで設定したインタフェースに割り当てられるプレフィックスを通知します。

設定例 1　RA を送信する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd send-ra
```

コマンド書式

```
ipv6 nd send-ra
```

パラメータ

パラメータはありません。

この設定を行わない場合

RA を送信しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 ns-interval-receive-enable

受信した RA で指定されている RetransTimer 値を有効とする場合に指定します。
受信した RA で規定されている RetransTimer 値と、インタフェースに設定されている RetransTimer 値(ipv6 nd ns-interval コマンド)を比較し、小さい値をインタフェースの RetransTimer 値として使用します。
本設定を行う場合は、ipv6 nd receive-ra コマンドの設定が必要です。

設定例 1　EWAN1 インタフェースで受信した RA で指定されている RetransTimer 値を有効とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# ipv6 reachable-time-receive-enable
```

コマンド書式

```
ipv6 ns-interval-receive-enable
```

パラメータ

パラメータはありません。

この設定を行わない場合

ipv6 nd ns-interval コマンドの設定に従います。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 reachable-time-receive-enable

受信した RA で指定されている Reachable Time 値を有効とする場合に指定します。
受信した RA で規定されている ReachableTime 値と、インタフェースに設定されている ReachableTime 値(ipv6 nd reachable-time コマンド)を比較し、小さい値をインタフェースの BaseReachableTime 値として使用します。
本設定を行う場合は、ipv6 nd receive-ra コマンドの設定が必要です。

設定例 1　EWAN1 インタフェースで受信した RA で指定されている Reachable Time 値を有効とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# ipv6 reachable-time-receive-enable
```

コマンド書式

```
ipv6 reachable-time-receive-enable
```

パラメータ

パラメータはありません。

この設定を行わない場合

ipv6 nd reachable-time コマンドの設定に従います。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

RIPng

aggregate-address

経路情報を集約し、その情報を RIPng で通知します。通知する際は、集約後の経路情報のみを通知し、集約された元の情報は通知されません。
この機能により、RIPng で通知するプレフィックスの数を減らすことができ、ネットワークを有効に利用することができるようになります。
例えば、以下のようなケースで有効です。

EWAN 側に、2001:db8:100::/32 ネットワーク、2001:db8:110::/32 ネットワーク、2001:db8:120::/32 ネットワーク・・・・等、1 バイト目が 2001 であるネットワークが数多く存在する。
↓↓↓
2001:db8::/32 として、LAN 側に RIPng で通知

refresh コマンド後に有効になるコマンドです。

設定例 1　2001:db8::/32 に集約して RIPng を通知します。

```
Router(config)#router ripng
Router(config-ripng)# aggregate-address 2001:db8::/32
```

コマンド書式

aggregate-address〈集約後の IPv6 プレフィックス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
集約後の IPv6 プレフィックス	集約後の IPv6 プレフィックスを設定します。	IPv6 プレフィックス形式	省略不可

この設定を行わない場合

Aggregate しません。

設定モード

RIPng サービス設定モード

default-information originate

自身をデフォルトルートとして、RIPng で通知するかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　デフォルトルートの情報を RIP で送信する

```
Router(config)#router ripng
Router(config-ripng)#default-information originate
```

コマンド書式

```
default-information originate
```

パラメータ

パラメータはありません。

この設定を行わない場合

自身をデフォルトルートとしては通知しません。

注意

この設定は、デフォルトルートの情報を持っていないときに、RIPng でデフォルトルートを通知するかどうかの設定です。
スタティック設定でデフォルトルートを設定していたり、ルーティングプロトコルによりデフォルトルートを学習していた場合は、この設定によらずデフォルトルートの情報を RIPng で広告します。

設定モード

RIPng サービス設定モード

distribute-list

RIPng 送受信に対してフィルタリングの設定を行ないます。
ipv6 prefix-list コマンドで指定したプレフィックスの情報のみを受け入れる／受け入れない、または送信する／送信しないといった制御を行なうことができます。
また、フィルタリング制御を行なうためのインタフェースを指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　3ffe:100::/64 のプレフィックス情報のみを受け付ける

```
Router(config)#prefix-list 1 permit 3ffe:100::/64

Router(config)#router ripng
Router(config-ripng)# distribute-list prefix 1 in
```

設定例２　3ffe:100::/64 のプレフィックス情報のみを送信しない

```
Router(config)#prefix-list 1 deny 3ffe:100::/64

Router(config)#router ripng
Router(config-ripng)# distribute-list prefix 1 out
```

※上記の設定を行う場合は、必ず ipv6 prefix-list コマンドで permit any を追加する必要があります。
permit any を追加しないと、全てのプレフィックスの送信をフィルタしてしまいます。

設定例３　3ffe:100::/64 のプレフィックス情報を、LAN からは受信しない

```
Router(config)#prefix-list 1 deny 3ffe:100::/64

Router(config)#router ripng
Router(config-ripng)# distribute-list prefix 1 in lan 1
```

コマンド書式

distribute-list prefix <prefix 番号> { in | out } [インタフェース名]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
prefix 番号	prefix-list コマンドで指定したリスト番号を指定します。	1～99	省略不可
in | out	in（受信）／out（送信）のどちらでフィルタするかを指定します。	in out	省略不可

インタフェース名	適用するインタフェースのインタフェース名を指定します。	インタフェース名形式	全インタフェースで適用

この設定を行わない場合

全てのプレフィックスを送受信します。

設定モード

RIPng サービス設定モード

ipv6 prefix-list

IPv6 のプレフィックスリスト情報を設定します。
プレフィックスリストは、RIPng で広告する／広告しないプレフィックスを制御するために使用します。
本コマンドで、プレフィックス値、許可するかどうかを指定し、RIPng サービス設定モードの、distribute-list コマンドで、広告する／受け入れるプレフィックスを指定するために、本コマンドで設定したプレフィックスリスト番号を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　2001:db8::/32 を許可するプレフィックスリスト（リスト番号１）を作成する

```
Router(config)#ipv6 prefix-list 1 permit 2001:db8::/32
```

コマンド書式

ipv6 prefix-list <リスト番号> <permit | deny > <IPv6 プレフィックス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リスト番号	プレフィックスリスト番号	1～99	省略不可
permit | deny	許可する場合は permit、許可しない場合は deny を指定します。	permit or deny	省略不可
IPv6 プレフィックス	対象となる IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可

この設定を行わない場合

全ての IPv6 経路情報を RIPng で送受信します。

設定モード

基本設定モード

network

RIPng サービスを提供するインタフェースをインタフェース名もしくは IPv6 アドレス形式で決定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　LAN インタフェースで RIPng を運用する

```
Router(config)#router ripng
Router(config-ripng)# network lan 1
```

コマンド書式

network ｛〈インタフェース名〉｜〈IPv6 アドレス〉｝

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	RIPng を運用するインタフェース名を指定します。	インタフェース名形式	省略不可
IPv6 アドレス	RIPng を運用するインタフェースを、インタフェースの IPv6 アドレスで指定します。	IPv6 アドレス形式	

この設定を行わない場合

全てのインタフェースで RIPng を運用しません。

設定モード

RIPng サービス設定モード

redistribute

RIPng 以外の手段で取得した経路情報のうち、RIPng で再配布する手段を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　スタティックで登録した経路情報を RIPng で再配布する

```
Router(config)#router ripng
Router(config-ripng)#redistribute static
```

設定例２　直接ルートの経路情報を RIPng で再配布する。

```
Router(config)#router ripng
Router(config-ripng)#redistribute connected
```

コマンド書式

redistribute〈再配布する経路情報〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
再配布する経路情報	RIPng 以外の手段で取得した経路情報のうち、RIPng で配布するものを指定します。 connected：直接経路 kernel：kernel にセットされた経路情報 static：スタティックルーティング情報	connected kernel static	省略不可

この設定を行わない場合

RIPng で受信した情報のみを広告します。

設定モード

RIPng サービス設定モード

route

RIPng エントリをマニュアルで登録します。
ここで設定した経路情報は、RIPng で広告するためだけに使用されます。装置のスタティックルートとしては登録されませんので注意してください。

refresh コマンド後に有効になるコマンドです。

設定例 1　2001:db8::/32 の経路情報を RIPng で広告する

```
Router(config)#router ripng
Router(config-ripng)#route 2001:db8::/32
```

コマンド書式

route <RIPng で広告する Prefix>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
RIPng で広告する Prefix	RIPng で広告するプレフィックスを設定します。	IPv6 プレフィックス形式	省略不可

この設定を行わない場合

スタティック情報はありません。
redistribute コマンドの指定および学習した RIPng 情報のみを、RIPng で広告します。

設定モード

RIPng サービス設定モード

router ripng

RIPng サービス設定モードへ移行します。RIPng の各種設定を行ないます。

設定例 1　RIPng サービス設定モードに移行する

```
Router(config)# router ripng
Router(config-ripng)#
```

コマンド書式

router ripng

パラメータ

パラメータはありません。

この設定を行わない場合

RIPng を使用できません。

設定モード

基本設定モード

timers basic

RIPng に関する以下のタイマ値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　定期送信間隔（30 秒）、経路情報を削除するまでの時間（180 秒）、経路情報を一時到達不能にするまでの時間（120 秒）とする

```
Router(config)#router ripng
Router(config-ripng)#timers basic 30 180 120
```

コマンド書式

timers basic〈定期送信間隔〉〈経路情報を削除するまでの時間〉〈経路情報を一時到達不能にするまでの時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
定期送信間隔	RIP の定期送信間隔(単位:秒)を指定します。	5～2147483647	省略不可
経路情報を削除するまでの時間	経路情報を削除するまでの時間(単位:秒)を設定します。	5～2147483647	省略不可
経路情報を一時到達不能にするまでの時間	経路情報を一時到達不能にするまでの時間(単位:秒)を設定します。	5～2147483647	省略不可

この設定を行わない場合

タイマの内容	デフォルト値
定期送信間隔	30
経路情報を削除するまでの時間	180
経路情報を一時到達不能にするまでの時間	120

設定モード

RIPng サービス設定モード

フィルタリングの設定

access-list

特定のパケットと、そのパケットの動作（中継 or 廃棄 or 学習フィルタリング）を指定します。
指定したパケットは、以下の機能で使用します。
・フィルタリング（ip access-group コマンド）
・学習フィルタリング（ip access-group コマンド）
・オフセットリスト（offset-list コマンド）
・RIP/BGP で送信するメトリック値の指定（distance コマンド）
・BGP で送信する経路の指定（neighbor <IP-address> distribute-list コマンド）
・経路情報の指定（match ip address コマンド）
・NextHop の指定（match ip nexthop コマンド）
・NAT 変換前のアドレス指定（ip nat inside コマンド）
・ポリシールーティング（match ip access-group コマンド）

使用方法は、まず本コマンドでパケットを指定した後、上記機能を使用するモードで、
指定したアクセスリスト番号を指定します。
access-list は、番号順に適用されます。
また、同じ番号の access-list に複数行の設定をした場合は、上の行から適用されます。

refresh コマンド後に有効になるコマンドです。

アクセスリスト番号について

本装置のアクセスリスト番号は、以下の規定があります。

アクセスリスト番号	名称	設定内容
1～99、1300～1999 10000～11200	IPv4 標準設定	IPv4 送信元アドレス指定
100～199、2000～2699 20000～21199	IPv4 拡張設定	IPv4 送信元／宛先アドレス指定 プロトコル番号指定 送信元／宛先ポート番号指定
3000～3499 30000～31499	IPv6 標準設定	IPv6 送信元／宛先アドレス指定
3500～3999 35000～36499	IPv6 拡張設定	IPv6 送信元アドレス指定 プロトコル番号指定 送信元／宛先ポート番号指定

指定パケットの動作指定について

指定したパケットを中継対象とするか、廃棄対象とするかを指定します。中継対象とする場合は permit、廃棄対象とする場合は deny を指定します。
この指定が必要なのは、フィルタリング／経路情報の指定／NextHop の指定のためにアクセスリストを指定する場合のみです。他の用途で指定する場合は permit を指定してください。

IP アドレス範囲指定

アクセスリストコマンドで IPv4 アドレスを指定する場合、マスク(Wildcard マスク)を使用して 1 エントリでアドレス範囲を指定することができます。
Wildcard マスクは、サブネットマスクとは書式が異なりますので注意してください。Wildcard マスクとサブネットマスクは、"1"と"0"の判別が逆になります。
例1)24bit マスクを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
Wildcard マスクの場合:0.0.0.255
サブネットマスクの場合:255.255.255.0
例2)ホストを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
Wildcard マスクの場合:0.0.0.0
サブネットマスクの場合:255.255.255.255

ポート番号の指定

IPv4/IPv6 拡張設定では、TCP/UDP 上位ポート番号を指定することができます。この指定は、フィルタリング/学習フィルタリングの指定のためにアクセスリストを指定する場合に効果があります。他の用途で指定する場合は、標準設定でアクセスリストを指定してください。

学習フィルタリング

インターネットの常時接続で使用する場合、セキュリティとしては危険な状態に常にさらされています。
学習フィルタリング機能では、LAN 側からのインターネット接続に対する応答データ以外はフィルタリング(廃棄)することができます。
学習フィルタリング機能を使用する場合は、外部からのアクセス(Web 等)はできなくなります。(アクセスを許可するアドレスを限定することはできます)
ただし、VPN からの受信に関してはフィルタリングを行いません。(ルートベースの VPN を除く)

本装置で、学習フィルタリングを使用する場合は、access-list コマンドの属性で、"dynamic"を指定します。

設定例 1　IPv4 標準アクセスリストに、192.168.100.0/24 を設定する (許可属性)

```
Router(config)# access-list 1 permit 192.168.100.0 0.0.0.255
```

設定例 2　IPv4 拡張アクセスリストに、src=192.168.100.0/24 dst=192.168.200.0/24 を設定する (不許可属性)

```
Router(config)# access-list 100 deny ip 192.168.100.0 0.0.0.255 192.168.200.0
0.0.0.255
```

設定例 3　IPv6 標準アクセスリストに、src=3ffe:110::/64 を dst=3ffe:111::/64 を設定する (許可属性)

```
Router(config)# access-list 3000 permit 3ffe:110::/64 3ffe:111::/64
```

設定例４　IPv6 拡張アクセスリストに、src=any srcport=any dst=any dstport=80 を設定する（不許可属性）

```
Router(config)# access-list 3500 deny tcp any gt 0 any eq 80
```

設定例５　学習フィルタリングを指定する（IPv4）

```
Router(config)# access-list 100 dynamic permit ip any any
```

設定例６　宛先が fnsc.co.jp 宛のポリシールーティング(ipsecif1 経由)を設定する

```
Router(config)#fqdn-list 1 www.fnsc.co.jp
Router(config)#access-list 100 permit ip any fqdn-list 1

Router(config)#class-map FNSC
Router(config-class-map)#match ip access-group 100
Router(config-class-map)#exit

Router(config)#action-map ipsecif1
Router(config-action-map)#set ip next-hop connected ipsecif 1
Router(config-action-map)#exit

Router(config)#policy-map FNSC
Router(config-policy-map)#class FNSC action ipsecif1
Router(config-policy-map)#exit

Router(config)#interface lan 1
Router(config-if lan 1)#service-policy input FNSC
Router(config-if lan 1)#exit
```

コマンド書式

IPv4 標準アクセスリスト（番号：1～99、1300～1999、10000-11200）
access-list <access-list 番号> { permit | deny } { any | <送信元 IP アドレス> <送信元 Wildcard マスク> }[log][count]

IPv4 拡張アクセスリスト（番号：100～199、2000～2699、20000～21199）
access-list <access-list 番号> { [dynamic] permit | deny } <プロトコル番号> { any | host <送信元 IP アドレス> | <送信元 IP アドレス> <送信元 Wildcard マスク> } [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] { any | host <宛先 IP アドレス> | <宛先 IP アドレス> <宛先 Wildcard マスク> | fqdn-list <fqdn-list 番号> } [ICMP タイプ] [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] [[precedence

{<precedence-value>|<precedence-named-value>}] [tos {<tos-value>|<tos-named-value>}]| [dscp {<dscp-value>|<dscp-named-value>}]] [ip-flag {<ip-flag-value>|<ip-flag-value:wildcard mask>}][log] [count]

IPv6 標準アクセスリスト（番号：3000～3499、30000～31499）
access-list <access-list 番号> { permit | deny } { any | <送信元 IPv6 プレフィックス> } { any | <宛先 IPv6 プレフィックス> } [count]

IPv6 拡張アクセスリスト（番号：3500～3999、35000～36499）
access-list <access-list 番号> { [dynamic] permit | deny } <プロトコル番号> { any | <送信元 IPv6 プレフィックス> } [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] { any | <宛先 IPv6 プレフィックス> | fqdn-list <fqdn-list 番号>} [ICMPv6 タイプ] [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] [tcp-flag {<tcp-flag-value>|<tcpflag-value:wildcard-mask>}] [traffic-class <traffic-class-value>|dscp {<dscp-level>|<dscp-name>}] [flow-label <flow-label-value>][count]

パラメータ

パラメータ	設定内容	設定範囲		省略時の値
access-list 番号	それぞれの属性の番号を指定します。	1～99、1300～1999 10000～11200	IPv4 標準アクセスリスト	省略不可
		100～199、2000～2699, 20000～21199	IPv4 拡張アクセスリスト	
		3000～3499 30000～31499	IPv6 標準アクセスリスト	
		3500～3999 35000～36499	IPv6 拡張アクセスリスト	
dynamic	学習フィルタリングを使用する場合に指定します。	dynamic		学習フィルタリングのエントリではない
{ permit | deny }	許可属性か、不許可属性かを選択します。	permit	許可属性	省略不可
		deny	不許可属性	
プロトコル番号	プロトコル名もしくはプロトコル番号を選択します。	esp	ESP	省略不可
		gre	Cisco's GRE	

		tunneling icmp：ICMP（IPv4 拡張アクセスリスト時） icmpv6：ICMPv6（IPv6 拡張アクセスリスト時） ip：IP ipinip：IP トンネル tcp：TCP udp：UDP 0～255：プロトコル番号を指定	
any	各パラメータ（アドレスやポート番号など）で、「全て」を指定する場合は"any"を入力します。	any	–
送信元 IP アドレス	送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
送信元 Wildcard マスク	送信元アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
宛先 IP アドレス	宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
宛先 Wildcard マスク	宛先アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
fqdn-list※2	fqdn-list を指定します。	1～50※3	省略不可
host	IPv4 拡張アクセスリストで、送信元/宛先アドレスとしてホストアドレスを指定する場合につけます。	host	–
送信元 IPv6 プレフィックス	送信元 IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可
宛先 IPv6 プレフィックス	宛先 IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可
ICMP タイプ	プロトコル番号で"icmp"を指定した場合に、対象とする ICMP タイプを指定します。	**指定できる ICMP タイプ** administratively-prohibited alternate-address conversion-error dod-host-prohibited dod-net-prohibited	全ての ICMP タイプ

		echo echo-reply general-parameter-problem host-isolated host-precedence-unreachable host-redirect host-tos-redirect host-tos-unreachable host-unknown host-unreachable information-reply information-request mask-reply mask-request mobile-redirect net-redirect net-tos-redirect net-tos-unreachable net-unreachable network-unknown no-room-for-option option-missing packet-too-big parameter-problem port-unreachable precedence-unreachable protocol-unreachable reassembly-timeout redirect router-advertisement router-solicitation source-quench source-route-failed time-exceeded timestamp-reply	

		timestamp-request traceroute ttl-exceeded unreachable ICMP タイプ値(0～255)	
ICMPv6 タイプ(IPv6)	プロトコル番号で"icmpv6"を指定した場合に、対象とする ICMPv6 タイプを指定します。	**ICMPv6 タイプ** address-unreachable administratively-prohibited dest-unreachable echo-reply echo-request erroneous-header-field hop-limit-exceeded-in-transit multicast-listener-done multicast-listener-query multicast-listener-report neighbor-advertisement neighbor-solicitation no-route-to-destination packet-too-big parameter-problem port-unreachable reassembly-time-exceeded redirect router-advertisement router-solicitation time-exceeded unrecognized-next-header unrecognized-option ICMPv6 タイプ値(0～255)	全ての ICMPv6 タイプ
ポート属性	ポート番号を範囲で指定するために、ポート属性を指定します。	eq　指定するポートが対象	全てのポート(以降設定な

		gt：指定するポート番号より大きいポート番号が対象 lt：指定するポート番号より小さいポート番号が対象 neq：指定するポート番号以外のポート番号が対象 range：ポートの範囲を指定する	し）
TCP ポート番号	プロトコルで"tcp"を指定した場合に、対象とする TCP ポート番号を指定します。	**TCP ポート番号** bgp chargen cmd daytime discard domain echo exec finger ftp ftp-data gopher hostname ident irc klogin kshell login lpd nntp pim-auto-rp pop2 pop3 smtp sunrpc syslog	全ての TCP ポート番号

		tacacs tacacs-ds talk telnet time uucp whois www TCP ポート番号（0～65535）	
UDP ポート番号	プロトコルで"udp"を指定した場合に、対象とする UDP ポート番号を指定します。	**UDP ポート番号** biff bootpc bootps discard dnsix domain echo isakmp mobile-ip nameserver netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip snmp snmptrap sunrpc syslog tacacs tacacs-ds talk tftp time	全ての UDP ポート番号

		who xdmcp UDP ポート番号(0～65535)	
precedence-value※1	precedence-value を設定します。	0～7	省略不可
precedence-named-value※1	precedence-named-value を設定します。	routine(0) priority(1) immediate(2) flash(3) flash-override(4) critical(5) internet(6) network(7)	省略不可
tos-value※1	tos-value を設定します。	0～15	省略不可
tos-named-value※1	tos-named-value を設定します。	min-momentary-cost(1) max-reliability(2) max-throughput(4) min-delay(8) normal(0)	省略不可
dscp-value※1	dscp-value を設定します。	0～63	省略不可
dscp-named-value※1	dscp-named-value を設定します。	ef(101110b) bf(000000b) af11(001010b) af12(001100b) af13(001110b) af21(010010b) af22(010100b) f23(010110b) af31(011010b) af32(011100b) af33(011110b) af41(100010b) af42(100100b) af43(100110b)	省略不可
ip-flag-value※1	ip-flag-value を設定します。	0～3、もしくは、0～3:0～3	省略不可

		(ワイルドカードマスク)	
tcp-flag-value※1	tcp-flag-value を設定します。	0～63、もしくは、0～63:0～63(ワイルドカードマスク)	省略不可
traffic-class-value	traffic-class-value を設定します。	0～255、もしくは、0～255:0～255(ワイルドカードマスク)	省略不可
flow-label	flow-label を設定します。	0～1048575	省略不可
log	パケットフィルタリング機能において該当条件(行単位)にヒットしたパケットが、フィルタリングログに記録されます。 ※dynamic 指定の場合、学習した学習フィルタにヒットしたパケットは記録しません。	log	フィルタリングログを記録しません。
count	統計情報としてフィルタにヒットしたパケット数、バイト数を表示します。 ※dynamic 指定の場合、学習した学習フィルタにヒットしたパケットは記録しません。	count	カウントを行いません。

※1 これらのパラメータをフィルタリングで使用する事はできません。
※2 パラメータ fqdn-list は、V1.02(00)以降サポート
※3 パラメータ fqdn-list 番号の設定範囲 1～50 は、V01.04(00)以降サポート

この設定を行わない場合

access-list を使用した機能を使用できません。

設定モード

基本設定モード

ipv6 access-group

access-list コマンドで指定したフィルタリングデータを、各インタフェースで適用します。
フィルタリングデータは、各インタフェースで受信したパケットに適用するのか、各インタフェースに送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　access-list 3001 で指定したデータを、PPPoE1 送信時に適用する

```
Router(config)#interface pppoe 1
Router(config-if lan 1)#ipv6 access-group 3001 out
```

設定例２　access-list 3002 で指定したデータを、PPPoE1 からの受信時に適用する

```
Router(config)#interface pppoe 1
Router(config-if lan 1)#ipv6 access-group 3002 in
```

コマンド書式

ipv6 access-group <access-list 番号> { in | out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	フィルタリングのデータを設定したアクセスリストの番号を指定します。	3000～3499 3500～3999 30000～31499 35000～36499	省略不可
{in | out}	インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。	in out	省略不可

この設定を行わない場合

該当インタフェースでは、IP パケットフィルタリングを使用しません。

IP フィルタリングについて

指定したパケット以外は中継しないといったように、セキュリティ強化のため使用する機能です。

設定モード

PPPoE インタフェース設定モード
LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
トンネルインタフェース設定モード

ip stateful max-sessions

学習フィルタリングテーブルの総数を設定します。
ここで設定する総数は、IPv4/IPv6 で使用する学習フィルタリングテーブルの総数となります。
NAT を併用している場合、NAT 変換テーブルのセッション数も併せて拡張してください。

設定例　学習フィルタリングテーブルを 16384 セッション分設定する

```
Router(config)#ip stateful max-sessions 16384
```

コマンド書式

ip stateful max-sessions〈セッション数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セッション数	学習フィルタリングテーブルの最大数を設定します。	2048～65535	省略不可

この設定を行わない場合

学習フィルタリングテーブルの最大数は、2048 になります。

設定モード

基本設定モード

スタティックルーティングの設定

ipv6 route

本装置の、IPv6 スタティックルートを指定します。
PPPoE や EWAN 使用する場合は、Nexthop の IP アドレスが分からないケースがありますので、Nexthop としてインタフェースを指定することもできます。
Nexthop に IPv6 アドレス(インタフェースではない)を指定した場合は、その宛先へのメトリック値を指定することができます。
デフォルトルートを指定する場合、宛先には”::0/0 ”を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　2001:db8::/32 宛の Nexthop を 2001:db8::1 とする場合（メトリックは指定しない）

```
Router(config)#ipv6 route 2001:db8::/32 2001:db8::1
```

設定例２　2001:db8::/32 宛の Nexthop を、PPPoE1 インタフェースとする場合

```
Router(config)#ipv6 route 2001:db8::/32 pppoe 1
```

設定例３　デフォルトルートを PPPoE１インタフェースとする場合

```
Router(config)#ipv6 route ::0/0 pppoe 1
```

設定例４　RA を送信するルータを nexthop に指定する場合

```
Router(config)#ipv6 route 0::/0  ewan 1
```

RA を送信するルータが複数存在した場合、それらを「RA 送信ルータリスト」として登録します。
RA 送信ルータリストとは、インタフェースあたり3件まで登録することができます。

設定例５　Nexthop をリンクローカルアドレスで指定する場合

```
Router(config)#ipv6 route 0::/0 fe80:3::1 ewan 1
```

コマンド書式

ipv6 route <宛先プレフィックス>{<NextHop>[<インタフェース名※1>]|<インタフェース名※2>}
[<distance>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先プレフィックス	スタティックルーティングの宛先 IPv6 プレフィックス	IPv6 アドレス形式	省略不可
NextHop	宛先へ到達するための NextHop の IPv6 アドレス	IPv6 アドレス形式	省略不可
インタフェース名※1	NextHop にリンクローカルアドレスを指定した場合に、その GW がどのインタフェースに存在するかの指定となります。	lan 1 ewan 1～2 pppoe 1～24 vlanif 1～150 dialer 1～20	–
インタフェース名※2	宛先へ到達するためのインタフェースとして指定します。 PPPoE のように、NextHop の IP アドレスが明確にわからない場合や、複数 RA を送信するルータが存在する場合に指定します。	lan 1 ewan 1～2 pppoe 1～24 vlanif 1～150 tunnel 1～2000	省略不可
distance	スタティックルーティングの distance 値を指定します。	2～255※	1

最大エントリ数：30000 エントリ（ルーティングテーブル自体は 60000 エントリ）
※ distance 値に 255 を設定した場合、その経路情報は無効扱いとなります。

この設定を行わない場合

スタティックルーティングは設定されません。

設定モード

基本設定モード

MTU 長の設定

ipv6 mtu

インタフェースの MTU 長を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　LAN の MTU 長を 1400byte にする

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 mtu 1400
```

コマンド書式

ipv6 mtu <MTU 長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MTU 長	MTU 長を指定します。	lan 1280～1500 pppoe 1280～1492 ewan 1280～1500 vlan 1280～1500 tunnel 1280～1500	省略不可

この設定を行わない場合

各インタフェースにより以下のようになります。通常は変更の必要はありません。

LAN：1500
PPPoE：1454
EWAN：1454
VLAN：1500
Tunnel：1460

MTU 長とは？

MTU とは（Max Transfer Unit）の略で、MTU 長とは、通常、1 パケットで運ぶことができる IP パケット（IP ヘッダ＋IP ペイロード）の長さをいいます。

設定モード

LAN インタフェース設定モード
PPPoE インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード

ipv6 mtu-receive-enable

設定しているインタフェースで、受信した RA の MTU オプションで指定されている MTU 値を有効とする場合に指定します。
有効とした場合、受信した MTU 長と、設定された MTU 長を比較し、小さい値を実際のインタフェースの MTU 長とします。
本設定を行う場合は、ipv6 nd receive-ra コマンドの設定が必要です。

設定例 1　EWAN1 インタフェースで、受信した RA の MTU オプションで指定されている MTU 値を有効とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# ipv6 mtu-receive-enable
```

コマンド書式

ipv6 mtu-receive-enable

パラメータ

パラメータはありません。

この設定を行わない場合

ipv6 mtu コマンドの設定に従います。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ポリシールーティング

クラスマップの定義

class-map

クラスマップモードに移行し、トラフィックを分類するクラシファイアを定義します。
クラスマップモードでは、match ip もしくは、match ipv6 コマンドによってトラフィックの分類条件が設定されます。
複数の条件が設定された場合、match-any の有無によって、複数の条件が OR 条件となるか、AND 条件となるかが指定されます。
IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合は、指定された条件は無視されるのではなく、不成立と判定されます。

設定例 1　クラスマップ設定モードへ移行する

```
Router(config)#class-map video-class
Router(config-class-map)#
```

コマンド書式

class-map <クラスマップ名 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クラスマップ名	クラスマップ名称を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップ名によるトラフィックの分類を行いません。

設定モード

基本設定モード

match-any

同一 class-map 内で複数の match 行が記述された場合の動作を指定します。
いずれか 1 つの match 行にマッチした場合に class-map に適合したと判断します。

refresh コマンド後に有効になるコマンドです。

設定例 1　IP アクセスリストの 100 番もしくは 101 番にマッチするトラフィックを対象とする

```
Router(config)# class-map video-class
Router(config-class-map)# match-any
Router(config-class-map)# match ip access-group 100
Router(config-class-map)# match ip access-group 101
Router(config-class-map)# exit
```

コマンド書式

```
match-any
```

パラメータ

パラメータはありません

この設定を行わない場合

全ての match 行にマッチした場合に、クラスマップに適合したと判断します。

例として、設定例 1 で match-any を指定しなかった場合は以下のようになります。

```
Router(config)# class-map video-class
Router(config-class-map)# match ip access-group 100
Router(config-class-map)# match ip access-group 101
Router(config-class-map)# exit
```

この場合、IP アクセスリストの 100 番にマッチ、かつ 101 番にマッチするトラフィックを対象とします。

設定モード

クラスマップ設定モード

match ip/ipv6 access-group

クラスマップ内でマッチするトラフィックを、IP アクセスリストにより設定します。
トラフィックが IPv4 パケットの場合、match ipv6 コマンドは不成立となります。逆にトラフィックが IPv6 パケットの場合、match ip コマンドは不成立となります。
複数の match が定義された場合、定義された順に評価されます。
同一 class-map において match-any が指定されている場合には、いずれの match 行にもトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
match-any が指定されていない場合には、いずれかの match 行にトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
アクセスリストの log と count は無視されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　IP アクセスリストの 2000 番をマッチするトラフィックとして設定する

```
Router(config)#class-map video-class
Router(config-class-map)#match-any
Router(config-class-map)#match ip access-group 2000
Router(config-class-map)#exit
```

コマンド書式

match ip access-group <ext-ipv4 アクセスリスト番号 > [input-interface {<インタフェース名> [port <ポート番号>}]
match ipv6 access-group <ext-ipv6 アクセスリスト番号 > [input-interface {<インタフェース名> [port <ポート番号>]}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ext-ipv4 アクセスリスト番号	クラスマップ内でマッチするトラフィックを ext-ipv4 アクセスリスト番号で指定します。	100～199 2000～2699 20000～21199	省略不可
ext-ipv6 アクセスリスト番号	クラスマップ内でマッチするトラフィックを ext-ipv6 アクセスリスト番号で指定します。	3500～3999 35000～36499	省略不可
インタフェース名	クラスマップ内でマッチするトラフィックを入力インタフェースで指定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 ipsecif 1～2000 tunnel 1～2000 vlanif 1～150	全てのインタフェース
ポート番号	LAN インタフェースの物理ポート番号を指定します。	port 1～8	LAN インタフェースの

			ポート番号

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません

設定モード

クラスマップ設定モード

match ip/ipv6 input-interface

クラスマップ内でマッチするトラフィックを、入力インタフェースにより設定します。
トラフィックが IPv4 パケットの場合、match ipv6 コマンドは不成立となります。逆にトラフィックが IPv6 パケットの場合、match ip コマンドは不成立となります。
複数の match が定義された場合、定義された順に評価されます。同一 class-map において match-any が指定されている場合には、いずれの match 行にもトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
match-any が指定されていない場合には、いずれかの match 行にトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
refresh コマンド後に有効になるコマンドです。

設定例 1　トラフィックを分類するインタフェースを EWAN 1 として設定する

```
Router(config)#class-map video-class
Router(config-class-map)#match-any
Router(config-class-map)#match ip input-interface ewan 1
Router(config-class-map)#exit
```

コマンド書式

```
match ip input-interface <インタフェース名> [port <ポート番号>]
match ipv6 input-interface <インタフェース名> [port <ポート番号>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	クラスマップ内でマッチするトラフィックを入力インタフェースで指定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 ipsecif 1～2000 tunnel 1～2000 vlanif 1～150	全てのインタフェース
ポート番号	LAN インタフェースの物理ポート番号を指定します。	port 1～8	LAN インタフェースのポート番号

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません

設定モード

クラスマップ設定モード

match policy-flag

QoS 変更用のフラグがセットされている、もしくはセットされていない場合の class として動作します。
イベントアクションからの通知が 1 度もない状態では、ポリシーフラグを OFF として扱います。

refresh コマンド後に有効になるコマンドです。

設定例 1　QoS 変更用フラグの class を POLI1-FLAG とする。

```
Router(config)# class-map video-class
Router(config-class-map)# match policy-flag POLI1-FLAG set
Router(config-class-map)# exit
```

コマンド書式

match policy-flag <ポリシーフラグ名> {set|unset}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシーフラグ名	QoS 変更用フラグの class を指定します。	最大 64 文字	省略不可
set|unset	QoS 変更用フラグがセットされているもしくは、されていない場合を対象とします。 set：ポリシーフラグがセットされている場合に適用 unset：ポリシーフラグがセットされていない場合に適用	set unset	省略不可

この設定を行わない場合

設定を行っていない場合は、このフラグの情報はクラスわけの情報として使用しません。

設定モード

クラスマップ設定モード

アクションマップの定義

action-map

action-map モードに移行し、トラフィックに対するアクションを定義します。
実行場所によってサポートされないアクションや、IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合、指定されたアクションは無視されます。

設定例１　アクションマップ設定モードへ移行する

```
Router(config)#action-map stream-action
Router(config-action-map)#
```

コマンド書式

action-map〈アクションマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクションマップ名	アクションマップ名を設定します	16 文字以内の文字列	省略不可

この設定を行わない場合

アクションは定義されません。

設定モード

基本設定モード

set ipv6 next-hop

アクションとして、パケット中継先を設定します(ポリシールーティング)。
有効な中継先のうち、distance 値がもっとも小さい中継先が有効になります。
有効な中継先のうち、もっとも distance 値が小さい中継先が同一 distance 値で複数存在する場合、config 表示で最も上の設定が適用されます。
distance 値が省略された場合のデフォルトは"1"とします。
中継先が到達不能な場合、その経路は無視されます。
個々の中継先が全て到達不能な場合、もしくは指定されていない場合、set {ip|ipv6}next-hop default が指定されている場合には、通常のルーティングが行なわれます。指定されていない場合には、パケットは中継不能パケットとして廃棄されます。
パケットが IPv4 の場合、set ipv6 は無視されます。逆にパケットが IPv6 の場合、set ip は無視されます。
本コマンドは、I/F 受信時のサービスポリシーとして設定された場合と、自局送信時のサービスポリシーとして設定された場合にのみ有効となり、I/F 送信時のサービスポリシーとして設定された場合には無視されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　パケット中継先を 2001:db8::1 に distance 10 で設定する

```
Router(config)#action-map stream-action
Router(config-action-map)#set ipv6 next-hop 2001:db8::1 distance 10
```

コマンド書式

```
set ipv6 next-hop <IP アドレス> [インタフェース※1][distance (1-255)]
set ipv6 next-hop <インタフェース※2> [distance (1-255)]
set ipv6 next-hop default
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	中継先の IP アドレスを設定します。	IPv6 アドレス形式	省略不可
インタフェース※1	中継先インタフェースを指定します。 NextHop にリンクローカルアドレスを設定した場合は、インタフェースの指定が必須となります。	lan 1 ewan 1～2 pppoe 1～24 vlanif 1～150	—
インタフェース※2	PPPoE インタフェースのように、宛先へ到達するための NextHop の IP アドレスが明確に分からない場合に設定します。	pppoe 1～24 tunnel 1～2000	省略不可
distance	中継先の distance 値を設定します。	1～255	1
default	ポリシールーティングを行わずに、通常のルーティングをおこないます。	なし	省略不可

この設定を行わない場合

中継先設定は行なわれません。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

アクションマップ設定モード

ポリシーマップの定義

class

クラスマップとアクションとを対応付け、クラシフィケーションされたトラフィックに対するアクションを定義します。
複数のクラスが定義された場合、登録順に検索され、最初にマッチしたクラスに対するアクションのみが実行されます。
同一クラスマップ名に対しては、一つのアクションのみ記述できます(同一クラスマップ名に対しては、置換型となります)。

refresh コマンド後に有効になるコマンドです。

設定例 1　クラスマップ（video-class）とアクションマップ（stream-action）を対応づける

```
Router(config)# policy-map stream-service
Router(config-policy-map)# class video-class action stream-action
Router(config-policy-map)# class audio-class action stream-action
Router(config-policy-map)# exit
```

コマンド書式

class〈クラスマップ名〉action〈アクションマップ名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クラスマップ名	対応づけるクラスマップ名を設定します。	16 文字以内の文字列	省略不可
アクションマップ名	対応づけるアクションマップ名を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップとアクションとの対応は定義されません。

設定モード

ポリシーマップ設定モード

policy-map

policy-map モードに移行し、クラスマップによって分類したトラフィックに対して、どのような制御を行なうかを定義します。
ここで指定したポリシーマップを有効にするには、各インタフェース設定モードで、"service-policy input/output"コマンドで登録します。
また、自局送信をポリシールーティングする場合は、"service-policy local"コマンドで登録します。

設定例１　ポリシーマップ設定モードへ移行する

```
Router(config)#policy-map stream-service
Router(config-policy-map)#
```

コマンド書式

policy-map 〈ポリシーマップ名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシーマップ名	ポリシーマップ名を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

ポリシーマップの設定を行うことができません。

設定モード

基本設定モード

statistics update

統計情報のカウントを行うかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　統計情報のカウントを行う

```
Router(config)# policy-map stream-service
Router(config-policy-map)# statistics update enable
Router(config-policy-map)# exit
```

コマンド書式

statistics update〈カウント設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
カウント設定	統計情報のカウントを行うかどうかを指定します。 enable　統計情報のカウントを行う disable　統計情報のカウントを行わない	enable disable	省略不可

この設定を行わない場合

統計情報のカウントを行いません。

設定モード

ポリシーマップ設定モード

ポリシールーティング時の NextHop 監視

ipv6 polling-interval

ポリシールーティング時に有効な中継先かどうかを判断するために、指定された中継先に対して監視パケットを送信する際の Ipv6 監視パケット(Neighbor Solicit)の送信間隔を指定します。
ARP またはネイバのキャシュテーブルの参照を行い、IPv6 では状態が ND6_LLINFO_REACHABLE、ND6_LLINFO_STALE、ND6_LLINFO_DELAY、及び ND6_LLINFO_PROBE である場合に有効であると判定されます。
それ以外は、有効でないと判定されます。
有効である場合、ポリシールーティング機能では、指定された中継先への到達性があると判定し、その中継先を有効な経路と認識します。有効でない場合は、set ip next hop コマンドで設定された次の候補の判定を行います。
定変更後のリフレッシュでは変更前の監視パケット送信後、変更された指定が有効となります。

refresh コマンド後に有効になるコマンドです。

設定例 1　監視パケットの送信間隔を 10 秒にする

```
Router(config)#ipv6 polling-interval 10
```

コマンド書式

ipv6 polling-interval [監視パケット送信間隔]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
監視パケット送信間隔	Ipv6 監視パケット(Neighbor Solicit)の送信間隔を指定します。	5～60	送信間隔を 5 秒に設定します。

この設定を行わない場合

監視パケットの送信間隔が 5 秒に設定されます。

設定モード

基本設定モード

ドメインルーティングの設定

fqdn-list

access-list から参照する fqdn-list を設定します。
fqdn-list では、アドレス解決したい FQDN を指定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　www.fnsc.co.jp を fqdn-list に設定する

```
Router(config)#fqdn-list 1 www.fnsc.co.jp
```

コマンド書式

fqdn-list <fqdn-list 番号> <FQDN>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
fqdn-list 番号	access-list と紐付ける fqdn-list の番号を指定します。	1～50※	省略不可
FQDN	アドレス解決したい FQDN を指定します。	最大 254 文字	省略不可

※ パラメータ fqdn-list 番号の設定範囲 1～50 は、V01.04(00)以降サポート

この設定を行わない場合

access-list で指定された fqdn-list の設定がなければ、該当 access-list の設定が無効になります。

設定モード

基本設定モード

fqdn-list lifetime

fqdn-list に登録された FQDN のアドレスが解決してから、該当アドレスをキャッシュとして保持する時間(単位:秒)を設定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　キャッシュ保持時間を 3600 秒に設定する

```
Router(config)# fqdn-list lifetime 3600
```

コマンド書式

fqdn-list lifetime <保持時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
保持時間	解決したアドレスを保持する時間(単位:秒)を指定します。	120～3600	180

この設定を行わない場合

180 秒となります。

設定モード

基本設定モード

fqdn-list query-interval

fqdn-list に登録された FQDN のアドレス解決を行う間隔(単位:秒)を設定します。
初回アドレス解決時に限り、本設定に関係なく解決するまで 10 回リトライを 10 秒間隔で行います。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　FQDN のアドレス解決を行う間隔を 90 秒に設定する

```
Router(config)# fqdn-list query-interval 90
```

コマンド書式

fqdn-list query-interval <アドレス解決間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレス解決間隔	FQDN の解決を行う間隔(単位:秒)を指定します。	60～90	60

この設定を行わない場合

60 秒間隔となります。

設定モード

基本設定モード

マルチキャストの設定

ipv6 mld fast-done

各インタフェースで、Fast Done を有効にするかどうかの設定をします。

refresh コマンド後に有効になるコマンドです。

設定例 1　Fast Done を有効にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 mld fast-done
```

コマンド書式

ipv6 mld fast-done

パラメータ

パラメータはありません。

この設定を行わない場合

Query に対して、Report メッセージがタイムアウトしてから、上流に対して Done メッセージを通知します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 mld group-membership-timeout

マルチキャストグループに参加するインタフェース情報の保持時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　保持時間を 1500 秒とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 mld group-membership-timeout 1500
```

コマンド書式

ipv6 mld group-membership-timeout <保持時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
保持時間	マルチキャストグループに参加するインタフェース情報の保持時間(単位:秒)を設定します。	30～65535	省略不可

この設定を行わない場合

保持時間を 260 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 mld last-listener-query-interval

各インタフェースで、Done 受信後の Group Specific Query に対応する MLD Report を受信するための待機時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　保持時間を 10 秒とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 mld last-listener-query-interval 10
```

設定例 2　保持時間を 500 ミリ秒とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 mld last-listener-query-interval dsec 5
```

コマンド書式

ipv6 mld last-listener-query-interval [dsec] <待機時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
待機時間	Done 受信後の Group Specific Query に対応する MLD Report を受信するための待機時間(単位:秒)を設定します。	1～25	省略不可
dsec	待機時間を 100 ミリ秒単位で設定する場合に指定します。	1～255	秒単位の設定になります。

この設定を行わない場合

保持時間を 1 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 mld limit

マルチキャストルーティングの設定しているインタフェースで、マルチキャストグループに参加するユーザ数の上限を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　マルチキャストグループに参加するユーザ数を 10 とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 mld limit 10
```

コマンド書式

ipv6 mld limit <上限値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
上限値	マルチキャストグループに参加するユーザ数の上限を設定します。	1～128	省略不可

この設定を行わない場合

マルチキャストグループに参加するユーザ数の上限を設定しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 mld mode

マルチキャストルーティングを行う際のフィルタモードの設定をします。

refresh コマンド後に有効になるコマンドです。

設定例 1　RFC3810 準拠の MLDv2 動作をおこなう

```
Router(config)#ipv6 mld mode normal
Router(config)#
```

コマンド書式

ipv6 mld mode <フィルタモード>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
フィルタモード	フィルタモードを選択します。 exclude-filter：downstream からの Exclude Join を無視します。 normal：RFC3810 準拠の MLDv2 動作をします。	exclude-filter normal	省略不可

この設定を行わない場合

exclude-filter モードで動作します。

設定モード

基本設定モード

ipv6 mld proxy upstream-forwarding

マルチキャストルーティングを行う際に、上流インタフェースへのトラフィック中継を許可するかどうかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　上流インタフェースへのトラフィック中継を許可する

```
Router(config)#ipv6 mld proxy upstream-forwarding
Router(config)#
```

コマンド書式

```
ipv6 mld proxy upstream-forwarding
```

パラメータ

パラメータはありません。

この設定を行わない場合

上流インタフェースへのトラフィックを中継しません。

設定モード

基本設定モード

ipv6 mld proxy-group

各インタフェースにおいてマルチキャストルーティングを行う際の、MLD Proxy の動作を有効とするグループアドレスをアクセスリスト番号で指定します。
複数設定された場合には、アクセスリスト番号順にソートされます。

refresh コマンド後に有効になるコマンドです。

設定例 1　アクセスリスト番号 3300 をグループアドレスとして指定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip mld proxy-group 3300
```

コマンド書式

ipv6 mld proxy-group〈アクセスリスト番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクセスリスト番号	グループアドレスを IPv6 標準アクセスリストの中から選択します。	3000～3499 30000～31499	省略不可

この設定を行わない場合

MLD Proxy によるマルチキャストルーティングを中継しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 mld proxy-group-upstream

装置全体としてマルチキャストルーティングを行う際の、MLD Proxy の動作を有効とするグループアドレスをアクセスリスト番号で指定します。
複数設定された場合には、アクセスリスト番号順にソートされます。
また、インタフェース設定モードと基本設定モードでアクセスリスト番号が重複する場合は、インタフェース設定モードが優先されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　アクセスリスト番号 3300 をグループアドレス、ewan 1 を上流インタフェースとして指定する

```
Router(config)#ipv6 mld proxy-group-upstream ewan 1 3300
Router(config)#
```

コマンド書式

ipv6 mld proxy-group-upstream <インタフェース名> <アクセスリスト番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	上流インタフェースに指定するインタフェースを選択します。	lan 1 ewan 1～2 vlanif 1～150	省略不可
アクセスリスト番号	グループアドレスを IPv6 標準アクセスリストの中から選択します。	3000～3499 30000～31499	省略不可

この設定を行わない場合

MLD Proxy によるマルチキャストルーティングを中継しません。

設定モード

基本設定モード

ipv6 mld querier-timeout

各インタフェースで、MLD Querier の生存タイマ時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　生存タイマ時間を 100 秒とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 mld querier-timeout 100
```

コマンド書式

ipv6 mld querier-timeout <生存タイマ時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
生存タイマ時間	MLD Querier の生存タイマ時間(単位:秒)を設定します。	60～300	省略不可

この設定を行わない場合

生存タイマ時間を 255 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 mld query-interval

各インタフェースで、MLD Query メッセージの送信間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　送信間隔を 100 秒とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 mld query-interval 100
```

コマンド書式

ipv6 mld query-interval 〈送信間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	MLD Querier メッセージの送信間隔(単位:秒)を設定します。	30～31744	省略不可

この設定を行わない場合

送信間隔を 125 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 mld query-max-response-time

各インタフェースで、MLD Querier 内に設定する最大応答待ち時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　最大応答時間を 10 秒とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 mld query-max-response-time 10
```

設定例 2　最大応答時間を 500 ミリ秒とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 mld query-max-response-time dsec 5
```

コマンド書式

ipv6 mld query-max-response-time [dsec] <最大応答待ち時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
最大応答待ち時間	MLD Query 内に設定する最大応答待ち時間(単位:秒)を設定します。	1～25	省略不可
dsec	最大応答待ち時間を 100 ミリ秒単位で設定する場合に指定します。	1～255	秒単位の設定になります。

この設定を行わない場合

最大応答時間を 10 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 mld static-group

各インタフェースで、静的に登録するマルチキャストグループを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　2001:db8::1 をマルチキャストグループに追加する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 mld static-group 2001:db8::1
```

コマンド書式

ipv6 mld static-group <グループアドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
グループアドレス	静的に登録するマルチキャストグループを設定します。	IPv6 アドレス形式	省略不可

この設定を行わない場合

マルチキャストグループを静的に登録しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 mld version

各インタフェースで、MLD Querier の動作バージョンを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　MLD Querier の動作バージョンを MLDv2 とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 mld version 2
```

コマンド書式

ipv6 mld version <動作バージョン>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
動作バージョン	MLD Querier の動作バージョンを設定します。 1：MLDv1 を指定します。受信した MLDv2 Report は廃棄します。 2：MLDv2 を指定します。MLDv1 Report を受信した場合、MLDv1-Compatible で動作します。	1 2	省略不可

この設定を行わない場合

MLD Querier の動作バージョンは、MLDv1 となります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ipv6 multicast-routing proxy

MLD Proxy によるマルチキャストルーティングを中継するかどうかの設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　MLD Proxy によるマルチキャストルーティングを中継する

```
Router(config)#ipv6 multicast-routing proxy
Router(config)#
```

コマンド書式

ipv6 multicast-routing proxy

パラメータ

パラメータはありません。

この設定を行わない場合

MLD Proxy によるマルチキャストルーティングを中継しません。

設定モード

基本設定モード

ECMP の設定

ip multi-path max-paths

ECMP で登録できる最大経路数を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　ECMP で登録できる最大経路数を２にする

```
Router(config)#ip multi-path max-paths 2
```

コマンド書式

ip multi-path max-paths〈経路数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
経路数	最大経路数を設定します。	1～2	省略不可

この設定を行わない場合

ECMP で登録できる最大経路数は1です。

設定モード

基本設定モード

IPv4 ルーティングの設定

IP アドレスの設定

ip address

インタフェースの IP アドレス、サブネットマスクを設定します。

refresh コマンド後に有効になるコマンドです。(IPsec インタフェースのみ対応)

設定例 1　PPPoE 1 の IP アドレスを 158. ｘｘｘ. ｘｘｘ. 1 に設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip address 158.xxx.xxx.1
```

設定例 2　EWAN 1 の IP アドレスを 158. ｘｘｘ. ｘｘｘ. 1、サブネットマスクを 255.255.255.0 に設定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip address 158.xxx.xxx.1 255.255.255.0
```

コマンド書式

ip address <IP アドレス> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	インタフェースに割り当てる IP アドレスを設定します。	IPv4 アドレス形式	省略不可
サブネットマスク	インタフェースに割り当てるサブネットマスク※を設定します。	IPv4 アドレス形式	省略不可

※PPPoE およびループバックインタフェースでは、サブネットマスクの指定はできません。トンネルインタフェースおよび IPsec インタフェースでは、unnumbered オプションの選択が可能です。詳細は ip address unnumbered を参照して下さい。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
IPsec インタフェース設定モード
ループバックインタフェース設定モード
トンネルインタフェース設定モード
BVI インタフェース設定モード

USB Ethernet インタフェース設定モード

ip address dhcp

EWAN、USB Ethernet インタフェースで、DHCP クライアント機能を使用する場合に指定します。
ADSL モデムで PPP を終端し EWAN 側に DHCP でアドレスを通知するようなケースや、CATV インターネット等 DHCP でアドレスを割り当てるプロバイダに契約している場合等は、このモードで使用することがあります。加入しているインターネットサービスに確認してください。

このモードの場合、DHCP サーバから「クライアント ID」もしくは「ホスト名」の指定を指示される場合があります。この場合は、コマンドのオプションとして指示された内容を設定してください。

設定例 1　EWAN インタフェースで DHCP クライアント機能を使用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip address dhcp
```

コマンド書式

```
ip address dhcp { client-id [{ascii | hex} <クライアント ID>] [[type <タイプ >]
                [hostname <ホスト名>]| [hostname <ホスト名>] ]|hostname<ホスト名>}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
{ ascii | hex} クライアント ID	クライアント ID を ASCII または、hex で指定します。 ascii：最大 63 文字(ASCII) hex：最大 126 桁(16 進数)	ascii hex	クライアント ID を付けない
タイプ	クライアント ID のタイプを指定します。	0～255	クライアント ID が ASCII の場合：0 クライアント ID が hex の場合：1
ホスト名	ホスト名を指定します。	最大 63 文字	ホスト名を付けない

この設定を行わない場合

DHCP クライアント機能を使用できません。

DHCP クライアント機能とは？

DHCP プロトコルを利用して、IP アドレス等の情報を割り当ててもらい、その内容にしたがって IP 通信を行なう機能を、DHCP クライアント機能といいます。
本装置は、LAN インタフェースで DHCP サーバ機能または DHCP リレーエージェント機能が使用でき、EWAN、USB Ethernet インタフェースで DHCP クライアント機能を使用できます。

設定モード

EWAN インタフェース設定モード
USB Ethernet インタフェース設定モード

ip address secondary

インタフェースの IP セカンダリアドレスを設定します。
1 つのインタフェースに複数のセカンダリアドレスを設定することができますが、セカンダリアドレスのみ設定されたインタフェースは使用できません。

設定例 1　EWAN 1 の IP セカンダリアドレスを 192.168.100.1 255.255.255.0 に設定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip address secondary 192.168.100.1 255.255.255.0
```

コマンド書式

ip address secondary <IP アドレス> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	インタフェースに割り当てる IP アドレスを設定します。	IPv4 アドレス形式	省略不可
サブネットマスク	インタフェースに割り当てるサブネットマスクを設定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

セカンダリアドレスを使用できません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

RIP に関する設定

default-information originate

自身をデフォルトルートとして、RIP で通知するかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　デフォルトルートの情報を RIP で送信する

```
Router(config)#router rip
Router(config-rip)#default-information originate
```

コマンド書式

```
default-information originate
```

パラメータ

パラメータはありません。

この設定を行わない場合

自身をデフォルトルートとしては通知しません。

注意

この設定は、デフォルトルートの情報を持っていないときに、RIP でデフォルトルートを通知するかどうかの設定です。
スタティック設定でデフォルトルートを設定していたり、ルーティングプロトコルによりデフォルトルートを学習していた場合は、この設定によらずデフォルトルートの情報を RIP で広告します。

設定モード

RIP サービス設定モード

default-metric

本装置で生成した経路情報(static の情報)を RIP で広告する際のメトリック値を設定します。ただし、デフォルトルートのメトリックについては、static 設定していたとしても"1"で広告します。

refresh コマンド後に有効になるコマンドです。

工場出荷時あるいは no default-metric を指定した場合は、1 が設定されます。

表示例 1　設定したスタティックルートの情報を RIP で広告する際は、メトリック値を 5 とする

```
Router(config)#router rip
Router(config-rip)#default-metric 5
```

コマンド書式

default-metric 〈メトリック値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
メトリック値	スタティックルートを RIP で広告する場合のメトリック値を設定します。	1～16	省略不可

この設定を行わない場合

メトリック値は、1 で動作します。

メトリックとは？

IP パケットが通過するルータの数をメトリックといいます。
RIP で広告するメトリック値とは、その経路に到達するために、どのくらいのルータを経由しなくてはならないかを規定しています。
IPv4 では、メトリック値は 1～15 までと決められており、16 は到達不能を意味します。

通常、ルータは IP パケットを中継した際に、IP ヘッダ内にあるメトリックフィールドの値を1加算します。このようにして、メトリック値が加算され、16 になったら廃棄されます。

設定モード

RIP サービス設定モード

distance

同じ宛先への経路情報が複数存在した場合、どの情報を有効にするかを決定するための優先度を設定します。
例えば、スタティックルーティングで設定した情報と、RIP で受信した経路情報で、同じ宛先の情報があった場合に、どちらを優先とするかどうかの決定に使用します。
特定の宛先に対して、distance 値(優先度)をいくつにするかの指定もできます。さらに、どのルータから受信した RIP を対象とするかの指定もできます(ルータの限定は access-list を使用します)。
distance 値は、値が小さいほど優先度が高くなります。

refresh コマンド後に有効になるコマンドです。

設定例１　RIP の distance 値を 10 に設定する

```
Router(config)#router rip
Router(config-rip)#distance 10
```

設定例２　192.168.0.0/24 の経路情報を RIP で受信した際の distance 値を 30 に設定する

```
Router(config)#router rip
Router(config-rip)#distance 30 192.168.0.0 255.255.255.0
```

設定例３　192.168.100.0/24 上のルータから受信した 192.168.0.0/24 の経路情報は distance 値を 100 とする

```
Router(config)#access-list 1 permit 192.168.100.0 255.255.255.0

Router(config)#router rip
Router(config-rip)#distance 30 192.168.0.0 255.255.255.0 1
```

コマンド書式

distance <distance 値> [<IP アドレス> <ネットマスク> <access-list 番号>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
distance 値	RIP の distance 値を指定します。	1～255	省略不可
IP アドレス	distance 値を設定する特定の宛先アドレスを指定します。	IPv4 アドレス形式	経路ごとの distance 値を指定しません。
ネットマスク	distance 値を設定するための、ネットマスク値を指定します。	IPv4 アドレス形式	
access-list 番号	distance 値を特定する、RIP 送信元ルータを指定します。	1～99 1300～1999 10000～11200	

この設定を行わない場合

distance 値は、110 で動作します。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

RIP サービス設定モード

distribute-list

RIP 送受信に対してフィルタリングの設定を行ないます。
プレフィックスのアドレス部分が access-list コマンドで permit にマッチする情報のみを受け入れる／受け入れない、または送信する／送信しないといった制御を行なうことができます。

また、フィルタリング制御を行なうためのインタフェースを指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.100.0/24 にマッチするプレフィックスのみを受け付ける

```
Router(config)#access-list 1 permit 192.168.100.0 0.0.0.255

Router(config)#router rip
Router(config-rip)# distribute-list 1 in
```

設定例２　192.168.100.0/24 にマッチするプレフィックスのみを送信しない

```
Router(config)#access-list 1 deny 192.168.100.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#router rip
Router(config-rip)# distribute-list 1 out
```

※上記の設定を行う場合は、必ず access-list コマンドで permit any を追加する必要があります。
permit any を追加しないと、全てのアクセスリストの送信をフィルタしてしまいます。

設定例３　192.168.100.0/24 にマッチするプレフィックスのみを、LAN からは受信しない

```
Router(config)#access-list 1 deny 192.168.100.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#router rip
Router(config-rip)# distribute-list 1 in lan 1
```

設定例４　デフォルトルート（0.0.0.0/0）にマッチするプレフィックスのみを受け付ける

```
Router(config)#access-list 1 permit 0.0.0.0 0.0.0.0
Router(config)#router rip
Router(config-rip)# distribute-list 1 in
```

コマンド書式

distribute-list <access-list 番号> { in | out } [インタフェース名]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	access-list コマンドで指定したリスト番号を指定します。	1～99 1300～1999 10000～11200	省略不可
in | out	受信(in)／送信(out)のどちらでフィルタするかを指定します※。	in out	省略不可
インタフェース名	適用するインタフェースのインタフェース名を指定します。	インタフェース名形式	全インタフェースで適用

rip distribute-list in,out 共に

- **access list (permit)で指定された経路情報のみを送受信の対象とします。**
- **permit 指定がない経路情報はすべてフィルタします。**

この設定を行わない場合

全てのプレフィックスを送受信します。

設定モード

RIP サービス設定モード

ip rip authentication key-chain

key chain 設定で設定した key-chain 名を指定し、インタフェースの RIP2 のパスワード制御を行ないます。
key chain 設定では、key フレーズ／key-chain が有効な時間帯を指定することができます。
この設定が異なるルータとは、RIP2 での経路交換を行なうことができません。

refresh コマンド後に有効になるコマンドです。

設定例 1　RIP2 の認証で使用する key に、"key-rip2"を使用する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip rip authentication key-chain key-rip2
```

コマンド書式

ip rip authentication key-chain <key-chain 名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
key-chain 名称	key chain コマンドで指定した key-chain 名称	-	省略不可

この設定を行わない場合

RIP2 の認証を行なうことはできません。

RIP2 とは？

RIP version 2 は、距離ベクタアルゴリズムをもつ、経路制御プロトコルです。
RIP version 1 とは、以下の点が異なります。
・送信する際の宛先アドレスがマルチキャスト(224.0.0.9)
・サブネットマスク情報を通知することができる
・NextHop を通知することができる
・認証データを通知することができ、認証データが異なるルータからの経路情報は有効としない。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
ダイヤラーインタフェース設定モード

ip rip authentication mode

インタフェースに RIP2 を送信する場合に、key chain 設定で定義した key フレーズをそのまま（Simple Text）で送信するか／md5 でハッシュ計算した後のデータ（Unrecognized Authentication Type）で送信するかを設定します。
そのまま送信する場合は"text"、ハッシュ計算した後のデータ（MD5 形式）で送信する場合は"md5"を指定します。
この設定が異なるルータとは、RIP2 での経路交換を行なうことができません。

refresh コマンド後に有効になるコマンドです。

設定例 1　RIP2 の認証データを MD5 形式とする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip rip authentication mode md5
```

コマンド書式

ip rip authentication mode <認証方式>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
認証方式	RIP2 で、パスワードを送る方式を選択します。 text　Simple Text で送信する md5　MD5 形式で送信する	text md5	省略不可

この設定を行わない場合

Simple Text で送信します。

RIP2 とは？

RIP version 2 は、距離ベクタアルゴリズムをもつ、経路制御プロトコルです。
RIP version 1 とは、以下の点が異なります。
・送信する際の宛先アドレスがマルチキャスト（224.0.0.9）
・サブネットマスク情報を通知することができる
・NextHop を通知することができる
・認証データを通知することができ、認証データが異なるルータからの経路情報は有効としない。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
ダイヤラーインタフェース設定モード

ip rip receive version

インタフェースの RIP 受信バージョン(1 or 2)を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　PPPoE1 で受信する RIP のバージョンを Version2 とする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip rip receive version 2
```

コマンド書式

ip rip receive version <受信バージョン>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
受信 バージョン	受信する RIP のバージョンを指定します。 V1/V2 の両方を受信する場合は、1 2 のように2つ指定します。	1 2	省略不可

この設定を行わない場合

version コマンドで指定したバージョンとなります。

RIP2 とは？

RIP version 2 は、距離ベクタアルゴリズムをもつ、経路制御プロトコルです。
RIP version 1 とは、以下の点が異なります。
・送信する際の宛先アドレスがマルチキャスト(224.0.0.9)
・サブネットマスク情報を通知することができる
・NextHop を通知することができる
・認証データを通知することができ、認証データが異なるルータからの経路情報は有効としない。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
VLAN インタフェース設定モード

ip rip send version

インタフェースの RIP 送信バージョン(1 or 2)を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　PPPoE1 で送信する RIP のバージョンを Version2 とする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip rip send version 2
```

コマンド書式

ip rip send version <送信バージョン>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信 バージョン	送信する RIP のバージョンを指定します。 V1/V2 の両方を送信する場合は、1 2 のように2つ指定します。	1 2	省略不可

この設定を行わない場合

version コマンドで指定したバージョンとなります。

RIP2 とは？

RIP version 2 は、距離ベクタアルゴリズムをもつ、経路制御プロトコルです。
RIP version 1 とは、以下の点が異なります。
・送信する際の宛先アドレスがマルチキャスト(224.0.0.9)
・サブネットマスク情報を通知することができる
・NextHop を通知することができる
・認証データを通知することができ、認証データが異なるルータからの経路情報は有効としない。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
VLAN インタフェース設定モード

ip split-horizon

インタフェースで Split-Horizon 制御を行なうかどうかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　PPPoE インタフェースで Split-Horizon 制御を行なう

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip split-horizon enable
```

コマンド書式

ip split-horizon <Split-Horizon 制御>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Split-Horizon 制御		enable disable	省略不可

この設定を行わない場合

Split-Horizon 制御を行います。

Split-horizon 制御とは？

RIP 送信制御の方法です。
受信した RIP の宛先情報を、RIP を受信したインタフェースに対して送信するかどうかを規定します。Split-Horizon 制御を行なう場合は、RIP を受信したインタフェースには送信しません。
Split-Horizon 制御を行なっていないルータがネットワーク上に存在する場合、RIP で送信した情報を同じインタフェースから受信するため、そのインタフェース側にも経路が存在すると判断され、実際に送信するインタフェースが使用不可となっても、そちら側のインタフェースに経路が存在すると考えられ、データを送信してしまいます。
この機能がない場合は、経路がなくなった場合の収束が遅くなる原因となります。

Split-Horizon の拡張機能で、Split-Horizon with Poison Reverse という機能があります。この機能は、Split-Horizon のように、RIP を受信したインタフェースに同じ宛先の情報をもつ RIP を送信しないのではなく、その宛先の情報のメトリックを 16（到達不能）として RIP を送信する機能です。この機能により、さらに誤動作が防止できます。
本装置は、Split-Horizon with Poison Reverse 機能をサポートしていません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
VLAN インタフェース設定モード

key <number> accept-lifetime

キーの受信時有効期限を設定します。
ここで設定した時間内であれば、RIP2 の認証キーを有効とします。<number>は、key <number> key-string コマンド、key <number> send-lifetime コマンドと連携する際の番号です。

refresh コマンド後に有効になるコマンドです。

設定例１　number=1 の受信時有効期限を"2014.4.1 12:00:00 - 2014.4.30 11:59:59"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 accept-lifetime 12:00:00 1 Apr 2014 11:59:59 30 Apr 2014
```

設定例２　number=1 の受信時有効期限を"2014.4.1 12:00:00 - 無限"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 accept-lifetime 12:00:00 1 Apr 2014 infinity
```

設定例３　number=1 の受信時有効期限を"2014.4.1 12:00:00 - 100 秒間"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 accept-lifetime 12:00:00 1 Apr 2014 duration 100
```

コマンド書式

key <key 番号> accept-lifetime <有効開始時刻> { <終了時刻> | duration <有効期間> | infinity }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
key 番号	key <number> key-string コマンド、key <number> send-lifetime コマンドと連携する際の番号を指定します。	0～2147483647	省略不可
有効開始時刻	認証キーが有効になる開始時刻を hh:mm:ss 日 月の順に設定します。	hh:mm:ss 日 月 年	省略不可
終了時刻	認証キーが無効になる終了時刻を、hh:mm:ss で設定します。	hh:mm:ss	3 種類のうちどれか 1 種類を指定する必要あり
有効期間	認証キーの有効期間(単位:秒)を指定します。	1～2147483646	
infinity	認証キーの有効期限を、無限とします。	infinity	

この設定を行わない場合

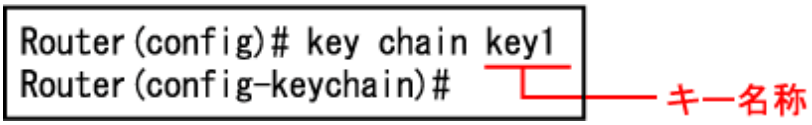
常に使用可能です。

設定モード

key-chain 設定モード

key chain

RIP2 の認証を有効にするための key-chain モードに移行します。
key-chain の設定は、キー名称を指定して行ないます。key-chain モードで、キーの情報を設定し、各インタフェースの RIP2 に関する設定で、使用するキー名称を指定します。



設定例 1　キー名称が"key1"である key-chain モードに移行する

```
Router(config)# key chain key1
Router(config-keychain)#
```

コマンド書式

key chain <キー名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キー名称	RIP2 で参照するキー(パスワード)の名称 インタフェース設定モードで参照する名称なので、わかりやすい名前にしてください。	-	省略不可

RIP2 の認証について

RIP2 では、認証キーによる認証を行い、信用できるルータからのルーティング情報であるかどうかを制御することができます。
この認証キーが異なる RIP2 の情報は、ルーティングテーブルに登録しません。

実際の RIP2 に付加される認証の情報には、以下の 2 種類があります。
・simple password （設定されたテキストの情報）
・MD5 digest （設定されたテキストから MD5 で計算されたデータ）
本装置で、RIP2 の認証を使用する場合は、RIP2 を使用するインタフェースのインタフェース設定モードの"ip rip authentication"コマンドで、key-chain で設定するキー名称を指定する形で設定します。

```
Router(config-if lan 1)#ip rip authentication key-chain key1
```

キー名称

設定モード

基本設定モード

key <number> key-string

キーワードの文字列を指定します。
<number>は、key <number> accept-lifetime コマンド、key <number> send-lifetime コマンドと連携する際の番号です。

refresh コマンド後に有効になるコマンドです。

設定例 1　number=1 のキーワードに"secret-secret"を設定する

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 key-string secret-secret
```

コマンド書式

key <key 番号> key-string <キーワード>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
key 番号	key <number> key-string コマンド、key <number> accept-lifetime コマンドと連携する際の番号を指定します	0～2147483647	省略不可
キーワード	キーワードを指定します。	-	省略不可

この設定を行わない場合

RIP2 の認証を行なうことはできません。

設定モード

key-chain 設定モード

key <number> send-lifetime

キーの送信時有効期限を設定します。
ここで設定した時間内であれば、RIP2 の認証キーをつけて送信します。
<number>は、key <number> key-string コマンド、key <number> accept-lifetime コマンドと連携する際の番号です。

refresh コマンド後に有効になるコマンドです。

設定例１　number=1 の送信時有効期限を"2014.4.1 12:00:00 - 2003.4.30 11:59:59"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 send-lifetime 12:00:00 1 Apr 2014 11:59:59 30 Apr 2014
```

設定例２　number=1 の送信時有効期限を"2014.4.1 12:00:00 - 無限"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 send-lifetime 12:00:00 1 Apr 2014 infinity
```

設定例３　number=1 の送信時有効期限を"2014.4.1 12:00:00 - 100 秒間"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 send-lifetime 12:00:00 1 Apr 2014 duration 100
```

コマンド書式

key <key 番号> send-lifetime <有効開始時刻> { <終了時刻> | duration <有効期間> | infinity }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
key 番号	key <number> key-string コマンド、key <number> accept-lifetime コマンドと連携する際の番号を指定します。	0～2147483647	省略不可
有効開始時刻	認証キーが有効になる開始時刻を hh:mm:ss 日 月の順に設定します。	hh:mm:ss 日 月 年	省略不可
終了時刻	認証キーが無効になる終了時刻を、hh:mm:ss で設定します。	hh:mm:ss	3 種類のうちどれか 1 種類を指定する必要あり
有効期間	認証キーの有効期間(単位:秒)を指定します。	1～2147483646	
infinity	認証キーの有効期限を、無限とします。	infinity	

この設定を行わない場合

常に使用可能です。

設定モード

key-chain 設定モード

neighbor

RIP の宛先アドレスを指定します。
通常の RIP は、Version1 ではサブネットブロードキャスト(192.168.0.255 等)宛、Version2 ではマルチキャスト(224.0.0.9)宛に送信しますが、RIP を広告する相手を限定したい場合に、宛先アドレスを指定します。
併せて unicastrip の設定が必要となります。

refresh コマンド後に有効になるコマンドです。

設定例 1　RIP の宛先を 192.168.100.1 に限定する

```
Router(config)#router rip
Router(config-rip)# neighbor 192.168.100.1
Router (config-rip)# unicastrip
```

コマンド書式

neighbor <IP アドレス> [source-interface <インタフェース名>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	RIP の宛先を指定します。	IPv4 アドレス形式	省略不可
インタフェース名	RIP を送信する際の送信元アドレスに使用するインタフェースアドレスを指定します。 送信元インタフェースの指定は、最大 32 エントリとなります。33 エントリ以上、送信元インタフェースを指定したエントリがある場合、33 件目以降のエントリについては、送信元エントリの指定が無効になり、実際に送信するインタフェースのアドレスが、送信元アドレスとなります。	lan 1 ewan 1～2 loopback 1～100	実際に送信するインタフェース

この設定を行わない場合

Version1 ではサブネットブロードキャスト(192.168.0.255 等)宛、Version2 ではマルチキャスト(224.0.0.9)宛に送信します。

設定モード

RIP サービス設定モード

network

RIP サービスを提供するインタフェースを IP アドレスまたは、インタフェースで決定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　192.168.0.0/24 のインタフェースで RIP を運用する

```
Router(config)#router rip
Router(config-rip)# network 192.168.0.0 255.255.255.0
```

設定例 2　pppoe1 のインタフェースで RIP を運用する

```
Router(config)#router rip
Router(config-rip)# network pppoe 1
```

コマンド書式

network {<IP アドレス> <ネットマスク> | インタフェース名}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	RIP を運用するインタフェースを、インタフェースの IP アドレスで指定します。	IPv4 アドレス形式	省略不可
ネットマスク	RIP を運用するインタフェースを、IP アドレスとネットマスクの組み合わせで指定することもできます	IPv4 アドレス形式	省略不可
インタフェース名	RIP を運用するインタフェースを指定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 ipsecif 1～2000 vlanif 1～150	省略不可

この設定を行わない場合

全てのインタフェースでも RIP を運用しません。

設定モード

RIP サービス設定モード

offset-list

access-list で指定した経路情報の送受信 RIP に対して、任意のメトリック値を加算します。
RIP 送信時は、設定したメトリック値を加算後に RIP を送信し、RIP 受信時は設定したメトリック値を加算後に経路登録を行います。

refresh コマンド後に有効になるコマンドです。

設定例 1　192.168.100.0/24 にマッチする経路情報の RIP 受信時に、メトリック値に 3 を加算して RIP テーブルに登録する

```
Router(config)#access-list 10 permit 192.168.100.0 0.0.0.255
Router(config)#router rip
Router(config-rip)# offset-list 10 in 3
```

コマンド書式

offset-list <access-list 番号> { in | out } <メトリック値> [インタフェース名]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	メトリック値を加算対象とするアクセスリストの番号を指定します。	1～99 1300～1999 10000～11200	省略不可
{in | out}	in(受信時)または、out(送信時)のどちらでメトリック値を加算するかを指定します。	in out	省略不可
メトリック値	加算するメトリック値を指定します。	0～16	省略不可
インタフェース名	適用するインタフェースのインタフェース名を指定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 vlanif 1～150 ipsecif 1～2000	全インタフェースで適用

この設定を行わない場合

RIP 受信時にメトリック値が 1 加算されます。

設定モード

RIP サービス設定モード

passive-interface

RIP の受信のみを行い、送信はしないインタフェースを設定します。
ただし、このコマンドを設定しても unicastRIP の送信は行われます。
unicastRIP の送信を行わない場合には、neighbor コマンドを削除してください。

refresh コマンド後に有効になるコマンドです。

設定例 1　EWAN1 インタフェースは、RIP の受信のみを行なう（送信しない）設定

```
Router(config)#router rip
Router(config-rip)#passive-interface ewan 1
```

コマンド書式

passive interface <インタフェース名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	RIP の受信のみを行なうインタフェースを指定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 vlanif 1～150	省略不可

この設定を行わない場合

RIP を制御するインタフェースでは、送受信を行ないます。

設定モード

RIP サービス設定モード

redistribute

RIP 以外の手段で取得した経路情報のうち、RIP で再配布する経路を選択し必要に応じてメトリック値等を設定します。
メトリック値を省略した場合は、"1"で配布します。

ただし、経路情報に変化が無い場合は再配布が行われないため、追加した経路情報を再配布するためには、clear ip rip redistribute コマンドを実行してください。

refresh コマンド後に有効になるコマンドです。

設定例１　スタティックで登録した経路情報を RIP で再配布する（メトリック 1）

```
Router(config)#router rip
Router(config-rip)#redistribute static
```

設定例２　BGP で取得した経路情報を RIP で再配布する。このときメトリックを 3 として配布する

```
Router(config)#router rip
Router(config-rip)#redistribute bgp metric 3
```

コマンド書式

redistribute <再配布する経路情報>[metric <メトリック値>][route-map <Route-map 名>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
再配布する経路情報	RIP 以外の手段で取得した経路情報のうち、RIP で配布するものを指定します。 bgp：BGP で取得した経路情報 connected：直接経路 event-action：イベントアクションで追加した経路情報 kernel：kernel にセットされた経路情報 local-prot1：SA-UP ルート情報 local-prot2：SA-UP ルート情報 ospf：OSPF で取得した経路情報 static：スタティックルーティング情報	bgp connected event-action kernel local-prot1 local-prot2 ospf static	省略不可
メトリック値	RIP で広告する際のメトリック値を指定します。	0～16	メトリック値 1
Route-map 名	必要に応じて、適用する Route-map を指定します。	-	Route-map を適用しない

この設定を行わない場合

RIP で受信した情報および SA-UP ルート情報を広告します。

設定モード

RIP サービス設定モード

route

RIP エントリをスタティックで登録します。
ここで設定した経路情報は、RIP で広告するためだけに使用されます。装置のスタティックルートとしては登録されませんので注意してください。

refresh コマンド後に有効になるコマンドです。

設定例 1　192.168.200.0/24 の経路情報を RIP で広告する

```
Router(config)#router rip
Router(config-rip)#route 192.168.200.0 255.255.255.0
```

コマンド書式

route 〈IP アドレス〉〈ネットマスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	RIP で広告する IP アドレスを設定します。	IPv4 アドレス形式	省略不可
ネットマスク	RIP（RIP2 のみ）で広告するネットマスクを設定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

スタティック情報はありません。
redistribute コマンドの指定および学習した RIP 情報のみを、RIP で広告します。

設定モード

RIP サービス設定モード

router rip

RIP サービス設定モードに移行します。RIP の各種設定を行ないます。

設定例 1　RIP サービス設定モードに移行する

```
Router(config)# router rip
Router(config-rip)#
```

コマンド書式

```
router rip
```

パラメータ

パラメータはありません。

この設定を行わない場合

RIP を使用できません。

設定モード

基本設定モード

timers basic

RIP に関する以下のタイマ値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　定期送信間隔を 20 秒、経路情報を無効とするまでの時間を 120 秒、経路情報を RIP テーブルから削除するまでの時間を 80 秒とする

```
Router(config)#router rip
Router (config-rip)#timers basic 20 120 80
```

コマンド書式

timers basic〈定期送信間隔〉〈経路情報を無効とするまでの時間〉
〈経路情報を削除するまでの時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
定期送信間隔	RIP の定期送信間隔(単位:秒)を指定します。	5～2147483647	省略不可
経路情報を無効とするまでの時間	RIP のレスポンスを受信しなくなってから、経路情報を無効とするまでの時間(単位:秒)を指定します。 指定した時間内にレスポンスを受信しないと該当経路情報は無効となり、ルーティングテーブルからは削除されます。	5～2147483647	省略不可
経路情報を削除するまでの時間	経路情報を無効として、RIP テーブルから削除するまでの時間(単位:秒)を指定します。 この状態では、RIP テーブルにメトリック 16 で保持されて経路が無効になった事を広告します。	5～2147483647	省略不可

この設定を行わない場合

タイマの内容	デフォルト値
定期送信間隔	30
経路情報を無効とするまでの時間	180
経路情報を削除するまでの時間	120

設定モード

RIP サービス設定モード

version

装置として採用する RIP のバージョンを指定します。インタフェース毎の指定は ip rip {send/receive} version を用います。

refresh コマンド後に有効になるコマンドです。

設定例 1　RIP version 2 を使用する

```
Router(config)#router rip
Router (config-rip)# version 2
```

コマンド書式

version 〈バージョン〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
バージョン	RIP のバージョンを指定します。 1　RIP バージョン 1 2　RIP バージョン 2	1 2	省略不可

この設定を行わない場合

バージョン 2 となります。

設定モード

RIP サービス設定モード

unicastrip

unicastRIP の送受信を許可するかどうかの設定を行います。

refresh コマンド後に有効になるコマンドです。

設定例 1　unicastRIP の送受信を許可します。

```
Router(config-rip)# unicastrip
Router(config-rip)#
```

コマンド書式

unicastrip

パラメータ

パラメータはありません。

この設定を行わない場合

unicastRIP の送受信を許可しません。

unicastRIP の動作条件

unicastRIP を送信、受信する為に必要な条件。

受信可能条件	unicastrip 設定がされている。
	network コマンドで RIP サービスを動作させるインターフェース指定されている。
	受信した unicastrip の RIP バージョン(RIP1, RIP2) と、自身の RIP バージョン設定 (ip rip receive version(優先)もしくは router rip の version) が一致している。
	unicastrip 送信元アドレスへの経路がルーティングテーブルに事前に存在している。
送信可能条件	unicastrip 設定がされている。
	network コマンドで RIP サービスを動作させるインターフェース指定されている。
	neighbor コマンドでの unicastrip 送信先アドレスを設定されている。
	unicastrip 送信先アドレスへの経路がルーティングテーブルに事前に存在している。 (RIP バージョン指定 (ip rip send version 優先))

設定モード

RIP サービス設定モード

OSPF に関する設定

OSPF 基本設定

router-id

OSPF のルータ ID を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　OSPF のルータ ID を 192.168.10.1 にする

```
Router(config)#router ospf
Router(config-ospf)#router-id 192.168.10.1
```

コマンド書式

router-id <ルータ ID>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ルータ ID	OSPF のルータ ID を設定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

全インタフェースの IP アドレスのうち最大のものをルータ ID とします。

設定モード

OSPF サービス設定モード

network

OSPF エリアに含まれるネットワーク範囲を設定します。
エリアは、IP アドレスもしくは(0-4294967295)の値で指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　OSPF エリアに含まれるネットワーク範囲を、192.168.10.0/24 とします

```
Router(config)#router ospf
Router(config-ospf)#network 192.168.10.0 0.0.0.255 area 0
```

コマンド書式

network〈ネットワークアドレス〉〈マスク〉area〈エリア〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ネットワークアドレス	OSPF に含まれるネットワーク範囲を指定します。	IPv4 アドレス形式	省略不可
マスク	ワイルドカードを指定します。	IPv4 アドレス形式	省略不可
エリア	エリアを IP アドレスまたは、数値で指定します。	IPv4 アドレス形式 0～4294967295	省略不可

この設定を行わない場合

OSPF エリアに含まれるネットワーク範囲を指定しません。

設定モード

OSPF サービス設定モード

OSPF 経路制御の設定

default-information originate

ルーティングテーブルにデフォルト経路(0.0.0.0/0)があれば、その情報を AS 外 LSA として配布するように設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　デフォルトルートを AS 外 LSA として配布する。

```
Router(config)#router ospf
Router(config-ospf)#default-information originate
```

コマンド書式

```
default-information originate [ always] [ metric <0-16777214>] [ metric-
                                type{type-1|type-2}] [ route-map <Route-map 名>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
always	ルーティングテーブルにデフォルト経路が存在しなくても、自分自身をデフォルト経路としてアナウンスします。	always	自分自身をデフォルト経路としてアナウンスしません。
metric	メトリック値を指定します。	0～16777214	自分自身をデフォルト経路としてアナウンスします。
metric-type	メトリックタイプを指定します。	type-1 type-2	
Route-map 名	Route-map 名を指定します。	英数字	

この設定を行わない場合

メトリック値：10
メトリックタイプ：type-2
ただし、always オプションが有効な場合はメトリック値のデフォルトは 1 となります。

設定モード

OSPF サービス設定モード

default-metric

他のルーティングプロトコルで学習した経路を OSPF で再配布する際のメトリック値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　メトリック値を 30 に設定する

```
Router(config)#router ospf
Router(config-ospf)#default-metric 30
```

コマンド書式

default-metric 〈メトリック値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
メトリック値	他のルーティングプロトコルで学習した経路を OSPF で再配布する際のメトリック値を設定します。	0～16777214	省略不可

この設定を行わない場合

メトリック値を 20 に設定します。

設定モード

OSPF サービス設定モード

distance

OSPF の distance 値を設定します。
同じ宛先への経路を異なる手段で学習した場合に、どの情報を採用するかのパラメータとなります。

refresh コマンド後に有効になるコマンドです。

設定例 1　distance 値を 120 とします

```
Router(config)#router ospf
Router(config-ospf)#distance 120
```

コマンド書式

distance <distance 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
distance 値	OSPF の distance 値を設定します。	1～255	省略不可

この設定を行わない場合

distance 値を 110 に設定します。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	–	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

OSPF サービス設定モード

distance ospf

external ルート、inter-area ルート、intra-area ルートの各 distance 値を設定します。
同じ宛先への経路を異なる手段で学習した場合に、どの情報を採用するかのパラメータとなります。

refresh コマンド後に有効になるコマンドです。

設定例 1　external ルートの distance 値を 150 とします

```
Router(config)#router ospf
Router(config-ospf)#distance ospf external 150
```

コマンド書式

distance ospf {external <distance 値>|inter-area <distance 値>|intra-area <distance 値>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
distance 値	external ルート、inter-area ルート、intra-area ルートの各 distance 値を設定します。	1～255	省略不可

この設定を行わない場合

distance コマンドで設定した値になります。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	–	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

OSPF サービス設定モード

neighbor

ネイバを登録します。
priority では、ネイバの優先度、poll-interval ではネイバへのポーリング間隔を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　192.168.0.1 に対する優先度を 16 にする

```
Router(config)#router ospf
Router(config-ospf)#neighbor 192.168.0.1 priority 16
```

コマンド書式

neighbor <IP アドレス>[priority <優先度>] [poll-interval <ポーリング間隔>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	ネイバを登録する IP アドレスを設定します。	IPv4 アドレス形式	省略不可
優先度	ネイバの優先度を指定します。	0～255	優先度を指定しません
ポーリング間隔	ネイバへのポーリング間隔(単位:秒)を指定します。	1～65535	ポーリング間隔を指定しません

この設定を行わない場合

ネイバの優先度:0、ポーリング間隔:60 秒となります。

設定モード

OSPF サービス設定モード

redistribute

OSPF 以外の手段で取得した経路情報のうち、OSPF で再配布する経路を選択し必要に応じてメトリック値等を設定します。
メトリック値を省略した場合は、"1"で配布します。

ただし、経路情報に変化が無い場合は再配布が行われないため、追加した経路情報を再配布するためには、clear ip ospf redistribute コマンドを実行してください。

refresh コマンド後に有効になるコマンドです。

設定例 1　RIP で取得した情報を OSPF で再配布する

```
Router(config)#router ospf
Router(config-ospf)# redistribute rip
```

コマンド書式

```
redistribute <再配布する経路情報>[metric<メトリック値>][route-map <Route-map 名
>][ metric-type <1|2>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
再配布する経路情報	OSPF 以外の手段で取得した経路情報のうち、OSPF で再配布するものを指定します。 bgp：BGP で取得した経路情報 connected：直接経路 event-action：イベントアクションで追加した経路情報 kernel：kernel にセットされた経路情報 local-prot1：SA-UP ルート情報 local-prot2：SA-UP ルート情報 rip：RIP で取得した経路情報 static：スタティックルーティング情報	bgp connected event-action kernel local-prot1 local-prot2 rip static	省略不可
メトリック値	OSPF で広告する際の metric を指定します。	0～16777214	省略不可
Route-map 名	必要に応じて適用する Route-map を指定します。	–	Route-map を適用しない
1|2	OSPF の外部リンクタイプ ASBR が外部ルートをアドバタイズする場合に、どちらかを指定します。 1：自 AS 内で広告される際にコスト加算する場合は、metric-type1 を指定します。 2：自 AS 内で広告される際にコスト加算しない場合	1 2	2

	は、metric-type2 を指定します。		

この設定を行わない場合

OSPF で受信した情報のみ配布します。

設定モード

OSPF サービス設定モード

summary-address

経路情報を Aggregate します。この経路を OSPF で広告しない場合は not-advertise を指定します。
また、tag 値を設定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例 1　192.168.0.0/16 の経路情報を Tag 0 で Aggregate する。

```
Router(config)#router ospf
Router(config-ospf)#summary-address 192.168.0.0 255.255.0.0 tag 0
```

コマンド書式

summary-address <IP アドレス> <ネットマスク> [not-advertise] [tag <タグ値>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	経路情報を Aggregate する IP アドレスを指定します。	IPv4 アドレス形式	省略不可
ネットマスク	経路情報を Aggregate する IP アドレスのネットマスク指定します。	IPv4 アドレス形式	省略不可
not-advertise	経路を OSPF で広告しない場合に指定します。	not-advertise	経路を OSPF で広告する
タグ値	tag 値を設定します。	0～4294967295	0

この設定を行わない場合

経路情報を Aggregate しません。

設定モード

OSPF サービス設定モード

OSPF エリア情報

area default-cost

スタブエリアにデフォルト経路をアナウンスする際のコスト値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　デフォルト経路をアナウンスする際のコスト値を 100 にする

```
Router(config)#router ospf
Router(config-ospf)#area 192.168.10.1 default-cost 100
```

コマンド書式

area 〈エリア ID〉 default-cost 〈コスト値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エ リア ID を整数または、IP アドレスで指定します。	0～4294967295 IP アドレス形式	省略不可
コスト値	デフォルト経路をアナウンスする際のコスト値を設定します。	0～16777215	省略不可

この設定を行わない場合

コスト値を 1 に設定します。

設定モード

OSPF サービス設定モード

area export-list

他のエリアにアナウンスする経路をフィルタリングします。
アクセスリストにマッチしない経路はアナウンスしません。

refresh コマンド後に有効になるコマンドです。

設定例１　フィルタリングする経路をアクセスリスト番号１で指定する

```
Router(config)#router ospf
Router(config-ospf)#area 1 export-list 1
```

コマンド書式

area 〈エリア ID〉 export-list 〈アクセスリスト番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エ リア ID を整数または、IP アドレスで指定します。	0～4294967295 IPv4 アドレス形式	省略不可
アクセスリスト番号	フィルタしたい経路を標準アクセスリスト番号でしていします。	1～99 1300～1999 10000～11200	省略不可

この設定を行わない場合

フィルタリングしません。

設定モード

OSPF サービス設定モード

area import-list

他のエリアからアナウンスされた経路をフィルタリングします。
アクセスリストにマッチしない経路は受け入れません。

refresh コマンド後に有効になるコマンドです。

設定例１　フィルタリングする経路をアクセスリスト番号１で指定する

```
Router(config)#router ospf
Router(config-ospf)#area 1 import-list 1
```

コマンド書式

area〈エリア ID〉import-list〈アクセスリスト番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エ リア ID を整数または、IP アドレスで指定します。	0～4294967295 IPv4 アドレス形式	省略不可
アクセスリスト番号	フィルタしたい経路を標準アクセスリスト番号でしていします。	1～99 1300～1999 10000～11200	省略不可

この設定を行わない場合

フィルタリングしません。

設定モード

OSPF サービス設定モード

area nssa

OSPF エリアを NSSA(Not So Stub Area)に設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　外部経路を NSSA に再配布しない

```
Router(config)#router ospf
Router(config-ospf)#area 1 nssa no-redistribution
```

コマンド書式

```
area <エリア ID> nssa [ translate-always|translate-never][ no-redistribution|
                        default-information-originate|no-summary]
```

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>エリア ID</td><td>エリア ID を整数または、IP アドレスで指定します。</td><td>0～4294967295
IPv4 アドレス形式</td><td>省略不可</td></tr>
<tr><td>translate-always | translate-never</td><td>タイプ7LSA をタイプ5に変換して中継するかどうかを設定します。<table><tr><td>translate-always</td><td>タイプ7LSA をタイプ5に変換して中継する</td></tr><tr><td>translate-never</td><td>変換しない</td></tr></table></td><td>translate-always
translate-never</td><td>タイプ7LSA をタイプ5に変換して中継します</td></tr>
<tr><td>no-redistribution</td><td>外部経路を NSSA に再配布しない場合に指定します。
※ASBR が NSSA ABR を兼務している場合のみ</td><td>no-redistribution</td><td rowspan="3">タイプ5LSA を受け入れない IGRP 経路をエリア内にタイプ7として配布します。</td></tr>
<tr><td>default-information-originate</td><td>タイプ7のデフォルトルートを生成する場合に指定します。</td><td>default-information-originate</td></tr>
<tr><td>no-summary</td><td>NSSA 完全スタブエリアを設定する場合に指定します。</td><td>no-summary</td></tr>
</table>

この設定を行わない場合

OSPF エリアを NSSA に設定しません。

NSSA とは？

バックボーンでないエリアを、NSSA として設定することができます。
エリアボーダルータは、NSSA として定義したエリアへほかのエリアから学習した AS 外経路を広告しません。
NSSA を設定することで、NSSA 内では経路情報を減らし、ルータの情報の交換や経路選択の負荷を減らすことができます。

設定モード

OSPF サービス設定モード

area range

他のエリアに経路をアナウンスする際に複数の経路を 1 つの経路に集約します。

refresh コマンド後に有効になるコマンドです。

設定例 1　集約する経路の IP アドレスを 192.168.10.0/16 にする

```
Router(config)#router ospf
Router(config-ospf)#area 1 range 192.168.0.0 255.255.0.0
```

コマンド書式

area <エリア ID> range <summary-address><summary-address-mask>[substitute <substitute-address><substitute-address-mask>|not-advertise]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IP アドレスで指定します。	0～4294967295 IPv4 アドレス形式	省略不可
summary-address	集約する経路の IP アドレスを設定します。	IPv4 アドレス形式	省略不可
summary-address-mask	集約する経路のネットワークマスクを設定します。	IPv4 アドレス形式	省略不可
substitute-address	集約する経路を別のアドレスでアナウンスする場合の IP アドレスを設定します。	IPv4 アドレス形式	省略不可
substitute-address-mask	集 約する経路を別のアドレスでアナウンスする場合のネットワークマスクを設定します。	IPv4 アドレス形式	省略不可
not-advertise	集約した経路をアナウンスしない場合に指定します。	not-advertise	-

この設定を行わない場合

経路の集約は行いません。

設定モード

OSPF サービス設定モード

area shortcut

エリアのショートカットモードを設定します。
※ospf abr-type shortcut コマンドと同時に設定して ABR タイプを shortcut モードにしておく必要があります。

refresh コマンド後に有効になるコマンドです。

設定例 1　ショートカットモードを有効にする

```
Router(config)#router ospf
Router(config-ospf)#area 1 shortcut enable
```

コマンド書式

area 〈エリア ID〉 shortcut 〈ショートカットモード〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IP アドレスで指定します。	0～4294967295 IPv4 アドレス形式	省略不可
ショートカットモード	ショートカットモードの状態を設定します。 default：ショートカットモードをデフォルトに戻す場合に指定します。 disable：ショートカットモードを無効にする場合に指定します。 enable：ショートカットモードを有効にする場合に指定します。	default disable enable	省略不可

この設定を行わない場合

ショートカットモードを使用しません。

設定モード

OSPF サービス設定モード

area stub

OSPF エリアをスタブエリアに設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　サマリ LSA をスタブエリアにアナウンスしない

```
Router(config)#router ospf
Router(config-ospf)#area 1 stub no-summary
```

コマンド書式

area <エリア ID> stub [no-summary]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IP アドレスで指定します。	0～4294967295 IPv4 アドレス形式	省略不可
no-summary	サマリ LSA をスタブエリアにアナウンスしない場合に指定します。	no-summary	サマリ LSA をスタブエリアにアナウンスします。

この設定を行わない場合

OSPF エリアをスタブエリアに設定しません。

スタブエリアとは？

スタブエリアには、外部経路を伝える LSA が流れません。そのため、このエリアには ASBR を設置することはできません。また、外部経路が伝わらないため、スタブエリアの ABR は、このエリア内にデフォルトルートをアナウンスする必要があります。

設定モード

OSPF サービス設定モード

ospf abr-type

エリア境界ルータのタイプを設定します。
オプションにより、エリア間ルートの計算の動作が異なります。

refresh コマンド後に有効になるコマンドです。

設定例１　エリア境界ルータのタイプを standard にする

```
Router(config)#router ospf
Router(config-ospf)#ospf abr-type standard
```

コマンド書式

ospf abr-type <ルータタイプ>

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>ルータタイプ</td><td>エリア境界ルータのタイプを設定します。
<table>
<tr><td>cisco</td><td>バックボーンエリアに隣接していて,かつバックボーンエリアの 1 台以上のルータと full ステータスとなっている場合にバックボーンエリアおよびトランジットエリアの summary lsa を計算。それ以外は全エリアの summary lsa を計算します。</td></tr>
<tr><td>ibm</td><td>バックボーンエリアに隣接していて,かつバックボーンエリアの 1 台以上のルータと full ステータスとなっている場合にバックボーンエリアおよびトランジットエリアの summary lsa を計算。それ以外は全エリアの summary lsa を計算します。</td></tr>
<tr><td>shortcut</td><td>バックボーンエリアに関しては,バックボーンエリアの 1 台以上のルータと full ステータスとなっている場合に summary LSA を計算。バックボーンエリア以外のエリアに関しては,以下のエリアに関して summary LSA を計算。
・トランジットエリア
・ルータがバックボーンに隣接していなくて,shortcut モードが disable 以外(default or enable)のエリア
・shortcut モードが enable のエリア</td></tr>
<tr><td>standard</td><td>エリア間ルートの計算は,バックボーンエリアおよびトランジットエリア(Virtual Link)で</td></tr>
</table></td><td>cisco
ibm
shortcut
standard</td><td>省略不可</td></tr>
</table>

		のみ summary LSA を計算。		

この設定を行わない場合

ABR のタイプを standard に設定します。

設定モード

OSPF サービス設定モード

OSPF 認証の設定

area authentication

OSPF 認証機能を有効にします。
認証キーは、ip ospf authentication-key,ip ospf message-digest-key コマンドで設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　エリア ID 1 の認証方式に MD5 を使用する

```
Router(config)#router ospf
Router(config-ospf)#area 1 authentication message-digest
```

コマンド書式

area 〈エリア ID〉 authentication [message-digest]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IP アドレスで指定します。	0～4294967295 IPv4 アドレス形式	省略不可
message-digest	OSPF 認証に MD5 を使用する場合に指定します。	message-digest	認証に MD5 を使用しない

この設定を行わない場合

OSPF 認証を行いません。

設定モード

OSPF サービス設定モード

ip ospf authentication

設定しているインタフェースで認証機能を使用するかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　EWAN1 の認証を MD5 で行う

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf authentication message-digest
```

コマンド書式

ip ospf authentication [認証設定]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
認証設定	認証方法を設定します。 message-digest：MD5 で認証を行います。 null：simple-password で認証を行います。	message-digest null	simple-password で認証を行ないます。

この設定を行わない場合

認証を行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf authentication-key

OSPF で認証機能を使用する場合の認証キーを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　認証キーを「ospfpaswd」にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf authentication-key ospfpswd
```

コマンド書式

ip ospf authentication-key <認証キー >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
認証キー	OSPF で認証機能を使用する場合の認証キーを設定します。	8 文字以内の英数字	省略不可

この設定を行わない場合

OSPF 認証機能で使用する認証キーを設定しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf message-digest-key

OSPF で MD5 認証機能を使用する場合の MD5 認証キーとキーID を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　MD5 認証キーを「md5pswd」、キーID を 1 にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf message-digest-key 1 md5 md5pswd
```

コマンド書式

ip ospf message-digest-key <キーID> md5 <認証キー>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キーID	OSPF で MD5 認証機能を使用する場合のキーID を設定します。	1～255	省略不可
認証キー	OSPF で MD5 認証機能を使用する場合の認証キーを設定します。	16 文字以内の英数字	省略不可

この設定を行わない場合

OSPF の認証機能に MD5 を使用しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
ループバックインタフェース設定モード

OSPF インタフェース

ip ospf cost

OSPF を使用する場合のインタフェースに割り当てるコスト値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　EWAN1 に割り当てるコスト値を 100 にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf cost 100
```

コマンド書式

ip ospf cost 〈コスト値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
コスト値	インタフェースのコスト値を設定します。	1～65535	省略不可

この設定を行わない場合

auto-cost reference-bandwidth コマンドの設定に従います。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf database-filter all out

このインタフェースに新しい LSA の情報を受け付けないようにする場合に指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　新しい LSA の情報を受け付けないようにする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf database-filter all out
```

コマンド書式

```
ip ospf database-filter all out
```

パラメータ

パラメータはありません

この設定を行わない場合

新しい LSA の情報を受け付けます。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf dead-interval

OSPF の dead interval を設定します。
ここで設定した時間、OSPF の Hello を受信しなかった場合、その Neighbor をテーブルから削除します。

refresh コマンド後に有効になるコマンドです。

設定例 1　OSPF の dead interval を 100 秒にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf dead-interval 100
```

コマンド書式

```
ip ospf dead-interval <dead-interval>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
dead-interval	Neighbor をテーブルから削除するまでの時間(単位:秒)を設定します。	1～65535	省略不可

この設定を行わない場合

40 秒間 Hello を受信しなかった場合にテーブルから削除します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf disable all

このインタフェースで OSPF を使用しない場合に指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　このインタフェースで OSPF を使用しないようにする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf disable all
```

コマンド書式

```
ip ospf disable all
```

パラメータ

パラメータはありません

この設定を行わない場合

OSPF を使用します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf hello-interval

OSPF の Hello interval を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　OSPF の Hello interval を 20 秒にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf hello-interval 20
```

コマンド書式

ip ospf hello-interval 〈再送間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
再送間隔	Hello メッセージの再送間隔（単位：秒）を設定します。	1～65535	省略不可

この設定を行わない場合

Hello メッセージを 10 秒間隔で定期的に送信します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf network

OSPF インタフェースのネットワークの型を明示的に指定したい場合にこのコマンドを使用します。

refresh コマンド後に有効になるコマンドです。

設定例 1　ネットワークタイプを non-broadcast multiple access タイプに指定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# ip ospf network non-broadcast
```

コマンド書式

ip ospf network <ネットワークタイプ>

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
ネットワークタイプ	OSPF で使用するネットワークタイプを指定します。		broadcast non-broadcast point-to-multipoint point-to-point	省略不可
	broadcast	broadcast タイプに設定します。		
	non-broadcast	non-broadcast multiple access タイプに設定します。		
	point-to-multipoint	point-to-multipoint タイプに設定します。		
	point-to-point	point-to-point タイプに設定します。		

この設定を行わない場合

broadcast タイプに設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf priority

OSPF を使用する優先度を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　OSPF を使用するインタフェースの priority を 20 にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf priority 20
```

コマンド書式

ip ospf priority <優先度>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
優先度	OSPF を使用するインタフェースの優先度を設定します。	0～255	省略不可

この設定を行わない場合

priority を 1 に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf retransmit-interval

OSPF（Database Description、Link State Request、Link State Update ）の再送間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　OSPF の再送間隔を 100 秒にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf retransmit-interval 100
```

コマンド書式

ip ospf retransmit-interval <再送間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
再送間隔	Database Description、Link State Request、Link State Update パケットの再送間隔（単位：秒）を設定します。	3～65535	省略不可

この設定を行わない場合

5 秒間隔で送信します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf transmit-delay

設定しているインタフェースにて、LinkStateUpdate を中継するためにかかる時間を設定します。
ここで設定した値が、LSA の Age に加算されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　OSPF の transmit delay を 10 にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf transmit-delay 10
```

コマンド書式

ip ospf transmit-delay <中継遅延時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
中継遅延時間	設定しているインタフェースにて、LinkStateUpdate を中継するためにかかる時間(単位:秒)を設定します。	1～65535	省略不可

この設定を行わない場合

中継遅延時間は 1 秒になります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
ループバックインタフェース設定モード

passive-interface

ここで指定したインタフェースには HELLO パケットの送受信を行いません。
ルータ ID 決定の際の計算の対象からも除外されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　EWAN1 で HELLO パケットの送受信を行わないようにする

```
Router(config)#router ospf
Router(config-ospf)#passive-interface ewan1
```

コマンド書式

passive-interface <インタフェース名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	HELLO パケットの送受信を行わないインタフェースを指定します。	lan 1 ewan 1～2 pppoe 1～24 vlanif 1～150	省略不可

この設定を行わない場合

HELLO パケットの送受信を行う。

設定モード

OSPF サービス設定モード

OSPF 全般の設定

auto-cost reference-bandwidth

インタフェースの OSPF コスト値を自動計算する際のベースとなる値を設定します。
auto-cost reference-bandwidth の設定単位は、Mbps となります。
計算式は以下のようになります。
　インタフェースの cost 値 = <auto-cost reference-bandwidth 値>/<回線速度>

refresh コマンド後に有効になるコマンドです。

設定例 1　OSPF コスト値を自動計算する際のベース値を 80 とします

```
Router(config)#router ospf
Router(config-ospf)#auto-cost reference-bandwidth 80
```

コマンド書式

auto-cost reference-bandwidth <ベース値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ベース値	OSPF コスト値を自動計算する際のベースとなる値を設定します。	1～4294967	省略不可

この設定を行わない場合

100Mbps に設定します。
各インタフェースのデフォルトコスト値は以下の通りです。

インタフェース	コスト値
LAN	1
EWAN	1
VLAN	1
Loopback	1
dialer	1562

設定モード

OSPF サービス設定モード

compatible rfc1583

AS 外の経路について、RFC1583 互換で動作するよう設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　AS 外の経路について、RFC1583 互換で動作するようにする

```
Router(config)#router ospf
Router(config-ospf)#compatible rfc1583
```

コマンド書式

compatible rfc1583

パラメータ

パラメータはありません

この設定を行わない場合

RFC 1583 非互換で動作します。

設定モード

OSPF サービス設定モード

log-adjacency-changes

OSPF ネイバの状態遷移を ttrlog に出力します。
出力内容は状態遷移前後のステートおよび状態遷移を引き起こしたイベントの種類です。
FULL ステートと FULL ステート以外のステートの間の遷移が発生した時のみ出力します。

refresh コマンド後に有効になるコマンドです。

設定例 1　OSPF ネイバの状態遷移を ttrlog に出力する

```
Router(config)#router ospf
Router(config-ospf)#log-adjacency-changes
```

コマンド書式

log-adjacency-changes

パラメータ

パラメータはありません

この設定を行わない場合

OSPF ネイバの状態遷移を ttrlog に出力しません。

設定モード

OSPF サービス設定モード

refresh timer

LSA リフレッシュの間隔を設定します。対象はサマリ LSA（タイプ 3,4 ）、AS 外 LSA 。

refresh コマンド後に有効になるコマンドです。

設定例 1　LSA リフレッシュの間隔を 30 秒にする

```
Router(config)#router ospf
Router(config-ospf)#refresh timer 30
```

コマンド書式

refresh timer 〈リフレッシュ間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リフレッシュ間隔	LSA リフレッシュの間隔（単位：秒）を指定します。	10～1800	省略不可

この設定を行わない場合

LSA リフレッシュの間隔を 10 秒に設定します。

設定モード

OSPF サービス設定モード

timers spf

LSA の更新を受信してから、実際に SPF 計算を開始するまでの遅延時間と、SPF 計算を行ってから次の計算に入るまでのホールドタイムを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　SPF 計算を開始するまでの遅延時間を 100 秒、SPF 計算を行ってから次の計算に入るまでのホールドタイムを 50 秒にします。

```
Router(config)#router ospf
Router(config-ospf)#timers spf 100 50
```

コマンド書式

timers spf <spf-delay> <spf-holdtime>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
spf-delay	LSA の更新を受信してから、実際に SPF 計算を開始するまでの遅延時間を設定します。	0～4294967295	省略不可
spf-holdtime	SPF 計算を行ってから次の計算に入るまでのホールドタイムを設定します。	0～4294967295	省略不可

この設定を行わない場合

spf-delay：5 秒
spf-holdtime：10 秒

設定モード

OSPF サービス設定モード

virtual-link の設定

area virtual-link

Virtual-link を確立する相手のルータ ID を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　仮想リンク先の IP アドレスを 192.168.10.1 にする

```
Router(config)#router ospf
Router(config-ospf)#area 1 virtual-link 192.168.10.1
```

コマンド書式

area 〈エリア ID〉 virtual-link 〈リモートルータ ID〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

仮想リンクを設定しません。

設定モード

OSPF サービス設定モード

area virtual-link authentication

設定しているインタフェースで認証機能を使用するかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　MD-5 認証機能を使用して認証する。

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2 authentication message-digest
```

コマンド書式

area 〈エリア ID〉 virtual-link 〈リモートルータ ID〉 authentication [認証設定]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
認証設定	認証方法を選択します。 message-digest：MD5 で認証を行います。 null：simple-password で認証を行います。	message-digest null	simple-password で認証を行います。

この設定を行わない場合

認証を行いません。

設定モード

OSPF サービス設定モード

area virtual-link authentication-key

Virtual-link で認証機能を使用する場合の認証キーを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　認証キーを ospfpswd に設定する。

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2 authentication-key ospfpswd
```

コマンド書式

area <エリア ID> virtual-link <リモートルータ ID> authentication-key <パスワード>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
パスワード	認証パスワードを指定します。	最大8文字の英数字	省略不可

この設定を行わない場合

Simple-password 認証のパスワードを設定しません。

設定モード

OSPF サービス設定モード

area virtual-link dead-interval

OSPF の dead interval を設定します。ここで設定した時間内に OSPF の Hello を受信しなかった場合、その Neighbor をテーブルから削除します。

refresh コマンド後に有効になるコマンドです。

設定例 1　20 秒間 Hello を受信しなかったらテーブルから削除する。

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2 dead-interval 20
```

コマンド書式

area〈エリア ID〉virtual-link〈リモートルータ ID〉dead-interval〈受信間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
受信間隔	近接ルータをダウンと認識するまでの Hello パケット未受信間隔(単位:秒)を指定します。	1～65535	省略不可

この設定を行わない場合

40 秒間 Hello を受信しなかったらテーブルから削除します。

設定モード

OSPF サービス設定モード

area virtual-link hello-interval

Hello パケットの送信間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　Hello パケットの送信間隔を 20 秒に設定する。

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2 20 hello-interval 20
```

コマンド書式

area 〈エリア ID〉 virtual-link 〈リモートルータ ID〉 hello-interval 〈送信間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
送信間隔	Hello パケットの送信間隔（単位：秒）を指定します。	1～65535	省略不可

この設定を行わない場合

Hello メッセージの送信間隔を 10 秒に設定します。

設定モード

OSPF サービス設定モード

area virtual-link message-digest-key

Virtual-link で MD5 認証機能を使用する場合の MD5 認証キーを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　192.168.0.0/16 の経路情報を Tag 0 で Aggregate する。

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2 message-digest-key 1 md5 md5pswd
```

コマンド書式

area 〈エリア ID〉 virtual-link 〈リモートルータ ID〉 message-digest-key 〈キーID〉 md5 〈認証キー〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
キーID	キーID を指定します。	1～255	省略不可
認証キー	認証キーを指定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

認証キーを設定しません。

設定モード

OSPF サービス設定モード

area virtual-link retransmit-interval

Virtual-Link の OSPF(Database Description および Link State Request)の再送間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　OSPF の再送間隔を 100 秒に設定する

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2 retransmit-interval 100
```

コマンド書式

area 〈エリア ID〉 virtual-link 〈リモートルータ ID〉 retransmit-interval 〈再送間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
再送間隔	Database Description および Link State Request パケットの再送間隔(単位:秒)を設定します。	1～65535	省略不可

この設定を行わない場合

再送間隔を 5 秒に設定します。

設定モード

OSPF サービス設定モード

area virtual-link transmit-delay

Virtual-Link の LinkStateUpdate を中継するためにかかる時間を設定します。
ここで設定した値が、LSA の Age に加算されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　LinkStateUpdate パケットの中継遅延時間を 10 秒にする

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2 transmit-delay 10
```

コマンド書式

area 〈エリア ID〉 virtual-link 〈リモートルータ ID〉 transmit-delay 〈中継遅延時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
中継遅延時間	設定しているインタフェースにて、LinkStateUpdate を中継するためにかかる時間（単位：秒）を設定します。	1～65535	省略不可

この設定を行わない場合

中継遅延間隔は 1 秒になります。

設定モード

OSPF サービス設定モード

フィルタリングの設定

access-list

特定のパケットと、そのパケットの動作（中継 or 廃棄 or 学習フィルタリング）を指定します。
指定したパケットは、以下の機能で使用します。
・フィルタリング（ip access-group コマンド）
・学習フィルタリング（ip access-group コマンド）
・オフセットリスト（offset-list コマンド）
・RIP/BGP で送信するメトリック値の指定（distance コマンド）
・BGP で送信する経路の指定（neighbor <IP-address> distribute-list コマンド）
・経路情報の指定（match ip address コマンド）
・NextHop の指定（match ip nexthop コマンド）
・NAT 変換前のアドレス指定（ip nat inside コマンド）
・ポリシールーティング（match ip access-group コマンド）

使用方法は、まず本コマンドでパケットを指定した後、上記機能を使用するモードで、
指定したアクセスリスト番号を指定します。
access-list は、番号順に適用されます。
また、同じ番号の access-list に複数行の設定をした場合は、上の行から適用されます。

refresh コマンド後に有効になるコマンドです。

アクセスリスト番号について

本装置のアクセスリスト番号は、以下の規定があります。

アクセスリスト番号	名称	設定内容
1～99、1300～1999 10000～11200	IPv4 標準設定	IPv4 送信元アドレス指定
100～199、2000～2699 20000～21199	IPv4 拡張設定	IPv4 送信元／宛先アドレス指定 プロトコル番号指定 送信元／宛先ポート番号指定
3000～3499 30000～31499	IPv6 標準設定	IPv6 送信元／宛先アドレス指定
3500～3999 35000～36499	IPv6 拡張設定	IPv6 送信元アドレス指定 プロトコル番号指定 送信元／宛先ポート番号指定

指定パケットの動作指定について

指定したパケットを中継対象とするか、廃棄対象とするかを指定します。中継対象とする場合は permit、廃棄対象とする場合は deny を指定します。
この指定が必要なのは、フィルタリング／経路情報の指定／NextHop の指定のためにアクセスリストを指定する場合のみです。他の用途で指定する場合は permit を指定してください。

IP アドレス範囲指定

アクセスリストコマンドで IPv4 アドレスを指定する場合、マスク(Wildcard マスク)を使用して 1 エントリでアドレス範囲を指定することができます。
Wildcard マスクは、サブネットマスクとは書式が異なりますので注意してください。Wildcard マスクとサブネットマスクは、"1"と"0"の判別が逆になります。
例1)24bit マスクを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
Wildcard マスクの場合:0.0.0.255
サブネットマスクの場合:255.255.255.0
例2)ホストを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
Wildcard マスクの場合:0.0.0.0
サブネットマスクの場合:255.255.255.255

ポート番号の指定

IPv4/IPv6 拡張設定では、TCP/UDP 上位ポート番号を指定することができます。この指定は、フィルタリング/学習フィルタリングの指定のためにアクセスリストを指定する場合に効果があります。他の用途で指定する場合は、標準設定でアクセスリストを指定してください。

学習フィルタリング

インターネットの常時接続で使用する場合、セキュリティとしては危険な状態に常にさらされています。
学習フィルタリング機能では、LAN 側からのインターネット接続に対する応答データ以外はフィルタリング(廃棄)することができます。
学習フィルタリング機能を使用する場合は、外部からのアクセス(Web 等)はできなくなります。(アクセスを許可するアドレスを限定することはできます)
ただし、VPN からの受信に関してはフィルタリングを行いません。(ルートベースの VPN を除く)

本装置で、学習フィルタリングを使用する場合は、access-list コマンドの属性で、"dynamic"を指定します。

設定例 1　IPv4 標準アクセスリストに、192.168.100.0/24 を設定する (許可属性)

```
Router(config)# access-list 1 permit 192.168.100.0 0.0.0.255
```

設定例 2　IPv4 拡張アクセスリストに、src=192.168.100.0/24 dst=192.168.200.0/24 を設定する (不許可属性)

```
Router(config)# access-list 100 deny ip 192.168.100.0 0.0.0.255 192.168.200.0
0.0.0.255
```

設定例 3　IPv6 標準アクセスリストに、src=3ffe:110::/64 を dst=3ffe:111::/64 を設定する (許可属性)

```
Router(config)# access-list 3000 permit 3ffe:110::/64 3ffe:111::/64
```

設定例４　IPv6 拡張アクセスリストに、src=any srcport=any dst=any dstport=80 を設定する（不許可属性）

```
Router(config)# access-list 3500 deny tcp any gt 0 any eq 80
```

設定例５　学習フィルタリングを指定する（IPv4）

```
Router(config)# access-list 100 dynamic permit ip any any
```

設定例６　宛先が fnsc.co.jp 宛のポリシールーティング(ipsecif1 経由)を設定する

```
Router(config)#fqdn-list 1 www.fnsc.co.jp
Router(config)#access-list 100 permit ip any fqdn-list 1

Router(config)#class-map FNSC
Router(config-class-map)#match ip access-group 100
Router(config-class-map)#exit

Router(config)#action-map ipsecif1
Router(config-action-map)#set ip next-hop connected ipsecif 1
Router(config-action-map)#exit

Router(config)#policy-map FNSC
Router(config-policy-map)#class FNSC action ipsecif1
Router(config-policy-map)#exit

Router(config)#interface lan 1
Router(config-if lan 1)#service-policy input FNSC
Router(config-if lan 1)#exit
```

コマンド書式

IPv4 標準アクセスリスト（番号：1～99、1300～1999、10000-11200）
access-list <access-list 番号> { permit | deny } { any | <送信元 IP アドレス> <送信元 Wildcard マスク> }[log][count]

IPv4 拡張アクセスリスト（番号：100～199、2000～2699、20000～21199）
access-list <access-list 番号> { [dynamic] permit | deny } <プロトコル番号> { any | host <送信元 IP アドレス> | <送信元 IP アドレス> <送信元 Wildcard マスク> } [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] { any | host <宛先 IP アドレス> | <宛先 IP アドレス> <宛先 Wildcard マスク> | fqdn-list <fqdn-list 番号> } [ICMP タイプ] [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] [[precedence

{<precedence-value>|<precedence-named-value>}] [tos {<tos-value>|<tos-named-value>}]| [dscp {<dscp-value>|<dscp-named-value>}]] [ip-flag {<ip-flag-value>|<ip-flag-value:wildcard mask>}][log] [count]

IPv6 標準アクセスリスト（番号：3000～3499、30000～31499）
access-list <access-list 番号> { permit | deny } { any | <送信元 IPv6 プレフィックス> } { any | <宛先 IPv6 プレフィックス> } [count]

IPv6 拡張アクセスリスト（番号：3500～3999、35000～36499）
access-list <access-list 番号> { [dynamic] permit | deny } <プロトコル番号> { any | <送信元 IPv6 プレフィックス> } [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] { any | <宛先 IPv6 プレフィックス> | fqdn-list <fqdn-list 番号>} [ICMPv6 タイプ] [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] [tcp-flag {<tcp-flag-value>|<tcpflag-value:wildcard-mask>}] [traffic-class <traffic-class-value>|dscp {<dscp-level>|<dscp-name>}] [flow-label <flow-label-value>][count]

パラメータ

パラメータ	設定内容	設定範囲		省略時の値
access-list 番号	それぞれの属性の番号を指定します。	1～99、1300～1999 10000～11200	IPv4 標準アクセスリスト	省略不可
		100～199、2000～2699, 20000～21199	IPv4 拡張アクセスリスト	
		3000～3499 30000～31499	IPv6 標準アクセスリスト	
		3500～3999 35000～36499	IPv6 拡張アクセスリスト	
dynamic	学習フィルタリングを使用する場合に指定します。	dynamic		学習フィルタリングのエントリではない
{ permit | deny }	許可属性か、不許可属性かを選択します。	permit	許可属性	省略不可
		deny	不許可属性	
プロトコル番号	プロトコル名もしくはプロトコル番号を選択します。	esp	ESP	省略不可
		gre	Cisco's GRE	

			tunneling	
		icmp	ICMP(IPv4 拡張アクセスリスト時)	
		icmpv6	ICMPv6(IPv6 拡張アクセスリスト時)	
		ip	IP	
		ipinip	IP トンネル	
		tcp	TCP	
		udp	UDP	
		0～255	プロトコル番号を指定	
any	各パラメータ(アドレスやポート番号など)で、「全て」を指定する場合は"any"を入力します。	any		-
送信元 IP アドレス	送信元アドレスを指定します。	IPv4 アドレス形式		省略不可
送信元 Wildcard マスク	送信元アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式		省略不可
宛先 IP アドレス	宛先アドレスを指定します。	IPv4 アドレス形式		省略不可
宛先 Wildcard マスク	宛先アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式		省略不可
fqdn-list※2	fqdn-list を指定します。	1～50※3		省略不可
host	IPv4 拡張アクセスリストで、送信元/宛先アドレスとしてホストアドレスを指定する場合につけます。	host		-
送信元 IPv6 プレフィックス	送信元 IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式		省略不可
宛先 IPv6 プレフィックス	宛先 IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式		省略不可
ICMP タイプ	プロトコル番号で"icmp"を指定した場合に、対象とする ICMP タイプを指定します。	**指定できる ICMP タイプ**		全ての ICMP タイプ
		administratively-prohibited		
		alternate-address		
		conversion-error		
		dod-host-prohibited		
		dod-net-prohibited		

		echo echo-reply general-parameter-problem host-isolated host-precedence-unreachable host-redirect host-tos-redirect host-tos-unreachable host-unknown host-unreachable information-reply information-request mask-reply mask-request mobile-redirect net-redirect net-tos-redirect net-tos-unreachable net-unreachable network-unknown no-room-for-option option-missing packet-too-big parameter-problem port-unreachable precedence-unreachable protocol-unreachable reassembly-timeout redirect router-advertisement router-solicitation source-quench source-route-failed time-exceeded timestamp-reply	

		timestamp-request traceroute ttl-exceeded unreachable ICMP タイプ値(0～255)	
ICMPv6 タイプ(IPv6)	プロトコル番号で"icmpv6"を指定した場合に、対象とする ICMPv6 タイプを指定します。	**ICMPv6 タイプ** address-unreachable administratively-prohibited dest-unreachable echo-reply echo-request erroneous-header-field hop-limit-exceeded-in-transit multicast-listener-done multicast-listener-query multicast-listener-report neighbor-advertisement neighbor-solicitation no-route-to-destination packet-too-big parameter-problem port-unreachable reassembly-time-exceeded redirect router-advertisement router-solicitation time-exceeded unrecognized-next-header unrecognized-option ICMPv6 タイプ値(0～255)	全ての ICMPv6 タイプ
ポート属性	ポート番号を範囲で指定するために、ポート属性を指定します。	eq　指定するポートが対象	全てのポート(以降設定な

<table>
<tr><td></td><td></td><td><table><tr><td>gt</td><td>指定するポート番号より大きいポート番号が対象</td></tr><tr><td>lt</td><td>指定するポート番号より小さいポート番号が対象</td></tr><tr><td>neq</td><td>指定するポート番号以外のポート番号が対象</td></tr><tr><td>range</td><td>ポートの範囲を指定する</td></tr></table></td><td>し）</td></tr>
<tr><td>TCP ポート番号</td><td>プロトコルで"tcp"を指定した場合に、対象とする TCP ポート番号を指定します。</td><td><table><tr><th>TCP ポート番号</th></tr><tr><td>bgp</td></tr><tr><td>chargen</td></tr><tr><td>cmd</td></tr><tr><td>daytime</td></tr><tr><td>discard</td></tr><tr><td>domain</td></tr><tr><td>echo</td></tr><tr><td>exec</td></tr><tr><td>finger</td></tr><tr><td>ftp</td></tr><tr><td>ftp-data</td></tr><tr><td>gopher</td></tr><tr><td>hostname</td></tr><tr><td>ident</td></tr><tr><td>irc</td></tr><tr><td>klogin</td></tr><tr><td>kshell</td></tr><tr><td>login</td></tr><tr><td>lpd</td></tr><tr><td>nntp</td></tr><tr><td>pim-auto-rp</td></tr><tr><td>pop2</td></tr><tr><td>pop3</td></tr><tr><td>smtp</td></tr><tr><td>sunrpc</td></tr><tr><td>syslog</td></tr></table></td><td>全ての TCP ポート番号</td></tr>
</table>

		tacacs tacacs-ds talk telnet time uucp whois www TCP ポート番号(0～65535)	
UDP ポート番号	プロトコルで"udp"を指定した場合に、対象とする UDP ポート番号を指定します。	**UDP ポート番号** biff bootpc bootps discard dnsix domain echo isakmp mobile-ip nameserver netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip snmp snmptrap sunrpc syslog tacacs tacacs-ds talk tftp time	全ての UDP ポート番号

		who xdmcp UDP ポート番号(0～65535)	
precedence-value※1	precedence-value を設定します。	0～7	省略不可
precedence-named-value※1	precedence-named-value を設定します。	routine(0) priority(1) immediate(2) flash(3) flash-override(4) critical(5) internet(6) network(7)	省略不可
tos-value※1	tos-value を設定します。	0～15	省略不可
tos-named-value※1	tos-named-value を設定します。	min-momentary-cost(1) max-reliability(2) max-throughput(4) min-delay(8) normal(0)	省略不可
dscp-value※1	dscp-value を設定します。	0～63	省略不可
dscp-named-value※1	dscp-named-value を設定します。	ef(101110b) bf(000000b) af11(001010b) af12(001100b) af13(001110b) af21(010010b) af22(010100b) f23(010110b) af31(011010b) af32(011100b) af33(011110b) af41(100010b) af42(100100b) af43(100110b)	省略不可
ip-flag-value※1	ip-flag-value を設定します。	0～3、もしくは、0～3:0～3	省略不可

		(ワイルドカードマスク)	
tcp-flag-value※1	tcp-flag-value を設定します。	0～63、もしくは、0～63:0～63(ワイルドカードマスク)	省略不可
traffic-class-value	traffic-class-value を設定します。	0～255、もしくは、0～255:0～255(ワイルドカードマスク)	省略不可
flow-label	flow-label を設定します。	0～1048575	省略不可
log	パケットフィルタリング機能において該当条件(行単位)にヒットしたパケットが、フィルタリングログに記録されます。 ※dynamic 指定の場合、学習した学習フィルタにヒットしたパケットは記録しません。	log	フィルタリングログを記録しません。
count	統計情報としてフィルタにヒットしたパケット数、バイト数を表示します。 ※dynamic 指定の場合、学習した学習フィルタにヒットしたパケットは記録しません。	count	カウントを行いません。

※1 これらのパラメータをフィルタリングで使用する事はできません。
※2 パラメータ fqdn-list は、V1.02(00)以降サポート
※3 パラメータ fqdn-list 番号の設定範囲 1～50 は、V01.04(00)以降サポート

この設定を行わない場合

access-list を使用した機能を使用できません。

設定モード

基本設定モード

ip access-group

access-list コマンドで指定したフィルタリングデータを、各インタフェースで適用します。
フィルタリングデータは、各インタフェースで受信したパケットに適用するのか、送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。(ダイヤラーは除く)

設定例１　access-list 1 で指定したデータを、LAN 送信時に適用する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip access-group 1 out
```

設定例２　access-list 2 で指定したデータを、LAN からの受信時に適用する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip access-group 2 in
```

コマンド書式

ip access-group <access-list 番号> { in [interface | vpn]| out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	フィルタリングのデータを設定したアクセスリストの番号を指定します。	1～99 100～199 1300～1999 2000～2699 10000～11200 20000～21199	省略不可
{ in[interface | vpn]| out }	インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。 受信時は、さらに以下のように設定ができます。 in vpn：自局宛 VPN 対象パケットを制御 in interface：自局宛非 VPN 対象パケットを制御	in in vpn in interface out	省略不可

LAN インタフェースおよび IPsec インタフェースでは、vpn を選択することはできません。
in vpn および in interface を選択した場合、適用する access-list の宛先は、any とする必要があります。

この設定を行わない場合

設定しているインタフェースでは、IP パケットフィルタリングを使用しません。

IP フィルタリングについて

指定したパケット以外は中継しないといったように、セキュリティ強化のため使用する機能です。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード
BVI インタフェース設定モード
USB Ethernet インタフェース設定モード

ip stateful max-sessions

学習フィルタリングテーブルの総数を設定します。
ここで設定する総数は、IPv4/IPv6 で使用する学習フィルタリングテーブルの総数となります。
NAT を併用している場合、NAT 変換テーブルのセッション数も併せて拡張してください。

設定例　学習フィルタリングテーブルを 16384 セッション分設定する

```
Router(config)#ip stateful max-sessions 16384
```

コマンド書式

ip stateful max-sessions 〈セッション数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セッション数	学習フィルタリングテーブルの最大数を設定します。	2048～65535	省略不可

この設定を行わない場合

学習フィルタリングテーブルの最大数は、2048 になります。

設定モード

基本設定モード

スタティックルーティングの設定

ip route

本装置の、IPv4 スタティックルートを指定します。
PPPoE や EWAN 使用する場合は、Nexthop の IP アドレスがわからないケースがありますので、Nexthop としてインタフェースを指定することもできます。
Nexthop として EWAN・USB Ethernet インタフェースを指定できるのは、WAN 側の運用形態が DHCP クライアントの場合のみです。
この場合、"nexthop"は DHCP サーバから取得した"default gateway の IP アドレス"となります。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.1.0/24 宛の Nexthop を 192.168.2.254 とする場合

```
Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.254
```

設定例２　192.168.1.0/24 宛の Nexthop を、PPPoE1 インタフェースとする場合

```
Router(config)#ip route 192.168.1.0 255.255.255.0 pppoe 1
```

設定例３　デフォルトルートを PPPoE１インタフェースとする場合

```
Router(config)#ip route 0.0.0.0 0.0.0.0 pppoe 1
```

コマンド書式

```
ip route <宛先ネットワーク> <マスク> { <NextHop> | <インタフェース名>|
        connected { ipsecif <1-2000> | null 0 | lan <1-1> | ewan <1-2> | vlan
        <1-150> | usb-ethernet <1-2> } } [<distance>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先ネットワーク	スタティックルーティングの宛先ネットワークアドレス	IPv4 アドレス形式	省略不可
マスク	宛先ネットワークに対するマスク	IPv4 アドレス形式	省略不可
NextHop	宛先へ到達するための NextHop の IP アドレス	IPv4 アドレス形式	インタフェース名を設定する必要があります

インタフェース名	宛先へ到達するためのインタフェース名 PPPoE のように、NextHop の IP アドレスが明確にわからない場合に指定します。	ewan 1～2 pppoe 1～24 tunnel 1～2000 dialer 1～20 usb-ethernet 1～2	NextHop の IP アドレスを設定する必要があります。
connected ipsecif <1-100>	宛先への経路として、IPsec インタフェースを指定します。	ipsecif 1～2000	
connected null 0	廃棄用の宛先経路情報とします	null 0	
connected lan <1-1>	宛先を LAN インタフェースの connected として扱います。	lan 1～1	
connected ewan <1-2>	宛先を EWAN インタフェースの connected として扱います。	ewan 1～2	
connected vlan <1-150>	宛先を VLAN インタフェースの connected として扱います。	vlan 1～150	
connected usb-ethernet <1-2>	宛先を USB Ethernet インタフェースの connected として扱います。	usb-ethernet 1～2	
distance	スタティックルーティングの distance 値を指定します。	2～255※1	1

最大エントリ数：30000 エントリ（ルーティングテーブル自体は 60000 エントリ）
※1 distance 値に 255 を設定した場合、その経路情報は無効扱いとなります。

この設定を行わない場合

スタティックルーティングは設定されません。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	–	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

基本設定モード

ルートマップの設定

match interface

ネクストホップへの送信インタフェースが一致する経路情報を対象とします。
この設定は、RIP、OSPF に対して有効となります。
この設定を OSPF で使用する場合、指定したインタフェースに対し OSPF の設定がされていないと、インタフェース名が同じでも一致の判定となりません。

refresh コマンド後に有効になるコマンドです。

設定例 1　スタティックルートについて EWAN1 から送信するもののみ RIP 広告（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#match interface ewan 1
Router(config-rmap map1 permit 1)#exit

Router(config)#router rip
Router(config-rip)#redistribute static route-map map1
Router(config-rip)#exit
```

コマンド書式

match interface <インタフェース名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	特定するインタフェース名を指定します。	インタフェース名形式	省略不可

この設定を行わない場合

パケット送信インタフェースの特定を行いません。

設定モード

Route-map 設定モード

match ip address

access-list(standard)に一致する経路情報を対象とします。
この設定は、RIP、BGP、OSPF に対して有効となります。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(10.0.0.1) には、"192.168.1.0"の情報のみ送信する（ルートマップ名：map1）

```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255

Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#match ip address 1
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

match ip address <access-list 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	IP アドレスに一致する access-list 番号を指定します	1～99 1300～1999 10000～11200	省略不可

設定モード

Route-map 設定モード

match ip next-hop

next-hop が一致する経路情報を対象とします。
この設定は、RIP、BGP、OSPF に対して有効となります。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(10.0.0.1) には、Next-Hop が"192.168.10.1"の情報のみ送信する（ルートマップ名：map1）

```
Router(config)#access-list 1 permit 192.168.10.1 0.0.0.0

Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#match ip next-hop 1
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

match ip next-hop <access-list 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	Next-hop に一致する access-list 番号、または IP アドレスを指定します。	1～99 1300～1999 10000～11200 IPv4 アドレス形式	省略不可

設定モード

Route-map 設定モード

match metric

metric/med/cost 値が一致する経路情報を対象とします。
この設定は、RIP、BGP、OSPF に対して有効となります。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(10.0.0.1) には、メトリック値=3 で保持している経路情報のみ送信する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#match metric 3
Router(config-rmap map1 permit 1)#exit



Router(config)#router bgp 100
Router(config-bgp)#redistribute connected route-map map1
```

コマンド書式

match metric <メトリック値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
メトリック値	メトリック値に一致する経路を特定します。	0～4294967295	省略不可

設定モード

Route-map 設定モード

route-map

Route-map 設定モードに移行します。
Route-MAP とは、ルート情報の送受信条件や送受信先を詳細に規定しておくものです。
ルート情報の送受信条件や送受信対象を"match "で特定し、送受信するルート情報を"set "で編集します。
no route-map を指定した場合は、Route-map で設定した内容をすべてクリアします。

設定例 1　Route-map 名=map1 の Route-map 設定モードに移行する

```
Router(config)# route-map map1 permit 1
Router(config-rmap map1 permit 1)#
```

コマンド書式

route-map <Route-map 名> <属性> <シーケンス番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Route-map 名	各種ルーティングプロトコルで、Route-map を指定する場合の名称になります。	文字列	省略不可
属性	このルートマップが許可する属性(permit)なのか、許可しない属性(deny)なのかを指定します。	permit deny	省略不可
シーケンス番号	同じルートマップ名で、複数の操作を行なう場合に、複数の属性を指定します。 ここにつける番号が、シーケンス番号です。	1～65535	省略不可

この設定を行わない場合

詳細な経路の制御を使用できない場合があります。

Route-map 詳細

Route-map の詳細について説明します。
Route-map は、ルーティングプロトコルの、各種パラメータの操作・経路情報のフィルタリングのために使用します。

例1　BGP で広告する場合は、メトリック(MED 値)を 5 としたい

本装置では、何も指定しない場合は MED のアトリビュートを付加せずに BGP のアップデート情報を通知しますが、Route-map を利用することにより、MED アトリビュートをつけて BGP のアップデートを通知することができます。

設定モード

基本設定モード

set aggregator

BGP で経路集約を行ったルータの AS 番号とルータ ID を Aggregator 属性に設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(10.0.0.1) には、Aggregator 属性をつけて UPDATE 情報を送信する (AggregatorAS=100、Aggregator Origin=192.168.100.1)

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set aggregator as 100 192.168.100.1
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set aggregator as <AS 番号> <IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
AS 番号	AggregatorAS の AS 番号を設定します。	1～65535	省略不可
IP アドレス	Aggregator Origin の IP アドレスを設定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

Aggregator 属性を操作しません。

設定モード

Route-map 設定モード

set as-path prepend

BGP で経路情報を広告する際に追加する AS 番号を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(10.0.0.1) には、AS-PATH 属性として、300 をつけて送信する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set as-path prepend 300
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set as-path prepend <AS 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
AS 番号	AS-PATH 属性に付加する AS 番号を設定します。	1～65535	省略不可

この設定を行わない場合

AS-PATH 属性を操作しません。

設定モード

Route-map 設定モード

set atomic-aggregate

BGP で経路集約したことを示す atomic-aggregate 属性を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(10.0.0.1) には、ATOMIC-AGGREGATE 属性をつけて送信する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set atomic-aggregate
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

```
set atomic-aggregate
```

パラメータ

パラメータはありません。

この設定を行わない場合

ATOMIC-AGGREGATE 属性を追加しません。

設定モード

Route-map 設定モード

set community

BGP で COMMUNITY 属性を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(10.0.0.1) には、COMMUNITY 属性として"no-export"を設定する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set community no-export
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set community <コミュニティ属性値>

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>コミュニティ属性値</td><td>コミュニティ属性値を設定します。
<table><tr><td>local-AS</td><td>NO-EXPORT-SUBCONFED コミュニティ</td></tr><tr><td>no-advertise</td><td>NO-ADVERTISE 属性</td></tr><tr><td>no-export</td><td>NO-EXPORT 属性</td></tr><tr><td>A:B</td><td>コミュニティ値を設定</td></tr></table></td><td>local-AS
no-advertise
no-export
A:B</td><td>省略不可</td></tr>
</table>

この設定を行わない場合

コミュニティ属性を操作しません。

設定モード

Route-map 設定モード

set community-additive

BGP で BGP COMMUNITIES 属性を設定します。set community が、BGP COMMUNITIES 属性の置換であるのに対し、set community-additive は追加することができます。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(10.0.0.1) には、COMMUNITY 属性として"no-advertise"を追加する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set community-addtive no-advertise
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set community-addtive <コミュニティ属性値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
コミュニティ属性値	追加するコミュニティ属性値を設定します。 local-AS：NO-EXPORT-SUBCONFED コミュニティ no-advertise：NO-ADVERTISE 属性 no-export：NO-EXPORT 属性 A:B：コミュニティ値を設定	local-AS no-advertise no-export A:B	省略不可

この設定を行わない場合

コミュニティ属性を追加しません。

設定モード

Route-map 設定モード

set ip next-hop

RIP、BGP で経路情報の nexthop を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(10.0.0.1) には、NEXT-HOP 属性として、192.168.100.1 をつけて送信する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set ip next-hop 192.168.100.1
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set ip next-hop <IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP の Next-Hop 属性に設定する IP アドレスを設定します	IPv4 アドレス形式	省略不可

この設定を行わない場合

Next-Hop 属性を操作しません。

設定モード

Route-map 設定モード

set local-preference

BGP で local-preference 値を設定します。
デフォルトは 100 で、値が大きい方が優先度が高くなります。
内部 AS のネイバールータに対して、外部 AS への優先パスを示す属性で、同一の AS 内のルータ間でのみ交換されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(10.0.0.1) には、LOCAL_PREF (300) で UPDATE 情報を送信する

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set local-preference 300
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set l ocal-preference <LOCAL-PRE 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
LOCAL-PREF 値	指定する BGP のローカルプリファレンス値を設定します。	0～4294967295	省略不可

この設定を行わない場合

ローカルプリファレンス値を操作しません。

設定モード

Route-map 設定モード

set metric

RIP の metric 値、BGP の MED 値、OSPF の cost 値を設定します。
いずれの場合も値が小さい方が優先度が高くなります。
BGP の場合、2 つの AS 間でのみ有効な属性で、別の AS に通知されることはありません。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(10.0.0.1)には、MED 値（300）で UPDATE 情報を送信する

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set metric 300
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set metric <メトリック値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
メトリック値	RIP や BGP で使用するメトリック値/MED 値を指定します。	1～4294967295	省略不可

この設定を行わない場合

メトリック値を操作しません。

設定モード

Route-map 設定モード

set origin

BGP で ORIGIN 属性を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(10.0.0.1) には、ORIGIN 属性として"EGP"を設定する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set origin egp
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set origin <ORIGIN 属性>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ORIGIN 属性	BGP の ORIGIN アトリビュートにセットする ORIGIN 属性を指定します。 egp：EGP を設定する igp：IGP を設定する incomplete：INCOMPLETE を設定する	egp igp incomplete	省略不可

この設定を行わない場合

ORIGIN 属性を変更しません。

設定モード

Route-map 設定モード

set originator-id

BGP で Originator-ID をセットします。
Originator-ID とは、プレフィックス情報を生成したルータの IP アドレスを意味します。

refresh コマンド後に有効になるコマンドです。

設定例１　Originator-ID に、192.168.1.1 をセットする

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set originator-id 192.168.1.1
```

コマンド書式

set originator-id <IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP の Originator-ID にセットする IP アドレスを設定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

Originator-ID を変更しません。

設定モード

Route-map 設定モード

set tag

OSPF で AS 外部経路のタグ値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　AS 外部経路のタグ値を 150 とします

```
Router(config)#route-map tag150 permit 1
Router(config-rmap tag150 permit 1)#set tag 150
```

コマンド書式

set tag <タグ値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タグ値	AS 外部経路のタグ値を指定します。	0～4294967295	省略不可

この設定を行わない場合

External Route Tag には 、0 が設定されます。

設定モード

Route-map 設定モード

set weight

BGP で受信した経路情報の weight 値を設定します。
自装置内でのみ有効になる属性で、Weight 値は大きい方が優先度は高くなります。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）の Weight 値を 65535（最優先）にする

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set weight 65535
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 in
```

コマンド書式

set weight <weight 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
weight 値	BGP の Weight 値にセットする値を設定します。 WEIGHT 値の大きい BGP ピアからの情報が優先されます。	0～65535	省略不可

この設定を行わない場合

weight 値は 0 となります。

設定モード

Route-map 設定モード

リゾルバの設定

ip name-server

本装置で、DNS リゾルバを動作させる場合に、DNS サーバの IP アドレスを設定します。

設定例　プライマリ DNS サーバに xxx. xxx. xxx. 1、セカンダリ DNS サーバに xxx. xxx. xxx. 2 を設定する

```
Router(config)#ip name-server xxx.xxx.xxx.1
Router(config)#ip name-server xxx.xxx.xxx.2
```

コマンド書式

ip name-server <DNS アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DNS アドレス	DHCP で通知するプライマリ DNS サーバの IP アドレス	IPv4 アドレス形式	省略不可

最大エントリ数：3 エントリ（ipv4,ipv6 合わせて3エントリ）

※ DNS アドレスの優先度は、入力した順に3つまで有効になります。すでに、3つ入力されている状態で4つ目以降を入力しても設定上無効となります。

この設定を行わない場合

DNS リゾルバを使用することはできません。ただし、PPPoE や DHCP クライアント機能で、DNS の IP アドレスを学習している場合は、DNS リゾルバ機能を使用できます。

DNS リゾルバとは・・・

本装置から送信(中継ではない)するデータに関して、ホスト名が指定されている場合に、名称から IP アドレスを獲得するために DNS サーバに問い合わせを行なう機能です。
本装置から送信するデータには、以下の種類があります。

本装置から送信するデータには、以下の種類があります。
・ping
・traceroute
・SMTP
・SNMP
・syslog
・telnet クライアント
があります。
ping / traceroute を実行する場合はコマンドのオプションで、SMTP/SNMP の場合はサーバの設定にホスト名を指定しても、DNS リゾルバ機能を使用して IP アドレスを解決し、通信を行なうことができます。
DNS リゾルバで取得した IP アドレスの情報は、"show ip resolver-cache"コマンドで確認することができます。

実行例

```
Router#ping www
Sending 5, 100-byte ICMP Echos to xxx.xxx.xxx.xxx, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/10 ms

Router#show ip resolver-cache

<resolver dns table>
1th direction = [1] (name to addr)
IPv4 Address = [xxx.xxx.xxx.xxx]
Hostname = [www.xxxxxx.ne.jp]

Router#
```

ip name-server に xxx.xxx.xxx.1／ip domain-name に xxxxxx.ne.jp が設定されている場合に、ホスト名(www)宛の ping を実行すると、DNS サーバ(xxx.xxx.xxx.1)に問い合わせを行い、ホスト名(www.xxxxxx.ne.jp)から IP アドレス(xxx.xxx.xxx.xxx)を解決し、ping を送信します。
show ip resolver-cache コマンドで、ホスト名(www.xxxxxx.ne.jp)が IP アドレス(xxx.xxx.xxx.xxx)であることが確認できます。

設定モード

基本設定モード

ip name-server source-interface

DNS リゾルバを使用する場合の、DNS サーバへ送出する送信元 IP アドレスとして使用するインタフェース名を指定します。

設定例 1　DNS サーバへ送信する際の送信元アドレスに LAN インタフェースの IP アドレスを使用する

```
Router(config)#ip name-server source-interface lan 1
```

コマンド書式

ip name-server source-interface <インタフェース名 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	DNS サーバへ送信する際の送信元アドレスに使用するインタフェースアドレス	lan 1 ewan 1～2 loopback 1～100 vlanif 1～150	省略不可

この設定を行わない場合

DNS サーバへ実際に送信するインタフェースになります。

設定モード

基本設定モード

ip domain-name

本装置で、DNS リゾルバを動作させる場合に、ドメイン名を設定します。
DNS リゾルバとは、名称から IP アドレスを獲得するために、DNS サーバにリクエストをする機能です。
ここで、ドメイン名を指定した場合、DNS にて IP アドレスを解決する際、ホスト名の後にここで設定したドメイン名をつけて、DNS サーバにリクエストします。

例）
ip domain-name xxxxx.ne.jp と設定して、"ping www"とした場合、DNS サーバには、www.xxxxx.ne.jp の IP アドレスを解決するようリクエストします。

設定例　DNS リゾルバで使用するドメイン名を"xxxxxx.ne.jp"に設定する

```
Router(config)#ip domain-name xxxxxx.ne.jp
```

コマンド書式

ip domain-name <ドメイン名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ドメイン名	DHCP で通知するドメイン名称	254 文字以内の文字列	省略不可

この設定を行わない場合

DNS リゾルバ使用時に、ドメイン名を省略することはできません。

DNS リゾルバとは・・・

本装置から送信(中継ではない)データに関して、ホスト名が指定されている場合に、DNS サーバに問い合わせを行なう機能です。
本装置から送信するデータには、以下の種類があります。

- ping
- traceroute
- SMTP
- SNMP
- syslog
- telnet クライアント

があります。
ping / traceroute を実行する場合はコマンドのオプションで、SMTP/SNMP の場合はサーバの設定にホスト名を指定しても、DNS リゾルバ機能を使用して IP アドレスを解決し、通信を行なうことができます。
DNS リゾルバで取得した IP アドレスの情報は、"show ip resolver-cache"コマンドで確認することができます。

実行例

```
Router#ping www
Sending 5, 100-byte ICMP Echos to xxx.xxx.xxx.xxx, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/10 ms

Router#show ip resolver-cache

<resolver dns table>
1th direction = [1] (name to addr)
IPv4 Address = [xxx.xxx.xxx.xxx]
Hostname = [www.xxxxxx.ne.jp]


Router#
```

ip name-server に xxx.xxx.xxx.1／ip domain-name に xxxxxx.ne.jp が設定されている場合に、ホスト名(www)宛の ping を実行すると、DNS サーバ(xxx.xxx.xxx.1)に問い合わせを行い、ホスト名(www.xxxxxx.ne.jp)から IP アドレス(xxx.xxx.xxx.xxx)を解決し、ping を送信します。
show ip resolver-cache コマンドで、ホスト名(www.xxxxxx.ne.jp)が IP アドレス(xxx.xxx.xxx.xxx)であることが確認できます。

設定モード

基本設定モード

ip resolver-cache-time

本装置で DNS リゾルバを動作させる場合に、学習した DNS 情報を保持しておく時間を設定します。

設定例 1　DNS 情報を保持しておく時間を 30 秒に設定する

```
Router(config)#ip resolver-cache-time 30
```

コマンド書式

ip resolver-cache-time <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	DNS 情報を保持しておく時間（秒）	0～3600	省略不可

この設定を行わない場合

DNS 情報を保持しません。

DNS リゾルバとは・・・

本装置から送信（中継ではない）データに関して、ホスト名が指定されている場合に、DNS サーバに問い合わせを行なう機能です。
本装置から送信するデータには、以下の種類があります。

- ping
- traceroute
- SMTP
- SNMP
- syslog
- telnet クライアント

があります。
ping / traceroute を実行する場合はコマンドのオプションで、SMTP/SNMP の場合はサーバの設定にホスト名を指定しても、DNS リゾルバ機能を使用して IP アドレスを解決し、通信を行なうことができます。
DNS リゾルバで取得した IP アドレスの情報は、"show ip resolver-cache"コマンドで確認することができます。

実行例

```
Router#ping www
Sending 5, 100-byte ICMP Echos to xxx.xxx.xxx.xxx, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/10 ms

Router#show ip resolver-cache

<resolver dns table>
1th direction = [1] (name to addr)
IPv4 Address = [xxx.xxx.xxx.xxx]
Hostname = [www.xxxxxx.ne.jp]


Router#
```

ip name-server に xxx.xxx.xxx.1／ip domain-name に xxxxxx.ne.jp が設定されている場合に、ホスト名（www）宛の ping を実行すると、DNS サーバ（xxx.xxx.xxx.1）に問い合わせを行い、ホスト名（www.xxxxxx.ne.jp）から IP アドレス（xxx.xxx.xxx.xxx）を解決し、ping を送信します。
show ip resolver-cache コマンドで、ホスト名（www.xxxxxx.ne.jp）が IP アドレス（xxx.xxx.xxx.xxx）であることが確認できます。

設定モード

基本設定モード

ip resolver-retries

本装置で、DNS リゾルバを動作させる場合の、リゾルバ問合せのリトライ回数、リトライ間隔(秒)、リクエストタイムアウト(秒)、タイムアウト(秒)を指定します。

設定例 1　DNS リゾルバの問い合わせを、リトライ回数 5 回、リトライ間隔 2 秒、リクエストタイムアウト 10 秒、タイムアウト 20 秒に設定する

```
Router(config)#ip resolver-retries 5 interval 2 request-timeout 10 timeout 20
```

コマンド書式

ip resolver-retries <リトライ回数> interval <リトライ間隔> request-timeout <リクエストタイムアウト時間> timeout <タイムアウト時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リトライ回数	リゾルバ問い合わせ回数を設定します。	0～5	省略不可
リトライ間隔	リゾルバ問い合わせ間隔を設定します。	1～5	省略不可
request-timeout 時間	リゾルバ問い合わせリクエストタイムアウトを設定します。	1～60	省略不可
timeout 時間	リゾルバ問い合わせタイムアウトを設定します。	1～60	省略不可

この設定を行わない場合

リトライ回数 3 回、リトライ間隔 1 秒 、リクエストタイムアウト 5 秒、タイムアウト 10 秒に設定します。

設定モード

基本設定モード

MTU 長

ip mtu

インタフェースの MTU 長を指定します。

PPPoE および Dialer インターフェースの MTU については、新規セッション(回線の再接続後)から有効となります。
また、LCP で取得した MRU オプション値と設定 MTU 値との比較により、小さい値をセッション MTU 値として使用します。

refresh コマンド後に有効になるコマンドです。

設定例 1　PPPoE1 の MTU 長を 1400byte にする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip mtu 1400
```

コマンド書式

ip mtu <MTU 長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MTU 長	MTU 長を指定します。	lan 256～1500 pppoe 578～1492 ewan 256～1500 modem 256～1500 vlan 256～1500 ipsec 576～1500 tunnel 256～1500 bvi 256～1500 USB Ethernet 256～1500	省略不可

この設定を行わない場合

各インタフェースにより以下のようになります。通常は変更の必要はありません。

LAN：1500
PPPoE：1454
EWAN：1454
MOCEM：1500
VLAN：1500
IPsec：1390
Tunnel：1480
BVI：1500
USB Ethernet：1500

MTU 長とは？

MTU とは（Max Transfer Unit）の略で、MTU 長とは、通常、1 パケットで運ぶことができる IP パケット（IP ヘッダ＋IP ペイロード）の長さをいいます。

設定モード

LAN インタフェース設定モード
PPPoE インタフェース設定モード
EWAN インタフェース設定モード
モデムインタフェース設定モード
VLAN インタフェース設定モード
IPsec インタフェース設定モード
トンネルインタフェース設定モード
BVI インタフェース設定モード

TCP MSS

mss

インタフェースの MSS 値を指定します。
本装置では、TCP ヘッダオプションに含まれる MSS 値を適切な値に書き換えることができます。
パケットに書かれている値と設定値を比較して小さい方の値にします。

refresh コマンド後に有効になるコマンドです。

設定例 1　LAN の MSS 値を 1300byte にする

```
Router(config)#mss lan 1 1300
```

コマンド書式

mss {<インタフェース名>|ipsec}　<MSS 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	インタフェースを指定します。	lan 1 ewan 1～2 pppoe 1～24 ipsecif 1～2000 vlanif 1～150 tunnel 1～2000 usb-ethernet 1～2	省略不可
ipsec	ポリシーベース IPsec の場合に指定します。	ipsec	省略不可
MSS 値	MSS 値を指定します。 off を指定した場合は、MSS 値を変更しません。 ipseif の場合は、VPN セレクタの MSS 値を指定します。※1	216※3～1460※2 off	省略不可

※1 IPsec interface 以外に提供される VPN セレクタの MSS 値の指定となります。
※2 次の設定値の上限は、ipsec 1420、tunnel 1440、usb-ethernet 1440、pppoe 1452 となります。
※3 設定値の下限の 216 はV01.04(00)以降サポート

この設定を行わない場合

各インタフェースからパケットを送出する際に、下記の値とパケットに書かれている値を比較して小さい方の値にします。通常は変更の必要はありません。

LAN interface：MTU 長 −40
EWAN interface：MTU 長 −40
PPPoE interface：MTU 長 −40
IPsec interface：MTU 長 −40
IPsec VPN selector：（送信 IF の MTU ）−113
Tunnel interface：MTU 長 −40
VLANIF interface：MTU 長 −40
USB Ethernet interface：MTU 長 −40

MSS 長とは？

MSS (Maximum Segment Size)とは、TCP で一度に伝送できるデータの最大量。
最大セグメントサイズ。

設定モード

基本設定モード

ProxyARP の設定

ip proxy-arp

インタフェースで ProxyARP を動作させる場合に指定します。

refresh コマンド後に有効になるコマンドです。(VLAN インタフェース設定モードのみ)

設定例 1　LAN インタフェースで ProxyARP 機能を動作させる

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip proxy-arp
```

コマンド書式

```
ip proxy-arp [include-default-route]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
include-default-route	デフォルトルートにヒットするあて先の ARP Request に対して、ProxyARP を行う場合に指定します。	include-default-route	デフォルトルートのみにヒットするあて先への ARP Request に対しては ProxyARP しない。

この設定を行わない場合

ProxyARP 機能が動作しません。

ProxyARP 機能とは？

自身が中継すべき相手の IP アドレスに対する ARP を受信した際に、代理にその ARP に答える機能を ProxyARP 機能といいます。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ARP 制御の設定

ip arp 802.1p-priority

ARP パケット(リクエスト/リプライ)の、出力時の 802.1p 値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例　ARP パケット出力時の 802.1p 値を 6 とする

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip arp 802.1p 6
```

コマンド書式

ip arp 802.1p-priority <802.1p 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
802.1p 値	ARP パケット出力時の 802.1p 値を設定します。	0～7	省略不可

この設定を行わない場合

ARP パケット出力時の 802.1p 値を 0 とします。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ip arp learning

受信した ARP により、ARP テーブルを登録するかどうかの設定をします。

refresh コマンド後に有効になるコマンドです。

設定例　ARP テーブルの登録を行わない

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip arp learning disable
```

コマンド書式

ip arp learning <登録設定>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
登録設定	受信した ARP により、ARP テーブルを登録するかどうかの指定をします。 enable：ARP の登録を行う disable：ARP の登録を行わない request：ARP リクエストでのみ登録を行う reply：ARP リプライでのみ登録を行う	enable disable request reply	省略不可

この設定を行わない場合

ARP リクエストおよびリプライにより、ARP テーブルの登録を行います。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ip arp reply

ARP リクエストに応答するかどうかを設定します。
ARP テーブルで管理されている相手からのみ応答する制御を行うことにより、管理外の端末からのデータ中継を行わない制御が可能になります。

refresh コマンド後に有効になるコマンドです。

設定例　ARP テーブルに登録されている IP アドレスからの ARP リクエストにのみ応答する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip arp reply authorized
```

コマンド書式

ip arp reply <応答設定>

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
応答設定	ARP リクエストに応答するかどうかを設定します。		enable disable authorized	省略不可
	enable	ARP Reply を送信する		
	disable	ARP Reply を送信しない		
	authorized	ARP テーブルに存在する IP アドレスからの ARP リクエストにのみ応答する		

この設定を行わない場合

全ての ARP リクエストに応答します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ip arp request

ARP リクエストを送信するかどうかの設定をします。
全ての端末をスタティック ARP で管理するような場合は、ARP リクエストの送信を行わない運用が効果的です。

refresh コマンド後に有効になるコマンドです。

設定例　ARP リクエストを送信しない

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip arp request disable
```

コマンド書式

ip arp request <送信設定>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信設定	ARP リクエストを送信するかどうかの指定をします。 enable　ARP リクエストを送信する disable　ARP リクエストを送信しない	enable disable	省略不可

この設定を行わない場合

ARP リクエストを送信する。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ip arp static

スタティック ARP で使用する、IP アドレスと MAC アドレスの組み合わせを設定します。

refresh コマンド後に有効になるコマンドです。

設定例　IP アドレス（192.168.10.1）とＭＡＣアドレス（xxxx.xxxx.xxxx）をスタティック ARP に登録する

```
Router(config)#ip arp static 192.168.10.1 xxxx.xxxx.xxxx
```

コマンド書式

ip arp static <IP アドレス> <MAC アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	スタティック ARP で使用する、IP アドレスと MAC アドレスを指定します。	IPv4 アドレス形式	省略不可
MAC アドレス		MAC アドレス形式	省略不可

最大エントリ数：学習エントリとスタティックエントリあわせて 2048 エントリ。

この設定を行わない場合

スタティック ARP を登録しません。

設定モード

基本設定モード

ip arp timeout

ARP テーブルのエージアウト時間を設定します。
ARP タイムアウト値を変更後 refresh した際は、ARP エントリを全て初期化します。

refresh コマンド後に有効になるコマンドです。

設定例　ARP のエージアウトを 30 分とする

```
Router(config)#ip arp timeout 30
Router(config)#
```

コマンド書式

ip arp timeout <ARP タイムアウト値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ARP タイムアウト値	ARP テーブルのエージアウト時間（単位：分）を設定します。	1～60	省略不可

この設定を行わない場合

ARP タイムアウト値を 20 分とします。

設定モード

基本設定モード

ダイレクトブロードキャストの設定

ip directed-broadcast

インタフェースのネットワークブロードキャストアドレス宛の中継パケットを、ブロードキャストパケットとして中継する場合に設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN インタフェースに対して、ダイレクトブロードキャストを行う。

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip directed-broadcast
```

コマンド書式

ip directed-broadcast

パラメータ

パラメータはありません。

この設定を行わない場合

インタフェースのネットワークブロードキャストアドレス宛の中継パケットは、廃棄します。

ダイレクトブロードキャスト機能とは？

中継パケットにおいて、インタフェースのネットワークブロードキャストアドレス宛のパケットを、そのインタフェースの配下の端末に対してブロードキャスト中継する機能を、ダイレクトブロードキャストといいます。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ICMP 制御の設定

ip icmp error-ratelimit

本装置が、ICMP を使ってエラーを送信する際の、1 秒間に送信する最大送信パケット数を設定します。1 秒間に送信するパケット数が規定数を超過した場合に、次の 1 秒まで送信を抑止します。
0 を指定した場合、ICMP エラーメッセージおよび REDIRECT メッセージは送信されません
エラーパケットにより、データ通信のための帯域が減ってしまうのを防ぐ機能です。

refresh コマンド後に有効になるコマンドです。

設定例 1　エラーパケットを、最大 300 パケット/秒とする

```
Router(config)#ip icmp error-ratelimit 300
```

コマンド書式

```
ip icmp error-ratelimit {パケット数/秒 | unlimit}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
パケット数	IP ICMP でエラーを送信する際の 1 秒間に送信する最大送信パケット数を設定します。 unlimit を指定することで、ICMP エラーメッセージおよび REDIRECT メッセージのレート制限を行いません。	0～2147483647 unlimit	省略不可

この設定を行わない場合

100 パケット/秒が設定されます。

IP ICMP エラーパケットの種類

IP ICMP エラーパケットには、以下の種類があります。

Type	内容
3	受信したパケットの宛先への中継ができない
4	資源不足のため、パケットを廃棄
5	中継先を別のルータに変更したことを通知
11	ホップ数が制限を越えたため、転送できない
12	IPv4 ヘッダ（オプションを含む）が異常、もしくは未知

設定モード

基本設定モード

ip source-quench

ICMPv4 もしくは、SourceQuench を受信した際に、TCP ウィンドウ制御に反映するかどうかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　SourceQuench を受信した場合、TCP ウィンドウ制御に反映する

```
Router(config)#ip source-quench enable
```

コマンド書式

ip source-quench <ウィンドウ制御>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ウィンドウ制御	SourceQuench を受信した際に、TCP ウィンドウ制御に反映するかどうかを指定します。 enable　TCP ウィンドウ制御に反映する。 disable　TCP ウィンドウ制御に反映しない。	enable disable	省略不可

この設定を行わない場合

SourceQuench を受信しても TCP ウィンドウ制御に反映しません。

設定モード

基本設定モード

ポリシールーティング

クラスマップの定義

class-map

クラスマップモードに移行し、トラフィックを分類するクラシファイアを定義します。
クラスマップモードでは、match ip もしくは、match ipv6 コマンドによってトラフィックの分類条件が設定されます。
複数の条件が設定された場合、match-any の有無によって、複数の条件が OR 条件となるか、AND 条件となるかが指定されます。
IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合は、指定された条件は無視されるのではなく、不成立と判定されます。

設定例 1　クラスマップ設定モードへ移行します。

```
Router(config)#class-map video-class
Router(config-class-map)#
```

コマンド書式

class-map <クラスマップ名 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クラスマップ名	クラスマップ名称を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップ名によるトラフィックの分類を行いません。

設定モード

基本設定モード

match-any

同一 class-map 内で複数の match 行が記述された場合の動作を指定します。
いずれか 1 つの match 行にマッチした場合に class-map に適合したと判断します。

refresh コマンド後に有効になるコマンドです。

設定例 1　IP アクセスリストの 100 番もしくは 101 番にマッチするトラフィックを対象とする。

```
Router(config)# class-map video-class
Router(config-class-map)# match-any
Router(config-class-map)# match ip access-group 100
Router(config-class-map)# match ip access-group 101
Router(config-class-map)# exit
```

コマンド書式

```
match-any
```

パラメータ

パラメータはありません

この設定を行わない場合

全ての match 行にマッチした場合に、クラスマップに適合したと判断します。

例として、設定例 1 で match-any を指定しなかった場合は以下のようになります。

```
Router(config)# class-map video-class
Router(config-class-map)# match ip access-group 100
Router(config-class-map)# match ip access-group 101
Router(config-class-map)# exit
```

この場合、IP アクセスリストの 100 番にマッチ、かつ 101 番にマッチするトラフィックを対象とします。

設定モード

クラスマップ設定モード

match ip/ipv6 access-group

クラスマップ内でマッチするトラフィックを、IP アクセスリストにより設定します。
トラフィックが IPv4 パケットの場合、match ipv6 コマンドは不成立となります。逆にトラフィックが IPv6 パケットの場合、match ip コマンドは不成立となります。
複数の match が定義された場合、定義された順に評価されます。
同一 class-map において match-any が指定されている場合には、いずれの match 行にもトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
match-any が指定されていない場合には、いずれかの match 行にトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
アクセスリストの log と count は無視されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　IP アクセスリストの 2000 番をマッチするトラフィックとして設定する。

```
Router(config)#class-map video-class
Router(config-class-map)#match-any
Router(config-class-map)#match ip access-group 2000
Router(config-class-map)#exit
```

コマンド書式

match ip access-group <ext-ipv4 アクセスリスト番号 > [input-interface {<インタフェース名> [port <ポート番号>}]
match ipv6 access-group <ext-ipv6 アクセスリスト番号 > [input-interface {<インタフェース名> [port <ポート番号>]}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ext-ipv4 アクセスリスト番号	クラスマップ内でマッチするトラフィックを ext-ipv4 アクセスリスト番号で指定します。	100～199、2000～2699 20000～21199	省略不可
ext-ipv6 アクセスリスト番号	クラスマップ内でマッチするトラフィックを ext-ipv6 アクセスリスト番号で指定します。	3500～3999 35000～36499	省略不可
インタフェース名	クラスマップ内でマッチするトラフィックを入力インタフェースで指定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 ipsecif 1～2000 tunnel 1～2000 vlanif 1～150	全てのインタフェース
ポート番号	LAN インタフェースの物理ポート番号を指定します。	port 1～8	LAN インタフェースのポート番号

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません

設定モード

クラスマップ設定モード

match ip/ipv6 input-interface

クラスマップ内でマッチするトラフィックを、入力インタフェースにより設定します。
トラフィックが IPv4 パケットの場合、match ipv6 コマンドは不成立となります。逆にトラフィックが IPv6 パケットの場合、match ip コマンドは不成立となります。
複数の match が定義された場合、定義された順に評価されます。
同一 class-map において match-any が指定されている場合には、いずれの match 行にもトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
match-any が指定されていない場合には、いずれかの match 行にトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。

refresh コマンド後に有効になるコマンドです。

設定例１　トラフィックを分類するインタフェースを EWAN 1 として設定する

```
Router(config)#class-map video-class
Router(config-class-map)#match-any
Router(config-class-map)#match ip input-interface ewan 1
Router(config-class-map)#exit
```

コマンド書式

```
match ip input-interface <インタフェース名> [port <ポート番号>]
match ipv6 input-interface <インタフェース名> [port <ポート番号>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	クラスマップ内でマッチするトラフィックを入力インタフェースで指定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 ipsecif 1～2000 tunnel 1～2000 vlanif 1～150	全てのインタフェース
ポート番号	LAN インタフェースの物理ポート番号を指定します。	port 1～8	LAN インタフェースのポート番号

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません

設定モード

クラスマップ設定モード

アクションマップの定義

action-map

アクションマップ設定モードに移行し、トラフィックに対するアクションを定義します。
実行場所によってサポートされないアクションや、IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合、指定されたアクションは無視されます。

設定例１　アクションマップ設定モードへ移行する。

```
Router(config)#action-map stream-action
Router(config-action-map)#
```

コマンド書式

action-map 〈アクションマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクションマップ名	アクションマップ名を設定します	16 文字以内の文字列	省略不可

この設定を行わない場合

アクションは定義されません。

設定モード

基本設定モード

set ip next-hop

アクションとして、パケット中継先を設定します(ポリシールーティング)。
有効な中継先のうち、distance 値がもっとも小さい中継先が有効になります。
有効な中継先のうち、もっとも distance 値が小さい中継先が同一 distance 値で複数存在する場合、config 表示で最も上の設定が適用されます。
distance 値が省略された場合のデフォルトは"1"とします。
中継先が到達不能な場合、その経路は無視されます。
個々の中継先が全て到達不能な場合、もしくは指定されていない場合、set {ip|ipv6} next-hop default が指定されている場合には、通常のルーティングが行なわれます。
指定されていない場合には、パケットは中継不能パケットとして廃棄されます。
パケットが IPv4 の場合、set ipv6 は無視されます。逆にパケットが IPv6 の場合、set ip は無視されます。
本コマンドは、I/F 受信時のサービスポリシーとして設定された場合と、自局送信時のサービスポリシーとして設定された場合にのみ有効となり、I/F 送信時のサービスポリシーとして設定された場合には無視されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　パケット中継先を 192.168.100.1 に distance 10 で設定する。

```
Router(config)#action-map stream-action
Router(config-action-map)#set ip next-hop 192.168.100.1 distance 10
```

コマンド書式

```
set ip next-hop <IP アドレス> [distance (1-255)]
set ip next-hop <インタフェース> [distance (1-255)]
set ip next-hop connected {ipsecif <1-2000> | null <0-0>} [distance (1-255)]
set ip next-hop default
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	中継先の IP アドレスを設定します。	IPv4 アドレス形式	省略不可
インタフェース	PPPoE インタフェースのように、宛先へ到達するための NextHop の IP アドレスが明確に分からない場合に設定します。	ewan 1～2 pppoe 1～24 dialer 1～20 tunnel 1～2000	省略不可
connected ipsecif	宛先への経路として IPsec インタフェースを指定します。	ipsecif 1～2000	省略不可
connected null	廃棄用の宛先経路情報とします。	null 0	省略不可
distance	中継先の distance 値を設定します。	1～255	省略不可
default	ポリシールーティングを行わずに、通常のル	なし	省略不可

	ーティングをおこないます。		

この設定を行わない場合

中継先設定は行なわれません。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

アクションマップ設定モード

ポリシーマップの定義

class

クラスマップとアクションとを対応付け、クラシフィケーションされたトラフィックに対するアクションを定義します。
複数のクラスが定義された場合、登録順に検索され、最初にマッチしたクラスに対するアクションのみが実行されます。
同一クラスマップ名に対しては、一つのアクションのみ記述できます(同一クラスマップ名に対しては、置換型となります)。

refresh コマンド後に有効になるコマンドです。

設定例１　クラスマップ（video-class）とアクションマップ（stream-action）を対応づける

```
Router(config)# policy-map stream-service
Router(config-policy-map)# class video-class action stream-action
Router(config-policy-map)# class audio-class action stream-action
Router(config-policy-map)# exit
```

コマンド書式

class〈クラスマップ名〉action〈アクションマップ名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クラスマップ名	対応づけるクラスマップ名を設定します。	16 文字以内の文字列	省略不可
アクションマップ名	対応づけるアクションマップ名を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップとアクションとの対応は定義されません。

設定モード

ポリシーマップ設定モード

policy-map

policy-map モードに移行し、クラスマップによって分類したトラフィックに対して、どのような制御を行なうかを定義します。

ここで指定したポリシーマップを有効にするには、各インタフェース設定モードで、"service-policy input/output"コマンドで登録します。

また、自局送信をポリシールーティングする場合は、"service-policy local"コマンドで登録します。

設定例１　ポリシーマップ設定モードへ移行する。

```
Router(config)#policy-map stream-service
Router(config-policy-map)#
```

コマンド書式

policy-map 〈ポリシーマップ名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシーマップ名	ポリシーマップ名を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

ポリシーマップの設定を行うことができません。

設定モード

基本設定モード

statistics update

統計情報のカウントを行うかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　統計情報のカウントを行う

```
Router(config)# policy-map stream-service
Router(config-policy-map)# statistics update enable
Router(config-policy-map)# exit
```

コマンド書式

statistics update〈カウント設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
カウント設定	統計情報のカウントを行うかどうかを指定します。 enable　統計情報のカウントを行う disable　統計情報のカウントを行わない	enable disable	省略不可

この設定を行わない場合

統計情報のカウントを行いません。

設定モード

ポリシーマップ設定モード

ポリシールーティング時の NextHop 監視

ip polling-interval

ポリシールーティング時に有効な中継先かどうかを判断するために、指定された中継先に対して監視パケットを送信する際の Ipv4 監視パケット(ARP)の送信間隔を指定します。
ARP またはネイバのキャシュテーブルの参照を行い、IPv4 では MAC アドレスが解決済みであったときに有効であると判定されます。
それ以外は、有効でないと判定されます。
有効である場合、ポリシールーティング機能では、指定された中継先への到達性があると判定し、その中継先を有効な経路と認識します。有効でない場合は、set ip next hop コマンドで設定された次の候補の判定を行います。
定変更後のリフレッシュでは変更前の監視パケット送信後、変更された指定が有効となります。

refresh コマンド後に有効になるコマンドです。

設定例 1　監視パケットの送信間隔を 10 秒にする

```
Router(config)#ip polling-interval 10
```

コマンド書式

ip polling-interval < 監視パケット送信間隔 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
監視パケット送信間隔	IPv4 監視パケット(ARP)の送信間隔を指定します。	5～60	送信間隔を 5 秒に設定します。

この設定を行わない場合

監視パケットの送信間隔が 5 秒に設定されます。

設定モード

基本設定モード

ドメインルーティングの設定

fqdn-list

access-list から参照する fqdn-list を設定します。
fqdn-list では、アドレス解決したい FQDN を指定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　www.fnsc.co.jp を fqdn-list に設定する

```
Router(config)#fqdn-list 1 www.fnsc.co.jp
```

コマンド書式

fqdn-list <fqdn-list 番号> <FQDN>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
fqdn-list 番号	access-list と紐付ける fqdn-list の番号を指定します。	1～50※	省略不可
FQDN	アドレス解決したい FQDN を指定します。	最大 254 文字	省略不可

※ パラメータ fqdn-list 番号の設定範囲 1～50 は、V01.04(00)以降サポート

この設定を行わない場合

access-list で指定された fqdn-list の設定がなければ、該当 access-list の設定が無効になります。

設定モード

基本設定モード

fqdn-list lifetime

fqdn-list に登録された FQDN のアドレスが解決してから、該当アドレスをキャッシュとして保持する時間(単位:秒)を設定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　キャッシュ保持時間を 3600 秒に設定する

```
Router(config)# fqdn-list lifetime 3600
```

コマンド書式

fqdn-list lifetime <保持時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
保持時間	解決したアドレスを保持する時間(単位:秒)を指定します。	120～3600	180

この設定を行わない場合

180 秒となります。

設定モード

基本設定モード

fqdn-list query-interval

fqdn-list に登録された FQDN のアドレス解決を行う間隔(単位:秒)を設定します。
初回アドレス解決時に限り、本設定に関係なく解決するまで 10 回リトライを 10 秒間隔で行います。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　FQDN のアドレス解決を行う間隔を 90 秒に設定する

```
Router(config)# fqdn-list query-interval 90
```

コマンド書式

fqdn-list query-interval <アドレス解決間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレス解決間隔	FQDN の解決を行う間隔(単位:秒)を指定します。	60～90	60

この設定を行わない場合

60 秒間隔となります。

設定モード

基本設定モード

マルチキャストの設定

ip igmp access-group

各インタフェースで、マルチキャストルーティングを許可するグループアドレスをアクセスリスト番号で設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　許可するグループアドレスをアクセスリスト番号 10 とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp access-group 10
```

コマンド書式

ip igmp access-group <アクセスリスト番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクセスリスト番号	許可するグループアドレスを IPv4 標準アクセスリストの中から選択します。	1～99 1300～1999 10000～11200	省略不可

この設定を行わない場合

すべてのグループアドレスを許可します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp fast-leave

各インタフェースで、Fast Leave を有効にするかどうかの設定をします。
複数の受信者が存在するインタフェースでは、この設定を有効にしないでください。

refresh コマンド後に有効になるコマンドです。

設定例 1　Fast Leave を有効にする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp fast-leave
```

コマンド書式

```
ip igmp fast-leave
```

パラメータ

パラメータはありません。

この設定を行わない場合

Query に対して、Report メッセージがタイムアウトしてから、上流に対して Leave メッセージを通知します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp group-membership-timeout

マルチキャストグループに参加するインタフェース情報の保持時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　保持時間を 1500 秒とする

```
Router(config)#ip igmp group-membership-timeout 1500
```

コマンド書式

ip igmp group-membership-timeout <保持時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
保持時間	マルチキャストグループに参加するインタフェース情報の保持時間(単位:秒)を設定します。	30～65535	省略不可

この設定を行わない場合

保持時間を 260 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp last-membership-query-interval

各インタフェースで、Leave 受信後の Group Specific Query に対応する IGMP Report を受信するための待機時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　保持時間を 10 秒とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp last-membership-query-interval 10
```

設定例 2　保持時間を 500 ミリ秒とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp last-membership-query-interval dsec 5
```

コマンド書式

ip igmp last-membership-query-interval [dsec] <待機時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
待機時間	Leave 受信後の Group Specific Query に対応する IGMP Report を受信するための待機時間(単位:秒)を設定します。	1～25	省略不可
dsec	待機時間を 100 ミリ秒単位で設定する場合に指定します。	1～255	秒単位の設定になります。

この設定を行わない場合

保持時間を 1 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp proxy

各インタフェースで、IGMP Proxy によるマルチキャストルーティングを中継するかどうかの設定します。
Snooping および、PIM-SM に関して本装置ではサポートしていません。

refresh コマンド後に有効になるコマンドです。

設定例 1　ipsec インタフェースで IGMP Proxy によるマルチキャストルーティングを中継する

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp proxy
```

コマンド書式

```
ip igmp proxy
```

パラメータ

パラメータはありません。

この設定を行わない場合

マルチキャストルーティングを中継しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp proxy-group

各インタフェースにおいてマルチキャストルーティングを行う際の、IGMP Proxy の動作を有効とするグループアドレスをアクセスリスト番号で指定します。
複数設定された場合には、アクセスリスト番号順にソートされます。
また、インタフェース設定モードと基本設定モードでアクセスリスト番号が重複する場合は、インタフェース設定モードが優先されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　アクセスリスト番号 10 をグループアドレスとして指定する

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp proxy-group 10
```

コマンド書式

ip igmp proxy-group <アクセスリスト番号> [upstream <インタフェース名>]
[seq 優先度]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクセスリスト番号	グループアドレスを IPv4 標準アクセスリストの中から選択します。	1～99 1300～1999 10000～11200	省略不可
インタフェース名	上流インタフェースに指定するインタフェースを選択します。	lan 1 ewan 1～2 ipsecif 1～2000 vlanif 1～150	上流インタフェースを指定しません。
seq 優先度	上流インタフェースに指定したインタフェースに対して、優先度を設定します。 数値が小さい方が優先度が高くなります。	0～255	255

この設定を行わない場合

IGMP Proxy によるマルチキャストルーティングを中継しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp proxy-group-upstream

装置全体としてマルチキャストルーティングを行う際の、IGMP Proxy の動作を有効とするグループアドレスをアクセスリスト番号で指定します。
複数設定された場合には、アクセスリスト番号順にソートされます。
また、インタフェース設定モードと基本設定モードでアクセスリスト番号が重複する場合は、インタフェース設定モードが優先されます。

refresh コマンド後に有効になるコマンドです。

設定例１　アクセスリスト番号 10 をグループアドレス、ipsecif 1 を上流インタフェースとして指定する

```
Router(config)#ip igmp proxy-group-upstream ipsecif 1 10
```

コマンド書式

ip igmp proxy-group-upstream〈インタフェース名〉〈アクセスリスト番号〉
[seq 優先度]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	上流インタフェースに指定するインタフェースを選択します。	lan 1 ewan 1～2 ipsecif 1～2000 vlanif 1～150	省略不可
アクセスリスト番号	グループアドレスを IPv4 標準アクセスリストの中から選択します。	1～99 1300～1999	省略不可
seq 優先度	上流インタフェースに指定したインタフェースに対して、優先度を設定します。 数値が小さい方が優先度が高くなります。	0～255	255

この設定を行わない場合

IGMP Proxy によるマルチキャストルーティングを中継しません。

設定モード

基本設定モード

ip igmp proxy non-querier-behavior

Non-querier 時の動作を設定します。
2 台のルータで冗長構成を行う場合に、同一セグメント上の別ルータを Querier 状態とし本装置は Non-Querier 状態とする場合には、reject-report オプションを追加することで本装置のパケット中継を中止することができます。

refresh コマンド後に有効になるコマンドです。

設定例 1　Non-querier 時に上流に join することなくパケットの中継をしない

```
Router(config)#ip igmp proxy non-querier-behavior reject-report
```

コマンド書式

ip igmp proxy non-querier-behavior <Non-querier 設定>

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
Non-querier 設定	Non-querier 時の動作を設定します。		default reject-report no-join	default
	default	上流に join し、下流は report 受付しますが、流れてきたトラヒックは廃棄し中継しません。		
	reject-report	下流からの report を廃棄し、上流に join することはなくトラヒックは流れません。		
	no-join	下流からの report は受付るが上流には join しません。		

この設定を行わない場合

上流に join し、下流は report 受付しますが、流れてきたトラヒックは廃棄し中継しません。

設定モード

基本設定モード

ip igmp querier-timeout

各インタフェースで、IGMP Querier の生存タイマ時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　生存タイマ時間を 100 秒とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp querier-timeout 100
```

コマンド書式

ip igmp querier-timeout <生存タイマ時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
生存タイマ時間	IGMP Querier の生存タイマ時間(単位:秒)を設定します。	60～300	省略不可

この設定を行わない場合

生存タイマ時間を 255 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp query-interval

各インタフェースで、IGMP Query メッセージの送信間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　送信間隔を 100 秒とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp query-interval 100
```

コマンド書式

ip igmp query-interval <送信間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	IGMP Querier メッセージの送信間隔(単位:秒)を設定します。	30～65535	省略不可

この設定を行わない場合

送信間隔を 125 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp query-max-response-time

各インタフェースで、IGMP Query 内に設定する最大応答待ち時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　最大応答時間を 10 秒とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp query-max-response-time 10
```

設定例 2　最大応答時間を 500 ミリ秒とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp query-max-response-time dsec 5
```

コマンド書式

ip igmp query-max-response-time [dsec] <最大応答待ち時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
最大応答待ち時間	IGMP Query 内に設定する最大応答待ち時間(単位:秒)を設定します。	1～25	省略不可
dsec	最大応答待ち時間を 100 ミリ秒単位で設定する場合に指定します。	1～255	秒単位の設定になります。

この設定を行わない場合

最大応答時間を 10 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp static-group

各インタフェースで、静的に登録するマルチキャストグループを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　233.0.0.1 をマルチキャストグループに追加する

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp static-group 233.0.0.1
```

コマンド書式

ip igmp static-group <グループアドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
グループアドレス	静的に登録するマルチキャストグループを設定します。	IPv4 アドレスを設定	省略不可

この設定を行わない場合

マルチキャストグループを静的に登録しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp source-interface

各インタフェースで、IGMP パケットソースアドレスを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　EWAN 1 に IGMP パケットソースアドレスを設定する

```
Router(config)#interface ipsecif 1
Router(config-ipsecif 1)#ip igmp source-interface ewan 1
```

コマンド書式

ip igmp source-interface <インタフェース名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	IGMP パケットソースアドレス設定するインタフェースを指定します。	lan 1 ewan 1～2 vlanif 1～150 loopback 1～100	省略不可

この設定を行わない場合

他インタフェースの IP アドレスを自動設定します。
loopback 1-100 -> lan -> vlan 1-150 -> ewan 1 -> ewan 2 の順に検索し、使用できるアドレスが見つかった場合、そのインタフェースのアドレスを使用します。

設定モード

IPsec インタフェース設定モード

ip igmp version

各インタフェースで、IGMP Querier の動作バージョンを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　IGMP Querier の動作バージョンを 1 とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp version 1
```

コマンド書式

ip igmp version <IGMP Querier バージョン>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IGMP Querier バージョン	IGMP Querier の動作バージョンを設定します。 1　バージョン 1 2　バージョン 2	1 2	省略不可

この設定を行わない場合

IGMP Querier の動作バージョンは 2 となります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip multicast ttl-threshold

マルチキャスト中継時の TTL の閾値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　TTL の閾値を 10 とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip multicast ttl-threshold 10
```

コマンド書式

```
ip multicast ttl-threshold <TTL>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
TTL	マルチキャスト中継時の TTL の閾値を設定します。	1～255	省略不可

この設定を行わない場合

TTL の閾値を 1 に設定します。

設定モード

基本設定モード
LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip multicast-routing proxy

マルチキャストルーティングを行う場合のサポートプロトコルを設定します。
Snooping および、PIM-SM に関して本装置ではサポートしていません。

refresh コマンド後に有効になるコマンドです。

設定例１　サポートプロトコルに IGMP Proxy を選択する

```
Router(config)#ip multicast-routing proxy
```

コマンド書式

```
ip multicast-routing proxy
```

パラメータ

パラメータはありません。

この設定を行わない場合

マルチキャストルーティングを行いません。

設定モード

基本設定モード

set security-association selector bypass

IPsecSA のセレクタ検索を行わずに中継する場合に設定します。
mcast オプションを指定することにより、マルチキャストパケットのみセレクタ検索を行わずに中継します。
ルートベース(ipsecif)を使用した IPsec でのみ有効、ポリシーベースでは無視します。

IPsec 機能を使用してマルチキャストルーティングを行う場合に設定してください。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　マルチキャストパケットのみセレクタ検索を行わずに中継する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association selector bypass mcast
```

コマンド書式

```
set security-association selector bypass [mcast]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
mcast	マルチキャストパケットのみセレクタ検索を行わずに中継する場合に指定します。	mcast	全てのパケットでセレクタ検索を行わずに中継します。

この設定を行わない場合

セレクタにマッチしないパケットは破棄されます。

設定モード

VPN セレクタ設定モード

リミテッドブロードキャストの設定

ip limited-broadcast ttl

リミテッドブロードキャスト(255.255.255.255)宛の IP パケットの TTL 値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　リミテッドブロードキャストの TTL 値を 64 にする

```
Router(config)#interface lan 1
Router(config-if lan1)#ip limited-broadcast ttl 64
```

コマンド書式

ip limited-broadcast ttl < TTL 値 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
TTL 値	リミテッドブロードキャストの TTL 値を指定します。	1～255	省略不可

この設定を行わない場合

リミテッドブロードキャストの TTL 値は、1 となります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ECMP の設定

ip multi-path max-paths

ECMP で登録できる最大経路数を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　ECMP で登録できる最大経路数を２にする

```
Router(config)#ip multi-path max-paths 2
```

コマンド書式

ip multi-path max-paths 〈経路数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
経路数	最大経路数を設定します。	1～2	省略不可

この設定を行わない場合

ECMP で登録できる最大経路数は1です。

設定モード

基本設定モード

BGP に関する設定

BGP4 について

FITELnet-F シリーズは、IP-VPN 網を含めたイントラネットの経路制御をダイナミックに行うために、BGP4(Border Gateway Protocol Version4)をサポートしています。

背景

現在の IP-VPN 網は、BGP-MPLS を利用した形態が一般的です。
IP-VPN 網内は、I-BGP のフルメッシュ(もしくは RouteReflector を利用している)構成、ユーザ側は E-BGP もしくはデフォルトルートの構成となっています。

BGP は、経路情報毎に、Attribute(属性)を付加することができ、比較的柔軟に経路管理をすることができることから、ユーザ経路の追加・変更・削除を容易に行なうことができます。
また、IPv4-VPN という考え方がプロトコルとして確立されているため、VPN を容易に構築できるプロトコルです。

FITELnet-F シリーズは、主にユーザ側の装置(CE:Customer Edge)として動作しますので、BGP としては、IP-VPN 網側の装置(PE:Provider Edge)と E-BGP で接続することが考えられます。

BGP4 の設定

aggregate-address

経路情報を集約し、その情報を BGP で通知します。通知する際は、PATH 属性に、ATOMIC-AGGREGATE 属性、AGGREGATOR 属性をつけて通知します。summary-only を指定した場合は、集約後の経路情報のみを通知し、集約された他の情報は通知されません。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.0.0～192.168.255.0 の経路情報を 192.168.0.0/16 に集約する

```
Router(config)#router bgp 100
Router(config-bgp)#aggregate-address 192.168.0.0 255.255.0.0
```

設定例２　設定例１と同様（ただし集約後のアドレスのみを BGP で通知する）

```
Router(config)#router bgp 100
Router(config-bgp)#aggregate-address 192.168.0.0 255.255.0.0 summary-only
```

コマンド書式

aggregate-address〈IP アドレス〉〈ネットマスク〉[summary-only]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	集約後の IP アドレス	IPv4 アドレス形式	省略不可
ネットマスク	集約後のネットマスク	IPv4 アドレス形式	省略不可
summary-only	集約後の経路情報のみを通知する場合に指定します。	summary-only	集約前の経路情報も全て通知する

この設定を行わない場合

Aggregate しません。

設定モード

BGP サービス設定モード

bgp always-compare-med

異なる自律システムに属する複数の BGP ピアから受け取った経路の MED の比較を行います。

refresh コマンド後に有効になるコマンドです。

設定例 1　MED による最適経路の比較を行なう

```
Router(config)#router bgp 100
Router(config-bgp)# bgp always-compare-med
```

コマンド書式

bgp always-compare-med

パラメータ

パラメータはありません。

この設定を行わない場合

MED の比較は行ないません。

設定モード

BGP サービス設定モード

bgp bestpath med missing-as-worst

BGP の最適経路の選択において、MED 値(MULTI-EXIT-DESCRIMINATOR)を考慮する場合に指定します。missing-as-worst を指定した場合は、MED 属性のない経路を最も適していない経路とみなします(MED 値を非優先(4294967295)として扱う)。

refresh コマンド後に有効になるコマンドです。

設定例 1　MED 属性の無い経路を、非優先経路とする

```
Router(config)#router bgp 100
Router(config-bgp)# bgp bestpath med missing-as-worst
```

コマンド書式

```
bgp bestpath med missing-as-worst
```

パラメータ

パラメータはありません。

この設定を行わない場合

MED 属性のない経路は、MED 値を 0 として扱います。

本装置の BGP 最適経路選択

本装置の BGP では、以下の順で最適経路の選択を行ないます。

優先順位	属性	内容
1	NEXT_HOP 属性	NEXT_HOP 属性で指定された NEXT_HOP への経路がない場合は無効経路となる
2	WEIGHT 値	BGP ピアに設定した WEIGHT 値により、WEIGHT 値の大きい BGP ピアからの情報が優先される
3	LOCAL_PREF 属性	LOCAL_PREF 値の大きい経路が優先される
4	LOCAL	本装置が生成した BGP 経路が優先される
5	AS_PATH 属性	AS_PATH 長が短い経路が優先される。ただし、bgp bestpath as-path ignore コマンドが設定されている場合は、AS_PATH 長を考慮しない
6	ORIGIN 属性	ORIGIN 属性の優先度は IGP＞EGP＞incomplete
7	MED 値	MED 値の小さい経路が優先される
8	E-BGP or I-BGP	BGP のピアタイプの優先度は、E-BGP > I-BGP
9	IGP メトリック	NEXT_HOP 属性で指定された NEXT_HOP へのメトリック値が小さい経路が優先される
10	router-id	ピアの router-id 値の小さい経路が優先される。ただし bgp bestpath compare-routerid が指定されている場合に限ります。

設定モード

BGP サービス設定モード

bgp bestpath as-path ignore

BGP の最適経路の選択において、AS パスの長さを考慮しない場合に指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　最適経路の選択に、AS_PATH 長を考慮しない

```
Router(config)#router bgp 100
Router(config-bgp)# bgp bestpath as-path ignore
```

コマンド書式

bgp bestpath as-path ignore

パラメータ

パラメータはありません。

この設定を行わない場合

AS-PATH 長を考慮します

本装置の BGP 最適経路選択

本装置の BGP では、以下の順で最適経路の選択を行ないます。

優先順位	属性	内容
1	NEXT_HOP 属性	NEXT_HOP 属性で指定された NEXT_HOP への経路がない場合は無効経路となる
2	WEIGHT 値	BGP ピアに設定した WEIGHT 値により、WEIGHT 値の大きい BGP ピアからの情報が優先される
3	LOCAL_PREF 属性	LOCAL_PREF 値の大きい経路が優先される
4	LOCAL	本装置が生成した BGP 経路が優先される
5	AS_PATH 属性	AS_PATH 長が短い経路が優先される。ただし、bgp bestpath as-path ignore コマンドが設定されている場合は、AS_PATH 長を考慮しない
6	ORIGIN 属性	ORIGIN 属性の優先度は IGP＞EGP＞incomplete
7	MED 値	MED 値の小さい経路が優先される
8	E-BGP or I-BGP	BGP のピアタイプの優先度は、E-BGP > I-BGP
9	IGP メトリック	NEXT_HOP 属性で指定された NEXT_HOP へのメトリック値が小さい経路が優先される
10	router-id	ピアの router-id 値の小さい経路が優先される。ただし bgp bestpath compare-routerid が指定されている場合に限ります。

設定モード

BGP サービス設定モード

bgp bestpath compare-routerid

BGP の最適経路の選択において、ルータ ID を考慮する場合に指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　最適経路の選択に、ルータ ID を考慮する

```
Router(config)#router bgp 100
Router(config-bgp)# bgp bestpath compare-routerid
```

コマンド書式

bgp bestpath compare-routerid

パラメータ

パラメータはありません。

この設定を行わない場合

ルータ ID を考慮しません

本装置の BGP 最適経路選択

本装置の BGP では、以下の順で最適経路の選択を行ないます。

優先順位	属性	内容
1	NEXT_HOP 属性	NEXT_HOP 属性で指定された NEXT_HOP への経路がない場合は無効経路となる
2	WEIGHT 値	BGP ピアに設定した WEIGHT 値により、WEIGHT 値の大きい BGP ピアからの情報が優先される
3	LOCAL_PREF 属性	LOCAL_PREF 値の大きい経路が優先される
4	LOCAL	本装置が生成した BGP 経路が優先される
5	AS_PATH 属性	AS_PATH 長が短い経路が優先される。ただし、bgp bestpath as-path ignore コマンドが設定されている場合は、AS_PATH 長を考慮しない
6	ORIGIN 属性	ORIGIN 属性の優先度は IGP＞EGP＞incomplete
7	MED 値	MED 値の小さい経路が優先される
8	E-BGP or I-BGP	BGP のピアタイプの優先度は、E-BGP > I-BGP
9	IGP メトリック	NEXT_HOP 属性で指定された NEXT_HOP へのメトリック値が小さい経路が優先される
10	router-id	ピアの router-id 値の小さい経路が優先される。ただし bgp bestpath compare-routerid が指定されている場合に限ります。

設定モード

BGP サービス設定モード

bgp default ipv4-unicast

BGP ピアと交換するアドレスファミリーのデフォルトを IPv4 とします。IPv6 をデフォルトとする場合は、disable を設定します。
disable に設定した場合で、IPv4 の経路交換を行なう場合は、neighbor activate enable コマンドで BGP ピアを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピアとの経路交換デフォルトを IPv6 とする

```
Router(config)#router bgp 100
Router(config-bgp)#bgp default ipv4-unicast disable
```

コマンド書式

bgp default ipv4-unicast〈アドレスファミリ〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスファミリ	BGP ピアと交換するアドレスファミリーのデフォルトを IPv4 にするかを指定します。 enable：デフォルトを IPv4 とする disable：デフォルトを IPv6 とする	enable disable	省略不可

この設定を行わない場合

IPv4 ユニキャストは交換できます。

設定モード

BGP サービス設定モード

bgp encap nexthop ipv4

REMOTE-NEXT-HOP attribute に学習した Tunnel Endpoint 宛の経路をホストルートとして登録します。

refresh コマンド後に有効になるコマンドです。

設定例 1　Tunnel Endpoint 宛の経路のゲートウェイを ewan 1 に設定する

```
Router(config)# router bgp 65000
Router(config-bgp)# bgp encap nexthop ipv4 ewan 1
```

コマンド書式

bgp encap nexthop ipv4 {<IPv4 アドレス> | <インタフェース名>} [distance 値]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPv4 アドレス	IPv4 Nexthop address を指定します。	IPv4 アドレス形式	省略不可
インタフェース名	Next-IF を指定します。 ewan を指定した場合、DHCP router option で nexthop を解決します。	dialer <1-20> ewan <1-2> pppoe <1-24> connected null 0 tunnel <1-2000>	省略不可
distance 値	distance 値を指定します。	1-255	200

この設定を行わない場合

Tunnel Endpoint 宛の経路を登録しません。

設定モード

BGP サービス設定モード

bgp log-neighbor-changes

次のような場合に、slog に出力がなされます。
・BGP ピアとの間でセッションが確立された場合
・BGP ピアとの間でセッションが切断された場合
・BGP NOTIFICATION メッセージを送信した場合
・BGP NOTIFICATION メッセージを受信した場合

refresh コマンド後に有効になるコマンドです。

設定例 1　上記タイミングでログを出力する

```
Router(config)#router bgp 100
Router(config-bgp)# bgp log-neighbor-changes
```

コマンド書式

bgp log-neighbor-changes

パラメータ

パラメータはありません。

この設定を行わない場合

上記タイミングでのログ出力を行いません。

設定モード

BGP サービス設定モード

bgp router-id

BGP ルータ ID を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP のルータ ID を 10.1.1.1 に設定する

```
Router(config)#router bgp 100
Router(config-bgp)# bgp router-id 10.1.1.1
```

コマンド書式

bgp router-id <IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP のルータ ID を指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

ルータの全インタフェースアドレスで最大のものを BGP ルータ ID とします。

ルータ ID とは？

BGP で扱う、装置の ID です。通常は、そのルータのどこか 1 つのインタフェースの IP アドレスを割り当てます。

設定モード

BGP サービス設定モード

bgp default local-preference

LOCAL-PREF 属性のデフォルト値を設定します。
UPDATE メッセージで通知する全ての経路情報に関して、ここで設定した LOCAL-PREF 値をつけて通知します。

refresh コマンド後に有効になるコマンドです。

設定例 1　LOCAL-PREF 値を 200 に設定する

```
Router(config)#router bgp 100
Router(config-bgp)# bgp default local-preference 200
```

コマンド書式

bgp default local-preference <LOCAL-PREFERENCE 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
LOCAL-PREFERENCE 値	UPDATE メッセージで広告する際の LOCAL-PREF 値を設定します。	0～4294967295	省略不可

この設定を行わない場合

LOCAL-PREFERENCE 値は 100 になります。

LOCAL-PREF とは？

同じ宛先プレフィックスに対する優先度です。LOCAL-PREF 値が大きい経路情報が、優先されます。

設定モード

BGP サービス設定モード

bgp scan-time

各 BGP 経路のネクストホップに関する到達可能性の定期的なスキャンを行う間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　スキャン間隔を 5 秒に設定する

```
Router(config)#router bgp 100
Router(config-bgp)# bgp scan-time 5
```

コマンド書式

bgp scan-time 〈スキャン間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
スキャン間隔	スキャンを行なう間隔(単位:秒)を設定します。	5～60	省略不可

この設定を行わない場合

スキャン間隔は 60 秒に設定されます。

設定モード

BGP サービス設定モード

distance

特定の BGP ピアからアナウンスされた経路の distance 値を設定します。
distance 値は、値が小さいほど優先度が高くなります。

refresh コマンド後に有効になるコマンドです。

設定例 1　192.168.100.1 のピアから受信したアクセスリストに該当する経路情報の distance 値を 1 とする

```
Router(config)#router bgp 100
Router(config-bgp)# distance 1 192.168.100.1 255.255.255.255 1
```

コマンド書式

distance 〈distance 値〉〈IP アドレス〉〈ネットマスク〉［アクセスリスト番］

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
distance 値	設定している経路の distance 値を設定します。	1～255	省略不可
IP アドレス	distance 値を設定する経路情報の宛先 IP アドレスを指定します。	IPv4 アドレス形式	省略不可
ネットマスク	distance 値を設定する経路情報のネットマスクを指定します。	IPv4 アドレス形式	省略不可
アクセスリスト番号	標準アクセスリスト番号に合致した BGP ピアからアナウンスされた経路にだけディスタンス値を適用する。	–	全ての経路情報

この設定を行わない場合

BGP のディスタンス値（distance bgp コマンドで指定）に従います。

設定モード

BGP サービス設定モード

distance bgp

EBGP／IBGP／ローカル経路について distance 値を設定します。distance 値は、値が小さいほど優先度が高くなります。

refresh コマンド後に有効になるコマンドです。

設定例１　E-BGP／I-BGP／ローカル経路の distance 値を、それぞれ３０／２１０／２５０に設定する

```
Router(config)#router bgp 100
Router(config-bgp)#distance bgp 30 210 250
```

コマンド書式

distance bgp <distance 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
distance 値	external(EBGP), internal(IBGP), local それぞれについて distance 値を設定します。	1～255	省略不可

この設定を行わない場合

経路	distance 値
E-BGP	20
I-BGP	200
ローカル経路	200

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	–	変更不可
BGP（external）	20	変更可能
BGP（internal）	200	
BGP（local）	200	
RIP	120	変更可能
OSPF（external）	110	変更可能
OSPF（inter-area）	110	
OSPF（intra-area）	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

BGP サービス設定モード

ip as-path access-list

AS パスのリストを設定します。
AS パスのリストは明示的な許可設定がないと、不許可として扱われますので、許可したい場合には必ず permit の設定を行ってください。
複数の AS を設定する場合は、スペースで区切って記述します。
AS パスの指定方法は、設定した文字列が含まれるものが対象となります。
例えば"100"と指定した場合は、"100"だけでなく"1001", "1002", "10010"・・のように、"100"の文字列が含まれるものが対象となります。
また、正規表現での指定を行なうことができます。

refresh コマンド後に有効になるコマンドです。

設定例 1　as-path1 の AS アクセスリストとして、AS 番号（100 101 102）を許可する

```
Router(config)# ip as-path access-list as-path1 permit 100 101 102
```

コマンド書式

ip as-path access-list <AS アクセスリスト名> {deny|permit} <AS 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
AS アクセスリスト名	AS アクセスリストに名称をつけます。この名称は、BGP および address-family 設定モードの、neighbor filter-list コマンドで指定します。	254 文字以内の英数字	省略不可
deny|permit	許可属性(permit)か、不許可属性(deny)かを選択します。	deny permit	
AS 番号	AS パスを指定します。複数の AS パスを指定する場合は、スペースで区切って記述します。	1～65535	省略不可

正規表現について

複数の値を、1 つの書式で記載する機能を、正規表現（書式）と呼んでいます。
例えば、「0と1と2と3」を指定したい場合に、4 つのコマンドを入力するのではなく、1 つの入力で 4 つを表現することができ、ここで使用する書式が正規表現です。
本装置の正規表現で使用可能な文字を下表にまとめます。
なお、正規表現は本コマンドでのみ使用可能です。

正規表現で使用する文字設定内容		意味	使用例	
.	ピリオド	任意の 1 文字を意味します。（スペースを含む）	1.	10, 11, 12,・・・19 または 1a, 1b, ・・・が該当します。
*	アスタリスク	直前の文字を 0 回以上繰り返す	12*	1, 12, 122, 1222, 12222, ・・・など"1"

		ことを意味します。(スペースは含まない)		の次に"2"を 0 回以上繰り返したものが該当します。
+	プラス	直前の文字を 1 回以上繰り返すことを意味します。(スペースは含まない)	12+	12, 122, 1222, 12222, ・・・など"1"の次に"2"を 1 回以上繰り返したものが該当します。
^	キャレット	文字の先頭を表します。	^1	1, 10, 11, 100, 1a・・など、1 文字目が"1"のものが該当します。
			^11	11, 111, 112, 1123・・など、最初の 2 文字が"11"のものが該当します。
$	ドル	文字の最後を表します。	1$	1, 11, 21, 321・・など、最後の文字が"1"のものが該当します。
			11$	11, 111, 211, 3211・・など、最後の 2 文字が"11"のものが該当します。
_	アンダースコア	次の中の 1 文字を意味します。 , カンマ { 中括弧開く } 中括弧閉じる (括弧開く) 括弧閉じる 先頭文字(^と同等) 最終文字($と同等) スペース	1_	1, 1{ 1} 1(1)および 1, 11, 21, 321・・など、最後の文字が"1"のものが該当します。
[ ]	大括弧	文字の範囲を表します。	[1234]	1, 2, 3, 4 が該当します。
			[13]	1, 3 が該当します。
-	ハイフン		[1-4]	1, 2, 3, 4 が該当します。
			[a-bA-B]	a, b, A, B が該当します。
|	パイプ	「または」を表します。	^1|^2	1 文字目が"1"または"2"のものが該当します。
			^1|2$	1 文字目が"1"または最後の文字が"2"のものが該当します。
{ }	中括弧	繰り返しを表します。	1{2}	11, 111, 211, 11222 など、"1"を 2 回繰り返すものが該当します。
			1{2,}	11, 111, 211, 1112, 11112 など、"1"を 2 回以上繰り返すものが該当します。
			1{2,3}	11, 111, 211, 1112 など、"1"を 2 回以上 3 回以下繰り返すものが該当します。
¥	バックスラッシュ	正規表現用の文字の特殊な意味を取り除きます。	¥*1	"*1"という文字列が該当します。
			[a-z¥-]	a, b, c, ・・・z と、"-"が該当します。

正規表現の使用例

AS 番号 1000, 1001, 1002, 1003 を通過したプレフィックス情報は不許可とし、それ以外のプレフィックス情報は許可する。

```
Router(config)# ip as-path access-list 1 deny ^100[0-3]
Router(config)# ip as-path access-list 1 permit .*
```

この設定を行っていない場合の動作

AS パスリストによるフィルタは行いません。

ユーザモード

基本設定モード

match as-path

BPG で ip as-path access-list コマンドで指定した AS パス属性を、ルートマップとして適用させる。

refresh コマンド後に有効になるコマンドです。

設定例１　AS パスアクセスリスト（AS-1）にマッチさせる

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#match as-path as-1
```

コマンド書式

match as-path <AS アクセスリスト名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
AS アクセスリスト名	AS アクセスリスト名を指定します。AS アクセスリストは、ip as-path access-list コマンドで設定します。	254 文字の英数字	省略不可

この設定を行っていない場合の動作

AS パスアクセスリストの比較を行いません。

ユーザモード

Route-map 設定モード

neighbor activate

指定した IP アドレスを持つ BGP ピアを有効とするかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）を有効とする

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 activate enable
```

コマンド書式

neighbor <BGP ピアのアドレス> activate <BGP ピア設定>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
BGP ピア設定	BGP ピアを有効(enable)とするか無効(disable)とするかを設定します。	enable disable	省略不可

この設定を行わない場合

BGP ピアは有効になります。

設定モード

BGP サービス設定モード

neighbor default-originate

自身をネクストホップにしたデフォルトルート 0.0.0.0 を BGP ピアに広告する場合に設定します。
この設定を行っている場合は BGP 経路表に登録されているデフォルトルートは広告しません。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）に対して、デフォルトルートの情報を送る

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 default-originate
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 default-originate

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

BGP 経路表にデフォルトルートが登録されている場合は、そのデフォルトルートを広告します。
BGP 経路表にデフォルトルートが登録されていない場合は、デフォルトルートを広告しません。

設定モード

BGP サービス設定モード

neighbor description

BGP ピアに名前や説明のための文字列を指定します。
この設定は相手と同じでなければいけないという決まりはありません。わかりやすい名前を設定してください。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）の名称を"IP-VPN1"とする

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 description IP-VPN1
```

コマンド書式

neighbor <BGP ピアのアドレス> description <BGP ピア名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
BGP ピア名称	BGP ピアの名称を設定します。	80 文字以内の文字列	省略不可

この設定を行わない場合

設定なしとなります。BGP の経路制御に影響はありません。

設定モード

BGP サービス設定モード

neighbor distribute-list

BGP の送受信に対してフィルタリングの設定を行ないます。
プレフィックスのアドレス部分が access-list コマンドで permit にマッチする情報のみを受け入れる／受け入れない、または送信する／送信しないといった制御を行なうことができます。
refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）からは、192.168.110.0/24 の宛先情報のみを受け付ける

```
Router(config)# access-list 1 permit 192.168.110. 0.0.0.255

Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 distribute-list 1 in
```

設定例２　BGP ピア（10.0.0.1）には、192.168.110.0/24 にマッチするプレフィックスのみを送信しない

```
Router(config)# access-list 1 deny 192.168.110. 0.0.0.255
Router(config)#access-list 1 permit any

Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 distribute-list 1 out
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 distribute-list 〈アクセスリスト番号〉〈フィルタリング〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
アクセスリスト番号	指定している BGP ピアに対して、送信する/送信しない経路情報を指定するために access-list 番号を指定します。	1～99 1300～1999	省略不可
フィルタリング	指定している BPG ピアから受信時(in)/指定している BPG ピアへの送信時(out)のどちらでフィルタリングするのかを指定します。	in out	省略不可

この設定を行わない場合

全てのプレフィックスを送受信します。

設定モード

BGP サービス設定モード

neighbor dont-capability-negotiate

OPEN メッセージのオプションとしてケイパビリティ交渉つけないで送信する場合に指定します。
本装置がケイパビリティ交渉を行なう際に通知するケイパビリティは、以下です。
・Multi Protocol Extension Capability (address-family ipv4 unicast /multicast)
・Route Refresh(old & new)
refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）には、ケイパビリティ交渉を行なわない

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 dont-capability-negotiate
```

コマンド書式

neighbor <BGP ピアのアドレス> dont-capability-negotiate

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

設定に応じてケイパビリティ交渉を行います。

ケイパビリティ交渉とは？

BGP の通信の最初に行なう OPEN メッセージで、自身がサポートするオプション機能(能力:ケイパビリティ)を相手に通知します。
これは、新しい機能やマルチプロトコル機能などの能力を通知し合うことで相手の能力を知り、無意味な UPDATE メッセージを送受信する必要がなくなるメリットがあります。
ケイパビリティ交渉を行なわない場合は、全てのオプション能力がない物(そのような UPDATE メッセージは送られてこない)として扱われます。

設定モード

BGP サービス設定モード

neighbor ebgp-multihop

BGP ピアが、E-BGP セッションであり、直接接続されていないネットワークに存在する場合に指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）が、直接接続されていないネットワーク上にあり、E-BGP である

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 ebgp-multihop
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 ebgp-multihop [最大ホップ数]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
最大ホップ数	BGP ピアとしてセッションを確立するための最大ホップ数を設定します。	1～255	255

この設定を行わない場合

E-BGP の場合は、直接接続されていると判断します。

注意

ebgp-multihop を指定しなくてはいけない BGP ピアの場合は、他の経路情報手段（RIP やスタティックルーティング）で、その BGP ピアへの経路を取得しておく必要があります。
取得していない場合は、BGP のセッションを確立することはできません。

設定モード

BGP サービス設定モード

neighbor filter-list

ip as-path access-list コマンドで指定した AS パス属性を、指定する neighbor との経路交換に適用（フィルタ）します。

refresh コマンド後に有効になるコマンドです。

設定例 1　192.168.1.1 への送信時に、as-path1 のフィルタを適用する

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 192.168.1.1 filter-list as-path1 out
```

コマンド書式

neighbor ＜ BGP ピアのアドレス＞ filter-list ＜AS アクセスリスト名＞＜フィルタ＞

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
AS アクセスリスト名	AS アクセスリスト名を指定します。AS アクセスリストは、ip as-path access-list コマンドで設定します。	254 文字以内の英数字	省略不可
フィルタ	受信時(in)にフィルタを行うのか、送信時(out)に行うのかをを指定します。	in out	省略不可

この設定を行っていない場合の動作

AS パスリストによるフィルタは行いません。

ユーザモード

BGP サービス設定モード

neighbor maximum-prefix

BGP ピアから受け付けるプリフィック情報の最大数を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）からのプレフィックス情報の最大数を 10 に設定する

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 maximum-prefix 10
```

コマンド書式

neighbor <BGP ピアのアドレス> maximum-prefix <最大プレフィックス数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
最大 プレフィックス数	指定している BGP ピアから受信できる最大経路情報数	1～4294967295	省略不可

この設定を行わない場合

特定のネイバに対するプリフィックス数の制限はしません

設定モード

BGP サービス設定モード

neighbor next-hop-self

この BGP ピアに対して経路を広告する場合、NextHop を自装置に書き換えて広告します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）へ広告する経路情報の NextHop を自装置に書き換えて広告する

```
Router(config-bgp)# neighbor 10.0.0.1 next-hop-self
```

コマンド書式

neighbor <BGP ピアのアドレス> next-hop-self

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

NextHop を自装置に書き換えません。

設定モード

BGP サービス設定モード

neighbor override-capability

OPEN メッセージのオプションによるケイパビリティ交渉の結果を自身のケイパビリティで上書きします。
neighbor strict-capability-match と同時に設定することはできません。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）のケイパビリティ情報を、本装置自身のケイパビリティ情報に書き換える

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 override-capability
```

コマンド書式

neighbor <BGP ピアのアドレス> override-capability

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

ケイパビリティを上書きしません。

設定モード

BGP サービス設定モード

neighbor passive

自身からは BGP のセッションを開始しないようにします。
ただし、相手から開始要求があった場合には、BGP のセッションを確立します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）から開始要求があった場合に BGP セッションを確立する（相手 AS 番号は 100）

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 passive
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 passive

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

自身または、相手から開始要求があった場合に BGP のセッションを確立します。

設定モード

BGP サービス設定モード

neighbor password

TCP MD5 認証オプション(RFC2385:Protection of BGP Sessions via the TCP MD5 Signature Option)を有効にします。
また、パスワード文字列として使用する文字列を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　パスワードを secret-bgp1 として、TCP MD5 認証オプションを有効にする

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 192.168.1.1 password secret-bgp1
```

コマンド書式

neighbor <BGP ピアのアドレス> password <パスワード> [{secret | private}[encrypted]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
パスワード	TCP MD5 認証オプションで使用するパスワードを設定します。	25 文字以内の文字列	省略不可
secret | private	パスワードを暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。※1 secret：暗号化する際に共有暗号鍵を使用する private：暗号化する際に装置固有暗号鍵を使用する	secret private	パスワードを暗号化しません
encrypted	パスワードを暗号化処理するかどうかを設定します。 このオプションを付加することにより、パスワードは暗号化済みと判定されます。※2 secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。	encrypted	パスワードを暗号化データとして扱いません

※1 このオプションは、設定するとすぐに有効となり、パスワードが暗号化されて表示され encrypted オプションが自動的に付加されます。
※2 パスワードが既に暗号化済みの場合は、このオプションを指定する必要があります。

この設定を行わない場合

TCP MD5 認証オプションを使用しません。

共有および装置固有暗号鍵について

secret オプションを指定した場合は、F シリーズ共通の鍵を使って暗号化するのに対して、private オプションを指定した場合は、装置固有の鍵を使って暗号化します。

そのため、private オプションは secret オプションに対してセキュリティ上、優れますが保守などにより装置の入れ替えが必要となった場合に、設定内容を他の装置に適用することが出来ません。

設定モード

BGP サービス設定モード

neighbor port

BGP ピアが使用するの TCP ポート番号を指定します。
本装置が、BGP のセッションを確立するために送信する BGP パケットは、このポート宛に送信します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BPG ピア（10.0.0.1）の TCP ポート番号を 179 番に設定する

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 port 179
```

コマンド書式

neighbor <BGP ピアのアドレス> port <TCP ポート番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
TCP ポート番号	指定している BGP ピアが使用する、BGP ポート番号。	0～65535	省略不可

この設定を行わない場合

179 番を使用します。

設定モード

BGP サービス設定モード

neighbor remote-as

BGP ピアの属する AS 番号を指定します。自身の AS 番号と同じ場合は I-BGP、異なる場合は E-BGP となります。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）と BGP セッションを確立する（相手 AS 番号は 100）

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 remote-as 100
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 remote-as 〈AS 番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
AS 番号	指定している BGP ピアの AS 番号を設定します。	1～65535	省略不可

※ 最大エントリ：16 エントリ

この設定を行わない場合

BGP の通信を行なうことができません。

設定モード

BGP サービス設定モード

neighbor route-map

BGP ピアにルートマップを適用します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）間で、受信の際に Route-map（ルートマップ名：map1）を適用する

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 route-map map1 in
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 route-map 〈Route-map 名〉〈フィルタリング〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
Route-map 名	適用するルートマップの Route-map 名を指定します。	-	省略不可
フィルタリング	指定している BPG ピアから受信時(in)／指定している BPG ピアへの送信時(out)のどちらでフィルタリングするのかを指定します。	in out	省略不可

この設定を行わない場合

Route-map 制御を行ないません。

設定モード

BGP サービス設定モード

neighbor route-reflector-client

本コマンドを設定することにより、本装置は該当ネイバに対してルートリフレクタとして動作します。

refresh コマンド後に有効になるコマンドです。

設定例 1　該当ネイバに対して本装置をルートリフレクタとして動作させる

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 route-reflector-client
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 route-reflector-client

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

ルートリフレクタとして動作しません。

設定モード

BGP サービス設定モード

neighbor shutdown

設定されている BGP ピアを一時的に無効にします。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）を一時的に無効にする

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 shutdown
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 shutdown

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

指定している BGP ピアは有効になります。

設定モード

BGP サービス設定モード

neighbor soft-reconfiguration inbound

ネイバから受信した経路情報をルーティングテーブルとは別に保持しておく場合に指定します。
通常の BGP では、BGP ピアに対して、UPDATE メッセージを再度送付してもらうメカニズムはありません。このコマンドを指定することにより、BGP ピアからの UPDATE メッセージにより取得した経路情報を保管しておくことができます。
なお、Route-Refresh ケイパビリティを使用すると、UPDATE メッセージの再送を要求することができます。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）からの UPDATE メッセージの内容を保持する

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 soft-reconfiguration inbound
```

コマンド書式

neighbor <BGP ピアのアドレス> soft-reconfiguration inbound

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

フィルタリングされた経路情報は保持しません。

設定モード

BGP サービス設定モード

neighbor strict-capability-match

OPEN メッセージのオプションによるケイパビリティ交渉の際に，ネイバから未サポートのオプションを受信した場合や，自身の指定するオプションをネイバが受け入れなかった場合は，BGP コネクションを確立しないよう設定します。
neighbor override-capability と同時に設定することはできません。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）とのケイパビリティ交渉が一致しなかった場合は、BGP コネクションを確立しない

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 strict-capability-match
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 strict-capability-match

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

未サポートのケイパビリティを受信しても、BGP コネクションを確立します。

設定モード

BGP サービス設定モード

neighbor timers

特定の BGP ピアの各種タイマーをセットします。
KeepAlive 送信間隔と経路情報を削除するまでの時間の設定と、コネクトタイマの設定に分けて行います。
refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）に対応する KeepAlive の送間隔を 10 秒、BGP ピアがいなくなってから経路情報を削除するまでの時間を 30 秒とする

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 timers 10 30
```

設定例２　BGP ピア（10.0.0.1）に対応するコネクトタイマを 100 秒に設定する

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 timers connect 100
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 timers { 〈KeepAlive 送信間隔〉〈経路情報を削除するまでの時間〉 | connect 〈コネクトタイマ〉 }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
KeepAlive 送信間隔	KeepAlive 送信間隔（単位：秒）を指定します。 0 秒を指定した場合は、「経路情報を削除するまでの時間」で指定した時間の 1/3 になります。	0～65535	省略不可
経路情報を削除するまでの時間	経路情報を削除するまでの時間（単位：秒）を設定します。	0～65535	省略不可
コネクトタイマ	BGP コネクトタイマ（単位：秒）を設定します。	0～65535	省略不可

この設定を行わない場合

タイマの内容	デフォルト値
KeepAlive 再送間隔	60 秒
経路情報を削除するまでの時間	180 秒
connect	120 秒

設定モード

BGP サービス設定モード

neighbor transparent-as

AS PATH 属性に自身の AS 番号を付加しないように設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）には、自身の AS 番号をつけない

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 transparent-as
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 transparent-as

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

自身の AS 番号がつけられます。

設定モード

BGP サービス設定モード

neighbor transparent-nexthop

NEXTHOP 属性をネイバのアドレスで上書きしないように設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）には、自身を NextHop として通知しない（自分のルーティングテーブルにある NextHop を通知）

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 transparent-nexthop
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 transparent-nexthop

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

自身を NextHop として通知します。

設定モード

BGP サービス設定モード

neighbor update-source

BGP セッションの確立(OPEN メッセージ)の際、BGP の送信元アドレスに割り当てる IP アドレスを指定するために、インタフェースを指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）との BGP パケットの送信元アドレスに、PPPoE1 のアドレスを利用する

```
Router(config)# router bgp 100
Router(config-bgp)#neighbor A.B.C.D update-source pppoe 1
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 update-source 〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
インタフェース名	BGP の送信元アドレスに使用するインタフェースアドレス。	インタフェース名形式	省略不可

この設定を行わない場合

BGP パケットを実際に送信するインタフェースになります。

設定モード

BGP サービス設定モード

neighbor version

BGP ピアとの間で使用する BGP のプロトコルバージョンを指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）との BGP で使用するバージョンを"4"とする

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 version 4
```

コマンド書式

neighbor <BGP ピアのアドレス> version <バージョン>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
バージョン	指定している BGP ピアの BGP のバージョンを指定します。 4：BGP バージョン 4 を指定します。 draft：BGP バージョン 4 マルチプロトコル拡張ドラフト版を指定します。	4 draft	省略不可

この設定を行わない場合

バージョン 4 となります。

設定モード

BGP サービス設定モード

neighbor weight

BGP ピアに重み付けを設定します。
同じ宛先への複数経路を学習した場合に、どの情報(どの BGP ピアからの)を有効とするかの指針として使用します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（10.0.0.1）の WEIGHT 値を"65535（優先度最高）"に設定する

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 weight 65535
```

コマンド書式

neighbor <BGP ピアのアドレス> weight<Weight 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
weight 値	指定している BGP ピアからの経路情報の優先度を指定します。 優先度は、0(最低)～65535(最高)の範囲で設定できます。	0～65535	省略不可

この設定を行わない場合

他の BGP ピアを通って学習した経路ではデフォルトの weight は 0、ローカルルータによって生成された経路ではデフォルトの weight は 32768 になります。

本装置の BGP 最適経路選択

本装置の BGP では、以下の順で最適経路の選択を行ないます。

優先順位	属性	内容
1	NEXT_HOP 属性	NEXT_HOP 属性で指定された NEXT_HOP への経路がない場合は無効経路となる
2	WEIGHT 値	BGP ピアに設定した WEIGHT 値により、WEIGHT 値の大きい BGP ピアからの情報が優先される
3	LOCAL_PREF 属性	LOCAL_PREF 値の大きい経路が優先される
4	LOCAL	本装置が生成した BGP 経路が優先される
5	AS_PATH 属性	AS_PATH 長が短い経路が優先される。ただし、bgp bestpath as-path ignore コマンドが設定されている場合は、AS_PATH 長を考慮しない
6	ORIGIN 属性	ORIGIN 属性の優先度は IGP＞EGP＞incomplete
7	MED 値	MED 値の小さい経路が優先される
8	E-BGP or I-BGP	BGP のピアタイプの優先度は、E-BGP > I-BGP
9	IGP メトリック	NEXT_HOP 属性で指定された NEXT_HOP へのメトリック値が小さい経路が優先される
10	router-id	ピアの router-id 値の小さい経路が優先される。ただし bgp bestpath compare-routerid が指定されている場合に限ります。

設定モード

BGP サービス設定モード

network

BGP の経路情報として通知するプレフィックスをスタティックで登録します。

refresh コマンド後に有効になるコマンドです。

設定例 1　192.168.0.0/24 の経路情報を BGP で通知する

```
Router(config)#router bgp 100
Router(config-bgp)# network 192.168.0.0 255.255.255.0
```

コマンド書式

network <IP アドレス> <ネットマスク> [backdoor]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP を運用するインタフェースを、インタフェースの IP アドレスで指定します。	IPv4 アドレス形式	省略不可
ネットマスク	BGP を運用するインタフェースを、IP アドレスとネットマスクの組み合わせで指定することもできます	IPv4 アドレス形式	省略不可
backdoor	backdoor オプションをつけた場合は、この経路をローカル BGP 経路として扱います。 ローカル BGP 経路の distance 値は、distance bgp コマンドで設定します	backdoor	External 経路、もしくは Internal 経路として扱う。 (External/Internal は、BGP ピアによる)

この設定を行わない場合

自分の経路情報を通知します(redistribute コマンドの内容に従います。)

設定モード

BGP サービス設定モード

redistribute

BGP 以外の手段で取得した経路情報のうち、BGP で再配布する経路を選択し必要に応じて適用する Route-map を指定します。
ただし、経路情報に変化が無い場合は再配布が行われないため、追加した経路情報を再配布するためには、clear ip bgp redistribute コマンドを実行してください。

refresh コマンド後に有効になるコマンドです。

設定例１　スタティックで登録した経路情報を BGP で再配布する

```
Router(config)#router bgp 100
Router(config-bgp)# redistribute static
```

設定例２　RIP で取得した経路情報を BGP で再配布する

```
Router(config)#router bgp 100
Router(config-bgp)#redistribute rip
```

コマンド書式

redistribute <再配布する経路情報> [route-map <Route-map 名>]

パラメータ	設定内容		設定範囲	省略時の値
再配布する経路情報	BGP 以外の手段で取得した経路情報のうち、BGP で再配布するものを指定します。		connected event-action kernel local-prot1 local-prot2 ospf rip static	省略不可
	connected	直接経路		
	event-action	イベントアクションで追加した経路情報		
	kernel	kernel にセットされた経路情報		
	local-prot1	SA-UP ルート情報		
	local-prot2			
	ospf	OSPF で取得した経路情報		
	rip	RIP で取得した経路情報		
	static	スタティックルーティング情報		
Route-map 名	必要に応じて、適用する Route-map を指定します。		-	Route-map を適用しない

この設定を行わない場合

BGP で受信した情報のみを広告します。

設定モード

BGP サービス設定モード

router bgp

BGP サービス設定モードに移行します。(AS 番号を指定)
BGP サービス設定モードでは、E-BGP/I-BGP のピアのアドレスや、各種アトリビュート情報を設定します。
有効になる最大ピア数は、500 ピアです。

設定例 1　BGP サービス設定モードに移行する（自 AS 番号=64512）

```
Router (config)# router bgp 64512
Router (config-bgp)#
```

コマンド書式

router bgp <自 AS 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
自 AS 番号	自装置側の AS 番号を指定します。	1～65535	省略不可

この設定を行わない場合

BGP を使用できません。

設定モード

基本設定モード

BGP4+の設定

address-family ipv6 unicast

IPv6 アドレス交換を行うためのアドレスファミリー設定モードに移行します。
router bgp <AS 番号> の設定がない場合は、本設定を行なっても BGP は使用できません。

設定例 1　アドレスファミリー設定モードに移行する

```
Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)#
```

コマンド書式

address-family ipv6 unicast

パラメータ

パラメータはありません。

この設定を行わない場合

BGP で IPv6 ユニキャストの経路交換を行いません。

設定モード

基本設定モード

aggregate-address

経路情報を集約し、その情報を BGP で通知します。通知する際は、PATH 属性に、ATOMIC-AGGREGATE 属性、AGGREGATOR 属性をつけて通知します。
summary-only を指定した場合は、集約後の経路情報のみを通知し、集約された他の情報は通知されません。

refresh コマンド後に有効になるコマンドです。

設定例１　2001:db8::/64 の経路情報を集約する

```
Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)#aggregate-address 2001:db8::/64
```

コマンド書式

aggregate-address 〈IPv6 アドレス〉 [summary-only]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPv6 アドレス	経路情報を集約する IP アドレスを設定します。	IPv6 アドレス形式	省略不可
summary-only	集約後の経路情報のみを通知する場合に指定します。	summary-only	集約前の経路情報も全て通知します

この設定を行わない場合

経路情報を集約しません。

設定モード

アドレスファミリー設定モード

match ipv6 address

BPG で access-list(standard)に指定した IP アドレスを特定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア(2001:db8:400::1) には、"2001:db8:200::/32"の情報のみ送信する（ルートマップ名：map1）

```
Router(config)#access-list 3000 permit 2001:db8:200::/32

Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#match ipv6 address 3000
Router(config-rmap map1 permit 1)#exit

Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)#neighbor 2001:db8:400::1 route-map map1 out
```

コマンド書式

match ipv6 address <access-list 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	IP アドレスに一致する access-list 番号を指定します	3000～3499 30000～31499	省略不可

設定モード

Route-map 設定モード

match ipv6 next-hop

BPG で Next-Hop を指定し、経路を特定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(3ffe:400::1)には、Next-Hop が"3ffe:200::1"の情報のみ送信する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#match ipv6 next-hop 3ffe:200::/48
Router(config-rmap map1 permit 1)#exit

Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)#neighbor 3ffe:400::1 route-map map1 out
```

コマンド書式

match ipv6 next-hop <IPv6 アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPv6 アドレス	Next-hop に一致する IPv6 アドレスを指定します。	IPv6 アドレス形式	省略不可

設定モード

Route-map 設定モード

neighbor activate

IPv6 ユニキャストの経路情報交換を行なう BGP ピアを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（2001:db8::1）を設定する

```
Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)# neighbor 2001:db8::1 activate
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 activate

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

BGP で IPv6 ユニキャストの経路交換を行えません。

設定モード

アドレスファミリー設定モード

neighbor default-originate

自身をネクストホップにしたデフォルトルート::/0 を BGP ピアに広告する場合に設定します。
この設定を行っている場合は BGP 経路表に登録されているデフォルトルートは広告しません。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（2001:db8::1）に対して、デフォルトルートの情報を送る

```
Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)# neighbor 2001:db8::1 default-originate
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 default-originate

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

BGP 経路表にデフォルトルートが登録されている場合は、そのデフォルトルートを広告します。
BGP 経路表にデフォルトルートが登録されていない場合は、デフォルトルートを広告しません。

設定モード

アドレスファミリー設定モード

neighbor distribute-list

BGP の送受信に対してフィルタリングの設定を行ないます。
プレフィックスのアドレス部分が access-list コマンドで permit にマッチする情報のみを受け入れる／受け入れない、または送信する／送信しないといった制御を行なうことができます。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（2001:db8::1）からは、2001:db8::/32 宛のプレフィックスのみ受け付ける

```
Router(config)# access-list 3000 permit any 2001:db8::/32

Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)#neighbor 2001:db8::1 distribute-list 3000 in
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 distribute-list 〈アクセスリスト番号〉〈フィルタリング〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
アクセスリスト番号	指定している BGP ピアに対して、送信する/送信しない経路情報を指定するために access-list 番号を指定します。	3000～3499 30000～31499	省略不可
フィルタリング	指定している BPG ピアから受信時(in)／指定している BPG ピアへの送信時(out)のどちらでフィルタリングするのかを指定します。	in out	省略不可

この設定を行わない場合

全てのプレフィックスを送受信します。

設定モード

アドレスファミリー設定モード

neighbor interface

IPv6 リンクローカルアドレスを指定した BGP セッションを行うインタフェースを設定します。
neighbor に、IPv4 アドレスおよび IPv6 グローバルユニキャストアドレスを指定した場合は、本設定は無視されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　LAN 1 インタフェースのアドレスを 2001:db8::1 とし、BGP セッションを行う

```
Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)# neighbor 2001:db8::1 interface lan 1
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 interface 〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
インタフェース名	BGP セッションを行うインタフェースを指定します。	lan 1 ewan 1～2 vlanif 1～150	省略不可

この設定を行わない場合

IPv6 リンクローカルアドレスを指定した BGP セッションは確立できません。

設定モード

BGP サービス設定モード

neighbor maximum-prefix

BGP ピアから受け付ける IPv6 プリフィック情報の最大数を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（2001:db8::1）からのプレフィックス情報の最大数を 1000 にする

```
Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)# neighbor 2001:db8::1 maximum-prefix 1000
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 maximum-prefix 〈最大プレフィックス数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
最大プレフィックス数	指定している BGP ピアから受信できる最大経路情報数を指定します。	1～4294967295	省略不可

この設定を行わない場合

プリフィックス数の制限はしません。

設定モード

アドレスファミリー設定モード

neighbor next-hop-self

この BGP ピアに対して経路を広告する場合、NextHop を自装置に書き換えて広告します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（2001:db8::1）へ広告する経路情報の NextHop を自装置に書き換えて広告する

```
Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)# neighbor 2001:db8::1 next-hop-self
```

コマンド書式

neighbor <BGP ピアのアドレス> next-hop-self

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

NextHop を自装置として通知しません。

設定モード

アドレスファミリー設定モード

neighbor route-map

BGP ピアに Route-map を適用します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（2001:db8::1）間で、受信の際に Route-map（ルートマップ名：map1）を適用する。

```
Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)# neighbor 2001:db8::1 route-map map1 in
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 route-map 〈Route-map 名〉〈フィルタリング〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
Route-map 名	適用する Route-map の Route-map 名を指定します。	–	省略不可
フィルタリング	指定している BPG ピアから受信時(in)／指定している BPG ピアへの送信時(out)のどちらでフィルタリングするのかを指定します。	in out	省略不可

この設定を行わない場合

Route-map 制御を行ないません。

設定モード

アドレスファミリー設定モード

neighbor soft-reconfiguration inbound

ネイバから受信した経路情報をルーティングテーブルとは別に保持しておく場合に指定します。
通常の BGP では、BGP ピアに対して、UPDATE メッセージを再度送付してもらうメカニズムはありません。
このコマンドを指定することにより、BGP ピアからの UPDATE メッセージにより取得した経路情報を保管しておくことができます。
なお、Route-Refresh ケイパビリティを使用すると、UPDATE メッセージの再送を要求することができます。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア（2001:db8::1）からの UPDATE メッセージの内容を保持する

```
Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)# neighbor 2001:db8::1 soft-reconfiguration inbound
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 soft-reconfiguration inbound

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

経路情報をルーティングテーブルとは別に保持しません。
この状態で clear bgp soft in コマンドを事項した場合は、route-refresh を送信し相手から再度 UPDATE を受信します。

設定モード

アドレスファミリー設定モード

network

BGP の経路情報として通知するプレフィックスをスタティックで登録します。

refresh コマンド後に有効になるコマンドです。

設定例 1　2001:db8::/32 の経路情報を通知する

```
Router(config)# address-family ipv6 unicast
Router(config-af ipv6 unicast)#  network 2001:db8::/32
```

コマンド書式

network 〈IPv6 アドレス〉 [backdoor]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPv6 アドレス	BGP を運用するインタフェースを、インタフェースの IP アドレスで指定します。	IPv6 アドレス形式	省略不可
backdoor	backdoor オプションをつけた場合は、この経路をローカル BGP 経路として扱います。	backdoor	distance 値を 200 とします。

この設定を行わない場合

自分の経路情報を通知します（redistribute コマンドの内容に従います。）

設定モード

アドレスファミリー設定モード

redistribute

BGP 以外の手段で取得した経路情報のうち、BGP で再配布する経路を選択し必要に応じて適用する Route-map を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　スタティックで登録した経路情報を BGP で再配布する

```
Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)# redistribute static
```

コマンド書式

redistribute <再配布する経路情報> [route-map <Route-map 名>]

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>再配布する経路情報</td><td>BGP 以外の手段で取得した経路情報のうち、BGP で再配布するものを指定します。<table><tr><td>connected</td><td>直接経路</td></tr><tr><td>event-action</td><td>イベントアクションで追加した経路情報</td></tr><tr><td>kernel</td><td>kernel にセットされた経路情報</td></tr><tr><td>ripng</td><td>RIP で取得した経路情報</td></tr><tr><td>static</td><td>スタティックルーティング情報</td></tr></table></td><td>connected
event-action
kernel
ripng
static</td><td>省略不可</td></tr>
<tr><td>Route-map 名</td><td>必要に応じて、適用する Route-map を指定します。</td><td>-</td><td>Route-map を適用しない</td></tr>
</table>

この設定を行わない場合

BGP で経路を通知しません。

設定モード

アドレスファミリー設定モード

set ipv6 next-hop

BPG で経路情報の nexthop を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　BGP ピア(3ffe:400::1) には、NEXT-HOP 属性として、3ffe:200::1 をつけて送信する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set ipv6 next-hop local 3ffe:200::1
Router(config-rmap map1 permit 1)#exit

Router(config)#address-family ipv6 unicast
Router(config-af ipv6 unicast)#neighbor 3ffe:400::1 route-map map1 out
```

コマンド書式

set ipv6 next-hop {global|local} <IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
global|local	グローバルアドレス、ローカルアドレスを指定します。	global local	省略不可
IP アドレス	BGP の Next-Hop 属性に設定する IP アドレスを設定します。	IPv6 アドレス形式	省略不可

この設定を行わない場合

Next-Hop 属性を操作しません。

設定モード

Route-map 設定モード

MP-BGP の設定

neighbor encap type

カプセル化経路情報に付与するトンネルアトリビュートのタイプを指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　カプセル化経路情報に付与するトンネルアトリビュートのタイプを IPv4 で指定する

```
Router(config)#router bgp 65000
Router(config-bgp)# neighbor 192.0.2.1 encap type ipsec-tunnel
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 encap type 〈トンネルタイプ〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
トンネルタイプ	IPv6 または IPv4 のカプセル化経路情報に付与するトンネルアトリビュートのタイプを指定します。	ipsec-tunnel	省略不可

この設定を行わない場合

カプセル化経路情報に関するトンネルアトリビュートの通知を行いません。

設定モード

BGP サービス設定モード
アドレスファミリ設定モード

neighbor encap endpoint

カプセル化経路情報を広告する際に Nexthop として使用するトンネルエンドポイントを指定します。
インタフェース名が指定されている場合には、該当インタフェースのアドレスが採用され、付与されるアドレスが変化した場合にはネイバに対してUPDATEが通知されます

refresh コマンド後に有効になるコマンドです。

設定例 1　カプセル化経路情報の Nexthop アドレスとして EWAN 1 に設定したアドレスを使用する

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 encap endpoint ipv6 interface ewan 1
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 encap endpoint 〈トンネルエンドポイントアドレス〉
neighbor 〈BGP ピアのアドレス〉 encap endpoint ipv6 interface 〈インタフェース名(IPv6)〉
neighbor 〈BGP ピアのアドレス〉 encap endpoint ipv4 interface 〈インタフェース名(IPv4)〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
トンネルエンドポイントアドレス	トンネルエンドポイントとなる NexHop をアドレス(IPv6 または IPv4)で指定します。	IPv6 アドレス形式 IPv4 アドレス形式※1	省略不可
インタフェース名(IPv6)	トンネルエンドポイントとなる NexHop をインタフェース名で指定します。 インタフェース名を指定した場合は、グローバルユニキャストアドレス(複数 IPv6 アドレスが付与されている場合には最も先に付与されたアドレス)が使用されます。 該当アドレスがない場合、本設定は無効となり、該当する経路(Encap NLRI)は withdraw 扱いとなります。	lan 1 ewan 1～2 vlanif 1～16 loopback 1～100	省略不可
インタフェース名(IPv4)	トンネルエンドポイントとなる NexHop をインタフェース名で指定します。 インタフェース名を指定した場合は、インタフェースの IPv4 アドレス(プライマリアドレス)が使用されます。セカンダリアドレスは使用されません。 該当アドレスがない場合、本設定は無効となり、該当する経路(Encap NLRI)は withdraw 扱いとなります。	dialer 1～20 ewan 1～2 pppoe 1～24 ipsecif 1～2000 lan 1 loopback 1～100 vlanif 1～150 tunnel 1～2000 bvi 1～100	省略不可

この設定を行わない場合

カプセル化経路情報は広告されません。

設定モード

BGP サービス設定モード
アドレスファミリ設定モード

neighbor encap default interface

カプセル化経路情報に該当するパケットを中継するインタフェースを固定的に指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　カプセル化経路情報に該当するパケットを中継するインタフェースを IPsecIF 1 に固定する

```
Router(config)#router bgp 65000
Router(config-bgp)# neighbor 192.0.2.1 encap default interface ipsecif 1
```

コマンド書式

neighbor 〈BGP ピアのアドレス〉 encap default interface 〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
BGP ピアのアドレス	BGP ピアのアドレスを IPv4 または、IPv6 アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
インタフェース名	パケットを中継するインタフェースを指定します。	ipsecif 1～2000	省略不可

この設定を行わない場合

カプセル化経路情報に該当するパケットは、リカーシブに経路解決した結果に基づいて中継されます。

設定モード

BGP サービス設定モード
アドレスファミリ設定モード

IPsec 機能の設定

IPsec 基本コマンド

ipsec dynamic-session limit

ダイナミックセレクタ機能により生成する IPsec セッション数の上限を指定します。
crypto isakmp policy の設定数と上限値の合計が crypto isakmp policy の policy 番号の上限値以下になるように設定してください。
上限を超えた場合、crypto isakmp policy の若い policy 番号の設定から優先して設定が有効となります。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド
V01.02(00)以降サポート

設定例 1　ダイナミックセレクタの上限を 100 とする

```
Router(config)#ipsec dynamic-session limit 100
```

コマンド書式

ipsec dynamic-session limit <IPsec セッション上限数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPsec セッション上限数	ダイナミックセレクタ機能により生成する IPsec セッション数の上限を指定します。	1～2000	省略不可

この設定を行わない場合

ダイナミックセレクタ機能は使用できません。

REFRESH 時の動作

本設定の削除、もしくは IPsec セッションの上限数を減少させる設定変更を refresh で適用すると、ダイナミックセレクタによる全ての IPsec セッションを削除します。

設定モード

基本設定モード

vpn enable

IPsec 機能を有効にします。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　IPsec 機能を有効にする

```
Router(config)#vpn enable
```

コマンド書式

vpn enable [ewan <インタフェース>[modem]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース	セレクタ検索の対象とするインタフェースを指定します。 また、対象とする EWAN ポートを利用する PPPoE インタフェースにも適用されます。 1～2：指定した ewan のみ適用します。 all：ewan1、2 の両方に適用します。	1～2 all	LAN を除く全てのインタフェースがセレクタ検索の対象となります。
modem	セレクタ検索の対象とするインタフェースに、モデムインタフェースを指定します。 インタフェースに all を指定した場合は、modem を指定できません。	modem 1	モデムインタフェースをセレクタ検索の対象としません。

この設定を行わない場合

IPsec 機能は使用できません。

設定モード

基本設定モード

vpnlog enable

IPsec 機能を使用した VPN 通信動作中（SA の確立／解放）の VPN ログを残すか残さないかを設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　SA の確立／解放を VPN ログに残す

```
Router(config)#vpnlog enable
```

コマンド書式

```
vpnlog enable
```

パラメータ

パラメータはありません。

この設定を行わない場合

SA 確立／解放の情報がログに残されません。

vpnlog とは？

IPsec 機能に関するログです。
SA を確立できなかった場合の原因究明や、改ざん・なりすまし等を検知した場合に、ログを発行します。
コンソールもしくは TELNET でログインして、vpnlog の情報を表示する場合は、show vpnlog コマンドを使用します。

設定モード

基本設定モード

Phase1 ポリシーの設定

authentication

Phase1 の認証方式を設定します。認証方式には、電子証明書(RSA)方式／Pre-shared key※の 2 方式があり、それぞれ拡張認証を行うかどうかを指定します。
※Pre-shared key･･･一般的に「事前共有鍵」「共有秘密鍵」と呼ばれます。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　認証方式を、Pre-shared key（拡張認証なし）とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# authentication prekey
```

コマンド書式

authentication <認証方式>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
認証方式	Pre-Shared Key による方式とするか、RSA signature の方式とするか、および拡張認証を行なうかどうかを選択します。 prekey：Pre-Shared Key 認証・拡張認証なし prekeyxauth：Pre-Shared Key 認証・拡張認証あり rsasig：RSA signature 認証・拡張認証なし rsasigxauth：RSA signature 認証・拡張認証あり	prekey prekeyxauth rsasig rsasigxauth	省略不可

この設定を行わない場合

Pre-shared key(拡張認証しない)方式を使用します。

設定モード

IKE ポリシー設定モード

encryption

Phase1 の暗号アルゴリズムを設定します。本装置の暗号アルゴリズムには、DES(56bit DES-CBC)と、3DES(168bit DES)と AES(128bit、192bit、256bit)があります。
暗号化アルゴリズムは複数設定することができ、複数設定した場合は Initiator 時に複数の提案を行います。提案の優先度は設定した順序になります。
また、既に設定されている暗号化アルゴリズムを入力した場合、入力の前後で設定は変わりません。
この設定は、SA を確立する相手と同じ設定である必要があります。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　Phase1 の暗号化アルゴリズムを AES(128bit)方式とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#encryption aes 128
```

設定例 2　Phase1 の暗号化アルゴリズムを複数設定（AES(128bit)方式と DES 方式）する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#encryption aes 128
Router(config-isakmp)#encryption des
```

コマンド書式

encryption <暗号化アルゴリズム>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
暗号化アルゴリズム	Phase1 の暗号化アルゴリズムを指定します。 des：DES 方式 3des：3DES 方式 aes 128：AES 128bit aes 192：AES 192bit aes 256：AES 256bit	des 3des aes 128 aes 192 aes 256	省略不可

この設定を行わない場合

DES 方式を使用します。

設定モード

IKE ポリシー設定モード

group

Phase1 のネゴシエーション時に、Diffie-Hellman 鍵交換を使用した Oakley と呼ばれる暗号化技術を使用します。
このコマンドは Diffie-Hellman Group を指定します。
Diffie-Hellman Group には、1(768-bit)、2(1024-bit)、5(1536-bit)、14(2048-bit)の 4 種類があります。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　Phase1 のネゴシエーション時の Diffie-Hellman グループを”Group2”とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#group 2
```

コマンド書式

group <DH グループ番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DH グループ番号	Diffie-Hellman グループ番号を指定します。	1 2 5 14	省略不可

この設定を行わない場合

"Group 1"を使用します。

設定モード

IKE ポリシー設定モード

hash

Phase1 のハッシュアルゴリズムを設定します。
本装置のハッシュアルゴリズムには、MD5 と SHA-1 と SHA-2 があります。
ハッシュアルゴリズムは複数設定することができ、複数設定した場合は Initiator 時に複数の提案を行います。提案の優先度は設定した順序になります。
また、既に設定されているハッシュアルゴリズムを入力した場合、入力の前後で設定は変わりません。
この設定は、SA を確立する相手と同じ設定である必要があります。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　Phase1 のハッシュアルゴリズムを SHA-1 とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#hash sha
```

設定例 2　Phase1 のハッシュアルゴリズムを複数指定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#hash sha
Router(config-isakmp)#hash md5
```

コマンド書式

hash 〈ハッシュアルゴリズム〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ハッシュアルゴリズム	Phase1 のハッシュアルゴリズムを指定します。	md5 sha sha-256※ sha-384※ sha-512※	省略不可

※sha-256, sha384, sha-512 は、V01.01(00)以降サポート

この設定を行わない場合

MD5 方式を使用します。

設定モード

IKE ポリシー設定モード

idtype-pre

Aggressive モードで、通知する ID の形式を定義します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　Aggressive モードで通知する ID を、FQDN 形式とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#idtype-pre fqdn
```

コマンド書式

idtype-pre <ID タイプ>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ID タイプ	Aggressive モードで自身の ID を通知する際のタイプを指定します	fqdn userfqdn	省略不可

この設定を行わない場合

userfqdn(UserFQDN)を使用します。

FQDN/User-FQDN とは？

FQDN とは、Fully-qualified domain names の略です。ホスト名から全ての情報をもつドメイン名のことを言います。
User-FQDN 形式とは、電子メールアドレスの書式として使用される「ユーザ名@ドメイン名」の書式です。
Aggressive モードでは、通知する ID の形式を対向装置で受け入れ可能なものとする必要があります。

設定モード

IKE ポリシー設定モード

idtype-rsa

RSA signatures 認証の場合に、接続相手に認証してもらう自身の ID タイプを指定します。
ID タイプには、識別名、ドメイン名、電子メールアドレス、IP アドレスがあります。
識別名の場合は、peer-identity distinguished-name で設定した内容、ドメイン名と電子メールアドレスの場合は、peer-identity host で設定した内容、IP アドレスの場合は、peer-identity address で設定した内容と接続相手の証明書に書かれている内容を比較して認証を行います。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　RSA signatures 認証使用時の ID タイプに電子メールを使用する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#idtype-rsa email
```

コマンド書式

idtype-rsa <ID タイプ>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ID タイプ	RSA signatures 認証の場合に、接続相手に認証してもらう自身の ID タイプを指定。 distinguished-name：識別名 Domain-name：ドメイン名 email：電子メールアドレス ip：IP アドレス	distinguished-name domain-name email ip	省略不可

この設定を行わない場合

ドメイン名を ID タイプとして接続相手に通知します。

設定モード

IKE ポリシー設定モード

ip vpn-nat pool

VPN-NAT 変換する際の、変換後の IP アドレス範囲を指定します。NAT 変換(NAT+ではない)する場合に指定する必要があります。
このコマンドでは、VPN-NAT プール名称・変換後の IP アドレス範囲(アドレス/Wildcard Mask)を指定し、ip vpn-nat inside source/destination コマンドで、使用する VPN-NAT プール名を指定します。

VPN-NAT と、IPsec インタフェースでの NAT※の、それぞれ設定に不整合がない場合は、
IPsec インタフェースでの NAT が有効となり、VPN-NAT は無効となります。
※IPsec インタフェースでの NAT は V01.03(00)以降サポート

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例　変換後のアドレスとして、192.168.100.0/24 を指定する（プール名：vpn-pool1）

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# ip vpn-nat pool vpn-pool1 192.168.100.0 0.0.0.255
```

コマンド書式

ip vpn-nat pool 〈VPN プール名〉〈変換後のアドレス〉〈Wildcard マスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VPN-NAT プール名	VPN-NAT プールの名称を指定します。 ip vpn-nat inside source / destination のコマンドを設定する場合に指定する VPN-NAT プール名として使用しますので、わかりやすい名称にしてください。	–	省略不可
変換後のアドレス	変換後の IP アドレスを設定します。 変換後のアドレスを範囲で指定することができます。詳細は範囲指定方法を参照してください。	IPv4 アドレス形式	省略不可
Wildcard マスク	変換後のアドレスを範囲指定するために、Wildcard マスクを指定します。詳細は範囲指定方法を参照してください。	IPv4 アドレス形式	省略不可

最大エントリ数：2 エントリ(isakmp policy 毎)装置全体で 64 エントリ

この設定を行わない場合

VPN-NAT が使用できません。

範囲指定方法

ip vpn-nat pool コマンドで IP アドレスを指定する場合、マスク(Wildcard マスク)を使用して 1 エントリでアドレス範囲を指定することができます。
Wildcard マスクは、サブネットマスクとは書式が異なりますので注意してください。Wildcard マスクとサブネットマスクは、"1"と"0"の判別が逆になります。

例1)　24bit マスクを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い

Wildcard マスクの場合:0.0.0.255
サブネットマスクの場合:255.255.255.0

例2)　ホストを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い

Wildcard マスクの場合:0.0.0.0
サブネットマスクの場合:255.255.255.255

適用順序

NAT 変換ルールは以下の順序で適用されます。

1)static 変換ルール
2)list による変換ルール

同じ種類のルール内では、Prefix 長が長いルールが優先して適用されます。
同一 Prefix 長の設定が複数あった場合には、config 上で先に登録されたものが優先されます。
なお、config には、以下の順に登録され、同じ種類については入力順に登録されます。

1)static 変換ルール(既存のホストアドレス指定)
2)static-subnet 変換ルール
3)list による変換ルール

設定モード

IKE ポリシー設定モード

ip vpn-nat inside source

既存のネットワーク(LAN)同士を IPsec にて VPN を構築する際、互いのネットワークアドレスが重複している場合があります。
IPsec では同じネットワークアドレスの LAN を接続することが出来ません。
そのため、VPN-NAT 変換を行うことで見かけ上の重複を回避し、既存のネットワークの IP 再割り当てを行うことなく IPsec を実現します。

LAN 側から WAN 側への VPN-NAT 変換ルールを設定します。
NAT モードの場合と、NAT+モード(IP マスカレード)の場合で、設定のしかたが異なりますので注意してください。
パラメータ"static-subnet"を指定することにより VPN-NAT の変換ルールを、ネットワーク単位で指定することもできます。<ローカルアドレス・サブネットマスク>で指定したローカルアドレスから<グローバルアドレス・サブネットマスク>で指定したグローバルアドレスへの変換を、<サブネットマスク>で指定した単位で一括設定します。

VPN-NAT と、IPsec インタフェースでの NAT※の、それぞれ設定に不整合がない場合は、
IPsec インタフェースでの NAT が有効となり、VPN-NAT は無効となります。
※IPsec インタフェースでの NAT は V01.03(00)以降サポート

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　NAT 変換（192.168.0.0/24　→　192.168.100.0/24）

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# ip vpn-nat inside source list 1 pool vpn-pool1
Router(config-isakmp)# ip vpn-nat pool vpn-pool1 192.168.100..0 0.0.0.255



Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list 1 の部分の設定
```

【解説】

ip vpn-nat inside source <LAN 側のアドレス範囲> <WAN 側のアドレス範囲>
となります。
<LAN 側のアドレス範囲>は、access-list コマンドで指定します。
<WAN 側のアドレス範囲>は、ip-vpn nat pool <pool 名>コマンドで指定します。

設定例 2　NAT+変換（192.168.0.0/24　→　インタフェースアドレス）

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# ip vpn-nat inside source list 1 interface



Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list 1 の部分の設定
```

【解説】

ip vpn-nat inside source <LAN 側のアドレス範囲> <WAN 側のアドレス範囲>
となります。
<LAN 側のアドレス範囲>は、access-list コマンドで指定します。
<WAN 側のアドレス範囲>は、インタフェースアドレスに集約する場合は"interface"、Mode-config 機能により取得したアドレスに集約する場合は"modeconfig"、指定したアドレスに集約する場合は"peer <ip-address>"と指定します。

設定例３　NAT 変換（一括変換）158.xxx.xxx.xxx.0/24←→192.168.100.0/24 に変換する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#ip vpn-nat inside source static-subnet 158.xxx.xxx.0 192.168.100.0
255.255.255.0
```

【解説】
ip vpn-nat inside source static-subnet <ローカルサブネット> <グローバルサブネット> <サブネットマスク>
となります。
グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。
NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます（複数同時登録）。

例）local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT 時】　ip-vpn nat inside source list <access-list 番号> [変換前開始ポート番号 [変換前終了ポート番号]] pool <プール名> [overload | [変換後開始ポート番号 [変換後終了ポート番号]]]
【NAT+時】 ip-vpn nat inside source list <access-list 番号> [開始ポート番号 [終了ポート番号]] NAT+変換後のアドレス overload | [変換後開始ポート番号 [変換後終了ポート番号]]]
【スタティック変換】 ip vpn-nat inside source static <ローカルアドレス> <グローバルアドレス>
【NAT スタティック（一括変換）】 ip vpn-nat inside source static-subnet <ローカルサブネット> <グローバルサブネット> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前（ローカルアドレス）範囲を指定したアクセスリストを指定します。	1～99 1300～1399 10000～11200	省略不可
[変換前開始ポート番号 変換前終了ポート番号]	変換前の TCP/UDP ポート番号（範囲）を指定します。	1～65535	自動ポート変換

プール名	変換後(グローバルアドレス)範囲を指定した VPN-NAT プール名を指定します。	NAT プール名	NAT の場合は省略不可
NAT+変換後のアドレス	NAT+変換後のアドレスを指定します。	interface: 送信インタフェースのアドレスに変換 modeconfig: 相手から割り当てられたアドレスに変換 peer <IP アドレス>: 設定する IP アドレスに変換	NAT+の場合は省略不可
overload	local のポート番号を必ず別のポート番号に変換する場合に指定 ※変換後のポート番号は 1024～65535	overload	local のポート番号を基本的には変換せずに napt を試みます。 すでにそのポート番号が使用されている場合に限り、別のポート番号に変換します。 変換後のポート番号は 1024～65535。
[変換後開始ポート番号 変換後終了ポート番号]	変換後の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
ローカルアドレス	変換前のローカルアドレスを指定します。	IPv4 アドレス形式	省略不可
グローバルアドレス	変換後のグローバルアドレスを指定します。	IPv4 アドレス形式	省略不可
ローカルサブネット	変換前のローカルアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
グローバルサブネット	変換後のグローバルアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで	IPv4 アドレス形式	省略不可

	指定した単位で一括設定します。		

最大エントリ数：リスト 1 エントリ(isakmp policy 毎)装置全体で 200 エントリ
スタティック 5000 エントリ(装置全体)※isakmp policy 毎の制限はありません

この設定を行わない場合

VPN-NAT が使用できません。

適用順序

NAT 変換ルールは以下の順序で適用されます。

1）static 変換ルール
2）list による変換ルール

同じ種類のルール内では、Prefix 長が長いルールが優先して適用されます。
同一 Prefix 長の設定が複数あった場合には、config 上で先に登録されたものが優先されます。
なお、config には、以下の順に登録され、同じ種類については入力順に登録されます。

1）static 変換ルール（既存のホストアドレス指定）
2）static-subnet 変換ルール
3）list による変換ルール

設定モード

IKE ポリシー設定モード

ip vpn-nat inside destination

既存のネットワーク(LAN)同士を IPsec にて VPN を構築する際、互いのネットワークアドレスが重複している場合があります。
IPsec では同じネットワークアドレスの LAN を接続することが出来ません。
そのため、VPN-NAT 変換を行うことで見かけ上の重複を回避し、既存のネットワークの IP 再割り当てを行うことなく IPsec を実現します。

WAN 側から LAN 側への VPN-NAT 変換ルールを設定します。
NAT モードの場合と、NAT+モード(IP マスカレード)の場合で、設定のしかたが異なりますので注意してください。
パラメータ"static-subnet"を指定することにより VPN-NAT の変換ルールを、ネットワーク単位で指定することもできます。<グローバルアドレス・サブネットマスク>で指定したグローバルアドレスから<ローカルアドレス・サブネットマスク>で指定したローカルアドレスへの変換を、<サブネットマスク>で指定した単位で一括設定します。

VPN-NAT と、IPsec インタフェースでの NAT※の、それぞれ設定に不整合がない場合は、
IPsec インタフェースでの NAT が有効となり、VPN-NAT は無効となります。
※IPsec インタフェースでの NAT は V01.03(00)以降サポート

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　NAT 変換（スタティック登録）　192.168.100.1 宛で受信したら 192.168.0.1 に変換する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#ip vpn-nat inside destination static 192.168.100.1 192.168.0.1
```

【解説】
ip vpn-nat inside destination static <WAN 側アドレス> <LAN 側アドレス>
となります。
これ以外のパケットを NAT 変換したい場合は、ip vpn-nat inside source コマンドを使用して、設定します。

設定例 2　NAT+変換（スタティック登録）　192.168.100.1:ポート番号 1500 で受信したら、192.168.0.1:ポート番号 80 に変換する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#ip vpn-nat inside destination static 192.168.100.1 1500 192.168.0.1 80
```

【解説】
ip vpn-nat inside destination static <WAN 側アドレス WAN 側ポート番号> <LAN 側アドレス LAN 側ポート番号>
となります。
これ以外のパケットを NAT+変換したい場合は、ip vpn-nat inside source コマンドを使用して、設定します。

設定例３　NAT 変換（一括変換）192.168.100.0/24←→158.xxx.xxx.xxx.0/24 に変換する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#ip vpn-nat inside destination static-subnet 158.xxx.xxx.xxx.0
192.168.100.0 255.255.255.0
```

【解説】

ip vpn-nat inside destination static-subnet <グローバルサブネット> <ローカルサブネット> <サブネットマスク>
となります。
グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。
NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます（複数同時登録）。

例）local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT スタティック（複数指定）時】　ip vpn-nat inside destination list <access-list 番号> [開始ポート番号 [終了ポート番号]] pool <プール名> [ポート番号]
【NAT スタティック（1 対 1 変換）、NAT+スタティック時】 ip vpn-nat inside destination static <グローバルアドレス> [開始ポート番号 [終了ポート番号]] <ローカルアドレス> [ポート番号]
【NAT スタティック（一括変換）】 ip vpn-nat inside destination static-subnet <グローバルサブネット> <ローカルサブネット> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲		省略時の値
access-list 番号	変換前（グローバルアドレス）範囲を指定したアクセスリストを指定します。	1～99 1300～1399 10000～11200		省略不可
グローバルアドレス	変換前のグローバルアドレスを指定します。	list <access-list 番号>	アクセスリストで指定した IP アドレス範囲	省略不可
		<IP アドレス>	指定した IP アドレス	
		modeconfig	相手から割り当てられたアドレス	
		peer <IP アドレス>	VPN ピアから指定されて設定した IP アド	

		レス	
[開始ポート番号 終了ポート番号]	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	ポート変換しない
プール名	変換後(ローカルアドレス)範囲を指定した NAT プール名を指定します。	NAT プール名	省略不可
ローカルアドレス	変換後のローカルアドレスを指定します。	IPv4 アドレス形式	省略不可
ポート番号	変換後の TCP/UDP ポート番号を指定します。	1～65535	ポート変換しない
グローバルサブネット	変換前のグローバルアドレスを指定します。※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
ローカルサブネット	変換後のローカルアドレスを指定します。※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ数:リスト 1 エントリ(isakmp policy 毎)装置全体で 200 エントリ
スタティック 5000 エントリ(装置全体)※isakmp policy 毎の制限はありません

この設定を行わない場合

VPN-NAT が使用できません。

適用順序

NAT 変換ルールは以下の順序で適用されます。

1)static 変換ルール
2)list による変換ルール

同じ種類のルール内では、Prefix 長が長いルールが優先して適用されます。
同一 Prefix 長の設定が複数あった場合には、config 上で先に登録されたものが優先されます。
なお、config には、以下の順に登録され、同じ種類については入力順に登録されます。

1)static 変換ルール(既存のホストアドレス指定)
2)static-subnet 変換ルール
3)list による変換ルール

設定モード

IKE ポリシー設定モード

keepalive

SA が接続されているかどうかの確認を行なうために KeepAlive を行なうかどうかを設定します。
本装置では、IKE(Internet Key Exchange security association)プロトコルの KeepAlive 機能、および ICMP による KeepAlive 機能をサポートしています。

本装置では、何も設定をしない場合、IKE の KeepAlive を行います。IKE の KeepAlive は、SA を確立する VPN ピアも IKE の KeepAlive 機能をサポートしている必要があります。

※IKE での KeepAlive は、DPD(Dead Peer Detection)および古河独自の方式をサポートしています。
対向の装置がどちらもサポートしている場合は、DPD で動作します。
対向の装置がどちらの方式もサポートしていない場合は、ICMP を使用した方法で行ってください。

ICMP による KeepAlive を行う場合は、オプションに"icmp"を指定します。ICMP による KeepAlive を行なう場合は、keepalive-icmp peer-address コマンド、keepalive-icmp source-interface コマンドを指定する必要があるケースもあります。
KeepAlive を行なわない場合は、"disable"を指定します。

KeepAlive により、SA が使用できない状態になった場合は、SA を解放します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　KeepAlive を行なわない

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#keepalive disable
```

設定例 2　ICMP の KeepAlive を行なう

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#keepalive icmp
```

コマンド書式

```
keepalive { always-send | response-only | icmp [always-send|traffic-based
          [always-send]]| disable}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
response-only	応答動作のみ行い、自身では KeepAlive 要求パケットを送信しません。 ※DPD もしくは、古河独自 DPD でのみ指定可能	response-only	省略不可
icmp	ICMP を利用した KeepAlive を行います。	icmp	
always-send	VPN データが送信されなくても、常に KeepAlive を送信します。	always-send	
traffic-based	送信間隔中に該当 SA の Inbound トラフィックが存在する場合には、ICMP-KeepAlive のパケットを送信しません。	traffic-based	
disable	KeepAlive 機能を使用しません。	disable	

この設定を行わない場合

IKE の keepalive でネゴシエーションを行います。
対向の装置と合意できた際に、送信間隔中に Phase2 SA で Inbound のトラフィックが無く、Outbound のトラフィックがある場合に keepalive のパケットを送信します。

設定モード

IKE ポリシー設定モード

keepalive-icmp peer-address

SA が接続されているかどうかの確認を行なうための KeepAlive を ICMP で行なう場合に、KeepAlive の宛先 IP アドレスを設定します。
宛先を VPN ピア、送信元 IP アドレスを送信するインタフェースの IP アドレスとする場合は、このコマンドを設定する必要はありません。
KeepAlive により、SA が使用できない状態になった場合は、SA を解放します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　ICMP の KeepAlive の宛先を、192.168.0.1 にする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#keepalive-icmp peer-address 192.168.0.1
```

コマンド書式

keepalive-icmp peer-address <宛先 IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先 IP アドレス	ICMP の KeepAlive を行なう相手の IP アドレス	IPv4 アドレス形式	省略不可

この設定を行わない場合

keepalive icmp が設定されている場合、宛先 IP アドレスは VPN ピアの IP アドレスになります。

設定モード

IKE ポリシー設定モード

keepalive-icmp source-interface

SA が接続されているかどうかの確認を行なうための KeepAlive を ICMP で行なう場合に、KeepAlive パケットの送信元 IP アドレスを設定します。
宛先を VPN ピア、送信元 IP アドレスを送信するインタフェースの IP アドレスとする場合は、このコマンドを設定する必要はありません。
KeepAlive により、SA が使用できない状態になった場合は、SA を解放します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　ICMP の KeepAlive パケットの送信元アドレスに LAN インタフェースの IP アドレスを使用する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#keepalive-icmp source-interface lan 1
```

コマンド書式

keepalive-icmp source-interface <インタフェース名 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	ICMP の KeepAlive 送信する際の、送信元アドレスに使用するインタフェースアドレスを指定します。	lan 1 ewan 1 loopback 1～100 vlanif 1～150	省略不可

この設定を行わない場合

keepalive icmp が設定されている場合、送信元 IP アドレスは実際にパケットを送信するインタフェースの IP アドレスになります。

設定モード

IKE ポリシー設定モード

key

Pre-Shared Key*を設定します。
文字列で指定する場合は"ascii"を指定、16 進数で指定する場合は"binary"を指定した後、Pre-Shared Key を設定します。

refresh コマンド後に有効になるコマンドです。

※Pre-Shared Key･･･一般に「事前共有鍵」「共有秘密鍵」とも呼ばれます。

IKEv1/IKEv2 共通コマンド

設定例１　Pre-Shared Key に文字列の"secretF2200"設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#key ascii secretF2200
```

設定例２　Pre-Shared Key に 16 進数の"123456789abcdef"を設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#ke y  binary 123456789abcdef
```

コマンド書式

```
key {ascii|binary} <Pre-shared Ke> [{secret | private}[encrypted]]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ascii | binary	Pre-shared Key を文字列(ascii)として扱うか、16 進数(binary)として扱うかを指定します。	ascii binary	省略不可
Pre-shared Key	Pre-shared Key を設定します。	最大 64 文字の英数字	省略不可
secret | private	Pre-shared Key を暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。※1 secret：暗号化する際に共有暗号鍵を使用する private：暗号化する際に装置固有暗号鍵を使用する	secret private	パスワードを暗号化しません
encrypted	Pre-shared Key を暗号化処理するかどうかを設定します。 このオプションを付加することにより、パスワードは暗号化済みと判定されます。※2 secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。	encrypted	パスワードを暗号化データとして扱いません

※1 このオプションは、設定するとすぐに有効となり、Pre-shared Key が暗号化されて表示され encrypted オプションが自動的に付加されます。
※2 Pre-shared Key が既に暗号化済みの場合は、このオプションを指定する必要があります。

この設定を行わない場合

SA を確立できません。

設定モード

IKE ポリシー設定モード

lifetime

Phase1 SA の有効期限を設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　Phase1 SA の有効期限を 1200 秒に設定する

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)# lifetime 1200
```

コマンド書式

lifetime <有効期限>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
有効期限	Phase1 SA の有効期限(秒)を設定します。	60～4294967295	省略不可

この設定を行わない場合

1000 秒になります。

VPN ピアと設定が異なる場合

SA を確立しようとしている VPN ピアと、有効期限の設定が異なる場合は、次のようになります。

initiator の場合	自装置の設定値を採用します。
responder の場合	相手からの提案された値を採用します。

設定モード

IKE ポリシー設定モード

my-identity

Aggressive モードで使用する場合の自身の ID を設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　自身の ID として、"F2200"を設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#my-identity F2200
```

コマンド書式

my-identity <自身の ID>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
自身の ID	Aggressive モードで使用する場合の自身の ID を設定します。	最大 64 文字の英数字	省略不可

この設定を行わない場合

名前はありません。

ワンポイント

PPPoE のように、IP アドレスを自動で割り当てられるようなネットワークを介している場合、VPN ピアの IP アドレスが明確に設定できないため、ID を利用して相手を確定する必要があります。したがって、自身/相手の ID を保護する Main モードの通信を行なうことはできず、Aggressive モードでの通信を行なうことになります。

相手の設定

相手側の設定では、VPN ピアを識別する ID の設定に、ここで設定する値（設定例 1 では"F2200"）と同じ値を設定しないと、IPsec の通信を行なうことはできません。
FITELnet-F シリーズどうしの場合は、peer-identity コマンドで設定する値と同じである必要があります。

設定モード

IKE ポリシー設定モード

nat-traversal

NAT-Traversal 機能を使用する場合に指定します。VPN ピアとの通信経路中に NAT 動作を行なうルータが存在する場合は NAT-Traversal 機能が有効です。

NAT-Traversal 機能を使用する場合は、VPN ピアに KeepAlive パケットを送信する必要があります。これは経路上の NAT ルータ上の NAT 変換テーブル情報を保つために定期的に通信データを発生させるためです。

また、このコマンドで、KeepAlive の送信間隔も指定できます。

IKEv1 専用コマンド

設定例１　NAT-Traversal 機能を使用する。KeepAlive の送信間隔を 20 秒とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#nat-traversal enable alivefreq 20
```

設定例２　NAT-Traversal 機能を使用する（RFC 準拠モード）

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#nat-traversal enable rfc3948-also
```

コマンド書式

nat-traversal enable [rfc3948-also [spoofed]][alivefreq <NAT KeepAlive 送信間隔>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
rfc3948-also	rfc3948-also を指定することにより、Initiator は RFC 準拠モードと draft 準拠モードの2つの VID を Responder に提案します。 Responder は提案された VID と自身の設定より、NAT-Traversal 動作モードを決定し（RFC 準拠モードを優先）、決定した VID を Initiator へ通知します。 RFC 準拠モードでは、NAT 検知するとポートを UDP/4500 へ移動させ、以降の通信は UDP/4500 で行います。 spoofed を指定することにより、間に NAT する装置が無い場合でも強制的に NAT-Traversal 動作をおこなうことが可能です。その際に、RFC 準拠モードで動作します。	rfc3948-also spoofed	draft 準拠モードで動作します。
NAT KeepAlive 送信間隔	NAT KeepAlive の送信間隔（単位：秒）を指定します。 off を指定した場合、NAT-Traversal 機能は有効ですが KeepAlive 機能は無効になります。	1～300 off	5 秒

この設定を行わない場合

NAT-Traversal 機能を使用しません。

ワンポイント

NAT-Traversal 機能を使用する場合は、以下の制限があります。

・Pre-shared key での VPN 接続の場合、Aggressive mode でのサポートになります。
Main mode はサポートしていません。
・set peer isakmp-policy で crypto map と IKEv1 ポリシーを紐づけている場合は、
Main mode、Aggressive mode の双方でサポートしています。
・RSA Signature での VPN 接続の場合、Main mode でのサポートになります。
Phase Ⅰ における ID タイプとして"IP アドレス"を使用することはできません。
ID タイプとして使用できるのは以下となります。
・Distinguished name
・Domain name
・E-Mail address
・FITELnet-F シリーズを responder 側として機能させる場合、VPN peer の IP アドレスが確定
（NAT スタティックにより常に一定）していてもその IP アドレスを設定しないでください。
center(config-isakmp)#peer-identity address 158.202.x.x -> ×
center(config-isakmp)#peer-identity host f200no1 -> ○
・ WAN 側アドレスが不定（フレッツ ADSL アドレス動的割当等）の場合には VPN_NAT は使用できません。

相手の設定

相手も NAT-Traversal 機能を使用する必要があります。

設定モード

IKE ポリシー設定モード

negotiation-mode

IKE(Internet Key Exchange security association) Phase1 のネゴシエーションモードを定義します。Phase1 のネゴシエーションモードには、Main モードと Aggressive モードがあります。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　Main モードで接続する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#negotiation-mode main
```

コマンド書式

negotiation-mode <ネゴシエーションモード>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ネゴシエーションモード	Phase1 のネゴシエーションモードを指定します。 main：Main モード aggressive：Aggressive モード	main aggressive	省略不可

この設定を行わない場合

インタフェースに IP アドレスの設定が無ければ、aggressivemode で動作します。

Main モードと Aggressive モード

Main モード、Aggressive モードの特徴は、以下のとおりです。

Main モード	自身および相手の ID を保護(暗号化)することができます。ただし ID が暗号化されてしまうので、ID による相手の特定を行なうことができません。 お互いの相手の特定は装置の IP アドレスになりますので、WAN 側の IP アドレスが不定の形態では、使用することができません。 ※PPPoE でも IP 固定契約なら”自動で固定 IP”が割り当てられます
Aggressive モード	自身および相手の ID により、相手を特定します。したがって、WAN 側の IP アドレスが不定の形態でも、VPN 通信を行なうことができます(どちらか一方は固定の IP アドレスが必要)。 ※IPsec は PPTP と異なり”サーバ-クライアント型”ではありません

設定モード

IKE ポリシー設定モード

peer-identity

VPN ピアの IP アドレスもしくは、ホスト名を設定します。
ホスト名は、Aggressive モードの Responder の場合に、相手が通知してくる ID として使用します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　VPN ピアの IP アドレスに、192.168.100.2 を設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#peer-identity address 192.168.100.2
```

設定例 2　VPN ピアのホスト名として、"center"を設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#peer-identity host center
```

コマンド書式

```
peer-identity address { VPN ピアの IP アドレス | ドメイン名 }
peer-identity host <VPN ピアのホスト名>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VPN ピアの IP アドレス	VPN ピアの IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
ドメイン名[v4 | v6]	VPN ピアをドメイン名で指定します。 ドメイン名で指定した場合は、ドメイン名の名前解決を v4、v6 のどちらかで行うか指定することができます。	ドメイン名※1 v4※2 v6※2	ドメイン名は、省略不可 v4、v6 を省略した場合は、両方で名前解決を行います。
VPN ピアのホスト名	Aggressive モードで使用する場合の VPN ピアの ID を設定します。	最大 64 文字の英数字記号	省略不可

※1 ドメイン名として設定できる文字は、127 文字までの大文字 (A ～ Z)、小文字 (a ～ z)、数字 (0 ～ 9)、ハイフン (-) 、ドット(.)のみが設定できます。
※2 vpn enable となっているインタフェースで v4 と v6 が有効になっている場合は、v4 と v6 のどちらに名前解決させるか指定する必要があります。

この設定を行わない場合

VPN ピアのアイデンティティはありません。

相手の設定

Aggressive モードで接続する場合、相手側の設定では、VPN ピアを識別する ID の設定に、ここで設定する値（設定例 2 では"center"）と同じ値を設定しないと、IPsec の通信を行なうことはできません。FITELnet-F シリーズどうしの場合は、my-identity コマンドで設定する値と同じである必要があります。

ホスト名について

このホスト名は、Aggressive モードで Responder の場合に、相手が通知してくる ID として使用されます。

設定モード

IKE ポリシー設定モード

peer-identity distinguished-name

相手の証明書の DN(distinguished name)を設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　相手の DN として、C=JP,O=furukawa,CN=honsya を設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#peer-identity distinguished-name C=JP,O=furukawa,CN=honsya
```

コマンド書式

peer-identity distinguished-name <DN>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DN	相手の DN を指定します。	最大 128 文字の英数字	省略不可

※peer-identity distinguished-name を登録する際、文字列の間にスペースを入れた形式で登録することは出来ません。スペースを省いた形式で登録してください。

この設定を行わない場合

相手を DN で認証することはできません。

設定モード

IKE ポリシー設定モード

re-establish-sa rekey

Phase1 の SA の Rekey 動作を行います。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　Phase1 の SA の Rekey 動作を行う。

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#re-establish-sa rekey
```

コマンド書式

```
re-establish-sa rekey
```

パラメータ

パラメータはありません。

この設定を行わない場合

Phase1 の SA の Rekey 動作を行いません。

設定モード

IKE ポリシー設定モード

release security-association

WAN 回線切断時に、SA（Security Association）を解放するか、そのまま残すかを設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例１　ＷＡＮ回線異常時には、ＳＡを解放する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#release security-association
```

コマンド書式

```
release security-association
```

パラメータ

パラメータはありません。

この設定を行わない場合

SA を解放せず、そのまま残します。

設定モード

IKE ポリシー設定モード

release session addr-changed

IKE パケットのソースアドレス変化の確認を行い、セッション確立時に使用していた送信元アドレスと、これから送信しようとしている IKE パケットの送信元アドレスが異なっていた場合、関連する SA（Phase 1、Phase 2 共に）をすべて削除します。
運用中に送信元アドレスが変化する構成（冗長により経路情報が変化する構成）の時に使用します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　IKE パケットのソースアドレス変化の確認を行う

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#release session addr-changed
```

コマンド書式

```
release session addr-changed
```

パラメータ

パラメータはありません。

この設定を行わない場合

IKE パケットのソースアドレス変化の確認を行いません。
また、変化しても SA は削除されません。

設定モード

IKE ポリシー設定モード

source-interface

IPsec トンネルを確立する IP アドレスが設定されているインタフェース番号を指定します。受信した IKE パケットの宛先 IP アドレスが一致しない場合は該当 IKE ポリシーを使用しません。
source-interface 指定を使用する際は、全てのポリシーに設定してください。

VRID を指定することにより、VRID にマッチする VRRP アドレスを使用します。この時、VRRP ステータスが Master 以外では、IKE パケットの送信を行ないません。また、SA を張っている状態で VRRP ステータスが、Master 以外に遷移した場合、PhaseI,II SA の削除を行います。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　送信元アドレスを EWAN 1 インターフェースのアドレスに変更して送信する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# source-interface ewan 1
```

コマンド書式

source-interface <インタフェース名> [VRID]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	IPsec トンネルを確立する IP アドレスとして、設定したインタフェースの IP アドレスを使用します。	ewan 1～2 vlanif 1～150 loopback 1～100※1	省略不可
VRID	IPsec トンネルを確立する IP アドレスとして、設定したインタフェースの<VRID>にマッチする VRRP アドレスを使用します。	1～254	VRRP アドレスを使用しません。

※1 設定範囲 loopback 1～100 は V01.03 (00)以降サポート

この設定を行わない場合

VPN ピアと通信するインタフェースの IP アドレスを送信元アドレスとします。

設定モード

IKE ポリシー設定モード

tunnel-route

IPsec 通信において、本装置が Aggressive モードの Responder となった場合に、VPN ピアへの経路情報をテーブルに登録する場合に指定します。
この場合、VPN ピアへの NextHop も合わせて指定します。
tunnel-route の設定をした装置に crypto isakmp policy の peer-identity distinguished-name を設定すると tunnel-route が動作しません。
crypto security-association モードで、設定する tunnel-route コマンドは装置に対し1つしか設定できないのに対して、本コマンドは、peer 単位で設定することができます。
本コマンドが設定されると、crypto security-association モードで設定されている tunnel-route コマンドより優先的に利用されます。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例１　VPN ピアへの経路情報を登録する（NextHop は 192.168.100.1 とする）

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#tunnel-route address 192.168.100.1
```

設定例２　VPN ピアへの経路情報を登録する（NextHop は PPPoE#1 とする）

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#tunnel-route interface pppoe 1
```

コマンド書式

tunnel-route { address <IP アドレス> | interface <インタフェース名称>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	VPN ピアへの経路情報を登録し、NextHop のアドレスを設定します。	IPv4 アドレス形式	省略不可
インタフェース名称	VPN ピアへの経路情報を登録し、NextHop のインタフェースを設定します。	ewan 1 pppoe 1～24 dialer 1～20	

この設定を行わない場合

Aggressive モードの Responder の場合でも、VPN ピアへの経路情報を登録しません。

何のための設定？

Aggressive モードでは、IP アドレスではなく ID で認証できるため、Responder では IPsec のネゴシエーションが始まってから相手の IP アドレスがわかるというケースがあります。
この場合、相手（VPN ピア）の IP アドレスへの経路は、（多くの場合）デフォルトルートにしたがってしまうことになります。
このコマンドにて、まだわからない VPN ピアへの経路情報の NextHop を指定しておき、デフォルトルートとは違う経路で通信を行なうことができるようになります。

設定モード

IKE ポリシー設定モード

Phase2 ポリシーの設定

anti-replay

IPsec 通信時の、Replay Attack 防御機能について設定します。本コマンドがない場合は Replay Attack とみなされるパケットを廃棄しますが、disable を設定することによりそれらのパケットも受信されます。

使用する回線によっては、パケットの到着順序が前後するような状態が発生し、Replay Attack と誤認してパケットを廃棄してしまい、スループットの低下が発生することがあります。
show vpnlog コマンドを実行して、ログに Replay Attack が表示されるようであれば、本コマンドで disable を指定する事により、スループットの改善が図れる場合があります。
セキュリティを考慮して Replay Attack 防御が不要であれば、通信状況に応じて disable に設定してください。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　Replay Attack 防御機能を停止して、全てのパケットを受信する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#anti-replay disable
```

コマンド書式

anti-replay < Replay Attack 設定>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Replay Attack 設定	Replay Attack に該当するパケットを破棄するかどうかの設定をします。 enable：Replay Attack に該当するパケットを破棄します。 disable：全てのパケットを受信します。	enable disable	省略不可

この設定を行わない場合

Replay Attack に該当するパケットを破棄します。

Replay Attack 防御機能とは？

Replay Attack 防御機能とは、受信したパケットのシーケンス番号の最大値を保存し、その値と同一もしくはその値より小さなシーケンス番号を受信した場合に、パケットを廃棄する機能です。

ただし、ネットワーク遅延の関係上、ESP フレーム入れ替わりの可能性があるため、受信した Sequence Number の最大値から一定の数（本装置では 32）は受信済・未受信を管理し、その管理の範囲内で未受信の場合は Replay Attack error としての廃棄は行わずに通常の受信処理を行います。

設定モード

VPN セレクタ設定モード

crypto map（基本設定モード）

VPN ピアとのセレクタ情報のエントリを設定する為に、VPN セレクタ設定モードに移行します。
設定の際は、セレクタ名称、シーケンス番号を指定します。

IKEv1/IKEv2 共通コマンド

設定例１　VPN セレクタ設定モード（セレクタ名称：Tokyo）に移行します。

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#
```

コマンド書式

crypto map〈セレクタ名称〉〈シーケンス番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セレクタ名称	VPN セレクタの名称を指定します。 PPPoE インタフェース設定モード/EWAN インタフェース設定モードで、適用する VPN セレクタを指定しますので、わかりやすい名称にしてください。	最大 16 文字の英数字	省略不可
シーケンス番号	シーケンス番号を指定します。 既に使用したシーケンス番号と同じ番号を重複して使用すると以前設定した内容を上書きします。	1～4000	省略不可

設定モード

基本設定モード

crypto map（各インタフェース設定モード）

インタフェースに対応付ける VPN セレクタの MAP 名を定義します。
VPN セレクタは、crypto map コマンドで、VPN セレクタ設定モードに移行して、設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　EWAN1 インタフェースに、MAP 名（Tokyo）の VPN セレクタを対応付けます

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#crypto map Tokyo
```

コマンド書式

crypto map <セレクタ名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セレクタ名称	crypto map コマンドで指定したセレクタ名称を指定します。	–	省略不可

この設定を行わない場合

このインタフェースでは、VPN（IPsec）を使用しません。

設定モード

EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード

ipsec access-list

IPsec のセレクタ情報を定義します。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例１　全てのパケットを暗号化する

```
Router(config)#ipsec access-list 1 ipsec ip any any
```

設定例２　192.168.100.0/24　→　192.168.200.0/24　宛のパケットを暗号化する

```
Router(config)#ipsec access-list 1 ipsec ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

設定例３　TCP パケットのみ暗号化する

```
Router(config)#ipsec access-list 1 ipsec tcp any any
```

設定例４　全てのパケットを暗号化しない（bypass）

```
Router(config)#ipsec access-list 64 bypass ip any any
```

設定例５　自局発信パケットを暗号化しない（bypass）

bypass で local 指定する場合、下記のように crypto map を設定して、明示的にインタフェースとの紐付けを行う必要があります。
なお、local 指定の場合、1 つの crypto map を複数のインタフェースに紐付けることはできず（ipsec、bypass 指定のどちらも）、インタフェースが異なる場合には、別の ipsec access-list と crypto map にする必要があります。

```
Router(config)#ipsec access-list 61 bypass ip local any
Router(config)#ipsec access-list 62 bypass ip local any
Router(config)#
Router(config)#interface ewan 1
Router(config-if ewan 1)# crypto map bypass-1
Router(config-if ewan 1)# ip address 192.168.1.254 255.255.255.0
Router(config-if ewan 1)#exit
Router(config)#
Router(config)#interface ewan 2
Router(config-if ewan 2)# crypto map bypass-2
```

```
Router(config-if ewan 2)# ip address 192.168.2.254 255.255.255.0
Router(config-if ewan 2)#exit
Router(config)#
Router(config)#crypto map bypass-1 61
Router(config-crypto-map)# match address 61
Router(config-crypto-map)#exit
Router(config)#
Router(config)#crypto map bypass-2 62
Router(config-crypto-map)# match address 62
Router(config-crypto-map)#exit
```

コマンド書式

ipsec access-list <ipsec-access-list 番号> { ipsec | bypass | discard } <プロトコル番号> { any | local | host <送信元 IP アドレス> | <送信元 IP アドレス> <送信元 Wildcard マスク> } [eq <TCP ポート番号>] [eq <UDP ポート番号>] { any | peer | host <宛先 IP アドレス> | <宛先 IP アドレス> <宛先 Wildcard マスク> } [eq <TCP ポート番号>] [eq <UDP ポート番号>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ipsec-access-list 番号	それぞれの属性の番号を指定します。また、この番号は、VPN セレクタの優先度としても使用されます(数字が小さいほど優先度が高い)	1～4000	省略不可
ipsec | bypass | discard	暗号化対象、透過対象、廃棄対象のいずれかを指定します。 ipsec：暗号化対象とする bypass：透過対象とする discard：廃棄対象とする	ipsec bypass discard	省略不可
プロトコル番号	プロトコル名もしくは、プロトコル番号を選択します。 icmp：ICMP ip：IP tcp：TCP udp：UDP 0～255：プロトコル番号を指定	icmp ip tcp udp 0～255	省略不可
any	各パラメータ(アドレスやポート番号など)で、「全て」を指定する場合は"any"を入力します。 セレクタ情報として相手に通知する場合	any	-

	は、IPaddr=0.0.0.0 Mask=0.0.0.0 で通知します。		
local	自局発信パケットを指定する場合は、"local"を指定します。EWAN でアドレスを固定設定している場合のみ使用可能です。	local	–
host	送信元/宛先アドレスとしてホストアドレスを指定する場合につけます。	host	–
送信元 IP アドレス	送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
送信元 Wildcard マスク	送信元アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
宛先 IP アドレス	宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
宛先 Wildcard マスク	宛先アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
peer	VPN ピア宛を指定する場合は、"peer"を指定します。	peer	
TCP ポート番号	プロトコルで"tcp"を指定した場合に、対象とする TCP ポート番号を指定します。	TCP ポート番号(0～65535)	省略不可
UDP ポート番号	プロトコルで"udp"を指定した場合に、対象とする UDP ポート番号を指定します。	UDP ポート番号(0～65535)	省略不可

この設定を行わない場合

IPsec 機能を使用することはできません。

設定モード

基本設定モード

ipsec transform-set

IPSEC-SA/CHILD SA のポリシーとして、暗号化アルゴリズム、認証アルゴリズムを設定します。
暗号化アルゴリズム、認証アルゴリズムは複数指定することができ、複数指定した場合はネゴシエーション時に複数の提案を行います。
複数の提案をする際の payload 内の暗号化方式は、IKEv1、IKEv2 でそれぞれ以下の様になります。
IKEv1 の場合は設定した順に提案します。
暗号化アルゴリズム、認証アルゴリズムが共に複数設定されている場合は、暗号化アルゴリズムを優先して提案します。
IKEv2 の場合は、暗号化アルゴリズムを AES,3DES,DES,NULL の順に提案し、認証アルゴリズムを sha-256,sha-384,sha-512,sha1,md5 の順に提案します。

CBQ によって帯域制御を行う場合、ipsecif での帯域計算で使用する ICV 長の補正値はデフォルトで 12 バイトとなっています。
しかし、sha256,sha384,sha512 の ICV 長は 12 バイトでないので、必要に応じて qos frame-length-offset で補正値を指定してください。
それぞれのアルゴリズムでの ICV 長は下記の通りです。

- HMAC-MD5: 12 バイト
- HMAC-SHA: 12 バイト
- HMAC-SHA2-256: 16 バイト
- HMAC-SHA2-384: 24 バイト
- HMAC-SHA2-512: 32 バイト

本装置は、複数の Phase2 ポリシーを設定できますので、各 Phase2 ポリシーには、Phase2 ポリシー名称を設定します。
この Phase2 ポリシー名称は、実際にどのセレクタ情報に対して使用するかの指定に使用しますので、わかりやすい名称としてください。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　IKEv1 のポリシー（ポリシー名称：P2-POLICY）として、暗号化方式：AES(256bit)、認証アルゴリズム：HMAC-SHA-1 を登録する

```
Router(config)#ipsec transform-set P2-POLICY esp-aes-256 esp-sha-hmac
```

設定例 2　IKEv2 のポリシー（ポリシー名称：P2V2-POLICY）として、暗号化方式：AES、認証アルゴリズム：HMAC-SHA-1 を登録する

```
Router(config)#ipsec transform-set P2V2-POLICY ikev2 esp-aes esp-sha-hmac
```

コマンド書式

```
ipsec transform-set <ポリシー名> {<IKEv1 暗号化アルゴリズム> [IKEv1 認証アルゴリズム] | ikev2 <IKEv2 暗号化アルゴリズム> [IKEv2 認証アルゴリズム] }
```

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>ポリシー名</td><td>ポリシー名として、わかりやすい名称を指定します。</td><td>16 文字以内の英数字</td><td>省略不可</td></tr>
<tr><td>IKEv1 暗号化アルゴリズム</td><td>IPSEC-SA の暗号化アルゴリズムを指定します。
<table><tr><td>esp-des</td><td>DES 方式</td></tr><tr><td>esp-3des</td><td>3DES 方式</td></tr><tr><td>esp-aes-128</td><td>AES 128bit</td></tr><tr><td>esp-aes-192</td><td>AES 192bit</td></tr><tr><td>esp-aes-256</td><td>AES 256bit</td></tr><tr><td>esp-null</td><td>暗号化しない</td></tr></table></td><td>esp-des
esp-3des
esp-aes-128
esp-aes-192
esp-aes-256
esp-null</td><td>省略不可</td></tr>
<tr><td>IKEv1 認証アルゴリズム</td><td>IPSEC-SA の認証アルゴリズムを指定します。
<table><tr><td>esp-md5-hmac</td><td>HMAC-MD5 アルゴリズム</td></tr><tr><td>esp-sha-hmac</td><td>HMAC-SHA-1 アルゴリズム</td></tr><tr><td>esp-sha256-hmac ※</td><td>HMAC-SHA2-256 アルゴリズム</td></tr><tr><td>esp-sha384-hmac ※</td><td>HMAC-SHA2-384 アルゴリズム</td></tr><tr><td>esp-sha512-hmac ※</td><td>HMAC-SHA2-512 アルゴリズム</td></tr></table></td><td>esp-md5-hmac
esp-sha-hmac
esp-sha256-hmac
esp-sha384-hmac
esp-sha512-hmac</td><td>HMAC-MD5 で動作します。</td></tr>
<tr><td>IKEv2 暗号化アルゴリズム</td><td>CHILD SA の暗号化アルゴリズムを指定します。
<table><tr><td>esp-des</td><td>DES 方式</td></tr><tr><td>esp-3des</td><td>3DES 方式</td></tr><tr><td>esp-aes</td><td>AES 方式</td></tr><tr><td>esp-null</td><td>暗号化しない</td></tr></table></td><td>esp-des
esp-3des
esp-aes
esp-null</td><td>省略不可</td></tr>
<tr><td>IKEv2 認証アルゴリズム</td><td>CHILD SA の認証アルゴリズムを指定します。
<table><tr><td>esp-md5-hmac</td><td>HMAC-MD5 アルゴリズム</td></tr><tr><td>esp-sha-hmac</td><td>HMAC-SHA-1 アルゴリズム</td></tr><tr><td>esp-sha256-hmac ※</td><td>HMAC-SHA2-256 アルゴリズム</td></tr><tr><td>esp-sha384-hmac ※</td><td>HMAC-SHA2-384 アルゴリズム</td></tr><tr><td>esp-sha512-hmac ※</td><td>HMAC-SHA2-512 アルゴリズム</td></tr></table></td><td>esp-md5-hmac
esp-sha-hmac
esp-sha256-hmac
esp-sha384-hmac
esp-sha512-hmac</td><td>HMAC-SHA-1 で動作します。</td></tr>
</table>

最大エントリ:64 エントリ
※認証アルゴリズム　sha-256,sha-384,sha-512 は、V01.01(00)以降サポート

この設定を行わない場合

IKEv1 では暗号化アルゴリズム：DES、認証アルゴリズム：HMAC-MD5 で動作します。
IKEv2 では暗号化アルゴリズム：3DES、認証アルゴリズム：HMAC-SHA-1 で動作します。

設定モード

基本設定モード

map-type-dynamic

VPN セレクタをダイナミックセレクタとして使用します。
ダイナミックセレクタとは、条件を規定せず相手からの提案に従って通信を行うためのセレクタとなります。
1 つのセレクタで複数のセッションを収容できます。
ダイナミックセレクタを用いる場合、以下の機能との併用は未サポートとなります。
・IKEv2
・IPsec の終端アドレスが IPv6 アドレス
・Aggressive mode

ダイナミックセレクタで使用するポリシーは装置で一つだけとなります。
ダイナミックセレクタにより接続可能なセッションは最大で「IPsec セッションの収容可能数」と同一となります。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド
V01.02(00)以降サポート

設定例 1　設定している crypto map をダイナミックセレクタとして使用する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)# map-type-dynamic
```

コマンド書式

map-type-dynamic

パラメータ

パラメータはありません。

この設定を行わない場合

VPN セレクタを通常のセレクタとして使用します。

設定モード

VPN セレクタ設定モード

match address

暗号化するパケットを指定します。
パケットの送信元・宛先アドレスは、ipsec access-list コマンドで指定し、match address コマンドでは、採用する ipsec access-list 番号を指定します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　192.168.100.0/24 <-> 192.168.200.0/24 を暗号化するパケットとして指定する

```
Router(config)#ipsec access-list 1ipsec ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255

Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#match address 1
```

コマンド書式

match address <IPsec access-list 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPsec access-list 番号	暗号化するパケットとして、IPsec access-list 番号を指定します。	1～4000	省略不可

この設定を行わない場合

IPsec を使用できません。

設定モード

VPN セレクタ設定モード

mode

IPsec 通信を行う際の通信モードを設定します。
トランスポートモードの場合、以下の機能との併用は未サポートとなります。
・IKEv2
・sa-up route
・IPsec の終端アドレスが IPv6 アドレス

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド
V01.02(00)以降サポート

設定例 1　通信モードを transport に設定する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map) #mode transport
```

コマンド書式

mode <IPsec の通信モード>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPsec の通信モード	IPsec の通信モードを指定します。 tunnel　トンネルモード transport　トランスポートモード	tunnel transport	省略不可

この設定を行わない場合

トンネルモードで動作します。

設定モード

VPN セレクタ設定モード

set peer

設定している crypto map が SA を確立する VPN ピアのアドレスまたはホスト名を設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例１　設定している crypto map の VPN ピアを"192.168.1.1"に設定する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set peer address 192.168.1.1
```

設定例２　設定している crypto map の VPN ピアを"vpnpeer1"に設定する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set peer host VPN1
```

設定例３　設定している crypto map と紐づける IKEv1 ポリシーを"isakmp policy 1"にする

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set peer isakmp-policy 1
```

コマンド書式

```
set peer address　{ VPN ピアの IP アドレス | ドメイン名 }
set peer host <VPN ピアのホスト名>
set peer isakmp-policy <policy 番号>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VPN ピアの IP アドレス｜ドメイン名	VPN ピアの IP アドレス、またはドメイン名※1を指定します。 IKE ポリシー設定モードで設定した VPN ピアの IP アドレス、またはドメイン名と同じである必要があります。	IPv4、v6 アドレス形式 ドメイン名※1	省略不可
VPN ピアのホスト名称	VPN ピアの名称を指定します。 IKE ポリシー設定モードで設定した VPN ピアの ID と同じである必要があります。	最大 64 文字の英数字記号	省略不可
policy 番号※2	使用する IKEv1 ポリシーの番号を指定します。 policy 番号は装置内で 1 つだけ有効となり、複数の crypto map にて、NAT Main モード設定を行った場合、crypto map 番号が一番小さい物だけが有効となり、その他は無効となります。 NAT Main モード設定を行っていない場合、crypto map 番号が一番大きい物だけが有効となります。	1 ～ 2000	省略不可

※1 ドメイン名として設定できる文字は、127 文字までの大文字 (A ～ Z)、小文字 (a ～ z)、数字 (0 ～ 9)、ハイフン (-) 、ドット(.)のみが設定できます。
※2 パラメータ policy 番号は、V01.01(00)以降サポート

この設定を行わない場合

IPsec を使用できません。

ホスト名について

このホスト名は、Aggressive モードで Responder の場合に、相手が通知してくる ID として使用されます。

設定モード

VPN セレクタ設定モード

set pfs

PFS (Perfect Forward Security)を行なう際に、Diffie-Hellman 鍵交換を使用した Oakley と呼ばれる暗号化技術を使用します。
このコマンドは Oakley Group を指定します。
Diffie-Hellman Group には、1(768-bit)、2(1024-bit)、5(1536-bit)、14(2048-bit)の 4 種類があります。
IKEv2 で複数の提案をする場合 payload 内では、group14, group5, group2, group1 の順で提案します。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　PFS 使用時の Oakley Group に、Group2 を使用する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set pfs group2
```

コマンド書式

set pfs <DH グループ>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DH グループ	Diffie-Hellman グループ番号を指定します。	group1 group2 group5 group14	省略不可

この設定を行わない場合

IKEv1 では Initiator となる場合、PFS を使用しません。
Responder となる場合は、Initiator からの提案が Group 1、2、5、14 であれば、それを受け入れます。
IKEv2 では PFS を使用しません。

PFS とは？

Quick Mode キーが生成されるたびにキーの再交換を要求する Internet Key Exchange (IKE)の手順です。また、その際にキーの大きさ(Group1 or Group2)を指定します。
セキュリティの面では強固となりますが、キーの交換に時間がかかる欠点があります。

設定モード

VPN セレクタ設定モード

set security-association always-up

SA の確立状態を維持するかどうかを指定します。
このコマンドを設定した場合、一度確立した SA は確立し続けます。万一、SA が切断した場合は確立するまでリトライし続けます。
always-up の監視間隔は、always-up check-interval コマンドで指定することができます。

IPsec の Aggressive モードで運用する場合に、Initiator 側に設定しておくと効果的です。
センタ側 FITELnet-F シリーズ(固定 IP)-----拠点側 FITELnet-F シリーズ(動的 IP)
上記の環境では通常センタ側契機の VPN は張れないため、ライフタイム等で SA の消失後はセンタ側から通信が行えません。
このコマンドを使用することで拠点側より常時 SA が確立されるため、センタ側からの通信が不能になることはありません。

本設定または、if-state sync-sa のどちらか一方の設定が有効であれば、UP/DOWN 動作します。
また、両方の設定がない場合は常に IPsec インタフェースは UP の状態となります。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　SA を常時接続とする

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association always-up
```

コマンド書式

```
set security-association always-up
```

パラメータ

パラメータはありません。

この設定を行わない場合

確立した SA は、Lifetime の設定に従い解放します。

設定モード

VPN セレクタ設定モード

set security-association ipsec-src-id

Phase2 ID ペイロードの IP アドレスおよびアドレスマスクを定義します。
NAT 動作モードが”nat”(1 対 1 変換)の場合で、変換後のアドレスが複数存在する場合に、その複数のアドレス(範囲)をこのコマンドで指定します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　NAT 変換後のアドレスが 192.168.100.0/29 になる場合

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association ipsec-src-id 192.168.100.0 0.0.0.7
```

コマンド書式

set security-association ipsec-src-id <IP アドレス> [Wildcard マスク]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	NAT 変換後のネットワークアドレスを指定します。	IPv4 アドレス形式	省略不可
Wildcard マスク	変換後のアドレスを範囲指定するために、Wildcard マスクを指定します。詳細は範囲指定方法を参照してください。	IPv4 アドレス形式	Wildcard マスクは、0.0.0.0 となります。

この設定を行わない場合

1 つのアドレス情報でセレクタ情報を送信します。

範囲指定方法

set security-association ipsec-src-id コマンドで IP アドレスを指定する場合、マスク(Wildcard マスク)を使用して 1 エントリでアドレス範囲を指定することができます。
Wildcard マスクは、サブネットマスクとは書式が異なりますので注意してください。Wildcard マスクとサブネットマスクは、"1"と"0"の判別が逆になります。

例1)24bit マスクを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
Wildcard マスクの場合:0.0.0.255
サブネットマスクの場合:255.255.255.0

例2)ホストを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
Wildcard マスクの場合:0.0.0.0
サブネットマスクの場合:255.255.255.255

設定モード

VPN セレクタ設定モード

set security-association lifetime

IPSEC-SA/CHILD SA の生存時間を設定します。
IPSEC-SA の生存時間は、以下の 2 種類のパラメータで指定することができます。
CHILD SA は時間のパラメータのみ設定可能です。

IPsec では、生存時間の満了時に SA を解放します。
これは、同じ SA を使いつづけると暗号化の鍵を見破られる可能性が高くなり、安全な通信ができなくなるための対策としての機能です。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　Phase2 SA の生存時間を 3600 秒に設定する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association lifetime seconds 3600
```

設定例 2　Phase2 SA の生存中継データ量を 1000byte に設定する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association lifetime kilobytes 1000
```

コマンド書式

set security-association lifetime { seconds <生存時間> | kilobytes <生存中継データ量> }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
生存時間	IPSEC-SA/CHILD SA の生存時間を時間(単位:秒)で指定します。 ここで指定した時間経過後、IPSEC-SA/CHILD SA を解放します。	60～4294967295	省略不可
生存中継データ量	SA 上で通信するデータ量(単位:キロバイト数)を指定します。 ここで指定したデータ量を通信した後、IPSEC-SA/CHILD SA を解放します。	1000～4294967295	省略不可

※ 時間とデータの両方を指定した場合は、時間が経過したもしくは指定したデータ量の通信が行なわれた場合(先に満了したタイミングで)に、IPSEC-SA を解放します。
※ IKEv2 CHILD SA の生存時間に 946080000 秒(30 年)より大きな値が設定された場合は、946080000 秒として動作します。

この設定を行わない場合

生存時間は、600 秒です。
バイト数での生存時間は存在しません。

VPN ピアと設定が異なる場合

SA を確立しようとしている VPN ピアと、生存時間の設定が異なる場合は、次のようになります。

initiator の場合	自装置の設定値を採用します。	
responder の場合	IKEv1	自装置の設定値と相手からの提案された値を比較して、小さい方を採用します。
	IKEv2	自装置の設定値を採用

設定モード

VPN セレクタ設定モード

set transform-set

ipsec transform-set コマンドで設定する IPSEC-SA/CHILD SA の暗号化ポリシーを対応付けます。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　このセレクタにおいては、ipsec transform-set で指定した"policy1"のポリシーを使用する

```
Router(config)#ipsec transform-set policy1 esp-des esp-md5-hmac

Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set transform-set policy1
```

コマンド書式

set transform-set <ポリシー名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシー名称	ipsec transform-set で設定したポリシー名称を指定します。	16 文字以内の英数字	省略不可

この設定を行わない場合

IKEv1 では暗号化アルゴリズム:DES、認証アルゴリズム:HMAC-MD5 で動作します。
IKEv2 では暗号化アルゴリズム:3DES、認証アルゴリズム:HMAC-SHA-1 で動作します。

設定モード

VPN セレクタ設定モード

Mode-config の設定

configuration mode(isakmp policy)

mode-config のネゴシエーションにおいて、REQUEST/REPLY 制御で動作するか SET/ACK 制御で動作するかを設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　REQUEST/REPLY 制御で動作する

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#configuration mode initiate
```

コマンド書式

configuration mode <制御モード> [skip]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
制御モード	REQUEST/REPLY 制御で動作するか SET/ACK 制御で動作するかを設定します。 initiate：REQUEST/REPLY 制御モードで動作し、自装置から req を送信します。 respond：SET/ACK 制御モードで動作し、set を受信待ちをします。	initiate respond	省略不可
skip	skip を指定することで、mode-config を省略することができます。	skip	mode-config を行います。

この設定を行わない場合

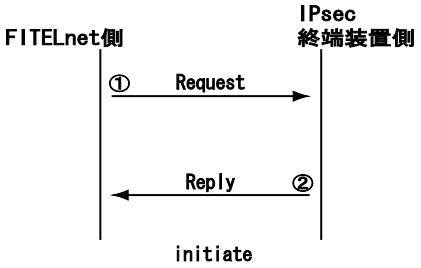
set-ack モードで動作し、set の受信待ちをします。
Mode Config を使用する場合は、ip vpn-nat inside source コマンドで modeconfig で割り当てられた NAT+変換する設定を行う必要があります。

モードコンフィグの手法

モードコンフィグは、VPN 通信を行う際に Peer 同士の情報を交換する手法であり、情報交換方法は 2 パターンあります。

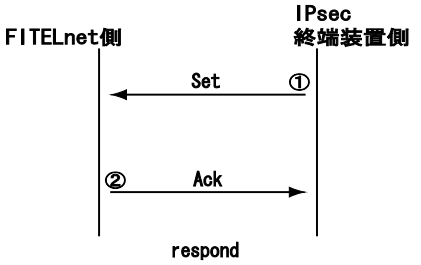
1）configuration mode initiate を指定した場合

本装置はモードコンフィグのイニシエータとして動作します。
本装置から、モードコンフィグのレスポンダに対して、要求（Request）を送信して、返答（Reply）を待ちます。



2）configuration mode respond を指定した場合

本装置はモードコンフィグのレスポンダとして動作します。
本装置は、モードコンフィグのイニシエータから通知（Set）を受けて、承認（Ack）を返します。



設定モード

IKE ポリシー設定モード

configuration mode（security-association）

mode-config のネゴシエーションにおいて、REQUEST/REPLY 制御で動作するか SET/ACK 制御で動作するかを設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　REQUEST/REPLY 制御で動作する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#configuration mode initiate
```

コマンド書式

configuration mode <制御モード>

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
制御モード	REQUEST/REPLY 制御で動作するか SET/ACK 制御で動作するかを設定します。		initiate respond	省略不可
	initiate	REQUEST/REPLY 制御モードで動作し、自装置から req を送信します。		
	respond	SET/ACK 制御モードで動作し、set を受信待ちをします。		

この設定を行わない場合

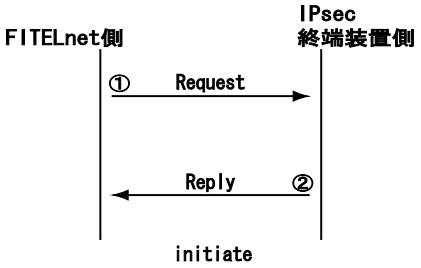
set-ack モードで動作し、set の受信待ちをします。
Mode Config を使用する場合は、ip vpn-nat inside source コマンドで modeconfig で割り当てられた NAT+変換する設定を行う必要があります。

モードコンフィグの手法

モードコンフィグは、VPN 通信を行う際に Peer 同士の情報を交換する手法であり、情報交換方法は 2 パターンあります。

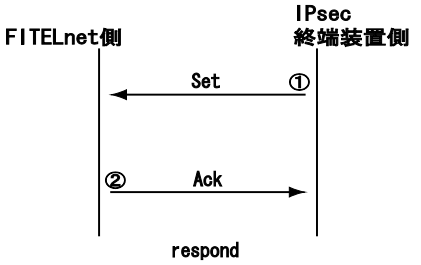
1）configuration mode initiate を指定した場合

本装置はモードコンフィグのイニシエータとして動作します。
本装置から、モードコンフィグのレスポンダに対して、要求（Request）を送信して、返答（Reply）を待ちます。



2）configuration mode respond を指定した場合

本装置はモードコンフィグのレスポンダとして動作します。
本装置は、モードコンフィグのイニシエータから通知（Set）を受けて、承認（Ack）を返します。



設定モード

IPsec 各種設定モード

ip vpn-nat inside source

既存のネットワーク(LAN)同士を IPsec にて VPN を構築する際、互いのネットワークアドレスが重複している場合があります。
IPsec では同じネットワークアドレスの LAN を接続することが出来ません。
そのため、VPN-NAT 変換を行うことで見かけ上の重複を回避し、既存のネットワークの IP 再割り当てを行うことなく IPsec を実現します。

LAN 側から WAN 側への VPN-NAT 変換ルールを設定します。
NAT モードの場合と、NAT+モード(IP マスカレード)の場合で、設定のしかたが異なりますので注意してください。
パラメータ"static-subnet"を指定することにより VPN-NAT の変換ルールを、ネットワーク単位で指定することもできます。<ローカルアドレス・サブネットマスク>で指定したローカルアドレスから<グローバルアドレス・サブネットマスク>で指定したグローバルアドレスへの変換を、<サブネットマスク>で指定した単位で一括設定します。

VPN-NAT と、IPsec インタフェースでの NAT※の、それぞれ設定に不整合がない場合は、
IPsec インタフェースでの NAT が有効となり、VPN-NAT は無効となります。
※IPsec インタフェースでの NAT は V01.03(00)以降サポート

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　NAT 変換 (192.168.0.0/24　→　192.168.100.0/24)

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# ip vpn-nat inside source list 1 pool vpn-pool1
Router(config-isakmp)# ip vpn-nat pool vpn-pool1 192.168.100..0 0.0.0.255



Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list 1 の部分の設定
```

【解説】

ip vpn-nat inside source <LAN 側のアドレス範囲> <WAN 側のアドレス範囲>
となります。
<LAN 側のアドレス範囲>は、access-list コマンドで指定します。
<WAN 側のアドレス範囲>は、ip-vpn nat pool <pool 名>コマンドで指定します。

設定例 2　NAT+変換 (192.168.0.0/24　→　インタフェースアドレス)

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# ip vpn-nat inside source list 1 interface



Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list 1 の部分の設定
```

【解説】

ip vpn-nat inside source <LAN 側のアドレス範囲> <WAN 側のアドレス範囲>
となります。
<LAN 側のアドレス範囲>は、access-list コマンドで指定します。
<WAN 側のアドレス範囲>は、インタフェースアドレスに集約する場合は"interface"、Mode-config 機能により取得したアドレスに集約する場合は"modeconfig"、指定したアドレスに集約する場合は"peer <ip-address>"と指定します。

設定例３　NAT 変換（一括変換）158.xxx.xxx.xxx.0/24←→192.168.100.0/24 に変換する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#ip vpn-nat inside source static-subnet 158.xxx.xxx.0 192.168.100.0
255.255.255.0
```

【解説】
ip vpn-nat inside source static-subnet <ローカルサブネット> <グローバルサブネット> <サブネットマスク>
となります。
グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。
NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます（複数同時登録）。

例）local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT 時】　ip-vpn nat inside source list <access-list 番号> [変換前開始ポート番号 [変換前終了ポート番号]] pool <プール名> [overload | [変換後開始ポート番号 [変換後終了ポート番号]]]
【NAT+時】 ip-vpn nat inside source list <access-list 番号> [開始ポート番号 [終了ポート番号]] NAT+変換後のアドレス overload | [変換後開始ポート番号 [変換後終了ポート番号]]]
【スタティック変換】 ip vpn-nat inside source static <ローカルアドレス> <グローバルアドレス>
【NAT スタティック（一括変換）】 ip vpn-nat inside source static-subnet <ローカルサブネット> <グローバルサブネット> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前（ローカルアドレス）範囲を指定したアクセスリストを指定します。	1～99 1300～1399 10000～11200	省略不可
[変換前開始ポート番号 変換前終了ポート番号]	変換前の TCP/UDP ポート番号（範囲）を指定します。	1～65535	自動ポート変換

プール名	変換後(グローバルアドレス)範囲を指定した VPN-NAT プール名を指定します。	NAT プール名	NAT の場合は省略不可
NAT+変換後のアドレス	NAT+変換後のアドレスを指定します。	interface：送信インタフェースのアドレスに変換 modeconfig：相手から割り当てられたアドレスに変換 peer <IP アドレス>：設定する IP アドレスに変換	NAT+の場合は省略不可
overload	local のポート番号を必ず別のポート番号に変換する場合に指定 ※変換後のポート番号は 1024～65535	overload	local のポート番号を基本的には変換せずに napt を試みます。 すでにそのポート番号が使用されている場合に限り、別のポート番号に変換します。 変換後のポート番号は 1024～65535。
[変換後開始ポート番号 変換後終了ポート番号]	変換後の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
ローカルアドレス	変換前のローカルアドレスを指定します。	IPv4 アドレス形式	省略不可
グローバルアドレス	変換後のグローバルアドレスを指定します。	IPv4 アドレス形式	省略不可
ローカルサブネット	変換前のローカルアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
グローバルサブネット	変換後のグローバルアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで	IPv4 アドレス形式	省略不可

	指定した単位で一括設定します。		

最大エントリ数：リスト 1 エントリ(isakmp policy 毎)装置全体で 200 エントリ
スタティック 5000 エントリ(装置全体)※isakmp policy 毎の制限はありません

この設定を行わない場合

VPN-NAT が使用できません。

適用順序

NAT 変換ルールは以下の順序で適用されます。

1）static 変換ルール
2）list による変換ルール

同じ種類のルール内では、Prefix 長が長いルールが優先して適用されます。
同一 Prefix 長の設定が複数あった場合には、config 上で先に登録されたものが優先されます。
なお、config には、以下の順に登録され、同じ種類については入力順に登録されます。

1）static 変換ルール（既存のホストアドレス指定）
2）static-subnet 変換ルール
3）list による変換ルール

設定モード

IKE ポリシー設定モード

トンネルルート機能の設定

tunnel-route（装置単位のトンネルルート）

IPsec 通信において、本装置が Aggressive モードの Responder となった場合に、VPN ピアへの経路情報をテーブルに登録する場合に指定します。
この場合、VPN ピアへの NextHop も合わせて指定します。
tunnel-route の設定をした装置に crypto isakmp policy の peer-identity distinguished-name を設定すると tunnel-route が動作しません。

IKEv1 専用コマンド

設定例１　VPN ピアへの経路情報を登録する（NextHop は 192.168.100.1 とする）

```
Router(config)#crypto security-association
Router(config-crypto-sa)#tunnel-route address 192.168.100.1
```

設定例２　VPN ピアへの経路情報を登録する（NextHop は PPPoE#1 とする）

```
Router(config)#crypto security-association
Router(config-crypto-sa)#tunnel-route interface pppoe 1
```

コマンド書式

tunnel-route { address <IP アドレス> | interface <インタフェース名称> }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	VPN ピアへの経路情報を登録し、NextHop のアドレスを設定します。	IPv4 アドレス形式	省略不可
インタフェース名称	VPN ピアへの経路情報を登録し、NextHop のインタフェースを設定します。	インタフェース名称	

この設定を行わない場合

Aggressive モードの Responder の場合でも、VPN ピアへの経路情報を登録しません。

何のための設定？

Aggressive モードでは、IP アドレスではなく ID で認証できるため、Responder では IPsec のネゴシエーションが始まってから相手の IP アドレスがわかるというケースがあります。この場合、相手（VPN ピア）の IP アドレスへの経路は、（多くの場合）デフォルトルートにしたがってしまうことになります。

このコマンドにて、まだわからない VPN ピアへの経路情報の NextHop を指定しておき、デフォルトルートとは違う経路で通信を行なうことができるようになります。

設定モード

IPsec 各種設定モード

tunnel-route（VPN ピア単位のトンネルルート）

IPsec 通信において、本装置が Aggressive モードの Responder となった場合に、VPN ピアへの経路情報をテーブルに登録する場合に指定します。
この場合、VPN ピアへの NextHop も合わせて指定します。
tunnel-route の設定をした装置に crypto isakmp policy の peer-identity distinguished-name を設定すると tunnel-route が動作しません。

crypto security-association モードで、設定する tunnel-route コマンドは装置に対し1つしか設定できないのに対して、本コマンドは、peer 単位で設定することができます。
本コマンドが設定されると、crypto security-association モードで設定されている tunnel-route コマンドより優先的に利用されます。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例１　VPN ピアへの経路情報を登録する（NextHop は 192.168.100.1 とする）

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#tunnel-route address 192.168.100.1
```

設定例２　VPN ピアへの経路情報を登録する（NextHop は PPPoE#1 とする）

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#tunnel-route interface pppoe 1
```

コマンド書式

```
tunnel-route { address <IP アドレス> | interface <インタフェース名称>
               {ewan <1-2> | pppoe <1-24>}}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	VPN ピアへの経路情報を登録し、NextHop のアドレスを設定します。	IPv4 アドレス形式	省略不可
インタフェース名称	VPN ピアへの経路情報を登録し、NextHop のインタフェースを設定します。	ewan 1～2 pppoe 1～24 dialer 1～20	

この設定を行わない場合

Aggressive モードの Responder の場合でも、VPN ピアへの経路情報を登録しません。

何のための設定？

Aggressive モードでは、IP アドレスではなく ID で認証できるため、Responder では IPsec のネゴシエーションが始まってから相手の IP アドレスがわかるというケースがあります。
この場合、相手（VPN ピア）の IP アドレスへの経路は、（多くの場合）デフォルトルートにしたがってしまうことになります。
このコマンドにて、まだわからない VPN ピアへの経路情報の NextHop を指定しておき、デフォルトルートとは違う経路で通信を行なうことができるようになります。

設定モード

IKE ポリシー設定モード

SA-UP ルート機能の設定

sa-up route

SA-up ルートの nexthop を設定します。
これにより、IPsec SA が張られた際、その ipsec access-list の宛先 IP アドレスの経路情報をルーティングテーブル上に追加します。(SA が消失した際は、その経路情報はルーティングテーブルから削除されます)
特に、センタ側などで 2 台構成の機器冗長も行う場合、上位で経路制御を行うルータ(又は L3 スイッチ)に対し RIP 等のダイナミックルーティングプロトコルを組み合わせ経路情報の広告のために使用します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　SA-up ルートの nexthop に 192.168.3.8 を指定します。

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#sa-up route address 192.168.3.8
```

コマンド書式

sa-up route <nexthop> [プロトコル] [distance]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
nexthop	SA-up ルートの nexthop を IP アドレスまたは、インタフェースで設定します。 IP アドレス：SA-up ルートの nexthop をアドレスで設定します。 インタフェース名：SA-up ルートの nexthop をインタフェースで設定します。	IP アドレス形式 ewan 1～2 pppoe 1～24 dialer 1～20 ipsecif 1～2000	省略不可
プロトコル	経路情報を広告するためのプロトコルを選択します。	local-prot1 local-prot2	rip で metric 1 で配信します。
distance	登録する経路情報の distance 値を指定します。	1～255	0

この設定を行わない場合

SA-up ルート機能を使用することができません。

設定モード

VPN セレクタ設定モード

拡張認証の設定

aaa enable

接続相手との認証に、拡張認証（Xautu）を行うかどうかを設定します。
拡張認証（Xautu）を行う場合は、相手のユーザ名・パスワードを aaa peer-name コマンドで設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　拡張認証を行う

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#aaa enable
```

コマンド書式

```
aaa enable
```

パラメータ

パラメータはありません。

この設定を行わない場合

拡張認証を行いません。

拡張認証とは？

IPsec では、電子証明書または Pre-shared key での認証のほかに、ユーザ名・パスワードの認証を行うことができ、これを拡張認証といいます。

設定モード

IKE ポリシー設定モード

aaa my-name

接続相手から拡張認証(Xauth)される場合の、自身のユーザ名とパスワードを設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　拡張認証で使用する自身のユーザ名を"FITELnet F2200"、パスワードを"F2200-pass"とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#aaa my-name FITELnet F2200 password F2200-pass
```

コマンド書式

aaa my-name <ユーザ名> <パスワード> [{secret | private}[encrypted]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ユーザ名	相手から拡張認証(Xauth)される場合の相手のユーザ名を設定します。	最大 64 文字の英数字	省略不可
パスワード	相手から拡張認証(Xauth)される場合の相手のパスワードを設定します。	最大 64 文字の英数字	省略不可
secret | private	パスワードを暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。※1 secret：暗号化する際に共有暗号鍵を使用する private：暗号化する際に装置固有暗号鍵を使用する	secret private	パスワードを暗号化しません
encrypted	パスワードを暗号化処理するかどうかを設定します。 このオプションを付加することにより、パスワードは暗号化済みと判定されます。※2 secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。	encrypted	パスワードを暗号化データとして扱いません

※1 このオプションは、設定するとすぐに有効となり、パスワードが暗号化されて表示され encrypted オプションが自動的に付加されます。
※2 パスワードが既に暗号化済みの場合は、このオプションを指定する必要があります。

この設定を行わない場合

拡張認証で使用する自身の名前とパスワードはありません。

拡張認証とは？

IPsec では、電子証明書または Pre-shared key での認証のほかに、ユーザ名・パスワードの認証を行うことができ、これを拡張認証といいます。

ワンポイント

相手を拡張認証する場合、相手のユーザ名・パスワードは、"aaa peer-name"コマンドで設定します。

設定モード

IKE ポリシー設定モード

aaa peer-name

相手を拡張認証(Xauth)する場合の、相手のユーザ名とパスワードを設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　拡張認証で使用する相手のユーザ名を"VPN-Peer1"、パスワードを"VPN-Peer1-pass"とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#aaa peer-name VPN-Peer1 password VPN-Peer1-pass
```

コマンド書式

aaa peer-name 〈ユーザ名〉〈パスワード〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ユーザ名	相手から拡張認証(Xauth)される場合の自身のユーザ名を設定します。	最大 64 文字の英数字	省略不可
パスワード	相手から拡張認証(Xauth)される場合の自身のパスワードを設定します。	最大 64 文字の英数字	省略不可

この設定を行わない場合

相手を拡張認証することはできません。

拡張認証とは？

IPsec では、電子証明書または Pre-shared key での認証のほかに、ユーザ名・パスワードの認証を行うことができ、これを拡張認証といいます。

ワンポイント

自分が拡張認証される場合、自分のユーザ名・パスワードは、"aaa my-name"コマンドで設定します。

設定モード

IKE ポリシー設定モード

電子証明書に関する設定

crypto ca identity

証明書のリクエストを作成する上で、自身の情報を設定する必要があります。
本コマンドでは、証明書のリクエストを作成する上での、自身の情報を設定するために、電子証明書（自身の ID）設定モードに移行します。

IKEv1/IKEv2 共通コマンド

設定例１　電子証明書（自身の ID）設定モードに移行する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#
```

コマンド書式

```
crypto ca identity
```

パラメータ

パラメータはありません。

設定モード

基本設定モード

crl-optional

証明書の有効性を CRL で確認するかしないかを設定します。

IKEv1/IKEv2 共通コマンド

設定例 1　証明書の有効性を必ず CRL で確認する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#crl-optional must
```

コマンド書式

crl-optional <CRL 設定>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
CRL 設定	この証明書に関して、CRL を使用するかどうかを指定します。 must：証明書の有効性を必ず CRL で確認します。CRL が取得できない場合は、無効と判断されます。 notuse：証明書の有効性を CRL で確認しません。	must notuse	省略不可

この設定を行わない場合

CRL を取得（20 秒以内）できれば証明書の有効性を確認しますが、取得できなければ確認を行いません。

設定モード

電子証明書（自身の ID）設定モード

email

証明書リクエストファイルに含める電子メールアドレスを設定します。電子メールアドレスの情報を含めない場合は、設定の必要はありません。

IKEv1/IKEv2 共通コマンド

設定例１　証明書リクエストファイルに含める電子メールアドレスとして、F2200@xxxxx.ne.jp を設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#email F2200@xxxxx.ne.jp
```

コマンド書式

email〈電子メールアドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
電子メールアドレス	証明書リクエストファイルに含める電子メールアドレスを設定します。	最大 64 文字	省略不可

この設定を行わない場合

証明書リクエストファイルに、E-Mail アドレスを含めることはできません。

設定モード

電子証明書（自身の ID）設定モード

ip address

証明書リクエストファイルに含める IP アドレスを設定します。IP アドレスの情報を含めない場合は、設定の必要はありません。

IKEv1/IKEv2 共通コマンド

設定例 1　証明書リクエストファイルに含める IP アドレスとして、192.168.1.1 を設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#ip address 192.168.1.1
```

コマンド書式

ip address <IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	証明書リクエストファイルに含める IP アドレス	IPv4 アドレス形式	省略不可

この設定を行わない場合

証明書リクエストファイルに、IP アドレスを含めることはできません。

設定モード

電子証明書(自身の ID)設定モード

ip domain-name

証明書リクエストファイルに含めるドメイン名称を設定します。ドメイン名称の情報を含めない場合は、設定の必要はありません。

IKEv1/IKEv2 共通コマンド

設定例１　証明書リクエストファイルに含めるドメイン名称として、xxxxx.ne.jp を設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#ip domain-name xxxxx.ne.jp
```

コマンド書式

ip domain-name <ドメイン名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ドメイン名	証明書リクエストファイルに含めるドメイン名称	最大 64 文字	省略不可

この設定を行わない場合

証明書リクエストファイルに、ドメイン名を含めることはできません。

設定モード

電子証明書（自身の ID）設定モード

ipv6 address

証明書リクエストファイルに含める IPv6 アドレスを設定します。
IPv6 アドレスの情報を含めない場合は、設定の必要はありません。

IKEv1/IKEv2 共通コマンド

設定例 1　証明書リクエストファイルに含める IPv6 アドレスとして、3ffe:200::1 を設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#ipv6 address 3ffe:200::1
```

コマンド書式

ipv6 address <IPv6 アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPv6 アドレス	証明書リクエストファイルに含める IPv6 アドレス	IPv6 アドレス形式	省略不可

この設定を行わない場合

証明書リクエストファイルに、IPv6 アドレスを含めることはできません。

設定モード

電子証明書（自身の ID）設定モード

name server

CRL を HTTP サーバに取りに行く場合の名前解決に使用するネームサーバーの IP アドレスを設定します。

IKEv1 専用コマンド

設定例 1　ネームサーバの IP アドレスを、192.168.100.1 に設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#name server 192.168.100.1
```

コマンド書式

name server 〈ネームサーバの IP アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ネームサーバの IP アドレス	CRL を HTTP サーバに取りに行く場合の名前解決に使用するネームサーバーの IP アドレスを設定します。	IPv4 アドレス形式	省略不可

設定モード

電子証明書(自身の ID)設定モード

query-ip

CRL を LDAP サーバに取りに行く場合の LDAP サーバの IP アドレスを設定します。

IKEv1 専用コマンド

設定例 1　LDAP サーバの IP アドレスを 192.168.100.2 に設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#query-ip 192.168.100.2
```

コマンド書式

query-ip <LDAP サーバの IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
LDAP サーバの IP アドレス	CRL を LDAP サーバに取りに行く場合の LDAP サーバの IP アドレスを設定します。	IPv4 アドレス形式	省略不可

設定モード

電子証明書(自身の ID)設定モード

IPsec のログ情報に関する設定

nolog-block-type-discard

vpnlog の"block type discard ～"を抑制する設定を行います。
受信したパケットを暗号化するかどうか判断するためにセレクタ検索をする際に、下記のような場合に上記ログが記載されます。
1）マッチした ipsec access-list が discard だった場合。
2）設定された ipsec access-list にマッチしなかった場合。
このコマンドで該当するログを抑制することにより、他のログを参照しやすくすることができます。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例１　block type discard を制御する設定する

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#nolog-block-type-discard
```

コマンド書式

nolog-block-type-discard

パラメータ

パラメータはありません

設定モード

IPsec ログモード

nolog-spi-no-match

"SPI no match ～"の vpnlog を抑制する設定を行います。
受信した ESP パケットが自装置宛にもかかわらず、パケットに格納されている SA が自装置管理下にある SA にマッチしなかった場合に出力されるログを抑制します。
このコマンドで該当するログを抑制することにより、他のログを参照しやすくすることができます。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例１　"SPI no match ～"の vpnlog を抑制する設定を行う

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#nolog-spi-no-match
```

コマンド書式

nolog-spi-no-match

パラメータ

パラメータはありません

設定モード

IPsec ログモード

vpnlog-detail

IKE、IPSEC ネゴの vpnlog と、keepalivefail の vpnlog 出力をピア No.ごとに設定します。
また、本コマンドを設定すると、vpnlog enable コマンドで設定した内容が有効になりません。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　keepalivefail の vpnlog 出力を全て表示する

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#vpnlog-detail all
```

コマンド書式

crypto ipsec-log vpnlog-detail <属性>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
属性	ピア番号を範囲で指定するために、ポート属性を指定します。 all：全てのピア番号が対象となります eq 1～2000：指定するピア番号を持つパスが対象となります。 gt 1～1999：指定するピア番号より大きい番号を持つパスが対象となります。 lt 2～2000：指定するピア番号より小さい番号を持つパスが対象となります。 neq 1～2000：指定するピア番号以外の番号を持つパスが対象となります。 range 1～2000 1～2000：ピア番号の範囲を指定し範囲内の番号を持つパスが対象となります。	all eq 1～2000 gt 1～1999 lt 2～2000 neq 1～2000 range 1～2000 1～2000	省略不可

設定モード

IPsec ログモード

IPsec の各種設定

alive

ICMP-KeepAlive 機能を使用する場合のタイマ値/送信回数等を設定します。

IKEv1/IKEv2 共通コマンド

設定例１　１回の KeepAlive で４つの ICMP を送信する、そのうち３つの応答を受け取れなかった場合に SA の障害とみなす

```
Router(config)#crypto security-association
Router(config-crypto-sa)#alive count 4 3
```

設定例２　１回の KeepAlive で４つの ICMP を送信し、そのうち３つ以上応答が無い状態が３回以上続いた場合に SA の障害とみなす

```
Router(config)#crypto security-association
Router(config-crypto-sa)#alive count 4 3 fail 3
```

設定例３　ICMP の KeepAlive のタイムアウト時間を３秒とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#alive timeout 3
```

設定例４　ICMP の KeepAlive を 60 秒間隔で送信する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#alive freq 60
```

コマンド書式

```
alive count <ICMP 送信数> <ICMP 失敗数> [fail <ICMP リトライ回数>]
alive freq <送信間隔> [degraded-freq <送信間隔>]
alive timeout <timeout 時間>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ICMP 送信数	1 回の KeepAlive で送信する ICMP の数を設定します。	1～15	省略不可
ICMP 失敗数	1 回の KeepAlive で送信した ICMP 数のうち、何個応答を受け取れなかった時に監視失敗と判定するかを設定します。	1～15	省略不可
ICMP 連続失敗回数	何回連続して ICMP 監視に失敗したら SA の障害と判定するかを設定します。	1～10	1
送信間隔	正常時の ICMP KeepAlive の送信間隔(秒)を設定します。	5～1000	省略不可
degraded-freq <送信間隔>	リトライ時の ICMP KeepAlive の送信間隔(秒)を設定します。	5～1000	60
timeout 時間	ICMP KeepAlive の応答待ち時間(秒)	3～60	省略不可

この設定を行わない場合

ICMP 送信数	4 回
ICMP 失敗数	3 回
ICMP 連続失敗回数	1 回
送信間隔	60 秒
degraded-freq 送信間隔	60 秒
timeout 時間	3 秒

設定モード

IPsec 各種設定モード

always-up check-interval

SA の確立状態を維持する場合の、always-up の監視間隔を指定します。
本コマンドは、set security-association always-up コマンドで、SA の確立状態を維持する設定にした場合のみ有効です。

IKEv1/IKEv2 共通コマンド

設定例 1　always-up の監視間隔を 10 秒とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)# always-up check-interval 10
```

コマンド書式

always-up check-interval <監視間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
監視間隔	always-up の監視間隔(秒単位)を設定します。	1～20	省略不可

この設定を行わない場合

always-up の監視間隔は 20 秒となります。

設定モード

IPsec 各種設定モード

am-3-encr

Aggressive モードによるネゴシエーションの 3 番目の ISAKMP パケットを暗号化する場合に指定します。
VPN ピアが CISCO3030 の場合は、指定が必要です。

IKEv1 専用コマンド

設定例 1　Aggressive モードの 3 番目のパケットを暗号化する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#am-3-encr
```

コマンド書式

am-3-encr

パラメータ

パラメータはありません。

この設定を行わない場合

Aggressive モードのネゴシエーションの 3 番目の ISAKMP パケットは、暗号化しません。

設定モード

IPsec 各種設定モード

am-3-initcont

Aggressive モードによるネゴシエーションの 3 番目の ISAKMP パケットに、INITIAL-CONTACT を送出します。

IKEv1 専用コマンド

設定例 1　3 番目の Aggressive パケットに INITIAL-CONTACT を送出する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#am-3-initcont
```

コマンド書式

am-3-initcont

パラメータ

パラメータはありません。

この設定を行わない場合

Aggressive の完了後に informational パケットの INITIAL-CONTACT を送出します。

設定モード

IPsec 各種設定モード

configuration mode

mode-config のネゴシエーションにおいて、REQUEST/REPLY 制御で動作するか SET/ACK 制御で動作するかを設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　REQUEST/REPLY 制御で動作する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#configuration mode initiate
```

コマンド書式

configuration mode <制御モード>

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>制御モード</td><td>REQUEST/REPLY 制御で動作するか SET/ACK 制御で動作するかを設定します。<table><tr><td>initiate</td><td>REQUEST/REPLY 制御モードで動作し、自装置から req を送信します。</td></tr><tr><td>respond</td><td>SET/ACK 制御モードで動作し、set を受信待ちをします。</td></tr></table></td><td>initiate
respond</td><td>省略不可</td></tr>
</table>

この設定を行わない場合

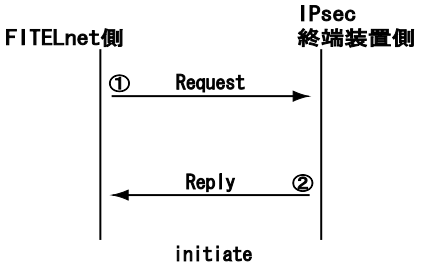
set-ack モードで動作し、set の受信待ちをします。
Mode Config を使用する場合は、ip vpn-nat inside source コマンドで modeconfig で割り当てられた NAT+変換する設定を行う必要があります。

モードコンフィグの手法

モードコンフィグは、VPN 通信を行う際に Peer 同士の情報を交換する手法であり、情報交換方法は 2 パターンあります。

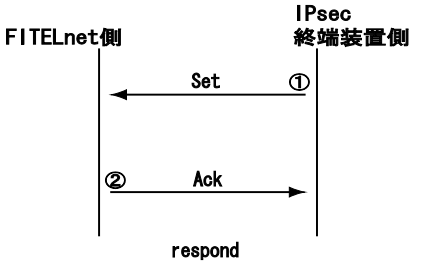
1）configuration mode initiate を指定した場合

本装置はモードコンフィグのイニシエータとして動作します。
本装置から、モードコンフィグのレスポンダに対して、要求（Request）を送信して、返答（Reply）を待ちます。



2）configuration mode respond を指定した場合

本装置はモードコンフィグのレスポンダとして動作します。
本装置は、モードコンフィグのイニシエータから通知（Set）を受けて、承認（Ack）を返します。



設定モード

IPsec 各種設定モード

configuration application-version message

configuration mode コマンドで initiate を選択した場合に、アプリケーションバージョン属性にセットする値を指定します。
respond を選択した場合は、利用しません。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例１　アプリケーションバージョンの値をセットする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#configuration  application-version message fitel
```

コマンド書式

configuration application-version message <Word>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Word	アプリケーションバージョン属性にセットする値を指定します。	127 文字以内	省略不可

※ スペースも文字数としてカウントされます。
例：ＡＢＣの場合、5 文字としてカウントされます。

この設定を行わない場合

装置名と版数をセットします。

設定モード

IPsec 各種設定モード

configuration application-version push

configuration application-version message コマンドの設定があり、かつ、configuration mode コマンドで initiate が設定されている場合に、configuration application-version message コマンドのメッセージをセットして req パケットを送信します。
configuration application-version message コマンドの設定がない場合は、configuration application-version message コマンドのデフォルト値を使用して req パケットを送信します。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　アプリケーションバージョンに値をセットして request を送信する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#configuration application-version push
```

コマンド書式

```
configuration application-version push
```

パラメータ

パラメータはありません

この設定を行わない場合

request パケットのアプリケーションバージョン欄を null で送信します。

設定モード

IPsec 各種設定モード

crypto security-association

IPsec 機能全般の、各種タイマ値等を設定するために、IPsec 各種設定モードに移行します。

IKEv1/IKEv2 共通コマンド

設定例 1　IPsec 各種設定モードに移行します。

```
Router(config)#crypto security-association
Router(config-crypto-sa)#
```

コマンド書式

```
crypto security-association
```

パラメータ

パラメータはありません。

設定モード

基本設定モード

if-state sync-sa

IPsec インタフェースの UP/DOWN を SA 有無に連携する場合に設定します。
本設定または、crypto map の set security-association always-up のどちらか一方の設定が有効であれば、UP/DOWN 動作します。
また、両方の設定がない場合は常に IPsec インタフェースは UP の状態となります。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　IPsec インタフェースの UP/DOWN 制御を SA 有無に連携させる

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#if-state sync-sa
```

コマンド書式

```
if-state sync-sa
```

パラメータ

パラメータはありません

この設定を行わない場合

IPsec インタフェースは、常に UP となります。

設定モード

IPsec インタフェース設定モード

ikealive freq

IKE KeepAlive 機能として使用する DPD(Dead Peer Detection)のパラメータを設定します。

IKEv1/IKEv2 共通コマンド

設定例 1　DPD メッセージの送信間隔を 30 秒に設定する

```
Router(config)#crypto security-association
Router(config-crypto-sa)# ikealive freq 30
```

コマンド書式

ikealive freq <送信間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	DPD メッセージの送信間隔(単位:秒)を設定します。	10～3600 秒	省略不可

この設定を行わない場合

送信間隔は 60 秒です。

設定モード

IPsec 各種設定モード

ikealive retry max

IKE KeepAlive のリトライ回数を設定します。

IKEv1 専用コマンド

設定例 1　IKE KeepAlive のリトライ回数を 3 回に設定する

```
Router(config)#crypto security-association
Router(config-crypto-sa)# ikealive retry max 3
```

コマンド書式

ikealive retry max <リトライ回数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リトライ回数	IKE KeepAlive のリトライ回数を設定します。	1～5	省略不可

この設定を行わない場合

リトライ回数は 1 回です。

設定モード

IPsec 各種設定モード

ikealive retry timer

IKE KeepAlive のリトライ間隔を設定します。

IKEv1 専用コマンド

設定例 1　IKE KeepAlive のリトライ間隔を 10 秒に設定する

```
Router(config)#crypto security-association
Router(config-crypto-sa)# ikealive retry timer 10
```

コマンド書式

ikealive retry timer <リトライ間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リトライ間隔	IKE KeepAlive のリトライ間隔を設定します。	2～60 秒	省略不可

この設定を行わない場合

リトライ間隔は 20 秒です。

設定モード

IPsec 各種設定モード

isakmp-negotiation

ISAKMP-SA のライフタイムが満了する前に、新しい SA を確立するために Phase1 のネゴシエーションを開始します。
本コマンドでは、ライフタイムが満了する何秒前に新しい SA のためのネゴシエーションを開始するかを設定します。

IKEv1 専用コマンド

設定例 1　本装置が Initiator の場合は、ライフタイム満了の 100 秒前にネゴシエーションを開始する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#isakmp-negotiation initiate 100
```

コマンド書式

isakmp-negotiation <initiate| respond> <差動時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
initiate| respond	この設定を、Initiator の SA に適用するか、Responder の SA に適用するかを選択します。	initiate respond	省略不可
差動時間	ライフタイムが満了する何秒前に新しい SA のためのネゴシエーションを開始するかを設定します。	1～86400	省略不可

この設定を行わない場合

Initiator 時のネゴシエーション開始時期：90 秒前
Responder 時のネゴシエーション開始時期：30 秒前

設定モード

IPsec 各種設定モード

negotiation

本装置では、IPSEC-SA/CHILD の SA のライフタイムが満了する前に、新しい SA を確立するために IKE-SA/CREATE CHILD SA のネゴシエーションを開始します。
本コマンドでは、ライフタイムが満了する何秒前に新しい SA のためのネゴシエーションを開始するかを設定します。
この値は、本装置自身が Initiator の場合と Responder の場合で、設定値を変更することができます。

IKEv1/IKEv2 共通コマンド

設定例１　本装置が Initiator の場合は、ライフタイム満了の 90 秒前にネゴシエーションを開始する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#negotiation initiate 90
```

設定例２　本装置が Responder の場合は、ライフタイム満了の 30 秒前にネゴシエーションを開始する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#negotiation respond 30
```

コマンド書式

negotiation <initiate| respond> <作動時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
initiate| respond	この設定を、Initiator の SA に適用するか、Responder の SA に適用するかを選択します。	initiate respond	省略不可
作動時間	Rekey の際、Lifetime 満了時間からどれくらい前(単位:秒)に、新しい SA を確立するかを設定します。	1～65535※	省略不可

※　設定範囲の最大値の 65535 は、V01.06 (00)以降サポート

この設定を行わない場合

initiator は 90 秒前、responder は 30 秒前に rekey を開始します。

設定モード

IPsec 各種設定モード

re-establish-sa rekey

Phase1 の SA の Rekey 動作を行います。

refresh コマンド後に有効になるコマンドです。

IKEv1 専用コマンド

設定例 1　Phase1 の SA の Rekey 動作を行う。

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#re-establish-sa rekey
```

コマンド書式

```
re-establish-sa rekey
```

パラメータ

パラメータはありません。

この設定を行わない場合

Phase1 の SA の Rekey 動作を行いません。

設定モード

IKE ポリシー設定モード

retry

ISAKMP による自動鍵交換の再送間隔(パラメータ:timer)と、最大再送回数(パラメータ:max)を設定します。

IKEv1/IKEv2 共通コマンド

設定例 1　ISAKMP による自動鍵交換の再送間隔を 20 秒とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry timer 20
```

設定例 2　ISAKMP による自動鍵交換の最大再送回数を 1 回とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry max 1
```

コマンド書式

```
retry timer <再送間隔>
retry max <最大送信回数>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	ISAKMP による自動鍵交換の再送間隔(単位:秒)を設定します。 再送を行う毎に間隔は 2 倍に増加していきます。	1～30	省略不可
最大送信回数	ISAKMP による自動鍵交換の最大再送回数を設定します。	1～5	省略不可

この設定を行わない場合

送信間隔	20 秒
最大送信回数	1 回

設定モード

IPsec 各種設定モード

retry guard-time

IKE ネゴパケットの送受信において、自身が送信してから対向の再送パケットを受け入れ可能とするまでの時間を設定します。

IKEv1/IKEv2 共通コマンド

設定例 1　対向の再送パケットの受け入れ可能時間を 5 秒に設定する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry guard-time 5
```

コマンド書式

retry guard-time<受信可能時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
受信可能時間	IKE ネゴパケットの送受信において、自身が送信してから対向の再送パケットを受け入れ可能とするまでの時間(単位:秒)を設定します。	1～30	省略不可

この設定を行わない場合

受信可能時間を 1 秒に設定します。

設定モード

IPsec 各種設定モード

retry rekey-ipsec

IPsec-SA の Rekey のリトライ間隔(パラメータ:timer)と、リトライ回数(パラメータ:max)を設定します。

IKEv1 専用コマンド

設定例 1　IPsec-SA の Rekey のリトライ間隔を 20 秒とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry rekey-ipsec timer 20
```

設定例 2　IPsec-SA の Rekey のリトライ回数を 3 回とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry rekey-ipsec max 3
```

コマンド書式

retry rekey-ipsec timer <リトライ間隔>
retry rekey-ipsec max <リトライ回数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リトライ間隔	IPsec-SA の Rekey のリトライ間隔(単位:秒)を設定します。	1～30	省略不可
リトライ回数	IPsec-SA の Rekey のリトライ回数を設定します。lifetime を指定すると Rekey のリトライを lifetime 満了まで繰り返します。	1～20 lifetime	省略不可

この設定を行わない場合

送信間隔	retry timer コマンドで設定した間隔になります。
送信回数	retry max コマンドで設定した回数になります。

設定モード

IPsec 各種設定モード

retry rekey-ipsec negotiation

IPsec-SA の Rekey のリトライオーバー後、再度 Rekey 機能を行う場合の Rekey 回数(パラメータ:max)を設定します。

IKEv1 専用コマンド

設定例 1　IPsec-SA の Rekey のリトライオーバー後に再度 Rekey を行う回数を 3 回とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry rekey-ipsec negotiation 3
```

コマンド書式

retry rekey-ipsec negotiation {<Rekey 回数>|lifetime}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Rekey 回数	IPsec-SA の Rekey のリトライオーバー後、再度 Rekey 機能を行う場合の回数を指定します。	1～20	省略不可
lifetime	IPsec-SA の Rekey のリトライオーバー後、lifetime 満了まで Rekey 機能を繰り返します。	lifetime	省略不可

この設定を行わない場合

Rekey を行いません。

設定モード

IPsec 各種設定モード

IPsec 基本コマンド(IKEv2)

vpn enable

IPsec 機能を有効にします。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　IPsec 機能を有効にする

```
Router(config)#vpn enable
```

コマンド書式

vpn enable [ewan <インタフェース>[modem]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース	セレクタ検索の対象とするインタフェースを指定します。 また、対象とする EWAN ポートを利用する PPPoE インタフェースにも適用されます。 1～2：指定した ewan のみ適用します。 all：ewan1、2 の両方に適用します。	1～2 all	LAN を除く全てのインタフェースがセレクタ検索の対象となります。
modem	セレクタ検索の対象とするインタフェースに、モデムインタフェースを指定します。 インタフェースに all を指定した場合は、modem を指定できません。	modem 1	モデムインタフェースをセレクタ検索の対象としません。

この設定を行わない場合

IPsec 機能は使用できません。

設定モード

基本設定モード

vpnlog enable

IPsec 機能を使用した VPN 通信動作中（SA の確立／解放）の VPN ログを残すか残さないかを設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　SA の確立／解放を VPN ログに残す

```
Router(config)#vpnlog enable
```

コマンド書式

```
vpnlog enable
```

パラメータ

パラメータはありません。

この設定を行わない場合

SA 確立／解放の情報がログに残されません。

vpnlog とは？

IPsec 機能に関するログです。
SA を確立できなかった場合の原因究明や、改ざん・なりすまし等を検知した場合に、ログを発行します。
コンソールもしくは TELNET でログインして、vpnlog の情報を表示する場合は、show vpnlog コマンドを使用します。

設定モード

基本設定モード

IKE-SA の設定（IKEv2）

authentication

IKE SA の認証方式を設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　IKE SA の認証方式を RSA signatures 方式とする

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#authentication rsa-sig
```

コマンド書式

authentication <認証方式>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
認証方式	IKE SA の認証方式をを指定します。 pre-share：Preshared key 方式 rsa-sig：RSA signatures 方式	pre-share rsa-sig	省略不可

この設定を行わない場合

認証方式は Pre-shared key 方式で動作します。

設定モード

IKEv2 ポリシー設定モード

configuration mode

CP Payload を用いたアドレス払い出し動作を REQUEST/REPLY 制御で動作させる際に設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　CP Payload を用いたアドレス払い出し動作を REQUEST/REPLY 制御で動作させる

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#configuration mode initiate
```

コマンド書式

configuration mode <制御モード>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
制御モード	アドレス払い出し動作を設定します。 initiate：REQUEST/REPLY 制御モードで動作し、自装置から req を送信します。	initiate	省略不可

この設定を行わない場合

CP Payload を用いたアドレス払い出し動作を行いません。

設定モード

IKEv2 ポリシー設定モード

encryption

IKE SA の暗号アルゴリズムを設定します。本装置の暗号アルゴリズムには、DES(56bit DES-CBC)、3DES(168bit DES)、AES があります。
AES で使用する鍵長は、encryption-keysize aes コマンドで設定します。
暗号化アルゴリズムは複数指定することができ、複数指定した場合は Initiator 時に複数の提案を行います。提案の優先度は、AES、3DES、DES の順になります。

また、既に encryption が設定されている状態で新たに encrypiton を設定すると上書きされます。
この設定は、SA を確立する相手と同じ設定である必要があります。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　IKE SA の暗号化アルゴリズムを 3DES 方式とする

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#encryption 3des
```

設定例 2　IKE SA の暗号化アルゴリズムを複数（3DES 方式と AES 方式）設定する

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#encryption 3des aes
```

コマンド書式

encryption <暗号化アルゴリズム>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
暗号化アルゴリズム	IKE SA の暗号化アルゴリズムを指定します。暗号化アルゴリズムを複数設定する際は、半角スペースで区切り入力してください。 des：DES(56bit DES-CBC)方式 3des：3DES(168bit DES)方式 aes：AES 方式	des 3des aes	省略不可

この設定を行わない場合

暗号化アルゴリズムは 3DES で動作します。

設定モード

IKEv2 ポリシー設定モード

encryption-keysize aes

IKE SA のネゴシエーションで使用する AES の鍵長を設定します。
各パラメータの値を<鍵長の下限値> ≦ <優先する鍵長> ≦ <鍵長の上限値>となるように設定してください。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　鍵長の下限値（128）、優先する鍵長（192）、鍵長の上限値（256）とする

```
Router(config)#encryption-keysize aes 128 192 256
```

コマンド書式

encryption-keysize aes <鍵長の下限値> <鍵長の上限値> <優先する鍵長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
鍵長の下限値	鍵長の最小値を設定します。	128 192 256	省略不可
鍵長の上限値	鍵長の最大値を設定します。	128 192 256	省略不可
優先する鍵長	Initiator の時の提案で最優先の鍵長を指定します。	128 192 256	省略不可

この設定を行わない場合

以下の値で動作します。
・鍵長の下限値:128
・鍵長の上限値:256
・優先する鍵長:128

設定モード

IKEv2 ポリシー設定モード

group

Diffie-Hellman グループ番号を設定します。
Diffie-Hellman グループ番号には、1(768-bit)、2(1024-bit)、5(1536-bit)、14(2048-bit)の 4 種類があります。
Diffie-Hellman グループ番号は複数指定することができ、複数指定した場合は Initiator 時に複数の提案を行います。提案の優先度は、group1、group2、group5、group14 の順になります。

また、既に group が設定されている状態で新たに group を設定すると上書きされます。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　IKE SA のネゴシエーション時の Diffie-Hellman グループ番号を 14 とする

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#group 14
```

設定例 2　IKE SA のネゴシエーション時の Diffie-Hellman グループ番号を複数（14、5）設定する

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#group 14 5
```

コマンド書式

group <DH グループ番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DH グループ番号	Diffie-Hellman グループ番号を指定します。Diffie-Hellman グループ番号を複数設定する際は、半角スペースで区切り入力してください。	1 2 5 14	省略不可

この設定を行わない場合

DH グループ番号は、2 で動作します。

設定モード

IKEv2 ポリシー設定モード

hash

IKE SA のハッシュアルゴリズムを設定します。
本装置のハッシュアルゴリズムには、MD5 と SHA-1 と SHA-2 があります。
ハッシュアルゴリズムは複数指定することができ、複数指定した場合は Initiator 時に複数の提案を行います。提案の優先度は SHA-256、SHA-384、SHA-512、SHA-1、MD5 の順になります。

また、既に hash が設定されている状態で新たに hash を設定すると上書きされます。
この設定は、SA を確立する相手と同じ設定である必要があります。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　IKE SA のハッシュアルゴリズムを MD5 にする

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#hash md5
```

設定例 2　IKE SA のハッシュアルゴリズムを複数（MD5、SHA-1）設定する

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#hash md5 sha
```

コマンド書式

hash〈ハッシュアルゴリズム〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ハッシュアルゴリズム	IKE SA のハッシュアルゴリズムを指定します。ハッシュアルゴリズムを複数設定する際は、半角スペースで区切り入力してください。	md5 sha sha-256※ sha-384※ sha-512※	省略不可

※sha-256, sha384, sha-512 は、V01.01(00)以降サポート

この設定を行わない場合

ハッシュアルゴリズムは SHA-1 で動作します。

設定モード

IKEv2 ポリシー設定モード

lifetime

IKE SA の有効期限を設定します。ここで指定した時間が経過した後、CHILD SA が存在する場合に IKE SA の Rekey を開始し、存在しない場合には IKE SA を解放します。
refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　IKE SA の有効期限を 1200 秒にする

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#lifetime 1200
```

コマンド書式

lifetime <有効期限>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
有効期限	IKE SA の有効期限(単位:秒)を指定します。	120～946080000	省略不可

この設定を行わない場合

有効期限は 86400 秒になります。

設定モード

IKEv2 ポリシー設定モード

keepalive

SA の接続確認を行なうために KeepAlive を行なうかどうかを設定します。
本装置では、IKEv2(Internet Key Exchange version 2)プロトコルの KeepAlive 機能、および ICMP による KeepAlive 機能をサポートしています。
本装置では、何も設定をしない場合、IKEv2 の KeepAlive(DPD)を行います。

ICMP による KeepAlive を行う場合は、オプションに"icmp"を指定します。ICMP による KeepAlive を行なう場合は、keepalive-icmp peer-address コマンド、keepalive-icmp source-interface コマンドを指定する必要があるケースもあります。
KeepAlive を行なわない場合は、"disable"を指定します。

KeepAlive により、SA が使用できない状態になった場合は、SA を解放します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　VPN データが送信されていない場合でも常に KeepAlive を送信する

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#keepalive always-send
```

コマンド書式

```
keepalive {always-send|icmp[always-send|traffic-based]|disable}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
always-send	VPN データが送信されなくても、常に KeepAlive を送信します。	always-send	一定期間通信がなかった場合に DPD メッセージを送信します。
icmp	ICMP を利用した KeepAlive を行います。	icmp	一定期間通信がなかった場合に DPD メッセージを送信します。
traffic-based	一定期間 INBOUND SPI による通信が発生せず、OUTBOUND SPI による通信が発生した場合にのみ HELLO を送信します(ICMP-Keepalive のみ対象)。	traffic-based	OUTBOUND で一定期間通信がなかった場合に ICMP メッセージを送信します。
disable	KeepAlive 機能を使用しません。	disable	KeepAlive 機能を使用します。

この設定を行わない場合

IKEv2 の keepalive(DPD)を行います。

設定モード

IKEv2 ポリシー設定モード

keepalive-icmp peer-address

SA が接続されているかどうかの確認を行なうための KeepAlive を ICMP で行なう場合に、KeepAlive の宛先 IP アドレスを設定します。
宛先を VPN ピア、送信元 IP アドレスを送信するインタフェースの IP アドレスとする場合は、このコマンドを設定する必要はありません。
KeepAlive により、SA が使用できない状態になった場合は、SA を解放します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　ICMP の KeepAlive の宛先を、192.168.0.1 にする

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#keepalive-icmp peer-address 192.168.0.1
```

コマンド書式

keepalive-icmp peer-address <宛先 IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先 IP アドレス	ICMP の KeepAlive を行なう相手の IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

keepalive icmp が設定されている場合、宛先 IP アドレスは VPN ピアの IP アドレスになります。

設定モード

IKEv2 ポリシー設定モード

key

Pre-Shared Key*を設定します。
文字列で指定する場合は"ascii"を指定、16 進数で指定する場合は"binary"を指定した後、Pre-Shared Key を設定します。

refresh コマンド後に有効になるコマンドです。

※Pre-Shared Key･･･一般に「事前共有鍵」「共有秘密鍵」とも呼ばれます。

IKEv1/IKEv2 共通コマンド

設定例１　Pre-Shared Key に文字列の"secretF2200"設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#key ascii secretF2200
```

設定例２　Pre-Shared Key に 16 進数の"123456789abcdef"を設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#ke y  binary 123456789abcdef
```

コマンド書式

```
key {ascii|binary} <Pre-shared Ke> [{secret | private}[encrypted]]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ascii | binary	Pre-shared Key を文字列(ascii)として扱うか、16 進数(binary)として扱うかを指定します。	ascii binary	省略不可
Pre-shared Key	Pre-shared Key を設定します。	最大 64 文字の英数字	省略不可
secret | private	Pre-shared Key を暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。※1 secret：暗号化する際に共有暗号鍵を使用する private：暗号化する際に装置固有暗号鍵を使用する	secret private	パスワードを暗号化しません
encrypted	Pre-shared Key を暗号化処理するかどうかを設定します。 このオプションを付加することにより、パスワードは暗号化済みと判定されます。※2 secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。	encrypted	パスワードを暗号化データとして扱いません

※1 このオプションは、設定するとすぐに有効となり、Pre-shared Key が暗号化されて表示され encrypted オプションが自動的に付加されます。
※2 Pre-shared Key が既に暗号化済みの場合は、このオプションを指定する必要があります。

この設定を行わない場合

SA を確立できません。

設定モード

IKE ポリシー設定モード

keepalive-icmp source-interface

SA が接続されているかどうかの確認を行なうための KeepAlive を ICMP で行なう場合に、KeepAlive パケットの送信元インタフェースの IP アドレスを設定します。
宛先を VPN ピア、送信元 IP アドレスを送信するインタフェースの IP アドレスとする場合は、このコマンドを設定する必要はありません。
KeepAlive により、SA が使用できない状態になった場合は、SA を解放します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　ICMP の KeepAlive パケットの送信元アドレスに LAN インタフェースの IP アドレスを使用する

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#keepalive-icmp source-interface lan 1
```

コマンド書式

keepalive-icmp source-interface <インタフェース名 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	ICMP の KeepAlive 送信する際の、送信元アドレスに使用するインタフェースアドレスを指定します。	lan 1 ewan 1～2 loopback 1～100 vlanif 1～150	省略不可

この設定を行わない場合

keepalive icmp が設定されている場合、送信元 IP アドレスは実際にパケットを送信するインタフェースの IP アドレスになります。

設定モード

IKEv2 ポリシー設定モード

self-identity

VPN ピアを識別するために通知する Identity を設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　VPN ピアを識別するために通知する Identity に自装置のアドレス（192.168.1.1）を使用する

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#self-identity address 192.168.1.1
```

コマンド書式

self-identity {address <本装置のアドレス>|fqdn <ホスト名>|user-fqdn <ユーザ名>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
本装置の IP アドレス	本装置の identity を IP アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
ホスト名	本装置の identity を FQDN 形式で指定します。	最大 64 文字の英数字	省略不可
ユーザ名	本装置の Identity を User-FQDN 形式で指定します。	最大 64 文字の英数字	省略不可

この設定を行わない場合

VPN ピアと通信するインタフェースの IP アドレスを利用します。

設定モード

IKEv2 ポリシー設定モード

CHILD SA の設定（IKEv2）

anti-replay

IPsec 通信時の、Replay Attack 防御機能について設定します。本コマンドがない場合は Replay Attack とみなされるパケットを廃棄しますが、disable を設定することによりそれらのパケットも受信されます。

使用する回線によっては、パケットの到着順序が前後するような状態が発生し、Replay Attack と誤認してパケットを廃棄してしまい、スループットの低下が発生することがあります。
show vpnlog コマンドを実行して、ログに Replay Attack が表示されるようであれば、本コマンドで disable を指定する事により、スループットの改善が図れる場合があります。
セキュリティを考慮して Replay Attack 防御が不要であれば、通信状況に応じて disable に設定してください。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　Replay Attack 防御機能を停止して、全てのパケットを受信する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#anti-replay disable
```

コマンド書式

anti-replay < Replay Attack 設定>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Replay Attack 設定	Replay Attack に該当するパケットを破棄するかどうかの設定をします。 enable：Replay Attack に該当するパケットを破棄します。 disable：全てのパケットを受信します。	enable disable	省略不可

この設定を行わない場合

Replay Attack に該当するパケットを破棄します。

Replay Attack 防御機能とは？

Replay Attack 防御機能とは、受信したパケットのシーケンス番号の最大値を保存し、その値と同一もしくはその値より小さなシーケンス番号を受信した場合に、パケットを廃棄する機能です。

ただし、ネットワーク遅延の関係上、ESP フレーム入れ替わりの可能性があるため、受信した Sequence Number の最大値から一定の数（本装置では 32）は受信済・未受信を管理し、その管理の範囲内で未受信の場合は Replay Attack error としての廃棄は行わずに通常の受信処理を行います。

設定モード

VPN セレクタ設定モード

crypto map（基本設定モード）

VPN ピアとのセレクタ情報のエントリを設定する為に、VPN セレクタ設定モードに移行します。
設定の際は、セレクタ名称、シーケンス番号を指定します。

IKEv1/IKEv2 共通コマンド

設定例１　VPN セレクタ設定モード（セレクタ名称：Tokyo）に移行します。

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#
```

コマンド書式

crypto map〈セレクタ名称〉〈シーケンス番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セレクタ名称	VPN セレクタの名称を指定します。 PPPoE インタフェース設定モード/EWAN インタフェース設定モードで、適用する VPN セレクタを指定しますので、わかりやすい名称にしてください。	最大 16 文字の英数字	省略不可
シーケンス番号	シーケンス番号を指定します。 既に使用したシーケンス番号と同じ番号を重複して使用すると以前設定した内容を上書きします。	1～4000	省略不可

最大エントリ：4000 エントリ

設定モード

基本設定モード

crypto map（各インタフェース設定モード）

インタフェースに対応付ける VPN セレクタの MAP 名を定義します。
VPN セレクタは、crypto map コマンドで、VPN セレクタ設定モードに移行して、設定します。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　EWAN1 インタフェースに、MAP 名（Tokyo）の VPN セレクタを対応付けます

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#crypto map mymap
```

コマンド書式

crypto map <セレクタ名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セレクタ名称	crypto map コマンドで指定したセレクタ名称を指定します。	–	省略不可

この設定を行わない場合

このインタフェースでは、VPN（IPsec）を使用しません。

設定モード

EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード

ipsec access-list

IPsec のセレクタ情報を定義します。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例１　全てのパケットを暗号化する

```
Router(config)#ipsec access-list 1 ipsec ip any any
```

設定例２　192.168.100.0/24　→　192.168.200.0/24　宛のパケットを暗号化する

```
Router(config)#ipsec access-list 1 ipsec ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

設定例３　TCP パケットのみ暗号化する

```
Router(config)#ipsec access-list 1 ipsec tcp any any
```

設定例４　全てのパケットを暗号化しない（bypass）

```
Router(config)#ipsec access-list 64 bypass ip any any
```

設定例５　自局発信パケットを暗号化しない（bypass）

bypass で local 指定する場合、下記のように crypto map を設定して、明示的にインタフェースとの紐付けを行う必要があります。
なお、local 指定の場合、1 つの crypto map を複数のインタフェースに紐付けることはできず（ipsec、bypass 指定のどちらも）、インタフェースが異なる場合には、別の ipsec access-list と crypto map にする必要があります。

```
Router(config)#ipsec access-list 61 bypass ip local any
Router(config)#ipsec access-list 62 bypass ip local any
Router(config)#
Router(config)#interface ewan 1
Router(config-if ewan 1)# crypto map bypass-1
Router(config-if ewan 1)# ip address 192.168.1.254 255.255.255.0
Router(config-if ewan 1)#exit
Router(config)#
Router(config)#interface ewan 2
Router(config-if ewan 2)# crypto map bypass-2
```

```
Router(config-if ewan 2)# ip address 192.168.2.254 255.255.255.0
Router(config-if ewan 2)#exit
Router(config)#
Router(config)#crypto map bypass-1 61
Router(config-crypto-map)# match address 61
Router(config-crypto-map)#exit
Router(config)#
Router(config)#crypto map bypass-2 62
Router(config-crypto-map)# match address 62
Router(config-crypto-map)#exit
```

コマンド書式

ipsec access-list 〈ipsec-access-list 番号〉 {ipsec | bypass | discard } 〈プロトコル番号〉 { any | local | host 〈送信元 IP アドレス〉 | 〈送信元 IP アドレス〉〈送信元 Wildcard マスク〉 } [eq 〈TCP ポート番号〉] [eq 〈UDP ポート番号〉] { any | peer | host 〈宛先 IP アドレス〉 | 〈宛先 IP アドレス〉〈宛先 Wildcard マスク〉 } [eq 〈TCP ポート番号〉] [eq 〈UDP ポート番号〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ipsec-access-list 番号	それぞれの属性の番号を指定します。また、この番号は、VPN セレクタの優先度としても使用されます(数字が小さいほど優先度が高い)	1～4000	省略不可
ipsec | bypass | discard	暗号化対象とするか、透過(bypass)対象とするか、廃棄対象とするかを指定します。 ipsec 暗号化対象とする bypass 透過対象とする discard 廃棄対象とする	ipsec bypass discard	省略不可
プロトコル番号	プロトコル名もしくは、プロトコル番号を選択します。 icmp ICMP ip IP tcp TCP udp UDP 0～255 プロトコル番号を指定	icmp ip tcp udp 0～255	省略不可
any	各パラメータ(アドレスやポート番号など)で、「全て」を指定する場合は"any"を入力します。セレクタ情報として相手に通知する場合は、IPaddr=0.0.0.0 Mask=0.0.0.0 で通知します。	any	–
local	自局発信パケットを指定する場合は、"local"を	local	–

	指定します。EWAN でアドレスを固定設定している場合のみ使用可能です。		
host	送信元/宛先アドレスとしてホストアドレスを指定する場合につけます。	host	–
送信元 IP アドレス	送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
送信元 Wildcard マスク	送信元アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
宛先 IP アドレス	宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
宛先 Wildcard マスク	宛先アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
peer	VPN ピア宛を指定する場合は、"peer"を指定します。	peer	
TCP ポート番号	プロトコルで"tcp"を指定した場合に、対象とする TCP ポート番号を指定します。	TCP ポート番号（0～65535）	省略不可
UDP ポート番号	プロトコルで"udp"を指定した場合に、対象とする UDP ポート番号を指定します。	UDP ポート番号（0～65535）	省略不可

この設定を行わない場合

IPsec 機能を使用することはできません。

設定モード

基本設定モード

ipsec transform-keysize

CHILD SA のネゴシエーションで使用する AES の鍵長を指定します。
各パラメータの値を<鍵長の下限値> ≦ <優先する鍵長> ≦ <鍵長の上限値>となるように設定してください。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　鍵長名（v2key）、鍵長の下限値（128）、提案する鍵長（192）、鍵長の上限値（256）とする

```
Router(config)#ipsec transform-keysize v2key esp-aes-cbc 128 256 192
```

コマンド書式

ipsec transform-keysize <鍵長名> esp-aes-cbc <鍵長の下限値> <鍵長の上限値> <Initiator 時に提案する鍵長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
鍵長名	設定する鍵長属性の名称を指定します。	16 文字以内の英数字	省略不可
鍵長の下限値	Responder 時に、受け入れる AES の鍵長の最小値を指定します。これより短い鍵長でのネゴシエーションを受けた場合は、エラーとなります。	128 192 256	省略不可
鍵長の上限値	Responder 時に、受け入れる AES の鍵長の最大値を指定します。これより長い鍵長でのネゴシエーションを受けた場合は、エラーとなります。	128 192 256	省略不可
Initiator 時に提案する鍵長	Initiator 時の提案で最優先の AES 鍵長を指定します。	128 192 256	省略不可

この設定を行わない場合

以下の値で動作します。
・鍵長の下限値:128
・鍵長の上限値:256
・優先する鍵長:128

設定モード

基本設定モード

ipsec transform-set

IPSEC-SA/CHILD SA のポリシーとして、暗号化アルゴリズム、認証アルゴリズムを設定します。
暗号化アルゴリズム、認証アルゴリズムは複数指定することができ、複数指定した場合はネゴシエーション時に複数の提案を行います。
複数の提案をする際の payload 内の暗号化方式は、IKEv1、IKEv2 でそれぞれ以下の様になります。
IKEv1 の場合は設定した順に提案します。
暗号化アルゴリズム、認証アルゴリズムが共に複数設定されている場合は、暗号化アルゴリズムを優先して提案します。
IKEv2 の場合は、暗号化アルゴリズムを AES,3DES,DES,NULL の順に提案し、認証アルゴリズムを sha-256,sha-384,sha-512,sha1,md5 の順に提案します。

CBQ によって帯域制御を行う場合、ipsecif での帯域計算で使用する ICV 長の補正値はデフォルトで 12 バイトとなっています。
しかし、sha256,sha384,sha512 の ICV 長は 12 バイトでないので、必要に応じて qos frame-length-offset で補正値を指定してください。
それぞれのアルゴリズムでの ICV 長は下記の通りです。

- HMAC-MD5: 12 バイト
- HMAC-SHA: 12 バイト
- HMAC-SHA2-256: 16 バイト
- HMAC-SHA2-384: 24 バイト
- HMAC-SHA2-512: 32 バイト

本装置は、複数の Phase2 ポリシーを設定できますので、各 Phase2 ポリシーには、Phase2 ポリシー名称を設定します。
この Phase2 ポリシー名称は、実際にどのセレクタ情報に対して使用するかの指定に使用しますので、わかりやすい名称としてください。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　IKEv1 のポリシー（ポリシー名称：P2-POLICY）として、暗号化方式：AES(256bit)、認証アルゴリズム：HMAC-SHA-1 を登録する

```
Router(config)#ipsec transform-set P2-POLICY esp-aes-256 esp-sha-hmac
```

設定例 2　IKEv2 のポリシー（ポリシー名称：P2V2-POLICY）として、暗号化方式：AES、認証アルゴリズム：HMAC-SHA-1 を登録する

```
Router(config)#ipsec transform-set P2V2-POLICY ikev2 esp-aes esp-sha-hmac
```

コマンド書式

```
ipsec transform-set <ポリシー名> {<IKEv1 暗号化アルゴリズム> [IKEv1 認証アルゴリズム] | ikev2 <IKEv2 暗号化アルゴリズム> [IKEv2 認証アルゴリズム] }
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシー名	ポリシー名として、わかりやすい名称を指定します。	16 文字以内の英数字	省略不可
IKEv1 暗号化アルゴリズム	IPSEC-SA の暗号化アルゴリズムを指定します。 esp-des：DES 方式 esp-3des：3DES 方式 esp-aes-128：AES 128bit esp-aes-192：AES 192bit esp-aes-256：AES 256bit esp-null：暗号化しない	esp-des esp-3des esp-aes-128 esp-aes-192 esp-aes-256 esp-null	省略不可
IKEv1 認証アルゴリズム	IPSEC-SA の認証アルゴリズムを指定します。 esp-md5-hmac：HMAC-MD5 アルゴリズム esp-sha-hmac：HMAC-SHA-1 アルゴリズム esp-sha256-hmac※：HMAC-SHA2-256 アルゴリズム esp-sha384-hmac※：HMAC-SHA2-384 アルゴリズム esp-sha512-hmac※：HMAC-SHA2-512 アルゴリズム	esp-md5-hmac esp-sha-hmac esp-sha256-hmac esp-sha384-hmac esp-sha512-hmac	HMAC-MD5 で動作します。
IKEv2 暗号化アルゴリズム	CHILD SA の暗号化アルゴリズムを指定します。 esp-des：DES 方式 esp-3des：3DES 方式 esp-aes：AES 方式 esp-null：暗号化しない	esp-des esp-3des esp-aes esp-null	省略不可
IKEv2 認証アルゴリズム	CHILD SA の認証アルゴリズムを指定します。 esp-md5-hmac：HMAC-MD5 アルゴリズム esp-sha-hmac：HMAC-SHA-1 アルゴリズム esp-sha256-hmac※：HMAC-SHA2-256 アルゴリズム esp-sha384-hmac※：HMAC-SHA2-384 アルゴリズム esp-sha512-hmac※：HMAC-SHA2-512 アルゴリズム	esp-md5-hmac esp-sha-hmac esp-sha256-hmac esp-sha384-hmac esp-sha512-hmac	HMAC-SHA-1 で動作します。

最大エントリ：64 エントリ
※認証アルゴリズム　sha-256,sha-384,sha-512 は、V01.01(00)以降サポート

この設定を行わない場合

IKEv1 では暗号化アルゴリズム：DES、認証アルゴリズム：HMAC-MD5 で動作します。
IKEv2 では暗号化アルゴリズム：3DES、認証アルゴリズム：HMAC-SHA-1 で動作します。

設定モード

基本設定モード

match address

暗号化するパケットを指定します。
パケットの送信元・宛先アドレスは、ipsec access-list コマンドで指定し、match address コマンドでは、採用する ipsec access-list 番号を指定します。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　192.168.100.0/24 <-> 192.168.200.0/24 を暗号化するパケットとして指定する

```
Router(config)#ipsec access-list 1ipsec ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255

Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#match address 1
```

コマンド書式

match address <IPsec access-list 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPsec access-list 番号	暗号化するパケットとして、ipsec access-list 番号を指定します。	1～4000	省略不可

この設定を行わない場合

IPsec を使用できません。

設定モード

VPN セレクタ設定モード

match identity

VPN ピアの識別方法を設定します。
VPN ピアを識別するために通知される Identity は、IP アドレス形式/FQDN 形式/User-FQDN 形式のいずれかで通知されます。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　VPN ピアの識別を IP アドレス（192.168.1.1）でおこなう

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#match identity address 192.168.1.1
```

コマンド書式

match identity {address <VPN ピアアドレス>|host <ホスト名>|user <ユーザ名>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VPN ピアアドレス	VPN ピアの identity を IP アドレス形式で指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
ホスト名	VPN ピアの identity を FQDN 形式で指定します。	最大 64 文字の英数字	省略不可
ユーザ名	ユーザ名を指定します。	最大 64 文字の英数字	省略不可

この設定を行わない場合

VPN ピアの識別方法を参照しません。

設定モード

IKEv2 ポリシー設定モード

set ikev2-policy

使用する IKEv2 ポリシーの番号を指定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　IKEv2 ポリシー番号 1 を使用する

```
Router(config)#crypto map SELECTOR1
Router(config-crypto-map)#set ikev2-policy 1
```

コマンド書式

set ikev2-policy <policy 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
policy 番号	使用する IKEv2 ポリシーの番号を指定します。	1～2000	省略不可

この設定を行わない場合

この VPN セレクタを使用することができません。

設定モード

VPN セレクタ設定モード

set peer

SA を確立する際の VPN ピアの IP アドレスまたはホスト名を設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例１　VPN ピアを"192.168.1.1"に設定する

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#set peer 192.168.1.1
```

設定例２　VPN ピアを"vpnpeer1"に設定する

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#set peer vpnpeer1
```

コマンド書式

set peer {<VPN ピアの IP アドレス>|<ドメイン名> [v4|v6]}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VPN ピアの IP アドレス｜ドメイン名	VPN ピアを IP アドレスまたは、ドメイン名で指定します。	IPv4、v6 アドレス形式 ドメイン名※	省略不可
v4|v6	VPN ピアにドメイン名を指定した場合は、ドメイン名の名前解決を v4、v6 のどちらかで行うか指定することができます。	v4 v6	両方で名前解決を行います。

※ ドメイン名として設定できる文字は、64 文字までの大文字 (A ～ Z)、小文字 (a ～ z)、数字 (0 ～ 9)、ハイフン (-) 、ドット(.)のみが設定できます。
※ vpn enable となっているインタフェースで、v4 と v6 の両方が有効になっている場合は、v4 と v6 のどちらに名前解決させるか指定する必要があります。

この設定を行わない場合

Initiator として動作しません。

設定モード

IKEv2 ポリシー設定モード

set pfs

PFS (Perfect Forward Security)を行なう際に、Diffie-Hellman 鍵交換を使用した Oakley と呼ばれる暗号化技術を使用します。
このコマンドは Oakley Group を指定します。
Diffie-Hellman Group には、1(768-bit)、2(1024-bit)、5(1536-bit)、14(2048-bit)の 4 種類があります。
IKEv2 で複数の提案をする場合 payload 内では、group14, group5, group2, group1 の順で提案します。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　PFS 使用時の Oakley Group に、Group2 を使用する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set pfs group2
```

コマンド書式

set pfs <DH グループ>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DH グループ	Diffie-Hellman グループ番号を指定します。	group1 group2 group5 group14	省略不可

この設定を行わない場合

IKEv1 では Initiator となる場合、PFS を使用しません。
Responder となる場合は、Initiator からの提案が Group 1、2、5、14 であれば、それを受け入れます。
IKEv2 では PFS を使用しません。

PFS とは？

Quick Mode キーが生成されるたびにキーの再交換を要求する Internet Key Exchange (IKE)の手順です。また、その際にキーの大きさ(Group1、Group2、Group5、Group14)を指定します。
セキュリティの面では強固となりますが、キーの交換に時間がかかる欠点があります。

設定モード

VPN セレクタ設定モード

set session release ipsec-lost-time

CHILD SA がない状態が継続した場合に、IKE SA を解放するまでの時間を設定します。
設定変更後に確立された CHILD SA から有効になります。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　CHILD SA がない状態が継続した場合に、IKE SA を解放するまでの時間を 30 秒にする

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#set session release ipsec-lost-time 30
```

コマンド書式

set session release ipsec-lost-time <継続時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
継続時間	CHILD SA がない状態が継続した場合に、IKE SA を解放するまでの時間(単位:秒)を指定します。	1～600	省略不可

この設定を行わない場合

IKE SA のライフタイムに従って、SA を解放します。

設定モード

IKEv2 ポリシー設定モード

set security-association always-up

SA の確立状態を維持するかどうかを指定します。
このコマンドを設定した場合、一度確立した SA は確立し続けます。万一、SA が切断した場合は確立するまでリトライし続けます。
always-up の監視間隔は、always-up check-interval コマンドで指定することができます。

IPsec の Aggressive モードで運用する場合に、Initiator 側に設定しておくと効果的です。
センタ側 FITELnet-F シリーズ(固定 IP)-----拠点側 FITELnet-F シリーズ(動的 IP)
上記の環境では通常センタ側契機の VPN は張れないため、ライフタイム等で SA の消失後はセンタ側から通信が行えません。
このコマンドを使用することで拠点側より常時 SA が確立されるため、センタ側からの通信が不能になることはありません。

本設定または、if-state sync-sa のどちらか一方の設定が有効であれば、UP/DOWN 動作します。
また、両方の設定がない場合は常に IPsec インタフェースは UP の状態となります。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　SA を常時接続とする

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association always-up
```

コマンド書式

```
set security-association always-up
```

パラメータ

パラメータはありません。

この設定を行わない場合

確立した SA は、Lifetime の設定に従い解放します。

設定モード

VPN セレクタ設定モード

set security-association lifetime

IPSEC-SA/CHILD SA の生存時間を設定します。
IPSEC-SA の生存時間は、以下の 2 種類のパラメータで指定することができます。
CHILD SA は時間のパラメータのみ設定可能です。

IPsec では、生存時間の満了時に SA を解放します。
これは、同じ SA を使いつづけると暗号化の鍵を見破られる可能性が高くなり、安全な通信ができなくなるための対策としての機能です。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　Phase2 SA の生存時間を 3600 秒に設定する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association lifetime seconds 3600
```

設定例 2　Phase2 SA の生存中継データ量を 1000byte に設定する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association lifetime kilobytes 1000
```

コマンド書式

set security-association lifetime { seconds <生存時間> | kilobytes <生存中継データ量> }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
生存時間	IPSEC-SA/CHILD SA の生存時間を時間(単位:秒)で指定します。 ここで指定した時間経過後、IPSEC-SA/CHILD SA を解放します。	60～4294967295	省略不可
生存中継データ量	SA 上で通信するデータ量(単位:キロバイト数)を指定します。 ここで指定したデータ量を通信した後、IPSEC-SA/CHILD SA を解放します。	1000～4294967295	省略不可

※ 時間とデータの両方を指定した場合は、時間が経過したもしくは指定したデータ量の通信が行なわれた場合(先に満了したタイミングで)に、IPSEC-SA を解放します。
※ IKEv2 CHILD SA の生存時間に 946080000 秒(30 年)より大きな値が設定された場合は、946080000 秒として動作します。

この設定を行わない場合

生存時間は、600 秒です。
バイト数での生存時間は存在しません。

VPN ピアと設定が異なる場合

SA を確立しようとしている VPN ピアと、生存時間の設定が異なる場合は、次のようになります。

initiator の場合	自装置の設定値を採用します。	
responder の場合	IKEv1	自装置の設定値と相手からの提案された値を比較して、小さい方を採用します。
	IKEv2	自装置の設定値を採用

設定モード

VPN セレクタ設定モード

set security-association selector bypass

IPSEC-SA/CHILD SA のセレクタ検索を行わずに中継する場合に設定します。
mcast オプションを指定することにより、マルチキャストパケットのみセレクタ検索を行わずに中継します。
ルートベース(ipsecif)を使用した IPsec でのみ有効、ポリシーベースでは無視します。

IPsec 機能を使用してマルチキャストルーティングを行う場合に設定してください。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　マルチキャストパケットのみセレクタ検索を行わずに中継する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association selector bypass mcast
```

コマンド書式

```
set security-association selector bypass [mcast]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
mcast	マルチキャストパケットのみセレクタ検索を行わずに中継する場合に指定します。	mcast	全てのパケットでセレクタ検索を行わずに中継します。

この設定を行わない場合

セレクタにマッチしないパケットは破棄されます。

設定モード

VPN セレクタ設定モード

set transform-keysize

ipsec transform-keysize コマンドで設定する鍵長属性を対応付けます。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　鍵長名（v2key）、鍵長の下限値（128）、提案する鍵長（192）、鍵長の上限値（256）とする

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set transform-keysize v2key
```

コマンド書式

set transform-keysize <鍵長名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
鍵長名	このセレクタで使用する暗号アルゴリズムの鍵長属性を指定するために、鍵長名を指定します。	16 文字以内の英数字	省略不可

この設定を行わない場合

AES の場合以下の値で動作します。
・鍵長の下限値:128
・鍵長の上限値:256
・優先する鍵長:128

設定モード

VPN セレクタ設定モード

set transform-set

ipsec transform-set コマンドで設定する IPSEC-SA/CHILD SA の暗号化ポリシーを対応付けます。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　このセレクタにおいては、ipsec transform-set で指定した"policy1"のポリシーを使用する

```
Router(config)#ipsec transform-set policy1 esp-des esp-md5-hmac

Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set transform-set policy1
```

コマンド書式

set transform-set <ポリシー名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシー名称	ipsec transform-set で設定したポリシー名称を指定します。	16 文字以内の英数字	省略不可

この設定を行わない場合

IKEv1 では暗号化アルゴリズム:DES、認証アルゴリズム:HMAC-MD5 で動作します。
IKEv2 では暗号化アルゴリズム:3DES、認証アルゴリズム:HMAC-SHA-1 で動作します。

設定モード

VPN セレクタ設定モード

拡張認証の設定（IKEv2）

client authentication password

拡張認証のクライアントとして動作する際のパスワードを設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例１　拡張認証のクライアントとして動作する際のパスワードを"F2200-pass"とする

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#client authentication password F2200-pass
```

コマンド書式

client authentication password <パスワード>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
パスワード	接続相手から拡張認証される際のパスワードを設定します。	最大 128 文字の英数字	省略不可

この設定を行わない場合

拡張認証のクライアントとして動作しません。

設定モード

IKEv2 ポリシー設定モード

client authentication peer-password

相手を拡張認証する場合の、相手のパスワードを設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　拡張認証で使用する相手のパスワードを"VPN-Peer1-pass"とする

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)# client authentication peer-password VPN-Peer1-pass
```

コマンド書式

client authentication peer-password <パスワード>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
パスワード	接続相手を拡張認証する際の相手のパスワードを設定します。	最大 128 文字の英数字	省略不可

この設定を行わない場合

相手を拡張認証することはできません。

設定モード

IKEv2 ポリシー設定モード

電子証明書に関する設定（IKEv2）

crl-optional

証明書の有効性を CRL で確認するかしないかを設定します。

IKEv1/IKEv2 共通コマンド

設定例１　証明書の有効性を必ず CRL で確認する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#crl-optional must
```

コマンド書式

crl-optional <CRL 設定>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
CRL 設定	この証明書に関して、CRL を使用するかどうかを指定します。 must：証明書の有効性を必ず CRL で確認します。CRL が取得できない場合は、無効と判断されます。 notuse：証明書の有効性を CRL で確認しません。	must notuse	省略不可

この設定を行わない場合

CRL を取得（20 秒以内）できれば証明書の有効性を確認しますが、取得できなければ確認を行いません。

設定モード

電子証明書（自身の ID）設定モード

email

証明書リクエストファイルに含める電子メールアドレスを設定します。電子メールアドレスの情報を含めない場合は、設定の必要はありません。

IKEv1/IKEv2 共通コマンド

設定例１　証明書リクエストファイルに含める電子メールアドレスとして、F2200@xxxxx.ne.jp を設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#email F2200@xxxxx.ne.jp
```

コマンド書式

email〈電子メールアドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
電子メールアドレス	証明書リクエストファイルに含める電子メールアドレスを設定します。	最大 64 文字	省略不可

この設定を行わない場合

証明書リクエストファイルに、E-Mail アドレスを含めることはできません。

設定モード

電子証明書（自身の ID）設定モード

ip address

証明書リクエストファイルに含める IP アドレスを設定します。IP アドレスの情報を含めない場合は、設定の必要はありません。

IKEv1/IKEv2 共通コマンド

設定例 1　証明書リクエストファイルに含める IP アドレスとして、192.168.1.1 を設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#ip address 192.168.1.1
```

コマンド書式

ip address <IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	証明書リクエストファイルに含める IP アドレス	IPv4 アドレス形式	省略不可

この設定を行わない場合

証明書リクエストファイルに、IP アドレスを含めることはできません。

設定モード

電子証明書(自身の ID)設定モード

ip domain-name

証明書リクエストファイルに含めるドメイン名称を設定します。ドメイン名称の情報を含めない場合は、設定の必要はありません。

IKEv1/IKEv2 共通コマンド

設定例１　証明書リクエストファイルに含めるドメイン名称として、xxxxx.ne.jp を設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#ip domain-name xxxxx.ne.jp
```

コマンド書式

ip domain-name <ドメイン名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ドメイン名	証明書リクエストファイルに含めるドメイン名称	最大 64 文字	省略不可

この設定を行わない場合

証明書リクエストファイルに、ドメイン名を含めることはできません。

設定モード

電子証明書（自身の ID）設定モード

ipv6 address

証明書リクエストファイルに含める IPv6 アドレスを設定します。
IPv6 アドレスの情報を含めない場合は、設定の必要はありません。

IKEv1/IKEv2 共通コマンド

設定例 1　証明書リクエストファイルに含める IPv6 アドレスとして、3ffe:200::1 を設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#ipv6 address 3ffe:200::1
```

コマンド書式

ipv6 address <IPv6 アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPv6 アドレス	証明書リクエストファイルに含める IPv6 アドレス	IPv6 アドレス形式	省略不可

この設定を行わない場合

証明書リクエストファイルに、IPv6 アドレスを含めることはできません。

設定モード

電子証明書(自身の ID)設定モード

IPsec のログ情報に関する設定（IKEv2）

nolog-block-type-discard

vpnlog の"block type discard ～"を抑制する設定を行います。
受信したパケットを暗号化するかどうか判断するためにセレクタ検索をする際に、下記のような場合に上記ログが記載されます。
1）マッチした ipsec access-list が discard だった場合。
2）設定された ipsec access-list にマッチしなかった場合。
このコマンドで該当するログを抑制することにより、他のログを参照しやすくすることができます。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例１　block type discard の vpnlog を制御する設定をします

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#nolog-block-type-discard
```

コマンド書式

nolog-block-type-discard

パラメータ

パラメータはありません

設定モード

IPsec ログモード

nolog-spi-no-match

"SPI no match ～"の vpnlog を抑制する設定を行います。
受信した ESP パケットが自装置宛にもかかわらず、パケットに格納されている SA が自装置管理下にある SA にマッチしなかった場合に出力されるログを抑制します。
このコマンドで該当するログを抑制することにより、他のログを参照しやすくすることができます。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例１　"SPI no match ～"の vpnlog を抑制する設定を行う

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#nolog-spi-no-match
```

コマンド書式

nolog-spi-no-match

パラメータ

パラメータはありません

設定モード

IPsec ログモード

IPsec の各種設定（IKEv2）

alive

ICMP-KeepAlive 機能を使用する場合のタイマ値/送信回数等を設定します。

IKEv1/IKEv2 共通コマンド

設定例１　１回の KeepAlive で４つの ICMP を送信する、そのうち３つの応答を受け取れなかった場合に SA の障害とみなす

```
Router(config)#crypto security-association
Router(config-crypto-sa)#alive count 4 3
```

設定例２　１回の KeepAlive で４つの ICMP を送信し、そのうち３つ以上応答が無い状態が３回以上続いた場合に SA の障害とみなす

```
Router(config)#crypto security-association
Router(config-crypto-sa)#alive count 4 3 fail 3
```

設定例３　ICMP の KeepAlive のタイムアウト時間を３秒とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#alive timeout 3
```

設定例４　ICMP の KeepAlive を 60 秒間隔で送信する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#alive freq 60
```

コマンド書式

```
alive count <ICMP 送信数> <ICMP 失敗数> [fail <ICMP リトライ回数>]
alive freq <送信間隔> [degraded-freq <送信間隔>]
alive timeout <timeout 時間>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ICMP 送信数	1 回の KeepAlive で送信する ICMP の数を設定します。	1～15	省略不可
ICMP 失敗数	1 回の KeepAlive で送信した ICMP 数のうち、何個応答を受け取れなかった時に監視失敗と判定するかを設定します。	1～15	省略不可
ICMP 連続失敗回数	何回連続して ICMP 監視に失敗したら SA の障害と判定するかを設定します。	1～10	1
送信間隔	正常時の ICMP KeepAlive の送信間隔(秒)を設定します。	5～1000	省略不可
degraded-freq <送信間隔>	リトライ時の ICMP KeepAlive の送信間隔(秒)を設定します。	5～1000	60
timeout 時間	ICMP KeepAlive の応答待ち時間(秒)	3～60	省略不可

この設定を行わない場合

ICMP 送信数	4 回
ICMP 失敗数	3 回
ICMP 連続失敗回数	1 回
送信間隔	60 秒
degraded-freq 送信間隔	60 秒
timeout 時間	3 秒

設定モード

IPsec 各種設定モード

always-up check-interval

SA の確立状態を維持する場合の、always-up の監視間隔を指定します。
本コマンドは、set security-association always-up コマンドで、SA の確立状態を維持する設定にした場合のみ有効です。

IKEv1/IKEv2 共通コマンド

設定例 1　always-up の監視間隔を 10 秒とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)# always-up check-interval 10
```

コマンド書式

always-up check-interval <監視間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
監視間隔	always-up の監視間隔(秒単位)を設定します。	1～20	省略不可

この設定を行わない場合

always-up の監視間隔は 20 秒となります。

設定モード

IPsec 各種設定モード

crypto security-association

IPsec 機能全般の、各種タイマ値等を設定するために、IPsec 各種設定モードに移行します。

IKEv1/IKEv2 共通コマンド

設定例１　IPsec 各種設定モードに移行します。

```
Router(config)#crypto security-association
Router(config-crypto-sa)#
```

コマンド書式

```
crypto security-association
```

パラメータ

パラメータはありません。

設定モード

基本設定モード

if-state sync-sa

IPsec インタフェースの UP/DOWN を SA 有無に連携する場合に設定します。
本設定または、crypto map の set security-association always-up のどちらか一方の設定が有効であれば、UP/DOWN 動作します。
また、両方の設定がない場合は常に IPsec インタフェースは UP の状態となります。

refresh コマンド後に有効になるコマンドです。

IKEv1/IKEv2 共通コマンド

設定例 1　IPsec インタフェースの UP/DOWN 制御を SA 有無に連携させる

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#if-state sync-sa
```

コマンド書式

```
if-state sync-sa
```

パラメータ

パラメータはありません

この設定を行わない場合

IPsec インタフェースは、常に UP となります。

設定モード

IPsec インタフェース設定モード

ikealive freq

IKE KeepAlive 機能として使用する DPD（Dead Peer Detection）のパラメータを設定します。

IKEv1/IKEv2 共通コマンド

設定例 1　DDP メッセージの送信間隔を 30 秒に設定する

```
Router(config)#crypto security-association
Router(config-crypto-sa)# ikealive freq 30
```

コマンド書式

ikealive freq <送信間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	IDPD メッセージの送信間隔(単位：秒)を設定します。	10～3600 秒	省略不可

この設定を行わない場合

送信間隔は 60 秒です。

設定モード

IPsec 各種設定モード

negotiation

本装置では、IPSEC-SA/CHILD の SA のライフタイムが満了する前に、新しい SA を確立するために IKE-SA/CREATE CHILD SA のネゴシエーションを開始します。
本コマンドでは、ライフタイムが満了する何秒前に新しい SA のためのネゴシエーションを開始するかを設定します。
この値は、本装置自身が Initiator の場合と Responder の場合で、設定値を変更することができます。

IKEv1/IKEv2 共通コマンド

設定例１　本装置が Initiator の場合は、ライフタイム満了の 90 秒前にネゴシエーションを開始する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#negotiation initiate 90
```

設定例２　本装置が Responder の場合は、ライフタイム満了の 30 秒前にネゴシエーションを開始する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#negotiation respond 30
```

コマンド書式

negotiation <initiate| respond> <作動時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
initiate| respond	この設定を、Initiator の SA に適用するか、Responder の SA に適用するかを選択します。	initiate respond	省略不可
作動時間	Rekey の際、Lifetime 満了時間からどれくらい前(単位:秒)に、新しい SA を確立するかを設定します。	1～65535※	省略不可

※　設定範囲の最大値の 65535 は、V01.06 (00)以降サポート

この設定を行わない場合

initiator は 90 秒前、responder は 30 秒前に rekey を開始します。

設定モード

IPsec 各種設定モード

negotiation expire-time

ISAKMP ネゴシエーションのエクスパイア時間についての設定を行います。
IKEv2 の responder 側でのみ有効となり、IKE_SA_INIT から IKE_AUTH 完了までの request パケットを受信(再送を除く)してからのネゴシエーションタイムアウト時間を指定します。

IKEv2 専用コマンド

設定例 1　ISAKMP ネゴシエーションのエクスパイア時間を 180 秒にする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#negotiation expire-time 180
```

コマンド書式

negotiation expire-time <エクスパイア時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エクスパイア時間	ISAKMP ネゴシエーションのエクスパイア時間(単位:秒)を指定します。	30～600	省略不可

この設定を行わない場合

60 秒で動作します。

設定モード

IPsec 各種設定モード

retry

ISAKMP による自動鍵交換の再送間隔(パラメータ:timer)と、最大再送回数(パラメータ:max)を設定します。

IKEv1/IKEv2 共通コマンド

設定例 1　ISAKMP による自動鍵交換の再送間隔を 20 秒とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry timer 20
```

設定例 2　ISAKMP による自動鍵交換の最大再送回数を 1 回とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry max 1
```

コマンド書式

```
retry timer <再送間隔>
retry max <最大送信回数>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	ISAKMP による自動鍵交換の再送間隔(単位:秒)を設定します。 再送を行う毎に間隔は 2 倍に増加していきます。	1～30	省略不可
最大送信回数	ISAKMP による自動鍵交換の最大再送回数を設定します。	1～5	省略不可

この設定を行わない場合

送信間隔	20 秒
最大送信回数	1 回

設定モード

IPsec 各種設定モード

retry guard-time

IKE ネゴパケットの送受信において、自身が送信してから対向の再送パケットを受け入れ可能とするまでの時間を設定します。

IKEv1/IKEv2 共通コマンド

設定例 1　対向の再送パケットの受け入れ可能時間を 5 秒に設定する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry guard-time 5
```

コマンド書式

retry guard-time<受信可能時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
受信可能時間	IKE ネゴパケットの送受信において、自身が送信してから対向の再送パケットを受け入れ可能とするまでの時間(単位:秒)を設定します。	1～30	省略不可

この設定を行わない場合

受信可能時間を 1 秒に設定します。

設定モード

IPsec 各種設定モード

グループ鍵 IPsec 機能の設定

crypto group-security map

マルチポイント SA クライアントにおいて、マルチポイント SA を受信する VPN ピアに対応する VPN セレクタ名を設定します。

IKEv2 専用コマンド

設定例 1　マルチポイント SA を受信する VPN ピアにタイするセレクタ名称を MPSA1 とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#crypto group-security map MPSA1
```

コマンド書式

crypto group-security map <セレクタ名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セレクタ名称	マルチポイント SA を受信する VPN ピアに対応する VPN セレクタ名称を指定します。	最大 16 文字の英数字	省略不可

この設定を行わない場合

マルチポイント SA は適用されません。

設定モード

IPsec インタフェース設定モード

group-security client

マルチポイント SA クライアントにおいて、VPN ピアとなるマルチポイント SA サーバから
マルチポイント SA を受信する場合に設定します。

SPI-AND マスクは 1 を指定したビットを 16 個以上、SPI-OR マスクは 1 を指定したビットが
SPI-AND マスクでは 0 となるように設定してください。

正しく設定していない場合、参照する crypto map が無効となりますのでご注意ください。
本設定はマルチポイント SA サーバ側で設定する spi mask と同じ設定にしてください。

IKEv2 専用コマンド

設定例 1　マルチポイント SA サーバからマルチポイント SA を受信する

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#group-security client
```

コマンド書式

group-security client [spi mask hex <SPI-AND マスク> <SPI-OR マスク>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
SPI-AND マスク	マルチポイント SA の SPI 値の範囲を、乱数となるビットを1、SPI-OR マスクで指定されるビットを0として、HEX で指定します。	最大 8 桁の 16 進数	IPsec SA の SPI 値の範囲が任意となります。
SPI-OR マスク	マルチポイント SA の SPI 値の範囲を、SPI-OR マスクで0指定されたビットに格納される値を指定します。このマルチポイント SA の SPI 値の範囲以外の値で、通常の IPsec SA の SPI 値を生成します。	最大 8 桁の 16 進数	IPsec SA の SPI 値の範囲が任意となります。

この設定を行わない場合

マルチポイント SA を受信しません。

設定モード

IKEv2 ポリシー設定モード

group-security server

マルチポイント SA サーバにおいて、VPN ピアとなるマルチポイント SA クライアントに配布するポリシー名称を設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　マルチポイント SA クライアントに配布するポリシー名称を MPSA1 とする

```
Router(config)#crypto ikev2 policy 1
Router(config-ikev2)#group-security server MPSA1
```

コマンド書式

group-security server 〈ポリシー名称〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシー名称	VPN ピアとなるマルチポイント SA クライアントに配布するポリシー名称を設定します。	最大 64 文字の英数字	省略不可

この設定を行わない場合

マルチポイント SA は配布されません。

設定モード

IKEv2 ポリシー設定モード

ipsec group-security server ha ack-msg-timeout

マルチポイント SA サーバ冗長の ack メッセージの応答タイムアウト時間を設定します。
この時間以上マルチポイント SA サーバ冗長の ack メッセージによる応答を受信しなかった場合、対向サーバとの TCP 接続を切断します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　マルチポイント SA サーバ冗長の ack メッセージの応答タイムアウト時間を 120 秒とする

```
Router(config)#ipsec group-security server ha ack-msg-timeout 120
```

コマンド書式

ipsec group-security server ha ack-msg-timeout <タイムアウト時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タイムアウト時間	マルチポイント SA サーバ冗長の ack メッセージの応答タイムアウト時間(単位:秒)を指定します。	1～3600	省略不可

この設定を行わない場合

タイムアウト時間は 30 秒で動作します。

設定モード

基本設定モード

ipsec group-security server ha init-timeout

マルチポイント SA のサーバ状態において、Init 状態から抜け出すタイムアウト時間を設定します。
この時間以上マルチポイント SA のサーバ状態が Init 状態に留まった場合、強制的に Backup-synced 状態へ遷移します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　Init 状態から抜け出すタイムアウト時間を 120 秒とする

```
Router(config)#ipsec group-security server ha init-timeout 120
```

コマンド書式

ipsec group-security server ha init-timeout <タイムアウト時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タイムアウト時間	マルチポイント SA サーバ冗長の Init 状態から抜け出すタイムアウト時間(単位:秒)を指定します。	1～3600	省略不可

この設定を行わない場合

強制的に Init 状態から抜け出すことはありません。

設定モード

基本設定モード

ipsec group-security server ha keepalive-interval

マルチポイント SA サーバ冗長の Keepalive メッセージの送信間隔を設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　マルチポイント SA サーバ冗長の Keepalive メッセージの送信間隔を 120 秒とする

```
Router(config)#ipsec group-security server ha keepalive-interval 120
```

コマンド書式

ipsec group-security server ha keepalive-interval 〈送信間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	マルチポイント SA サーバ冗長の Keepalive メッセージの送信間隔(単位:秒)を指定します。	1～3600	省略不可

この設定を行わない場合

送信間隔は 30 秒で動作します。

設定モード

基本設定モード

ipsec group-security server ha keepalive-timeout

マルチポイント SA サーバ冗長の Keepalive メッセージのタイムアウト時間を設定します。
この時間以上マルチポイント SA サーバ冗長の Keepalive メッセージを受信しなかった場合、対向サーバとの TCP 接続を切断します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　マルチポイント SA サーバ冗長の Keepalive メッセージの送信間隔を 120 秒とする

```
Router(config)#ipsec group-security server ha keepalive-timeout 120
```

コマンド書式

ipsec group-security server ha keepalive-timeout <タイムアウト時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タイムアウト時間	マルチポイント SA サーバ冗長の Keepalive メッセージのタイムアウト時間(単位:秒)を指定します。	1～3600	省略不可

この設定を行わない場合

タイムアウト時間は 90 秒で動作します。

設定モード

基本設定モード

ipsec group-security server ha local-address

マルチポイント SA サーバの冗長機能を有効にする場合に設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　マルチポイント SA サーバ冗長を行う際のローカルアドレス（192.168.10.1）とリモートアドレス（192.168.100.1）を設定する

```
Router(config)#ipsec group-security server ha local-address 192.168.10.1 remote-address
192.168.100.1
```

コマンド書式

ipsec group-security server ha local-address〈ローカルアドレス〉remote-address〈リモートアドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ローカルアドレス	マルチポイント SA サーバ冗長を行う際のローカル IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
リモートアドレス	マルチポイント SA サーバ冗長を行う際のリモート IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

マルチポイント SA サーバにおける冗長機能は無効になります。

設定モード

基本設定モード

ipsec group-security server ha next-key-sync

マルチポイント SA サーバの冗長機能において、サーバ間で同時に 2 つのマルチポイント SA の同期を行います。
マルチポイント SA のサーバ間で通信ができなくなった場合に 1 回リキーが発生しても次に使用するマルチポイント SA も同期することで SA の不一致を防ぐことが可能です。
さらにリキーが発生すると SA の不一致が発生しますのでご注意ください。

IKEv2 専用コマンド
V01.03(00)以降サポート

設定例 1　サーバ間で同時に 2 つのマルチポイント SA の同期を行う

```
Router(config)#ipsec group-security server ha next-key-sync
```

コマンド書式

```
ipsec group-security server ha next-key-sync
```

パラメータ

パラメータはありません。

この設定を行わない場合

マルチポイント SA のサーバ間では 1 つのマルチポイント SA の同期を行います。

設定モード

基本設定モード

ipsec group-security server ha rekey-delay-time

マルチポイント SA サーバ冗長 ReKey タイミングの遅延時間を設定します。
マルチポイント SA サーバ冗長の soft lifetime 満了からこの時間だけ経過した後、ReKey を行います。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　マルチポイント SA サーバ冗長の ReKey タイミングの遅延時間を 120 秒とする

```
Router(config)#ipsec group-security server ha rekey-delay-time 120
```

コマンド書式

ipsec group-security server ha rekey-delay-time <Re-Key 遅延時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ReKey 遅延時間	マルチポイント SA サーバ冗長の ReKey タイミングの遅延時間(単位:秒)を指定します。	0～3600	省略不可

この設定を行わない場合

遅延時間は 0 秒で動作します。

設定モード

基本設定モード

ipsec group-security server ha request-msg-timeout

マルチポイント SA サーバ冗長の要求メッセージ応答タイムアウト時間を設定します。
この時間以上マルチポイント SA サーバ冗長の要求メッセージに対する応答がなかった場合、対向サーバとの TCP 接続を切断します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　マルチポイント SA サーバ冗長の要求メッセージ応答タイムアウト時間を 120 秒とする

```
Router(config)#ipsec group-security server ha request-msg-timeout 120
```

コマンド書式

ipsec group-security server ha request-msg-timeout <タイムアウト時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タイムアウト時間	マルチポイント SA サーバ冗長の要求メッセージの応答タイムアウト時間(単位:秒)を指定します。	1～3600	省略不可

この設定を行わない場合

タイムアウト時間は 30 秒で動作します。

設定モード

基本設定モード

ipsec group-security server ha send-timeout

マルチポイント SA サーバ冗長機能のサーバ間メッセージ送信タイムアウト時間を設定します。
この時間以上サーバ間メッセージが送信できなかった場合、対向マルチポイント SA サーバとの TCP 接続を切断しますす。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　マルチポイント SA サーバ冗長機能のサーバ間メッセージ送信タイムアウト時間を 120 秒とする

```
Router(config)#ipsec group-security server ha send-timeout 120
```

コマンド書式

ipsec group-security server ha send-timeout <タイムアウト時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タイムアウト時間	マルチポイント SA サーバ冗長機能のサーバ間メッセージ送信タイムアウト時間(単位:秒)を指定します。	1～3600	省略不可

この設定を行わない場合

タイムアウト時間は 30 秒で動作します。

設定モード

基本設定モード

ipsec group-security server priority

マルチポイント SA サーバの冗長機能で使用するサーバ優先度を設定します。
冗長するサーバ間で異なる値になるよう設定してください。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　マルチポイント SA サーバの優先度 255 とする

```
Router(config)#ipsec group-security server priority 255
```

コマンド書式

ipsec group-security server priority <優先度>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
優先度	マルチポイント SA サーバの優先度を設定します。 大きい数字ほど優先度は高くなります。	1～255	省略不可

この設定を行わない場合

マルチポイント SA サーバ優先度は 100 で動作します。

設定モード

基本設定モード

ipsec group-security vendor-id

マルチポイント SA を使用する際の IKE_SA_INIT に含める Vendor ID ペイロードの中の文字列を設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　F2200 MPSA をベンダーID として使用する

```
Router(config)#ipsec group-security vendor-id F2200 MPSA
```

コマンド書式

ipsec group-security vendor-id <ベンダーID>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ベンダーID	IKE_SA_INIT に含める Vendor ID ペイロードの中の文字列指定します。	最大 20 文字以内の英数字	省略不可

この設定を行わない場合

FITELnet GSA をベンダーID として使用します。

設定モード

基本設定モード

lifetime

マルチポイント SA のライフタイムを設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　マルチポイント SA のライフタイムを ReKey 開始時間（1200 秒）、マルチポイント SA 削除時間(60 秒)とする

```
Router(config)#crypto ipsec group-security policy MPSA1
Router(config-gr-sec)#lifetime 1200 60
```

コマンド書式

lifetime <ReKey 開始時間> <マルチポイント SA 削除時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ReKey 開始時間	マルチポイント SA 情報配布後、次回の ReKey を開始する時間(単位:秒)を設定します。	60～946079940	省略不可
マルチポイント SA 削除時間	クライアントがマルチポイント SA を削除する時間(単位:秒)を、ReKey 開始予定時間からの差で指定します。クライアントはマルチポイント SA 情報を受信してから、<ReKey 開始時間>+<マルチポイント SA 削除時間>秒後に削除をおこいます。	60～946079940	省略不可

この設定を行わない場合

クライアントは、マルチポイント SA 情報を受信してから 3600 秒後に削除をおこないます。
ReKey 開始時間：3300 秒
マルチポイント SA 削除時間：300 秒

設定での注意事項

マルチポイント SA サーバの冗長機能を有効にする場合、マルチポイント SA サーバ冗長 Keepalive メッセージの送信間隔※1 と、マルチポイント SA サーバ冗長 Keepalive メッセージのタイムアウト時間※2 の合計時間よりも長い時間をマルチポイント SA 削除時間として設定したください。
合計時間よりもマルチポイント SA 削除時間を短く設定してしまうと、冗長の Master がダウンした際の切り替えが発生する前にマルチポイント SA が ReKey されず、ライフタイム満了時に一時的に通信ができなくなることがあります。

※1 ipsec group-security server ha keepalive-interval コマンドを参照してください。
※2 ipsec group-security server ha keepalive-timeout コマンドを参照してください。

下記の 2 つの設定が、ReKey 開始時間 ＞（新 Outbound マルチポイント SA 登録時間 + 旧 Inbound マルチポイント SA 削除時間）
となるように設定してください。

lifetime <ReKey 開始時間> <マルチポイント SA 削除時間>
rollover <新 Outbound マルチポイント SA 登録時間> <旧 Inbound マルチポイント SA 削除時間>

設定モード

グループ鍵 IPsec 設定モード

reverse-path-check enable

uRPF 機能を有効にします。
MPSA を使用しているインタフェースのみ有効となります。
指定したインタフェースにてパケットを受信した際に、以下の確認を行い不正であると判断した場合にパケットを破棄します。

・受信したパケットの送信元 Inner IP アドレス(復号化後)の宛先が経路表に存在すること
・経路のネクストホップアドレスと送信元 Outer IP アドレス(ESP パケット)のアドレスが一致すること

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド
V01.03(00)以降サポート

設定例 1　uRPF 機能を有効にする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)# reverse-path-check enable
```

コマンド書式

reverse-path-check enable

パラメータ

パラメータはありません。

この設定を行わない場合

uRPF 機能は無効となります。

設定モード

IPsec インタフェース設定モード

rollover

マルチポイント SA の更新遅延時間を設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　新 Outbound マルチポイント SA 登録時間（180 秒）、旧 Inbound マルチポイント SA 削除時間(180 秒)とする

```
Router(config)#crypto ipsec group-security policy MPSA1
Router(config-gr-sec)#rollover 180 180
```

コマンド書式

rollover <新 Outbound マルチポイント SA 登録時間> <旧 Inbound マルチポイント SA 削除時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
新 Outbound マルチポイント SA 登録時間	ReKey 後、新 Outbound マルチポイント SA 登録されるまでの時間(単位:秒)を指定します。	5～946080000	省略不可
旧 Inbound マルチポイント SA 削除時間	新 Outbound マルチポイント SA 登録後、旧 Inbound マルチポイント SA が削除されるまでの時間(単位:秒)を指定します。	5～946080000	省略不可

この設定を行わない場合

新 Outbound マルチポイント SA 登録時間:60 秒
旧 Inbound マルチポイント SA 削除時間:60 秒

設定での注意事項

下記の 2 つの設定が、ReKey 開始時間 ＞(新 Outbound マルチポイント SA 登録時間 + 旧 Inbound マルチポイント SA 削除時間)
となるように設定してください。

lifetime <ReKey 開始時間> <マルチポイント SA 削除時間>
rollover <新 Outbound マルチポイント SA 登録時間> <旧 Inbound マルチポイント SA 削除時間>

設定モード

グループ鍵 IPsec 設定モード

set transform-keysize

マルチポイント SA で使用する鍵長名を設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　マルチポイント SA で使用する鍵長名を v2key とする

```
Router(config)#crypto ipsec group-security policy MPSA1
Router(config-gr-sec)#set transform-keysize v2key
```

コマンド書式

set transform-keysize <鍵長名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
鍵長名	このセレクタで使用する暗号アルゴリズムの鍵長属性を指定するために、ipsec transform-keysize コマンドで設定した鍵長名を指定します。	最大 16 文字の英数字	省略不可

この設定を行わない場合

AES 使用時の鍵長は 128 として動作します。

設定モード

マルチポイント SA 設定モード

set transform-set

マルチポイント SA で使用する IKEv2 の暗号アルゴリズムを設定します。

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　Phase2 ポリシー名称（P2-POLICY）を指定する

```
Router(config)#crypto ipsec group-security policy MPSA1
Router(config-gr-sec)#set transform-set P2-POLICY
```

コマンド書式

set transform-set <Phase2 ポリシー名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Phase2 ポリシー名称	ipsec transform-set コマンドで設定した Phase2 ポリシー名称を指定します。	最大 16 文字の英数字	省略不可

この設定を行わない場合

マルチポイント SA サーバ機能を使用できません。

設定モード

グループ鍵 IPsec 設定モード

spi mask hex

SA で使用する SPI 値に対して、AND マスクと OR マスクを設定します。
マスクされた SPI 値は、装置内でユニークとなるように管理されます。

SPI-AND マスクは 1 を指定したビットを 16 個以上、SPI-OR マスクは 1 を指定したビットが SPI-AND マスクでは 0 となるように設定してください。
正しく設定していない場合、該当 group-security policy が無効となりますのでご注意ください。

また、マルチポイント SA クライアントが FITELnet FX1 の場合、以下の 2 つの条件にあてはまるよう設定を行ってください。条件を満たさない場合、クライアントの FX1 において IPsec の復号化が正常に行われないことがあります。

1：同一のクライアントに配布する SPI の下位 16bit がマルチポイント SA サーバ毎に異なること
2：SPI の下位 17bit 目が 1 であること(00010000)

refresh コマンド後に有効になるコマンドです。

IKEv2 専用コマンド

設定例 1　SPI 値が 0x01xxxxxx となるように SPI-AND マスク（00ffffff）、SPI-OR マスク(01000000)を設定する

```
Router(config)#crypto ipsec group-security policy MPSA1
Router(config-gr-sec)#spi mask hex 00ffffff 01000000
```

コマンド書式

spi mask hex <SPI-AND マスク> <SPI-OR マスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
SPI-AND マスク	マルチポイント SA の SPI 値が特定の範囲をとるように、乱数となるビットを1、SPI-OR マスクで指定されるビットを0として、HEX で指定します。	最大 8 桁の 16 進数	省略不可
SPI-OR マスク	マルチポイント SA の SPI 値が特定の範囲をとるように、SPI-OR マスクで0指定されたビットに格納される値を指定します。	最大 8 桁の 16 進数	省略不可

この設定を行わない場合

マスクは適用されず、マルチポイント SA の SPI 値の範囲が任意となります。

設定モード

グループ鍵 IPsec 設定モード

IP in IP 機能

IP in IP 機能

ip address

インタフェースの IP アドレス、サブネットマスクを設定します。
refresh コマンド後に有効になるコマンドです。(IPsec インタフェースのみ対応)

設定例 1　PPPoE 1 の IP アドレスを 158.ｘｘｘ.ｘｘｘ.１に設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip address 158.xxx.xxx.1
```

設定例 2　EWAN 1 の IP アドレスを 158.ｘｘｘ.ｘｘｘ.１、サブネットマスクを 255.255.255.0 に設定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip address 158.xxx.xxx.1 255.255.255.0
```

コマンド書式

ip address 〈IP アドレス〉〈サブネットマスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	インタフェースに割り当てる IP アドレスを設定します。	IPv4 アドレス形式	省略不可
サブネットマスク	インタフェースに割り当てるサブネットマスク※を設定します。	IPv4 アドレス形式	省略不可

※PPPoE およびループバックインタフェースでは、サブネットマスクの指定はできません。トンネルインタフェースでは、unnumbered オプションの選択が可能です。詳細は ip address unnumbered を参照して下さい。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
IPsec インタフェース設定モード

ループバックインタフェース設定モード
トンネルインタフェース設定モード

ip address unnumbered

指定したインタフェースに設定されている IP アドレスを使用します。
指定したインタフェースのアドレスが固定設定されていない場合は、トンネルインタフェースに使用することは出来ません。
このインタフェースからデータを送信する必要がある場合に、送信元アドレスとして使用します。

設定例 1　LAN インタフェースの IP アドレスをトンネルインタフェースのアドレスに使用する

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#ip address unnumbered lan 1
```

設定例 2　LAN インタフェースの IP アドレスを IPsec インタフェースのアドレスに使用する

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip address unnumbered lan 1
```

コマンド書式

ip address unnumbered〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	指定したインタフェースに設定されている IP アドレスを使用します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 vlanif 1～150 loopback 1～100	省略不可

この設定を行わない場合

インタフェースのアドレスを送信元アドレスとして使用しない。

設定モード

IPsec インタフェース設定モード
トンネルインタフェース設定モード

tunnel destination

トンネルの宛先アドレスを IP アドレス形式で指定します。
tunnel source コマンドの設定とアドレスファミリを合わせてください。

設定例 1　トンネルの宛先アドレスを 192.168.100.1 とする

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#tunnel destination 192.168.100.1
```

コマンド書式

tunnel destination〈宛先アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先アドレス	トンネルの宛先アドレスを設定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

トンネルの宛先アドレスを指定しません。

設定モード

トンネルインタフェース設定モード

tunnel mode

トンネルインタフェースに対して、カプセル化モードを設定します。

設定例 1　トンネルのモードを IPinIP とする

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#tunnel mode ipip
```

コマンド書式

tunnel mode <モード設定>

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>モード設定</td><td>トンネルモードを IPinIP、EtherIP、L2TP から選択します。
<table>
<tr><td>ipip</td><td>トンネルモードを IPinIP とします。</td></tr>
<tr><td>ether-ip</td><td>トンネルモードを EtherIP とします。</td></tr>
<tr><td>l2tp pseudowire</td><td>トンネルモードに L2TPv3 を指定した場合は、L2TP pseudowire ID の指定が必要になります。</td></tr>
<tr><td>l2tpv2※1</td><td>トンネルモードに L2TPv2 とします。</td></tr>
</table></td><td>Ipip
ether-ip
l2tp pseudowire <1-2000>
l2tpv2</td><td>省略不可</td></tr>
</table>

※1 パラメータ l2tpv2 は、V01.02(00)以降サポート

この設定を行わない場合

トンネルインタフェースを使用できません。

設定モード

トンネルインタフェース設定モード

tunnel source

トンネルの送信元アドレスを IPv4/IPv6 アドレス形式または、インタフェース名で指定します。
tunnel destination コマンドの設定とアドレスファミリを合わせてください。

設定例 1　トンネルの送信元アドレスを 192.168.0.1 とする

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#tunnel source 192.168.0.1
```

設定例 2　トンネルの送信元アドレスを EWAN 1 とする

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#tunnel source ipv6 ewan 1
```

コマンド書式

tunnel source {<送信元アドレス>| ipv6<インタフェース名>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信元アドレス	トンネルの送信元アドレスを設定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
インタフェース名※	トンネルの送信元アドレスとしてインタフェースを指定します。	lan 1 ewan 1～2 loopback 1～100 vlanif 1～150	省略不可

※インタフェース名指定は、該当トンネルのカプセル化モードを IPinIP で使用する場合に限定されます。カプセル化モードの設定は、tunnel mode コマンドで設定します。

この設定を行わない場合

トンネルの送信元アドレスを指定しません。

設定モード

トンネルインタフェース設定モード

Layer2 中継機能

EtherIP/L2TPv2/L2TPv3 共通コマンド

tunnel mode

トンネルインタフェースに対して、カプセル化モードを設定します。

設定例 1　トンネルのモードを IPinIP とする

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#tunnel mode ipip
```

コマンド書式

tunnel mode <モード設定>

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>モード設定</td><td>トンネルモードを IPinIP、EtherIP、L2TP から選択します。
<table>
<tr><td>ipip</td><td>トンネルモードを IPinIP とします。</td></tr>
<tr><td>ether-ip</td><td>トンネルモードを EtherIP とします。</td></tr>
<tr><td>l2tp pseudowire</td><td>トンネルモードに L2TPv3 を指定した場合は、L2TP pseudowire ID の指定が必要になります。</td></tr>
<tr><td>l2tpv2※1</td><td>トンネルモードに L2TPv2 とします。</td></tr>
</table></td><td>Ipip
ether-ip
l2tp pseudowire <1-2000>
l2tpv2</td><td>省略不可</td></tr>
</table>

※1 パラメータ l2tpv2 は、V01.02(00)以降サポート

この設定を行わない場合

トンネルインタフェースを使用できません。

設定モード

トンネルインタフェース設定モード

EtherIP/L2TPv3 共通コマンド

bridge ip adjust-mss

設定したインタフェースから送信される Layer2 中継パケットの MSS 値を指定します。

refresh コマンド後に有効になるコマンドです。

設定例　tunnel 1 インタフェースから送信される Layer2 中継パケットの MSS 値を 1420 にする

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#bridge ip adjust-mss 1420
```

コマンド書式

bridge ip adjust-mss <MSS 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MSS 値	MSS 値を指定します。	254～1460	省略不可

この設定を行わない場合

Layer2 中継パケットの MSS 値を変更しません。

設定モード

LAN インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード

internal-bridge

設定しているインタフェース設定モードが、どのインターナルブリッジグループに接続するかを設定します。

設定例　接続先インターナルブリッジ番号１、tag 情報を透過送受信する

```
Router(config)#interface lan 1
Router(config-if lan 1)# internal-bridge 1 transparent
```

コマンド書式

internal-bridge 〈インターナルブリッジ番号〉〈転送設定〉 [tx-priority 〈送信優先度〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インターナルブリッジ番号	接続先のインターナルブリッジ番号を指定します。	1～100	省略不可
転送設定	tag 情報を変更することなくそのまま転送するか、異なる vlan として取り扱う(tag 情報は除去して転送)かを指定します。 transparent：インターナルブリッジに対して透過送受信を行います。 terminate：vlan を終端します(tag 情報を除去して送受信)。	transparent terminate	省略不可
送信優先度※	送信優先度は、値が大きいほど優先度が高くなります。 同一インターナルブリッジに、複数のトンネルインタフェースが属し、同じ優先度に設定されている場合は、トンネルインタフェース番号が若いトンネルが高優先となります。	1～255	送信優先度は、1 になります。

※パラメータ送信優先度は、トンネルインタフェース指定時のみ選択可能です。

この設定を行わない場合

設定しているインタフェースでのブリッジ中継はできません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード
BVI インタフェース設定モード

internal-bridge address-learning

本コマンドを指定することにより、該当するインターナルブリッジで MAC アドレス学習を行い、学習した MAC アドレス情報にしたがって中継します。
学習していない MAC アドレス宛および、ブロードキャストフレーム／マルチキャストフレームは、全てのポートにフラッディングします。
MAC アドレステーブルのエージアウト時間は、internal-bridge aging-time コマンドで設定します。

refresh コマンド後に有効になるコマンドです。

設定例　MAC アドレス学習を行う接続先インターナルブリッジ番号を 1 とする

```
Router(config)# internal-bridge 1 address-learning
```

コマンド書式

internal-bridge <インターナルブリッジ番号> address-learning

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インターナルブリッジ番号	MAC アドレス学習を行う接続先のインターナルブリッジ番号を指定します。	1～100	省略不可

この設定を行わない場合

Ether インタフェース(lan/vlan)とトンネルインタフェースのスイッチポート動作となります。

設定モード

基本設定モード

internal-bridge aging-time

MAC アドレステーブルのエージアウト時間を設定します。
本コマンドは、internal-bridge address-learning コマンドを設定した際に有効となります。

refresh コマンド後に有効になるコマンドです。

設定例　MAC アドレステーブルのエージアウト時間を 90 秒とする

```
Router(config)# internal-bridge 1 aging-time 90
```

コマンド書式

internal-bridge 〈インターナルブリッジ番号〉 aging-time 〈エージアウト時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インターナルブリッジ番号	MAC アドレステーブルのエージアウト時間を設定するインターナルブリッジ番号を指定します。	1～100	省略不可
エージアウト時間	MAC アドレステーブルのエージアウト時間(単位:秒)を指定します。	1～65535	省略不可

この設定を行わない場合

MAC アドレステーブルのエージアウト時間は 300 秒になります。

設定モード

基本設定モード

internal-bridge permanent-address

MAC アドレステーブルにスタティックでエントリを登録します。

refresh コマンド後に有効になるコマンドです。

設定例　インターナルブリッジ１にトンネル IF 向けの MAC アドレス（xxxx.xxxx.xxxx）のエントリを登録する

```
Router(config)# internal-bridge 1 permanent-address xxxx.xxxx.xxxx vlan-id 0 tunnel 1
```

コマンド書式

internal-bridge <インターナルブリッジ番号> permanent-address <MAC アドレス>
vlan-id <VLAN-ID 値> <インタフェース名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インターナルブリッジ番号	MAC アドレス学習を行う接続先のインターナルブリッジ番号を指定します。	1～100	省略不可
MAC アドレス	登録する MAC アドレスを指定します。	mac アドレス形式	省略不可
VLAN-ID 値	MAC アドレスを登録するインターナルブリッジの vlan-id を指定します。	0～4049	省略不可
インタフェース名	送信するインタフェースを指定します。	lan 1 tunnel 1～2000 vlanif 1～150	省略不可

この設定を行わない場合

Ether インタフェース(lan/vlan)とトンネルインタフェースのスイッチポート動作となります。

設定モード

基本設定モード

internal-bridge redundancy default indicate-selected

本コマンドを指定することにより、対向装置に送信する Circuit Status AVP を制御します。
送信インタフェースとして有効なトンネルについては active を通知し、それ以外は inactive を通知します。

refresh コマンド後に有効になるコマンドです。

設定例　Circuit Status AVP を制御するインターナルブリッジ番号を 1 とする

```
Router(config)# internal-bridge 1 redundancy default indicate-selected
```

コマンド書式

internal-bridge <インターナルブリッジ番号> redundancy default indicate-selected

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インターナルブリッジ番号	Circuit Status AVP を制御する場合に、該当するインターナルブリッジ番号を指定します。	1～100	省略不可

この設定を行わない場合

常に active を通知する動作となります。

設定モード

基本設定モード

internal-bridge redundancy default receive-unselected

本コマンドを指定することにより、送信インタフェースとして選択していないトンネルにおけるパケットの受信可否を選択可能となります。

refresh コマンド後に有効になるコマンドです。

設定例　送信インタフェースでないトンネルのパケット受信を拒否するブリッジ番号を 1 とする

```
Router(config)# internal-bridge 1 redundancy default receive-unselected disable
```

コマンド書式

internal-bridge <インターナルブリッジ番号> redundancy default receive-unselected <enable|disable [delay (1-300)]>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インターナルブリッジ番号	送信インタフェースとして選択していないトンネルにおけるパケットの受信可否を設定する場合に、該当するインターナルブリッジ番号を指定します。	1～100	省略不可
受信可否	enable : 受信を可能にします disable : 受信を拒否します	enable disable	enable で動作します
delay	disable の場合に、受信停止時間を遅らせます	1～300	0 で動作します

この設定を行わない場合

送信インタフェースとして選択されていないトンネルから受信したパケットもそのまま転送します。

設定モード

基本設定モード

internal-bridge relay inter-tunnel-interface

本コマンドを指定することにより、該当するインターナルブリッジでのトンネルインタフェース間の中継を可能とします。

refresh コマンド後に有効になるコマンドです。

設定例　トンネルインタフェース間で中継するインターナルブリッジ番号を 1 とする

```
Router(config)# internal-bridge 1 relay inter-tunnel-interface
```

コマンド書式

internal-bridge <インターナルブリッジ番号> relay inter-tunnel-interface

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インターナルブリッジ番号	インターナルブリッジでのトンネルインタフェース間の中継を行う場合に、該当するインターナルブリッジ番号を指定します。	1～100	省略不可

この設定を行わない場合

トンネルインタフェース間の中継は行いません。

設定モード

基本設定モード

pw-type

トンネルインタフェースの PseudoWire タイプを指定します。
Etherport を指定した場合は、L2TPv3 ネゴシエーションの際に PseudoWire タイプとして etherport を使用し、ethervlan を指定した場合は、PseudoWire タイプとして ethervlan を使用します。
本コマンドは L2TPv3 動作に対する設定であり、EtherIP 動作時は特に何も影響は与えません。

設定例　トンネルインタフェースの PseudoWire タイプに etherport を指定する

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#pw-type etherport
```

コマンド書式

```
pw-type {etherport|ethervlan}
```

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
PseudoWire タイプ	トンネルインタフェースの PseudoWire タイプを指定します。		etherport ethervlan	省略不可
	etherport	L2TPv3 動作時の PseudoWire タイプとして etherport を使用します。		
	ethervlan	L2TPv3 動作時の PseudoWire タイプとして ethervlan を使用します。		

この設定を行わない場合

EtherIP、L2TPv3 が使用できません。

設定モード

トンネルインタフェース設定モード

tagging never

本コマンドを設定することにより、nulltag を除去し untag フレームで HUB に対して出力をおこないます。

設定例　nulltag を除去したフレームを出力する

```
Router(config)#interface lan 1
Router(config-if lan 1)#tagging never
```

コマンド書式

tagging never

パラメータ

パラメータはありません

この設定を行わない場合

nulltag を付与します。

設定モード

LAN インタフェース設定モード

vlan-id

トンネルインタフェースを EtherIP,L2TPv3 で使用する場合で、かつ該当するインターナルブリッジで MAC アドレス学習による中継を行う場合、該当トンネルインタフェースで取り扱う VLAN-ID を設定します。
any とした場合は全 VLAN-ID を該当トンネルインタフェースで取り扱います。

MAC アドレス学習に関しても、ここで指定した VLAN-ID のもの以外のフレームでは、MAC アドレス学習しません。
ただし、ここで指定した VLAN-ID でないスタティック登録については有効となります。

refresh コマンド後に有効になるコマンドです。

設定例 1　トンネルインタフェースで取り扱う VLAN-ID を 1 とする

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)# vlan-id 1
```

コマンド書式

vlan-id {<VLAN-ID 値> | any}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VLAN-ID 値	トンネルインタフェースを EtherIP,L2TPv3 で使用する場合で、かつ該当するインターナルブリッジで MAC アドレス学習による中継を行う場合に、該当トンネルインタフェースで取り扱う VLAN-ID を指定します。	0～4094	省略不可
any	全 VLAN-ID を該当トンネルインタフェースで取り扱います。	any	省略不可

この設定を行わない場合

トンネルインタフェースでは、VLAN-ID のフレームを中継しません。

設定モード

トンネルインタフェース設定モード

L2TPv2/L2TPv3 共通コマンド

digest type

L2TP の認証で使用する Digest に関する設定をします。
refresh コマンド後に有効になるコマンドです。

設定例　L2TP の認証で使用する Digest のアルゴリズムを"md5"、パスワードを"F2200-pass"にする

```
Router(config)#l2tp profile 1
Router(config-l2tp-profile 1)#digest type md5 F2200-pass
```

コマンド書式

digest type <アルゴリズム> <パスワード> [{secret | private} [encrypted]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アルゴリズム	digest のアルゴリズムを指定します。 L2TPv2 の場合は常に md5 を使用します。	md5 sha1	省略不可
パスワード	digest のパスワードを設定します。	最大 64 文字の英数字	省略不可
secret | private	パスワードを暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。※1 secret：暗号化する際に共有暗号鍵を使用する private：暗号化する際に装置固有暗号鍵を使用する	secret private	パスワードを暗号化しません
encrypted	パスワードを暗号化処理するかどうかを設定します。このオプションを付加することにより、パスワードは暗号化済みと判定されます。※2 secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。	encrypted	パスワードを暗号化データとして扱いません

※1 このオプションは、設定するとすぐに有効となり、パスワードが暗号化されて表示され encrypted オプションが自動的に付加されます。
※2 パスワードが既に暗号化済みの場合は、このオプションを指定する必要があります。

この設定を行わない場合

L2TP 認証を使用しません。

設定モード

L2TP プロファイル設定モード(L2TPv2/L2TPv3 で有効)

hello interval

L2TP の keepalive で使用する Hello メッセージの送信間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例　L2TP の keepalive で使用する Hello メッセージの送信間隔を 20 秒にする

```
Router(config)#l2tp profile 1
Router(config-l2tp-profile 1)#hello interval 20
```

コマンド書式

hello interval 〈送信間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	L2TP の keepalive で使用する Hello メッセージの送信間隔(単位:秒)を設定します。	1～3600	省略不可

この設定を行わない場合

Hello メッセージの送信を行いません。

設定モード

L2TP プロファイル設定モード(L2TPv2/L2TPv3 で有効)

hostname local

L2TP でセッションを識別するための自装置のホスト名を設定します。
ここで設定した値は、自装置から送信される Host Name AVP に含まれます。

refresh コマンド後に有効になるコマンドです。

設定例　L2TP でセッションを識別するためのホスト名"F2200_honten"にする

```
Router(config)#l2tp profile 1
Router(config-l2tp-profile 1)#hostname local F2200_honten
```

コマンド書式

hostname local <ホスト名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ホスト名	L2TP でセッションを識別するためのホスト名を設定します。	最大 64 文字の英数字	省略不可

この設定を行わない場合

L2TP が使用できません。

設定モード

L2TP プロファイル設定モード(L2TPv2/L2TPv3 で有効)

hostname remote

L2TP でセッションを識別するための対向装置のホスト名を設定します。
ここで設定した値は、対向装置から受信した Host Name AVP の値と一致するかチェックする際に使用されます。

refresh コマンド後に有効になるコマンドです。

設定例　L2TP でセッションを識別するためのホスト名"F2200_kyoten"にする

```
Router(config)#l2tp profile 1
Router(config-l2tp-profile 1)#hostname remote F2200_kyoten
```

コマンド書式

hostname remote <ホスト名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ホスト名	L2TP でセッションを識別するためのホスト名を設定します。	最大 64 文字の英数字	省略不可

この設定を行わない場合

受信した Host Name AVP のチェックを行いません。

設定モード

L2TP プロファイル設定モード(L2TPv2/L2TPv3 で有効)

l2tp profile

L2TP プロファイル設定モードへ移行します。

refresh コマンド後に有効になるコマンドです。

設定例　L2TP プロファイル設定モードへ移行する

```
Router(config)#l2tp profile 1
Router(config-l2tp-profile 1)#
```

コマンド書式

l2tp profile <L2TP プロファイル ID>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
L2TP プロファイル ID	L2TP プロファイル ID を指定します。 ここで指定した L2TP プロファイル ID は、L2TP Pseudowire 設定モードの tunnel mode l2tp で指定する番号に対応します。	1～2000	省略不可

この設定を行わない場合

L2TP 機能を使用できません。

設定モード

基本設定モード

protocol

L2TP で使用するプロトコルを指定します。

refresh コマンド後に有効になるコマンドです。

設定例　L2TP のプロトコルを l2tpv3 にする

```
Router(config)#l2tp profile 1
Router(config-l2tp-profile 1)#protocol l2tpv3
```

コマンド書式

protocol 〈プロトコル〉

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
プロトコル	L2TP で使用するプロトコルを指定します。		l2tpv3 l2tpv3ext l2tpv2	省略不可
	l2tpv3	対向装置と RFC 準拠の L2TPv3 接続を行う場合は l2tpv3 を指定します。		
	l2tpv3ext	対向装置が cisco 社製装置の場合は、L2TPv3ext を指定します。		
	l2tpv2※1	対向装置と RFC 準拠の L2TPv2 接続を行う場合は l2tpv2 を指定します。		

※1　パラメータ「l2tpv2」は、V01.02(00)以降サポート

この設定を行わない場合

L2TP が使用できません。

設定モード

L2TP プロファイル設定モード(L2TPv2/L2TPv3 で有効)

retransmit retries

L2TP メッセージを再送する際の再送回数を設定します。

refresh コマンド後に有効になるコマンドです。

設定例　L2TP メッセージの再送回数を 30 回にする

```
Router(config)#l2tp profile 1
Router(config-l2tp-profile 1)#retransmit retries 30
```

コマンド書式

retransmit retries〈再送回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
再送回数	L2TP メッセージの再送回数を指定します。	1～255	省略不可

この設定を行わない場合

再送回数は 10 回になります。

設定モード

L2TP プロファイル設定モード(L2TPv2/L2TPv3 で有効)

L2TPv2 関連コマンド

aaa authentication ppp

PPP セッションの認証方式を設定します。
本設定内容は PPP テンプレート設定モードで参照されます。
本装置では認証方式として、装置内に設定したデータベースによる認証をサポートしています。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　PPP セッションの認証方式を設定する

(認証方式名：list-A、認証方式：装置内データベースによる認証、認証グループ名：local-group-A)

```
Router(config)#aaa authentication ppp list-A local-group local-group-A
```

コマンド書式

aaa authentication ppp〈認証方式名〉〈認証方式〉〈認証グループ名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
認証方式名	認証方式名を指定します。	最大 16 文字の英数字	省略不可
認証方式	認証方式を指定します。 local-group　装置内データベースによる認証	local-group	省略不可
認証グループ名	認証グループ名を指定します。	最大 16 文字の英数字	省略不可

この設定を行わない場合

PPP セッションの認証を行うことができません。

設定モード

基本設定モード

aaa local group

認証(L2TP/PPP による認証) を行うデータベースを登録するために、CLIENT-データベース設定モードに移行します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　CLIENT-データベース設定モードに移行する(認証グループ名 : local-A)

```
Router(config)#aaa local group local-A
Router(config-lg-user)#
```

コマンド書式

aaa local group <認証グループ名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
認証グループ名	認証グループ名を指定します。	最大 16 文字の英数字	省略不可

設定モード

基本設定モード

dns

PPP で通知する DNS サーバアドレスを設定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　払い出しアドレスブロックを 192.168.0.0/24 とする

```
Router(config)#ppp-template ppp-A
Router(config-ppp-tmp)#dns 192.0.2.1 192.0.2.2
```

コマンド書式

dns 〈プライマリ DNS サーバアドレス〉[〈セカンダリ DNS サーバアドレス〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プライマリ DNS サーバアドレス	PPP で通知するプライマリ DNS サーバアドレスを指定します。	IPv4 アドレス形式	省略不可
セカンダリ DNS サーバアドレス	PPP で通知するセカンダリ DNS サーバアドレスを指定します。	IPv4 アドレス形式	セカンダリ DNS サーバアドレスを通知しません。

この設定を行わない場合

DNS サーバアドレスを通知しません。

設定モード

L2TP-PPP テンプレート設定モード

ip local pool

PPP/L2TP を利用して通知するアドレス範囲を設定します。
本設定は、同一アドレスプール名によってソートされます。
同一アドレスプール名で複数の設定を行うことができます。
同一アドレスプール名で複数設定した場合は、設定を行った順番で表示し、上に表示されるプールから使用を開始します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　払い出しアドレスブロックを 192.168.0.0/24 とする

```
Router(config)#ip local pool POOL1 192.168.0.0 255.255.255.0
```

コマンド書式

ip local pool〈アドレスプール名〉〈ネットワークアドレス〉〈ネットマスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスプール名	アドレスプール名を指定します。	最大 16 文字の英数字	省略不可
ネットワークアドレス	払い出しアドレスブロックを指定します。	IPv4 アドレス形式	省略不可
ネットマスク	払い出しアドレス範囲をネットマスクで指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

固定払い出しブロックはありません。

設定モード

基本設定モード

keepalive

PPP LCP ECHO REQUEST メッセージの送信間隔(単位:秒)と再送回数を設定します。
送信間隔に 0 を指定した場合、PPP LCP ECHO REQUEST を送信しません。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　PPP LCP ECHO REQUEST メッセージの送信間隔(30 秒) と再送回数(3 回) を設定する

```
Router(config)#l2tp-ppp-template ppp-A
Router(config-l2tp-ppp-tmp)#keepalive 30 3
```

コマンド書式

keepalive 〈送信間隔〉 [〈再送回数〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	PPP LCP ECHO REQUEST メッセージの送信間隔(単位:秒)を指定します。	0～32767	省略不可
再送回数	PPP LCP ECHO REQUEST メッセージの再送回数を指定します。	1～255	5

この設定を行わない場合

以下の値で動作します。
送信間隔 : 60 秒
再送回数 : 5 回

設定モード

L2TP-PPP テンプレート設定モード

l2tp-ppp-template

L2TP-PPP テンプレート設定モードに移行します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　L2TP-PPP テンプレート設定モードに移行する (L2TP-PPP テンプレート名：ppp-A)

```
Router(config)#l2tp-ppp-template ppp-A
Router(config-l2tp-ppp-tmp)#
```

コマンド書式

l2tp-ppp-template <L2TP-PPP テンプレート名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
L2TP-PPP テンプレート名	L2TP-PPP テンプレート名を指定します。	最大 16 文字の英数字	省略不可

設定モード

基本設定モード

pool

PPP で通知する IP アドレス範囲のアドレスプール名を設定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　アドレスプール名を設定する(アドレスプール名：pool-A)

```
Router(config)#l2tp-ppp-template ppp-A
Router(config-l2tp-ppp-tmp)#pool chap list-A
```

コマンド書式

pool〈アドレスプール名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスプール名	アドレスプール名を設定します。	最大 16 文字の英数字	省略不可

この設定を行わない場合

PPP で通知する IP アドレスがローカルプール払い出しの場合、PPP セッションを確立できません。

設定モード

L2TP-PPP テンプレート設定モード

ppp accept template

該当 L2TPv2 トンネル上で収容する PPP セッションを関連付けます。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　L2TPv2 トンネル上で収容する PPP セッションを関連付けする(L2TP-PPP テンプレート名：ppp-A)

```
Router(config)#l2tp profile 1
Router(config-l2tp-profile 1)#ppp accept template ppp-A
```

コマンド書式

ppp accept template <L2TP-PPP テンプレート名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
L2TP-PPP テンプレート名	L2TPv2 トンネルに関連付ける L2TP-PPP テンプレート名を指定します。	最大 16 文字の英数字	省略不可

この設定を行わない場合

L2TPv2 トンネルを確立できません。

設定モード

L2TP プロファイル設定モード(L2TPv2 でのみ有効)

ppp authentication

PPP の認証タイプと認証方式名を設定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　PPP の認証タイプ(chap)と認証方式名(list-A)を設定する

```
Router(config)#l2tp-ppp-template ppp-A
Router(config-l2tp-ppp-tmp)#ppp authentication chap list-A
```

コマンド書式

ppp authentication <PPP の認証タイプ> <認証方式名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
PPP の認証タイプ	PPP の認証タイプを指定します。 chap：chap 認証のみ受け付ける pap：pap 認証のみ受け付ける auto：chap 認証、または、pap 認証を受け付ける	最大 16 文字の英数字	省略不可
認証方式名	PPP セッションの認証方式名を指定します。	最大 16 文字の英数字	省略不可

この設定を行わない場合

L2TPv2 セッションを確立できません。

設定モード

L2TP-PPP テンプレート設定モード

tunnel protection

L2TPv2 のパケットを IPsec により保護したい場合に VPN セレクタを指定します。
IKEv1 でのみ有効です。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　L2TPv2 のパケットを IPsec により保護する(crypto map MAP1 を指定)

```
Router(config)#l2tp profile 1
Router(config-l2tp-profile)#tunnel protection ipsec map MAP1
```

コマンド書式

tunnel protection ipsec map <セレクタ名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セレクタ名称	L2TPv2 パケットをカプセル化する VPN セレクタを指定します。 crypto map コマンドで指定したセレクタ名称で指定します。	最大 16 文字の英数字	省略不可

この設定を行わない場合

L2TPv2 のパケットを暗号化せずに、そのまま送受信します。

設定モード

L2TP プロファイル設定モード(L2TPv2 でのみ有効)

username

認証(L2TP/PPP による認証)により接続を許可するユーザ名とパスワードを設定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　PPP の認証タイプ(chap)と認証方式名(list-A)を設定する

```
Router(config)#aaa local group local-A
Router(config-lg-user)#username user-A password furukawa
```

コマンド書式

username 〈ユーザ名〉 password 〈パスワード〉 [{secret|private} [encrypted]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ユーザ名	ユーザ名を指定します。	最大 128 文字の英数字	省略不可
パスワード	パスワードを指定します。	最大 128 文字の英数字	省略不可
secret | private	パスワードを暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。※1 secret：暗号化する際に共有暗号鍵を使用する private：暗号化する際に装置固有暗号鍵を使用する	secret private	パスワードを暗号化しません
encrypted	パスワードを暗号化処理するかどうかを設定します。このオプションを付加することにより、パスワードは暗号化済みと判定されます。※2 secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。	最大 16 文字の英数字	省略不可

※1 このオプションは、設定するとすぐに有効となり、パスワードが暗号化されて表示され encrypted オプションが自動的に付加されます。
※2 パスワードが既に暗号化済みの場合は、このオプションを指定する必要があります。

この設定を行わない場合

認証をこの認証グループを利用して行うことができません。

設定モード

CLIENT-データベース設定モード

username interface tunnel

認証(L2TP/PPP) による接続時に、ユーザに対して固定のインタフェース番号を使用する場合のインタフェース番号を設定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例　固定のインタフェース番号を使用したい場合の tunnel インタフェース番号を設定する　(ユーザ名：user-A、tunnel インタフェース番号：50)

```
Router(config)#aaa local group local-A
Router(config-lg-user)#username user-A interface tunnel 50
```

コマンド書式

username 〈ユーザ名〉 interface tunnel 〈tunnel インタフェース番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ユーザ名	ユーザ名を指定します。	最大 128 文字の英数字	省略不可
tunnel インタフェース番号	tunnel インタフェース番号を指定します。	1～2000	省略不可

この設定を行わない場合

L2TPv2 セッションを確立できません。

設定モード

CLIENT-データベース設定モード

L2TPv3 関連コマンド

cookie size

L2TPv3 のデータプレーンで使用する自局側の Cookie のサイズを設定します

refresh コマンド後に有効になるコマンドです。

設定例　Cookie のサイズを 8 バイトとする

```
Router(config)#l2tp pseudowire 1
Router(config-l2tp-pseudowire 1)#cookie size 8
```

コマンド書式

cookie size <Cookie size>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Cookie size	Cookie のサイズを 4 バイトまたは、8 バイトから指定します。 4　Cookie size を 4 バイトとする。 8　Cookie size を 8 バイトとする。	4 8	省略不可

この設定を行わない場合

L2TPv3 Cookie を使用しません。

設定モード

L2TP Pseudowire 設定モード

hidden

L2TPv3 の AVP hiding 機能を使用する場合に設定します。
この機能を使用する場合、digest type の設定も必要です

refresh コマンド後に有効になるコマンドです。

設定例　L2TPv3 の AVP hiding 機能を使用する

```
Router(config)#l2tp profile 1
Router(config-l2tp-profile 1)#hidden
```

コマンド書式

hidden

パラメータ

パラメータはありません

この設定を行わない場合

L2TPv3 の AVP hiding を使用しません。

設定モード

L2TP プロファイル設定モード(L2TPv3 でのみ有効)

initial-state discard

本コマンドを設定することにより、制御状態が Unknown に移行した場合の実動作を Discard 状態とします。

refresh コマンド後に有効になるコマンドです。

設定例　制御状態が Unknown に移行した場合の実動作を Discard 状態とする

```
Router(config)#l2tp pseudowire 1
Router(config-l2tp-pseudowire 1)#initial-state discard
```

コマンド書式

```
initial-state discard
```

パラメータ

パラメータはありません

この設定を行わない場合

制御状態が Unknown に移行した場合の実動作を Connect とします。

設定モード

L2TP Pseudowire 設定モード

l2tp pseudowire

L2TP Pseudowire 設定モードへ移行します。

refresh コマンド後に有効になるコマンドです。

設定例　L2TP Pseudowire 設定モードへ移行する

```
Router(config)#l2tp pseudowire 1
Router(config-l2tp-pseudowire 1)#
```

コマンド書式

l2tp pseudowire <L2TP Pseudowire ID>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
L2TP Pseudowire ID	L2TP Pseudowire ID を指定します。 ここで指定した L2TP Pseudowire ID は、トンネルインタフェース設定モードの tunnel mode l2tp で指定する番号に対応します。 ただし、複数の tunnel mode l2tpv3 から1つの L2TP Pseudowire ID への紐付けはできません。	1～2000	省略不可

この設定を行わない場合

L2TP 機能を使用できません。

設定モード

基本設定モード

remote-end-id ascii

L2TPv3 でセッションを識別するための値を設定します。
ここで設定した値は、Remote End ID AVP に含まれます。

refresh コマンド後に有効になるコマンドです。

設定例　Remote End ID を 1000 とする

```
Router(config)#l2tp pseudowire 1
Router(config-l2tp-pseudowire 1)#remote-end-id ascii 1000
```

コマンド書式

remote-end-id ascii <Remote End ID>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Remote End ID	Remote End ID を設定します。	最大 32 文字の英数字	省略不可

この設定を行わない場合

L2TPv3 が使用できません。

設定モード

L2TP Pseudowire 設定モード

router-id local

L2TPv3 でセッションを識別するための自装置のルータ ID を設定します。
ここで設定した値は、自装置から送信される Router-ID AVP に含まれます。

refresh コマンド後に有効になるコマンドです。

設定例　L2TPv3 でセッションを識別するためのルータ ID を 192.168.1.1 にする

```
Router(config)#l2tp profile 1
Router(config-l2tp-profile 1)#router-id local 192.168.1.1
```

コマンド書式

router-id local <ルータ ID>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ルータ ID	L2TPv3 でセッションを識別するためのルータ ID を設定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

L2TPv3 セッションの端点が IPv4 の場合は、tunnel source コマンドで設定したアドレスを使用します。
IPv6 の場合は本設定が必須であり、L2TP が使用できません。

設定モード

L2TP プロファイル設定モード(L2TPv3 でのみ有効)

router-id remote

L2TPv3 でセッションを識別するための対向装置のルータ ID を設定します。
ここで設定した値は、対向装置から受信した Router-ID AVP の値と一致するかチェックする際に使用されます。

refresh コマンド後に有効になるコマンドです。

設定例　L2TPv3 でセッションを識別するためのルータ ID を 192.168.10.1 にする

```
Router(config)#l2tp profile 1
Router(config-l2tp-profile 1)#router-id remote 192.168.10.1
```

コマンド書式

router-id remote <ルータ ID>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ルータ ID	L2TPv3 でセッションを識別するためのルータ ID を設定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

受信した Router-ID AVP のチェックを行いません。

設定モード

L2TP プロファイル設定モード(L2TPv3 でのみ有効)

sequencing both

本コマンドを設定することで、L2TPv3 カプセル化の際に L2-Specific Sublayer を追加してシーケンス番号をセットします。

refresh コマンド後に有効になるコマンドです。

設定例　順序が入れ替わったパケットを破棄する

```
Router(config)#l2tp pseudowire 1
Router(config-l2tp-pseudowire 1)#sequencing both
```

コマンド書式

```
sequencing both
```

パラメータ

パラメータはありません

この設定を行わない場合

sequencing を使用しません。

設定モード

L2TP Pseudowire 設定モード

set profile

L2TP プロファイル ID を指定します。

refresh コマンド後に有効になるコマンドです。

設定例　L2TP プロファイル ID を 1 とする

```
Router(config)#l2tp pseudowire 1
Router(config-l2tp-pseudowire 1)#set profile 1
```

コマンド書式

set profile <L2TP プロファイル ID>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
L2TP プロファイル ID	L2TP プロファイル ID を指定します。	1～2000	省略不可

この設定を行わない場合

L2TPv3 が使用できません。

設定モード

L2TP Pseudowire 設定モード

NAT 機能

NAT 機能

ip nat log-table-changes

NAT 変換テーブルの作成/削除時に、slog に出力するかどうかの設定です。

refresh コマンド後に有効になるコマンドです。

設定例　NAT 変換テーブルの作成/削除時に、slog に出力する

```
Router(config)#ip nat log-table-changes
```

コマンド書式

ip nat log-table-changes

パラメータ

パラメータはありません

この設定を行わない場合

NAT 変換テーブルの作成/削除時に、slog に出力しません。

設定モード

基本設定モード

ip nat reserved-sessions

NAT 変換動作において、UPnP で要求された変換ルールや自局発着の通信のため、指定したセッション数だけ変換テーブルを予約することができます。
この設定により、NAT 変換テーブルが溢れてしまった場合でも、UPnP でポート変換を予約した通信や、DNS 問合せ等の自局発着通信が可能となります。

refresh コマンド後に有効になるコマンドです。

設定例　NAT 変換テーブルを 10 セッション分予約する

```
Router(config)#ip nat reserved-sessions 10
```

コマンド書式

ip nat reserved-sessions 〈セッション数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セッション数	NAT 変換動作において、予約する変換テーブルの数を設定します。	1～100	省略不可

この設定を行わない場合

変換テーブルの予約は行いません。

設定モード

基本設定モード

ip nat max-sessions

NAT 変換テーブルの総数を設定します。
学習フィルタリングを併用している場合、学習フィルタリングのセッション数も併せて拡張してください。

設定例　NAT 変換テーブルを 20000 セッション分設定する

```
Router(config)#ip nat max-sessions 20000
```

コマンド書式

ip nat max-sessions <セッション数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セッション数	NAT テーブルの最大数を設定します。	2048～65535	省略不可

この設定を行わない場合

2048

設定モード

基本設定モード

ip nat translation finrst-timeout

TCP の FIN フラグまたは RST フラグが設定されたパケットについて NAT/NAT+変換する場合に、装置の内部テーブルにデータをエージアウトする時間(秒)を設定します。

設定例　FIN/RST フラグが設定されたパケットの NAT 変換タイムアウトを 10 秒に設定する

```
Router(config)#ip nat translation finrst-timeout 10
```

コマンド書式

ip nat translation finrst-timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	FIN/RST フラグが設定されたパケットについての NAT/NAT+変換テーブルのタイムアウト時間(秒)	1～86400	省略不可

この設定を行わない場合

60 秒が設定されます。

FIN フラグとは？

TCP コネクションで、コネクションを解放する場合に、FIN フラグをセットした TCP パケットを送信します。
TCP のプロトコルでは、FIN を送信した側は FIN-ACK を受信することで、TCP のコネクションの解放となります。
つまり、FIN を送信した側が FIN-ACK を受信できなかった場合、TCP コネクションの解放を行なうことができません。

本装置で NAT 機能を使用するような場合、FIN のデータは TCP の解放であり、その後このコネクションを使用してデータ通信を行なう必要がないため、他のデータに比べて NAT テーブルを長期間保持しておく必要がありません。したがって、他のデータより、タイムアウト時間を短く設定しておく運用が考えられます。

ご使用の環境に合わせて、設定変更を行なってください。

RST フラグとは？

TCP コネクションで、アプリケーションの指定により TCP コネクションを中断する場合に、RST フラグをセットした TCP パケットを送信します。

本装置で NAT 機能を使用するような場合、RST のデータは TCP の中断であり、その後このコネクションを使用してデータ通信を行なう必要がないため、他のデータに比べて NAT テーブルを長期間保持しておく必要がありません。したがって、他のデータより、タイムアウト時間を短く設定しておく運用が考えられます。

ご使用の環境に合わせて、設定変更を行なってください。

設定モード

基本設定モード

ip nat translation icmp-timeout

ICMP について NAT/NAT+変換する場合に、装置の内部テーブルにデータをエージアウトする時間(秒)を設定します。

設定例　ICMP パケットの NAT 変換タイムアウトを 10 秒に設定する

```
Router(config)#ip nat translation icmp-timeout 10
```

コマンド書式

ip nat translation icmp-timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	ICMP パケットについての NAT/NAT+変換テーブルのタイムアウト時間(秒)	1～86400	省略不可

この設定を行わない場合

60 秒が設定されます。

設定モード

基本設定モード

ip nat translation syn-timeout

TCP の SYN フラグが設定されたパケットについて NAT/NAT+変換する場合に、装置の内部テーブルにデータをエージアウトする時間(秒)を設定します。

V01.07(00)以降サポート

設定例　ICMP パケットの NAT 変換タイムアウトを 10 秒に設定する

```
Router(config)#ip nat translation syn-timeout 10
```

コマンド書式

ip nat translation syn-timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	SYN フラグが設定されたパケットについての NAT/NAT+変換テーブルのタイムアウト時間(秒)	1～86400	省略不可

この設定を行わない場合

30 秒が設定されます。

SYN フラグとは？

TCP コネクションで、コネクションを接続する場合に、SYN フラグをセットした TCP パケットを送信します。
TCP のプロトコルでは、SYN を送信した側は SYN-ACK を受信して、ACK を送信することで、TCP のコネクションの接続となります。
つまり、SYN を送信した側が SYN-ACK を受信できなかった場合、TCP コネクションの接続を行なうことができません。

FITELnet F60 で NAT 機能を使用するような場合、SYN のデータを送信して SYN-ACK を受信しない場合、TCP の接続ができず、このコネクションを使用したデータ通信も行なわれないため、他のデータに比べて NAT テーブルを長期間保持しておく必要がありません。したがって、他のデータより、タイムアウト時間を短く設定しておく運用が考えられます。

ご使用の環境に合わせて、設定変更を行なってください。

設定モード

基本設定モード

ip nat translation tcp-timeout

TCP について NAT/NAT+変換する場合に、装置の内部テーブルにデータをエージアウトする時間(秒)を設定します。

設定例　TCP パケットの NAT 変換タイムアウトを 10 秒に設定する

```
Router(config)#ip nat translation tcp-timeout 10
```

コマンド書式

ip nat translation tcp-timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	TCP パケットについての NAT/NAT+変換テーブルのタイムアウト時間(秒)	1～86400	省略不可

この設定を行わない場合

3600 秒が設定されます。

設定モード

基本設定モード

ip nat translation timeout

NAT/NAT+変換する場合に、装置の内部テーブルにデータをエージアウトする時間(秒)を設定します。

設定例　NAT 変換タイムアウトを 10 秒に設定する

```
Router(config)#ip nat translation timeout 10
```

コマンド書式

ip nat translation timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	NAT/NAT+変換テーブルのタイムアウト時間(秒)	1～86400	省略不可

この設定を行わない場合

86400 秒が設定されます。

他のコマンドとの連携

特定のパケットに対するタイムアウト時間を設定することができます。

- TCP　(ip nat translation tcp-timeout)
- TCP(FIN/RST)　(ip nat translation finrst-timeout)
- TCP(SYN)　(ip nat translation syn-timeout)
- UDP　(ip nat translation udp-timeout)
- ICMP　(ip nat translation icmp-timeout)

これらが設定されている場合は、そちらのタイマに従い、特定されていないパケットについては、本コマンドの設定に従います。

設定モード

基本設定モード

ip nat translation udp-timeout

UDP について NAT/NAT+変換する場合に、装置の内部テーブルにデータをエージアウトする時間(秒)を設定します。

設定例　UDP パケットの NAT 変換タイムアウトを 10 秒に設定する

```
Router(config)#ip nat translation udp-timeout 10
```

コマンド書式

ip nat translation udp-timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	UDP パケットについての NAT/NAT+変換テーブルのタイムアウト時間(秒)	1～86400	省略不可

この設定を行わない場合

300 秒が設定されます。

設定モード

基本設定モード

ip nat inside source

そのインタフェースから送信するパケットの送信元アドレスの変換ルールを設定します。
NAT モードの場合と、NAT+モード(IP マスカレード)の場合で、設定のしかたが異なりますので注意してください。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例 1　NAT 変換（192.168.0.0/24　→　158.xxx.xxx.2～158.xxx.xxx.7）

```
Router(config)#interface ewan 1
Router(config-if ewan1)#ip nat inside source list 1 pool pool1



Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255   ←list 1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.2 158.xxx.xxx.7 ←pool1 の部分の設定
```

【解説】
ip nat inside source <変換前のアドレス範囲> <変換後のアドレス範囲>となります。
<変換前のアドレス範囲>は、access-list コマンドで指定します。
<変換後のアドレス範囲>は、ip nat pool <pool 名>コマンドで指定します。

設定例 2　NAT+変換（192.168.0.0/24　→　インタフェースアドレス）

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat inside source list 1 interface



Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list 1 の部分の設定
```

【解説】
ip nat inside source <変換前のアドレス範囲> <変換後のアドレス範囲>となります。
<変換前のアドレス範囲>は、access-list コマンドで指定します。
<変換後のアドレス範囲>は、インタフェースアドレスに集約しますので、"interface"と指定します。

設定例３　NAT 変換（スタティック登録）　設定例１の中で 192.168.0.1⇔158.xxx.xxx.2 のみ固定変換

```
Router(config)#interface ewan 1
Router(config-if ewan1)#ip nat inside source static 192.168.0.1 158.xxx.xxx.2
Router(config-if ewan1)#ip nat inside source list 1 pool pool1



Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255  ←list 1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.3 158.xxx.xxx.7 ←pool1 の部分の設定
```

【解説】

設定例1とほぼ同じです。

違う点は、ip nat inside source static で、NAT スタティック変換をしている箇所ですが、この場合も、ip nat inside source <変換前のアドレス> <変換後のアドレス>となります。

設定例４　NAT 変換（一括変換）192.168.100.0/24←→158.ｘｘｘ.ｘｘｘ.0/24 に変換する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat inside source static-subnet 192.168.100.0 158.xxx.xxx.0
255.255.255.0
```

【解説】

ip nat inside source static-subnet <変換前の送信元ネットワークアドレス> <変換後の送信元ネットワークアドレス> <サブネットマスク>となります。

グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。

NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます（複数同時登録）。

例）local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT 時】
ip nat inside source list <access-list 番号> [変換前開始ポート番号 [変換前終了ポート番号]] pool <プール名> [overload | [変換後開始ポート番号 [変換後終了ポート番号]]]

【NAT+時】
ip nat inside source list <access-list 番号> [開始ポート番号 [終了ポート番号]] interface [overload | [変換後開始ポート番号 [変換後終了ポート番号]]]

【スタティック変換】
ip nat inside source static <変換前のアドレス> <変換後のアドレス>

【NAT スタティック（一括変換）】
ip nat inside source static-subnet <変換前のネットワークアドレス> <変換後のネットワークアドレス> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前のアドレス範囲を指定したアクセスリストを指定します。	1～99 1300～1399 10000～11200	省略不可
[変換前開始ポート番号 変換前終了ポート番号]	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
プール名	変換後のアドレス範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	NAT の場合は省略不可
interface	インタフェースのアドレスに NAT+変換します。	interface	NAT+の場合は省略不可
overload	local のポート番号を必ず別のポート番号に変換する場合に指定 ※変換後のポート番号は 1024～65535	overload	local のポート番号を基本的には変換せずに napt を試みます。 すでにそのポート番号が使用されている場合に限り、別のポート番号に変換します。 変換後のポート番号は 1024～65535。
[変換後開始ポート番号 変換後終了ポート番号]	変換後の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
変換前のアドレス	変換前の送信元アドレスを指定します。	IPv4 アドレス形式	省略不可

変換後のアドレス	変換後の送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
変換前のネットワークアドレス	変換前の送信元ネットワークアドレスを指定します。 static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
変換後のネットワークアドレス	変換後の送信元ネットワークアドレスを指定します。 static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ：スタティック 5000 エントリ、リスト 128 エントリ
送信パケットに対する NAT（ip nat inside source＋ip nat outside destination）の合計となります。

この設定を行わない場合

アドレス変換は行いません。

適用順序

NAT 変換ルールは以下の順序で適用されます。

1）static 変換ルール
2）list による変換ルール

同じ種類のルール内では、Prefix 長が長いルールが優先して適用されます。
同一 Prefix 長の設定が複数あった場合には、config 上で先に登録されたものが優先されます。
なお、config には、以下の順に登録され、同じ種類については入力順に登録されます。

1）static 変換ルール（既存のホストアドレス指定）
2）static-subnet 変換ルール
3）list による変換ルール

IPsec インタフェースで NAT を使用する上での注意事項 ※V01.03(00)以降サポート

・VPN-NAT と、IPsec インタフェースでの NAT の、それぞれ設定に不整合がない場合は、
　IPsec インタフェースの NAT が有効となり、VPN-NAT は無効となります。
・IPsec インタフェースの動的割り当てには対応していません。
　IKEv1: mode-config
　IKEv2: Configuration-Payload
・IPsec インタフェースで NAT 変換する場合でも、該当 SA のセレクタ交換時に使用する
　Phase2-ID は、自動的に変換しません。NAT 変換後のアドレスでセレクタ交換しなくて
　はいけないケースでは、set security-association ipsec-src-id コマンドを利用してください。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
IPsec インタフェース設定モード
ダイヤラーインタフェース設定モード
トンネルインタフェース設定モード
USB-Ethernet インタフェース設定モード

ip nat inside destination

そのインタフェースで受信するパケットの宛先アドレスの変換ルールを設定します。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（スタティック登録）　158.xxx.xxx.2 宛で受信したら 192.168.0.1 に変換する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat inside destination static 158.xxx.xxx.2 192.168.0.1
```

【解説】
ip nat inside destination static <変換前の宛先アドレス> <変換後の宛先アドレス>となります。

設定例２　NAT+変換（スタティック登録）　158.xxx.xxx.2:ポート番号 1500 で受信したら、192.168.0.1:ポート番号 80 に変換する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat inside destination static 158.202.232.1 1500 192.168.0.1 80
```

【解説】
ip nat inside destination static <変換前の送信元アドレス　ポート番号> <変換後の宛先アドレス　ポート番号>となります。

設定例３　NAT 変換（一括変換）158.xxx.xxx.xxx.0/24⇔192.168.100.0/24 に変換する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat inside destination static-subnet 158.xxx.xxx.xxx.0 192.168.100.0
255.255.255.0
```

【解説】
ip nat inside destination static-subnet <変換前のネットワークアドレス> <変換後のネットワークアドレス> <サブネットマスク>となります。
グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。
NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます（複数同時登録）。

例）local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT スタティック（複数指定）時】
ip nat inside destination list <access-list 番号> [開始ポート番号 [終了ポート番号]] pool <プール名> [ポート番号]

【NAT スタティック（1 対 1 変換）、NAT+スタティック時】
ip nat inside destination static <変換前のアドレス> [開始ポート番号 [終了ポート番号]] <変換後のアドレス> [ポート番号]

【NAT スタティック（一括変換）】
ip nat inside destination static-subnet <変換前のネットワークアドレス> <変換後のネットワークアドレス> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前のアドレス範囲を指定したアクセスリストを指定します。	1～99 1300～1399 10000～11200	省略不可
変換前のアドレス	変換前の宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
[開始ポート番号 終了ポート番号]	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	ポート変換しない
プール名	変換後のアドレス範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	省略不可
変換後のアドレス	変換後の宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
ポート番号	変換後の TCP/UDP ポート番号を指定します。	1～65535	ポート変換しない
変換前のネットワークアドレス	変換前の宛先ネットワークアドレスを指定します。 static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
変換後のネットワークアドレス	変換後の宛先ネットワークアドレスを指定します。 static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ：スタティック 5000 エントリ、リスト 64 エントリ
受信パケットに対する NAT(ip nat inside destination＋ip nat outside source)の合計となります。

この設定を行わない場合

アドレス変換は行いません。

適用順序

NAT 変換ルールは以下の順序で適用されます。

1）static 変換ルール
2）list による変換ルール

同じ種類のルール内では、Prefix 長が長いルールが優先して適用されます。
同一 Prefix 長の設定が複数あった場合には、config 上で先に登録されたものが優先されます。
なお、config には、以下の順に登録され、同じ種類については入力順に登録されます。

1）static 変換ルール（既存のホストアドレス指定）
2）static-subnet 変換ルール
3）list による変換ルール

IPsec インタフェースで NAT を使用する上での注意事項 ※V01.03(00)以降サポート

・VPN-NAT と、IPsec インタフェースでの NAT の、それぞれ設定に不整合がない場合は、
　IPsec インタフェースの NAT が有効となり、VPN-NAT は無効となります。
・IPsec インタフェースの動的割り当てには対応していません。
　IKEv1: mode-config
　IKEv2: Configuration-Payload
・IPsec インタフェースで NAT 変換する場合でも、該当 SA のセレクタ交換時に使用する
　Phase2-ID は、自動的に変換しません。NAT 変換後のアドレスでセレクタ交換しなくて
　はいけないケースでは、set security-association ipsec-src-id コマンドを利用してください。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
IPsec インタフェース設定モード
ダイヤラーインタフェース設定モード
トンネルインタフェース設定モード

ip nat outside source

そのインターフェースで受信するパケットの送信元アドレスの変換ルールを設定します。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（192.168.0.0/24　→　158.xxx.xxx.2～158.xxx.xxx.7）

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside source list 1 pool pool1

Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←ist 1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.2 158.xxx.xxx.7 ←pool1 の部分の設定
```

【解説】
ip nat outside source <変換前の送信元アドレス範囲> <変換後の送信元アドレス範囲>となります。
<変換前の送信元アドレス範囲>は、access-list コマンドで指定します。
<変換後の送信元アドレス範囲>は、ip nat pool <pool 名>コマンドで指定します。

設定例２　NAT+変換（192.168.0.1：～80　→　192.168.100.1：8080）

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat outside source static 192.168.0.1 80 192.168.100.1 8080
```

【解説】
ip nat outside source static <変換前の送信元アドレス　ポート番号> <変換後の送信元アドレス　ポート番号>となります。

設定例３　NAT 変換（スタティック登録）　設定例１の中で 192.168.0.1⇔158.xxx.xxx.2 のみ固定変換

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside source static 192.168.0.1 158.xxx.xxx.2
Router(config-if lan 1)#ip nat outside source list 1 pool pool1
Router(config-if lan 1)#ip nat outside destination static 158.xxx.xxx.2 192.168.0.1

Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list 1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.3 158.xxx.xxx.7 ← pool1 の部分の設定
```

【解説】
設定例1とほぼ同じです。
違う点は、ip nat outside source static で、NAT スタティック変換をしている箇所ですが、この場合も、
ip nat inside source <変換前の送信元アドレス> <変換後の送信元アドレス>

となります。
この場合、ip nat outside destination コマンドを使用して、グローバル側→ローカル側のスタティック登録を行なう必要があります。(①の部分)

設定例４　NAT 変換（一括変換）192.168.100.0/24←→158.ｘｘｘ.ｘｘｘ.0/24 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside source static-subnet 192.168.100.0 158.xxx.xxx.0
255.255.255.0
```

【解説】

ip nat outside source static-subnet <変換前の送信元ネットワークアドレス> <変換後の送信元ネットワークアドレス> <サブネットマスク>となります。

グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。

NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます(複数同時登録)。

例)local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
: :
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT 時】
ip nat outside source list <access-list 番号> pool <プール名>

【NAT+時】
ip nat outside source list <access-list 番号> [変換前開始ポート番号 [変換前終了ポート番号]] pool <プール名> [変換後ポート番号]

【スタティック変換】
ip nat outside source static <変換前のアドレス> [変換前開始ポート番号 [変換前終了ポート番号]] <変換前のアドレス> [変換後ポート番号]

【NAT スタティック（一括変換）】
ip nat outside source static-subnet <変換前のネットワークアドレス> <変換後のネットワークアドレスト> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前のアドレス範囲を指定したアクセスリストを指定します。	1～99 1300～1399 10000～11200	省略不可

変換前開始ポート番号 変換前終了ポート番号	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
プール名	変換後のアドレス範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	NAT の場合は省略不可
変換後開始ポート番号 変換後終了ポート番号	変換後の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
変換前のアドレス	変換前の送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
変換後のアドレス	変換後の送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
変換前のネットワークアドレス	変換前の送信元アドレスを指定します。static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
変換後のネットワークアドレス	変換後の送信元アドレスを指定します。static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ:スタティック 5000 エントリ、リスト 64 エントリ
受信パケットに対する NAT(ip nat inside destination＋ip nat outside source)の合計となります。
※ この印がついた設定範囲は、V01.13(00)以降サポート

この設定を行わない場合

アドレス変換は行いません。

適用順序

NAT 変換ルールは以下の順序で適用されます。

1)static 変換ルール
2)list による変換ルール

同じ種類のルール内では、Prefix 長が長いルールが優先して適用されます。
同一 Prefix 長の設定が複数あった場合には、config 上で先に登録されたものが優先されます。
なお、config には、以下の順に登録され、同じ種類については入力順に登録されます。

1)static 変換ルール(既存のホストアドレス指定)
2)static-subnet 変換ルール
3)list による変換ルール

IPsec インタフェースで NAT を使用する上での注意事項 ※V01.03(00)以降サポート

・VPN-NAT と、IPsec インタフェースでの NAT の、それぞれ設定に不整合がない場合は、
IPsec インタフェースの NAT が有効となり、VPN-NAT は無効となります。
・IPsec インタフェースの動的割り当てには対応していません。
IKEv1: mode-config
IKEv2: Configuration-Payload
・IPsec インタフェースで NAT 変換する場合でも、該当 SA のセレクタ交換時に使用する
Phase2-ID は、自動的に変換しません。NAT 変換後のアドレスでセレクタ交換しなくて
はいけないケースでは、set security-association ipsec-src-id コマンドを利用してください。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
IPsec インタフェース設定モード
ダイヤラーインタフェース設定モード
トンネルインタフェース設定モード

ip nat outside destination

そのインターフェースから送信するパケットの宛先アドレスの変換ルールを設定します。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（スタティック登録）　192.168.0.1 宛で受信したら 158.xxx.xxx.2 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside destination static  192.168.0.1 158.xxx.xxx.2
```

【解説】
ip nat outside destination static <変換前の宛先アドレス> <変換後の宛先アドレス>
となります。

設定例２　NAT+変換（スタティック登録）　158.xxx.xxx.2:ポート番号 1500 で受信したら、192.168.0.1:ポート番号 80 に変換する

```
Router(config)#access-list 1 permit 158.xxx.xxx..2
Router(config)#ip nat pool pl-1 192.168.0.1 192.168.0.1
Router(config)#
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside destination list 1 1500 pool pl-1 80
```

【解説】
ip nat outside destination static <変換前の宛先アドレス　ポート番号> <変換後の宛先アドレス　ポート番号>
となります。

設定例３　NAT 変換（一括変換）158.xxx.xxx.xxx.0/24⇔192.168.100.0/24 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside destination static-subnet 158.xxx.xxx.xxx.0 192.168.100.0
255.255.255.0
```

【解説】
ip nat outside destination static-subnet <変換前のネットワークアドレス> <変換後のネットワークアドレス> <サブネットマスク>となります。
グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。
NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます（複数同時登録）。

例）local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0

192.168.100.1 ⇔ 158.xxx.xxx.1
: :
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT スタティック（複数指定）時】
ip nat outside destination list <access-list 番号> [変換前開始ポート番号 [変換前終了ポート番号]] pool <プール名> [変換後ポート番号]

【NAT スタティック（1 対 1 変換）、NAT+スタティック時】
ip nat outside destination static <変換前のアドレス> <変換後のアドレス>

【NAT スタティック（一括変換）】
ip nat outside destination static-subnet <変換前のネットワークアドレス> <変換後のネットワークアドレス> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前のアドレス範囲を指定したアクセスリストを指定します。	1～99 1300～1399 10000～11200	省略不可
変換前のアドレス	変換前の宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
開始ポート番号 終了ポート番号	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	ポート変換しない
プール名	変換後のアドレス範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	省略不可
変換後のアドレス	変換後の宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
ポート番号	変換後の TCP/UDP ポート番号を指定します。	1～65535	ポート変換しない
変換前のネットワークアドレス	変換前の宛先ネットワークアドレスを指定します。 static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
変換後のネットワークアドレス	変換後の宛先ネットワークアドレスを指定します。 static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ：スタティック 5000 エントリ、リスト 128 エントリ
送信パケットに対する NAT(ip nat inside source＋ip nat outside destination)の合計となります。

この設定を行わない場合

アドレス変換は行いません。

適用順序

NAT 変換ルールは以下の順序で適用されます。

1）static 変換ルール
2）list による変換ルール

同じ種類のルール内では、Prefix 長が長いルールが優先して適用されます。
同一 Prefix 長の設定が複数あった場合には、config 上で先に登録されたものが優先されます。
なお、config には、以下の順に登録され、同じ種類については入力順に登録されます。

1）static 変換ルール（既存のホストアドレス指定）
2）static-subnet 変換ルール
3）list による変換ルール

IPsec インタフェースで NAT を使用する上での注意事項 ※V01.03(00)以降サポート

・VPN-NAT と、IPsec インタフェースでの NAT の、それぞれ設定に不整合がない場合は、
　IPsec インタフェースの NAT が有効となり、VPN-NAT は無効となります。
・IPsec インタフェースの動的割り当てには対応していません。
　IKEv1: mode-config
　IKEv2: Configuration-Payload
・IPsec インタフェースで NAT 変換する場合でも、該当 SA のセレクタ交換時に使用する
　Phase2-ID は、自動的に変換しません。NAT 変換後のアドレスでセレクタ交換しなくて
　はいけないケースでは、set security-association ipsec-src-id コマンドを利用してください。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
IPsec インタフェース設定モード
ダイヤラーインタフェース設定モード
トンネルインタフェース設定モード

ip nat pool

NAT 変換する際の、変換後の IP アドレス範囲を指定します。NAT 変換(NAT+ではない)する場合に指定する必要があります。
このコマンドでは、プール名称・変換後の IP アドレス範囲(Start/End)を指定し、実際に NAT 変換するインタフェースで、使用するプール名を指定します。

ここで指定する範囲と、実際に NAT 変換するインタフェースの IP アドレスが重複している場合は、NAT 変換できません。refresh コマンド後に有効になるコマンドです。

refresh コマンド後に有効になるコマンドです。

設定例 1　変換後のアドレスとして、158.xxx.xxx.2～158.xxx.xxx.7 を指定する（プール名：pool1）

```
Router(config)#ip nat pool pool1 158.xxx.xxx.2 158.xxx.xxx.7
```

コマンド書式

ip nat pool〈プール名〉〈変換後のアドレス：先頭〉〈変換後のアドレス：最後〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プール名	プールの名称を指定します。 NAT 変換するインタフェースの設定モードで、NAT のコマンドを設定する場合に指定するプール名として使用しますので、わかりやすい名称にしてください。	16 文字以内の文字列	省略不可
変換後のアドレス:先頭	NAT 変換における、変換後のアドレスを範囲指定する場合の先頭アドレス	IPv4 アドレス形式	省略不可
変換後のアドレス:最後	NAT 変換における、変換後のアドレスを範囲指定する場合の最後のアドレス	IPv4 アドレス形式	省略不可

最大エントリ:8 エントリ

NAT 機能とは・・・

LAN 側にローカルアドレスを割り当てている場合、そのままのアドレスでは公共のネットワーク(インターネット等)に接続することはできません。
このような場合に、ローカルアドレスをグローバルアドレスに変換して、インターネットに接続できるようにする機能が NAT(Network Address Translation)です。
複数のアドレスに変換する機能を NAT 機能、1つのアドレスに集約する機能を NAT+機能と呼んでいます。

他のコマンドとの連携

NAT 機能を使用するインタフェースで、NAT 機能の設定(ip nat inside コマンド)を行なう必要があります。
その際、NAT 変換後のアドレスとして、ip nat pool コマンドで指定したプール名を指定します。

適用順序

NAT 変換ルールは以下の順序で適用されます。

1)static 変換ルール
2)list による変換ルール

同じ種類のルール内では、Prefix 長が長いルールが優先して適用されます。
同一 Prefix 長の設定が複数あった場合には、config 上で先に登録されたものが優先されます。
なお、config には、以下の順に登録され、同じ種類については入力順に登録されます。

1)static 変換ルール(既存のホストアドレス指定)
2)static-subnet 変換ルール
3)list による変換ルール

設定モード

基本設定モード

DHCP サーバ機能

DHCP サーバ機能

allocate-address

割り当て開始アドレスの先頭値(DHCP アロケート開始アドレス)、割り当て可能な IP アドレスの個数(DHCP アロケート数)を設定します。
0.0.0.0 を指定した場合は、ホストアドレスの先頭から割り当てます。
設定行(アドレスブロック)は最大 10 エントリです。
複数エントリを設定した場合は IP アドレスでソートされます。
最大払い出し IP アドレスの数はインタフェース毎で 2000、装置全体で 2048 となります。

設定例 1　192.168.0.1 から 254 個分のアドレスを配布する

```
Router(config)#ip dhcp pool lan 1
Router(config-dhcp-pool)#allocate-address 192.168.0.1 254
```

コマンド書式

allocate-address <IP アドレス> <アロケート数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	DHCP で通知する IP アドレスの割り当て開始アドレス	IPv4 アドレス形式	省略不可
アロケート数	割り当て可能な IP アドレスの個数	1～2000	255

※　パラメータ アロケート数 1～2000 は、V01.05(00)以降サポート

この設定を行わない場合

先頭値:0.0.0.0、アロケート数:255 で動作します。

設定モード

DHCP サーバ設定モード

default-router

デフォルトゲートウェイの IP アドレスを設定します。
但し、0.0.0.0 を設定した場合は、LAN の IP アドレスをデフォルトルータとして広告します。

設定例 1　デフォルトゲートウェイの IP アドレスに 10.0.0.1 を広告する

```
Router(config)#ip dhcp pool lan 1
Router(config-dhcp-pool)#default-router 10.0.0.1
```

コマンド書式

default-router 〈IP アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	DHCP で通知するデフォルトゲートウェイの IP アドレス	IPv4 アドレス形式	省略不可

この設定を行わない場合

DHCP でデフォルトゲートウェイの情報を通知しません。

デフォルトゲートウェイとは？

ルーティングテーブルにない宛先のパケットを送信する場合に、中継先としてパケットを送信するノードを、デフォルトゲートウェイといいます。
通常、パソコンはルーティングテーブルを持っていませんので、異なるサブネット宛の全てのパケットを、デフォルトゲートウェイに送ります。

言い方を替えると、デフォルトゲートウェイが設定されていないパソコンは、(ほとんど)ネットワーク機能を利用できないことになります。

設定モード

DHCP サーバ設定モード

dns-server

DNS サーバの IP アドレスを設定します。最大2件まで設定でき、DHCP で広告します。

設定例１　プライマリ DNS サーバに 192.168.1.100、セカンダリ DNS サーバに 192.168.1.101 を設定する

```
Router(config)#ip dhcp pool lan 1
Router(config-dhcp-pool)#dns-server 192.168.1.100 192.168.1.101
```

コマンド書式

dns-server 〈プライマリ DNS アドレス〉〈セカンダリ DNS アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プライマリ DNS アドレス	DHCP で通知するプライマリ DNS サーバの IP アドレス	IPv4 アドレス形式	省略不可
セカンダリ DNS アドレス	DHCP で通知するセカンダリ DNS サーバの IP アドレス	IPv4 アドレス形式	セカンダリ DNS を使用しない

この設定を行わない場合

DHCP で DNS サーバの情報を通知しません。

DNS サーバとは？

DNS は Domain Name System の略で、ホスト名から IP アドレス（またはその逆）を探し出すシステムのことです。
このシステムのために、ホスト名と IP アドレスの組み合わせデータベースが存在し、そのデータベースをもつホストのことを、DNS サーバといいます。

DNS サーバは、世界中のホストと IP アドレスの組み合わせデータベースを持っているわけではなく、自分の属するドメインの組み合わせのみを保有し、わからないホスト名のリクエストを受けた場合は、他の DNS サーバに問い合わせるという仕組みを持っています。

設定モード

DHCP サーバ設定モード

domain-name

ドメイン名を設定します。

設定例１　DHCP で配布するドメイン名に"abc.com"を指定する

```
Router(config)#ip dhcp pool lan 1
Router(config-dhcp-pool)#domain-name abc.com
```

コマンド書式

domain-name <ドメイン名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ドメイン名	DHCP で通知するドメイン名称	39 文字以内の文字列	省略不可

この設定を行わない場合

DHCP でドメイン名を通知しません。

設定モード

DHCP サーバ設定モード

hosttable

DHCP サーバ機能で配布する IP アドレスを端末に対して固定値を割り付けるために、端末の MAC アドレスと配布する IP アドレスの組み合わせを登録します。

設定例 1　MAC アドレス 00:80:bd:f0:01:23 のホストには、10.0.0.1 を割り当てる

```
Router(config)#ip dhcp pool lan 1
Router(config-dhcp-pool)#hosttable 10.0.0.1 0080.bdf0.0123
```

コマンド書式

hosttable <IP アドレス> <MAC アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	DHCP で割り当てる IP アドレス	IPv4 アドレス形式	省略不可
MAC アドレス	DHCP で割り当てるホストの MAC アドレス	MAC アドレス形式	省略不可

この設定を行わない場合

固定的に IP アドレスを割り当てることはできません。

有効エントリ数

16 エントリ

設定モード

DHCP サーバ設定モード

ip dhcp pool

DHCP サーバ設定モードに移行します。
本装置を DHCP サーバとして使用する場合には設定が必要です。

DHCP サーバ機能と、DHCP リレーエージェント機能は共存できません。両方の設定がされている場合は、DHCP リレーエージェント機能が採用されます。

設定例　LAN インタフェースで DHCP サーバ機能を使用するために、DHCP サーバ設定モードに移行する

```
Router(config)#ip dhcp pool lan 1
Router(config-dhcp-pool)#
```

コマンド書式

ip dhcp pool〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	DHCP サーバ機能を使用するインタフェースを指定します。	lan 1 ewan 1～2 vlanif 1～150	省略不可

この設定を行わない場合

DHCP サーバ機能を使用できません。

DHCP サーバ機能とは？

DHCP サーバ機能とは、DHCP(Dynamic Host Configuration Protocol)を使用して、LAN 上の端末(PC)に IP アドレスなどの情報を割り当てる機能です。
本装置の DHCP サーバ機能では、以下の情報を通知することができます。
・IP アドレス／サブネットマスク
・DNS サーバの IP アドレス
・デフォルトゲートウェイの IP アドレス
・ドメイン名

本装置では、DHCP リレーエージェント機能もサポートしています。DHCP リレーエージェント機能は、自身がサーバになるのではなく、外部の DHCP サーバに問い合わせしなおす機能です。双方の設定がされている場合、DHCP リレーエージェント機能が有効になります。

設定モード

基本設定モード

lease

配布する IP アドレスの有効期限を設定します。有効期限は「日」「時間」「分」もしくは「無限（infinite）」で指定します。
no 指定すると、設定を削除し、デフォルト設定値に戻します。

設定例１　リース期限を１日と１１時間２２分に設定する

```
Router(config)#ip dhcp pool lan 1
Router(config-dhcp-pool)#lease 1 11 22
```

設定例２　リース期限を無限に設定する

```
Router(config)#ip dhcp pool lan 1
Router(config-dhcp-pool)#lease infinite
```

コマンド書式

lease〈日〉〈時間〉〈分〉
　もしくは
lease infinite

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
日	DHCP で割り当てる期限（日）	0～365	省略不可
時間	DHCP で割り当てる期限（時間）	0～23	0（ただし分を設定する場合は省略不可）
分	DHCP で割り当てる期限（分）	0～59	0

パラメータ	設定内容	設定範囲	省略時の値
Infinite	DHCP で割り当てる期限を無限とする	infinite	省略不可

この設定を行わない場合

infinite となります。

設定モード

DHCP サーバ設定モード

netbios-name-server

NetBIOS サーバの IP アドレスを設定します。最大2件まで設定でき、DHCP で広告します。

設定例 1　プライマリ NetBIOS サーバに 192.168.1.200、セカンダリ NetBIOS サーバに 192.168.1.201 を設定する

```
Router(config)#ip dhcp pool lan 1
Router(config-dhcp-pool)#netbios-name-server 192.168.1.200 192.168.1.201
```

コマンド書式

netbios-name-server 〈プライマリ NetBIOS サーバアドレス〉〈セカンダリ NetBIOS サーバアドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プライマリ NetBIOS サーバアドレス	DHCP で通知するプライマリ NetBIOS サーバの IP アドレス	IPv4 アドレス形式	省略不可
セカンダリ NetBIOS サーバアドレス	DHCP で通知するセカンダリ NetBIOS サーバの IP アドレス	IPv4 アドレス形式	セカンダリ NetBIOS サーバを使用しない

この設定を行わない場合

DHCP で NetBIOS サーバを通知しません。

設定モード

DHCP サーバ設定モード

option hex

本設定により、任意の DHCP 標準オプションの送信を行うことができます。
hex の後に 16 進数で任意の文字列を指定することができます。

設定例 1　X Window システムの Display Manager オプション（49）として、IP アドレス 192.168.1.1 を通知する

```
Router(config)#ip dhcp pool lan 1
Router(config-dhcp-pool)#option 49 hex c0a80101
```

コマンド書式

option 〈オプションコード〉 hex 〈オプション内容〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
オプションコード	送信するオプションコードを指定します。 4 エントリ以上指定した場合は、オプションコードの小さい順に 4 エントリが有効になります。	1～254	省略不可
オプション内容	送信する文字列を 16 進数で指定します。 全てのオプション値の合計長が 312 文字を超えた場合は、254 文字以内であっても超えたオプションは無効となります。	最大 254 文字の英数字	省略不可

この設定を行わない場合

任意のオプションは送信されません。

設定モード

DHCP サーバ設定モード

search-address

割り当て可能アドレスを立ち上がり時に調べる時の調査用の ARP に関する以下の項目を設定します。
通常の運用形態では、変更の必要はありません。

設定例１　ARP 送信回数（１回）、タイムアウト値（１秒）、アドレス検索パケット数（１６）に設定する

```
Router(config)#ip dhcp pool lan 1
Router(config-dhcp-pool)#search-address 1 10 16
```

コマンド書式

search-address〈ARP 送信回数〉〈タイムアウト値〉〈アドレス検索パケット数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ARP 送信回数	ARP を送信する回数	1～255	省略不可
タイムアウト値	割り当て可能とするためのタイムアウト値（単位 100m 秒）	1～255	省略不可
アドレス検索パケット数	1 回の検索で送信する ARP パケット数	0～255	省略不可

この設定を行わない場合

以下で動作します。

タイマの内容	値
ARP を送信する回数	1
割り当て可能とするためのタイムアウト値（単位 100m 秒）	10
アドレス検索パケット数	16

設定モード

DHCP サーバ設定モード

service dhcp-server

DHCP サーバ機能を利用する場合に指定します。

設定例 1　DHCP サーバ機能を使用する

```
Router(config)# service dhcp-server
```

コマンド書式

service dhcp-server

パラメータ

パラメータはありません。

この設定を行わない場合

DHCP サーバ機能を使用できません。

DHCP サーバ機能とは？

DHCP サーバ機能とは、DHCP(Dynamic Host Configuration Protocol)を使用して、LAN 上の端末(PC)に IP アドレスなどの情報を割り当てる機能です。
本装置の DHCP サーバ機能では、以下の情報を通知することができます。

- IP アドレス／サブネットマスク
- DNS サーバの IP アドレス
- デフォルトゲートウェイの IP アドレス
- ドメイン名

本装置では、DHCP リレーエージェント機能もサポートしています。DHCP リレーエージェント機能は、自身がサーバになるのではなく、外部の DHCP サーバに問い合わせしなおす機能です。双方の設定がされている場合、DHCP リレーエージェント機能が有効になります。

設定モード

基本設定モード

DHCP リレーエージェント機能

DHCP リレーエージェント機能

ip dhcp relay maxhops

DHCP リレーエージェント機能を使用する場合に、何段先までのサーバまでアクセスを許可するかを指定します。

設定例 1　DHCP サーバまでの許容段数を 10 とする

```
Router(config)#ip dhcp relay maxhops 10
```

コマンド書式

ip dhcp relay maxhops <HOP 数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
HOP 数	何段先までのサーバまでアクセスを許可するか	1～16	省略不可

この設定を行わない場合

4 段が設定されます。

DHCP リレーエージェント機能とは？

LAN 上の DHCP クライアントからの要求を、WAN 側にリレーし、WAN 側の DHCP サーバから割り当ててもらう機能です。
本社側で、支店の LAN 側の IP アドレスを一括で管理する場合に有効な機能です。

設定モード

基本設定モード

ip helper-address

本装置で、DHCP リレーエージェント機能を使用する際、リレー先の DHCP サーバを登録します。
本装置では、最大4つまでの DHCP サーバを登録できます。

設定例 1　DHCP リレーエージェント機能で問い合わせる DHCP サーバに 192.168.100.1 を設定する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip helper-address 192.168.100.1
```

コマンド書式

ip helper-address <DHCP サーバの IP アドレス> [source-interface <インタフェース名>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DHCP サーバの IP アドレス	DHCP リレーエージェント機能でリレーする際の、リレー先 DHCP サーバの IP アドレスを指定します。 CLI 上は、5 エントリ以上入力できますが、有効になるのは、アドレスの若い順に 4 エントリ迄です。	IPv4 アドレス形式	省略不可
インタフェース名	DHCP リレーする際の送信元アドレスに使用するインタフェースアドレス	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 loopback 1～100 vlanif 1～150	実際に送信するインタフェース

この設定を行わない場合

DHCP リレーエージェント機能を使用できません。

設定モード

LAN インタフェース設定モード
VLAN インタフェース設定モード

service dhcp-relayagent

DHCP リレーエージェント機能を利用する場合に指定します。
DHCP リレーエージェント機能を使用する場合、DHCP パケットをリレーするインタフェース(DHCP サーバへの中継方向)で NAT 機能を使用することは出来ません。

設定例 1　DHCP リレーエージェント機能を使用する

```
Router(config)# service dhcp-relayagent
```

コマンド書式

```
service dhcp-relayagent
```

パラメータ

パラメータはありません。

この設定を行わない場合

DHCP リレーエージェント機能を使用できません。

DHCP リレーエージェント機能とは

LAN 上の DHCP クライアントからの要求を、WAN 側にリレーし、WAN 側の DHCP サーバから割り当ててもらう機能です。
本社側で、支店の LAN 側の IP アドレスを一括で管理する場合に有効な機能です。

設定モード

基本設定モード

簡易 DNS 機能

簡易 DNS 機能の設定

proxydns default domain-name

proxyDNS 機能で、上流の DNS サーバに問い合わせる際につけるドメイン名を指定します。
LAN 側からの DNS のリクエスト(Query)にドメイン名がついていなかった場合、ここで設定したドメイン名をつけてサーバに問い合わせます。

設定例 1　ドメイン名に furukawa.co.jp を設定する

```
Router(config)# proxydns default domain-name furukawa.co.jp
```

コマンド書式

proxydns default domain-name <ドメイン名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ドメイン名	DNS のリクエストにドメイン名がついていなかった場合につけるドメイン名	-	省略不可

この設定を行わない場合

ProxyDNS 使用時に、ドメイン名を省略することはできません。

設定モード

基本設定モード

proxydns default name-server

ProxyDNS 機能を使用する場合の、DNS サーバの IP アドレスを指定します。
また、PPPoE／DHCP により、DNS アドレスを学習している場合であっても、本コマンドによる設定が優先されます。
IPv4 用の DNS サーバ／IPv6 用の DNS サーバを登録します。
アドレスを連続して入力する事により、プライマリ、セカンダリの順で DNS サーバを設定します。別のアドレスを入力すると以前入力したアドレスに上書きされます。セカンダリーのみ変更したい場合は、設定されているプライマリアドレスの後に続けて、新たにセカンダリアドレスを入力してください。

設定例１　IP v 4 用の DNS サーバに、プライマリ：192.168.200.1／セカンダリ：192.168.200.10 を設定する

```
Router(config)# proxydns default name-server v4 192.168.200.1 192.168.200.10
```

設定例２　IPv6 用の DNS サーバに、プライマリ：2003:113::1／セカンダリ：2003:113::2 を設定する

```
Router(config)# proxydns default name-server v6 2003:113::1 2003:113::2
```

コマンド書式

proxydns default name-server { v4 | v6 } <プライマリ DNS アドレス> [セカンダリ DNS アドレス]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
v4|v6	DNS サーバの属性（IPv4 用（A レコード） or IPv6 用（AAAA レコード））を指定	v4 or v6	省略不可
プライマリ DNS アドレス	ProxyDNS で使用するプライマリ DNS サーバの IP アドレス	IPv4 アドレス形式 もしくは IPv6 アドレス形式	省略不可
セカンダリ DNS アドレス	ProxyDNS で使用するセカンダリ DNS サーバの IP アドレス	IPv4 アドレス形式 もしくは IPv6 アドレス形式	セカンダリ DNS を使用しない

この設定を行わない場合

ProxyDNS 機能を使用できません。ただし、PPPoE や DHCP クライアント機能で、DNS の IP アドレスを学習している場合は、ProxyDNS 機能を使用できます。

設定モード

基本設定モード

proxydns default retrans-time

問い合わせパケットを中継し、それに対する応答待ち時間を設定します。
応答待ち時間経過しても応答がない場合は、再送します。

設定例 1　ProxyDNS の応答待ち時間を 5 秒に設定する

```
Router(config)# proxydns default retrans-time 5
```

コマンド書式

proxydns default retrans-time <応答待ち時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
応答待ち時間	DNS サーバからの応答を待つ時間(秒)	1～10	省略不可

この設定を行わない場合

3 秒となります。

設定モード

基本設定モード

proxydns default retry

応答パケットタイムアウトに対する再送回数を設定します。

設定例 1　ProxyDNS 機能の再送を 3 回とする

```
Router(config)# proxydns default retry 3
```

コマンド書式

proxydns default retry <リトライ回数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リトライ回数	DNS サーバからの応答がない場合のリトライ回数	0～10	省略不可

この設定を行わない場合

2 回となります。

設定モード

基本設定モード

proxydns default cache-time

LAN 側の端末から DNS のリクエストを受信し、proxyDNS 機能により解決した情報について、内部のテーブルに保持しておく時間を設定します。
学習した DNS 情報について、ここで指定した時間リクエストを受信しなかった場合は、該当 DNS 情報を削除します。

設定例 1　PxoxyDNS のテーブルの保持時間を 60 分に設定する

```
Router(config)# proxydns default cache-time 3600
```

コマンド書式

proxydns default cache-time <キャッシュ時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キャッシュ時間	ProxyDNS のテーブル保持時間(秒)を設定します。off を指定すると保持しません。	0～259200 off	省略不可

※ キャッシュ時間に、0 秒を指定すると学習した DNS 情報を保持し続けます。
off を指定した場合は、必ず DNS サーバに問い合わせを行ないます。

この設定を行わない場合

86400 秒となります。

設定モード

基本設定モード

proxydns default source-interface

ProxyDNS 機能により、上位の DNS サーバに名前解決のパケットを送出する際の、送信元 IP アドレスとして使用するインタフェース名を指定します。

設定例１　送信元アドレスに LAN を指定する。

```
Router(config)# proxydns default source-interface lan 1
```

コマンド書式

proxydns default source-interface〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	送信元アドレスとして指定するインタフェース	lan 1 ewan 1～2 loopback 1～100 vlanif 1～150	省略不可

この設定を行わない場合

実際にパケットを送信するインタフェースの IP アドレスになります。

設定モード

基本設定モード

proxydns mode

本装置の簡易 DNS 機能を使用するプロトコル(IPv4 or IPv6)を指定します。
双方を使用する場合は"both"を指定します。

設定例１　IPｖ4、IPv6 パケットによるリクエストに対して簡易 DNS 機能を使用する

```
Router(config)# proxydns mode both
```

設定例２　IPv4 パケットによるリクエストに対して簡易 DNS 機能を使用する

```
Router(config)# proxydns mode v4
```

コマンド書式

proxydns mode <プロトコル>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プロトコル	本装置の簡易 DNS 機能に対して問合せを行なう際に使用するプロトコルを指定します。 v4：IPv4 パケットによる name のリクエストに対して、代理要求/応答をする v6：IPv6 パケットによる name のリクエストに対して、代理要求/応答をする both：IPv4／IPv6 の両方のパケットでの nmae のリクエストに対して、代理要求/応答をする	v4 v6 both	省略不可

この設定を行わない場合

ProxyDNS 機能を使用できません。

設定モード

基本設定モード

ドメイン名による DNS 振り分け

proxydns domain

ドメイン名称とそのドメイン名称に対応する DNS IP アドレスを登録します。
別のアドレスを入力すると以前入力したアドレスに上書きされます。

設定例 1　furukawa.co.jp ドメイン宛の DNS リクエストは、192.168.200.1 もしくは 2003:113::c0a8:c801 に問い合わせる

```
Router(config)# proxydns domain furukawa.co.jp v4 192.168.200.1
Router(config)# proxydns domain furukawa.co.jp v6 2003:113::c0a8:c801
```

コマンド書式

proxydns domain <ドメイン名> <プロトコル> <プライマリ DNS> [セカンダリ DNS]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ドメイン名	DNS リクエストのドメイン名を設定します。	最大 64 文字の英数字	省略不可
プロトコル	IPv4 アドレスで DNS サーバを指定する場合には v4 を使用し、IPv6 アドレスで DNS サーバを指定する場合には v6 を使用します。	v4 v6	省略不可
プライマリ DNS	プライマリ DNS サーバの IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
セカンダリ DNS	セカンダリ DNS サーバの IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	セカンダリ DNS に問い合わせを行いません。

最大エントリ数:8 エントリ

この設定を行わない場合

どのようなリクエストでも、全て固定の DNS サーバに問い合わせます。

設定モード

基本設定モード

ホスト名称と DNS IP アドレスの登録

proxydns hosts

ホスト名称と IP アドレスの組み合わせを登録することができます。本装置に DNS 要求が来た場合、このリストを参照して応答します。

設定例 1　host.furukawa.co.jp の IPv4 アドレスを 192.168.100.1／IPv6 アドレスを 2003:113::c0a8:6401 に設定する

```
Router(config)# proxydns hosts host.furukawa.co.jp v4 192.168.100.1
Router(config)# proxydns hosts host.furukawa.co.jp v6 2003:113::c0a8:6401
```

コマンド書式

proxydns hosts〈ホスト名〉〈属性〉〈IP アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ホスト名	ホスト名を指定します。	最大 254 文字の英数字	省略不可
属性	DNS サーバの属性（IPv4 用（A レコード） or IPv6 用（AAAA レコード））を指定を指定します。	v4 v6	省略不可
IP アドレス	DNS のリプライとして送信する IP アドレス（IPv4 アドレスまたは IPv6 アドレス）を指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

最大エントリ数：16 エントリ（キャッシュテーブルの最大数は 64 エントリ）

この設定を行わない場合

ホスト名称とアドレスの組み合わせを持たず、全て DNS システムを使用します。

設定モード

基本設定モード

ダイナミック DNS 機能

サーバ機能

ddns-server accept-fqdn type

ダイナミック DNS サーバ機能を使用時に、受け入れを許可するレコードの内容(FQDN、アドレス種別)と、アクセスパスワード、レコードのライフタイムを設定します。
ここで指定したレコードと異なるダイナミック DNS 要求を受信しても本装置の DNS データベースには反映されません。

なお、ダイナミック DNS サーバ機能を利用する場合には、かならず HTTP サーバ機能および簡易 DNS サーバ機能を動作させるようにしてください。

refresh コマンド後に有効になるコマンドです。

設定例 1　FQDN (host1.furukawa.co.jp) 、受付アドレス種別 : IPv4、アクセスパスワード"pass1"、有効時間を 300 秒とする

```
Router(config)#ddns-server accept-fqdn type v4 host1.furukawa.co.jp password pass1 lifetime 300
Router(config)#
```

コマンド書式

```
ddns-server accept-fqdn type {v4|v6} <FQDN> password <パスワード> |
                                ifetime <有効時間>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
v4|v6	指定する FQDN に対応するアドレスの IP バージョンを指定します。 v4　IPv4 アドレスで指定 v6　IPv6 アドレスで指定	v4 v6	省略不可
FQDN	登録要求を受け付ける FQDN を設定します。	64 文字までの英数字	省略不可
パスワード	アクセスパスワードを設定します。	32 文字までの英数字	省略不可
有効時間	有効時間を設定します。単位:秒	1～86400	省略不可

この設定を行わない場合

ダイナミック DNS サーバ機能は使用できません。

FQDN とは？

FQDN とは、ホスト名.ドメイン名の形式をいいます。

ダイナミック DNS サーバの動作

本装置のダイナミック DNS サーバは、HTTP の GET リクエストを受信し CGI でレコードを登録する動作となります。
CGI プログラム名は、"(V4) cgi-bin/ddns-v4.cgi, (V6) cgi-bin/ddns-v6.cgi"です。
レコードを登録するための CGI パラメータは以下となります。

内容	CGI パラメータ	登録例
FQDN	dn	dn=host1.furukawa.co.jp
IPv4 アドレス	i4	i4=192.168.0.1
IPv6 アドレス	i6	i6=aaaa:bbbb::1
パスワード	pw	pw=pass1

注意１：i4,i6 の両方が存在しない GET リクエストの場合は、HTTP の送信元アドレスを、アドレス情報として登録します。
注意２：i4,i6 の両方が存在する GET リクエストは、エラー(403)となります。

設定モード

基本設定モード

ddns-server enable

ダイナミック DNS サーバ機能を使用する場合に設定します。
ダイナミック DNS サーバ機能を利用する場合には、かならず HTTP サーバ機能および簡易 DNS サーバ機能を動作させるようにしてください。

refresh コマンド後に有効になるコマンドです。

設定例 1　ダイナミック DNS サーバ機能を有効にする

```
Router(config)#ddns-server enable
Router(config)#
```

コマンド書式

```
ddns-server enable
```

パラメータ

パラメータはありません。

この設定を行わない場合

ダイナミック DNS サーバ機能を使用できません。

設定モード

基本設定モード

ddns-server logging address-changes

ダイナミック DNS サーバ機能を利用時、同じ FQDN に対して、アドレスの変更があったことをログ(slog)に出力する場合に、本コマンドを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　登録アドレス変更ログを出力する

```
Router(config)#ddns-server logging address-changes
Router(config)#
```

コマンド書式

```
ddns-server logging address-changes
```

パラメータ

パラメータはありません。

この設定を行わない場合

登録アドレス変更ログを出力しません。

設定モード

基本設定モード

クライアント機能(ダイナミック DNS 動作の設定)

ddns-client

ダイナミック DNS クライアントが、登録要求メッセージを送信するイベントと送信内容の設定を行います。
設定 I/F モードの IPv4/IPv6 アドレスの変化毎に実行する http-client 設定を選択します。
また、I/F アドレス状態変化の判断に一定の間隔を設ける遅延処理の設定及び、一定期間イベントが発生しない場合の定期送信を行うこともできます。

refresh コマンド後に有効になるコマンドです。

設定例 1　LAN インタフェースの Ipv4 アドレス状態変化時に、http-client モード 1 に登録したメッセージを送信

```
Router(config)#interface lan 1
Router(config-if lan 1)#ddns-client address ip action http-client 1
```

コマンド書式

```
ddns-client　{ address { ip | ipv6 }} action http-client <http-client モード>
　　[ delay <遅延処理設定> ] [ interval <定期送信間隔> ]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
address { ip | ipv6 }	登録要求メッセージを設定 I/F の IPv4 アドレス変化、または IPv6 アドレス変化のどちらで送信するかを指定します。 IPv4 アドレス変化時に送信する場合：address ip IPv6 アドレス変化時に送信する場合：address ipv6	address ip address ipv6	省略不可
http-client モード	送信する登録要求メッセージを選択します	1～16	省略不可
遅延処理設定	I/F アドレス状態変化の判断に一定の間隔を設ける場合に指定します。単位：秒	0～60	5 秒
定期処理間隔	一定期間、I/F アドレス状態変化が起きない場合に定期送信する場合に指定します。単位：秒	10～86400	定期送信を行いません。

この設定を行わない場合

I/F アドレスの状態変化時にメッセージを送信しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード

クライアント機能（HTTP クライアントに関する設定）

description

http-client の Description を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　http-client の Description を HTTP-CLIENT1 とする

```
Router(config)#http-client 1
Router(http-client 1)#description HTTP-CLIENT1
```

コマンド書式

description <文字>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
文字	http-client の Description を設定します。	半角英数字、記号※1	省略不可

※1 連続 254 文字まで、スペースで区切ることにより 2033 文字まで入力可能です。
ただし、show コマンド(コンフィグの表示を除く※2)で表示される文字数は、最初の 254 文字までとなります。
※2 コンフィグの表示では、2033 文字まで表示されます。

この設定を行わない場合

http-client の Description を設定しません。

設定モード

HTTP クライアント設定モード

logging

HTTP クライアントの動作において、出力するログの種別を、以下のなかから選択します。
・ログを出力しない
・エラー時のみログを出力する
・エラー時だけでなく、成功時にもログを出力する

refresh コマンド後に有効になるコマンドです。

設定例１　全てのログを出力する

```
Router(config)#http-client 1
Router(http-client 1)#logging detailed
```

コマンド書式

logging〈ログ出力レベル〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ログ出力レベル	ログ出力レベルを設定し出力ログを選択します。 detailed　全てのログを出力 error　エラーログのみ出力 none　ログを出力しません	detailed error none	省略不可

この設定を行わない場合

エラーログのみ出力します。

設定モード

HTTP クライアント設定モード

method

HTTP の Request-Line を指定します。HTTP の Request-Line は、以下の書式となります。
メソッド Request-URI HTTP バージョン
本装置の HTTP クライアントでは、メソッドは GET のみ指定可となります。Request-URI は、URL と CGI オプションの指定となります。
HTTP バージョンは 1.0 固定となります。

Request-URI の指定方法は、以下のとおりです。
FITELnet のダイナミック DNS サーバ宛に送信する場合は、IPv4 アドレスであれば ddns-v4.cgi、IPv6 アドレスであれば ddns-v6.cgi を指定してください。
Request-URL <CGI オプション 1> <CGI オプション値 1> <CGI オプション 2> <CGI オプション値 2> ・・・
たとえば、http://192.168.0.1/cgi-bin/ddns-v4.cgi に、dn=abc.co.jp, pw=pass1 を送りたい場合は、以下のような指定になります。
http://192.168.0.1/cgi-bin/ddns-v4.cgi dn abc.co.jp pw pass1

また、通知したいアドレスが PPPoE のような不定アドレスのケースでは、アドレス情報としてマクロ登録を行います。
FITELnet でサポートしているマクロ登録は、以下の 2 つです。
$i4・・IPv4 アドレス
$i6・・IPv6 アドレス
$sn・・装置のシリアル番号
どのインタフェースのアドレスを通知するかは、reference-interface コマンドで設定します。

ベーシック認証サーバにアクセスする場合は、"ユーザ名":"パスワード"@ホストの順に入力してください。

refresh コマンド後に有効になるコマンドです。

設定例 1 http://192.168.0.1/cgi-bin/ddns-v4.cgi に、i4=pppoe 1 の IPv4 アドレス dn=abc.co.jp, pw=pass1 を送る

```
Router(config)#http-client 1
Router(http-client 1)#method 1 get url http://192.168.0.1/cgi-bin/ddns-v4.cgi dn abc.co.jp i4 $i4
pw pass1
Router(http-client 1)#reference-interface pppoe 1
```

設定例 2 http://192.168.1.1/cgi-bin/ddns-v4.cgi に、i6=pppoe 1 の IPv6 アドレス dn=abc.co.jp, pw=pass1 を送る

```
Router(config)#http-client 1
Router(http-client 1)#method 1 get url http://192.168.1.1/cgi-bin/ddns-v4.cgi dn abc.co.jp i6 $i6
pw pass1
Router(http-client 1)#reference-interface pppoe 1
```

設定例３ http://192.168.0.1/cgi-bin/ddns-v4.cgi に、i6=pppoe 1 の IPv4 アドレス dn=abc.co.jp, pw=装置のシリアル番号を送る

```
Router(config)#http-client 1
Router(http-client 1)#method 1 get url http://192.168.0.1/cgi-bin/ddns-v4.cgi dn abc.co.jp i4 $i4
pw $sn
Router(http-client 1)#reference-interface pppoe 1
```

設定例４ ベーシック認証サーバにアクセスする（ユーザ名：furukawa、パスワード：fitelnet）

```
Router(config)#http-client 1
Router(http-client 1)#method 1 get url http://furukawa:fitelnet@192.168.0.1/cgi-bin/ddns-v4.cgi
```

コマンド書式

method 〈番号〉 get url 〈登録要求先〉 [〈CGI オプション〉〈CGI オプション値〉 ・・・]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
番号	シーケンス番号	1～16	省略不可
登録要求先	DDNS サーバの URL を半角で指定します。	1～254	省略不可
〈CGI オプション〉 〈CGI オプション値〉	CGI オプションとその値をスペースで区切って指定します。 この組み合わせは複数指定することができます。	–	引数名、引数を指定しません。

この設定を行わない場合

ダイナミック DNS サーバへ登録要求メッセージを送信しません。

設定モード

HTTP クライアント設定モード

reference-interface

method コマンドで、不定アドレス登録のためにマクロ登録を行った場合に、どのインタフェースの状態を参照するのかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　LAN インタフェースを登録要求メッセージのアドレス（IPv4/IPv6）置換時に参照する

```
Router(config)#http-client 1
Router(http-client 1)#reference-interface lan 1
```

コマンド書式

reference-interface <インタフェース名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	登録要求メッセージのアドレス(IPv4/IPv6)置換時に参照するインターフェース名を指定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 loopback 1～100 vlanif 1～150	省略不可

この設定を行わない場合

インタフェースのアドレスを参照しません。

設定モード

HTTP クライアント設定モード

request-timeout

ダイナミック DNS サーバに対して送信した登録要求メッセージの応答受信待ち許容時間、およびリトライ回数を指定します。
ここで指定した時間応答を受信しなかった場合はリトライを行います。

refresh コマンド後に有効になるコマンドです。

設定例 1　登録要求メッセージの応答受信待ちタイムアウト 10 秒、リトライ回数 2 回に設定

```
Router(config)#http-client 1
Router(http-client 1)#request-timeout 10 retry 2
```

コマンド書式

request-timeout 〈登録要求タイムアウト〉[retry 〈リトライ回数〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
登録要求タイムアウト	ダイナミック DNS サーバに対して送信した登録要求メッセージの応答受信待ちタイムアウト時間を指定します。単位：秒	1～60	省略不可
リトライ回数	ダイナミック DNS サーバに対して送信した登録要求メッセージのリトライ回数を指定します。	0～5	リトライしません。

この設定を行わない場合

登録要求タイムアウト 10 秒、リトライしないに設定されます。

設定モード

HTTP クライアント設定モード

source-interface

登録要求メッセージの送信元アドレスをインターフェース名で設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　LAN インタフェースを登録要求メッセージの送信元アドレスとする

```
Router(config)#http-client 1
Router(http-client 1)#reference-interface lan 1
```

コマンド書式

source-interface 〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	登録要求メッセージの送信元アドレスをインターフェース名で設定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 loopback 1～100 vlanif 1～150	省略不可

この設定を行わない場合

source-interface 指定無しで動作します。

設定モード

HTTP クライアント設定モード

簡易ファイアウォール機能

外部からの接続制御機能

remote-access limitation

パスワードを指定回数以上間違えたときにはアクセス拒否する機能の、パスワード誤りを許可する回数を設定します。0 を指定すると不正アクセス抑制を行わなくなります。

設定例 1　パスワード誤り許容回数を 2 回に設定する

```
Router(config)#remote-access limitation 2
```

コマンド書式

remote-access limitation 〈パスワード誤り許容回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
パスワード誤り許容回数	不正アクセスではないとみなすパスワード誤り許容回数。 この設定上の誤りがあった場合は、不正アクセスとみなし、電子メール通知／ログ出力／アクセス拒否されます。	0～5	省略不可

この設定を行わない場合

3 回となります。
4 回以上パスワードを間違えると、10 分間アクセスが拒否します。

不正アクセスが発覚した場合

不正アクセスが発覚した場合は、以下の制御が行なわれます。

●電子メールによる通知

電子メールにより、管理者宛に、不正アクセスが起こったこと、不正アクセス元の IP アドレス等の情報を通知します。

電子メール通知機能の設定は mail コマンドを使用します。

●ログ出力

slog に『Security Emergency from xxx.xxx.xxx.xxx』(xxx.xxx.xxx.xxx は不正アクセスもとの IP アドレス)と表示します。

syslog の設定がされている場合は、遠隔地の syslog サーバにリアルタイムに通知することもできます。

●アクセス拒否

不正アクセス元からのアクセスを、一定時間アクセスを制限します。アクセス制限時間の設定は remote-access time コマンドで設定します。

設定モード

基本設定モード

remote-access time

パスワードを指定回数以上間違えたときにはアクセス拒否する機能の、アクセス制限時間を設定します。

設定例１　不正アクセス発生時のアクセス制限時間を５分に設定する

```
Router(config)#remote-access time 5
```

コマンド書式

remote-access time〈アクセス制限時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクセス制限時間	不正アクセスの相手に対して、アクセス制限を行なう時間（分）を設定します。	1～60	省略不可

この設定を行わない場合

10 分となります。

不正アクセスが発覚した場合

不正アクセスが発覚した場合は、以下の制御が行なわれます。

●電子メールによる通知

電子メールにより、管理者宛に、不正アクセスが起こったこと、不正アクセス元の IP アドレス等の情報を通知します。

電子メール通知機能の設定は mail コマンドを使用します。

●ログ出力

slog に『Security Emergency from xxx.xxx.xxx.xxx』（xxx.xxx.xxx.xxx は不正アクセスもとの IP アドレス）と表示します。

syslog の設定がされている場合は、遠隔地の syslog サーバにリアルタイムに通知することもできます。

●アクセス拒否

不正アクセス元からのアクセスを、一定時間アクセスを制限します。パスワード誤りの許容回数は remote-access limitation コマンドで設定します。

設定モード

基本設定モード

IP パケットフィルタリング機能

ipv6 access-group

access-list コマンドで指定したフィルタリングデータを、各インタフェースで適用します。
フィルタリングデータは、各インタフェースで受信したパケットに適用するのか、各インタフェースに送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　access-list 3001 で指定したデータを、PPPoE1 送信時に適用する

```
Router(config)#interface pppoe 1
Router(config-if lan 1)#ipv6 access-group 3001 out
```

設定例２　access-list 3002 で指定したデータを、PPPoE1 からの受信時に適用する

```
Router(config)#interface pppoe 1
Router(config-if lan 1)#ipv6 access-group 3002 in
```

コマンド書式

ipv6 access-group <access-list 番号> { in | out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	フィルタリングのデータを設定したアクセスリストの番号を指定します。	3000～3499 3500～3999 30000～31499 35000～36499	省略不可
{in | out}	インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。	in out	省略不可

この設定を行わない場合

該当インタフェースでは、IP パケットフィルタリングを使用しません。

IP フィルタリングについて

指定したパケット以外は中継しないといったように、セキュリティ強化のため使用する機能です。

設定モード

PPPoE インタフェース設定モード
LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
トンネルインタフェース設定モード

ip access-group

access-list コマンドで指定したフィルタリングデータを、各インタフェースで適用します。
フィルタリングデータは、各インタフェースで受信したパケットに適用するのか、送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　access-list 1 で指定したデータを、PPPoE1 送信時に適用する

```
Router(config)#interface pppoe 1
Router(config-if lan 1)#ip access-group 1 out
```

設定例２　access-list 2 で指定したデータを、PPPoE1 からの受信時に適用する

```
Router(config)#interface pppoe 1
Router(config-if lan 1)#ip access-group 2 in
```

コマンド書式

ip access-group <access-list 番号> { in [interface | vpn]| out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	フィルタリングのデータを設定したアクセスリストの番号を指定します。	1～99 100～199 1300～1999 2000～2699 10000～11200 20000～21199	省略不可
{ in[interface | vpn]| out }	インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。 受信時は、さらに以下のように設定ができます。 in vpn：自局宛 VPN 対象パケットを制御 in interface：自局宛非 VPN 対象パケットを制御	in in vpn in interface out	省略不可

LAN インタフェースおよび IPsec インタフェースでは、vpn を選択することはできません。
in vpn および in interface を選択した場合、適用する access-list の宛先は、any とする必要があります。

この設定を行わない場合

該当インタフェースでは、IP パケットフィルタリングを使用しません。

IP フィルタリングについて

指定したパケット以外は中継しないといったように、セキュリティ強化のため使用する機能です。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード
BVI インタフェース設定モード
USB Ethernet インタフェース設定モード

ip stateful max-sessions

学習フィルタリングテーブルの総数を設定します。
ここで設定する総数は、IPv4/IPv6 で使用する学習フィルタリングテーブルの総数となります。
NAT を併用している場合、NAT 変換テーブルのセッション数も併せて拡張してください。

設定例　学習フィルタリングテーブルを 20000 セッション分設定する

```
Router(config)#ip stateful max-sessions 20000
```

コマンド書式

ip stateful max-sessions〈セッション数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セッション数	学習フィルタリングテーブルの最大数を設定します。	2048～65535	省略不可

この設定を行わない場合

2048

設定モード

基本設定モード

MAC アドレスフィルタリング機能

aaa authentication macfilter default group

MAC アドレスの認証を RADIUS サーバで行うインタフェースに、対応付ける Radius サーバグループ名を定義します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　LAN1 インタフェースに、Radius サーバグループ名（Radius-A）の VPN セレクタを対応付ける場合

```
Router(config)#interface lan 1
Router(config-if lan 1)# aaa authentication macfilter default group Radius-A
```

コマンド書式

aaa authentication macfilter default group <Radius サーバグループ名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Radius サーバグループ名	Radius サーバグループの名称を指定します。	最大 16 文字の英数字	省略不可

この設定を行わない場合

MAC アドレスの認証を RADIUS サーバで行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

changeback-time

プライマリサーバへの問い合わせがタイムアウトしてから、問い合わせ順序を再度プライマリサーバへ切り戻すまでの時間(単位:分)を設定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　プライマリサーバへ切り戻すまでの時間を 10 分に設定する

```
Router(config)#aaa group server radius Radius-A
Router(config-sg-radius)#changeback-time 10
```

コマンド書式

changeback-time <切り戻し時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
切り戻し時間	問い合わせ順序を再度プライマリサーバへ切り戻すまでの時間(分)を設定します。 0 分を指定した場合は、切り戻しを行いません。	0～1440	省略不可

この設定を行わない場合

切り戻しを行いません。

設定モード

RADIUS サーバ設定モード

mac access-list

MAC アドレスによるフィルタリングを行う場合の MAC アクセスリストの設定を行います。
使用方法は、まず本コマンドで MAC アドレスを指定した後、mac access-group コマンドで指定した MAC アクセスリスト番号を指定します。
mac access-list は、番号順に適用されます。
また、同じ番号の mac access-list に複数行の設定をした場合は、上の行から適用されます。
EtherType によるフィルタリングの指定も可能です。

refresh コマンド後に有効になるコマンドです。

MAC アクセスリスト番号について

本装置の MAC アクセスリスト番号は、以下の規定があります。

MAC アクセスリスト番号	名称	設定内容
1～10240	MAC アクセスリスト標準設定 フィルタリングで使用	送信元 MAC アドレス指定
20000～20199	MAC アクセスリスト拡張設定 フィルタリングで使用	送信元 MAC アドレス指定 EtherType 指定
30000～30199	MAC アクセスリスト拡張設定 QoS で使用	送信元 MAC アドレス指定 宛先 MAC アドレス指定 EtherType 指定

設定例１　MAC アクセスリストに、MAC アドレス 1122.3344.5566 を許可属性として設定する

```
Router(config)# mac access-list 1 permit 1122.3344.5566
```

設定例２　MAC アクセスリストに、全ての MAC アドレスを不許可属性として設定する

```
Router(config)# mac access-list 1 deny any
```

設定例３　MAC アクセスリストで、PPPoE フレームを許可する

```
Router(config)# mac access-list 20000 permit any ethertype pppoe-discovery
Router(config)# mac access-list 20000 permit any ethertype pppoe-session
Router(config)# mac access-list 20000 deny any
```

設定例４　MAC アクセスリストに、送信元 MAC アドレス；全て／宛先 MAC アドレス：1122.3344.0000～1122.3344.ffff を許可属性として設定する

```
Router(config)# mac access-list 30000 permit any 1122.3344.0000 ffff.ffff.0000
```

コマンド書式

```
mac access-list <mac access-list 番号> remark<コメント>
mac access-list <mac access-list 番号> permit <MAC アドレス> [log] [count]
mac access-list <mac access-list 番号> deny {<MAC アドレス>|any} [log] [count]
mac access-list <mac access-list 番号> {permit|deny} <any> ethertype <フィル
                                       タリング対象>] [log] [count]
mac access-list <mac access-list 番号> {permit|deny} {any|host <送信元 MAC ア
                ドレス>|<送信元 MAC アドレス> <送信元 MAC アドレス範囲>} {any|
                host <宛先 MAC アドレス>|<宛先 MAC アドレス> <宛先 MAC アドレス
                範囲>} [ethertype <フィルタリング対象>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
mac access-list 番号	設定する MAC アクセスリスト番号を指定します。	1～10240 20000～20199 30000～30199	省略不可
permit	設定する MAC アクセスリストに許可属性を与える場合に指定します。	permit	省略不可
deny	設定する MAC アクセスリストに不許可属性を与える場合に指定します。	deny	省略不可
MAC アドレス	MAC アドレスを H.H.H の形式で設定します。 MAC アドレスが、11.22.33.44.55.66 の場合は、1122.3344.5566 となります。	MAC アドレス形式	省略不可
送信元 MAC アドレス	送信元 MAC アドレスを H.H.H の形式で設定します。	MAC アドレス形式	省略不可
送信元 MAC アドレス範囲	送信元 MAC アドレスを範囲指定するために、マスクを指定します。	MAC アドレス形式	省略不可
宛先 MAC アドレス	宛先 MAC アドレスを H.H.H の形式で設定します。	MAC アドレス形式	省略不可
宛先 MAC アドレス範囲	宛先 MAC アドレスを範囲指定するために、マスクを指定します。	MAC アドレス形式	省略不可
any	mac access-list 番号が 20000～20199 , 30000～301999 または deny を指定した場合は、MAC アドレスの代わりに any を指定することにより、全ての MAC アドレスを指定することができます。	any	省略不可
フィルタリング対象	EtherType によるフィルタリング対象を指定します。 hex：EtherType を直接指定します。 pppoe-：PPPoE Discovery Stage	hex pppoe-discovery pppoe-session arp ip	EtherType によるフィルタリングを行いません。

	discovery	EtherType (0x8863)をフィルタリング対象とします。	ipv6	
	pppoe-session	PPPoE Session Stage EtherType (0x8864)をフィルタリング対象とします。		
	arp	ARP EtherType (0x0806)をフィルタリング対象とします。		
	ip	IP EtherType (0x0800)をフィルタリング対象とします。		
	ipv6	IPv6 EtherType (0x86DD)をフィルタリング対象とします。		
log	パケットフィルタリング機能において該当条件(行単位)にヒットしたパケットが、フィルタリングログに記録されます。		log	フィルタリングログを記録しません。
count	統計情報としてフィルタにヒットしたパケット数、バイト数を表示します。		count	カウントを行いません。
コメント	MAC アクセスリストに付けるコメントを指定します。		240 文字までの半角英数字、記号	省略不可

この設定を行わない場合

MAC アドレスや EtherType によるフィルタリング、QoS を行いません。

設定モード

基本設定モード

mac access-group

mac access-list コマンドで指定したフィルタリングデータを、各インタフェースで適用します。
フィルタリングデータは、各インタフェースで受信したパケットに適用するのか／各インタフェースに送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　mac access-list 1 で指定したデータを、EWAN 1 送信時に適用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#mac access-group 1 out
```

設定例２　mac access-list 2 で指定したデータを、EWAN 1 からの受信時に適用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#mac access-group 2 in
```

コマンド書式

mac access-group <mac access-list 番号> { in | out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
mac access-list 番号	フィルタリングデータを設定した MAC アクセスリストの番号を指定します。	1～10240 20000～20199	省略不可
{ in | out }	インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。	in out	省略不可

この設定を行わない場合

MAC アドレスによるフィルタリングを行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

macfilter ignore broadcast

認証していない端末からのブロードキャストフレームを受信する場合に設定します。
各種ルーティングプロトコルを使用する場合に設定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例１　LAN1 インタフェースで、未認証の端末からのブロードキャストフレームを受信する

```
Router(config)#interface lan 1
Router(config-if lan 1)# macfilter ignore broadcast
```

コマンド書式

```
macfilter ignore broadcast
```

パラメータ

パラメータはありません。

この設定を行わない場合

認証していない端末からのブロードキャストフレームは受信しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

macfilter ignore multicast

認証していない端末からのマルチキャストフレームを受信する場合に設定します。
各種ルーティングプロトコルや VRRP 機能を使用する場合に設定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　LAN1 インタフェースで、未認証の端末からのマルチキャストフレームを受信する

```
Router(config)#interface lan 1
Router(config-if lan 1)# macfilter ignore  multicast
```

コマンド書式

```
macfilter ignore multicast
```

パラメータ

パラメータはありません。

この設定を行わない場合

認証していない端末からのマルチキャストフレームは受信しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

macfilter logging enable

認証成功、認証失敗、セッション終了のログを slog に出力する場合に設定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例１　認証成功、認証失敗、セッション終了のログを slog に出力させる

```
Router(config)#interface lan 1
Router(config-if lan 1)# macfilter logging enable
```

コマンド書式

macfilter logging enable

パラメータ

パラメータはありません。

この設定を行わない場合

認証成功、認証失敗、セッション終了のログを slog に出力しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

macfilter statistics update enable

統計情報のカウントを行うかどうかを指定します。
統計情報は、認証成功からセッションタイムアウトまでの時間に送受信されたパケット数とイーサヘッダ込みのバイト数をカウントします。
本設定を有効にすると、中継性能に影響がありますのでご注意ください。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例１　統計情報のカウントを行うようにする

```
Router(config)#interface lan 1
Router(config-if lan 1)# macfilter statistics update enable
```

コマンド書式

```
macfilter statistics update enable
```

パラメータ

パラメータはありません。

この設定を行わない場合

統計情報のカウントを行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

nas-ip-address

NAS-IP-Address アトリビュートとして通知する IPv4/IPv6 アドレスを設定します。
1 台の RADIUS サーバで複数の拠点装置の MAC アドレス認証を行う構成で、
端末の接続を特定の拠点に限定したい場合などに使用します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　NAS-IP-Address アトリビュートとして通知する IPv4 アドレスを 192.168.100.1 に設定する

```
Router(config)#aaa group server radius Radius-A
Router(config-sg-radius)#nas-ip-address 192.168.100.1
```

コマンド書式

nas-ip-address <IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	NAS-IP-Address アトリビュートとして通知する IPv4/IPv6 アドレスを設定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

NAS-IP-Address アトリビュートを通知しません。

設定モード

RADIUS サーバ設定モード

nas-port interface-number

NAS-PORT アトリビュートとして未認証の端末が接続したインタフェースナンバーを通知します。
端末の接続を特定のインタフェースに限定したい場合などに使用します。
各インタフェースのインタフェースナンバーは以下のようになっています。

インタフェース名	インタフェースナンバー
lan 1	1
ewan 1	2
ewan 2	3
vlanif 1	4
・	・
・	・
・	・
vlanif 150	153

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　NAS-PORT アトリビュートとして該当インタフェースナンバーを通知するように設定する

```
Router(config)#aaa group server radius Radius-A
Router(config-sg-radius)#nas-port interface-number
```

コマンド書式

```
nas-port interface-number
```

パラメータ

パラメータはありません。

この設定を行わない場合

NAS-PORT アトリビュートを通知しません。

設定モード

RADIUS サーバ設定モード

retransmit

RADIUS サーバへの送信再送回数を設定します。
ここで指定した回数を送信しても応答がなかった場合は、次優先度の RADIUS サーバへ問い合わせを行います。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　RADIUS サーバへの送信再送回数を 5 回に設定する

```
Router(config)#aaa group server radius Radius-A
Router(config-sg-radius)#retransmit 5
```

コマンド書式

retransmit〈送信再送回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信再送回数	RADIUS サーバへの送信再送回数を設定します。	0～100	省略不可

この設定を行わない場合

再送回数は 3 回となります。

設定モード

RADIUS サーバ設定モード

server-private

RADIUS サーバの IP アドレス、使用するポート番号、共有シークレットを設定します。
指定したサーバが有効になるのは、設定順の上位 3 エントリとなります。
複数の設定がある場合は、設定した順番で問い合わせを行い、許可(Accept)の応答があった場合は、以降のサーバへの問い合わせは行いません。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　192.168.10.1 の RADIUS サーバ（共有シークレット：secret ）を登録する

```
Router(config)#aaa group server radius Radius-A
Router(config-sg-radius)#server-private 192.168.10.1 key secret
```

コマンド書式

```
server-private {<RADIUS サーバアドレス>} [auth-port <UDP ポート番号>]
                key <共有シークレット> [{secret|private} [encrypted]]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
RADIUS サーバアドレス	RADIUS サーバを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
UDP ポート番号	RADIUS サーバが使用する UDP ポート番号を指定します。	1～65535	1812
共有シークレット	RADIUS サーバとの暗号キーを指定します。	最大 254 文字以内の英数字	省略不可
secret | private	パスワードを暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。 secret：暗号化する際に共有暗号鍵を使用する private：暗号化する際に装置固有暗号鍵を使用する	secret private	パスワードを暗号化しません
encrypted	パスワードを暗号化処理するかどうかを設定します。 このオプションを付加することにより、パスワードは暗号化済みと判定されます。 secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。	encrypted	暗号化データとして扱いません

この設定を行わない場合

Radius 認証を行えません。

設定モード

RADIUS サーバ設定モード

source-address

RADIUS パケットの送信元アドレスとして使用するアドレスを設定します。
指定したアドレスがインタフェースにセットされていない場合、またはセットされているインタフェースが down している場合は、該当の RADIUS グループ設定が無効となります。

refresh コマンド後に有効になるコマンドです。

注意:VRRP 冗長構成の場合は、source-address に Master/Backup の実 IP アドレスを設定してください。また、Radius サーバ側にクライアントアドレスを設定する場合は Master/Backup の実 IP アドレスを指定してください。

V01.02(00)以降サポート

設定例 1　RADIUS パケットの送信元アドレスを 192.168.0.1 に設定する

```
Router(config)#aaa group server radius Radius-A
Router(config-sg-radius)#source-address 192.168.0.1
```

コマンド書式

source-address 〈送信元アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信元アドレス	RADIUS パケットの送信元アドレスとして使用するアドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

実際にパケットを送信するインタフェースのアドレスになります。

設定モード

RADIUS サーバ設定モード

timeout

RADIUS サーバからの応答タイムアウト時間(単位:秒)を設定します。
ここで指定した時間 RADIUS サーバからの応答がなかった場合は再送します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例 1　RADIUS サーバからの応答タイムアウト時間を 30 秒に設定する

```
Router(config)#aaa group server radius Radius-A
Router(config-sg-radius)#timeout 30
```

コマンド書式

timeout 〈タイムアウト〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タイムアウト	RADIUS サーバからの応答タイムアウト時間(秒)を設定します。	1～600	省略不可

この設定を行わない場合

タイムアウト時間は 5 秒となります。

設定モード

RADIUS サーバ設定モード

サービス制限機能

console exec-timeout

コンソールでログインされている状態で、無通信監視時間(単位:分)を設定します。コンソールでログインされ、このコマンドで設定した時間何もコマンドの入力がなかった場合は、自動でログアウトします。

設定例 1　タイムアウト時間を 30 分に設定する場合

```
Router(config)#console exec-timeout 30
```

設定例 2　自動ログアウトさせない場合

```
Router(config)#console exec-timeout off
```

コマンド書式

console exec-timeout <タイムアウト時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タイムアウト時間	コンソールでログインされ、オペレーションが行われなくなってから自動ログアウトするまでの時間(単位:分)を指定します。 off を指定すると自動ログアウトしません。	1～60 off	省略不可

この設定を行わない場合

60 分で自動ログアウトするようになっています。

注意！

自動ログアウト／意図的なログアウトにかかわらず、コンソールで設定した内容は記録されています。
他のユーザが TELNET でログインして、save コマンドを入力し、再起動した時点で有効となってしまいます。

設定を途中で止め、元の状態に戻すには、load コマンドを利用してからログアウトしてください。

設定モード

基本設定モード

ftp-server exec-timeout

FTP でログインされている状態で、無通信監視時間(単位:分)を設定します。FTP でログインされ、このコマンドで設定した時間何もコマンドの入力がなかった場合は、自動でログアウトします。

設定例 1　タイムアウト時間を 30 分に設定する場合

```
Router(config)#ftp-server exec-timeout 30
```

設定例 2　自動ログアウトさせない場合

```
Router(config)#ftp-server exec-timeout off
```

コマンド書式

ftp-server exec-timeout <タイムアウト時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タイムアウト時間	FTP でログインされ、オペレーションが行われなくなってから自動ログアウトするまでの時間(単位:分)を指定します。 off を指定すると自動ログアウトしません。	1～60 off	省略不可

この設定を行わない場合

5 分で自動ログアウトするようになっています。

設定モード

基本設定モード

ftp-server shutdown

FTP によるアクセスを拒否する場合に指定します。

設定例１　FTP のアクセスを拒否する

```
Router(config)#ftp-server shutdown
```

コマンド書式

```
ftp-server shutdown
```

パラメータ

パラメータはありません。

この設定を行わない場合

FTP によるアクセスを受け付けます。

設定モード

基本設定モード

telnet-server exec-timeout

TELNET でログインされている状態で、無通信監視時間(単位:分)を設定します。TELNET でログインされ、このコマンドで設定した時間何もコマンドの入力がなかった場合は、自動でログアウトします。

設定例 1　タイムアウト時間を 30 分に設定する場合

```
Router(config)#telnet-server exec-timeout 30
```

設定例 2　自動ログアウトさせない場合

```
Router(config)#telnet-server exec-timeout off
```

コマンド書式

telnet-server exec-timeout <タイムアウト時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タイムアウト時間	TELNET でログインされ、オペレーションが行われなくなってから自動ログアウトするまでの時間(単位:分)を指定します。 off を指定すると自動ログアウトしません。	1～60 off	省略不可

この設定を行わない場合

5 分で自動ログアウトするようになっています。

注意！

自動ログアウト／意図的なログアウトにかかわらず、TELNET で設定した内容は記録されています。
コンソールや、他のユーザが TELNET でログインして、save コマンドを入力し、再起動した時点で有効となってしまいます。
設定を途中で止め、元の状態に戻すには、load コマンドを利用してからログアウトしてください。

設定モード

基本設定モード

telnet-server shutdown

TELNET によるアクセスを拒否する場合に指定します。

設定例１　TELNET のアクセスを拒否する

```
Router(config)#telnet-server shutdown
```

コマンド書式

```
telnet-server shutdown
```

パラメータ

パラメータはありません。

この設定を行わない場合

TELNET によるアクセスを受け付けます。

設定モード

基本設定モード

冗長機能

VRRP 機能について

VRRP（Virtual Router Redundancy Protocol）は、経路の冗長化を目的とする機能です。

TCP/IP のネットワークでは、目的の宛先にデータが到達するまでに、いくつものルータを中継します。各ルータは、ダイナミックルーティング（RIP や OSPF など）を利用して、宛先までの最適経路を計算しています。このダイナミックルーティングでは、宛先への経路に障害が起きた場合に、別の迂回経路に自動で切り替える機能を持っています。

TCP/IP ネットワーク上の、すべての端末が、ダイナミックルーティングをサポートしているわけではありません（特に通信のエンドポイントにある端末）。これにはいろいろな理由が考えられます。管理の面倒さ／処理の重さ。。。等々。ダイナミックルーティングをサポートせずに、宛先へデータを中継させる代替方法として、経路を設定により行うスタティックルーティングがあります。エンドポイントの端末では、スタティックルーティングの中でも、デフォルトルートのみを指定するケースが大半を占めています。

ダイナミックルーティングでは、経路の障害に対して、自動で迂回経路に切り替える機能があるのに対し、スタティックルーティングでは、自動で迂回経路に切り替える機能がありません。例えば、エンドポイントの端末にデフォルトルートとして登録されているルータが故障した場合は、その設定を変更しない限り、データを送ることができなくなってしまいます。

VRRP は、このようなケースにおいて通信を継続するための機能です。

経路上に複数のルータを配備し、そのルータ間で、VRRP のやり取りを行い、データを中継します。データを中継するルータが故障した場合などには、別のルータが中継を担当します。このようにして、スタティックルーティング（デフォルトルート）のみをサポートしている端末がある場合でも、経路の障害時に自動で迂回することができます。

VRRP のしくみ

VRRP パケットフォーマット

VRRP パケットフォーマットについて説明します。
VRRP をサポートするルータは、VRRP パケット(ADVERTISEMENT)を使用し、自分が VRRP 機能を使用するルータであることを、ネットワークに対して広告します。ただし、一度代表ルータが決定した後は、代表ルータのみが VRRP パケットを、定期的に送信します。
VRRP は、プロトコル番号 112 の IP パケットです。VRRP パケットを送信する際、送信元アドレスは実際に送信するインタフェースの IP アドレス／宛先アドレスは 224.0.0.18 となります。IP ヘッダの TTL 値は、"255"でなくてはいけません。

VRRP パケットフォーマットは、以下のとおりです。

0 1 2 3 4 5 6 7		8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3	4 5 6 7 8 9 0 1
Version	Type	Vertual Rtr ID	Priority	Count IP Addrs
Auth Type		Adver Int	Checksum	
IP Address (1)				
:				
IP Address (n)				
Authentication Data (1)				
Authentication Data (2)				

Version	VRRP バージョンです。FITELnet-F シリーズでは、"2"になります。
Type	VRRP タイプです。ADVERTISEMENT では、"1"になります。
Virtual Rtr ID	VRID 値です。 同じ VRRP グループに属するルータは、この値が同じである必要があります。
Priority	優先度です。 この値が大きいほうが、優先度が高くなります。優先度の高いルータが、代表ルータになります
Count IP Addrs	この VRRP パケットで広告する IP アドレスの個数です。
Auth Type	認証タイプです。 認証を使用しない場合は"0"、テキストパスワードによる認証を行う際は"1"、IP 認証ヘッダを使用する場合は"2"となります。 FITELnet-F シリーズでは、IP 認証ヘッダによる認証はサポートしていません。
Adver Int	ADVERTISEMENT パケットの送信間隔です。
Checksum	このパケットのチェックサムです。
IP Address (1)～(N)	仮想 IP アドレスで使用可能な IP アドレスです。 FITELnet-F シリーズでは、通知できる IP アドレスは、1 つです。
Authentication Data	認証データです。 Auth Type が"1"（テキストパスワード）の場合に、パスワード文字列が入ります。

代表ルータの決定ルール

代表ルータは、以下のルールに従い決定されます。

【代表ルータが決定していないとき】
・優先度が高い
　VRRP グループ内で、最も優先度が高いルータが代表ルータになります。優先度が同じであった場合は、ADVERTISEMENT パケット内の IP アドレス(1)で、最も大きい値を通知したルータが代表ルータになります。

【代表ルータが異常のとき】
　代表ルータが定期的に送信する ADVERTISEMENT パケットを一定時間受信しなかった場合は、次に優先度の高いルータが代表ルータになります。
　ここで、一定時間とは、ADVERTISEMENT メッセージ中の「Adver Int」値（ADVERTISEMENT パケットの送信間隔）の3 倍＋（(256-優先度値)／256 ）秒 で計算されます。例えば、【Adver Int ＝ 1/優先度 255 の代表ルータ】の場合、(3*1)+((256-255)/256)=3.00390625 秒（≒3.00 秒）間、ADVERTISEMENT メッセージを受け取らなかった場合に、代表ルータ異常と判断します。

【新しいルータが VRRP グループに属した場合】
　新しいルータが VRRP グループに属した（異常になった元代表ルータが復旧したケースも含みます）場合は、以下のルールに従い、代表ルータが決定されます。
・Preempt モード（先制モード）でない場合は、優先度に関係なく、現在の代表ルータが、そのまま代表ルータを継続することを承認します。
・Preempt モード（先制モード）の場合は、優先度に従い、代表ルータを決定しなおします。

仮想 IP アドレスの決定ルール

【代表ルータが決定していないとき】
代表ルータの ADVERTISEMENT に含まれていた IP アドレス(1)～(N)が、仮想 IP アドレスとなります。

【代表ルータが変更になったとき】
今まで使用されていた仮想 IP アドレスが、そのまま継承されます。

VRRP グループ

VRRP をサポートするルータにより形成されているグループを、VRRP グループといいます。
VRRP は、仮想的に 1 台のルータとして動作することになります。したがって、VRRP グループを、仮想ルータという場合もあります。

仮想 IP アドレス

仮想ルータとしてネットワークに接続する際の IP アドレスです。VRRP グループを形成する各ルータが使用するインタフェースの IP アドレスのうちの 1 つでもかまいませんし、VRRP グループ内のルータが使用しないアドレスでもかまいません。ただし、VRRP を動作させるインタフェースのサブネットで使用するアドレスである必要があります。また、VRRP グループの各ルータに設定される仮想 IP アドレスの設定は、すべて同じアドレスである必要があります。

仮想 MAC アドレス

仮想ルータの MAC アドレスです。VRRP グループの代表ルータは、仮想 IP アドレスに対する ARP リクエストに対して、この仮想 MAC アドレスを返信(Response)します。仮想 MAC アドレスは、00:00:5e:00:01:<VRID>となります。例えば VRID が"10"の場合の仮想 MAC アドレスは、00:00:5e:00:01:0a となります(MAC アドレスでは 16 進数になります)。

VRID

VRRP グループの番号です。VRRP を形成するルータには、同じ値を設定する必要があります。

代表ルータ

VRRP グループのルータの中で、実際にデータ中継を行うルータを代表ルータあるいはマスタールータといいます。代表ルータは、データを中継するだけでなく、ARP のリクエストに対する応答も行います。

バックアップルータ

代表ルータが故障等で使用できなくなった場合に、代表ルータとして動作するルータです。
VRRP グループのルータでは、1 台の代表ルータ以外は、すべてバックアップルータとなります。

Preempt (先制) モード

後から起動した優先度の高い VRRP ルータが、先に起動していた優先度の低い代表ルータに替わり代表ルータとすることを許可するかどうかのモードです。Preempt モードの場合は、代表ルータの交替を許可し、Preempt モードでない場合は許可しません。

VRRP と IPsec

EWAN 側で VRRP を動作させ、IPsec を動作させる場合は、以下の注意が必要です。
FITELnet F2200 などの CPE から、FITELnet F200 に対して IPsec の通信を行う場合、VRRP で指定した仮想 IP アドレス宛にネゴシエーションを行うことが可能です。ただし、VRRP の代表ルータに障害が発生した場合、バックアップ側のルータが IPsec 通信の継続を試みますが、暗号化されたデータを復号化するための情報がないため、通信を継続することができません。
FITELnet F200 で VRRP を使用し、IPsec の通信を行う場合、CPE 側で SA の監視を行う必要があります。FITELnet F2200 では、DPD(Dead Peer Detection)などの、SA 監視機能がサポートされていますので、必ず設定するようにしてください。この SA 監視機能により、SA が切れたことを認識でき、再度ネゴシエーションを行うことができます。
また、FITELnet F200 の Preempt(先制)モードが ON になっていると、VRRP の優先度が高いルータが起動することにより、代表ルータの切り替えが発生するため、IPsec の SA が一時切断されます。
Preempt の設定の際は注意が必要です。

FITELnet-F シリーズでの注意事項

F シリーズでは、複数のインタフェースで VRRP を動作させることが可能です。
複数のインタフェースで同一の VRID を使用した場合、1つのインタフェースが DOWN すると他のインタフェースでも代表ルータ権限を放棄します。(具体的には、Priority=0 の VRRP パケットを送信する)。
例えば、LAN と EWAN#1 で同一の VRID を使って VRRP を動作させ、両方を代表ルータとしている状態で、EWAN#1 回線のケーブルが抜けた場合、LAN インタフェースでも代表ルータ権限を放棄します。

ip vrrp enable

ルータ自身が VRRP ルータとして動作するか否かを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　VRRP ルータとして動作させる

```
Router(config)#ip vrrp enable
```

コマンド書式

```
ip vrrp enable
```

パラメータ

パラメータはありません。

この設定を行わない場合

VRRP ルータとして動作しません。

設定モード

基本設定モード

vrrp address

本インタフェースで動作するルータグループの仮想 IP アドレスを指定します。
Owner を指定した場合は、IP アドレスを指定する必要がありません。
自分が Master ルータの場合であっても通常、実 IP アドレスと違うアドレスをグループの仮想 IP アドレスとして指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　EWAN の VRRP ルータアドレスを 192.168.0.254 に設定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#vrrp 1 address 192.168.0.254
```

コマンド書式

vrrp 〈VRID〉 address 〈VRRP ルータアドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VRID	本インタフェースで動作する VRRP ルータの VRID を設定します。	1～255※1	省略不可
VRRP ルータアドレス	本インタフェースに対しての仮想 IP アドレスを設定します。 owner：本インタフェースの持つプライマリ IP アドレスを VRRP ルータの IP アドレスとして使用します。※2 IP アドレス形式：同一 VRID 値を持つ仮想ルータ間で使用される IP アドレスを設定します。	owner IP アドレス形式	省略不可

※VRRP ルータアドレスに関しては、仮想 IP アドレスを参照してください。
※1 VRID の設定範囲は 1～255 ですが、1 台の装置に設定できる VRID は32までとなります。ただし、各インタフェースに設定できる VRID は、2つまでになります。
※2 VRRP owner 設定を使用する場合には、同じ VRID で動作する全インタフェースで owner 設定を行ってください。また、同じ VRID で動作する全インタフェースで一致している必要があります。

VRID とは？

VRRP 機能で使用される、VRRP ルータグループの識別子です。
VRID が同一の VRRP ルータは、同じグループに所属します。

Master ルータとは？

VRID が同じグループの中で、パケットの配送を行えるのが Master です。
他のルータはバックアップとして待機し、Master に障害が発生した場合に即座に動作を引き継ぎます。

この設定を行わない場合

VRRP アドレスの設定を行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

vrrp adver-interval

本論理インタフェースで動作する VRRP ルータの ADVERTISEMENT パケットの送信間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　ADVERTISEMENT パケットの送信間隔を 3 秒に設定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#vrrp 1 adver-interval 3
```

コマンド書式

vrrp 〈VRID〉 adver-interval 〈送信間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VRID	本インタフェースで動作する VRRP ルータの VRID を設定します。	1～255※	省略不可
送信間隔	Advertisement パケットの送信間隔(単位:秒)を設定します。	1～30	省略不可

※ VRID の設定範囲は 1～255 ですが、1 台の装置に設定できる VRID は32までとなります。ただし、各インタフェースに設定できる VRID は、2つまでになります。

VRID とは？

VRRP 機能で使用される、VRRP ルータグループの識別子です。
VRID が同一の VRRP ルータは、同じグループに所属します。

ADVERTISEMENT パケットとは？

Master ルータから定期的に送信される稼働状態確認用のパケットです。

この設定を行わない場合

ADVERTISEMENT パケットの送信間隔を 1 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

vrrp auth-type

本論理インタフェースで動作する VRRP ルータの認証方法及び認証データを設定します。
認証を行う場合は、同一グループ内で同じパスワードを使用しないとグループ形成が行えません。

本設定の text-password は、古い VRRP プロトコルとの互換性のために用意されたものであり、セキュリティレベルの向上に寄与するものではありません。通常は、auth-type none-auth でご利用ください。

refresh コマンド後に有効になるコマンドです。

設定例 1　認証方式を text-password とし、認証パスワードを vrrppass とします

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#vrrp 1 auth-type text-password vrrppass
```

コマンド書式

vrrp <VRID> auth-type <認証タイプ> <認証パスワード>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VRID	本インタフェースで動作する VRRP ルータの VRID を設定します。	1～255※2	省略不可
認証タイプ	パケットの認証タイプを設定します。 none-auth：認証を行なわない。※1 text-password：8 文字以内のテキストデータを使用して認証を行なう。	none-auth text-password	省略不可
認証パスワード	認証タイプに”text-password”を指定した場合に、パスワード文字列を設定します。	8 文字以内の英数字	省略不可

※1 認証タイプに none-auth を選択した場合は、認証パスワードは入力できません。
※2 VRID の設定範囲は 1～255 ですが、1 台の装置に設定できる VRID は32までとなります。
ただし、各インタフェースに設定できる VRID は、2つまでになります。

VRID とは？

VRRP 機能で使用される、VRRP ルータグループの識別子です。
VRID が同一の VRRP ルータは、同じグループに所属します。

この設定を行わない場合

none-auth が設定されます。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

vrrp preempt

本論理インタフェースで動作する VRRP ルータの Preempt mode 有効を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　VRRP ルータの Preempt mode を有効にします

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#vrrp 1 preempt
```

コマンド書式

vrrp <VRID> preempt

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VRID	本インタフェースで動作する VRRP ルータの VRID を設定します。	1～255※	省略不可

※ VRID の設定範囲は 1～255 ですが、1 台の装置に設定できる VRID は32までとなります。ただし、各インタフェースに設定できる VRID は、2つまでになります。

VRID とは？

VRRP 機能で使用される、VRRP ルータグループの識別子です。
VRID が同一の VRRP ルータは、同じグループに所属します。

Preempt mode とは？

Master ルータに障害が発生してバックアップルータに切り替わる場合や、Master ルータが復旧して、バックアップルータから切り替わる場合の動作を指定します。
※起動した時に、自分の優先度が一番高かった場合の動作の規定

Preempt mode が有効な場合	vrrp priority コマンドで設定した優先度で判断し、常に優先度の高いルータが Master ルータとなります。
Preempt mode が無効の場合	Master ルータに障害が発生しバックアップルータが Master ルータになった後に、最初の Master ルータが復旧したとしても、vrrp priority コマンドで設定した優先度に関係なく現在の Master ルータ（元バックアップルータ）が保持されます。

VRRP と IPsec の連携

EWAN 側で VRRP を動作させ、IPsec を動作させる場合は、以下の注意が必要です。

FITELnet F2200 などの CPE から、FITELnet F200 に対して IPsec の通信を行う場合、VRRP で指定した仮想 IP アドレス宛にネゴシエーションを行うことが可能です。ただし、VRRP の代表ルータに障害が発生した場合、バックアップ側のルータが IPsec 通信の継続を試みますが、暗号化されたデータを復号化するための情報がないため、通信を継続することができません。

FITELnet F200 で VRRP を使用し、IPsec の通信を行う場合、CPE 側で SA の監視を行う必要があります。FITELnet F2200 では、DPD（Dead Peer Detection ）などの、SA 監視機能がサポートされていますので、必ず設定するようにしてください。この SA 監視機能により、SA が切れたことを認識でき、再度ネゴシエーションを行うことができます。

また、FITELnet F200 の Preempt（先制）モードが ON になっていると、VRRP の優先度が高いルータが起動することにより、代表ルータの切り替えが発生するため、IPsec の SA が一時切断されます。Preempt の設定の際は注意が必要です。

この設定を行わない場合

Preempt mode は無効です。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

vrrp priority

Master ルータを決定する優先度を設定します。大きい数字ほど優先度は高くなります。
この優先度は、Master ルータに障害が発生した場合に作動する順番に使用されます。
優先度が同じであった場合は、ADVERTISEMENT パケット内の IP アドレス(1)で、最も大きい値を通知したルータが Master ルータになります。

refresh コマンド後に有効になるコマンドです。

設定例１　ルータの優先度を 120 に設定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#vrrp 1 priority 120
```

コマンド書式

vrrp 〈VRID〉 priority 〈優先度〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VRID	本インタフェースで動作する VRRP ルータの VRID を設定します。	1～255※	省略不可
優先度	Master router に遷移するための優先度を設定します。	1～254	省略不可

※ VRID の設定範囲は 1～255 ですが、1台の装置に設定できる VRID は32までとなります。ただし、各インタフェースに設定できる VRID は、2つまでになります。

VRID とは？

VRRP 機能で使用される、VRRP ルータグループの識別子です。
VRID が同一の VRRP ルータは、同じグループに所属します。

この設定を行わない場合

ルータの優先度を 100 に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

イベント-アクション機能

イベントクラス

check behavior modem

アタッチ状態のデータ通信端末へのアクセスが正常であれば真(true)、データ通信端末へのアクセスが失敗した場合(データ通信端末が故障したとき等)は偽(false)をイベント通知します。
アタッチ状態でない場合は、未定(unknown)を通知します。

refresh コマンド後に有効になるコマンドです。

設定例 1　データ通信端末へのアクセスが正常であれば true として通知する

```
Router(config)#event-class 1
Router(config-event-class 1)#check behavior modem 1
```

コマンド書式

```
check behavior modem 1 [invert]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
invert	真(true)と偽(false)の状態を反転させて通知する場合に指定します。	invert	真(true)、偽(false)をそのまま通知します。

この設定を行わない場合

データ通信端末のアクセス状態によるイベント通知を行いません。

設定モード

イベントクラス設定モード

check fan fail

FAN が故障状態となったら真(true)、それ以外は偽(false)をイベント通知します。

refresh コマンド後に有効になるコマンドです。

設定例 1　FAN が故障状態となった場合は、true として通知する

```
Router(config)#event-class 1
Router(config-event-class 1)#check fan fail
```

コマンド書式

```
check fan fail [invert]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
invert	真(true)と偽(false)の状態を反転させて通知する場合に指定します。	invert	真(true)、偽(false)をそのまま通知します。

この設定を行わない場合

FAN の状態によるイベント通知を行いません。

設定モード

イベントクラス設定モード

check initialization modem

データ通信端末の異常状態からの復旧時に初期化が成功した場合は真(true)、失敗した場合は偽(false)をイベント通知します。
異常状態からの復旧は、reset-modem イベントアクションでの復旧も含みます。

refresh コマンド後に有効になるコマンドです。

設定例 1　データ通信端末の初期化が成功した場合に true として通知する

```
Router(config)#event-class 1
Router(config-event-class 1)#check initialization modem 1
```

コマンド書式

```
check initialization modem 1 [invert]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
invert	真(true)と偽(false)の状態を反転させて通知する場合に指定します。	invert	真(true)、偽(false)をそのまま通知します。

この設定を行わない場合

データ通信端末のリセット処理によるイベント通知を行いません。

設定モード

イベントクラス設定モード

check insertion modem

アタッチ状態においてデータ通信端末が挿入されていれば真(true)データ通信端末がデタッチされずに抜けた場合は偽(false)をイベント通知します。
データ通信端末が、デタッチ状態になると未定(unknown)を通知します。

refresh コマンド後に有効になるコマンドです。

設定例 1　アタッチ状態においてデータ通信端末が挿入されている場合に true として通知する

```
Router(config)#event-class 1
Router(config-event-class 1)#check insertion modem 1
```

コマンド書式

```
check insertion modem 1 [invert]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
invert	真(true)と偽(false)の状態を反転させて通知する場合に指定します。	invert	真(true)、偽(false)をそのまま通知します。

この設定を行わない場合

データ通信端末の装着によるイベント通知を行いません。

設定モード

イベントクラス設定モード

check interface status

設定したインタフェースの状態監視を行います。
本設定項目を複数設定した場合には、インタフェース名が同一のものに関しては上書きとし、インタフェース名が異なる場合には、追加設定とします。

refresh コマンド後に有効になるコマンドです。

設定例 1　EWAN1 の状態監視を行う

```
Router(config)#event-class 1
Router(config-event-class 1)# check interface status ewan 1
```

コマンド書式

check interface status <インタフェース名> [invert]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	状態監視を行うインタフェースを指定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 usb-ethernet 1～2※ ipsecif 1～2000 tunnel 1～2000 vlanif 1～150	省略不可
invert	真(true)と偽(false)の状態を反転させて通知する場合に指定します。	invert	真(true)、偽(false)をそのまま通知します。

※ パラメータ usb-ethernet 1～2 は、V01.04(00)以降サポート

この設定を行わない場合

冗長機能は使用できません。

設定モード

イベントクラス設定モード

check ip-icmp

L3ping による到達確認の ICMP-CLASS 番号(宛先)設定を行います。
本設定項目を複数設定した場合には、<ICMP-CLASS 番号>が同一のものに関しては上書きとし、<ICMP-CLASS 番号>が異なる場合には、追加設定となります。
複数の設定が合った場合には、ICMP-CLASS 番号で優先度をつけます。
例(1:優先度高い ー 2000:優先度低い)

refresh コマンド後に有効になるコマンドです。

設定例 1 L3ping による到達確認の ICMP-CLASS 番号を 1 とする

```
Router(config)#event-class 1
Router(config-event-class 1)# check ip-icmp 1
```

コマンド書式

check ip-icmp <ICMP-CLASS 番号> [invert]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ICMP-CLASS 番号	L3ping による到達確認の ICMP-CLASS 番号(宛先)設定します。	1～2000	省略不可
invert	真(true)と偽(false)の状態を反転させて通知する場合に指定します。	Invert	真(true)、偽(false)をそのまま通知します。

この設定を行わない場合

冗長機能は使用できません。

設定モード

イベントクラス設定モード

check signal-level

電波状態監視機能により取得したデータ通信端末の電波レベルの値と、本設定のレベルで指定された値の比較により真(true)、偽(false)をイベント通知します。
電波状態監視ができないデータ通信端末や、対象となるデータ通信端末がデタッチ状態になった場合は、invert の有無に関わらず未定(unknown)をイベント通知します。

電波状態を監視する対象が modem の場合、電波状態を定期的に取得するには、monitor signal-level コマンドの設定が併せて必要です。
監視対象が usb-ethernet の場合は、monitor signal-level コマンドの設定が無くても動作します。

refresh コマンド後に有効になるコマンドです。

設定例 1　10 秒以上、電波レベルが 3 以上の場合は true として通知する

```
Router(config)#event-class 1
Router(config-event-class 1)#check signal-level 3 modem 1 hold-times 10
```

コマンド書式

```
check signal-level <レベル> modem 1 [hold-times <TRUE 確定時間> [<FALSE 確定時間
                    >]] [invert]
check signal-level <レベル> usb-ethernet <USB Ethernet ポート番号> [invert]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
レベル	イベント発生レベルを指定します。	1～255	省略不可
TRUE 確定時間	前回の状態が真(true)以外で、TRUE 確定時間(単位:秒)の間にデータ通信端末の電波レベルが、指定したレベル以上となった場合に状態を真(true)としてイベント通知も真(true)を通知します。ただし、invert が指定されている場合のイベント通知は偽(false)を通知します。	0～86400	TRUE 確定時間は、0 秒となります。
FALSE 確定時間	前回の状態が偽(false)以外で、FALSE 確定時間(単位:秒)の間にデータ通信端末の電波レベルが、指定したレベル未満となった場合に状態を偽(false)としイベント通知も偽(false)を通知します。ただし、invert が指定されている場合のイベント通知は真(true)を通知します。	0～86400	FALSE 確定時間は、1 秒となります。
invert	真(true)と偽(false)の状態を反転させて通知する場合に指定します。	invert	真(true)、偽(false)をそのまま通知します。
USB Ethernet ポート番号	状態監視を行う USB Ethernet ポート番号を指定します。	1～2	省略不可

この設定を行わない場合

電波レベルをイベントアクションとして通知しません。

設定モード

イベントクラス設定モード

check signal-quality

電波状態監視機能により取得したデータ通信端末の電波信号品質の値と、本設定で指定した電波信号品質値の比較により真(true)、偽(false)をイベント通知します。
電波状態監視ができないデータ通信端末や、対象となるデータ通信端末がデタッチ状態になった場合は、invert の有無に関わらず未定(unknown)をイベント通知します。

電波信号品質を定期的に取得するには、monitor signal-quality コマンドの設定が併せて必要です。監視対象が usb-ethernet の場合は、monitor signal-quality コマンドの設定が無くても動作します。

refresh コマンド後に有効になるコマンドです。

設定例 1　10 秒以上電波信号品質値が-90dBm 以上の場合は、true として通知する

```
Router(config)#event-class 1
Router(config-event-class 1)#check signal-quality -90 modem 1 hold-times 10
```

コマンド書式

```
check signal-quality <電波信号品質> modem 1 [hold-times <TRUE 確定時間>
                     [<FALSE 確定時間>]] [invert]
check signal-quality <電波信号品質> usb-ethernet <USB Ethernet ポート番号>
                     [invert]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
電波信号品質	判定基準とする電波信号品質を指定します。	-113～-50	省略不可
TRUE 確定時間	前回の状態が真(true)以外で、TRUE 確定時間(単位:秒)の間にデータ通信端末の電波信号品質が、指定した値以上となった場合に状態を真(true)としてイベント通知も真(true)を通知します。ただし、invert が指定されている場合のイベント通知は偽(false)を通知します。	0～86400	TRUE 確定時間は、0 秒となります。
FALSE 確定時間	前回の状態が偽(false)以外で、FALSE 確定時間(単位:秒)の間にデータ通信端末の電波信号品質が、指定した値未満となった場合に状態を偽(false)としイベント通知も偽(false)を通知します。ただし、invert が指定されている場合のイベント通知は真(true)を通知します。	0～86400	TRUE 確定時間と同じになります。
invert	真(true)と偽(false)の状態を反転させて	invert	真(true)、偽(false)を

	通知する場合に指定します。		そのまま通知します。
USB Ethernet ポート番号※	状態監視を行う USB Ethernet ポート番号を指定します。	1～2	省略不可

※USB Ethernet ポート番号は、V01.04(00)以降サポート

この設定を行わない場合

電波信号品質値をイベントアクションとして通知しません。

設定モード

イベントクラス設定モード

check vrrp status vrid

本機能により、設定した VRID の VRRP 状態監視を行うことができます。
通常の設定では、Master の場合が true、Master 以外の場合が false となります。
invert 設定の場合は逆（Master が false／Master 以外が true）。

refresh コマンド後に有効になるコマンドです。

設定例 1　VRID 1 の VRRP 状態監視を行う

```
Router(config)#event-class 1
Router(config-event-class 1)# check vrrp status vrid 1
```

コマンド書式

check vrrp status vrid <VRID> [invert]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VRID	VRRP 状態監視を行う VRID を設定します。	1～255	省略不可
invert	真(true)と偽(false)の状態を反転させて通知する場合に指定します。	invert	真(true)、偽(false)をそのまま通知します。

この設定を行わない場合

VRID の VRRP 状態監視を行いません。

設定モード

イベントクラス設定モード

dampening disable

イベントフラップダンプニング機能を使用するかどうかの設定をします。
1 回のイベントで加算されるペナルティ値は 1000、ペナルティ値の計算間隔は 15 秒です。

refresh コマンド後に有効になるコマンドです。

設定例 1　イベントフラップダンプニング機能を無効とする

```
Router(config)#event-class 1
Router(config-event-class 1)# dampening disable
```

コマンド書式

```
dampening disable
```

パラメータ

パラメータはありません

この設定を行わない場合

イベントフラップダンプニング機能は有効です。

イベントフラップダンプニング機能とは

イベントフラップダンプニング機能とは、イベントのフラッピング（ばたつき）を考慮し不安定なイベントに対してペナルティを付加することにより、一定値をこえるとそのイベントをこえる直前の状態（true or false）に固定し、ペナルティ値を下回ることで再びイベントの状態により変動できるようにする機能です。
本機能は、イベントクラスごとに設定することができます。

設定モード

イベントクラス設定モード

dampening-parameter

イベントフラップダンプニング機能の各種設定を行います。

refresh コマンド後に有効になるコマンドです。

設定例 1　半値時間を 45 分、フラッピング状態閾値を 2000、フラッピング復旧閾値を 750 とする

```
Router(config)#event-class 1
Router(config-event-class 1)# dampening-parameter 45 2000 750
```

コマンド書式

dampening-parameter 〈半値時間〉〈フラッピング状態発生閾値〉〈フラッピング復旧閾値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
半値時間	ペナルティ値の減少割合を、ペナルティ値が半分に減少するまでの時間で設定します。(単位:分)	1～45	省略不可
フラッピング状態発生閾値	フラッピング状態とみなすペナルティ値(ペナルティ値が設定値をこえた場合にフラッピング状態とみなす)を設定します。	1～65535	省略不可
フラッピング復旧閾値	フラッピング状態から復旧したとみなすペナルティ値(ペナルティ値が設定値と以下(同値を含む)になったの場合に復旧とみなす)を設定します。	1～65535	省略不可

この設定を行わない場合

半値時間:5 分、フラッピング状態閾値:20000、フラッピング復旧閾値:10000 とします。

イベントフラップダンプニング機能とは

イベントフラップダンプニング機能とは、イベントのフラッピング(ばたつき)によってアクションが多発するのを抑止するための機能です。
イベントの状態変化が発生した際にペナルティ値を累積し、フラッピング状態発生閾値を超えるとそのイベントを超える直前の状態(True もしくは False)に固定する機能です。
ペナルティ値は時間とともに減少し、フラッピング状態復旧閾値を下回ると、再びイベントの状態が変化するようになります。
本機能は、イベントクラスごとに設定することができます。

設定モード

イベントクラス設定モード

description

event-class に Description を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　event-class の Description を Event-class Description Class#1 とする

```
Router(config)#event-class 1
Router(config-event-class 1)# description Event-class Description Class#1
```

コマンド書式

description 〈文字〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
文字	event-class に Description を設定します。	半角英数字および記号※1	省略不可

※1 連続 254 文字まで、スペースで区切ることにより 2033 文字まで入力可能です。
ただし、show コマンド(コンフィグの表示を除く※2)で表示される文字数は、最初の 254 文字までとなります。

※2 コンフィグの表示では、2033 文字まで表示されます。

この設定を行わない場合

event-class に Description を設定しません。

設定モード

イベントアクション設定モード

event continuation-time

イベント状態の変化の継続時間を指定します。
ここで指定した時間状態が継続した場合に状態が変化したと判断します。

refresh コマンド後に有効になるコマンドです。

設定例 1　true、false 共にイベント状態の変化の継続時間を 10 秒とする

```
Router(config)#event-class 1
Router(config-event-class 1)# event continuation-time true 10 false 10
```

コマンド書式

event continuation-time true〈継続時間〉false〈継続時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
継続時間	true で設定する値は True となった場合の継続時間(単位:秒)、false で設定する値は、False となった場合の継続時間(単位:秒)を設定します。	0～3600	省略不可

この設定を行わない場合

0 秒(状態が変化した直後に状態が変化したと判断します。)

設定モード

イベントクラス設定モード

event match-any

イベントクラスに設定されているイベント個別設定の何れかのステータスが True の場合にイベントクラスのステータスを true とします。

refresh コマンド後に有効になるコマンドです。

設定例 1　L3Ping1 と L3Ping2 のどちらかが true の時 event-class を true とする

```
Router(config)#event-class 1
Router(config-event-class 1)# event match-any
Router(config-event-class 1)# check ip-icmp 1
Router(config-event-class 1)# check ip-icmp 2
Router(config-event-class 1)# exit
```

コマンド書式

```
event match-any
```

パラメータ

パラメータはありません

この設定を行わない場合

全ての match 行にマッチした場合に、クラスマップに適合したと判断します。

例として、設定例 1 で event match-any を指定しなかった場合は以下のようになります。

```
Router(config)#event-class 1
Router(config-event-class 1)# check ip-icmp 1
Router(config-event-class 1)# check ip-icmp 2
Router(config-event-class 1)# exit
```

この場合、L3Ping1 が true、かつ 3Ping2 が true の時 event-class が true となります。

設定モード

イベントクラス設定モード

logging event state-change

本コマンドで、enable が設定されている場合、各クラスの状態変化が発生するとログを記載します。disable または、未設定(デフォルト)の場合は記載されません。

refresh コマンド後に有効になるコマンドです。

設定例１　event-class の状態変化が発生した場合ログを記載する

```
Router(config)#event-class 1
Router(config-event-class 1)# logging event state-change enable
Router(config-event-class 1)# exit
```

コマンド書式

logging event state-change <ログ設定>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ログ設定	状態変化によりログを記載するかどうかを指定します。 enable　ログを記載する disable　ログを記載しない	enable disable	省略不可

この設定を行わない場合

状態が変化してもログを記載しません。

設定モード

イベントクラス設定モード
イベントアクション設定モード
ICMP クラス設定モード
Watch クラス設定モード

match duration

イベントクラスにて時刻の範囲指定を行う場合に設定します。
from で指定した時刻から、to で指定した時刻までを TRUE の状態とします。
また、range minute オプションを指定することで、指定した時刻から経過時間内を TRUE 状態とする事も出来ます。

refresh コマンド後に有効になるコマンドです。

設定例 1　範囲指定を 2014/02/01 00:00 ～ 2014/02/15 00:00 とする

```
Router(config)#event-class 1
Router(config-event-class 1)# match duration from 2014 2 1 0 0 to 2014 2 15 0 0
```

設定例 2　範囲指定を 2014/02/01 12:10 から 12 時間とする

```
Router(config)#event-class 1
Router(config-event-class 1)# match duration from 2014 2 1 12 10 range minute 720
```

コマンド書式

```
match duration from <年> <月> { 日 | 曜日 } <時> <分> to <年> <月> { 日 |
                    曜日 } <時> <分> [invert]

match duration from <年> <月> { 日 | 曜日 } <時> <分> range minute <分>
                    [invert]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
年	西暦、または any を指定します。 any を指定することにより"毎年"として扱われます。	any 2000～2035	省略不可
月	月、または any を指定します。 any を指定することにより"毎月"として扱われます。	any 1～12	省略不可
日 | 曜日	日にち/曜日、または any を指定します。 any を指定することにより"毎日"として扱われます。 また、last を指定することで月末を指定することが出来ます。	any 1～31 sun mon tue wed thu fri sat	省略不可

		last	
時	時、または any を指定します。 any を指定することにより"毎時"として扱われます。	any 0～23	省略不可
分	分、または any を指定します。 any を指定することにより"毎分"として扱われます。	any 0～59	省略不可
range minute <分>	分単位で範囲を指定します。	1～5000000	省略不可
invert	真(true)と偽(false)の状態を反転させて通知する場合に指定します。	invert	真(true)、偽(false)をそのまま通知します。

この設定を行わない場合

イベントクラスとして時刻の範囲指定を行いません。

設定モード

イベントクラス設定モード

宛先到達確認

address

L3ping による到達確認の宛先設定を行ないます。

本設定は同一の icmp-class 内では複数設定を行なうことはできません。
また、同一の icmp-class 内では IPv4 アドレスと IPv6 アドレスを両方設定することもできません。

source-interface の設定がある場合には、指定したインタフェースの IP アドレスを送信元 IP アドレスとして送信します。指定したインタフェースに複数のアドレスが付いている場合は、1 つ目のアドレスを使用します。
IPv6 アドレスを使用していて、到達確認先がリンクローカルアドレスの場合は、送信元にリンクローカルアドレスを使用し、宛先がグローバルアドレスの場合は、送信元にグローバルアドレスを使用します。
リンクローカルアドレスの場合は、source-interface 指定が必ず必要でです。

IPv6 アドレスを使用していて、到達確認先がグローバルアドレスで、source-interface の設定が無い場合は、到達確認先のロンゲストマッチで送信します。

nexthop の設定がある場合は、続く引数がインタフェース名、IP アドレス、ホスト名のいずれかにより動作が異なります。
続く引数が、インタフェース名の場合には、インタフェース名で指定するインターフェースへ L3Ping の送信を行ないます。

ホスト名を使用するには、名前解決を行うために PPPoE や DHCP クライアント機能で、DNS の IP アドレスを学習しているか、ip name-server コマンドにて DNS サーバのアドレスが設定されている必要があります。
また、宛先到達確認に IPv6 を指定してホスト名を使用する際は、名前解決後のアドレスがグローバルアドレスのホスト名を使用してください。
名前解決後のアドレスが link-local の場合は、icmp 監視機能が動作しません。

IPv6 アドレスは、V01.03(00)以降サポートです。

refresh コマンド後に有効になるコマンドです。

設定例 1　192.168.1.1 宛へ LAN1 側の IP アドレスを送信元として、EWAN1 インタフェース経由で送信する

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# address 192.168.1.1 source-interface lan 1 nexthop ewan 1
```

設定例 2　fe80::1 宛へ LAN1 側の IP アドレスを送信元として送信する

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# address ipv6 fe80::1 source-interface lan 1
```

コマンド書式

address <到達確認先> [source-interface <インタフェース名(ipv4)>] [nexthop <ネクストホップ>]
address <ipv6> <到達確認先> [source-interface <インタフェース名(ipv6)>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ipv6※	宛先到達確認に IPv6 を使用する場合に設定します。	ipv6	IPv4 で宛先到達確認します。
到達確認先	到達確認用の L3ping を送信する宛先を設定します。	IPv4/IPv6 アドレス形式 ホスト名(254 文字以内)	省略不可
インタフェース名(ipv4)	L3ping(IPv4)を送信する際に、送信元アドレスとするインタフェースを指定する場合に設定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 loopback 1～100 tunnel 1～2000 vlanif 1～150	実際に送信するインタフェースのアドレスとなります。
インタフェース名(ipv6※)	L3ping(IPv6)を送信する際に、送信元アドレスとするインタフェースを指定する場合に設定します。	lan 1 ewan 1～2 loopback 1～100 vlanif 1～150	到達確認先がリンクローカルアドレスの場合は、設定が必ず必要。グローバルアドレスの場合は、到達確認先のロンゲストマッチで送信
ネクストホップ	L3ping を送信する際のネクストホップを設定します。	ewan 1～2 pppoe 1～24 dialer 1～20 tunnel 1～2000 connected ipsecif 1～2000 connected null 0 IPv4 アドレス形式 ホスト名(254 文字以内)	装置の経路情報に従います。

※ IPv6 は、V01.03 (00)以降サポート

この設定を行わない場合

冗長機能は使用できません。

設定モード

ICMP クラス設定モード

description

icmp-class の Description を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　icmp-class の Description を L3PING ICMP Class Description#1 とする

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# description L3PING ICMP Class Description#1
```

コマンド書式

description <文字>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
文字	icmp-class の Description を設定します。	半角英数字および記号※1	省略不可

※1 連続 254 文字まで、スペースで区切ることにより 2033 文字まで入力可能です。
ただし、show コマンド(コンフィグの表示を除く※2)で表示される文字数は、最初の 254 文字までとなります。

※2 コンフィグの表示では、2033 文字まで表示されます。

この設定を行わない場合

icmp-class の Description を設定しません。

設定モード

ICMP クラス設定モード

icmp-class

ICMP クラス設定モードに移行します。

設定例１　ICMP クラス設定モードに移行します。

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)#
```

コマンド書式

icmp-class <ICMP クラス番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ICMP クラス番号	ICMP クラス番号を指定します。	1～2000	省略不可

設定モード

基本設定モード

interval

L3ping の到達間隔設定を行います。
refresh によりタイマ値が変更となった場合においては、それまでのタイマ値を引き継ぎます。

refresh コマンド後に有効になるコマンドです。

設定例 1　true 時の送信間隔を 120 秒、false 時の送信間隔を 60 秒とする

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# interval 120 restoration 60
```

コマンド書式

```
interval <INTERVAL> [restoration <REST-INTERVAL>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
INTERVAL	true 時の L3ping の送信間隔(単位:秒)を設定します。	1～2000000	省略不可
REST-INTERVAL	装置再起動後および false 時の送信間隔(単位:秒)を設定します。	1～2000000	30

この設定を行わない場合

true 時 30 秒、false 時 30 秒毎に L3ping 確認を行います。

設定モード

ICMP クラス設定モード

logging event state-change

本コマンドで、enable が設定されている場合、各クラスの状態変化が発生するとログを記載します。disable または、未設定(デフォルト)の場合は記載されません。

refresh コマンド後に有効になるコマンドです。

設定例１　event-class の状態変化が発生した場合ログを記載する

```
Router(config)#event-class 1
Router(config-event-class 1)# logging event state-change enable
Router(config-event-class 1)# exit
```

コマンド書式

logging event state-change <ログ設定>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ログ設定	状態変化によりログを記載するかどうかを指定します。 enable　ログを記載する disable　ログを記載しない	enable disable	省略不可

この設定を行わない場合

状態が変化してもログを記載しません。

設定モード

イベントクラス設定モード
イベントアクション設定モード
ICMP クラス設定モード
Watch クラス設定モー

probe

L3ping を送出する際に、複数個の ICMP メッセージを送出します。
指定パケット数のうち1パケットでも戻りがあれば成功と判断します。
また、(Layer3 タスクが)成功判断後は、残りパケットの送信しません。

refresh コマンド後に有効になるコマンドです。

設定例 1　送出パケット数を 10 とする

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# probe 10
```

コマンド書式

probe <PROBE PACKET>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
PROBE PACKET	L3ping の送出パケット数を設定します。	1～10	省略不可

この設定を行わない場合

パケット数は、2 になります。

設定モード

ICMP クラス設定モード

size

L3ping のパケットサイズを指定します。
指定したサイズは、ICMP-ECHO のデータ部サイズになります。

refresh コマンド後に有効になるコマンドです。

設定例 1　パケットサイズを 256 とする

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# size 256
```

コマンド書式

size 〈パケットサイズ〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
パケットサイズ	L3ping のパケットサイズを設定します。	10～3000	省略不可

この設定を行わない場合

パケットサイズは、56 になります。

設定モード

ICMP クラス設定モード

timeout

L3ping の送信タイムアウト時間(秒)の設定を行います。
連続送信時に最後の1パケットの送信から timeout 設定時間が経過したらタイムアウトと判断します。
refresh による即時有効コマンドですが、送信処理中の場合は、以前のタイムアウト値を使用し次の送信開始から設定されたタイムアウトを使用します。

refresh コマンド後に有効になるコマンドです。

設定例 1　タイムアウトを 10 秒とする

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# timeout 10
```

コマンド書式

timeout <タイムアウト>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タイムアウト	L3ping の送信タイムアウト時間(秒)の設定を行います。	1～10	省略不可

この設定を行わない場合

タイムアウトを 3 秒とします。

設定モード

ICMP クラス設定モード

trial

L3ping における状態遷移までの回数を設定します。
L3ping の状態が false 時に連続して<TRIAL-TIME>回疎通確認になった時点で出力状態を true とします。
また、true 時は連続して<FAIL-TIME>回疎通未確認となった時点で出力状態を false とします。
refresh により確認回数が変更となった場合においては、それまでのタイマ値を引き継ぎます。

refresh コマンド後に有効になるコマンドです。

設定例１　疎通回数１回、未疎通回数１回を確認回数とする

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# trial 1 fail 1
```

コマンド書式

trial <TRAIAL-TIME> fail <FAIL-TIME>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
TRAIAL-TIME	疎通確認とみなすまでの確認回数を設定します。	1～16	省略不可
FAIL-TIME	未疎通確認とみなすまでの確認回数を設定します。	1～16	省略不可

この設定を行わない場合

TRAIAL-TIME:3 回、FAIL-TIME:2 回の確認を行います。

設定モード

ICMP クラス設定モード

アクション

add ip route

経路情報の追加を行います。

refresh コマンド後に有効になるコマンドです。

設定例 1　192.168.1.0 255.255.255.0 への経路を NextHop192.168.100.1 とする

```
Router(config)#event-action 1
Router(config-event-action 1)# add ip route 192.168.1.0 255.255.255.0 192.168.100.1
```

コマンド書式

add ip route <宛先ネットワーク> <マスク> <NextHop> [<distance>] [onetime]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先ネットワーク	スタティックルーティングの宛先ネットワークアドレス	IPv4 アドレス形式	省略不可
マスク	宛先ネットワークに対するマスク	IPv4 アドレス形式	省略不可
NextHop	宛先へ到達するための NextHop の IP アドレスまたは、インタフェースを指定します。	IPv4 アドレス形式 ewan 1～2 pppoe 1～24 loopback 1～100 dialer 1～20 connected ipsecif 1～2000 connected null 0 tunnel 1～2000 usb-ethernet 1～2	省略不可
distance	スタティックルーティングの distance 値を指定します。	1～255	1
onetime	true から false へ遷移時の経路情報の削除をおこなわない場合に指定します。 onetime 動作時の経路削除は装置再起動時または、該当の onetime 設定した経路を消去し即時有効させた場合に削除されます。	onetime	true から false へ遷移時の経路情報の削除を行う

この設定を行わない場合

経路情報を追加しません。

設定モード

イベントアクション設定モード

clear ipsec-session isakmp-policy

指定した ISAKMP ポリシー番号に関連する Phase 1 SA と Phase 2 SA のセッションを解放します。true→false になった場合には、何も行いません。

refresh コマンド後に有効になるコマンドです。

設定例１　isakmp-policy 1 のセッションを解放する

```
Router(config)#event-action 1
Router(config-event-action 1)# clear ipsec-session isakmp-policy 1
```

コマンド書式

clear ipsec-session isakmp-policy <ISAKMP ポリシー番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ISAKMP ポリシー番号	セッションを解放する ISAKMP ポリシー番号を指定します。	1～2000	省略不可

この設定を行わない場合

セッションを解放しません。

設定モード

イベントアクション設定モード

description

event-action の Description を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　event-action に Description を description EVENT_ACTION 1 Main Route とする

```
Router(config)#event-action 1
Router(config-event-action 1)# description EVENT_ACTION 1 Main Route
```

コマンド書式

description <文字>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
文字	icmp-class の Description を設定します。	半角英数字および記号※1	省略不可

※1 連続 254 文字まで、スペースで区切ることにより 2033 文字まで入力可能です。
ただし、show コマンド(コンフィグの表示を除く※2)で表示される文字数は、最初の 254 文字までとなります。

※2 コンフィグの表示では、2033 文字まで表示されます。

この設定を行わない場合

event-action に Description を設定しません。

設定モード

イベントアクション設定モード

disconnect modem

回線が接続状態の場合に、無通信判定時間で設定された間に送信トラヒックが無ければ回線を切断します。

refresh コマンド後に有効になるコマンドです。

設定例 1　回線接続中の場合に、30 秒間送信トラヒックが無ければ回線を切断する

```
Router(config)#event-action 1
Router(config-event-action 1)#disconnect modem 1 idle-timer send 30
```

コマンド書式

disconnect modem 1 [forced | idle-timer send <無通信判定時間>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
無通信判定時間	無通信状態を確定するまでの時間(単位:秒)を設定します。	1～3600	無通信状態を確立するまでは、60 秒となります。
forced	forced を指定することにより、送信トラヒックに関係なく接続中の回線を切断します。	forced	

この設定を行わない場合

接続中の回線を切断するイベントアクションは行わない。

設定モード

イベントアクション設定モード

e-mail body false-to-true

イベントアクションとして送信する電子メールの本文を設定します。
電子メールの本文は、定型文となっており、設定した内容は、定型文の最下行に追加されます。
この指定は、イベントが False→True となった場合のアクションの場合に追加されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　通知する電子の本文に VRRP status changes to Master. を追加する

```
Router(config)#event-action 1
Router(config-event-action 1)# e-mail body false-to-true VRRP status changes to Master.
```

コマンド書式

e-mail body false-to-true<本文>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
本文	False->True のイベントにより送信する電子メールの本文に追加する 1 行を設定します。	最大 254 文字	省略不可

この設定を行わない場合

定型文のみ送信します。定型文は、以下の書式となります。

＜定型文例＞

SysDescr　　: FITELnet F2200 Ver 01.00-112814 Ver 01.00 112814
IP Address　: 192.168.2.254
Time　　: 2014/11/30(SUN) 12:45:18

設定モード

イベントアクション設定モード

e-mail body true-to-false

イベントアクションとして送信する電子メールの本文を設定します。
電子メールの本文は、定型文となっており、設定した内容は、定型文の最下行に追加されます。
この指定は、イベントが True→False となった場合のアクションの場合に追加されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　通知する電子の本文に VRRP status change to Backup.！を追加する

```
Router(config)#event-action 1
Router(config-event-action 1)# e-mail body true-to-false VRRP status changes to Backup.!
```

コマンド書式

e-mail body true-to-false<本文>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
本文	True→False のイベントにより送信する電子メールの本文に追加する 1 行を設定します。	最大 254 文字	省略不可

この設定を行わない場合

定型文のみ送信します。定型文は、以下の書式となります。

＜定型文例＞

```
SysDescr        : FITELnet F2200 Ver 01.00-112814 Ver 01.00 112814
IP Address      : 192.168.2.254
Time            : 2014/11/30(SUN) 12:45:18
```

設定モード

イベントアクション設定モード

e-mail subject

イベントアクションとして、電子メール通知を行う際のサブジェクトを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　通知する電子のサブジェクトを VRRP status change !!とする

```
Router(config)#event-action 1
Router(config-event-action 1)# e-mail subject VRRP status change !!
```

コマンド書式

e-mail subject <サブジェクト>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
サブジェクト	電子メール通知を行う際のサブジェクトを設定します。	最大 254 文字	省略不可

この設定を行わない場合

Event-action occurred on FITELnet F2200 (<LAN 側 IP アドレス>) True->False もしくは False->True（アクションの起動契機により変更）

設定モード

イベントアクション設定モード

execute usb-reset

イベントアクションとして、USB ポートのリセット※を実行します。
リセット後の USB ポートの状態は、USB デバイス挿入時と同等の状態になります。

※USB ポートの電源供給を 10 秒間停止することでリセットを行います。

refresh コマンド後に有効になるコマンドです。

設定例　イベントアクションとして USB ポート番号 1 をリセットする

```
Router(config)#event-action 1
Router(config-event-action 1)# execute usb-reset 1
```

コマンド書式

execute usb-reset < USB ポート番号 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
USB ポート番号	イベントアクションとして、リセットする USB ポートを指定します。	1～2	省略不可

この設定を行わない場合

イベントアクションで USB ポートのリセットを実行しません。

設定モード

イベントアクション設定モード

igmp-proxy disable-upstream

本コマンドを設定することにより、イベントアクション稼働時に、指定したインタフェースでは IGMP Proxy の動作を無効にします。
refresh コマンド後に有効になるコマンドです。

設定例 1　EWAN 1 インタフェースに対して、イベントアクション稼働時に IGMP Proxy の動作を無効にする

```
Router(config)#event-action 1
Router(config-event-action 1)# igmp-proxy ewan 1 disable-upstream
```

コマンド書式

igmp-proxy 〈インタフェース名〉 disable-upstream

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	イベントアクション稼働時に、IGMP Proxy の動作を有効としないインタフェースを指定します。	lan 1 ewan 1～2 ipsecif 1～2000 vlanif 1～150	省略不可

この設定を行わない場合

インタフェースで IGMP Proxy の動作を無効にしません。

設定モード

イベントアクション設定モード

igmp-proxy non-querier

本コマンドを設定することにより、イベントアクションが稼働した時に non-querier 状態に移行します。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN 1 インタフェースに対して non-querier 状態とする

```
Router(config)#event-action 1
Router(config-event-action 1)# igmp-proxy ewan 1 non-querier
```

コマンド書式

igmp-proxy <インタフェース名> non-querier

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	non-querier 状態とするインタフェースを指定します。	lan 1 ewan 1～2 ipsecif 1～2000 vlanif 1～150	省略不可

この設定を行わない場合

non-querier 通知をしません。

設定モード

イベントアクション設定モード

internal-bridge tunnel

イベントアクションのアクションとして、False→True に遷移した際に internal-bridge コマンドで指定した送信優先度を下げるアクションを追加します。

refresh コマンド後に有効になるコマンドです。

設定例 1　状態変化が発生した場合に、優先度を 100 減算する

```
Router(config)#event-action 1
Router(config-event-action 1)# internal-bridge tunnel 1 tx-priority decrement 100
```

コマンド書式

internal-bridge tunnel 〈トンネルインタフェース番号〉 tx-priority decrement 〈優先度〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
トンネルインタフェース番号	対象とするトンネルインタフェース番号を指定します。	1～2000	省略不可
優先度	優先度を指定します。 False→True に遷移した場合に設定値分減算します。	1～255	省略不可

この設定を行わない場合

優先度を変更しません。

設定モード

イベントアクション設定モード

logging event state-change

本コマンドで、enable が設定されている場合、各クラスの状態変化が発生するとログを記載します。disable または、未設定(デフォルト)の場合は記載されません。

refresh コマンド後に有効になるコマンドです。

設定例１　event-class の状態変化が発生した場合ログを記載する

```
Router(config)#event-class 1
Router(config-event-class 1)# logging event state-change enable
Router(config-event-class 1)# exit
```

コマンド書式

logging event state-change <ログ設定>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ログ設定	状態変化によりログを記載するかどうかを指定します。 enable　ログを記載する disable　ログを記載しない	enable disable	省略不可

この設定を行わない場合

状態が変化してもログを記載しません。

設定モード

イベントクラス設定モード
イベントアクション設定モード
ICMP クラス設定モード
Watch クラス設定モー

reset modem

イベントアクションとして、データ通信端末のリセット※を行います。
データ通信端末が接続状態の場合は、接続状態を解除しデータ通信端末のリセットを行います。
データ通信端末の状態変化を state-timeout オプションで指定した時間待機します。
タイムアウトした場合は、データ通信端末の問題等が考えられるため、装置を再起動してデータ通信端末を使用可能な状態に復旧することも可能です。

refresh コマンド後に有効になるコマンドです。

※データ通信端末のリセットとは、データ通信端末を接続する USB ポートに対して電源供給を 10 秒間停止する動作を指します。

設定例１　イベントアクションとしてモデム番号１をリセットする

```
Router(config)#event-action 1
Router(config-event-action 1)# reset modem 1
```

コマンド形式

reset modem〈モデム番号〉 [state-timeout〈待機時間〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
モデム番号	イベントアクションとして、リセットするデータ通信端末を指定します。	1	省略不可
待機時間	データ通信端末が detach 可能になるまでの待機時間（単位：秒）を指定します。	10～2000000	600 秒

この設定を行わない場合

イベントアクションでデータ通信端末のリセットを行わない。

設定モード

イベントアクション設定モード

reset system

イベントアクションとして装置をリセットします。
ただし、以下の状況の場合は、装置リセットが実施されません。
・起動ファームウェアが正常でない場合
・起動ファームウェアを書き換えている場合
・起動コンフィグを書き換えている場合
・boot firmware/configuration コマンドを実行中
・編集中のコンフィグが、save コマンドで保存されていない場合

また、以下の状況の場合は、一定時間経過後強制的に装置リセットが実施されますので注意してください。
この時間は、condition-wait オプションで設定します。
・起動面でないファームウェアが正常でない場合
・起動面でないファームウェアを書き換えている場合
・起動面でないコンフィグが書き換えられている場合
・FTP および SCP のセッションが確立している場合

なお、本イベントが Activate になってから、指定時間後に装置リセット動作を実施させることができます。
この時間は action-delay オプションで設定します。

このアクションは、イベントが True に変化したときに有効とします。
FLASH 領域更新中は装置リセットを行わず、更新が終了するのを待ってから装置をリセットします。

refresh コマンド後に有効になるコマンドです。

設定例 1　action-delay を 120 秒、condition-wait を 20 秒にする

```
Router(config)#event-action 1
Router(config-event-action 1)# reset system action-delay 120 condition-wait 20
```

コマンド形式

reset system [action-delay <遅延時間>] [condition-wait <待機時間>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
遅延時間	装置がリセット可能かチェックを開始するまでの時間(単位:秒)を指定します。	0～2000000	180 秒
待機時間	装置がリセット可能かチェックが開始されてからリセットするまでの時間(単位:秒)を指定します。	30～2000000	600 秒

この設定を行わない場合

イベントアクションとして装置をリセットしません。

設定モード

イベントアクション設定モード

send e-mail

イベントアクションとして、電子メール通知を行うかどうかの設定を行います。
電子メールは、イベントの true->false, false->true のどちらの場合でも送信します。
本コマンドを使用するには、電子メールによる障害通知機能（mail to コマンド）を設定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　イベントアクションとして、電子メール通知を行う

```
Router(config)#event-action 1
Router(config-event-action 1)# send e-mail
```

コマンド書式

```
send e-mail
```

パラメータ

パラメータはありません

この設定を行わない場合

電子メール通知を行いません。

設定モード

イベントアクション設定モード

send snmp-trap

本コマンドを指定した場合は、ステータスが activate および deactivate に遷移した際に、SNMP トラップを送信します。

refresh コマンド後に有効になるコマンドです。

設定例１　送信する SNMP トラップに description コマンドで指定した情報を含める

```
Router(config)#event-action 1
Router(config-event-action 1)# send snmp-trap
```

コマンド書式

```
send snmp-trap  [description]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
description	イベントアクション設定モードの description コマンドで指定した内容を SNMP トラップに含めて通知できるのは、最初の 254 文字までです。	description	SNMP トラップに description を含めない

この設定を行わない場合

SNMP トラップを送信しません。

設定モード

イベントアクション設定モード

set ipsec-status discard isakmp-policy

イベントアクションのアクションとして、指定する ISAKMP ポリシーを利用する SA を DISCARD 状態にします。
DISCARD 状態になると、接続している IPsec-SA／IKE-SA を解放し、指定した SA との接続は行わなくなります。

refresh コマンド後に有効になるコマンドです。

設定例１　SA １の IPsec 状態を DISCARD とする

```
Router(config)#event-action 1
Router(config-event-action 1)# set ipsec-status discard isakmp-policy 1
```

コマンド書式

```
set ipsec-status discard isakmp-policy <SA>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
SA	IPsec 状態を DISCARD にする SA を指定します。	1～2000	省略不可

この設定を行わない場合

IPsec 状態を DISCARD にしません。

設定モード

イベントアクション設定モード

set l2tp-status discard tunnel

イベントアクションのアクションとして、False→True に遷移した際に該当する L2TP を Discard 状態とします。
True→False に遷移した際に、Discard 状態を解除します。

refresh コマンド後に有効になるコマンドです。

設定例１　状態変化が発生した際に、該当する L2TP を Discard 状態とする

```
Router(config)#event-action 1
Router(config-event-action 1)# set l2tp-status discard tunnel 1
```

コマンド書式

set l2tp-status discard tunnel <トンネルインタフェース番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
トンネルインタフェース番号	対象とするトンネルインタフェース番号を指定します。	1～2000	省略不可

この設定を行わない場合

Discard 状態にしません。

設定モード

イベントアクション設定モード

set policy-flag

指定したポリシーフラグ名(任意の文字列:64 文字以内)のフラグを ON にします。
複数のイベントで同じポリシーフラグを操作する設定の場合、全ての状態においてポリシーフラグが OFF になった場合に OFF となり、1つでも ON の状態が存在する場合には ON となります。

指定したポリシーフラグは、QoS 機能のクラスマップで使用します。
指定したポリシーフラグの状態で、QoS のクラス分けを行うことができます。
ポリシーフラグを使用した QoS のクラス分けは、match policy-flag コマンドで指定します。

本コマンドおよび、クラスマップ設定モードの"match policy-flag"コマンドを使用することにより、イベントが発生した場合としていない場合で、QoS やポリシールーティングの制御を変えることが可能です。
インタフェースの状態や、VRRP の状態などを検知し、柔軟に QoS やポリシールーティングの制御を変えて運用することができます。

refresh コマンド後に有効になるコマンドです。

設定例 1　POLI1-FLAG のフラグを ON にする

```
Router(config)#event-action 1
Router(config-event-action 1)# set policy-flag POLI1-FLAG
```

コマンド書式

set policy-flag <ポリシーフラグ名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシーフラグ名	フラグを ON にするポリシーフラグ名を指定します。	最大 64 文字	省略不可

この設定を行わない場合

フラグを ON にするポリシーフラグを指定しません。

設定モード

イベントアクション設定モード

shutdown port

event-action の状態によりポートのシャットダウン 又はシャットダウン解除を行います。
シャットダウン時は、該当 LED も消灯となります。

event-action が Activated ： 指定物理ポートのシャットダウンを行う。
event-action が Inactivated： 指定物理ポートのシャットダウン解除を行う。

但し、Ethernet 設定モードに shutdown 設定がある場合は、Ethernet 設定モードの shutdown を優先します。
※event-action が Inactivated に変化しても、シャットダウン解除は行いません。

また、event-action に shutdown port 設定があり、状態が Activated 時、Ethernet 設定モードで no shutdown を実行してもシャットダウン解除は行いません。

refresh コマンド後に有効になるコマンドです。

V01.01(00)以降サポート

設定例 1　LAN ポート 1 番をポートシャットダウンする

```
Router(config)#event-action 1
Router(config-event-action 1)# shutdown port lan 1
```

コマンド書式

shutdown port { インターフェース名 } <ポート番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インターフェース名	シャットダウンするインターフェースを指定します。	lan ewan	省略不可
ポート番号	LAN インタフェースの場合は、1～8 のポート番号を指定します。 EWAN インタフェースの場合は、1～2 のポート番号を指定します。	1～8	省略不可

この設定を行わない場合

イベントアクションでは、ポートシャットダウンは実施されません。

設定モード

イベントアクション設定モード

suspend icmp-class

icmp-class コマンドで指定した ICMP クラスの経路監視を停止します。
停止した際は、経路監視の状態は Suspend 状態となります。ただし、統計情報のクリアはせず、継続してカウントします。

suspend icmp-class コマンドを使用することで、本装置が経路監視を行う必要が無い場合（VRRP におけるバックアップルータ等）に経路監視を停止することができます。

refresh コマンド後に有効になるコマンドです。

設定例１　ICMP クラス番号 100 の経路監視を停止する

```
Router(config)#event-action 1
Router(config-event-action 1)# suspend icmp-class 100
```

コマンド書式

suspend icmp-class <ICMP クラス番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ICMP クラス番号	経路監視を停止する ICMP クラス番号を指定します。	1～2000	省略不可

この設定を行わない場合

経路監視を停止しません。

設定モード

イベントアクション設定モード

vrrp

vrid の Priority の変更を行います。

refresh コマンド後に有効になるコマンドです。

設定例 1　vrrp：10、track：1、decrement：120 とします

```
Router(config)#event-action 1
Router(config-event-action 1)# vrrp 10 track 1 decrement 120
```

コマンド書式

vrrp <vrid> track <track_no> decrement <priority>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
vrid	変更したい vrid を指定します。	1～255	省略不可
track_no	track_no 値を設定します。 VRRP の priority 減算が4つまで設定できます。 tack 番号の重複は無効になります。(重複の場合両方とも無効) また、4つ以上の登録は無効とになります。	1～4	省略不可
priority	priority 値を設定します。	1～255	省略不可

この設定を行わない場合

vrid の Priority 値を変更しません。

設定モード

イベントアクション設定モード

マッピング

event-class event-action

ルータ冗長機能における event-class と event-action のマッピングを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　イベントクラス番号１とイベントアクション番号１を関連づける

```
Router(config)#event-map
Router(config-event-map)# event-class 1 event-action 1
```

コマンド書式

event-class〈イベントクラス番号〉event-action〈イベントアクション番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
イベントクラス番号	関連づけるイベントクラス番号を設定します。	1～2000	省略不可
イベントアクション番号	関連づけるイベントアクション番号を設定します。	1～2000	省略不可

この設定を行わない場合

ルータ冗長機能を使用できません。

設定モード

イベントマップ設定モード

event-map

イベントマップ設定モードに移行します。

設定例１　イベントマップ設定モードに移行します。

```
Router(config)#event-map
Router(config-event-map)
```

コマンド書式

event-map〈イベントマップ番号〉

パラメータ

パラメータはありません。

設定モード

基本設定モード

QoS/CoS 機能

クラスマップの定義

class-map

クラスマップモードに移行し、トラフィックを分類するクラシファイアを定義します。
クラスマップモードでは、match ip もしくは、match ipv6 コマンドによってトラフィックの分類条件が設定されます。
複数の条件が設定された場合、match-any の有無によって、複数の条件が OR 条件となるか、AND 条件となるかが指定されます。
IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合は、指定された条件は無視されるのではなく、不成立と判定されます。

設定例 1　クラスマップ設定モードへ移行する

```
Router(config)#class-map video-class
Router(config-class-map)#
```

コマンド書式

class-map〈クラスマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クラスマップ名	クラスマップ名称を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップ名によるトラフィックの分類を行いません。

設定モード

基本設定モード

match-any

同一 class-map 内で複数の match 行が記述された場合の動作を指定します。
いずれか 1 つの match 行にマッチした場合に class-map に適合したと判断します。

refresh コマンド後に有効になるコマンドです。

設定例 1　IP アクセスリストの 2000 番をマッチするトラフィックとして設定する

```
Router(config)#class-map video-class
Router(config-class-map)#match-any
Router(config-class-map)#match ip access-group 2000
Router(config-class-map)#exit
```

コマンド書式

match-any

パラメータ

パラメータはありません。

この設定を行わない場合

全ての match 行にマッチした場合に、クラスマップに適合したと判断します。

例として、設定例 1 で match-any を指定しなかった場合は以下のようになります。

```
Router(config)# class-map video-class
Router(config-class-map)# match ip access-group 100
Router(config-class-map)# match ip access-group 101
Router(config-class-map)# exit
```

この場合、IP アクセスリストの 100 番にマッチ、かつ 101 番にマッチするトラフィックを対象とします。

設定モード

クラスマップ設定モード

match bridge 802.1p priority

クラスマップ内でマッチする Ether 中継フレームを、802.1p 値を利用して指定します。

refresh コマンド後に有効になるコマンドです。

設定例　802.1p 値 4 を Ether 中継フレームを対象とする

```
Router(config)#class-map bc
Router(config-class-map)# match bridge 802.1p priority 4
Router(config-class-map)#exit
```

コマンド書式

match bridge 802.1p priority < 802.1p 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
802.1p 値	クラスマップ内でマッチする Ether 中継フレームを、802.1p 値を利用して設定します。	0-7	省略不可

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません。

設定モード

クラスマップ設定モード

match bridge access-group

クラスマップ内でマッチする Ether 中継フレームを、MAC アクセスリストを利用して指定します。
MAC アクセスリストのエントリーが deny エントリーの場合は、対象とはなりません。

refresh コマンド後に有効になるコマンドです。

設定例　MAC アクセスリストの 30000 番にマッチする Ether 中継フレームを対象とする

```
Router(config)#class-map bc
Router(config-class-map)# match bridge access-group 30000
Router(config-class-map)#exit
```

コマンド書式

match bridge access-group < MAC アクセスリスト番号 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MAC アクセスリスト番号	クラスマップ内でマッチする Ether 中継フレームを MAC アクセスリスト番号で指定します。	30000-30199	省略不可

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません。

設定モード

クラスマップ設定モード

match bridge input-interface

クラスマップ内でマッチする Ether 中継フレームを、受信インタフェースを利用して指定します。

refresh コマンド後に有効になるコマンドです。

設定例　LAN のポート 4 番で受信した Ether 中継フレームを対象とする

```
Router(config)#class-map bc
Router(config-class-map)# match bridge input-interface lan 1 port 4
Router(config-class-map)#exit
```

コマンド書式

match bridge input-interface {インタフェース名 [ポート番号]}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	クラスマップ内でマッチする Ether 中継フレームを、受信インタフェースを利用して指定します。	lan 1-1 ewan 1-2 vlanif 1-150 tunnel 1-2000	省略不可
ポート番号	LAN インタフェースには、8 つのポートがあるので、その番号を指定します。 インタフェース名を LAN に指定した場合のみ設定できます。	1-8	全 LAN ポートが対象となります。

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません。

設定モード

クラスマップ設定モード

match bridge vlan-id

クラスマップ内でマッチする Ether 中継フレームを、VLAN-ID を利用して指定します。

refresh コマンド後に有効になるコマンドです。

設定例　VLAN-ID 100 の Ether 中継フレームを対象とする

```
Router(config)#class-map bc
Router(config-class-map)# match bridge vlan-id 100
Router(config-class-map)#exit
```

コマンド書式

match bridge vlan-id < VLAN-ID >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VLAN-ID	クラスマップ内でマッチする Ether 中継フレームを、VLAN-ID を利用して設定します。	0-4094	省略不可

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません。

設定モード

クラスマップ設定モード

match ip/ipv6 access-group

クラスマップ内でマッチするトラフィックを、IP アクセスリストにより設定します。
トラフィックが IPv4 パケットの場合、match ipv6 コマンドは不成立となります。逆にトラフィックが IPv6 パケットの場合、match ip コマンドは不成立となります。
同一 class-map 内で複数の match ip もしくは match ipv6 が定義された場合、定義された順に評価されます。
同一 class-map において match-any が指定されている場合には、いずれの match 行にもトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
match-any が指定されていない場合には、いずれかの match 行にトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
アクセスリストの log と count は無視されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　IP アクセスリストの 2000 番をマッチするトラフィックとして設定する

```
Router(config)#class-map video-class
Router(config-class-map)#match-any
Router(config-class-map)#match ip access-group 2000
Router(config-class-map)#exit
```

コマンド書式

```
match ip access-group <ext-ipv4 アクセスリスト番号 > [input-interface
                        {<インタフェース名> [port <ポート番号>} ]
match ipv6 access-group <ext-ipv6 アクセスリスト番号 > [input-interface
                        {<インタフェース名> [port <ポート番号>]}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ext-ipv4 アクセスリスト番号	クラスマップ内でマッチするトラフィックを ext-ipv4 アクセスリスト番号で指定します。	100～199、2000～2699 20000～21199	省略不可
ext-ipv6 アクセスリスト番号	クラスマップ内でマッチするトラフィックを ext-ipv6 アクセスリスト番号で指定します。	3500～3999 35000～36499	省略不可
インタフェース名	クラスマップ内でマッチするトラフィックを入力インタフェースで指定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 ipsecif 1～2000 tunnel 1～2000 vlanif 1～150	全てのインタフェース
ポート番号	LAN インタフェースの物理ポート番号を指定します。	port 1～8	LAN インタフェースのポ

			ート番号

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません。

設定モード

クラスマップ設定モード

match ip/ipv6 input-interface

クラスマップ内でマッチするトラフィックを、入力インタフェースにより設定します。
トラフィックが IPv4 パケットの場合、match ipv6 コマンドは不成立となります。逆にトラフィックが IPv6 パケットの場合、match ip コマンドは不成立となります。
同一 class-map 内で複数の match ip もしくは match ipv6 が定義された場合、定義された順に評価されます。
同一 class-map において match-any が指定されている場合には、いずれの match 行にもトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
match-any が指定されていない場合には、いずれかの match 行にトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。

refresh コマンド後に有効になるコマンドです。

設定例１　トラフィックを分類するインタフェースを EWAN 1 として設定する

```
Router(config)#class-map video-class
Router(config-class-map)#match-any
Router(config-class-map)#match ip input-interface ewan 1
Router(config-class-map)#exit
```

コマンド書式

```
match ip input-interface <インタフェース名> [port <ポート番号>]
match ipv6 input-interface <インタフェース名> [port <ポート番号>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	クラスマップ内でマッチするトラフィックを入力インタフェースで指定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20 ipsecif 1～2000 vlanif 1～150 tunnel 1～2000	全てのインタフェース
ポート番号	LAN インタフェースの物理ポート番号を指定します。	port 1～8	LAN インタフェースのポート番号

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません。

設定モード

クラスマップ設定モード

match policy-flag

QoS 変更用のフラグがセットされている、もしくはセットされていない場合の class として動作します。
イベントアクションからの通知が 1 度もない状態では、ポリシーフラグを OFF として扱います。

refresh コマンド後に有効になるコマンドです。

設定例 1　QoS 変更用フラグの class を POLI1-FLAG とする。

```
Router(config)# class-map video-class
Router(config-class-map)# match policy-flag POLI1-FLAG set
Router(config-class-map)# exit
```

コマンド書式

match policy-flag <ポリシーフラグ名> {set|unset}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシーフラグ名	QoS 変更用フラグの class を指定します。	最大 64 文字	省略不可
set|unset	QoS 変更用フラグがセットされているもしくは、されていない場合を対象とします。 set：ポリシーフラグがセットされている場合に適用 unset：ポリシーフラグがセットされていない場合に適用	set unset	省略不可

この設定を行わない場合

設定を行っていない場合は、このフラグの情報はクラスわけの情報として使用しません。

設定モード

クラスマップ設定モード

アクションマップの定義

action-map

action-map モードに移行し、トラフィックに対するアクションを定義します。
実行場所によってサポートされないアクションや、IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合、指定されたアクションは無視されます。

設定例１　アクションマップ設定モードへ移行する。

```
Router(config)#action-map stream-action
Router(config-action-map)#
```

コマンド書式

action-map〈アクションマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクションマップ名	アクションマップ名を設定します	16 文字以内の文字列	省略不可

この設定を行わない場合

アクションは定義されません。

設定モード

基本設定モード

drop

アクションとして、パケット廃棄を設定します。
同一アクションマップに他のコマンドが設定されていても、本コマンドが優先されます。

refresh コマンド後に有効になるコマンドです。

設定例１　アクションとしてパケット廃棄を設定する。

```
Router(config)#action-map stream-action
Router(config-action-map)#drop
```

コマンド書式

drop

パラメータ

パラメータはありません

この設定を行わない場合

パケットは破棄されません。

設定モード

アクションマップ設定モード

set encap ip dscp

アクションとして、カプセル化する IPv4 ヘッダに対するマーキングを設定します。
出力インタフェースが IPsec インタフェースもしくはトンネルインタフェースで、かつ Outer が IPv4 の場合に、カプセル化する IPv4 ヘッダの dscp を指定した値にマーキングします。
prec と tos は組み合わせて用いることができますが、dscp とは排他となります。
dscp が設定されている場合は dscp 設定が優先され prec と tos の設定は無効となります。
dscp が設定されていない場合のみ prec と tos の設定が有効になります。
本設定は output の QoS でのみ指定する事ができます。

refresh コマンド後に有効になるコマンドです。

V01.01(00)以降サポート

設定例 1　カプセル化する IPv4 ヘッダに対するマーキングとして、dscp に ef を設定する。

```
Router(config)#action-map stream-action
Router(action-map stream-action)#set encap ip dscp ef
```

コマンド書式

```
set encap ip dscp {<dscp 値>|<dscp 名称>|<copy>}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
dscp 値	dscp 値を設定します。	0～63	省略不可
dscp 名称	dscp 名称を設定します。	ef(101110b), bf(000000b) af11(001010b), af12(001100b) af13(001110b), af21(010010b) af22(010100b), af23(010110b) af31(011010b), af32(011100b) af33(011110b), af41(100010b) af42(100100b), af43(100110b)	省略不可
copy	マーキング設定があった場合でも、inner の元データの値をコピーします。	copy	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set encap ip prec

アクションとして、カプセル化する IPv4 ヘッダに対するマーキングを設定します。
出力インタフェースが IPsec インタフェースもしくはトンネルインタフェースで、かつ Outer が IPv4 の場合に、カプセル化する IPv4 ヘッダの prec を指定した値にマーキングします。
prec と tos は組み合わせて用いることができますが、dscp とは排他となります。
dscp が設定されている場合は dscp 設定が優先され prec と tos の設定は無効となります。
dscp が設定されていない場合のみ prec と tos の設定が有効になります。
本設定は output の QoS でのみ指定する事ができます。
refresh コマンド後に有効になるコマンドです。

V01.01(00)以降サポート

設定例 1　カプセル化する IPv4 ヘッダに対するマーキングとして、prec に routine を設定する。

```
Router(config)#action-map stream-action
Router(action-map stream-action)#set encap ip prec routine
```

コマンド書式

set encap ip prec {<precedence 値>|<precedence 名称>|<copy>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
precedence 値	precedence 値を設定します。	0～7	省略不可
precedence 名称	precedence 名称を設定します。	routine(0), priority(1) immediate(2), flash(3) flash-override(4) critical(5), internet(6) network(7)	省略不可
copy	マーキング設定があった場合でも、inner の元データの値をコピーします。	copy	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set encap ip tos

アクションとして、カプセル化する IPv4 ヘッダに対するマーキングを設定します。
出力インタフェースが IPsec インタフェースもしくはトンネルインタフェースで、かつ Outer が IPv4 の場合に、カプセル化する IPv4 ヘッダの tos を指定した値にマーキングします。
prec と tos は組み合わせて用いることができますが、dscp とは排他となります。
dscp が設定されている場合は dscp 設定が優先され prec と tos の設定は無効となります。
dscp が設定されていない場合のみ prec と tos の設定が有効になります。
本設定は output の QoS でのみ指定する事ができます。

refresh コマンド後に有効になるコマンドです。

V01.01(00)以降サポート

設定例 1　カプセル化 IPv4 ヘッダに対するマーキングとして、tos に min-momentary-cost を設定する。

```
Router(config)#action-map stream-action
Router(action-map stream-action)#set encap ip tos min-momentary-cost
```

コマンド書式

```
set encap ip tos {<precedence 値>|<precedence 名称>|<copy>}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
tos 値	tos 値を設定します	0～15	省略不可
tos 名称	tos 名称を設定します。	min-momentary-cost(1) max-reliability(2) max-throughput(4), min-delay(8) ,normal(0)	省略不可
copy	マーキング設定があった場合でも、inner の元データの値をコピーします。	copy	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set encap ipv6 dscp

出力インタフェースがトンネルインタフェースでかつ Outer が IPv6 の場合に、カプセル化する IPv6 ヘッダの dscp を指定した値にマーキングします。
対象パケットが IPv6 パケットではなかった場合、本設定は無視されます。traffic-class と dscp とは排他となります。
コンフィグ読み込み側での処理とし、dscp が設定されている場合は dscp 設定が優先され traffic-class の設定は無効になります。
dscp が設定されていない場合のみ traffic-class の設定が有効になります。
本設定は output の QoS でのみ指定する事ができます。

refresh コマンド後に有効になるコマンドです。

V01.01(00)以降サポート

設定例 1　カプセル化する IPv6 ヘッダに対するマーキングとして、dscp に ef を設定する

```
Router(config)#action-map stream-action
Router(action-map stream-action)#set encap ipv6 dscp ef
```

コマンド書式

set encap ipv6 dscp {<dscp 値>|<dscp 名称>|<copy>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
dscp 値	dscp 値を設定します。	0～63	省略不可
dscp 名称	dscp 名称を設定します。	ef(101110b), bf(000000b) af11(001010b), af12(001100b) af13(001110b), af21(010010b) af22(010100b), af23(010110b) af31(011010b), af32(011100b) af33(011110b), af41(100010b) af42(100100b), af43(100110b)	省略不可
copy	マーキング設定があった場合でも、inner の元データの値をコピーします。	copy	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set encap ipv6 traffic-class

アクションとして、カプセル化する IPv6 ヘッダに対するマーキングを設定します。
出力インタフェースがトンネルインタフェースでかつ Outer が IPv6 の場合に、カプセル化する IPv6 ヘッダの traffic-class を指定した値にマーキングします。
対象パケットが IPv6 パケットではなかった場合、本設定は無視されます。traffic-class と dscp とは排他となります。
コンフィグ読み込み側での処理とし、dscp が設定されている場合は dscp 設定が優先され traffic-class の設定は無効になります。
dscp が設定されていない場合のみ traffic-class の設定が有効になります。
本設定は output の QoS でのみ指定する事ができます。

refresh コマンド後に有効になるコマンドです。

V01.01(00)以降サポート

設定例 1　カプセル化する IPv6 ヘッダに対するマーキングとして、traffic-class の値を 5 に設定する。

```
Router(config)#action-map stream-action
Router(action-map stream-action)#set encap ipv6 traffic-class 5
```

コマンド書式

```
set encap ipv6 traffic-class {<traffic-class-value>|<copy>}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
traffic-class-value	traffic-class-value を設定します。	0～255	省略不可
copy	マーキング設定があった場合でも、inner の元データの値をコピーします。	copy	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set ip dscp

アクションとして、IPv4 ヘッダに対するマーキングを設定します。
対象パケットが IPv4 パケットではなかった場合、本設定は無視されます。
prec と tos は組み合わせて用いることができますが、dscp とは排他となります。
コンフィグ読み込み側での処理として、dscp が設定されている場合は dscp 設定が優先され prec と tos の設定は無効となります。
dscp が設定されていない場合のみ prec と tos の設定が有効になります。
アクションが指定されなかったヘッダフィールドは、マーキングされずにそのまま転送されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　IPv4 ヘッダに対するマーキングとして、dscp に ef を設定する。

```
Router(config)#action-map stream-action
Router(config-action-map)#set ip dscp ef
```

コマンド書式

```
set ip dscp {< dscp 値>|< dscp 名称>}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
dscp 値	dscp 値を設定します。	0～63	省略不可
dscp 名称	dscp 名称を設定します。	ef(101110b), bf(000000b) af11(001010b), af12(001100b) af13(001110b), af21(010010b) af22(010100b), af23(010110b) af31(011010b), af32(011100b) af33(011110b), af41(100010b) af42(100100b), af43(100110b)	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set ip next-hop

アクションとして、パケット中継先を設定します(ポリシールーティング)。
有効な中継先のうち、distance 値がもっとも小さい中継先が有効になります。
有効な中継先のうち、もっとも distance 値が小さい中継先が同一 distance 値で複数存在する場合、config 表示で最も上の設定が適用されます。
distance 値が省略された場合のデフォルトは"1"とします。
中継先が到達不能な場合、その経路は無視されます。
個々の中継先が全て到達不能な場合、もしくは指定されていない場合、set {ip|ipv6} next-hop default が指定されている場合には、通常のルーティングが行なわれます。
指定されていない場合には、パケットは中継不能パケットとして廃棄されます。
パケットが IPv4 の場合、set ipv6 は無視されます。逆にパケットが IPv6 の場合、set ip は無視されます。
本コマンドは、I/F 受信時のサービスポリシーとして設定された場合と、自局送信時のサービスポリシーとして設定された場合にのみ有効となり、I/F 送信時のサービスポリシーとして設定された場合には無視されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　パケット中継先を 192.168.100.1 に distance 10 で設定する。

```
Router(config)#action-map stream-action
Router(config-action-map)#set ip next-hop 192.168.100.1 distance 10
```

コマンド書式

```
set ip next-hop <IP アドレス> [distance (1-255)]
set ip next-hop <インタフェース> [distance (1-255)]
set ip next-hop connected {ipsecif <1-100> | null <0-0>} [distance (1-255)]
set ip next-hop default
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	中継先の IP アドレスを設定します。	IPv4 アドレス形式	省略不可
インタフェース	PPPoE インタフェースのように、宛先へ到達するための NextHop の IP アドレスが明確に分からない場合に設定します。	ewan 1～2 pppoe 1～24 dialer 1～20 tunnel 1～2000	省略不可
connected ipsecif	宛先への経路として IPsec インタフェースを指定します。	ipsecif 1～2000	省略不可
connected null	廃棄用の宛先経路情報とします。	null 0	省略不可
distance	中継先の distance 値を設定します。	1～255	省略不可
default	ポリシールーティングを行わずに、通常	なし	省略不可

	のルーティングをおこないます。		

この設定を行わない場合

中継先設定は行なわれません。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

アクションマップ設定モード

set ip prec

アクションとして、IPv4 ヘッダに対するマーキングを設定します。
対象パケットが IPv4 パケットではなかった場合、本設定は無視されます。
prec と tos は組み合わせて用いることができますが、dscp とは排他となります。
コンフィグ読み込み側での処理として、dscp が設定されている場合は dscp 設定が優先され prec と tos の設定は無効となります。
dscp が設定されていない場合のみ prec と tos の設定が有効になります。
アクションが指定されなかったヘッダフィールドは、マーキングされずにそのまま転送されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　IPv4 ヘッダに対するマーキングとして、prec に routine を設定する。

```
Router(config)#action-map stream-action
Router(config-action-map)#set ip prec routine
```

コマンド書式

set ip prec {< precedence 値>|< precedence 名称>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
precedence 値	precedence 値を設定します。	0～7	省略不可
precedence 名称	precedence 名称を設定します。	routine(0), priority(1) immediate(2), flash(3) flash-override(4) critical(5), internet(6) network(7)	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set ip tos

アクションとして、IPv4 ヘッダに対するマーキングを設定します。
対象パケットが IPv4 パケットではなかった場合、本設定は無視されます。
prec と tos は組み合わせて用いることができますが、dscp とは排他となります。
コンフィグ読み込み側での処理として、dscp が設定されている場合は dscp 設定が優先され prec と tos の設定は無効となります。
dscp が設定されていない場合のみ prec と tos の設定が有効になります。
アクションが指定されなかったヘッダフィールドは、マーキングされずにそのまま転送されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　IPv4 ヘッダに対するマーキングとして、tos に min-momentary-cost を設定する。

```
Router(config)#action-map stream-action
Router(config-action-map)#set ip tos min-momentary-cost
```

コマンド書式

set ip tos {<tos 値>|<tos 名称}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
tos 値	tos 値を設定します。	0～15	省略不可
tos 名称	tos 名称を設定します。	min-momentary-cost(1) max-reliability(2) max-throughput(4), min-delay(8) ,normal(0)	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set ipv6 dscp

アクションとして、IPv6 ヘッダに対するマーキングを設定します。
対象パケットが IPv6 パケットではなかった場合、本設定は無視されます。traffic-class と dscp とは排他となります。
コンフィグ読み込み側での処理とし、dscp が設定されている場合は dscp 設定が優先され traffic-class の設定は無効になります。
dscp が設定されていない場合のみ traffic-class の設定が有効になります。
アクションが指定されなかったヘッダフィールドは、マーキングされずにそのまま転送されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　IPv6 ヘッダに対するマーキングとして、dscp に ef を設定する

```
Router(config)#action-map stream-action
Router(config-action-map)#set ipv6 dscp ef
```

コマンド書式

set ipv6 dscp{< dscp 値>|< dscp 名称>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
dscp 値	dscp 値を設定します。	0～63	省略不可
dscp 名称	dscp 名称を設定します。	ef(101110b), bf(000000b) af11(001010b), af12(001100b) af13(001110b), af21(010010b) af22(010100b), af23(010110b) af31(011010b), af32(011100b) af33(011110b), af41(100010b) af42(100100b), af43(100110b)	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set ipv6 next-hop

アクションとして、パケット中継先を設定します（ポリシールーティング）。
有効な中継先のうち、distance 値がもっとも小さい中継先が有効になります。
有効な中継先のうち、もっとも distance 値が小さい中継先が同一 distance 値で複数存在する場合、config 表示で最も上の設定が適用されます。
distance 値が省略された場合のデフォルトは"1"とします。
中継先が到達不能な場合、その経路は無視されます。
個々の中継先が全て到達不能な場合、もしくは指定されていない場合、set {ip|ipv6}next-hop default が指定されている場合には、通常のルーティングが行なわれます。
指定されていない場合には、パケットは中継不能パケットとして廃棄されます。
パケットが IPv4 の場合、set ipv6 は無視されます。逆にパケットが IPv6 の場合、set ip は無視されます。
本コマンドは、I/F 受信時のサービスポリシーとして設定された場合と、自局送信時のサービスポリシーとして設定された場合にのみ有効となり、I/F 送信時のサービスポリシーとして設定された場合には無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　パケット中継先を 2001:db8::1 に distance 10 で設定する

```
Router(config)#action-map stream-action
Router(config-action-map)#set ipv6 next-hop 2001:db8::1 distance 10
```

コマンド書式

```
set ipv6 next-hop <IP アドレス> [インタフェース※1][distance (1-255)]
set ipv6 next-hop <インタフェース※2> [distance (1-255)]
set ipv6 next-hop default
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	中継先の IP アドレスを設定します。	IPv6 アドレス形式	省略不可
インタフェース※1	中継先インタフェースを指定します。 NextHop にリンクローカルアドレスを設定した場合は、インタフェースの指定が必須となります。	lan 1 ewan 1～2 pppoe 1～24 vlanif 1～150	―
インタフェース※2	PPPoE インタフェースのように、宛先へ到達するための NextHop の IP アドレスが明確に分からない場合に設定します。	pppoe 1～24 tunnel 1～2000	省略不可
distance	中継先の distance 値を設定します。	1～255	1
default	ポリシールーティングを行わずに、通常のルーティングをおこないます。	なし	省略不可

この設定を行わない場合

中継先設定は行なわれません。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

アクションマップ設定モード

set ipv6 traffic-class

アクションとして、IPv6 ヘッダに対するマーキングを設定します。
対象パケットが IPv6 パケットではなかった場合、本設定は無視されます。traffic-class と dscp とは排他となります。
コンフィグ読み込み側での処理とし、dscp が設定されている場合は dscp 設定が優先され traffic-class の設定は無効になります。
dscp が設定されていない場合のみ traffic-class の設定が有効になります。
アクションが指定されなかったヘッダフィールドは、マーキングされずにそのまま転送されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　IPv6 ヘッダに対するマーキングとして、traffic-class の値を 5 に設定する。

```
Router(config)#action-map stream-action
Router(config-action-map)#set ipv6 traffic-class 5
```

コマンド書式

```
set ipv6 traffic-class <traffic-class-value>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
traffic-class-value	traffic-class-value を設定します。	0～255	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set queuing

アクションとして、CBQ もしくは PRIQ によって優先制御や帯域制御を行ないます。
指定したキュー名が定義されていない場合、設定エラーとなり、無視されます。

refresh コマンド後に有効になるコマンドです。

設定例 1　stream-action に stream-que を設定する

```
Router(config)#action-map stream-action
Router(config-action-map)#set queuing stream-que
```

コマンド書式

set queuing <que-name>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
que-name	que-name を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

優先制御や帯域制御は行われません。

設定モード

アクションマップ設定モード

set 802.1p priority

アクションとして、Ethernet ヘッダ 802.1p Priority に対するマーキングを設定します。
アクションが指定されなかった場合、マーキングされずにそのまま転送されます。
出力インタフェースが Ethernet インタフェース（EWAN もしくは LAN）もしくは PPPoE 以外であった場合には、本設定は無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　優先度 7 で、802.1p Priority に対するマーキングを設定する

```
Router(config)#action-map stream-action
Router(config-action-map)# set 802.1p priority 7
```

コマンド書式

set 802.1p priority <優先度 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
優先度	Ethernet ヘッダ 802.1p Priority に対するマーキングの優先度を設定します。	0～7	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

ポリシーマップの定義

class

クラスマップとアクションとを対応付け、クラシフィケーションされたトラフィックに対するアクションを定義します。
複数のクラスが定義された場合、登録順に検索され、最初にマッチしたクラスに対するアクションのみが実行されます。
同一クラスマップ名に対しては、一つのアクションのみ記述できます（同一クラスマップ名に対しては、置換型となります）。

refresh コマンド後に有効になるコマンドです。

設定例１　クラスマップ（video-class）とアクションマップ（stream-action）を対応づける

```
Router(config)# policy-map stream-service
Router(config-policy-map)# class video-class action stream-action
Router(config-policy-map)# class audio-class action stream-action
Router(config-policy-map)# exit
```

コマンド書式

class <class-map-name> action <action-map-name>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
class-map-name	class-map-name を設定します。	16 文字以内の文字列	省略不可
action-map-name	action-map-name を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップとアクションとの対応は定義されません。

設定モード

ポリシーマップ設定モード

policy-map

policy-map モードに移行し、クラスマップによって分類したトラフィックに対して、どのような制御を行なうかを定義します。

ここで指定したポリシーマップを有効にするには、各インタフェース設定モードで、"service-policy input/output"コマンドで登録します。

また、自局送信をポリシールーティングする場合は、"service-policy local"コマンドで登録します。

設定例１　ポリシーマップ設定モードへ移行する

```
Router(config)#policy-map stream-service
Router(config-action-map)#
```

コマンド書式

policy-map <policy-map-name>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
policy-map-name	policy-map-name を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

ポリシーマップの設定を行うことができません。

設定モード

基本設定モード

statistics update

統計情報のカウントを行うかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　統計情報のカウントを行う

```
Router(config)# policy-map stream-service
Router(config-policy-map)# statistics update enable
Router(config-policy-map)# exit
```

コマンド書式

statistics update 〈カウント設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
カウント設定	統計情報のカウントを行うかどうかを指定します。 enable　統計情報のカウントを行う disable　統計情報のカウントを行わない	enable disable	省略不可

この設定を行わない場合

統計情報のカウントを行いません。

設定モード

ポリシーマップ設定モード

ポリシーマップの適用とキューの定義

qos frame-length-offset

CBQ によって帯域制御が行なわれる場合、帯域計算で使用するフレーム長の補正値を指定します。

帯域計算は、適用するインタフェースごとに予め定められたフレームを想定して行なわれますが、必ずしもご使用のネットワーク構成とは一致しない場合があるため、必要に応じて本コマンドによって補正を行うことができます。
なお、インタフェースが PPP を利用する場合は、PPP カプセル化処理により一部の文字列に置き換えが発生しフレーム長が変更されることがあります。
帯域計算は PPP カプセル化処理前に行うため、変更されたフレーム長を正確に補正することができません。
PPPoE カプセル化ではフレーム長の変更が行われないため、このような制限は発生しません。

各インタフェースで、帯域計算に使用されるフレーム長は、以下となります。

lan, ewan, vlanif, pppoe：Ether フレーム長＋24 *1
ipsecif：IP パケット長＋112 *2*4
tunnel：IP/IPv6 パケット長＋66 *5

*1：プリアンブル＋IFG（20 バイト）＋ FCS（4 バイト）がつく想定
*2：プリアンブル＋IFG（20 バイト）＋ FCS（4 バイト）+Ether ヘッダ（14 バイト）+ PPPoE ヘッダ（8 バイト） + IPv4 ヘッダ（20 バイト） + ESP（38 バイト）*3 + パディング（AES 時の想定平均）（8 バイト）がつく想定
*3：ESP ヘッダ(8)、IV(16)、パディング長(1)、次ヘッダ番号(1)、ICV(12)*4
*4：ICV 長は使用するアルゴリズムによって異なります。
・HMAC-MD5： 12 バイト
・HMAC-SHA： 12 バイト
・HMAC-SHA2-256： 16 バイト
・HMAC-SHA2-384： 24 バイト
・HMAC-SHA2-512： 32 バイト
*5：プリアンブル＋IFG（20 バイト）＋ FCS（4 バイト）+Ether ヘッダ（14 バイト）+ PPPoE ヘッダ（8 バイト） + IPv4 ヘッダ（20 バイト）がつく想定

使用するネットワーク環境が、上記想定と異なる場合には、本コマンドを使用して補正を行うことができます。
補正は、上記想定でのフレーム長に対して行ってください。

refresh コマンド後に有効になるコマンドです。

設定例 1　帯域計算で使用するフレーム長を 20 オフセットさせる

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# qos frame-length-offset increment 20
```

コマンド書式

qos frame-length-offset {increment < オフセット値 > | decrement < オフセット値 >}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
increment	フレーム長を増加させる場合のオフセット値を設定します。	0～127	省略不可
decrement	フレーム長を減少させる場合のオフセット値を設定します。	0～128	省略不可

この設定を行わない場合

想定したフレーム長で帯域計算を行います。

最小フレームサイズに関して

各インタフェース毎に、最小フレームサイズが規定されており、本コマンドの指定により最小フレームサイズを下回った場合には、最小フレームサイズで帯域計算を行います。
各インタフェースの最小フレームサイズは以下の通りです。

lan, ewan, vlanif, pppoe：60 バイト
ipsecif, tunnel：なし。常に設定内容どおりに帯域計算を行います

本装置の dialer インタフェースは、想定フレーム長、最小サイズは以下となります。

想定フレーム長：データの IP パケット長＋7 *6
最小フレーム長：7 バイト

*6：HDLC ヘッダ部（3 バイト）+ PPP ヘッダ（2 バイト） + FCS（2 バイト）

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード

qos output bandwidth

インタフェースで使用できる帯域および、QoS の方式を指定します。
帯域は、物理速度と同じ値を設定してください。

refresh コマンド後に有効になるコマンドです。

設定例 1　LAN インタフェースの全帯域を 100Mbps とし、QoS の方式を CBQ とする

```
Router(config)#interface lan 1
Router(config-if lan 1)# qos output bandwidth 100M cbq
```

コマンド書式

qos output bandwidth <最大使用帯域> <QoS 設定>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
最大使用帯域	設定しているインタフェースで、全体の帯域幅（単位：bps）を設定します。 通常は、物理インタフェース速度を設定します。 kbps を示す場合は"K"、Mbps を示す場合は"M"が使用できます。 例）100kbps→"100K"、50Mbps→"50M"	範囲無し	省略不可
QoS 設定	QoS の方式を指定します。 cbq：CBQ（Class-Based Queueing）方式を指定します。 priq：PRIQ（Priority Queueing）方式を指定します。	cbq priq	省略不可

この設定を行わない場合

QoS 制御を行なわない（常にベストエフォート）。帯域幅は物理インタフェース速度。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード

qos-que cbq

QoS 機能において、CBQ で使用するキューを定義します。
キュー名は、アクションマップにおいてキューを指定する際に参照されます。
パラメータ bandwidth で、qos output bandwidth コマンドで指定した帯域の何パーセントをこのキューに割り当てるかを指定します。
また、bps オプションを付けることによって bps 単位で使用帯域を設定することもできます。
borrow が指定されている場合に、親キューの帯域に余裕がある時は、その帯域を利用できることを示します。
Priority はキューからパケットを送信する際の優先度として参照され、7 が最高優先度、0 が最低優先度となります
キュー長は qlimit で指定され、あふれたパケットは廃棄されます。
red(Random EarlyDetection)が指定されている場合、TCP のパケット再送を意図し、あふれる以前の段階でランダムに廃棄が行なわれます。
default を指定すると、本キューがデフォルトキューであることを示し、action-map でキューが指定されなかったパケットがキューイングされます。
parent に"NULL"を指定すると ROOT queue を示すものとします。
delay が指定されている場合、エンキューされた時点から設定時間を超えてキューに溜まり続けたパケットは廃棄されます。
delay 指定がない場合は上記のような動作、時間でパケットを廃棄する動作は行われません。

refresh コマンド後に有効になるコマンドです。

設定例 1　root-que の 10%を video-que の帯域として使用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# qos-que cbq video-que bandwidth 10 parent root-que
```

設定例 2　root-que の帯域から 10Mbps を video-que の帯域として使用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# qos-que cbq video-que bandwidth bps 10M parent root-que
```

コマンド書式

qos-que cbq <キュー名> bandwidth {bps <使用帯域>|<帯域使用率>} parent <キュー名>
[優先度][qlimit <キュー長さ>] [delay <最大遅延時間>] [borrow] [red]
[default]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キュー名	CBQ のキュー名称を設定します。	16 文字以内の文字列	省略不可
使用帯域	帯域幅（単位：bps）を指定します。 帯域幅を指定する際は、数値(1 以上の整数)の先頭に bps オプションを設定します。 kbps を示す場合は"K"、Mbps を示す場合は"M"を使用します。 例）100kbps→"100K"、50Mbps→"50M" IPsec インタフェースに対して帯域制御を行った場合は、送信時に EWAN 側の帯域制御も適用されます。 IPsec インタフェース→EWAN の順に2段階に帯域制御されます。	bps 帯域幅	省略不可
帯域使用率	回線全帯域の帯域幅に対する帯域使用率（単位：%）を指定します。 IPsec インタフェースに対して帯域制御を行った場合は、送信時に EWAN 側の帯域制御も適用されます。 IPsec インタフェース→EWAN の順に2段階に帯域制御されます。	1～100	省略不可
優先度	優先度を指定します。優先度が高いクラスは、優先度の低いクラスに比べ、送信処理の時間が増えます。この値が大きいほど、優先度は高くなります。	0～7	0
最大遅延時間	このクラスの最大遅延時間（単位：?秒）を設定します。	1～999999	0
キュー長	キュー長（パケットの個数）を設定します。	1～200	50
borrow	帯域不足で送信できない場合に、親クラスに空きがあればその帯域を利用するかどうかを指定します。その帯域を利用する場合は、borrow を指定します。	borrow	親クラスの帯域を利用しない
red	キューバッファ管理方式に、RED（Random Early Detection）を使用する場合に、red を指定します。 RED を使用しない場合は、キューバッファがいっぱいになってからパケットを破棄（Tail-Drop）しますが、RED を使用した場合は、キューあふれによる輻輳が発生する前にランダム破棄を開始するため、TCP のようなトラフィックを変動できるようなプロトコルでは、より早く破棄を感知できるので、通信全体でみると効率が良くなります。	red	RED を使用しない
default	デフォルトクラスの場合に指定します。デフォルトクラスは、ルートクラスに属している必要があります。	default	default 以外

この設定を行わない場合

キューは定義されません。
priority のデフォルトは 0、qlimit のデフォルトは 50。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード

qos-que priq

QoS 機能において、PRIQ で使用するキューを定義します。
キュー名は、アクションマップにおいてキューを指定する際に参照されます。
Priority はキューからパケットを送信する際の優先度として参照され、7 が最高優先度、0 が最低優先度となります。
キュー長は qlimit で指定され、あふれたパケットは廃棄されます。RED（Random EarlyDetection）が指定されている場合、TCP のパケット再送を意図し、あふれる以前の段階でランダムに廃棄が行なわれます。
default を指定すると、本キューがデフォルトキューであることを示し、アクションマップでキューが指定されなかったパケットがキューイングされます。

refresh コマンド後に有効になるコマンドです。

設定例 1　voice-que の優先度を 0、キュー長を 50 に設定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# qos-que priq voice-que priority 0 qlimit 50
```

コマンド書式

qos-que priq <キュー名 > priority <優先度> [qlimit <キュー長>] [default] [red]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キュー名	PRIQ のキュー名称を設定します。	16 文字以内の文字列	省略不可
優先度	優先度を指定します。 優先度が高いキューにパケットがある間は、優先度の低いキューからパケットが送出されることはありません。 この値が大きいほど、優先度は高くなります。	0～7	省略不可
キュー長	キュー長（パケットの個数）を設定します。	1～200	50
red	キューバッファ管理方式に、RED（Random Early Detection）を使用する場合に、red を指定します。 RED を使用しない場合は、キューバッファがいっぱいになってからパケットを破棄（Tail-Drop）しますが、RED を使用した場合は、キューあふれによる輻輳が発生する前にランダム破棄を開始するため、TCP のようなトラフィックを変動できるようなプロトコルでは、より早く破棄を感知できるので、通信全体でみると効率が良くなります。	red	RED を使用しない
default	デフォルトクラスの場合に指定します。	default	default 以外

この設定を行わない場合

キューは定義されません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード

service-policy

インタフェースの入出力パケットに対して、サービスポリシーを適用します。
サービスポリシーが未定義であったり、必要な定義が不足したりしている場合、エラーメッセージをelog に出力し、設定は適用されません。
インタフェースの出力パケットに対するサービスポリシーにおいては、以下のアクションは適用されず、無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　入力パケットに対して、ポリシーマップ名 pre-service を適用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# service-policy input pre-service
```

コマンド書式

service-policy 〈入出力設定〉〈ポリシーマップ名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
入出力設定	入力側(input)、出力側(output)のどちらにサービスポリシーを適用するか設定します。	input output	省略不可
ポリシーマップ名	ポリシーマップ名を設定します	16 文字以内の文字列	省略不可

この設定を行わない場合

サービスポリシーは適用されません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード

service-policy local

自局送信パケットに対して、サービスポリシーを適用します。
サービスポリシーが未定義であったり、必要な定義が不足したりしている場合、エラーメッセージを elog に出力し、設定は適用されません。

refresh コマンド後に有効になるコマンドです。

設定例１　自局送信パケットに対して、ポリシーマップ名 local-service を適用する

```
Router(config)#service-policy local local-service
Router(config)#
```

コマンド書式

service-policy local <ポリシーマップ名 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシーマップ名	ポリシーマップ名を設定します	16 文字以内の文字列	省略不可

この設定を行わない場合

サービスポリシーは適用されません。

設定モード

基本設定モード

L2 QoS 機能

L2 QoS 機能

priority 802.1p classification

L2 QoS を動作させる場合に設定します。
受信ポートにて、データの 802.1p 値から受信優先制御を行います。

refresh コマンド後に有効になるコマンドです。

設定例 1　物理ポート 1 で L2 QoS 動作を行う

```
Router(config)#line ewan 1
Router(config line ewan 1)#priority 1 802.1p classification
```

コマンド書式

priority {<1-8> | <host>} 802.1p classification

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
<1-8>|<host>	802.1p 値による受信優先制御を行うポートを物理ポート毎に動作させるか、内部ポートで動作させるかを指定します。 ※ line ewan モードの場合は、"1"のみ選択可能 1～8　物理ポートで動作させる host　内部ポートで動作させる	1～8 host	省略不可

この設定を行わない場合

802.1p による優先制御をおこないません。
設定のないポートからの受信データは全て非優先データとします。

設定モード

Ethernet 設定モード

priority 802.1p default-classification

untag フレームに対して、ドライバの受信を High-Que とするか Low-Que とするかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　untag フレームに対して、ドライバの受信を High-Que とする

```
Router(config)#line ewan 1
Router(config line ewan 1) priority 802.1p default-classification high
```

コマンド書式

priority 802.1p default-classification {high|low}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
high | low	untag フレームに対して、ドライバの受信を High-Que とするか Low-Que とするかを指定します。 high　ドライバの受信を High-Que とする。 low　ドライバの受信を Low-Que とする。	high low	省略不可

この設定を行わない場合

untag フレームは、Low-Que として扱われます。

設定モード

Ethernet 設定モード

priority 802.1p threshold

優先データとして動作するパケットを、802.1p 値で指定します。
802.1p 値が大きいほど優先度が高くなります。

refresh コマンド後に有効になるコマンドです。

設定例 1　優先データとしてあつかうパケットを 802.1p 値 5 とする

```
Router(config)#line lan
Router(config line lan) priority 802.1p threshold 5
```

コマンド書式

priority 802.1p threshold <802.1p 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
802.1p 値	優先データとして動作するパケットを、802.1p 値で指定します。 ここで指定した値以上の 802.1p 値を持つデータを優先データ、ここで指定した値未満の 802.1p 値を持つデータを非優先データとして扱います。 LAN インタフェースに送信する際に、送信キューの中に優先データが存在する場合は、非優先データは送信されません。	0～7	省略不可

この設定を行わない場合

802.1p 値は 4 として動作します。

802.1p 値の優先度に関して

802.1p 値は、優先度を 0～7 で指定することができます。
802.1p のプライオリティレベルは、以下８段階に規定されています。

優先度	802.1p 値	プライオリティレベルの内容
高い	7	予約
↑	6	会議型の音声
↑	5	会話型マルチメディア
↑	4	制御を必要とするアプリケーション
↑	3	クリティカルアプリケーション
↓	2	標準的なストリーム
↓	1	バックグラウンド
↓	0	ベストエフォート
↓		
低い		

設定モード

Ethernet 設定モード

priority port-priority

LAN の各ポート(1～8 および host)からの受信フレームの優先度を設定します。
priority 802.1p threshold 設定で設定した値以上のポートからのフレームは優先、priority 802.1p threshold 設定で設定した値未満のポートからのフレームの場合は非優先として取り扱います。
802.1p のクラシフィケーションを同時に設定している場合は、本設定が優先となります。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN１ポートからの受信フレームの優先度を４とする

```
Router(config)#line lan
Router(config line lan)#priority 1 port-priority 4
```

コマンド書式

```
priority {<1-8> | <host>} port-priority <802.1p 値>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
<1-8>|<host>	受信フレームの優先度を設定する LAN ポートを指定します。 1～8　物理ポートを指定 host　内部ポートを指定	1～8 host	省略不可
802.1p 値	802.1Q VLAN タグがついていなかった場合の 802.1p 値を指定します。	0～7	省略不可

この設定を行わない場合

受信したポートでの QoS は行いません。
常に非優先となります。

802.1p 値の優先度に関して

802.1p 値は、優先度を 0～7 で指定することができます。
802.1p のプライオリティレベルは、以下８段階に規定されています。

優先度	802.1p 値	プライオリティレベルの内容
高い	7	予約
↑	6	会議型の音声
↑	5	会話型マルチメディア
↑	4	制御を必要とするアプリケーション
↓	3	クリティカルアプリケーション
↓	2	標準的なストリーム
↓	1	バックグラウンド
低い	0	ベストエフォート

設定モード

Ethernet 設定モード

UPnP 機能

UPnP 機能

upnp-server access-group

UPnP 機能を利用可能な端末を、アクセスリスト番号で制限します。
permit となった端末のみ、UPnP 機能に対するアクセスやイベント受信が可能になります。
ただし、マルチキャストによるアナウンスメッセージは、本設定とは関係なく、パケット到達可能範囲の全端末が受信することができます。

refresh コマンド後に有効になるコマンドです。

設定例 1　アクセス番号 90 番の端末の UPnP 機能を制限する

```
Router(config)#upnp-server access-group 90
```

コマンド書式

upnp-server access-group <access-list 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	UPnP 機能の利用を制限する端末を指定します。	1～99	省略不可

この設定を行わない場合

UPnP 機能を利用する端末を制限しません。

設定モード

基本設定モード

upnp-server enable

UPnP 機能を使用する場合に設定します。
UPnP 機器は、LAN#1 インタフェースのみ使用することが出来ます。

refresh コマンド後に有効になるコマンドです。

設定例 1　UPnP 機能を使用する場合

```
Router(config)#upnp-server enable
```

コマンド書式

```
upnp-server enable
```

パラメータ

パラメータはありません

この設定を行わない場合

UPnP 機能を使用することができません。

設定モード

基本設定モード

upnp-server target-interface

グローバルアドレスとしてどのインタフェースのアドレスを使用するかを指定します。
UP しているインタフェースのうち、priority が最も小さいインタフェースを使用します。
ただし、同じ priority の場合には、config に表示される順となります。

refresh コマンド後に有効になるコマンドです。

設定例 1　PPPoE 1 を UPnP 機能を使用するインタフェースに指定する

```
Router(config)#upnp-server target-interface pppoe1
```

コマンド書式

upnp-server target-interface <インタフェース名> [priority]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	UPnP 機能を使用するインタフェースを指定します。	ewan 1～2 pppoe 1～24 dialer 1～20	省略不可
priority	UPnP 機能を使用するインタフェースの優先度を指定します。	0～100	50

この設定を行わない場合

設定をしていないインタフェースで、UPnP 機能を使用できません。
全てのインタフェースを設定していない場合は、Connection サービスは down 状態とみなします。

設定モード

基本設定モード

モデム接続機能

モデム接続機能

auto connect

データ発生時に、データ通信端末によるワイヤレス接続を自動的に行うかどうかの設定をします。
refresh コマンド後に有効になるコマンドです。

設定例 1　常時接続モードを有効にし再接続間隔を 5 秒にする

```
Router(config)#interface modem 1
Router(config-if modem 1)#auto connect on continuous delay 5
```

設定例 2　データ発生時に自動接続を行わない

```
Router(config)#interface modem 1
Router(config-if modem 1)#auto connect off
```

コマンド形式

```
auto connect {on [continuous [delay <1-255>]] | off}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
on | off	データ発生時に自動的に接続する(on)か、接続しない(off)かを設定します。	on off	省略不可
continuous	常時接続モードを有効にする場合に指定します。	continuous	常時接続モード無効
delay	常時接続モードを有効とした場合の回線切断後から再接続するまでの間隔(単位:秒)を設定します。	1～255	回線切断後即再接続

この設定を行わない場合

データ発生時に、データ通信端末によるワイヤレス接続を自動的に行います。

設定モード

モデムインタフェース設定モード

caller

接続先アクセスポイントの電話番号を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　接続するアクセスポイントの電話番号を*99***1#に設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#caller *99***1#
```

コマンド形式

caller 〈AP 電話番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
AP 電話番号	接続するアクセスポイントの電話番号を設定します。	32 桁以下の英数字・記号	省略不可

この設定を行わない場合

発信によるワイヤレス回線の接続ができません。

設定モード

ダイヤラーインタフェース設定モード

disable

disable コマンドを設定することにより、データ通信端末に問題が発生した場合に行うモデムの初期化や、データ通信端末の初期化を行っても復旧しない場合の装置リセットを抑制することができます。

refresh コマンド後に有効になるコマンドです。

設定例１　データ通信端末の初期化、装置のリセットを行わない

```
Router(config)#interface modem 1
Router(config-if modem 1)#disable modem-reset system-reset
```

コマンド書式

disable〈初期化抑制項目〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
初期化抑制項目	抑制したい初期化およびリセット処理を指定します。 パラメータをスペースで区切り(modem-reset system-reset)入力することにより、データ通信端末の初期化および、装置のリセット処理の両方を停止することも可能です。 modem-reset：データ通信端末の初期化を実施しません。 system-reset：データ通信端末の初期化を実施してもデータ通信端末が復旧しない場合の装置リセットを実施しません。	modem-reset system-reset	省略不可

この設定を行わない場合

データ通信端末に問題が発生した場合にモデムを初期化します。
また、データ通信端末の初期化を行っても復旧しない場合に装置リセットを行います。

設定モード

モデムインタフェース設定モード

forced disconnect cumulative-time

1ヶ月で許可する累積許容時間を指定します。
累積許容時間がここで設定した値を超えた場合は、現在接続中であれば切断し、以降の発信動作を停止します。
mail to コマンドを設定することにより、プレアラート値に到達した時、および設定時間を超えた時にメールで通知することができます。
calender set コマンドや、SNTP 機能により、現在時刻の内容に、月が進む変更があった場合は、課金リミッタの状態を初期化します。

・毎月 1 日の 0:0:0 に、課金リミッタ情報はクリアされます。
その際、発信が制限されている状態も解除されます。
・現在の状況は、show limiter cumulative-time status コマンドで確認できます。
・発信が制限されている場合は、clear forced disconnect cumulative-time modem で解除することができます。

refresh コマンド後に有効になるコマンドです。

※回線接続中に設定を変更して refresh した場合、タイマはそのまま保持されます。
また、強制切断のタイマが設定値を超えていた場合、接続は強制的に解除されます。

設定例１　1ヶ月の累積許容時間を 2000 分に制限する

```
Router(config)#interface modem 1
Router(config-if modem 1)#forced disconnect cumulative-time 2000
```

コマンド形式

forced disconnect cumulative-time <累積許容時間> [プレアラート値 | warning-only]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
累積許容時間	1ヶ月の接続累積許容時間(分)を設定します。 off を指定することで制限を無効にします。	60～2400 off	省略不可
プレアラート値	設定した累積許容時間に対して、警告を発する値(単位:%)を設定します。	1～99	設定値の 90%で警告状態となります。
warning-only	warning-only を指定することで、累積許容時間を超えた場合にログを残しますが、回線は接続されたままになります。	warning-only	

この設定を行わない場合

累積許容時間を制限しません。

設定モード

モデムインタフェース設定モード

forced disconnect packet

1 日(24 時間)で送受信を許可するパケット数を指定します。
送受信パケット数がここで設定した値を超えた場合は、現在接続中であれば切断し、以降の発信動作を停止します。
mail to コマンドを設定することにより、許容パケット数の 90%に達したとき、および許容パケット数を超えたときに、メールで通知することできます。
forced disconnect cumulative-time コマンドとは異なり、発信制限がかかると、自動では解除されません。
発信制限は、clear forced disconnect packet modem コマンドにより解除できます。

・現在の状況は、show limiter packet status コマンドで確認できます。
・発信が制限されている場合は、clear forced disconnect packet で解除することができます。

refresh コマンド後に有効になるコマンドです。

※回線接続中に設定を変更して refresh した場合、タイマはそのまま保持されます。
また、強制切断のタイマが設定値を超えていた場合、接続は強制的に解除されます。

設定例 1　24 時間の送受信パケット数を 75000 パケットに制限する

```
Router(config)#interface modem 1
Router(config-if modem 1)#forced disconnect packet 75000
```

コマンド形式

forced disconnect packet <上限パケット数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
上限パケット数	1 日(24 時間)で送受信を許可するパケット数を指定します。off を指定することによりパケット数の制限が無くなります。 ※このパケット数は、ルータ内部で算出している数値であり、目安です。	off 1～ 4294967294	省略不可

この設定を行わない場合

送受信を許可するパケット数を制限しません。

参考

1 パケットは、128 バイトのユーザデータとして算出しています。

設定モード

モデムインタフェース設定モード

idle-timer send

送信データに関する無通信監視時間(秒)を設定します。
ここで指定した時間送信データがない場合は、データ通信端末によるワイヤレス接続を切断します。

refresh コマンド後に有効になるコマンドです。

設定例 1　送信データに関する無通信監視時間を 60 秒に設定する

```
Router(config)#interface modem 1
Router(config-if modem 1)#idle-timer send 60
```

コマンド形式

idle-timer send <無通信監視時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
無通信監視時間	送信データに関する無通信監視時間を設定します。 off を指定することで、無通信監視を無効にします。	off 1～3600	省略不可

この設定を行わない場合

送信するデータが 60 秒間無い場合は、データ通信端末によるワイヤレス接続を切断します。

設定モード

モデムインタフェース設定モード

idle-timer receive

受信データに関する無通信監視時間(秒)を設定します。
ここで指定した時間受信データがない場合は、データ通信端末によるワイヤレス接続を切断します。

refresh コマンド後に有効になるコマンドです。

設定例 1　受信データに関する無通信監視時間を 60 秒に設定する

```
Router(config)#interface modem 1
Router(config-if modem 1)#idle-timer receive 60
```

コマンド形式

idle-timer receive <無通信監視時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
無通信監視時間	受信データに関する無通信監視時間を設定します。 off を指定することで、無通信監視を無効にします。	off 1～3600	省略不可

この設定を行わない場合

受信するデータが 60 秒間無い場合は、データ通信端末によるワイヤレス接続を切断します。

設定モード

モデムインタフェース設定モード

ip address

自装置のダイヤラーインタフェースの IP アドレスを設定します。
接続相手先からアドレスを割り振ってもらう場合は「negotiated」を指定します。
該当するワイヤレス回線が接続中の場合は強制切断します。また、ルート情報も変更します。

refresh コマンド後に有効になるコマンドです。

設定例 1　IP アドレスを 10.1.1.1、サブネットマスクを 255.255.255.0 に設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#ip address 10.1.1.1 255.255.255.0
```

コマンド書式

ip address <IP アドレス>

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>IP アドレス</td><td>ワイヤレス接続で使用するダイヤラーインタフェースの IP アドレスを設定します。<table><tr><td>negotiated</td><td>接続相手から IP アドレスを割り振ってもらう場合</td></tr><tr><td>IPv4 アドレス形式</td><td>IP アドレスとサブネットマスクを IPv4 アドレス形式で設定する場合。</td></tr></table></td><td>negotiated
IPv4 アドレス形式</td><td>省略不可</td></tr>
</table>

この設定を行わない場合

データ通信端末を使用したワイヤレス接続を行うことができません。
設定を行わない場合は、ip address negotiated として機能します。

設定モード

ダイヤラーインタフェース設定モード

ip access-group

access-list コマンドで指定したフィルタリングデータを、各インタフェースで適用します。
フィルタリングデータは、各インタフェースで受信したパケットに適用するのか、送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　access-list 1 で指定したデータを、PPPoE1 送信時に適用する

```
Router(config)#interface pppoe 1
Router(config-if lan 1)#ip access-group 1 out
```

設定例２　access-list 2 で指定したデータを、PPPoE1 からの受信時に適用する

```
Router(config)#interface pppoe 1
Router(config-if lan 1)#ip access-group 2 in
```

コマンド書式

ip access-group <access-list 番号> { in [interface | vpn]| out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	フィルタリングのデータを設定したアクセスリストの番号を指定します。	1～99 100～199 1300～1999 2000～2699 10000～11200 20000～21199	省略不可
{ in[interface | vpn]| out }	インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。 受信時は、さらに以下のように設定ができます。 in vpn：自局宛 VPN 対象パケットを制御 in interface：自局宛非 VPN 対象パケットを制御	in in vpn in interface out	省略不可

LAN インタフェースおよび IPsec インタフェースでは、vpn を選択することはできません。
in vpn および in interface を選択した場合、適用する access-list の宛先は、any とする必要があります。

この設定を行わない場合

該当インタフェースでは、IP パケットフィルタリングを使用しません。

IP フィルタリングについて

指定したパケット以外は中継しないといったように、セキュリティ強化のため使用する機能です。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード
BVI インタフェース設定モード
USB Ethernet インタフェース設定モード

ip nat inside source

そのインタフェースから送信するパケットの送信元アドレスの変換ルールを設定します。
NAT モードの場合と、NAT+モード(IP マスカレード)の場合で、設定のしかたが異なりますので注意してください。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例 1　NAT 変換（192.168.0.0/24　→　158.xxx.xxx.2～158.xxx.xxx.7）

```
Router(config)#interface ewan 1
Router(config-if ewan1)#ip nat inside source list 1 pool pool1



Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255   ←list 1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.2 158.xxx.xxx.7 ←pool1 の部分の設定
```

【解説】
ip nat inside source <変換前のアドレス範囲> <変換後のアドレス範囲>となります。
<変換前のアドレス範囲>は、access-list コマンドで指定します。
<変換後のアドレス範囲>は、ip nat pool <pool 名>コマンドで指定します。

設定例 2　NAT+変換（192.168.0.0/24　→　インタフェースアドレス）

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat inside source list 1 interface



Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list 1 の部分の設定
```

【解説】
ip nat inside source <変換前のアドレス範囲> <変換後のアドレス範囲>となります。
<変換前のアドレス範囲>は、access-list コマンドで指定します。
<変換後のアドレス範囲>は、インタフェースアドレスに集約しますので、"interface"と指定します。

設定例３　NAT 変換（スタティック登録）　設定例１の中で 192.168.0.1⇔158.xxx.xxx.2 のみ固定変換

```
Router(config)#interface ewan 1
Router(config-if ewan1)#ip nat inside source static 192.168.0.1 158.xxx.xxx.2
Router(config-if ewan1)#ip nat inside source list 1 pool pool1



Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255  ←list 1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.3 158.xxx.xxx.7 ←pool1 の部分の設定
```

【解説】

設定例1とほぼ同じです。

違う点は、ip nat inside source static で、NAT スタティック変換をしている箇所ですが、この場合も、ip nat inside source <変換前のアドレス> <変換後のアドレス>となります。

設定例４　NAT 変換（一括変換）192.168.100.0/24←→158.ｘｘｘ.ｘｘｘ.0/24 に変換する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat inside source static-subnet 192.168.100.0 158.xxx.xxx.0
255.255.255.0
```

【解説】

ip nat inside source static-subnet <変換前の送信元ネットワークアドレス> <変換後の送信元ネットワークアドレス> <サブネットマスク>となります。

グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。

NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます（複数同時登録）。

例）local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT 時】
ip nat inside source list <access-list 番号> [変換前開始ポート番号 [変換前終了ポート番号]] pool <プール名> [overload | [変換後開始ポート番号 [変換後終了ポート番号]]]

【NAT+時】
ip nat inside source list <access-list 番号> [開始ポート番号 [終了ポート番号]] interface [overload | [変換後開始ポート番号 [変換後終了ポート番号]]]

【スタティック変換】
ip nat inside source static <変換前のアドレス> <変換後のアドレス>

【NAT スタティック（一括変換）】
ip nat inside source static-subnet <変換前のネットワークアドレス> <変換後のネットワークアドレス> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前のアドレス範囲を指定したアクセスリストを指定します。	1～99 1300～1399 10000～11200	省略不可
[変換前開始ポート番号 変換前終了ポート番号]	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
プール名	変換後のアドレス範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	NAT の場合は省略不可
interface	インタフェースのアドレスに NAT+変換します。	interface	NAT+の場合は省略不可
overload	local のポート番号を必ず別のポート番号に変換する場合に指定 ※変換後のポート番号は 1024～65535	overload	local のポート番号を基本的には変換せずに napt を試みます。 すでにそのポート番号が使用されている場合に限り、別のポート番号に変換します。 変換後のポート番号は 1024～65535。
[変換後開始ポート番号 変換後終了ポート番号]	変換後の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
変換前のアドレス	変換前の送信元アドレスを指定します。	IPv4 アドレス形式	省略不可

変換後のアドレス	変換後の送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
変換前のネットワークアドレス	変換前の送信元ネットワークアドレスを指定します。 static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
変換後のネットワークアドレス	変換後の送信元ネットワークアドレスを指定します。 static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ：スタティック 5000 エントリ、リスト 128 エントリ
送信パケットに対する NAT（ip nat inside source＋ip nat outside destination）の合計となります。

この設定を行わない場合

アドレス変換は行いません。

適用順序

NAT 変換ルールは以下の順序で適用されます。

1）static 変換ルール
2）list による変換ルール

同じ種類のルール内では、Prefix 長が長いルールが優先して適用されます。
同一 Prefix 長の設定が複数あった場合には、config 上で先に登録されたものが優先されます。
なお、config には、以下の順に登録され、同じ種類については入力順に登録されます。

1）static 変換ルール（既存のホストアドレス指定）
2）static-subnet 変換ルール
3）list による変換ルール

IPsec インタフェースで NAT を使用する上での注意事項 ※V01.03(00)以降サポート

・VPN-NAT と、IPsec インタフェースでの NAT の、それぞれ設定に不整合がない場合は、
　IPsec インタフェースの NAT が有効となり、VPN-NAT は無効となります。
・IPsec インタフェースの動的割り当てには対応していません。
　IKEv1: mode-config
　IKEv2: Configuration-Payload
・IPsec インタフェースで NAT 変換する場合でも、該当 SA のセレクタ交換時に使用する
　Phase2-ID は、自動的に変換しません。NAT 変換後のアドレスでセレクタ交換しなくて
　はいけないケースでは、set security-association ipsec-src-id コマンドを利用してください。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
IPsec インタフェース設定モード
ダイヤラーインタフェース設定モード
トンネルインタフェース設定モード
USB-Ethernet インタフェース設定モード

ip nat inside destination

そのインタフェースで受信するパケットの宛先アドレスの変換ルールを設定します。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（スタティック登録）　158.xxx.xxx.2 宛で受信したら 192.168.0.1 に変換する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat inside destination static 158.xxx.xxx.2 192.168.0.1
```

【解説】
ip nat inside destination static <変換前の宛先アドレス> <変換後の宛先アドレス>となります。

設定例２　NAT+変換（スタティック登録）　158.xxx.xxx.2:ポート番号 1500 で受信したら、192.168.0.1:ポート番号 80 に変換する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat inside destination static 158.202.232.1 1500 192.168.0.1 80
```

【解説】
ip nat inside destination static <変換前の送信元アドレス　ポート番号> <変換後の宛先アドレス　ポート番号>となります。

設定例３　NAT 変換（一括変換）158.xxx.xxx.xxx.0/24⇔192.168.100.0/24 に変換する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat inside destination static-subnet 158.xxx.xxx.xxx.0 192.168.100.0
255.255.255.0
```

【解説】
ip nat inside destination static-subnet <変換前のネットワークアドレス> <変換後のネットワークアドレス> <サブネットマスク>となります。
グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。
NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます（複数同時登録）。

例）local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT スタティック（複数指定）時】
ip nat inside destination list <access-list 番号> [開始ポート番号 [終了ポート番号]] pool <プール名> [ポート番号]

【NAT スタティック（1 対 1 変換）、NAT+スタティック時】
ip nat inside destination static <変換前のアドレス> [開始ポート番号 [終了ポート番号]] <変換後のアドレス> [ポート番号]

【NAT スタティック（一括変換）】
ip nat inside destination static-subnet <変換前のネットワークアドレス> <変換後のネットワークアドレス> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前のアドレス範囲を指定したアクセスリストを指定します。	1～99 1300～1399 10000～11200	省略不可
変換前のアドレス	変換前の宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
[開始ポート番号 終了ポート番号]	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	ポート変換しない
プール名	変換後のアドレス範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	省略不可
変換後のアドレス	変換後の宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
ポート番号	変換後の TCP/UDP ポート番号を指定します。	1～65535	ポート変換しない
変換前のネットワークアドレス	変換前の宛先ネットワークアドレスを指定します。 static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
変換後のネットワークアドレス	変換後の宛先ネットワークアドレスを指定します。 static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ：スタティック 5000 エントリ、リスト 128 エントリ
受信パケットに対する NAT(ip nat inside destination＋ip nat outside source)の合計となります。

この設定を行わない場合

アドレス変換は行いません。

適用順序

NAT 変換ルールは以下の順序で適用されます。

1）static 変換ルール
2）list による変換ルール

同じ種類のルール内では、Prefix 長が長いルールが優先して適用されます。
同一 Prefix 長の設定が複数あった場合には、config 上で先に登録されたものが優先されます。
なお、config には、以下の順に登録され、同じ種類については入力順に登録されます。

1）static 変換ルール（既存のホストアドレス指定）
2）static-subnet 変換ルール
3）list による変換ルール

IPsec インタフェースで NAT を使用する上での注意事項 ※V01.03(00)以降サポート

・VPN-NAT と、IPsec インタフェースでの NAT の、それぞれ設定に不整合がない場合は、
　IPsec インタフェースの NAT が有効となり、VPN-NAT は無効となります。
・IPsec インタフェースの動的割り当てには対応していません。
　IKEv1: mode-config
　IKEv2: Configuration-Payload
・IPsec インタフェースで NAT 変換する場合でも、該当 SA のセレクタ交換時に使用する
　Phase2-ID は、自動的に変換しません。NAT 変換後のアドレスでセレクタ交換しなくて
　はいけないケースでは、set security-association ipsec-src-id コマンドを利用してください。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
IPsec インタフェース設定モード
ダイヤラーインタフェース設定モード
トンネルインタフェース設定モード

ip nat outside source

そのインターフェースで受信するパケットの送信元アドレスの変換ルールを設定します。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（192.168.0.0/24　→　158.xxx.xxx.2～158.xxx.xxx.7）

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside source list 1 pool pool1

Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←ist 1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.2 158.xxx.xxx.7 ←pool1 の部分の設定
```

【解説】
ip nat outside source <変換前の送信元アドレス範囲> <変換後の送信元アドレス範囲>となります。
<変換前の送信元アドレス範囲>は、access-list コマンドで指定します。
<変換後の送信元アドレス範囲>は、ip nat pool <pool 名>コマンドで指定します。

設定例２　NAT+変換（192.168.0.1：～80　→　192.168.100.1：8080）

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat outside source static 192.168.0.1 80 192.168.100.1 8080
```

【解説】
ip nat outside source static <変換前の送信元アドレス　ポート番号> <変換後の送信元アドレス　ポート番号>となります。

設定例３　NAT 変換（スタティック登録）　設定例１の中で 192.168.0.1⇔158.xxx.xxx.2 のみ固定変換

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside source static 192.168.0.1 158.xxx.xxx.2
Router(config-if lan 1)#ip nat outside source list 1 pool pool1
Router(config-if lan 1)#ip nat outside destination static 158.xxx.xxx.2 192.168.0.1

Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list 1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.3 158.xxx.xxx.7 ← pool1 の部分の設定
```

【解説】
設定例1とほぼ同じです。
違う点は、ip nat outside source static で、NAT スタティック変換をしている箇所ですが、この場合も、
ip nat inside source <変換前の送信元アドレス> <変換後の送信元アドレス>

となります。
この場合、ip nat outside destination コマンドを使用して、グローバル側→ローカル側のスタティック登録を行なう必要があります。(①の部分)

設定例４　NAT 変換（一括変換）192.168.100.0/24←→158.ｘｘｘ.ｘｘｘ.0/24 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside source static-subnet 192.168.100.0 158.xxx.xxx.0
255.255.255.0
```

【解説】

ip nat outside source static-subnet <変換前の送信元ネットワークアドレス> <変換後の送信元ネットワークアドレス> <サブネットマスク>となります。

グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。

NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます(複数同時登録)。

例)local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
: :
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT 時】
ip nat outside source list <access-list 番号> pool <プール名>

【NAT+時】
ip nat outside source list <access-list 番号> [変換前開始ポート番号 [変換前終了ポート番号]] pool <プール名> [変換後ポート番号]

【スタティック変換】
ip nat outside source static <変換前のアドレス> [変換前開始ポート番号 [変換前終了ポート番号]] <変換前のアドレス> [変換後ポート番号]

【NAT スタティック（一括変換）】
ip nat outside source static-subnet <変換前のネットワークアドレス> <変換後のネットワークアドレスト> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前のアドレス範囲を指定したアクセスリストを指定します。	1～99 1300～1399 10000～11200	省略不可

変換前開始ポート番号 変換前終了ポート番号	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
プール名	変換後のアドレス範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	NAT の場合は省略不可
変換後開始ポート番号 変換後終了ポート番号	変換後の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
変換前のアドレス	変換前の送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
変換後のアドレス	変換後の送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
変換前のネットワークアドレス	変換前の送信元アドレスを指定します。static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
変換後のネットワークアドレス	変換後の送信元アドレスを指定します。static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ:スタティック 5000 エントリ、リスト 128 エントリ
受信パケットに対する NAT(ip nat inside destination＋ip nat outside source)の合計となります。
※ この印がついた設定範囲は、V01.13(00)以降サポート

この設定を行わない場合

アドレス変換は行いません。

適用順序

NAT 変換ルールは以下の順序で適用されます。

1)static 変換ルール
2)list による変換ルール

同じ種類のルール内では、Prefix 長が長いルールが優先して適用されます。
同一 Prefix 長の設定が複数あった場合には、config 上で先に登録されたものが優先されます。
なお、config には、以下の順に登録され、同じ種類については入力順に登録されます。

1)static 変換ルール(既存のホストアドレス指定)
2)static-subnet 変換ルール
3)list による変換ルール

IPsec インタフェースで NAT を使用する上での注意事項 ※V01.03(00)以降サポート

・VPN-NAT と、IPsec インタフェースでの NAT の、それぞれ設定に不整合がない場合は、
IPsec インタフェースの NAT が有効となり、VPN-NAT は無効となります。
・IPsec インタフェースの動的割り当てには対応していません。
IKEv1: mode-config
IKEv2: Configuration-Payload
・IPsec インタフェースで NAT 変換する場合でも、該当 SA のセレクタ交換時に使用する
Phase2-ID は、自動的に変換しません。NAT 変換後のアドレスでセレクタ交換しなくて
はいけないケースでは、set security-association ipsec-src-id コマンドを利用してください。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
IPsec インタフェース設定モード
ダイヤラーインタフェース設定モード
トンネルインタフェース設定モード

ip nat outside destination

そのインターフェースから送信するパケットの宛先アドレスの変換ルールを設定します。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（スタティック登録）　192.168.0.1 宛で受信したら 158.xxx.xxx.2 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside destination static  192.168.0.1 158.xxx.xxx.2
```

【解説】
ip nat outside destination static <変換前の宛先アドレス> <変換後の宛先アドレス>
となります。

設定例２　NAT+変換（スタティック登録）　158.xxx.xxx.2:ポート番号 1500 で受信したら、192.168.0.1:ポート番号 80 に変換する

```
Router(config)#access-list 1 permit 158.xxx.xxx..2
Router(config)#ip nat pool pl-1 192.168.0.1 192.168.0.1
Router(config)#
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside destination list 1 1500 pool pl-1 80
```

【解説】
ip nat outside destination static <変換前の宛先アドレス　ポート番号> <変換後の宛先アドレス　ポート番号>
となります。

設定例３　NAT 変換（一括変換）158.xxx.xxx.xxx.0/24⇔192.168.100.0/24 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside destination static-subnet 158.xxx.xxx.xxx.0 192.168.100.0
255.255.255.0
```

【解説】
ip nat outside destination static-subnet <変換前のネットワークアドレス> <変換後のネットワークアドレス> <サブネットマスク>となります。
グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。
NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます（複数同時登録）。

例）local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0

192.168.100.1 ⇔ 158.xxx.xxx.1
: :
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT スタティック（複数指定）時】
ip nat outside destination list <access-list 番号> [変換前開始ポート番号 [変換前終了ポート番号]] pool <プール名> [変換後ポート番号]

【NAT スタティック（1 対 1 変換）、NAT+スタティック時】
ip nat outside destination static <変換前のアドレス> <変換後のアドレス>

【NAT スタティック（一括変換）】
ip nat outside destination static-subnet <変換前のネットワークアドレス> <変換後のネットワークアドレス> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前のアドレス範囲を指定したアクセスリストを指定します。	1～99 1300～1399 10000～11200	省略不可
変換前のアドレス	変換前の宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
開始ポート番号 終了ポート番号	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	ポート変換しない
プール名	変換後のアドレス範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	省略不可
変換後のアドレス	変換後の宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
ポート番号	変換後の TCP/UDP ポート番号を指定します。	1～65535	ポート変換しない
変換前のネットワークアドレス	変換前の宛先ネットワークアドレスを指定します。 static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
変換後のネットワークアドレス	変換後の宛先ネットワークアドレスを指定します。 static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ：スタティック 5000 エントリ、リスト 128 エントリ
送信パケットに対する NAT(ip nat inside source＋ip nat outside destination)の合計となります。

この設定を行わない場合

アドレス変換は行いません。

適用順序

NAT 変換ルールは以下の順序で適用されます。

1）static 変換ルール
2）list による変換ルール

同じ種類のルール内では、Prefix 長が長いルールが優先して適用されます。
同一 Prefix 長の設定が複数あった場合には、config 上で先に登録されたものが優先されます。
なお、config には、以下の順に登録され、同じ種類については入力順に登録されます。

1）static 変換ルール（既存のホストアドレス指定）
2）static-subnet 変換ルール
3）list による変換ルール

IPsec インタフェースで NAT を使用する上での注意事項 ※V01.03(00)以降サポート

・VPN-NAT と、IPsec インタフェースでの NAT の、それぞれ設定に不整合がない場合は、
　IPsec インタフェースの NAT が有効となり、VPN-NAT は無効となります。
・IPsec インタフェースの動的割り当てには対応していません。
　IKEv1: mode-config
　IKEv2: Configuration-Payload
・IPsec インタフェースで NAT 変換する場合でも、該当 SA のセレクタ交換時に使用する
　Phase2-ID は、自動的に変換しません。NAT 変換後のアドレスでセレクタ交換しなくて
　はいけないケースでは、set security-association ipsec-src-id コマンドを利用してください。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
IPsec インタフェース設定モード
ダイヤラーインタフェース設定モード
トンネルインタフェース設定モード

lcp keepalive

データ通信端末を利用したワイヤレス接続を常時接続モードで使用する場合に、LCP Echo による KeepAlive でデータ通信端末の接続確認を行う場合に指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　LCP Echo による KeepAlive を行う

```
Router(config)#interface dialer 1
Router(config-if dialer 1)# lcp keepalive
```

コマンド形式

lcp keepalive [送信間隔 [retry <再送回数>]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	LCP Echo フレームの送信間隔(単位:秒)を指定します。	10～120	60 秒間隔
再送回数	LCP Echo の応答がない場合に行う再送の回数を指定します。ここで指定した回数応答がなかった場合は、ワイヤレス接続回線を切断します。 ※retry 以降を省略し、送信間隔のみ指定した場合の再送回数は2回となります。	0～10	省略不可

この設定を行わない場合

LCP Echo による KeepAlive を行いません。

設定モード

ダイヤラーインタフェース設定モード

lcp maxtimes

LCP の再送回数の設定をします。

refresh コマンド後に有効になるコマンドです。

設定例 1　LCP の再送回数を 5 回に設定する

```
Router(config)#interface modem 1
Router(config-if modem 1)#lcp maxtimes 5
```

コマンド形式

lcp maxtimes〈再送回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
再送回数	LCP の再送回数を設定します。	0～255	省略不可

この設定を行わない場合

LCP の再送回数を 10 回に設定します。

設定モード

モデムインタフェース設定モード

lcp restart

LCP のリスタート時間の設定をします。

refresh コマンド後に有効になるコマンドです。

設定例 1　LCP のリスタート時間を 1000msec に設定する

```
Router(config)#interface modem 1
Router(config-if modem 1)#lcp restart 100
```

コマンド形式

lcp restart <リスタート時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リスタート時間	LCP のリスタート時間(単位:10msec)を設定します。	100～6000	省略不可

この設定を行わない場合

LCP のリスタート時間を 3000msec に設定します。

設定モード

モデムインタフェース設定モード

logging signal-level

電波状態が取得できるデータ通信端末がアタッチ状態であり、かつ電波状態が取得可能な場合に限り、指定時間毎にその電波状態を slog に記録します。
電波状態が取得できないデータ通信端末の場合や、電波状態が確定していない場合は slog の記録は行いません。

refresh コマンド後に有効になるコマンドです。

設定例１　２分ごとにデータ通信端末の電波状態を slog に記録する

```
Router(config)#interface modem 1
Router(config-if modem 1)#logging signal-level interval 120
```

コマンド形式

logging signal-level [interval <記録間隔>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
記録間隔	電波状態を slog に記録する間隔(単位:秒)を設定します。	10～86400	300 秒ごとに記録します。

※ データ通信端末が通信中の場合は、電波状態を取得できません。

この設定を行わない場合

データ通信端末の電波状態を slog に記録しません。

slog 記録例

slog には、次のようにデータ通信端末の電波状態が記録されます。

```
Router#show slog
00005 0000:34:47.72 2014/12/07 (mon) 18:07:20   5 00000000 00000000
      Modem 1 signal level 3 at 2014/12/07 17:57:10 (0000:04:35:00)
              ^^^^^^(1)^^^^^   ^^^^^^^^(2)^^^^^^^^  ^^^^^^(3)^^^^^
```

(1):ロギング時に検知されている電波レベル(0(圏外)～4(最大))※
(2):ロギングした電波レベルを検知した時刻(年月日時分秒)
(3):記録されたレベルに変化してからの経過時間(日時分秒)

※ 電波レベルは、データ通信端末により最大値が異なります。

設定モード

モデムインタフェース設定モード

logging signal-quality

+CSQ コマンドに対応したデータ通信端末がアタッチ状態であり、かつ電波信号品質が取得可能な場合に限り指定時間毎にその電波信号品質を slog に記録します。
電波信号品質が取得できないデータ通信端末の場合や、電波信号品質が確定していない場合は slog の記録は行いません。

refresh コマンド後に有効になるコマンドです。

設定例１　２分ごとにデータ通信端末の電波信号品質を slog に記録する

```
Router(config)#interface modem 1
Router(config-if modem 1)#logging signal-quality 120
```

コマンド形式

logging signal-quality [interval <記録間隔>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
記録間隔	電波信号品質を slog に記録する間隔（単位：秒）を設定します。	10～86400	300 秒ごとに記録します。

※ データ通信端末が通信中の場合は、電波信号品質を取得できません。

この設定を行わない場合

データ通信端末の電波信号品質を slog に記録しません。

slog 記録例

slog には、次のようにデータ通信端末の電波信号品質が記録されます。

```
Router#show slog
00005 0000:34:47.72 2014/05/17 (mon) 18:07:20   5 00000000 00000000
      Modem 1 signal quality -100dBm at 2014/05/17 17:57:10 (0000:04:35:00)
                ^^^^^^^^^^(1)^^^^^^^^^^    ^^^^^^^^(2)^^^^^^^^  ^^^^^^(3)^^^^^
```

(1)：ロギング時に検知されている電波信号品質（-113dBm（最低）～-51dBm（最高））※
(2)：ロギングした電波信号品質を検知した時刻（年月日時分秒）
(3)：記録された電波信号品質に変化してからの経過時間（日時分秒）
※電波信号品質は、データ通信端末により最高値が異なります。

設定モード

モデムインタフェース設定モード

max-call

データ通信端末によるワイヤレス接続で、リミッタが動作する1時間あたりの接続回数の設定をします。
設定を変更して refresh した場合、リミッタが動作していれば解除し、カウンタもゼロクリアされます。

refresh コマンド後に有効になるコマンドです。

設定例１　リミッタが動作する 1 時間あたりの接続回数を 100 回に設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#max-call 100
```

コマンド形式

max-call〈リミッタが動作する回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リミッタが動作する回数	ワイヤレス接続で、リミッタが動作する1時間あたりの接続回数の設定をします。 off を指定すると、接続回数制限の監視を行いません。	1～1000 off	省略不可

この設定を行わない場合

データ通信端末によるワイヤレス接続で、1時間あたりの発呼回数を 40 回にします。

設定モード

ダイヤラーインタフェース設定モード

modem out-strings special-init

データ通信端末固有の設定情報等を設定することができます。
GL03D で、回線種別(LTE or 3G)を指定する場合に設定します。
詳細は、設定例のページを参照してください。

refresh コマンド後に有効になるコマンドです。

コマンド形式

modem out-strings special-init <シーケンス番号> <設定情報>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
シーケンス番号	シーケンス番号を選択します。	1	省略不可
設定情報	データ通信端末固有の設定情報を設定します。	最大 254 文字の英数字	省略不可

この設定を行わない場合

データ通信端末固有の設定情報等を設定できません。

設定モード

モデムインタフェース設定モード

modem out-strings init

本コマンドを設定することにより、データ通信端末を初期化するための文字列を任意に指定することができます。
初期化する文字列が異なる場合は、使用するデータ通信端末に合わせて適切な文字列を設定してください。
本コマンドを設定しない場合は、ファームウェアが個別に保持している適切な文字列（ATE0V1Q0&D2&C1）が使用されます。

refresh コマンド後に有効になるコマンドです。

設定例１　データ通信端末に対して初期化文字列※を設定する

```
Router(config)#interface modem 1
Router(config-if modem 1)#modem out-strings init 1 ATE0V1Q0&C1&D2
```

※初期化の内容は、下記を参照してください。

設定内容	AT コマンド例
コマンドエコー制御 データ通信端末に対して送信したコマンドを、装置側にエコーバックしない設定	E0
リザルトコード形式 リザルトコードを文字形式に設定	V1
リザルトコード表示制御 リザルトコードを表示する設定	Q0
DCD 制御 DCD 信号をデータリンク確立時のみ ON にする設定	&C1
DTR 制御 DTR 信号を ON から OFF に制御した場合に回線を切断する設定	&D2

コマンド形式

modem out-strings init〈シーケンス番号〉〈初期化文字列〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
シーケンス番号	シーケンス番号を選択します。	1	省略不可
初期化文字列	データ通信端末を初期化するための文字列を設定します。	最大 254 文字の英数字	省略不可

この設定を行わない場合

ファームウェアが個別に保持している適切な文字列（ATE0V1Q0&D2&C1）が送信されます。

設定モード

モデムインタフェース設定モード

monitor signal-level

データ通信端末に対して、interval で指定した間隔毎に電波状態の取得を行います。
取得した電波状態は、slog への記録、show コマンドでの表示、イベントクラス通知判定に利用ことができます。

refresh コマンド後に有効になるコマンドです。

設定例１　２分ごとにデータ通信端末の電波状態を取得する

```
Router(config)#interface modem 1
Router(config-if modem 1)#monitor signal-level interval 120
```

コマンド形式

monitor signal-level [interval <監視間隔>] [average range <平滑化範囲>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
監視間隔	電波状態を監視する間隔(単位:秒)を設定します。	10～86400	監視間隔は、60秒になります。
平滑化範囲	データ通信端末の電波状態を指定時間範囲(単位:秒)で平滑化した値となります。	1～10	取得したデータは、最新の電波状態となります。

※ データ通信端末が通信中の場合は、電波状態を取得できません。

この設定を行わない場合

データ通信端末の電波状態を定期的に取得しません。

設定モード

モデムインタフェース設定モード

monitor signal-quality

データ通信端末が+CSQ コマンドに対応している場合に、interval で指定した間隔毎に電波信号品質の取得を行ないます。
取得した電波信号品質は、slog への記録、show コマンドでの表示、イベントクラス通知判定に利用ことができます。

refresh コマンド後に有効になるコマンドです。

設定例１　２分ごとにデータ通信端末の電波信号品質を取得する

```
Router(config)#interface modem 1
Router(config-if modem 1)#monitor signal-quality 120
```

コマンド形式

monitor signal-quality [interval <監視間隔>] [average range <平滑化範囲>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
監視間隔	電波信号品質を監視する間隔(単位:秒)を設定します。	10～86400	監視間隔は、60秒になります。
平滑化範囲	データ通信端末の電波信号品質を指定時間範囲(単位:秒)で平滑化した値となります。	1～10	取得したデータは、最新の電波状態となります。

※ データ通信端末が通信中の場合は、電波信号品質を取得できません。

この設定を行わない場合

データ通信端末の電波信号品質を定期的に取得しません。

設定モード

モデムインタフェース設定モード

physical-layer

本コマンドで設定することにより、本装置に装着したデータ通信端末でモデム通信が可能になります。
設定を削除または変更し、本装置のリフレッシュを行うと接続中の回線は強制切断されます。

refresh コマンド後に有効になるコマンドです。

設定例１　モデム通信に USB ポート１に接続したデータ通信端末を使用する

```
Router(config)#interface modem 1
Router(config-if modem 1)#physical-layer usb 1
```

コマンド形式

physical-layer 〈USB ポート〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
USB ポート	モデム通信に使用するデータ通信端末を接続する USB ポートを指定します。	usb 1 usb 2	省略不可

この設定を行わない場合

装置に装着したデータ通信端末を使用できません。

設定モード

モデムインタフェース設定モード

ppp account

インタフェースにデータ通信端末を選択した場合に、接続先に送信する自分の認証用ユーザ名、パスワードを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　ユーザ ID に em, パスワードに em を設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#ppp account em em
```

コマンド形式

ppp account <userid> <password>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
userid	接続先に送信する、自分の認証ユーザ名を設定します。	127 文字以内の文字列	省略不可
password	接続先に送信する、自分の認証パスワードを設定します。	32 文字以内の文字列	省略不可

※ 認証ユーザ名および認証パスワードに関しては、ご利用のプロバイダ等にお問い合わせ下さい。

この設定を行わない場合

ワイヤレス接続を行うことができません。

設定モード

ダイヤラーインタフェース設定モード

usb ethernet-monitor

HTTP で情報を取得するためのオプションを指定します。

refresh コマンド後に有効になるコマンドです。

V01.02(00)以降サポート

設定例１　USB STICK U01 の情報を、HTTP で取得する

```
Router(config)# usb ethernet-monitor 1 device U01
```

設定例２　PIX-MT100 の情報を、HTTP で取得する

```
Router(config)# usb ethernet-monitor 1 device MT100
```

※ PIX-MT100 を USB Ethernet インタフェースで使用する場合は、本設定が必要です。

設定例３　604HW の情報を、HTTP で取得する

```
Router(config)# usb ethernet-monitor 1 device 604HW
```

※ 604HW を USB Ethernet インタフェースで使用する場合は、本設定が必要です。

コマンド形式

usb ethernet-monitor 〈モニタリング番号〉 device 〈デバイス名称〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
モニタリング番号	モニタリング番号を設定します。	1	省略不可
デバイス名称	モニタリングするデバイスを設定します。 U01：au USB STICK U01 U03：au USB STICK U03 MT100：ピクセラ PIX-MT100 604HW：SoftBank 604HW	U01 U03※1 MT100※1 604HW※1	省略不可

※1 パラメータ U03、MT100、604HW は、V01.04(00)以降サポート

この設定を行わない場合

USB STICK LTE HWD12 として HTTP で情報を取得します。

設定モード

基本設定モード

usb mode-switch

Ethernet モードに対応するデバイスに関して、Ethernet モードにて動作させるか、Modem モードにて動作させるかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例　HWD12 を Ethernet モードにて動作させる

```
Router(config)# usb mode-switch 1 vid 12d1 pid 1f03 network
```

コマンド形式

usb mode-switch <デバイスリスト番号> vid <ベンダーID> pid <プロダクト ID > <動作モード>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
デバイスリスト番号	デバイスリスト番号を設定します。	1～16	省略不可
ベンダーID	ベンダーID を設定します。	16 進数表記	省略不可
プロダクト ID	プロダクト ID を設定します。	16 進数表記	省略不可
動作モード	Ethernet モード(network)、Modem(modem)モードのどちらで動作させるか設定します。	network ・ modem	省略不可

データ通信端末一覧

データ通信端末	ベンダーID	プロダクト ID
au : USB STICK LTE HWD12	12d1	1f03

この設定を行わない場合

Modem モードにて動作します。

設定モード

基本設定モード

障害監視／通知機能

SNMP エージェント機能

snmp-server community

SNMP マネージャからの要求に応答する場合に設定します。

設定例１　コミュニティ名を"public"に設定する

```
Router(config)# snmp-server community public
```

設定例２　コミュニティ名を"public"に設定し、アクセスを許可するホストは access-list 番号１に従う

```
Router(config)# snmp-server community public  1
```

コマンド書式

snmp-server community〈コミュニティ名〉[ro | rw][アクセスリスト番号]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
コミュニティ名	SNMP の通信を行なう際のコミュニティ名を設定します。	32 文字以内の文字列	省略不可
ro | rw	read のみとするか、read/write 可能とするかを指定します。 ro　read のみ可能 rw　read/write 共に可能	ro rw	read のみ可能
アクセスリスト番号	アクセスを許可するホストを指定するために指定するアクセスリスト番号を設定します。	1～99 3000～3499	全ホストからの SNMP アクセスが可能

最大エントリ数:5 エントリ

この設定を行わない場合

SNMP マネージャからの要求には応答しません。

設定モード

基本設定モード

snmp-server contact

本装置の管理者を設定します。
通知されたテキストは、system グループの sysContact に設定されます。

設定例１　本装置の管理者を"root@fitelnetF2200"に設定する

```
Router(config)# snmp-server contact root@fitelnetf2200
```

コマンド書式

snmp-server contact〈管理者名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
管理者名	本装置の管理者を指定します。	32 文字以内の文字列	省略不可

この設定を行わない場合

指定なしになります。

設定モード

基本設定モード

snmp-server enable traps

トラップの動作を行う場合に設定します。
トラップを送信するには、併せて snmp-server host コマンドの設定も必要です。
また、送信先毎に異なる種類のトラップを送信したい場合は、snmp-server host コマンドで、送信するトラップを指定します。

設定例１　トラップの送信を有効にし、標準トラップのみ送信する

```
Router(config)# snmp-server enable traps snmp
```

コマンド書式

snmp-server enable traps [トラップの種類]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
トラップの種類	送信するトラップの種類を指定します。 snmp：標準トラップのみ送信する config：拡張トラップのみ送信する event：イベントトラップのみ送信する	snmp config event	全てのトラップを送信

この設定を行わない場合

トラップを送信しません。

設定モード

基本設定モード

snmp-server host

トラップの送信先を設定します。
送信先は、8件まで登録することができます。
トラップを送信するには、併せて snmp-server enable traps コマンドの設定も必要です。

設定例 1　トラップの送信先を 10.0.0.1 とし、コミュニティ名を public、バージョンを 2 としてトラップを送信する

```
Router(config)#snmp-server host 10.0.0.1 public v2c
```

コマンド書式

snmp-server host <トラップの送信先> <コミュニティ名> [バージョン] [トラップの種類]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
トラップの送信先	トラップの送信先を指定します。	ホスト名称	省略不可
コミュニティ名	トラップに記載するコミュニティ名を指定します。	32 文字以内の文字列	省略不可
バージョン	SNMP のバージョンを指定します。 v1　SNMPv1 v2c　SNMPv2(Community Based)	v1 v2c	SNMPv1
トラップの種類	送信するトラップの種類を指定します。 snmp　標準トラップのみ送信する config　拡張トラップのみ送信する event　イベントトラップのみ送信する	snmp config event	snmp-server enable traps の設定に従う

最大エントリ数:8 エントリ

この設定を行わない場合

トラップを送信することはできません。

設定モード

基本設定モード

snmp-server location

本装置の設置場所を設定します。
通知されたテキストは、system グループの sysLocation に設定されます。

設定例１　本設置場所を"Honsha（本社）"に設定する

```
Router(config)# snmp-server location Honsha
```

コマンド書式

snmp-server contact〈設置場所名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
設置場所名	本装置の設置場所を指定します。	64 文字以内の文字列	省略不可

この設定を行わない場合

指定なしになります。

設定モード

基本設定モード

snmp-server name

本装置の名称を設定します。
通知されたテキストは、system グループの sysName に設定されます。

設定例１　本装置の名前を"FITELnetF2200#1"に設定する

```
Router(config)# snmp-server name FITELnetF2200#1
```

コマンド書式

snmp-server name〈装置名称 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
装置名称	本装置の名称を指定します。	32 文字以内の文字列	省略不可

この設定を行わない場合

指定なしになります。

設定モード

基本設定モード

snmp-server source-interface

トラップを送出する際の送信元 IP アドレスとして使用するインタフェース名を指定します。

設定例 1　トラップを送信する際の送信元アドレスに LAN インタフェースの IP アドレスを使用する

```
Router(config)#snmp-server source-interface lan 1
```

コマンド書式

snmp-server source-interface〈インタフェース名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	トラップの送信元アドレスに使用するインタフェースアドレス	lan 1 ewan 1～2 loopback 1～100 vlanif 1～150	省略不可

この設定を行わない場合

トラップを実際に送信するインタフェースのアドレスになります。

設定モード

基本設定モード

SYSLOGD への障害通知機能

logging-level elog

elog を syslog で送信する際の、ログ出力レベルを設定します。
elog を syslog で送信したい場合は、syslog level コマンドで指定したレベル以上のレベル値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　elog の出力レベルを 3（ERR）とする

```
Router (config)# logging-level elog 3
```

コマンド書式

logging-level elog <出力レベル値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
出力レベル値	elog の出力レベル値を設定します。 また、none を指定すると elog を送信しません。	0～7 none	省略不可

この設定を行わない場合

elog をレベル4(WARNING)で出力します。

出力エラーレベルとは？

syslog のメッセージでは、レベルという領域が規定されています。
通常は、メッセージを受信した管理者が、どのような緊急性のあるメッセージなのかを把握するために利用します。
syslog のレベルは、プロトコルにより以下８段階に規定されています。

レベル名	レベル番号	メッセージの内容・緊急度
EMERG	0	システムが利用できなくなった（ぐらい緊急度が高い）
ALERT	1	早急に対応しなくてはならない
CRIT	2	緊急状態
ERR	3	エラー発生状態
WARNING	4	注意が必要
NOTICE	5	お知らせ程度
INFO	6	情報
DEBUG	7	デバッグメッセージ

elog とは？

本装置で発生している中／軽度のエラー情報のメッセージです。
このメッセージが発生した場合は、本装置を含むネットワーク環境をご確認ください。
コンソールもしくは TELNET でログインして、elog の情報を表示する場合は、show elog コマンドを使用します。

設定モード

基本設定モード

logging-level flog

flog を syslog で送信する際の、ログ出力レベルを設定します。
flog を syslog で送信したい場合は、syslog level コマンドで指定したレベル以上のレベル値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　flog の出力レベルを 3（ERR）とする

```
Router (config)# logging-level flog 3
```

コマンド書式

logging-level flog <出力レベル値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
出力レベル値	flog の出力レベル値を設定します。 また、none を指定すると flog を送信しません。	0～7 none	省略不可

この設定を行わない場合

flog を syslog で送信しません。

出力レベルとは？

syslog のメッセージでは、レベルという領域が規定されています。
通常は、メッセージを受信した管理者が、どのような緊急性のあるメッセージなのかを把握するために利用します。
syslog のレベルは、プロトコルにより以下８段階に規定されています。

レベル名	レベル番号	メッセージの内容・緊急度
EMERG	0	システムが利用できなくなった（ぐらい緊急度が高い）
ALERT	1	早急に対応しなくてはならない
CRIT	2	緊急状態
ERR	3	エラー発生状態
WARNING	4	注意が必要
NOTICE	5	お知らせ程度
INFO	6	情報
DEBUG	7	デバッグメッセージ

flog とは？

本装置で、log オプション付きのアクセスリスト（dynamic 設定のものは除く）でフィルタリング対象となったパケットをロギング（Filtering Log）することができます。
コンソールもしくは TELNET でログインして、flog の情報を表示する場合は、show flog コマンドを使用します。

設定モード

基本設定モード

logging-level slog

slog を syslog で送信する際の、ログ出力レベルを設定します。
slog を syslog で送信したい場合は、syslog level コマンドで指定したレベル以上のレベル値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　slog の出力レベルを 4(WARNING)とする

```
Router(config)# logging-level slog 4
```

コマンド書式

logging-level slog <出力レベル値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
出力レベル値	slog の出力レベル値を設定します。 また、none を指定すると slog を送信しません。	0～7 none	省略不可

この設定を行わない場合

slog をレベル5(NOTICE)で出力します。

出力レベルとは？

syslog のメッセージでは、レベルという領域が規定されています。
通常は、メッセージを受信した管理者が、どのような緊急性のあるメッセージなのかを把握するために利用します。
syslog のレベルは、プロトコルにより以下８段階に規定されています。

レベル名	レベル番号	メッセージの内容・緊急度
EMERG	0	システムが利用できなくなった（ぐらい緊急度が高い）
ALERT	1	早急に対応しなくてはならない
CRIT	2	緊急状態
ERR	3	エラー発生状態
WARNING	4	注意が必要
NOTICE	5	お知らせ程度
INFO	6	情報
DEBUG	7	デバッグメッセージ

slog とは？

本装置の slog では、本装置に TELNET や FTP でアクセスがあった場合の情報や、インタフェースの UP/DOWN 情報等のメッセージです。
コンソールもしくは TELNET でログインして、slog の情報を表示する場合は、show slog コマンドを使用します。

設定モード

基本設定モード

logging-level tlog

tlog を syslog で送信する際の、ログ出力レベルを設定します。
tlog を syslog で送信したい場合は、syslog level コマンドで指定したレベル以上のレベル値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　tlog の出力レベルを 2（CRIT）とする

```
Router(config)# logging-level tlog 2
```

コマンド書式

logging-level tlog <出力レベル値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
出力レベル値	tlog の出力レベル値を設定します。 また、none を指定すると tlog を送信しません。	0～7 none	省略不可

この設定を行わない場合

tlog をレベル3(ERR)で出力します。

出力レベルとは？

syslog のメッセージでは、レベルという領域が規定されています。
通常は、メッセージを受信した管理者が、どのような緊急性のあるメッセージなのかを把握するために利用します。
syslog のレベルは、プロトコルにより以下８段階に規定されています。

レベル名	レベル番号	メッセージの内容・緊急度
EMERG	0	システムが利用できなくなった（ぐらい緊急度が高い）
ALERT	1	早急に対応しなくてはならない
CRIT	2	緊急状態
ERR	3	エラー発生状態
WARNING	4	注意が必要
NOTICE	5	お知らせ程度
INFO	6	情報
DEBUG	7	デバッグメッセージ

tlog とは？

本装置で発生している重度のエラー情報のメッセージです。
このメッセージが発生した場合は、本装置を含むネットワーク環境をご確認ください。また、必要があれば、本装置を再起動する等の処置をしてください。
コンソールもしくは TELNET でログインして、tlog の情報を表示する場合は、show tlog コマンドを使用します。

設定モード

基本設定モード

logging-level vpnlog

vpnlog を syslog で送信する際の、ログ出力レベルを設定します。
vpnlog を syslog で送信したい場合は、syslog level コマンドで指定したレベル以上のレベル値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　vpnlog の出力レベルを 5（NOTICE）とする

```
Router(config)# logging-level vpnlog 5
```

コマンド書式

logging-level vpnlog <出力レベル値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
出力レベル値	vpnlog の出力レベル値を設定する。 また、none を指定すると vpnlog を送信しません。	0～7 none	省略不可

この設定を行わない場合

vpnlog をレベル6(INFO)で出力します。

出力レベルとは？

syslog のメッセージでは、レベルという領域が規定されています。
通常は、メッセージを受信した管理者が、どのような緊急性のあるメッセージなのかを把握するために利用します。
syslog のレベルは、プロトコルにより以下８段階に規定されています。

レベル名	レベル番号	メッセージの内容・緊急度
EMERG	0	システムが利用できなくなった（ぐらい緊急度が高い）
ALERT	1	早急に対応しなくてはならない
CRIT	2	緊急状態
ERR	3	エラー発生状態
WARNING	4	注意が必要
NOTICE	5	お知らせ程度
INFO	6	情報
DEBUG	7	デバッグメッセージ

vpnlog とは？

本装置の IPsec 機能に関するログです。
SA を確立できなかった場合の原因究明や、改ざん・なりすまし等を検知した場合に、ログを発行します。SA の確立／解放を vpnlog に残す場合は、vpnlog enable コマンドを設定します。
コンソールもしくは TELNET でログインして、vpnlog の情報を表示する場合は、show vpnlog コマンドを使用します。

設定モード

基本設定モード

syslog facility

ログ情報を syslog で通知する際のファシリティコード番号(0～23)を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　syslog のファシリティ値を”local0″に設定する

```
Router(config)# syslog facility 16
```

コマンド書式

syslog facility <ファシリティコード番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ファシリティコード番号	syslog のファシリティ値を指定します。	0～23	省略不可

この設定を行わない場合

ファシリティコード番号 1 になります。

syslog のファシリティとは？

syslog のファシリティとは、ログメッセージの種類を表します。
一般的には、どのような状況でログが発生したかを表す番号として指定されます。
RFC3164 では、以下のように規定されています。（OS により捕らえ方が同じように見えるファシリティ値もあります）

コード番号	ファシリティ	コード番号	ファシリティ
0	kernel message	12	NTP subsystem
1	user-level messages	13	log audit
2	mail system	14	log alert
3	system daemons	15	clock daemon
4	security/authorization messages	16	local use 0 (local0)
5	messages generated internally by syslogd	17	local use 1 (local1)
6	line printer subsystem	18	local use 2 (local2)
7	network news subsystem	19	local use 3 (local3)
8	UUCP subsystem	20	local use 4 (local4)
9	clock daemon	21	local use 5 (local5)
10	security/authorization messages	22	local use 6 (local6)
11	FTP daemon	23	local use 7 (local7)

syslog を通知した場合、サーバ側ではファシリティ毎に保存するファイルを変えるというような運用方法も可能となります。

設定モード

基本設定モード

syslog file

指定したレベル以上のログ情報を、指定したディレクトリ配下にシリアル番号のディレクトリを作成しログ情報を出力します。

refresh コマンド後に有効になるコマンドです。

設定例 1　ERR(3) レベル以上のログ情報を USB ポート 1 に接続された USB メモリに出力する

```
Router (config)# syslog file /usb1 level 3
```

コマンド書式

```
syslog file <保存先ディレクトリ>[max-size-kilobyte <保存サイズ>][max-files <保存数>][level <レベル>][password <パスワード>[{secret | private} [encrypted]]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
保存先ディレクトリ	ログ情報を保存するディレクトリを指定します。	最大 64 文字の英数字	省略不可
保存サイズ	保存する1ファイルあたりのサイズ(単位:キロバイト)を指定します。指定したサイズを超える場合は、別ファイルとして保存されます。	100～1000	1ファイルあたり1000Kbyte になります。
保存数	保存するファイル数の最大数を指定します。	1～100	最大 100 ファイルになります。
レベル	出力するログ情報のレベルを指定します。	0～7	syslog レベル 7 以上になります。
パスワード	パスワードオプションを指定した場合は、ログ情報のバックアップを取るタイミングで暗号化します。	最大 16 文字の英数字	ログ情報のバックアップを取る際に暗号化しません。
secret | private	パスワードを暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。※1 secret：暗号化する際に共有暗号鍵を使用する private：暗号化する際に装置固有暗号鍵を使用する	secret private	パスワードを暗号化しません。
encrypted	パスワードを暗号化処理するかどうかを設定します。 このオプションを付加することにより、パスワードは暗号化済みと判定	encrypted	パスワードを暗号化データとして扱いません。

	されます。※2 secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。		

※1 このオプションは、設定するとすぐに有効となり、パスワードが暗号化されて表示され encrypted オプションが自動的に付加されます。
※2 パスワードが既に暗号化済みの場合は、このオプションを指定する必要があります。

この設定を行わない場合

ログ情報をファイルに出力しません。

出力レベルとは？

syslog のメッセージでは、レベルという領域が規定されています。
通常は、メッセージを受信した管理者が、どのような緊急性のあるメッセージなのかを把握するために利用します。
syslog のレベルは、プロトコルにより以下８段階に規定されています。

レベル名	レベル番号	メッセージの内容・緊急度
EMERG	0	システムが利用できなくなった（ぐらい緊急度が高い）
ALERT	1	早急に対応しなくてはならない
CRIT	2	緊急状態
ERR	3	エラー発生状態
WARNING	4	注意が必要
NOTICE	5	お知らせ程度
INFO	6	情報
DEBUG	7	デバッグメッセージ

設定モード

基本設定モード

syslog format bsd

本装置が送出する syslog メッセージのフォーマットを BSD タイプ（PRI 部、HEADER 部、MSG 部からなるファーマット）とします。
フォーマットは、(facility*8)+level で算出されるプライオリティ値、タイムスタンプ、ホスト名、ログのタイプ、シーケンス番号、アップタイム、TID、ログ ID、メッセージ本体の順になります。
本コマンドは、elog メッセージ、flog メッセージ、slog メッセージ、tlog メッセージ、vpnlog メッセージが対象となります。

refresh コマンド後に有効になるコマンドです。

設定例１　SYSLOG メッセージのフォーマットを BSD タイプとする

```
Router (config)# syslog format bsd
```

コマンド書式

```
syslog format bsd
```

パラメータ

パラメータはありません。

この設定を行わない場合

syslog メッセージのフォーマットは、プライオリティ値、シーケンス番号、アップタイム、タイムスタンプ、TID、ログ ID、メッセージ本体の順になります。

設定モード

基本設定モード

syslog level

ログ情報を syslog で通知する際の出力制限レベル(0～7)を設定します。
ここで設定したレベル値以上の緊急度をもつレベルのログ情報を syslog サーバに通知します。

refresh コマンド後に有効になるコマンドです。

設定例１　Debug(7) レベル以上の緊急度をもつログ情報を syslog で通知する

```
Router (config)# syslog level 7
```

コマンド書式

syslog level <レベル番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
レベル番号	syslog で通知する際の出力制限ラベル値を設定します。	0～7	省略不可

この設定を行わない場合

レベル番号 7 になります。

syslog のレベルとは？

syslog のレベルとは、ログメッセージの緊急度を表します。
RFC3164 では、以下のように規定されています。

レベル名	レベル番号	メッセージの内容・緊急度
EMERG	0	システムが利用できなくなった(ぐらい緊急度が高い)
ALERT	1	早急に対応しなくてはならない
CRIT	2	緊急状態
ERR	3	エラー発生状態
WARNING	4	注意が必要
NOTICE	5	お知らせ程度
INFO	6	情報
DEBUG	7	デバッグメッセージ

レベル値設定

本装置では、各種ログ（elog/slog/tlog/vpnlog）毎にレベル値を設定します。
各種ログのレベル値の設定は、logging level コマンドで行ないます。

設定モード

基本設定モード

syslog sending

syslog サーバにログ情報を送信するかどうかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　syslog サーバにログ情報を通知する

```
Router(config)# syslog sending
```

コマンド書式

```
syslog sending
```

パラメータ

パラメータはありません。

この設定を行わない場合

ログ情報を、syslog サーバに送信しません。

設定モード

基本設定モード

syslog server

syslog サーバホストの IP アドレスを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　syslog サーバに、192.168.100.1 を設定する

```
Router(config)# syslog server 192.168.100.1
```

コマンド書式

syslog server <syslog サーバ 1> [syslog サーバ 2]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
syslog サーバ 1	syslog を通知するサーバの IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
syslog サーバ 2			syslog サーバ 1 に設定したアドレスに通知されます。

この設定を行わない場合

ログ情報を、syslog サーバに送信しません。

設定モード

基本設定モード

syslog source-interface

syslog パケット送出の際の送信元 IP アドレスとして使用するインタフェース名を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　syslog 送信時の送信元アドレスに、LAN インタフェースの IP アドレスを使用する

```
Router(config)# syslog source-interface lan 1
```

コマンド書式

syslog source-interface <インタフェース名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	syslog を通知する際のパケットの送信元アドレスに使用するインタフェースアドレスを指定します。	lan 1 ewan 1～2 loopback 1～100 vlanif 1～150	省略不可

この設定を行わない場合

syslog パケットを実際に送信するインタフェースになります。

設定モード

基本設定モード

電子メールによる障害通知機能

mail from

メールの送信元アドレスを設定します。

設定例１　メールの送信元アドレスとして"F2200@xxxxx.co.jp"を指定する

```
Router(config)# mail from F2200@xxxxx.co.jp
```

コマンド書式

mail from〈送信元メールアドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信元メールアドレス	メール通知機能で送信する電子メールの From に入れるメールアドレス	–	省略不可

この設定を行わない場合

From には、何も設定されません。
その結果、メールでの通知機能も働きません。

設定モード

基本設定モード

mail to

メールの送信先アドレスを設定／解除します。
複数行入力することにより、5 つまで指定可能です。
また、電子メール通知機能で通知する種類を以下の中から選択します。

種類	電子メール送信タイミング	オプション
不正アクセス	不正アクセスを認識したタイミング	invader
自動再起動	ファームウェアの自動再起動がおこったタイミング	filemaintenance
ワイヤレス自動切断	規定パケット数の 90%を超えるデータの送受信、あるいは規定パケット数以上のデータの送受信があったタイミング 累積許容時間のプレアラート値に到達したタイミング、および許容時間を超えたタイミング	limiter
イベントアクション	イベントアクション機能のアクションにメール通知を指定し、そのアクションに対応するイベントの状態変化が発生した場合。 イベントアクション機能のメール通知については、send e-mail コマンドを参照してください	event-action

設定例 1　メールの宛先アドレスを admin@xxxx.co.jp に設定する（送信種類：不正アクセス）

```
Router(config)#mail to admin@xxxx.co.jp invader
```

コマンド書式

mail to〈宛先メールアドレス〉[電子メールの種類]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先メールアドレス	メール通知機能で送信する電子メールの To に入れるメールアドレス	–	省略不可
電子メールの種類	電子メールにて通知するメッセージの種類	invader filemaintenance limiter event-action のいずれかもしくは複数	全ての種類のメールを通知する

この設定を行わない場合

電子メールによる通知を行ないません。

設定モード

基本設定モード

mail server

mail 通知機能が電子メールを送信する際のメールサーバを指定します。
複数行入力することにより 3 つまで有効, 4 つ以上は無視されます。
また先に入力したサーバが優先されます。メールサーバはホスト名と IP アドレスを設定できます。

設定例 1　メールサーバの IP アドレスを 192.168.100.1 に設定する

```
Router(config)#mail server 192.168.100.1
```

コマンド書式

mail server <SMTP サーバの IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
SMTP サーバの IP アドレス	電子メールを送信するための SMTP サーバの IP アドレス	IPv4 アドレス形式 IPv6 アドレス形式 ホスト名形式 のいずれか	省略不可

最大エントリ数:3 エントリ

この設定を行わない場合

電子メールによる通知を行ないません。

設定モード

基本設定モード

mail source-interface

SMTP パケット送出の際の送信元 IP アドレスとして使用するインタフェース名を指定します。

設定例 1　SMTP パケットの送信元アドレスに LAN の IP アドレスを使用する

```
Router(config)# mail source-interface lan 1
```

コマンド書式

mail interface〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	SMTP パケットの送信元アドレスとしてつけるインタフェース	lan 1 ewan 1～2 loopback 1～100 vlanif 1～150	省略不可

この設定を行わない場合

実際にパケットを送信するインタフェースの IP アドレスになります。

設定モード

基本設定モード

自律監視機能

check watch-class

自律監視機能の監視モードを適用する場合に設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　監視モードを適用する

```
Router(config)#event-class 1
Router(config-event-class 1)# check watch-class 1
```

コマンド書式

check watch-class <watch クラス番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
watch クラス番号	監視モードを適用する watch クラス番号を指定します。	1～16	省略不可

この設定を行わない場合

監視モードを適用しません。

設定モード

イベントクラス設定モード

interval

リソースの監視を行なう際の TURE 状態時の監視間隔と、FALSE 状態時の監視間隔を設定します。
UNKNOWN 状態の場合は、FALSE 状態時の監視間隔を採用します。

refresh コマンド後に有効になるコマンドです。

設定例 1　TURE 状態時の監視間隔を 120 秒、FALSE 状態時の監視間隔を 120 秒とする

```
Router(config)#watch-class 1
Router(config-watch-class 1)#interval 120 120
```

コマンド書式

interval <TURE 監視間隔> <FALSE 監視間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
TURE 監視間隔	TURE 状態の監視間隔(単位:秒)を設定します。	1～2000000	省略不可
FALSE 監視間隔	FALSE 状態の監視間隔(単位:秒)を設定します。	1～2000000	省略不可

この設定を行わない場合

TURE 監視間隔、FALSE 監視間隔共に 300 秒です。

設定モード

Watch クラス設定モード

logging event state-change

本コマンドで、enable が設定されている場合、各クラスの状態変化が発生するとログを記載します。disable または、未設定(デフォルト)の場合は記載されません。

refresh コマンド後に有効になるコマンドです。

設定例１　event-class の状態変化が発生した場合ログを記載する

```
Router(config)#event-class 1
Router(config-event-class 1)# logging event state-change enable
Router(config-event-class 1)# exit
```

コマンド書式

logging event state-change 〈ログ設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ログ設定	状態変化によりログを記載するかどうかを指定します。 enable　ログを記載する disable　ログを記載しない	enable disable	省略不可

この設定を行わない場合

状態が変化してもログを記載しません。

設定モード

イベントクラス設定モード
イベントアクション設定モード
ICMP クラス設定モード
Watch クラス設定モード

target

自律監視機能で監視する対象を指定します。
1 つの watch クラス設定モードで監視できる対象は1つです。

refresh コマンド後に有効になるコマンドです。

設定例１　Watch クラス番号１で監視する対象を CPU 使用率とする

```
Router(config)#watch-class 1
Router(config-watch-class 1)#target cpu-utilization
```

コマンド書式

target 〈監視対象〉 [remains]

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>監視対象</td><td>監視の対象を指定します。
<table>
<tr><td>cpu-utilization</td><td>CPU 使用率を監視対象とします。</td></tr>
<tr><td>memory</td><td>メモリ使用率を監視対象とします。</td></tr>
<tr><td>ip-nat-sessions</td><td>NAT テーブルの使用率を監視対象とします。</td></tr>
<tr><td>stateful-packet-sessions</td><td>フィルタリングテーブルの使用率を監視対象とします。</td></tr>
<tr><td>ip-routing-entries</td><td>IPv4 ルーティングテーブルの使用率を監視対象とします。</td></tr>
<tr><td>ipv6-routing-entries</td><td>IPv6 ルーティングテーブルの使用率を監視対象とします。</td></tr>
<tr><td>buffer</td><td>バッファの使用率を監視対象とします。</td></tr>
<tr><td>ipv4-arp-entries</td><td>ARP テーブルの使用率を監視対象とします。</td></tr>
<tr><td>ipv6-neighbor-cache-entries</td><td>NDP キャッシュの使用率を監視対象とします。</td></tr>
<tr><td>temperature</td><td>装置内部の温度が 0℃以下の場合のリソースを 0、1℃以上の場合はその温度値を監視対象とします。</td></tr>
</table></td><td>cpu-utilization
memory
ip-nat-sessions
stateful-packet-sessions
ip-routing-entries
ipv6-routing-entries
buffer
ipv4-arp-entries
ipv6-neighbor-cache-entries
temperature</td><td>省略不可</td></tr>
<tr><td>remains</td><td>remains を指定することで、監視対象の残量を監視します。</td><td>remains</td><td>監視対象の使用率を監視します。</td></tr>
</table>

※ temperature を監視対象に選択した場合は、remains を指定することはできません。

この設定を行わない場合

監視を行いません。

設定モード

Watch クラス設定モード

threshold

監視のポリシーと閾値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　上方監視、TRUE とする使用率を 80%、FALSE とする使用率を 75%とする

```
Router(config)#watch-class 1
Router(config-watch-class 1)#threshold ge percentage 80 hysteresis 5
```

コマンド書式

threshold {ge|gt|le|lt} {value <閾値> hysteresis <変移値> | percentage <使用率> hysteresis <変移率>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
監視ポリシー	監視の方法を指定します。 ge：上方監視、閾値含み設定値以上の場合に TRUE gt：上方監視、閾値含まず設定値を超える場合に TRUE le：下方監視、閾値含み設定値以下の場合に TRUE lt：下方監視、閾値含ず設定値未満の場合に TRUE	ge gt le lt	省略不可
閾値	監視する際の、TRUE と判定する閾値を設定します。	0～2147483647	省略不可
変移値	設定閾値に達した後、どのくらい値が変移したら FALSE と判定するかを設定します。 閾値から変移値を引いた値が判定値となります。	0～2147483647	省略不可
使用率	監視する際の、TRUE と判定する使用率を設定します	0～100	省略不可
変移率	設定使用率に達した後、使用率が何パーセント変移したら FALSE と判定するかを設定します。 使用率から変移率を引いた値が判定値となります。	0～100	省略不可

自律監視機能の説明

```
Router(config)#watch-class 1
Router(config-watch-class 1)#target cpu
Router(config-watch-class 1)#threshold ge percentage 80 hysteresis 5
Router(config-watch-class 1)#interval 10 2
Router(config-watch-class 1)#times 5 2
exit
```

監視対象	CPU 使用率
監視ポリシーと閾値	上方監視、CPU 使用率 80%以上で TRUE、75%以下で FALSE
監視間隔	TRUE 状態では 10 秒間隔、FALSE 状態では 2 秒間隔で監視
監視回数	TRUE 状態では 5 回、FALSE 状態では 2 回

FALSE 状態では 2 秒間隔で監視。5 回連続で CPU 使用率が 80%以上の場合に TRUE に遷移します。
TRUE 状態では 10 秒間隔で監視。2 回連続で CPU 使用率が 75%を下回っている場合に FALSE に遷移します。

この設定を行わない場合

監視を行いません。

設定モード

Watch クラス設定モード

times

リソースの監視を行なう際の状態遷移と判断する回数を設定します。
TURE から FALSE への状態遷移の際の判断回数と、FALSE から TRUE への状態遷移の際の判断回数を別々に指定することができます。

refresh コマンド後に有効になるコマンドです。

設定例 1　TURE に状態遷移する判定回数 5 回、FALSE に状態遷移する判定回数を 5 回とする

```
Router(config)#watch-class 1
Router(config-watch-class 1)#interval 5 5
```

コマンド書式

times <TURE 判定回数> <FALSE 判定回数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
TURE 判定回数	TURE に状態遷移する判定回数を設定します。	1～2000000	省略不可
FALSE 判定回数	FALSE に状態遷移する判定回数を設定します。	1～2000000	省略不可

この設定を行わない場合

TURE 判定回数、FALSE 判定回数共に 3 回です。

設定モード

Watch クラス設定モード

watch-class

Watch クラス設定モードに移行します。

設定例１　Watch クラス設定モードに移行する

```
Router(config)#watch-class 1
Router(config-watch-class 1)#
```

コマンド書式

watch-class <Watch クラス番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Watch クラス番号	Watch クラス番号を指定します。	1～16	省略不可

設定モード

基本設定モード

FAN 制御機能

fan control

冷却ファンの回転制御を行う場合に設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　CPU コアの温度に関係なく冷却 FAN を高速回転とする

```
Router(config)#fan control high
Router(config)#
```

コマンド書式

fan control 〈FAN 制御〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
FAN 制御	冷却ファンの回転制御を指定します。 auto：CPU コア温度の値により冷却ファンの停止、低速～高速回転の選択を自動的に行います。 high：CPU コア温度の値に関係なく高速回転とします。	auto high	省略不可

この設定を行わない場合

FAN 制御は auto となります。

設定モード

基本設定モード

NTP 機能

SNTP クライアント機能

sntp retry

タイムサーバからの応答がなかった場合のリトライ間隔およびリトライ動作時間を設定します。
リトライ間隔は"sntp retry interval"コマンドで、リトライ動作時間は"sntp retry keepalive"コマンドで設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　SNTP のリトライ間隔を 100 秒に設定する

```
Router(config)#sntp retry interval 100
```

設定例２　SNTP のリトライ動作時間を 10 分（600 秒）に設定する

```
Router(config)#sntp retry keepalive 600
```

設定例３　SNTP のリトライをしない

```
Router(config)#sntp retry interval off
```

コマンド書式

```
sntp retry interval <リトライ間隔>
sntp retry keepalive <リトライ時間>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リトライ間隔	SNTP サーバから応答がなかった場合のリトライ間隔(秒)を指定します。 リトライしない場合は、off を指定します。	16～1024 off	省略不可
リトライ時間	リトライ継続時間(秒)を指定します。 この時間経過したら、リトライ動作を終了します。	64～1024	省略不可

この設定を行わない場合

リトライ間隔（64 秒）、リトライ時間（1024 秒）になります。

設定モード

基本設定モード

sntp schedule

サーバに問い合わせるスケジュールを指定します。
ここで設定するスケジュールは、以下の項目です。
・本装置の起動時に問い合わせを行なうかどうか？
・何時間おきに問い合わせを行なうか／何時に問い合わせを行なうか？

本装置起動時に問い合わせを行なう場合は、boot を指定します。
次に問い合わせを行なう間隔もしくは時間の設定は"interval"もしくは"time"で設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　本装置の起動時に問い合わせを行い、起動後は 1 時間おきに問い合わせる

```
Router(config)#sntp schedule boot interval 1
```

設定例２　本装置の起動時には問い合わせを行なわず、起動後は毎日 12:00 に問い合わせを行なう

```
Router(config)#sntp schedule time 12:00
```

コマンド書式

```
sntp schedule [boot] interval hour < 問い合わせ間隔 >
sntp schedule [boot] interval sec < 問い合わせ間隔 >
sntp schedule [boot] time < 問い合わせ時刻 >
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
boot	装置起動時に SNTP で時刻の問い合わせを行なうかどうか行なう場合に、boot を指定します。	boot	装置起動時には問い合わせを行なわない
問い合わせ間隔	SNTP サーバに時刻を問い合わせる間隔(単位:時間)を指定します。 off を指定すると問い合わせを行いません。 hour 指定の場合は、1～65534 sec 指定の場合は、16～16384 ※0 または、off を指定した場合は、問い合わせを行いません。 ※hour および sec を省略した場合は、単位が時間(hour)となります。	0～65535 off	省略不可
問い合わせ時刻	SNTP サーバに時刻を問い合わせる時刻(時:分)を指定します。 時刻を指定することで、毎日この時刻に、SNTP サーバに時刻を問い合わせます。 ※0:0 を指定した場合は、問い合わせを行いません。	0:0～23:59	省略不可

この設定を行わない場合

起動時問い合わせなし、1時間間隔で NTP サーバへ問い合わせします。
但し、NTP サーバ機能が有効な場合は 1024 秒毎に問い合わせします。

設定モード

基本設定モード

sntp server

接続するタイムサーバ(プライマリ,セカンダリ)の IP アドレスを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　SNTP サーバ（プライマリ：192.168.100.1、セカンダリ：192.168.100.2）を設定する

```
Router(config)#sntp server 192.168.100.1 192.168.100.2
```

コマンド書式

sntp server 〈プライマリ SNTP サーバ〉〈セカンダリ SNTP サーバ〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プライマリ SNTP サーバ	プライマリの SNTP サーバを指定	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
セカンダリ SNTP サーバ	セカンダリの SNTP サーバを指定	IPv4 アドレス形式 IPv6 アドレス形式	セカンダリ SNTP サーバを使用しない

この設定を行わない場合

SNTP 機能を使用できません。

設定モード

基本設定モード

sntp source-interface

SNTP 送出の際の送信元 IP アドレスとして使用するインタフェース名を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　SNTP を送信する際の送信元アドレスに LAN インタフェースの IP アドレスを使用する

```
Router(config)#sntp source-interface lan 1
```

コマンド書式

sntp source-interface <インタフェース名 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	SNTP パケットの送信元アドレスに使用するインタフェースアドレス	lan 1 ewan 1～2 loopback 1～100 vlanif 1～150	省略不可

この設定を行わない場合

SNTP を実際に送信するインタフェースになります。

設定モード

基本設定モード

NTP サーバ機能

ntp-server enable

NTP サーバ機能を使用する場合に設定します。
NTP サーバ機能は、上位 NTP サーバから時刻情報を受信していなくても利用可能ですが、時刻の精度が本装置の内蔵時計の精度となってしまうため、SNTP クライアント機能の設定を行ない、上位 NTP サーバから時刻情報を受信するようにしてください。

refresh コマンド後に有効になるコマンドです。

設定例 1　NTP サーバ機能を使用する

```
Router(config)#ntp-server enable
```

コマンド書式

```
ntp-server enable
```

パラメータ

パラメータはありません

この設定を行わない場合

NTP サーバ機能を使用できません。

設定モード

基本設定モード

ntp-server stratum

本装置で NTP サーバ機能を使用する際の Stratum 値を設定します。
Stratum 値とは、NTP サーバの階層を示すもので、Stratum1 が最上位の階層になります。

refresh コマンド後に有効になるコマンドです。

設定例 1　Stratum 値を 2 に設定する

```
Router(config)#ntp-server stratum 2
```

コマンド書式

ntp-server stratum <stratum 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
stratum 値	NTP の Stratum 値を指定します。	1～15	省略不可

この設定を行わない場合

Stratum 値を1とします。

設定モード

基本設定モード

SSH サーバ機能

SSH サーバ機能

ip scp server enable

Secure Copy の機能を有効にします。
本装置の SCP サーバ機能を使用すると、ファームウェアファイル／設定ファイルを、暗号化して転送することができます。
SCP サーバ機能を使用する際は、ssh-server enable が必要です。

refresh コマンド後に有効になるコマンドです。

設定例 1　SCP 機能を有効にする

```
Router(config)#ip scp server enable
```

コマンド書式

```
ip scp server enable
```

この設定を行わない場合

SCP サービスは動作しません

設定モード

基本設定モード

ssh-server access-group

本装置にアクセスする SSH クライアントを、指定したアクセスリストに従いフィルタリングします。
permitn に該当する端末のみアクセスが許可されます。
該当する permit のアクセスリストがない場合、アクセスは拒否されます。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.0.0/24 のネットワークのホストからのアクセスのみを許可する

```
Router(config)# access-list 10 permit 192.168.0.0 0.0.0.255
Router(config)# ssh-server access-group 10
```

設定例２　2001:db8::/32 のネットワークのホストからのアクセスのみを許可する

```
Router(config)# access-list 3000 permit 2001:db8::/32
Router(config)# ssh-server ipv6 access-group 3000
```

コマンド書式

ssh-server [ipv6] access-group <アクセスリスト番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ipv6	IPv6 アクセスリスト番号を使用する場合に指定します。	ipv6	IPv6 アクセスリスト番号を指定できません。
アクセスリスト番号	アクセスリストで、アクセスを許可する SSH クライアントを指定し、その番号をここで指定します	1～99 3000～3499 10000～11200 30000～31499	省略不可

この設定を行わない場合

すべての SSH アクセスを許可します

設定モード

基本設定モード

ssh-server enable

SSH サーバを動作させる場合に指定します。本装置は SSH version1、および SSH version2 をサポートしています。version 指定しない場合は、SSHv1/SSHv2 どちらのバージョンも動作します。
バージョンを指定したい場合は、本コマンドで version を指定してください。

暗号化アルゴリズムは、aes256-ctr／aes192-ctr／aes128-ctr／aes256-cbc／aes192-cbc／aes128-cbc／3des-cbc をサポートしています。
また、generate key ssh でホスト固有鍵を生成しておく必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　SSH サーバを動作させる

```
Router(config)#ssh-server enable
```

コマンド書式

```
ssh-server enable [version <1-2>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
version 1 version 2	SSH サーバで使用する version を指定します。 version 1：SSH サーバにおいて version1 で動作します version 2：SSH サーバにおいて version2 で動作します	1 2	SSHv1/SSHv2 どちらのバージョンも動作します。

この設定を行わない場合

SSH サーバ機能は動作しません。

設定モード

基本設定モード

ssh-server exec-timeout

無通信監視時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　TELNET では、3 分間入力がない場合は自動ログアウトする

```
Router(config)# ssh-server exec-timeout 3
```

コマンド書式

ssh-server exec-timeout <無通信監視時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
無通信 監視時間	無通信監視時間(単位:分)を設定します。 ここで設定した時間なにも入力がない場合は、自動的にログアウトします。 off を指定すると自動ログアウトを無効とします。	1～60 off	省略不可

この設定を行わない場合

5 分間入力がない場合はログアウトします

設定モード

基本設定モード

ssh-server port

SSH サーバ機能で使用する TCP ポート番号を指定します。
本設定を変更した場合でも、既に確立しているセッションは維持します。
新たなセッション確立の場合に指定したポートを使用します。

refresh コマンド後に有効になるコマンドです。

設定例 1　SSH サーバ機能で使用する TCP ポート番号として 8192 番を指定する

```
(config)# ssh-server port 8192
```

コマンド書式

ssh-server port <ポート番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	SSH サーバ機能で使用する TCP ポート番号を指定します。本設定を変更した場合でも、既に確立しているセッションは維持します。新たなセッション確立の場合に指定したポートを使用します。	8192～49151	省略不可

この設定を行わない場合

SSH サーバ機能で使用する TCP ポート番号として 22 番を使用します。

設定モード

基本設定モード

ssh-server response-timeout

SSH のネゴシエーションにおいて、SSH クライアントからの応答待ち時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　60 秒間応答がない場合は セッションを切断する

```
Router(config)# ssh-server response-timeout 60
```

コマンド書式

ssh-server response-timeout <タイムアウト時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タイムアウト時間	SSH クライアントからの応答待ち時間(単位:秒)。ここで設定した時間クライアントからの応答がない場合、SSH セッションを解放します。	1～120	省略不可

この設定を行わない場合

SSH クライアントからの応答待ち時間は、120 秒になります。

設定モード

基本設定モード

Ethernet 機能

Ethernet 機能

if-state spoofing-up

インタフェースの UP/DOWN の状態を、Ethernet リンクの状態に連動させるか常に UP とするかを指定します。
本コマンドを設定した場合は、設定しているインタフェースが属するブリッジグループのリンク状態に関係なく、常に UP となります。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN１のリンク状態を常に UP とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#if-state spoofing-up
```

コマンド書式

```
if-state spoofing-up
```

パラメータ

パラメータはありません。

この設定を行わない場合

インタフェースが属するブリッジグループの全てのポートがリンクダウンした場合に "down"、1つでもリンクアップしている場合に "up"となります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

lag mode enable

リンクアグリゲーションを使用する場合に設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　リンクアグリゲーションを使用する

```
Router(config)#line lan
Router(config line lan)# lag mode enable
```

コマンド書式

lag mode enable

パラメータ

パラメータはありません。

この設定を行わない場合

リンクアグリゲーションを使用しない。

設定モード

Ethernet 設定モード

line

Ethernet インタフェースについて、速度/デュプレックス/SFP/MDI/MDI-X の設定を行なう Ethernet 設定モードに移行するためのコマンドです。

refresh コマンド後に有効になるコマンドです。

設定例 1　EWAN#1 ポートの設定を行なうモードに移行する

```
Router(config)# line ewan 1
Router(config line ewan 1)#
```

コマンド書式

line〈物理インタフェース〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
物理 インタフェース	設定を行なう物理インタフェースを選択します。 lan：LAN インタフェース（SW-HUB 8 ポート） ewan 1：EWAN#1 ポート ewan 2：EWAN#2 ポート	lan ewan 1 ewan 2	省略不可

設定モード

基本設定モード

mac access-list

MAC アドレスによるフィルタリングを行う場合の MAC アクセスリストの設定を行います。
使用方法は、まず本コマンドで MAC アドレスを指定した後、mac access-group コマンドで指定した MAC アクセスリスト番号を指定します。
mac access-list は、番号順に適用されます。
また、同じ番号の mac access-list に複数行の設定をした場合は、上の行から適用されます。
EtherType によるフィルタリングの指定も可能です。

refresh コマンド後に有効になるコマンドです。

MAC アクセスリスト番号について

本装置の MAC アクセスリスト番号は、以下の規定があります。

MAC アクセスリスト番号	名称	設定内容
1～10240	MAC アクセスリスト標準設定 フィルタリングで使用	送信元 MAC アドレス指定
20000～20199	MAC アクセスリスト拡張設定 フィルタリングで使用	送信元 MAC アドレス指定 EtherType 指定
30000～30199	MAC アクセスリスト拡張設定 QoS で使用	送信元 MAC アドレス指定 宛先 MAC アドレス指定 EtherType 指定

設定例１　MAC アクセスリストに、MAC アドレス 1122.3344.5566 を許可属性として設定する

```
Router(config)# mac access-list 1 permit 1122.3344.5566
```

設定例２　MAC アクセスリストに、全ての MAC アドレスを不許可属性として設定する

```
Router(config)# mac access-list 1 deny any
```

設定例３　MAC アクセスリストで、PPPoE フレームを許可する

```
Router(config)# mac access-list 20000 permit any ethertype pppoe-discovery
Router(config)# mac access-list 20000 permit any ethertype pppoe-session
Router(config)# mac access-list 20000 deny any
```

設定例４　MAC アクセスリストに、送信元 MAC アドレス；全て／宛先 MAC アドレス：1122.3344.0000～1122.3344.ffff を許可属性として設定する

```
Router(config)# mac access-list 30000 permit any 1122.3344.0000 ffff.ffff.0000
```

コマンド書式

```
mac access-list <mac access-list 番号> remark<コメント>
mac access-list <mac access-list 番号> permit <MAC アドレス> [log] [count]
mac access-list <mac access-list 番号> deny {<MAC アドレス>|any} [log] [count]
mac access-list <mac access-list 番号> {permit|deny} <any> ethertype <フィル
                                       タリング対象>] [log] [count]
mac access-list <mac access-list 番号> {permit|deny} {any|host <送信元 MAC ア
                 ドレス>|<送信元 MAC アドレス> <送信元 MAC アドレス範囲>}  {any|
                 host <宛先 MAC アドレス>|<宛先 MAC アドレス> <宛先 MAC アドレス
                 範囲>} [ethertype <フィルタリング対象>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
mac access-list 番号	設定する MAC アクセスリスト番号を指定します。	1～10240 20000～20199 30000～30199	省略不可
permit	設定する MAC アクセスリストに許可属性を与える場合に指定します。	permit	省略不可
deny	設定する MAC アクセスリストに不許可属性を与える場合に指定します。	deny	省略不可
MAC アドレス	MAC アドレスを H.H.H の形式で設定します。 MAC アドレスが、11.22.33.44.55.66 の場合は、1122.3344.5566 となります。	MAC アドレス形式	省略不可
送信元 MAC アドレス	送信元 MAC アドレスを H.H.H の形式で設定します。	MAC アドレス形式	省略不可
送信元 MAC アドレス範囲	送信元 MAC アドレスを範囲指定するために、マスクを指定します。	MAC アドレス形式	省略不可
宛先 MAC アドレス	宛先 MAC アドレスを H.H.H の形式で設定します。	MAC アドレス形式	省略不可
宛先 MAC アドレス範囲	宛先 MAC アドレスを範囲指定するために、マスクを指定します。	MAC アドレス形式	省略不可
any	mac access-list 番号が 20000～20199 , 30000～301999 または deny を指定した場合は、MAC アドレスの代わりに any を指定することにより、全ての MAC アドレスを指定することができます。	any	省略不可
フィルタリング対象	EtherType によるフィルタリング対象を指定します。 hex：EtherType を直接指定します。 pppoe-：PPPoE Discovery Stage	hex pppoe-discovery pppoe-session arp ip	EtherType によるフィルタリングを行いません。

	discovery	EtherType (0x8863)をフィルタリング対象とします。	ipv6	
	pppoe-session	PPPoE Session Stage EtherType (0x8864)をフィルタリング対象とします。		
	arp	ARP EtherType (0x0806)をフィルタリング対象とします。		
	ip	IP EtherType (0x0800)をフィルタリング対象とします。		
	ipv6	IPv6 EtherType (0x86DD)をフィルタリング対象とします。		
log	パケットフィルタリング機能において該当条件(行単位)にヒットしたパケットが、フィルタリングログに記録されます。		log	フィルタリングログを記録しません。
count	統計情報としてフィルタにヒットしたパケット数、バイト数を表示します。		count	カウントを行いません。
コメント	MAC アクセスリストに付けるコメントを指定します。		240 文字までの半角英数字、記号	省略不可

この設定を行わない場合

MAC アドレスや EtherType によるフィルタリング、QoS を行いません。

設定モード

基本設定モード

mac access-group

mac access-list コマンドで指定したフィルタリングデータを、各インタフェースで適用します。
フィルタリングデータは、各インタフェースで受信したパケットに適用するのか／各インタフェースに送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　mac access-list 1 で指定したデータを、EWAN 1 送信時に適用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#mac access-group 1 out
```

設定例２　mac access-list 2 で指定したデータを、EWAN 1 からの受信時に適用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#mac access-group 2 in
```

コマンド書式

mac access-group <mac access-list 番号> { in | out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
mac access-list 番号	フィルタリングデータを設定した MAC アクセスリストの番号を指定します。	1～10240 20000～20199	省略不可
{ in | out }	インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。	in out	省略不可

この設定を行わない場合

MAC アドレスによるフィルタリングを行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

select-port

EWAN ポート 1～2 を 1000BASE-T として使用するか、SFP として使用するかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　EWAN ポート 1 を SFP で使用する

```
Router(config)# line ewan 1
Router(config line ewan 1)# select-port 1 sfp
```

コマンド書式

select-port <ポート番号> < fixed | sfp >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	EWAN インタフェースの 1～2 のポート番号を指定します。	1～2	省略不可
fixed | sfp	設定している Ethernet インタフェースを fixed (1000BASE-T)として使用するか、SFP として使用するかを設定します。	fixed sfp	省略不可

この設定を行わない場合

1000BASE-T として動作します。

SFP とは？

SFP とは、Small Form Factor Pluggable の呼称で、光モジュールの一種です。

EWAN ポート 1～2 のギガイーサネットインタフェースは、1000BASE-T と SFP を排他的に使用することができます。

設定モード

Ethernet 設定モード

shutdown

物理的にポートを停止させる場合に指定します。
本コマンドでポートを停止させた場合、該当するポートはリンクアップしなくなります。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN インタフェースのポート 1 をリンクアップしない状態にする

```
Router(config)#line lan
Router(config-line lan)#shutdown 1
```

設定例１　EWAN#2 インタフェースをリンクアップしない状態にする

```
Router(config)#line ewan 2
Router(config-line ewan 2)#shutdown 1
```

コマンド書式

shutdown〈ポート番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	LAN インタフェースの場合は、1～8 のポート番号を指定します。 EWAN インタフェースの場合は、ポート番号 1 を指定します。	1～8	省略不可

この設定を行わない場合

LAN および EWAN インタフェースが使用可能です。

設定モード

Ethernet 設定モード

speed-duplex

Ethernet の通信速度/デュプレックス(全二重 or 半二重)を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　LAN（ポート番号 6）の通信速度を、1000Mbps/Full デュプレックス（全二重）に設定する

```
Router(config)#line lan
Router(config line lan)# speed-duplex 6 1000-full
```

コマンド書式

speed-duplex <ポート番号> < 通信速度とデュプレックス >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	LAN インタフェースには、8 つのポートがあるので、その番号を指定します。 EWAN インタフェースの場合は、"1"を指定します。	1～8	省略不可
通信速度とデュプレックス	設定している Ethernet インタフェースの通信速度／デュプレックスを設定します。 10-full　10Mbps/Full デュプレックス 10-half　10Mbps/Half デュプレックス 100-full　100Mbps/Full デュプレックス 100-half　100Mbps/Half デュプレックス 1000-full　1000Mbps/Full デュプレックス 1000-half　1000Mbps/Half デュプレックス auto　AUTO ネゴシエーション	10-full 10-half 100-full 100-half 1000-full 1000-half auto	省略不可

この設定を行わない場合

AUTO ネゴシエーションで動作します。

設定モード

Ethernet 設定モード

sw

Ethernet の MDI/MDI-X を設定します。
refresh コマンド後に有効になるコマンドです。

設定例 1　LAN（ポート番号 6）を、MDI-X に設定する

```
Router(config)#line lan
Router(config line lan)# sw 6 mdi-x
```

コマンド書式

sw 〈ポート番号〉〈MDI 設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	LAN インタフェースには、8 つのポートがあるので、その番号を指定します。 EWAN インタフェースの場合は、"1"を指定します。	1～8	省略不可
MDI 設定	設定している Ethernet インタフェースの MDI/MDI-X を設定します。 mdi　MDI ポート mdi-x　MDI-X ポート auto　自動切換	mdi mdi-x auto	省略不可

この設定を行わない場合

自動切換で動作します。

MDI/MDI-X とは？

Ethernet ポートにおいて、DTE として使用するポートを"MDI ポート"、DCE として使用するポートを"MDI-X ポート"といいます。
通常の NIC は MDI ポート、HUB は MDI-X ポートで運用されています。
ストレートケーブルを使用する場合、相手が MDI である場合は自分は MDI-X、相手が MDI-X である場合は自分は MDI でなくてはなりません。

接続相手が自動切換の装置の場合は、本装置では自動切換にしないようにしてください。
Ethernet が使用できない場合があります。

設定モード

Ethernet 設定モード

vlan lag-group

指定するポートがどのリンクアグリゲーショングループに属するかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN ポート２をリンクアグリゲーショングループ２に関連づける

```
Router(config)#line lan
Router(config line lan)# vlan 2 lag-group 2
```

コマンド書式

vlan 〈ポート番号〉 lag-group 〈LAG グループ〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	LAN の物理ポート番号を指定します。	1～8	省略不可
LAG グループ	リンクアグリゲーショングループの番号を指定します。	1～2	省略不可

この設定を行わない場合

LAN ポートをリンクアグリゲーショングループに関連づけない。

設定モード

Ethernet 設定モード

VLAN 機能

VLAN 機能

ip access-group

access-list コマンドで指定したフィルタリングデータを、各インタフェースで適用します。
フィルタリングデータは、各インタフェースで受信したパケットに適用するのか、送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　access-list 1 で指定したデータを、PPPoE1 送信時に適用する

```
Router(config)#interface pppoe 1
Router(config-if lan 1)#ip access-group 1 out
```

設定例２　access-list 2 で指定したデータを、PPPoE1 からの受信時に適用する

```
Router(config)#interface pppoe 1
Router(config-if lan 1)#ip access-group 2 in
```

コマンド書式

ip access-group <access-list 番号> { in [interface | vpn]| out }

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>access-list 番号</td><td>フィルタリングのデータを設定したアクセスリストの番号を指定します。</td><td>1～99
100～199
1300～1999
2000～2699
10000～11200
20000～21199</td><td>省略不可</td></tr>
<tr><td>{ in[interface | vpn]| out }</td><td>インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。
受信時は、さらに以下のように設定ができます。
<table><tr><td>in vpn</td><td>自局宛 VPN 対象パケットを制御</td></tr><tr><td>in interface</td><td>自局宛非 VPN 対象パケットを制御</td></tr></table></td><td>in
in vpn
in interface
out</td><td>省略不可</td></tr>
</table>

LAN インタフェースおよび IPsec インタフェースでは、vpn を選択することはできません。
in vpn および in interface を選択した場合、適用する access-list の宛先は、any とする必要があります。

この設定を行わない場合

該当インタフェースでは、IP パケットフィルタリングを使用しません。

IP フィルタリングについて

指定したパケット以外は中継しないといったように、セキュリティ強化のため使用する機能です。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード
BVI インタフェース設定モード
USB Ethernet インタフェース設定モード

ip address

VLAN インタフェースの IP アドレスとサブネットマスクを指定します。

設定例 1　VLAN インタフェースの IP アドレスを 158.ｘｘｘ.ｘｘｘ.1 に設定する

```
Router(config)#interface vlanif 1
Router(config-if vlanif 1)#ip address 158.202.232.2 255.255.255.0
```

コマンド書式

ip address <IP アドレス> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	インタフェースに割り当てる IP アドレスを設定します。	IPv4 アドレス形式	省略不可
サブネットマスク	サブネットマスクを設定します。	IPv4 アドレス形式	省略不可

設定モード

VLAN インタフェース設定モード

bridge-group

設定している VLAN インタフェースで使用するブリッジグループ番号を指定します。
この設定により、VLAN インタフェースと、ブリッジグループのひも付けを行うことができます。

設定例 1　VLAN インタフェースで使用するブリッジグループを 1 番とする

```
Router(config)#interface vlanif 1
Router(config-if vlanif 1) bridge-group lan 1
```

コマンド書式

bridge-group lan <ブリッジグループ番号>
bridge-group ewan <1-2>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ブリッジグループ番号	ブリッジグループ番号を指定します。	0～15	省略不可

この設定を行わない場合

インタフェースを使用することができません。

設定モード

VLAN インタフェース設定モード

tagging never

本コマンドを設定することにより、nulltag を除去し untag フレームで HUB に対して出力をおこないます。

設定例　nulltag を除去したフレームを出力する

```
Router(config)#line lan
Router(config-line lan)#tagging never
```

コマンド書式

```
tagging never
```

パラメータ

パラメータはありません

この設定を行わない場合

nulltag を付与します。

設定モード

LAN インタフェース設定モード

vlan bridge-group

ブリッジグループ番号を指定します。この設定により、物理ポートとブリッジグループのひも付けを行うことができます。
LAN ポートのみ指定することができます。

設定例 1　VLAN 機能で使用する物理ポート 1 番と、ブリッジグループ 5 番をひも付ける

```
Router(config)#line lan
Router(config line lan) vlan 1 bridge-group 5
```

コマンド書式

vlan <ポート番号> bridge-group <ブリッジグループ番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	物理ポート番号を指定します。	1～8	省略不可
ブリッジグループ番号	ブリッジグループ番号を指定します。	0～15	省略不可

この設定を行わない場合

ブリッジグループ番号=0 で動作します。

設定モード

Ethernet 設定モード

vlan egress-tagging null-tag

LAN のインターフェースでタグ VLAN 機能を利用していないときに、送信フレームに NULL タグを付与するかどうかを指定します。
タグ VLAN を利用していないインターフェースで 802.1p 優先制御を行う際に利用します。

設定例 1　送信するパケットに対して 802.1p の優先度タグを付加する

```
Router(config)#line lan
Router(config-line lan)#vlan 1 egress-tagging null-tag always
```

コマンド書式

vlan <ポート番号> egress-tagging null-tag <TAG 設定>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	物理ポート番号を LAN ポートの場合 1～8、EWAN ポートの場合 1～2 で指定します。	1～8	省略不可
TAG 設定	優先度タグを付加するか、しないかを指定します。 always：パケットに優先度タグを付加して送信します。 never：パケットに優先度タグを付加しないで送信します。	always never	省略不可

この設定を行わない場合

優先度タグは付加されません。

設定モード

Ethernet 設定モード

vlan-id

このインタフェースで扱うタグフレーム ID 値を指定します。
この値は、接続する相手(L2 スイッチなど)と同じである必要があります。
また、BVI インタフェースをどの VID のインターナルブリッジに紐付けるかを指定します。

設定例 1　送信する VLAN-ID を 1 とします

```
Router(config)#interface vlanif 1
Router(config-if vlanif 1)# vlan-id 1
```

コマンド書式

vlan-id {<VLAN-ID 値> | any}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VLAN-ID 値	VLAN インタフェースでは、インタフェースで送信する際の VLAN-ID を指定します。	1～4094	省略不可
	BVI インタフェースでは、紐付ける VID のインターナルブリッジを指定します。	0～4094	
any	全 VLAN-ID を該当トンネルインタフェースで取り扱います。	any ※	省略不可

※ パラメータ　any は VLAN インタフェース設定モードのみ対応

この設定を行わない場合

インタフェースを使用することができません。

設定モード

VLAN インタフェース設定モード
BVI インタフェース設定モード

vlan port-vlan

HUB の各ポート(物理ポート)で、ポート VLAN を運用する場合に設定します。

設定例 1　ポート VLAN を使用するポートを物理ポート 1 番、VLAN-ID を 10 とする

```
Router(config)#line lan
Router(config line lan)#vlan 1 port-vlan 10
```

コマンド書式

vlan <ポート番号> port-vlan <VLAN-ID 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	ポート VLAN を運用する物理ポート番号を指定します。	1～8	省略不可
VLAN-ID 値	ポート VLAN で使用する VLAN-ID を指定します。	1～4094	省略不可

この設定を行わない場合

ポート VLAN を使用することができません。

設定モード

Ethernet 設定モード

アクセスリスト

アクセスリスト

access-list

特定のパケットと、そのパケットの動作（中継 or 廃棄 or 学習フィルタリング）を指定します。
指定したパケットは、以下の機能で使用します。
・フィルタリング（ip access-group コマンド）
・学習フィルタリング（ip access-group コマンド）
・オフセットリスト（offset-list コマンド）
・RIP/BGP で送信するメトリック値の指定（distance コマンド）
・BGP で送信する経路の指定（neighbor <IP-address> distribute-list コマンド）
・経路情報の指定（match ip address コマンド）
・NextHop の指定（match ip nexthop コマンド）
・NAT 変換前のアドレス指定（ip nat inside コマンド）
・ポリシールーティング（match ip access-group コマンド）

使用方法は、まず本コマンドでパケットを指定した後、上記機能を使用するモードで、
指定したアクセスリスト番号を指定します。
access-list は、番号順に適用されます。
また、同じ番号の access-list に複数行の設定をした場合は、上の行から適用されます。

refresh コマンド後に有効になるコマンドです。

アクセスリスト番号について

本装置のアクセスリスト番号は、以下の規定があります。

アクセスリスト番号	名称	設定内容
1～99、1300～1999 10000～11200	IPv4 標準設定	IPv4 送信元アドレス指定
100～199、2000～2699 20000～21199	IPv4 拡張設定	IPv4 送信元／宛先アドレス指定 プロトコル番号指定 送信元／宛先ポート番号指定
3000～3499 30000～31499	IPv6 標準設定	IPv6 送信元／宛先アドレス指定
3500～3999 35000～36499	IPv6 拡張設定	IPv6 送信元アドレス指定 プロトコル番号指定 送信元／宛先ポート番号指定

指定パケットの動作指定について

指定したパケットを中継対象とするか、廃棄対象とするかを指定します。中継対象とする場合は permit、廃棄対象とする場合は deny を指定します。
この指定が必要なのは、フィルタリング／経路情報の指定／NextHop の指定のためにアクセスリストを指定する場合のみです。他の用途で指定する場合は permit を指定してください。

IP アドレス範囲指定

アクセスリストコマンドで IPv4 アドレスを指定する場合、マスク(Wildcard マスク)を使用して 1 エントリでアドレス範囲を指定することができます。
Wildcard マスクは、サブネットマスクとは書式が異なりますので注意してください。Wildcard マスクとサブネットマスクは、"1"と"0"の判別が逆になります。
例1)24bit マスクを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
Wildcard マスクの場合:0.0.0.255
サブネットマスクの場合:255.255.255.0
例2)ホストを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
Wildcard マスクの場合:0.0.0.0
サブネットマスクの場合:255.255.255.255

ポート番号の指定

IPv4/IPv6 拡張設定では、TCP/UDP 上位ポート番号を指定することができます。この指定は、フィルタリング/学習フィルタリングの指定のためにアクセスリストを指定する場合に効果があります。他の用途で指定する場合は、標準設定でアクセスリストを指定してください。

学習フィルタリング

インターネットの常時接続で使用する場合、セキュリティとしては危険な状態に常にさらされています。
学習フィルタリング機能では、LAN 側からのインターネット接続に対する応答データ以外はフィルタリング(廃棄)することができます。
学習フィルタリング機能を使用する場合は、外部からのアクセス(Web 等)はできなくなります。(アクセスを許可するアドレスを限定することはできます)
ただし、VPN からの受信に関してはフィルタリングを行いません。(ルートベースの VPN を除く)

本装置で、学習フィルタリングを使用する場合は、access-list コマンドの属性で、"dynamic"を指定します。

設定例 1　IPv4 標準アクセスリストに、192.168.100.0/24 を設定する (許可属性)

```
Router(config)# access-list 1 permit 192.168.100.0 0.0.0.255
```

設定例 2　IPv4 拡張アクセスリストに、src=192.168.100.0/24 dst=192.168.200.0/24 を設定する (不許可属性)

```
Router(config)# access-list 100 deny ip 192.168.100.0 0.0.0.255 192.168.200.0
0.0.0.255
```

設定例 3　IPv6 標準アクセスリストに、src=3ffe:110::/64 を dst=3ffe:111::/64 を設定する (許可属性)

```
Router(config)# access-list 3000 permit 3ffe:110::/64 3ffe:111::/64
```

設定例４　IPv6 拡張アクセスリストに、src=any srcport=any dst=any dstport=80 を設定する（不許可属性）

```
Router(config)# access-list 3500 deny tcp any gt 0 any eq 80
```

設定例５　学習フィルタリングを指定する（IPv4）

```
Router(config)# access-list 100 dynamic permit ip any any
```

設定例６　宛先が fnsc.co.jp 宛のポリシールーティング(ipsecif1 経由)を設定する

```
Router(config)#fqdn-list 1 www.fnsc.co.jp
Router(config)#access-list 100 permit ip any fqdn-list 1

Router(config)#class-map FNSC
Router(config-class-map)#match ip access-group 100
Router(config-class-map)#exit

Router(config)#action-map ipsecif1
Router(config-action-map)#set ip next-hop connected ipsecif 1
Router(config-action-map)#exit

Router(config)#policy-map FNSC
Router(config-policy-map)#class FNSC action ipsecif1
Router(config-policy-map)#exit

Router(config)#interface lan 1
Router(config-if lan 1)#service-policy input FNSC
Router(config-if lan 1)#exit
```

コマンド書式

IPv4 標準アクセスリスト（番号：1～99、1300～1999、10000-11200）
access-list <access-list 番号> { permit | deny } { any | <送信元 IP アドレス> <送信元 Wildcard マスク> }[log][count]

IPv4 拡張アクセスリスト（番号：100～199、2000～2699、20000～21199）
access-list <access-list 番号> { [dynamic] permit | deny } <プロトコル番号> { any | host <送信元 IP アドレス> | <送信元 IP アドレス> <送信元 Wildcard マスク> } [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] { any | host <宛先 IP アドレス> | <宛先 IP アドレス> <宛先

Wildcard マスク> | fqdn-list <fqdn-list 番号> } [ICMP タイプ] [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] [[precedence {<precedence-value>|<precedence-named-value>}] [tos {<tos-value>|<tos-named-value>}]| [dscp {<dscp-value>|<dscp-named-value>}]] [ip-flag {<ip-flag-value>|<ip-flag-value:wildcard mask>}][log] [count]

IPv6 標準アクセスリスト（番号：3000～3499、30000～31499）
access-list <access-list 番号> { permit | deny } { any | <送信元 IPv6 プレフィックス> } { any | <宛先 IPv6 プレフィックス> } [count]

IPv6 拡張アクセスリスト（番号：3500～3999、35000～36499）
access-list <access-list 番号> { [dynamic] permit | deny } <プロトコル番号> { any | <送信元 IPv6 プレフィックス> } [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] { any | <宛先 IPv6 プレフィックス> | fqdn-list <fqdn-list 番号>} [ICMPv6 タイプ] [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] [tcp-flag {<tcp-flag-value>|<tcpflag-value:wildcard-mask>}] [traffic-class <traffic-class-value>|dscp {<dscp-level>|<dscp-name>}] [flow-label <flow-label-value>][count]

パラメータ

パラメータ	設定内容	設定範囲		省略時の値
access-list 番号	それぞれの属性の番号を指定します。	1～99、1300～1999 10000～11200	IPv4 標準アクセスリスト	省略不可
		100～199、2000～2699, 20000～21199	IPv4 拡張アクセスリスト	
		3000～3499 30000～31499	IPv6 標準アクセスリスト	
		3500～3999 35000～36499	IPv6 拡張アクセスリスト	
dynamic	学習フィルタリングを使用する場合に指定します。	dynamic		学習フィルタリングのエントリではない
{ permit | deny }	許可属性か、不許可属性かを選択します。	permit	許可属性	省略不可
		deny	不許可属性	

プロトコル番号	プロトコル名もしくはプロトコル番号を選択します。	esp: ESP gre: Cisco's GRE tunneling icmp: ICMP(IPv4 拡張アクセスリスト時) icmpv6: ICMPv6(IPv6 拡張アクセスリスト時) ip: IP ipinip: IP トンネル tcp: TCP udp: UDP 0～255: プロトコル番号を指定	省略不可
any	各パラメータ(アドレスやポート番号など)で、「全て」を指定する場合は"any"を入力します。	any	-
送信元 IP アドレス	送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
送信元 Wildcard マスク	送信元アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
宛先 IP アドレス	宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
宛先 Wildcard マスク	宛先アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
fqdn-list※2	fqdn-list を指定します。	1～50※3	省略不可
host	IPv4 拡張アクセスリストで、送信元/宛先アドレスとしてホストアドレスを指定する場合につけます。	host	-
送信元 IPv6 プレフィックス	送信元 IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可
宛先 IPv6 プレフィックス	宛先 IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可
ICMP タイプ	プロトコル番号で"icmp"を指定した場合に、対象とする ICMP タイプを指定します。	**指定できる ICMP タイプ** administratively-prohibited alternate-address conversion-error	全ての ICMP タイプ

		dod-host-prohibited	
		dod-net-prohibited	
		echo	
		echo-reply	
		general-parameter-problem	
		host-isolated	
		host-precedence-unreachable	
		host-redirect	
		host-tos-redirect	
		host-tos-unreachable	
		host-unknown	
		host-unreachable	
		information-reply	
		information-request	
		mask-reply	
		mask-request	
		mobile-redirect	
		net-redirect	
		net-tos-redirect	
		net-tos-unreachable	
		net-unreachable	
		network-unknown	
		no-room-for-option	
		option-missing	
		packet-too-big	
		parameter-problem	
		port-unreachable	
		precedence-unreachable	
		protocol-unreachable	
		reassembly-timeout	
		redirect	
		router-advertisement	
		router-solicitation	
		source-quench	
		source-route-failed	

		time-exceeded timestamp-reply timestamp-request traceroute ttl-exceeded unreachable ICMP タイプ値(0～255)	
ICMPv6 タイプ(IPv6)	プロトコル番号で"icmpv6"を指定した場合に、対象とする ICMPv6 タイプを指定します。	**ICMPv6 タイプ** address-unreachable administratively-prohibited dest-unreachable echo-reply echo-request erroneous-header-field hop-limit-exceeded-in-transit multicast-listener-done multicast-listener-query multicast-listener-report neighbor-advertisement neighbor-solicitation no-route-to-destination packet-too-big parameter-problem port-unreachable reassembly-time-exceeded redirect router-advertisement router-solicitation time-exceeded unrecognized-next-header unrecognized-option ICMPv6 タイプ値(0～255)	全ての ICMPv6 タイプ

ポート属性	ポート番号を範囲で指定するために、ポート属性を指定します。	eq	指定するポートが対象	全てのポート（以降設定なし）
		gt	指定するポート番号より大きいポート番号が対象	
		lt	指定するポート番号より小さいポート番号が対象	
		neq	指定するポート番号以外のポート番号が対象	
		range	ポートの範囲を指定する	
TCP ポート番号	プロトコルで"tcp"を指定した場合に、対象とする TCP ポート番号を指定します。	TCP ポート番号		全ての TCP ポート番号
		bgp		
		chargen		
		cmd		
		daytime		
		discard		
		domain		
		echo		
		exec		
		finger		
		ftp		
		ftp-data		
		gopher		
		hostname		
		ident		
		irc		
		klogin		
		kshell		
		login		
		lpd		
		nntp		
		pim-auto-rp		
		pop2		
		pop3		
		smtp		

		sunrpc syslog tacacs tacacs-ds talk telnet time uucp whois www TCP ポート番号(0～65535)	
UDP ポート番号	プロトコルで"udp"を指定した場合に、対象とする UDP ポート番号を指定します。	**UDP ポート番号** biff bootpc bootps discard dnsix domain echo isakmp mobile-ip nameserver netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip snmp snmptrap sunrpc syslog tacacs tacacs-ds talk	全ての UDP ポート番号

		tftp time who xdmcp UDP ポート番号(0～65535)	
precedence-value※1	precedence-value を設定します。	0～7	省略不可
precedence-named-value※1	precedence-named-value を設定します。	routine(0) priority(1) immediate(2) flash(3) flash-override(4) critical(5) internet(6) network(7)	省略不可
tos-value※1	tos-value を設定します。	0～15	省略不可
tos-named-value※1	tos-named-value を設定します。	min-momentary-cost(1) max-reliability(2) max-throughput(4) min-delay(8) normal(0)	省略不可
dscp-value※1	dscp-value を設定します。	0～63	省略不可
dscp-named-value※1	dscp-named-value を設定します。	ef(101110b) bf(000000b) af11(001010b) af12(001100b) af13(001110b) af21(010010b) af22(010100b) f23(010110b) af31(011010b) af32(011100b) af33(011110b) af41(100010b) af42(100100b)	省略不可

		af43(100110b)	
ip-flag-value※1	ip-flag-value を設定します。	0～3、もしくは、0～3:0～3（ワイルドカードマスク）	省略不可
tcp-flag-value※1	tcp-flag-value を設定します。	0～63、もしくは、0～63:0～63（ワイルドカードマスク）	省略不可
traffic-class-value	traffic-class-value を設定します。	0～255、もしくは、0～255:0～255（ワイルドカードマスク）	省略不可
flow-label	flow-label を設定します。	0～1048575	省略不可
log	パケットフィルタリング機能において該当条件（行単位）にヒットしたパケットが、フィルタリングログに記録されます。 ※dynamic 指定の場合、学習した学習フィルタにヒットしたパケットは記録しません。	log	フィルタリングログを記録しません。
count	統計情報としてフィルタにヒットしたパケット数、バイト数を表示します。 ※dynamic 指定の場合、学習した学習フィルタにヒットしたパケットは記録しません。	count	カウントを行いません。

※1 これらのパラメータをフィルタリングで使用する事はできません。
※2 パラメータ fqdn-list は、V1.02(00)以降サポート
※3 パラメータ fqdn-list 番号の設定範囲 1～50 は、V01.04(00)以降サポート

この設定を行わない場合

access-list を使用した機能を使用できません。

設定モード

基本設定モード

access-list remark

アクセスリストに対して、コメントを記述することができます。
記述した内容は show access-list で表示されます。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.100.1 からのアクセスを拒否しているコメントを付ける

```
Router(config)#access-list 100 remark Reject access from 192.168.100.1
Router(config)
```

コマンド書式

access-list <access-list 番号> remark <文字>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	コメントを付けるアクセスリスト番号を指定します。	1～3999※	省略不可
文字	コメントを入力します。	240 文字までの半角英数字、記号	省略不可

※ access-list 番号の設定範囲に関しては、access-list コマンドを参照してください。

設定モード

基本設定モード

mac access-list

MAC アドレスによるフィルタリングを行う場合の MAC アクセスリストの設定を行います。
使用方法は、まず本コマンドで MAC アドレスを指定した後、mac access-group コマンドで指定した MAC アクセスリスト番号を指定します。
mac access-list は、番号順に適用されます。
また、同じ番号の mac access-list に複数行の設定をした場合は、上の行から適用されます。
EtherType によるフィルタリングの指定も可能です。

refresh コマンド後に有効になるコマンドです。

MAC アクセスリスト番号について

本装置の MAC アクセスリスト番号は、以下の規定があります。

MAC アクセスリスト番号	名称	設定内容
1～10240	MAC アクセスリスト標準設定 フィルタリングで使用	送信元 MAC アドレス指定
20000～20199	MAC アクセスリスト拡張設定 フィルタリングで使用	送信元 MAC アドレス指定 EtherType 指定
30000～30199	MAC アクセスリスト拡張設定 QoS で使用	送信元 MAC アドレス指定 宛先 MAC アドレス指定 EtherType 指定

設定例１　MAC アクセスリストに、MAC アドレス 1122.3344.5566 を許可属性として設定する

```
Router(config)# mac access-list 1 permit 1122.3344.5566
```

設定例２　MAC アクセスリストに、全ての MAC アドレスを不許可属性として設定する

```
Router(config)# mac access-list 1 deny any
```

設定例３　MAC アクセスリストで、PPPoE フレームを許可する

```
Router(config)# mac access-list 20000 permit any ethertype pppoe-discovery
Router(config)# mac access-list 20000 permit any ethertype pppoe-session
Router(config)# mac access-list 20000 deny any
```

設定例４　MAC アクセスリストに、送信元 MAC アドレス；全て／宛先 MAC アドレス：1122.3344.0000～1122.3344.ffff を許可属性として設定する

```
Router(config)# mac access-list 30000 permit any 1122.3344.0000 ffff.ffff.0000
```

コマンド書式

```
mac access-list <mac access-list 番号> remark<コメント>
mac access-list <mac access-list 番号> permit <MAC アドレス> [log] [count]
mac access-list <mac access-list 番号> deny {<MAC アドレス>|any} [log] [count]
mac access-list <mac access-list 番号> {permit|deny} <any> ethertype <フィル
                                       タリング対象>] [log] [count]
mac access-list <mac access-list 番号> {permit|deny} {any|host <送信元 MAC ア
                ドレス>|<送信元 MAC アドレス> <送信元 MAC アドレス範囲>}  {any|
                host <宛先 MAC アドレス>|<宛先 MAC アドレス> <宛先 MAC アドレス
                範囲>} [ethertype <フィルタリング対象>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
mac access-list 番号	設定する MAC アクセスリスト番号を指定します。	1～10240 20000～20199 30000～30199	省略不可
permit	設定する MAC アクセスリストに許可属性を与える場合に指定します。	permit	省略不可
deny	設定する MAC アクセスリストに不許可属性を与える場合に指定します。	deny	省略不可
MAC アドレス	MAC アドレスを H.H.H の形式で設定します。 MAC アドレスが、11.22.33.44.55.66 の場合は、1122.3344.5566 となります。	MAC アドレス形式	省略不可
送信元 MAC アドレス	送信元 MAC アドレスを H.H.H の形式で設定します。	MAC アドレス形式	省略不可
送信元 MAC アドレス範囲	送信元 MAC アドレスを範囲指定するために、マスクを指定します。	MAC アドレス形式	省略不可
宛先 MAC アドレス	宛先 MAC アドレスを H.H.H の形式で設定します。	MAC アドレス形式	省略不可
宛先 MAC アドレス範囲	宛先 MAC アドレスを範囲指定するために、マスクを指定します。	MAC アドレス形式	省略不可
any	mac access-list 番号が 20000～20199 , 30000～301999 または deny を指定した場合は、MAC アドレスの代わりに any を指定することにより、全ての MAC アドレスを指定することができます。	any	省略不可
フィルタリング対象	EtherType によるフィルタリング対象を指定します。 hex：EtherType を直接指定します。 pppoe-：PPPoE Discovery Stage	hex pppoe-discovery pppoe-session arp ip	EtherType によるフィルタリングを行いません。

	discovery	EtherType (0x8863)をフィルタリング対象とします。	ipv6	
	pppoe-session	PPPoE Session Stage EtherType (0x8864)をフィルタリング対象とします。		
	arp	ARP EtherType (0x0806)をフィルタリング対象とします。		
	ip	IP EtherType (0x0800)をフィルタリング対象とします。		
	ipv6	IPv6 EtherType (0x86DD)をフィルタリング対象とします。		
log	パケットフィルタリング機能において該当条件(行単位)にヒットしたパケットが、フィルタリングログに記録されます。		log	フィルタリングログを記録しません。
count	統計情報としてフィルタにヒットしたパケット数、バイト数を表示します。		count	カウントを行いません。
コメント	MAC アクセスリストに付けるコメントを指定します。		240 文字までの半角英数字、記号	省略不可

この設定を行わない場合

MAC アドレスや EtherType によるフィルタリング、QoS を行いません。

設定モード

基本設定モード

mac access-group

mac access-list コマンドで指定したフィルタリングデータを、各インタフェースで適用します。
フィルタリングデータは、各インタフェースで受信したパケットに適用するのか／各インタフェースに送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　mac access-list 1 で指定したデータを、EWAN 1 送信時に適用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#mac access-group 1 out
```

設定例２　mac access-list 2 で指定したデータを、EWAN 1 からの受信時に適用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#mac access-group 2 in
```

コマンド書式

mac access-group <mac access-list 番号> { in | out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
mac access-list 番号	フィルタリングデータを設定した MAC アクセスリストの番号を指定します。	1～10240 20000～20199	省略不可
{ in | out }	インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。	in out	省略不可

この設定を行わない場合

MAC アドレスによるフィルタリングを行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ループバックインタフェースの設定

ループバックインタフェースの設定

description

各インタフェースに対して、コメントを記述することができます。
記述した内容は show interface で表示されます。

refresh コマンド後に有効になるコマンドです。

設定例１　ダイヤラーインタフェースにコメントを付ける

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#description backup line
```

コマンド書式

description 〈文字〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
文字	コメントを入力します。	240 文字までの半角英数字、記号	省略不可

設定モード

LAN インタフェース設定モード
PPPoE インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
ループバックインタフェース設定モード
トンネルインタフェース設定モード
BVI インタフェース設定モード
USB Ethernet インタフェース設定モード

ip address

ループバックインタフェースの IP アドレスを指定します。
サブネットマスクは、自動的に 255.255.255.255 に設定されます。

設定例 1　ループバックの IP アドレスを 192.168.0.1 に設定する

```
Router(config)#interface loopback 1
Router(config-if loopback 1)#ip address 192.168.0.1
```

コマンド書式

ip address <IP アドレス>

この設定を行わない場合

ループバックインタフェースに、IP アドレスが割り当てられません。

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	インタフェースに割り当てる IP アドレスを設定します。	IPv4 アドレス形式	省略不可

設定モード

ループバックインタフェース設定モード

ipv6 address

ループバックインタフェースの IPv6 アドレス(グローバル・リンクローカル)を指定します。
リンクローカルアドレスを指定しなかった場合は、EUI-64 形式のリンクローカルアドレスが自動で設定されます。
本装置では、1つのインタフェースに4つのグローバルアドレスを指定することができます。

設定例１　プレフィックス：2001:db8::/32　EUI-64 形式で指定する

```
Router(config)#interface loopback 1
Router(config-if loopback 1)#ipv6 address 2001:db8::/32 eui-64
```

設定例２　リンクローカルアドレスを、2001:db8::1 に設定する

```
Router(config)#interface loopback 1
Router(config-if loopback 1)#ipv6 address 2001:db8::1 link-local
```

コマンド書式

ipv6 address { <IPv6 アドレス> link-local | <IPv6 プレフィックス> [eui-64] }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPv6 アドレス	IPv6 リンクローカルアドレスを指定します。	IPv6 アドレス形式	省略不可
link-local	リンクローカルアドレスである場合に指定します。	link-local	省略不可
IPv6 プレフィックス	IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可
eui-64	EUI-64 方式でグローバルアドレスを設定する場合に指定します。	eui-64	省略した場合はグローバルアドレスとして使用しません。RA で広告するプレフィックスにのみ使用します。

最大エントリ数:256 エントリ(装置全体)

この設定を行わない場合

ループバックインタフェースでは、IPv6 アドレスが割り当てられません。ただし、PD を使用してインターネットと接続する場合は、設定の必要はありません。

設定モード

ループバックインタフェース設定モード

sFlow Agent 機能

sFlow Agent 機能

collector address

sFlow データを送信する collector の IP アドレスと UDP の宛先ポート番号を設定します。
※送信元ポート番号は自動で空きポート番号を使います。
local を指定した場合には，装置内部に統計を保持します。
CLI 上は、4 エントリ以上入力できますが、有効になるのは、アドレスの若い順に 2 エントリと local の 1 エントリ、合計 3 エントリ迄です。

refresh コマンド後に有効になるコマンドです。

V01.03(00)以降サポート

設定例 1　collector の IP アドレス:192.168.10.1,宛先ポート番号:UDP6343 に設定する

```
Router(config-sflow-prof)# collector address 192.168.10.1 port 6343
```

コマンド書式

collector address <collector の IP アドレス> [port <ポート番号>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
collector の IP アドレス	collector の IP アドレスを指定します。	IPv4/IPv6 アドレス形式	省略不可
ポート番号	UDP の宛先ポート番号を指定します。	1～65535	6343
local	装置内部にサンプルデータ毎の統計を保持する場合に指定します。	local	省略不可

この設定を行わない場合

sFlow Agent 機能が無効になります。

設定モード

sflow profile 設定モード

max-datagram-size

collector に送信する sflow データの UDP データ部の最大データ長を設定します。

refresh コマンド後に有効になるコマンドです。

V01.03(00)以降サポート

設定例１　送信する sflow データの UDP データ部の最大データ長を 1200byte に設定する

```
Router(config-sflow-prof)# max-datagram-size 1200
```

コマンド書式

max-datagram-size〈最大データ長〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
最大データ長	collector に送信する sflow データの最大データ長（byte）を指定します。	512～1400	省略不可

この設定を行わない場合

1400byte を使用します。

設定モード

sflow profile 設定モード

max-sampled-size

サンプリングするパケットのサイズを設定します。

refresh コマンド後に有効になるコマンドです。

V01.03(00)以降サポート

設定例１　サンプリングするパケットサイズを 100byte に設定する

```
Router(config-sflow-prof)# max-sampled-size 100
```

コマンド書式

max-sampled-size 〈パケットサイズ〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
パケットサイズ	サンプリングするパケットのサイズ(byte)を指定します。	64～256	省略不可

この設定を行わない場合

128byte を使用します。

設定モード

sflow profile 設定モード

sflow polling-interval

カウンタサンプリングのポーリング間隔(秒)を設定します.
ポーリング間隔を 0 秒に設定するとカウンタサンプリングを行いません。

refresh コマンド後に有効になるコマンドです。

V01.03(00)以降サポート

設定例 1　ポーリング間隔を 60 秒に設定する

```
Router(config)#interface lan 1
Router(config-if lan 1)# sflow polling-interval 60
```

コマンド書式

sflow polling-interva <ポーリング間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポーリング間隔	カウンタサンプリングのポーリング間隔(秒)を指定します。	0～86400	省略不可

この設定を行わない場合

ポーリング間隔が 0 秒となり、カウンタサンプリングを行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
USB Ethernet インタフェース設定モード

sflow profile

sFlow Agent 機能を有効にするインタフェースを設定します。

refresh コマンド後に有効になるコマンドです。

V01.03(00)以降サポート

設定例 1　LAN1 にて sFlow Agent 機能を使用する

```
Router(config)#interface lan 1
Router(config-if lan 1)#sflow profile 1
```

コマンド書式

sflow profile <sflow profile 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
sflow profile 番号	sflow profile 番号を指定します。	1～1	省略不可

この設定を行わない場合

sflow agent 機能を使用できません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
USB Ethernet インタフェース設定モード

sflow sampling-rate

フローサンプリングのレートを設定します。
レートを設定しないとフローサンプリングを行いません。
レートによっては中継性能が低下することがあります。

refresh コマンド後に有効になるコマンドです。

V01.03(00)以降サポート

設定例１　フローサンプリングのレートを 10000 に設定する

```
Router(config)#interface lan 1
Router(config-if lan 1)# sflow sampling-rate 10000
```

コマンド書式

sflow sampling-rate <サンプリングレート>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
サンプリングレート	フローサンプリングするレートを指定します。	10～8388608	省略不可

この設定を行わない場合

フローサンプリングを行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
USB Ethernet インタフェース設定モード

sflow-agent address

sFlow Agent の IP アドレスを設定します。

refresh コマンド後に有効になるコマンドです。

V01.03(00)以降サポート

設定例 1　sflow agent の IP アドレスを 10.1.1.1 に設定する

```
Router(config)# sflow-agent address 10.1.1.1
```

コマンド書式

sflow-agent address <sflow-agent の IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
sflow-agent の IP アドレス	sflow agent の IP アドレスを指定します。	IPv4/IPv6 アドレス形式	省略不可

この設定を行わない場合

sFlow Agent 機能が無効になります。

設定モード

基本設定モード

source-interface

sFlow データを送信する送信元アドレスとなるインタフェースを設定します。

refresh コマンド後に有効になるコマンドです。

V01.03(00)以降サポート

設定例１　送信元アドレスに loopback1 インタフェースのアドレスを指定する

```
Router(config-sflow-prof)# source-interface loopback 1
```

コマンド書式

source-interface <インタフェース名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	sFlow データを送信する送信元アドレスとなるインタフェースを指定します。	lan 1 ewan 1～2 vlanif 1～150 loopback 1～100	省略不可

この設定を行わない場合

sFlow データを送信する送信元アドレスは、送信先の collector アドレスを経路表に従い検索し、確定した送信インタフェースのアドレスを使用します。
また、設定したインタフェースにアドレスが設定されていない場合や設定インタフェースが無効な場合には、送信インタフェース設定がされていないものとして動作します。

設定モード

sflow profile 設定モード

その他の機能

CLI の表示に関する機能

alias

よく発行するコマンドや、長くて入力が面倒なコマンドを、alias コマンドで簡単化して登録しておきます。このコマンドは、入力完了した時点で有効になります。

refresh コマンド後に有効になるコマンドです。

設定例 1　show interface lan 1 コマンドの alias 名を、"shlan"とする

```
Router(config)# alias shlan show interface lan 1
```

コマンド書式

alias <alias 名> <コマンド>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
alias 名	コマンドを簡単化する際の名称	-	省略不可
コマンド	簡単化するコマンド	-	255

この設定を行わない場合

コマンドの省略形は使用できません。

設定での注意事項

注意1：本装置のコマンドを alias 名に使用しないでください。
【設定してはいけない例】
alias save save /var/card1a/config/boot.cfg
"save" というコマンド名は本装置のコマンドであるため、このように設定してはいけない。

注意2：すでに設定してある alias のコマンド名を、alias 名に使用しないでください。
【設定してはいけない例】
alias aaa bbb
alias bbb aaa
"bbb" というコマンド名はすでに alias 登録されているため、このように設定してはいけない。

設定モード

基本設定モード

description

各インタフェースに対して、コメントを記述することができます。
記述した内容は show interface で表示されます。

refresh コマンド後に有効になるコマンドです。

設定例１　ダイヤラーインタフェースにコメントを付ける

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#description backup line
```

コマンド書式

description <文字>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
文字	コメントを入力します。	240 文字までの半角英数字、記号	省略不可

設定モード

LAN インタフェース設定モード
PPPoE インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード
ダイヤラーインタフェース設定モード
IPsec インタフェース設定モード
ループバックインタフェース設定モード
トンネルイタフェース設定モード
USB Ethernet インタフェース設定モード

shutdown

設定を残したままでインタフェースを停止させる場合に指定します。

refresh コマンド後に有効になるコマンドです。
（refresh 対応は、モデムインタフェース、ダイヤラーインタフェース、VLAN インタフェースの各設定モードのみです。）

設定例 1　LAN インタフェースを一時的に使用できない状態にする

```
Router(config)#interface lan 1
Router(config-if lan 1)#shutdown
```

コマンド書式

shutdown

パラメータ

パラメータはありません。

この設定を行わない場合

インタフェースが使用可能です。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
モデムインタフェース設定モード
ダイヤラーインタフェース設定モード
VLAN インタフェース設定モード
トンネルイタフェース設定モード

hostname

プロンプトを設定します。
このコマンドは、入力完了した時点で有効になります。

設定例１　プロンプトを"F2200#1"に設定する

```
Router(config)#hostname F2200#1
F2200#1(config)#
```

コマンド書式

hostname <プロンプト文字列>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プロンプト文字列	プロンプトに使用する文字列を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

"Router"となります。

設定モード

基本設定モード

高速化キャッシュ機能

flow-cache ip

パケット中継を、flow キャッシュを用いて高速に実行します。

refresh コマンド後に有効になるコマンドです。

設定例１　flow キャッシュを使用しない

```
Router(config)#flow-cache ip disable
```

コマンド書式

flow-cache ip〈キャッシュ設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キャッシュ設定	flow キャッシュを使用するかどうかの指定をします。 enable　flow キャッシュを有効にする disable　flow キャッシュを無効にする	enable disable	省略不可

この設定を行わない場合

flow キャッシュを使用します。

設定モード

基本設定モード

flow-cache ipv6

IPv6 パケット中継を、flow キャッシュを用いて高速に実行します。

refresh コマンド後に有効になるコマンドです。

設定例１　flow キャッシュを使用しない

```
Router(config)#flow-cache ipv6 disable
```

コマンド書式

flow-cache ipv6 〈キャッシュ設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キャッシュ設定	flow キャッシュを使用するかどうかの指定をします。 enable　flow キャッシュを有効にする disable　flow キャッシュを無効にする	enable disable	省略不可

この設定を行わない場合

flow キャッシュを使用します。

設定モード

基本設定モード

flow-cache l2

L2 パケット中継を flow キャッシュを用いて高速に実行します。

refresh コマンド後に有効になるコマンドです。

設定例 1　flow キャッシュを使用しない

```
Router(config)#flow-cache l2 disable
```

コマンド書式

flow-cache l2 〈キャッシュ設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キャッシュ設定	flow キャッシュを使用するかどうかの指定をします。 enable　flow キャッシュを有効にする disable　flow キャッシュを無効にする	enable disable	省略不可

この設定を行わない場合

flow キャッシュを使用します。

設定モード

基本設定モード

設定内容の削除方法

no

登録した設定内容を削除したい場合は、コマンドの先頭に no を追記することにより、該当する登録内容を削除することができます。

設定例１　設定した登録内容を削除する

```
Router(config)# no access-list 100
```

索引

A

aaa authentication macfilter default group 761
aaa authentication ppp..... 666
aaa enable..... 521
aaa group server radius..... 54
aaa local group..... 52, 667
aaa my-name..... 522
aaa peer-name..... 524
access-list..... 143, 280, 1023
access-list remark..... 1034
action-map..... 36, 170, 343, 862
add ip route..... 825
address..... 815
address-family ipv6 unicast.... 21, 427
address-pool..... 74, 90
address-pool ipv6..... 27, 95
aggregate-address..... 132, 373, 428
alias..... 1051
alive..... 536, 607
allocate address..... 75, 91
allocate prefix-length..... 76, 92
allocate retention-time..... 77, 93
allocate-address..... 715
always-up check-interval..... 538, 609
am-3-encr..... 539
am-3-initcont..... 540
anti-replay..... 486, 575
area authentication..... 253
area default-cost..... 243
area export-list..... 244
area import-list..... 245
area nssa..... 246
area range..... 248
area shortcut..... 249
area stub..... 250
area virtual-link..... 272
area virtual-link authentication... 273
area virtual-link authentication-key 274
area virtual-link dead-interval.... 275
area virtual-link hello-interval... 276
area virtual-link message-digest-key 277
area virtual-link retransmit-interval 278
area virtual-link transmit-delay... 279
authentication..... 449, 559
auto connect..... 902
auto-cost reference-bandwidth..... 267

B

bgp always-compare-med..... 374
bgp bestpath as-path ignore..... 377
bgp bestpath compare-routerid..... 379
bgp bestpath med missing-as-worst .. 375
bgp default ipv4-unicast..... 381
bgp default local-preference..... 385
bgp encap nexthop ipv4..... 382
bgp log-neighbor-changes..... 383
bgp router-id..... 384
bgp scan-time..... 386
BGP4について 372
bridge ip adjust-mss..... 647
bridge-group..... 1017

C

caller..... 903
changeback-time..... 762
check behavior modem..... 796
check fan fail..... 797
check initialization modem..... 798
check insertion modem..... 799
check interface status..... 800
check ip-icmp..... 801
check signal-level..... 802
check signal-quality..... 804
check vrrp status vrid..... 806
check watch-class..... 977
class..... 173, 346, 880
class-map..... 35, 162, 338, 851
clear ipsec-session isakmp-policy .. 827
client authentication password..... 598
client authentication peer-password 599
collector address..... 1043
compatible rfc1583..... 268
configuration application-version message..... 543
configuration application-version push 544
configuration mode..... 541, 560
configuration mode (isakmp polcy) . 508
configuration mode (security-association) 510
console exec-timeout..... 778
cookie size..... 679
crl-optional..... 526, 600

crypto ca identity..... 41, 525
crypto group-security map..... 617
crypto ikev2 policy..... 43
crypto ipsec group-security policy.. 42
crypto ipsec-log..... 47
crypto isakmp policy..... 44
crypto map..... 45, 488, 489, 577, 578
crypto security-association... 46, 545, 610

D

dampening disable..... 807
dampening-parameter..... 808
ddns-client..... 744
ddns-server accept-fqdn type..... 740
ddns-server enable..... 742
ddns-server logging address-changes 743
default-information originate 133, 200, 233
default-metric..... 201, 234
default-router..... 716
description 78, 94, 746, 809, 817, 828, 1040, 1052
dhcp-client retries infinitely..... 69
digest type..... 658
disable..... 904
disconnect modem..... 829
distance..... 202, 235, 387
distance bgp..... 388
distance ospf..... 237
distribute-list..... 134, 204
dns..... 668
dns-server..... 79, 717
dns-server forward dhcp-client..... 80
domain-name..... 718
domain-search-list fixed..... 81
domain-search-list forward dhcp-client 82
drop..... 863

E

email..... 527, 601
e-mail body false-to-true..... 830
e-mail body true-to-false..... 831
e-mail subject..... 832
encryption..... 450, 561
encryption-keysize aes..... 563
event continuation-time..... 810
event match-any..... 811
event-action..... 31
event-class..... 30
event-class event-action..... 849
event-map..... 32, 850
execute usb-reset..... 833

F

fan control..... 986
flow-cache ip..... 1055
flow-cache ipv6..... 1056
flow-cache l2..... 1057
forced disconnect cumulative-time.. 905
forced disconnect packet..... 907
fqdn-list..... 177, 350
fqdn-list lifetime..... 178, 351
fqdn-list query-interval..... 179, 352
ftp-server exec-timeout..... 779
ftp-server shutdown..... 780

G

group..... 452, 564
group-security client..... 618
group-security server..... 619

H

hash..... 453, 565
hello interval..... 660
hidden..... 680
hostname..... 1054
hostname local..... 661
hostname remote..... 662
hosttable..... 719
http-client..... 53

I

icmp-class..... 33, 818
idle-timer receive..... 910
idle-timer send..... 909
idtype-pre..... 455
idtype-rsa..... 456
if-state spoofing-up..... 1001
if-state sync-sa..... 546, 611
igmp-proxy disable-upstream..... 834
igmp-proxy non-querier..... 835
ikealive freq..... 547, 612
ikealive retry max..... 548
ikealive retry timer..... 549
initial-state discard..... 681
interface bvi..... 10
interface dialer..... 15
interface ewan..... 13

interface ipsecif..... 38
interface lan..... 11
interface loopback..... 17
interface modem..... 14
interface pppoe..... 12
interface tunnel..... 40
interface usb-ethernet..... 16
interface vlanif..... 39
internal-bridge..... 648
internal-bridge address-learning... 649
internal-bridge aging-time..... 650
internal-bridge permanent-address.. 651
internal-bridge redundancy default
indicate-selected 652
internal-bridge redundancy default
receive-unselected 653
internal-bridge relay inter-tunnel-
interface 654
internal-bridge tunnel..... 836
interval..... 819, 978
ip access-group.... 291, 758, 912, 1014
ip address 63, 195, 528, 602, 639, 911,
1016, 1041
ip address dhcp..... 70, 197
ip address secondary..... 199
ip address unnumbered..... 641
ip arp 802.1p-priority..... 328
ip arp learning..... 329
ip arp reply..... 330
ip arp request..... 331
ip arp static..... 332
ip arp timeout..... 333
ip as-path access-list..... 390
ip dhcp pool..... 25, 720
ip dhcp relay maxhops..... 727
ip directed-broadcast..... 334
ip domain-name..... 318, 529, 603
ip helper-address..... 728
ip icmp error-ratelimit..... 335
ip igmp access-group..... 353
ip igmp fast-leave..... 354
ip igmp group-membership-timeout... 355
ip igmp last-membership-query-interval
..... 356
ip igmp proxy..... 357
ip igmp proxy non-querier-behavior. 360
ip igmp proxy-group..... 358
ip igmp proxy-group-upstream..... 359
ip igmp querier-timeout..... 361
ip igmp query-interval..... 362
ip igmp query-max-response-time 363
ip igmp source-interface 365
ip igmp static-group 364
ip igmp version 366
ip limited-broadcast ttl 370
ip local pool 669
ip mtu 65, 72, 323
ip multicast ttl-threshold 367
ip multicast-routing proxy 368
ip multi-path max-paths 194, 371
ip name-server 64, 315
ip name-server source-interface 317
ip nat inside destination 703, 919
ip nat inside source 698, 914
ip nat log-table-changes 688
ip nat max-sessions 690
ip nat outside destination 710, 926
ip nat outside source 706, 922
ip nat pool 713
ip nat reserved-sessions 689
ip nat translation finrst-timeout .. 691
ip nat translation icmp-timeout 693
ip nat translation syn-timeout 694
ip nat translation tcp-timeout 695
ip nat translation timeout 696
ip nat translation udp-timeout 697
ip ospf authentication 254
ip ospf authentication-key 255
ip ospf cost 257
ip ospf database-filter all out 258
ip ospf dead-interval 259
ip ospf disable all 260
ip ospf hello-interval 261
ip ospf message-digest-key 256
ip ospf network 262
ip ospf priority 263
ip ospf retransmit-interval 264
ip ospf transmit-delay 265
ip polling-interval 349
ip proxy-arp 327
ip resolver-cache-time 320
ip resolver-retries 322
ip rip authentication key-chain 206
ip rip authentication mode 207
ip rip receive version 209
ip rip send version 210
ip route 294
ip scp server enable 995
ip source-quench 337
ip split-horizon 211

ip stateful max-sessions. 156, 293, 760
ip vpn-nat inside destination..... 463
ip vpn-nat inside source..... 459, 512
ip vpn-nat pool..... 457
ip vrrp enable..... 787
ipsec access-list..... 490, 579
ipsec dynamic-session limit..... 446
ipsec group-security server ha ack-msg-timeout 620
ipsec group-security server ha init-timeout 621
ipsec group-security server ha keepalive-interval 622
ipsec group-security server ha keepalive-timeout 623
ipsec group-security server ha local-address 624
ipsec group-security server ha next-key-sync 625
ipsec group-security server ha rekey-delay-time 626
ipsec group-security server ha request-msg-timeout 627
ipsec group-security server ha send-timeout 628
ipsec group-security server priority 629
ipsec group-security vendor-id..... 630
ipsec transform-keysize..... 582
ipsec transform-set..... 493, 583
ipv6 access-group..... 154, 756
ipv6 address..... 110, 530, 604, 1042
ipv6 address address-pool prefix-length 96
ipv6 address autoconfig..... 112, 114
ipv6 dhcp client..... 97
ipv6 dhcp client-profile..... 28, 98
ipv6 dhcp server..... 83
ipv6 dhcp server-profile..... 84
ipv6 enable..... 113
ipv6 hop-limit..... 115
ipv6 hoplimit-receive-enable..... 116
ipv6 icmp error-ratelimit..... 117
ipv6 mld fast-done..... 180
ipv6 mld group-membership-timeout.. 181
ipv6 mld last-listener-query-interval 182
ipv6 mld limit..... 183
ipv6 mld mode..... 184
ipv6 mld proxy upstream-forwarding. 185
ipv6 mld proxy-group 186
ipv6 mld proxy-group-upstream 187
ipv6 mld querier-timeout 188
ipv6 mld query-interval 189
ipv6 mld query-max-response-time ... 190
ipv6 mld static-group 191
ipv6 mld version 192
ipv6 mtu 66, 73, 159
ipv6 mtu-receive-enable 161
ipv6 multicast-routing proxy 193
ipv6 nd managed-config-flag 118
ipv6 nd ns-interval 119
ipv6 nd other-config-flag 120
ipv6 nd prefix-advertisement 121
ipv6 nd ra-interval 123
ipv6 nd ra-lifetime 124
ipv6 nd reachable-time 125
ipv6 nd receive-ra 126
ipv6 nd rs-delay 127
ipv6 nd rs-times 128
ipv6 nd send-ra 129
ipv6 ns-interval-receive-enable 130
ipv6 polling-interval 176
ipv6 prefix-list 137
ipv6 reachable-time-receive-enable . 131
ipv6 route 157
IPv6 アドレスについて..... 103
isakmp-negotiation 550

K

keepalive 466, 568, 670
keepalive-icmp peer-address ... 468, 570
keepalive-icmp source-interface ... 469, 573
key 470, 571
key <number> accept-lifetime 213
key <number> key-string 217
key <number> send-lifetime 218
key chain 29, 215

L

l2tp profile 50, 663
l2tp pseudowire 51, 682
l2tp-ppp-template 49, 671
lag mode enable 1002
lcp keepalive 929
lcp maxtimes 930
lcp restart 931
lease 722
lifetime 472, 567, 631

line..... 48, 1003
log-adjacency-changes..... 269
logging..... 747
logging enable..... 85
logging event state-change... 812, 820, 837, 979
logging signal-level..... 932
logging signal-quality..... 934
logging-level elog..... 952
logging-level flog..... 954
logging-level slog..... 956
logging-level t log..... 958
logging-level vpnlog..... 960

M

mac access-group..... 766, 1007, 1038
mac access-list..... 763, 1004, 1035
macfilter ignore broadcast..... 767
macfilter ignore multicast..... 768
macfilter logging enable..... 769
macfilter statistics update enable. 770
mail from..... 972
mail server..... 975
mail source-interface..... 976
mail to..... 973
map-type-dynamic..... 496
match address..... 497, 586
match as-path..... 393
match bridge 802.1p priority..... 853
match bridge access-group..... 854
match bridge input-interface..... 855
match bridge vlan-id..... 856
match duration..... 813
match identity..... 587
match interface..... 297
match ip address..... 298
match ip next-hop..... 299
match ip/ipv6 access-group... 164, 340, 857
match ip/ipv6 input-interface 167, 342, 859
match ipv6 address..... 429
match ipv6 next-hop..... 430
match metric..... 300
match policy-flag..... 169, 861
match-any..... 163, 339, 852
max-call..... 935
max-datagram-size..... 1044
max-sampled-size..... 1045
method..... 748
mode..... 498
modem out-strings init..... 937
modem out-strings special-init..... 936
monitor signal-level..... 939
monitor signal-quality..... 940
mss..... 67, 325
my-identity..... 473

N

name server..... 531
nas-ip-address..... 771
nas-port interface-number..... 772
nat-traversal..... 474
negotiation..... 551, 613
negotiation expire-time..... 614
negotiation-mode..... 476
neighbor..... 220, 239
neighbor activate..... 394, 431
neighbor default-originate.... 395, 432
neighbor description..... 396
neighbor distribute-list..... 397, 433
neighbor dont-capability-negotiate. 399
neighbor ebgp-multihop..... 400
neighbor encap default interface... 445
neighbor encap endpoint..... 443
neighbor encap type..... 442
neighbor filter-list..... 401
neighbor interface..... 434
neighbor maximum-prefix..... 402, 435
neighbor next-hop-self..... 403, 436
neighbor override-capability..... 404
neighbor passive..... 405
neighbor password..... 406
neighbor port..... 408
neighbor remote-as..... 409
neighbor route-map..... 410, 437
neighbor route-reflector-client.... 411
neighbor shutdown..... 412
neighbor soft-reconfiguration inbound 413, 438
neighbor strict-capability-match... 414
neighbor timers..... 415
neighbor transparent-as..... 417
neighbor transparent-nexthop..... 418
neighbor update-source..... 419
neighbor version..... 420
neighbor weight..... 421
netbios-name-server..... 723
network..... 138, 221, 232, 423, 439
no 1058

nolog-block-type-discard..... 533, 605
nolog-spi-no-match..... 534, 606
ntp-server enable..... 993
ntp-server stratum..... 994

O

offset-list..... 222
option forward dhcp-client..... 87
option hex..... 86, 724
option-request dns-servers..... 99
option-request prefix-delegation... 100
ospf abr-type..... 251

P

passive-interface..... 223, 266
peer-identity..... 477
peer-identity distinguished-name... 479
physical-layer..... 941
policy-map..... 37, 174, 347, 881
pool..... 672
pooled-route..... 88, 102
ppp accept template..... 673
ppp account..... 942
ppp authentication..... 674
pppoe account..... 56
pppoe auth-accept..... 57
pppoe interface..... 58
pppoe ncp..... 59
pppoe server..... 60
pppoe service..... 61
pppoe type..... 62
prefix-delegation address-pool..... 89
priority 802.1p classification..... 893
priority 802.1p default-classification
..... 894
priority 802.1p threshold..... 895
priority port-priority..... 897
probe..... 821
protocol..... 664
proxydns default cache-time..... 735
proxydns default domain-name..... 730
proxydns default name-server..... 731
proxydns default retrans-time..... 733
proxydns default retry..... 734
proxydns default source-interface.. 736
proxydns domain..... 738
proxydns hosts..... 739
proxydns mode..... 737
pw-type..... 655

Q

qos frame-length-offset..... 883
qos output bandwidth..... 885
qos-que cbq..... 886
qos-que priq..... 889
query-ip..... 532

R

redistribute... 139, 224, 240, 424, 440
re-establish-sa rekey..... 480, 552
reference-interface..... 750
refresh timer..... 270
release security-association..... 481
release session addr-changed..... 482
remote-access limitation..... 753
remote-access time..... 755
remote-end-id ascii..... 683
request-timeout..... 751
reset modem..... 838
reset system..... 839
retransmit..... 773
retransmit retries..... 665
retry..... 553, 615
retry guard-time..... 554, 616
retry rekey-ipsec..... 555
retry rekey-ipsec negotiation..... 556
reverse-path-check enable..... 633
rollover..... 634
route..... 140, 226
route-map..... 23, 301
Router Advertisement (RA) について. 106
router bgp..... 20, 426
router ospf..... 19
router rip..... 18, 227
router ripng..... 22, 141
router-id..... 231
router-id local..... 684
router-id remote..... 685

S

sa-up route..... 520
search-address..... 725
select-port..... 1008
self-identity..... 574
send e-mail..... 841
send snmp-trap..... 842
sequencing both..... 686
server-private..... 774
service dhcp-relayagent..... 729

service dhcp-server..... 726
service-policy..... 891
service-policy local..... 892
set 802.1p priority..... 879
set aggregator..... 303
set as-path prepend..... 304
set atomic-aggregate..... 305
set community..... 306
set community-additive..... 307
set encap ip dscp..... 864
set encap ip prec..... 865
set encap ip tos..... 866
set encap ipv6 dscp..... 867
set encap ipv6 traffic-class..... 868
set ikev2-policy..... 588
set ip dscp..... 869
set ip next-hop..... 308, 344, 870
set ip prec..... 872
set ip tos..... 873
set ipsec-status discard isakmp-policy
..... 843
set ipv6 dscp..... 874
set ipv6 next-hop..... 171, 441, 875
set ipv6 traffic-class..... 877
set l2tp-status discard tunnel..... 844
set local-preference..... 309
set metric..... 310
set origin..... 311
set originator-id..... 312
set peer..... 499, 589
set pfs..... 501, 590
set policy-flag..... 845
set profile..... 687
set queuing..... 878
set security-association always-up 502,
592
set security-association ipsec-src-id
..... 503
set security-association lifetime. 505,
593
set security-association selector
bypass 369, 595
set session release ipsec-lost-time 591
set tag..... 313
set transform-keysize..... 596, 635
set transform-set..... 507, 597, 636
set weight..... 314
sflow polling-interval..... 1046
sflow profile..... 55, 1047
sflow sampling-rate..... 1048
sflow-agent address..... 1049
shutdown..... 1009, 1053
shutdown port..... 846
size..... 822
snmp-server community..... 945
snmp-server contact..... 946
snmp-server enable traps..... 947
snmp-server host..... 948
snmp-server location..... 949
snmp-server name..... 950
snmp-server source-interface..... 951
sntp retry..... 987
sntp schedule..... 989
sntp server..... 991
sntp source-interface..... 992
source-address..... 776
source-interface..... 483, 752, 1050
speed-duplex..... 1010
spi mask hex..... 637
ssh-server access-group..... 996
ssh-server enable..... 997
ssh-server exec-timeout..... 998
ssh-server port..... 999
ssh-server response-timeout..... 1000
statistics update..... 175, 348, 882
summary-address..... 242
suspend icmp-class..... 847
sw 1011
syslog facility..... 962
syslog file..... 964
syslog format bsd..... 966
syslog level..... 967
syslog sending..... 969
syslog server..... 970
syslog source-interface..... 971

T

tagging never..... 656, 1018
target..... 980
telnet-server exec-timeout..... 781
telnet-server shutdown..... 782
threshold..... 982
timeout(ICMP-CLASS)..... 823
timeout (RADIUS) 777
timers basic..... 142, 228
timers spf..... 271
times..... 984
trial..... 824
tunnel destination..... 642
tunnel mode..... 643, 645

tunnel protection..... 675
tunnel source..... 644
tunnel-route..... 484, 516, 518

U

unicastrip..... 230
upnp-server access-group..... 899
upnp-server enable..... 900
upnp-server target-interface..... 901
usb ethernet-monitor..... 943
usb mode-switch..... 944
username..... 676
username interface tunnel..... 678

V

version..... 229
vlan bridge-group..... 1019
vlan egress-tagging null-tag..... 1020
vlan lag-group..... 1013
vlan port-vlan..... 1022
vlan-id..... 657, 1021
vpn enable..... 447, 557
vpnlog enable..... 448, 558
vpnlog-detail..... 535
vrrp..... 848
vrrp address..... 788
vrrp adver-interval..... 790
vrrp auth-type..... 791
vrrp preempt..... 793
vrrp priority..... 795
VRRP のしくみ 784
VRRP 機能について..... 783

W

watch-class..... 34, 985

こ

コマンドの基本操作..... 8
コマンド形式の見方..... 7
コマンド操作の手順..... 8

漢字

基本設定ユーザモードへの移行..... 9
使用可能文字について..... 7
特権ユーザモードへの移行..... 9

refresh 対応コマンド索引

A

aaa authentication macfilter default group 761
aaa authentication ppp..... 666
aaa enable..... 521
aaa group server radius..... 54
aaa local group..... 52, 667
aaa my-name..... 522
aaa peer-name..... 524
access-list..... 143, 280, 1023
access-list remark..... 1034
add ip route..... 825
address..... 815
address-pool..... 74, 90
aggregate-address..... 132, 373, 428
alias..... 1051
allocate address..... 75, 91
allocate prefix-length..... 76, 92
allocate retention-time..... 77, 93
anti-replay..... 486, 575
area authentication..... 253
area default-cost..... 243
area export-list..... 244
area import-list..... 245
area nssa..... 246
area range..... 248
area shortcut..... 249
area stub..... 250
area virtual-link..... 272
area virtual-link authentication... 273
area virtual-link authentication-key 274
area virtual-link dead-interval.... 275
area virtual-link hello-interval... 276
area virtual-link message-digest-key 277
area virtual-link retransmit-interval 278
area virtual-link transmit-delay... 279
authentication..... 449, 559
auto connect..... 902
auto-cost reference-bandwidth..... 267

B

bgp always-compare-med..... 374
bgp bestpath as-path ignore..... 377
bgp bestpath compare-routerid..... 379
bgp bestpath med missing-as-worst .. 375
bgp default ipv4-unicast..... 381
bgp default local-preference..... 385
bgp encap nexthop ipv4..... 382
bgp log-neighbor-changes..... 383
bgp router-id..... 384
bgp scan-time..... 386
bridge ip adjust-mss..... 647

C

caller..... 903
changeback-time..... 762
check behavior modem..... 796
check fan fail..... 797
check initialization modem..... 798
check insertion modem..... 799
check interface status..... 800
check ip-icmp..... 801
check signal-level..... 802
check signal-quality..... 804
check vrrp status vrid..... 806
check watch-class..... 977
class..... 173, 346, 880
clear ipsec-session isakmp-policy .. 827
client authentication password..... 598
client authentication peer-password 599
collector address..... 1043
compatible rfc1583..... 268
configuration application-version message..... 543
configuration application-version push 544
configuration mode..... 541, 560
configuration mode (isakmp polcy) . 508
configuration mode (security-association) 510
cookie size..... 679
crypto map..... 489, 578

D

dampening disable..... 807
dampening-parameter..... 808
ddns-client..... 744
ddns-server accept-fqdn type..... 740
ddns-server enable..... 742
ddns-server logging address-changes 743
default-information originate 133, 200, 233

default-metric..... 201, 234
description 78, 94, 746, 809, 817, 828, 1040, 1052
dhcp-client retries infinitely..... 69
digest type..... 658
disable..... 904
disconnect modem..... 829
distance..... 202, 235, 387
distance bgp..... 388
distance ospf..... 237
distribute-list..... 134, 204
dns..... 668
dns-server..... 79
dns-server forward dhcp-client..... 80
domain-search-list fixed..... 81
domain-search-list forward dhcp-client 82
drop..... 863

E

e-mail body false-to-true..... 830
e-mail body true-to-false..... 831
e-mail subject..... 832
encryption..... 450, 561
encryption-keysize aes..... 563
event continuation-time..... 810
event match-any..... 811
event-class event-action..... 849
execute usb-reset..... 833

F

fan control..... 986
flow-cache ip..... 1055
flow-cache ipv6..... 1056
flow-cache l2..... 1057
forced disconnect cumulative-time.. 905
forced disconnect packet..... 907
fqdn-list..... 177, 350
fqdn-list lifetime..... 178, 351
fqdn-list query-interval..... 179, 352

G

group..... 452, 564
group-security server..... 619

H

hash..... 453, 565
hello interval..... 660
hidden..... 680
hostname local..... 661
hostname remote..... 662

I

idle-timer receive..... 910
idle-timer send..... 909
idtype-pre..... 455
idtype-rsa..... 456
if-state spoofing-up..... 1001
if-state sync-sa..... 546, 611
igmp-proxy disable-upstream..... 834
igmp-proxy non-querier..... 835
initial-state discard..... 681
internal-bridge address-learning... 649
internal-bridge aging-time..... 650
internal-bridge permanent-address.. 651
internal-bridge redundancy default indicate-selected..... 652
internal-bridge redundancy default receive-unselected..... 653
internal-bridge relay inter-tunnel-interface..... 654
internal-bridge tunnel..... 836
interval..... 819, 978
ip access-group.... 291, 758, 912, 1014
ip address..... 195, 639, 911
ip arp 802.1p-priority..... 328
ip arp learning..... 329
ip arp reply..... 330
ip arp request..... 331
ip arp static..... 332
ip arp timeout..... 333
ip as-path access-list..... 390
ip directed-broadcast..... 334
ip icmp error-ratelimit..... 335
ip igmp access-group..... 353
ip igmp fast-leave..... 354
ip igmp group-membership-timeout... 355
ip igmp last-membership-query-interval 356
ip igmp proxy..... 357
ip igmp proxy non-querier-behavior. 360
ip igmp proxy-group..... 358
ip igmp proxy-group-upstream..... 359
ip igmp querier-timeout..... 361
ip igmp query-interval..... 362
ip igmp query-max-response-time.... 363
ip igmp source-interface..... 365
ip igmp static-group..... 364
ip igmp version..... 366
ip limited-broadcast ttl..... 370

ip local pool..... 669
ip mtu..... 65, 72, 323
ip multicast ttl-threshold..... 367
ip multicast-routing proxy..... 368
ip multi-path max-paths..... 194, 371
ip nat inside destination..... 703, 919
ip nat inside source..... 698, 914
ip nat log-table-changes..... 688
ip nat outside destination.... 710, 926
ip nat outside source..... 706, 922
ip nat pool..... 713
ip nat reserved-sessions..... 689
ip ospf authentication..... 254
ip ospf authentication-key..... 255
ip ospf cost..... 257
ip ospf database-filter all out.... 258
ip ospf dead-interval..... 259
ip ospf disable all..... 260
ip ospf hello-interval..... 261
ip ospf message-digest-key..... 256
ip ospf network..... 262
ip ospf priority..... 263
ip ospf retransmit-interval..... 264
ip ospf transmit-delay..... 265
ip polling-interval..... 349
ip proxy-arp..... 327
ip rip authentication key-chain.... 206
ip rip authentication mode..... 207
ip rip receive version..... 209
ip rip send version..... 210
ip route..... 294
ip scp server enable..... 995
ip source-quench..... 337
ip split-horizon..... 211
ip vpn-nat inside destination..... 463
ip vpn-nat inside source..... 459, 512
ip vpn-nat pool..... 457
ip vrrp enable..... 787
ipsec access-list..... 490, 579
ipsec dynamic-session limit..... 446
ipsec group-security server ha ack-msg-timeout 620
ipsec group-security server ha init-timeout 621
ipsec group-security server ha keepalive-interval 622
ipsec group-security server ha keepalive-timeout 623
ipsec group-security server ha local-address 624
ipsec group-security server ha rekey-delay-time..... 626
ipsec group-security server ha request-msg-timeout..... 627
ipsec group-security server ha send-timeout..... 628
ipsec group-security server priority 629
ipsec group-security vendor-id 630
ipsec transform-keysize 582
ipsec transform-set 493, 583
ipv6 access-group 154, 756
ipv6 address address-pool prefix-length..... 96
ipv6 dhcp client 97
ipv6 dhcp server 83
ipv6 icmp error-ratelimit 117
ipv6 mld fast-done 180
ipv6 mld group-membership-timeout .. 181
ipv6 mld last-listener-query-interval 182
ipv6 mld limit 183
ipv6 mld mode 184
ipv6 mld proxy upstream-forwarding . 185
ipv6 mld proxy-group 186
ipv6 mld proxy-group-upstream 187
ipv6 mld querier-timeout 188
ipv6 mld query-interval 189
ipv6 mld query-max-response-time ... 190
ipv6 mld static-group 191
ipv6 mld version 192
ipv6 mtu 66, 73, 159
ipv6 multicast-routing proxy 193
ipv6 polling-interval 176
ipv6 prefix-list 137
ipv6 route 157

K

keepalive 466, 568, 670
keepalive-icmp peer-address ... 468, 570
keepalive-icmp source-interface ... 469, 573
key 470, 571
key <number> accept-lifetime 213
key <number> key-string 217
key <number> send-lifetime 218

L

l2tp profile 663
l2tp pseudowire 682

l2tp-ppp-template..... 49, 671
lag mode enable..... 1002
lcp keepalive..... 929
lcp maxtimes..... 930
lcp restart..... 931
lifetime..... 472, 567, 631
line..... 1003
log-adjacency-changes..... 269
logging..... 747
logging enable..... 85
logging event state-change... 812, 820, 837, 979
logging signal-level..... 932
logging signal-quality..... 934
logging-level elog..... 952
logging-level flog..... 954
logging-level slog..... 956
logging-level t log..... 958
logging-level vpnlog..... 960

M

mac access-group..... 766, 1007, 1038
mac access-list..... 763, 1004, 1035
macfilter ignore broadcast..... 767
macfilter ignore multicast..... 768
macfilter logging enable..... 769
macfilter statistics update enable. 770
map-type-dynamic..... 496
match address..... 497, 586
match as-path..... 393
match bridge 802.1p priority..... 853
match bridge access-group..... 854
match bridge input-interface..... 855
match bridge vlan-id..... 856
match duration..... 813
match identity..... 587
match interface..... 297
match ip address..... 298
match ip next-hop..... 299
match ip/ipv6 access-group... 164, 340, 857
match ip/ipv6 input-interface 167, 342, 859
match ipv6 address..... 429
match ipv6 next-hop..... 430
match metric..... 300
match policy-flag..... 169, 861
match-any..... 163, 339, 852
max-call..... 935
max-datagram-size..... 1044
max-sampled-size..... 1045
method..... 748
mode..... 498
modem out-strings init..... 937
modem out-strings special-init..... 936
monitor signal-level..... 939
monitor signal-quality..... 940
mss..... 67, 325
my-identity..... 473

N

nas-ip-address..... 771
nas-port interface-number..... 772
negotiation-mode..... 476
neighbor..... 220, 239
neighbor activate..... 394, 431
neighbor default-originate.... 395, 432
neighbor description..... 396
neighbor distribute-list..... 397, 433
neighbor dont-capability-negotiate . 399
neighbor ebgp-multihop..... 400
neighbor encap default interface... 445
neighbor encap endpoint..... 443
neighbor encap type..... 442
neighbor filter-list..... 401
neighbor interface..... 434
neighbor maximum-prefix..... 402, 435
neighbor next-hop-self..... 403, 436
neighbor override-capability..... 404
neighbor passive..... 405
neighbor password..... 406
neighbor port..... 408
neighbor remote-as..... 409
neighbor route-map..... 410, 437
neighbor route-reflector-client.... 411
neighbor shutdown..... 412
neighbor soft-reconfiguration inbound 413, 438
neighbor strict-capability-match... 414
neighbor timers..... 415
neighbor transparent-as..... 417
neighbor transparent-nexthop..... 418
neighbor update-source..... 419
neighbor version..... 420
neighbor weight..... 421
network..... 138, 221, 232, 423, 439
nolog-block-type-discard..... 533, 605
nolog-spi-no-match..... 534, 606
ntp-server enable..... 993
ntp-server stratum..... 994

O

offset-list..... 222
option forward dhcp-client..... 87
option hex..... 86
option-request dns-servers..... 99
option-request prefix-delegation... 100
ospf abr-type..... 251

P

passive-interface..... 223, 266
peer-identity..... 477
peer-identity distinguished-name... 479
physical-layer..... 941
pool..... 672
pooled-route..... 88, 102
ppp accept template..... 673
ppp account..... 942
ppp authentication..... 674
prefix-delegation address-pool..... 89
priority 802.1p classification..... 893
priority 802.1p default-classification
..... 894
priority 802.1p threshold..... 895
priority port-priority..... 897
probe..... 821
protocol..... 664

Q

qos frame-length-offset..... 883
qos output bandwidth..... 885
qos-que cbq..... 886
qos-que priq..... 889

R

redistribute... 139, 224, 240, 424, 440
re-establish-sa rekey..... 480, 552
reference-interface..... 750
refresh timer..... 270
release security-association.. 481, 482
remote-end-id ascii..... 683
request-timeout..... 751
reset modem..... 838
reset system..... 839
retransmit..... 773
retransmit retries..... 665
reverse-path-check enable..... 633
rollover..... 634
route..... 140, 226
router-id..... 231
router-id local..... 684
router-id remote..... 685

S

sa-up route..... 520
select-port..... 1008
self-identity..... 574
send e-mail..... 841
send snmp-trap..... 842
sequencing both..... 686
server-private..... 774
service-policy..... 891
service-policy local..... 892
set 802.1p priority..... 879
set aggregator..... 303
set as-path prepend..... 304
set atomic-aggregate..... 305
set community..... 306
set community-additive..... 307
set encap ip dscp..... 864
set encap ip prec..... 865
set encap ip tos..... 866
set encap ipv6 dscp..... 867
set encap ipv6 traffic-class..... 868
set ikev2-policy..... 588
set ip dscp..... 869
set ip next-hop..... 308, 344, 870
set ip prec..... 872
set ip tos..... 873
set ipsec-status discard isakmp-policy
..... 843
set ipv6 dscp..... 874
set ipv6 next-hop..... 171, 441, 875
set ipv6 traffic-class..... 877
set l2tp-status discard tunnel..... 844
set local-preference..... 309
set metric..... 310
set origin..... 311
set originator-id..... 312
set peer..... 499, 589
set pfs..... 501, 590
set policy-flag..... 845
set profile..... 687
set queuing..... 878
set security-association always-up 502,
592
set security-association ipsec-src-id
..... 503
set security-association lifetime . 505,
593

set security-association selector
bypass 369, 595
set session release ipsec-lost-time 591
set tag..... 313
set transform-keysize..... 596, 635
set transform-set..... 507, 597, 636
set weight..... 314
sflow polling-interval..... 1046
sflow profile..... 55, 1047
sflow sampling-rate..... 1048
sflow-agent address..... 1049
shutdown..... 1009, 1053
shutdown port..... 846
size..... 822
sntp retry..... 987
sntp schedule..... 989
sntp server..... 991
sntp source-interface..... 992
source-address..... 776
source-interface..... 483, 752, 1050
speed-duplex..... 1010
spi mask hex..... 637
ssh-server access-group..... 996
ssh-server enable..... 997
ssh-server exec-timeout..... 998
ssh-server port..... 999
ssh-server response-timeout..... 1000
statistics update..... 175, 348, 882
summary-address..... 242
suspend icmp-class..... 847
sw 1011
syslog facility..... 962
syslog file..... 964
syslog format bsd..... 966
syslog level..... 967
syslog sending..... 969
syslog server..... 970
syslog source-interface..... 971

T

target..... 980
threshold..... 982
timeout(ICMP-CLASS) 823
timeout (RADIUS) 777
timers basic..... 142, 228
timers spf..... 271
times..... 984
trial..... 824
tunnel protection..... 675
tunnel-route..... 484, 518

U

unicastrip..... 230
upnp-server access-group..... 899
upnp-server enable..... 900
upnp-server target-interface..... 901
usb ethernet-monitor..... 943
usb mode-switch..... 944
username..... 676
username interface tunnel..... 678

V

version..... 229
vlan lag-group..... 1013
vlan-id..... 657
vpn enable..... 447, 557
vpnlog enable..... 448, 558
vpnlog-detail..... 535
vrrp..... 848
vrrp address..... 788
vrrp adver-interval..... 790
vrrp auth-type..... 791
vrrp preempt..... 793
vrrp priority..... 795

- 本書は改善のため事前連絡なしに変更することがあります。
- 本書に記載されたデータの使用に起因する第三者の特許権その他の権利について、
  弊社はその責を負いません。
- 無断転載を禁じます。
- Copyright© 2014-2021 FURUKAWA ELECTRIC CO., LTD. All rights reserved.

発行責任：古河電気工業株式会社
130-B0462-AH01-H
2021.3