IP

概要・基本設定

IP（Internet Protocol）の基本設定について説明します。
本製品のご購入直後は、デフォルトユーザー「manager」の登録情報以外、まったく設定が行われていない状態になっています。本製品を IP ルーターとして使用するためには、物理層、データリンク層の設定を行い、その上に少なくとも 2 つの IP インターフェースを作成する必要があります。また、IP モジュールを有効にする必要があります。
以下、そのための基本設定について説明します。

IP ホストとしての基本設定

ここでは、ルーターとしての設定を説明する前に、LAN 上の別のコンピューターから Telnet でログインできるよう、LAN 側インターフェースに IP アドレスを割り当てる方法について説明します。
IP アドレス（IP インターフェース）が 1 つしかない状態では、IP パケットを転送することができないためルーターとしては機能しませんが、IP パケットを送受信する IP ホストとしては機能します。
たとえば、他のコンピューターから Telnet でログインしたり、本製品から他のコンピューターに Telnet したり、PING コマンド（319 ページ）を実行したり、TFTP を使ってファイルをダウンロード、アップロードしたりすることができます。

1. コンソールターミナルからログインします。
2. IP モジュールを有効にします。

   ```
   ENABLE IP ↵
   ```

3. LAN 側インターフェースに IP アドレスを設定します。LAN に接続されているインターフェースを指定してください。ここでは、vlan1 が LAN に接続されていると仮定します。

   ```
   ADD IP INT=vlan1 IP=192.168.10.1 MASK=255.255.255.0 ↵
   ```

以上で設定は完了です。

■ 別サブネットからもアクセスしたい場合は経路の設定が必要になります。たとえば、192.168.20.0/24 への経路を設定するには次のようにします。

```
ADD IP ROUTE=192.168.20.0 MASK=255.255.255.0 INT=vlan1
  NEXTHOP=192.168.10.254 ↵
```

あるいは、デフォルト経路を設定するには次のようにします。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=vlan1 NEXTHOP=192.168.10.254 ↵
```

■ IP モジュールの全般的な情報は SHOW IP コマンド（429 ページ）で確認します。

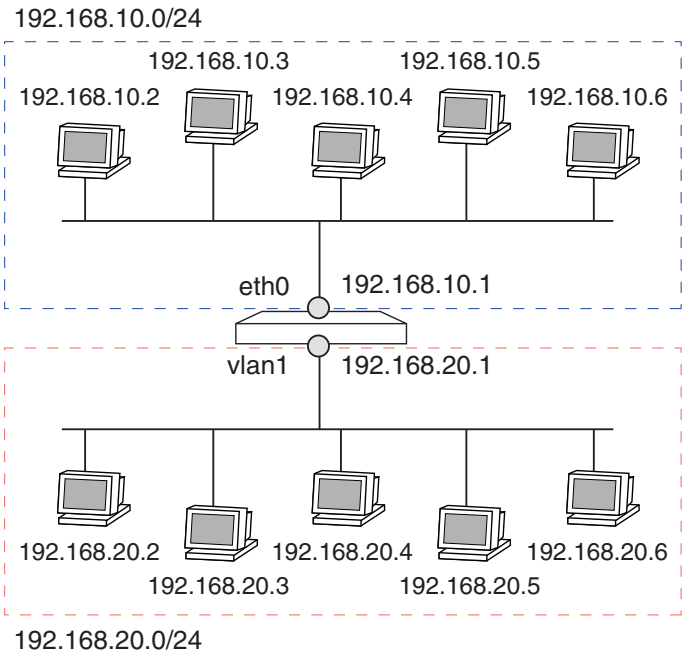
■ インターフェースに割り当てられた IP アドレスの情報は SHOW IP INTERFACE コマンド（458 ページ）で確認します。

■ 経路情報は SHOW IP ROUTE コマンド（473 ページ）で確認します。

IP ルーターとしての基本設定

IP のルーティング機能を利用するには、少なくとも 2 つの IP インターフェースが必要です。そのためには、データリンク層インターフェース（vlan、eth、ppp）をセットアップし、IP アドレスを割り当てる必要があります。

ここでは、次のような構成のネットワークを例に、eth0、vlan1 間で IP パケットをルーティングするための設定を示します。



1. IP モジュールを有効にします。

   ```
   ENABLE IP ↵
   ```

2. 2 つのインターフェースに IP アドレスを割り当てます。

   ```
   ADD IP INT=eth0 IP=192.168.10.1 MASK=255.255.255.0 ↵
   ADD IP INT=vlan1 IP=192.168.20.1 MASK=255.255.255.0 ↵
   ```

設定は以上です。IP インターフェースを複数作成した時点で IP ルーティングが有効になります。

■ 外部への経路は ADD IP ROUTE コマンド（189 ページ）で追加します。たとえば、vlan1 側にサブネット 192.168.30.0/24 への経路が存在する場合は次のように設定します。

```
ADD IP ROUTE=192.168.30.0 MASK=255.255.255.0 INT=vlan1
  NEXTHOP=192.168.20.254 ↵
```

■ デフォルト経路を設定するには、ROUTE、MASK パラメーターに 0.0.0.0 を指定します（この場合 MASK は省略可能です）。INTERFACE パラメーターにはデフォルトゲートウェイ（ルーター）のあるネットワー

クに直接接続されたインターフェースを、NEXTHOP にはデフォルトゲートウェイの IP アドレスを指定します。たとえば、eth0 側にデフォルトゲートウェイ 192.168.10.32 がある場合は次のように設定します。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=eth0 NEXTHOP=192.168.10.32 ↵
```

■ IP モジュールの全般的な情報は SHOW IP コマンド（429 ページ）で確認します。

■ インターフェースに割り当てられた IP アドレスの情報は SHOW IP INTERFACE コマンド（458 ページ）で確認します。

■ 経路情報は SHOW IP ROUTE コマンド（473 ページ）で確認します。

デバッグ用コマンド

IP のデバッグ用には、以下のコマンドが用意されています。

- PING コマンド（319 ページ）：指定した IP ノードに到達できるかどうかを調べます。

```
Manager > ping 172.16.28.32

Echo reply 1 from 172.16.28.32 time delay 8 ms

Echo reply 2 from 172.16.28.32 time delay 5 ms

Echo reply 3 from 172.16.28.32 time delay 5 ms

Echo reply 4 from 172.16.28.32 time delay 5 ms

Echo reply 5 from 172.16.28.32 time delay 5 ms
```

- TRACE コマンド（527 ページ）（Traceroute）：指定した IP ノードまでの経路（経由するルーター）を調べます。

```
Manager > trace 172.16.60.32

Trace from 172.16.28.160 to 172.16.60.32, 1-30 hops
 0. 172.16.28.1          2      2      3 (ms)
 1. 172.16.31.32         5      6      7 (ms)
 2. 172.16.16.1          8      8      8 (ms)
 3. 172.16.48.254        7      7      8 (ms)
 4. 172.16.60.32         7      8      9 (ms)
***
Target reached
```

IP インターフェース

IP インターフェースは、IP パケットの送受信を行うためのインターフェースです。IP モジュールを有効にし、IP インターフェースを複数作成した時点で IP パケットの転送（ルーティング）が行われるようになります。
IP インターフェースは、ADD IP INTERFACE コマンド（179 ページ）でデータリンク層インターフェース（eth、vlan、ppp）に IP アドレス（とネットマスク）を割り当てることによって作成します。

データリンク層インターフェースのセットアップ

IP に限りませんが、ネットワーク層プロトコルの設定時には下位のデータリンク層インターフェースを指定する場面が数多くあります。
IP アドレスを割り当てることのできるデータリンク層インターフェースには次の種類があります。

- Ethernet インターフェース（eth）
- VLAN インターフェース（vlan）
- PPP インターフェース（ppp）

データリンク層インターフェースのセットアップ手順については「インターフェース」、「PPP」の各章をご覧ください。

IP インターフェースの作成・削除

■ IP インターフェースを作成するには ADD IP INTERFACE コマンド（179 ページ）を使って、データリンク層インターフェースに IP アドレスとネットマスクを割り当てます。ネットマスク省略時は、指定した IP アドレスのクラス標準マスクが使用されます。

```
ADD IP INT=vlan1 IP=192.168.100.1 MASK=255.255.255.0 ↵
```

✎ 複数のインターフェースに対し、同一サブネットの IP アドレスを割り当てることはできません。たとえば、vlan1 に IP アドレス 192.168.100.1、ネットマスク 255.255.255.0 を割り当てた場合、192.168.100.2〜192.168.100.254 の範囲は同一 IP サブネットになるので、この範囲を他のインターフェースに割り当てることはできません。

■ IP インターフェースの設定を変更するには SET IP INTERFACE コマンド（364 ページ）を使います。

```
SET IP INT=vlan1 IP=192.168.100.20 MASK=255.255.255.0 ↵
```

■ IP インターフェースを削除するには DELETE IP INTERFACE コマンド（233 ページ）を使います。

```
DELETE IP INT=vlan1 ↵
```

■ 割り当てられた IP アドレスなど、IP インターフェースの情報は SHOW IP INTERFACE コマンド（458 ページ）で確認できます。

```
SHOW IP INTERFACE ↵
```

■ IP インターフェース名は、下位のデータリンク層インターフェースと同じ名前（ADD IP INTERFACE コマンド（179 ページ）で指定した名前）になります（eth0、vlan1、ppp0 など）。

Unnumbered IP インターフェース

PPP による 2 点間接続時には、IP アドレスを持たない Unnumbered（無番号）インターフェースを使用することもできます。Unnumbered IP インターフェースを使用するには、ADD IP INTERFACE コマンド（179 ページ）の IP パラメーターに 0.0.0.0 を指定します。

```
ADD IP INT=ppp0 IP=0.0.0.0 ↵
```

PPP（IPCP）による IP アドレス自動設定

PPP インターフェースでは、IPCP ネゴシエーション時に相手側から IP アドレスの割り当てを受けることができます。

1. PPP インターフェースの作成時に IPREQUEST=ON を指定します。

   ```
   CREATE PPP=0 OVER=eth0-any IDLE=ON LQR=OFF BAP=OFF USERNAME=isp
     PASSWORD=isppasswd IPREQUEST=ON ↵
   ```

2. IP アドレスの動的設定機能を有効にします。

   ```
   ENABLE IP REMOTEASSIGN ↵
   ```

   ✎ ENABLE IP REMOTEASSIGN コマンド（308 ページ）の実行を忘れると、PPP の接続先からアドレスの割り当てを受けつけません。PPP インターフェースへのアドレス割り当てがうまくいかない場合は、SHOW IP コマンド（429 ページ）を実行して、「Remote IP address assignment」が Enabled になっているかどうかを確認してください。Disabled のときは ENABLE IP REMOTEASSIGN を実行し、その後該当する IP インターフェースを DELETE IP INTERFACE コマンド（233 ページ）でいったん削除し、再度作成してください。

3. IP インターフェースを作成します。このとき、IP パラメーターに 0.0.0.0 を指定します。これは、PPP の接続が確立するまで IP アドレスが未決定であることを示します。

   ```
   ADD IP INT=ppp0 IP=0.0.0.0 ↵
   ```

■ CREATE PPP コマンド（「PPP」の 19 ページ）、SET PPP コマンド（「PPP」の 41 ページ）の IPREQUEST パラメーターは、IPCP のネゴシエーションで相手にアドレスを要求するかどうかを指定するパラメーターです。

■ ENABLE IP REMOTEASSIGN コマンド（308 ページ）は、IPCP で相手から与えられたアドレスを自インターフェースに設定するかどうかを制御するコマンドです。

■ PPP 接続時には、IPCP ネゴシエーションによって、IP アドレスに加え、DNS サーバーアドレス（2 個まで）の情報も取得・自動設定できます。

■ IPCP ネゴシエーションで割り当てられた IP アドレス、DNS サーバーアドレスは、SHOW PPP CONFIG コマンド（「PPP」の 50 ページ）で確認できます（自分が採用した値は「Negotiated/Local」セクションに表示されます）。

■ インターフェースに設定された IP アドレスは、SHOW IP INTERFACE コマンド（458 ページ）で確認します。

■ デフォルト経路は SHOW IP ROUTE コマンド（473 ページ）で確認します。「Destination」が 0.0.0.0 のエントリーがデフォルト経路です。

■ DNS サーバーアドレスの設定状況は、SHOW IP コマンド（429 ページ）で確認します。「Primary Name Server」、「Secondary Name Server」欄をご覧ください。

DHCP による IP アドレス自動設定

ネットワーク上の DHCP サーバーを利用して、Ethernet および VLAN インターフェースの IP アドレスを自動設定することもできます（DHCP クライアント機能）。

✎ 本製品は DHCP サーバーとして、クライアントに IP アドレスや IP パラメーターを割り当てることもできます。ここで説明しているのは、本製品が DHCP クライアントとして別の DHCP サーバーからアドレスをもらうための設定です。

1. IP アドレスの動的設定機能を有効にします。DHCP クライアント機能を使うときは、必ず最初に動的設定を有効にしてください。

   ```
   ENABLE IP REMOTEASSIGN ↵
   ```

   ✎ ENABLE IP REMOTEASSIGN コマンド（308 ページ）の実行を忘れると、DHCP サーバーからアドレスの割り当てを受けても、インターフェースにはアドレスが設定されません。SHOW DHCP コマンド（「DHCP サーバー」の 32 ページ）では IP アドレスを取得したと表示されるにもかかわらず、SHOW IP INTERFACE コマンド（458 ページ）では IP アドレスが「0.0.0.0」のままといった場合は、SHOW IP コマンド（429 ページ）を実行して、「Remote IP address assignment」が Enabled になっているかどうかを確認してください。Disabled のときは ENABLE IP REMOTEASSIGN を実行し、その後該当する IP インターフェースを DELETE IP INTERFACE コマンド（233 ページ）でいったん削除し、再度 DHCP を指定してください。

2. IP インターフェースを作成します。このとき、IPADDRESS パラメーターに DHCP を指定します。

   ```
   ADD IP INT=eth0 IP=DHCP ↵
   ```

■ DHCP で IP アドレスを配布するインターネットサービスプロバイダー（ISP）をご利用の場合、接続認証用の「コンピューター名」を指定されることがあります。その場合は、DHCP クライアント機能の設定に先立ち、SET SYSTEM NAME コマンド（「運用・管理」の 267 ページ）で指定されたコンピューター名を設定してください。これにより、同コマンドで設定したコンピューター名が、DHCP パケットの Hostname フィールドにセットされて送信されるようになります。

```
SET SYSTEM NAME="mycomputername" ↵
```

■ 本製品の DHCP クライアント機能では、IP アドレス、サブネットマスクに加え、DNS サーバーアドレス（2 個まで）、デフォルト経路、ドメイン名の情報も取得・自動設定できます。

■ DHCP サーバーから割り当てられた IP アドレス、DNS サーバーアドレス、ゲートウェイアドレスなどは、SHOW DHCP コマンド（「DHCP サーバー」の 32 ページ）で確認できます（「DHCP Client」セクションに表示されます）。

■ インターフェースに設定された IP アドレスは、SHOW IP INTERFACE コマンド（458 ページ）で確認します。

■ デフォルト経路は SHOW IP ROUTE コマンド（473 ページ）で確認します。「Destination」が 0.0.0.0 のエントリーがデフォルト経路です。

■ DNS サーバーアドレスの設定状況は、SHOW IP コマンド（429 ページ）で確認します。「Primary Name Server」、「Secondary Name Server」欄をご覧ください。

マルチホーミング

マルチホーミングは、1 つのデータリンク上に複数の論理 IP インターフェースを作成する機能です。この機能は IP エイリアスなどとも呼ばれ、1 つのデータリンクインターフェースに複数の IP アドレスを割り当て、同一物理セグメント上に複数の IP サブネットを混在させることができます。論理インターフェースは 1 データリンクあたり 16 個まで作成できます。
論理インターフェースは「vlan1-n」の形式で指定します（vlan1 はデータリンク層インターフェース名）。「n」は論理インターフェース番号（0〜15）です。「-n」を省略した場合は、論理インターフェース 0 を指定したことになります（例では vlan1-0）。

■ vlan1 上に IP インターフェースを 2 つ作成します。「vlan1-0」は単に「vlan1」と書いてもかまいません。

```
ADD IP INT=vlan1-0 IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan1-1 IP=192.168.20.1 MASK=255.255.255.0 ↵
```

✎ 複数のインターフェースに対し、同一サブネットの IP アドレスを割り当てることはできません。たとえば、vlan1-0 に IP アドレス 192.168.10.1、ネットマスク 255.255.255.0 を割り当てた場合、192.168.10.2〜192.168.10.254 の範囲は同一 IP サブネットになるので、この範囲を他のインターフェース（たとえば vlan1-1）に割り当てることはできません。この制限はマルチホーミングによる論理インターフェースに限らず、すべてのインターフェースに適用されます。

始点 IP アドレスの決定

ルーターは複数のインターフェースを持つため、IP アドレスも複数あるのが普通です。ルーター本来の役割を果たすとき、すなわち他のホストが送信したパケットを中継するときには、IP パケットにルーター自身の IP アドレスが入ることはありません。
しかし、ルーター自身がパケットを送信するときには、複数ある IP アドレスのどれが始点アドレスとして使われるのかが重要なケースがあります。たとえば、IPsec ではルーター（セキュリティーゲートウェイ）間の通信がトンネルを形成します。このとき、もっとも基本的な相手ルーターの識別手段は、パケットの始点

アドレスです。IPsec の設定で相手ルーターのアドレスを指定したつもりでも、指定したのとは異なるインターフェースのアドレスが始点アドレスとして使われてしまうと、相手を識別することができず、結果として通信できないケースが出てきます。ここでは、ルーター自身が送信するパケットの始点アドレスとして、どのアドレスが使われるのかを例を挙げながら解説します。
本製品自身が IP パケットを送信するとき、始点アドレスは以下の基準にしたがって決定されます。

1. コマンド等で始点アドレスまたは始点インターフェースを明示的に指定した場合は、そのアドレスが使われる。PING コマンド（319 ページ）の SIPADDRESS パラメーターや、CREATE ISAKMP POLICY コマンド（「IPsec」の 45 ページ）の SRCINTERFACE パラメーターがこれに当たる。
2. 1 に該当せず、なおかつ、SET IP LOCAL コマンド（367 ページ）で IP アドレスが指定されている場合は、そのアドレスが使われる。
3. 1、2 のいずれにも該当しない場合は、パケットを送出するインターフェースのアドレスが使われる。ただし、送出インターフェースが Unnumbered のばあいは、一番最初に設定したインターフェースのアドレス（最初に ADD IP INTERFACE コマンド（179 ページ）を実行したインターフェースのアドレス）が使われる。

✎ PPPoE LAN 型接続では、WAN 側 Unnumbered というものの、実際には Unnumbered ではなく、ネットワークアドレスが WAN 側に割り当てられるケースがあるようです。この場合は、始点アドレスとして WAN 側インターフェースに設定されたネットワークアドレスを使おうとするため、他のインターフェースのアドレスが始点になるよう設定を工夫してください。

ローカル IP インターフェース

ローカル IP インターフェース（ループバックインターフェース）は、下位層（物理層/データリンク層）との関連を持たない仮想的な IP インターフェースです。物理的なインターフェースに割り当てた IP アドレスは、該当インターフェースのリンクダウンにより到達不能になる可能性がありますが、ローカル IP インターフェースは下位層の状態に依存しないため、このインターフェースの IP アドレスを広告することで、本製品への到達性を高めることができます。
ローカル IP インターフェースに割り当てたアドレスは、本製品が送信する RIP、OSPF、BGP-4、RADIUS、SNMP、PIM、NTP、Ping パケットなどの始点アドレスとして使用することができます。

■ ローカル IP インターフェースを作成するには、ADD IP LOCAL コマンド（182 ページ）を使います。ローカル IP インターフェースは 15 個まで作成可能です。LOCAL パラメーターにはローカル IP インターフェース番号（1〜15）を指定します。作成したローカル IP インターフェースには「localX」形式の名前が付きます（X は番号。1〜15）。

```
ADD IP LOCAL=1 IP=192.168.0.1 ↵
```

■ ローカル IP インターフェースの IP アドレスを変更するには、SET IP LOCAL コマンド（367 ページ）を使います。

```
SET IP LOCAL=1 IP=172.28.0.1 ↵
```

■ ローカル IP インターフェースを削除するには、DELETE IP LOCAL コマンド（234 ページ）を使います。

```
DELETE IP LOCAL=1 ↵
```

■ ローカル IP インターフェースの情報を確認するには、SHOW IP INTERFACE コマンド（458 ページ）を使います。「localX」がローカル IP インターフェースです。なお、「LOCAL」はデフォルトのローカル IP インターフェース（後述）です。

```
SHOW IP INTERFACE ↵
```

■ デフォルトローカル IP インターフェースは、システム起動時に自動的に作成されるローカル IP インターフェースです。SHOW IP INTERFACE コマンド（458 ページ）では、インターフェース名「LOCAL」として表示されます。
ADD IP LOCAL コマンド（182 ページ）で作成する通常のローカル IP インターフェースには任意の IP アドレスを割り当てることができますが、デフォルトローカル IP インターフェースに割り当てるアドレスは、実インターフェースに設定されている IP アドレスのどれか 1 つでなくてはなりません。
すなわち、デフォルトローカル IP インターフェースは、独立したインターフェースというよりも、本製品が持つ複数の IP インターフェースの中でどれを「デフォルト」のインターフェースとして使うか（どのインターフェースのアドレスをデフォルトの IP アドレスとして使うか）を指定するものといえます。
デフォルトローカル IP インターフェースの IP アドレスを指定するには、SET IP LOCAL コマンド（367 ページ）を使います。LOCAL パラメーターには値を指定しないか、キーワード DEFAULT を指定してください。また、IP パラメーターには、実インターフェースに割り当てた IP アドレスのうちの 1 つを指定してください。これにより、指定したアドレスがデフォルトの IP アドレスとして使用されるようになります。

```
SET IP LOCAL IP=192.168.10.1 ↵
```

または

```
SET IP LOCAL=DEFAULT IP=192.168.10.1 ↵
```

■ ローカル IP インターフェースは、以下の各機能で使用することができます。

- RADIUS クライアント
  RADIUS 要求パケットの始点 IP アドレスとして、任意のローカル IP インターフェースのアドレスを使用することができます。使用するローカル IP インターフェースは、通信相手の RADIUS サーバーごとに ADD RADIUS SERVER コマンド（「運用・管理」の 110 ページ）の LOCAL パラメーターで指定します。

  ```
  ADD RADIUS SERVER=192.168.10.5 PORT=1812 ACCPORT=1813 SECRET=hgap9er
    LOCAL=1 ↵
  ```

- SNMP

SNMP パケットの始点 IP アドレスとして、任意のローカル IP インターフェースのアドレスを使用することができます。本製品は SNMP の各バージョン（v1/v2c/v3）に対応していますが、バージョンごとに異なるローカル IP インターフェースを使用することも可能です。使用するローカル IP インターフェースは、SET SNMP LOCAL コマンド（「運用・管理」の 260 ページ）で指定します。

```
SET SNMP LOCAL=1 VERSION=ALL ↵
```

- BGP-4

  BGP パケットの始点 IP アドレスとして、任意のローカル IP インターフェースのアドレスを使用することができます。使用するローカル IP インターフェースは、通信相手の BGP ピアごとに ADD BGP PEER コマンド（154 ページ）、SET BGP PEER コマンド（343 ページ）の LOCAL パラメーターで指定します。また、BGP ピアテンプレートを使用する場合は、ADD BGP PEERTEMPLATE コマンド（158 ページ）、SET BGP PEERTEMPLATE コマンド（346 ページ）の LOCAL パラメーターで指定します。

  ```
  ADD BGP PEER=192.168.0.2 REMOTEAS=65001 LOCAL=1 ↵
  ```

  また、BGP 識別子（ルーター ID) としてデフォルトローカル IP インターフェース（LOCAL）のアドレスが使用されることもあります。本製品のデフォルト動作では、インターフェースに設定された IP アドレスの中でもっとも大きなものが BGP 識別子（ルーター ID）として使われます。ただし、SET IP LOCAL コマンド（367 ページ）でデフォルトローカル IP インターフェース（LOCAL）のアドレスを指定している場合は、そのアドレスがルーター ID として使われます。

経路制御（スタティック）

本製品は以下の IP ユニキャスト経路制御方式に対応しています。

- スタティックルーティング
- ダイナミックルーティング
  - RIP Version 1
  - RIP Version 2
  - OSPF
  - BGP-4

また、ダイナミックルーティングプロトコルによる経路情報のやりとりに制限をかける機能も備えています。
ここでは、スタティックルーティングの設定手順について解説します。ダイナミックルーティングの設定については、「IP」の「経路制御（RIP）」、「経路制御（OSPF）」、「経路制御（BGP-4）」をご覧ください。
スタティックルーティング（静的経路制御）は、管理者が経路情報を手動で登録するもっとも基本的な経路制御方式です。静的経路には次の種類があります。

- インターフェース（ダイレクト）経路
- スタティック経路
- デフォルト経路

インターフェース（ダイレクト）経路

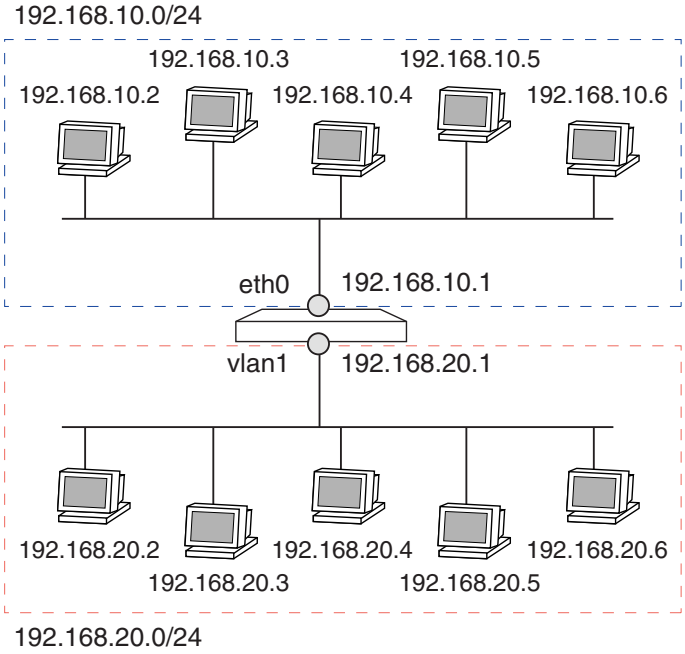
本製品に直接接続されているネットワークへの経路情報です。ADD IP INTERFACE コマンド（179 ページ）でインターフェース（eth、vlan、ppp）に IP アドレスを割り当てると、インターフェースに接続されたネットワークへの経路が自動的に登録されます。たとえば、次のコマンドを実行すると、

```
ADD IP INTERFACE=eth0 IP=192.168.10.1 MASK=255.255.255.0 ↵
```

次のような経路情報が自動的に登録されます。

```
IP Routes
-------------------------------------------------------------------------------
Destination       Mask              NextHop             Interface           Age
                  Type     Policy   Protocol            Metrics      Preference
-------------------------------------------------------------------------------
192.168.10.0      255.255.255.0     0.0.0.0             eth0               7124
                  direct   0        interface           1                     0
-------------------------------------------------------------------------------
```

本製品は、IP モジュールを有効にし、複数のインターフェースに IP アドレスを割り当てた時点でインターフェース間の IP ルーティングが有効になります。
ここでは例として、2 つのインターフェースに IP アドレスを割り当て、IP がルーティングされるよう設定します。



1. IP モジュールを有効にします。

   ```
   ENABLE IP ↵
   ```

2. 各インターフェースに IP アドレスを割り当てます。

   ```
   ADD IP INT=eth0 IP=192.168.10.1 MASK=255.255.255.0 ↵
   ADD IP INT=vlan1 IP=192.168.20.1 MASK=255.255.255.0 ↵
   ```

以上で設定は完了です。IP 割り当てと同時に各インターフェースへの経路情報が登録され、インターフェース間で IP のルーティングが行われるようになります。経路表を確認するには、SHOW IP ROUTE コマンド（473 ページ）を使います。

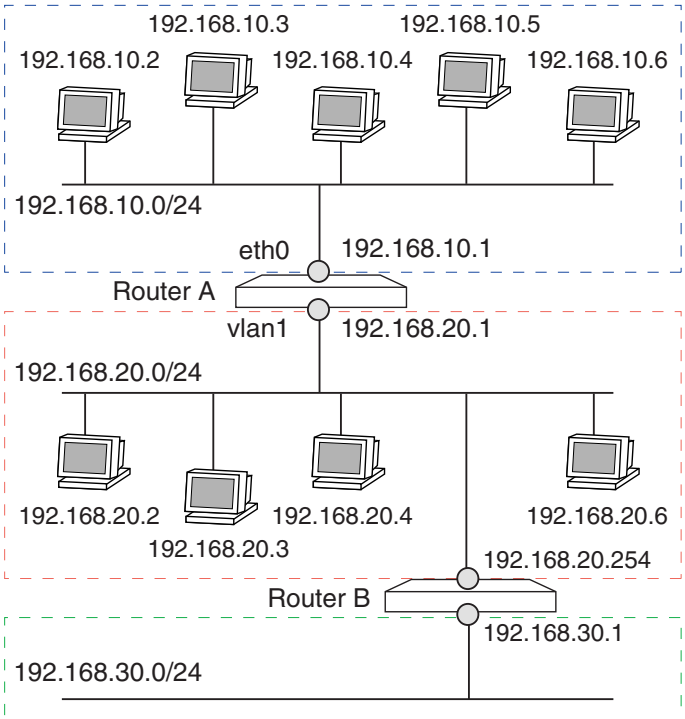
```
Manager > show ip route

IP Routes
-------------------------------------------------------------------------------
Destination       Mask              NextHop             Interface          Age
                  Type     Policy   Protocol            Metrics      Preference
-------------------------------------------------------------------------------
192.168.10.0      255.255.255.0     0.0.0.0             eth0               7475
                  direct   0        interface           1                     0
192.168.20.0      255.255.255.0     0.0.0.0             vlan1              7472
                  direct   0        interface           1                     0
-------------------------------------------------------------------------------
```

スタティック経路

ネットワーク上に他のルーターが存在するような場合には、ADD IP ROUTE コマンド（189 ページ）を使って、離れたネットワークへの経路を手動で登録することができます。
経路の登録には、次の情報が必要です。

- 宛先のネットワークアドレス（IP アドレスとマスクで指定する）
- 宛先にもっとも近い（パケットを送り出す）インターフェース
- 宛先への経路上にある最初のルーター（ネクストホップルーター）の IP アドレス
- 宛先までの距離（メトリック）。パケットを送り出すインターフェースから宛先ネットワークまでの間に存在するルーターの数＋ 1 で表します。

ここでは例として、次のようなネットワークにおけるルーター A の設定を示します。



1. IP モジュールを有効にします。

   ```
   ENABLE IP ↵
   ```

2. 各インターフェースに IP アドレスを割り当てます。

   ```
   ADD IP INT=eth0 IP=192.168.10.1 MASK=255.255.255.0 ↵
   ADD IP INT=vlan1 IP=192.168.20.1 MASK=255.255.255.0 ↵
   ```

3. ネットワーク 192.168.30.0/24 への経路をスタティックに登録します。自分以外のルーターを 1 つ経由するため、METRIC パラメーターには 1+1=2 を指定します。

```
ADD IP ROUTE=192.168.30.0 MASK=255.255.255.0 INT=vlan1
  NEXTHOP=192.168.20.254 METRIC=2 ↵
```

以上で設定は完了です。IP 割り当てと同時に各インターフェースへの経路情報が登録され、インターフェース間で IP のルーティングが行われるようになります。また、静的経路設定により、192.168.30.0/24 宛てのパケットはルーター「192.168.20.254」に転送されるようになります。

■ 経路表を確認するには、SHOW IP ROUTE コマンド（473 ページ）を使います。

```
Manager > show ip route

IP Routes
-------------------------------------------------------------------------------
Destination       Mask              NextHop             Interface          Age
                  Type     Policy   Protocol            Metrics      Preference
-------------------------------------------------------------------------------
192.168.10.0      255.255.255.0     0.0.0.0             eth0               7475
                  direct   0        interface           1                     0
192.168.20.0      255.255.255.0     0.0.0.0             vlan1              7472
                  direct   0        interface           1                     0
192.168.30.0      255.255.255.0     192.168.20.254      vlan1                 1
                  remote   0        static              2                    60
-------------------------------------------------------------------------------
```

■ 経路を削除するには DELETE IP ROUTE コマンド（237 ページ）を使います。経路削除時は、ROUTE、MASK、INTERFACE、NEXTHOP の全パラメーターを指定する必要があります。

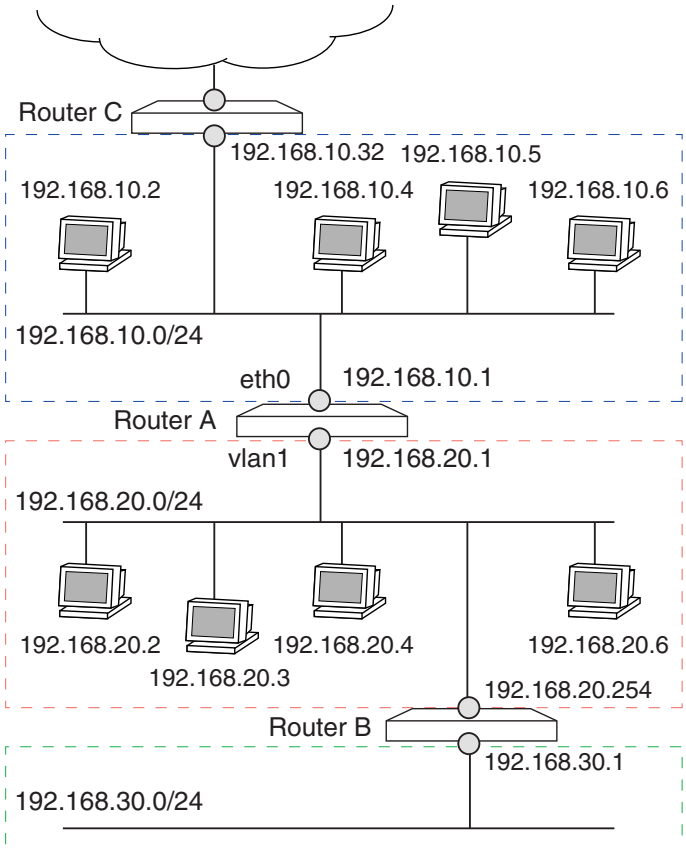
```
DELETE IP ROUTE=192.168.30.0 MASK=255.255.255.0 INT=vlan1
  NEXTHOP=192.168.20.254 ↵
```

デフォルト経路

末端のネットワークでは、経路表にないネットワーク宛てのパケットをすべて特定のルーターに転送するよう設定することにより、経路設定を簡素化することができます。このような経路をデフォルト経路（デフォルトルート）と呼びます。デフォルト経路は、ADD IP ROUTE コマンド（189 ページ）の ROUTE、MASK オプションに 0.0.0.0 を指定することによって作成します（この場合 MASK は省略可能です）。たとえば、eth0 上にデフォルト経路 192.168.10.32 があるならば、次のようにして登録します。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=eth0 NEXTHOP=192.168.10.32 ↵
```

ここでは例として、次のようなネットワークにおけるルーター A の設定を示します。



1. IP モジュールを有効にします。

```
ENABLE IP ↵
```

2. 各インターフェースに IP アドレスを割り当てます。

```
ADD IP INT=eth0 IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan1 IP=192.168.20.1 MASK=255.255.255.0 ↵
```

3. ネットワーク 192.168.30.0/24 への経路をスタティックに登録します。

```
ADD IP ROUTE=192.168.30.0 MASK=255.255.255.0 INT=vlan1
  NEXTHOP=192.168.20.254 METRIC=2 ↵
```

4. それ以外のネットワーク宛てのパケットはルーター C に転送します。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=eth0 NEXTHOP=192.168.10.32 ↵
```

以上で設定は完了です。IP 割り当てと同時に各インターフェースへの経路情報が登録され、インターフェース間で IP のルーティングが行われるようになります。また、静的経路設定により、192.168.30.0/24 宛てのパケットはルーター B のインターフェース「192.168.20.254」に転送されるようになります。また、それ以外のネットワーク（ルーター A 直下の 192.168.10.0/24、192.168.20.0/24 と、スタティック登録された

192.168.30.0/24 以外）宛てのパケットは、デフォルトゲートウェイ（ルーター C）192.168.10.32 に転送されるようになります。

■ 経路表を確認するには、SHOW IP ROUTE コマンド（473 ページ）を使います。

```
Manager > show ip route

IP Routes
-------------------------------------------------------------------------------
Destination       Mask              NextHop             Interface          Age
                  Type     Policy   Protocol            Metrics      Preference
-------------------------------------------------------------------------------
0.0.0.0           0.0.0.0           192.168.10.32       eth0              6800
                  direct   0        static              1                  360
192.168.10.0      255.255.255.0     0.0.0.0             eth0              7475
                  direct   0        interface           1                    0
192.168.20.0      255.255.255.0     0.0.0.0             vlan1             7472
                  direct   0        interface           1                    0
192.168.30.0      255.255.255.0     192.168.20.254      vlan1                1
                  remote   0        static              2                   60
-------------------------------------------------------------------------------
```

■ 経路を削除するには DELETE IP ROUTE コマンド（237 ページ）を使います。経路削除時は、ROUTE、MASK、INTERFACE、NEXTHOP の全パラメーターを指定する必要があります。

```
DELETE IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=eth0 NEXTHOP=192.168.10.32 ↵
```

経路制御（RIP）

ネットワークの規模が大きくなると、手動で経路情報を登録するスタティックルーティングでは管理の手間が大きくなり、設定ミスなどによる通信障害も起きやすくなります。ダイナミックルーティングは、ルーター間で経路情報を自動的に交換しあう「ダイナミックルーティング（経路制御）プロトコル」を用いて、経路情報の管理を自動化する方法です。本製品では以下のルーティングプロトコルを使用できます。

- RIP（Version 1/2）
- OSPF

ここでは、RIP の設定手順について解説します。OSPF の設定については「経路制御（OSPF）」を、スタティックルーティングの設定方法については「IP」の「経路制御（スタティック）」をご覧ください。

プロトコル概要

RIP（Routing Information Protocol）は比較的小規模なネットワーク用に設計されたシンプルなダイナミックルーティングプロトコルです。RIP ルーターは、自分の持つ経路表を定期的にブロードキャスト（RIP2 ではマルチキャスト）し、隣接するルーターに経路情報を伝えます。RIP パケットを受け取った各ルーターは、自分の経路表と受け取った情報を比べ、必要に応じて経路エントリーを追加・削除・修正して経路情報を最新に保ちます。
RIP にはさまざまな制限がありますが、そのシンプルさゆえに設定が簡単であり、小規模なネットワークでは有効に機能します。より大規模なネットワークでは後述する OSPF のほうが適しています。
RIP はトランスポート層として UDP を利用します。始点・終点ポートは 520 番です。

RIP Version1 と 2

現在使用されている RIP には 2 つのバージョンがあります。オリジナルの RIP（RIP Version 1）は RFC1058 で、改良版の RIP Version 2 は RFC2453 でそれぞれ規定されています。
RIP Version1（以下 RIP1）で交換される経路情報は次のとおりです。

- 宛先ネットワークアドレス
- メトリック（ホップ数）

RIP1 にはサブネットマスクの概念がないため、RIP1 の経路エントリーにはクラス A、B、C に基づく標準マスクが適用されます。
一方、RIP Version2（以下 RIP2）は、RIP1 の未使用フィールドを用いて以下の点を改良しています。

- サブネットマスクの情報を扱える
- ネクストホップルーターアドレスを扱える
- ブロードキャストではなくマルチキャスト（224.0.0.9）で送信する
- 簡単な認証機構（平文パスワードまたは MD5）がある

基本設定

■ 指定した IP インターフェースで RIP パケットの送受信が行われるようにするには、ADD IP RIP コマンド（187 ページ）でインターフェース名を指定します。たとえば、vlan1 と ppp0 で RIP（RIP1）を有効にするには、次のようにします。

```
ADD IP RIP INT=vlan1 ↵
ADD IP RIP INT=ppp0 ↵
```

■ ADD IP RIP コマンド（187 ページ）を実行すると、デフォルトでは RIP1 が使用されます。RIP2 を使う場合は SEND、RECEIVE パラメーターで RIP2 を指定してください。

```
ADD IP RIP INT=vlan1 SEND=RIP2 RECEIVE=RIP2 ↵
ADD IP RIP INT=ppp0 SEND=RIP2 RECEIVE=RIP2 ↵
```

■ RIP インターフェースの設定を確認するには SHOW IP RIP コマンド（468 ページ）を使います。

```
SHOW IP RIP ↵
```

■ 経路表を確認するには、SHOW IP ROUTE コマンド（473 ページ）を使います。

```
SHOW IP ROUTE ↵
```

■ RIP パケットの送受信をオフにするには、DELETE IP RIP コマンド（236 ページ）で IP インターフェース名を指定します。

```
DELETE IP RIP INT=vlan1 ↵
```

■ RIP の受信のみで送信を行わないようにするには SEND パラメーターに NONE を指定します。

```
ADD IP RIP INT=vlan1 SEND=NONE RECEIVE=RIP1 ↵
```

■ 末端のネットワークなどで RIP 情報の送信のみを行い、受信を行わないようにするには RECEIVE パラメーターに NONE を指定します。

```
ADD IP RIP INT=vlan1 SEND=RIP1 RECEIVE=NONE ↵
```

■ RIP インターフェースの設定を変更するには SET IP RIP コマンド（369 ページ）を使います。

```
SET IP RIP INT=vlan1 SEND=RIP1 RECEIVE=RIP1 ↵
```

■ RIP2 の認証機構を使う場合は次のようにします。各ルーターに同じパスワードを設定してください。パ

スワードの最大長は 16 文字です。

```
ADD IP RIP INT=vlan1 SEND=RIP2 RECEIVE=RIP2 AUTHENTICATION=PASSWORD
  PASSWORD=himitsu ↵
```

■ RIP パケットの送受信統計は SHOW IP RIP COUNTER コマンド（470 ページ）で確認できます。

■ RIP タイマーの変更は SET IP RIPTIMER コマンド（371 ページ）で行います。

RIP ユニキャスト

通常、RIP パケットはブロードキャスト（RIP1）またはマルチキャスト（RIP2）で送信されますが、本製品では、通信相手の IP アドレスを指定することにより、ユニキャストによる送受信も可能です。

■ 同一サブネット上のルーターに経路情報を送信するには、ADD IP RIP コマンド（187 ページ）の SEND パラメーターに NONE 以外（RIP1、RIP2、COMPATIBLE のいずれか）を指定し、IP パラメーターに相手ルーターの IP アドレスを指定します。たとえば、vlan1 上の RIP2 ルーター「192.168.20.2」に対して、経路情報をユニキャストで送信するには、次のようにします。この例では「192.168.20.2」からは経路情報を受信しません。

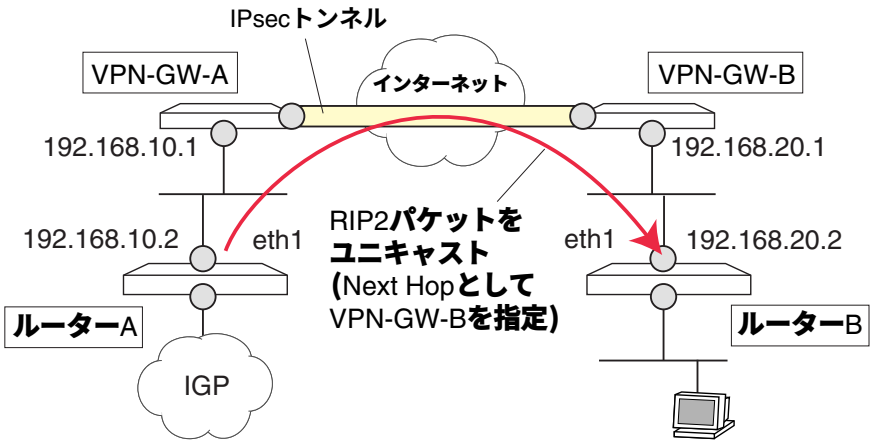
```
ADD IP RIP INT=vlan1 IP=192.168.20.2 SEND=RIP2 RECEIVE=NONE ↵
```

一方、「192.168.20.2」の側は次のように設定します。ここでは、送信側が「192.168.20.1」であるとします。こちらは受信のみの設定です。

```
ADD IP RIP INT=vlan1 IP=192.168.20.1 SEND=NONE RECEIVE=RIP2 ↵
```

■ 同一サブネット上にないルーターに経路情報を送信するには、ADD IP RIP コマンド（187 ページ）の SEND パラメーターに RIP2 か COMPATIBLE を、IP パラメーターに相手ルーターの IP アドレスを、NEXTHOP パラメーターに相手ルーターから見て適切なネクストホップアドレスを指定します。ここでは、次の図のような IPsec VPN の構成を考えます。

✎ 本例のような構成では、必ず RIP2 を使ってください。RIP1 パケットには Next Hop フィールドがないため、ネクストホップアドレスを通知できません。



ここで、ルーター A からルーター B に RIP2 で経路情報を通知するには、ルーター A で次の設定を行います。IP にはルーター B のアドレス（RIP2 パケットの終点アドレス）を、NEXTHOP には RIP2 パケットの Next Hop フィールドにセットするネクストホップアドレス（ここでは、VPN-GW-B の LAN 側アドレス）を指定します。

```
ADD IP RIP INT=eth0 IP=192.168.20.2 NEXTHOP=192.168.20.1 SEND=RIP2
  RECEIVE=NONE ↵
```

一方、ルーター B では、ルーター A からの RIP2 ユニキャストパケットを受信するために、次のような設定をします。IP にはルーター A のアドレス（RIP2 パケットの始点アドレス）を指定します。

```
ADD IP RIP INT=eth0 IP=192.168.10.2 SEND=NONE RECEIVE=RIP2 ↵
```

経路制御（OSPF）

ネットワークの規模が大きくなると、手動で経路情報を登録するスタティックルーティングでは管理の手間が大きくなり、設定ミスなどによる通信障害が起きやすくなります。ダイナミックルーティングは、ルーター間で経路情報を自動的に交換しあう「ダイナミックルーティング（経路制御）プロトコル」を用いて、経路情報の管理を自動化する方法です。本製品では以下のルーティングプロトコルを使用できます。

- RIP（Version 1/2）
- OSPF

ここでは、OSPF の設定手順について解説します。RIP の設定については「経路制御（RIP）」を、スタティックルーティングの設定方法については「IP」の「経路制御（スタティック）」をご覧ください。

プロトコル概要

OSPF（Open Shortest Path First）は中規模以上のネットワークでの使用を想定して開発された経路制御プロトコルです。現在のバージョンである OSPF Version 2 は RFC2328 で規定されています。
RIP がネットワーク全体をフラットなものとして扱うのに対し、OSPF ではネットワークをエリアと呼ばれる小さな単位に分割して、経路情報をエリアごとに管理する点が特徴的です。また、使用するアルゴリズムも異なり、OSPF ではリンクステートアルゴリズム、RIP はディスタンスベクターアルゴリズムを使用しています。
OSPF が採用するリンクステートアルゴリズムでは、同一エリア内のすべてのルーターが同じトポロジーデータベースを保持しています。各ルーターはこのデータベースをもとに経路表を作成し、これに基づいてエリア内の経路選択を行います。エリア内部の詳細なトポロジーは他のエリアからは見えないようになっており、経路情報の削減に貢献しています。

AS（Autonomous System）

経路制御プロトコルには、組織内で使用する IGP（Interior Gateway Protocol）と組織間で使用する EGP（Exterior Gateway Protocol）がありますが、OSPF は RIP と同様 IGP に分類されます。
ここでいう「組織」は、より正確には「AS（Autonomous System = 自律システム）」と呼ぶべきものです。AS とは、同じルーティングプロトコルを使用して経路情報を交換しあっているルーターの集まり、すなわち、OSPF なら OSPF、RIP なら RIP を使用しているネットワークの範囲を示します。AS は経路制御ドメインなどと呼ばれることもあります。

エリア

OSPF では、ネットワークを複数のエリアに分割して、それぞれを経路情報の管理範囲とします。各エリアは、エリア ID と呼ばれる 32 ビットの数値で識別されます。通常エリア ID は「1.1.1.1」のように IP アドレスと同じ形式で書き表します。エリア ID は ADD OSPF AREA コマンド（199 ページ）でエリアを作成するときに指定します。エリア ID 0.0.0.0 は、後述するバックボーンエリアのために予約されています。

✎ エリア ID は IP アドレスと同じ形式で表しますが、IP アドレスと直接の関係はありません。任意の数値を使うことができます。管理上わかりやすい番号を付けるとよいでしょう。

各エリアで分散管理されている経路情報を束ねるのは、バックボーンと呼ばれる特殊なエリアです。OSPF ネットワークを構成する各エリアは必ずバックボーンエリア（エリア ID 0.0.0.0）に接続されており、エリアごとに管理されている経路情報は、バックボーンエリア経由で他のエリアに伝えられます。
このとき重要な役割を果たすのが、各エリアとバックボーンの境界に位置するエリア境界ルーター（ABR) です。ABR はエリア内の情報を要約した上で、これを他エリアの ABR にバックボーン経由で伝える役割を持ちます。また、バックボーン経由で入手した他エリアの経路情報をエリア内部に通知する役割も果たします。
始点・終点ともに同一エリア内のトラフィックは、エリア内の情報だけに基づいて配送されます（エリア内ルーティング)。一方、エリアをまたがるトラフィックは、エリア内→エリア間→エリア内の 2 レベル 3 段階で配送されます（エリア間ルーティング)。
OSPF エリアには次のような種類があります。

名称	役割
バックボーンエリア（0.0.0.0）	OSPF ネットワークの根幹をなす重要なエリア。どの OSPF ネットワークにも必要です。バックボーン以外のエリアは何らかの形でバックボーンエリアと接続されていなくてはなりません。これは、各エリアの経路情報が、バックボーンを通じて交換されるためです。エリア情報の交換は、バックボーンと他のエリアの境界に位置する ABR（エリア境界ルーター）が行います
スタブエリア	1 つのエリアとしか隣接しておらず、出口が 1 つしかないエリアをスタブエリアと呼びます。スタブエリア内には、AS 外部（OSPF ネットワークの範囲外）の詳細な経路情報が通知されず、デフォルト経路だけが通知されます。これにより、エリア内のルーターにかかる計算負荷を下げることができます。本製品では、バックボーン以外のエリアを作成するとデフォルトでスタブエリアとなります。スタブエリア内には ASBR（AS 境界ルーター）を置くことができず、また、後述する仮想リンクの通過エリアとなることもできません
ノーマルエリア	バックボーンエリアでもスタブエリアでもない通常のエリアです。ノーマルエリアを作成するときは、ADD OSPF AREA コマンドの STUBAREA パラメーターに NO を指定します。仮想リンクを通過させたいエリアは、ノーマルエリアでなくてはなりません

表 1: OSPF エリアの種類

OSPF ルーター

OSPF ルーターは、それぞれルーター ID という識別子を持ちます。ルーター ID はエリア ID と同様の 32 ビット値で、通常はエリア ID と同じように IP アドレスと同じ形式で書き表します（例：2.2.2.2)。
ルーター ID は、SET OSPF コマンド（381 ページ）の ROUTERID パラメーターで設定することができます。特に設定しなかった場合はルーターのインターフェースに割り当てられた IP アドレスのうち、もっとも大きなものがルーター ID として使用されます。

✎ ルーター ID は IP アドレスと同じ形式で表しますが、IP アドレスと直接の関係はありません。明示的に設定しなかった場合はインターフェースのアドレスのうちもっとも大きなものが使われますが、これも一意の識別子を得

るための方法として使っているだけであり、実際には任意の数値を使うことができます。管理上わかりやすい番号を付けるとよいでしょう。

OSPF ルーターは、役割によって以下のとおり分類できます。

名称	略称	役割
内部ルーター（Internal Router）	IR	1 つのエリアにだけ所属しているルーター（すべてのインターフェースが同一エリア内にあるルーター）
エリア境界ルーター（Area Border Router）	ABR	複数のエリア（バックボーンとそれ以外）に所属しているルーター。エリア内の経路情報を要約し、バックボーンエリア経由で他のエリアに伝える役目を負う。また、バックボーンエリア経由で入手した他エリアの経路情報を自エリア内部に通知する役割もある
バックボーンルーター（Backbone Router）	-	バックボーンエリアに所属しているルーター。ABR は必ずバックボーンルーターになるが、バックボーンルーターがつねに ABR とは限らない。すべてのインターフェースがバックボーンエリア内にある IR もバックボーンルーターである
AS 境界ルーター（Autonomous System Boundary Router）	ASBR	OSPF ネットワークと他のルーティングプロトコルを使用しているネットワークとの境界に位置するルーター。外部ネットワークの経路情報を OSPF ネットワーク内に通知する

表 2: OSPF ルーターの種類

OSPF メッセージ

OSPF は IP を直接使用します。プロトコル番号は 89（OSPFIGP）です。メッセージのやりとりには、ユニキャストアドレスに加え、以下のマルチキャストグループアドレスが使用されます。

- 224.0.0.5（OSPF ルーター）
- 224.0.0.6（OSPF 代表ルーター）

OSPF メッセージには以下の種類があります。

タイプ	メッセージ名	説明
1	Hello（Hello）	隣接ルーターの探索、代表ルーター（DR）の決定などに使用する
2	Database Description（データベース記述）	隣接関係の形成時にトポロジーデータベースの内容を要約して通知する
3	Link State Request（リンク状態要求）	隣接関係形成の最終段階において追加の LSA（トポロジー情報）を要求する
4	Link State Update（リンク状態更新）	LSA（トポロジー情報）を通知する
5	Link State Ack（リンク状態確認）	リンク状態更新パケットに対する確認応答

表 3:

LSA（Link State Advertisement）

OSPF のトポロジーデータベースを構成する基本レコードを LSA と呼びます。各ルーターは LSA を交換しあうことによって、トポロジーデータベースを構築します。LSA には以下の種類があります。

LSA タイプ	名称	説明
1	ルーター LSA	エリア内にあるルーターインターフェースの情報。すべてのルーターが生成する。通知範囲はエリア内に限定される
2	ネットワーク LSA	複数のルーターが接続されているマルチアクセス型ネットワークの情報。接続されているルーターの一覧を示す。該当ネットワークの代表ルーター（DR）が生成する。通知範囲はエリア内に限定される
3	ネットワークサマリー LSA	エリア外（ただし AS 内）ネットワークへの経路情報（ネクストホップ、メトリックなど）。エリア境界ルーター（ABR）が生成する。ABR が接続されているすべてのエリアに通知される
4	ASBR サマリー LSA	エリア外にある AS 境界ルーター（ASBR）への経路情報。ABR が生成する。ABR が接続されているすべてのエリアに通知される
5	AS 外部 LSA	AS 外部への経路情報。ASBR が生成する。AS 内全体に通知される

表 4: LSA の種類

設定手順

OSPF ネットワークを構築するための基本的な手順について説明します。具体的な設定例については、次項「基本設定」をご覧ください。

1. エリアを作成します。
   OSPF ルーターは必ずエリアに属さなければなりません。また、OSPF ネットワークには、必ずバックボーンエリア（0.0.0.0）というエリアが存在しなければなりません。最初に ADD OSPF AREA コマンド（199 ページ）を実行して、バックボーンエリアを作成します。

   ```
   ADD OSPF AREA=0.0.0.0 ↵
   ```

   ✎ 複数のエリアで構成されるネットワークの場合、それぞれのルーターには所属するエリアの設定だけを行います。

2. エリアに所属するネットワークの範囲を設定します。
   手順 1 で作成したエリアの範囲を IP アドレスとネットマスクによって定義します。たとえば、バックボーンエリアの範囲として 172.16.0.0〜172.16.255.255 を指定するには、ADD OSPF RANGE コマンド（208 ページ）を使って以下のように定義します。

```
ADD OSPF RANGE=172.16.0.0 MASK=255.255.0.0 AREA=0.0.0.0 ↵
```

✎ ネットワーク範囲は、同じエリアに所属するルーター間で矛盾のないよう設定してください。それぞれのルーターに対し、直接接続されているネットワークの範囲だけを指定すれば基本的な動作が可能です。また、エリアの範囲があらかじめわかっている場合は、直接接続されているかどうかにかかわらず、エリア内のすべてのルーターに同じ範囲設定をすることができます。

✎ エリア境界ルーター（ABR）では、ネットワーク範囲の設定にしたがって経路情報の要約（ネットワークサマリー LSA の生成）を行います。詳細は「ABR（エリア境界ルーター）」をご覧ください。

3. OSPF インターフェースの設定をします。
   OSPF メッセージの送受信を行う IP インターフェースをエリアに割り当てます。これには ADD OSPF INTERFACE コマンド（202 ページ）を使います。ここで指定するインターフェースのアドレスは、手順 2 で設定したネットワーク範囲内のアドレスでなくてはなりません。この例では、eth0 の IP アドレスは、172.16.0.1〜172.16.255.254 の範囲内である必要があります。

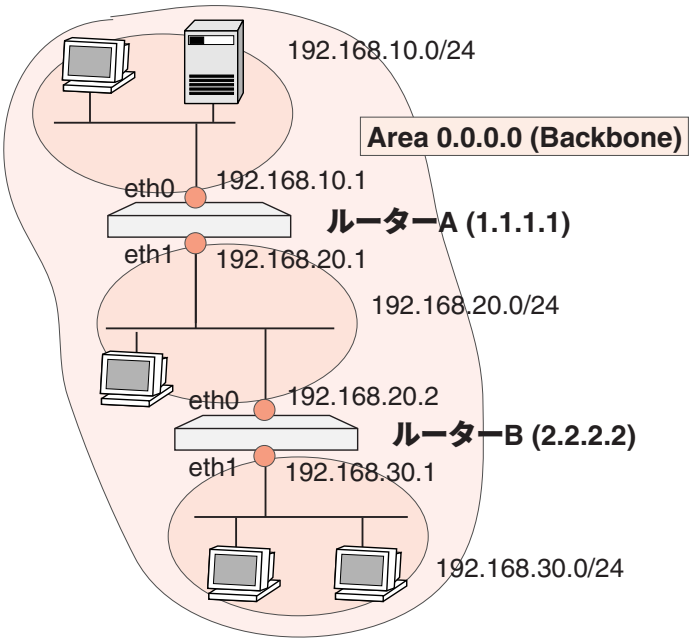
   ```
   ADD OSPF INTERFACE=eth0 AREA=0.0.0.0 ↵
   ```

4. OSPF を有効にします。

   ```
   ENABLE OSPF ↵
   ```

基本設定

バックボーンエリアだけで構成されたシンプルな OSPF ネットワークの設定例を示します。ここでは、次のようなネットワーク構成を例に解説します。



ルーター A の設定

1. IP モジュールを有効にし、各インターフェースに IP アドレスを設定します。

```
ENABLE IP ↵
ADD IP INT=eth0 IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=eth1 IP=192.168.20.1 MASK=255.255.255.0 ↵
```

2. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=1.1.1.1 ↵
```

3. バックボーンエリア（0.0.0.0）を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

4. バックボーンエリアに所属する IP アドレスの範囲を設定します。ここでは、直接接続されているネットワークの範囲を指定します。

```
ADD OSPF RANGE=192.168.10.0 MASK=255.255.255.0 AREA=0.0.0.0 ↵
ADD OSPF RANGE=192.168.20.0 MASK=255.255.255.0 AREA=0.0.0.0 ↵
```

5. バックボーンエリアに所属する IP インターフェースを指定します。

```
ADD OSPF INT=eth0 AREA=0.0.0.0 ↵
ADD OSPF INT=eth1 AREA=0.0.0.0 ↵
```

6. OSPF を有効にします。

```
ENABLE OSPF ↵
```

ルーター B の設定

1. IP モジュールを有効にし、各インターフェースに IP アドレスを設定します。

```
ENABLE IP ↵
ADD IP INT=eth0 IP=192.168.20.2 MASK=255.255.255.0 ↵
ADD IP INT=eth1 IP=192.168.30.1 MASK=255.255.255.0 ↵
```

2. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=2.2.2.2 ↵
```

3. バックボーンエリア（0.0.0.0）を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

4. バックボーンエリアに所属する IP アドレスの範囲を設定します。ここでは、直接接続されているネットワークの範囲を指定します。

```
ADD OSPF RANGE=192.168.20.0 MASK=255.255.255.0 AREA=0.0.0.0 ↵
ADD OSPF RANGE=192.168.30.0 MASK=255.255.255.0 AREA=0.0.0.0 ↵
```

5. バックボーンエリアに所属する IP インターフェースを指定します。

```
ADD OSPF INT=eth0 AREA=0.0.0.0 ↵
ADD OSPF INT=eth1 AREA=0.0.0.0 ↵
```

6. OSPF を有効にします。

```
ENABLE OSPF ↵
```

設定は以上です。

■ 経路表を確認するには、SHOW IP ROUTE コマンド（473 ページ）を使います。

■ OSPF インターフェースの状態は SHOW OSPF INTERFACE コマンド（493 ページ）で確認します。

```
SHOW OSPF INT ↵
SHOW OSPF INT=eth0 ↵
```

■ 隣接ルーターの情報を確認するには、SHOW OSPF NEIGHBOUR コマンド（503 ページ）を使います。

```
SHOW OSPF NEIGHBOUR ↵
```

■ OSPF エリアの情報を確認するには、SHOW OSPF AREA コマンド（487 ページ）を使います。

```
SHOW OSPF AREA ↵
SHOW OSPF AREA=0.0.0.0 ↵
```

■ OSPF エリアの範囲を確認するには、SHOW OSPF RANGE コマンド（505 ページ）を使います。

```
SHOW OSPF RANGE ↵
```

■ トポロジーデータベースの情報を確認するには SHOW OSPF LSA コマンド（497 ページ）を使います。

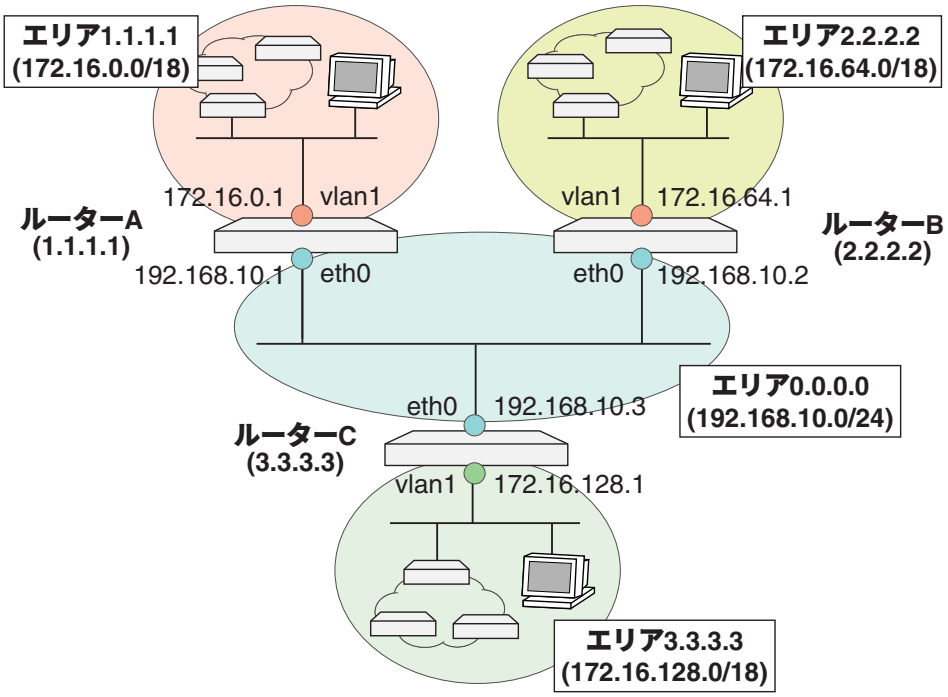
```
SHOW OSPF LSA ↵
SHOW OSPF LSA FULL ↵
```

■ OSPF の設定情報を確認するには SHOW OSPF コマンド（485 ページ）を使います。

```
SHOW OSPF ↵
```

ABR（エリア境界ルーター）

バックボーン（0.0.0.0）とエリア 1.1.1.1、2.2.2.2、3.3.3.3 の 4 エリアで構成される OSPF ネットワークの設定例を示します。エリア間に位置する ABR は、各エリア内の経路情報を要約して他のエリアに伝える役割を果たします。ここでは、ルーター A、B、C を ABR とする次のようなネットワーク構成を例に解説します。ここでは、ABR でのエリア範囲設定（ADD OSPF RANGE コマンド（208 ページ））によって、各エリア内の経路情報を集約してバックボーンに広報するよう設定します。



各エリアの範囲は次の通りです。

エリア	範囲
0.0.0.0（バックボーン）	192.168.10.0/24（192.168.10.0 ～ 192.168.10.255）
1.1.1.1（スタブエリア）	172.16.0.0/18（172.16.0.0 ～ 172.16.63.255）
2.2.2.2（スタブエリア）	172.16.64.0/18（172.16.64.0 ～ 172.16.127.255）
3.3.3.3（スタブエリア）	172.16.128.0/18（172.16.128.0 ～ 172.16.191.255）

表 5:

ルーター A の設定

1. IP モジュールを有効にし、各インターフェースに IP アドレスを設定します。

```
ENABLE IP ↵
ADD IP INT=vlan1 IP=172.16.0.1 MASK=255.255.255.0 ↵
ADD IP INT=eth0 IP=192.168.10.1 MASK=255.255.255.0 ↵
```

2. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=1.1.1.1 ↵
```

3. バックボーンエリア（0.0.0.0）を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

4. バックボーンエリアに所属するIPアドレスの範囲を設定します。ここでは、直接接続されているネットワークの範囲を指定します。

```
ADD OSPF RANGE=192.168.10.0 MASK=255.255.255.0 AREA=0.0.0.0 ↵
```

5. バックボーンエリアに所属するIPインターフェースを指定します。

```
ADD OSPF INT=eth0 AREA=0.0.0.0 ↵
```

6. エリア1.1.1.1を作成します。

```
ADD OSPF AREA=1.1.1.1 ↵
```

7. エリア1.1.1.1に所属するIPアドレスの範囲を設定します。直結されているネットワークの範囲は「172.16.0.0/24」ですが、ここではエリア全体を包含するCIDRブロック「172.16.0.0/18」を指定することにより、エリア外に1つの経路「172.16.0.0/18」だけを通知しています。

```
ADD OSPF RANGE=172.16.0.0 MASK=255.255.192.0 AREA=1.1.1.1 ↵
```

8. エリア1.1.1.1に所属するIPインターフェースを指定します。

```
ADD OSPF INT=vlan1 AREA=1.1.1.1 ↵
```

9. OSPFを有効にします。

```
ENABLE OSPF ↵
```

ルーターBの設定

1. IPモジュールを有効にし、各インターフェースにIPアドレスを設定します。

```
ENABLE IP ↵
ADD IP INT=vlan1 IP=172.16.64.1 MASK=255.255.255.0 ↵
ADD IP INT=eth0 IP=192.168.10.2 MASK=255.255.255.0 ↵
```

2. OSPFのルーターIDを設定します。

```
SET OSPF ROUTERID=2.2.2.2 ↵
```

3. バックボーンエリア（0.0.0.0）を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

4. バックボーンエリアに所属するIPアドレスの範囲を設定します。ここでは、直接接続されているネットワークの範囲を指定します。

```
ADD OSPF RANGE=192.168.10.0 MASK=255.255.255.0 AREA=0.0.0.0 ↵
```

5. バックボーンエリアに所属する IP インターフェースを指定します。

```
ADD OSPF INT=eth0 AREA=0.0.0.0 ↵
```

6. エリア 2.2.2.2 を作成します。

```
ADD OSPF AREA=2.2.2.2 ↵
```

7. エリア 2.2.2.2 に所属する IP アドレスの範囲を設定します。直結されているネットワークの範囲は「172.16.64.0/24」ですが、ここではエリア全体を包含する CIDR ブロック「172.16.64.0/18」を指定することにより、エリア外に 1 つの経路「172.16.64.0/18」だけを通知しています。

```
ADD OSPF RANGE=172.16.64.0 MASK=255.255.192.0 AREA=2.2.2.2 ↵
```

8. エリア 2.2.2.2 に所属する IP インターフェースを指定します。

```
ADD OSPF INT=vlan1 AREA=2.2.2.2 ↵
```

9. OSPF を有効にします。

```
ENABLE OSPF ↵
```

ルーター C の設定

1. IP モジュールを有効にし、各インターフェースに IP アドレスを設定します。

```
ENABLE IP ↵
ADD IP INT=vlan1 IP=172.16.128.1 MASK=255.255.255.0 ↵
ADD IP INT=eth0 IP=192.168.10.3 MASK=255.255.255.0 ↵
```

2. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=3.3.3.3 ↵
```

3. バックボーンエリア（0.0.0.0）を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

4. バックボーンエリアに所属する IP アドレスの範囲を設定します。ここでは、直接接続されているネットワークの範囲を指定します。

```
ADD OSPF RANGE=192.168.10.0 MASK=255.255.255.0 AREA=0.0.0.0 ↵
```

5. バックボーンエリアに所属する IP インターフェースを指定します。

```
ADD OSPF INT=eth0 AREA=0.0.0.0 ↵
```

6. エリア 3.3.3.3 を作成します。

```
ADD OSPF AREA=3.3.3.3 ↵
```

7. エリア 3.3.3.3 に所属する IP アドレスの範囲を設定します。直結されているネットワークの範囲は「172.16.128.0/24」ですが、ここではエリア全体を包含する CIDR ブロック「172.16.128.0/18」を指定することにより、エリア外に 1 つの経路「172.16.128.0/18」だけを通知しています。

```
ADD OSPF RANGE=172.16.128.0 MASK=255.255.192.0 AREA=3.3.3.3 ↵
```

8. エリア 3.3.3.3 に所属する IP インターフェースを指定します。

```
ADD OSPF INT=vlan1 AREA=3.3.3.3 ↵
```

9. OSPF を有効にします。

```
ENABLE OSPF ↵
```

設定は以上です。

■ 経路表を確認するには、SHOW IP ROUTE コマンド（473 ページ）を使います。

■ OSPF インターフェースの状態は SHOW OSPF INTERFACE コマンド（493 ページ）で確認します。

```
SHOW OSPF INT ↵
SHOW OSPF INT=eth0 ↵
```

■ 隣接ルーターの情報を確認するには、SHOW OSPF NEIGHBOUR コマンド（503 ページ）を使います。

```
SHOW OSPF NEIGHBOUR ↵
```

■ OSPF エリアの情報を確認するには、SHOW OSPF AREA コマンド（487 ページ）を使います。

```
SHOW OSPF AREA ↵
SHOW OSPF AREA=0.0.0.0 ↵
```

■ OSPF エリアの範囲を確認するには、SHOW OSPF RANGE コマンド（505 ページ）を使います。

```
SHOW OSPF RANGE ↵
```

■ トポロジーデータベースの情報を確認するには SHOW OSPF LSA コマンド（497 ページ）を使います。

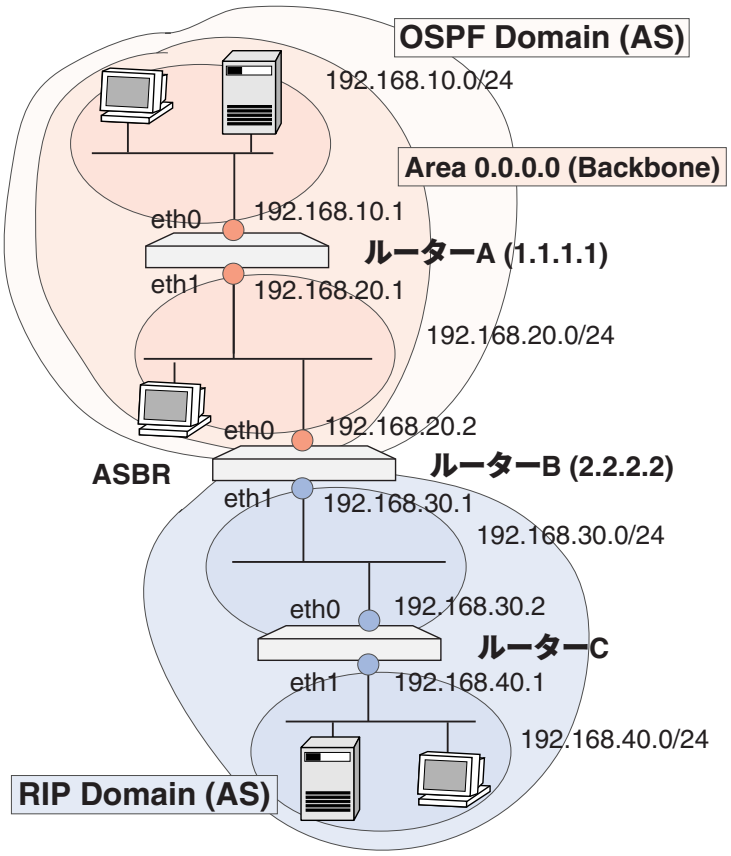
```
SHOW OSPF LSA ↵
SHOW OSPF LSA FULL ↵
```

■ OSPF の設定情報を確認するには SHOW OSPF コマンド（485 ページ）を使います。

```
SHOW OSPF ↵
```

ASBR（AS 境界ルーター）

OSPF と RIP のように、異なるルーティングプロトコルを使用するネットワークの境界に位置するルーターを AS 境界ルーター（ASBR=Autonomous System Boundary Router）と呼びます。ここでは、次のようなネットワーク構成を例として、本製品を ASBR として使用するための設定方法について説明します。



ルーター A の設定

1. IP モジュールを有効にし、各インターフェースに IP アドレスを設定します。

```
ENABLE IP ↵
ADD IP INT=eth0 IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=eth1 IP=192.168.20.1 MASK=255.255.255.0 ↵
```

2. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=1.1.1.1 ↵
```

3. OSPF のバックボーンエリア（0.0.0.0）を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

4. バックボーンエリアに所属する IP アドレスの範囲を設定します。ここでは、直接接続されているネットワークの範囲を指定します。

```
ADD OSPF RANGE=192.168.10.0 MASK=255.255.255.0 AREA=0.0.0.0 ↵
ADD OSPF RANGE=192.168.20.0 MASK=255.255.255.0 AREA=0.0.0.0 ↵
```

5. バックボーンエリアに所属する IP インターフェースを設定します。

```
ADD OSPF INT=eth0 AREA=0.0.0.0 ↵
ADD OSPF INT=eth1 AREA=0.0.0.0 ↵
```

6. OSPF を有効にします。

```
ENABLE OSPF ↵
```

ルーター B の設定

1. IP モジュールを有効にし、各インターフェースに IP アドレスを設定します。

```
ENABLE IP ↵
ADD IP INT=eth0 IP=192.168.20.2 MASK=255.255.255.0 ↵
ADD IP INT=eth1 IP=192.168.30.1 MASK=255.255.255.0 ↵
```

2. eth1 側で RIP パケットの送受信を有効にします。

```
ADD IP RIP INT=eth1 ↵
```

> ✎ RIP ではなくスタティックルーティングを行う場合は、ADD IP ROUTE コマンド（189 ページ）で経路情報を登録してください。たとえば、この例では「ADD IP ROUTE=192.168.40.0 MASK=255.255.255.0 INT=eth1 NEXT=192.168.30.2」などとします。

3. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=2.2.2.2 ↵
```

4. バックボーンエリア（0.0.0.0）を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

5. バックボーンエリアに所属する IP アドレスの範囲を設定します。ここでは、直接接続されているネットワークの範囲を指定します。

```
ADD OSPF RANGE=192.168.20.0 MASK=255.255.255.0 AREA=0.0.0.0 ↵
```

6. バックボーンエリアに所属する IP インターフェースを設定します。

```
ADD OSPF INT=eth0 AREA=0.0.0.0 ↵
```

7. ASBR ルーターの設定をします。

```
SET OSPF RIP=BOTH ASEXTERNAL=ON ↵
```

✎ RIP ではなくスタティックルーティングを行う場合は、「RIP=BOTH」は不要です。「ASEXTERNAL=ON」だけで、スタティック経路が OSPF に取り込まれるようになります。

8. OSPF を有効にします。

```
ENABLE OSPF ↵
```

ルーター C の設定

1. IP モジュールを有効にし、各インターフェースに IP アドレスを設定します。

```
ENABLE IP ↵
ADD IP INT=eth0 IP=192.168.30.2 MASK=255.255.255.0 ↵
ADD IP INT=eth1 IP=192.168.40.1 MASK=255.255.255.0 ↵
```

2. eth0 で RIP パケットの送受信を有効にします。

```
ADD IP RIP INT=eth0 ↵
```

3. eth1 では RIP パケットの送信のみを有効にします。

```
ADD IP RIP INT=eth1 SEND=RIP1 RECEIVE=NONE ↵
```

✎ RIP ではなくスタティックルーティングを行う場合は、ADD IP ROUTE コマンド（189 ページ）で経路情報を登録してください。たとえば、この例では「ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=eth0 NEXT=192.168.30.1」とすれば、直接接続されていないネットワーク宛てのパケットがすべてデフォルト経路（ルーター B）に送られるようになります。

■ 経路表を確認するには、SHOW IP ROUTE コマンド（473 ページ）を使います。

■ OSPF インターフェースの状態は SHOW OSPF INTERFACE コマンド（493 ページ）で確認します。

```
SHOW OSPF INT ↵
SHOW OSPF INT=eth1 ↵
```

■ 隣接ルーターの情報を確認するには、SHOW OSPF NEIGHBOUR コマンド（503 ページ）を使います。

```
SHOW OSPF NEIGHBOUR ↵
```

■ OSPF エリアの情報を確認するには、SHOW OSPF AREA コマンド（487 ページ）を使います。

```
SHOW OSPF AREA ↵
SHOW OSPF AREA=0.0.0.0 ↵
```

■ OSPF エリアの範囲を確認するには、SHOW OSPF RANGE コマンド（505 ページ）を使います。

```
SHOW OSPF RANGE ↵
```

■ トポロジーデータベースの情報を確認するには SHOW OSPF LSA コマンド（497 ページ）を使います。

```
SHOW OSPF LSA ↵
SHOW OSPF LSA FULL ↵
```

■ OSPF の設定情報を確認するには SHOW OSPF コマンド（485 ページ）を使います。

```
SHOW OSPF ↵
```

■ RIP の設定を確認するには SHOW IP RIP コマンド（468 ページ）を使います。

経路制御（BGP-4）

BGP-4（Border Gateway Protocol 4）について解説します。
BGP-4 は ISP などのネットワーク運用組織（経路制御ドメインまたは自律システム（AS）と呼びます）間で経路情報の交換を行うためのプロトコルです。組織内で経路情報をやりとりする OSPF や RIP などの IGP（Interior Gateway Protocol）に対し、BGP-4 のようなプロトコルは EGP（Exterior Gateway Protocol）と呼ばれます。BGP-4 は現在のインターネットを支える基幹的な経路制御プロトコルです。

✎ BGP-4 を使用するにはフィーチャーライセンス AT-FL-08 または AT-FL-08-B が必要です。

プロトコル概要

BGP-4（Border Gateway Protocol 4）は、インターネットに代表される相互接続型ネットワークにおいて、自律システム（AS）と呼ばれる組織（ISP や企業など）間で経路情報をやりとりするための経路制御プロトコルです。次に、BGP-4 に関連するおもな RFC を挙げます。

- RFC1771, A Border Gateway Protocol 4 (BGP-4)
- RFC1772, Application of the Border Gateway Protocol in the Internet
- RFC1997, BGP Communities Attribute
- RFC2385, Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC2439, BGP Route Flap Damping
- RFC2796, BGP Route Reflection - An Alternative to Full Mesh IBGP
- RFC2842, Capabilities Advertisement with BGP-4
- RFC2918, Route Refresh Capability for BGP-4
- RFC3065, Autonomous System Confederations for BGP

BGP-4 は、よりなじみの深い RIP や OSPF とは使用場所が異なります。RIP や OSPF は組織内のトラフィックを配送するために使用されます。一方、BGP-4 は組織間でトラフィックを配送するために使用されます。アルゴリズム的に見ると、BGP-4 はディスタンスベクターアルゴリズム（パスベクター）を使用した比較的シンプルな設計になっています。ただし、他組織との関係（契約など）に応じた配送制御ができるよう、各 AS において経路情報にさまざまな情報（「属性」と呼びます）を付加して、ポリシーに基づくルーティングが可能なようになっています。

AS（Autonomous System）

BGP-4 は組織間で経路情報を交換する EGP（Exterior Gateway Protocol）です。
ここでいう「組織」は、より正確には「AS（Autonomous System = 自律システム）」と呼ぶべきものです。BGP-4 では、RIP や OSPF でいう AS と比べ、若干その意味が拡張されています。すなわち、「1 つの経路制御プロトコルとメトリックを使って経路情報を交換しあっているルーターの集まり」という旧来の定義ではなく、「外部から見たときに、首尾一貫した経路制御ポリシーを持つように見えるルーターの集合（ネットワーク）。内部では複数の経路制御プロトコルやメトリックを使用していてもよい」という意味で AS という言葉を使っています。AS は通常同一組織の管理下に置かれており、経路制御ドメインなどと呼ばれることもあります。

AS は 1〜65535 の番号（ASN = AS 番号）によって識別されます。AS 番号は ICANN（Internet Corporation for Assigned Names and Numbers）が管理していますが、64512〜65535 はプライベート AS 番号として予約されており、各組織内で自由に使用できます。ただし、プライベート AS 番号は絶対にインターネット上に流してはなりません。
RFC1930, Guidelines for creation, selection, and registration of an Autonomous System (AS)

AS の種類

AS は他 AS との接続形態やトラフィックの配送ポリシーによって次のように分類できます。

名称	説明
スタブ AS（Stub AS）	1 つの AS とだけ 1 点で接続している AS。自 AS 宛てのトラフィックだけを受け入れる
マルチホーム AS（Multihomed AS）	1 つの AS と複数点で接続している、あるいは、複数の AS と接続している AS のうち、自 AS 宛てのトラフィックだけを受け入れ、他 AS 宛てのトラフィックは通過させないもの
トランジット AS（Transit AS）	複数の AS と接続しており、自 AS 宛てのトラフィックだけでなく、他 AS 宛てのトラフィックも（ポリシーに応じて）通過を許可する AS

表 6: AS の種類

AS とトラフィック

AS 間の関係を考慮した場合、トラフィックは次の 2 つに分類して考えることができます。

- ローカルトラフィック：始点か終点のどちらかが自 AS 内のアドレスであるトラフィック。すなわち、自 AS 宛てのトラフィックや自 AS から他 AS に向けて送られるトラフィック。
- トランジットトラフィック：始点と終点の両方が他 AS のアドレスであるトラフィック。すなわち、自 AS を単なる通過点とするトラフィック。

また、BGP-4 では、トラフィックの配送ポリシーを表すときに「トランジット」「非トランジット」という言葉が使われます。この場合それぞれの意味は次のとおりです。

- トランジット：他 AS 宛てトラフィックが自 AS を通過することを許可する。
- 非トランジット：他 AS 宛てトラフィックが自 AS を通過することを許可しない（自 AS 宛てのトラフィックしか受け取らない）。

BGP-4 の基本は、自 AS 内のプレフィックスを他 AS に通知することで自 AS 宛てのトラフィックを受け取れるようにすること、および、他 AS から経路を学習することで他 AS 宛てにトラフィックを送信できるようにすることです。
また、トランジット AS の場合は、特定のトランジットトラフィックだけが自 AS を通過できるよう、他 AS に通知する経路情報を操作することも重要になります。BGP-4 には、このようなポリシーを実施するために必要な機能が備えられています。

プレフィックス

プレフィックスとは、IP ネットワーク（IP アドレスの範囲）をネットワークアドレスとネットマスクの組で表したものです。次に表記例を挙げます。

```
172.16.10.0/24
172.16.10.0/255.255.255.0
```

2 つの例は同じプレフィックス（IP アドレス 172.16.10.0～172.16.10.255 の範囲）を表しています。最初の例では、ネットマスクをマスク長（ビット数）で表しています。一方 2 番目の例では、ネットマスクを IP アドレスと同じ形式で表しています。どちらも同じ意味ですが、（文字数が少ないためか）どちらかというと最初の例のほうがよく使われています。
このように、ナチュラルサブネットマスク（クラス A、B、C）にこだわらないネットワークの設定方法を「CIDR」（Classless Inter-Domain Routing）と呼びます。
RFC1519, Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
CIDR は、限られた IP アドレスを効率的に割り当てるため、また、次に述べる経路集約によってインターネット上の経路数を少なくするために役立っています。

経路集約

経路集約とは、複数のプレフィックスを 1 つのプレフィックスにまとめることを言います。たとえば、172.16.0.0/24、172.16.1.0/24、172.16.2.0/24～172.16.255.0/24 という 256 個のプレフィックスは、172.16.0.0/16 という 1 個のプレフィックスに集約することができます。
経路情報を適切に集約することで、ネットワーク全体に通知される経路エントリーの数を減らし、経路制御にかかる負荷を軽減することができます。

BGP スピーカー

BGP-4 の仕様では、BGP-4 実装機器を BGP スピーカー（BGP speaker）と呼んでいます。BGP スピーカーは通常ルーターですが、経路情報を配布できるのであれば通常のホストであってもかまいません。
BGP スピーカーは、それぞれ BGP 識別子（BGP Identifier）という値を持ちます。BGP 識別子は 32 ビットの符号なし整数値で、通常は自身の IP アドレスの 1 つを使います（例：10.10.10.1）。

BGP セッション

BGP-4 は TCP 上で動作するため、必ず 2 つの BGP スピーカー間でセッションを張ることになります。互いにセッションを張っている BGP スピーカーを「BGP ピア」と呼びます。また、BGP セッションを張って経路情報を交換することを「ピアリングする」などと呼ぶこともあります。
異なる AS に属するスピーカー同士のセッションを E-BGP（External BGP）、同じ AS に属するスピーカー同士のセッションを I-BGP（Internal BGP）と呼びます。
E-BGP は AS 間で経路情報を交換するためのセッション、I-BGP は他 AS から学習した経路情報を同一 AS 内の他のスピーカーに伝えるためのセッションです。
E-BGP と I-BGP は原則的に同じ動作ですが、学習した経路を他の BGP ピアに再通知するときのルールに違

いがあります。BGP スピーカーは、ある I-BGP ピアから学習した経路を別の I-BGP ピアに通知することができません。これは AS 内における経路情報のループを防ぐためです。I-BGP で学習した経路を E-BGP ピアに通知すること、E-BGP ピアから学習した経路を I-BGP で通知することは問題ありません。
このような制限があるため、BGP スピーカーは同一 AS に所属する他のすべての BGP スピーカーとセッションを張る必要があります。結果として AS 内にはメッシュ状に I-BGP セッションが張られることになります。メッシュ構成の煩雑さを避けるための手段として「ルートリフレクション」や「AS コンフェデレーション」があります。

BGP メッセージ

BGP-4 メッセージは TCP を使って送信されます。TCP ポート番号は 179 です。
BGP-4 のメッセージには以下の種類があります。

タイプ	メッセージ名	説明
1	OPEN	BGP セッションを開始するためのメッセージ。ルーター間に TCP コネクションが確立した直後に送られる。各ルーターの所属 AS を通知しあったり、タイマー値のネゴシエーションを行ったりする
2	UPDATE	経路情報の通知に使うメッセージ。新規プレフィックスの通知や無効になったプレフィックスの取り消し依頼などを相手に通知する
3	NOTIFICATION	プロトコル上のエラーを相手に通知するためのメッセージ。BGP セッションの終了通知にも使われる
4	KEEPALIVE	BGP セッションが有効であることを確認するためのメッセージ。定期的に送信される
5	ROUTE-REFRESH	BGP ピアに対し、すべての経路情報を送信しなおすよう要求するためのメッセージ（RFC2918 による拡張）

表 7:

パス属性

BGP-4 では、UPDATE メッセージで送信される経路情報にさまざまな情報を付加することができます。この付加情報をパス属性と呼びます。属性はポリシールーティングの基礎となる情報を相手に提供します。属性には以下の種類があります。

タイプ	属性名	種類	説明
1	ORIGIN	well-known mandatory	プレフィックスがどのようにして BGP に取り込まれたかを示す
2	AS_PATH	well-known mandatory	プレフィックスがどのような経路をたどって通知されてきたかを示す

3	NEXT_HOP	well-known mandatory	プレフィックス宛トラフィックのネクストホップアドレスを示す
4	MULTI_EXIT_DISC	optional non-transitive	隣接 AS と複数点で接続している場合に、特定プレフィックス宛トラフィックの NEXTHOP としてどちらが適切であるかを（隣接 AS に対して）示す一種のメトリック（コスト）。小さいほどコストが低い（優先度が高い）
5	LOCAL_PREF	well-known discretionary	AS 内における（I-BGP）経路選択のための優先度。大きいほど優先度が高い
6	ATOMIC_AGGREGATE	well-known discretionary	プレフィックスが集約されたものであることを示す
7	AGGREGATOR	optional transitive	プレフィックスを集約した AS および BGP スピーカーの BGP 識別子を示す
8	COMMUNITIES	optional transitive	コミュニティーを示す（RFC1997 による拡張属性）
9	ORIGINATOR_ID	optional non-transitive	該当経路を最初に学習した I-BGP ピアの BGP 識別子（ルーター ID）を示す。ルートリフレクション使用時に経路情報のループを防ぐために使われる（RFC2796 による拡張属性）
10	CLUSTER_LIST	optional non-transitive	AS 内における該当経路のリフレクトパスを示す。ルートリフレクターは、経路を再通知（リフレクト）するときに自身のクラスター ID（CLUSTER_ID）を本属性に付加する。ルートリフレクション使用時に経路情報のループを防ぐために使われる（RFC2796 による拡張属性）

表 8: BGP 属性の種類

以下、おもなパス属性について説明します。

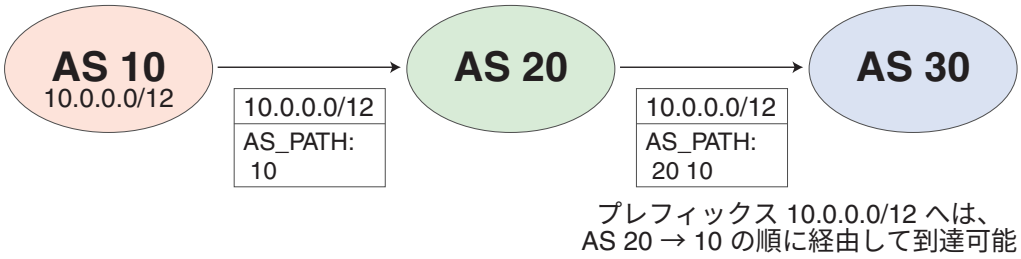
AS_PATH

AS_PATH（AS パス）とは、あるプレフィックスの経路情報がどの AS をどんな順番で経由してきたのかを示す AS 番号のリストです。

たとえば、次の図では AS 10 が「10.0.0.0/12」というプレフィックスを他の AS に通知しています。AS 10 は同プレフィックスの AS_PATH 属性に「10」をセットして AS 20 に通知します。

AS 20 から見ると、プレフィックス 10.0.0.0/12 へは、AS 10 経由で到達できるという意味になります。次に AS 20 は、同プレフィックスの AS_PATH 属性に自 AS 番号を追加し、「20 10」として AS 30 に通知します。

AS 30 から見ると、プレフィックス 10.0.0.0/12 へは、AS 20、AS 10 の順番に経由して到達できるという意味になります。



一般的に、AS_PATH 属性は「30 20 10」のように表します。「30」「20」「10」はいずれも AS 番号を示します。先ほどの例にもあるように、リストの末尾（右端）がプレフィックスの通知元（起源 AS）、リストの先頭（左端）が直前の AS となります。

BGP スピーカーは、あるプレフィックスへの経路が複数ある場合、AS_PATH の短い経路を優先します。この仕組みを利用し、自 AS に向かうトラフィックを操作することもできます。たとえば、自 AS 内のプレフィックスを通知するときに、AS_PATH 属性に自 AS 番号を複数回含めることがあります。こうすることにより、AS_PATH を長くし、他 AS にとって該当経路の優先度を引き下げさせることができます。

AS_PATH は、経路情報のループを検出するためにも使用されます。BGP スピーカーは、受信した経路情報のうち、AS_PATH に自 AS 番号を含むものを受け取らずに破棄します。これによりループを防いでいます。

MULTI_EXIT_DISC

MULTI_EXIT_DISC（MED = MULTI-EXIT DISCRIMINATOR）属性は、隣接 AS と複数点で接続している場合に、特定プレフィックスへの NEXT HOP としてどちらの接続点がより望ましいかを通知するために使用する一種のメトリック（コスト指標）です。

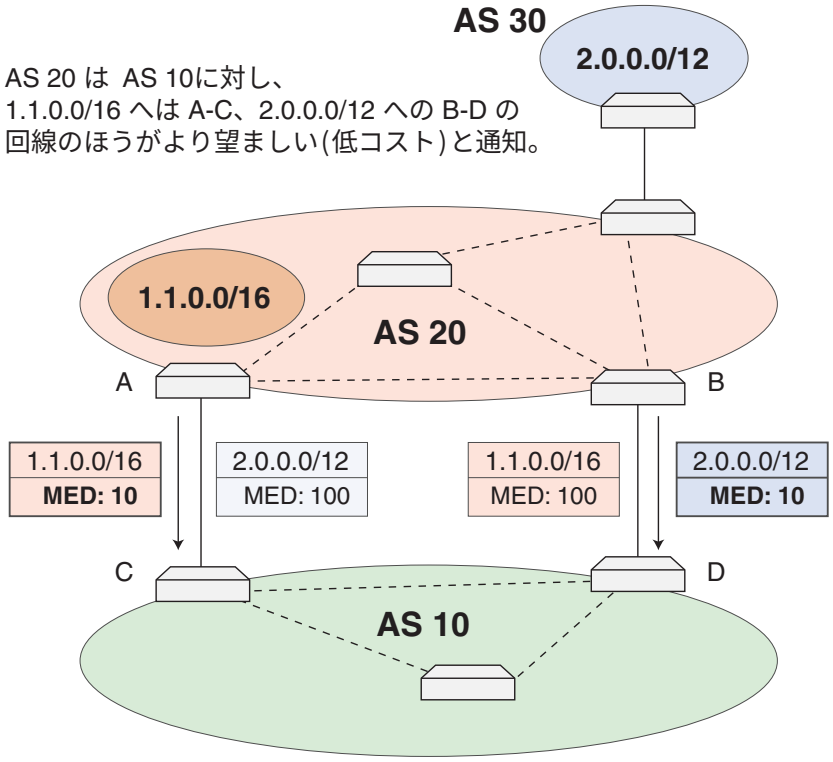
次の図では、AS 20 が AS 10 に対して 2 つのプレフィックス「1.1.0.0/16」と「2.0.0.0/12」を通知しようとしています。

AS 20 と AS 10 は A-C、B-D という 2 つの回線で接続しています。ここで、AS 20 は AS 10 に対し、

「1.1.0.0/16」宛てのトラフィックは A-C 経由で、「2.0.0.0/12」宛てのトラフィックは B-D 経由で送ってほしいと考えています。そのほうが AS 20 内での配送コストが低いためです。MED 属性はこのような場合に使います。

MED 属性は小さい値ほどコストが低いことを示します。そのため、AS 20 は AS 10 にプレフィックスを通知するにあたり、「1.1.0.0/16」の MED 属性は A-C のほうが小さくなるようにし、「2.0.0.0/12」の MED 属性は B-D のほうが小さくなるようにします。

これにより、AS 10 で MED 属性を考慮するポリシーが運用されていれば、AS 20 の意図通り、「1.1.0.0/16」宛てのトラフィックは A-C 経由で、「2.0.0.0/12」宛てのトラフィックは B-D 経由で AS 20 に送信されることになります。



本製品は、デフォルトでは経路情報に MED 属性を含めません。しかし、後述するルートマップを使えば、特定の経路に任意の MED 値を設定することができます。

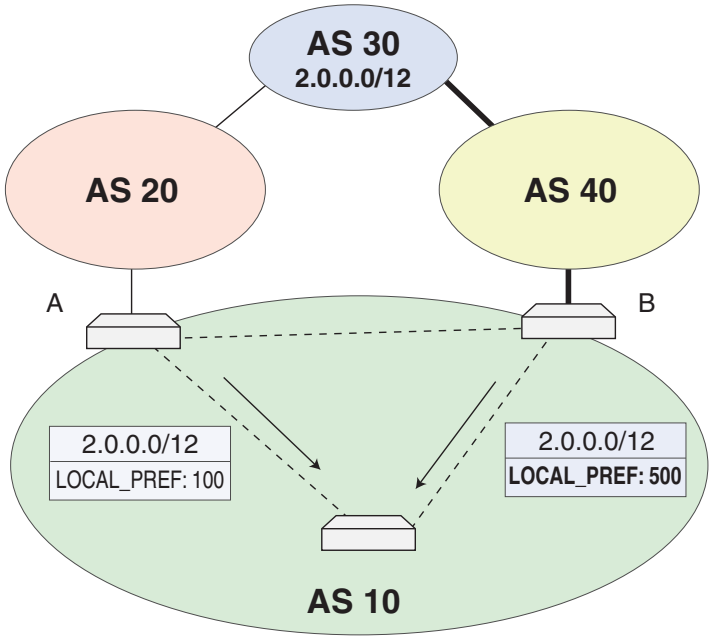
LOCAL_PREF

LOCAL_PREF 属性は、1 つの AS 内部において、特定プレフィックスへの経路としてどれがもっとも望ましいかを選択するための優先度です。複数の AS と接続しているなど、あるプレフィックス宛ての経路が複数存在する場合に使用します。

たとえば次の図では、AS 10 からプレフィックス「2.0.0.0/12」への経路として、AS 20 経由と AS 40 経由の 2 通りがあります。

ここで、AS 10 では AS 40 経由のほうが回線が太いなど条件がよいことを知っているとします。このような場合、AS 10 ではルーター A、B に設定を施し、プレフィックス「2.0.0.0/12」の LOCAL_PREF 属性値を B

のほうが高くなるよう設定することで、「2.0.0.0/12」宛ての経路としてルーター B 側を使うようにできます。

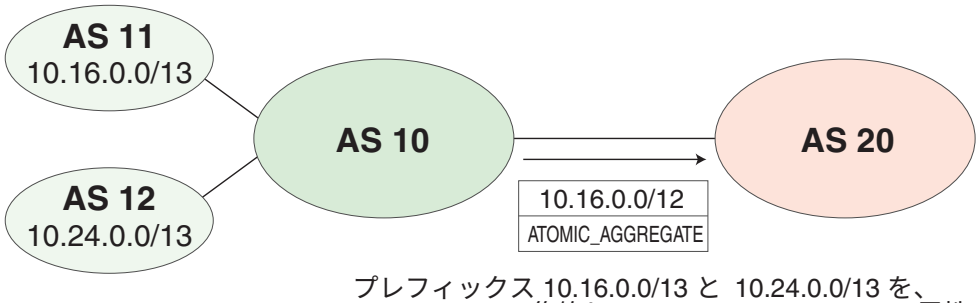


AS 10 では、2.0.0.0/12 への経路として、AS 20 経由と AS 40 経由の 2 通りあるが、AS 40 経由のほうが望ましいことを知っている。
このことをAS 10内に周知するため、2.0.0.0/12 宛て経路の LOCAL_PREF を B のほうが高くなるよう設定し、I-BGPにのせている。

本製品は、I-BGP セッションにおけるデフォルト LOCAL_PREF 値として 100 を通知します。後述するルートマップを使えば、特定の経路情報に任意の LOCAL_PREF 値を設定することも可能です。

ATOMIC_AGGREGATE

ATOMIC_AGGREGATE 属性は、プレフィックスが集約されたものであることを示すフラグ属性（「あり」か「なし」だけが意味を持つ属性）です。



プレフィックス 10.16.0.0/13 と 10.24.0.0/13 を、10.16.0.0/12 に集約し、ATOMIC_AGGREGATE 属性付きで AS 20 に通知

経路情報が ATOMIC_AGGREGATE 属性付きで通知された場合、通知されたプレフィックスに含まれる特定のプレフィックスへの経路が AS_PATH とは異なることがあります。

COMMUNITIES

COMMUNITIES 属性は、BGP-4 のポリシー運用を簡略化するために追加された属性です。共通の性質を持つプレフィックスを「コミュニティー」にグループ化し、コミュニティー単位でポリシー制御を行うことを目的としています。
「コミュニティー」は 32 ビットの整数値で表します。コミュニティー値の意味は各 AS が独自に定義できます。たとえば、コミュニティー「100」はトランジットさせる経路、コミュニティー「200」はトランジットさせない経路、といった使い方ができます。慣例として、コミュニティーの前半 16 ビットは自 AS 番号、後半 16 ビットは自 AS 内でのコミュニティー識別子とします。この場合、読みやすさを考慮して「65001:100」といった表記がよく使われます。
デフォルトでは、すべてのプレフィックスが「インターネット」コミュニティーに所属していると仮定されます。また、0x00000000～0x0000FFFF（0:0～0:65535）の範囲と、0xFFFF0000～0xFFFFFFFF（65535:0～65535:65535）の範囲は予約済みとなっています。
また、定義済みの特殊なコミュニティー（Well-known Communities）として次のものが定義されています。

- NO_EXPORT（0xFFFFFF01）：NO_EXPORT コミュニティーに属する経路情報を受け取った場合、その経路を他の AS（正確には AS コンフェデレーション）に再通知してはならない。
- NO_ADVERTISE（0xFFFFFF02）：NO_ADVERTISE コミュニティーに属する経路情報を受け取った場合、その経路を他の BGP スピーカーに再通知してはならない。
- NO_EXPORT_SUBCONFED（0xFFFFFF03）：NO_EXPORT_SUBCONFED コミュニティーに属する経路情報を受け取った場合、その経路を他の AS（同一 AS コンフェデレーション内の他のメンバー AS も含む）に再通知してはならない。

本製品では、ルートマップを使って、特定の経路情報に任意のコミュニティー値を設定することができます。

設定手順

BGP-4 を設定するための基本的な手順について説明します。具体的な設定例については、次項「基本設定」をご覧ください。

1. 自 AS 番号を設定します。

   ```
   SET IP AUTONOMOUS=65001 ↵
   ```

2. 接続相手の BGP スピーカー（BGP ピア）を指定します。相手の IP アドレスと相手の所属 AS 番号を指定してください。REMOTEAS が自 AS と同じなら I-BGP、違うなら E-BGP ピアとなります。

   ```
   ADD BGP PEER=10.10.10.2 REMOTEAS=65002 ↵
   ```

3. 自らが提供する経路情報を設定します。たとえばインターフェース（ダイレクト）経路と静的経路を BGP で広報したいときは次のようにします。

   ```
   ADD BGP IMPORT=INTERFACE ↵
   ADD BGP IMPORT=STATIC ↵
   ```

   広報するプレフィックスを明示的に指定したいときは、ADD BGP IMPORT コマンド（152 ページ）

でなく ADD BGP NETWORK コマンド（153 ページ）で該当プレフィックスを指定します。

```
ADD BGP NETWORK=192.168.10.0/24 ↵
```

4. BGP ピアとのセッションを開始します。

```
ENABLE BGP PEER=10.10.10.2 ↵
```

設定項目

BGP-4 のおもな設定項目について説明します。

■ 自 AS 番号の設定は SET IP AUTONOMOUS コマンド（355 ページ）を使います。

```
SET IP AUTONOMOUS=65001 ↵
```

■ 本製品のデフォルト動作では、インターフェースに設定された IP アドレスの中でもっとも大きなものが BGP 識別子（ルーター ID）として使われます。ただし、SET BGP コマンド（335 ページ）の ROUTERID パラメーターでルーター ID を明示的に指定した場合はその値が使われます。また、明示的に指定していない場合でも、SET IP LOCAL コマンド（367 ページ）でデフォルトローカル IP インターフェース（LOCAL）のアドレスを指定している場合は、そのアドレスがルーター ID として使われます。

- ルーター ID を明示的に指定するには、SET BGP コマンド（335 ページ）の ROUTERID パラメーターを使います。ROUTERID パラメーターが設定されている場合は、この値がルーター ID として使われます。

  ```
  SET BGP ROUTERID=10.1.1.1 ↵
  ```

- SET BGP コマンド（335 ページ）の ROUTERID パラメーターが設定されていない場合、SET IP LOCAL コマンド（367 ページ）でデフォルトローカル IP インターフェース（LOCAL）のアドレスを指定していれば、その値がルーター ID として使われます。デフォルトローカル IP インターフェースのアドレスには、実インターフェースに設定されている IP アドレスのうちの 1 つを指定します。

  ```
  SET IP LOCAL IP=10.10.10.1 ↵
  ```

- 上記の方法でルーター ID が指定されていない場合は、インターフェースに設定された IP アドレスの中でもっとも大きなものが BGP 識別子（ルーター ID）として使われます。

■ BGP ピアの指定は ADD BGP PEER コマンド（154 ページ）で行います。PEER にピアの IP アドレスを、REMOTEAS にピアの所属 AS を指定してください。REMOTEAS と自 AS 番号が違うなら E-BGP ピア（外部ピア）、同じなら I-BGP ピア（内部ピア）となります。ピアを追加した直後は無効（IDLE）状態です。その他の設定を行った後、ENABLE BGP PEER コマンド（291 ページ）でセッションを開始してください。

```
ADD BGP PEER=10.10.10.2 REMOTEAS=65002 ↵
```

■ BGP ピアの有効・無効（BGP セッションの開始・切断）は ENABLE BGP PEER コマンド（291 ページ）、DISABLE BGP PEER コマンド（261 ページ）で行います。ADD BGP PEER コマンド（154 ページ）で追加したばかりのピアは無効状態であり、ENABLE BGP PEER コマンド（291 ページ）を実行するまでセッションは張られません。

```
ENABLE BGP PEER=10.10.10.2 ↵
ENABLE BGP PEER=ALL ↵
```

■ BGP ピア固有の設定パラメーターは SET BGP PEER コマンド（343 ページ）で変更します。ピア固有のパラメーターは、該当ピアとセッションを張っていない状態（無効状態）でしか変更できません。ADD BGP PEER コマンド（154 ページ）でピアを追加した直後は無効状態なので、そのまま SET BGP PEER コマンド（343 ページ）による設定が行えます。すでにセッションを開始している場合は、DISABLE BGP PEER コマンド（261 ページ）でいったん切断し、設定を変更した後に ENABLE BGP PEER コマンド（291 ページ）でセッションを再開してください。

```
DISABLE BGP PEER=10.10.10.2 ↵
SET BGP PEER=10.10.10.2 OUTPATHFILTER=1 ↵
ENABLE BGP PEER=10.10.10.2 ↵
```

■ BGP のグローバル設定パラメーターは、SET BGP コマンド（335 ページ）で変更できます。たとえば、E-BGP セッションで通知する経路のデフォルト MED 値を 10 にするには、次のようにします。なお、本製品はデフォルトでは MED 属性を付加しません。

```
SET BGP MED=10 ↵
```

■ BGP プロセスに導入する経路情報は ADD BGP IMPORT コマンド（152 ページ）で指定します。インターフェース（ダイレクト）経路、静的経路、RIP 経路、OSPF 経路のそれぞれについて、取り込み時にルートマップによる属性設定が可能です。

```
ADD BGP IMPORT=INTERFACE ↵
ADD BGP IMPORT=STATIC ↵
ADD BGP IMPORT=RIP ROUTEMAP=set_rip_attr ↵
```

■ 経路情報のソースではなく、プレフィックスによって BGP への導入を指定することもできます。ADD BGP NETWORK コマンド（153 ページ）でプレフィックスを指定してください。ルートマップを指定することによって、取り込み時の属性設定も可能です。

```
ADD BGP NETWORK=172.16.0.0/16 ↵
ADD BGP NETWORK=10.0.0.0/12 ROUTEMAP=set_ten_net ↵
```

ADD BGP NETWORK コマンド（153 ページ）で指定したプレフィックスは、静的設定や RIP、OSPF などにより同一のプレフィックスがルーターの経路表に登録された場合に、BGP 経路表に取り込まれます。

■ 経路情報を集約したいときは、ADD BGP AGGREGATE コマンド（149 ページ）を使います。同コマンドで指定したプレフィックスよりも狭い経路（マスクが長い経路）がルーターの BGP 経路表に現れた場合、BGP 経路表に集約された経路も登録されます。SUMMARY パラメーターに YES を指定した場合は集約経路のみが残り、NO を指定した場合は集約経路と個々の経路の両方が BGP 経路表に残ります。集約経路の取り込み時に適用するルートマップを指定することもできます。

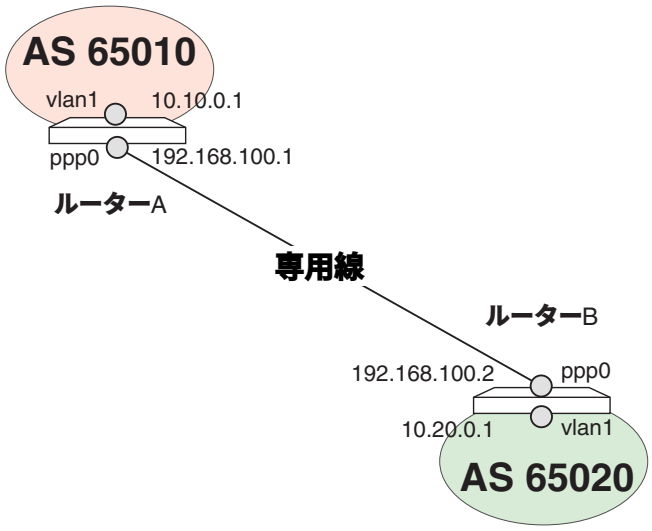
```
ADD BGP AGGREGATE=10.0.0.0/12 SUMMARY=YES ↵
ADD BGP AGGREGATE=172.16.0.0/12 SUMMARY=YES ROUTEMAP=set_aggr_attr ↵
```

■ AS コンフェデレーションの設定は SET BGP コマンド（335 ページ）の CONFEDERATIONID パラメーターでコンフェデレーション AS 番号を、ADD BGP CONFEDERATIONPEER コマンド（151 ページ）で同じコンフェデレーションに所属するピアのサブ AS（メンバー AS）番号を指定します。ADD BGP CONFEDERATIONPEER コマンド（151 ページ）で指定するのは、直接セッションを張っているピアのサブ AS 番号だけです。コンフェデレーションに所属するすべてのサブ AS を指定する必要はありません。また、コンフェデレーション AS を構成するときは、自 AS 番号としてサブ AS 番号（メンバー AS 番号）を設定します。
たとえば、自分のサブ AS 番号が 65001、コンフェデレーション AS 番号が 65000、コンフェデレーション EBGP（C-EBGP）ピア 192.168.10.2 のサブ AS 番号が 65002 の場合、次のように設定します。

```
SET IP AUTONOMOUS=65001 ↵
SET BGP CONFEDERATIONID=65000 ↵
ADD BGP PEER=192.168.10.2 REMOTEAS=65002 ↵
ADD BGP CONFEDERATIONPEER=65002 ↵
ADD BGP IMPORT=INTERFACE ↵
ADD BGP IMPORT=STATIC ↵
ENABLE BGP PEER=192.168.10.2 ↵
```

基本設定

シンプルな BGP-4 ネットワークの設定例を示します。ここでは、次のようなネットワーク構成を例に解説します。



ルーター A の設定

1. 専用線と PPP の設定を行います。

```
SET BRI=0 MODE=TDM ACTIVATION=ALWAYS TDMSLOTS=1-2 ↵
CREATE TDM GROUP=remote INT=bri0 SLOTS=1-2 ↵
CREATE PPP=0 OVER=TDM-remote ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. 各インターフェースに IP アドレスを割り当てます。

```
ADD IP INT=vlan1 IP=10.10.0.1 MASK=255.255.255.0 ↵
ADD IP INT=ppp0 IP=192.168.100.1 MASK=255.255.255.0 ↵
```

4. LAN 側（vlan1）インターフェースで RIP2 を有効にします。

```
ADD IP RIP INT=vlan1 SEND=RIP2 RECEIVE=RIP2 ↵
```

5. 自 AS 番号を設定します。

```
SET IP AUTONOMOUS=65010 ↵
```

6. BGP ピアを指定します。

```
ADD BGP PEER=192.168.100.2 REMOTEAS=65020 ↵
```

7. BGP で通知する経路情報を指定します。ここでは静的経路と RIP 経由で学習した経路を相手に通知します。

```
ADD BGP IMPORT=STATIC ↵
ADD BGP IMPORT=RIP ↵
```

8. BGP ピアとのセッションを開始します。

```
ENABLE BGP PEER=192.168.100.2 ↵
```

ルーター B の設定

1. 専用線と PPP の設定を行います。

```
SET BRI=0 MODE=TDM ACTIVATION=ALWAYS TDMSLOTS=1-2 ↵
CREATE TDM GROUP=remote INT=bri0 SLOTS=1-2 ↵
CREATE PPP=0 OVER=TDM-remote ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. 各インターフェースに IP アドレスを割り当てます。

```
ADD IP INT=vlan1 IP=10.20.0.1 MASK=255.255.255.0 ↵
ADD IP INT=ppp0 IP=192.168.100.2 MASK=255.255.255.0 ↵
```

4. LAN 側（vlan1）インターフェースで RIP2 を有効にします。

```
ADD IP RIP INT=vlan1 SEND=RIP2 RECEIVE=RIP2 ↵
```

5. 自 AS 番号を設定します。

```
SET IP AUTONOMOUS=65020 ↵
```

6. BGP ピアを指定します。

```
ADD BGP PEER=192.168.100.1 REMOTEAS=65010 ↵
```

7. BGP で通知する経路情報を指定します。ここでは静的経路と RIP 経由で学習した経路を相手に通知

します。

```
ADD BGP IMPORT=STATIC ↵
ADD BGP IMPORT=RIP ↵
```

8. BGP ピアとのセッションを開始します。

```
ENABLE BGP PEER=192.168.100.1 ↵
```

設定は以上です。

■ 経路表を確認するには、SHOW IP ROUTE コマンド（473 ページ）を使います。

```
SHOW IP ROUTE ↵
```

■ BGP ピアの状態は SHOW BGP PEER コマンド（418 ページ）で確認します。

```
SHOW BGP PEER ↵
SHOW BGP PEER=192.168.100.2 ↵
```

■ BGP-4 の経路表を確認するには、SHOW BGP ROUTE コマンド（425 ページ）を使います。

```
SHOW BGP ROUTE ↵
```

■ BGP-4 の設定情報を確認するには SHOW BGP コマンド（399 ページ）を使います。

```
SHOW BGP ↵
```

■ 本製品は BGP4-MIB をサポートしています。SNMP の設定をしておけば、ネットワーク管理ステーションから BGP に関する MIB 情報を引き出すことができます。SNMP の設定については、「運用・管理」の「SNMP」をご覧ください。

経路のフィルタリング

BGP-4 の運用においては、どの経路情報を受け入れるかといったフィルタリング機能、また、特定の経路情報に付加的情報を追加するポリシー設定機能が重要な意味を持ちます。本製品の BGP-4 実装には、次に示すフィルタリング/ポリシー設定機能が用意されています。

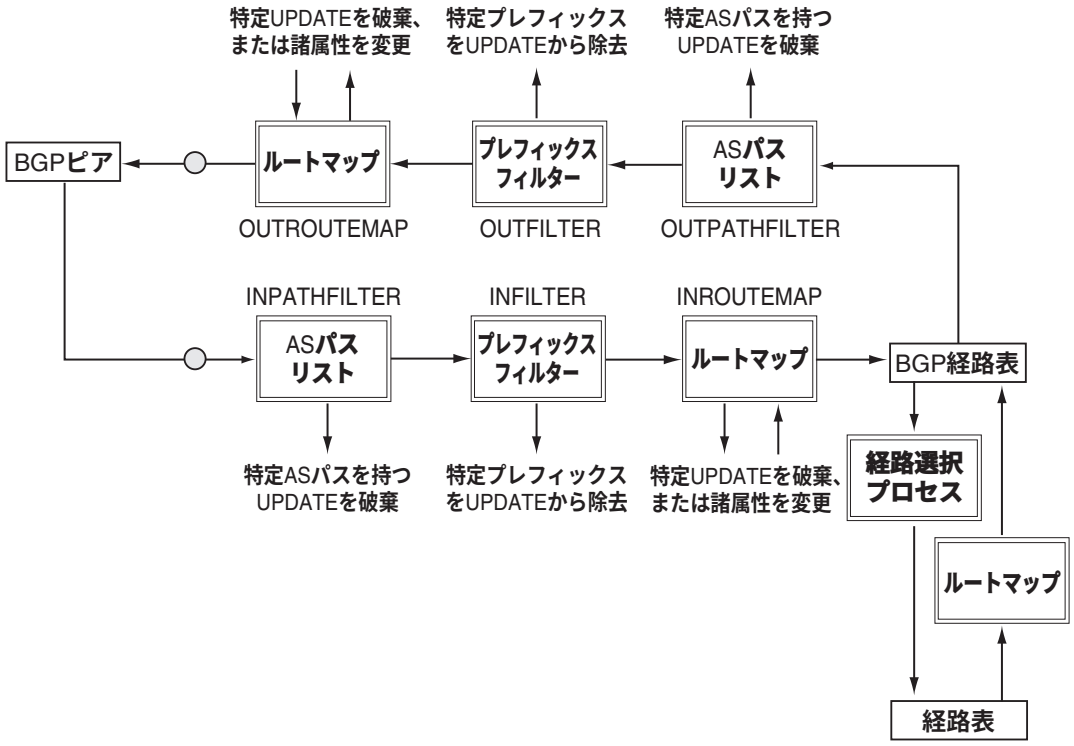
名称	比較対象	単独使用	MATCH 節	許可・破棄	属性設定	備考
AS パスリスト	AS_PATH 属性	○	○	○	△	ADD IP ASPATHLIST コマンドで作成。単独使用時は、ADD BGP PEER コマンドの INPATHFILTER、OUTPATHFILTER で指定。マッチ条件として使うときは、ADD IP ROUTEMAP コマンドの MATCH ASPATH で指定
プレフィックスフィルター	プレフィックス	○	×	○	×	ADD IP FILTER コマンドで作成。ADD BGP PEER コマンドの INFILTER、OUTFILTER で指定
コミュニティーリスト	COMMUNITIES 属性	○	○	△	△	ADD IP COMMUNITYLIST コマンドで作成。ADD IP ROUTEMAP コマンドの MATCH COMMUNITY で指定
ルートマップ	各種（後述）	○	×	○	○	ADD IP ROUTEMAP コマンドで作成。ADD BGP PEER コマンドの INROUTEMAP、OUTROUTEMAP で指定

表 9:

記号で示されている各欄の意味は次のとおりです（○ = 可能。△ = ルートマップと併用することで可能。× = 不可能）。

- 「単独使用」: 該当機能を単独で使用できるかどうか
- 「MATCH 節」: 該当機能をルートマップのマッチ条件として使用できるかどうか。
- 「許可・破棄」: 該当機能で経路情報のフィルタリング（許可・破棄）が可能かどうか。
- 「属性設定」: 該当機能で経路情報の属性設定が可能かどうか。

✎ フィルタリングにおける「許可」とは、他のルーターから受信した経路情報を受け入れること、また、他のルーターに経路情報を通知することを意味しています。同様に「拒否」とは、他のルーターから受信した経路情報を受け入れずに破棄すること、また、他のルーターに特定の経路情報を通知しないことを意味します。



また、BGP 経由で学習した経路をルーターの経路表に取り込むときにも、一定の基準にしたがって経路の選択が行われます。

経路選択プロセス

BGP-4 経由で学習した経路情報の中には、同じプレフィックスを持つものが複数存在する可能性があります。一般的にこれは、該当プレフィックス宛ての経路が複数あることを意味しますが、この場合どの経路をルーターの経路表に取り入れるかが重要になってきます。
あるプレフィックスへの経路が 1 つしか存在しない場合は、その経路を使用します。しかし、複数の経路が存在する場合は、次の流れにしたがって 1 つの経路に絞ります。

1. LOCAL_PREF 属性の大きい経路を優先。
   E-BGP 経由で学習した経路や IGP・静的設定で学習した経路の場合は、自ら計算した値を用いる。
   I-BGP 経由で学習した経路の場合は、LOCAL_PREF 属性の値を用いる。
2. 経路のソース（起源）。次の順序で優先。
   (1) 手動で取り込んだ経路
   (2) 集約経路エントリーから学習した経路
   (3) その他の方法で学習した経路（I-BGP ピア、E-BGP ピア、コンフェデレーション E-BGP ピア（C-BGP ピア））
3. AS_PATH 属性の短い経路を優先。
4. ORIGIN 属性。次の順序で優先。
   (1) IGP
   (2) EGP

(3) INCOMPLETE
5. MULTI_EXIT_DISC 属性の小さい経路を優先。
6. AS_PATH 属性の内容。次の順序で優先。
   (1) AS_PATH 属性に外部の AS 番号だけが含まれている経路
   (2) AS_PATH 属性に AS コンフェデレーションの AS 番号が含まれている経路
7. NEXT_HOP 属性へのコストが小さい経路を優先。
8. 学習元 BGP ピアのルーター ID が小さい経路を優先。
9. CLUSTER_LIST 属性の短い経路を優先。
10. 学習元 BGP ピアの IP アドレス（BGP セッションで使用しているアドレス）が小さい経路を優先。

AS パスリスト

AS パスリストは、UPDATE メッセージの AS_PATH 属性に基づいて、経路情報を許可するか拒否するかを決定するフィルターです。
この機能を使うと、特定の AS 経由で通知された経路情報を送受信しないよう設定したり、特定の AS を起源とする経路情報を送受信しないよう設定したりすることができます。
また、AS パスリストをルートマップと組み合わせることにより、特定の AS 経由で通知された経路情報の属性を変更して、なんらかの「経路制御ポリシー」を与えることもできます。
AS パスリストは、ADD IP ASPATHLIST コマンド（163 ページ）で作成し、ADD BGP PEER コマンド（154 ページ）、SET BGP PEER コマンド（343 ページ）の INPATHFILTER、OUTPATHFILTER パラメーターで BGP ピアごとに適用します。また、ルートマップと併用する場合は、ADD IP ROUTEMAP コマンド（195 ページ）の MATCH ASPATH パラメーターでルートマップエントリーの選別条件として指定します。

■ E-BGP ピア「10.10.10.2」に対し、自 AS 起源の経路（ローカル経路）だけを通知するには、次のようにします。

1. AS パスリスト「1」を作成し、AS_PATH 属性が空の UPDATE メッセージだけを許可するエントリーを追加します。1 つでもエントリーを持つ AS パスリストは、末尾にすべて破棄の暗黙のエントリーが存在するため、この例では AS パスが空でない UPDATE はすべて破棄されます。

   ```
   ADD IP ASPATHLIST=1 INCLUDE="^$" ↵
   ```

2. BGP ピア「10.10.10.2」（所属 AS は 65002）を追加します。OUTPATHFILTER パラメーターに AS パスリスト「1」を指定し、AS パスが空の UPDATE メッセージ（ローカル経路）だけを送信するよう設定します。

   ```
   ADD BGP PEER=10.10.10.2 REMOTEAS=65002 OUTPATHFILTER=1 ↵
   ```

■ E-BGP ピア「10.10.10.2」との BGP セッションにおいて、AS 65100 を起源とする UPDATE メッセージを受信しないよう設定するには、次のようにします。

1. AS パスリスト「1」を作成し、AS_PATH 属性の末尾が「65100」の UPDATE メッセージを拒否す

るエントリーを追加します（AS_PATH 属性は UPDATE メッセージが通過してきた AS のリストで、リストの末尾（右端）に起源 AS が置かれます）。

```
ADD IP ASPATHLIST=1 EXCLUDE="65100$" ↵
```

2. AS パスリスト「1」にすべての UPDATE メッセージを許可するエントリーを追加します。1 つでもエントリーを持つ AS パスリストは、末尾にすべて破棄の暗黙のエントリーが存在するので注意してください。

```
ADD IP ASPATHLIST=1 INCLUDE=".*" ↵
```

3. BGP ピア「10.10.10.2」（所属 AS は 65002）を追加します。INPATHFILTER パラメーターに AS パスリスト「1」を指定し、該当ピアから受信した UPDATE メッセージのうち、AS「65100」を起源とするものだけは受け取らないよう設定します。

```
ADD BGP PEER=10.10.10.2 REMOTEAS=65002 INPATHFILTER=1 ↵
```

■ AS パスリストでは、UPDATE メッセージに含まれる AS_PATH 属性とのマッチングに簡易的な正規表現（Regular Expression）を使用できます。正規表現とは、特殊文字（メタ文字）を使って文字列を一定の「パターン」として表すための表記法で、ファイル名指定に使う「ワイルドカード」といくらか似ています。正規表現には様々な方言がありますが、AS パスリストで使用できるのは AS パスの表現に特化した限定版です。

構成要素	意味	例
^	AS パスの先頭にマッチ	^65010（AS パスの先頭が 65010 のときにマッチ）
$	AS パスの末尾にマッチ	65100$（AS パスの末尾が 65100 のときにマッチ）
（スペース）	個々の AS を区切る	65001 65002（AS パスに「65001 65002」という並びが含まれればマッチ）
（AS 番号）	個々の AS を表す（単独の数字ではないことに注意）	65123（AS パスに AS「65123」が含まれていればマッチ）
.	任意の AS 番号にマッチ。*や+と組み合わせて使うことが多い	65010 . 65030（65010 と 65030 の間に任意の AS 番号がくる場合にマッチ）
*	直前の正規表現が 0 個以上続く場合に最長マッチ	.*（空の AS パスを含むすべての AS パスにマッチ）
+	直前の正規表現が 1 個以上続く場合に最長マッチ	.+（空でないすべての AS パスにマッチ）

表 10: AS パス正規表現の構成要素

✎ AS パス正規表現では、スペースとメタ文字を除き、AS 番号が最小単位となります。したがって、「1」という

正規表現は AS「1」にマッチしますが、AS「12」にはマッチしません。また、「.」という正規表現は AS「1」、「12」、「65001」のいずれにもマッチします。

以下、正規表現の例をいくつか示します。

- 空の AS パスにマッチ（例：「」のみ）

  ```
  ^$
  ```

- 空を含むすべての AS パスにマッチ（例：「」「65111」「65111 65222」など）

  ```
  .*
  ```

- 空でないすべての AS パスにマッチ（例：「65001」「65002 65003」など）

  ```
  .+
  ```

- AS を 1 つだけ含む AS パスにマッチ（例：「65001」「65002」など）

  ```
  ^.$
  ```

- AS を 2 つだけ含む AS パスにマッチ（例：「65001 65002」「65002 65100」など）

  ```
  ^.  .$
  ```

- 先頭が「65200」の AS パスにマッチ（例：「65200」「65200 65001 65002」など）

  ```
  ^65200
  ```

- 末尾が「65012」の AS パスにマッチ（例：「65012」「65001 65002 65012」など）

  ```
  65012$
  ```

- 末尾に「65300」、「65310」、「65330」をこの順番で含む AS パスにマッチ（例：「65300 65310 65330」「65100 65300 65310 65330」など）

  ```
  65300 65310 65330$
  ```

- AS「65110」だけからなる AS パスにマッチ（例：「65110」のみ）

  ```
  ^65110$
  ```

- AS「65300」を含む AS パスにマッチ（例：「65001 65300」「65300」など）

```
65300
```

- AS「65300」、「65310」、「65330」をこの順番で含む AS パスにマッチ（例：「65300 65310 65330」「65299 65300 65310 65330 65432」など）

```
65300 65310 65330
```

- AS「65300」、「65330」の間に任意の AS 番号が 1 つだけ入るパスにマッチ（例：「65300 65311 65330」など）

```
65300 .  65330
```

- AS「65300」、「65330」の間に 1 個以上の任意の AS 番号がくるパスにマッチ（例：「65300 65311 65330」「65300 65311 65324 65330」など）

```
65300 .+ 65330
```

■ AS パスリストの内容を表示するには、SHOW IP ASPATHLIST コマンド（433 ページ）を使います。

```
SHOW IP ASPATHLIST ↵
SHOW IP ASPATHLIST=1 ↵
```

■ 特定ピアとの BGP セッションに適用される AS パスリストの情報は、SHOW BGP PEER コマンド（418 ページ）で確認できます。「Filtering」セクションの「In path filter」（受信時）、「Out path filter」（送信時）をご覧ください。

```
SHOW BGP PEER=10.10.10.2 ↵
```

プレフィックスフィルター

プレフィックスフィルターは、UPDATE メッセージに含まれる宛先ネットワークプレフィックス（NLRI フィールドの内容）の値（プレフィックスのみ。プレフィックス長には関知しない）に基づいて、経路情報を許可するか拒否するかを決定するフィルターです。
この機能を使うと、特定のプレフィックス宛ての経路情報だけを受け取ったり、特定のプレフィックス宛ての経路情報だけを通知したりすることができます。
プレフィックスフィルターは、ADD IP FILTER コマンド（169 ページ）で作成（フィルター番号 300〜399）し、ADD BGP PEER コマンド（154 ページ）、SET BGP PEER コマンド（343 ページ）の INFILTER、OUTFILTER パラメーターで BGP ピアごとに適用します。

■「10.10.10.1」との BGP セッションにおいて、先頭が「172.20」のプレフィックスだけを通知するようにするには、次のようにします。これにより、自 AS 宛てでないトラフィックが自 AS に流れ込むことを防ぎます。

1. IP プレフィックスフィルター「300」を作成し、UPDATE メッセージの NLRI フィールドから、先頭が「172.20.0.0/16」のプレフィックスだけを許可し、それ以外は除去するように設定します。プレフィックスフィルターには、フィルター番号 300～399 を使います。

   ```
   ADD IP FILTER=300 SOURCE=172.20.0.0 SMASK=255.255.0.0
     ACTION=INCLUDE ↵
   ```

   SMASK パラメーターは、SOURCE パラメーターの指定値とプレフィックスを比較するときに、どの部分（ビット）を比較するか指定するものです。この例（SMASK=255.255.0.0）では、先頭 16 ビットを比較します。
   なお、先頭が「172.20」でないプレフィックスは、暗黙の拒否エントリーによりすべて除去（EXCLUDE）されます。
2. BGP ピア「10.10.10.1」（所属 AS は 65001）を追加します。OUTFILTER パラメーターにプレフィックスフィルター「300」を指定し、該当ピアに送信する UPDATE メッセージには「172.20」で始まるプレフィックスだけが含まれるようにします。

   ```
   ADD BGP PEER=10.10.10.1 REMOTEAS=65001 OUTFILTER=300 ↵
   ```

■「1.2.2.2」との BGP セッションにおいて、先頭が「172.16」のプレフィックスを受信しないよう設定するには、次のようにします。

1. IP プレフィックスフィルター「300」を作成し、UPDATE メッセージの NLRI フィールドから、先頭が「172.16」のプレフィックスを除去するエントリーを追加します。プレフィックスフィルターには、フィルター番号 300～399 を使います。

   ```
   ADD IP FILTER=300 SOURCE=172.16.0.0 SMASK=255.255.0.0
     ACTION=EXCLUDE ↵
   ```

   SMASK パラメーターは、SOURCE パラメーターの指定値とプレフィックスを比較するときに、どの部分（ビット）を比較するか指定するものです。この例（SMASK=255.255.0.0）では、先頭 16 ビットを比較します。
2. IP プレフィックスフィルター「300」にすべてのプレフィックスを通過させるエントリーを追加します。IP プレフィックスフィルターの末尾には、すべてのプレフィックスを除去する暗黙のエントリーが存在するので注意してください。

   ```
   ADD IP FILTER=300 SOURCE=0.0.0.0 ACTION=INCLUDE ↵
   ```

3. BGP ピア「1.2.2.2」（所属 AS は 65112）を追加します。INFILTER パラメーターにプレフィックス

フィルター「300」を指定し、該当ピアから受信したUPDATEメッセージから「172.16」で始まるプレフィックスを削除するよう設定します。

```
ADD BGP PEER=1.2.2.2 REMOTEAS=65112 INFILTER=300 ↵
```

■ IPプレフィックスフィルターの内容を表示するには、SHOW IP FILTERコマンド（449ページ）を使います。

```
SHOW IP FILTER ↵
SHOW IP FITLER=300 ↵
```

■ 特定ピアとのBGPセッションに適用されるIPプレフィックスフィルターの情報は、SHOW BGP PEERコマンド（418ページ）で確認できます。「Filtering」セクションの「In filter」（受信時）、「Out filter」（送信時）をご覧ください。

```
SHOW BGP PEER=10.10.10.1 ↵
```

■ プレフィックスフィルターは、経路エントリーの「プレフィックス長」には関知しません。経路エントリー「prefix」、「prefixlen」に対して、プレフィックスフィルター「SOURCE」、「SMASK」が存在する場合、(prefix & SMASK) == (SOURCE & SMASK) が真のときにマッチとなります（ここで「&」はビットごとのAND演算、「==」は等号を示す）。たとえば、SOURCE=192.168.10.0 SMASK=255.255.255.0のプレフィックスフィルターは、192.168.10.0/24、192.168.10.0/28、192.168.10.128/25のいずれにもマッチします。

■ プレフィックスフィルターの末尾には、すべてのプレフィックスを破棄（EXCLUDE）する暗黙のエントリーが存在するので注意してください。

コミュニティーリスト

コミュニティーリストは、UPDATEメッセージのCOMMUNITIES属性に基づいて、経路情報を許可するか拒否するかを決定するフィルターです。
COMMUNITIES属性は経路制御ポリシーを実施するために設けられた属性で、同じ性質を持つ経路をグループ化するために使用されます。
コミュニティーリストはルートマップと組み合わせて使用するもので、特定のCOMMUNITIES属性を持つ経路情報を受け取らないように設定したり、特定のCOMMUNITIES属性を持つ経路情報になんらかの「経路制御ポリシー」を与えるために使用できます。
コミュニティーリストは、ADD IP COMMUNITYLISTコマンド（165ページ）で作成し、ADD IP ROUTEMAPコマンド（195ページ）のMATCH COMMUNITYパラメーターでルートマップエントリーの選別条件として指定します。

■ コミュニティーリスト「1」を作成し、UPDATEメッセージのCOMMUNITIES属性にコミュニティー「65001:10000」が含まれている場合にマッチするよう設定する。

```
ADD IP COMMUNITYLIST=1 INCLUDE=65001:10000 ↵
```

✎ コミュニティーリストは、必ずルートマップと組み合わせて使用します。ADD IP COMMUNITYLIST コマンド（165 ページ）でリストを作成しただけでは、何も行われません。

ルートマップ

ルートマップは、さまざまな基準に基づいて経路を選別し、該当経路を許可・破棄したり、属性を書き換えたりするための機能です。おもに経路制御ポリシーを実施するために使用します。
ルートマップは、経路エントリーと照合するための MATCH 節（0〜1 個）、マッチ時のアクション（INCLUDE か EXCLUDE）、アクションが INCLUDE だった場合にマッチした経路の属性を変更するための SET 節（0〜複数個）からなります。
MATCH 節では、以下の情報を条件として使用できます。

- AS_PATH 属性（AS パスリストで指定）
- COMMUNITIES 属性（コミュニティーリストで指定）
- NEXT_HOP 属性
- ORIGIN 属性
- 静的経路に設定されたタグ値

また、SET 節では以下の情報を変更できます。

- AS_PATH 属性（AS 番号の追加）
- ルートフラップダンピング用のカスタムパラメーターセット
- COMMUNITIES 属性
- LOCALPREF 属性
- MED 属性
- ORIGIN 属性

ルートマップは ADD IP ROUTEMAP コマンド（195 ページ）で作成します。ルートマップの設定は、次のステップで行います。

1. （必要ならば）UPDATE メッセージを選別するための AS パスリスト、コミュニティーリストを作成します。
2. ルートマップエントリーを作成し、アクションを指定します。
3. 手順 2 で作成したエントリーに対し、MATCH 節を追加して条件を指定します。このとき、（必要に応じて）AS パスリストやコミュニティーリストの番号を指定します。なお、MATCH 節がないエントリーは、すべての経路にマッチします。
4. 手順 2 で作成したエントリーのアクションが INCLUDE の場合、（必要ならば）該当エントリーに SET 節を追加して属性変更の設定を追加します。

作成したルートマップは、次に示す箇所に適用することで初めて効果を発揮します。

- BGP ピアに経路を通知する直前（ADD BGP PEER コマンド（154 ページ）、SET BGP PEER コマンド（343 ページ）の OUTROUTEMAP パラメーター）
- BGP ピアから経路を受信した直後（ADD BGP PEER コマンド（154 ページ）、SET BGP PEER コマンド（343 ページ）の INROUTEMAP パラメーター）
- 経路を BGP に登録するとき（ADD BGP NETWORK コマンド（153 ページ）コマンドの ROUTEMAP パラメーター）
- 経路を集約するとき（ADD BGP AGGREGATE コマンド（149 ページ）、SET BGP AGGREGATE コマンド（336 ページ）の ROUTEMAP パラメーター）
- 静的経路や IGP 経路を BGP にインポートするとき（ADD BGP IMPORT コマンド（152 ページ）、SET BGP IMPORT コマンド（341 ページ）の ROUTEMAP パラメーター）
- BGP 経路をルーターの経路表に登録するとき（SET BGP コマンド（335 ページ）の TABLEMAP パラメーター）

以下、ルートマップのサンプルをいくつか示します。

■ コミュニティー値「65001:100」を設定するルートマップ「comm100」を作成します。エントリーは 1 個だけです。この例のように MATCH 節のないエントリーはすべてにマッチします。

```
ADD IP ROUTEMAP=comm100 ENTRY=1 ACTION=INCLUDE ↵
ADD IP ROUTEMAP=comm100 ENTRY=1 SET COMMUNITY=65001:100 ↵
```

ローカルプレフィックス「172.16.0.0/16」にコミュニティー値「65001:100」を設定するには、作成したルートマップを使って次のようにします。

```
ADD BGP NETWORK=172.16.0.0/16 ROUTEMAP=comm100 ↵
```

■ MED 値「1000」をセットするルートマップ「med1000」を作成します。エントリーは 1 個だけです。この例のように MATCH 節のないエントリーはすべてにマッチします。

```
ADD IP ROUTEMAP=med1000 ENTRY=1 ACTION=INCLUDE ↵
ADD IP ROUTEMAP=med1000 ENTRY=1 SET MED=1000 ↵
```

BGP ピア「10.2.1.1」（AS 番号 65020）に通知する経路すべてに MED 値「1000」を設定するには、作成したルートマップを使って次のようにします。

```
ADD BGP PEER=10.2.1.1 REMOTEAS=65020 OUTROUTEMAP=med1000 ↵
```

✎ すでに BGP ピアとセッションが張られている場合は、SET BGP PEER コマンド（343 ページ）の OUTROUTEMAP パラメーターでルートマップを指定し、その後 RESET BGP PEER コマンド（326 ページ）を SOFT パラメーター付きで実行してください（ソフトリセット）。なお、ENABLE BGP AUTOSOFTUPDATE コマンド（285 ページ）で自動ソフトリセット機能を有効化している場合は、自動的に経路情報が更新されるので、RESET BGP PEER コマンド（326 ページ）は不要です。

■ コミュニティー値「65003:1234」を持つ経路に MED 値「200」を付加し、AS_PATH 属性に自 AS 番号「65003」を 2 個追加するルートマップ「med_n_prepend」を作成します。この例では MATCH 節でコミュニティーリストを使っています。MATCH COMMUNITY パラメーターにコミュニティー値そのものではなく、コミュニティーリストの番号を指定している点に注意してください。

```
ADD IP COMMUNITYLIST=1 INCLUDE=65003:1234 ↵
ADD IP ROUTEMAP=med_n_prepend ENTRY=1 ACTION=INCLUDE ↵
ADD IP ROUTEMAP=med_n_prepend ENTRY=1 MATCH COMMUNITY=1 ↵
ADD IP ROUTEMAP=med_n_prepend ENTRY=1 SET MED=200 ↵
ADD IP ROUTEMAP=med_n_prepend ENTRY=1 SET ASPATH=65003,65003 ↵
```

作成したルートマップ「med_n_prepend」を、BGP ピア「10.2.1.1」（AS 番号 65020）に通知する経路に適用するには次のようにします。

```
ADD BGP PEER=10.2.1.1 REMOTEAS=65020 OUTROUTEMAP=med_n_prepend ↵
```

✎ すでに BGP ピアとセッションが張られている場合は、SET BGP PEER コマンド（343 ページ）の OUTROUTEMAP パラメーターでルートマップを指定し、その後 RESET BGP PEER コマンド（326 ページ）を SOFT パラメーター付きで実行してください（ソフトリセット）。なお、ENABLE BGP AUTOSOFTUPDATE コマンド（285 ページ）で自動ソフトリセット機能を有効化している場合は、自動的に経路情報が更新されるので、RESET BGP PEER コマンド（326 ページ）は不要です。

■ 「10.10.10.1」との BGP セッションにおいて、プレフィックス「172.16.20.0/24」の AS_PATH 属性に自 AS 番号（65002）を 2 個追加します。これにより、自 AS を経由して「172.16.20.0/24」に向かう経路が高コストであることを他 AS に通知し、結果として「172.16.20.0/24」宛てのトラフィックが自 AS に流れ込む可能性を低くします。

1. ルートマップ「mark_it_slow」を作成し、すべてにマッチするエントリー「1」を作成します（MATCH 節のないエントリーはすべてにマッチ）。また、属性設定のための SET 節を追加します。ここではマッチした経路にコミュニティー値「65002:1000」を設定し、この値を「自 AS 番号を 2 個追加すべき経路」という意味にします。

   ```
   ADD IP ROUTEMAP=mark_it_slow ENTRY=1 ACTION=INCLUDE ↵
   ADD IP ROUTEMAP=mark_it_slow ENTRY=1 SET COMMUNITY=65002:1000 ↵
   ```

2. BGP で通知するネットワークとして「172.16.20.0/24」を追加します。このとき、ルートマップ「mark_it_slow」を適用するよう指定します。これにより、プレフィックス「172.16.20.0/24」が BGP 経路に取り込まれるときに、COMMUNITIES 属性「65002:1000」が設定されます。

   ```
   ADD BGP NETWORK=172.16.20.0/24 ROUTEMAP=mark_it_slow ↵
   ```

3. コミュニティー「65002:1000」に属する経路にマッチするコミュニティーリスト「1」を作成します。

```
ADD IP COMMUNITYLIST=1 INCLUDE=65002:1000 ↵
```

4. BGP ピア「10.10.10.1」とのセッションにおいて、経路を通知するときに適用するルートマップ「add_myasn_twice」を作成し、コミュニティー「65002:1000」を持つ経路にマッチするエントリー「1」を作成します。COMMUNITY パラメーターには、前の手順で作成したコミュニティーリスト「1」を指定します。

```
ADD IP ROUTEMAP=add_myasn_twice ENTRY=1 ACTION=INCLUDE ↵
ADD IP ROUTEMAP=add_myasn_twice ENTRY=1 MATCH COMMUNITY=1 ↵
```

5. ルートマップ「add_myasn_twice」のエントリー「1」に自 AS 番号（65002）を追加する SET 節を追加します。

```
ADD IP ROUTEMAP=add_myasn_twice ENTRY=1 SET ASPATH=65002,65002 ↵
```

6. BGP ピア「10.10.10.1」（所属 AS は 65001）を追加します。OUTROUTEMAP パラメーターにルートマップ「add_myasn_twice」を指定し、該当ピアに送信する経路情報のうち、コミュニティー「65002:1000」に属するものに AS_PATH を追加します。

```
ADD BGP PEER=10.10.10.1 REMOTEAS=65001 OUTROUTEMAP=add_myasn_twice ↵
```

I-BGP フルメッシュの回避

AS 内部で BGP-4 を使用する環境、すなわち I-BGP 環境においては、経路情報がループすることを防ぐため、すべての BGP スピーカーがフルメッシュでセッションを張る必要があります。このため、BGP スピーカーの数が N のとき、I-BGP セッション数 nSess は次のようになります。

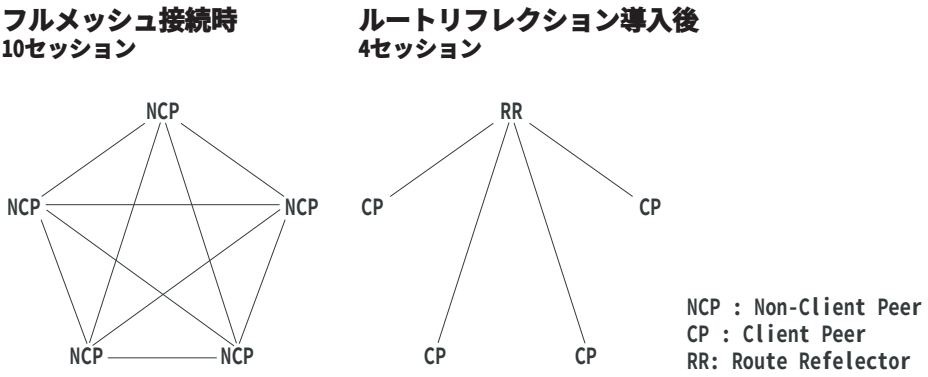
```
nSess = N × (N - 1) ÷ 2
```

たとえば、BGP スピーカーが 4 台のとき、セッション数は 6（= 4 × (4 - 1) ÷ 2）ですが、8 台のときは 28（= 8 × (8 - 1) ÷ 2）となります。
このように、BGP スピーカーの数が少ないうちはそれほど問題になりませんが、数が増えてくると、システム資源（メモリーや CPU）や設定作業にかかる負荷が非常に大きくなります。
この問題を回避するための手段として、本製品は「ルートリフレクション」と「AS コンフェデレーション」をサポートしています。以下、それぞれについて解説します。

ルートリフレクション

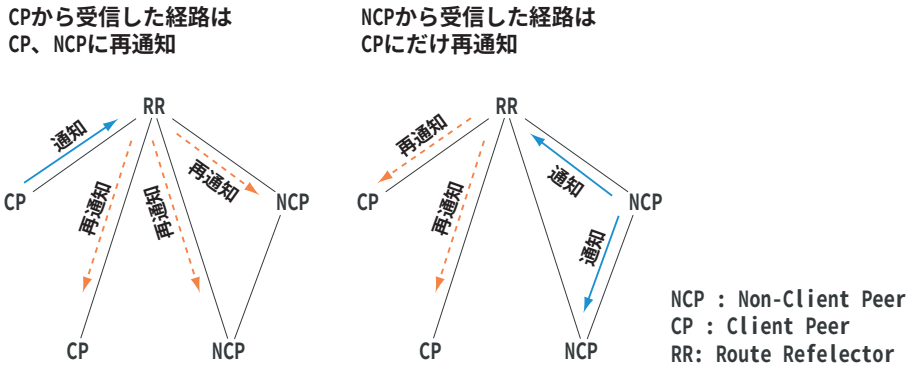
ルートリフレクションは、「ルートリフレクター」（RR）と呼ばれる特殊な役割の I-BGP スピーカーを導入して、I-BGP セッション数を削減するための仕組みです（RFC2796）。

次図の左側は通常のフルメッシュ構成を示しています。ここでは、I-BGP スピーカーが 5 台あるため、合計 10 本の BGP セッションが必要になります。ここで、5 台のうちの 1 台を RR にすると、右側のような構成となり、必要なセッション数は 4 本に削減されます。

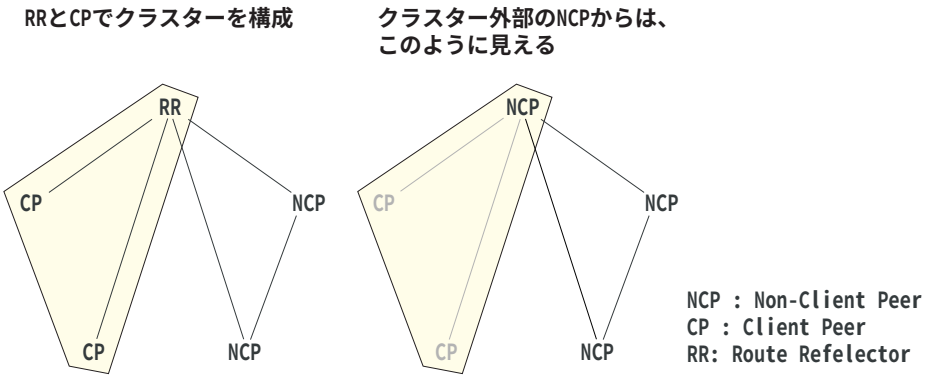


通常の I-BGP スピーカーは、他の I-BGP ピアから学習した経路を別の I-BGP ピアに通知することができませんが、RR として設定されたルーターにはこれ（I-BGP で学習した経路の再通知）が許可されます。RR は、他の I-BGP ピアを次の 2 種類に分けて扱います。

- クライアントピア（CP）: RR に依存しており、RR 経由で経路情報の送受信を行っている I-BGP ピア。RR は、CP から受信した経路を他の CP および NCP に再通知（リフレクト）します。
- ノンクライアントピア（NCP）: RR に依存していない通常の I-BGP ピア。RR は、NCP から受信した経路を CP にだけ再通知（リフレクト）します。



RR が経路を再通知するときは、該当経路に ORIGINATOR_ID 属性が付加されているかどうかを確認し、付加されていなければ通知元の BGP 識別子（ルーター ID）を値としてこれを追加します。
ルートリフレクションでは、RR とそれに依存する CP で「クラスター」と呼ばれるグループを構成します。各クラスターは 4 バイトのクラスター ID（通常は RR の BGP 識別子となる）で識別されます。クラスター外部の BGP スピーカー（NCP）からは、クラスターは 1 つの大きな NCP としか意識されないことになります。



RR が経路を再通知するときは、該当経路に CLUSTER_LIST 属性が付加されているかどうかを確認し、付加されていなければ自身のクラスター ID を値としてこれを追加します。すでに CLUSTER_LIST 属性が付加されていたときは、自身のクラスター ID が含まれていないかどうかを確認し、含まれている場合は経路がループしているとみなして該当経路を破棄します。自身のクラスター ID が含まれていない場合は、これを追加して再通知します。

■ ルートリフレクションを使用するには、RR として動作させるルーター上で BGP ピアを指定するとき（ADD BGP PEER コマンド（154 ページ）、SET BGP PEER コマンド（343 ページ））、CLIENT パラメーターで該当ピアが CP であるか NCP であるかを指定します。

- ピアが CP のときは、CLIENT=YES を指定します。

  ```
  ADD BGP PEER=172.28.28.7 REMOTEAS=65001 CLIENT=YES ↵
  ```

- ピアが NCP のときは、CLIENT=NO を指定します（CLIENT パラメーター省略時は CLIENT=NO と見なされるため、実際には CLIENT=NO を指定する必要はありません）

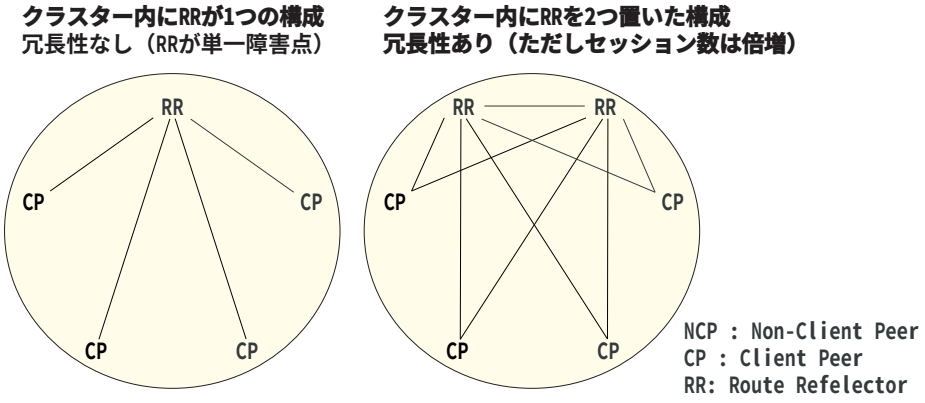
  ```
  ADD BGP PEER=172.28.28.8 REMOTEAS=65001 CLIENT=NO ↵
  ```

✎ ルートリフレクションに対応している必要があるのは RR だけです。RR 以外の CP、NCP は通常の I-BGP の動作をするだけなので、RR をピアとして指定するときにも特殊な設定は必要ありません（デフォルトの CLIENT=NO でよい）。また、CP、NCP は、ルートリフレクションに対応していない機器でもかまいません。

✎ CLIENT パラメーターは I-BGP ピアの設定時にだけ意味を持ちます。

■ RR として動作している場合、デフォルトではクラスター ID として自身の BGP 識別子（ルーター ID）を使います。通常はこれで問題ありませんが、次図の右側の構成のようにクラスター内に複数の RR を置いて冗長性を確保する場合は、クラスター内のすべての RR に同じクラスター ID（いずれかの RR の BGP 識別子）を設定する必要があります。これには、SET BGP コマンド（335 ページ）の CLUSTER パラメーターを使います。

```
SET BGP CLUSTERID=172.28.28.1 ↵
```



クラスター ID の設定は SHOW BGP コマンド（399 ページ）で確認できます。「Cluster ID」欄に「Not defined」と表示されている場合は、デフォルトの設定（未指定）であることを示しています。この場合は自身の BGP 識別子が使われます。「Cluster ID」欄に具体的な ID が表示されている場合は、その値が使われます。

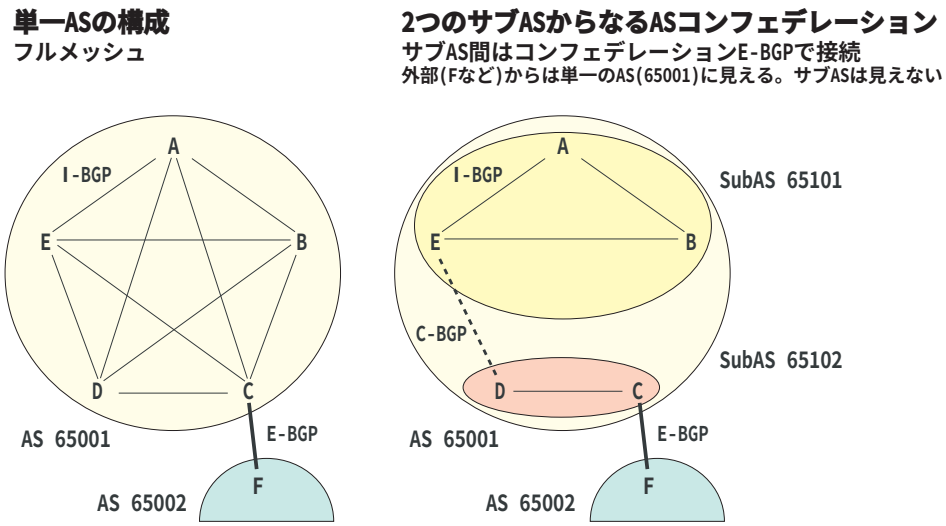
```
SHOW BGP ↵
```

■ ルートリフレクションの設定は、SHOW BGP PEER コマンド（418 ページ）でピアごとに確認します。「Role」欄に「Client」と表示されている場合、該当ピアは CP であり、自身は該当ピアの RR として動作しています。「Non-Client」と表示されている場合、該当ピアは NP です。また、「eBGP」や「eBGP Peer」と表示されている場合、該当ピアは E-BGP ピアです。

```
SHOW BGP PEER ↵
SHOW BGP PEER=172.28.28.7 ↵
```

AS コンフェデレーション

AS コンフェデレーションは、大きな AS を複数の「サブ AS」に分割することで、I-BGP セッション数を削減するための仕組みです（RFC3065）。
次図の左側は、ある AS（65001）内における通常のフルメッシュ構成を示しています。ここでは、I-BGP スピーカーが 5 台あるため、合計 10 本の BGP セッションが必要になります。ここで、AS 65001 を 2 つのサブ AS「65101」と「65102」に分割し、全体を AS コンフェデレーション「65001」として設定すると、右側のような構成となり、必要なセッション数は 5 本に削減されます。



サブ AS「65101」「65102」間は、コンフェデレーション E-BGP（C-BGP）と呼ばれる特殊な E-BGP セッションで接続しています。サブ AS はコンフェデレーションの中からしか見えず、コンフェデレーションの外部（図ではルーター F）からは単一の AS（ここでは AS 65001）として見えます。

■ AS コンフェデレーションを使用するために必要な設定項目を示します。

✎ AS コンフェデレーションを使用する場合は、コンフェデレーション内のすべての BGP スピーカーに AS コンフェデレーションの設定をする必要があります。

- サブ AS の番号を自 AS 番号として設定する（SET IP AUTONOMOUS コマンド（355 ページ））。

  ```
  SET IP AUTONOMOUS=65102 ↵
  ```

- AS コンフェデレーションの番号を指定する（SET BGP コマンド（335 ページ）の CONFEDERATIONID パラメーター）。

  ```
  SET BGP CONFEDERATIONID=65001 ↵
  ```

- ピアを設定するときは次のようにする（ADD BGP PEER コマンド（154 ページ））。
  - AS コンフェデレーション内のピアを指定するときは、REMOTEAS パラメーターにピアのサブ AS 番号を指定する。
    サブ AS 番号が同じピアは、I-BGP ピアとなる。

    ```
    ADD BGP PEER=172.28.28.5 REMOTEAS=65101 ↵
    ```

    サブ AS 番号が異なるピアを指定する場合は、ADD BGP PEER コマンド（154 ページ）のほかに、ADD BGP CONFEDERATIONPEER コマンド（151 ページ）を実行して、ピアのサブ AS 番号を指定する。このようにして設定したピアは、コンフェデレーション E-BGP ピア（C-BGP ピア）となる。

```
ADD BGP PEER=172.28.29.10 REMOTEAS=65102 ↵
ADD BGP CONFEDERATIONPEER=65102 ↵
```

– AS コンフェデレーション外部のピアを指定するときは、REMOTEAS パラメーターにピアの AS 番号を指定する。このピアは、E-BGP ピアとなる。

```
ADD BGP PEER=10.10.10.2 REMOTEAS=65002 ↵
```

■ AS コンフェデレーションの設定は、SHOW BGP CONFEDERATION コマンド（405 ページ）で確認できます。

```
SHOW BGP CONFEDERATION ↵
```

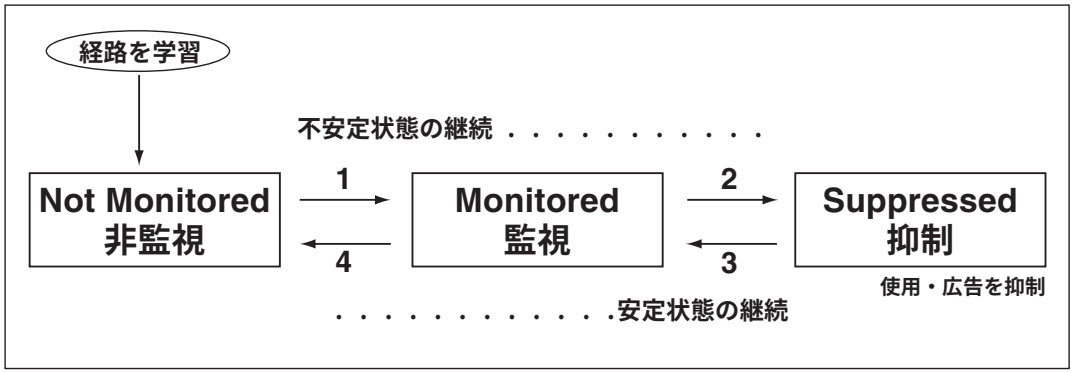
■ SHOW BGP PEER コマンド（418 ページ）の「Role」欄には、通常の E-BGP ピア、コンフェデレーション E-BGP ピア（C-BGP ピア）のどちらとも「eBGP Peer」と表示されますが、「Connection type」欄を見れば両者を区別できます。同欄には、E-BGP ピアなら「EXTERNAL」、C-BGP ピアなら「CONFEDERATION」と表示されます（I-BGP ピアなら「INTERNAL」）。

```
SHOW BGP PEER ↵
SHOW BGP PEER=172.28.29.10 ↵
```

その他の機能

ルートフラップダンピング

ルートフラップダンピング（Route Flap Damping）は、通知と取り消しを繰り返すような（「フラップ」する）不安定な E-BGP 経路がネットワーク全体におよぼす影響を軽減するための機能です（RFC2439）。
ルートフラップダンピングでは、E-BGP で学習した経路の 1 つ 1 つについて、その経路の不安定さを示す「ペナルティー値」を保持します。ペナルティー値は、経路が取り消されるたびに加算され、安定状態が続いているときは減算されます。ペナルティー値があらかじめ設定しておいたしきい値を超えたら、その経路の使用・広告を一定の期間抑制します。これにより、UPDATE メッセージの数を減らし、各ルーターやネットワークへの負荷を軽減することができます。
各経路は、ペナルティー値の推移にしたがって、次に示す 3 つの状態を行き来します。経路が学習された時点でのペナルティー値は 0、状態は「Not Monitored」（非監視）となります。



状態間の遷移は次のときに発生します。

遷移前の状態	図中の番号	遷移条件	遷移後の状態
Not Monitored（非監視）	1	経路が取り消された（フラップした）	Monitored（監視）
Monitored（監視）	2	ペナルティー値が SUPPRESSION（抑制しきい値）を上回った	Suppressed（抑制）
Suppressed（抑制）	3	ペナルティー値が REUSE（再使用（抑制解除）しきい値）を下回った。あるいは安定状態が HALFLIFE × MAXHOLD（分）続いた	Monitored（監視）
Monitored（監視）	4	ペナルティー値が 0 になった	Not Monitored（非監視）

表 11: 機器の状態遷移

経路のペナルティー値は、次のようにして推移します。

- 経路が初めて学習されたときは、0
- 経路が取り消された（フラップした）ときは、1000 を加算
- 経路の安定状態が続いたときは、徐々に減算（HALFLIFE（分）経過するたびに半分になる速度で減少）

次に、ルートフラップダンピングの動作を制御するためのパラメーターをまとめます。本製品では、これら一式を「パラメーターセット」と呼びます。複数のパラメーターセットを定義しておくことで、経路ごとに異なるパラメーターセットを使用することも可能です。

パラメーター名	意味	解説	デフォルト値
SUPPRESSION	抑制しきい値	ペナルティー値が本しきい値を上回ると、該当経路は Suppressed（抑制）状態となり、ペナルティー値が再使用しきい値（REUSE）を下回るか、安定状態が最大抑制時間（HALFLIFE × MAXHOLD）続くまで、同経路は使用も広告もされなくなる	2000

REUSE	再使用（抑制解除）しきい値	いったんSuppressed（抑制）状態となった経路は、ペナルティー値が本しきい値を下回るか、安定状態が最大抑制時間（HALFLIFE × MAXHOLD）続くまでは使用も広告もされない。ペナルティー値が本しきい値を下回ると、該当経路の抑制状態は解除され、Monitored（監視）状態に遷移する	750
HALFLIFE	ペナルティー値の半減期（分）	安定状態にある経路のペナルティー値は徐々に減少していくが、そのときの速度は「HALFLIFE（分）経過するごとに半分になる」レートである	15
MAXHOLD	最大抑制時間を求めるための係数	実際の最大抑制時間はHALFLIFE × MAXHOLD（分）で求められる。Suppressed（抑制）状態にある経路のペナルティー値が再使用しきい値（REUSE）を上回っていても、安定状態が最大抑制時間（HALFLIFE × MAXHOLD）続いた場合は抑制状態が解除される	4

表 12: ルートフラップダンピングのパラメーター

■ すべての経路に対して同じパラメーターセットを使用する場合、ルートフラップダンピングを使用するための手順は次のようになります。

1. デフォルトパラメーターセット（番号は 0）の内容を必要に応じて変更します。デフォルト設定を使う場合、本手順は不要です。

```
SET BGP DAMPING PARAMETERSET=0 SUPPRESSION=5000 REUSE=1250 ↵
```

2. ルートフラップダンピング機能（とパラメーターセット）を有効にします。

```
ENABLE BGP DAMPING ↵
```

3. 設定は以上です。これにより、すべての経路がデフォルトパラメーターセットに基づいて管理されます。

■ 経路ごとに異なるパラメーターセットを使いたい場合は、次のようにします。
ここでは、E-BGP ピア 10.10.10.2 から受信した経路に対してはカスタムパラメーターセット「1」を、その他の経路に対してはデフォルトパラメーターセットを使うものとします。また、すでにその他の設定は完了しており、各 BGP ピアとセッションが確立しているものと仮定しています。

1. E-BGP ピア 10.10.10.2 から受信した経路に適用するカスタムパラメーターセット「1」を作成します。

```
CREATE BGP DAMPING PARAMETERSET=1 SUPPRESSION=3000 REUSE=800 ↵
```

2. その他のピアから受信した経路に適用するデフォルトパラメーターセット（番号は 0）の内容を必要に応じて変更します。デフォルト設定を使う場合、本手順は不要です。

```
SET BGP DAMPING PARAMETERSET=0 SUPPRESSION=5000 REUSE=1250 ↵
```

3. すべての経路をカスタムパラメーターセット「1」と関連付けるルートマップ「in2」を作成します。

```
ADD IP ROUTEMAP=in2 ENTRY=1 ACTION=INCLUDE ↵
ADD IP ROUTEMAP=in2 ENTRY=1 SET BGPDAMPID=1 ↵
```

4. E-BGP ピア 10.10.10.2 から受信した経路にルートマップ「in2」を適用します。

```
SET BGP PEER=10.10.10.2 INROUTEMAP=in2 ↵
```

5. ルートマップの設定を有効にするため、該当ピアから受信した経路だけを更新します。

```
RESET BGP PEER=10.10.10.2 SOFT=IN ↵
```

6. ルートフラップダンピング機能（とパラメーターセット）を有効にします。

```
ENABLE BGP DAMPING ↵
```

7. 設定は以上です。これにより、10.10.10.2 から受信した経路は、カスタムパラメーターセット「1」に基づいて管理されます。その他の経路に対しては、自動的にデフォルトパラメーターセットが使われます。

■ カスタムパラメーターセットの設定を変更するには、SET BGP DAMPING PARAMETERSET コマンド（339 ページ）を使います。

```
SET BGP DAMPING PARAMETERSET=1 HALFLIFE=10 ↵
```

■ ルートフラップダンピング機能を無効化するには、DISABLE BGP DAMPING コマンド（258 ページ）を実行します。

```
DISABLE BGP DAMPING ↵
```

■ 特定のパラメーターセットだけを無効化するには、DISABLE BGP DAMPING コマンド（258 ページ）を PARAMETERSET パラメーター付きで実行します。なお、すべてのパラメーターセットを無効化すると、ルートフラップダンピング機能自体も自動的に無効化されます。

```
DISABLE BGP DAMPING PARAMETERSET=1 ↵
```

■ ルートフラップダンピング機能の有効・無効、各パラメーターセットの設定は SHOW BGP DAMPING

コマンド（409 ページ）で確認できます。

```
SHOW BGP DAMPING ↵
```

■ ルートフラップダンピング機能が管理している経路の情報（ペナルティー値など）を表示するには、SHOW BGP DAMPING ROUTES コマンド（411 ページ）を使います。

```
SHOW BGP DAMPING ROUTES ↵
```

TCP MD5 認証

TCP MD5 認証は、TCP のオプション機能である MD5 ダイジェスト認証を利用して、BGP セッションの信頼性・安全性を高めるための機能です（RFC2385）。

■ TCP MD5 認証を使用するには、ADD BGP PEER コマンド（154 ページ）、SET BGP PEER コマンド（343 ページ）の AUTHENTICATION パラメーターに MD5 を指定します。また、PASSWORD パラメーターでパスワード（認証鍵）を指定します。パスワードはピアと同じ値を指定してください。

```
ADD BGP PEER=10.10.10.2 REMOTEAS=65002 AUTHENTICATION=MD5
  PASSWORD=himitsu ↵
```

■ TCP MD5 認証の設定は、SHOW BGP PEER コマンド（418 ページ）で確認できます。「Authentication」、「Password」欄をご覧ください。

```
SHOW BGP PEER=10.10.10.2 ↵
```

プライベート AS フィルター

プライベート AS フィルターは、UPDATE メッセージの送信時に AS_PATH 属性からプライベート AS 番号（64512～65535）を取り除く機能です。

■ プライベート AS フィルターを使用するには、ADD BGP PEER コマンド（154 ページ）の PRIVATEAS-FILTER パラメーターでピアごとに設定します。同パラメーターに YES を指定すると、該当ピアに送信する UPDATE メッセージの AS_PATH 属性からプライベート AS 番号が取り除かれます。

```
ADD BGP PEER=10.10.10.2 REMOTEAS=12345 PRIVATEASFILTER=YES ↵
```

■ プライベート AS フィルターの設定は、SHOW BGP PEER コマンド（418 ページ）で確認できます。「Private AS Filter」欄をご覧ください。

```
SHOW BGP PEER=10.10.10.2 ↵
```

BGP ピアテンプレート

BGP ピアテンプレートは、同じフィルタリングポリシーを適用する多数のピアとセッションを張る場合に、設定の手間を軽減するための機能です。
フィルタリングポリシーや各種制限値など、通常はピアごとに設定するパラメーターを、「ピアテンプレート」と呼ばれるひな形にまとめておき、個々のピアを指定するときにはパラメーターを提供するテンプレートの番号を指定するようにします。

■ ピアテンプレートを作成するには、ADD BGP PEERTEMPLATE コマンド（158 ページ）を使います。

```
ADD BGP PEERTEMPLATE=1 INROUTEMAP=common1-in OUTROUTMAP=common1-out ↵
```

■ ピアテンプレートを使用して BGP ピアの設定をするには、ADD BGP PEER コマンド（154 ページ）の POLICYTEMPLATE パラメーターにテンプレートの番号を指定します。大部分のパラメーターはテンプレートで指定するため、POLICYTEMPLATE 以外に指定できるパラメーターは PEER、REMOTEAS、DESCRIPTION、AUTHENTICATION、PASSWORD、FASTFALLOVER、EHOPS だけとなります。このうち、必須なのは PEER と REMOTEAS です。

```
ADD BGP PEER=10.10.10.2 POLICYTEMPLATE=1 REMOTEAS=65002 ↵
ADD BGP PEER=10.10.10.3 POLICYTEMPLATE=1 REMOTEAS=65003 ↵
ADD BGP PEER=10.10.10.4 POLICYTEMPLATE=1 REMOTEAS=65004 ↵
```

■ テンプレートによって設定したピアのパラメーターを変更したいときは、該当パラメーターをテンプレートで指定可能かどうかによって、次のいずれかの方法を使います。
該当パラメーターをテンプレートで指定できる場合は、SET BGP PEERTEMPLATE コマンド（346 ページ）でテンプレートの設定を変更します。これにより、テンプレートを使用しているすべてのピアの設定が変更されます。

```
SET BGP PEERTEMPLATE=1 INROUTEMAP=common1a-in ↵
```

SET BGP PEER コマンド（343 ページ）の POLICYTEMPLATE パラメーターで異なるテンプレートを指定すれば、新しいテンプレートが該当ピアに適用されます。テンプレートを使っていないピアに対して実行した場合は、該当ピアのパラメーターのうちテンプレートで指定可能なものすべてが、テンプレートの設定値で上書きされます。

```
SET BGP PEER=10.10.10.2 POLICYTEMPLATE=2 ↵
```

該当パラメーターをテンプレートで指定できない場合は、個々のピアに対して SET BGP PEER コマンド（343 ページ）を実行してパラメーターを変更します。

```
SET BGP PEER=10.10.10.3 AUTHENTICATION=MD5 PASSWORD=foobarbar ↵
```

■ ピアからテンプレートを取り除くには、SET BGP PEER コマンド（343 ページ）の POLICYTEMPLATE パラメーターを「POLICYTEMPLATE=」のように指定します。

```
SET BGP PEER=10.10.10.4 POLICYTEMPLATE= ↵
```

このようにしてテンプレートを解除した場合、テンプレートが提供していたパラメーターはそのまま引き継がれます（ADD BGP PEER コマンド（154 ページ）で指定したのと同じ扱い）。テンプレートを解除した後は、SET BGP PEER コマンド（343 ページ）で通常どおり各パラメーターを変更できます。

```
SET BGP PEER=10.10.10.4 INFILTER=300 OUTFILTER=301 ↵
```

■ ピアの変更を反映するには、RESET BGP PEER コマンド（326 ページ）を SOFT パラメーター付きで実行してください（ソフトリセット）。

```
RESET BGP PEER=ALL SOFT=ALL ↵
```

✎ SOFT パラメーターを付けずに実行すると、BGP セッションがいったん切断されるのでご注意ください。SOFT パラメーターを付けた場合は、BGP セッションをクローズせずに経路情報を更新します。

また、ENABLE BGP AUTOSOFTUPDATE コマンド（285 ページ）で自動ソフトリセットを有効にしている場合は、パラメーターの変更後、ただちに変更が反映されます。自動ソフトリセットは、デフォルトでは無効です。

```
ENABLE BGP AUTOSOFTUPDATE ↵
```

■ ピアテンプレートの設定内容は、SHOW BGP PEERTEMPLATE コマンド（422 ページ）で確認できます。

```
SHOW BGP PEERTEMPLATE ↵
SHOW BGP PEERTEMPLATE=1 ↵
```

■ 特定のピアにどのテンプレートが適用されているかは、SHOW BGP PEER コマンド（418 ページ）で確認できます。「Policy Template」欄をご欄ください。

```
SHOW BGP PEER=10.10.10.2 ↵
```

システム資源の調整

メモリー不足時の一時停止

通常運用時には、BGP-4 以外にも多くの機能（モジュール）が動作しています。このような環境では、他のモジュールが一時的にメモリーを大量に使用し、BGP-4 モジュールの実行に必要なメモリーが足りなくなる可能性があります。

本製品には、メモリー不足時に（セッションを維持したまま）BGP-4 の処理を一時停止（バックオフ）し、メモリー不足が解消するまで待機する機能があります。

デフォルトでは、システム全体のメモリー使用量が 95%に達すると、BGP-4 の処理を 10 秒間停止します。10 秒待機してもメモリー使用率が 95%以上だった場合は、再び 10 秒間待機します。連続 5 回待機してもメモリー使用量が 95%より下がらない場合は、回復の見込みなしと判断して、すべての BGP セッションを切断（ピアを無効化）します。

BGP バックオフ機能の動作は、以下のパラメーターを変更することで調整可能です。

パラメーター名	意味	解説	デフォルト値
BACKOFF	バックオフしきい値（%）	システム全体のメモリー使用量が本しきい値に達した場合、BGP-4 の処理は一時停止（バックオフ）される。LOW パラメーターよりも大きい値に設定しなくてはならない	95
LOW	バックオフ解除しきい値（%）	BGP-4 の処理が一時停止（バックオフ）された後、システム全体のメモリー使用量が本しきい値を下回ると、BGP-4 の処理が再開される。BACKOFF パラメーターよりも小さい値に設定しなくてはならない	90
BASETIME	バックオフ時間の基準値（秒）	実際のバックオフ時間は BASETIME、MULTIPLIER、STEP の組み合わせと何回目のバックオフであるかによって決まる	10
CONSECUTIVE	連続したバックオフの制限回数（回）	バックオフが CONSECUTIVE 回連続して発生した場合は、回復不可能と判断してすべての BGP セッションを停止する	5
MULTIPLIER	バックオフ時間を決定するための係数	初回のバックオフ時間は BASETIME × MULTIPLIER ÷ 100 で求められる（小数点以下は切り捨て）。バックオフが連続して発生した場合、初回を含めて STEP 回は同じバックオフ時間が用いられる、その次の回のバックオフ時間は前回のバックオフ時間 × MULTIPLIER ÷ 100（小数点以下は切り捨て）となる。すなわち、MULTIPLIER を 100 より大きく設定すればバックオフ時間は次第に長くなり、100 より小さく設定すればバックオフ時間は次第に短くなる	100

STEP	同一バックオフ時間を使用する回数（回）	バックオフが連続して発生した場合、何回ごとにバックオフ時間を再計算するか	1
TOTALLIMIT	バックオフの合計制限回数（回）	バックオフが合計 TOTALLIMIT 回発生した場合（システム起動後の合計回数。連続していなくてもよい）は、すべての BGP セッションを切断（ピアを無効化）する。0 は無制限を意味する	0

表 13:

■ BGP バックオフ機能のパラメーターを変更するには、SET BGP BACKOFF コマンド（337 ページ）を使います。

```
SET BGP BACKOFF BASETIME=60 CONSECUTIVE=6 MULTIPLIER=110 STEP=2 ↵
```

このように設定した場合、メモリー使用量 95%以上の状態が続くと、バックオフ時間は次のように推移します。

-	**バックオフ時間（秒）**	**備考**
1	66	60 × 110 ÷ 100 = 60 × 1.1
2	66	
3	72	66 × 110 ÷ 100 = 66 × 1.1
4	72	
5	79	72 × 110 ÷ 100 = 72 × 1.1
6	79	
7	-	すべての BGP セッションを切断

表 14:

■ BGP バックオフ機能の設定を確認するには、SHOW BGP BACKOFF コマンド（402 ページ）を使います。

```
SHOW BGP BACKOFF ↵
```

メモリー使用量の制限

通常運用時には、BGP-4 以外にも多くの機能（モジュール）が動作しています。BGP-4 モジュールが大量にメモリーを消費すると、他のモジュールの実行に必要なメモリーが足りなくなる可能性があります。
本製品には、BGP-4 に割り当て可能なメモリー量を制限する機能があります。
デフォルトでは、BGP-4 に割り当て可能なメモリー量はシステム全体の 85%に制限されています。BGP-4 モジュールのメモリー使用量が 85%に達した場合は、すべての BGP セッションを切断（ピアを無効化）します。

■ BGP-4 に割り当て可能なメモリー量は、SET BGP MEMLIMIT コマンド（342 ページ）で変更できます。

```
SET BGP MEMLIMIT=75 ↵
```

■ BGP-4 に割り当て可能なメモリー量の設定、および、実際のメモリー使用量は、SHOW BGP MEMLIMIT コマンド（414 ページ）で確認できます。

```
SHOW BGP MEMLIMIT ↵
```

トリガー

モジュールトリガーを使用すると、BGP ピアの状態変化時や BGP 用のメモリー領域が不足したときに、任意のスクリプトを実行させることができます。
BGP のモジュールトリガーを作成するには、CREATE TRIGGER MODULE コマンド（「運用・管理」の 143 ページ）の MODULE パラメーターに BGP を指定し、EVENT パラメーターにイベント名を指定します。イベントには次のものがあります。以下、各イベントを捕捉するトリガーの設定方法について解説します。

- MEMORY：メモリー不足のため BGP の経路情報を破棄しなくてはならなくなったときに発生
- PEERSTATE：BGP ピアとの通信状態が変化したときに発生

MEMORY イベント

BGP MEMORY イベントは、メモリー不足により BGP モジュールが経路情報を破棄しなくてはならなくなったときに発生します。
MEMORY イベントを捕捉するには、CREATE TRIGGER MODULE コマンド（「運用・管理」の 143 ページ）を次の構文で使用します。MODULE、EVENT 以外に BGP モジュール固有のパラメーターはありません。

```
CREATE TRIGGER=trigger-id MODULE=BGP EVENT=MEMORY [AFTER=time]
  [BEFORE=time] [{DATE=date|DAYS=day-list}] [NAME=string]
  [REPEAT={YES|NO|ONCE|FOREVER|count}] [SCRIPT=filename...]
  [STATE={ENABLED|DISABLED}] [TEST={YES|NO|ON|OFF}]
```

BGP MEMORY トリガーから実行されるスクリプトには、特殊な引数として%D（日付）、%T（時刻）、%N（システム名）、%S（シリアル番号）が渡されます（これらの引数はすべてのトリガーに共通です）。なお、BGP MEMORY トリガー固有の引数（%1 など）はありません。

■ メモリー不足により BGP の経路情報が破棄されはじめたときにスクリプト memlow.scp を実行するトリガー「1」を作成するには、次のようにします。

```
CREATE TRIGGER=1 MODULE=BGP EVENT=MEMORY SCRIPT=memlow.scp ↵
```

PEERSTATE イベント

BGP PEERSTATE イベントは、BGP ピアとの通信状態が変化したときに発生します。
PEERSTATE イベントを捕捉するには、CREATE TRIGGER MODULE コマンド（「運用・管理」の 143 ページ）、SET TRIGGER MODULE コマンド（「運用・管理」の 278 ページ）を次の構文で使用します。MODULE、EVENT 以外に、BGP PEERSTATE トリガー固有のパラメーターとして、PEER、BGPSTATE、DIRECTION の 3 つがあります。

```
CREATE TRIGGER=trigger-id MODULE=BGP EVENT=PEERSTATE PEER={ANY|ipadd}
  BGPSTATE={IDLE|CONNECT|ACTIVE|OPENSENT|OPENCONFIRM|ESTABLISHED|ANY}
  DIRECTION={ENTER|LEAVE|ANY} [AFTER=time] [BEFORE=time]
  [{DATE=date|DAYS=day-list}] [NAME=string]
  [REPEAT={YES|NO|ONCE|FOREVER|count}] [SCRIPT=filename...]
  [STATE={ENABLED|DISABLED}] [TEST={YES|NO|ON|OFF}]
```

```
SET TRIGGER=trigger-id [PEER={ANY|ipadd}]
  [BGPSTATE={IDLE|CONNECT|ACTIVE|OPENSENT|OPENCONFIRM|ESTABLISHED|ANY}]
  [DIRECTION={ENTER|LEAVE|ANY}] [AFTER=time] [BEFORE=time]
  [{DATE=date|DAYS=day-list}] [NAME=string]
  [REPEAT={YES|NO|ONCE|FOREVER|count}] [TEST={YES|NO|ON|OFF}]
```

BGP PEERSTATE トリガーは、PEER パラメーターで指定した BGP ピア（との通信）の状態が、BGPSTATE パラメーターで指定した状態に遷移した場合（DIRECTION=ENTER）、または、BGPSTATE パラメーターで指定した状態から他の状態に遷移した場合（DIRECTION=LEAVE）、または、その両方の場合（DIRECTION=BOTH）に起動されます。
BGPSTATE パラメーターで指定する状態については、SHOW BGP PEER コマンド（418 ページ）の表（State 欄）をご参照ください。
DIRECTION パラメーターは、次のような意味を持ちます。

- ENTER：他の状態から BGPSTATE パラメーターで指定した状態への遷移
- LEAVE：BGPSTATE パラメーターで指定した状態から他の状態への遷移
- BOTH：ENTER と LEAVE の両方

✎ BGPSTATE パラメーターに ANY を指定し、DIRECTION パラメーターに BOTH を指定した場合、1 つの状態遷移にともなって 2 つのイベントが発生します。たとえば、BGP ピア 10.10.10.2 が Idel から Connect 状態に遷移した場合、Connect 状態への ENTER イベントと Idle 状態からの LEAVE イベントの 2 つが発生します。

BGP PEERSTATE トリガーから実行されるスクリプトには、特殊な引数として%D（日付）、%T（時刻）、%N（システム名）、%S（シリアル番号）が渡されます（これらの引数はすべてのトリガーに共通です）。また、BGP PEERSTATE トリガー固有の引数として、以下の値も渡されます。

- %1：状態遷移した BGP ピアの IP アドレス
- %2：遷移後（ENTER イベントのとき）または遷移前（LEAVE イベントのとき）の状態

- %3：状態遷移の方向（enter または leave）

■ BGP ピア 10.10.10.2 との通信状態が Established でなくなったときにスクリプト peerdown.scp を実行するトリガー「2」を作成するには、次のようにします。

```
CREATE TRIGGER=2 MODULE=BGP EVENT=PEERSTATE PEER=10.10.10.2
  BGPSTATE=ESTABLISHED DIRECTION=LEAVE SCRIPT=peerdown.scp ↵
```

経路制御フィルター

経路情報フィルター機能について説明します。
本製品には、ダイナミックルーティング使用時に経路情報を制御する方法として、次の機能が用意されています。

機能	概要
IP ルートフィルター	ルーティングプロトコルによって送受信される経路情報に制限をかける機能です。特定の経路情報を外部に通知しないようにしたり、外部から受信した経路情報を破棄するよう設定したりできます
Trusted Router フィルター	特定のルーターだけを「信頼できる RIP ルーター」と見なし、他のルーターから受信した RIP 情報は無効なものとして受け入れないよう設定する機能です

表 15:

IP ルートフィルター

IP ルートフィルターは、おもにダイナミックルーティングプロトコル（RIP/OSPF）による経路情報のやりとりに一定の制限をかける機能です。特定の経路情報を他のルーターに通知しないようにしたり、受信した経路情報から任意のエントリーを破棄したりすることができます。

基本

■ IP ルートフィルターは、ADD IP ROUTE FILTER コマンド（191 ページ）で作成します。特定の経路情報を拒否するには次のようにします。これにより、宛先が「200.200.*.*」となる経路情報の送受信が行われなくなります。

```
ADD IP ROUTE FILTER=1 IP=200.200.*.* MASK=*.*.*.* ACTION=EXCLUDE ↵
ADD IP ROUTE FILTER=2 IP=*.*.*.* MASK=*.*.*.* ACTION=INCLUDE ↵
```

IP ルートフィルターは最大 100 個のフィルターエントリー（1〜100）で構成されるリストです。経路情報の交換時にはリストの先頭から順に各エントリーがチェックされ、最初にマッチしたエントリーのアクションが実行されます。

✎ 1つでもフィルターエントリーが設定されているときは、フィルターの末尾にすべてを拒否する暗黙のエントリーが存在します。そのため、一部の経路情報だけを制限したいとき（デフォルト許可の設定）は、リストの末尾に「すべてを許可する」エントリーを明示的に作成してください。また、フィルターエントリーを追加するときはエントリーの順序に気を付けてください。

■ ADD IP ROUTE FILTER コマンド（191 ページ）の FILTER パラメーターにエントリー番号を指定しなかった場合は、作成順にエントリー番号が振られます。エントリー番号は SHOW IP ROUTE FILTER コマンド（476 ページ）で確認できます。

■ FILTER パラメーターでエントリー番号を明示的に指定した場合、指定した番号のエントリーがすでに存在していたときは、指定エントリーの前に新規エントリーが挿入されます。

■ デフォルトでは経路情報の送受信両方にフィルターがかかります。送信時のみ、受信時のみを明示的に指定したいときは、DIRECTION パラメーターに SEND（送信時）、RECEIVE（受信時）を指定します。「172.20.*.*」の経路を外部に通知しないようにするには次のようにします。

```
ADD IP ROUTE FILTER=1 IP=172.20.*.* MASK=*.*.*.* DIRECTION=SEND
  ACTION=EXCLUDE ↵
ADD IP ROUTE FILTER=2 IP=*.*.*.* MASK=*.*.*.* ACTION=INCLUDE ↵
```

✎ ただし、PROTOCOL に OSPF を指定するときは、SEND と RECEIVE が別々に処理されるため、必ず明示的に方向を指定してください。

■ 特定のルーティングプロトコルだけを対象にしたいときは、PROTOCOL パラメーターにプロトコル名を指定します。RIP 経由でのみ「10.*.*.*」の経路を受け取りたいときは次のようにします。

```
ADD IP ROUTE FILTER=1 IP=10.*.*.* MASK=*.*.*.* DIRECTION=RECEIVE
  PROTOCOL=RIP ACTION=INCLUDE ↵
ADD IP ROUTE FILTER=2 IP=10.*.*.* MASK=*.*.*.* DIRECTION=RECEIVE
  ACTION=EXCLUDE ↵
ADD IP ROUTE FILTER=3 IP=*.*.*.* MASK=*.*.*.* ACTION=INCLUDE ↵
```

■ プロトコルとして OSPF を指定する場合は、DIRECTION パラメーターで SEND（送信）と RECEIVE（受信）を明示的に指定してください。たとえば、次の例では eth0 で受信した OSPF の経路情報のうち、192.168.100.0/24 に関する情報だけを受け取らないように設定します。その他の経路情報は、送信・受信とも通常どおり行います。

```
ADD IP ROUTE FILTER IP=192.168.100.* MASK=255.255.255.* AC=EXCLUDE
  DIR=RECEIVE INT=eth0 PROTO=OSPF ↵
ADD IP ROUTE FILTER IP=*.*.*.* MASK=*.*.*.* AC=INCLUDE DIR=SEND INT=eth0
  PROTO=OSPF ↵
ADD IP ROUTE FILTER IP=*.*.*.* MASK=*.*.*.* AC=INCLUDE DIR=RECEIVE
  INT=eth0 PROTO=OSPF ↵
```

✎ OSPF に対して DIRECTION=SEND の設定を持つフィルターは、自身の IP ルーティングテーブルから OSPF に経路情報をエクスポートするタイミングで適用されます。そのため、LSDB 内の情報を元に送信されるエリア内経路（Intra-area route）に対しては機能しません。DIRECTION=SEND のフィルターは、ABR 上においてエリア間経路、エリア外経路に対してのみ機能します。また、ASBR 上において、エリア外経路に対してのみ機能します。

2 行目と 3 行目で 192.168.100.0/24 以外の経路情報をすべて通すようにしていますが、このとき送信（SEND）と受信（RECEIVE）を明示的に指定していることに注意してください。

■ 一方、プロトコルとして RIP を指定する場合は、DIRECTION パラメーターを省略すると SEND、RECEIVE の両方が対象になります。

```
ADD IP ROUTE FILTER IP=*.*.*.* MASK=*.*.*.* AC=INCLUDE INT=ppp0
  PROTO=RIP ↵
```

■ 特定のインターフェースでのみ経路情報のやりとりを制限したい場合は、INTERFACE パラメーターにインターフェースを指定します。ppp0 からは「192.168.*.*」の経路情報だけを送信するようにするには次のようにします。

```
ADD IP ROUTE FILTER=1 IP=192.168.*.* MASK=*.*.*.* INTERFACE=ppp0
  DIRECTION=SEND ACTION=INCLUDE ↵
ADD IP ROUTE FILTER=2 IP=*.*.*.* MASK=*.*.*.* INTERFACE=ppp0
  DIRECTION=SEND ACTION=EXCLUDE ↵
ADD IP ROUTE FILTER=3 IP=*.*.*.* MASK=*.*.*.* ACTION=INCLUDE ↵
```

■ フィルターエントリーを修正するには SET IP ROUTE FILTER コマンド（374 ページ）を使います。エントリー番号は可変なので、必ず SHOW IP ROUTE FILTER コマンド（476 ページ）で希望するエントリーの番号を確認してから指定してください。

```
SET IP ROUTE FILTER=1 IP=192.168.*.* MASK=*.*.*.* ACTION=EXCLUDE ↵
```

■ IP ルートフィルターからエントリーを削除するには DELETE IP ROUTE FILTER コマンド（238 ページ）を使います。エントリー番号は可変なので、必ず SHOW IP ROUTE FILTER コマンド（476 ページ）で希望するエントリーの番号を確認してから指定してください。削除したエントリーより後ろのエントリー（番号が大きいエントリー）は 1 つずつ番号が繰り上がります。

```
DELETE IP ROUTE FILTER=2 ↵
```

■ IP ルートフィルターの内容を確認するには、SHOW IP ROUTE FILTER コマンド（476 ページ）を使います。

RIP に対する動作

RIP に対する IP ルートフィルターの動作について説明します。
RIP による経路情報の交換に対するフィルターは、次のパラメーターを使って作成します。

```
ADD IP ROUTE FILTER[=entry-id] IP=ipadd MASK=ipadd
  ACTION={INCLUDE|EXCLUDE} PROTOCOL=RIP [DIRECTION={RECEIVE|SEND|BOTH}]
  [INTERFACE=interface] [NEXTHOP=ipadd]
```

- INTERFACE パラメーターには、RIP パケットを送受信するインターフェースを指定します。DIRECTION=SEND の場合、指定したインターフェースから送信される RIP パケット内の経路情報だけがフィルターの対象になります。DIRECTION=RECEIVE の場合は、指定したインターフェー

スで受信した RIP パケット内の経路情報だけがフィルターの対象になります。

- NEXTHOP は、DIRECTION=RECEIVE のときだけ有効なパラメーターです。受信した RIP 経路のネクストホップが、本パラメーターの値と一致する場合にだけ条件にマッチします。RIP1 のときは、RIP パケットの始点 IP アドレスが本パラメーターと一致するときにマッチします。RIP2 のときは、Next Hop フィールドの値が本パラメーターと一致するか、Next Hop フィールドが 0.0.0.0（送信元ルーター自身を示す）で、なおかつ、RIP パケットの始点アドレスが本パラメーターと一致する場合にマッチします。DIRECTION=SEND の場合、本パラメーターは無視されます。

✎ RIP に対する IP ルートフィルターをコマンドラインから作成または変更したときは、RESET IP コマンド（327 ページ）で IP モジュールを初期化するか、RESTART コマンド（「運用・管理」の 237 ページ）でシステムを再起動してください。

OSPF に対する動作

OSPF は、リンクステートアルゴリズムを使用するプロトコルのため、RIP とは IP ルートフィルターの動作が異なります。
OSPF による経路情報の交換に対するフィルターは、次のパラメーターを使って作成します。OSPF に対しては、INTERFACE パラメーターと NEXTHOP パラメーターが無視されることに注意してください。

```
ADD IP ROUTE FILTER[=entry-id] IP=ipadd MASK=ipadd
  ACTION={INCLUDE|EXCLUDE} PROTOCOL=OSPF [DIRECTION={RECEIVE|SEND|BOTH}]
```

OSPF に対する IP ルートフィルターの動作の特長を次にまとめます。

- DIRECTION=RECEIVE の設定を持つフィルターは、リンクステートデータベース（LSDB）から IP ルーティングテーブルに経路情報をインポートするタイミングで適用されます。ACTION=EXCLUDE のエントリーにマッチした経路情報は、自身のルーティングテーブルには登録されませんが、LSDB には登録されます。そのため、EXCLUDE された経路情報であっても、同一エリア内の他のルーターには通知されます。なお、ABR 上においては、DIRECTION=RECEIVE で EXCLUDE された経路情報は、自身のルーティングテーブルには登録されないため、結果として他のエリアには通知されません。
- DIRECTION=SEND の設定を持つフィルターは、自身の IP ルーティングテーブルから OSPF に経路情報をエクスポートするタイミングで適用されます。そのため、LSDB 内の情報を元に送信されるエリア内経路（Intra-area route）に対しては機能しません。DIRECTION=SEND のフィルターは、ABR 上においてエリア間経路、エリア外経路に対してのみ機能します。また、ASBR 上において、エリア外経路に対してのみ機能します。
- INTERFACE パラメーターと NEXTHOP パラメーターは無視されます。
- フィルター適用前に IP ルーティングテーブルに登録された経路情報は、該当エリアの関連する LSA がタイムアウトするまで残り続けます。

✎ OSPF に対する IP ルートフィルターをコマンドラインから作成または変更したときは、RESET OSPF コマンド（330 ページ）で OSPF モジュールを初期化するか、RESET IP コマンド（327 ページ）で IP モジュールを初期化するか、RESTART コマンド（「運用・管理」の 237 ページ）でシステムを再起動してください。

Trusted Router フィルター

Trusted Router フィルターは、指定された RIP ルーターだけを「信頼できるルーター」と見なし、その他のルーターから受け取った RIP ブロードキャストの情報は受け入れないようにする機能です。

■ Trusted Router を登録するには、ADD IP TRUSTED コマンド（198 ページ）を使います。

```
ADD IP TRUSTED=172.30.100.1 ↵
```

✎ Trusted Router が 1 つでも登録されている場合、登録されていないルーターからの RIP 情報は無効なものとして受け入れなくなります。1 つも登録されていないときは、すべての RIP 情報を受け入れます。

■ Trusted Router の一覧は SHOW IP TRUSTED コマンド（483 ページ）で確認できます。

■ Trusted Router を削除するには DELETE IP TRUSTED コマンド（241 ページ）を使います。

レンジ NAT

本製品には 2 種類の NAT 機能があります。1 つは IP モジュールの一部として実装されているレンジ NAT（または IP NAT）、もう 1 つはファイアウォールモジュールの一部として実装されているファイアウォール NAT です。
ここではレンジ NAT の使用方法について解説します。なお、2 つの NAT の併用はできませんので、ファイアウォール機能を使用する場合はレンジ NAT ではなくファイアウォール NAT を使ってください。

NAT とは

IP では、プライベートアドレスと呼ばれる特殊なアドレスの範囲が定められています。次にその範囲を示します（RFC1918）。

```
10.0.0.0-10.255.255.255 (10.0.0.0/8)
172.16.0.0-172.31.255.255 (172.16.0.0/12)
192.168.0.0-192.168.255.255 (192.168.0.0/16)
```

これらは、社内 LAN のように閉じたネットワークで自由に使用できるアドレスです。アドレスの割り当て方法は各組織が自由に選択できます。割当機関などのアドレスの使用申請をする必要はありません。個々の LAN は完全に独立しているため、複数の組織が同じアドレスを使用していても問題は起こりません。それぞれの LAN でアドレスが重複していなければよいのです。
これに対し、インターネットにアクセスする場合は、全世界で唯一無二のグローバルな IP アドレスを使用しなくてはなりません。グローバルアドレスは、一意性を保証するため各地の割り当て機関が管理しており、通常エンドユーザーは ISP（インターネットサービスプロバイダー）などから一定数のアドレス割り当てを受けます。
ここで問題になるのは、インターネットの急激な普及等により IP アドレスが不足気味になったことです。ネットワークの規模にもよりますが、インターネットへのアクセスが必要な端末の数だけグローバルアドレスを取得することは困難になっています。そこで、少数のグローバルアドレスを有効活用するために考え出されたのが NAT（Network Address Translation）です。
NAT は、ルーターなどの機器で IP ヘッダーのアドレスを自動的に書き換える機能です。LAN 上の各端末には通常プライベートアドレスを使用し、インターネットにアクセスするときだけ始点アドレスをグローバルアドレスに変換して通信させようというのが、NAT の基本的な考え方です。
NAT はアドレス変換のパターンによっていくつかの種類に分類できますが、もっとも基本的な NAT では、トラフィックの識別に IP ヘッダーの始点および終点 IP アドレスのみを使用します。このため、プライベートアドレスとグローバルアドレスの対応は常に 1 対 1 となります。すなわち、グローバルネットワークにアクセスする端末の数だけ、グローバルアドレスが必要になります。
これに対し、トラフィックの識別に IP アドレスと TCP/UDP ポートの両方を使用することにより、1 つのグローバル IP アドレスで複数のプライベートアドレスに対応できる機能を ENAT（Enhanced NAT）と呼びます（IP マスカレードなどと呼ばれることもあります）。ENAT を使用すれば、端末型ダイヤルアップのように 1 つしかグローバルアドレスを割り当てられない環境でも、LAN 側の複数の端末が同時にインターネットにアクセスできるようになります。

NAT の種類

以下、レンジ NAT でサポートしている NAT の種類について説明します。

スタティック NAT

プライベート IP アドレスからグローバル IP アドレスへの 1 対 1 変換を行います。どのアドレスからどのアドレスに変換するかは、あらかじめ固定的に設定します。

- プライベート IP アドレス「A」を、あらかじめ設定したグローバル IP アドレス「X」に 1 対 1 で変換します。また、その逆変換を行います。
- IP アドレス変換なので、上位のプロトコルタイプには依存しません。
- 両方向からの接続が可能です（プライベート IP アドレス←→グローバル IP アドレス）

■ グローバル側インターフェースが PPP の場合は、単に次のように入力します。IP がプライベートアドレス、GBLIP がグローバルアドレスです。

```
ENABLE IP NAT ↵
ADD IP NAT IP=192.168.10.5 GBLIP=1.1.1.5 ↵
```

■ グローバル側インターフェースが Ethernet か VLAN の場合は、上記の設定に加え、グローバル側 LAN での ARP 要求に応えるため、次のコマンドを追加してプロキシー ARP を効かせる必要があります。ここでは、プライベート側インターフェースを vlan1、グローバル側インターフェースを eth0 とします。

```
ADD IP ROUTE=1.1.1.5 MASK=255.255.255.255 INT=vlan1 NEXTHOP=0.0.0.0
  PREFERENCE=0 ↵
```

これは、ホスト「1.1.1.5」が vlan1 側に存在することを教えるコマンドです。PREFERENCE=0（優先度最高）を指定しているため、この経路エントリーは他のエントリーよりも優先されます。グローバル LAN 上で 1.1.1.5 への ARP 要求があった場合、このエントリーに基づきルーターが代理応答します（プロキシー APR）。

✎ スタティック NAT をダイナミック ENAT と併用する場合は、先にスタティック NAT の設定を行ってください。レンジ NAT では、NAT テーブルを設定順に検索し、最初にマッチした条件に基づいて変換を行います。そのため、スタティック NAT を先に設定しないとダイナミック ENAT の設定条件と一致してしまい、スタティック NAT の設定が有効にならなくなります。

スタティック ENAT

プライベート IP アドレス＋ TCP/UDP ポート番号から、グローバル IP アドレス＋ TCP/UDP ポート番号への 1 対 1 変換を行います。どのアドレス＋ポートをどのアドレス＋ポートに変換するかは、あらかじめ固定的に設定します。固定グローバルアドレスが 1 個しかないような環境で、特定のサービスを外部に公開したいようなときに利用できます。

✎ スタティック ENAT は、必ずダイナミック ENAT と組み合わせて使用します。あらかじめダイナミック ENAT の設定を行い、スタティック ENAT で使用するアドレスの範囲を指定しておく必要があります。

- プライベート IP アドレス「A」＋ TCP/UDP ポート番号「aa」を、あらかじめ設定したグローバル

IP アドレス「X」＋ TCP/UDP ポート番号「xx」に変換します。また、その逆変換を行います。
- TCP/UDP ポート番号を使用するため、プロトコルタイプは TCP/UDP のみとなります。
- 両方向からの接続が可能です（プライベート IP アドレス←→グローバル IP アドレス）

■ 次のようなアドレス変換を行うスタティック ENAT の設定例を示します。

- プライベート IP アドレス「192.168.10.3」の TCP ポート 80 番を、グローバル IP アドレス「1.1.1.3」の TCP ポート 80 番 に変換します。また、その逆を行います。
- プライベート IP アドレス「192.168.10.4」の TCP ポート 20 番を、グローバル IP アドレス「1.1.1.3」の TCP ポート 20 番 に変換します。また、その逆を行います。
- プライベート IP アドレス「192.168.10.4」の TCP ポート 21 番を、グローバル IP アドレス「1.1.1.3」の TCP ポート 21 番 に変換します。また、その逆を行います。

また、スタティック ENAT の前提として、プライベート IP アドレス「192.168.10.0/24」をグローバル IP アドレス「1.1.1.3」に変換するダイナミック ENAT の設定を施します。

```
ENABLE IP NAT ↵
ADD IP NAT IP=192.168.10.0 MASK=255.255.255.0 GBLIP=1.1.1.3 ↵
ADD IP NAT IP=192.168.10.3 PROT=TCP PORT=80 GBLIP=1.1.1.3 GBLPORT=80 ↵
ADD IP NAT IP=192.168.10.4 PROT=TCP PORT=20 GBLIP=1.1.1.3 GBLPORT=20 ↵
ADD IP NAT IP=192.168.10.4 PROT=TCP PORT=21 GBLIP=1.1.1.3 GBLPORT=21 ↵
```

✎ レンジ NAT では、グローバル IP アドレスが不定な場合はスタティック ENAT を使えません。その場合は、ファイアウォール NAT を使用してください。

ダイナミック NAT

複数のプライベート IP アドレスから複数のグローバル IP アドレスへの多対多変換を行います。アドレス変換時には、あらかじめ指定された範囲から使用されていないアドレスが自動的に選択されて変換されます。

- 複数のプライベート IP アドレス「A～C」を、複数のグロ―バル IP アドレス「X～Z」の中で使用されていないアドレスに変換します。
- IP アドレス変換なので、上位のプロトコルタイプには依存しません。
- 片方向からのみ接続できます（プライベート IP アドレス→グローバル IP アドレス）。

✎ ダイナミック NAT は、他の NAT に比べてメリットが少ないためあまり使われません。

■ プライベート IP アドレス「192.168.1.1」～「192.168.1.254」を、グローバル IP アドレス「192.168.100.1」～「192.168.100.127」の範囲内で未使用の IP アドレスに変換するダイナミック NAT の設定例を示します。

```
ENABLE IP NAT ↵
ADD IP NAT IP=192.168.1.0 MASK=255.255.255.0 GBLIP=192.168.100.1
  GBLMASK=255.255.255.128 ↵
```

ダイナミック ENAT

1 つのグローバルアドレスを複数のホストで共用するもっとも一般的な NAT で、アドレス・ポート変換、NAPT（Network Address Port Translation）、IP マスカレードなどとも呼ばれます。複数のプライベート IP アドレス＋ TCP/UDP ポート番号を、1 つのグローバル IP アドレス＋複数の TCP/UDP ポート番号に変換します。ポート番号の割り当ては動的に行われます。

- 複数のプライベート IP アドレス＋ TCP/UDP ポート番号「A:aa」、「B:bb」、「C:cc」を、あらかじめ設定した 1 つのグローバル IP アドレス＋それぞれ固有のポート番号「X:xa」、「X:xb」、「X:xc」に変換します。グローバルアドレスを 1 つしか使わないため、各トラフィックの識別はポート番号によることになります。これにより、1 つのグローバル IP アドレスを利用して、複数の端末がグローバルネットワークにアクセスできるようになります。
- TCP/UDP ポート番号を使用するため、プロトコルタイプは TCP/UDP のみとなります。
- 片方向からのみ接続できます（プライベート IP アドレス→グローバル IP アドレス）。

ダイナミック ENAT の設定は、GBLIP パラメーターでグローバルアドレスを明示的に指定する形式と、GBLINTERFACE パラメーターでグローバル側インターフェースを指定するだけの形式があります。後者の場合、GBLINTERFACE パラメーターで指定したインターフェースのアドレスが NAT 用アドレスとして使用されます（ダイヤルアップ環境など、WAN 側のアドレスが不定なときに使用します）。

■ NAT 用グローバルアドレスを明示する場合は、GBLIP パラメーターを使用します。次に、プライベート IP アドレス 192.168.10.1～254 をグローバル IP アドレス 1.2.3.4 に変換するダイナミック ENAT の設定例を示します。

```
ENABLE IP NAT ↵
ADD IP NAT IP=192.168.10.0 MASK=255.255.255.0 GBLIP=1.2.3.4 ↵
```

■ PPP 接続などでグローバル IP アドレスを動的に取得する場合は、GBLIP の代わりに GBLINTERFACE パラメーターで、グローバル側インターフェース名を指定することもできます。この場合、ENAT のグローバル IP アドレスとしては、GBLINTERFACE で指定したインターフェースに割り当てられた IP アドレスが使用されます。

```
ENABLE IP NAT ↵
ADD IP NAT IP=192.168.10.0 MASK=255.255.255.0 GBLINT=ppp0 ↵
```

■ NAT 用グローバルアドレスとしてインターフェースアドレスを使う場合（GBLINT 指定時など）、ルーターからグローバル側に対して MAIL コマンド（「運用・管理」の 224 ページ）、TRACE コマンド（527 ペー

ジ）が使えなくなります。ルーターからグローバル側に TELNET することはできます。ファイアウォールの ENAT では、いずれも可能です。

■ NAT 用グローバルアドレスとしてインターフェースアドレスを使う場合（GBLINT 指定時など）、グローバル側からルーターへの Ping には応答しません。一方、ファイアウォールのダイナミック ENAT では応答します。

■ ダイナミック ENAT 使用時であっても、グローバル側からルーターへの Telnet は可能です。これを防ぐには、ファイアウォール NAT を使うとよいでしょう。ファイアウォール NAT では、グローバル側からのアクセスはすべて拒否します。あるいは、レンジ NAT を使用するのであれば、次のような IP フィルターを併用してください。

```
ADD IP FILTER=0 SO=0.0.0.0 PROTO=TCP DPORT=TELNET AC=EXCLUDE ↵
ADD IP FILTER=0 SO=0.0.0.0 AC=INCLUDE ↵
SET IP INT=ppp0 FILTER=0 ↵
```

■ スタティック ENAT を使用する場合、あらかじめダイナミック ENAT の設定を行ない、スタティック ENAT で使用する IP アドレスの範囲を設定しておく必要があります。

■ スタティック NAT とダイナミック ENAT の両方を使用してアドレス変換を行う場合、設定順序に注意する必要があります。レンジ NAT では、NAT テーブルを設定順に検索し、最初にマッチした条件に基づいて変換を行います。そのため、スタティック NAT を先に設定しないとダイナミック ENAT の設定条件と一致してしまい、スタティック NAT の設定が有効にならなくなります

- よくない設定例（ダイナミック ENAT の設定を先に行っている）

```
ENABLE IP NAT ↵
ADD IP NAT IP=192.168.10.0 MASK=255.255.255.0 GBLIP=1.2.3.4 ↵
ADD IP NAT IP=192.168.10.10 GBLIP=1.2.3.4 ↵
```

- 正しい設定例（スタティック NAT の設定を先に行っている）

```
ENABLE IP NAT ↵
ADD IP NAT IP=192.168.10.10 GBLIP=1.2.3.4 ↵
ADD IP NAT IP=192.168.10.0 MASK=255.255.255.0 GBLIP=1.2.3.4 ↵
```

✎ レンジ NAT で ENAT を設定した場合、ルーターからグローバル側への TRACE、MAIL（メール送信）ができません。

Ethernet 上で NAT を使用する場合の注意事項

ここでは、Ethernet（VLAN を含む）上で NAT を使う場合の注意点について解説します。
Ethernet 上で NAT を使用する場合、NAT 後のグローバルアドレスとして、グローバル側インターフェース

の IP アドレスと異なるアドレスを使用するためには、NAT 用グローバルアドレスを経路表に手動登録し、プロキシー ARP を有効にする必要があります。

✎ NAT 後のグローバルアドレスとしてインターフェースアドレスを使用するときは、経路登録の必要はありません。また、グローバル側が Ethernet か VLAN でないときも必要ありません。

次に、スタティック NAT を使用した場合とダイナミック NAT を使用した場合それぞれについて、ローカル NAT 機能の設定例を示します。以下の各例では、各インターフェースの IP アドレスを次のように設定してあるものと仮定しています。

- vlan1（プライベート側）：192.168.10.1/24
- eth0（グローバル側）：1.1.1.1/24

スタティック NAT

次に示すのは、192.168.10.2 → 1.1.1.2 のスタティック NAT 設定例です。

```
ENABLE IP NAT ↵
ADD IP NAT IP=192.168.10.2 GBLIP=1.1.1.2 ↵
ADD IP ROUTE=1.1.1.2 MASK=255.255.255.255 INT=vlan1 NEXT=0.0.0.0 PREF=0 ↵
```

3 行目の経路設定により、グローバル（eth0）側における 1.1.1.2 への ARP 要求にルーターが代理で応答するようになります。

ダイナミック NAT

次に示すのは、192.168.10.0/24 →1.1.1.16/28 のダイナミック NAT 設定例です。この設定では、192.168.10.0/24 のネットワークから eth0 側への通信時に、送信元 IP アドレスが 1.1.1.16～1.1.1.31 のいずれかの IP アドレスに変換されます。

```
ENABLE IP NAT ↵
ADD IP NAT IP=192.168.10.0 MASK=255.255.255.0 GBLIP=1.1.1.16
  GBLMASK=255.255.255.240 ↵
ADD IP ROUTE=1.1.1.16 MASK=255.255.255.240 INT=vlan1 NEXT=0.0.0.0
  PREF=0 ↵
```

3 行目の経路設定により、グローバル（eth0）側における 1.1.1.16～1.1.1.31 への ARP 要求にルーターが代理で応答するようになります。

グローバル側インターフェースアドレスを使用したダイナミック ENAT

次の例のように、NAT アドレスとしてグローバル側インターフェースに割り当てた IP アドレスを使用する場合は、ARP エントリーの登録は不要です。
ただし、インターフェースアドレスを NAT アドレスとして使用する場合は、グローバル側ネットワークか

らルーターに対して Ping 等ができなくなります。

```
ENABLE IP NAT ↵
ADD IP NAT IP=192.168.10.0 MASK=255.255.255.0 GBLINT=eth0 ↵
```

名前解決

ホスト名から IP アドレスを検索する名前解決の設定方法について解説します。本製品は IP の名前解決に、次の 2 つのメカニズムを使用します。

- ホストテーブル
- DNS（Domain Name System/Domain Name Server）

検索はホストテーブル、DNS の順に行われます。

ホストテーブル

ホストテーブルはホスト名と IP アドレスの対応付けをスタティックに登録したものです。ホストテーブルは本製品がローカルに保持するため、DNS サーバーがないような環境で使用すると便利です。登録したホスト名は TELNET コマンド（「運用・管理」の 380 ページ）、TRACE コマンド（527 ページ）、PING コマンド（319 ページ）などで使用できます。

■ ホストテーブルにホスト名を登録するには ADD IP HOST コマンド（178 ページ）を使います。次の例ではホスト名 bulbul に IP アドレス 192.168.1.1 を対応付けています。

```
ADD IP HOST=bulbul IPADDRESS=192.168.1.1 ↵
```

■ ホストテーブルからエントリーを削除するには DELETE IP HOST コマンド（232 ページ）を使います。

```
DELETE IP HOST=bulbul ↵
```

■ ホスト名に対応するアドレスを変更するには SET IP HOST コマンド（363 ページ）を使います。

```
SET IP HOST=bulbul IPADDRESS=192.168.1.5 ↵
```

■ ホストテーブルの内容を確認するには SHOW IP HOST コマンド（455 ページ）を使います。

DNS

DNS とは、ホスト名から IP アドレスを検索するための分散データベースシステム（Domain Name System）、または、そのためのデータベースサーバー（Domain Name Server）を指します。DNS サーバーは TELNET コマンド（「運用・管理」の 380 ページ）、TRACE コマンド（527 ページ）、PING コマンド（319 ページ）で使用されるほか、DNS リレー機能の転送先としても使用されます。DNS リレー機能の設定については、「IP」の「DNS リレー」をご覧ください。

■ 本製品が使用する DNS サーバーは、ADD IP DNS コマンド（167 ページ）で設定します。PRIMARY パラメーターでプライマリーサーバーを、SECONDARY パラメーターでセカンダリーサーバーを指定します。プライマリー DNS サーバーから 20 秒間応答がなかったときは、セカンダリーサーバーに問い合わせます。セカンダリーサーバーを運用していないときは、SECONDARY パラメーターは省略できます。

```
ADD IP DNS PRIMARY=192.168.10.1 SECONDARY=192.168.10.2 ↵
```

■ IP インターフェースの設定を DHCP で行う場合、DHCP サーバーから DNS サーバーアドレスを取得す

ることもできます。ただし、DHCP サーバーが DNS サーバーアドレスを提供するよう設定されている必要があります。詳細は「IP」の「IP インターフェース」をご覧ください。

■ DNS サーバーは、問い合わせ先のドメインごとに個別に設定することもできます。この機能を使うと、A ドメインの問い合わせはサーバー A に、B ドメインの問い合わせはサーバー B に、その他の問い合わせはすべてサーバー C に送るよう設定することもできます。ドメインを指定するには、ADD IP DNS コマンド（167 ページ）の DOMAIN パラメーターを指定します。
次の例では、mikan.fruit.xxx ドメインの問い合わせは 172.20.10.1、172.20.10.2 に、ringo.fruit.xxx ドメインの問い合わせは 172.20.20.1、172.20.20.2 に、その他の問い合わせはすべて 192.168.10.1 に送ります。

```
ADD IP DNS PRIMARY=192.168.10.1 ↵
ADD IP DNS DOMAIN=mikan.fruit.xxx PRIMARY=172.20.10.1
  SECONDARY=172.16.10.2 ↵
ADD IP DNS DOMAIN=ringo.fruit.xxx PRIMARY=172.20.20.1
  SECONDARY=172.16.20.2 ↵
```

✎ ドメイン指定で DNS サーバーを登録するには、あらかじめデフォルトの DNS サーバーを設定しておく必要があります。

✎ DNS サーバーは 10 ドメインまで指定できます（ANY を除く）。

■ DNS サーバーの設定は SHOW IP DNS コマンド（445 ページ）、SHOW IP コマンド（429 ページ）で確認できます。

■ システム名（sysName）にフル表記のホスト名を設定しておくと、DNS 検索時に必要に応じてドメイン名が補完されます。たとえば、sysName に「gw.example.com」を設定している場合（システム名は SET SYSTEM NAME コマンド（「運用・管理」の 267 ページ）で設定します）、次のように TELNET コマンド（「運用・管理」の 380 ページ）を実行すると、bulbul のあとにドメイン名「example.com」が補われ、「bulbul.example.com」に対して DNS の検索が行われます。

```
SET SYSTEM NAME=gw.example.com ↵
TELNET bulbul ↵
```

DNS キャッシュ

DNS キャッシュ機能は、DNS サーバーからの応答をルーターのメモリーに保存しておくことで、2 回目以降 DNS サーバーへの問い合わせを行わずにメモリー上の情報を参照する機能です。DNS キャッシュは、ルーター自身がアドレス解決する場合と DNS リレー機能で別ホストの要求を処理するときの両方で有効です。DNS キャッシュ機能はデフォルトではオフになっています。DNS キャッシュ機能をオンにするには、SET IP DNS CACHE コマンド（358 ページ）の SIZE パラメーターで、キャッシュエントリー容量を 0 以外に設定します。

■ DNS 情報を 100 個まで保持できるようにするには、次のようにします。

```
SET IP DNS CACHE SIZE=100 ↵
```

✎ キャッシュエントリーは 100 個当たり約 30KB のメモリーを消費します。

■ キャッシュエントリーの有効期限は SET IP DNS CACHE コマンド（358 ページ）の TIMEOUT パラメーターで設定します。有効範囲は 1〜60 分。デフォルトは 30 分です。

```
SET IP DNS CACHE TIMEOUT=15 ↵
```

■ キャッシュサイズ、登録エントリー数などの情報は、SHOW IP DNS コマンド（445 ページ）で確認できます。

```
SHOW IP DNS ↵
```

■ キャッシュテーブルの内容は、SHOW IP DNS CACHE コマンド（447 ページ）で確認できます。

```
SHOW IP DNS CACHE ↵
```

ARP

IP アドレスから物理アドレスを検索する ARP（Address Resolution Protocol）関係の機能について説明します。

概要

ARP

Ethernet 上での通信は、たとえ上位で IP を使用していたとしても、最終的には Ethernet アドレス（MAC アドレス）を使って行われます。ARP はこれを支援する IP の重要なサポートプロトコルです。
同じ Ethernet LAN に所属する 2 台のホストが IP で通信する場合を考えます。ホスト 192.168.10.1 は Telnet サーバー、ホスト 192.168.10.100 が Telnet クライアントだとします。
Telnet セッションを開始しようとするクライアントは、最初に ARP Request パケットをブロードキャストして、サーバーの IP アドレス「192.168.10.1」に対応する MAC アドレスを要求します。これに対し、サーバーは ARP Reply パケットでクライアントに自分の MAC アドレスを伝えます。これで初めて、クライアントはサーバーに IP パケット（TCP Syn パケット）を直接送信できるようになります。
ルーター越えの通信でも ARP は使用されます。なぜならば、別の IP ネットワーク上にあるホストと通信するためには、ルーターにパケットを送りつけて IP パケットの転送を依頼しなくてはならないからです。ルーターに IP パケットを送る手順は、前述したクライアント、サーバー間の通信と何ら変わりません。ルーターに IP パケットを届けるためには、最初にルーターの MAC アドレスを知らなくてはならないからです。
通常 IP ホストは、ARP によって学習した MAC アドレスと IP アドレスの対応付けを ARP キャッシュと呼ばれるテーブルに保存しています。これは、ARP パケットのブロードキャストを減らすためです。IP 通信の開始時には、最初に ARP キャッシュを検索し、検索に失敗したときだけ ARP リクエストをブロードキャストします。また、ARP エントリーにはタイマーが設定され、一定時間通信のなかったエントリーは削除（エージング）されるようになっています。

ARP エントリーの手動登録

通常、ARP キャッシュはプロトコルスタックの働きによって動的に構築・維持されていくため、管理者が手動で行うべきことはありません。しかしながら、状況に応じて手動で ARP エントリーを登録することもできます。

■ スタティック ARP エントリーを追加するには、ADD IP ARP コマンド（162 ページ）を使います。

- Ethernet 上の ARP エントリーを登録するには、ETHERNET パラメーターで MAC アドレスを指定します。

```
ADD IP ARP=192.168.10.5 INT=eth0 ETHERNET=00-00-f4-33-22-11 ↵
```

- VLAN 上の ARP エントリーを登録するには、ETHERNET パラメーターで MAC アドレスを、PORT パラメーターでスイッチポートの番号を指定します。

```
ADD IP ARP=192.168.10.8 INT=vlan1 PORT=2 ETHERNET=00-00-f4-86-86-46 ↵
```

■ ARP エントリーを削除するには、DELETE IP ARP コマンド（225 ページ）を使います。スタティックエントリーだけでなく、ダイナミックエントリーを削除することも可能です。

```
DELETE IP ARP=192.168.10.5 ↵
```

■ ARP キャッシュの内容を確認するには、SHOW IP ARP コマンド（432 ページ）を実行します。

```
SHOW IP ARP ↵
```

ARP キャッシュログ

本製品は、ARP キャッシュの変更（登録・削除）をログに記録できます。

■ ARP キャッシュログを有効にするには、ENABLE IP ARP LOG コマンド（294 ページ）を使います。デフォルトは無効です。

```
ENABLE IP ARP LOG ↵
```

■ ARP キャッシュログを表示するには、SHOW LOG コマンド（「運用・管理」の 315 ページ）を使います。SHOW LOG コマンド（「運用・管理」の 315 ページ）では他のログメッセージも表示されますが、「TYPE=ARP」を指定すれば ARP 関連のログだけを見ることができます。

```
SHOW LOG TYPE=ARP ↵
```

```
Manager > show log type=arp

 Date/Time   S Mod  Type  SType Message
 ------------------------------------------------------------------------------
 18 08:18:55 3 IPG  ARP   UPDAT  vlan1 del 00-00-f4-90-19-9b (172.17.28.5)
 18 08:18:55 3 IPG  ARP   UPDAT  vlan1 del 00-00-f4-95-30-6a (172.17.28.157)
 18 08:18:55 3 IPG  ARP   UPDAT  vlan1 del 00-00-f4-95-9f-31 (172.17.28.164)
 18 08:18:55 3 IPG  ARP   UPDAT  vlan1 del 00-50-56-07-36-81 (172.17.28.220)
 18 08:18:55 3 IPG  ARP   UPDAT  vlan1 del 00-0c-76-14-3f-c5 (172.17.28.232)
 18 08:18:57 3 IPG  ARP   UPDAT  vlan1 add 00-00-f4-90-19-9b (172.17.28.5)
 18 08:19:04 3 IPG  ARP   UPDAT  vlan1 add 00-90-99-c2-2b-00 (172.17.28.32)
 18 08:19:06 3 IPG  ARP   UPDAT  vlan1 add 00-50-56-07-36-81 (172.17.28.220)
 18 08:19:19 3 IPG  ARP   UPDAT  vlan1 add 00-00-f4-95-30-6a (172.17.28.157)
 18 08:19:22 3 IPG  ARP   UPDAT  vlan1 add 00-00-fe-be-ef-00 (172.17.28.238)
 18 08:20:19 3 IPG  ARP   UPDAT  vlan1 add 00-00-f4-95-fb-d4 (172.17.28.101)
 18 08:20:25 3 IPG  ARP   UPDAT  vlan1 add 00-00-e2-59-56-48 (172.17.28.233)
 18 08:20:26 3 IPG  ARP   UPDAT  vlan1 add 00-e0-18-8a-30-ad (172.17.28.230)
 18 08:20:30 3 IPG  ARP   UPDAT  vlan1 add 00-03-93-6b-70-a0 (172.17.28.219)
 18 08:20:32 3 IPG  ARP   UPDAT  vlan1 add 00-03-93-70-f3-84 (172.17.28.141)
 18 08:20:58 3 IPG  ARP   UPDAT  vlan1 add 00-06-5b-88-80-41 (172.17.28.1)
 18 08:21:51 3 IPG  ARP   UPDAT  vlan1 add 00-09-41-1c-5d-2f (172.17.28.185)
 18 08:22:25 3 IPG  ARP   UPDAT  vlan1 add 00-00-cd-0a-40-4e (172.17.28.185)
 18 08:22:59 3 IPG  ARP   UPDAT  vlan1 add 00-0c-76-14-3f-c5 (172.17.28.232)
 18 08:23:20 3 IPG  ARP   UPDAT  vlan1 add 00-00-f4-95-9f-31 (172.17.28.164)
 18 08:23:35 3 IPG  ARP   UPDAT  vlan1 add 00-e0-06-09-55-66 (172.17.28.251)
```

```
18 08:24:16 3 IPG  ARP   UPDAT  vlan1 add 00-90-99-15-08-fc (172.17.28.105)
18 08:25:07 3 IPG  ARP   UPDAT  eth1 add 00-90-99-ae-b0-02 (192.168.129.201)
--------------------------------------------------------------------------------
```

ログメッセージ本体（Message）の表示項目は、左から順に IP インターフェース名、イベント（add か del）、MAC アドレス、IP アドレスです。

✎ あるIPアドレスに対応するMACアドレスが変更された場合は、delイベントとaddイベントが生成されます。

■ ARP キャッシュログの有効・無効は SHOW IP コマンド（429 ページ）で確認できます。「IP ARP LOG」欄をご覧ください。

```
SHOW IP ↵
```

プロキシー ARP

プロキシー ARP は、実際に IP アドレスを所有しているホストに代わって、ルーターが自分自身の MAC アドレスで代理応答する機能です。おもに、同じ IP サブネットに所属しているものの、物理的には同一 LAN 上でないため ARP が届かない機器同士の通信を可能にする目的で使用されます。
SLIP や PPP で LAN に接続しているリモートホストと、実際に LAN 上にいるホストとの通信を可能にしたり、サブネットマスクをサポートしていないデバイスをサブネット環境で使用する場合などに使われます。また、Ethernet・Ethernet 間で NAT を使用する場合にも、プロキシー ARP が必要なケースがあります。
デフォルトでは、Ethernet 上のすべての IP インターフェースでプロキシー ARP が有効になっており、受信した ARP Request の対象アドレス（への最適経路）が受信インターフェースとは異なるインターフェース上にあることを知っている場合、自分自身の MAC アドレスで代理応答し、代理応答に基づいて送られてきたパケットを実際の宛先にルーティングします。

■ プロキシー ARP の有効・無効は ADD IP INTERFACE コマンド（179 ページ）、SET IP INTERFACE コマンド（364 ページ）の PROXYARP パラメーターで変更できます。ON を指定した場合は有効に、OFF を指定した場合は無効になります。デフォルトは ON です。

```
ADD IP INT=eth0 IP=192.168.10.1 MASK=255.255.255.0 PROXYARP=OFF ↵
```

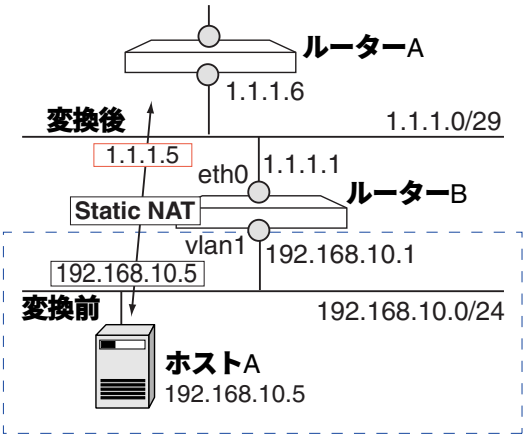
```
SET IP INT=eth0 PROXYARP=OFF ↵
```

マルチホーミングを使って同一 Ethernet 上に複数の論理インターフェースを作成している場合、プロキシー ARP の有効・無効はすべての論理インターフェースに共通して適用されます。

■ プロキシー ARP の状態は、SHOW IP INTERFACE コマンド（458 ページ）で確認できます。「PArp」欄の表示が「On」なら有効、「Off」なら無効です。

スタティック NAT 時の設定

プロキシー ARP を効かせるために手動で設定を行う例として、Ethernet・Ethernet 間の NAT で、グローバルアドレスにインターフェースアドレス以外を使うケースを考えます。



ルーター B には、ホスト A のプライベートアドレス「192.168.10.5」をグローバルアドレス「1.1.1.5」に固定的に変換するスタティック NAT の設定が施されています。グローバル側のホストにとって、ホスト A はルーター A とルーター B の間、すなわち、サブネット 1.1.1.0/29（1.1.1.0〜1.1.1.7）に存在するように見えます。これは、先ほどの PPP 接続の例において、LAN 側ホストには PPP ホストが同一 LAN 上にあるように見えたのとよく似た状況です。

しかし、先ほどの例と異なるのは、ルーター B のルーティングモジュールがホスト A の所在を知らないことです。本製品は、その仕様上 NAT の設定だけでは自分宛てでない ARP Request に代理応答しません。Ethernet・PPP 間の NAT ならば ARP を使わないためこのような問題は起きませんが、Ethernet・Ethernet 間の NAT ではこの点に気を付ける必要があります。

最初に、この構成で NAT の設定だけを行った場合の動作について解説します。例として、ルーター A がホスト A と IP の通信を行うとします（実際にはルーター A 経由で外部のホストがアクセスしてきたとお考えください）。

ルーター A にとって、ホスト A のアドレスは 1.1.1.5 です。ルーター A はホスト A が同一 Ethernet セグメントに所属するものと見なして、1.1.1.5 に対する ARP Request をブロードキャストしますが、ホスト A は別セグメント上にあるため応答できません。また、ルーター B も、1.1.1.5 が自分のアドレスではないため応答しません。そのため、ルーター A はホスト A の MAC アドレスを知ることができず、通信が成立しません。

このようなケースでは、管理者が手動で設定を行うことにより、ルーター B に代理応答をさせることができます。レンジ NAT（IP NAT）とファイアウォール NAT では設定方法が異なるため、以下ではそれぞれのケースについて解説します。

■ 前記の構成でレンジ NAT を使っている場合は、ADD IP ROUTE コマンド（189 ページ）でホスト A への経路を明示的に登録し、ルーター B にホスト A の場所を知らせます。ここでは次のようにします。MASK にはホスト経路であることを示すため 32 ビットマスクを指定し、INTERFACE にはホスト A が存在するインターフェース（vlan1）を指定します。PREFERENCE は経路の優先度を指定するもので、0 はもっとも優先度の高い経路であることを示します。

```
ADD IP ROUTE=1.1.1.5 MASK=255.255.255.255 INT=vlan1 NEXTHOP=0.0.0.0
  PREFERENCE=0 ↵
```

これにより、ホスト A（1.1.1.5）に対するプロキシー ARP が有効になり、ルーター A からの ARP Request に代理応答するようになります。

■ 一方、ファイアウォール NAT を使っている場合はもう少し複雑な手順になります。

1. 最初にグローバル側（eth0）インターフェースをマルチホーミングし、代理応答したいアドレス（ホスト A のアドレス）を 32 ビットマスクで割り当てます。

   ```
   ADD IP INT=eth0-1 IP=1.1.1.5 MASK=255.255.255.255 ↵
   ```

2. 次に作成した論理インターフェースをファイアウォールポリシーに追加します。ここでは、PUBLIC（外部）インターフェースとして設定しています。

   ```
   ADD FIREWALL POLICY=net INT=eth0-1 TYPE=PUBLIC ↵
   ```

3. PUBLIC 側からのパケットはデフォルトで遮断されるため、これを通過させるためのルールを設定します。ホスト A に対するすべてのパケットを許可する場合は次のようにします。GBLIP は NAT 変換後のグローバルアドレス、IP は NAT 前のプライベートアドレスです。

   ```
   ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=eth0-1 PROT=ALL
     GBLIP=1.1.1.5 IP=192.168.10.5 ↵
   ```

   また、セキュリティーを重視するなら、特定のサービスだけを許可するほうがよいかもしれません。HTTP サービスだけを許可するには次のようにします。

   ```
   ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=eth0-1 PROT=TCP
     GBLIP=1.1.1.5 GBLPORT=80 IP=192.168.10.5 PORT=80 ↵
   ```

4. さらに、ホスト A から通信を開始した場合もスタティック NAT が有効に働くように、ホスト A からのパケットがスタティック NAT インターフェース（eth0-1）にルーティングされるよう、ポリシーフィルターを設定します。

   ```
   ADD IP FILTER=100 SOURCE=192.168.10.5 SMASK=255.255.255.255
     POLICY=1 ↵
   SET IP INT=vlan1 POLICYFILTER=100 ↵
   ADD IP ROUTE=0.0.0.0 INT=eth0-1 NEXTHOP=1.1.1.6 POLICY=1 ↵
   ```

   このフィルターは必須というわけではありませんが、設定しなかった場合、ホスト A から外部への通信を開始した場合に、始点アドレスがスタティック NAT アドレス（ここでは 1.1.1.5）ではなく、ダイナミック ENAT 用のアドレスに変換されてしまうことがあります。詳細については、「ファイアウォール」の章の「スタティック NAT」の説明をご覧ください。この動作は、ファイアウォール NAT の仕様となっています。

これにより、ルーター A から 1.1.1.5 への ARP Request に対して、ルーター B が応答するようになります。1.1.1.5 はルーター B 自身のアドレスなので厳密には代理応答と呼べないかもしれませんが、NAT 設定にしたがいルーター B は受け取ったパケットの終点アドレスを変換してホスト A に転送します。

IP フィルター

✎ 以下の説明内容は、旧バージョン仕様のものです。最新バージョンでは、任意の番号の ID に対して、IP フィルターの種類を設定できるよう拡張されています。（参照：ADD IP FILTER コマンド（169 ページ）の TYPE パラメーター）

IP フィルターは、送受信インターフェースにおいて IP パケットのフィルタリングを行う機能です。
ここでのフィルタリングとは、IP および上位プロトコルヘッダーの情報に基づいてパケットをふるいわけ、一定の条件を満たしたパケットに対して何らかの処理を行うことを意味します。
IP フィルターの機能は、ふるいわけ後の処理内容によって次の 3 つに分類できます。

種類	フィルター番号	機能
トラフィックフィルター	0〜99	受信パケットのヘッダー情報に基づき、パケットを破棄または許可する。不正アクセスを防ぐなど、おもにセキュリティーを高めるために使用する
ポリシーフィルター	100〜199	受信パケットのヘッダー情報に基づき、パケットに内部的な経路選択ポリシー（サービスタイプ）を割り当て、経路選択時の動作に影響を与える。別途、サービスタイプ指定の経路エントリーを作成することにより、パケットごとに異なる経路をとらせることができる（ポリシールーティング）。また、パケットの TOS ビット（D、T、R）書き換えも可
プライオリティーフィルター	200〜299	送信パケットのヘッダー情報に基づき、出力時の絶対優先度を設定する。特定のアプリケーショントラフィックを最優先で出力するような設定ができる（プライオリティールーティング）

表 16:

✎ プライオリティーフィルターは送信側インターフェースに設定するため、Firewall NAT や IP NAT と併用時、フィルターの条件にソースアドレスを指定する場合、NAT 変換後のアドレスを指定する必要があります。

✎ Eth/PPPoE インターフェースでプライオリティーフィルターが動作する条件は以下のいずれかになりますのでご注意ください。(1) 100Mbps の受信インターフェース 1 つに対して、10Mbps の送信インターフェースが 1 つあるとき (2) 100Mbps の受信インターフェース 2 つに対して、100Mbps の送信インターフェースが 1 つあるとき。

✎ IPsec、GRE、L2TP などパケットのカプセリングを行う機能と併用時、フィルターはカプセリング処理後のパケットに対して適用されます。

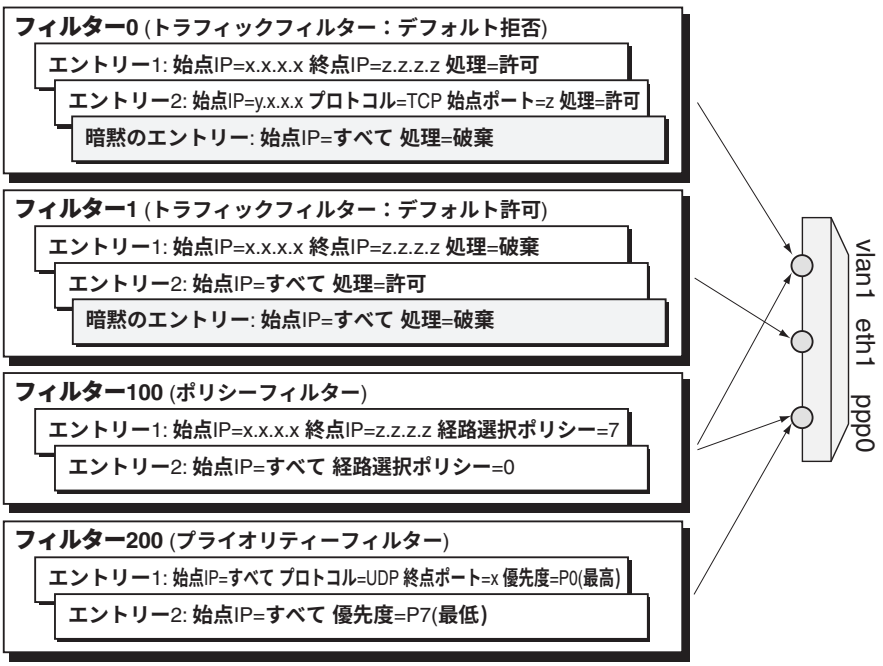
✎ 上記以外にフィルター番号 300〜399 も使用できますが、この範囲は BGP-4 の経路交換を制御するプレフィックスフィルター用の番号であり、パケットフィルタリングとは異なるためここでは扱いません。プレフィックスフィルターの使用方法については「IP」の「経路制御（BGP-4）」をご覧ください。

基本動作

IP フィルターの基本動作について説明します。

フィルターの構成

IP フィルターは、複数のフィルターエントリーで構成されるリストです。各フィルターはフィルター番号で、フィルター内の各エントリーはエントリー番号で識別します。
また、フィルター番号はフィルターの種類（トラフィックフィルター、ポリシーフィルター、プライオリティーフィルター）によって使用できる範囲が決まっています。
個々のフィルターエントリーでは、パケットをふるいわけるための条件と、マッチ時のアクションを指定します。アクションはフィルターの種類によって異なります。



作成可能なフィルター数は次のとおりです。

- トラフィックフィルター 100 個（フィルター番号 0～99）
- ポリシーフィルター 100 個（フィルター番号 100～199）
- プライオリティーフィルター 100 個（フィルター番号 200～299）

各フィルターに追加できるエントリー数（エントリー番号 1～）は空きメモリー容量により変化します。
作成したフィルターは、IP インターフェースに適用して初めて効果を発揮します。フィルターの条件チェック（ふるいわけ）は、トラフィックフィルターとポリシーフィルターは受信インターフェース、プライオリティーフィルターは送信インターフェースで行われます。
一方、フィルターの効果は、トラフィックフィルターでは受信直後（破棄・許可）、ポリシーフィルターでは受信直後（TOS ビット書き換え）と経路表検索時（サービスタイプに基づく経路選択）、プライオリティー

フィルターでは出力時（優先度の高いものから出力）に現れます。
IP インターフェースには、トラフィックフィルター、ポリシーフィルター、プライオリティーフィルターをそれぞれ 1 つずつ適用できます。同じフィルターを複数のインターフェースに割り当ててもかまいません。

フィルター処理の流れ

概要

IP フィルターの処理内容は、次の 2 段階に大きく分けられます。

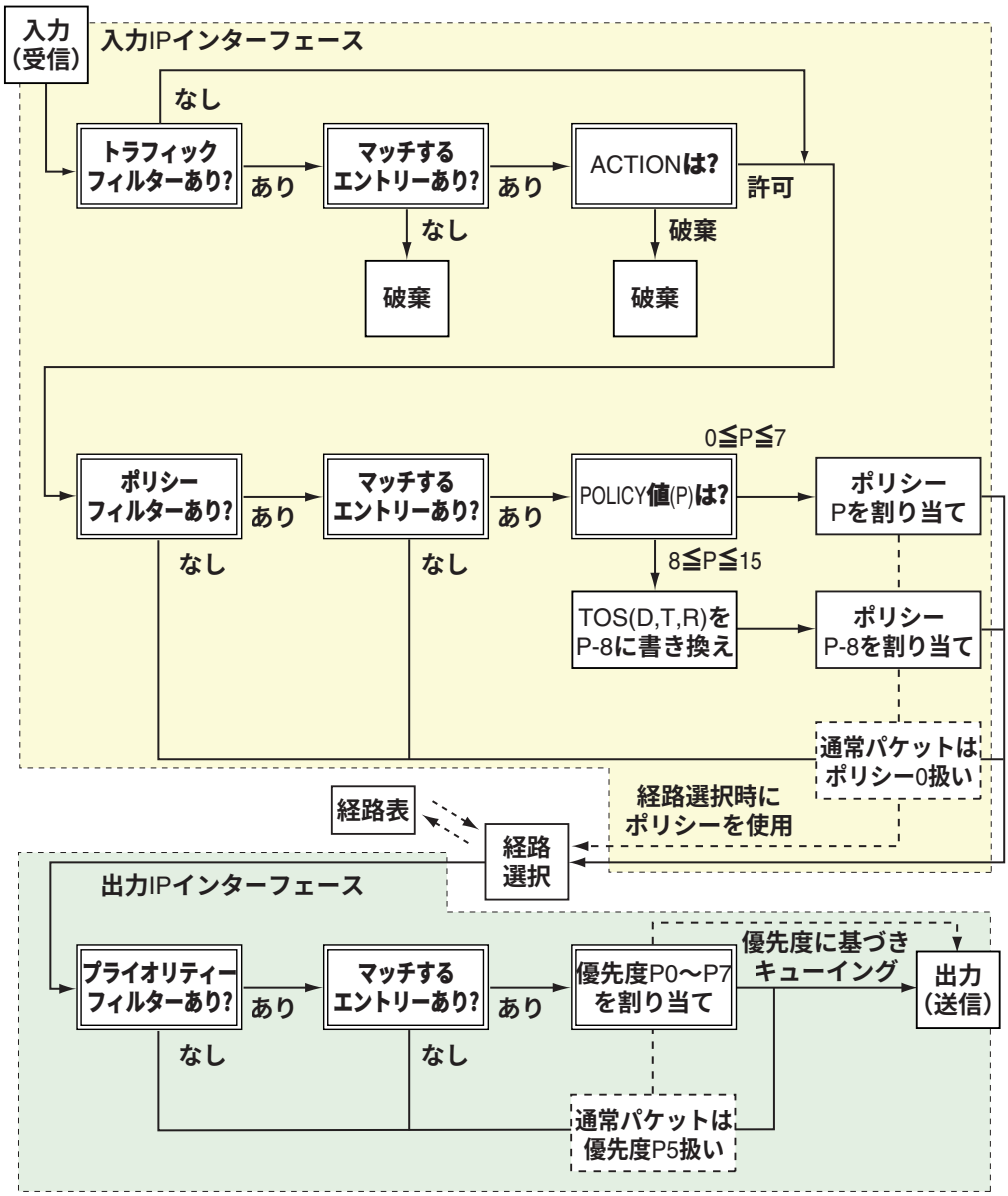
1. 受信（入力）IP インターフェース（トラフィック、ポリシーフィルター）または送信（出力）IP インターフェース（プライオリティーフィルター）において、ヘッダー情報（IP アドレス、ポート番号など）に基づきパケットをふるいわける（フィルタリング）
2. 選別されたパケットに対してなんらかの処理（破棄、経路選択ポリシー設定、優先度設定など）を実行する

トラフィックフィルター、ポリシーフィルター、プライオリティーフィルターは 2 の処理内容が異なるだけであり、パケットを選別するプロセスは共通です。

詳細

IP フィルターの詳細な処理順序について説明します。
ルーターの基本動作をパケット受信、経路選択（転送先決定）、送信の 3 ステップに分けた場合、トラフィックフィルターとポリシーフィルターのチェックはパケット受信時、プライオリティーフィルターのチェックはパケット送信時に行われます。

✎ 以下の説明は、設定上の便宜を最優先して書いたものであり、実際の内部動作を正確に記述したものではありません。あらかじめご了承ください。



1. IP パケットを受信すると、受信インターフェースに適用されているフィルターを、トラフィックフィルター、ポリシーフィルターの順にチェックします。
2. 受信インターフェースにトラフィックフィルターが適用されている場合、フィルター内の各エントリーをエントリー番号の若い順にチェックし、受信パケットのヘッダー情報と一致するものがあるかどうかを調べていきます。

   受信インターフェースにトラフィックフィルターが適用されていない場合は、ポリシーフィルターのチェックに移ります。

   （a） マッチするエントリーが見つかった場合は、該当エントリーの ACTION パラメーターで指定されている処理（アクション）を実行します。トラフィックフィルターでは、最初にマッチしたエントリーが適用されます。

   - EXCLUDE（破棄）の場合はパケットを破棄し、該当パケットの処理を完了します。

- INCLUDE（許可）の場合はトラフィックフィルターのチェックを終了し、ポリシーフィルターのチェックに移ります。

（b） すべてのエントリーをチェックしてもマッチするエントリーが見つからなかった場合は、パケットを破棄して該当パケットの処理を完了します。このように、トラフィックフィルターの末尾には「すべてを破棄する」暗黙のエントリーが存在するので、フィルター作成時には注意が必要です。

3. 受信インターフェースにポリシーフィルターが適用されている場合、フィルター内の各エントリーをエントリー番号の若い順にチェックし、受信パケットのヘッダー情報と一致するものがあるかどうかを調べていきます。

   受信インターフェースにポリシーフィルターが適用されていない場合は、受信インターフェースにおける IP フィルター処理を完了し、通常のパケット処理（転送先決定など）に移ります。

   （a） マッチするエントリーが見つかった場合は、該当エントリーの POLICY パラメーターの指定に基づき、経路選択ポリシー（0〜7）をパケットに割り当てます。ポリシーフィルターでは、最初にマッチしたエントリーが適用されます。

   - POLICY パラメーターの値（ここでは「P」とします）が 0〜7 の場合は、経路選択ポリシー「P」をパケットに割り当てます。
   - POLICY パラメーターの値が 8〜15 の場合は、経路選択ポリシー「P - 8」をパケットに割り当て、さらにパケットの TOS ビット（D、T、R）を「P - 8」に書き換えます。たとえば、マッチしたエントリーの POLICY パラメーターが 10 であれば、経路選択ポリシーは 2（10 - 8）になります。また、TOS ビットも 2（D=0、T=1、R=0）に書き換えられます。

   ここで割り当てる経路選択ポリシーは、経路選択時にのみ使用する内部的な値です。同一宛先に対し、サービスタイプの異なる経路エントリーを複数作成しておくことにより、パケットごとに異なる経路をとらせることができます。

   ✎ 経路エントリーの作成は ADD IP ROUTE コマンド（189 ページ）で行います。また、経路エントリーのサービスタイプ（0〜7）は同コマンドの POLICY パラメーターで指定します。

   （b） すべてのエントリーをチェックしてもマッチするエントリーが見つからなかった場合は、受信インターフェースにおける IP フィルター処理を完了し、通常のパケット処理（転送先決定など）に移ります。

4. パケットの最終宛先がルーター自身でない場合、経路表を検索して転送先（送信インターフェースとネクストホップアドレス）を決定します。このとき、パケットに割り当てられた経路選択ポリシー値と経路エントリーのサービスタイプ（0〜7）が比較され、マッチした経路が優先的に使用されます。経路表に該当するサービスタイプの経路がないときは、デフォルトサービスタイプ（0）の経路エントリーが使用されます。また、ポリシーフィルターにマッチしなかったパケットはポリシー値 0 を持つものとみなされます。転送先が決定すると、パケット送信のための処理に移ります。

5. 送信インターフェースにプライオリティーフィルターが適用されている場合、フィルター内の各エントリーをエントリー番号の若い順にチェックし、送信パケットのヘッダー情報と一致するものがあるかどうかを調べていきます。

   送信インターフェースにプライオリティーフィルターが適用されていない場合は、通常の優先度でパケットを出力し、IP 層の出力処理を完了します。

   （a） マッチするエントリーが見つかった場合は、該当エントリーの PRIORITY パラメーターで指定されている優先度をパケットに割り当てます。パケットの出力は、つねに優先度の高いパケット

から順に行われます。より高い優先度を持つパケットがある場合、下位のパケットは送信されません。これにより、特定のパケット（たとえば UDP のビデオストリーム）を最優先で送信するような設定が可能です。プライオリティーフィルターでは、最初にマッチしたエントリーが適用されます。

(b) すべてのエントリーをチェックしてもマッチするエントリーが見つからなかった場合は、送信インターフェースにおける IP フィルター処理を完了し、通常の優先度でパケットを出力します。

設定手順

IP フィルターの設定は、次の流れで行います。

1. フィルターの作成
   パケットのフィルタリング条件を指定し、マッチしたときのアクション（トラフィックフィルター）、経路選択ポリシー（ポリシーフィルター）、優先度（プライオリティーフィルター）を指定します。フィルターは ADD IP FILTER コマンド（169 ページ）/SET IP FILTER コマンド（360 ページ）で作成・編集します。
2. インターフェースへの適用
   作成したフィルターを IP インターフェースに適用します。フィルターを作成しただけではフィルタリングが行われないので注意してください。フィルターの条件チェック（ふるいわけ）は、トラフィックフィルターとポリシーフィルターは受信インターフェース、プライオリティーフィルターは送信インターフェースで行われます。一方、フィルターの効果がいつ現れるかはフィルターの種類によって異なります。フィルターの適用は ADD IP INTERFACE コマンド（179 ページ）/SET IP INTERFACE コマンド（364 ページ）で行います。
   IP インターフェースには、トラフィックフィルター、ポリシーフィルター、プライオリティーフィルターをそれぞれ 1 つずつ適用できます。1 つのフィルターを複数のインターフェースに割り当ててもかまいません。

以下、各手順について詳しく解説します。

フィルタリング条件の指定

パケットをふるいわけるためのパラメーターとしては、以下のものがあります。これらはフィルターの種類に関係なく共通です。

パラメーター	説明
SOURCE	始点 IP アドレス。必須パラメーター
SMASK	始点マスク（始点 IP アドレスに対するマスク）
DESTINATION	終点 IP アドレス
DMASK	終点マスク（終点 IP アドレスに対するマスク）
PROTOCOL	IP の上位プロトコル
OPTIONS	IP オプション付きかどうか
SIZE	フラグメント再構成後の最大データグラムサイズ

SPORT	始点 TCP/UDP ポート
DPORT	終点 TCP/UDP ポート
ICMPTYPE	ICMP メッセージタイプ
ICMPCODE	ICMP サブコード
SESSION	TCP セッションの方向。すべて、接続開始（Syn=1、Ack=0）、接続済み（Ack=1）から選択する

表 17: IP フィルターの条件パラメーター

以下、条件指定の部分だけの例を挙げます。

SOURCE パラメーター（始点アドレス）は必須です。任意の始点アドレスを対象とするときは、SOURCE=0.0.0.0 のように指定します。また、SOURCE に有効なアドレス（0.0.0.0 以外）を指定するときは、必ず SMASK パラメーターでネットマスクも指定してください。

■ ホスト 192.168.20.100 からの IP パケット

```
SOURCE=192.168.20.100 SMASK=255.255.255.255 ↵
```

■ ホスト 10.10.10.1 宛ての IP パケット

```
SOURCE=0.0.0.0 DESTINATION=10.10.10.1 ↵
```

✎ DMASK 省略時は 255.255.255.255（ホスト）と見なされます。

■ サブネット 172.16.20.0/24 からのパケット

```
SOURCE=172.16.20.0 SMASK=255.255.255.0 ↵
```

■ サブネット 10.10.10.0/24 宛てのパケット

```
SOURCE=0.0.0.0 DESTINATION=10.10.10.0 DMASK=255.255.255.0 ↵
```

■ すべての IP パケット

```
SOURCE=0.0.0.0 ↵
```

■ すべての TCP パケット

```
SOURCE=0.0.0.0 PROTOCOL=TCP ↵
```

■ すべての Ping（ICMP echo）パケット

```
SOURCE=0.0.0.0 PROTOCOL=ICMP ICMPTYPE=ECHO ↵
```

■ Web サーバー 192.168.10.5 からの接続済み HTTP パケット

```
SOURCE=192.168.10.5 SMASK=255.255.255.255 PROTOCOL=TCP SPORT=80
  SESSION=ESTABLISHED ↵
```

■ 10.1.2.3 宛ての Ping（ICMP echo）パケット

```
SOURCE=0.0.0.0 DESTINATION=10.1.2.3 PROTOCOL=ICMP ICMPTYPE=ECHO ↵
```

処理内容の指定

処理内容の指定方法は、フィルターの種類によって異なります。

フィルターの種類	パラメーター	指定内容
トラフィックフィルター（0〜99）	ACTION	EXCLUDE（パケットを破棄する）か INCLUDE（通過させる）を選択する。トラフィックフィルターは、エントリーリストの末尾に「すべてを破棄」する暗黙のエントリーが存在するので、「デフォルト拒否」のフィルターを作成するときは、例外的に許可するルールだけを記述すればよい。一方、「デフォルト許可」のフィルターを作成するときは、拒否するトラフィックのルールを列挙した上で、リストの最後に「すべて許可」のルールを必ず作成すること。そうでないと、暗黙の「すべて破棄」ルールによってすべてのトラフィックが拒否されてしまう。トラフィックフィルターは受信インターフェースで条件のチェックが行われ、マッチした場合はただちにアクションが実行される
ポリシーフィルター（100〜199）	POLICY	パケットに割り当てる「経路選択ポリシー」を指定する。経路選択ポリシー値の範囲は 0〜7 だが、POLICY パラメーターには 0〜15 の範囲を指定することができる。0〜7 を指定した場合は、指定値がそのまま経路選択ポリシー値となる。8〜15 を指定した場合は、経路選択ポリシーとして「POLICY - 8」を割り当て、さらに、パケットの TOS ビット（D、T、R）を「POLICY - 8」に書き換える。たとえば、ポリシーフィルターのエントリー作成時に「POLICY=15」を指定した場合、該当エントリーにマッチしたパケットには経路選択ポリシー「7」（15 - 8）が割り当てられ、TOS ビットも 7（15 - 8）、すなわち、「D=1、T=1、R=1」に書き換えられる。経路選択時には、パケットに割り当てられた経路選択ポリシー値と経路エントリーのサービスタイプ（0〜7）が比較され、マッチした経路が優先的に使用される。経路表に該当するサービスタイプの経路がないときは、デフォルトサービスタイプ（0）の経路エントリーが使用される。ポリシーフィルターにマッチしなかったパケットはポリシー値 0 を持つものとみなされる。また、登録時にサービスタイプを指定しなかった経路エントリーはサービスタイプ 0 とみなされる。ポリシーフィルターは受信インターフェースで条件のチェックとポリシー値の付与（とオプションで TOS ビットの書き換え）が行われ、経路選択時にポリシー値に基づいた選択が行われる

プライオリティーフィルター（200～299）	PRIORITY	パケット送信時の絶対優先度を P0（最高）～P7（最低）で指定する。パケットの送信は、つねに優先度の高いパケットから順に行われる。上位のパケットがある限り、下位のパケットは送信されない。プライオリティーフィルターは送信インターフェースで条件のチェックが行われ、マッチした場合はフィルターが設定した優先度に基づいてパケットの送信順序が決められる

表 18: IP フィルターの処理内容パラメーター

以下、条件指定の例と処理内容の例を組み合わせた、完全なコマンド行の例を示します。

■ ネットワーク 172.16.20.0/24 からのパケットを破棄するトラフィックフィルターを作成する。

```
ADD IP FILTER=0 SOURCE=172.16.20.0 SMASK=255.255.255.0 ACTION=EXCLUDE ↵
```

■ すべての TCP トラフィックに経路選択ポリシー「1」を設定する。

```
ADD IP FILTER=100 SOURCE=0.0.0.0 PROTOCOL=TCP POLICY=1 ↵
```

■ ホスト 192.168.10.100 からのパケットに経路選択ポリシー「7」(= 15 - 8）を設定し、パケットの TOS ビット（TOS オクテットの D、T、R ビット）を 7（= 15 - 8）に書き換える。

```
ADD IP FILTER=100 SOURCE=192.168.10.100 SMASK=255.255.255.255 POLICY=15 ↵
```

192.168.10.100 からのパケットを他のパケットとは別経路で送信したいときは、たとえば次のような経路エントリーを登録してください。

```
ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXT=0.0.0.0 ↵
ADD IP ROUTE=0.0.0.0 INT=ppp1 NEXT=0.0.0.0 POLICY=7 ↵
```

192.168.10.100 からのパケットには経路選択ポリシー「7」が割り当てられるため、デフォルト経路の選択では 2 番目の経路エントリーが選択されます。結果的に同パケットは、ppp1 インターフェースから送出されます。
一方、その他のパケット（ポリシーフィルターにマッチしなかったパケット）は、デフォルトの経路選択ポリシー「0」を持つものとして扱われます。よって、デフォルト経路の選択では 1 番目の経路エントリーが選択され、ppp0 インターフェースから送出されます。

✎ ADD IP ROUTE コマンド（189 ページ）でスタティック経路を登録する際に POLICY パラメーターを省略した場合、同経路のサービスタイプは「0」となります。

✎ パケットに割り当てられているのと同じポリシー値（サービスタイプ）を持つ経路エントリーがないときは、デフォルトサービスタイプ（0）の経路エントリーが使用されます。

ADD IP FILTER コマンド（169 ページ）の POLICY パラメーターに指定した値（0～15）と、パケットに割り当てられる経路選択ポリシー値（0～7)、TOS ビット書き換えの有無と書き換え後の値の関係を次の表にまとめます。

POLICY に指定した値	パケットに割り当てる経路選択ポリシー	TOS ビットの書き換え
0	0	しない
1	1	しない
2	2	しない
3	3	しない
4	4	しない
5	5	しない
6	6	しない
7	7	しない
8	0（8 - 8）	0（D=0, T=0, M=0）
9	1（9 - 8）	1（D=0, T=0, M=1）
10	2（10 - 8）	2（D=0, T=1, M=0）
11	3（11 - 8）	3（D=0, T=1, M=1）
12	4（12 - 8）	4（D=1, T=0, M=0）
13	5（13 - 8）	5（D=1, T=0, M=1）
14	6（14 - 8）	6（D=1, T=1, M=0）
15	7（15 - 8）	7（D=1, T=1, M=1）

表 19: POLICY パラメーターの指定値とその効果

- 「POLICY に指定した値」とは、ADD IP FILTER コマンド（169 ページ）の POLICY パラメーターに指定した値（0〜15）のことです。
- 「パケットに割り当てる経路選択ポリシー」とは、該当エントリーにマッチしたパケットに割り当てられる内部的な経路選択ポリシー値（サービスタイプ値）のことです。経路表を検索するときは、この値と経路エントリーのサービスタイプが比較され、一致したものが優先的に使用されます。経路エントリーのサービスタイプ値は、ADD IP ROUTE コマンド（189 ページ）の POLICY パラメーターで指定できます（0〜7）。
- 「TOS ビットの書き換え」とは、該当エントリーにマッチしたパケットの TOS ビットを書き換えるかどうか、書き換える場合はどのような値に書き換えるかを示します。

■ Telnet トラフィックを最優先で転送する。

```
ADD IP FITLER=200 SOURCE=0.0.0.0 PROTOCOL=TCP DPORT=23 PRIORITY=P0 ↵
```

マッチしたパケットの記録

トラフィックフィルターでは、マッチしたパケットをログに記録するよう設定することもできます。これには、ADD IP FILTER コマンド（169 ページ）の LOG パラメーターを使います。LOG パラメーターを指定しなかった場合は、ログには記録されません。

値	ログタイプ/サブタイプ	記録される情報
NONE		記録しない（デフォルト）

4～1600	「IPFIL/PASS」（INCLUDE 時）、「IPFIL/FAIL」（EXCLUDE 時）	フィルター番号、エントリー番号、IP ヘッダー情報（IP アドレス、プロトコル、ポート番号、サイズ）
	「IPFIL/DUMP」	TCP/UDP/ICMP の場合はデータ部分の先頭 4～1600 バイト。その他プロトコルの場合は IP データの先頭 4～1600 バイト
DUMP	「IPFIL/PASS」（INCLUDE 時）、「IPFIL/FAIL」（EXCLUDE 時）	フィルター番号、エントリー番号、IP ヘッダー情報（IP アドレス、プロトコル、ポート番号、サイズ）
	「IPFIL/DUMP」	TCP/UDP/ICMP の場合はデータ部分の先頭 32 バイト。その他プロトコルの場合は IP データの先頭 32 バイト。「LOG=32」と指定した場合と同じ
HEADER	「IPFIL/PASS」（INCLUDE 時）、「IPFIL/FAIL」（EXCLUDE 時）	フィルター番号、エントリー番号、IP ヘッダー情報（IP アドレス、プロトコル、ポート番号、サイズ）

表 20: LOG オプションの指定値と記録される情報

■ フィルター「2」のエントリー「1」（2/1）により許可（Pass）。IP アドレスは始点が 192.168.20.100 で、終点が 192.168.10.100。プロトコルは TCP で、始点ポート 1040、終点ポート 21。セッション開始パケット（Start）。サイズは 44 バイト（44:0）。

```
16 22:52:29 3 IPG  IPFIL PASS  2/1 Pass 192.168.20.100>192.168.10.100 TCP
                               1040>21 Start 44:0
```

このログは次のフィルターエントリーにマッチしたときのものです。

```
ADD IP FILT=2 SO=192.168.20.100 SMA=255.255.255.255 DEST=192.168.10.100
  DMA=255.255.255.255 AC=INCLUDE ↵
SET IP FILT=2 ENTRY=1 PROTO=TCP DPORT=FTP LOG=HEADER ↵
```

■ フィルター「2」のエントリー「3」（2/3）により拒否（Fail）。IP アドレスは始点が 192.168.20.100 で、終点が 192.168.10.100。プロトコルは TCP で、始点ポート 1042、終点ポート 23。セッション開始パケット（Start）。サイズは 44 バイト（44:0）。

```
16 22:59:48 3 IPG  IPFIL FAIL  2/3 Fail 192.168.20.100>192.168.10.100 TCP
                               1042>23 Start 44:0
```

このログは次のフィルターエントリーにマッチしたときのものです。

```
ADD IP FILT=2 SO=0.0.0.0 DPORT=23 PROTO=TCP AC=EXCLUDE LOG=HEADER ↵
```

■ フィルター「0」のエントリー「1」（0/1）により拒否（Fail）。IP アドレスは始点が 192.168.20.100 で、終点が 192.168.20.1。プロトコルは ICMP で、タイプが 8、コードは 0（8/0）。サイズは 1328:1304 バイト（1328:1304）。

```
16 23:04:03 3 IPG  IPFIL FAIL  0/1 Fail 192.168.20.100>192.168.20.1 ICMP 8/0
                               1328:1304
```

このログは次のフィルターエントリーにマッチしたときのものです。

```
ADD IP FILT=0 AC=EXCLUDE LOG=HEADER SO=0.0.0.0 PROTO=ICMP ICMPTYPE=ECHO ↵
```

インターフェースへの適用

作成したフィルターは IP インターフェースに適用して初めて効果を発揮します。トラフィックフィルター、ポリシーフィルターは受信インターフェースに、プライオリティーフィルターは送信インターフェースに適用してください。すでに存在するインターフェースにフィルターを割り当てるときは SET IP INTERFACE コマンド（364 ページ）を使います。
IP インターフェースには、トラフィックフィルター、ポリシーフィルター、プライオリティーフィルターをそれぞれ 1 つずつ適用できます。1 つのフィルターを複数のインターフェースに割り当ててもかまいません。

■ トラフィックフィルター「0」を ppp0 に割り当て。

```
SET IP INT=ppp0 FILTER=0 ↵
```

■ ポリシーフィルター「100」を vlan1 に割り当て。

```
SET IP INT=vlan1 POLICYFILTER=100 ↵
```

■ プライオリティーフィルター「200」を ppp0 に割り当て。

```
SET IP INT=pp0 PRIORITYFILTER=200 ↵
```

■ フィルターの適用をとりやめるには、フィルター番号の代わりにキーワード NONE を指定します。

```
SET IP INT=ppp0 FILTER=NONE ↵
```

基本は以上です。各フィルタータイプの詳細設定については、以下の各節をご覧ください。

フィルターの削除

■ IP フィルターから特定のエントリーを削除するには、DELETE IP FILTER コマンド（230 ページ）を使います。エントリー番号は可変なので、削除時には必ず SHOW IP FILTER コマンド（449 ページ）で希望するエントリーの番号を調べてから指定してください。

```
DELETE IP FILTER=10 ENTRY=2 ↵
```

✎ エントリーを削除しても、他のエントリーの番号は変わりません。

■ フィルター内の全エントリーを削除するには、ALL を指定します。

```
DELETE IP FILTER=10 ENTRY=ALL ↵
```

■ インターフェースに設定したフィルターの適用を取りやめるには、SET IP INTERFACE コマンド（364 ページ）の FILTER、POLICYFILTER、PRIORITYFILTER パラメーターに NONE を指定します。

```
SET IP INT=vlan1 POLICYFILTER=NONE ↵
```

トラフィックフィルターの設定例

トラフィックフィルターは、受信 IP インターフェースにおいて、ヘッダー情報に基づきパケットの破棄・通過を決定するフィルターです。トラフィックフィルターにはフィルター番号 0〜99 番を割り当てます。

■ 192.168.20.7 からのパケットだけを vlan1 インターフェースで拒否するには次のようにします。その他の IP トラフィックはすべて許可します。いわゆる「デフォルト許可」の設定になります。

```
ADD IP FILTER=0 SOURCE=192.168.20.7 SMASK=255.255.255.255
  ACTION=EXCLUDE ↵
ADD IP FILTER=0 SOURCE=0.0.0.0 ACTION=INCLUDE ↵
SET IP INT=vlan1 FILTER=0 ↵
```

「デフォルト許可」の設定では、拒否するパターンだけを記述します（1 行目）。ただし、トラフィックフィルターのエントリーリストの末尾には、「すべて破棄」を意味する暗黙のエントリーが存在しているため、拒否パターンの後に必ず「すべて許可」のエントリーを明示的に作成する必要があります（2 行目）。拒否パターンだけを書くとすべてのトラフィックが拒否されてしまいますのでご注意ください。
なお、vlan1 側に 192.168.20.0/24 しかサブネットがない場合は、2 行目を次のように書いた方が不正なパケットを遮断できるのでより好ましいかもしれません。

```
ADD IP FILTER=0 SOURCE=192.168.20.0 SMASK=255.255.255.0 ACTION=INCLUDE ↵
```

3 行目では、作成したフィルター「0」を IP インターフェース vlan1 に適用しています。フィルターはインターフェースに適用して初めて効果を持ちます。

■ フィルターにかかったパケットをログに記録するには、LOG パラメーターを使います。LOG パラメーターはエントリーごとに設定するものです。つまり、該当エントリーにマッチしたパケットがログに記録されます。トラフィックフィルター「0」の先頭エントリー（エントリー番号「1」）にマッチしたパケットをログに記録するには次のようにします。

```
SET IP FILTER=0 ENTRY=1 LOG=HEADER ↵
```

✎ エントリー番号は可変なので、必ず SHOW IP FILTER コマンド（449 ページ）で希望するエントリーの番号を調べてから指定してください。

■ vlan1 では原則すべてのパケットを遮断し、192.168.20.7 から 192.168.10.5 の Telnet サービスへのパケットだけを通過させるよう設定するには、次のようにします。いわゆる「デフォルト拒否」の設定です。

```
ADD IP FILT=1 SO=192.168.20.7 SMA=255.255.255.255 DEST=192.168.10.5
  DMA=255.255.255.255 AC=INCLUDE ↵
SET IP FILT=1 ENTRY=1 PROTO=TCP DPORT=TELNET ↵
SET IP INT=vlan1 FILTER=1 ↵
```

「デフォルト拒否」の設定では、許可するパターンだけを記述します。トラフィックフィルターのエントリーリスト末尾には、「すべて破棄」を意味する暗黙のエントリーが存在しているため、拒否パターンを明示的に書く必要はありません。明示的に許可しなかったトラフィックは何もしなくても破棄されます。

■ 2 つのインターフェースの片側からのみ TCP の通信を開始できるようにするには、SESSION パラメーターを使います。ここでは、vlan1 側（192.168.20.0/24）からのみ TCP セッションを開始できるように設定します。eth0 側（192.168.10.0/24）からの TCP パケットは、すでにセッションが開始されている場合（Ack フラグが立っているとき）に限って許可します。

```
ADD IP FILT=0 SO=192.168.10.0 SMA=255.255.255.0 DES=192.168.20.0
  DMA=255.255.255.0 PROTO=TCP SESS=ESTAB AC=INCLUDE ↵
SET IP INT=eth0 FILTER=0 ↵
ADD IP FILT=1 SO=192.168.20.0 SMA=255.255.255.0 DES=192.168.10.0
  DMA=255.255.255.0 PROTO=TCP SESS=ANY AC=INCLUDE ↵
SET IP INT=vlan1 FILTER=1 ↵
```

ポリシーフィルターの設定例

ポリシーフィルターは、受信パケットのヘッダー情報に基づき、パケットに内部的な経路選択ポリシー（サービスタイプ）を割り当て、経路選択時の動作に影響を与えるフィルターです。別途、サービスタイプ指定の経路エントリーを作成することにより、パケットごとに異なる経路をとらせることができます。また、オプションでパケットの TOS ビット（TOS オクテットの D、T、R ビット）を書き換えることもできます。ポリシーフィルターには、フィルター番号 100～199 番を割り当てます。

■ 192.168.10.100 から 192.168.20.0/24 宛てのパケットだけを、ppp0 経由でルーティングするには次のようにします。その他のパケットは ppp1 経由で送信します。

```
ADD IP FILT=100 SO=192.168.10.100 SM=255.255.255.255 DEST=192.168.20.0
  DM=255.255.255.0 POLICY=1 ↵
ADD IP FILT=100 SO=0.0.0.0 DEST=192.168.20.0 DMA=255.255.255.0 POLICY=2 ↵
SET IP INT=vlan1 POLICYFILTER=100 ↵
ADD IP ROUTE=192.168.20.0 MASK=255.255.255.0 INTERFACE=ppp0
  NEXT=192.168.100.2 POLICY=1 ↵
ADD IP ROUTE=192.168.20.0 MASK=255.255.255.0 INTERFACE=ppp1
  NEXT=192.168.100.2 POLICY=2 ↵
```

この例では、192.168.10.100 から 192.168.20.0/24 宛てのパケットに経路選択ポリシー「1」を割り当て（1 行目）、その他のパケットにはポリシー「2」を設定しています（2 行目）。作成したポリシーフィルターを vlan1 に適用したのち（3 行目）、192.168.20.0/24 へのスタティック経路をポリシーごとに 2 つ登録し、それぞれ異なる回線経由で送信させています（4〜5 行目）。

プライオリティーフィルターの設定例

プライオリティーフィルターは、送信パケットのヘッダー情報に基づき、パケット送信時の絶対優先度を設定するフィルターです。特定のトラフィックを最優先で送信するよう設定できます。プライオリティーフィルターには、フィルター番号 200〜299 番を割り当てます。

■ ネットワーク 192.168.20.0/24 側の SSH クライアントと SSH サーバー（192.168.10.5）の間のトラフィックを最優先（P0）で送信し、その他の IP トラフィックは最低の優先度（P7）で送信するプライオリティーフィルターを設定するには次のようにします。

```
ADD IP FILT=200 SO=192.168.20.0 SMA=255.255.255.0 DEST=192.168.10.5
  DMA=255.255.255.255 PROTO=TCP DPORT=22 PRIORITY=P0 ↵
ADD IP FILT=200 SO=192.168.20.0 SMA=255.255.255.0 PROTO=ANY PRIORITY=P7 ↵
SET IP INT=ppp0 PRIORITYFILTER=200 ↵
```

その他

■ IP フィルターはパラメーターが多く、コマンドが長くなりがちです。コマンドラインの入力文字数制限により入力できない場合は、コマンドの省略形を使って入力するか、コマンドを複数行に分割するなどして対処してください。詳細は「運用・管理」の「コマンドプロセッサー」をご覧ください。

■ コマンドパラメーターの詳細についてはコマンドリファレンス編をご覧ください。

■ IP フィルターの設定状況を確認するには SHOW IP FILTER コマンド（449 ページ）を使います。

```
SHOW IP FILTER ↵
```

■ どの IP インターフェースにどの IP フィルターが適用されているかを確認するには SHOW IP INTERFACE コマンド（458 ページ）を使います。

```
SHOW IP INT ↵
```

DNS リレー

DNS リレーは、本製品に対する DNS リクエストを、（実際の）DNS サーバーにリレーする機能です。クライアント側で本製品を DNS サーバーに指定しておけば、サーバーのアドレスが変更されても、本製品に設定されているサーバーアドレスを変更するだけですむため、管理・保守効率が向上します。
また、DNS キャッシュ機能を併用することにより、DNS サーバーへの問い合わせ回数を減らすことができます。
本機能は、DHCP サーバー機能と組み合わせて、本製品が DNS サーバーであるとクライアントに通知することにより、いっそう効果的な運用が可能となります。

基本設定

1. DNS サーバーのアドレスを設定します。

   ```
   ADD IP DNS PRIMARY=192.168.10.5 ↵
   ```

2. DNS リレー機能を有効にします。

   ```
   ENABLE IP DNSRELAY ↵
   ```

設定は以上です。
これで本製品宛ての DNS リクエストが実際の DNS サーバー（192.168.10.5）に転送されるようになります。

DNS キャッシュ

DNS キャッシュ機能は、DNS サーバーからの応答をルーターのメモリーに保存しておくことで、2 回目以降 DNS サーバーへの問い合わせを行わずにメモリー上の情報を参照する機能です。DNS キャッシュは、ルーター自身がアドレス解決する場合と DNS リレー機能で別ホストの要求を処理するときの両方で有効です。
DNS キャッシュ機能はデフォルトではオフになっています。DNS キャッシュ機能をオンにするには、SET IP DNS CACHE コマンド（358 ページ）の SIZE パラメーターで、キャッシュエントリー容量を 0 以外に設定します。

■ DNS 情報を 100 個まで保持できるようにするには、次のようにします。

```
SET IP DNS CACHE SIZE=100 ↵
```

✎ キャッシュエントリーは 100 個当たり約 30KB のメモリーを消費します。

■ キャッシュエントリーの有効期限は SET IP DNS CACHE コマンド（358 ページ）の TIMEOUT パラメーターで設定します。有効範囲は 1〜60 分。デフォルトは 30 分です。

```
SET IP DNS CACHE TIMEOUT=15 ↵
```

■ キャッシュサイズ、登録エントリー数などの情報は、SHOW IP DNS コマンド（445 ページ）で確認できます。

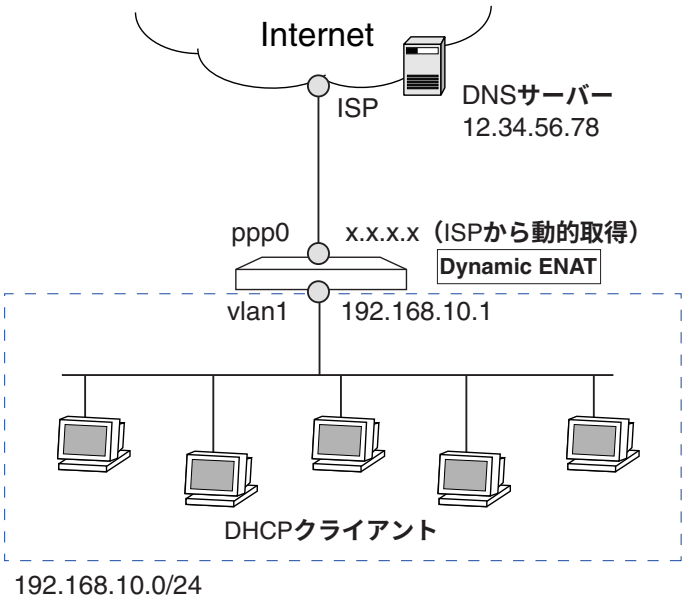
```
SHOW IP DNS ↵
```

■ キャッシュテーブルの内容は、SHOW IP DNS CACHE コマンド（447 ページ）で確認できます。

```
SHOW IP DNS CACHE ↵
```

DHCP サーバー機能と組み合わせた設定例

次のようなネットワーク構成を例に解説します。DHCP クライアントには、192.168.10.240～192.168.20.249 の範囲の IP アドレスを提供します（リース時間 2 時間）。また、DNS サーバーアドレスとしてルーター自身のアドレスを通知し、クライアントからの DNS リクエストを ISP の DNS サーバーに中継します。
ここでは、IP の設定まではすんでいるものと仮定します。



1. DNS リレー機能を有効にします。

   ```
   ENABLE IP DNSRELAY ↵
   ```

2. ISP の DNS サーバーアドレスを設定します。

   ```
   ADD IP DNS PRIMARY=12.34.56.78 ↵
   ```

3. DHCP サーバー機能を有効にします。

   ```
   ENABLE DHCP ↵
   ```

4. DHCP ポリシーを作成し、クライアントに提供する IP パラメーターを設定します。このとき、DNS サーバーの IP アドレスとしてルーター自身のアドレスを通知するよう設定します。

```
CREATE DHCP POLICY=mynet LEASETIME=7200 ↵
ADD DHCP POLICY=mynet SUBNET=255.255.255.0 ROUTER=192.168.10.1
  DNSSERVER=192.168.10.1 ↵
```

5. クライアントに貸し出す IP アドレスの範囲を設定します。

```
CREATE DHCP RANGE=myip POLICY=mynet IP=192.168.10.240 NUMBER=10 ↵
```

設定は以上です。

■ ルーターが IPCP などで DNS サーバーアドレスを動的に取得するよう設定しているときは、手順 2 を次のように変更します。INTERFACE パラメーターには DNS アドレスを取得するインターフェースを指定します。これは通常、WAN 側の PPP（IPCP の場合）または Ethernet（DHCP の場合）インターフェースになります。

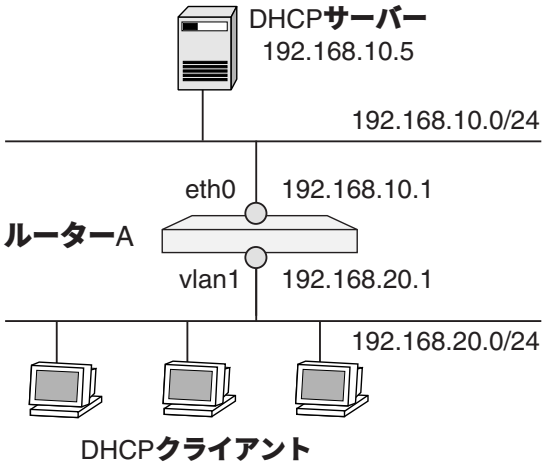
```
ADD IP DNS INT=ppp0 ↵
```

DHCP/BOOTP リレー

DHCP/BOOTP リレーエージェント機能は、受信した DHCP/BOOTP パケットを別セグメントの DHCP/BOOTP サーバーに転送する機能です。
一般的に、DHCP/BOOTP パケットはブロードキャストで送信されるため、クライアントとサーバーは同一のセグメント（LAN）上にある必要があります。
このような場合でも、DHCP/BOOTP リレーエージェント機能を使用すれば、クライアントとサーバーが別の LAN にある場合でも、DHCP/BOOTP を利用することができます。

基本設定

ここでは、次のようなネットワーク構成を例に解説します。



ルーター A の設定

1. IP モジュールを有効にします。

   ```
   ENABLE IP ↵
   ```

2. Ethernet インターフェースに IP アドレスを設定します。

   ```
   ADD IP INT=eth0 IP=192.168.10.1 MASK=255.255.255.0 ↵
   ADD IP INT=vlan1 IP=192.168.20.1 MASK=255.255.255.0 ↵
   ```

3. DHCP/BOOTP リレーエージェント機能を有効にします。

   ```
   ENABLE BOOTP RELAY ↵
   ```

4. DHCP/BOOTP パケットの転送先を指定します。

   ```
   ADD BOOTP RELAY=192.168.10.5 ↵
   ```

以上で設定は完了です。

■ DHCP/BOOTP リレーエージェント機能の設定内容を確認するには、SHOW BOOTP RELAY コマンド（427 ページ）を使います。

■ DHCP/BOOTP パケットの最大転送回数を設定するには、SET BOOTP MAXHOPS コマンド（349 ページ）を使います。デフォルトは 4 ホップです。

```
SET BOOTP MAXHOPS=3 ↵
```

UDP ブロードキャストヘルパー

UDP ブロードキャストヘルパー（UDP ヘルパー、IP ヘルパー）は、特定サービスポート宛ての UDP ブロードキャストを、あらかじめ指定した IP アドレス（ユニキャスト、ブロードキャスト）に転送する機能です。この機能は、ルーターによって隔てられた Windows ネットワークにおいて、クライアントに特別な設定を施さずに別サブネットのドメインコントローラにログインさせたいような場合に便利です。

基本設定

UDP ヘルパー機能の基本的な設定方法について説明します。

1. UDP ブロードキャストヘルパー機能を有効にします。

   ```
   ENABLE IP HELPER ↵
   ```

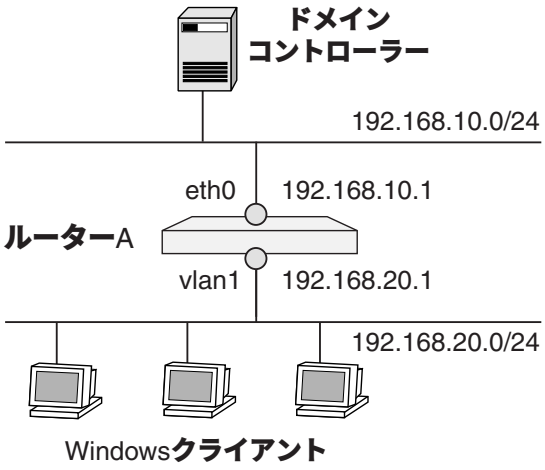
2. 転送元の LAN 側インターフェース、転送対象の UDP パケット（終点 UDP ポートまたは定義済みのサービス名）、転送先の IP アドレスを指定する。定義済みのサービス名については、ADD IP HELPER コマンド（176 ページ）の説明をご覧ください。

   ```
   ADD IP HELPER DESTINATION=192.168.20.100 INT=vlan1 PORT=NETBIOS ↵
   ```

基本設定は以上です。
これで、vlan1 で受信した NetBIOS ブロードキャストパケットが、192.168.20.100 に転送されるようになります。

設定例

次のようなネットワーク構成を例に解説します。ここでは、vlan1 側の Windows クライアントが eth0 側のドメインコントローラーにログインできるようにします。



1. IP モジュールを有効にします。

```
ENABLE IP ↵
```

2. Ethernet インターフェースに IP アドレスを割り当てます。

```
ADD IP INT=eth0 IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan1 IP=192.168.20.1 MASK=255.255.255.0 ↵
```

3. UDP ブロードキャストヘルパー機能を有効にします。

```
ENABLE IP HELPER ↵
```

4. vlan1 で受信した NetBIOS ブロードキャスト（終点ポート 137〜138）をドメインコントローラ 192.168.10.5 に転送するよう設定します。

```
ADD IP HELPER DESTINATION=192.168.10.5 INT=vlan1 PORT=NetBIOS ↵
```

設定は以上です。

■ UDP ブロードキャストヘルパーの設定内容を確認するには、SHOW IP HELPER コマンド（453 ページ）を使います。

■ UDP ブロードキャストヘルパーの設定を解除するには、DELETE IP HELPER コマンド（231 ページ）を使います。

```
DELETE IP HELPER DESTINATION=192.168.10.5 INT=vlan1 PORT=NetBIOS ↵
```

■ UDP ブロードキャストヘルパー機能を無効にするには、DISABLE IP HELPER コマンド（270 ページ）を使います。

セキュリティー

IP 層でのセキュリティーオプションについて紹介します。なお、以下のオプションはデフォルトの状態が推奨設定です。明確な理由がない限り、設定を変更することはお勧めできません。したがって、以下は設定方法の説明というよりもセキュリティー機能の紹介としてお読みください。

ソースルートパケットフィルタリング

デフォルトでは、始点経路制御オプション付きの IP パケット（ソースルートパケット）は転送されずに破棄されます。IP の始点経路制御（ソースルーティング）オプションは通常使用されておらず、むしろ悪用される可能性のほうが高いため、デフォルト設定のままご使用ください。

■ ソースルートパケットの転送許可・不許可は、ENABLE IP SRCROUTE コマンド（310 ページ）、DISABLE IP SRCROUTE コマンド（278 ページ）で変更できます。

```
ENABLE IP SRCROUTE ↵
DISABLE IP SRCROUTE ↵
```

デフォルトは転送不許可（DISABLED）、すなわちソースルートパケットのフィルタリングが有効な状態です。前述の理由から、デフォルト設定のままご使用になることをお勧めします。
ソースルートパケットのフィルタリングが有効な場合（転送不許可の場合）は、始点経路制御オプション付きの IP パケットを受信すると、メッセージタイプ「IPFIL」でサブタイプ「SRCRT」のログメッセージが生成されます。

■ ソースルートパケットのフィルタリングが有効かどうかは、SHOW IP コマンド（429 ページ）で確認できます。「Source-Routed Packets」が「Discarded」ならフィルタリングが有効（転送不許可）です（デフォルト設定）。フィルタリング無効時（転送有効時）は「Forwarded」と表示されます。

フラグメントオフセットフィルタリング

デフォルトでは、フラグメントオフセットが 1 の IP パケットは転送されずに破棄されます。これは、RFC1858 で述べられている Tiny Fragment 攻撃や Overlapping Fragment 攻撃を防ぐためです。デフォルト状態のままご使用ください。
Tiny Fragment 攻撃は、先頭フラグメント（オフセット 0）を最小サイズ（64 ビット=8 オクテット）にし、TCP の制御フラグを第 2 フラグメント（オフセット 1）に送り込むことによって、Syn/Ack フラグによるパケットフィルタリングをかわそうとするものです。
一方、Overlapping Fragment 攻撃では、先頭フラグメント（オフセット 0）に TCP の制御フラグを入れますが、その際にフィルターを通過できるようなパターン（Syn=0、Ack=1）にフラグを設定しておきます。そして、第 2 フラグメントではオフセット値を 1 に設定し、再構成時に第 1 フラグメントの途中から先を上書きすることによって、パケットフィルタリングをかわそうとします。

■ フラグメントオフセットフィルタリングの有効・無効は、ENABLE IP FOFILTER コマンド（299 ページ）と DISABLE IP FOFILTER コマンド（268 ページ）で変更できます。

```
ENABLE IP FOFILTER ↵
DISABLE IP FOFILTER ↵
```

デフォルトではフィルタリングが有効です。上記の攻撃を防ぐため、デフォルト設定のままご使用になることをお勧めします。
フラグメントオフセットフィルタリングが有効な場合は、フラグメントオフセットが 1 の IP パケットを受信すると、メッセージタイプ「IPFIL」、サブタイプ「FRAG」のログメッセージが生成されます。

■ フラグメントオフセットフィルタリングが有効かどうかは、SHOW IP コマンド（429 ページ）で確認できます。「IP Fragment Offset Filtering」が「Enabled」ならフィルタリングが有効です（デフォルト設定）。フィルタリング無効時は「Disabled」と表示されます。

ディレクティドブロードキャストパケットフィルタリング

デフォルトでは、配下のネットワークに対するサブネット/ネットワーク指定ブロードキャストは該当ネットワークに転送されません（ディレクティドブロードキャストフィルタリング）。ディレクティドブロードキャストパケットはサービス妨害（DOS）攻撃などで悪用される恐れがあるため、デフォルト状態のままご使用になることをお勧めします。

■ ディレクティドブロードキャストパケットフィルタリングの設定は IP インターフェースごとに行います。マルチホーミングを使用している場合は、論理インターフェースごとに設定できます。
ADD IP INTERFACE コマンド（179 ページ）、SET IP INTERFACE コマンド（364 ページ）の DIRECTEDBROADCAST パラメーターに OFF を指定するとフィルタリングが有効になります（デフォルト）。一方、ON を指定するとフィルタリングが無効になり、該当インターフェース配下のネットワークに対するブロードキャストパケットが転送されるようになります。

```
ADD IP INT=vlan1 DIRECTEDBROADCAST=ON ↵
SET IP INTERFACE=vlan1 DIRECTEDBROADCAST=OFF ↵
```

デフォルトではフィルタリングが有効です。前述の理由により、デフォルト設定のままご使用になることをお勧めします。
ディレクティドブロードキャストパケットのフィルタリングが有効な場合（転送不許可の場合）は、ディレクティドブロードキャストパケットを受信すると、メッセージタイプ「IPFIL」でサブタイプ「FRAG」のログメッセージが生成されます。

■ ディレクティドブロードキャストフィルタリングの設定は SHOW IP INTERFACE コマンド（458 ページ）で確認できます。「DBcast」の項目が「No」ならフィルタリングが有効（転送しない）、「Yes」ならフィルタリングが無効（転送する）です。

IP アドレスプール

IP アドレスプールは、リモートからの接続時などに、あらかじめプールしておいた範囲から空いている IP アドレスを動的に割り当てる機能です。
ユーザーごとに IP アドレスを固定する必要がない場合、本機能を利用することにより少ない IP アドレスを有効に活用することができます。

■ IP アドレスプールを作成するには、CREATE IP POOL コマンド（217 ページ）を使います。プールには、それぞれ任意の名前を付けることができます。ここでは「ips」とします。

```
CREATE IP POOL=ips IP=192.168.20.200-192.168.20.210 ↵
```

■ L2TP トンネル経由で PPP 接続を受け入れる場合、使用する IP アドレスプールは PPP テンプレート（CREATE PPP TEMPLATE コマンド（「PPP」の 22 ページ）、SET PPP TEMPLATE コマンド（「PPP」の 46 ページ））で指定します。

```
CREATE PPP TEMPLATE=0 BAP=OFF LQR=OFF AUTHENTICATION=EITHER IPPOOL=ips ↵
```

■ IP アドレスプールの設定内容は SHOW IP POOL コマンド（466 ページ）で確認します。

```
SHOW IP POOL ↵
```

■ IP アドレスプールを削除するには、DESTROY IP POOL コマンド（254 ページ）を使います。

```
DESTROY IP POOL=ips ↵
```

設定例

IP アドレスプールを使用した設定例を示します。
ここでは、L2TP トンネル経由で PPP 接続を受け入れる LNS（L2TP Network Server）の設定例を示します。接続してくるユーザーに対しては、IP アドレスプールから空いているアドレスを動的に割り当てます。IP の基本設定までは完了しているものと仮定します。

1. L2TP トンネル経由で接続してくる PPP ユーザーを登録します。

   ```
   ADD USER=remuser PASSWORD=rempass LOGIN=NO ↵
   ```

2. IP プール「ips」を作成し、接続してきたユーザーに割り当てる IP アドレスの範囲を指定します。

   ```
   CREATE IP POOL=ips IP=192.168.20.200-192.168.20.210 ↵
   ```

3. トンネル経由でユーザーが接続してきたときに動的に作成する PPP インターフェース（ダイナミック PPP インターフェース）のテンプレートを作成します。

   ```
   CREATE PPP TEMPLATE=0 BAP=OFF LQR=OFF AUTHENTICATION=EITHER
     IPPOOL=ips ↵
   ```

4. L2TP モジュールを有効にします。

```
ENABLE L2TP ↵
```

5. L2TP サーバーを LNS モードで起動します。

```
ENABLE L2TP SERVER=LNS ↵
```

6. LAC から L2TP トンネルの確立要求を受けたときに、相手を認証するためのパスワードを設定します。

```
ADD L2TP PASSWORD=password ↵
```

7. トンネル確立のために接続してくる LAC の IP アドレスを指定し、またトンネル確立時に動的に作成する PPP インターフェースのテンプレートを指定します。ここでは LAC の IP アドレスを 1.1.1.1 としています。

```
ADD L2TP IP=1.1.1.1 PPPTEMPLATE=0 ↵
```

設定は以上です。

Ping ポーリング

Ping ポーリングは、監視対象機器に Ping パケットを定期送信し、通信が可能かどうか（到達可能かどうか）を監視する機能です。トリガー機能と組み合わせることで、柔軟なネットワーク構成が可能になります。

基本設定

Ping ポーリングの基本的な使用方法について説明します。
ここでは、IP アドレス「10.1.2.3」の機器を監視するものとします。トリガー機能を用いて、到達性が失われたときにスクリプト「pingdown.scp」が、到達性が回復したときにはスクリプト「pingup.scp」が実行されるよう設定します。
なお、IP の設定までは完了しているものとします。

1. ADD PING POLL コマンド（213 ページ）で監視対象機器を指定します。POLL には、識別子として 1〜100 の数値を指定します。本コマンド実行直後はポーリングが停止（無効）状態になっているため、すぐにはポーリングが行われません。実際にポーリングを開始するには、トリガーの設定などをすませた後、ENABLE PING POLL コマンド（316 ページ）を実行する必要があります。

   ```
   ADD PING POLL=1 IP=10.1.2.3 ↵
   ```

2. トリガー機能を有効にします。

   ```
   ENABLE TRIGGER ↵
   ```

3. 対象機器への到達性が失われたときには、PING モジュールの DEVICEDOWN イベントが発生します。これを捕捉するモジュールトリガー「1」を作成します。POLL には、手順 1 で指定した Ping ポーリングの識別子を指定します。

   ```
   CREATE TRIGGER=1 MODULE=PING EVENT=DEVICEDOWN POLL=1
     SCRIPT=pingdown.scp ↵
   ```

   本製品は、10.1.2.3 への Ping に 5 回連続して応答がなかったときに到達性が失われたと判断し、DEVICEDOWN イベントを発生します。到達性喪失の判断条件は、ADD PING POLL コマンド（213 ページ）、SET PING POLL コマンド（396 ページ）の FAILCOUNT、SAMPLESIZE パラメーターで調整可能です。詳しくは次節「機器の状態」、および、各コマンドの解説をご覧ください。
4. 対象機器への到達性が復旧したときには、PING モジュールの DEVICEUP イベントが発生します。これを捕捉するモジュールトリガー「2」を作成します。POLL には、手順 1 で指定した Ping ポーリングの識別子を指定します。

   ```
   CREATE TRIGGER=2 MODULE=PING EVENT=DEVICEUP POLL=1
     SCRIPT=pingup.scp ↵
   ```

本製品は、いったん到達性が失われたと判断した後、10.1.2.3 への Ping に 30 回連続で応答があったとき、到達性が回復したと判断し、DEVICEUP イベントを発生します。到達性回復の判断条件は、ADD PING POLL コマンド（213 ページ）、SET PING POLL コマンド（396 ページ）の UPCOUNT パラメーターで調整可能です。詳しくは次節「機器の状態」、および、各コマンドの解説をご覧ください。

5. Ping ポーリングを開始します。

```
ENABLE PING POLL=1 ↵
```

■ Ping ポーリングの設定は、SHOW PING POLL コマンド（515 ページ）で確認します。

```
SHOW PING POLL ↵
SHOW PING POLL=1 ↵
```

■ トリガーの設定は、SHOW TRIGGER コマンド（「運用・管理」の 364 ページ）で確認します。

```
SHOW TRIGGER ↵
SHOW TRIGGER=1 ↵
```

■ Ping ポーリングのカウンターは、SHOW PING POLL コマンド（515 ページ）の COUNTER オプションで確認します。

```
SHOW PING POLL=1 COUNTER ↵
```

■ Ping ポーリングを最初からやりなおすには、RESET PING POLL コマンド（334 ページ）を実行します。本コマンドを実行すると、カウンターが初期化され、対象機器の状態が「Up」に戻ります。

```
RESET PING POLL=1 ↵
```

✎ 本コマンドの実行により機器の状態が「Down」「Critical Down」から「Up」に戻っても、DEVICEUP イベントは発生しません。

■ Ping ポーリングを一時停止するには、DISABLE PING POLL コマンド（283 ページ）を使います。

```
DISABLE PING POLL=1 ↵
```

■ Ping ポーリングを再開するには、ENABLE PING POLL コマンド（316 ページ）を使います。

```
ENABLE PING POLL=1 ↵
```

■ Ping ポーリングの設定を削除するには、DELETE PING POLL コマンド（251 ページ）を使います。

```
DELETE PING POLL=1 ↵
```

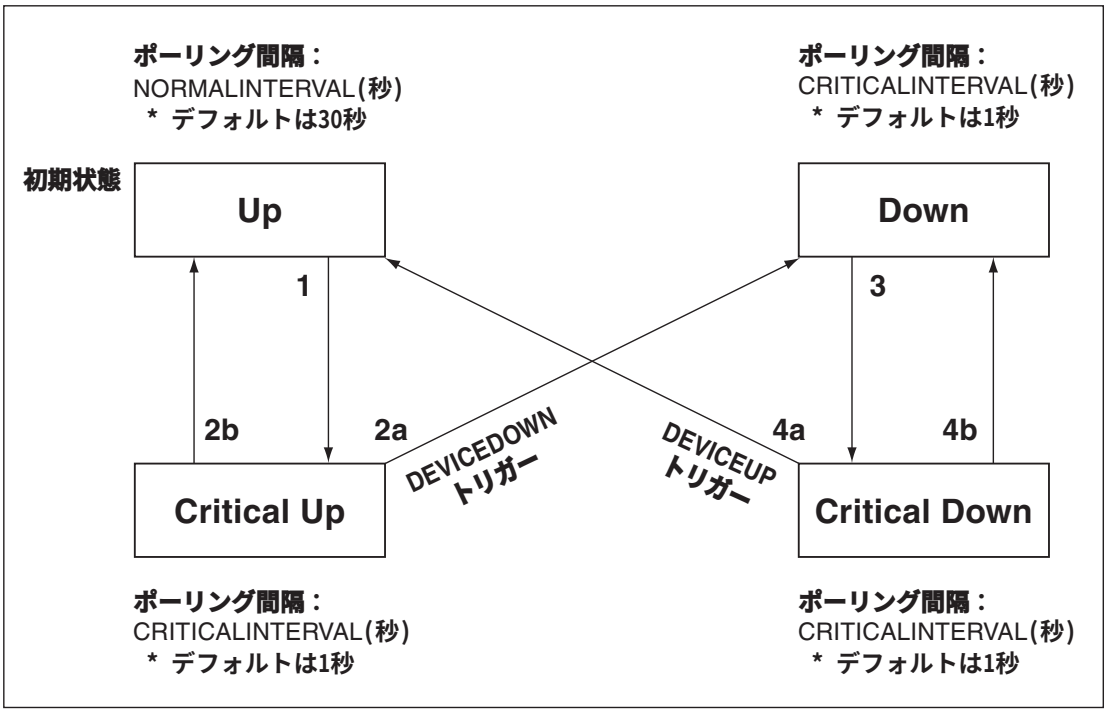
■ Ping ポーリングの実行中であっても、PING コマンド（319 ページ）、TRACE コマンド（527 ページ）は問題なく使用できます。

機器の状態

Ping ポーリングでは、監視対象機器の状態を次の 4 つに分類しています。初期状態は「Up」です。
Ping パケットの送信間隔（ポーリング間隔）には NORMALINTERVAL と CRITICALINTERVAL の 2 種類があり、機器の状態によって使い分けられます。

状態	条件	ポーリング間隔
Up	直前の SAMPLESIZE 回（デフォルト 5 回）の Ping に対して、すべて応答があった状態（無応答が 1 回もない状態）。Ping ポーリング開始時の初期状態です	NORMALINTERVAL（デフォルト 30 秒）
Critical Up	直前の SAMPLESIZE 回（デフォルト 5 回）の Ping に対して、1 回以上、FAILCOUNT 回（デフォルト 5 回）未満の無応答があった状態	CRITICALINTERVAL（デフォルト 1 秒）
Down	（Down 状態への遷移後）直前の Ping に応答がなかった状態	CRITICALINTERVAL（デフォルト 1 秒）
Critical Down	（Down 状態への遷移後）直前の Ping に応答があった状態	CRITICALINTERVAL（デフォルト 1 秒）

表 21: 機器の状態



これら状態間での遷移は次のときに発生します。

遷移前の状態	図中の番号	遷移条件	遷移後の状態
Up	1	直前の Ping に応答がなかった	Critical Up
Critical Up	2a	直前の SAMPLESIZE 回（デフォルト 5 回）の Ping に対して、FAILCOUNT 回（デフォルト 5 回）の無応答があった	Down
	2b	直前の SAMPLESIZE 回（デフォルト 5 回）の Ping に対して、すべて応答があった	Up
Down	3	直前の Ping に応答があった	Critical Down
Critical Down	4a	直前の UPCOUNT 回（デフォルト 30 回）の Ping に対して、すべて応答があった	Up
	4b	直前の Ping に応答がなかった	Down

表 22: 機器の状態遷移

トリガー

Ping ポーリングは、トリガーと併用することを想定した機能です。
トリガーを使用すると、監視対象機器への到達性喪失時と到達性回復時に任意のスクリプトを実行させることができます。
到達性の喪失と回復は、PING モジュール固有のモジュールトリガーを使って捕捉します。
CREATE TRIGGER MODULE コマンド（「運用・管理」の 143 ページ）、SET TRIGGER MODULE コマ

ンド（「運用・管理」の 278 ページ）に、PING モジュール固有のパラメーターを加えたコマンド構文は次のようになります。

```
CREATE TRIGGER=trigger-id MODULE=PING EVENT={DEVICEDOWN|DEVICEUP}
  POLL=poll-id [AFTER=time] [BEFORE=time] [{DATE=date|DAYS=day-list}]
  [NAME=string] [REPEAT={YES|NO|ONCE|FOREVER|count}] [SCRIPT=filename...]
  [STATE={ENABLED|DISABLED}] [TEST={YES|NO|ON|OFF}]


SET TRIGGER=trigger-id POLL=poll-id [AFTER=time] [BEFORE=time]
  [{DATE=date|DAYS=day-list}] [NAME=string]
  [REPEAT={YES|NO|ONCE|FOREVER|count}] [TEST={YES|NO|ON|OFF}]
```

POLL パラメーターには、監視対象機器の Ping ポーリング ID（ADD PING POLL コマンド（213 ページ）の POLL パラメーターに指定した番号）を指定します。また、EVENT パラメーターには、DEVICEDOWN（到達性喪失）か DEVICEUP（到達性回復）のいずれかを指定します。
このトリガーは、POLL パラメーターで指定した ID を持つ監視対象機器への到達性が失われるか（EVENT=DEVICEDOWN のとき）、回復するか（EVENT=DEVICEUP のとき）したときに起動されます。
トリガーから実行されるスクリプトには、特殊な引数として%D（日付）、%T（時刻）、%N（システム名）、%S（シリアル番号）が渡されます。また、引数%1 として Ping ポーリング ID も渡されます。
次にトリガーの例を示します。

■ Ping ポーリング「1」によって監視対象機器への到達性喪失を検出したら、スクリプト「pingdown.scp」を実行するモジュールトリガー「1」を作成します。

```
CREATE TRIGGER=1 MODULE=PING EVENT=DEVICEDOWN POLL=1
  SCRIPT=pingdown.scp ↵
```

ログ

Ping ポーリングによって検出された監視対象機器への到達性喪失と回復は、ログにも記録されます。ログレベルは 3（INFO）、モジュールは PING（58）です。

■ Ping ポーリングのログを表示するには、SHOW LOG コマンド（「運用・管理」の 315 ページ）を使います。SHOW LOG コマンド（「運用・管理」の 315 ページ）では他のログメッセージも表示されますが、「MODULE=PING」を指定すれば PING モジュールのログだけを見ることができます。

```
SHOW LOG MODULE=PING ↵
```

```
Manager > show log module=ping

Date/Time   S Mod  Type  SType Message
-------------------------------------------------------------------------------
```

```
13 23:27:30 3 PING 00061 00001 172.17.28.100 is not reachable (poll=1)
13 23:28:30 3 PING 00061 00001 172.17.28.100 is reachable (poll=1)
-------------------------------------------------------------------------------
```

コマンドリファレンス編

機能別コマンド索引

一般コマンド

IP インターフェース

経路制御（BGP-4）

名前解決

ARP

IP フィルター

DNS リレー

DHCP/BOOTP リレー

ADD BGP AGGREGATE

カテゴリー：IP / 経路制御（BGP-4）

ADD BGP AGGREGATE=*prefix* [MASK=*ipadd*] [SUMMARY={NO|YES}]
[ROUTEMAP[=*routemap*]]

prefix: プレフィックス（IP アドレス/プレフィックス長）
ipadd: IP アドレスまたはネットマスク
routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）

解説

集約経路エントリーを作成する。
集約経路エントリーは、指定したプレフィックスの範囲に収まる、より具体的な経路を 1 つにまとめるもの。たとえば、集約経路エントリー「192.168.0.0/19」を作成すると、この範囲に収まる BGP 経路「192.168.10.0/24」「192.168.20.0/24」「192.168.30.0/24」は、1 つのエントリー「192.168.0.0/19」として BGP の経路表に登録される。
ただし、集約経路エントリーが BGP の経路表に登録されるのは、指定したプレフィックスよりも具体的な（マスクが長い）プレフィックスが BGP で学習された場合だけ。集約経路エントリーは、ATOMIC_AGGREGATE 属性付きで他の AS に通知される。

パラメーター

AGGREGATE　集約後のプレフィックス。ネットワークアドレスとプレフィックス長で指定する。プレフィックス長は MASK パラメーターで指定することも可能。
MASK　AGGREGATE で指定したプレフィックスの有効長。
SUMMARY　集約経路だけを BGP の経路表に入れる場合は YES を指定する。NO を指定したときは、集約前の（より具体的な）個々のエントリーも BGP 経路表に残る。デフォルトは NO。
ROUTEMAP　ルートマップ名。集約経路に属性を設定するために用いる。

例

■集約経路「192.168.0.0/19」を作成する。「SUMMARY=YES」により、集約経路だけが BGP の経路表に入るようにしている。

```
ADD BGP AGGREGATE=192.168.0.0/19 SUMMARY=YES
```

備考・注意事項

集約経路エントリーは、指定範囲内に収まるプレフィックスが BGP で学習された場合にのみ有効となる。

関連コマンド

ADD BGP IMPORT（152 ページ）
ADD BGP NETWORK（153 ページ）
DELETE BGP AGGREGATE（218 ページ）
SET BGP AGGREGATE（336 ページ）
SHOW BGP AGGREGATE（401 ページ）
SHOW BGP ROUTE（425 ページ）

ADD BGP CONFEDERATIONPEER

カテゴリー：IP / 経路制御（BGP-4）

ADD BGP CONFEDERATIONPEER=*1..65534*

解説

コンフェデレーション EBGP ピアのサブ AS 番号を指定する。
自分が所属する AS コンフェデレーションの番号は、SET BGP コマンドの CONFEDERATIONID パラメーターで設定する。また、自分が所属するサブ AS（メンバー AS）番号は、SET IP AUTONOMOUS コマンドで設定する。

パラメーター

CONFEDERATIONPEER　コンフェデレーション EBGP ピアが所属するサブ AS の番号。自サブ AS 番号や AS コンフェデレーション ID と別の番号でなくてはならない。

例

■「192.168.100.2」とコンフェデレーション EBGP セッションを張る。両者が所属するコンフェデレーションの AS 番号は 8686。自分が所属するサブ AS 番号は 10、相手のサブ AS 番号は 20 とする。

```
SET IP AUTONOMOUS=10
SET BGP CONFEDERATIONID=8686
ADD BGP PEER=192.168.100.2 REMOTEAS=20
ADD BGP CONFEDERATIONPEER=20
ENABLE BGP PEER=192.168.100.2
```

備考・注意事項

コンフェデレーションに所属しているすべての AS を指定する必要はない。C-EBGP セッションを張っているピアのサブ AS 番号だけを指定すればよい。

関連コマンド

ADD BGP PEER（154 ページ）
DELETE BGP CONFEDERATIONPEER（219 ページ）
SET BGP（335 ページ）
SET IP AUTONOMOUS（355 ページ）
SHOW BGP CONFEDERATION（405 ページ）

ADD BGP IMPORT

カテゴリー：IP / 経路制御（BGP-4）

ADD BGP IMPORT={**OSPF**|**RIP**|**STATIC**|**INTERFACE**} [ROUTEMAP[=*routemap*]]

routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）

解説

BGP で配布する経路情報のソース（インターフェース経路、静的経路、RIP、OSPF）を指定する。
オプションでルートマップを使えば、経路情報を BGP にインポートする際にフィルタリングを行うこともできる。

パラメーター

IMPORT　BGP に取り込む経路情報のソース。INTERFACE はインターフェース（ダイレクト）経路、STATIC はインターフェース経路を除く静的経路、RIP は RIP 経路、OSPF は OSPF 経路を示す。

ROUTEMAP　インポート時に適用するルートマップ。デフォルトはなし。

例

■インターフェース経路と静的経路を BGP で配布する。

```
ADD BGP IMPORT=INTERFACE
ADD BGP IMPORT=STATIC
```

■OSPF 起源の経路情報を BGP で使用する。インポート時にはルートマップ「ospf_import」を使って、フィルタリングと属性設定を行う。

```
ADD BGP IMPORT=OSPF ROUTEMAP=ospf_import
```

関連コマンド

ADD IP ROUTEMAP（195 ページ）
DELETE BGP IMPORT（220 ページ）
SET BGP IMPORT（341 ページ）
SHOW BGP IMPORT（413 ページ）

ADD BGP NETWORK

カテゴリー：IP / 経路制御（BGP-4）

ADD BGP NETWORK=*prefix* [MASK=*ipadd*] [ROUTEMAP[=*routemap*]]

prefix: プレフィックス（IP アドレス/プレフィックス長）
ipadd: IP アドレスまたはネットマスク
routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）

解説

BGP で配布するネットワークプレフィックスを指定する。
ルーターの経路表に本コマンドで指定したプレフィックスが追加された場合（静的設定や RIP、OSPF などによる）、同プレフィックスは BGP 経路表にもインポートされる。

パラメーター

NETWORK プレフィックス。ネットワークアドレスとプレフィックス長で指定する。プレフィックス長は MASK パラメーターで指定することも可能。
MASK NETWORK で指定したネットワークアドレスに対するプレフィックスの有効長。
ROUTEMAP ルートマップ名。該当プレフィックスに対するフィルタリングや通知時の属性設定に用いる。

例

■プレフィックス 192.168.100.0/24 を BGP で配布する。

```
ADD BGP NETWORK=192.168.100.0/24
```

備考・注意事項

本コマンドで指定したプレフィックスが外部に通知されるのは、ルーターの経路表に該当プレフィックスが登録されている間だけであることに注意。

関連コマンド

DELETE BGP NETWORK（221 ページ）
SHOW BGP NETWORK（417 ページ）
SHOW BGP ROUTE（425 ページ）

ADD BGP PEER

カテゴリー：IP / 経路制御（BGP-4）

■ 通常の構文

```
ADD BGP PEER=ipadd REMOTEAS=1..65534 [CONNECTRETRY={DEFAULT|
    0..4294967295}] [DESCRIPTION[=string]] [EHOPS={DEFAULT|1..255}]
    [HOLDTIME={DEFAULT|0|3..65535}] [INFILTER={NONE|300..399}]
    [INPATHFILTER={NONE|1..99}] [INROUTEMAP[=routemap]] [KEEPALIVE={DEFAULT|
    1..21845}] [MAXPREFIX={OFF|1..4294967295}] [MAXPREFIXACTION={WARNING|
    TERMINATE}] [MINASORIGINATED={DEFAULT|0..3600}] [MINROUTEADVERT={DEFAULT|
    0..3600}] [NEXTHOPSELF={NO|YES}] [OUTFILTER={NONE|300..399}]
    [OUTPATHFILTER={NONE|1..99}] [OUTROUTEMAP[=routemap]] [SENDCOMMUNITY={NO|
    YES}] [LOCAL={NONE|1..15}] [AUTHENTICATION={MD5|NONE}]
    [PASSWORD=password] [CLIENT={NO|YES}] [FASTFALLOVER={NO|YES}]
    [PRIVATEASFILTER={NO|YES}] [DEFAULTORIGINATE={NO|YES}]
```

■ BGP ピアテンプレートを使う場合の構文

```
ADD BGP PEER=ipadd POLICYTEMPLATE=1..30 REMOTEAS=1..65534
    [DESCRIPTION[=string]] [EHOPS={DEFAULT|1..255}] [AUTHENTICATION={MD5|
    NONE}] [PASSWORD=password] [FASTFALLOVER={NO|YES}] [DEFAULTORIGINATE={NO|
    YES}]
```

ipadd: IP アドレス
string: 文字列（1〜63 文字）
routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）
password: パスワード（1〜80 文字。クエスチョンマーク（?）とダブルクォート（"）は使用できない）

解説

BGP ピアを追加する。
ピアは IDLE 状態（セッションを開始していない状態）で追加されるので、BGP セッションを開始するときは ENABLE BGP PEER コマンドを使う。

パラメーター

PEER　BGP ピアの IP アドレス。
REMOTEAS　BGP ピアが所属する AS 番号。自 AS 番号と同じなら I-BGP、違うなら E-BGP ピアとなる。自 AS 番号は SET IP AUTONOMOUS コマンドで設定する。
CONNECTRETRY　BGP コネクション確立の再試行間隔（秒）。デフォルトは 120 秒。0 は再試行しない。
DESCRIPTION　BGP ピアに関する覚え書き（メモ）。
EHOPS　E-BGP セッションにおける BGP メッセージの初期 TTL 値。デフォルトは 1。ルーターをまたい

で E-BGP セッションを張るためには、EHOPS を 2 以上に設定する必要がある。

HOLDTIME　該当ピアとの BGP セッションがダウンしたと認識するまでの時間（Hold Time）（秒）を設定する。実際の Hold Time はセッション開始時のネゴシエーションによって決まる。本パラメーターで設定するのは OPEN メッセージで相手に提案する値。デフォルトは 90 秒。0 はこちらからは提案しないことを意味する。

INFILTER　該当ピアから受信した経路情報に適用する IP プレフィックスフィルターの番号。INFILTER を使用すると、プレフィックス（宛先ネットワークアドレス）によって経路の受け入れ・破棄を行うことができる。IP プレフィックスフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 300～399）。

INPATHFILTER　該当ピアから受信した経路情報に適用する AS パスリストの番号。INPATHFILTER を使用すると、AS_PATH 属性の内容によって経路の受け入れ・破棄を行うことができる。AS パスリストは ADD IP ASPATHLIST コマンドで作成する。

INROUTEMAP　該当ピアから受信した経路情報に適用するルートマップ名。INROUTEMAP を使用すると、各種の基準に基づいて、経路情報をフィルタリングしたり、属性を変更したりできる。ルートマップは ADD IP ROUTEMAP コマンドで作成する。

KEEPALIVE　KEEPALIVE メッセージの送信間隔。HOLDTIME の 1/3 に設定する必要がある。実際の送信間隔は HOLDTIME のネゴシエーションによって決まる。

MAXPREFIX　該当ピアから受け入れ可能な最大プレフィックス数を設定する。OFF の場合は制限を設けない。デフォルトは OFF。

MAXPREFIXACTION　MAXPREFIX パラメーターの値を超えるプレフィックスを受信したときの動作。WARNING はログに記録するだけ。TERMINATE はログに記録した上で該当ピアとのセッションをリセットする。デフォルトは WARNING。

MINASORIGINATED　自 AS 起源の経路情報を含む UPDATE メッセージの最小連続送信間隔。デフォルトは 15 秒

MINROUTEADVERT　他 AS 起源の経路情報を含む UPDATE メッセージの最小連続送信間隔。デフォルトは 30 秒

NEXTHOPSELF　該当ピアに通知する経路の NEXT_HOP として必ず自アドレスを使うかどうか。デフォルトは NO。

OUTFILTER　該当ピアに経路情報を通知する前に適用する IP プレフィックスフィルターの番号。OUTFILTER を使用すると、プレフィックス（宛先ネットワークアドレス）によって経路の通知・破棄を行うことができる。IP プレフィックスフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 300～399）。

OUTPATHFILTER　該当ピアに経路情報を通知する前に適用する AS パスリストの番号。OUTPATHFILTER を使用すると、AS_PATH 属性の内容によって経路の通知・破棄を行うことができる。AS パスリストは ADD IP ASPATHLIST コマンドで作成する。

OUTROUTEMAP　該当ピアに経路情報を通知する前に適用するルートマップ名。OUTROUTEMAP を使用すると、各種の基準に基づいて、経路情報をフィルタリングしたり、属性を変更したりできる。ルートマップは ADD IP ROUTEMAP コマンドで作成する。

SENDCOMMUNITY　UPDATE メッセージに COMMUNITIES 属性を含めるかどうか。同属性の具体的内容はルートマップで設定する。デフォルトは NO。

LOCAL　該当ピアとの通信に使用するローカル IP インターフェースの番号。ローカル IP インターフェースを指定した場合、本ピア宛ての BGP パケットの始点 IP アドレスとして、指定したローカル IP イ

ンターフェースの IP アドレスが使用される。省略時は NONE（ローカル IP インターフェースを使用しない。この場合、BGP パケットの始点 IP アドレスはシステムが決める）。

AUTHENTICATION　該当ピアとの TCP 通信において MD5 認証オプション（TCP MD5 認証）を使用するかどうか。 使用する場合は MD5 を、使用しない場合は NONE を指定する。MD5 を指定した場合は、PASSWORD パラメーターでパスワード（認証鍵）を設定すること。デフォルトは NONE。

PASSWORD　TCP MD5 認証で使用するパスワード（認証鍵）。ピアと同じ値を指定すること。本パラメーターは、AUTHENTICATION パラメーターに MD5 を指定した場合のみ有効。デフォルトはなし。

CLIENT　該当ピアがルートリフレクター（RR）クライアントであるかどうか。本パラメーターは、該当ピアが I-BGP ピアである場合のみ意味を持つ。該当ピアが I-BGP ピアであり、なおかつ、本パラメーターが YES の場合、本製品は該当ピアをクライアントであると見なし、ルートリフレクターとしての動作を行う（クライアントから受信した経路を他のすべてのクライアントとノンクライアントに送信する。また、ノンクライアントから受信した経路は、クライアントにだけ送信する）。NO を指定した場合は、該当ピアをノンクライアントと見なして通常の I-BGP 通信を行う。デフォルトは NO。

FASTFALLOVER　該当ピアとの通信に使用するインターフェースがリンクダウンした場合に、Hold Time の満了を待たず、ただちに該当ピアとの BGP セッションをリセットするかどうか。デフォルトは NO。なお、VLAN インターフェースがリンクダウンしたと認識されるためには、メンバーポートがすべてリンクダウンする必要があることに注意。

PRIVATEASFILTER　プライベート AS 番号（64512～65535）をフィルタリングするかどうか。本パラメーターに YES を指定した場合、該当ピアに UPDATE メッセージを送信するとき、AS_PATH 属性からプライベート AS 番号を削除した上で送信する。デフォルトは NO。

DEFAULTORIGINATE　該当ピアにデフォルト経路（0.0.0.0/0）を通知するかどうか。デフォルトは NO。デフォルト経路を通知するには、ENABLE BGP DEFAULTORIGINATE コマンドの設定が必要。

POLICYTEMPLATE　該当ピアとの通信パラメーターを提供する BGP ピアテンプレートの番号。BGP ピアテンプレートは ADD BGP PEERTEMPLATE コマンドで作成する。BGP ピアテンプレートを使用している場合、本コマンドで指定できるその他のパラメーターは PEER、REMOTEAS、DESCRIPTION、AUTHENTICATION、PASSWORD、FASTFALLOVER、EHOPS だけとなる（このうち PEER と REMOTEAS は必須）。その他のパラメーターについては、BGP ピアテンプレートで指定する。

例

■AS20 の BGP ルーター 10.10.10.2 を E-BGP ピアとして登録する（自 AS 番号を 10 と仮定）。実際の BGP セッションは ENABLE BGP PEER コマンドを実行するまで開始されない。

```
ADD BGP PEER=10.10.10.2 REMOTEAS=20
```

備考・注意事項

経路情報受信時のフィルタリングは INPATHFILTER、INFILTER、INROUTEMAP の順に行われる。また、経路情報送信時のフィルタリングは OUTPATHFILTER、OUTFILTER、OUTROUTEMAP の順に行われる。

BGP 識別子（ルーター ID）には、デフォルトではインターフェースに設定された IP アドレスの中でもっと

も大きなものが使われる。ただし、SET BGP コマンドの ROUTERID パラメーターで明示的に指定した場合はその値が使われる。また、明示的に指定していない場合でも、SET IP LOCAL コマンドでデフォルトローカル IP インターフェース（LOCAL）のアドレスを指定している場合は、そのアドレスがルーター ID として使われる。

関連コマンド

ADD IP ASPATHLIST（163 ページ）
ADD IP FILTER（169 ページ）
ADD IP LOCAL（182 ページ）
ADD IP ROUTEMAP（195 ページ）
DELETE BGP PEER（222 ページ）
DISABLE BGP PEER（261 ページ）
ENABLE BGP DEFAULTORIGINATE（290 ページ）
ENABLE BGP PEER（291 ページ）
RESET BGP PEER（326 ページ）
SET BGP PEER（343 ページ）
SET IP LOCAL（367 ページ）
SHOW BGP PEER（418 ページ）

ADD BGP PEERTEMPLATE

カテゴリー：IP / 経路制御（BGP-4）

ADD BGP PEERTEMPLATE=*1..30* [CONNECTRETRY={DEFAULT|*0..4294967295*}] [DESCRIPTION[=*string*]] [HOLDTIME={DEFAULT|*0*|*3..65535*}] [INFILTER={NONE|*300..399*}] [INPATHFILTER={NONE|*1..99*}] [INROUTEMAP[=*routemap*]] [KEEPALIVE={DEFAULT|*1..21845*}] [MAXPREFIX={OFF|*1..4294967295*}] [MAXPREFIXACTION={WARNING|TERMINATE}] [MINASORIGINATED={DEFAULT|*0..3600*}] [MINROUTEADVERT={DEFAULT|*0..3600*}] [NEXTHOPSELF={NO|YES}] [OUTFILTER={NONE|*300..399*}] [OUTPATHFILTER={NONE|*1..99*}] [OUTROUTEMAP[=*routemap*]] [SENDCOMMUNITY={NO|YES}] [LOCAL={NONE|*1..15*}] [CLIENT={NO|YES}] [PRIVATEASFILTER={NO|YES}]

string: 文字列（1〜63 文字）
routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）

解説

BGP ピアテンプレートを作成する。
BGP ピアテンプレートを使用するには、ADD BGP PEER コマンドの POLICYTEMPLATE パラメーターにテンプレート番号を指定すればよい。

パラメーター

PEERTEMPLATE　BGP ピアテンプレート番号。
CONNECTRETRY　BGP コネクション確立の再試行間隔（秒）。デフォルトは 120。0 は再試行しない。
DESCRIPTION　BGP ピアテンプレートに関する覚え書き（メモ）。
HOLDTIME　BGP セッションがダウンしたと認識するまでの時間（Hold Time）（秒）を設定する。実際の Hold Time はセッション開始時のネゴシエーションによって決まる。本パラメーターで設定するのは OPEN メッセージで相手に提案する値。デフォルトは 90 秒。0 はこちらからは提案しないことを意味する。
INFILTER　該当ピアから受信した経路情報に適用する IP プレフィックスフィルターの番号。INFILTER を使用すると、プレフィックス（ネットワーク番号）によって経路の受け入れ・破棄を行うことができる。IP プレフィックスフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 300〜399）。
INPATHFILTER　該当ピアから受信した経路情報に適用する AS パスリストの番号。INPATHFILTER を使用すると、AS_PATH 属性の内容によって経路の受け入れ・破棄を行うことができる。AS パスリストは ADD IP ASPATHLIST コマンドで作成する。
INROUTEMAP　該当ピアから受信した経路情報に適用するルートマップ名。INROUTEMAP を使用すると、各種の基準に基づいて、経路情報をフィルタリングしたり、属性を変更したりできる。ルートマップは ADD IP ROUTEMAP コマンドで作成する。

KEEPALIVE　KEEPALIVE メッセージの送信間隔。HOLDTIME の 1/3 に設定する必要がある。実際の送信間隔は HOLDTIME のネゴシエーションによって決まる。

MAXPREFIX　該当ピアから受け入れ可能な最大プレフィックス数を設定する。OFF の場合は制限を設けない。デフォルトは OFF。

MAXPREFIXACTION　MAXPREFIX パラメーターの値を超えるプレフィックスを受信したときの動作。WARNING はログに記録するだけ。TERMINATE はログに記録した上で該当ピアとのセッションをリセットする。デフォルトは WARNING。

MINASORIGINATED　自 AS 起源の経路情報を含む UPDATE メッセージの最小連続送信間隔。デフォルトは 15 秒

MINROUTEADVERT　他 AS 起源の経路情報を含む UPDATE メッセージの最小連続送信間隔。デフォルトは 30 秒

NEXTHOPSELF　該当ピアに通知する経路の NEXT_HOP として必ず自アドレスを使うかどうか。デフォルトは NO。

OUTFILTER　該当ピアに経路情報を通知する前に適用する IP プレフィックスフィルターの番号。OUTFILTER を使用すると、プレフィックス（ネットワーク番号）によって経路の通知・破棄を行うことができる。IP プレフィックスフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 300～399）。

OUTPATHFILTER　該当ピアに経路情報を通知する前に適用する AS パスリストの番号。OUTPATHFILTER を使用すると、AS_PATH 属性の内容によって経路の通知・破棄を行うことができる。AS パスリストは ADD IP ASPATHLIST コマンドで作成する。

OUTROUTEMAP　該当ピアに経路情報を通知する前に適用するルートマップ名。OUTROUTEMAP を使用すると、各種の基準に基づいて、経路情報をフィルタリングしたり、属性を変更したりできる。ルートマップは ADD IP ROUTEMAP コマンドで作成する。

SENDCOMMUNITY　UPDATE メッセージに COMMUNITIES 属性を含めるかどうか。同属性の具体的内容はルートマップで設定する。デフォルトは NO。

LOCAL　該当ピアとの通信に使用するローカル IP インターフェースの番号。ローカル IP インターフェースを指定した場合、本ピア宛ての BGP パケットの始点 IP アドレスとして、指定したローカル IP インターフェースの IP アドレスが使用される。省略時は NONE（ローカル IP インターフェースを使用しない。この場合、BGP パケットの始点 IP アドレスはシステムが決める）。

CLIENT　該当ピアがルートリフレクター（RR）クライアントであるかどうか。本パラメーターは、該当ピアが I-BGP ピアである場合のみ意味を持つ。該当ピアが I-BGP ピアであり、なおかつ、本パラメーターが YES の場合、本製品は該当ピアをクライアントであると見なし、ルートリフレクターとしての動作を行う（クライアントから受信した経路を他のすべてのクライアントとノンクライアントに送信する。また、ノンクライアントから受信した経路は、クライアントにだけ送信する）。NO を指定した場合は、該当ピアをノンクライアントと見なして通常の I-BGP 通信を行う。デフォルトは NO。

PRIVATEASFILTER　プライベート AS 番号（64512～65535）をフィルタリングするかどうか。本パラメーターに YES を指定した場合、該当ピアに UPDATE メッセージを送信するとき、AS_PATH 属性からプライベート AS 番号を削除した上で送信する。デフォルトは NO。

関連コマンド

ADD BGP PEER（154 ページ）

ADD IP ASPATHLIST（163 ページ）
ADD IP FILTER（169 ページ）
ADD IP LOCAL（182 ページ）
ADD IP ROUTEMAP（195 ページ）
DELETE BGP PEER（222 ページ）
DELETE BGP PEERTEMPLATE（223 ページ）
DISABLE BGP PEER（261 ページ）
ENABLE BGP PEER（291 ページ）
RESET BGP PEER（326 ページ）
SET BGP PEER（343 ページ）
SET BGP PEERTEMPLATE（346 ページ）
SET IP LOCAL（367 ページ）
SHOW BGP PEER（418 ページ）
SHOW BGP PEERTEMPLATE（422 ページ）

ADD BOOTP RELAY

カテゴリー：IP / DHCP/BOOTP リレー

ADD BOOTP RELAY=*ipadd*

ipadd: IP アドレス

解説

DHCP/BOOTP リクエストの転送先 IP アドレスを設定する。
アドレスは 50 個まで登録可能。DHCP/BOOTP リクエストは登録されているすべての転送先に送られる。
そのため、複数のサーバーから応答が戻ってくる可能性がある。

パラメーター

RELAY　DHCP/BOOTP サーバーの IP アドレス

例

■DHCP/BOOTP リレーを有効にし、転送先として 192.168.100.10 を設定する。

```
ENABLE BOOTP RELAY
ADD BOOTP RELAY=192.168.100.10
```

関連コマンド

DELETE BOOTP RELAY（224 ページ）
DISABLE BOOTP RELAY（262 ページ）
ENABLE BOOTP RELAY（292 ページ）
PURGE BOOTP RELAY（322 ページ）
SET BOOTP MAXHOPS（349 ページ）
SHOW BOOTP RELAY（427 ページ）

ADD IP ARP

カテゴリー：IP / ARP

ADD IP ARP=*ipadd* INTERFACE=*interface* ETHERNET=*macadd* [PORT=*port-num*]

ipadd: IP アドレス
interface: IP インターフェース名（eth0、ppp0 など）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）
port-num: スイッチポート番号（1〜）

解説

ARP キャッシュにスタティックエントリーを追加する。

パラメーター

ARP　IP アドレス
INTERFACE　IP インターフェース
ETHERNET　物理（MAC）アドレス
PORT　スイッチポート番号。INTERFACE に VLAN を指定した場合のみ必要。

例

■eth0 配下に存在する IP アドレス 192.168.100.20、MAC アドレス 00:00:f4:12:34:56 のホストの情報を、ARP キャッシュに追加する。

```
ADD IP ARP=192.168.100.20 INT=eth0 ETHERNET=00-00-f4-12-34-56
```

■スイッチポート 3 に接続されている IP アドレス 192.168.10.54、MAC アドレス 00:00:f4:aa:bb:cc のホストの情報を ARP キャッシュに追加する。

```
ADD IP ARP=192.168.10.54 INT=vlan1 PORT=3 ETHERNET=00-00-f4-aa-bb-cc
```

関連コマンド

DELETE IP ARP（225 ページ）
SET IP ARP（351 ページ）
SHOW IP ARP（432 ページ）

ADD IP ASPATHLIST

カテゴリー：IP / 経路制御（BGP-4）

ADD IP ASPATHLIST=*1..99* [ENTRY=*1..4294967295*] {**INCLUDE**|
EXCLUDE}=***aspathregexp***

aspathregexp: AS パス正規表現

解説

AS パスフィルターにエントリーを追加する。
AS パスフィルターは、BGP 経路に対するフィルタリング機能の 1 つ。AS_PATH 属性の内容に基づいて経路をフィルタリング（INCLUDE、EXCLUDE）するときに使う。
AS パスフィルターは複数のエントリーから構成されるリスト。検索はエントリー番号の若い順に行われ、最初にマッチしたエントリーでアクション（INCLUDE、EXCLUDE）が実行される。
エントリーを持たないフィルターは「すべて許可」の意味になる。また、1 つでもエントリーを持つフィルターには、末尾に「すべて拒否」となる暗黙のエントリーが存在する。
AS パスフィルターは、ADD BGP PEER コマンド、SET BGP PEER コマンドの INPATHFILTER、OUTPATHFILTER でピアごとに適用するか、ルートマップの MATCH 条件（ADD IP ROUTEMAP コマンドの MATCH ASPATH パラメーターに指定）として使用する。

パラメーター

ASPATHLIST　AS パスフィルター番号

ENTRY　フィルター内におけるエントリーの位置。省略時はフィルターの末尾に追加される。既存エントリーと同じ番号を指定した場合は、既存エントリーの前に新規エントリーが追加され、既存エントリー以降はひとつずつ後ろに下がる。

INCLUDE　AS パスのパターンを正規表現で指定する。指定したパターンにマッチする AS パスは許可（受け入れ）される。

EXCLUDE　AS パスのパターンを正規表現で指定する。指定したパターンにマッチする AS パスは拒否（破棄）される。

例

■ローカル経路（AS_PATH 属性が空）にマッチする AS パスフィルター「2」を作成する。

```
ADD IP ASPATHLIST=2 INCLUDE="^$"
```

■AS「10」を起源とする経路を受け取らない（受信時）または通知しない（送信時）AS パスフィルター「1」を作成する。

```
ADD IP ASPATHLIST=1 EXCLUDE="10$"
ADD IP ASPATHLIST=1 INCLUDE=".*"
```

関連コマンド

ADD BGP PEER（154 ページ）
ADD IP ROUTEMAP（195 ページ）
DELETE IP ASPATHLIST（226 ページ）
SET BGP PEER（343 ページ）
SHOW IP ASPATHLIST（433 ページ）

ADD IP COMMUNITYLIST

カテゴリー：IP / 経路制御（BGP-4）

```
ADD IP COMMUNITYLIST=1..99 [ENTRY=1..4294967295] {INCLUDE|
   EXCLUDE}={INTERNET|NOEXPORT|NOADVERTISE|1..4294967295}[,...]
```

解説

コミュニティーフィルターにエントリーを追加する。
コミュニティーフィルターは、BGP 経路に対するフィルタリング機能の 1 つ。COMMUNITIES 属性の値に基づいて経路をフィルタリング（INCLUDE、EXCLUDE）するときに使う。
コミュニティーフィルターは複数のエントリーから構成されるリスト。検索はエントリー番号の若い順に行われ、最初にマッチしたエントリーでアクション（INCLUDE、EXCLUDE）が実行される。
エントリーを持たないフィルターは「すべて許可」の意味になる。また、1 つでもエントリーを持つフィルターには、末尾に「すべて拒否」となる暗黙のエントリーが存在する。
コミュニティーフィルターは、ルートマップの MATCH 条件（ADD IP ROUTEMAP コマンドの MATCH COMMUNITY パラメーターに指定）として使用する。

パラメーター

COMMUNITYLIST　コミュニティーフィルター番号

ENTRY　フィルター内におけるエントリーの位置。省略時はフィルターの末尾に追加される。既存エントリーと同じ番号を指定した場合は、既存エントリーの前に新規エントリーが追加され、既存エントリー以降はひとつずつ後ろに下がる。

INCLUDE　コミュニティー番号、または、Well-known コミュニティーを表すキーワードを指定する。カンマ区切りで 10 個まで指定できる。ここで指定したコミュニティーすべてが、経路エントリーの COMMUNITIES 属性に含まれている場合、許可（受け入れ）アクションが実行される。

EXCLUDE　コミュニティー番号、または、Well-known コミュニティーを表すキーワードを指定する。カンマ区切りで 10 個まで指定できる。ここで指定したコミュニティーすべてが、経路エントリーの COMMUNITIES 属性に含まれている場合、拒否（破棄）アクションが実行される。

例

■コミュニティー値「100」にマッチするコミュニティーフィルター「1」を作成する。

```
ADD IP COMMUNITYLIST=1 INCLUDE=100
```

関連コマンド

ADD BGP PEER（154 ページ）
ADD IP ROUTEMAP（195 ページ）
DELETE IP COMMUNITYLIST（227 ページ）
SET BGP PEER（343 ページ）
SHOW IP COMMUNITYLIST（436 ページ）

ADD IP DNS

カテゴリー：IP / 名前解決

ADD IP DNS [DOMAIN={ANY|*domain-name*}] {**INTERFACE=*interface*|PRIMARY=*ipadd***
[SECONDARY=*ipadd*]}

domain-name: ドメイン名
interface: IP インターフェース名（eth0、ppp0 など）
ipadd: IP アドレス

解説

DNS サーバーリストに DNS サーバーの IP アドレスを追加する。
DNS サーバーは TELNET コマンドなどが使うほか、DNS リレーエージェント機能の転送先としても使用される。名前解決時の検索処理は、ホストテーブル、DNS の順で実行される。DNS サーバーアドレスの設定は SHOW IP DNS コマンド、SHOW IP コマンドで確認できる。

パラメーター

DOMAIN ドメイン名。特定ドメインの名前解決にだけ指定のサーバーを使いたいような場合に使う。本パラメーターで指定したドメインの問い合わせは、同一コマンドラインで指定したサーバーに送られる。本パラメーターを省略した場合（および ANY を指定した場合）、指定したサーバーは、問い合わせがどのドメインにも一致しないときに用いられるデフォルトサーバーとなる。なお、特定ドメイン用のサーバーを登録するときは、あらかじめデフォルトサーバーを設定しておくこと。

INTERFACE IP インターフェース名。DNS サーバーアドレスを動的取得する場合に、アドレスを取得するインターフェースを指定する。ダイヤルアップ PPP の場合は PPP インターフェース、DHCP でアドレスを取得する場合は Ethernet か VLAN インターフェースを指定する。

PRIMARY プライマリー DNS サーバーの IP アドレス

SECONDARY セカンダリー DNS サーバーの IP アドレス

例

■プライマリー DNS サーバーとして 192.168.10.1、セカンダリー DNS サーバーとして 192.168.10.2 を設定する。

```
ADD IP DNS PRIMARY=192.168.10.1 SECONDARY=192.168.10.2
```

■DNS サーバーアドレスを IPCP（IP パラメーターの折衝を行う PPP のサブプロトコル）によって動的に取得する。この場合は、INTERFACE パラメーターで IPCP を実行する PPP インターフェースを指定する。

```
ADD IP DNS INT=ppp0
```

■DNS サーバーアドレスを DHCP で動的に取得する。この場合は、INTERFACE パラメーターで DHCP クライアントとして動作させるインターフェースを指定する。

```
ADD IP DNS INT=eth0
```

■デフォルトの DNS サーバーとして 192.168.10.1 を設定し、ringo.fruit.xxx ドメインの問い合わせ用 DNS サーバーとして 172.20.20.1、172.20.20.2 を設定する。この設定では、xxx.ringo.fruit.xxx 宛ての問い合わせは 172.20.20.1、172.20.20.2 に、その他のドメイン宛ての問い合わせは 192.168.10.1 に送られる。

```
ADD IP DNS PRIMARY=192.168.10.1
ADD IP DNS DOMAIN=ringo.fruit.xxx PRIMARY=172.20.20.1
  SECONDARY=172.20.20.2
```

備考・注意事項

MIB 変数 sysName に本製品のドメイン名（FQDN）が設定されている場合、sysName に基づくドメイン名が DNS 検索に使用される。たとえば、sysName に「white.joge.xxx」が設定されている場合、コマンドラインでホスト名「black」だけを指定すると、「black.joge.xxx」に対する検索が実施される。
DNS サーバーは 10 ドメインまで指定できる（ANY を除く）。

関連コマンド

DELETE IP DNS（228 ページ）
DISABLE IP DNSRELAY（266 ページ）
ENABLE IP DNSRELAY（297 ページ）
SET IP DNS（356 ページ）
SET IP DNS CACHE（358 ページ）
SHOW IP DNS（445 ページ）
SHOW IP DNS CACHE（447 ページ）
TELNET（「運用・管理」の 380 ページ）

ADD IP FILTER

カテゴリー：IP / IP フィルター

```
ADD IP FILTER=filter-id [TYPE={TRAFFIC|POLICY|PRIORITY|ROUTING}]
   SOURCE=ipadd {ACTION={INCLUDE|EXCLUDE}|POLICY=0..15|PRIORITY=P0..P7}
   [SMASK=ipadd] [SPORT={port-name|[port]:[port]}] [DESTINATION=ipadd
   [DMASK=ipadd]] [DPORT={port-name|[port]:[port]}]
   [ICMPCODE={icmp-code-name|icmp-code-id}] [ICMPTYPE={icmp-type-name|
   icmp-type-id}] [LOG={4..1600|DUMP|HEADER|NONE}] [OPTIONS={YES|NO}]
   [PROTOCOL={protocol|ANY|ICMP|OSPF|TCP|UDP}] [SESSION={ANY|ESTABLISHED|
   START}] [SIZE=size] [ENTRY=entry-id]
```

filter-id: フィルター番号（0〜999）
ipadd: IP アドレスまたはネットマスク
port-name: サービス名
port: TCP/UDP ポート番号（0〜65535）
icmp-code-name: ICMP コード名
icmp-code-id: ICMP コード番号（0〜65535）
icmp-type-name: ICMP メッセージ名
icmp-type-id: ICMP メッセージ番号（0〜65535）
protocol: IP プロトコル番号（0〜255）
size: データグラム長
entry-id: エントリー番号（1〜3071）

解説

IP フィルターにエントリー（ルール）を追加する。
IP フィルターには、受信パケットを許可・破棄するトラフィックフィルター（ACTION パラメーターで動作を指定）、受信パケットに内部的な経路選択ポリシー（サービスタイプ）を割り当て、経路選択時の動作に影響を与えるポリシーフィルター（POLICY パラメーターで動作を指定）、送信パケットに優先度を与え、出力順序に影響を与えるプライオリティーフィルター（PRIORITY パラメーターで動作を指定）、BGP-4 の経路交換を制御するプレフィックスフィルター（ACTION パラメーターで動作を指定）の 4 種類がある。
各 IP インターフェースには、トラフィック、ポリシー、プライオリティーフィルターをそれぞれ 1 つずつ適用できる。同じフィルターを複数のインターフェースに適用することも可能。これら 3 種類のフィルターは、インターフェースに適用して初めて効果を発揮する。トラフィックフィルターとポリシーフィルターは受信インターフェースに、プライオリティーフィルターは送信インターフェースに適用する。インターフェースへの適用は、ADD IP INTERFACE コマンド、SET IP INTERFACE コマンドで行う。
また、プレフィックスフィルターを使用するには、ADD BGP PEER コマンド、SET BGP PEER コマンドの INFILTER、OUTFILTER パラメーターでフィルター番号を指定する。
トラフィックフィルター、ポリシーフィルター、プライオリティーフィルターは、動作指定が異なるだけでパケットを選別するパラメーターは共通。一方、プレフィックスフィルターで使用できるパラメーターは、SOURCE、SMASK、ENTRY、ACTION だけに限定されている。

パラメーター

FILTER　フィルター番号。フィルターの種類は、0〜999 の任意の番号に対して TYPE パラメーターで自由に設定可能。

TYPE　フィルターの種類を指定する。TRAFFIC:トラフィックフィルター、POLICY:ポリシーフィルター、PRIORITY:プライオリティーフィルター、ROUTING:プレフィックスフィルター。（以前のバージョンでは、0〜99 はトラフィックフィルター、100〜199 はポリシーフィルター、200〜299 はプライオリティーフィルター、300〜399 はプレフィックスフィルター用に固定で割り当てられていた。）TYPE パラメーターを省略すると、他のパラメーター設定に応じて、次のようにデフォルト値が設定される。POLICY パラメーターが設定されている場合:TYPE は POLICY に設定される。PRIORITY パラメーターが設定されている場合:TYPE は PRIORITY に設定される。ACTION パラメーターの指定があり、SOURCE/SMASK/ENTRY パラメーター以外の指定がなく、フィルター番号が 99 より大きい場合:TYPE は ROUTING に設定される。その他の場合:TYPE は TRAFFIC に設定される。TYPE パラメーターは省略しないことを推奨する。

SOURCE　始点 IP アドレスまたはネットワークプレフィックス。0.0.0.0 はすべてのアドレスを意味する。必須パラメーター

ACTION　トラフィックフィルター（TYPE=TRAFFIC）、プレフィックスフィルター（TYPE=ROUTING）の動作を指定する。INCLUDE はマッチしたパケット、プレフィックスを通過させる。EXCLUDE はマッチしたパケット、プレフィックスを破棄する。POLICY、PRIORITY とは同時に指定できない

POLICY　ポリシーフィルター（TYPE=POLICY）において、マッチしたパケットに割り当てる経路選択ポリシー（サービスタイプ）を指定する。経路選択ポリシーの範囲は 0〜7 だが、POLICY パラメーターには 0〜15 の範囲を指定することができる。0〜7 を指定した場合は、指定値がそのまま経路選択ポリシー値となる。8〜15 を指定した場合は、経路選択ポリシーとして「POLICY - 8」を割り当て、さらに、パケットの TOS ビット（D、T、R）を「POLICY - 8」に書き換える。詳細は別表を参照。経路表を検索するときは、本フィルターによって割り当てられた経路選択ポリシー値と経路エントリーのサービスタイプがつきあわされ、一致する経路が最優先で使用される。フィルターにマッチしなかったパケットの経路選択ポリシーは「0」。ACTION、PRIORITY とは同時に指定できない

PRIORITY　プライオリティーフィルター（TYPE=PRIORITY）において、マッチしたパケットを出力するときの優先度を P0（最高）〜P7（最低）で指定する。フィルターにマッチしなかった通常パケットの優先度は「P5」。ACTION、POLICY とは同時に指定できない。また、Eth/PPPoE インターフェースでこの機能が動作するのは、受信インターフェースの速度の合計より送信インターフェースの速度の合計が小さい場合。（例 1）受信インターフェース：100Mbps × 1、送信インターフェース：10Mbps × 1。（例 2）受信インターフェース：100Mbps × 2、送信インターフェース：100Mbps × 1。

SMASK　SOURCE に対応するマスク値。SOURCE と組み合わせて、ホストアドレス/ネットワークアドレスの区別、または、プレフィックス長（プレフィックスフィルター）を指定する。SOURCE で指定した IP アドレスがネットワークアドレスなら適切な長さのネットマスクを、ホストアドレスなら 255.255.255.255 を指定する。また、SOURCE に 0.0.0.0（ANY）を指定した場合は 0.0.0.0 を指定する（省略可）。

SPORT　始点 TCP/UDP ポートあるいは定義済みのサービス名。本パラメーター指定時は PROTOCOL パラメーターに TCP か UDP を指定する必要がある。low:high の形式で low〜high の範囲指定も可能。「low:」は low〜65535 の意味、「:high」は 0〜high の意味になる。デフォルトは ANY（すべてのポート）。

DESTINATION　終点 IP アドレス。デフォルトは 0.0.0.0（すべて）

DMASK　終点 IP アドレスに対応するマスク値。DESTINATION と組み合わせてホストアドレスまたはネットワークアドレスを指定する。省略時は 255.255.255.255（ホストマスク）とみなされる。

DPORT　終点 TCP/UDP ポートあるいは定義済みのサービス名。本パラメーター指定時は PROTOCOL パラメーターに TCP か UDP を指定する必要がある。low:high の形式で low〜high の範囲指定も可能。「low:」は low〜65535 の意味、「:high」は 0〜high の意味になる。デフォルトは ANY（すべてのポート）。

ICMPCODE　ICMP コード番号または定義済みのコード名。PROTOCOL=ICMP の場合のみ有効

ICMPTYPE　ICMP メッセージ番号または定義済みのメッセージ名。PROTOCOL=ICMP の場合のみ有効

LOG　このエントリーにマッチしたパケットの情報をログに記録するかどうか、記録する場合はどの情報を記録するかを指定する。NONE はログに記録しないことを意味する。4〜1600 の数値を指定した場合は、フィルター番号、エントリー番号、IP ヘッダー情報（IP アドレス、プロトコル、ポート番号、サイズ）が「IPFIL/PASS」（INCLUDE アクションの場合）または「IPFIL/FAIL」（EXCLUDE アクションの場合）タイプのメッセージとして記録される。これに加え、TCP、UDP、ICMP の場合はデータ部分の先頭 4〜1600 バイトが、その他プロトコルの場合は IP データの先頭 4〜1600 バイトが、「IPFIL/DUMP」タイプのメッセージとして記録される。DUMP は LOG=32 と同じ動作となる。HEADER を指定した場合は、フィルター番号、エントリー番号、IP ヘッダー情報のみが記録される。デフォルトは NONE（記録しない）。

OPTIONS　パケットが IP オプション付きかどうか。

PROTOCOL　IP プロトコル番号または定義済みのプロトコル名。DPORT、SPORT を指定するときは、PROTOCOL に TCP か UDP を指定する必要がある。また、ICMPCODE、ICMPTYPE 指定時は ICMP を指定する。

SESSION　TCP のセッション制御情報。ANY はすべての TCP パケット、START は接続開始パケット（SYN=1、ACK=0）、ESTABLISHED は接続済みパケット（ACK=1）を意味する。

SIZE　再構成後のデータグラムサイズ。パケット（フラグメント）ごとに length + offset * 8 <= SIZE がチェックされ、真ならマッチし、偽ならマッチしない。length と offset は、それぞれ IP ヘッダーの Length フィールドと Fragment Offset フィールドを示す。

ENTRY　エントリー番号。省略時は現在最後尾のエントリーの後に追加される（最後尾のエントリー番号を「n」とすると、新規エントリーは「n+1」になる）。「n+1」より大きなエントリー番号を指定した場合は、指定した番号で追加される。既存エントリーと同じ番号を指定した場合は、既存エントリーの位置に新規エントリーが挿入され、既存エントリー以降は番号が 1 つずつ後ろにずれる。

POLICY に指定した値	パケットに割り当てる経路選択ポリシー	TOS ビットの書き換え
0	0	しない
1	1	しない
2	2	しない
3	3	しない
4	4	しない
5	5	しない
6	6	しない

7	7	しない
8	0（8 - 8）	0（D=0, T=0, M=0）
9	1（9 - 8）	1（D=0, T=0, M=1）
10	2（10 - 8）	2（D=0, T=1, M=0）
11	3（11 - 8）	3（D=0, T=1, M=1）
12	4（12 - 8）	4（D=1, T=0, M=0）
13	5（13 - 8）	5（D=1, T=0, M=1）
14	6（14 - 8）	6（D=1, T=1, M=0）
15	7（15 - 8）	7（D=1, T=1, M=1）

表 23: POLICY パラメーターの指定値とその効果

サービス名	**該当サービス/アプリケーション（ポート/プロトコル）**
ANY	すべてのポート
BOOTPC	BOOTP クライアント（68/udp）
BOOTPS	BOOTP サーバー（67/udp）
DOMAIN	DNS サーバー（53/tcp、53/udp）
FINGER	Finger（79/tcp）
FTP	FTP コントロールセッション（21/tcp）
FTPDATA	FTP データセッション（20/tcp）
GOPHER	Gopher（70/tcp）
HOSTNAME	NIC Host Name Server（101/tcp、101/udp）
IPX	IPX（213/tcp、213/udp）
KERBEROS	Kerberos（88/udp）
LOGIN	Login（49/udp）
MSGICP	MSG ICP（29/tcp、29/udp）
NAMESERVER	Host Name Server（42/udp）
NEWS	NewS（144/tcp）
NNTP	NNTP サーバー（119/tcp）
NTP	NTP サーバー（123/tcp）
RTELNET	Remote Telnet（107/tcp、107/udp）
SFTP	Simple FTP（115/tcp、115/udp）
SMTP	SMTP サーバー（25/tcp）
SNMP	SNMP（161/udp）
SNMPTRAP	SNMP トラップ（162/udp）
SYSTAT	Active Users（11/tcp）
TELNET	Telnet（23/tcp）
TFTP	TFTP（69/udp）
TIME	Time（37/tcp、37/udp）
UUCP	uucpd（540/tcp）

UUCPRLOGIN	uucp-rlogin（541/tcp、541/udp）
WWWHTTP	80/TCP（World Wide Web HTTP）
XNSTIME	XNS Time Protocol（52/tcp、52/udp）

表 24: 定義済みのサービス名一覧

メッセージタイプ名	タイプ番号	サブコード	説明
ECHORPLY	0	なし	エコー応答（Echo Reply）
UNREACHABLE	3	あり	宛先到達不可能（Unreachable）
QUENCH	4	なし	送信抑制要求（Source Quench）
REDIRECT	5	あり	経路変更要求（Redirect）
ECHO	8	なし	エコー要求（Echo Request）
ADVERTISEMENT	9	なし	ルーター通知（Router Advertisement）
SOLICITATION	10	なし	ルーター要請（Router Solicitation）
TIMEEXCEED	11	あり	時間超過（Time Exceeded）
PARAMETER	12	あり	パラメーター異常（Parameter Problem）
TSTAMP	13	なし	タイムスタンプ要求（Timestamp Request）
TSTAMPRPLY	14	なし	タイムスタンプ応答（Timestamp Reply）
INFOREQ	15	なし	情報要求（Information Request）
INFOREP	16	なし	情報応答（Information Reply）
ADDRREQ	17	なし	アドレスマスク要求
ADDRREP	18	なし	アドレスマスク応答

表 25: 定義済みの ICMP メッセージタイプ名一覧

コード名	コード番号	説明
ANY		すべて
	UNREACHABLE（Type=3）	
NETUNREACH	0	ネットワーク到達不可能
HOSTUNREACH	1	ホスト到達不可能
PROTUNREACH	2	プロトコル到達不可能
PORTUNREACH	3	ポート到達不可能
FRAGMENT	4	フラグメント化不可能
SOURCEROUTE	5	始点経路制御失敗
NETUNKNOWN	6	宛先ネットワーク不明
HOSTUNKNOWN	7	宛先ホスト不明
HOSTISOLATED	8	始点ホスト隔離
NETCOMM	9	宛先ネットワークとの通信が禁止されている
HOSTCOMM	10	宛先ホストとの通信が禁止されている
NETTOS	11	指定のサービスタイプでは宛先ネットワークに到達不可能
HOSTTOS	12	指定のサービスタイプでは宛先ホストに到達不可能

FILTER	13	フィルタリングにより通信が禁止されている
HOSTPREC	14	ホスト優先度違反
PRECEDENT	15	優先度制限
	REDIRECT（Type=5）	
NETREDIRECT	0	ネットワーク経路変更要求
HOSTREDIRECT	1	ホスト経路変更要求
NETRTOS	2	指定サービスタイプのネットワーク経路変更要求
HOSTRTOS	3	指定サービスタイプのホスト経路変更要求
	TIMEEXCEEDED（Type=11）	
TTL	0	生存時間超過
FRAGREASSM	1	フラグメント再構成時間超過
	PARAMETER（Type=12）	
PTRPROBLEM	0	ポインターフィールドの値がエラーのあった箇所を示す
NOPTR	1	ポインターなし

表 26: 定義済みの ICMP コード名一覧

例

■200.100.10.100 からのパケットだけを通過させるトラフィックフィルター「0」を ppp0 に適用する。

```
ADD IP FILTER=0 TYPE=TRAFFIC SOURCE=200.100.10.100 SMASK=255.255.255.255
  ACTION=INCLUDE
SET IP INT=ppp0 FILTER=0
```

■10.1.1.10 から 10.2.2.12 へのトラフィックに経路選択ポリシー 4 を設定するポリシーフィルター「100」を作成して vlan1 に適用。

```
ADD IP FILTER=100 TYPE=POLICY SOURCE=10.1.1.10 SMASK=255.255.255.255
  DEST=10.2.2.12 POLICY=4
SET IP INT=vlan1 POLICYFILTER=100
```

■TCP を最優先で送信するプライオリティーフィルター「200」を ppp0 に適用

```
ADD IP FILTER=200 TYPE=PRIORITY SOURCE=0.0.0.0 PROTOCOL=TCP PRIORITY=P0
SET IP INT=ppp0 PRIORITYFILTER=200
```

備考・注意事項

トラフィックフィルターの末尾には、すべてのパケットを破棄する暗黙のエントリーが存在する。そのため、特定のパケットだけを破棄したい場合は、エントリーリストの最後に「すべてを許可」するエントリーを明

示的に作成する必要がある。

関連コマンド

ADD BGP PEER（154 ページ）
ADD IP INTERFACE（179 ページ）
DELETE IP FILTER（230 ページ）
SET BGP PEER（343 ページ）
SET IP FILTER（360 ページ）
SET IP INTERFACE（364 ページ）
SHOW IP FILTER（449 ページ）

ADD IP HELPER

カテゴリー：IP / UDP ブロードキャストヘルパー

ADD IP HELPER DESTINATION=*ipadd* INTERFACE=*interface* PORT={*port*|*port-name*}

ipadd: IP アドレス
interface: IP インターフェース名（eth0、ppp0 など）
port: UDP ポート番号（1〜65535）
port-name: サービス名

解説

UDP ブロードキャストパケットの転送先を設定する。32 個まで設定可能。

パラメーター

DESTINATION　UDP パケットの転送先 IP アドレス。ユニキャスト、ブロードキャストともに指定可能
INTERFACE　UDP ブロードキャストを監視する IP インターフェース。このインターフェースで受信した UDP ブロードキャストのうち、終点ポートが PORT で指定された値と一致したものを、DESTINATION に転送する。
PORT　転送対象の UDP ポート番号、または、あらかじめ定義されている UDP サービス名（別表を参照）を指定する

サービス名	UDP ポート番号
DNS	53
NT または NETBIOS	137 と 138
TACACS	49
TIME	37
TFTP	69

表 27: 定義済みの UDP サービス名

例

■vlan1 側で受信した NetBIOS ブロードキャスト（終点 UDP ポート=137-138）を、ドメインコントローラー 192.168.30.8 に転送する。

```
ENABLE IP HELPER
ADD IP HELPER DESTINATION=192.168.30.8 INT=vlan1 PORT=NETBIOS
```

■vlan1 側で受信した NetBIOS ブロードキャストを eth0 側（192.168.10.0/24）に再ブロードキャストする。

```
ENABLE IP HELPER
ADD IP HELPER DESTINATION=192.168.10.255 INT=vlan1 PORT=NETBIOS
```

備考・注意事項

DESTINATION パラメーターでリモートのブロードキャストアドレス（直接接続されていないサブネットのブロードキャストアドレス）を指定した場合、相手ルーターのディレクティドブロードキャストフィルターでパケットが破棄される可能性があることに注意。

関連コマンド

DELETE IP HELPER（231 ページ）
DISABLE IP HELPER（270 ページ）
ENABLE IP HELPER（301 ページ）
SHOW IP HELPER（453 ページ）

ADD IP HOST

カテゴリー：IP / 名前解決

ADD IP HOST=*hostname* IPADDRESS=*ipadd*

hostname: ホスト名
ipadd: IP アドレス

解説

IP ホストテーブルにホスト名を追加する。
登録したホスト名は TELNET コマンド、TRACE コマンド、PING コマンドで使用できる。

パラメーター

HOST　ホスト名
IPADDRESS　IP アドレス

例

■192.168.1.1 にホスト名「bulbul」を付ける

```
ADD IP HOST=bulbul IPADDRESS=192.168.1.1
```

関連コマンド

ADD IP DNS（167 ページ）
DELETE IP DNS（228 ページ）
DELETE IP HOST（232 ページ）
DISABLE IP DNSRELAY（266 ページ）
ENABLE IP DNSRELAY（297 ページ）
FINGER
PING（319 ページ）
SET IP DNS（356 ページ）
SET IP DNS CACHE（358 ページ）
SET IP HOST（363 ページ）
SHOW IP DNS（445 ページ）
SHOW IP DNS CACHE（447 ページ）
SHOW IP HOST（455 ページ）
TELNET（「運用・管理」の 380 ページ）

ADD IP INTERFACE

カテゴリー：IP / IP インターフェース

ADD IP INTERFACE=*interface* IPADDRESS={*ipadd*|DHCP} [MASK=*ipadd*]
[BROADCAST={*0*|*1*}] [DIRECTEDBROADCAST={YES|NO|ON|OFF}] [FILTER={*0..99*|NONE}] [FRAGMENT={YES|NO}] [MULTICAST={OFF|SEND|RECEIVE|BOTH|ON}]
[OSPFMETRIC=*1..65534*] [POLICYFILTER={*100..199*|NONE}]
[PRIORITYFILTER={*200..299*|NONE}] [PROXYARP={ON|OFF}] [RIPMETRIC=*1..16*]
[VJC={ON|OFF}]

interface: 第 2 層インターフェース名（eth0、ppp0 など）
ipadd: IP アドレスまたはネットマスク

解説

IP インターフェースを作成する。

パラメーター

INTERFACE　下位のインターフェースを指定する。1 つのインターフェースに複数の IP アドレスを設定するとき（マルチホーミング）は、vlan1-0、vlan1-1、vlan1-2 のように、インターフェース名の後にハイフンと論理インターフェース番号（0〜15）を付ける。論理インターフェース番号を省略したとき（例：vlan1）は「0」を指定したものと見なされる（例：vlan1-0 として扱われる）。

IPADDRESS　インターフェースに割り当てる IP アドレス。DHCP を指定した場合は、DHCP サーバーから IP 設定情報を取得し自動設定する。DHCP で取得できる情報は、IP アドレス、ネットマスク、DNS サーバーアドレス（プライマリー、セカンダリー）、デフォルト経路、ドメイン名。DHCP を使う場合は、あらかじめ ENABLE IP REMOTEASSIGN コマンドを実行して、IP アドレスの動的設定を有効にしておく必要がある。

MASK　サブネットマスク。省略時は IP アドレスのクラス標準マスクが用いられる。DHCP を使う場合は自動的に設定されるので指定しないこと。

BROADCAST　IP ブロードキャストアドレスをオール 1 で表すか、オール 0 で表すかを示す。通常は 1（デフォルト）。

DIRECTEDBROADCAST　この IP インターフェース配下のネットワークに対するディレクティドブロードキャストパケットを転送するかどうかを示す。デフォルトは NO。

FILTER　このインターフェースで受信した IP パケットに適用するトラフィックフィルターの番号。トラフィックフィルターのアクションは受信直後に適用される。デフォルトは NONE。IP トラフィックフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 0〜99）。

FRAGMENT　このインターフェースから送出するパケットがインターフェースの MTU よりも大きい場合の動作を指定する。NO（デフォルト）を指定した場合、DF（Don't Fragment）ビットの指示通り、DF ビットが立っているパケットはフラグメント化せずに破棄する。YES を指定した場合は、DF ビットを無視してフラグメント化する。

MULTICAST IP マルチキャストパケットの扱いを指定する。OFF を指定した場合は送受信とも行わない。ON または BOTH を指定した場合は送受信を行う。SEND は送信のみ、RECEIVE は受信のみ行うことを示す。デフォルトは RECEIVE。マルチホーミングを使用している場合、本パラメーターの設定はおおもとの IP インターフェース全体に適用される。また、マルチキャスト経路制御プロトコル DVMRP を使用している場合、本パラメーターは意味を持たない。

OSPFMETRIC OSPF が用いる本インターフェースのメトリック（通過コスト）。デフォルトは 1

POLICYFILTER このインターフェースで受信した IP パケットに適用するポリシーフィルターの番号。ポリシーフィルターによって設定された経路選択ポリシー（サービスタイプ）は経路表の検索時に使用される。デフォルトは NONE。IP ポリシーフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 100〜199）。

PRIORITYFILTER このインターフェースから送信する IP パケットに適用するプライオリティーフィルターの番号。IP パケットの出力は、プライオリティーフィルターによって設定された優先度に基づいて行われる。デフォルトは NONE。IP プライオリティーフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 200〜299）。

PROXYARP プロキシー ARP（RFC1027）の有効・無効。デフォルトは ON。

RIPMETRIC RIP が用いる本インターフェースのメトリック（通過コスト）。METRIC も同じ意味。デフォルトは 1

VJC PPP インターフェース上の IP インターフェースで Van Jacobson の TCP/IP ヘッダー圧縮（VJ 圧縮）を使用するかどうかを指定する。この設定は PPP インターフェース上のすべての IP インターフェースに適用される。VJ 圧縮は、48Kbps 程度までの低速な回線上で効果を発揮する。64Kbps 以上の回線ではかえって効率が落ちるので注意が必要。また、MP（Multilink PPP）を使用している場合は ON にしないこと。デフォルトは OFF。

例

■vlan1 に IP アドレス 192.168.100.1 を設定する。

```
ADD IP INT=vlan1 IP=192.168.100.1 MASK=255.255.255.0
```

■eth0 に DHCP サーバーから取得したアドレスを設定する。

```
ENABLE IP REMOTEASSIGN
ADD IP INT=eth0 IP=DHCP
```

■vlan1 に 2 つの IP アドレスを設定する（マルチホーミング）。

```
ADD IP INT=vlan1-0 IP=172.16.10.1 MASK=255.255.255.0
ADD IP INT=vlan1-1 IP=172.16.20.1 MASK=255.255.255.0
```

■ppp0 を Unnumbered に設定する。

```
ADD IP INT=ppp0 IP=0.0.0.0
```

備考・注意事項

複数のインターフェースに対し、同一サブネットのIPアドレスを割り当てることはできない。たとえば、vlan1にIPアドレス192.168.10.1、ネットマスク255.255.255.0を割り当てた場合、192.168.10.2～192.168.10.254の範囲は同一IPサブネットになるため、この範囲を同じネットマスクで他のインターフェース（たとえばvlan1-1やeth0）に割り当てることはできない。
DHCPでアドレスを設定するには、ENABLE IP REMOTEASSIGNコマンドが必要。また、一部のISPでは、SET SYSTEM NAMEコマンドでISPから指定されたコンピューター名を設定する必要がある。

関連コマンド

DELETE IP INTERFACE（233ページ）
DISABLE IP INTERFACE（272ページ）
ENABLE IP INTERFACE（303ページ）
RESET IP INTERFACE（329ページ）
SET IP INTERFACE（364ページ）
SHOW IP INTERFACE（458ページ）

ADD IP LOCAL

カテゴリー：IP / IP インターフェース

ADD IP LOCAL=*1..15* IPADDRESS=*ipadd* [FILTER={*filter-id*|NONE}]
[GRE={*0..100*|NONE}] [POLICYFILTER={*filter-id*|NONE}]
[PRIORITYFILTER={*filter-id*|NONE}]

ipadd: IP アドレス
filter-id: フィルター番号（0〜999）

解説

ローカル IP インターフェース（ループバックインターフェース）を追加する。15 個まで作成可能。
ローカル IP インターフェースは、下位層（物理層/データリンク層）との関連を持たない仮想的な IP インターフェース。物理的なインターフェースに割り当てた IP アドレスは、該当インターフェースのリンクダウンにより到達不能になる可能性があるが、ローカル IP インターフェースは下位層の状態に依存しないため、このインターフェースの IP アドレスを広告することで、本製品への到達性を高めることができる。
ローカル IP インターフェースに割り当てたアドレスは、本製品が送信する BGP-4 パケットの始点アドレスとして使用することができる。
本製品自身が IP パケットを送信するとき、始点アドレスは以下の基準にしたがって決定される。
1. コマンドで始点アドレスまたは始点インターフェースを明示的に指定した場合は、そのアドレスが使用される。ADD BGP PEER コマンドの LOCAL パラメーターがこれに当たる。
2. 1 に該当せず、なおかつ、デフォルトローカル IP インターフェース（LOCAL）の IP アドレスが指定されている場合は、そのアドレスが使用される。デフォルトローカル IP インターフェースのアドレスは、SET IP LOCAL コマンドで指定する。
3. 1、2 のいずれにも該当しない場合は、パケットを送出するインターフェースの IP アドレスが始点アドレスとして使用される。

パラメーター

LOCAL　ローカル IP インターフェース番号
IPADDRESS　ローカル IP インターフェースの IP アドレス
FILTER　このインターフェースに適用するトラフィックフィルターの ID
GRE　このインターフェースに割り当てる GRE 設定の ID
POLICYFILTER　このインターフェースに適用するポリシーフィルターの ID
PRIORITYFILTER　このインターフェースに適用するプライオリティーフィルターの ID

備考・注意事項

ローカル IP インターフェースは、BGP-4 のみに対して使用可能。

デフォルトのローカル IP インターフェースに IP アドレスを設定するには、SET IP LOCAL コマンドを使う。このとき、LOCAL パラメーターには、値を指定しないかキーワード DEFAULT を指定する。

関連コマンド

DELETE IP LOCAL（234 ページ）
SET IP LOCAL（367 ページ）

ADD IP NAT

カテゴリー：IP / レンジ NAT

ADD IP NAT IP=*ipadd* [MASK=*ipadd*] [GBLIP=*ipadd*] [GBLMASK=*ipadd*] [GBLPORT={*port*|*port-name*}] [GBLINTERFACE=*interface*] [PORT={*port*|*port-name*}] [PROTOCOL={*protocol*|ALL|GRE|ICMP|OSPF|SA|TCP|UDP}]

ipadd: IP アドレスまたはネットマスク
port: TCP/UDP ポート番号（0～65535）
port-name: サービス名
interface: IP インターフェース名（eth0、ppp0 など）
protocol: IP プロトコル番号（0～255）

解説

IP NAT（レンジ NAT）の変換ルールを追加する。
本コマンドで設定する NAT は、IP アドレスの範囲をもとにアドレス変換を行うもので、レンジ NAT とも呼ぶ。一方、ファイアウォールの NAT 機能（ファイアウォール NAT）には、インターフェース単位で設定するインターフェース NAT と、アドレスベースで設定するルール NAT の 2 種類がある。IP NAT とファイアウォール NAT を同時に使用することはできない。IP NAT はファイアウォールを使用しないときに使う。ファイアウォールを使用する場合は、ファイアウォール NAT を使う。
必要なパラメーターは NAT の種類によって異なる。
スタティック NAT（IP アドレスを 1 対 1 で固定的に変換）の場合は、IP（プライベート IP）、GBLIP（グローバル IP）を指定する。
ダイナミック NAT（IP アドレスを多対多で動的に変換）の場合は、IP（プライベート IP）、MASK（IP に対するマスク）、GBLIP（グローバル IP）、GBLMASK（GBLIP に対するマスク）を指定する。この場合、IP/MASK で指定した範囲のプライベートアドレスを、GBLIP/GBLMASK で指定した範囲内で空いているグローバルアドレスに変換する。ただし、他の NAT に比べてメリットが少ないため、あまり使われない。
スタティック ENAT（IP アドレス、プロトコル（、ポート）を 1 対 1 で固定的に変換）の場合は、IP（プライベート IP）、PROTOCOL（IP プロトコル）、PORT（プライベート側ポート番号）、GBLIP（グローバル IP）、GBLPORT（グローバル側ポート番号）を指定する。なお、スタティック ENAT を使用するためには、IP を範囲に含むダイナミック ENAT の設定が必要。
ダイナミック ENA T（IP アドレス、プロトコル（、ポート）を多対多で動的に変換）の場合は、IP（プライベート IP）、MASK（IP に対するマスク）、GBLIP（グローバル IP）または GBLINTERFACE（グローバル側インターフェース）を指定する。これにより、動的なポート割り当てにより、GBLINTERFACE に割り当てられた 1 つのグローバルアドレス、または、GBLIP で指定したアドレスを、IP/MASK で指定したプライベートアドレスを持つホスト間で共有する。

パラメーター

IP　プライベート IP アドレス。MASK と組み合わせて範囲指定が可能。
MASK　プライベート IP アドレスの範囲を指定するためのマスク値

GBLIP　グローバル IP アドレス。GBLMASK と組み合わせて範囲指定が可能
GBLMASK　グローバル IP アドレスの範囲を指定するためのマスク値
GBLPORT　スタティック ENAT におけるグローバル側ポート番号またはサービス名
GBLINTERFACE　ダイナミック ENAT における、グローバル IP アドレスを持つインターフェース
PORT　スタティック ENAT におけるプライベートホストのポート番号またはサービス名
PROTOCOL　スタティック ENAT における IP プロトコル指定。TCP か UDP を指定した場合は、PORT の指定も必要。

例

■プライベート IP とグローバル IP の一対一変換（スタティック NAT）

```
ADD IP NAT IP=192.168.10.5 GBLIP=200.100.10.5
```

■プライベート側全ホストでグローバル IP16 個を共有（ダイナミック NAT）

```
ADD IP NAT IP=192.168.10.0 MASK=255.255.255.0 GBLIP=200.100.10.1
  GBLMASK=255.255.255.240
```

■プライベート側全ホストでグローバル IP1 個を共有（ダイナミック ENAT）

```
ADD IP NAT IP=192.168.10.0 MASK=255.255.255.0 GBLIP=200.100.10.1
```

■上記ダイナミック ENAT 設定にスタティック ENAT 設定を追加。グローバル側（200.100.10.1）TCP ポート 80 番へのアクセスをプライベート側の Web サーバー（192.168.10.5 のポート 80）に転送

```
ADD IP NAT IP=192.168.10.5 PROTO=TCP PORT=80 GBLIP=200.100.10.1
  GBLPORT=80
```

■プライベート側全ホストで ppp0 に割り当てられたグローバル IP1 個を共有（インターフェース指定のダイナミック ENAT）

```
ADD IP NAT IP=192.168.10.0 MASK=255.255.255.0 GBLINT=ppp0
```

備考・注意事項

スタティック ENAT の設定をするためには、あらかじめダイナミック ENAT の設定をしておく必要がある。

関連コマンド

DELETE IP NAT（235 ページ）

DISABLE IP NAT（273 ページ）
ENABLE IP NAT（305 ページ）
SHOW IP NAT（461 ページ）

ADD IP RIP

カテゴリー：IP / 経路制御（RIP）

```
ADD IP RIP INTERFACE=interface [IP=ipadd] [SEND={NONE|RIP1|RIP2|
    COMPATIBLE}] [RECEIVE={NONE|RIP1|RIP2|BOTH}] [NEXTHOP=ipadd]
    [DEMAND={YES|NO}] [AUTHENTICATION={NONE|PASSWORD|MD5}]
    [PASSWORD=password] [STATICEXPORT={YES|NO}]
```

interface: IP インターフェース名（eth0、ppp0 など）
ipadd: IP アドレス
password: パスワード（1〜16 文字）

解説

指定した IP インターフェースで RIP を有効にする。

パラメーター

INTERFACE　RIP パケットの送受信を行う IP インターフェース

IP　RIP ルーターの IP アドレス。本パラメーター指定時は、INTERFACE で受信した RIP パケットのうち、始点アドレスが IP と一致するものだけを受け入れる。また、RIP パケット送信時には、IP で指定されたアドレス宛てにユニキャストする。一方、本パラメーター省略時は、受信した RIP パケットの始点アドレスをチェックせず、RIP パケット送信時には、ブロードキャスト（SEND=RIP1 のとき）、または、マルチキャスト（SEND=RIP2 または COMPATIBLE のとき）する。

SEND　送信する RIP パケットのフォーマット。NONE は送信しない。RIP1 はバージョン 1 形式、RIP2 はバージョン 2 形式で送信する。COMPATIBLE はバージョン 2 形式で送信するが、RIP1 互換の経路エントリー（ナチュラルサブネットマスク（クラス標準マスク）を使用したネットワークアドレス）しか送信しない。デフォルトは RIP1。

RECEIVE　受信する RIP パケットのフォーマット。NONE は受信しない。RIP1 はバージョン 1 形式のみ受信。RIP2 はバージョン 2 形式のみ受信。BOTH はバージョン 1、2 ともに受信するが、ナチュラルサブネットマスク（クラス標準マスク）を使用したネットワークアドレスしか受信できない。デフォルトは BOTH。

NEXTHOP　RIP バージョン 2 パケットの Next Hop フィールドにセットするネクストホップ IP アドレス。本パラメーターを使用するには、SEND パラメーターに RIP2 か COMPATIBLE を指定し、IP パラメーターに RIP ルーターのユニキャスト IP アドレスを指定する必要がある。省略時は 0.0.0.0（自分自身がネクストホップ）

DEMAND　トリガーアップデート（RFC1582）を使用するかどうか。デフォルトは NO。

AUTHENTICATION　RIP Version2 使用時の認証方式。PASSWORD は平文テキストのパスワード、MD5 は鍵付き MD5 によるメッセージダイジェスト、NONE は認証を行わない。デフォルトは NONE。

PASSWORD　RIP Version2 で認証を行うときのパスワードまたはキー。AUTHENTICATION に PASS-

WORD か MD5 を指定した場合にのみ有効

STATICEXPORT　スタティック経路を RIP で通知するかどうか。デフォルトは YES（通知する）。

例

■eth0 で RIP2 の送受信（マルチキャスト）を有効にする。

```
ADD IP RIP INT=eth0 SEND=RIP2 RECEIVE=RIP2
```

■vlan1 で RIP2 の受信だけを有効にする。

```
ADD IP RIP INT=vlan1 SEND=NONE RECEIVE=RIP2
```

■vlan1 上の RIP2 ルーター 192.168.10.5 からユニキャストで経路情報を受信し、同じ LAN 上に RIP1 のブロードキャストで経路情報を通知する。

```
ADD IP RIP INT=vlan1 IP=192.168.10.5 SEND=NONE RECEIVE=RIP2 AUTH=PASSWORD
  PASSWORD=secrets
ADD IP RIP INT=vlan1 SEND=RIP1 RECEIVE=NONE
```

■同一サブネット上にない RIP2 ルーター「192.168.30.1」に対して、経路情報をユニキャストで送信する。RIP2 パケットの Next Hop フィールドには、「192.168.30.1」と同じサブネット上にあるルーターのアドレス「192.168.30.2」をセットする。

```
ADD IP RIP INT=ppp0 IP=192.168.30.1 NEXTHOP=192.168.30.2 SEND=RIP2
  RECEIVE=NONE
```

関連コマンド

DELETE IP RIP（236 ページ）
SET IP RIP（369 ページ）
SHOW IP（429 ページ）
SHOW IP RIP（468 ページ）

ADD IP ROUTE

カテゴリー：IP / 経路制御（スタティック）

ADD IP ROUTE=*ipadd* INTERFACE=*interface* NEXTHOP=*ipadd* [MASK=*ipadd*]
[METRIC=*1..16*] [METRIC1=*1..16*] [METRIC2=*1..65535*] [POLICY=*0..7*]
[PREFERENCE=*0..65535*]

ipadd: IP アドレスまたはネットマスク
interface: IP インターフェース名（eth0、ppp0 など）

解説

IP ルーティングテーブルにスタティック経路を追加する。

パラメーター

ROUTE 宛先ネットワークの IP アドレス。MASK と組み合わせて指定する。デフォルト経路の場合は 0.0.0.0 を指定する

INTERFACE 本経路宛てのパケットを送出する IP インターフェース

NEXTHOP ネクストホップルーターの IP アドレス。ダイレクト経路の場合は 0.0.0.0 を指定する。また、PPP インターフェース側に向けた経路の場合も 0.0.0.0 を指定できる。

MASK 宛先ネットワークのネットマスク。省略時は ROUTE パラメーターで指定した IP アドレスの標準クラスマスクが使用される。デフォルト経路のマスクは 0.0.0.0 とする（省略可能）

METRIC RIP が使用するメトリック。METRIC1 パラメーターも同じ意味。省略時は 1

METRIC1 RIP が使用するメトリック。METRIC パラメーターも同じ意味。省略時は 1

METRIC2 OSPF が使用するメトリック。省略時は 1

POLICY 本経路のサービスタイプ（TOS）。省略時は 0

PREFERENCE 経路選択時の優先度。小さいほど優先度が高い。複数の経路が存在するときはもっとも優先度の高い経路が使用される。省略時の値はデフォルト経路（0.0.0.0）が 360、その他のスタティック経路が 60。なお、インターフェース経路は優先度 0、RIP 経路は優先度 100、BGP 経路は優先度 170 となる。

例

■ppp0 上にデフォルト経路を設定する。

```
ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
```

■ネットワーク 172.20.53.0/24 への経路を設定する。

```
ADD IP ROUTE=172.20.53.0 MASK=255.255.255.0 INT=vlan1 NEXTHOP=172.16.1.1
```

関連コマンド

DELETE IP ROUTE（237 ページ）
SET IP ROUTE（372 ページ）
SHOW IP ROUTE（473 ページ）

ADD IP ROUTE FILTER

カテゴリー：IP / 経路制御フィルター

ADD IP ROUTE FILTER[=*entry-id*] **IP=*ipadd* MASK=*ipadd* ACTION=**{**INCLUDE**|**EXCLUDE**} [DIRECTION={RECEIVE|SEND|BOTH}] [INTERFACE=*interface*] [NEXTHOP=*ipadd*] [POLICY=*0..7*] [PROTOCOL={ANY|RIP|OSPF}]

entry-id: エントリー番号（1〜100）
ipadd: IP アドレスまたはネットマスク
interface: IP インターフェース名（eth0、ppp0 など）

解説

IP ルートフィルターリストにフィルターエントリーを追加する。
経路情報の送受信時には、ルートフィルターリストが番号の若い順に検索され、最初にマッチしたエントリーが適用される。
ルートフィルターは、おもにダイナミックルーティングプロトコルによる経路情報の交換を制御するもので、内部の経路情報（の一部）を外部に知らせないようにしたり、他のルーターから得た経路情報の一部を破棄したりする設定が可能。

パラメーター

FILTER　フィルターエントリー番号。省略時はフィルターリストの末尾に追加される。すでに n 個のエントリーが存在している場合（1〜n が存在）、本パラメーターを省略すると「n+1」を指定したのと同じ動作になる。また、「n+1」より大きなエントリー番号を指定した場合も「n+1」を指定したものと見なされる。既存エントリーと同じ番号を指定した場合は、既存エントリーの前に新規エントリーが追加され、既存エントリー以降は番号が 1 つずつ後ろにずれる。

IP　ネットワークアドレスを指定する。バイト単位でワイルドカード（*）の指定が可能。たとえば、「192.168.*.*」は「192.168」で始まるすべてのアドレスにマッチする。「192.168.12*.*」のような指定は無効。

MASK　ネットマスクを指定。IP パラメーター同様、ワイルドカードを使用可能。

ACTION　条件にマッチした経路情報に対するアクションを指定する。INCLUDE は経路情報をメッセージに含める（送信時）あるいはルーティングテーブルに追加する（受信時）。EXCLUDE は経路情報をメッセージに含めない（送信時）あるいはルーティングテーブルに追加しない（受信時）。

DIRECTION　経路情報の送信時（SEND）にフィルターをかけるか、受信時（RECEIVE）にかけるか、あるいは、送信時受信時とも（BOTH）かを指定する。PROTOCOL に RIP を指定したときは、DIRECTION を省略すると BOTH の意味になるが、PROTOCOL に OSPF を指定したときは、必ず SEND、RECEIVE を明示的に指定しなくてはならない。

INTERFACE　フィルターを適用する IP インターフェースを指定する。指定時は、該当インターフェースで送受信される経路情報に対してのみフィルターが適用される。

NEXTHOP　ネクストホップルーターの IP アドレス。本パラメーターを指定したときは、ネクストホップ

が一致する経路エントリーだけがフィルターの適用対象となる。

POLICY　フィルターの適用対象となる経路エントリーのサービスタイプ（TOS）値を指定する。無指定時はすべてのサービスタイプが対象。

PROTOCOL　フィルターの適用対象となるルーティングプロトコルを指定する。デフォルトは ANY（すべて）。

例

■宛先が「200.200.*.*」となる経路情報の送受信を行わないようにする

```
ADD IP ROUTE FILTER=1 IP=200.200.*.* MASK=*.*.*.* ACTION=EXCLUDE
ADD IP ROUTE FILTER=2 IP=*.*.*.* MASK=*.*.*.* ACTION=INCLUDE
```

備考・注意事項

OSPF と RIP で DIRECTION パラメーターの意味が異なるので注意すること。OSPF を指定した場合は、SEND、RECEIVE を明示的に指定する。

関連コマンド

DELETE IP ROUTE FILTER（238 ページ）
SET IP ROUTE FILTER（374 ページ）
SHOW IP ROUTE FILTER（476 ページ）

ADD IP ROUTE TEMPLATE

カテゴリー：IP / 経路制御

ADD IP ROUTE TEMPLATE=*template* INTERFACE=*interface* NEXTHOP=*ipadd*
[METRIC=*1..16*] [METRIC1=*1..16*] [METRIC2=*1..65535*] [POLICY=*0..7*]
[PREFERENCE=*0..65535*]

template: ルートテンプレート名（1〜31 文字。大文字小文字を区別しない）
interface: IP インターフェース名（eth0、ppp0 など）
ipadd: IP アドレス

解説

IP ルートテンプレート（動的に登録される経路エントリーのひな形）を作成する。
IPsec ポリシーの IPROUTETEMPLATE パラメーターにルートテンプレート名を指定しておくと、該当 IPsec ポリシーに基づいて SA が確立されたときに、相手ネットワークへの経路が経路表に自動登録される。主に、対向ネットワークが間欠的に VPN 接続してくる環境で、相手ネットワークの経路情報を明示的に登録しなくてはならない場合に使う。たとえば、デフォルト経路を使っていない場合などが考えられる。

パラメーター

TEMPLATE　IP ルートテンプレート名
INTERFACE　パケットを送出する IP インターフェース
NEXTHOP　ネクストホップルーターの IP アドレス。ダイレクト経路の場合は 0.0.0.0 を指定する。また、PPP インターフェース側に向けた経路の場合も 0.0.0.0 を指定できる。
METRIC　RIP が使用するメトリック。METRIC1 パラメーターも同じ意味。省略時は 1
METRIC1　RIP が使用するメトリック。METRIC パラメーターも同じ意味。省略時は 1
METRIC2　OSPF が使用するメトリック。省略時は 1
POLICY　本経路のサービスタイプ（TOS）。省略時は 0
PREFERENCE　経路選択時の優先度。小さいほど優先度が高い。複数の経路が存在するときはもっとも優先度の高い経路が使用される。省略時の値はデフォルト経路（0.0.0.0）が 360、その他のスタティック経路が 60。なお、インターフェース経路は優先度 0、RIP 経路は優先度 100、BGP 経路は優先度 170 となる。

例

■IP ルートテンプレート net10 を作成し、IPsec ポリシー vp10 に関連づける。この例では、IPsec ポリシー vp10 に基づいて IPsec SA が作成されたときに、10.10.10.0/24 への経路が経路表に自動登録される。また、該当経路は SA が削除されると同時に削除される。

```
ADD IP ROUTE TEMPLATE=net10 INT=ppp0 NEXT=0.0.0.0
CREATE IPSEC POLICY=vp10 INT=ppp0 ACTION=IPSEC KEY=ISAKMP BUNDLE=1
  PEER=DYNAMIC IPROUTE=net10
SET IPSEC POLICY=vp10 LAD=192.168.10.0 LMA=255.255.255.0 RAD=10.10.10.0
  RMA=255.255.255.0
```

関連コマンド

CREATE IPSEC POLICY（「IPsec」の 39 ページ）
DELETE IP ROUTE TEMPLATE（239 ページ）
SET IP ROUTE TEMPLATE（378 ページ）
SHOW IP ROUTE TEMPLATE（479 ページ）

ADD IP ROUTEMAP

カテゴリー：IP / 経路制御（BGP-4）

```
ADD IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]

ADD IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   MATCH ASPATH=1..99

ADD IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   MATCH COMMUNITY=1..99 [EXACT={NO|YES}]

ADD IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   SET ASPATH={1..65534}[,...]

ADD IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   SET COMMUNITY={INTERNET|NOEXPORT|NOADVERTISE|1..4294967295}[,...]
   [ADD={NO|YES}]

ADD IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   SET LOCALPREF=0..4294967295

ADD IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   SET MED=0..4294967295

ADD IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   SET ORIGIN={IGP|EGP|INCOMPLETE}
```

routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）

解説

ルートマップにエントリーを追加する。
ルートマップは、BGP 経路に対するフィルタリング機能の 1 つ。AS パスフィルターやコミュニティーフィルターと組み合わせて、送受信する経路エントリーをフィルタリングしたり、特定の経路エントリーの属性値を書き換えたりするときに使用する。
ルートマップは複数のエントリーで構成されるリスト。個々のフィルターは名前によって区別される。
フィルター内の各エントリーは、0〜1 個の MATCH 節と、1 個以上の SET 節によって構成される。MATCH 節は経路エントリーとマッチするための条件。MATCH 節がない場合はすべての経路にマッチする。SET 節はマッチしたエントリーの属性を変更するための指定。複数の SET 節を使う場合、各 SET 節は別の属性を対象としていなくてはならない。
作成したルートマップは、次のタイミングで適用できる

・BGP ピアに経路を通知する直前（ADD BGP PEER コマンド、SET BGP PEER コマンドの OUT-ROUTEMAP）
・BGP ピアから経路を受信した直後（ADD BGP PEER コマンド、SET BGP PEER コマンドの IN-ROUTEMAP）
・経路を BGP に登録するとき（ADD BGP NETWORK コマンド）
・経路を集約するとき（ADD BGP AGGREGATE コマンド、SET BGP AGGREGATE コマンド）
・静的経路や IGP 経路を BGP にインポートするとき（ADD BGP IMPORT コマンド、SET BGP IMPORT コマンド）
・BGP 経路をルーターの経路表に登録するとき（SET BGP コマンドの TABLEMAP）
MATCH節で指定したフィルター（ASパスフィルターやコミュニティーフィルター）がINCLUDEを返してきた場合、該当経路エントリーはルートマップエントリーのアクション（ACTION={INCLUDE|EXCLUDE}）によって処理される。
マッチしたルートマップエントリーのアクションが INCLUDE の場合、SET 節が実行される。EXCLUDE の場合は、該当経路の処理を続行しない（経路を受信しない、送信しない、など）。アクションは、最初にマッチしたエントリーで実行される。各ルートマップの末尾には、すべてを INCLUDE する SET 節が空の暗黙のエントリーが存在する。

パラメーター

ROUTEMAP　ルートマップ名

ENTRY　ルートマップ内におけるエントリーの位置。他のフィルターとは異なり、1〜4294967295 の範囲の任意の番号を指定できる（絶対指定）。間隔をあけてエントリーを配置することにより、エントリーの追加に対応できる。

ACTION　ルートマップエントリーにマッチした場合のアクション（INCLUDE、EXCLUDE）。INCLUDE の場合は SET 節の処理に進む。EXCLUDE の場合は該当経路の処理を行わない（破棄 = 通知しない、受信しない、など）。デフォルトは INCLUDE

MATCH ASPATH　AS パスフィルター番号。AS_PATH 属性の値によってマッチを行う場合に指定する。

MATCH COMMUNITY　コミュニティーフィルター番号。COMMUNITIES 属性の値によってマッチを行う場合に指定する。

SET ASPATH　AS パス。MATCH 節にマッチした経路エントリーの AS_PATH 属性の末尾に指定した AS パス値を追加する。AS パスは、AS 番号をカンマ区切りで並べることによって指定する。AS 番号は最大 10 個まで指定可能。

SET COMMUNITY　コミュニティーリスト。MATCH 節にマッチした経路エントリーの COMMUNITIES 属性に指定したコミュニティー値をセットする。コミュニティー値か Well-known コミュニティーを示すキーワードをカンマ区切りで列挙する。

EXACT　コミュニティーフィルターとのマッチングを完全一致で行うかどうか。NO（デフォルト）は部分一致。YES は完全一致。MATCH COMMUNITY パラメーターを指定した場合のみ有効。

ADD　SET COMMUNITY パラメーターを指定した場合、既存の COMMUNITIES 属性を置き換えるか、既存の属性に追加するかを指定する。NO（デフォルト）は COMMUNITIES 属性を置き換える。YES を指定した場合は、既存の COMMUNITIES 属性値に SET COMMUNITY パラメーターで指定した値を追加する。

SET LOCALPREF　マッチした経路エントリーの LOCAL_PREF 属性に指定した値をセットする。

SET MED　マッチした経路エントリーの MULTI_EXIT_DISCRIMINATOR 属性に指定した値をセットする。

SET ORIGIN　マッチした経路エントリーの ORIGIN 属性に指定した値をセットする。

例

■コミュニティー「100」を設定するルートマップ「mark_it_100」を作成。MATCH 節がないのですべての経路に適用される。

```
ADD IP ROUTEMAP=mark_it_100 ENTRY=1 SET COMMUNITY=1
```

■ローカル経路（AS パスが空）に AS 番号「2」を 2 度追加するルートマップ「prepend2_2」を作成。MATCH ASPATH には、対象の AS パスそのものではなく、AS パスフィルターの番号を指定することに注意。

```
ADD IP ASPATHLIST=1 INCLUDE="^$"
ADD IP ROUTEMAP=prepend2_2 ENTRY=1 MATCH ASPATH=1
ADD IP ROUTEMAP=prepend2_2 ENTRY=1 SET ASPATH=2,2
```

■コミュニティー「100」を持つ経路に MED 値「500」をセットするルートマップ「med_on_c100」を作成。MATCH COMMUNITY には、対象のコミュニティー値そのものではなく、コミュニティーフィルターの番号を指定することに注意。

```
ADD IP COMMUNITYLIST=1 INCLUDE=100
ADD IP ROUTEMAP=med_on_c100 ENTRY=1 MATCH COMMUNITY=1
ADD IP ROUTEMAP=med_on_c100 ENTRY=1 SET MED=500
```

関連コマンド

ADD BGP PEER（154 ページ）
DELETE IP ROUTEMAP（240 ページ）
SET BGP PEER（343 ページ）
SET IP ROUTEMAP（379 ページ）
SHOW IP ROUTEMAP（481 ページ）

ADD IP TRUSTED

カテゴリー：IP / 経路制御フィルター

ADD IP TRUSTED=*ipadd*

ipadd: IP アドレス

解説

RIP の Trusted Router リストに IP アドレスを追加する。
Trusted Router がひとつでも定義されている場合、リストに登録されている IP アドレスからの RIP 情報だけを使用する。Trusted Router が定義されていないときは、すべての RIP 情報を使用する。Trusted Router は 32 個まで登録できる。

パラメーター

TRUSTED　Trusted Router の IP アドレス

例

■172.30.100.1 からの RIP 情報だけを使用する。

```
ADD IP TRUSTED=172.30.100.1
```

関連コマンド

ADD IP FILTER（169 ページ）
DELETE IP FILTER（230 ページ）
DELETE IP TRUSTED（241 ページ）
SET IP FILTER（360 ページ）
SHOW IP FILTER（449 ページ）
SHOW IP TRUSTED（483 ページ）

ADD OSPF AREA

カテゴリー：IP / 経路制御（OSPF）

ADD OSPF AREA={**BACKBONE**|***area-number***} [AUTHENTICATION={NONE|PASSWORD|MD5}] [STUBAREA={ON|OFF|YES|NO|TRUE|FALSE|NSSA}] [STUBMETRIC=*0..16777215*] [SUMMARY={SEND|NONE|OFF|NO|FALSE}]

area-number: OSPF エリア ID（a.b.c.d の形式）

解説

OSPF エリアを作成する。

パラメーター

AREA　エリア ID。0.0.0.0（バックボーンエリア）はキーワード「BACKBONE」で指定することもできる。

AUTHENTICATION　エリア内での認証方式。NONE（無認証）、PASSWORD（簡易パスワード）、MD5（MD5 ダイジェスト）がある。実際のパスワード（簡易パスワード認証時）は ADD OSPF INTERFACE コマンドで、MD5 認証鍵（MD5 ダイジェスト認証時）は ADD OSPF MD5KEY コマンドでインターフェースごとに設定する。また、ADD OSPF INTERFACE コマンドでインターフェースごとに認証方式を設定することもできる。この場合、インターフェースごとに設定した認証方式が優先される。デフォルトは NONE。

STUBAREA　対象エリアをスタブエリアにするかどうか。ON、YES、TRUE（スタブエリアにする）および OFF、NO、FALSE（スタブエリアにしない）はそれぞれ同じ意味。スタブエリアは AS 外部の経路情報を持たないエリアで、AS 外部へのトラフィックはすべてデフォルトルートに送られる。バックボーン（0.0.0.0）エリアと仮想リンクの通過エリアでは必ず OFF に設定すること。また、スタブエリア内に複数の OSPF ルーターが存在する場合は、STUBAREA パラメーターの設定を同じにすること。また、本パラメーターに NSSA を指定した場合、対象エリアは準スタブエリア（NSSA = Not-So-Stubby Area）となる。スタブエリアとは異なり、準スタブエリアには AS 境界ルーター（ASBR）を配置することができ、AS 外部の経路情報をタイプ 7 の LSA として取り込むことができる。バックボーンエリアのデフォルトは OFF、その他のエリアのデフォルトは ON。

STUBMETRIC　スタブエリア内に通知するデフォルトルート（デフォルトサマリー LSA）のメトリック。デフォルトは 1。本パラメーターはスタブエリアのエリア境界ルーター（ABR）でのみ有効。

SUMMARY　スタブエリア内にデフォルトルート以外の経路情報を通知するかどうか。NONE、OFF、NO、FALSE（通知しない）は同じ意味。SEND を指定した場合は、デフォルト以外のエリア情報もサマリー LSA でスタブエリア内に通知される。NONE を指定した場合は、デフォルトのサマリー LSA だけが ABR によってスタブエリア内に通知される。STUBAREA=NSSA のときのデフォルトは SEND、それ以外の場合のデフォルトは NONE。

例

■バックボーンエリアを作成する。

```
ADD OSPF AREA=0.0.0.0
```

■仮想リンクが通過するエリア 1.1.1.1 を作成する。

```
ADD OSPF AREA=1.1.1.1 STUBAREA=OFF
```

備考・注意事項

・各ルーター上では、自分の所属するエリアだけを作成すればよい。
・仮想リンクの通過エリアを作成するときは、必ず STUBAREA=OFF を指定すること。

関連コマンド

ADD OSPF INTERFACE（202 ページ）
ADD OSPF RANGE（208 ページ）
DELETE OSPF AREA（242 ページ）
DELETE OSPF RANGE（247 ページ）
SET OSPF AREA（384 ページ）
SET OSPF RANGE（390 ページ）
SHOW OSPF AREA（487 ページ）
SHOW OSPF RANGE（505 ページ）

ADD OSPF HOST

カテゴリー：IP / 経路制御（OSPF）

ADD OSPF HOST=*ipadd* [METRIC=*0..65535*]

ipadd: IP アドレス

解説

OSPF ルーティングテーブルにホスト経路を追加する。
ホスト経路は、経路マスク 255.255.255.255 でエリア内に通知される経路。PPP や SLIP でルーターと一対一接続されているホストへの経路を示すために使用される。

パラメーター

HOST　ホストの IP アドレス。ルーター上で設定したエリア範囲内のアドレスでなくてはならない。
METRIC　メトリック。デフォルトは 1。

関連コマンド

ADD OSPF INTERFACE（202 ページ）
DELETE OSPF HOST（243 ページ）
SET OSPF HOST（385 ページ）
SHOW OSPF HOST（491 ページ）
SHOW OSPF INTERFACE（493 ページ）

ADD OSPF INTERFACE

カテゴリー：IP / 経路制御（OSPF）

ADD OSPF INTERFACE=*interface* AREA={**BACKBONE**|***area-number***}
[DEADINTERVAL=*2..2147483647*] [DEMAND={ON|OFF|YES|NO|TRUE|FALSE}]
[HELLOINTERVAL=*1..65535*] [AUTHENTICATION={NONE|PASSWORD|MD5}]
[PASSWORD=*password*] [PRIORITY=*0..255*] [RXMTINTERVAL=*1..3600*]
[TRANSITDELAY=*1..3600*] [VIRTUALLINK=*area-number*] [NETWORK={BROADCAST|
NON-BROADCAST}] [POLLINTERVAL=*1..2147483647*] [PASSIVE={ON|OFF|YES|NO|
TRUE|FALSE}]

interface: IP インターフェース名（eth0、ppp0 など）または仮想インターフェース名（VIRTn）
area-number: OSPF エリア ID（a.b.c.d の形式）
password: パスワード（1〜8 文字。任意の印刷可能文字を使用可能。空白を含む場合はダブルクォートで囲む）

解説

OSPF インターフェースを追加する。仮想リンクの作成も本コマンドで行う。
インターフェースを追加するには、あらかじめエリアの作成とアドレスレンジの指定が必要。

パラメーター

INTERFACE　IP インターフェース（VLAN）名または仮想インターフェース名（VIRTn）を指定する。該当インターフェースは、AREA で指定したエリアの範囲内になくてはならない。

AREA　エリア ID。仮想インターフェースの場合は通過エリアのエリア ID を指定する。

DEADINTERVAL　Hello パケットの Router Dead Interval タイマー（秒）。隣接ルーターから Hello パケットを受信できなくなったときに、隣接ルーターがダウンしたと判断するまでの時間を示す。同一ネットワーク上のすべてのルーターに同じ値を設定する必要がある。最小値は HELLOINTERVAL × 2、推奨値は HELLOINTERVAL × 4。デフォルト値は HELLOINTERVAL × 4（秒）。

DEMAND　OSPF オンデマンド（RFC1793）を使用するかどうか。デフォルトは OFF

HELLOINTERVAL　Hello パケットの送信間隔（Hello Interval）（秒）。同一ネットワーク上のすべてのルーターに同じ値を設定する必要がある。デフォルトは 10 秒。

AUTHENTICATION　本インターフェースにおける認証方式。NONE（無認証）、PASSWORD（簡易パスワード）、MD5（MD5 ダイジェスト）から選択する。パスワード（簡易パスワード認証時）は PASSWORD パラメーターで、MD5 認証鍵（MD5 ダイジェスト認証時）は ADD OSPF MD5KEY コマンドでインターフェースごとに設定する。本パラメーターの設定は、ADD OSPF AREA コマンドで設定したエリアごとの設定よりも優先される。デフォルトは NONE（エリアの設定が使用される）。

PASSWORD　認証用パスワード。エリア内またはインターフェースでの認証方法が簡易パスワード認証の場合（AUTHENTICATION パラメーターに PASSWORD を指定した場合）にのみ必要。デフォルトはパスワードなし（null）。なお、MD5 ダイジェスト認証の場合は、ADD OSPF MD5KEY コ

マンドで認証鍵を設定する。

PRIORITY　ルーター優先度（0～255）。大きいほど優先度が高く、指名ルーター（DR）に選出される可能性が高くなる。優先度が同じときはルーター ID の大きいほうが DR となる。0 は DR になる資格がないことを示す。デフォルトは 1。

RXMTINTERVAL　データベース記述パケット（タイプ 2）、リンク状態要求パケット（タイプ 3）、リンク状態更新パケット（タイプ 4）の再送間隔（秒）。隣接ルーター間のパケット往復時間よりも十分に大きな値でなくてはならない。LAN では 5 秒が標準的。デフォルトは 5 秒。

TRANSITDELAY　リンク状態更新パケットの送信遅延時間（秒）。同パケットに含まれる LSA のエイジフィールドはこの値だけ増分される。LAN では通常 1 に設定される。デフォルトは 1

VIRTUALLINK　仮想リンクの対向に位置するバックボーンルーター（ABR）のルーター ID。仮想インターフェース追加時（INTERFACE=VIRTn）の必須パラメーター。このとき、AREA には通過エリアの ID を指定する。

NETWORK　該当インターフェースに接続されているネットワークの種別。BROADCAST（ブロードキャスト型マルチアクセス）、NON-BROADCAST（非ブロードキャスト型マルチアクセス（NBMA））から選択する。本パラメーターは VLAN インターフェースでのみ有効。デフォルトは BROADCAST。

POLLINTERVAL　非ブロードキャスト型のマルチアクセスネットワーク（NBMA）における、非アクティブな隣接ルーターへの Hello パケット送信間隔（秒）。NETWORK=NON-BROADCAST を指定したときのみ有効。HELLOINTERVAL よりも大きな値を指定する必要がある。デフォルトは HELLOINTERVAL × 4（秒）。

PASSIVE　該当インターフェースをパッシブインターフェースにするかどうか。ON、YES、TRUE（パッシブインターフェースにする）および OFF、NO、FALSE（パッシブインターフェースにしない）はそれぞれ同じ意味。パッシブインターフェースでは OSPF パケットの送受信を行わないが、パッシブインターフェースに接続されているネットワークの情報は、スタブネットワークとしてルーター LSA に追加される。デフォルトは OFF だが、SET OSPF コマンドの PASSIVEINTERFACEDEFAULT パラメーターに値を指定しているとき（デフォルトは未指定）は、その値が本パラメーター省略時の値となる。

例

■バックボーンエリアに VLAN orange のインターフェースを追加する。

```
ADD OSPF INT=vlan-orange AREA=BACKBONE
```

■ルーター 192.168.10.1 と 192.168.10.254 の間に仮想リンクを作成する。通過エリアは 1.1.1.1。通過エリア 1.1.1.1 を作成するときは STUBAREA=OFF を指定して、スタブエリアでないように設定しなくてはならない。

[**ルーター** 192.168.10.254 **側**]

```
ADD OSPF INT=virt0 AREA=1.1.1.1 VIRTUALLINK=192.168.10.1
```

[**ルーター** 192.168.10.1 **側**]

```
ADD OSPF INT=virt0 AREA=1.1.1.1 VIRTUALLINK=192.168.10.254
```

備考・注意事項

・仮想リンクは両エンドで設定する必要がある。
・仮想リンクを作成するときは、SET OSPF コマンドの ROUTERID パラメーターでルーター ID を明示的に指定しておくと設定がやりやすい。
・NETWORK=BROADCAST を指定した場合は、該当インターフェースに接続されたネットワークをブロードキャスト可能なネットワークと見なし、隣接ルーターの動的探索を行う（Ethernet/VLAN 上における通常の動作）。NETWORK=NON-BROADCAST を指定した場合は、該当インターフェースに接続されたネットワークを非ブロードキャスト型のマルチアクセスネットワーク（NBMA）と見なし、隣接ルーターの動的探索を行わない。したがって、NETWORK=NONBROADCAST を指定した場合は、ADD OSPF NEIGHBOUR コマンドで隣接ルーターをスタティックに設定する必要がある。

関連コマンド

ADD OSPF AREA（199 ページ）
ADD OSPF MD5KEY（205 ページ）
ADD OSPF NEIGHBOUR（207 ページ）
ADD OSPF RANGE（208 ページ）
DELETE OSPF INTERFACE（244 ページ）
DISABLE OSPF INTERFACE（281 ページ）
ENABLE OSPF INTERFACE（313 ページ）
RESET OSPF INTERFACE（332 ページ）
SET OSPF（381 ページ）
SET OSPF AREA（384 ページ）
SET OSPF INTERFACE（386 ページ）
SET OSPF RANGE（390 ページ）
SHOW OSPF AREA（487 ページ）
SHOW OSPF INTERFACE（493 ページ）
SHOW OSPF RANGE（505 ページ）

ADD OSPF MD5KEY

カテゴリー：IP / 経路制御（OSPF）

ADD OSPF MD5KEY=*string* ID=*1..255* INTERFACE=*interface*

string: 文字列（1〜16 文字。英数字のみ。大文字小文字を区別する）
interface: IP インターフェース名（eth0、ppp0 など）または仮想インターフェース名（VIRTn）

解説

指定した OSPF インターフェースで使用する MD5 ダイジェスト認証用の鍵を追加する。1 つの OSPF インターフェースには、255 個まで鍵を設定できる。
本コマンドは、エリア内またはインターフェースでの認証方法が MD5 ダイジェスト認証の場合（AUTHENTICATION パラメーターに MD5 を指定した場合）にのみ有効。MD5 ダイジェスト認証を使うときは、同一サブネット上のすべての OSPF インターフェースで同じ鍵セットを使用するよう設定しなくてはならない（鍵の番号と値が一致していなくてはならない）。
認証方式は MD5 に設定されているが、鍵がまだ設定されていない場合は、鍵番号「0」のデフォルト鍵が自動的に作成され使用される。
なお、簡易パスワード認証を使用する場合は、ADD OSPF INTERFACE コマンドでパスワードを設定する。

パラメーター

MD5KEY　鍵の値（文字列）。英数字 16 文字以内で指定する。
ID　鍵番号（Key ID）。この番号は、受信パケットを認証する時に、どの鍵を使用すべきかを判断するために使用される。
INTERFACE　OSPF インターフェース名。1 つのインターフェースには 255 個まで鍵を設定できる。各鍵はインターフェースと鍵番号の組み合わせによって一意に識別される。

例

■OSPF インターフェース vlan10 で使う MD5 認証の鍵として、値「e8bvDISff63」（鍵番号「1」）を追加する。

```
ADD OSPF MD5KEY=e8bvDISff63 ID=1 INTERFACE=vlan10
```

関連コマンド

ADD OSPF AREA（199 ページ）
ADD OSPF INTERFACE（202 ページ）
DELETE OSPF MD5KEY（245 ページ）

SET OSPF AREA（384 ページ）
SET OSPF INTERFACE（386 ページ）
SHOW OSPF AREA（487 ページ）
SHOW OSPF INTERFACE（493 ページ）
SHOW OSPF MD5KEY（501 ページ）

ADD OSPF NEIGHBOUR

カテゴリー：IP / 経路制御（OSPF）

ADD OSPF NEIGHBOUR=*ipadd* PRIORITY=*0..255*

ipadd: IP アドレス

解説

OSPF 隣接ルーターをスタティックに設定する。
ブロードキャストを使用できないフレームリレーなどの非ブロードキャスト型ネットワークで使用する。

パラメーター

NEIGHBOUR　OSPF 隣接ルーターの IP アドレス。ルーター上で定義されている OSPF エリアの範囲内になくてはならない。
PRIORITY　隣接ルーターのルーター優先度。

関連コマンド

ADD OSPF INTERFACE（202 ページ）
DELETE OSPF INTERFACE（244 ページ）
DELETE OSPF NEIGHBOUR（246 ページ）
SET OSPF INTERFACE（386 ページ）
SET OSPF NEIGHBOUR（389 ページ）
SHOW OSPF INTERFACE（493 ページ）
SHOW OSPF NEIGHBOUR（503 ページ）

ADD OSPF RANGE

カテゴリー：IP / 経路制御（OSPF）

ADD OSPF RANGE=*ipadd* AREA={**BACKBONE**|***area-number***} [MASK=*ipadd*]
[EFFECT={ADVERTISE|DONOTADVERTISE}]

ipadd: IP アドレスまたはネットマスク
area-number: OSPF エリア ID（a.b.c.d の形式）

解説

OSPF エリアを構成するネットワークの範囲を定義する。
基本的には直接接続されているネットワークの範囲だけを指定すればよいが、ABR ではエリア範囲を広く（短いマスクで）指定することにより、他エリアに通知する経路情報をまとめることができる。

パラメーター

RANGE　IP ネットワークアドレス
AREA　エリア ID
MASK　ネットマスク。RANGE パラメーターと組み合わせてエリアに所属するネットワークの範囲を指定する。省略時は RANGE で指定した IP アドレスのクラス（クラス A、B、C）に応じた標準ネットマスクが使用される
EFFECT　指定したネットワーク範囲をエリア外部に通知するかどうか。エリア境界ルーター（ABR）でのみ有効。ADVERTISE を指定した場合、該当範囲の情報を 1 つのサマリー LSA としてエリア外に通知する。DONOTADVERTISE を指定した場合は情報を通知しない。デフォルトは ADVERTISE

例

■バックボーンエリアに所属するネットワークの範囲を定義する。ここでは、172.16.0.0～172.16.255.255 と 172.17.0.0～172.17.255.255 の範囲を指定している。基本的には直接接続されているネットワークの範囲だけを指定すればよいが、ABR ではエリア範囲を広く（短いマスクで）指定することにより、他エリアに通知する経路情報をまとめることができる。

```
ADD OSPF RANGE=172.16.0.0 MASK=255.255.0.0 AREA=BACKBONE
ADD OSPF RANGE=172.17.0.0 MASK=255.255.0.0 AREA=BACKBONE
```

関連コマンド

DELETE OSPF RANGE（247 ページ）
SET OSPF RANGE（390 ページ）

SHOW OSPF RANGE（505 ページ）

ADD OSPF REDISTRIBUTE

カテゴリー：IP / 経路制御（OSPF）

ADD OSPF REDISTRIBUTE PROTOCOL={**STATIC**|**INTERFACE**|**RIP**|**BGP**}
[METRIC=*0..16777214*] [TYPE={*1*|*2*}]

解説

非 OSPF 経路を取り込み、AS 外部 LSA で AS 内に通知するよう設定する。
本コマンドは AS 境界ルーター（ASBR）でのみ意味を持つ。

パラメーター

PROTOCOL 取り込む AS 外部経路の起源。STATIC（スタティック経路）、INTERFACE（非 OSPF インターフェースの直結経路）、RIP（RIP 経路）、BGP（BGP 経路）から選択する。
METRIC PROTOCOL パラメーターで指定した起源を持つ AS 外部経路のメトリック。デフォルトは 20
TYPE PROTOCOL パラメーターで指定した起源を持つ AS 外部経路のメトリックタイプ（1 または 2）。デフォルトは 2

関連コマンド

DELETE OSPF REDISTRIBUTE（248 ページ）
SET OSPF REDISTRIBUTE（391 ページ）
SHOW OSPF REDISTRIBUTE（507 ページ）

ADD OSPF STUB

カテゴリー：IP / 経路制御（OSPF）

ADD OSPF STUB=*ipadd* MASK=*ipadd* [METRIC=*0..65535*]

ipadd: IP アドレスまたはネットマスク

解説

OSPF ルーティングテーブルに、OSPF を使用していないネットワーク（スタブネットワーク）への経路情報を追加する。

パラメーター

STUB　スタブネットワークのネットワークアドレス。ルーター上で定義されているエリアの範囲内でなくてはならない
MASK　STUB に対するネットワークマスク
METRIC　メトリック。デフォルトは 1

関連コマンド

ADD OSPF HOST（201 ページ）
ADD OSPF INTERFACE（202 ページ）
DELETE OSPF STUB（249 ページ）
SET OSPF STUB（392 ページ）
SHOW OSPF STUB（510 ページ）

ADD OSPF SUMMARYADDRESS

カテゴリー：IP / 経路制御（OSPF）

ADD OSPF SUMMARYADDRESS=*ipadd* MASK=*ipadd* [ADVERTISE={ON|OFF|YES|NO|TRUE|FALSE}] [TAG=*0..65535*]

ipadd: IP アドレスまたはネットマスク

解説

AS 外部経路の集約設定（集約経路エントリー）を追加する。
集約経路エントリーは、指定したネットワークの範囲に収まる、より具体的な外部経路を 1 つにまとめるもの。たとえば、集約経路エントリー「192.168.0.0/16」を作成すると、この範囲に収まる AS 外部経路「192.168.10.0/24」「192.168.20.0/24」「192.168.30.0/24」は、1 つの AS 外部 LSA「192.168.0.0/19」に集約された上で AS 内に通知される（ADVERTISE=NO で広告しない設定も可能）。
本コマンドは AS 境界ルーター（ASBR）でのみ意味を持つ。

パラメーター

SUMMARYADDRESS　集約後のネットワークアドレス。
MASK　SUMMARYADDRESS に対するネットワークマスク。
ADVERTISE　集約経路（SUMMARYADDRESS/MASK）を AS 外部 LSA で AS 内に通知するかどうか。ON、YES、TRUE を指定した場合は、集約経路を 1 つの AS 外部 LSA として AS 内に通知する。OFF、NO、FALSE を指定した場合は該当経路を AS 内に通知しない。デフォルトは ON。
TAG　集約経路の AS 外部 LSA にセットする外部経路タグ。デフォルトは 0。

関連コマンド

DELETE OSPF SUMMARYADDRESS（250 ページ）
SET OSPF（381 ページ）
SET OSPF SUMMARYADDRESS（393 ページ）
SHOW OSPF SUMMARYADDRESS（512 ページ）

ADD PING POLL

カテゴリー：IP / Ping ポーリング

```
ADD PING POLL=poll-id IPADDRESS=ipadd [CRITICALINTERVAL=1..65535]
    [DESCRIPTION=string] [FAILCOUNT=1..100] [LENGTH=4..1500]
    [NORMALINTERVAL=1..65535] [SAMPLESIZE=1..100] [SIPADDRESS=ipadd]
    [TIMEOUT=1..30] [UPCOUNT=1..100]
```

poll-id: Ping ポーリング ID（1〜100）
ipadd: IP アドレス（IPv4 または IPv6）
string: 文字列（1〜32 文字。空白を含む場合はダブルクォートで囲む）

解説

Ping ポーリングの監視対象機器を追加する。
本コマンド実行直後はポーリングが停止（無効）状態になっているので、実際にポーリングを開始するには、（トリガーの設定などを済ませたあとに）ENABLE PING POLL コマンドを実行する必要がある。

パラメーター

POLL　Ping ポーリング ID

IPADDRESS　監視対象機器の IP アドレス。IPv4 アドレスか IPv6 アドレスを指定する。IPv6 のリンクローカルアドレスを指定するときは、どのインターフェースからパケットを送出するかを示すため、アドレスの末尾にインターフェース名を付ける必要がある。その場合、アドレス、パーセント記号、インターフェース名の順に指定する（例：fe80::1234%eth1）。

CRITICALINTERVAL　機器の状態が「Up」以外のときのポーリング間隔（秒）。「Up」時のポーリング間隔（NORMALINTERVAL）よりも大幅に小さくすること。デフォルトは 1 秒。

DESCRIPTION　メモ。任意の文字列を指定できる。

FAILCOUNT　到達性が失われたと判断するために必要な Ping 無応答の回数。直前の SAMPLESIZE 回の Ping に対して、FAILCOUNT 回の無応答があった場合、監視対象機器が到達不可能になったと判断する。FAILCOUNT <= SAMPLESIZE となるよう設定すること。FAILCOUNT = SAMPLESIZE のときは、FAILCOUNT 回連続して無応答だったときだけ、到達不可能と判断する。FAILCOUNT < SAMPLESIZE のときは、無応答が連続していなくてもよい。デフォルトは 5 回。

LENGTH　Ping パケットのデータ部分の長さ（バイト）。省略時は 32 バイト

NORMALINTERVAL　機器の状態が「Up」のときのポーリング間隔（秒）。デフォルトは 30 秒。

SAMPLESIZE　到達性判断のために保持しておく Ping パケットの数。直前の SAMPLESIZE 回の Ping に対して、FAILCOUNT 回の無応答があった場合、監視対象機器が到達不可能になったと判断する。FAILCOUNT <= SAMPLESIZE となるよう設定すること。省略時は FAILCOUNT と同じ値になる。

SIPADDRESS　Ping パケットの始点 IP アドレス（IPv4、IPv6）。本パラメーター未指定時は、SET IP LOCAL コマンドでローカル IP アドレスが設定されているときはローカル IP アドレスが、ローカル

IP アドレスが設定されていないときは、送出インターフェースの IP アドレスが使われる。

TIMEOUT　Ping パケットの応答待ち時間（秒）。Ping（Echo request）パケット送信後、この時間内に応答パケットを受信しなかった場合は「無応答」と見なす。デフォルトは 1 秒

UPCOUNT　機器の状態が「Down」「Critical Down」から「Up」に戻るために必要な連続した「応答あり」の回数。「Down」「Critical Down」状態において、UPCOUNT 回連続して応答を受信すると、監視対象機器への到達性が回復したと判断する。デフォルトは 30 回。

備考・注意事項

本製品の PING コマンドは IPv4/IPv6 に対応しているが、Ping ポーリングは IPv4 と IPv6 だけの対応なので注意。

関連コマンド

DELETE PING POLL（251 ページ）
ENABLE PING POLL（316 ページ）
SET PING POLL（396 ページ）
SHOW PING POLL（515 ページ）

CREATE BGP DAMPING PARAMETERSET

カテゴリー：IP / 経路制御（BGP-4）

CREATE BGP DAMPING PARAMETERSET=*1..100* [DESCRIPTION[=*string*]]
[SUPPRESSION={DEFAULT|*1..32000*}] [REUSE={DEFAULT|*1..32000*}]
[HALFLIFE={DEFAULT|*1..45*}] [MAXHOLD={DEFAULT|*1..8*}]

string: 文字列（1〜63 文字）

解説

BGP-4 ルートフラップダンピング用のカスタムパラメーターセットを作成する。
ルートフラップダンピング有効時に作成したパラメーターセットの初期状態は「有効」、そうでないときに作成したパラメーターセットの初期状態は「無効」となる。無効状態のパラメーターセットを有効化するには、ENABLE BGP DAMPING コマンドの PARAMETERSET パラメーターを使う。
なお、カスタムパラメーターセットを使用するには、ルートマップの SET BGPDAMPID パラメーター（ADD IP ROUTEMAP コマンド）を使って、適用対象の経路に作成したカスタムパラメーターセットを関連付ける必要がある。
カスタムパラメーターセットと関連付けられていない経路に対しては、デフォルトで存在するパラメーターセット「0」（デフォルトパラメーターセット）が適用される。

パラメーター

PARAMETERSET　パラメーターセット番号。

DESCRIPTION　パラメーターセットに関する覚え書き（メモ）。

SUPPRESSION　抑制しきい値。経路のペナルティー値（経路の不安定さを示す）が本しきい値を上回ると、該当経路は Suppressed（抑制）状態となり、ペナルティー値が再使用しきい値（REUSE）を下回るか、安定状態が最大抑制時間（HALFLIFE × MAXHOLD）続くまで、同経路は使用も広告もされなくなる。REUSE よりも小さな値は指定できない。デフォルトは 2000。

REUSE　再使用（抑制解除）しきい値。いったん抑制状態となった経路は、ペナルティー値が本しきい値を下回るか、安定状態が最大抑制時間（HALFLIFE × MAXHOLD）続くまでは使用も広告もされない。ペナルティー値が本しきい値を下回ると、該当経路の抑制状態は解除され、Monitored（監視）状態に遷移する。SUPPRESSION よりも大きな値は指定できない。デフォルトは 750。

HALFLIFE　ペナルティー値の半減期（単位は分）。安定状態にある経路のペナルティー値は徐々に減少していくが、そのときの速度は「HALFLIFE（分）経過するごとに半分になる」レートである。デフォルトは 15 分。

MAXHOLD　最大抑制時間を求めるための係数。実際の最大抑制時間は HALFLIFE × MAXHOLD（分）で求められる。Suppressed（抑制）状態にある経路のペナルティー値が再使用しきい値（REUSE）を上回っていても、安定状態が最大抑制時間（HALFLIFE × MAXHOLD）続いた場合は抑制状態が解除される。デフォルトは 4。

関連コマンド

ADD BGP PEER（154 ページ）
ADD IP ROUTEMAP（195 ページ）
DESTROY BGP DAMPING PARAMETERSET（253 ページ）
DISABLE BGP DAMPING（258 ページ）
ENABLE BGP DAMPING（288 ページ）
PURGE BGP DAMPING（321 ページ）
RESET BGP DAMPING（325 ページ）
SET BGP DAMPING PARAMETERSET（339 ページ）
SET BGP PEER（343 ページ）
SET IP ROUTEMAP（379 ページ）
SHOW BGP DAMPING（409 ページ）
SHOW BGP DAMPING ROUTES（411 ページ）

CREATE IP POOL

カテゴリー：IP / IP アドレスプール

CREATE IP POOL=*pool-name* IP=*ipadd* [-*ipadd*]

pool-name: IP プール名（1〜15 文字）
ipadd: IP アドレス

解説

IP アドレスプールを作成する。
IP アドレスプールは、接続してきた PPP ユーザーに IP アドレスを動的割り当てするために使用する。

パラメーター

POOL　IP プール名
IP　IP アドレス。ハイフンにより範囲指定が可能。他のプールとアドレス範囲がオーバーラップしないように注意。

例

■IP アドレスプール「addr」（プール範囲 192.168.10.230〜192.168.10.239）を作成する。

```
CREATE IP POOL=addr IP=192.168.10.230-192.168.10.239)
```

関連コマンド

CREATE PPP TEMPLATE（「PPP」の 22 ページ）
DESTROY IP POOL（254 ページ）
SHOW IP POOL（466 ページ）

DELETE BGP AGGREGATE

カテゴリー：IP / 経路制御（BGP-4）

DELETE BGP AGGREGATE=*prefix* [MASK=*ipadd*]

prefix: プレフィックス（IP アドレス/プレフィックス長）
ipadd: IP アドレスまたはネットマスク

解説

集約経路エントリーを削除する。

パラメーター

AGGREGATE　集約した経路のプレフィックス。ネットワークアドレスとプレフィックス長で指定する。プレフィックス長は MASK パラメーターで指定することも可能。

MASK　AGGREGATE で指定したプレフィックスの有効長。

関連コマンド

ADD BGP AGGREGATE（149 ページ）
SET BGP AGGREGATE（336 ページ）
SHOW BGP AGGREGATE（401 ページ）
SHOW BGP ROUTE（425 ページ）

DELETE BGP CONFEDERATIONPEER

カテゴリー：IP / 経路制御（BGP-4）

DELETE BGP CONFEDERATIONPEER=*1..65534*

解説

指定したサブ AS をコンフェデレーションから除外する。

パラメーター

CONFEDERATIONPEER　現在自分と同じ AS コンフェデレーションに所属しているサブ AS の番号。

関連コマンド

ADD BGP CONFEDERATIONPEER（151 ページ）
SET BGP（335 ページ）
SET IP AUTONOMOUS（355 ページ）
SHOW BGP CONFEDERATION（405 ページ）

DELETE BGP IMPORT

カテゴリー：IP / 経路制御（BGP-4）

DELETE BGP IMPORT={**OSPF**|**RIP**|**STATIC**|**INTERFACE**}

解説

BGP 経路表へのインポート対象から、指定したソース（インターフェース経路、静的経路、RIP、OSPF）を削除する。

パラメーター

IMPORT　経路情報のソース

関連コマンド

ADD BGP IMPORT（152 ページ）
ADD IP ROUTEMAP（195 ページ）
SET BGP IMPORT（341 ページ）
SHOW BGP IMPORT（413 ページ）

DELETE BGP NETWORK

カテゴリー：IP / 経路制御（BGP-4）

DELETE BGP NETWORK=*prefix* [MASK=*ipadd*]

prefix: プレフィックス（IP アドレス/プレフィックス長）
ipadd: IP アドレスまたはネットマスク

解説

BGP で配布するネットワークプレフィックスを削除する。
本コマンドを実行すると、BGP 経路表から該当プレフィックス（登録されている場合）が削除され、すべての BGP ピアに対し、該当プレフィックスの取り消し（Withdraw）が通知される。

パラメーター

NETWORK　プレフィックス。ネットワークアドレスとプレフィックス長で指定する。プレフィックス長は MASK パラメーターで指定することも可能。
MASK　NETWORK で指定したネットワークアドレスに対するプレフィックスの有効長。

関連コマンド

ADD BGP NETWORK（153 ページ）
SHOW BGP NETWORK（417 ページ）
SHOW BGP ROUTE（425 ページ）

DELETE BGP PEER

カテゴリー：IP / 経路制御（BGP-4）

DELETE BGP PEER=*ipadd*

ipadd: IP アドレス

解説

BGP ピアを削除する。該当ピアは無効状態（DISABLE BGP PEER コマンド）でなくてはならない。

パラメーター

PEER　BGP ピアの IP アドレス。

DELETE BGP PEERTEMPLATE

カテゴリー：IP / 経路制御（BGP-4）

```
DELETE BGP PEERTEMPLATE=1..30
```

解説

BGP ピアテンプレートを削除する。該当テンプレートを使用していたピアとの通信パラメーターは、テンプレートの設定が引き継がれた状態となる。

パラメーター

PEERTEMPLATE　BGP ピアテンプレート番号。

関連コマンド

ADD BGP PEER（154 ページ）
ADD BGP PEERTEMPLATE（158 ページ）
DELETE BGP PEER（222 ページ）
DISABLE BGP PEER（261 ページ）
ENABLE BGP PEER（291 ページ）
RESET BGP PEER（326 ページ）
SET BGP PEER（343 ページ）
SET BGP PEERTEMPLATE（346 ページ）
SHOW BGP PEER（418 ページ）
SHOW BGP PEERTEMPLATE（422 ページ）

DELETE BOOTP RELAY

カテゴリー：IP / DHCP/BOOTP リレー

DELETE BOOTP RELAY=*ipadd*

ipadd: IP アドレス

解説

DHCP/BOOTP リクエストの転送先を削除する。

パラメーター

RELAY　DHCP/BOOTP サーバーの IP アドレス

関連コマンド

ADD BOOTP RELAY（161 ページ）
DISABLE BOOTP RELAY（262 ページ）
ENABLE BOOTP RELAY（292 ページ）
PURGE BOOTP RELAY（322 ページ）
SET BOOTP MAXHOPS（349 ページ）
SHOW BOOTP RELAY（427 ページ）

DELETE IP ARP

カテゴリー：IP / ARP

DELETE IP ARP=*ipadd*

ipadd: IP アドレス

解説

指定した IP アドレスを持つホストのエントリーを ARP キャッシュから削除する。
エントリーは、スタティックに登録したものでも、ダイナミックに登録されたものでもよい。

パラメーター

ARP　削除するホストの IP アドレスを指定する。

例

■ARP キャッシュから、IP アドレス 192.168.100.100 のホストエントリーを削除する。

```
DELETE IP ARP=192.168.100.100
```

関連コマンド

ADD IP ARP（162 ページ）
SHOW IP ARP（432 ページ）

DELETE IP ASPATHLIST

カテゴリー：IP / 経路制御（BGP-4）

DELETE IP ASPATHLIST=*1..99* [ENTRY=*1..4294967295*]

解説

AS パスフィルターからエントリーを削除する。

パラメーター

ASPATHLIST　AS パスフィルターの番号
ENTRY　フィルター内のエントリー番号。省略時はすべてのエントリーが対象となる。

例

■AS パスフィルター「1」からエントリー「3」を削除する。

```
DELETE IP ASPATHLIST=1 ENTRY=3
```

■AS パスフィルター「2」の全エントリーを削除する。

```
DELETE IP ASPATHLIST=2
```

関連コマンド

ADD IP ASPATHLIST（163 ページ）
SHOW IP ASPATHLIST（433 ページ）

DELETE IP COMMUNITYLIST

カテゴリー：IP / 経路制御（BGP-4）

DELETE IP COMMUNITYLIST=*1..99* [ENTRY=*1..4294967295*]

解説

コミュニティーフィルターからエントリーを削除する。

パラメーター

COMMUNITYLIST　コミュニティーフィルター番号
ENTRY　フィルター内のエントリー番号。省略時はすべてのエントリーが対象となる。

例

■ コミュニティーフィルター「1」からエントリー「3」を削除する。

```
DELETE IP COMMUNITYLIST=1 ENTRY=3
```

■ コミュニティーフィルター「2」の全エントリーを削除する。

```
DELETE IP COMMUNITYLIST=2
```

関連コマンド

ADD IP COMMUNITYLIST（165 ページ）
SHOW IP COMMUNITYLIST（436 ページ）

DELETE IP DNS

カテゴリー：IP / 名前解決

DELETE IP DNS [DOMAIN={ANY|*domain-name*}]

domain-name: ドメイン名

解説

DNS サーバーリストから指定したドメインの DNS サーバー情報を削除する。

パラメーター

DOMAIN DNS サーバーの担当ドメイン名。省略時および ANY 指定時はデフォルトサーバーを指定したことになる。

例

■ringo.fruit.xxx ドメイン用の DNS サーバー情報を削除する。

```
DELETE IP DNS DOMAIN=ringo.fruit.xxx
```

■デフォルトの DNS サーバー情報を削除する。

```
DELETE IP DNS
```

備考・注意事項

ドメイン指定の DNS サーバーが登録されているときは、デフォルト DNS サーバーを削除することはできない。

関連コマンド

ADD IP DNS（167 ページ）
DISABLE IP DNSRELAY（266 ページ）
ENABLE IP DNSRELAY（297 ページ）
SET IP DNS（356 ページ）
SET IP DNS CACHE（358 ページ）
SHOW IP DNS（445 ページ）
SHOW IP DNS CACHE（447 ページ）

TELNET（「運用・管理」の 380 ページ）

DELETE IP FILTER

カテゴリー：IP / IP フィルター

DELETE IP FILTER=*filter-id* ENTRY={*entry-id*|ALL}

filter-id: フィルター番号（0〜399）
entry-id: エントリー番号（1〜3071）

解説

IP フィルターから指定したエントリー（ルール）を削除する。

パラメーター

FILTER　フィルター番号

ENTRY　エントリー番号。この番号は可変なので、必ず SHOW IP FILTER コマンドで確認してから指定すること（Ent.フィールド）。ALL を指定した場合は、該当するフィルターの全エントリーが削除される。

例

■トラフィックフィルター「0」からエントリー「2」を削除する。

```
DELETE IP FILTER=0 ENTRY=2
```

■ポリシーフィルター「100」の全エントリーを削除する。

```
DELETE IP FILTER=100 ENTRY=ALL
```

備考・注意事項

エントリーを削除しても、他のエントリーの番号は変わらない。

関連コマンド

ADD IP FILTER（169 ページ）
SET IP FILTER（360 ページ）
SHOW IP FILTER（449 ページ）

DELETE IP HELPER

カテゴリー：IP / UDP ブロードキャストヘルパー

DELETE IP HELPER DESTINATION=*ipadd* INTERFACE=*interface* PORT={*port*|
***port-name*}**

ipadd: IP アドレス
interface: IP インターフェース名（eth0、ppp0 など）
port: UDP ポート番号（1〜65535）
port-name: サービス名

解説

UDP ブロードキャストパケットの転送先登録を削除する。

パラメーター

DESTINATION　UDP ブロードキャストの転送先 IP アドレス
INTERFACE　UDP ブロードキャストを監視する IP インターフェース
PORT　UDP ポート番号

関連コマンド

ADD IP HELPER（176 ページ）
DISABLE IP HELPER（270 ページ）
ENABLE IP HELPER（301 ページ）
SHOW IP HELPER（453 ページ）

DELETE IP HOST

カテゴリー：IP / 名前解決

DELETE IP HOST=*hostname*

hostname: ホスト名

解説

IP ホストテーブルから登録済みホスト名を削除する。

パラメーター

HOST　ホスト名

例

■ホストテーブルからホスト名「bulbul」を削除する。

```
DELETE IP HOST=bulbul
```

関連コマンド

ADD IP DNS（167 ページ）
ADD IP HOST（178 ページ）
DELETE IP DNS（228 ページ）
DISABLE IP DNSRELAY（266 ページ）
ENABLE IP DNSRELAY（297 ページ）
FINGER
PING（319 ページ）
SET IP DNS（356 ページ）
SET IP DNS CACHE（358 ページ）
SET IP HOST（363 ページ）
SHOW IP DNS（445 ページ）
SHOW IP DNS CACHE（447 ページ）
SHOW IP HOST（455 ページ）
TELNET（「運用・管理」の 380 ページ）

DELETE IP INTERFACE

カテゴリー：IP / IP インターフェース

DELETE IP INTERFACE=*interface*

interface: IP インターフェース名（eth0、ppp0 など）

解説

IP インターフェースを削除する。

パラメーター

INTERFACE　IP インターフェース名

関連コマンド

ADD IP INTERFACE（179 ページ）
DISABLE IP INTERFACE（272 ページ）
ENABLE IP INTERFACE（303 ページ）
RESET IP INTERFACE（329 ページ）
SET IP INTERFACE（364 ページ）
SHOW IP INTERFACE（458 ページ）

DELETE IP LOCAL

カテゴリー：IP / IP インターフェース

DELETE IP LOCAL=*1..15*

解説

ローカル IP インターフェース（ループバックインターフェース）を削除する。

パラメーター

LOCAL　ローカル IP インターフェース番号

備考・注意事項

ローカル IP インターフェースは、BGP-4 のみに対して使用可能。

関連コマンド

SET IP LOCAL（367 ページ）

DELETE IP NAT

カテゴリー：IP / レンジ NAT

DELETE IP NAT IP=*ipadd* MASK=*ipadd* GBLINTERFACE=*interface* [GBLMASK=*ipadd*]
[GBLPORT={*port*|*port-name*}] [PORT={*port*|*port-name*}] [PROTOCOL={*protocol*|
ALL|GRE|ICMP|OSPF|SA|TCP|UDP}]

DELETE IP NAT IP=*ipadd* GBLIP=*ipadd* [MASK=*ipadd*] [GBLMASK=*ipadd*]
[GBLPORT={*port*|*port-name*}] [PORT={*port*|*port-name*}] [PROTOCOL={*protocol*|
ALL|GRE|ICMP|OSPF|SA|TCP|UDP}]

ipadd: IP アドレスまたはネットマスク
interface: IP インターフェース名（eth0、ppp0 など）
port: TCP/UDP ポート番号（0～65535）
port-name: サービス名
protocol: IP プロトコル番号（0～255）

解説

IP NAT（レンジ NAT）の変換ルールを削除する。
最初の構文はインターフェース NAT（インターフェース指定のダイナミック ENAT）設定を解除するときのもの。2 番目の構文はその他の NAT 設定を解除するためのもの。

パラメーター

IP　プライベート IP アドレス。MASK と組み合わせて範囲指定が可能。
MASK　プライベート IP アドレスの範囲を指定するためのマスク値
GBLINTERFACE　グローバル IP アドレスを持つインターフェース
GBLMASK　グローバル IP アドレスの範囲を指定するためのマスク値
GBLPORT　スタティック ENAT におけるグローバル側ポート番号またはサービス名
PORT　スタティック ENAT におけるプライベートホストのポート番号またはサービス名
PROTOCOL　スタティック ENAT における IP プロトコル指定。TCP か UDP を指定した場合は、PORT の指定も必要。
GBLIP　グローバル IP アドレス。GBLMASK と組み合わせて範囲指定が可能

関連コマンド

ADD IP NAT（184 ページ）
DISABLE IP NAT（273 ページ）
ENABLE IP NAT（305 ページ）
SHOW IP NAT（461 ページ）

DELETE IP RIP

カテゴリー：IP / 経路制御（RIP）

DELETE IP RIP INTERFACE=*interface* [IP=*ipadd*]

interface: IP インターフェース名（eth0、ppp0 など）
ipadd: IP アドレス

解説

指定した IP インターフェースで RIP を無効にする。

パラメーター

INTERFACE　IP インターフェース
IP　隣接 RIP ルーターの IP アドレス。本パラメーターを指定した場合は、指定したルーターとの通信だけが対象となる。

例

■eth0 上での RIP パケットの送受信を停止する。

```
DELETE IP RIP INT=eth0
```

■vlan1 上の RIP ルーター 192.168.20.254 との情報交換を停止する。

```
DELETE IP RIP INT=vlan1 IP=192.168.20.254
```

関連コマンド

ADD IP RIP（187 ページ）
SET IP RIP（369 ページ）
SHOW IP（429 ページ）
SHOW IP RIP（468 ページ）

DELETE IP ROUTE

カテゴリー：IP / 経路制御（スタティック）

DELETE IP ROUTE=*ipadd* MASK=*ipadd* INTERFACE=*interface* NEXTHOP=*ipadd*

ipadd: IP アドレスまたはネットマスク
interface: IP インターフェース名（eth0、ppp0 など）

解説

スタティック経路を削除する。ダイナミック経路は削除できない。

パラメーター

ROUTE　宛先ネットワークの IP アドレス
MASK　宛先ネットワークのネットマスク
INTERFACE　本経路宛てパケットを送出する IP インターフェース名
NEXTHOP　ネクストホップルーターの IP アドレス

例

■デフォルト経路を削除する。

```
DELETE IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=ppp0 NEXTHOP=192.168.100.2
```

関連コマンド

ADD IP ROUTE（189 ページ）
SET IP ROUTE（372 ページ）
SHOW IP ROUTE（473 ページ）

DELETE IP ROUTE FILTER

カテゴリー：IP / 経路制御フィルター

DELETE IP ROUTE FILTER=*entry-id*

entry-id: エントリー番号（1〜100）

解説

IP ルートフィルターリストから指定したフィルターエントリーを削除する。
フィルターエントリーの番号は可変なので、必ず SHOW IP ROUTE FILTER コマンドで確認してから指定すること。エントリーを削除すると、後続のエントリー番号が 1 つずつ前にずれるので注意。

パラメーター

FILTER　フィルターエントリー番号。この番号は可変なので、必ず SHOW IP ROUTE FILTER コマンドで確認してから指定すること（Ent.フィールド）。

関連コマンド

ADD IP ROUTE FILTER（191 ページ）
SET IP ROUTE FILTER（374 ページ）
SHOW IP ROUTE FILTER（476 ページ）

DELETE IP ROUTE TEMPLATE

カテゴリー：IP / 経路制御

DELETE IP ROUTE TEMPLATE=*template*

template: ルートテンプレート名（1〜31 文字。大文字小文字を区別しない）

解説

IP ルートテンプレートを削除する。

パラメーター

TEMPLATE　テンプレート名

関連コマンド

ADD IP ROUTE TEMPLATE（193 ページ）
CREATE IPSEC POLICY（「IPsec」の 39 ページ）
SET IP ROUTE TEMPLATE（378 ページ）
SHOW IP ROUTE TEMPLATE（479 ページ）

DELETE IP ROUTEMAP

カテゴリー：IP / 経路制御（BGP-4）

DELETE IP ROUTEMAP=*routemap* [ENTRY=*1..4294967295*]

DELETE IP ROUTEMAP=*routemap* ENTRY=*1..4294967295* MATCH={**ASPATH**|**COMMUNITY**}

DELETE IP ROUTEMAP=*routemap* ENTRY=*1..4294967295* SET={**ASPATH**|**COMMUNITY**|
LOCALPREF|**MED**|**ORIGIN**}

routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）

解説

ルートマップからエントリーを削除する。または、ルートマップのエントリーから MATCH 節あるいは SET 節を削除する。
使用中のルートマップは削除できない。

パラメーター

ROUTEMAP　ルートマップ名
ENTRY　ルートマップ内のエントリー番号。省略時はすべてのエントリーが削除対象となる。MATCH 節、SET 節を削除するときは、必ずエントリー番号を指定しなくてはならない。
MATCH　指定したエントリーから削除する MATCH 節の種類
SET　指定したエントリーから削除する SET 節の種類

例

■ルートマップ「set_locpref」のエントリー「2」から LOCAL_PREF 属性をセットする SET 節を削除する。

```
DELETE IP ROUTEMAP=set_locapref ENTRY=2 SET=LOCALPREF
```

関連コマンド

ADD IP ROUTEMAP（195 ページ）
SET IP ROUTEMAP（379 ページ）
SHOW IP ROUTEMAP（481 ページ）

DELETE IP TRUSTED

カテゴリー：IP / 経路制御フィルター

DELETE IP TRUSTED=*ipadd*

ipadd: IP アドレス

解説

RIP の Trusted Router リストから IP アドレスを削除する。

パラメーター

TRUSTED　Trusted Router の IP アドレス

関連コマンド

ADD IP FILTER（169 ページ）
ADD IP TRUSTED（198 ページ）
DELETE IP FILTER（230 ページ）
SET IP FILTER（360 ページ）
SHOW IP FILTER（449 ページ）
SHOW IP TRUSTED（483 ページ）

DELETE OSPF AREA

カテゴリー：IP / 経路制御（OSPF）

DELETE OSPF AREA={**BACKBONE**|***area-number***}

area-number: OSPF エリア ID（a.b.c.d の形式）

解説

OSPF エリアを削除する。

パラメーター

AREA　エリア ID。バックボーンエリア（0.0.0.0）はキーワード「BACKBONE」で指定することもできる

関連コマンド

ADD OSPF AREA（199 ページ）
ADD OSPF RANGE（208 ページ）
DELETE OSPF RANGE（247 ページ）
SET OSPF AREA（384 ページ）
SET OSPF RANGE（390 ページ）
SHOW OSPF AREA（487 ページ）
SHOW OSPF RANGE（505 ページ）

DELETE OSPF HOST

カテゴリー：IP / 経路制御（OSPF）

DELETE OSPF HOST=*ipadd*

ipadd: IP アドレス

解説

OSPF ルーティングテーブルからホスト経路を削除する。

パラメーター

HOST　ホストまたは Point-To-Point ネットワークの IP アドレス

関連コマンド

ADD OSPF HOST（201 ページ）
SET OSPF HOST（385 ページ）
SHOW OSPF HOST（491 ページ）

DELETE OSPF INTERFACE

カテゴリー：IP / 経路制御（OSPF）

DELETE OSPF INTERFACE=*interface*

interface: IP インターフェース名（eth0、ppp0 など）または仮想インターフェース名（VIRTn）

解説

OSPF インターフェースを削除する。
該当インターフェース上に隣接ルーターがスタティック登録されている場合（ADD OSPF NEIGHBOUR コマンド）、OSPF インターフェースを削除することはできない。先に隣接ルーターを削除してから、インターフェースを削除する。

パラメーター

INTERFACE　IP インターフェース名、または、仮想インターフェース名（VIRTn）。

関連コマンド

ADD OSPF INTERFACE（202 ページ）
DISABLE OSPF INTERFACE（281 ページ）
ENABLE OSPF INTERFACE（313 ページ）
RESET OSPF INTERFACE（332 ページ）
SET OSPF INTERFACE（386 ページ）
SHOW OSPF INTERFACE（493 ページ）

DELETE OSPF MD5KEY

カテゴリー：IP / 経路制御（OSPF）

DELETE OSPF MD5KEY ID=*1..255* INTERFACE=*interface* [FORCE]

interface: IP インターフェース名（eth0、ppp0 など）または仮想インターフェース名（VIRTn）

解説

指定した OSPF インターフェースで使用する MD5 ダイジェスト認証用の鍵を削除する。
現在使用中の鍵を削除しようとするとエラーになる（使用中の鍵は、SHOW OSPF MD5KEY コマンドの Active 欄に Yes と表示される）。このようなときは、ADD OSPF MD5KEY コマンドで新しい鍵を追加してから、本コマンドを実行すること。

パラメーター

ID　鍵番号（Key ID）。
INTERFACE　OSPF インターフェース名。
FORCE　使用中の鍵を強制的に削除するときに指定する。

関連コマンド

ADD OSPF AREA（199 ページ）
ADD OSPF INTERFACE（202 ページ）
ADD OSPF MD5KEY（205 ページ）
SET OSPF AREA（384 ページ）
SET OSPF INTERFACE（386 ページ）
SHOW OSPF AREA（487 ページ）
SHOW OSPF INTERFACE（493 ページ）
SHOW OSPF MD5KEY（501 ページ）

DELETE OSPF NEIGHBOUR

カテゴリー：IP / 経路制御（OSPF）

DELETE OSPF NEIGHBOUR=*ipadd*

ipadd: IP アドレス

解説

スタティック登録した OSPF 隣接ルーターの設定を削除する。

パラメーター

NEIGHBOUR　OSPF 隣接ルーターの IP アドレス。

関連コマンド

ADD OSPF NEIGHBOUR（207 ページ）
SET OSPF NEIGHBOUR（389 ページ）
SHOW OSPF NEIGHBOUR（503 ページ）

DELETE OSPF RANGE

カテゴリー：IP / 経路制御（OSPF）

DELETE OSPF RANGE=*ipadd*

ipadd: IP アドレス

解説

OSPF エリアを構成するネットワークの範囲を削除する。

パラメーター

RANGE　ネットワークアドレス

例

■エリア 1.1.1.1 からネットワーク 192.168.10.0 を削除する。

```
DELETE OSPF RANGE=192.168.10.0
```

関連コマンド

ADD OSPF AREA（199 ページ）
ADD OSPF RANGE（208 ページ）
SET OSPF RANGE（390 ページ）
SHOW OSPF RANGE（505 ページ）

DELETE OSPF REDISTRIBUTE

カテゴリー：IP / 経路制御（OSPF）

DELETE OSPF REDISTRIBUTE PROTOCOL={**STATIC**}

解説

スタティック経路を AS 外部 LSA で AS 内に通知するときのメトリックとメトリックタイプの設定値（ADD OSPF REDISTRIBUTE コマンドで設定したもの）を削除する。
本コマンドは AS 境界ルーター（ASBR）でのみ意味を持つ。

パラメーター

PROTOCOL　AS 外部経路の起源。現在指定できる値は STATIC（スタティック経路）のみ。

関連コマンド

ADD OSPF REDISTRIBUTE（210 ページ）
SET OSPF REDISTRIBUTE（391 ページ）
SHOW OSPF REDISTRIBUTE（507 ページ）

DELETE OSPF STUB

カテゴリー：IP / 経路制御（OSPF）

DELETE OSPF STUB=*ipadd* MASK=*ipadd*

ipadd: IP アドレスまたはネットマスク

解説

OSPF ルーティングテーブルから、OSPF を使用していないネットワーク（スタブネットワーク）への経路を削除する。

パラメーター

STUB　スタブネットワークのネットワークアドレス
MASK　STUB に対するネットマスク

関連コマンド

ADD OSPF STUB（211 ページ）
DELETE OSPF HOST（243 ページ）
DELETE OSPF INTERFACE（244 ページ）
SET OSPF STUB（392 ページ）
SHOW OSPF STUB（510 ページ）

DELETE OSPF SUMMARYADDRESS

カテゴリー：IP / 経路制御（OSPF）

DELETE OSPF SUMMARYADDRESS=*ipadd*

ipadd: IP アドレス

解説

AS 外部経路の集約設定（集約経路エントリー）を削除する。
集約されていた AS 外部経路は、再び個別通知されるようになる。
本コマンドは AS 境界ルーター（ASBR）でのみ意味を持つ。

パラメーター

SUMMARYADDRESS　集約後のネットワークアドレス。ADD OSPF SUMMARYADDRESS コマンドで指定したもの。

関連コマンド

ADD OSPF SUMMARYADDRESS（212 ページ）
SET OSPF（381 ページ）
SET OSPF SUMMARYADDRESS（393 ページ）
SHOW OSPF SUMMARYADDRESS（512 ページ）

DELETE PING POLL

カテゴリー：IP / Ping ポーリング

DELETE PING POLL=*poll-id*

poll-id: Ping ポーリング ID（1〜100）

解説

Ping ポーリングの監視対象機器を削除する。

パラメーター

POLL　Ping ポーリング ID

関連コマンド

ADD PING POLL（213 ページ）
DISABLE PING POLL（283 ページ）
ENABLE PING POLL（316 ページ）
RESET PING POLL（334 ページ）
SET PING POLL（396 ページ）
SHOW PING POLL（515 ページ）

DELETE TCP

カテゴリー：IP / 一般コマンド

DELETE TCP=*tcb*

tcb: TCP コネクション番号

解説

ルーター自身と任意の IP ノードとの間のアクティブな（Established）TCP コネクションを強制終了させる。

パラメーター

TCP TCP コネクション（Transmission Control Block）番号。SHOW TCP コマンドで表示される Connection Table の Index 値を指定する。

関連コマンド

SHOW TCP（519 ページ）

DESTROY BGP DAMPING PARAMETERSET

カテゴリー：IP / 経路制御（BGP-4）

DESTROY BGP DAMPING PARAMETERSET={**ALL**|***1..100***}

解説

BGP-4 ルートフラップダンピング用のパラメーターセットを削除する。
有効化されているパラメーターセットは削除できない。また、デフォルトのパラメーターセット（内部的な番号は 0）も削除できない。

パラメーター

PARAMETERSET　パラメーターセット番号。ALL を指定した場合は、すべてのパラメーターセットが対象となる。

関連コマンド

ADD BGP PEER（154 ページ）
CREATE BGP DAMPING PARAMETERSET（215 ページ）
DISABLE BGP DAMPING（258 ページ）
ENABLE BGP DAMPING（288 ページ）
PURGE BGP DAMPING（321 ページ）
RESET BGP DAMPING（325 ページ）
SET BGP DAMPING PARAMETERSET（339 ページ）
SHOW BGP DAMPING（409 ページ）
SHOW BGP DAMPING ROUTES（411 ページ）

DESTROY IP POOL

カテゴリー：IP / IP アドレスプール

DESTROY IP POOL=*pool-name*

pool-name: IP プール名（1〜15 文字）

解説

IP アドレスプールを削除する。

パラメーター

POOL　IP プール名

関連コマンド

CREATE IP POOL（217 ページ）
SHOW IP POOL（466 ページ）

DISABLE BGP AUTOSOFTUPDATE

カテゴリー：IP / 経路制御（BGP-4）

DISABLE BGP AUTOSOFTUPDATE

解説

BGP-4 の自動ソフトリセットを無効にする。デフォルトは無効。

関連コマンド

ENABLE BGP AUTOSOFTUPDATE（285 ページ）
RESET BGP PEER（326 ページ）
SET BGP PEER（343 ページ）
SHOW BGP PEER（418 ページ）

DISABLE BGP AUTOSUMMARY

カテゴリー：IP / 経路制御（BGP-4）

DISABLE BGP AUTOSUMMARY

解説

経路情報の自動集約機能を無効にする。デフォルトは無効。

関連コマンド

ENABLE BGP AUTOSUMMARY（286 ページ）

DISABLE BGP BACKOFF

カテゴリー：IP / 経路制御（BGP-4）

DISABLE BGP BACKOFF

解説

空きメモリー不足時の BGP-4 のバックオフ（一時停止）動作を無効にする。デフォルトは無効（最初にピアが追加されたとき自動で有効になる）。

関連コマンド

ENABLE BGP BACKOFF（287 ページ）
SET BGP BACKOFF（337 ページ）
SHOW BGP BACKOFF（402 ページ）

DISABLE BGP DAMPING

カテゴリー：IP / 経路制御（BGP-4）

DISABLE BGP DAMPING [PARAMETERSET={ALL|*0..100*}]

解説

BGP-4 ルートフラップダンピングを無効にする。デフォルトは無効。
本コマンドでは、特定のパラメーターセットだけを無効化することもできる。この場合でも、すべてのパラメーターセットを無効化すると、ルートフラップダンピング機能全体も自動的に無効化される。

パラメーター

PARAMETERSET パラメーターセット番号。パラメーターセット番号を指定した場合は、該当パラメーターセットだけが対象となる。0 はデフォルトのパラメーターセット。ALL を指定した場合、および、番号を省略した場合は、すべてのパラメーターセットが対象となる。

関連コマンド

ADD BGP PEER（154 ページ）
CREATE BGP DAMPING PARAMETERSET（215 ページ）
DESTROY BGP DAMPING PARAMETERSET（253 ページ）
ENABLE BGP DAMPING（288 ページ）
PURGE BGP DAMPING（321 ページ）
RESET BGP DAMPING（325 ページ）
SET BGP DAMPING PARAMETERSET（339 ページ）
SHOW BGP DAMPING（409 ページ）
SHOW BGP DAMPING ROUTES（411 ページ）

DISABLE BGP DEBUG

カテゴリー：IP / 経路制御（BGP-4）

DISABLE BGP DEBUG[={MSG|STATE|UPDATE|ALL}[,...]] [PEER=*ipadd*]

ipadd: IP アドレス

解説

BGP-4 のデバッグオプションを無効にする。

パラメーター

DEBUG　デバッグオプション。カンマ区切りで複数指定が可能。省略時は ALL（すべて）の意味になる。
PEER　デバッグの対象となる BGP ピアの IP アドレス。省略時はすべての BGP ピアが対象となる。

関連コマンド

ENABLE BGP DEBUG（289 ページ）

DISABLE BGP DEFAULTORIGINATE

カテゴリー：IP / 経路制御（BGP-4）

DISABLE BGP DEFAULTORIGINATE

解説

BGP の経路表にデフォルト経路（0.0.0.0/0）を取り込まないようにする。デフォルトは取り込まない。
デフォルト経路を取り込まない設定の場合、ADD BGP IMPORT コマンドや ADD BGP NETWORK コマンドで 0.0.0.0/0 を対象にしていても、BGP の経路表には取り込まれない。

関連コマンド

ENABLE BGP DEFAULTORIGINATE（290 ページ）

DISABLE BGP PEER

カテゴリー：IP / 経路制御（BGP-4）

DISABLE BGP PEER={**ALL**|***ipadd***}

ipadd: IP アドレス

解説

指定した BGP ピアとのセッションを停止（IDLE）状態にする。

パラメーター

PEER　BGP ピアの IP アドレス

関連コマンド

ADD BGP PEER（154 ページ）
ENABLE BGP PEER（291 ページ）
SHOW BGP PEER（418 ページ）

DISABLE BOOTP RELAY

カテゴリー：IP / DHCP/BOOTP リレー

DISABLE BOOTP RELAY

解説

DHCP/BOOTP リレー機能を無効にする。デフォルトは無効。

関連コマンド

ADD BOOTP RELAY（161 ページ）
DELETE BOOTP RELAY（224 ページ）
ENABLE BOOTP RELAY（292 ページ）
PURGE BOOTP RELAY（322 ページ）
SET BOOTP MAXHOPS（349 ページ）
SHOW BOOTP RELAY（427 ページ）

DISABLE IP

カテゴリー：IP / 一般コマンド

DISABLE IP

解説

IP モジュールを無効にする。デフォルトは無効。

関連コマンド

DISABLE IP FORWARDING（269 ページ）
DISABLE IP SRCROUTE（278 ページ）
ENABLE IP（293 ページ）
ENABLE IP FORWARDING（300 ページ）
ENABLE IP SRCROUTE（310 ページ）
SHOW IP（429 ページ）

DISABLE IP ARP LOG

カテゴリー：IP / ARP

DISABLE IP ARP LOG

解説

ARP キャッシュログを無効にする。デフォルトは無効。

関連コマンド

ENABLE IP ARP LOG（294 ページ）
SHOW IP（429 ページ）

DISABLE IP DEBUG

カテゴリー：IP / 一般コマンド

DISABLE IP DEBUG[=PACKET]

解説

IP デバッグキューへのエラーパケット保存機能、または、IP パケットのヘッダー情報表示機能を無効にする。デフォルトは無効。

パラメーター

DEBUG　PACKET を指定した場合、送受信した IP データグラムのヘッダー情報表示機能を停止する。何も指定しなかった場合は、エラーパケットの保存機能を無効にする。

関連コマンド

ENABLE IP DEBUG（296 ページ）
SHOW IP（429 ページ）
SHOW IP DEBUG（444 ページ）

DISABLE IP DNSRELAY

カテゴリー：IP / DNS リレー

DISABLE IP DNSRELAY

解説

DNS リレー機能を無効にする。デフォルトは無効。

関連コマンド

ADD IP DNS（167 ページ）
DELETE IP DNS（228 ページ）
ENABLE IP DNSRELAY（297 ページ）
SET IP DNS（356 ページ）
SET IP DNS CACHE（358 ページ）
SET IP DNSRELAY（359 ページ）
SHOW IP（429 ページ）
SHOW IP DNS（445 ページ）
SHOW IP DNS CACHE（447 ページ）

DISABLE IP ECHOREPLY

カテゴリー：IP / 一般コマンド

DISABLE IP ECHOREPLY

解説

ICMP エコー要求（PING）に対する応答を行わないようにする。デフォルトは行う。

関連コマンド

ENABLE IP ECHOREPLY（298 ページ）

DISABLE IP FOFILTER

カテゴリー：IP / セキュリティー

DISABLE IP FOFILTER

解説

IP フラグメントオフセットフィルターを無効にする。デフォルトは有効。
有効時は、フラグメントオフセットが 1 の IP パケットを破棄する。これは、Tiny Fragment 攻撃や Overlapping Fragment 攻撃（RFC1858）に対する防御措置。
有効時にフラグメントオフセットが 1 のパケットを受信すると、メッセージタイプ「IPFIL」、サブタイプ「FRAG」のログメッセージが記録される。

備考・注意事項

デフォルト設定（有効）のまま使用することが望ましい。

関連コマンド

ADD IP FILTER（169 ページ）
DELETE IP FILTER（230 ページ）
ENABLE IP FOFILTER（299 ページ）
SET IP FILTER（360 ページ）
SHOW IP FILTER（449 ページ）

DISABLE IP FORWARDING

カテゴリー：IP / 一般コマンド

DISABLE IP FORWARDING

解説

IP 転送機能（ルーティング）を無効にする。デフォルトは有効。

関連コマンド

DISABLE IP（263 ページ）
DISABLE IP SRCROUTE（278 ページ）
ENABLE IP（293 ページ）
ENABLE IP FORWARDING（300 ページ）
ENABLE IP SRCROUTE（310 ページ）
SHOW IP（429 ページ）

DISABLE IP HELPER

カテゴリー：IP / UDP ブロードキャストヘルパー

DISABLE IP HELPER

解説

UDP ブロードキャストパケットの転送機能を無効にする。デフォルトは無効。

関連コマンド

ADD IP HELPER（176 ページ）
DELETE IP HELPER（231 ページ）
ENABLE IP HELPER（301 ページ）
SHOW IP HELPER（453 ページ）

DISABLE IP ICMPREPLY

カテゴリー：IP / 一般コマンド

DISABLE IP ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]

解説

指定した ICMP メッセージを送信しないようにする。デフォルトではすべて送信する。

パラメーター

ICMPREPLY　送信しないメッセージタイプを指定する。指定できるのは、NETUNREACH（Network Unreachable）、HOSTUNREACH（Host Unreachable）、REDIRECT（Redirect）の 3 種類のみ。ALL を指定した場合は、前記の 3 種類すべてが対象となる。

関連コマンド

ENABLE IP ICMPREPLY（302 ページ）
SHOW IP ICMPREPLY（457 ページ）

DISABLE IP INTERFACE

カテゴリー：IP / IP インターフェース

DISABLE IP INTERFACE=*interface*

interface: IP インターフェース名（eth0、ppp0 など）

解説

IP インターフェースを一時的に無効にする。

パラメーター

INTERFACE　IP インターフェース

関連コマンド

ADD IP INTERFACE（179 ページ）
DELETE IP INTERFACE（233 ページ）
ENABLE IP INTERFACE（303 ページ）
RESET IP INTERFACE（329 ページ）
SET IP INTERFACE（364 ページ）
SHOW IP INTERFACE（458 ページ）

DISABLE IP NAT

カテゴリー：IP / レンジ NAT

DISABLE IP NAT

解説

IP NAT（レンジ NAT）モジュールを無効にする。デフォルトは無効。

関連コマンド

ADD IP NAT（184 ページ）
DELETE IP NAT（235 ページ）
ENABLE IP NAT（305 ページ）
SHOW IP NAT（461 ページ）

DISABLE IP NAT FRAGMENT

カテゴリー：IP / レンジ NAT

DISABLE IP NAT FRAGMENT={**UDP**}

解説

IP NAT（レンジ NAT）モジュールに対し、指定したプロトコルのフラグメント化パケットを透過しないよう指示する。

パラメーター

FRAGMENT　指定したプロトコルのフラグメント化パケットを透過しないよう設定する。デフォルトでは、再構成後の IP データサイズ（L4 パケットサイズ）が 1780 バイトを越えるパケットは IP NAT モジュールによって破棄される

関連コマンド

ADD IP NAT（184 ページ）
DELETE IP NAT（235 ページ）
ENABLE IP NAT（305 ページ）
ENABLE IP NAT FRAGMENT（306 ページ）
SHOW IP NAT（461 ページ）

DISABLE IP NAT LOG

カテゴリー：IP / レンジ NAT

DISABLE IP NAT LOG={**ALL**|**FAILS**|**INTCP**|**INUDP**|**OUTTCP**|**OUTUDP**}[,...]

解説

IP NAT（レンジ NAT）モジュールのログオプションを無効にする。

パラメーター

LOG ログに記録しない NAT イベントを指定する。カンマ区切りで複数指定可能。ALL（すべて）、FAILS（グローバル側で受信したがプライベート側サービスが未指定のため転送できなかったもの）、INTCP（グローバルからプライベートへの TCP セッション）、INUDP（グローバルからプライベートへの UDP フロー）、OUTTCP（プライベートからグローバルへの TCP セッション）、OUTUDP（プライベートからグローバルへの UDP フロー）

関連コマンド

ADD IP NAT（184 ページ）
DELETE IP NAT（235 ページ）
ENABLE IP NAT（305 ページ）
ENABLE IP NAT LOG（307 ページ）
SHOW IP NAT（461 ページ）

DISABLE IP REMOTEASSIGN

カテゴリー：IP / 一般コマンド

DISABLE IP REMOTEASSIGN

解説

IPCP（PPP のサブプロトコル）、または、DHCP による IP アドレスの動的設定機能を無効にする。デフォルトは無効。

関連コマンド

ENABLE IP REMOTEASSIGN（308 ページ）
SHOW IP（429 ページ）

DISABLE IP ROUTE

カテゴリー：IP / 経路制御（スタティック）

DISABLE IP ROUTE {**CACHE**|**COUNT**|**MULTIPATH**}

解説

IP ルートキャッシュ、ルートカウンター、等価コストマルチパスルーティングを無効にする。

パラメーター

CACHE　ルートキャッシュを無効にする。デフォルトは有効。
COUNT　ルートカウンターを無効にする。デフォルトは無効。
MULTIPATH　等価コストマルチパスルーティングを無効にする。デフォルトは有効。

関連コマンド

ENABLE IP ROUTE（309 ページ）
SHOW IP ROUTE（473 ページ）

DISABLE IP SRCROUTE

カテゴリー：IP / セキュリティー

DISABLE IP SRCROUTE

解説

始点経路制御（ソースルート）オプション付き IP パケットの転送を無効にする（ソースルートフィルターを有効にする）。デフォルトは無効（転送しない）。
無効設定時（ソースルートフィルター有効時）に始点経路制御オプション付きパケットを受信すると、メッセージタイプ「IPFIL」、サブタイプ「SRCRT」のログメッセージが記録される。

備考・注意事項

始点経路制御オプションは通常使われておらず、むしろ悪用される可能性があるため、デフォルト設定（無効）のまま使用することが望ましい。

関連コマンド

DISABLE IP（263 ページ）
ENABLE IP（293 ページ）
ENABLE IP FORWARDING（300 ページ）
ENABLE IP SRCROUTE（310 ページ）
SHOW IP（429 ページ）

DISABLE OSPF

カテゴリー：IP / 経路制御（OSPF）

DISABLE OSPF

解説

OSPF モジュールを無効にする。デフォルトは無効。

関連コマンド

ENABLE OSPF（311 ページ）
SHOW OSPF（485 ページ）

DISABLE OSPF DEBUG

カテゴリー：IP / 経路制御（OSPF）

DISABLE OSPF DEBUG={**ALL**|**IFSTATE**|**NBRSTATE**|**PACKET**|**STATE**}

解説

OSPF モジュールのデバッグ機能を無効にする。デフォルトは無効。

パラメーター

DEBUG　デバッグオプション。IFSTATE（自インターフェースの状態）、NBRSTATE（対向インターフェースの状態）、PACKET（OSPF パケットの送受信情報）、STATE（自インターフェースと対向インターフェースの状態）、ALL（すべて）から選択する。

関連コマンド

DISABLE OSPF LOG（282 ページ）
ENABLE OSPF DEBUG（312 ページ）
ENABLE OSPF LOG（314 ページ）
SHOW OSPF（485 ページ）

DISABLE OSPF INTERFACE

カテゴリー：IP / 経路制御（OSPF）

DISABLE OSPF INTERFACE=*interface*

interface: IP インターフェース名（eth0、ppp0 など）または仮想インターフェース名（VIRTn）

解説

OSPF インターフェースを一時的に無効にする。

パラメーター

INTERFACE　IP インターフェース名、または仮想インターフェース名（VIRTn）。

関連コマンド

ADD OSPF INTERFACE（202 ページ）
DELETE OSPF INTERFACE（244 ページ）
ENABLE OSPF INTERFACE（313 ページ）
RESET OSPF INTERFACE（332 ページ）
SET OSPF INTERFACE（386 ページ）
SHOW OSPF INTERFACE（493 ページ）

DISABLE OSPF LOG

カテゴリー：IP / 経路制御（OSPF）

DISABLE OSPF LOG

解説

OSPF イベントのログ記録を無効にする。デフォルトは無効。

関連コマンド

ENABLE OSPF LOG（314 ページ）
SHOW OSPF（485 ページ）

DISABLE PING POLL

カテゴリー：IP / Ping ポーリング

DISABLE PING POLL=*poll-id*

poll-id: Ping ポーリング ID（1〜100）

解説

Ping ポーリングを停止（無効）状態にする。

パラメーター

POLL　Ping ポーリング ID

関連コマンド

ENABLE PING POLL（316 ページ）
RESET PING POLL（334 ページ）
SET PING POLL（396 ページ）
SHOW PING POLL（515 ページ）

DISABLE PING POLL DEBUG

カテゴリー：IP / Ping ポーリング

DISABLE PING POLL=*poll-id* DEBUG

poll-id: Ping ポーリング ID（1〜100）

解説

Ping ポーリングのデバッグ表示を無効にする。デフォルトは無効。

パラメーター

POLL　Ping ポーリング ID

関連コマンド

ENABLE PING POLL DEBUG（317 ページ）
SHOW PING POLL（515 ページ）

ENABLE BGP AUTOSOFTUPDATE

カテゴリー：IP / 経路制御（BGP-4）

ENABLE BGP AUTOSOFTUPDATE

解説

BGP-4 の自動ソフトリセットを有効にする。デフォルトは無効。

関連コマンド

DISABLE BGP AUTOSOFTUPDATE（255 ページ）
RESET BGP PEER（326 ページ）
SET BGP PEER（343 ページ）
SHOW BGP PEER（418 ページ）

ENABLE BGP AUTOSUMMARY

カテゴリー：IP / 経路制御（BGP-4）

ENABLE BGP AUTOSUMMARY

解説

経路情報の自動集約機能を有効にする。デフォルトは無効。
自動集約機能が有効のときは、自ら生成もしくは取り込んだ複数の経路をクラスフルなネットワーク（クラス A、B、C ネットワーク）に集約した上で通知する。

関連コマンド

DISABLE BGP AUTOSUMMARY（256 ページ）

ENABLE BGP BACKOFF

カテゴリー：IP / 経路制御（BGP-4）

ENABLE BGP BACKOFF

解説

空きメモリー不足時の BGP-4 のバックオフ（一時停止）動作を有効にする。デフォルトは無効（最初にピアが追加されたとき自動で有効になる）。

関連コマンド

DISABLE BGP BACKOFF（257 ページ）
SET BGP BACKOFF（337 ページ）
SHOW BGP BACKOFF（402 ページ）

ENABLE BGP DAMPING

カテゴリー：IP / 経路制御（BGP-4）

ENABLE BGP DAMPING [PARAMETERSET={ALL|*0..100*}]

解説

BGP-4 ルートフラップダンピングを有効にする。デフォルトは無効。
本コマンドでは、特定のパラメーターセットだけを有効化することもできる。この場合、1 つでもパラメーターセットを有効化すると、ルートフラップダンピング機能全体も自動的に有効化される。

パラメーター

PARAMETERSET パラメーターセット番号。パラメーターセット番号を指定した場合は、該当パラメーターセットだけが対象となる。0 はデフォルトのパラメーターセット。ALL を指定した場合、および、番号を省略した場合は、すべてのパラメーターセットが対象となる。

関連コマンド

ADD BGP PEER（154 ページ）
CREATE BGP DAMPING PARAMETERSET（215 ページ）
DESTROY BGP DAMPING PARAMETERSET（253 ページ）
DISABLE BGP DAMPING（258 ページ）
PURGE BGP DAMPING（321 ページ）
RESET BGP DAMPING（325 ページ）
SET BGP DAMPING PARAMETERSET（339 ページ）
SHOW BGP DAMPING（409 ページ）
SHOW BGP DAMPING ROUTES（411 ページ）

ENABLE BGP DEBUG

カテゴリー：IP / 経路制御（BGP-4）

ENABLE BGP DEBUG={**MSG**|**STATE**|**UPDATE**|**ALL**}[,...] [PEER=*ipadd*]

ipadd: IP アドレス

解説

BGP-4 のデバッグオプションを有効にする。デフォルトはすべて無効。

パラメーター

DEBUG　デバッグオプション。カンマ区切りで複数指定が可能
PEER　デバッグの対象となる BGP ピアの IP アドレス。省略時はすべての BGP ピアが対象となる。

備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

関連コマンド

DISABLE BGP DEBUG（259 ページ）

ENABLE BGP DEFAULTORIGINATE

カテゴリー：IP / 経路制御（BGP-4）

ENABLE BGP DEFAULTORIGINATE

解説

BGP の経路表にデフォルト経路（0.0.0.0/0）を取り込むようにする。デフォルトは取り込まない。
実際にデフォルト経路を取り込むには、本コマンドを実行するだけでなく、以下の設定が必要。
・デフォルト経路を静的に設定するか、他のルーティングプロトコル経由で学習できるよう設定する。
・ADD BGP IMPORT コマンドか ADD BGP NETWORK コマンドを実行して、デフォルト経路が BGP の経路表に取り込まれるよう設定する。たとえば、ADD BGP IMPORT=STATIC、または ADD BGP NETWORK=0.0.0.0/0 のように設定する。
なお、取り込んだデフォルト経路を BGP ピアに通知するかどうかは、別途 ADD BGP PEER コマンドの DEFAULTORIGINATE パラメーターで設定する（デフォルトは通知しない）。

関連コマンド

ADD BGP PEER（154 ページ）
DISABLE BGP DEFAULTORIGINATE（260 ページ）
SET BGP PEER（343 ページ）

ENABLE BGP PEER

カテゴリー：IP / 経路制御（BGP-4）

ENABLE BGP PEER={**ALL**|***ipadd***}

ipadd: IP アドレス

解説

指定した BGP ピアとのセッションを開始（Active）状態にする。

パラメーター

PEER　BGP ピアの IP アドレス

関連コマンド

ADD BGP PEER（154 ページ）
DISABLE BGP PEER（261 ページ）
SHOW BGP PEER（418 ページ）

ENABLE BOOTP RELAY

カテゴリー：IP / DHCP/BOOTP リレー

ENABLE BOOTP RELAY

解説

DHCP/BOOTP リレー機能を有効にする。デフォルトは無効。

備考・注意事項

DHCP サーバー機能（ENABLE DHCP コマンド）とは併用できない。

関連コマンド

ADD BOOTP RELAY（161 ページ）
DELETE BOOTP RELAY（224 ページ）
DISABLE BOOTP RELAY（262 ページ）
PURGE BOOTP RELAY（322 ページ）
SET BOOTP MAXHOPS（349 ページ）
SHOW BOOTP RELAY（427 ページ）

ENABLE IP

カテゴリー：IP / 一般コマンド

ENABLE IP

解説

IP モジュールを有効にする。デフォルトは無効。

関連コマンド

DISABLE IP（263 ページ）
DISABLE IP FORWARDING（269 ページ）
DISABLE IP SRCROUTE（278 ページ）
ENABLE IP FORWARDING（300 ページ）
ENABLE IP SRCROUTE（310 ページ）
SHOW IP（429 ページ）

ENABLE IP ARP LOG

カテゴリー：IP / ARP

ENABLE IP ARP LOG

解説

ARP キャッシュログを有効にする。デフォルトは無効。
本コマンドを実行すると、ARP エントリーの追加、削除がログに記録されるようになる。

入力・出力・画面例

ARP キャッシュログの例

```
Manager > show log type=arp

 Date/Time   S Mod  Type  SType Message
 ------------------------------------------------------------------------------
 18 08:18:55 3 IPG  ARP   UPDAT  vlan1 del 00-00-f4-90-19-9b (172.17.28.5)
 18 08:18:55 3 IPG  ARP   UPDAT  vlan1 del 00-00-f4-95-30-6a (172.17.28.157)
 18 08:18:55 3 IPG  ARP   UPDAT  vlan1 del 00-00-f4-95-9f-31 (172.17.28.164)
 18 08:18:55 3 IPG  ARP   UPDAT  vlan1 del 00-50-56-07-36-81 (172.17.28.220)
 18 08:18:55 3 IPG  ARP   UPDAT  vlan1 del 00-0c-76-14-3f-c5 (172.17.28.232)
 18 08:18:57 3 IPG  ARP   UPDAT  vlan1 add 00-00-f4-90-19-9b (172.17.28.5)
 18 08:19:04 3 IPG  ARP   UPDAT  vlan1 add 00-90-99-c2-2b-00 (172.17.28.32)
 18 08:19:06 3 IPG  ARP   UPDAT  vlan1 add 00-50-56-07-36-81 (172.17.28.220)
 18 08:19:19 3 IPG  ARP   UPDAT  vlan1 add 00-00-f4-95-30-6a (172.17.28.157)
 18 08:19:22 3 IPG  ARP   UPDAT  vlan1 add 00-00-fe-be-ef-00 (172.17.28.238)
 18 08:20:19 3 IPG  ARP   UPDAT  vlan1 add 00-00-f4-95-fb-d4 (172.17.28.101)
 18 08:20:25 3 IPG  ARP   UPDAT  vlan1 add 00-00-e2-59-56-48 (172.17.28.233)
 18 08:20:26 3 IPG  ARP   UPDAT  vlan1 add 00-e0-18-8a-30-ad (172.17.28.230)
 18 08:20:30 3 IPG  ARP   UPDAT  vlan1 add 00-03-93-6b-70-a0 (172.17.28.219)
 18 08:20:32 3 IPG  ARP   UPDAT  vlan1 add 00-03-93-70-f3-84 (172.17.28.141)
 18 08:20:58 3 IPG  ARP   UPDAT  vlan1 add 00-06-5b-88-80-41 (172.17.28.1)
 18 08:21:51 3 IPG  ARP   UPDAT  vlan1 add 00-09-41-1c-5d-2f (172.17.28.185)
 18 08:22:25 3 IPG  ARP   UPDAT  vlan1 add 00-00-cd-0a-40-4e (172.17.28.185)
 18 08:22:59 3 IPG  ARP   UPDAT  vlan1 add 00-0c-76-14-3f-c5 (172.17.28.232)
 18 08:23:20 3 IPG  ARP   UPDAT  vlan1 add 00-00-f4-95-9f-31 (172.17.28.164)
 18 08:23:35 3 IPG  ARP   UPDAT  vlan1 add 00-e0-06-09-55-66 (172.17.28.251)
 18 08:24:16 3 IPG  ARP   UPDAT  vlan1 add 00-90-99-15-08-fc (172.17.28.105)
 18 08:25:07 3 IPG  ARP   UPDAT  eth1 add 00-90-99-ae-b0-02 (192.168.129.201)
 ------------------------------------------------------------------------------
```

備考・注意事項

ARP キャッシュログを見るには、SHOW LOG コマンドの TYPE オプションに ARP を指定するとよい

（SHOW LOG TYPE=ARP）。

関連コマンド

DISABLE IP ARP LOG（264 ページ）
SHOW IP（429 ページ）

ENABLE IP DEBUG

カテゴリー：IP / 一般コマンド

ENABLE IP DEBUG[=PACKET]

解説

IP デバッグキューをアクティブにし、ヘッダーエラーのある IP データグラムを保存するようにする。また、PACKET オプションを指定した場合は、送受信した IP データグラムのヘッダー情報をコンソールに表示するデバッグ機能が有効になる。
デバッグキューには、IP データグラムの先頭 64 オクテットを 40 個まで格納できる。エラーヘッダーの情報を見るには、SHOW IP DEBUG コマンドを使う。

パラメーター

DEBUG　PACKET を指定した場合は、送受信した IP データグラムのヘッダー情報がコンソールに出力されるようになる。何も指定しなかった場合は、エラーパケットの保存機能を有効化する。

入力・出力・画面例

```
Manager > enable ip debug=packet

Manager > <I/C/B=eth0/0/2, l=28, ttl=128, p=1, addr=172.16.28.119>224.0.0.2

Manager > <I/C/B=eth0/0/3, l=64, ttl=1, p=89, addr=172.16.28.32>224.0.0.5
```

備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

関連コマンド

DISABLE IP DEBUG（265 ページ）
SHOW IP（429 ページ）
SHOW IP DEBUG（444 ページ）

ENABLE IP DNSRELAY

カテゴリー：IP / DNS リレー

ENABLE IP DNSRELAY

解説

DNS リレー機能を有効にする。デフォルトは無効。
本機能を有効にすると、自分宛の DNS リクエストをあらかじめ設定した DNS サーバーに転送するようになる。
なお、DNS サーバーは ADD IP DNS コマンドで設定する。また、DNS キャッシュを使う場合は、SET IP DNS CACHE コマンドでキャッシュサイズを 0 以外の値に変更する。

関連コマンド

ADD IP DNS（167 ページ）
DELETE IP DNS（228 ページ）
DISABLE IP DNSRELAY（266 ページ）
SET IP DNS（356 ページ）
SET IP DNS CACHE（358 ページ）
SET IP DNSRELAY（359 ページ）
SHOW IP（429 ページ）
SHOW IP DNS（445 ページ）
SHOW IP DNS CACHE（447 ページ）

ENABLE IP ECHOREPLY

カテゴリー：IP / 一般コマンド

ENABLE IP ECHOREPLY

解説

ICMP エコー要求（PING）に対する応答を行うようにする。デフォルトは行う。

関連コマンド

DISABLE IP ECHOREPLY（267 ページ）

ENABLE IP FOFILTER

カテゴリー：IP / セキュリティー

ENABLE IP FOFILTER

解説

IP フラグメントオフセットフィルターを有効にする。デフォルトは有効。
有効時は、フラグメントオフセットが 1 の IP パケットを破棄する。これは、Tiny Fragment 攻撃や Overlapping Fragment 攻撃（RFC1858）に対する防御措置。
有効時にフラグメントオフセットが 1 のパケットを受信すると、メッセージタイプ「IPFIL」、サブタイプ「FRAG」のログメッセージが記録される。

備考・注意事項

デフォルト設定（有効）のまま使用することが望ましい。

関連コマンド

ADD IP FILTER（169 ページ）
DELETE IP FILTER（230 ページ）
DISABLE IP FOFILTER（268 ページ）
SET IP FILTER（360 ページ）
SHOW IP FILTER（449 ページ）

ENABLE IP FORWARDING

カテゴリー：IP / 一般コマンド

ENABLE IP FORWARDING

解説

IP 転送機能（ルーティング）を有効にする。デフォルトは有効。

関連コマンド

DISABLE IP（263 ページ）
DISABLE IP FORWARDING（269 ページ）
DISABLE IP SRCROUTE（278 ページ）
ENABLE IP（293 ページ）
ENABLE IP SRCROUTE（310 ページ）
SHOW IP（429 ページ）

ENABLE IP HELPER

カテゴリー：IP / UDP ブロードキャストヘルパー

ENABLE IP HELPER

解説

UDP ブロードキャストパケットの転送機能を有効にする。デフォルトは無効。

関連コマンド

ADD IP HELPER（176 ページ）
DELETE IP HELPER（231 ページ）
DISABLE IP HELPER（270 ページ）
SHOW IP HELPER（453 ページ）

ENABLE IP ICMPREPLY

カテゴリー：IP / 一般コマンド

ENABLE IP ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]

解説

指定した ICMP メッセージを送信するようにする。デフォルトではすべて送信する。

パラメーター

ICMPREPLY　送信するメッセージタイプを指定する。指定できるのは、NETUNREACH（Network Unreachable）、HOSTUNREACH（Host Unreachable）、REDIRECT（Redirect）の 3 種類のみ。ALL を指定した場合は、前記の 3 種類すべてが対象となる。

関連コマンド

DISABLE IP ICMPREPLY（271 ページ）
SHOW IP ICMPREPLY（457 ページ）

ENABLE IP INTERFACE

カテゴリー：IP / IP インターフェース

ENABLE IP INTERFACE=*interface*

interface: IP インターフェース名（eth0、ppp0 など）

解説

指定した IP インターフェースを有効にする。

パラメーター

INTERFACE　IP インターフェース名

関連コマンド

ADD IP INTERFACE（179 ページ）
DELETE IP INTERFACE（233 ページ）
DISABLE IP INTERFACE（272 ページ）
RESET IP INTERFACE（329 ページ）
SET IP INTERFACE（364 ページ）
SHOW IP INTERFACE（458 ページ）

ENABLE IP MACDISPARITY

カテゴリー：IP / ARP

ENABLE IP MACDISPARITY

解説

マルチキャスト MAC アドレスの ARP エントリー（例：IP=192.168.10.2 / MAC=01-00-5e-28-0a-02）を登録可能にする。デフォルトは登録不可。
本設定はダイナミックエントリーとスタティックエントリーの両方に適用される。

関連コマンド

ADD IP ARP（162 ページ）
DISABLE IP MACDISPARITY

ENABLE IP NAT

カテゴリー：IP / レンジ NAT

ENABLE IP NAT

解説

IP NAT（レンジ NAT）モジュールを有効にする。デフォルトは無効。

関連コマンド

ADD IP NAT（184 ページ）
DELETE IP NAT（235 ページ）
DISABLE IP NAT（273 ページ）
SHOW IP NAT（461 ページ）

ENABLE IP NAT FRAGMENT

カテゴリー：IP / レンジ NAT

ENABLE IP NAT FRAGMENT={**UDP**}

解説

IP NAT（レンジ NAT）モジュールに対し、指定したプロトコルのフラグメント化パケットを透過するよう指示する。

パラメーター

FRAGMENT　指定したプロトコルのフラグメント化パケットを透過するよう設定する。デフォルトでは、再構成後の IP データサイズ（L4 パケットサイズ）が 1780 バイトを越えるパケットは IP NAT モジュールによって破棄される。現時点でサポートしているプロトコルは UDP のみ

関連コマンド

ADD IP NAT（184 ページ）
DELETE IP NAT（235 ページ）
DISABLE IP NAT（273 ページ）
DISABLE IP NAT FRAGMENT（274 ページ）
SHOW IP NAT（461 ページ）

ENABLE IP NAT LOG

カテゴリー：IP / レンジ NAT

ENABLE IP NAT LOG={**ALL**|**FAILS**|**INTCP**|**INUDP**|**OUTTCP**|**OUTUDP**}[,...]

解説

IP NAT（レンジ NAT）モジュールのログオプションを有効にする。

パラメーター

LOG ログに記録する NAT イベントを指定する。カンマ区切りで複数指定可能。ALL（すべて）、FAILS（グローバル側で受信したがプライベート側サービスが未指定のため転送できなかったもの）、INTCP（グローバルからプライベートへの TCP セッション）、INUDP（グローバルからプライベートへの UDP フロー）、OUTTCP（プライベートからグローバルへの TCP セッション）、OUTUDP（プライベートからグローバルへの UDP フロー）

関連コマンド

ADD IP NAT（184 ページ）
DELETE IP NAT（235 ページ）
DISABLE IP NAT（273 ページ）
DISABLE IP NAT LOG（275 ページ）
SHOW IP NAT（461 ページ）

ENABLE IP REMOTEASSIGN

カテゴリー：IP / 一般コマンド

ENABLE IP REMOTEASSIGN

解説

IPCP（PPP のサブプロトコル）、または、DHCP による IP アドレスの動的設定機能を有効にする。
・PPP の場合は、ADD IP INTERFACE コマンドの IPADDRESS パラメーターに 0.0.0.0 を割り当てておく。
・DHCP の場合は、ADD IP INTERFACE コマンドの IPADDRESS パラメーターに DHCP を指定する。

備考・注意事項

本コマンドを実行して IP アドレスの動的設定機能を有効にしておかないと、ADD IP INTERFACE コマンドで DHCP によるアドレス取得をするよう指定してもインターフェースにアドレスが設定されないので注意（DHCP サーバーからのアドレス取得は行われるが、そのアドレスがインターフェースに設定されない）。

関連コマンド

DISABLE IP REMOTEASSIGN（276 ページ）
SHOW IP（429 ページ）

ENABLE IP ROUTE

カテゴリー：IP / 経路制御（スタティック）

ENABLE IP ROUTE {**CACHE**|**COUNT**|**MULTIPATH**}

解説

IP ルートキャッシュ、ルートカウンター、等価コストマルチパスルーティングを有効にする。

パラメーター

CACHE　ルートキャッシュを有効にする。デフォルトは有効。
COUNT　ルートカウンターを有効にする。デフォルトは無効。
MULTIPATH　等価コストマルチパスルーティングを有効にする。デフォルトは有効。

関連コマンド

DISABLE IP ROUTE（277 ページ）
SHOW IP ROUTE（473 ページ）

ENABLE IP SRCROUTE

カテゴリー：IP / セキュリティー

ENABLE IP SRCROUTE

解説

始点経路制御（ソースルート）オプション付き IP パケットの転送を有効にする（ソースルートフィルターを無効にする）。デフォルトは無効（転送しない ＝ ソースルートフィルターが有効）。
無効設定時（ソースルートフィルター有効時）に始点経路制御オプション付きパケットを受信すると、メッセージタイプ「IPFIL」、サブタイプ「SRCRT」のログメッセージが記録される。

備考・注意事項

始点経路制御オプションは通常使われておらず、むしろ悪用される可能性があるため、デフォルト設定（無効）のまま使用することが望ましい。

関連コマンド

DISABLE IP（263 ページ）
DISABLE IP SRCROUTE（278 ページ）
ENABLE IP（293 ページ）
ENABLE IP FORWARDING（300 ページ）
SHOW IP（429 ページ）

ENABLE OSPF

カテゴリー：IP / 経路制御（OSPF）

ENABLE OSPF

解説

OSPF モジュールを有効にする。デフォルトは無効。

関連コマンド

DISABLE OSPF（279 ページ）
SHOW OSPF（485 ページ）

ENABLE OSPF DEBUG

カテゴリー：IP / 経路制御（OSPF）

ENABLE OSPF DEBUG={**ALL**|**IFSTATE**|**NBRSTATE**|**PACKET**|**STATE**} [DETAIL={BRIEF|HEADER|LSAFULL|LSASUMMARY}]

解説

OSPF モジュールのデバッグ機能を有効にする。デフォルトは無効。

パラメーター

DEBUG デバッグオプション。IFSTATE（自インターフェースの状態）、NBRSTATE（対向インターフェースの状態）、PACKET（OSPF パケットの送受信情報）、STATE（自インターフェースと対向インターフェースの状態）、ALL（すべて）から選択する。

DETAIL デバッグオプション PACKET を有効にしたときに表示される情報の詳細さを指定する。BRIEF（OSPF ヘッダーとパケットの簡潔な情報）、HEADER（OSPF ヘッダーのみ）、LSAFULL（OSPF ヘッダーと LSA の詳細）、LSASUMMARY（OSPF ヘッダーと LSA のヘッダー情報）から選択する。デフォルトは HEADER。

備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

関連コマンド

DISABLE OSPF DEBUG（280 ページ）
DISABLE OSPF LOG（282 ページ）
ENABLE OSPF LOG（314 ページ）
SHOW OSPF（485 ページ）

ENABLE OSPF INTERFACE

カテゴリー：IP / 経路制御（OSPF）

ENABLE OSPF INTERFACE=*interface*

interface: IP インターフェース名（eth0、ppp0 など）または仮想インターフェース名（VIRTn）

解説

無効状態の OSPF インターフェースを有効にする。

パラメーター

INTERFACE　IP インターフェース名、または仮想インターフェース名（VIRTn）。

関連コマンド

ADD OSPF INTERFACE（202 ページ）
DELETE OSPF INTERFACE（244 ページ）
DISABLE OSPF INTERFACE（281 ページ）
RESET OSPF INTERFACE（332 ページ）
SET OSPF INTERFACE（386 ページ）
SHOW OSPF INTERFACE（493 ページ）

ENABLE OSPF LOG

カテゴリー：IP / 経路制御（OSPF）

ENABLE OSPF LOG

解説

OSPF イベントのログ記録を有効にする。デフォルトは無効。
OSPF イベントはログレベル 2 で（DETAIL）で記録される。各メッセージの先頭には、「OSPF-」に続けてイベント種別を示す下記コードが付加される。

T1	インターフェースの状態が変化
T2	隣接ルーターの状態が変化
T3	指名ルーター（DR）の変更
T4	新規 LSA の生成
T5	新規 LSA の受信
T6	ルーティングテーブル変更
C1	ヘッダーエラーにより OSPF パケットを破棄
C2	Hello パケットを破棄
C3	隣接ルーターの状態が不正なためその他のパケットを破棄
C4	データベース記述（DD）パケット再送
E1	受信 LSA のチェックサムエラー
E2	データベース LSA のチェックサムエラー
R1	同一 LSA が複数存在
R2	LSA のエイジ（Link State Age）不一致
R3	より新しい LSA を受信
R4	未知の LSA に対する Ack を受信
R5	古い LSA を受信
N1	LSA 更新タイマーが満了
N2	LSA が MaxAge に達した
N3	MaxAge に達した LSA をフラッシュ

表 28: イベント種別コード

備考・注意事項

本コマンドを実行しても、デフォルトのメッセージフィルター設定では、SHOW LOG コマンドで OSPF のログが表示されない。これは、OSPF イベントのログレベルが 2 であるため。オンメモリーのログ（TEMPORARY）には、デフォルトでレベル 3 以上のイベントしか記録されない。

関連コマンド

DISABLE OSPF LOG（282 ページ）
SHOW OSPF（485 ページ）

ENABLE PING POLL

カテゴリー：IP / Ping ポーリング

ENABLE PING POLL=*poll-id*

poll-id: Ping ポーリング ID（1〜100）

解説

Ping ポーリングを開始または再開する。
ADD PING POLL コマンドの実行直後は、該当機器への Ping ポーリングが停止（無効）状態になっているため、実際にポーリングを開始するには本コマンドを実行する必要がある。

パラメーター

POLL　Ping ポーリング ID

関連コマンド

DISABLE PING POLL（283 ページ）
RESET PING POLL（334 ページ）
SET PING POLL（396 ページ）
SHOW PING POLL（515 ページ）

ENABLE PING POLL DEBUG

カテゴリー：IP / Ping ポーリング

ENABLE PING POLL=*poll-id* DEBUG

poll-id: Ping ポーリング ID（1〜100）

解説

Ping ポーリングのデバッグ表示を有効にする。デフォルトは無効。

パラメーター

POLL　Ping ポーリング ID

入力・出力・画面例

```
Manager > enable ping poll=1 debug

Info (1058003): Operation successful.

Manager > Ping Poll(1): Sending Ping to 172.17.28.100

Manager > Ping Poll(1): Received a ping reply from 172.17.28.100
Ping Poll(1): State=UP upCount=33(30) failCount=0(5/5)

Manager > Ping Poll(1): Sending Ping to 172.17.28.100

Manager > Ping Poll(1): Received no reply from 172.17.28.100
Ping Poll(1): State=UP upCount=0(30) failCount=1(5/5)

Manager > Ping Poll(1): Sending Ping to 172.17.28.100

Manager > Ping Poll(1): Received no reply from 172.17.28.100
Ping Poll(1): State=UP upCount=0(30) failCount=2(5/5)
Ping Poll(1): Sending Ping to 172.17.28.100

Manager > Ping Poll(1): Received no reply from 172.17.28.100
Ping Poll(1): State=UP upCount=0(30) failCount=3(5/5)
Ping Poll(1): Sending Ping to 172.17.28.100

Manager > Ping Poll(1): Received no reply from 172.17.28.100
Ping Poll(1): State=UP upCount=0(30) failCount=4(5/5)
Ping Poll(1): Sending Ping to 172.17.28.100

Manager > Ping Poll(1): Received no reply from 172.17.28.100
```

```
Ping Poll(1): State=UP upCount=0(30) failCount=5(5/5)
Ping Poll(1): Old State=UP New State=DOWN
Ping Poll(1): Down Trigger
Ping Poll(1): Sending Ping to 172.17.28.100

Manager > Ping Poll(1): Received no reply from 172.17.28.100
Ping Poll(1): State=DOWN upCount=0(30) failCount=5(5/5)
Ping Poll(1): Sending Ping to 172.17.28.100

...

Manager > Ping Poll(1): Received a ping reply from 172.17.28.100
Ping Poll(1): State=DOWN upCount=1(30) failCount=4(5/5)
Ping Poll(1): Sending Ping to 172.17.28.100

Manager > Ping Poll(1): Received a ping reply from 172.17.28.100
Ping Poll(1): State=DOWN upCount=2(30) failCount=3(5/5)
Ping Poll(1): Sending Ping to 172.17.28.100

...

Manager > Ping Poll(1): Received a ping reply from 172.17.28.100
Ping Poll(1): State=DOWN upCount=29(30) failCount=0(5/5)
Ping Poll(1): Sending Ping to 172.17.28.100

Manager > Ping Poll(1): Received a ping reply from 172.17.28.100
Ping Poll(1): State=DOWN upCount=30(30) failCount=0(5/5)
Ping Poll(1): Old State=DOWN New State=UP
Ping Poll(1): Up Trigger
Ping Poll(1): Sending Ping to 172.17.28.100

Manager > Ping Poll(1): Received a ping reply from 172.17.28.100
Ping Poll(1): State=UP upCount=31(30) failCount=0(5/5)
```

備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

関連コマンド

DISABLE PING POLL DEBUG（284 ページ）
SHOW PING POLL（515 ページ）

PING

カテゴリー：IP / 一般コマンド

```
PING [[IPADDRESS=]{ipadd|hostname}] [DELAY=seconds] [LENGTH=0..1500]
    [NUMBER={count|CONTINUOUS}] [PATTERN=value] [SIPADDRESS=ipadd}]
    [SCREENOUTPUT={YES|NO}] [TIMEOUT=1..60] [TOS=0..255]
```

ipadd: IP アドレス
hostname: ホスト名
seconds: 時間（0〜4294967295 秒）
count: 個数（1〜4294967295）
value: バイト列（16 進数。最大 4 バイト）

解説

指定アドレスに対して PING を実行する。
未指定のパラメーターについては、SET PING コマンドで設定したデフォルト値が用いられる。

パラメーター

IPADDRESS　宛先 IP アドレス（IPv4、IPv6）。ホストテーブルに登録されているホスト名も使用可能。また、ADD IP DNS コマンドで DNS サーバーのアドレスを設定している場合は DNS に登録されているホスト名（ドメイン名）も使用可能。

DELAY　PING パケットの送信間隔。デフォルトは 1 秒。

LENGTH　PING パケットのデータ部分の長さ。

NUMBER　PING パケットの送信個数。CONTINUOUS を指定した場合は、STOP PING コマンドで停止させられるまでパケットの送信を続ける。

PATTERN　PING パケットのデータ部分に埋め込む 4 バイトのバイナリーパターンを 16 進数で指定する（例：686f6765）。

SIPADDRESS　PING パケットの始点 IP アドレス（IPv4、IPv6）。省略時は送出インターフェースの IP アドレスが使われる。IPv6 のリンクローカルアドレスは指定できない。

SCREENOUTPUT　結果を端末画面に表示するかどうか。

TIMEOUT　応答待ち時間を指定する。

TOS　宛先アドレスが IP（IPv4）の場合、TOS オクテットの値を指定する。また、IPv6 の場合は Traffic Class フィールドの値を指定する。有効範囲は 0〜255。

入力・出力・画面例

```
Manager > ping 172.16.28.32

Echo reply 1 from 172.16.28.32 time delay 8 ms
```

```
Echo reply 2 from 172.16.28.32 time delay 5 ms

Echo reply 3 from 172.16.28.32 time delay 5 ms

Echo reply 4 from 172.16.28.32 time delay 5 ms

Echo reply 5 from 172.16.28.32 time delay 5 ms
```

例

■IP ノードに対する PING

```
PING 192.168.10.23
```

■IPv6 ノードに対する PING

```
PING 3ffe:b80:3c:10:290:99ff:fe42:f2
```

■IPv6 ノード（リンクローカルアドレスで指定）に対する PING

```
PING fe80::290:99ff:fe42:f2%vlan1
```

関連コマンド

ADD IP DNS（167 ページ）
ADD IP HOST（178 ページ）
ADD IPV6 HOST（「IPv6」の 44 ページ）
SET PING（394 ページ）
SHOW PING（513 ページ）
STOP PING（525 ページ）

PURGE BGP DAMPING

カテゴリー：IP / 経路制御（BGP-4）

PURGE BGP DAMPING

解説

BGP-4 ルートフラップダンピングの設定情報をすべて削除する。
カスタムパラメーターセットやルートフラップの履歴情報は削除され、ルートフラップダンピング機能は無効化される。

備考・注意事項

ランタイムメモリー上にあるルートフラップダンピング関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

関連コマンド

ADD BGP PEER（154 ページ）
CREATE BGP DAMPING PARAMETERSET（215 ページ）
DESTROY BGP DAMPING PARAMETERSET（253 ページ）
DISABLE BGP DAMPING（258 ページ）
ENABLE BGP DAMPING（288 ページ）
RESET BGP DAMPING（325 ページ）
SET BGP DAMPING PARAMETERSET（339 ページ）
SHOW BGP DAMPING（409 ページ）
SHOW BGP DAMPING ROUTES（411 ページ）

PURGE BOOTP RELAY

カテゴリー：IP / DHCP/BOOTP リレー

PURGE BOOTP RELAY

解説

DHCP/BOOTP リレー機能の設定情報をすべて削除する。

備考・注意事項

不用意に本コマンドを実行しないよう注意。

関連コマンド

ADD BOOTP RELAY（161 ページ）
DELETE BOOTP RELAY（224 ページ）
DISABLE BOOTP RELAY（262 ページ）
ENABLE BOOTP RELAY（292 ページ）
SET BOOTP MAXHOPS（349 ページ）
SHOW BOOTP RELAY（427 ページ）

PURGE IP

カテゴリー：IP / 一般コマンド

PURGE IP

解説

IP の設定情報をすべて削除する。

備考・注意事項

ランタイムメモリー上にある IP 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

関連コマンド

RESET IP（327 ページ）

PURGE OSPF

カテゴリー：IP / 経路制御（OSPF）

PURGE OSPF

解説

OSPF の設定情報をすべて削除し、グローバルな設定パラメーターをデフォルトに戻す。OSPF モジュールは無効状態になる。

備考・注意事項

ランタイムメモリー上にある OSPF 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

関連コマンド

DISABLE OSPF（279 ページ）
ENABLE OSPF（311 ページ）
RESET OSPF（330 ページ）
SHOW OSPF（485 ページ）

RESET BGP DAMPING

カテゴリー：IP / 経路制御（BGP-4）

RESET BGP DAMPING [PARAMETERSET={ALL|*0..100*}]

解説

BGP-4 ルートフラップダンピングのルートフラップ履歴情報（ペナルティー値などの情報）をクリアする。

パラメーター

PARAMETERSET パラメーターセット番号。パラメーターセット番号を指定した場合は、該当パラメーターセットだけが対象となる。0 はデフォルトのパラメーターセット。ALL を指定した場合、および、番号を省略した場合は、すべてのパラメーターセットが対象となる。

関連コマンド

ADD BGP PEER（154 ページ）
CREATE BGP DAMPING PARAMETERSET（215 ページ）
DESTROY BGP DAMPING PARAMETERSET（253 ページ）
DISABLE BGP DAMPING（258 ページ）
ENABLE BGP DAMPING（288 ページ）
PURGE BGP DAMPING（321 ページ）
SET BGP DAMPING PARAMETERSET（339 ページ）
SHOW BGP DAMPING（409 ページ）
SHOW BGP DAMPING ROUTES（411 ページ）

RESET BGP PEER

カテゴリー：IP / 経路制御（BGP-4）

RESET BGP PEER={**ALL**|***ipadd***} [SOFT={IN|OUT|ALL}]

ipadd: IP アドレス

解説

指定したピアとの BGP セッションをリセットする。
SOFT パラメーターを指定しなかった場合は、指定したピアとのセッションをいったん切断し、その後再接続して経路情報を更新する。
SOFT パラメーターを指定した場合は、指定したピアとの BGP セッションをリセットすることなく、経路情報だけを更新する（ソフトリセット）。

パラメーター

PEER　BGP ピアの IP アドレス

SOFT　経路を更新する方向。ソフトリセット時に指定する。IN を指定した場合は、該当ピアに ROUTE-REFRESH メッセージを送信して、経路情報の再送信を要求する。OUT を指定した場合は、単に該当ピアに経路情報を送信しなおす。ALL を指定した場合は、IN と OUT の両方の動作を行う。

関連コマンド

DISABLE BGP PEER（261 ページ）
ENABLE BGP AUTOSOFTUPDATE（285 ページ）
ENABLE BGP PEER（291 ページ）
SET BGP PEER（343 ページ）
SHOW BGP PEER（418 ページ）

RESET IP

カテゴリー：IP / 一般コマンド

```
RESET IP
```

解説

IP モジュールをリセットする。

備考・注意事項

IP の下位インターフェース（PPP など）に変更を加えたときなどに使うもので、通常使う必要はない。

関連コマンド

PURGE IP（323 ページ）
RESET IP COUNTER（328 ページ）
RESET IP INTERFACE（329 ページ）

RESET IP COUNTER

カテゴリー：IP / 一般コマンド

RESET IP COUNTER={**ALL**|**ARP**|**ICMP**|**INTERFACE**|**IP**|**MULTICAST**|**ROUTE**|**SNMP**|**UDP**}

解説

IP 関連の統計カウンターをゼロにリセットする。

パラメーター

COUNTER　リセットするカウンターのカテゴリーを指定する。ALL を指定した場合はすべてのカウンターをリセットする。

関連コマンド

RESET IP（327 ページ）
RESET IP INTERFACE（329 ページ）
SHOW IP COUNTER（437 ページ）

RESET IP INTERFACE

カテゴリー：IP / IP インターフェース

RESET IP INTERFACE=*interface*

interface: IP インターフェース名（eth0、ppp0 など）

解説

指定した IP インターフェースをリセットする。
該当インターフェース上のダイナミック経路、ARP エントリーは消去され、また統計カウンターもリセットされる。

パラメーター

INTERFACE　リセットする IP インターフェース

関連コマンド

ADD IP INTERFACE（179 ページ）
DELETE IP INTERFACE（233 ページ）
DISABLE IP INTERFACE（272 ページ）
ENABLE IP INTERFACE（303 ページ）
RESET IP（327 ページ）
RESET IP COUNTER（328 ページ）
SET IP INTERFACE（364 ページ）
SHOW IP INTERFACE（458 ページ）

RESET OSPF

カテゴリー：IP / 経路制御（OSPF）

RESET OSPF

解説

OSPF モジュールをリセットし、各種データを再初期化する。
本コマンドでは OSPF の統計カウンターはリセットされない（RESET OSPF COUNTER コマンドでリセットする）。

関連コマンド

DISABLE OSPF（279 ページ）
ENABLE OSPF（311 ページ）
PURGE OSPF（324 ページ）
RESET OSPF COUNTER（331 ページ）
RESET OSPF INTERFACE（332 ページ）
SHOW OSPF（485 ページ）

RESET OSPF COUNTER

カテゴリー：IP / 経路制御（OSPF）

RESET OSPF COUNTER

解説

OSPF の統計カウンターをリセットする。

関連コマンド

PURGE OSPF（324 ページ）
RESET OSPF（330 ページ）
RESET OSPF INTERFACE（332 ページ）
SHOW OSPF（485 ページ）

RESET OSPF INTERFACE

カテゴリー：IP / 経路制御（OSPF）

RESET OSPF INTERFACE=*interface*

interface: IP インターフェース名（eth0、ppp0 など）または仮想インターフェース名（VIRTn）

解説

OSPF インターフェースをリセットする。
インターフェースをいったんクローズして配下ネットワークの経路情報をすべて破棄した後、インターフェースを再オープンし経路情報を再学習する。

パラメーター

INTERFACE　IP インターフェース名、または仮想インターフェース名（VIRTn）

関連コマンド

ADD OSPF INTERFACE（202 ページ）
DELETE OSPF INTERFACE（244 ページ）
DISABLE OSPF INTERFACE（281 ページ）
ENABLE OSPF INTERFACE（313 ページ）
SET OSPF INTERFACE（386 ページ）
SHOW OSPF INTERFACE（493 ページ）

RESET OSPF SPF

カテゴリー：IP / 経路制御（OSPF）

RESET OSPF SPF [DEBUG]

解説

OSPF ルートテーブルを再計算する。

パラメーター

DEBUG　ルートテーブル再計算に関するデバッグ情報をポートに出力する。

関連コマンド

PURGE OSPF（324 ページ）
RESET OSPF（330 ページ）
RESET OSPF COUNTER（331 ページ）
RESET OSPF INTERFACE（332 ページ）
SHOW OSPF（485 ページ）
SHOW OSPF DEBUG（490 ページ）
SHOW OSPF LSA（497 ページ）

RESET PING POLL

カテゴリー：IP / Ping ポーリング

RESET PING POLL=*poll-id*

poll-id: Ping ポーリング ID（1〜100）

解説

Ping ポーリングのカウンターを初期化し、機器の状態を初期値の「Up」に戻す。

パラメーター

POLL　Ping ポーリング ID

備考・注意事項

本コマンドの実行により機器の状態が「Down」「Critical Down」から「Up」に戻っても、DEVICEUP イベントは発生しない。

関連コマンド

DELETE PING POLL（251 ページ）
DISABLE PING POLL（283 ページ）
SHOW PING POLL（515 ページ）

SET BGP

カテゴリー：IP / 経路制御（BGP-4）

```
SET BGP [CONFEDERATIONID={NONE|1..65534}] [LOCALPREF={DEFAULT|
    0..4294967295}] [MED={NONE|0..4294967294}] [PREFEXT={DEFAULT|1..255}]
    [PREFINT={DEFAULT|1..255}] [TABLEMAP[=routemap]]
```

routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）

解説

BGP-4 のグローバル設定パラメーターを変更する。

パラメーター

CONFEDERATIONID　所属する AS コンフェデレーションの ID。デフォルトは NONE。

LOCALPREF　I-BGP セッションで通知する LOCAL_PREF 属性のデフォルト値。ルートマップで LOCAL_PREF 値を明示的に変更しない限り、このパラメーターの値が使用される。デフォルトは 100。LOCAL_PREF は AS 内での経路選択に用いられる優先度で、大きいほど優先度が高い。

MED　E-BGP セッションで通知する MULTI_EXIT_DISC（MED）属性のデフォルト値。ルートマップで MULTI_EXIT_DISC 値を明示的に変更しない限り、このパラメーターの値が使用される。デフォルトは NONE（MULTI_EXIT_DISC 属性を含めない）。MULTI_EXIT_DISC は、隣接 AS と複数点で接続している場合に、接続点を選択するために使う値。他の条件が同じであれば、MULTI_EXIT_DISC の値が小さい経路を選択する。

PREFEXT　ルーターの経路表（SHOW IP ROUTE コマンドで表示できるもの）における、E-BGP ピアから学習した経路の優先度。デフォルトは 170。

PREFINT　ルーターの経路表（SHOW IP ROUTE コマンドで表示できるもの）における、I-BGP ピアから学習した経路の優先度。デフォルトは 170。

TABLEMAP　BGP 経由で学習した経路をルーターの経路表にインポートする際に適用するルートマップ。ルートマップを解除するときは、ルートマップ名を指定せず、単に「TABLEMAP」と指定する。デフォルトはルートマップなし。

関連コマンド

ADD BGP CONFEDERATIONPEER（151 ページ）
DELETE BGP CONFEDERATIONPEER（219 ページ）
SHOW BGP（399 ページ）
SHOW BGP CONFEDERATION（405 ページ）

SET BGP AGGREGATE

カテゴリー：IP / 経路制御（BGP-4）

SET BGP AGGREGATE=*prefix* [MASK=*ipadd*] [SUMMARY={NO|YES}]
[ROUTEMAP[=*routemap*]]

prefix: プレフィックス（IP アドレス/プレフィックス長）
ipadd: IP アドレスまたはネットマスク
routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）

解説

集約経路エントリーの設定を変更する。

パラメーター

AGGREGATE　集約後のプレフィックス。ネットワークアドレスとプレフィックス長で指定する。プレフィックス長は MASK パラメーターで指定することも可能。
MASK　AGGREGATE で指定したプレフィックスの有効長。
SUMMARY　集約経路だけを BGP の経路表に入れる場合は YES を指定する。NO を指定したときは、集約前の（より具体的な）個々のエントリーも BGP 経路表に残る。デフォルトは NO。
ROUTEMAP　ルートマップ名。集約経路に属性を設定するために用いる。

関連コマンド

ADD BGP AGGREGATE（149 ページ）
DELETE BGP AGGREGATE（218 ページ）
SHOW BGP AGGREGATE（401 ページ）
SHOW BGP ROUTE（425 ページ）

SET BGP BACKOFF

カテゴリー：IP / 経路制御（BGP-4）

```
SET BGP BACKOFF[=20..100] [LOW=15..99] [BASETIME=0..100]
    [CONSECUTIVE=1..20] [MULTIPLIER=0..1000] [STEP=1..1000]
    [TOTALLIMIT=0..1000]
```

解説

空きメモリー不足時の BGP-4 のバックオフ（一時停止）動作を設定する。

パラメーター

BACKOFF　バックオフしきい値（%）。システム全体のメモリー使用量が本しきい値に達した場合、BGP-4 の処理は一時停止（バックオフ）される。LOW パラメーターよりも大きい値に設定しなくてはならない。デフォルトは 95%。

LOW　バックオフ解除しきい値（%）。BGP-4 の処理が一時停止（バックオフ）された後、システム全体のメモリー使用量が本しきい値を下回ると、BGP-4 の処理が再開される。BACKOFF パラメーターよりも小さい値に設定しなくてはならない。デフォルトは 90%。

BASETIME　バックオフ時間の基準値（秒）。バックオフ時間の基準値（秒）：実際のバックオフ時間は BASETIME、MULTIPLIER、STEP の組み合わせと何回目のバックオフであるかによって決まる。デフォルトは 10 秒。

CONSECUTIVE　連続したバックオフの制限回数。バックオフが CONSECUTIVE 回連続して発生した場合は、回復不可能と判断してすべての BGP セッションを停止する。デフォルトは 5 回。

MULTIPLIER　バックオフ時間を決定するための係数。初回のバックオフ時間は BASETIME × MULTIPLIER ÷ 100 で求められる（小数点以下は切り捨て）。バックオフが連続して発生した場合、初回を含めて STEP 回は同じバックオフ時間が用いられる、その次の回のバックオフ時間は前回のバックオフ時間 × MULTIPLIER ÷ 100（小数点以下は切り捨て）となる。すなわち、MULTIPLIER を 100 より大きく設定すればバックオフ時間は次第に長くなり、100 より小さく設定すればバックオフ時間は次第に短くなる。デフォルトは 100（バックオフ時間は一定）。

STEP　バックオフが連続して発生した場合、何回ごとにバックオフ時間を再計算するか。デフォルトは 1 回。

TOTALLIMIT　バックオフの合計制限回数。バックオフが合計 TOTALLIMIT 回発生した場合（システム起動後の合計回数。連続していなくてもよい）は、すべての BGP セッションを切断（ピアを無効化）する。0 は無制限を意味する。デフォルトは 0。

関連コマンド

SET BGP MEMLIMIT（342 ページ）
SHOW BGP BACKOFF（402 ページ）

SHOW BGP MEMLIMIT（414 ページ）

SET BGP DAMPING PARAMETERSET

カテゴリー：IP / 経路制御（BGP-4）

SET BGP DAMPING PARAMETERSET=*1..100* [DESCRIPTION[=*string*]]
[SUPPRESSION={DEFAULT|*1..32000*}] [REUSE={DEFAULT|*1..32000*}]
[HALFLIFE={DEFAULT|*1..45*}] [MAXHOLD={DEFAULT|*1..8*}]

string: 文字列（1〜63 文字）

解説

BGP-4 ルートフラップダンピング用のパラメーターセットの設定を変更する。

パラメーター

PARAMETERSET　パラメーターセット番号。

DESCRIPTION　パラメーターセットに関する覚え書き（メモ）。

SUPPRESSION　抑制しきい値。経路のペナルティー値（経路の不安定さを示す）が本しきい値を上回ると、該当経路は Suppressed（抑制）状態となり、ペナルティー値が再使用しきい値（REUSE）を下回るか、安定状態が最大抑制時間（HALFLIFE × MAXHOLD）続くまで、同経路は使用も広告もされなくなる。REUSE よりも小さな値は指定できない。デフォルトは 2000。

REUSE　再使用（抑制解除）しきい値。いったん抑制状態となった経路は、ペナルティー値が本しきい値を下回るか、安定状態が最大抑制時間（HALFLIFE × MAXHOLD）続くまでは使用も広告もされない。ペナルティー値が本しきい値を下回ると、該当経路の抑制状態は解除され、Monitored（監視）状態に遷移する。SUPPRESSION よりも大きな値は指定できない。デフォルトは 750。

HALFLIFE　ペナルティー値の半減期（単位は分）。安定状態にある経路のペナルティー値は徐々に減少していくが、そのときの速度は「HALFLIFE（分）経過するごとに半分になる」レートである。デフォルトは 15 分。

MAXHOLD　最大抑制時間を求めるための係数。実際の最大抑制時間は HALFLIFE × MAXHOLD（分）で求められる。Suppressed（抑制）状態にある経路のペナルティー値が再使用しきい値（REUSE）を上回っていても、安定状態が最大抑制時間（HALFLIFE × MAXHOLD）続いた場合は抑制状態が解除される。デフォルトは 4。

関連コマンド

ADD BGP PEER（154 ページ）
CREATE BGP DAMPING PARAMETERSET（215 ページ）
DESTROY BGP DAMPING PARAMETERSET（253 ページ）
DISABLE BGP DAMPING（258 ページ）
ENABLE BGP DAMPING（288 ページ）
PURGE BGP DAMPING（321 ページ）

RESET BGP DAMPING（325 ページ）
SHOW BGP DAMPING（409 ページ）
SHOW BGP DAMPING ROUTES（411 ページ）

SET BGP IMPORT

カテゴリー：IP / 経路制御（BGP-4）

SET BGP IMPORT={**OSPF**|**RIP**|**STATIC**|**INTERFACE**} [ROUTEMAP[=*routemap*]]

routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）

解説

BGP に経路情報を取り込むときに適用するルートマップを変更する。

パラメーター

IMPORT　BGP に取り込む経路情報の種類（起源）

ROUTEMAP　インポート時に適用するルートマップ。値を指定しない（単に ROUTEMAP と指定）とフィルター解除となる。デフォルトはなし。

関連コマンド

ADD BGP IMPORT（152 ページ）
DELETE BGP IMPORT（220 ページ）
SHOW BGP IMPORT（413 ページ）

SET BGP MEMLIMIT

カテゴリー：IP / 経路制御（BGP-4）

SET BGP MEMLIMIT=*0..100*

解説

BGP-4 に割り当て可能な最大メモリー量を指定する。

パラメーター

MEMLIMIT　BGP-4 に割り当て可能な最大メモリー量 (%)。BGP-4 によるメモリー使用率が MEMLIMIT を超えた場合は、すべての BGP セッションを停止する。デフォルトは 85%。

関連コマンド

SET BGP BACKOFF（337 ページ）
SHOW BGP BACKOFF（402 ページ）
SHOW BGP MEMLIMIT（414 ページ）

SET BGP PEER

カテゴリー：IP / 経路制御（BGP-4）

```
SET BGP PEER=ipadd [CONNECTRETRY={DEFAULT|0..4294967295}]
   [DESCRIPTION[=string]] [EHOPS={DEFAULT|1..255}] [HOLDTIME={DEFAULT|0|
   3..65535}] [INFILTER={NONE|300..399}] [INPATHFILTER={NONE|1..99}]
   [INROUTEMAP[=routemap]] [KEEPALIVE={DEFAULT|1..21845}] [LOCAL={NONE|
   1..15}] [MAXPREFIX={OFF|1..4294967295}] [MAXPREFIXACTION={WARNING|
   TERMINATE}] [MINASORIGINATED={DEFAULT|0..3600}] [MINROUTEADVERT={DEFAULT|
   0..3600}] [NEXTHOPSELF={NO|YES}] [OUTFILTER={NONE|300..399}]
   [OUTPATHFILTER={NONE|1..99}] [OUTROUTEMAP[=routemap]]
   [REMOTEAS=1..65534] [SENDCOMMUNITY={NO|YES}] [DEFAULTORIGINATE={NO|YES}]
```

ipadd: IP アドレス
string: 文字列（1〜63 文字）
routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）

解説

BGP ピアの設定パラメーターを変更する。該当ピアは無効状態（DISABLE BGP PEER コマンド）でなくてはならない。

パラメーター

PEER　BGP ピアの IP アドレス。
CONNECTRETRY　BGP コネクション確立の再試行間隔（秒）。デフォルトは 120。0 は再試行しない。
DESCRIPTION　BGP ピアに関する覚え書き（メモ）。
EHOPS　E-BGP セッションにおける BGP メッセージの初期 TTL 値。デフォルトは 1。ルーターをまたいで E-BGP セッションを張るためには、EHOPS を 2 以上に設定する必要がある。
HOLDTIME　該当ピアとの BGP セッションがダウンしたと認識するまでの時間（Hold Time）（秒）を設定する。実際の Hold Time はセッション開始時のネゴシエーションによって決まる。本パラメーターで設定するのは OPEN メッセージで相手に提案する値。デフォルトは 90 秒。0 はこちらからは提案しないことを意味する。
INFILTER　該当ピアからの経路情報に適用する IP プレフィックスフィルターの番号。このフィルターは、プレフィックス（ネットワーク番号）によって経路の受け入れ・破棄を決めるもの。IP プレフィックスフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 300〜399）。
INPATHFILTER　該当ピアからの経路情報に適用する AS パスフィルターの番号。このフィルターは、AS-PATH 属性の内容によって経路の受け入れ・破棄を決めるもの。AS パスフィルターは ADD IP ASPATHLIST コマンドで作成する。
INROUTEMAP　該当ピアからの経路情報に適用するルートマップ名。ルートマップは、経路情報の内容を変更したりするもの。ルートマップは ADD IP ROUTEMAP コマンドで作成する。

KEEPALIVE　KEEPALIVE メッセージの送信間隔。HOLDTIME の 1/3 に設定する必要がある。実際の送信間隔は HOLDTIME のネゴシエーションによって決まる。

LOCAL　該当ピアとの通信に使用するローカル IP インターフェースの番号。ローカル IP インターフェースを指定した場合、本ピア宛ての BGP パケットの始点 IP アドレスとして、指定したローカル IP インターフェースの IP アドレスが使用される。省略時は NONE（ローカル IP インターフェースを使用しない。この場合、BGP パケットの始点 IP アドレスはシステムが決める）。

MAXPREFIX　該当ピアから受け入れ可能な最大プレフィックス数を設定する。OFF の場合は制限を設けない。デフォルトは OFF。

MAXPREFIXACTION　MAXPREFIX パラメーターの値を超えるプレフィックスを受信したときの動作。WARNING はログに記録するだけ。TERMINATE はログに記録した上で該当ピアとのセッションをリセットする。デフォルトは WARNING。

MINASORIGINATED　自 AS 起源の経路情報を含む UPDATE メッセージの最小連続送信間隔。デフォルトは 15 秒

MINROUTEADVERT　他 AS 起源の経路情報を含む UPDATE メッセージの最小連続送信間隔。デフォルトは 30 秒

NEXTHOPSELF　該当ピアに通知する経路の NEXT_HOP として必ず自アドレスを使うかどうか。デフォルトは NO。

OUTFILTER　該当ピアに経路情報を通知する前に適用する IP プレフィックスフィルターの番号。このフィルターは、プレフィックス（ネットワーク番号）によって経路の通知・破棄を決めるもの。IP プレフィックスフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 300〜399）。

OUTPATHFILTER　該当ピアに経路情報を通知する前に適用する AS パスフィルターの番号。このフィルターは、AS-PATH 属性の内容によって経路の通知・破棄を決めるもの。AS パスフィルターは ADD IP ASPATHLIST コマンドで作成する。

OUTROUTEMAP　該当ピアに経路情報を通知する前に適用するルートマップ名。ルートマップは、経路情報の内容を変更したりするもの。ルートマップは ADD IP ROUTEMAP コマンドで作成する。

REMOTEAS　BGP ピアが所属する AS 番号。自 AS 番号と同じなら I-BGP、違うなら E-BGP ピアとなる。自 AS 番号は SET IP AUTONOMOUS コマンドで設定する。

SENDCOMMUNITY　UPDATE メッセージに COMMUNITIES 属性を含めるかどうか。同属性の具体的内容はルートマップで設定する。デフォルトは NO。

DEFAULTORIGINATE　該当ピアにデフォルト経路（0.0.0.0/0）を通知するかどうか。デフォルトは NO。デフォルト経路を通知するには、ENABLE BGP DEFAULTORIGINATE コマンドの設定が必要。

関連コマンド

ADD BGP PEER（154 ページ）
ADD IP ASPATHLIST（163 ページ）
ADD IP FILTER（169 ページ）
ADD IP ROUTEMAP（195 ページ）
DELETE BGP PEER（222 ページ）
DISABLE BGP PEER（261 ページ）
ENABLE BGP PEER（291 ページ）
RESET BGP PEER（326 ページ）

SHOW BGP PEER（418 ページ）

SET BGP PEERTEMPLATE

カテゴリー：IP / 経路制御（BGP-4）

```
SET BGP PEERTEMPLATE=1..30 [CONNECTRETRY={DEFAULT|0..4294967295}]
    [DESCRIPTION[=string]] [HOLDTIME={DEFAULT|0|3..65535}] [INFILTER={NONE|
    300..399}] [INPATHFILTER={NONE|1..99}] [INROUTEMAP[=routemap]]
    [KEEPALIVE={DEFAULT|1..21845}] [MAXPREFIX={OFF|1..4294967295}]
    [MAXPREFIXACTION={WARNING|TERMINATE}] [MINASORIGINATED={DEFAULT|
    0..3600}] [MINROUTEADVERT={DEFAULT|0..3600}] [NEXTHOPSELF={NO|YES}]
    [OUTFILTER={NONE|300..399}] [OUTPATHFILTER={NONE|1..99}]
    [OUTROUTEMAP[=routemap]] [SENDCOMMUNITY={NO|YES}] [LOCAL={NONE|1..15}]
    [CLIENT={NO|YES}] [PRIVATEASFILTER={NO|YES}]
```

string: 文字列（1〜63 文字）
routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）

解説

BGP ピアテンプレートの設定を変更する。

パラメーター

PEERTEMPLATE　BGP ピアテンプレート番号。
CONNECTRETRY　BGP コネクション確立の再試行間隔（秒）。デフォルトは 120。0 は再試行しない。
DESCRIPTION　BGP ピアテンプレートに関する覚え書き（メモ）。
HOLDTIME　BGP セッションがダウンしたと認識するまでの時間（Hold Time）（秒）を設定する。実際の Hold Time はセッション開始時のネゴシエーションによって決まる。本パラメーターで設定するのは OPEN メッセージで相手に提案する値。デフォルトは 90 秒。0 はこちらからは提案しないことを意味する。
INFILTER　該当ピアから受信した経路情報に適用する IP プレフィックスフィルターの番号。INFILTER を使用すると、プレフィックス（ネットワーク番号）によって経路の受け入れ・破棄を行うことができる。IP プレフィックスフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 300〜399）。
INPATHFILTER　該当ピアから受信した経路情報に適用する AS パスリストの番号。INPATHFILTER を使用すると、AS_PATH 属性の内容によって経路の受け入れ・破棄を行うことができる。AS パスリストは ADD IP ASPATHLIST コマンドで作成する。
INROUTEMAP　該当ピアから受信した経路情報に適用するルートマップ名。INROUTEMAP を使用すると、各種の基準に基づいて、経路情報をフィルタリングしたり、属性を変更したりできる。ルートマップは ADD IP ROUTEMAP コマンドで作成する。ルートマップを解除するときは、ルートマップ名を指定せず、単に「INROUTEMAP」と指定する。
KEEPALIVE　KEEPALIVE メッセージの送信間隔。HOLDTIME の 1/3 に設定する必要がある。実際の

送信間隔は HOLDTIME のネゴシエーションによって決まる。

MAXPREFIX　該当ピアから受け入れ可能な最大プレフィックス数を設定する。OFF の場合は制限を設けない。デフォルトは OFF。

MAXPREFIXACTION　MAXPREFIX パラメーターの値を超えるプレフィックスを受信したときの動作。WARNING はログに記録するだけ。TERMINATE はログに記録した上で該当ピアとのセッションをリセットする。デフォルトは WARNING。

MINASORIGINATED　自 AS 起源の経路情報を含む UPDATE メッセージの最小連続送信間隔。デフォルトは 15 秒

MINROUTEADVERT　他 AS 起源の経路情報を含む UPDATE メッセージの最小連続送信間隔。デフォルトは 30 秒

NEXTHOPSELF　該当ピアに通知する経路の NEXT_HOP として必ず自アドレスを使うかどうか。デフォルトは NO。

OUTFILTER　該当ピアに経路情報を通知する前に適用する IP プレフィックスフィルターの番号。OUTFILTER を使用すると、プレフィックス（ネットワーク番号）によって経路の通知・破棄を行うことができる。IP プレフィックスフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 300～399）。

OUTPATHFILTER　該当ピアに経路情報を通知する前に適用する AS パスリストの番号。OUTPATHFILTER を使用すると、AS_PATH 属性の内容によって経路の通知・破棄を行うことができる。AS パスリストは ADD IP ASPATHLIST コマンドで作成する。

OUTROUTEMAP　該当ピアに経路情報を通知する前に適用するルートマップ名。OUTROUTEMAP を使用すると、各種の基準に基づいて、経路情報をフィルタリングしたり、属性を変更したりできる。ルートマップは ADD IP ROUTEMAP コマンドで作成する。ルートマップを解除するときは、ルートマップ名を指定せず、単に「OUTROUTEMAP」と指定する。

SENDCOMMUNITY　UPDATE メッセージに COMMUNITIES 属性を含めるかどうか。同属性の具体的内容はルートマップで設定する。デフォルトは NO。

LOCAL　該当ピアとの通信に使用するローカル IP インターフェースの番号。ローカル IP インターフェースを指定した場合、本ピア宛ての BGP パケットの始点 IP アドレスとして、指定したローカル IP インターフェースの IP アドレスが使用される。省略時は NONE（ローカル IP インターフェースを使用しない。この場合、BGP パケットの始点 IP アドレスはシステムが決める）。

CLIENT　該当ピアがルートリフレクター（RR）クライアントであるかどうか。本パラメーターは、該当ピアが I-BGP ピアである場合のみ意味を持つ。該当ピアが I-BGP ピアであり、なおかつ、本パラメーターが YES の場合、本製品は該当ピアをクライアントであると見なし、ルートリフレクターとしての動作を行う（クライアントから受信した経路を他のすべてのクライアントとノンクライアントに送信する。また、ノンクライアントから受信した経路は、クライアントにだけ送信する）。NO を指定した場合は、該当ピアをノンクライアントと見なして通常の I-BGP 通信を行う。デフォルトは NO。

PRIVATEASFILTER　プライベート AS 番号（64512～65535）をフィルタリングするかどうか。本パラメーターに YES を指定した場合、該当ピアに UPDATE メッセージを送信するとき、AS_PATH 属性からプライベート AS 番号を削除した上で送信する。デフォルトは NO。

関連コマンド

ADD BGP PEER（154 ページ）

ADD BGP PEERTEMPLATE（158 ページ）
ADD IP ASPATHLIST（163 ページ）
ADD IP FILTER（169 ページ）
ADD IP LOCAL（182 ページ）
ADD IP ROUTEMAP（195 ページ）
DELETE BGP PEER（222 ページ）
DELETE BGP PEERTEMPLATE（223 ページ）
DISABLE BGP PEER（261 ページ）
ENABLE BGP PEER（291 ページ）
RESET BGP PEER（326 ページ）
SET BGP PEER（343 ページ）
SET IP LOCAL（367 ページ）
SHOW BGP PEER（418 ページ）
SHOW BGP PEERTEMPLATE（422 ページ）

SET BOOTP MAXHOPS

カテゴリー：IP / DHCP/BOOTP リレー

SET BOOTP MAXHOPS=*1..16*

解説

DHCP/BOOTP メッセージの最大転送回数を設定する。
リレーエージェントは DHCP/BOOTP パケットの hops フィールドをチェックし、その値が MAXHOPS の設定値よりも大きい場合は、同メッセージを転送せずに破棄する。デフォルトは 4。hops フィールドはルーターを越えるたびにインクリメントされる。

パラメーター

MAXHOPS　DHCP/BOOTP メッセージの最大転送回数を指定する。

関連コマンド

ADD BOOTP RELAY（161 ページ）
DELETE BOOTP RELAY（224 ページ）
DISABLE BOOTP RELAY（262 ページ）
ENABLE BOOTP RELAY（292 ページ）
PURGE BOOTP RELAY（322 ページ）
SHOW BOOTP RELAY（427 ページ）

SET DHCP

カテゴリー：IP / IP インターフェース

SET DHCP EXTENDID={**ON**|**OFF**}

解説

DHCP クライアントとしての動作時に用いる Client ID の形式を設定する。
本製品のデフォルト状態（EXTENDID=OFF）では、DHCP Discover や Request メッセージの Client ID として、スイッチ本体の MAC アドレス（SHOW SWITCH コマンドで確認可能）を使用する。
複数の VLAN インターフェースを DHCP クライアントとして動作させる場合であっても Client ID は同じものが使われるため、複数インターフェースが同じ DHCP サーバーを利用する場合は、サーバーが各インターフェースを同一クライアントと見なしてしまい、同じ IP アドレスが割り当てられてしまう。
複数の VLAN インターフェースが同一の DHCP サーバーを利用する場合は、本コマンドで EXTENDID=ON に設定し、各インターフェースが異なる Client ID を送信するようにすること。

パラメーター

EXTENDID　DHCP メッセージの Client ID として、標準形式（インターフェースの MAC アドレス）を使うか、拡張形式（インターフェース名ごとに異なる ID）を使うかを指定する。OFF なら標準形式、ON なら拡張形式を使う。デフォルトは OFF。

関連コマンド

ADD IP INTERFACE（179 ページ）
SET IP INTERFACE（364 ページ）
SHOW DHCP（「DHCP サーバー」の 32 ページ）
SHOW IP INTERFACE（458 ページ）

SET IP ARP

カテゴリー：IP / ARP

SET IP ARP=*ipadd* INTERFACE=*interface* ETHERNET=*macadd* [PORT=*port-num*]

ipadd: IP アドレス
interface: IP インターフェース名（eth0、ppp0 など）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）
port-num: スイッチポート番号（1〜）

解説

スタティック ARP エントリーの内容を変更する。

パラメーター

ARP　IP アドレス
INTERFACE　IP インターフェース
ETHERNET　Ethernet 物理（MAC）アドレス
PORT　スイッチポート番号。INTERFACE に VLAN を指定した場合のみ有効。

例

■IP アドレス 192.168.100.20 のホストの ARP エントリーを修正する。

```
SET IP ARP=192.168.100.20 INTERFACE=eth0 ETHERNET=00-00-F4-FE-DC-BA
```

関連コマンド

ADD IP ARP（162 ページ）
DELETE IP ARP（225 ページ）
SHOW IP ARP（432 ページ）

SET IP ARP REFRESHARP

カテゴリー：IP / ARP

SET IP ARP REFRESHARP={**ON**|**YES**|**TRUE**|**OFF**|**NO**|**FALSE**}

解説

ARP エントリーのリフレッシュを設定する。

パラメーター

REFRESHARP　キャッシュ内の IP ARP エントリーをリフレッシュし、エントリー使用時にエージングタイマーをリスタートするかどうか。デフォルトは ON。

関連コマンド

ADD IP ARP（162 ページ）
DELETE IP ARP（225 ページ）
ENABLE IP ARP AGEPOLL
SET IP ARP（351 ページ）
SET IP ARP TIMEOUT（353 ページ）
SHOW IP ARP（432 ページ）

SET IP ARP TIMEOUT

カテゴリー：IP / ARP

SET IP ARP TIMEOUT=*1..1023*

解説

ARP タイムアウトの決定に用いる乗数を変更する。

パラメーター

TIMEOUT　ARP タイムアウト（可変）の範囲を決定する乗数（正の整数）。ARP キャッシュのタイムアウトは、(256 * TIMEOUT) 〜 (512 * TIMEOUT) の可変値を持つ。デフォルトの乗数は 4 なので、ARP タイムアウトのデフォルト値は 1024〜2096 秒となる。たとえば、TIMEOUT に 2 を指定した場合、ARP タイムアウトは 512〜1024 秒の範囲となる。デフォルトは 4。

関連コマンド

ADD IP ARP（162 ページ）
DELETE IP ARP（225 ページ）
SET IP ARP（351 ページ）
SHOW IP（429 ページ）
SHOW IP ARP（432 ページ）

SET IP ARPWAITTIMEOUT

カテゴリー：IP / ARP

SET IP ARPWAITTIMEOUT=*1..30*

解説

ARP 要求に対する応答待ち時間を変更する。
ARP Request 送信後、この時間内に ARP Reply を受け取れなかった場合は、ARP 要求がタイムアウトしたと見なす。

パラメーター

ARPWAITTIMEOUT　ARP 要求に対する応答待ち時間（秒）。デフォルトは 1。

SET IP AUTONOMOUS

カテゴリー：IP / 経路制御（BGP-4）

SET IP AUTONOMOUS=*1..65534*

解説

自 AS（Autonomous System）番号を設定する。

パラメーター

AUTONOMOUS　AS 番号

備考・注意事項

自 AS 番号は SHOW IP コマンドで確認できる（「Autonomous System Number」欄）。
AS コンフェデレーションを構成するときは、自 AS 番号としてサブ AS 番号を設定する。コンフェデレーション AS 番号は SET BGP コマンドの CONFEDERATIONID パラメーターで指定する。

関連コマンド

ADD BGP PEER（154 ページ）
DELETE BGP PEER（222 ページ）
DISABLE BGP PEER（261 ページ）
ENABLE BGP PEER（291 ページ）
SHOW BGP PEER（418 ページ）
SHOW IP（429 ページ）

SET IP DNS

カテゴリー：IP / 名前解決

SET IP DNS [DOMAIN={ANY|*domain-name*}] {**INTERFACE=*interface***|
[PRIMARY=*ipadd*] [SECONDARY=*ipadd*]}

domain-name: ドメイン名
interface: IP インターフェース名（eth0、ppp0 など）
ipadd: IP アドレス

解説

DNS サーバーリストの内容を変更する。

パラメーター

DOMAIN ドメイン名。特定ドメインの名前解決にだけ指定のサーバーを使いたいような場合に使う。本パラメーターで指定したドメインの問い合わせは、同一コマンドラインで指定したサーバーに送られる。本パラメーターを省略した場合（および ANY を指定した場合）、指定したサーバーは、問い合わせがどのドメインにも一致しないときに用いられるデフォルトサーバーとなる。なお、特定ドメイン用のサーバーを登録するときは、あらかじめデフォルトサーバーを設定しておくこと。

INTERFACE IP インターフェース名。DNS サーバーアドレスを動的取得する場合に、アドレスを取得するインターフェースを指定する。ダイヤルアップ PPP の場合は PPP インターフェース、DHCP でアドレスを取得する場合は Ethernet か VLAN インターフェースを指定する。

PRIMARY プライマリー DNS サーバーの IP アドレス

SECONDARY セカンダリー DNS サーバーの IP アドレス

備考・注意事項

MIB 変数 sysName に本製品のドメイン名（FQDN）が設定されている場合、sysName に基づくドメイン名が DNS 検索に使用される。たとえば、sysName に「white.joge.xxx」が設定されている場合、コマンドラインでホスト名「black」だけを指定すると、「black.joge.xxx」に対する検索が実施される。

関連コマンド

ADD IP DNS（167 ページ）
DELETE IP DNS（228 ページ）
DISABLE IP DNSRELAY（266 ページ）
ENABLE IP DNSRELAY（297 ページ）
SET IP DNS CACHE（358 ページ）
SHOW IP DNS（445 ページ）

SHOW IP DNS CACHE（447 ページ）
TELNET（「運用・管理」の 380 ページ）

SET IP DNS CACHE

カテゴリー：IP / 名前解決

SET IP DNS CACHE [SIZE=*0..1000*] [TIMEOUT=*1..60*]

解説

DNS キャッシュに保持するエントリーの最大数と、キャッシュエントリーの有効期限を変更する。
デフォルトではキャッシュ保持数が 0 に設定されているため、DNS キャッシュ機能を使用する場合は必ず本コマンドでキャッシュ保持数を 1 以上に変更する必要がある。

パラメーター

SIZE DNS キャッシュに保持するエントリーの最大数。エントリー数が最大値に達している場合は、新規エントリーの追加時に最も古いエントリーが削除される。0 の場合はキャッシュしない。デフォルトは 0。

TIMEOUT DNS キャッシュエントリーの有効期限。キャッシュに登録後、有効期限内に更新されなかったエントリーは削除される。デフォルトは 30 分。

例

■DNS キャッシュサイズを 100 個に設定する。

```
SET IP DNS CACHE SIZE=100
```

備考・注意事項

DNS キャッシュエントリーはルーターのメモリーを消費するので、最大保持数を不必要に大きくしないこと。メモリーの消費量は、100 エントリーで約 30KB が目安。

関連コマンド

ADD IP DNS（167 ページ）
DELETE IP DNS（228 ページ）
DISABLE IP DNSRELAY（266 ページ）
ENABLE IP DNSRELAY（297 ページ）
SET IP DNS（356 ページ）
SHOW IP DNS（445 ページ）
SHOW IP DNS CACHE（447 ページ）
TELNET（「運用・管理」の 380 ページ）

SET IP DNSRELAY

カテゴリー：IP / DNS リレー

SET IP DNSRELAY INTERFACE={***interface***|**NONE**}

interface: IP インターフェース名（eth0、ppp0 など）

解説

DNS サーバーアドレスを取得するインターフェースを指定する。
通常は、ダイヤルアップ PPP インターフェースなど、DNS サーバーのアドレスを動的に取得するような環境で DNS リレー機能を使うときに指定する。

パラメーター

INTERFACE　IP インターフェース名

関連コマンド

ADD IP DNS（167 ページ）
DELETE IP DNS（228 ページ）
DISABLE IP DNSRELAY（266 ページ）
ENABLE IP DNSRELAY（297 ページ）
SET IP DNS（356 ページ）
SET IP DNS CACHE（358 ページ）
SHOW IP（429 ページ）
SHOW IP DNS（445 ページ）
SHOW IP DNS CACHE（447 ページ）

SET IP FILTER

カテゴリー：IP / IP フィルター

SET IP FILTER=*filter-id* ENTRY=*entry-id* [{ACTION={INCLUDE|EXCLUDE}|POLICY=*0..15*|PRIORITY=P0..P7}] [SOURCE=*ipadd*] [SMASK=*ipadd*] [SPORT={*port-name*|[*port*]:[*port*]}] [DESTINATION=*ipadd* [DMASK=*ipadd*]] [DPORT={*port-name*|[*port*]:[*port*]}] [ICMPCODE={*icmp-code-name*|*icmp-code-id*}] [ICMPTYPE={*icmp-type-name*|*icmp-type-id*}] [LOG={*4..1600*|DUMP|HEADER|NONE}] [OPTIONS={YES|NO}] [PROTOCOL={*protocol*|ANY|ICMP|OSPF|TCP|UDP}] [SESSION={ANY|ESTABLISHED|START}] [SIZE=*size*]

filter-id: フィルター番号（0〜999）
entry-id: エントリー番号（1〜3071）
ipadd: IP アドレスまたはネットマスク
port-name: サービス名
port: TCP/UDP ポート番号（0〜65535）
icmp-code-name: ICMP コード名
icmp-code-id: ICMP コード番号（0〜65535）
icmp-type-name: ICMP メッセージ名
icmp-type-id: ICMP メッセージ番号（0〜65535）
protocol: IP プロトコル番号（0〜255）
size: データグラム長

解説

IP フィルターエントリー（ルール）の設定を変更する。（フィルターの種類の確認は、SHOW IP FILTER コマンドで行う。）

パラメーター

FILTER　フィルター番号。

ENTRY　エントリー番号。この番号は可変なので、必ず SHOW IP FILTER コマンドで確認してから指定すること（Ent.フィールド）。

ACTION　トラフィックフィルター（フィルター番号 0〜99）、プレフィックスフィルター（フィルター番号 300〜399）の動作を指定する。INCLUDE はマッチしたパケット、プレフィックスを通過させる。EXCLUDE はマッチしたパケット、プレフィックスを破棄する。POLICY、PRIORITY とは同時に指定できない

POLICY　ポリシーフィルター（フィルター番号 100〜199）において、マッチしたパケットに割り当てる経路選択ポリシー（サービスタイプ）を指定する。経路選択ポリシーの範囲は 0〜7 だが、POLICY パラメーターには 0〜15 の範囲を指定することができる。0〜7 を指定した場合は、指定値がそのまま経路選択ポリシー値となる。8〜15 を指定した場合は、経路選択ポリシーとして「POLICY - 8」を割り当て、さらに、パケットの TOS ビット（D、T、R）を「POLICY - 8」に書き換える。詳細は ADD IP FILTER コマンドの表を参照。経路表を検索するときは、本フィルターによって割り当てられた経路

選択ポリシー値と経路エントリーのサービスタイプがつきあわされ、一致する経路が最優先で使用される。フィルターにマッチしなかったパケットの経路選択ポリシーは「0」。ACTION、PRIORITYとは同時に指定できない。

PRIORITY プライオリティーフィルター（フィルター番号 200〜299）において、マッチしたパケットを出力するときの優先度を P0（最高）〜P7（最低）で指定する。フィルターにマッチしなかった通常パケットの優先度は「P5」。ACTION、POLICY とは同時に指定できない。また、Eth/PPPoE インターフェースでこの機能が動作するのは、受信インターフェースの速度の合計より送信インターフェースの速度の合計が小さい場合。（例 1）受信インターフェース：100Mbps × 1、送信インターフェース：10Mbps × 1。（例 2）受信インターフェース：100Mbps × 2、送信インターフェース：100Mbps × 1。

SOURCE 始点 IP アドレスまたはネットワークプレフィックス。0.0.0.0 はすべてのアドレスを意味する。

SMASK SOURCE に対応するマスク値。SOURCE と組み合わせて、ホストアドレス/ネットワークアドレスの区別、または、プレフィックス長（プレフィックスフィルター）を指定する。SOURCE で指定した IP アドレスがネットワークアドレスなら適切な長さのネットマスクを、ホストアドレスなら 255.255.255.255 を指定する。また、SOURCE に 0.0.0.0（ANY）を指定した場合は 0.0.0.0 を指定する（省略可）。

SPORT 始点 TCP/UDP ポートあるいは定義済みのサービス名。本パラメーター指定時は PROTOCOL パラメーターに TCP か UDP を指定する必要がある。low:high の形式で low〜high の範囲指定も可能。「low:」は low〜65535 の意味、「:high」は 0〜high の意味になる。デフォルトは ANY（すべてのポート）。

DESTINATION 終点 IP アドレス。デフォルトは 0.0.0.0（すべて）

DMASK 終点 IP アドレスに対応するマスク値。DESTINATION と組み合わせてホストアドレスまたはネットワークアドレスを指定する。省略時は 255.255.255.255（ホストマスク）とみなされる。

DPORT 終点 TCP/UDP ポートあるいは定義済みのサービス名。本パラメーター指定時は PROTOCOL パラメーターに TCP か UDP を指定する必要がある。low:high の形式で low〜high の範囲指定も可能。「low:」は low〜65535 の意味、「:high」は 0〜high の意味になる。デフォルトは ANY（すべてのポート）。

ICMPCODE ICMP コード番号または定義済みのコード名。PROTOCOL=ICMP の場合のみ有効

ICMPTYPE ICMP メッセージ番号または定義済みのメッセージ名。PROTOCOL=ICMP の場合のみ有効

LOG このエントリーにマッチしたパケットの情報をログに記録するかどうか、記録する場合はどの情報を記録するかを指定する。NONE はログに記録しないことを意味する。4〜1600 の数値を指定した場合は、フィルター番号、エントリー番号、IP ヘッダー情報（IP アドレス、プロトコル、ポート番号、サイズ）が「IPFIL/PASS」（INCLUDE アクションの場合）または「IPFIL/FAIL」（EXCLUDE アクションの場合）タイプのメッセージとして記録される。これに加え、TCP、UDP、ICMP の場合はデータ部分の先頭 4〜1600 バイトが、その他プロトコルの場合は IP データの先頭 4〜1600 バイトが、「IPFIL/DUMP」タイプのメッセージとして記録される。DUMP は LOG=32 と同じ動作となる。HEADER を指定した場合は、フィルター番号、エントリー番号、IP ヘッダー情報のみが記録される。デフォルトは NONE（記録しない）。

OPTIONS パケットが IP オプション付きかどうか。

PROTOCOL IP プロトコル番号または定義済みのプロトコル名。DPORT、SPORT を指定するときは、PROTOCOL に TCP か UDP を指定する必要がある。また、ICMPCODE、ICMPTYPE 指定時は ICMP を指定する。

SESSION　TCP のセッション制御情報。ANY はすべての TCP パケット、START は接続開始パケット（SYN=1、ACK=0）、ESTABLISHED は接続済みパケット（ACK=1）を意味する。

SIZE　再構成後のデータグラムサイズ。パケット（フラグメント）ごとに length + offset * 8 <= SIZE がチェックされ、真ならマッチし、偽ならマッチしない。length と offset は、それぞれ IP ヘッダーの Length フィールドと Fragment Offset フィールドを示す。

関連コマンド

ADD BGP PEER（154 ページ）
ADD IP FILTER（169 ページ）
ADD IP INTERFACE（179 ページ）
DELETE IP FILTER（230 ページ）
SET BGP PEER（343 ページ）
SET IP INTERFACE（364 ページ）
SHOW IP FILTER（449 ページ）

SET IP HOST

カテゴリー：IP / 名前解決

SET IP HOST=*hostname* IPADDRESS=*ipadd*

ipadd: IP アドレス
hostname: ホスト名

解説

IP ホストテーブルエントリーの IP アドレスを変更する。

パラメーター

HOST　ホスト名
IPADDRESS　IP アドレス

例

■ホスト名「bulbul」に対応する IP アドレスを 192.168.1.5 に変更する。

```
SET IP HOST=bulbul IPADDRESS=192.168.1.5
```

関連コマンド

ADD IP DNS（167 ページ）
ADD IP HOST（178 ページ）
DELETE IP DNS（228 ページ）
DELETE IP HOST（232 ページ）
DISABLE IP DNSRELAY（266 ページ）
ENABLE IP DNSRELAY（297 ページ）
FINGER
PING（319 ページ）
SET IP DNS（356 ページ）
SET IP DNS CACHE（358 ページ）
SHOW IP DNS（445 ページ）
SHOW IP DNS CACHE（447 ページ）
SHOW IP HOST（455 ページ）
TELNET（「運用・管理」の 380 ページ）

SET IP INTERFACE

カテゴリー：IP / IP インターフェース

SET IP INTERFACE=*interface* [IPADDRESS={*ipadd*|DHCP}] [MASK=*ipadd*]
[BROADCAST={*0*|*1*}] [DIRECTEDBROADCAST={YES|NO|ON|OFF}] [FILTER={*0..99*|NONE}] [FRAGMENT={YES|NO}] [MULTICAST={OFF|SEND|RECEIVE|BOTH|ON}]
[OSPFMETRIC=*1..65534*] [POLICYFILTER={*100..199*|NONE}]
[PRIORITYFILTER={*200..299*|NONE}] [PROXYARP={ON|OFF}] [RIPMETRIC=*1..16*]
[VJC={ON|OFF}]

interface: IP インターフェース名（eth0、ppp0 など）
ipadd: IP アドレスまたはネットマスク

解説

IP インターフェースの設定を変更する。
IP フィルターを既存インターフェースに適用するときにも本コマンドを使う。

パラメーター

INTERFACE　下位のインターフェースを指定する。1 つのインターフェースに複数の IP アドレスを設定するとき（マルチホーミング）は、vlan1-0、vlan1-1、vlan1-2 のように、インターフェース名の後にハイフンと論理インターフェース番号（0〜15）を付ける。論理インターフェース番号を省略したとき（例：vlan1）は「0」を指定したものと見なされる（例：vlan1-0 として扱われる）。

IPADDRESS　インターフェースに割り当てる IP アドレス。DHCP を指定した場合は、DHCP サーバーから IP 設定情報を取得し自動設定する。DHCP で取得できる情報は、IP アドレス、ネットマスク、DNS サーバーアドレス（プライマリー、セカンダリー）、デフォルト経路、ドメイン名。DHCP を使う場合は、あらかじめ ENABLE IP REMOTEASSIGN コマンドを実行して、IP アドレスの動的設定を有効にしておく必要がある。

MASK　サブネットマスク。省略時は IP アドレスのクラス標準マスクが用いられる。DHCP を使う場合は自動的に設定されるので指定しないこと。

BROADCAST　IP ブロードキャストアドレスをオール 1 で表すか、オール 0 で表すかを示す。通常は 1（デフォルト）。

DIRECTEDBROADCAST　この IP インターフェース配下のネットワークに対するディレクティドブロードキャストパケットを転送するかどうかを示す。デフォルトは NO。

FILTER　このインターフェースで受信した IP パケットに適用するトラフィックフィルターの番号。トラフィックフィルターのアクションは受信直後に適用される。デフォルトは NONE。IP トラフィックフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 0〜99）。

FRAGMENT　このインターフェースから送出するパケットがインターフェースの MTU よりも大きい場合の動作を指定する。NO（デフォルト）を指定した場合、DF（Don't Fragment）ビットの指示通り、DF ビットが立っているパケットはフラグメント化せずに破棄する。YES を指定した場合は、DF

ビットを無視してフラグメント化する。

MULTICAST IP マルチキャストパケットの扱いを指定する。OFF を指定した場合は送受信とも行わない。ON または BOTH を指定した場合は送受信を行う。SEND は送信のみ、RECEIVE は受信のみ行うことを示す。デフォルトは RECEIVE。マルチホーミングを使用している場合、本パラメーターの設定はおおもとの IP インターフェース全体に適用される。また、マルチキャスト経路制御プロトコル DVMRP を使用している場合、本パラメーターは意味を持たない。

OSPFMETRIC OSPF が用いる本インターフェースのメトリック（通過コスト）。デフォルトは 1

POLICYFILTER このインターフェースで受信した IP パケットに適用するポリシーフィルターの番号。ポリシーフィルターによって設定された経路選択ポリシー（サービスタイプ）は経路表の検索時に使用される。デフォルトは NONE。IP ポリシーフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 100～199）。

PRIORITYFILTER このインターフェースから送信する IP パケットに適用するプライオリティーフィルターの番号。IP パケットの出力は、プライオリティーフィルターによって設定された優先度に基づいて行われる。デフォルトは NONE。IP プライオリティーフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 200～299）。

PROXYARP プロキシー ARP（RFC1027）の有効・無効。デフォルトは ON。

RIPMETRIC RIP が用いる本インターフェースのメトリック（通過コスト）。METRIC も同じ意味。デフォルトは 1

VJC PPP インターフェース上の IP インターフェースで Van Jacobson の TCP/IP ヘッダー圧縮（VJ 圧縮）を使用するかどうかを指定する。この設定は PPP インターフェース上のすべての IP インターフェースに適用される。VJ 圧縮は、48Kbps 程度までの低速な回線上で効果を発揮する。64Kbps 以上の回線ではかえって効率が落ちるので注意が必要。また、MP（Multilink PPP）を使用している場合は ON にしないこと。デフォルトは OFF。

例

■vlan1 の IP アドレスを変更する。

```
SET IP INT=vlan1 IP=10.1.1.1 MASK=255.255.255.0
```

■ppp0 に IP トラフィックフィルター「0」を適用する。

```
SET IP INT=ppp0 FILTER=0
```

関連コマンド

ADD IP INTERFACE（179 ページ）
DELETE IP INTERFACE（233 ページ）
DISABLE IP INTERFACE（272 ページ）
ENABLE IP INTERFACE（303 ページ）
RESET IP INTERFACE（329 ページ）

SHOW IP INTERFACE（458 ページ）

SET IP LOCAL

カテゴリー：IP / IP インターフェース

SET IP LOCAL [IPADDRESS=*ipadd*] [FILTER={*filter-id*|NONE}]
[POLICYFILTER={*filter-id*|NONE}] [PRIORITYFILTER={*filter-id*|NONE}]

filter-id: フィルター番号（0〜299）
ipadd: IP アドレス

解説

ローカル IP インターフェースの設定を変更する。
ローカル IP インターフェースは、IP モジュール自体をあらわす仮想的なインターフェースで、本製品自身がパケットを送信するときの始点インターフェース（始点アドレス）として使われる。
ローカル IP インターフェースに割り当てたアドレスは、本製品自身が送信する RIP、OSPF、PING、NTP パケット等の始点アドレスとして使用される可能性がある。本製品が送信する IP パケットの始点 IP アドレスは次のようにして決定される。
1. コマンド等で始点アドレスまたは始点インターフェースを明示的に指定した場合は、そのアドレスが使用される（PING コマンドの SIPADDRESS パラメーターなど）
2. 1 に該当せず、なおかつ、ローカル IP インターフェースに IP アドレスが割り当てられている場合は、そのアドレスが使用される
3. 1、2 ともに当てはまらない場合、パケットを送出するインターフェースの IP アドレスが始点アドレスとして使用される。ただし、送出インターフェースが Unnumbered の場合は、一番最初に設定された IP アドレス（最初に ADD IP INTERFACE コマンドでアドレスを設定されたインターフェースのアドレス）が使用される（注：PPPoE LAN 型接続の WAN 側インターフェースは、完全な Unnumbered ではないので注意が必要）

パラメーター

IPADDRESS　IP アドレス
FILTER　トラフィックフィルター番号
POLICYFILTER　ポリシーフィルター番号
PRIORITYFILTER　プライオリティーフィルター番号

関連コマンド

ADD IP INTERFACE（179 ページ）
DELETE IP INTERFACE（233 ページ）
SET IP INTERFACE（364 ページ）
SHOW IP INTERFACE（458 ページ）

SET IP NAT MAXFRAGMENTS

カテゴリー：IP / レンジ NAT

SET IP NAT MAXFRAGMENTS=*8..50*

解説

IP NAT（レンジ NAT）モジュールにフラグメント化パケットを透過するよう設定している場合（ENABLE IP NAT FRAGMENT コマンド）、許可するフラグメントの最大数を設定する。

パラメーター

MAXFRAGMENTS 許可するフラグメントの最大数。フラグメント化パケット透過に設定している場合であっても、本パラメーターの値より多くのフラグメントに分割されているパケットは破棄される。デフォルトは 20。フラグメント化パケット不透過に設定している場合（デフォルト）は、再構成後の IP データサイズ（L4 パケットサイズ）が 1780 バイトを越えるか、フラグメントの数が 8 個を超えるパケットは破棄される。

関連コマンド

DISABLE IP NAT FRAGMENT（274 ページ）
ENABLE IP NAT FRAGMENT（306 ページ）
SHOW IP NAT（461 ページ）

SET IP RIP

カテゴリー：IP / 経路制御（RIP）

```
SET IP RIP INTERFACE=interface [IP=ipadd] [SEND={NONE|RIP1|RIP2|
   COMPATIBLE}] [RECEIVE={NONE|RIP1|RIP2|BOTH}] [NEXTHOP=ipadd]
   [DEMAND={YES|NO}] [AUTHENTICATION={NONE|PASSWORD|MD5}]
   [PASSWORD=password] [STATICEXPORT={YES|NO}]
```

interface: IP インターフェース名（eth0、ppp0 など）
ipadd: IP アドレス
password: パスワード（1〜16 文字）

解説

指定した IP インターフェースにおける RIP の設定を変更する。

パラメーター

INTERFACE　RIP パケットの送受信を行う IP インターフェース

IP　RIP ルーターの IP アドレス。本パラメーター指定時は、INTERFACE で受信した RIP パケットのうち、始点アドレスが IP と一致するものだけを受け入れる。また、RIP パケット送信時には、IP で指定されたアドレス宛てにユニキャストする。一方、本パラメーター省略時は、受信した RIP パケットの始点アドレスをチェックせず、RIP パケット送信時には、ブロードキャスト（SEND=RIP1 のとき）、または、マルチキャスト（SEND=RIP2 または COMPATIBLE のとき）する。

SEND　送信する RIP パケットのフォーマット。NONE は送信しない。RIP1 はバージョン 1 形式、RIP2 はバージョン 2 形式で送信する。COMPATIBLE はバージョン 2 形式で送信するが、RIP1 互換の経路エントリー（ナチュラルサブネットマスク（クラス標準マスク）を使用したネットワークアドレス）しか送信しない。デフォルトは RIP1。

RECEIVE　受信する RIP パケットのフォーマット。NONE は受信しない。RIP1 はバージョン 1 形式のみ受信。RIP2 はバージョン 2 形式のみ受信。BOTH はバージョン 1、2 ともに受信するが、ナチュラルサブネットマスク（クラス標準マスク）を使用したネットワークアドレスしか受信できない。デフォルトは BOTH。

NEXTHOP　RIP バージョン 2 パケットの Next Hop フィールドにセットするネクストホップ IP アドレス。本パラメーターを使用するには、SEND パラメーターに RIP2 か COMPATIBLE を指定し、IP パラメーターに RIP ルーターのユニキャスト IP アドレスを指定する必要がある。省略時は 0.0.0.0（自分自身がネクストホップ）

DEMAND　トリガーアップデート（RFC1582）を使用するかどうか。デフォルトは NO。

AUTHENTICATION　RIP Version2 使用時の認証方式。PASSWORD は平文テキストのパスワード、MD5 は鍵付き MD5 によるメッセージダイジェスト、NONE は認証を行わない。デフォルトは NONE。

PASSWORD　RIP Version2 で認証を行うときのパスワードまたはキー。AUTHENTICATION に PASS-

WORD か MD5 を指定した場合にのみ有効

STATICEXPORT　スタティック経路を RIP で通知するかどうか。デフォルトは YES（通知する）。

例

■vlan1 で送受信する RIP パケットのフォーマットを RIP Version1 に変更する。

```
SET IP RIP INT=vlan1 SEND=RIP1 RECEIVE=RIP1
```

関連コマンド

ADD IP RIP（187 ページ）
DELETE IP RIP（236 ページ）
SET IP RIPTIMER（371 ページ）
SHOW IP RIP（468 ページ）

SET IP RIPTIMER

カテゴリー：IP / 経路制御（RIP）

SET IP RIPTIMER [FLUSH=*seconds*] [HOLDDOWN=*seconds*] [INVALID=*seconds*] [UPDATE=*seconds*]

seconds: 時間（秒）

解説

RIP のタイマー設定を変更する。

パラメーター

FLUSH　最後の更新パケット受信から経路情報が削除されるまでの期間（秒）。FLUSH >= INVALID + HOLDDOWN になるようにする。デフォルトは 300 秒。

HOLDDOWN　ホールドダウンタイム。ルートタイムアウトにより無効（メトリック 16）となった経路エントリーを無効状態のまま保持する期間（秒）。この期間中は、該当経路の更新情報を受け取ってもエントリーを更新せず、無効状態のまま止めおく。デフォルトは 120 秒。

INVALID　ルートタイムアウト。経路が更新されなくなってから、該当する経路情報を無効とみなす（メトリックを 16 にする）までの期間（秒）。デフォルトは 180 秒。

UPDATE　アップデートタイマー。RIP 更新パケットの送信間隔（秒）。デフォルトは 30 秒。

関連コマンド

SET IP RIP（369 ページ）
SHOW IP RIP（468 ページ）
SHOW IP RIPTIMER（472 ページ）

SET IP ROUTE

カテゴリー：IP / 経路制御（スタティック）

SET IP ROUTE=*ipadd* INTERFACE=*interface* MASK=*ipadd* NEXTHOP=*ipadd*
[DLCI=*dlci*] [METRIC=*1..16*] [METRIC1=*1..16*] [METRIC2=*1..65535*]
[POLICY=*0..7*] [PREFERENCE=*0..65535*]

interface: IP インターフェース名（eth0、ppp0 など）
ipadd: IP アドレスまたはネットマスク
dlci: DLCI（0〜1023）

解説

スタティック経路のメトリックやサービスタイプ、優先度を変更する。

パラメーター

ROUTE 宛先ネットワークの IP アドレス。MASK と組み合わせて指定する。デフォルト経路の場合は 0.0.0.0 を指定する

INTERFACE 本経路宛てのパケットを送出する IP インターフェース

MASK 宛先ネットワークのネットマスク。デフォルト経路のマスクは 0.0.0.0 とする

NEXTHOP ネクストホップルーターの IP アドレス。ダイレクト経路の場合は 0.0.0.0 を指定する。また、PPP インターフェース側に向けた経路の場合も 0.0.0.0 を指定できる。

DLCI フレームリレー論理パス番号（DLCI）。INTERFACE にフレームリレーインターフェースを指定した場合に必要。

METRIC RIP が使用するメトリック。METRIC1 パラメーターも同じ意味。省略時は 1

METRIC1 RIP が使用するメトリック。METRIC パラメーターも同じ意味。省略時は 1

METRIC2 OSPF が使用するメトリック。省略時は 1

POLICY 本経路のサービスタイプ（TOS）。省略時は 0

PREFERENCE 経路選択時の優先度。小さいほど優先度が高い。複数の経路が存在するときはもっとも優先度の高い経路が使用される。省略時の値はデフォルト経路（0.0.0.0）が 360、その他のスタティック経路が 60。なお、インターフェース経路は優先度 0、RIP 経路は優先度 100、BGP 経路は優先度 170 となる。また、経路制御プロトコルによって学習した経路の優先度は、SET IP ROUTE PREFERENCE コマンドで変更できる（確認は SHOW IP ROUTE PREFERENCE コマンドで行う）。

関連コマンド

ADD IP ROUTE（189 ページ）
DELETE IP ROUTE（237 ページ）
SET IP ROUTE PREFERENCE（376 ページ）
SHOW IP ROUTE（473 ページ）

SHOW IP ROUTE PREFERENCE（478 ページ）

SET IP ROUTE FILTER

カテゴリー：IP / 経路制御フィルター

SET IP ROUTE FILTER=*entry-id* IP=*ipadd* MASK=*ipadd* ACTION={INCLUDE|EXCLUDE} [DIRECTION={RECEIVE|SEND|BOTH}] [INTERFACE=*interface*] [NEXTHOP=*ipadd*] [POLICY=*0..7*] [PROTOCOL={ANY|RIP|OSPF}]

entry-id: エントリー番号（1〜100）
interface: IP インターフェース名（eth0、ppp0 など）
ipadd: IP アドレスまたはネットマスク

解説

IP ルートフィルターエントリーの設定内容を変更する。

パラメーター

FILTER　フィルターエントリー番号。この番号は可変なので、必ず SHOW IP ROUTE FILTER コマンドで確認してから指定すること（Ent.フィールド）。

IP　ネットワークアドレスを指定する。バイト単位でワイルドカード（*）の指定が可能。たとえば、「192.168.*.*」は「192.168」で始まるすべてのアドレスにマッチする。「192.168.12*.*」のような指定は無効。

MASK　ネットマスクを指定。IP パラメーター同様、ワイルドカードを使用可能。

ACTION　条件にマッチした経路情報に対するアクションを指定する。INCLUDE は経路情報をメッセージに含める（送信時）あるいはルーティングテーブルに追加する（受信時）。EXCLUDE は経路情報をメッセージに含めない（送信時）あるいはルーティングテーブルに追加しない（受信時）。

DIRECTION　経路情報の送信時（SEND）にフィルターをかけるか、受信時（RECEIVE）にかけるか、あるいは、送信時受信時とも（BOTH）かを指定する。

INTERFACE　フィルターを適用する IP インターフェースを指定する。指定時は、該当インターフェースで送受信される経路情報に対してのみフィルターが適用される。

NEXTHOP　ネクストホップルーターの IP アドレス。本パラメーターを指定したときは、ネクストホップが一致する経路エントリーだけがフィルターの適用対象となる。

POLICY　フィルターの適用対象となる経路エントリーのサービスタイプ（TOS）値を指定する。無指定時はすべてのサービスタイプが対象。

PROTOCOL　フィルターの適用対象となるルーティングプロトコルを指定する。デフォルトは ANY（すべて）。

関連コマンド

ADD IP ROUTE FILTER（191 ページ）
DELETE IP ROUTE FILTER（238 ページ）

SHOW IP ROUTE FILTER（476 ページ）

SET IP ROUTE PREFERENCE

カテゴリー：IP / 経路制御（スタティック）

SET IP ROUTE PREFERENCE={**DEFAULT**|***1..65535***} **PROTOCOL=**{**BGP-EXT**|**BGP-INT**|
OSPF-EXT1|**OSPF-EXT2**|**OSPF-INTER**|**OSPF-INTRA**|**OSPF-OTHER**|**RIP**}

解説

経路制御プロトコルによって学習した経路の優先度（preference）を変更する。
本製品は、特定宛先への経路が複数存在する場合、もっとも優先度の小さい経路を選択する。また、同じ優先度を持つ経路が複数存在する場合は、ネットマスクがもっとも長い経路を選択する。
本コマンドの効果は、コマンド実行後に学習した経路だけでなく、すでに学習済みの経路にも反映される。

パラメーター

PREFERENCE　経路選択時の優先度。小さいほど優先度が高い。DEFAULT を指定した場合は、該当経路種別のデフォルト値に設定される。

PROTOCOL　経路種別。詳細は別表を参照。

経路種別	本コマンドでの名称	デフォルト優先度
インターフェース経路	—	0
OSPF エリア内経路	OSPF-INTRA	10
OSPF エリア間経路	OSPF-INTER	11
スタティック経路	—	60
RIP 経路	RIP	100
OSPF AS 外部経路（タイプ 1）	OSPF-EXT1	150
OSPF AS 外部経路（タイプ 2）	OSPF-EXT2	151
OSPF その他経路	OSPF-OTHER	152
BGP-4 AS 内部（I-BGP）経路	BGP-INT	170
BGP-4 AS 外部（E-BGP）経路	BGP-EXT	170
デフォルト経路	—	360

表 29: 各種経路のデフォルト優先度

備考・注意事項

スタティック経路、デフォルト経路の優先度は、ADD IP ROUTE コマンド、SET IP ROUTE コマンドの PREFERENCE パラメーターで設定する。

関連コマンド

SHOW IP ROUTE（473 ページ）
SHOW IP ROUTE PREFERENCE（478 ページ）

SET IP ROUTE TEMPLATE

カテゴリー：IP / 経路制御

SET IP ROUTE TEMPLATE=*template* [NEXTHOP=*ipadd*] [METRIC=*1..16*]
[METRIC1=*1..16*] [METRIC2=*1..65535*] [POLICY=*0..7*] [PREFERENCE=*0..65535*]

template: ルートテンプレート名（1〜31 文字。大文字小文字を区別しない）
ipadd: IP アドレス

解説

IP ルートテンプレートの設定を変更する。

パラメーター

TEMPLATE　IP ルートテンプレート名
NEXTHOP　ネクストホップルーターの IP アドレス。ダイレクト経路の場合は 0.0.0.0 を指定する。また、PPP インターフェース側に向けた経路の場合も 0.0.0.0 を指定できる。
METRIC　RIP が使用するメトリック。METRIC1 パラメーターも同じ意味。省略時は 1
METRIC1　RIP が使用するメトリック。METRIC パラメーターも同じ意味。省略時は 1
METRIC2　OSPF が使用するメトリック。省略時は 1
POLICY　本経路のサービスタイプ（TOS）。省略時は 0
PREFERENCE　経路選択時の優先度。小さいほど優先度が高い。複数の経路が存在するときはもっとも優先度の高い経路が使用される。省略時の値はデフォルト経路（0.0.0.0）が 360、その他のスタティック経路が 60。なお、インターフェース経路は優先度 0、RIP 経路は優先度 100、BGP 経路は優先度 170 となる。

関連コマンド

ADD IP ROUTE TEMPLATE（193 ページ）
CREATE IPSEC POLICY（「IPsec」の 39 ページ）
DELETE IP ROUTE TEMPLATE（239 ページ）
SHOW IP ROUTE TEMPLATE（479 ページ）

SET IP ROUTEMAP

カテゴリー：IP / 経路制御（BGP-4）

```
SET IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]

SET IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   MATCH ASPATH=1..99

SET IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   MATCH COMMUNITY=1..99 [EXACT={NO|YES}]

SET IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   SET ASPATH={1..65534[,...]}

SET IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   SET COMMUNITY={INTERNET|NOEXPORT|NOADVERTISE|1..4294967295}[,...]
   [ADD={NO|YES}]

SET IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   SET LOCALPREF=0..4294967295

SET IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   SET MED=0..4294967295

SET IP ROUTEMAP=routemap ENTRY=1..4294967295 [ACTION={INCLUDE|EXCLUDE}]
   SET ORIGIN={IGP|EGP|INCOMPLETE}
```

routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）

解説

ルートマップのエントリーを変更する。

パラメーター

ROUTEMAP　ルートマップ名

ENTRY　ルートマップ内におけるエントリーの位置

ACTION　ルートマップエントリーにマッチした場合のアクション（INCLUDE、EXCLUDE）。INCLUDE の場合は SET 節の処理に進む。EXCLUDE の場合は該当経路の処理を行わない（破棄 = 通知しない、受信しない、など）。デフォルトは INCLUDE

MATCH ASPATH　AS パスフィルター番号。AS_PATH 属性の値によってマッチを行う場合に指定する。

MATCH COMMUNITY　コミュニティーフィルター番号。COMMUNITIES 属性の値によってマッチを行う場合に指定する。

SET ASPATH　AS パス。MATCH 節にマッチした経路エントリーの AS_PATH 属性の末尾に指定した AS パス値を追加する。AS パスは、AS 番号をカンマ区切りで並べることによって指定する。AS 番号は最大 10 個まで指定可能。

SET COMMUNITY　コミュニティーリスト。MATCH 節にマッチした経路エントリーの COMMUNITIES 属性に指定したコミュニティー値をセットする。コミュニティー値か Well-known コミュニティーを示すキーワードをカンマ区切りで列挙する。

EXACT　コミュニティーフィルターとのマッチングを完全一致で行うかどうか。NO（デフォルト）は部分一致。YES は完全一致。MATCH COMMUNITY パラメーターを指定した場合のみ有効。

ADD　SET COMMUNITY パラメーターを指定した場合、既存の COMMUNITIES 属性を置き換えるか、既存の属性に追加するかを指定する。NO（デフォルト）は COMMUNITIES 属性を置き換える。YES を指定した場合は、既存の COMMUNITIES 属性値に SET COMMUNITY パラメーターで指定した値を追加する。

SET LOCALPREF　マッチした経路エントリーの LOCAL_PREF 属性に指定した値をセットする。

SET MED　マッチした経路エントリーの MULTI_EXIT_DISCRIMINATOR 属性に指定した値をセットする。

SET ORIGIN　マッチした経路エントリーの ORIGIN 属性に指定した値をセットする。

関連コマンド

ADD BGP PEER（154 ページ）
ADD IP ROUTEMAP（195 ページ）
DELETE IP ROUTEMAP（240 ページ）
SET BGP PEER（343 ページ）
SHOW IP ROUTEMAP（481 ページ）

SET OSPF

カテゴリー：IP / 経路制御（OSPF）

```
SET OSPF [ASEXTERNAL={ON|OFF|NSSA}] [DEFROUTE={ON|OFF|TRUE|FALSE|YES|NO}
    [TYPE={1|2}] [METRIC=0..16777215]] [RIP={OFF|EXPORT|IMPORT|BOTH}]
    [ROUTERID=ipadd] [BGPIMPORT={ON|OFF}] [BGPLIMIT=1..4000]
    [BGPFILTER={NONE|300..399}] [AUTOCOST={ON|OFF}] [REFBANDWIDTH=10..10000]
    [STATICEXPORT={ON|OFF|TRUE|FALSE|YES|NO}]

[PASSIVEINTERFACEDEFAULT={ON|OFF|TRUE|FALSE|YES|NO}]
```

ipadd: IP アドレス

解説

OSPF のグローバル設定パラメーターを変更する。

パラメーター

ASEXTERNAL　AS 境界ルーター（ASBR）として動作させるかどうか。ON を指定した場合は、AS 外部の経路情報（他の経路制御プロトコルの情報とスタティック経路）を AS 内に通知する。このとき、通常エリアにはタイプ 5 の LSA で、準スタブエリア（NSSA）にはタイプ 7 の LSA で通知する。NSSA を指定した場合は、準スタブエリア（NSSA）にだけタイプ 7 の LSA で通知する。デフォルトは OFF

DEFROUTE　デフォルトルート（0.0.0.0）の AS 外部 LSA を生成し、AS 内に通知するかどうか。本パラメーターは ASBR として設定した（ASEXTERNAL=ON）場合のみ有効。デフォルトは OFF

TYPE　デフォルト AS 外部 LSA のメトリックタイプ（1 または 2）。DEFROUTE=ON の場合のみ有効。デフォルトは 2

METRIC　デフォルト AS 外部 LSA のメトリック。DEFROUTE=ON の場合のみ有効。デフォルトは 1

RIP　RIP と OSPF の間でどのように情報をやりとりするかを指定する。EXPORT を指定した場合、OSPF の経路情報が RIP のルーティングテーブルに取り込まれる。IMPORT を指定した場合、RIP の経路情報が OSPF のルーティングテーブルに取り込まれる。BOTH を指定した場合は、OSPF と RIP で互いに情報を交換しあう。OFF を指定した場合は、RIP と OSPF のやりとりは行われない。本パラメーターは ASBR として設定した（ASEXTERNAL=ON）場合のみ有効。デフォルトは OFF

ROUTERID　ルーター ID。IP アドレスと同じ形式で指定する。指定しなかった場合は、インターフェースに設定された IP アドレスの中でもっとも大きなものがルーター ID として使われる。

BGPIMPORT　BGP-4 で学習した経路を OSPF のルーティングテーブルに取り込むかどうか。本パラメーターは ASBR として設定した（ASEXTERNAL=ON）場合のみ有効。デフォルトは OFF。

BGPLIMIT　取り込む BGP-4 経路の最大数を指定する。「BGPIMPORT=ON」のときのみ有効。指定値に達した場合は、取り込み済みの経路が削除されて空きができるまで、BGP-4 経路の取り込みが停止される。デフォルトは 1000。

BGPFILTER　取り込む BGP-4 経路を取捨選択するために用いるプレフィックスフィルターの番号を指定

する。フィルターの適用をやめるには NONE を指定する。プレフィックスフィルターは ADD IP FILTER コマンドで作成する（フィルター番号 300～399）。「BGPIMPORT=ON」のときのみ有効。

AUTOCOST　OSPF インターフェースのコスト（メトリック）を実際のリンク速度に基づいて自動計算するかどうか。ON のときは、各インターフェースのリンク速度（VLAN の場合はリンクアップしているメンバーポートの平均速度）と REFBANDWIDTH パラメーターの値に基づいてコストが自動的に計算される（REFBANDWIDTH パラメーターの説明を参照）。ただし、ADD IP INTERFACE コマンド、SET IP INTERFACE コマンドの OSPFMETRIC パラメーターでメトリック値を明示的に指定している場合は、そちらが優先される。デフォルトは OFF。

REFBANDWIDTH　OSPF インターフェースのコスト（メトリック）を自動計算する場合に使う基準値。単位は Mbps。AUTOCOST=ON のとき、OSPF インターフェースのコストは、REFBANDWIDTH（Mbps）/ インターフェースのリンク速度（Mbps）となる。なお、VLAN インターフェースのリンク速度は、リンクアップしているメンバーポートの平均値となる。デフォルトは 1000。

STATICEXPORT　スタティック経路に対応する AS 外部 LSA を生成し、AS 内に通知するかどうか。本パラメーターは ASBR として設定した（ASEXTERNAL=ON）場合のみ有効。デフォルトは YES

PASSIVEINTERFACEDEFAULT　OSPF インターフェースの設定において PASSIVE パラメーターを省略したときの同パラメーターのデフォルト値を指定する。本パラメーターに値を指定しているときは、ADD OSPF INTERFACE コマンド、SET OSPF INTERFACE コマンドで PASSIVE パラメーターを指定しないと、本パラメーターの値がデフォルト値として用いられる。本パラメーターが未指定のときは、PASSIVE=OFF がデフォルトとなる。デフォルトは未指定。

例

■ルーター ID として「1.1.1.1」を設定する

```
SET OSPF ROUTERID=1.1.1.1
```

備考・注意事項

・仮想リンクを使用するときは、リンクの両エンドのルーターにルーター ID を設定しておくと設定がやりやすい。
・RIP および ASEXTERNAL パラメーターを変更すると、一時的にネットワークが不安定になるので注意。
・PASSIVEINTERFACEDEFAULT パラメーターの変更は、新規に作成する OSPF インターフェースでなく、既存の OSPF インターフェース（PASSIVE パラメーターを指定していないもの）にも適用されるので注意。

関連コマンド

ADD IP FILTER（169 ページ）
ADD OSPF INTERFACE（202 ページ）
DISABLE OSPF DEBUG（280 ページ）
DISABLE OSPF LOG（282 ページ）

ENABLE OSPF DEBUG（312 ページ）
SET OSPF INTERFACE（386 ページ）
SHOW OSPF（485 ページ）

SET OSPF AREA

カテゴリー：IP / 経路制御（OSPF）

SET OSPF AREA={**BACKBONE**|***area-number***} [AUTHENTICATION={NONE|PASSWORD}]
[STUBAREA={ON|OFF|YES|NO|TRUE|FALSE}] [STUBMETRIC=*0..16777215*]
[SUMMARY={SEND|NONE|OFF|NO|FALSE}]

area-number: OSPF エリア ID（a.b.c.d の形式）

解説

OSPF エリアの設定パラメーターを変更する。

パラメーター

AREA　エリア ID。0.0.0.0（バックボーンエリア）はキーワード「BACKBONE」で指定することもできる。

AUTHENTICATION　エリア内での認証方式。NONE（無認証）と PASSWORD（簡易パスワード）がある。実際のパスワードはインターフェースごとに設定する（ADD OSPF INTERFACE コマンド）。デフォルトは NONE。

STUBAREA　対象エリアをスタブエリアにするかどうか。ON、YES、TRUE（スタブエリアにする）および OFF、NO、FALSE（スタブエリアにしない）はそれぞれ同じ意味。スタブエリアは AS 外部の経路情報を持たないエリアで、AS 外部へのトラフィックはすべてデフォルト経路に送られる。バックボーン（0.0.0.0）エリアと仮想リンクの通過エリアでは必ず OFF に設定すること。また、スタブエリア内に複数の OSPF ルーターが存在する場合は、STUBAREA パラメーターの設定を同じにすること。バックボーンエリアのデフォルトは OFF、その他のエリアのデフォルトは ON。

STUBMETRIC　スタブエリア内に通知するデフォルト経路（デフォルトサマリー LSA）のメトリック。デフォルトは 1。本パラメーターはスタブエリアのエリア境界ルーター（ABR）でのみ有効。

SUMMARY　スタブエリア内にデフォルト経路以外の経路情報を通知するかどうか。NONE、OFF、NO、FALSE（通知しない）は同じ意味。SEND を指定した場合は、デフォルト以外のエリア情報もサマリー LSA でスタブエリア内に通知される。NONE を指定した場合は、デフォルトのサマリー LSA だけが ABR によってスタブエリア内に通知される。デフォルトは NONE。

関連コマンド

ADD OSPF AREA（199 ページ）
ADD OSPF RANGE（208 ページ）
DELETE OSPF AREA（242 ページ）
DELETE OSPF RANGE（247 ページ）
SET OSPF RANGE（390 ページ）
SHOW OSPF AREA（487 ページ）
SHOW OSPF RANGE（505 ページ）

SET OSPF HOST

カテゴリー：IP / 経路制御（OSPF）

SET OSPF HOST=*ipadd* METRIC=*0..65535*

ipadd: IP アドレス

解説

OSPF ルーティングテーブル内のホスト経路のメトリックを変更する。

パラメーター

HOST　ホストの IP アドレス。ルーター上で設定したエリア範囲内のアドレスでなくてはならない
METRIC　メトリック。デフォルトは 1

関連コマンド

ADD OSPF HOST（201 ページ）
DELETE OSPF HOST（243 ページ）
SHOW OSPF HOST（491 ページ）

SET OSPF INTERFACE

カテゴリー：IP / 経路制御（OSPF）

```
SET OSPF INTERFACE=interface [AREA={BACKBONE|area-number}]
    [DEADINTERVAL=2..2147483647] [HELLOINTERVAL=1..65535]
    [AUTHENTICATION={NONE|PASSWORD|MD5}] [PASSWORD=password]
    [PRIORITY=0..255] [RXMTINTERVAL=1..3600] [TRANSITDELAY=1..3600]
    [VIRTUALLINK=area-number] [NETWORK={BROADCAST|NON-BROADCAST}]
    [POLLINTERVAL=1..2147483647] [PASSIVE={ON|OFF|YES|NO|TRUE|FALSE}]
```

interface: IP インターフェース名（eth0、ppp0 など）または仮想インターフェース名（VIRTn）
area-number: OSPF エリア ID（a.b.c.d の形式）
password: パスワード（1〜8 文字。任意の印刷可能文字を使用可能。空白を含む場合はダブルクォートで囲む）

解説

OSPF インターフェースのパラメーターを変更する。

パラメーター

INTERFACE　IP インターフェース（VLAN）名または仮想インターフェース名（VIRTn）

AREA　エリア ID。仮想インターフェースの場合は通過エリアのエリア ID を指定する。

DEADINTERVAL　Hello パケットの Router Dead Interval タイマー（秒）。隣接ルーターから Hello パケットを受信できなくなったときに、隣接ルーターがダウンしたと判断するまでの時間を示す。同一ネットワーク上のすべてのルーターに同じ値を設定する必要がある。最小値は HELLOINTERVAL × 2、推奨値は HELLOINTERVAL × 4。デフォルト値は HELLOINTERVAL × 4（秒）。

HELLOINTERVAL　Hello パケットの送信間隔（Hello Interval）（秒）。同一ネットワーク上のすべてのルーターに同じ値を設定する必要がある。デフォルトは 10 秒。

AUTHENTICATION　本インターフェースにおける認証方式。NONE（無認証）、PASSWORD（簡易パスワード）、MD5（MD5 ダイジェスト）から選択する。パスワード（簡易パスワード認証時）は PASSWORD パラメーターで、MD5 認証鍵（MD5 ダイジェスト認証時）は ADD OSPF MD5KEY コマンドでインターフェースごとに設定する。本パラメーターの設定は、ADD OSPF AREA コマンドで設定したエリアごとの設定よりも優先される。デフォルトは NONE（エリアの設定が使用される）。

PASSWORD　認証用パスワード。エリア内またはインターフェースでの認証方法が簡易パスワード認証の場合（AUTHENTICATION パラメーターに PASSWORD を指定した場合）にのみ必要。デフォルトはパスワードなし（null）。なお、MD5 ダイジェスト認証の場合は、ADD OSPF MD5KEY コマンドで認証鍵を設定する。

PRIORITY　ルーター優先度（0〜255）。大きいほど優先度が高く、指名ルーター（DR）に選出される可能性が高くなる。優先度が同じときはルーター ID の大きいほうが DR となる。0 は DR になる資格がないことを示す。デフォルトは 1。

RXMTINTERVAL データベース記述パケット（タイプ 2）、リンク状態要求パケット（タイプ 3）、リンク状態更新パケット（タイプ 4）の送信間隔（秒）。隣接ルーター間のパケット往復時間よりも十分に大きな値でなくてはならない。LAN では 5 秒が標準的。デフォルトは 5 秒。

TRANSITDELAY リンク状態更新パケットの送信遅延時間（秒）。同パケットに含まれる LSA のエイジフィールドはこの値だけ増分される。LAN では通常 1 に設定される。デフォルトは 1

VIRTUALLINK 仮想リンクの対向に位置するバックボーンルーター（ABR）の ID。仮想インターフェース追加時（INTERFACE=VIRTn）の必須パラメーター。このとき、AREA には通過エリアの ID を指定する。

NETWORK 該当インターフェースに接続されているネットワークの種別。BROADCAST（ブロードキャスト型マルチアクセス）、NON-BROADCAST（非ブロードキャスト型マルチアクセス（NBMA））から選択する。本パラメーターは VLAN インターフェースでのみ有効。デフォルトは BROADCAST。

POLLINTERVAL 非ブロードキャスト型のマルチアクセスネットワーク（NBMA）における、非アクティブな隣接ルーターへの Hello パケット送信間隔（秒）。NETWORK=NON-BROADCAST を指定したときのみ有効。HELLOINTERVAL よりも大きな値を指定する必要がある。デフォルトは HELLOINTERVAL × 4（秒）。

PASSIVE 該当インターフェースをパッシブインターフェースにするかどうか。ON、YES、TRUE（パッシブインターフェースにする）および OFF、NO、FALSE（パッシブインターフェースにしない）はぞれぞれ同じ意味。パッシブインターフェースでは OSPF パケットの送受信を行わないが、パッシブインターフェースに接続されているネットワークの情報は、スタブネットワークとしてルーター LSA に追加される。デフォルトは OFF だが、SET OSPF コマンドの PASSIVEINTERFACEDEFAULT パラメーターに値を指定しているとき（デフォルトは未指定）は、その値が本パラメーター省略時の値となる。

備考・注意事項

・NETWORK=BROADCAST から NETWORK=NON-BROADCAST に変更した場合、(1) OSPF パケットがマルチキャストではなくユニキャストで送信されるようになる。そのため、ADD OSPF NEIGHBOUR コマンドで隣接ルーターをスタティック設定する必要がある (2) すでに動的に確立された隣接関係がある場合は自動的にスタティック設定に変更される (3) 最低でも 1 つ隣接ルーターがスタティック登録されるまで、Hello パケットは送出されない。

・NETWORK=NON-BROADCAST から NETWORK=BROADCAST に変更した場合、(1) スタティック登録された隣接ルーターはすべてクリアされる (2) Hello パケットがマルチキャストされるようになり、結果として隣接ルーターが動的に発見され、自動的に隣接関係が形成されるようになる。

関連コマンド

ADD OSPF INTERFACE（202 ページ）
ADD OSPF NEIGHBOUR（207 ページ）
ADD OSPF RANGE（208 ページ）
DELETE OSPF INTERFACE（244 ページ）
DISABLE OSPF INTERFACE（281 ページ）
ENABLE OSPF INTERFACE（313 ページ）

RESET OSPF INTERFACE（332 ページ）
SET OSPF（381 ページ）
SET OSPF AREA（384 ページ）
SET OSPF AREA（384 ページ）
SET OSPF NEIGHBOUR（389 ページ）
SET OSPF RANGE（390 ページ）
SHOW OSPF AREA（487 ページ）
SHOW OSPF INTERFACE（493 ページ）
SHOW OSPF RANGE（505 ページ）

SET OSPF NEIGHBOUR

カテゴリー：IP / 経路制御（OSPF）

SET OSPF NEIGHBOUR=*ipadd* PRIORITY=*0..255*

ipadd: IP アドレス

解説

スタティック登録した OSPF 隣接ルーターの設定パラメーターを変更する。

パラメーター

NEIGHBOUR　OSPF 隣接ルーターの IP アドレス
PRIORITY　隣接ルーターのルーター優先度。

関連コマンド

ADD OSPF NEIGHBOUR（207 ページ）
DELETE OSPF NEIGHBOUR（246 ページ）
SHOW OSPF NEIGHBOUR（503 ページ）

SET OSPF RANGE

カテゴリー：IP / 経路制御（OSPF）

SET OSPF RANGE=*ipadd* [AREA={BACKBONE|*area-number*}] [MASK=*ipadd*]
[EFFECT={ADVERTISE|DONOTADVERTISE}]

ipadd: IP アドレスまたはネットマスク
area-number: OSPF エリア ID（a.b.c.d の形式）

解説

OSPF エリアを構成するネットワーク範囲の設定を変更する。

パラメーター

RANGE ネットワークアドレス
AREA エリア ID
MASK ネットマスク。RANGE パラメーターと組み合わせてネットワークの範囲を指定する。省略時は RANGE で指定した IP アドレスのクラス（クラス A、B、C）に応じた標準ネットマスクが使用される
EFFECT 指定したアドレス範囲をエリア外部に通知するかどうか。エリア境界ルーター（ABR）でのみ有効。ADVERTISE を指定した場合、該当範囲の情報を 1 つのサマリー LSA としてエリア外に通知する。DONOTADVERTISE を指定した場合は情報を通知しない。デフォルトは ADVERTISE

関連コマンド

ADD OSPF RANGE（208 ページ）
DELETE OSPF RANGE（247 ページ）
SHOW OSPF RANGE（505 ページ）

SET OSPF REDISTRIBUTE

カテゴリー：IP / 経路制御（OSPF）

```
SET OSPF REDISTRIBUTE PROTOCOL={STATIC} [METRIC=0..16777214] [TYPE={1|
    2}]
```

解説

スタティック経路を AS 外部 LSA で AS 内に通知するときのメトリックとメトリックタイプの設定（ADD OSPF REDISTRIBUTE コマンドで設定したもの）を変更する。
本コマンドは AS 境界ルーター（ASBR）でのみ意味を持つ。

パラメーター

PROTOCOL　AS 外部経路の起源。現在指定できる値は STATIC（スタティック経路）のみ。
METRIC　PROTOCOL パラメーターで指定した起源を持つ AS 外部経路のメトリック。デフォルトは 20
TYPE　PROTOCOL パラメーターで指定した起源を持つ AS 外部経路のメトリックタイプ（1 または 2）。デフォルトは 2

関連コマンド

ADD OSPF REDISTRIBUTE（210 ページ）
DELETE OSPF REDISTRIBUTE（248 ページ）
SHOW OSPF REDISTRIBUTE（507 ページ）

SET OSPF STUB

カテゴリー：IP / 経路制御（OSPF）

SET OSPF STUB=*ipadd* MASK=*ipadd* METRIC=*0..65535*

ipadd: IP アドレスまたはネットマスク

解説

OSPF を使用していないネットワーク（スタブネットワーク）の設定を変更する。

パラメーター

STUB　スタブネットワークのネットワークアドレス。ルーター上で定義されているエリアの範囲内でなくてはならない
MASK　STUB に対するネットマスク
METRIC　メトリック。デフォルトは 1

関連コマンド

ADD OSPF STUB（211 ページ）
DELETE OSPF STUB（249 ページ）
SET OSPF HOST（385 ページ）
SET OSPF INTERFACE（386 ページ）
SHOW OSPF STUB（510 ページ）

SET OSPF SUMMARYADDRESS

カテゴリー：IP / 経路制御（OSPF）

SET OSPF SUMMARYADDRESS=*ipadd* [MASK=*ipadd*] [ADVERTISE={ON|OFF|YES|NO|TRUE|FALSE}] [TAG=*0..65535*]

ipadd: IP アドレスまたはネットマスク

解説

AS 外部経路の集約設定（集約経路エントリー）を変更する。
本コマンドは AS 境界ルーター（ASBR）でのみ意味を持つ。

パラメーター

SUMMARYADDRESS　集約後のネットワークアドレス。
MASK　SUMMARYADDRESS に対するネットワークマスク。
ADVERTISE　集約経路（SUMMARYADDRESS/MASK）を AS 外部 LSA で AS 内に通知するかどうか。ON、YES、TRUE を指定した場合は、集約経路を 1 つの AS 外部 LSA として AS 内に通知する。OFF、NO、FALSE を指定した場合は該当経路を AS 内に通知しない。デフォルトは ON。
TAG　集約経路の AS 外部 LSA にセットする外部経路タグ。デフォルトは 0。

関連コマンド

ADD OSPF SUMMARYADDRESS（212 ページ）
DELETE OSPF SUMMARYADDRESS（250 ページ）
SET OSPF（381 ページ）
SHOW OSPF SUMMARYADDRESS（512 ページ）

SET PING

カテゴリー：IP / 一般コマンド

```
SET PING [[IPADDRESS=]{ipadd|hostname}] [DELAY=seconds] [LENGTH=0..1500]
    [NUMBER={count|CONTINUOUS}] [PATTERN=value] [SIPADDRESS=ipadd]
    [SCREENOUTPUT={YES|NO}] [TIMEOUT=0..65535] [TOS=0..255]
```

ipadd: IP アドレス（IPv4 または IPv6）
hostname: ホスト名
seconds: 時間（0〜4294967295 秒）
count: 個数（1〜4294967295）
value: バイト列（16 進数。最大 4 バイト）

解説

PING コマンドのデフォルトパラメーターを設定する。
PING コマンド実行時に指定されなかったパラメーターについては、本コマンドで設定したデフォルト値が使用される。

パラメーター

IPADDRESS　宛先 IP アドレス（IPv4、IPv6）。ホストテーブルに登録されているホスト名も使用可能。また、ADD IP DNS コマンドで DNS サーバーのアドレスを設定している場合は DNS に登録されているホスト名（ドメイン名）も使用可能。

DELAY　PING パケットの送信間隔。デフォルトは 1 秒。

LENGTH　PING パケットのデータ部分の長さ。

NUMBER　PING パケットの送信個数。CONTINUOUS を指定した場合は、STOP PING コマンドで停止させられるまでパケットの送信を続ける。

PATTERN　PING パケットのデータ部分に埋め込む 4 バイトのバイナリーパターンを 16 進数で指定する（例：686f6765）。

SIPADDRESS　PING パケットの始点 IP アドレス（IPv4、IPv6）。省略時は送出インターフェースの IP アドレスが使われる。IPv6 のリンクローカルアドレスは指定できない。

SCREENOUTPUT　結果を端末画面に表示するかどうか。

TIMEOUT　応答待ち時間を指定する。

TOS　宛先アドレスが IP（IPv4）の場合、TOS オクテットの値を指定する。また、IPv6 の場合は Traffic Class フィールドの値を指定する。有効範囲は 0〜255。

関連コマンド

ADD IP DNS（167 ページ）
ADD IP HOST（178 ページ）

ADD IPV6 HOST（「IPv6」の 44 ページ）
PING（319 ページ）
SHOW PING（513 ページ）
STOP PING（525 ページ）

SET PING POLL

カテゴリー：IP / Ping ポーリング

```
SET PING POLL=poll-id [IPADDRESS=ipadd] [CRITICALINTERVAL=1..65535]
   [DESCRIPTION=string] [FAILCOUNT=1..100] [LENGTH=4..1500]
   [NORMALINTERVAL=1..65535] [SAMPLESIZE=1..100] [SIPADDRESS=ipadd]
   [TIMEOUT=1..30] [UPCOUNT=1..100]
```

poll-id: Ping ポーリング ID（1〜100）
ipadd: IP アドレス（IPv4 または IPv6）
string: 文字列（1〜32 文字。空白を含む場合はダブルクォートで囲む）

解説

Ping ポーリングの設定を変更する。

パラメーター

POLL　Ping ポーリング ID

IPADDRESS　監視対象機器の IP アドレス。IPv4 アドレスか IPv6 アドレスを指定する。IPv6 のリンクローカルアドレスを指定するときは、どのインターフェースからパケットを送出するかを示すため、アドレスの末尾にインターフェース名を付ける必要がある。その場合、アドレス、パーセント記号、インターフェース名の順に指定する（例：fe80::1234%eth1）。

CRITICALINTERVAL　機器の状態が「Up」以外のときのポーリング間隔（秒）。「Up」時のポーリング間隔（NORMALINTERVAL）よりも大幅に小さくすること。デフォルトは 1 秒。

DESCRIPTION　メモ。任意の文字列を指定できる。

FAILCOUNT　到達性が失われたと判断するために必要な Ping 無応答の回数。直前の SAMPLESIZE 回の Ping に対して、FAILCOUNT 回の無応答があった場合、監視対象機器が到達不可能になったと判断する。FAILCOUNT <= SAMPLESIZE となるよう設定すること。FAILCOUNT = SAMPLESIZE のときは、FAILCOUNT 回連続して無応答だったときだけ、到達不可能と判断する。FAILCOUNT < SAMPLESIZE のときは、無応答が連続していなくてもよい。デフォルトは 5 回。

LENGTH　Ping パケットのデータ部分の長さ（バイト）。省略時は 32 バイト

NORMALINTERVAL　機器の状態が「Up」のときのポーリング間隔（秒）。デフォルトは 30 秒。

SAMPLESIZE　到達性判断のために保持しておく Ping パケットの数。直前の SAMPLESIZE 回の Ping に対して、FAILCOUNT 回の無応答があった場合、監視対象機器が到達不可能になったと判断する。FAILCOUNT <= SAMPLESIZE となるよう設定すること。省略時は FAILCOUNT と同じ値になる。

SIPADDRESS　Ping パケットの始点 IP アドレス（IPv4、IPv6）。本パラメーター未指定時は、SET IP LOCAL コマンドでローカル IP アドレスが設定されているときはローカル IP アドレスが、ローカル IP アドレスが設定されていないときは、送出インターフェースの IP アドレスが使われる。本パラメーターを未指定に戻すには、未指定アドレス、すなわち、0.0.0.0（IPv4）または::（IPv6）を指定する。

TIMEOUT　Ping パケットの応答待ち時間（秒）。Ping（Echo request）パケット送信後、この時間内に応答パケットを受信しなかった場合は「無応答」と見なす。デフォルトは 1 秒

UPCOUNT　機器の状態が「Down」「Critical Down」から「Up」に戻るために必要な連続した「応答あり」の回数。「Down」「Critical Down」状態において、UPCOUNT 回連続して応答を受信すると、監視対象機器への到達性が回復したと判断する。デフォルトは 30 回。

備考・注意事項

本製品の PING コマンドは IPv4/IPv6 に対応しているが、Ping ポーリングは IPv4 と IPv6 だけの対応なので注意。

関連コマンド

ADD PING POLL（213 ページ）
RESET PING POLL（334 ページ）
SHOW PING POLL（515 ページ）

SET TRACE

カテゴリー：IP / 一般コマンド

SET TRACE [[IPADDRESS=]{*ipadd*|*hostname*}] [MAXTTL=*1..255*] [MINTTL=*1..255*] [NUMBER=*1..100*] [PORT=*port*] [SCREENOUTPUT={YES|NO}] [SOURCE=*ipadd*] [TIMEOUT=*0..65535*] [TOS=*0..255*]

ipadd: IP アドレス（IPv4 または IPv6）
hostname: ホスト名
port: UDP ポート番号（0～65535）

解説

TRACE コマンドのデフォルトパラメーターを設定する。
TRACE コマンド実行時に指定されなかったパラメーターについては、本コマンドで設定したデフォルト値が使用される。

パラメーター

IPADDRESS　宛先 IP アドレス（IPv4、IPv6）。ホストテーブルに登録されているホスト名も使用可能。また、ADD IP DNS コマンドで DNS サーバーのアドレスを設定している場合は DNS に登録されているホスト名（ドメイン名）も使用可能。
MAXTTL　最大ホップ数。トレースルートの範囲をここで指定したホップ数までに制限する。
MINTTL　最小ホップ数。1 個目のパケットの TTL フィールドには MINTTL の値が設定される。最初の数ホップをスキップするために使用する。
NUMBER　各ホップで送信するパケットの数。最大 100 個。デフォルトは 3 個。
PORT　トレースパケットの終点 UDP ポート。未使用と思われるポートを指定する。デフォルトは 33434。
SCREENOUTPUT　端末画面に結果を出力するかどうか。
SOURCE　始点 IP アドレス。省略時は送信インターフェースの IP アドレスが使われる。
TIMEOUT　ホップごとの応答待ち時間。デフォルトは 3 秒。
TOS　IPv4 の場合は TOS オクテットフィールドの値。IPv6 の場合は Traffic Class フィールドの値を指定する。0～255 の 10 進数値で指定する。

関連コマンド

ADD IP DNS（167 ページ）
ADD IP HOST（178 ページ）
ADD IPV6 HOST（「IPv6」の 44 ページ）
SHOW TRACE（523 ページ）
STOP TRACE（526 ページ）
TRACE（527 ページ）

SHOW BGP

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP

解説

BGP-4 モジュールのグローバル設定情報を表示する。

入力・出力・画面例

```
Manager > show bgp

BGP router ID ................. 10.10.10.2
Local autonomous system ....... 65020
Confederation ID .............. 0
Local preference .............. 100 (default)
Multi exit descriminator ...... -
EBGP route preference ......... 170 (default)
IBGP route preference ......... 170 (default)
Route table route map ......... -

Number of peers
  Defined ..................... 2
  Established ................. 2

BGP route table
  Iteration ................... 12
  Number of routes ............ 10
  Route table memory .......... 2596
```

BGP router ID	BGP ルーター ID
Local autonomous system	所属する AS の番号
Confederation ID	所属する AS コンフェデレーション番号
Local preference	LOCAL_PREF 属性のデフォルト値
Multi exit descriminator	MULTI_EXIT_DESC 属性のデフォルト値
EBGP route preference	E-BGP 経由で学習した経路に与える（ルーティングテーブル内での）優先度
IBGP route preference	I-BGP 経由で学習した経路に与える（ルーティングテーブル内での）優先度
Route table route map	BGP 経由で学習した経路をルーティングテーブルに登録する際に適用するルートマップ名

Number of peers	BGP ピア数
Defined	設定済みピア数（ADD BGP PEER コマンドで設定されたもの）
Established	セッション確立済みのピア数
BGP route table	BGP 経路表に関する情報
Iteration	経路表更新回数
Number of routes	経路エントリー数
Route table memory	BGP 経路表に使用しているメモリー量

表 30:

関連コマンド

SHOW BGP AGGREGATE（401 ページ）
SHOW BGP IMPORT（413 ページ）
SHOW BGP NETWORK（417 ページ）
SHOW BGP PEER（418 ページ）
SHOW BGP ROUTE（425 ページ）

SHOW BGP AGGREGATE

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP AGGREGATE

解説

集約経路エントリーの一覧を表示する。

入力・出力・画面例

```
Manager > show bgp aggregate

BGP aggregate entries

Prefix              Summary   Route map
------------------------------------------------
192.168.0.0/19      Yes       -
192.168.64.0/19     Yes       -
------------------------------------------------
```

Prefix	プレフィックス
Summary	集約経路だけを通知するか（Yes）、個々の経路も通知するか（No）
Route map	集約経路に適用するルートマップ名

表 31:

関連コマンド

ADD BGP AGGREGATE（149 ページ）
DELETE BGP AGGREGATE（218 ページ）
SET BGP AGGREGATE（336 ページ）
SHOW BGP ROUTE（425 ページ）

SHOW BGP BACKOFF

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP BACKOFF

解説

空きメモリー不足時の BGP-4 のバックオフ（一時停止）動作の設定を表示する。

入力・出力・画面例

```
Manager > show bgp backoff
BGP Backoff Stats:
 Stat                        Value
---------------------------------
command status            ENABLED
backOff state              NORMAL
total hist backOffs             0
total backOffs                  0
total backOff Limit             0
consecutive backOffs            0
consecutive backOffs limit      5
base Timeout                   10
Timeout multiplier            100%
Timeout step                    1
Timeout length (sec)           10
Mem Upper Threshold Value      95%
Mem Upper Notify             TRUE
Mem Lower Threshold Value      90%
Mem Lower Notify            FALSE
Current Mem use                 6%
---------------------------------
```

command status	BGP-4 バックオフ機能の有効・無効
backOff state	BGP-4 の動作状態。NORMAL（通常動作中）、BACKED OFF（バックオフ中（一時停止中））、PEER DISABLED（完全停止中）のいずれか
total hist backOffs	システム起動後の合計バックオフ回数（TOTALLIMIT、CONSECUTIVE によって完全停止してもリセットされない）
total backOffs	前回 TOTALLIMIT によって完全停止してからの合計バックオフ回数（CONSECUTIVE によって完全停止してもリセットされない）
total backOff Limit	TOTALLIMIT の設定値（バックオフの合計制限回数）
consecutive backOffs	バックオフ連続回数。現在までバックオフが何回連続して発生しているかを示す

consecutive backOffs limit	CONSECUTIVE の設定値（連続したバックオフの制限回数）
base Timeout	バックオフ時間の基準値（秒）
Timeout multiplier	バックオフ時間を決定するための係数
Timeout step	STEP の設定値（バックオフが連続して発生した場合、何回ごとにバックオフ時間を再計算するか）
Timeout length (sec)	現時点でのバックオフ時間（秒）
Mem Upper Threshold Value	バックオフしきい値（%）
Mem Upper Notify	システムがバックオフしきい値を監視中かどうか。すなわち、現在の backOff state が NORMAL かどうかを示す
Mem Lower Threshold Value	バックオフ解除しきい値（%）
Mem Lower Notify	システムがバックオフ解除しきい値を監視中かどうか。すなわち、現在の backOff state が BACKED OFF、PEER DISABLED のいずれかであるかを示す
Current Mem use	現在のメモリー使用量（%）

表 32:

関連コマンド

SET BGP BACKOFF（337 ページ）
SHOW BGP MEMLIMIT（414 ページ）

SHOW BGP CONFEDERATION

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP CONFEDERATION

解説

AS コンフェデレーションの設定情報を表示する。

入力・出力・画面例

```
Manager > show bgp confederationid

BGP confederation information

Local AS ................. 12
Confederation ID ........ 1
Confederation peers ..... 11
Peers .................... 192.168.10.1 (AS 11, CBGP)
```

Local AS	自 AS 番号
Confederation ID	所属するコンフェデレーションの AS 番号
Confederation peers	上記コンフェデレーションに所属する他 AS の一覧
Peers	BGP ピアの一覧。IP アドレス（AS 番号, BGP ピアの種類）

表 33:

関連コマンド

ADD BGP CONFEDERATIONPEER（151 ページ）
DELETE BGP CONFEDERATIONPEER（219 ページ）
SET BGP（335 ページ）
SET IP AUTONOMOUS（355 ページ）
SHOW BGP（399 ページ）

SHOW BGP COUNTERS

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP COUNTERS[={RIB|UPDATE|DB|DB-ALL|PROCESS|NEXTHOP}[,...]]

解説

BGP のカウンター情報を表示する。

パラメーター

COUNTERS　表示するカウンターの種類。RIB、UPDATE、DB、DB-ALL、PROCESS、NEXTHOP のいずれか

入力・出力・画面例

```
Manager > show bgp counters=update

Update Counters:
-------------------------------------------------
Update Message:
Header too small ................ 0
Header too long ................. 0
Withdrawn too long .............. 0
Total Path too long ............. 0
Prefix:
NLRI error ...................... 0
Withdrawn errors ................ 0
Mask > 32bits ................. 0
Data too long ................. 0
Invalid Address ............... 0
Path attributes ................. 0
Data shorter .................. 0
Seen twice .................... 0
Missing mandatory ............. 0
Origin ........................ 0
Length wrong ................ 0
Flags wrong ................. 0
Unknown origin .............. 0
AS path ....................... 0
Silently dropped .............. 0
Flags wrong ................. 0
List get failed ............. 0
Unknown Seg type ............ 0
Non-confed peer ............. 0
```

```
Data too long ..... 0
Data too short ..... 0
AS path loop ..... 0
Confed seg order ..... 0
Next hop ..... 0
Length wrong ..... 0
Flags wrong ..... 0
Address Zero ..... 0
Interface found ..... 0
Med ..... 0
Length wrong ..... 0
Flags wrong ..... 0
Local preference ..... 0
Length wrong ..... 0
Flags wrong ..... 0
External peer ..... 0
Atomic aggregate ..... 0
Length wrong ..... 0
Flags wrong ..... 0
Aggregate ..... 0
Length wrong ..... 0
Flags wrong ..... 0
Community ..... 0
Length wrong ..... 0
Flags wrong ..... 0
Originator ..... 0
Length wrong ..... 0
Flags wrong ..... 0
From eBGP Peer ..... 0
Loops detected ..... 0
Cluster List ..... 0
Flags wrong ..... 0
From eBGP Peer ..... 0
Loops detected ..... 0
Unknown Attributes ..... 0
Flag wrong ..... 0
Non-transitive ..... 0
Transitive ..... 0
Memory:
Low memory drops ..... 0
Filter:
Path exclude ..... 67022
Prefix exclude ..... 0
Routemap exclude ..... 0
Route Selection Fail ..... 0
Match List empty ..... 0
Select List empty ..... 0
NextHop No Route ..... 0
Internal Control:
Control Pointers ..... 0
Message Pointer ..... 0
```

```
Dropped Pointer ..............  0
```

SHOW BGP DAMPING

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP DAMPING

解説

BGP-4 ルートフラップダンピングの設定を表示する。

入力・出力・画面例

```
Manager > show bgp damping

BGP Route Flap Damping
  Status ..................... ENABLED
  Routes in Engine ............ 40
     Monitored Routes ......... 38
     Suppressed Routes ........ 2
  Forgotten Routes ............ 0

Parameterset 0
  DEFAULT
  Current status ..... ENABLED
  Suppression ........ 2000       Reuse .......... 750
  Half life .......... 15 min     Maximum Hold ... 1:4

Parameterset 1
  <Parameterset1>
  Current status ..... ENABLED
  Suppression ........ 5000       Reuse .......... 1250
  Half life .......... 2 min      Maximum Hold ... 1:2
```

Status	ルートフラップダンピングの有効・無効
Routes in Engine	ルートフラップダンピングの管理対象となりうる総経路数
Monitored Routes	Monitored（監視）状態の経路数
Suppressed Routes	Suppressed（抑制）状態の経路数
Forgotten Routes	Monitored（監視）状態から Not Monitored（非監視）状態に遷移した回数
Parameterset	パラメーターセット番号
Description	パラメーターセット番号の次行に表示される文字列は、パラメーターセットのメモ（DESCRIPTION パラメーターの値）を示す。DESCRIPTION パラメーターが空のときは、<ParametersetX>と表示される（X はパラメーターセット番号）

Current status	パラメーターセットの有効・無効
Suppression	抑制しきい値
Reuse	再使用（抑制解除）しきい値
Half life	ペナルティー値の半減期（分）
Maximum Hold	最大抑制時間を求めるための係数。Half life との比として表示される（1:X の「X」の部分が係数）。最大抑制時間は Half file × X で求められる

表 34:

関連コマンド

ADD BGP PEER（154 ページ）
CREATE BGP DAMPING PARAMETERSET（215 ページ）
DESTROY BGP DAMPING PARAMETERSET（253 ページ）
DISABLE BGP DAMPING（258 ページ）
ENABLE BGP DAMPING（288 ページ）
PURGE BGP DAMPING（321 ページ）
RESET BGP DAMPING（325 ページ）
SET BGP DAMPING PARAMETERSET（339 ページ）
SHOW BGP DAMPING ROUTES（411 ページ）

SHOW BGP DAMPING ROUTES

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP DAMPING ROUTES

解説

BGP-4 ルートフラップダンピング機能が管理している経路の情報（ペナルティー値など）を表示する。

入力・出力・画面例

```
Manager > show bgp damping routes

BGP Route Flap Damping

------------------------------------------------------------------------------
Par  Prefix/Mask         Next Hop     Current    Pen    Num   Last St   Next St
Set                                     State  (FoM)  Flaps    Change    Change
------------------------------------------------------------------------------
  0  10.157.20.0/24      172.28.28.158     WM    114      1  00:46:40  00:36:55
  0  10.158.40.0/24      172.28.28.158     WM    145      1  00:41:30  00:42:25
  0  10.157.30.0/24      172.28.28.158     WM    114      1  00:46:40  00:36:55
  0  10.157.40.0/24      172.28.28.158     WM    114      1  00:46:40  00:36:55
  0  10.157.50.0/24      172.28.28.158     WM    114      1  00:46:40  00:36:55
  0  10.158.50.0/24      172.28.28.158     WM    145      1  00:41:30  00:42:25
  0  10.158.30.0/24      172.28.28.158     WM    145      1  00:41:30  00:42:25
  0  10.158.20.0/24      172.28.28.158     WM    145      1  00:41:30  00:42:25
  0  10.158.10.0/24      172.28.28.158    >?S   1176      3  00:19:30  00:09:50
------------------------------------------------------------------------------
Status Flags : >=Best route for the given prefix, *=Unreachable next hop
               A=Aggregate route, S=Aggregate Suppressed
Origin Flags : i=Internal, e=External, ?=Incomplete, W=Withdrawn
Damping Flags: S=Damping Suppressed, M=Damping Monitored
```

Par Set	該当経路のペナルティー値を管理するために使用しているパラメーターセットの番号
Prefix/Mask	プレフィックス（宛先ネットワークアドレス）とプレフィックス長
Next Hop	ネクストホップアドレス
Current State	現在の状態。3 つのフラグ（記号）で表される。各フラグは、先頭からそれぞれ、ステータスフラグ（Status Flag）、起源フラグ（Origin Flag）、ダンピングフラグ（Damping Flag）を示す。ステータスフラグは、「>」（最適経路）、「*」（Next Hop が到達不能）、「a」（集約経路）、「s」（「SUMMARY=YES」の集約経路に内包されているため現在不使用）の 4 種類。起源フラグは、「i」（IGP）、「e」（EGP）、「?」（Imcomplete）、「W」（取り消されている）の 4 種類。ダンピングフラグは、「S」（抑制中）、「M」（監視中）の 2 種類
Pen (FoM)	ペナルティー値
Num Flaps	該当経路がフラップした回数（到達不能になった回数）
Last St Change	該当経路が現在の状態に遷移してからの経過時間
Next St Change	状態が「S」（抑制中）から「M」（監視中）、または、「M」（監視中）から非監視に遷移するまでの時間（該当経路が安定していなくてはならない時間）

表 35:

関連コマンド

ADD BGP PEER（154 ページ）
CREATE BGP DAMPING PARAMETERSET（215 ページ）
DESTROY BGP DAMPING PARAMETERSET（253 ページ）
DISABLE BGP DAMPING（258 ページ）
ENABLE BGP DAMPING（288 ページ）
PURGE BGP DAMPING（321 ページ）
RESET BGP DAMPING（325 ページ）
SET BGP DAMPING PARAMETERSET（339 ページ）
SHOW BGP DAMPING（409 ページ）

SHOW BGP IMPORT

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP IMPORT

解説

BGP への経路取り込み設定を表示する。

入力・出力・画面例

```
Manager > show bgp import

BGP import entries


Proto      Route map
---------------------------
STATIC     -
---------------------------
```

Proto	経路情報のソース。RIP、OSPF、STATIC（静的経路）、INTERFACE（インターフェース経路）がある
Route map	インポート時に適用するルートマップ名

表 36:

関連コマンド

ADD BGP IMPORT（152 ページ）
ADD IP ROUTEMAP（195 ページ）
DELETE BGP IMPORT（220 ページ）
SET BGP IMPORT（341 ページ）

SHOW BGP MEMLIMIT

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP MEMLIMIT

解説

BGP-4 に割り当て可能な最大メモリー量と実際に割り当てられているメモリー量を表示する。

入力・出力・画面例

```
Manager > show bgp memlimit
BGP Memory Limit:  85%,   Actual Use:  0%
```

BGP Memory Limit	BGP-4 に割り当て可能な最大メモリー量（%）
Actual Use	BGP-4 に割り当てられているメモリー量（%）

表 37:

関連コマンド

SET BGP MEMLIMIT（342 ページ）
SHOW BGP BACKOFF（402 ページ）

SHOW BGP MEMLIMIT SCAN

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP MEMLIMIT SCAN

解説

BGP モジュールのメモリー容量の情報を表示する。

入力・出力・画面例

```
Manager > show bgp memlimit scan

BGP Memory Limit: 85%, Actual Use: 57%
Module Freelist Stats: moduleId = 5
module buffer use: 18686
module percent use: 34%
      list          unitSize  freeUsed  buffersUsed
-------------------------------------------------
      00f33c6c      84        0         0
      00f46b6c      12        0         0
      00f46024      88        0         0
      00f33b04      68        0         0
      00f33c9c      48        104874    4996
      00f46c78      12        0         0
      00f4f0fc      32        196984    6156
      00f557e4      236       104874    26220
-------------------------------------------------
Module Freelist Stats: moduleId = 103
module buffer use: 31011
module percent use: 57%
list unitSize freeUsed buffersUsed
-------------------------------------------------
      00d0caf4      24        0         0
      00d0ca94      12        0         0
      00d0cc40      32        0         0
      00d0cff4      32        0         0
      00d0ccc8      8         155       1
      00d0ca64      512       0         0
      00d0cbb0      8         0         0
      00d0cf14      8         19439     76
      00d0cc10      8         0         0
      00d0c7e0      64        21643     677
      00d0cbe0      524       0         0
      00d0cf9c      116       180       11
      00d0cdf8      36        19262     338
      00d0c810      20        0         0
```

```
      00d0ce28      16        0         0
      00d0cf44      52        196980    5051
      00d0cc98      40        314616    6169
      00d0bc88      20        0         0
      00d0d024      20        0         0
      00d0b860      40        2         1
      00d0bc58      1012      2         1
      00d0d07c      40        0         0
      00d0cac4      16        0         0
      00f33c6c      84        0         0
      00f46b6c      12        0         0
      00f46024      88        0         0
      00f33b04      68        0         0
      00f33c9c      48        104874    4996
      00f46c78      12        0         0
      00f4f0fc      32        196984    6156
      00f557e4      236       104874    26220
-------------------------------------------------
```

関連コマンド

SET BGP BACKOFF（337 ページ）
SET BGP MEMLIMIT（342 ページ）
SHOW BGP MEMLIMIT（414 ページ）

SHOW BGP NETWORK

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP NETWORK

解説

BGP で通知可能なネットワークプレフィックスの一覧を表示する。

入力・出力・画面例

```
Manager > show bgp network

BGP network entries


Prefix              Route map
-------------------------------------
10.0.0.0/12         -
-------------------------------------
```

Prefix	プレフィックス
Route map	該当プレフィックスに適用するルートマップ名

表 38:

関連コマンド

ADD BGP NETWORK（153 ページ）
DELETE BGP NETWORK（221 ページ）
SHOW BGP ROUTE（425 ページ）

SHOW BGP PEER

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP PEER[=*ipadd*]

ipadd: IP アドレス

解説

BGP ピアの情報を表示する。

パラメーター

PEER　BGP ピアのＩＰアドレス。指定時は該当ピアの詳細情報が、省略時はピアの一覧が表示される。

入力・出力・画面例

```
Manager > show bgp peer

BGP peer entries

Peer              State      AS      InMsg        OutMsg
-------------------------------------------------------------
172.16.11.1       Estab      20      132          139
192.168.11.2      Estab      10      137          133
-------------------------------------------------------------

Manager > show bgp peer=192.168.11.2

Peer ................ 192.168.11.2
Description ......... -
State ............... Established
Remote AS ........... 10
BGP Identifier ...... 192.168.10.1
Connect retry ....... 120s
Hold time ........... 90s (actual 90s)
Keep alive .......... 30s (actual 30s)
Min AS originated ... 15
Min route advert .... 30

Filtering
  In filter ......... -
  In path filter .... -
  In route map ...... -
  Out filter ........ -
  Out path filter ... -
```

```
  Out route map ..... -

Max prefix ..... OFF
External hops ..... 1 (EBGP multihop disabled)
Next hop self ..... No
Send community ..... No
Messages In/Out ..... 137/133
Debugging ..... -
  Device ..... -

Connection type ..... EXTERNAL

Established transitions ..... 1
Established duration ..... 01:04:44
Time since last update received ... 00:43:32

Message counters:
  inOpen ..... 1       outOpen ..... 1
  inKeepAlive ..... 130       outKeepAlive ..... 130
  inUpdate ..... 6       outUpdate ..... 2
  inNotification ..... 0       outNotification ..... 0
```

Peer	BGP ピアの IP アドレス
State	ピアとの（通信の）状態。Idle（初期状態）、Idle(D)（初期状態。(D) は DISABLE BGP PEER コマンドによって無効状態にあることを示す）、Connect（TCP コネクション確立待ち）、Active（TCP コネクション確立再試行中）、OpenSent（OPEN メッセージを送信。ピアからの OPEN メッセージ待ち）、OpenConf（OPEN メッセージ受信。KEEPALIVE または NOTIFICATION 待ち）、Estab（BGP セッション確立）がある
AS	ピアの所属 AS
InMsg	TCP コネクション確立後にピアから受信したメッセージ数
OutMsg	TCP コネクション確立後にピアに送信したメッセージ数

表 39:

Peer	BGP ピアの IP アドレス
Description	ピアの説明（メモ）
State	ピアとの（通信の）状態。Idle（初期状態）、Idle(D)（初期状態。(D) は DISABLE BGP PEER コマンドによって無効状態にあることを示す）、Connect（TCP コネクション確立待ち）、Active（TCP コネクション確立再試行中）、OpenSent（OPEN メッセージを送信。ピアからの OPEN メッセージ待ち）、OpenConf（OPEN メッセージ受信。KEEPALIVE または NOTIFICATION 待ち）、Estab（BGP セッション確立）がある

Remote AS	ピアの所属 AS
BGP Identifier	BGP ルーター ID
Connect retry	該当ピアに対する TCP コネクション確立の再試行間隔
Hold time	該当ピアとの BGP セッションがダウンしたと認識するまでの時間（Hold Time）（秒）。カッコ内はセッション開始時のネゴシエーションで決定された値
Keep alive	KEEPALIVE メッセージの送信間隔。カッコ内は Hold Time のネゴシエーション結果に基づき実際に採用された値
Min AS originated	自 AS 起源の経路情報を含む UPDATE メッセージの最小連続送信間隔（秒）
Min route advert	他 AS 起源の経路情報を含む UPDATE メッセージの最小連続送信間隔（秒）
Filtering	BGP 経路のフィルタリング設定
In filter	該当ピアから受信した経路情報に適用する IP プレフィックスフィルター
In path filter	該当ピアから受信した経路情報に適用する AS パスフィルター
In route map	該当ピアから受信した経路情報に適用するルートマップ
Out filter	該当ピアに送信する経路情報に適用する IP プレフィックスフィルター
Out path filter	該当ピアに送信する経路情報に適用する AS パスフィルター
Out route map	該当ピアに送信する経路情報に適用するルートマップ
Max prefix	該当ピアから受け入れ可能な最大プレフィックス数
External hops	E-BGP セッションにおける BGP メッセージの初期 TTL 値
Next hop self	該当ピアに通知する経路の NEXTHOP として必ず自アドレスを使うかどうか
Send community	UPDATE メッセージに COMMUNITY 属性を含めるかどうか
Messages In/Out	該当ピアからの受信メッセージ数/該当ピアへの送信メッセージ数
Debugging	有効なデバッグオプション
Device	デバッグ情報の出力先デバイス番号
Connection type	BGP セッションタイプ
Established transitions	BGP セッションが Established 状態に遷移した回数
Established duration	セッション確立後の経過時間
Time since last update received	最後の UPDATE メッセージ受信後の経過時間
Message counters	メッセージカウンター
inOpen	OPEN メッセージ受信数
outOpen	OPEN メッセージ送信数
inKeepAlive	KEEPALIVE メッセージ受信数
outKeepAlive	KEEPALIVE メッセージ送信数

inUpdate	UPDATE メッセージ受信数
outUpdate	UPDATE メッセージ送信数
inNotification	NOTIFICATION メッセージ受信数
outNotification	NOTIFICATION メッセージ送信数

表 40:

関連コマンド

ADD BGP PEER（154 ページ）
DELETE BGP PEER（222 ページ）
SET BGP PEER（343 ページ）
SHOW BGP（399 ページ）
SHOW IP ROUTEMAP（481 ページ）

SHOW BGP PEERTEMPLATE

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP PEERTEMPLATE[*=1..30*]

解説

BGP ピアテンプレートの情報を表示する。

パラメーター

PEERTEMPLATE　BGP ピアテンプレート番号。省略時はすべての BGP ピアテンプレートが対象となる。

入力・出力・画面例

```
Manager > show bgp peertemplate
BGP Peer Template Information
-------------------------------------------------------------

Template.............. 1
Description ......... E-BGP policy
Role ................. Non-Client
Connect retry ....... 120s
Hold time ........... 90s
Keep alive .......... 30s
Min AS originated ... 15
Min route advert .... 30
Local Interface ..... Not defined

Filtering
  In filter ......... -
  In path filter .... -
  In route map ...... import_ebgp
  Out filter ........ -
  Out path filter ... -
  Out route map ..... export_ebgp

Max prefix .......... OFF
Next hop self ....... No
Send community ...... No

Private AS Filter ... Yes
-------------------------------------------------------------

Template.............. 2
Description ......... I-BGP(Non-client) policy
```

```
Role ................ Non-Client
Connect retry ....... 120s
Hold time ........... 90s
Keep alive .......... 30s
Min AS originated ... 15
Min route advert .... 30
Local Interface ..... Not defined

Filtering
  In filter ......... -
  In path filter .... -
  In route map ...... import_ibgp
  Out filter ........ -
  Out path filter ... -
  Out route map ..... export_ibgp

Max prefix .......... OFF
Next hop self ....... No
Send community ...... No

Private AS Filter ... No
-------------------------------------------------------------
```

Template	BGP ピアテンプレート番号
Description	テンプレートの説明（メモ）
Role	ピアの種類。eBGP Peer（E-BGP ピア）、Non-Client（I-BGP ピア）、Client（I-BGP ピア。ルートリフレクタークライアント）がある
Connect retry	該当ピアに対する TCP コネクション確立の再試行間隔
Hold time	該当ピアとの BGP セッションがダウンしたと認識するまでの時間（Hold Time）（秒）。カッコ内はセッション開始時のネゴシエーションで決定された値
Keep alive	KEEPALIVE メッセージの送信間隔。カッコ内は Hold Time のネゴシエーション結果に基づき実際に採用された値
Min AS originated	自 AS 起源の経路情報を含む UPDATE メッセージの最小連続送信間隔（秒）
Min route advert	他 AS 起源の経路情報を含む UPDATE メッセージの最小連続送信間隔（秒）
Local Interface	該当ピアとの通信に使用するローカル IP インターフェース
Filtering	BGP 経路のフィルタリング設定
In filter	該当ピアから受信した経路情報に適用する IP プレフィックスフィルター
In path filter	該当ピアから受信した経路情報に適用する AS パスリスト
In route map	該当ピアから受信した経路情報に適用するルートマップ
Out filter	該当ピアに送信する経路情報に適用する IP プレフィックスフィルター
Out path filter	該当ピアに送信する経路情報に適用する AS パスリスト
Out route map	該当ピアに送信する経路情報に適用するルートマップ
Max prefix	該当ピアから受け入れ可能な最大プレフィックス数

Next hop self	該当ピアに通知する経路の NEXTHOP として必ず自アドレスを使うかどうか
Send community	UPDATE メッセージに COMMUNITY 属性を含めるかどうか
Private AS Filter	プライベート AS 番号（64512～65535）をフィルタリングするかどうか

表 41:

関連コマンド

ADD BGP PEER（154 ページ）
ADD BGP PEERTEMPLATE（158 ページ）
ADD IP ASPATHLIST（163 ページ）
ADD IP FILTER（169 ページ）
ADD IP LOCAL（182 ページ）
ADD IP ROUTEMAP（195 ページ）
DELETE BGP PEER（222 ページ）
DELETE BGP PEERTEMPLATE（223 ページ）
DISABLE BGP PEER（261 ページ）
ENABLE BGP PEER（291 ページ）
RESET BGP PEER（326 ページ）
SET BGP PEER（343 ページ）
SET BGP PEERTEMPLATE（346 ページ）
SET IP LOCAL（367 ページ）
SHOW BGP PEER（418 ページ）

SHOW BGP ROUTE

カテゴリー：IP / 経路制御（BGP-4）

SHOW BGP ROUTE[=*prefix*] [REGEXP=*aspathregexp*] [COMMUNITY={INTERNET|
NOEXPORT|NOEXPORTSUBCONFED|NOADVERTISE|*1..4294967295*}]

prefix: プレフィックス（IP アドレス/プレフィックス長）
aspathregexp: AS パス正規表現

解説

BGP の経路表を表示する。

パラメーター

ROUTE ネットワークプレフィックス。指定時は、一致するプレフィックスだけが表示される。省略時はすべてのプレフィックスが表示される。

REGEXP AS パス正規表現。AS_PATH 属性の内容が指定した正規表現と一致するプレフィックスだけが表示される。

COMMUNITY コミュニティー値。COMMUNITIES 属性に指定したコミュニティー値が含まれるプレフィックスだけが表示される。本パラメーターを指定した場合、COMMUNITIES 属性のない経路は表示されない。

入力・出力・画面例

```
Manager > show bgp route

BGP route table
-------------------------------------------------------------------------
   Prefix              Next hop         Origin      MED         Local pref
   Path
-------------------------------------------------------------------------
RIB Out:
   10.10.10.0/29       10.10.10.2       INCOMPLETE  0           100
   SEQ 65020 65030;
   10.10.10.0/30       0.0.0.0          INCOMPLETE  0           0

   10.10.10.4/30       10.10.10.2       INCOMPLETE  0           100
   SEQ 65020;
   10.10.10.8/30       10.10.10.2       INCOMPLETE  0           100
   SEQ 65020 65030;
   10.128.0.0/12       10.10.10.2       IGP         0           100
   SEQ 65020 65030 65040 65040 65040;
   172.16.0.0/16       10.10.10.2       IGP         0           100
```

```
   SEQ 65020;
   172.16.10.0/24      10.10.10.2       INCOMPLETE  0           100
   SEQ 65020;
   172.31.0.0/16       10.10.10.2       INCOMPLETE  0           100
   SEQ 65020 65030;
   192.168.0.0/16      0.0.0.0          IGP         0           0

------------------------------------------------------------------------

Manager > show bgp route regexp="65040$"

BGP route table
------------------------------------------------------------------------
   Prefix              Next hop         Origin      MED         Local pref
   Path
------------------------------------------------------------------------
RIB Out:
   10.128.0.0/12       10.10.10.2       IGP         0           100
   SEQ 65020 65030 65040 65040 65040;
------------------------------------------------------------------------
```

Prefix	プレフィックス
Next hop	NEXT_HOP 属性値
Origin	ORIGIN 属性値
MED	MULTI_EXIT_DISC 属性値
Local pref	LOCAL_PREF 属性値
Path	AS_PATH 属性値

表 42:

例

■AS パスの末尾が「65040」であるプレフィックス（AS 65040 を起源とするプレフィックス）だけを表示する。

```
SHOW BGP ROUTE REGEXP="65040$"
```

関連コマンド

SHOW BGP（399 ページ）
SHOW BGP AGGREGATE（401 ページ）
SHOW BGP IMPORT（413 ページ）
SHOW BGP NETWORK（417 ページ）
SHOW BGP PEER（418 ページ）

SHOW BOOTP RELAY

カテゴリー：IP / DHCP/BOOTP リレー

SHOW BOOTP RELAY

解説

DHCP/BOOTP リレーエージェントの設定情報および統計情報を表示する。転送先サーバーの一覧も表示する。

入力・出力・画面例

```
Manager > show bootp relay

BOOTP Relaying Agent Configuration.

Status       : ENABLED
Maximum Hops : 4

BOOTP Relay Destinations
------------------------
192.168.10.100
------------------------


BOOTP Counters
---------------
InPackets    OutPackets    InRejects    InRequests    InReplies
0000000083   0000000002    0000000000   0000000082    0000000001
```

Status	DHCP/BOOTP リレーエージェントの状態
Maximum Hops	DHCP/BOOTP パケットの最大ホップ数
BOOTP Relay Destinations	DHCP/BOOTP パケットの転送先 IP アドレスリスト
InPackets	DHCP/BOOTP パケット受信数
OutPackets	DHCP/BOOTP パケット送信数
InRejects	DHCP/BOOTP パケット受信後破棄数（エラーによる）
InRequests	DHCP/BOOTP 要求受信数
InReplies	DHCP/BOOTP 応答受信数

表 43:

関連コマンド

ADD BOOTP RELAY（161 ページ）
DELETE BOOTP RELAY（224 ページ）
DISABLE BOOTP RELAY（262 ページ）
ENABLE BOOTP RELAY（292 ページ）
PURGE BOOTP RELAY（322 ページ）
SET BOOTP MAXHOPS（349 ページ）

SHOW IP

カテゴリー：IP / 一般コマンド

SHOW IP

解説

IP モジュールの基本的な設定情報を表示する。

入力・出力・画面例

```
Manager > show ip

IP Module Configuration
-------------------------------------------------------------------------------

Module Status .................. ENABLED
IP Packet Forwarding ........... ENABLED
IP Echo Reply .................. ENABLED
Debugging ...................... DISABLED
IP Fragment Offset Filtering ... ENABLED
Default Name Servers
  Primary Name Server .......... 192.168.10.100
  Secondary Name Server ........ 0.0.0.0
Source-Routed Packets .......... Discarded
Remote IP address assignment ... DISABLED
DNS Relay ...................... ENABLED
IP ARP LOG ..................... ENABLED

Routing Protocols

RIP Neighbours ................. 2
EGP Status ..................... DISABLED
Autonomous System Number ....... Not Set
Transfer RIP to EGP ............ Disabled
ARP aging timer multiplier...... 4 (1024-2048 secs)
OSPF Status .................... DISABLED
IGMP Status .................... DISABLED
DVMRP Status ................... DISABLED
PIM Status ..................... DISABLED
IP Multicast HW switching ...... DISABLED
BGP Status ..................... DISABLED

Active Routes

Static ......................... 0
Interface ...................... 2
```

```
RIP ............................ 3
EGP ............................ 0
OSPF ........................... 0
BGP ............................ 0
Other .......................... 0
Multicast ...................... 0

IP Filter Configuration

Total filters .................. 0

Dynamic Interfaces ............. 0
```

Module Status	IP モジュールの有効・無効
IP Packet Forwarding	IP 転送（ルーティング）機能の有効・無効
IP Echo Reply	ICMP エコー要求（PING）に応答するかどうか
Debugging	IP モジュールのデバッグ機能の有効・無効
IP Fragment Offset Filtering	IP フラグメントオフセットフィルターの有効・無効。（ENABLE IP FOFILTER コマンド/DISABLE IP FOFILTER コマンド）
Default Name Servers	デフォルト DNS サーバーに関する情報。ドメインごとの DNS サーバーを確認するには SHOW IP DNS コマンドを使う
Primary Name Server	デフォルトプライマリー DNS サーバーの IP アドレス
Secondary Name Server	デフォルトセカンダリー DNS サーバーの IP アドレス
Source-Routed Packets	始点経路制御オプション付き IP パケットの扱い。Forwarded（転送）か Discarded（破棄）
Remote IP address assignment	IPCP、DHCP による IP アドレスの動的設定を行うかどうか
DNS Relay	DNS リレー機能の有効・無効
IP ARP LOG	ARP キャッシュログの有効・無効
RIP Neighbours	隣接 RIP ルーター（RIP ピア）の数
Autonomous System Number	AS（自律システム）番号
ARP aging timer multiplier	ARP キャッシュタイムアウトを決定するための乗数。カッコ内は乗数に基づいて計算されたタイムアウト値の範囲
OSPF Status	OSPF の有効・無効
IGMP Status	IGMP の有効・無効
DVMRP Status	DVMRP の有効・無効
PIM Status	PIM の有効・無効
BGP Status	BGP の有効・無効
Static	スタティック経路数
Interface	インターフェース経路数
RIP	RIP 経路数
OSPF	OSPF 経路数

BGP	BGP 経路数
Other	その他の経路数
Multicast	マルチキャスト経路数
Filter n	IP フィルター「n」に設定されているフィルターエントリー数
Total Filters	IP フィルターの総数
Dynamic Interfaces	ダイナミックインターフェース（SLIP や PPP）の数

表 44:

関連コマンド

DISABLE IP（263 ページ）
DISABLE IP DEBUG（265 ページ）
DISABLE IP DNSRELAY（266 ページ）
DISABLE IP FORWARDING（269 ページ）
DISABLE IP SRCROUTE（278 ページ）
DISABLE SNMP（「運用・管理」の 180 ページ）
ENABLE IP（293 ページ）
ENABLE IP DEBUG（296 ページ）
ENABLE IP DNSRELAY（297 ページ）
ENABLE IP FORWARDING（300 ページ）
ENABLE IP SRCROUTE（310 ページ）
ENABLE SNMP（「運用・管理」の 205 ページ）

SHOW IP ARP

カテゴリー：IP / ARP

SHOW IP ARP

解説

ARP キャッシュの内容を表示する。

入力・出力・画面例

```
Manager > show ip arp

  Interface        IP Address       Physical Address      ARP Type    Status
--------------------------------------------------------------------------------
  vlan1(5)         192.168.1.200    00-90-99-1e-e0-0a     Dynamic     active
  vlan1(0)         192.168.1.255    ff-ff-ff-ff-ff-ff     Other       active
  eth0             192.168.100.2    00-90-99-0f-54-23     Dynamic     active
  eth0             192.168.100.255  ff-ff-ff-ff-ff-ff     Other       active
  eth0             255.255.255.255  ff-ff-ff-ff-ff-ff     Other       active
--------------------------------------------------------------------------------
```

Interface	インターフェース
IP Address	IP アドレス
Physical Address	物理アドレス（MAC アドレス）
ARP Type	エントリー種別。Static（スタティックエントリー。ADD IP ARP コマンドで登録）、Dynamic（ダイナミックエントリー。ARP パケットから学習）、Invalid（無効エントリー）、Other（システムによって自動生成されるエントリー。IP ブロードキャストアドレスなど）
Status	エントリーの状態。Active か Inactive

表 45:

関連コマンド

ADD IP ARP（162 ページ）
DELETE IP ARP（225 ページ）
SET IP ARP（351 ページ）

SHOW IP ASPATHLIST

カテゴリー：IP / 経路制御（BGP-4）

SHOW IP ASPATHLIST[*=1..99*]

解説

AS パスフィルターの情報を表示する。

パラメーター

ASPATHLIST　AS パスフィルターの番号。省略時は有効なエントリーを持つすべてフィルターが表示される。

入力・出力・画面例

```
Manager > show ip aspathlist
IP AS path lists

List  Entry       Regular Expression
------------------------------------------------------------
1     1           Exclude 10$
      2           Include .*
------------------------------------------------------------
```

List	AS パスフィルター番号
Entry	エントリー番号
Regular Expression	マッチ条件（AS_PATH 属性に対する正規表現）とマッチ時のアクション

表 46:

関連コマンド

ADD IP ASPATHLIST（163 ページ）
DELETE IP ASPATHLIST（226 ページ）

SHOW IP CACHE

カテゴリー：IP / 一般コマンド

SHOW IP CACHE

解説

IP アドレスキャッシュの内容を表示する。

入力・出力・画面例

```
Manager > show ip cache

IP Address Cache
------------------------------------------------------------------
Entries ................. 284
Max Entries ............. 284
Last Addition ........... 13:54:43 on Tuesday 21-Feb-2006
Last Rejection .......... -

Source      Destination     Interface Type    Age   Count
------------------------------------------------------------------------------
10.1.1.2    192.168.100.3   eth0-1    Forward 1     3
10.1.1.3    192.168.100.3   eth0-2    Forward 1     3
10.1.1.4    192.168.100.3   eth0-3    Forward 1     3
10.1.1.5    192.168.100.3   eth0-4    Forward 1     3
10.1.1.6    192.168.100.3   eth0-5    Forward 1     3
10.1.1.7    192.168.100.3   eth0-6    Forward 1     3
10.1.1.8    192.168.100.3   eth0-7    Forward 1     3
10.1.1.9    192.168.100.3   eth0-8    Forward 1     3
10.1.1.10   192.168.100.3   eth0-9    Forward 1     3
10.1.1.11   192.168.100.3   eth0-10   Forward 1     3
```

Entries	キャッシュエントリー数
Max Entries	ルーターが再起動してからのキャッシュエントリー最大数
Last Addition	キャッシュに最後にエントリーが追加された日付・時刻
Last Rejection	キャッシュで最後にエントリー追加に失敗した日付・時刻（通常、キャッシュが満杯の場合）
Source	送信元 IP アドレス
Destination	送信先 IP アドレス
Interface	IP パケットを受信したインターフェース
Type	種類。Forward、Local、GenBcast、SpcBcast、MultOsp、MultLmtd、MultNorm、MultLocl のいずれか

Age	エントリーの経過時間。エントリーが使用されると再始動する。
Count	エントリーが見つかった回数

表 47:

関連コマンド

RESET IP COUNTER（328 ページ）
SHOW IP COUNTER（437 ページ）

SHOW IP COMMUNITYLIST

カテゴリー：IP / 経路制御（BGP-4）

SHOW IP COMMUNITYLIST[*=1..99*]

解説

コミュニティーフィルターの情報を表示する。

パラメーター

COMMUNITYLIST　コミュニティーフィルターの番号。省略時は有効なエントリーを持つすべてフィルターが表示される。

入力・出力・画面例

```
Manager > show ip communitylist
IP Community lists

List  Entry       Community List
-------------------------------------------------------------
1     1           Include 1000
-------------------------------------------------------------
```

List	コミュニティーフィルター番号
Entry	エントリー番号
Community list	マッチ条件（コミュニティー番号のリスト）とマッチ時のアクション

表 48:

関連コマンド

ADD IP COMMUNITYLIST（165 ページ）
DELETE IP COMMUNITYLIST（227 ページ）

SHOW IP COUNTER

カテゴリー：IP / 一般コマンド

SHOW IP COUNTER[={ALL|ARP|ICMP|INTERFACE|IP|MULTICAST|ROUTES|SNMP|UDP}]

解説

IP に関する統計情報（IP MIB の情報）を表示する。

パラメーター

COUNTER　表示したい情報を指定する。省略時および ALL 指定時は IP MIB の全情報が表示される。

入力・出力・画面例

```
Manager > show ip counter


Management Information Block Counters
-------------------------------------------------------------------------------

IP Interface Counters
-------------------------------------------------------------------------------
Interface       ifInPkts    ifInBcastPkts    ifInUcastPkts     ifInDiscards
Type           ifOutPkts   ifOutBcastPkts   ifOutUcastPkts    ifOutDiscards
-------------------------------------------------------------------------------
eth0               19890              162            19728                0
Static             19898              165            19733                0

eth1               16922              162            16760                0
Static             16916              165            16751                0

-------------------------------------------------------------------------------


IP counters

  inReceives ................. 36812       outRequests ................. 3287
  inHdrErrors ................ 0           outDiscards ................. 0
  inAddrErrors ............... 0           outNoRoutes ................. 2
  inUnknownProtos ............ 0           forwDatagrams ............... 36816
  inDiscards ................. 0           routingDiscards ............. 0
  inDelivers ................. 3296
  reasmReqds ................. 0           fragCreates ................. 0
  reasmOKs ................... 0           fragOKs ..................... 0
```

```
  reasmFails ..................... 0       fragFails ..................... 0

IP Gateway Discards

  tinyFragments .................. 0       spoofedPkts ................... 0
  invalHdrOption ................. 0       dirBroadcasts ................. 0
  saSpoofedPkts .................. 0       ipsecSpoofedPkts .............. 0
  saBlockedPkts .................. 0       ipsecBlockedPkts .............. 0
  saEncodeFails .................. 0       ipsecEncodeFails .............. 0


ICMP counters

  inMsgs ........................ 23       outMsgs ....................... 5
  inErrors ...................... 0        outErrors ..................... 0
  inDestUnreachs ................ 9        outDestUnreachs ............... 0
  inTimeExcds ................... 9        outTimeExcds .................. 0
  inParamProbs .................. 0        outParamProbs ................. 0
  inSrcQuenchs .................. 0        outSrcQuenchs ................. 0
  inRedirects ................... 0        outRedirects .................. 0
  inEchos ....................... 0        outEchos ...................... 5
  inEchoReps .................... 5        outEchoReps ................... 0
  inTimestamps .................. 0        outTimestamps ................. 0
  inTimestampReps ............... 0        outTimestampReps .............. 0
  inAddrMasks ................... 0        outAddrMasks .................. 0
  inAddrMaskReps ................ 0        outAddrMaskReps ............... 0


UDP counters

  inDatagrams ................. 651        outDatagrams ................ 862
  inErrors ...................... 0        noPorts ....................... 0


EGP counters

  inMsgs ........................ 0        outMsgs ....................... 0
  inErrors ...................... 0        outErrors ..................... 0


SNMP counters:
  inPkts ........................ 0        outPkts ....................... 0
  inBadVersions ................. 0        outTooBigs .................... 0
  inBadCommunityNames ........... 0        outNoSuchNames ................ 0
  inBadCommunityUses ............ 0        outBadValues .................. 0
  inASNParseErrs ................ 0        outGenErrs .................... 0
  inTooBigs ..................... 0        outGetRequests ................ 0
  inNoSuchNames ................. 0        outGetNexts ................... 0
  inBadValues ................... 0        outSetRequests ................ 0
  inReadOnlys ................... 0        outGetResponses ............... 0
  inGenErrs ..................... 0        outTraps ...................... 0
```

```
  inTotalReqVars ................... 0
  inTotalSetVars ................... 0
  inGetRequests .................... 0
  inGetNexts ....................... 0
  inSetRequests .................... 0
  inGetResponses ................... 0
  inTraps .......................... 0
-------------------------------------------------------------------------------


Route Counters

 IP address       NextHop         Interface  Metric  Octets rcvd   Octets sent
-------------------------------------------------------------------------------
 172.16.10.0      172.16.20.1     eth0          2            184           224
 172.16.20.0      0.0.0.0         eth0          1             72             0
 192.168.10.0     172.16.20.1     eth0          3        1361648       1360795
 192.168.20.0     0.0.0.0         eth1          1        1360867       1361648
 192.168.30.0     192.168.20.200  eth1          2              0             0
-------------------------------------------------------------------------------

IP Multicast Counters
-------------------------------------------------------------------------------
Interface     ifInMultPkts   ifInMultDiscard   ifOutMultPkts   ifOutMultDiscards
-------------------------------------------------------------------------------
eth0                     0                 0               0                   0
eth1                     0                 0               0                   0
-------------------------------------------------------------------------------


IP ARP counters

  arpRxPkts ....................... 2       arpTxPkts ....................... 0
  arpRxReqPkts .................... 1       arpTxReqPkts .................... 1
  arpRxRespPkts ................... 1       arpTxRespPkts ................... 1
  arpRxDiscPkts ................... 0       arpTxDiscPkts ................... 0
```

arpRxPkts	受信 ARP パケット総数
arpRxReqPkts	受信 ARP 要求パケット数
arpRxRespPkts	受信 ARP 応答パケット数
arpRxDiscPkts	受信後に破棄した ARP パケット数
arpTxPkts	送信 ARP パケット総数
arpTxReqPkts	送信 ARP 要求パケット数
arpTxRespPkts	送信 ARP 応答パケット数
arpTxDiscPkts	送信前に破棄した ARP パケット数

表 49: ARP カウンター

inMsgs	ICMP パケット受信数
inErrors	ICMP エラーパケット受信数（ICMP チェックサムエラー、長さエラーなど）
inDestUnreachs	ICMP 宛先到達不可能メッセージ受信数
inTimeExcds	ICMP 時間超過メッセージ受信数
inParamProbs	ICMP パラメーター異常メッセージ受信数
inSrcQuenchs	ICMP 送信抑制要求メッセージ受信数
inRedirects	ICMP 経路変更要求メッセージ受信数
inEchos	ICMP エコー要求メッセージ受信数
inEchoReps	ICMP エコー応答メッセージ受信数
inTimestamps	ICMP タイムスタンプ要求メッセージ受信数
inTimestampReps	ICMP タイムスタンプ応答メッセージ受信数
inAddrMasks	ICMP アドレスマスク要求メッセージ受信数
inAddrMaskReps	ICMP アドレスマスク応答メッセージ受信数
outMsgs	ICMP パケット送信数
outErrors	ICMP パケット送信前破棄数
outDestUnreachs	ICMP 宛先到達不可能メッセージ送信数
outTimeExcds	ICMP 時間超過メッセージ送信数
outParamProbs	ICMP パラメーター異常メッセージ送信数
outSrcQuenchs	ICMP 送信抑制要求メッセージ送信数
outRedirects	ICMP 経路変更要求メッセージ送信数
outEchos	ICMP エコー要求メッセージ送信数
outEchoReps	ICMP エコー応答メッセージ送信数
outTimestamps	ICMP タイムスタンプ要求メッセージ送信数
outTimestampReps	ICMP タイムスタンプ応答メッセージ送信数
outAddrMasks	ICMP アドレスマスク要求メッセージ送信数
outAddrMaskReps	ICMP アドレスマスク応答メッセージ送信数

表 50: ICMP カウンター

Interface	IP インターフェース名
Type	インターフェース種別。Static、Dynamic、Inactive のいずれか
ifInPkts	受信パケット数
ifInBcastPkts	マルチキャストパケット受信数
ifInUcastPkts	ユニキャストパケット受信数
ifInDiscards	受信後破棄パケット数
ifOutPkts	送信パケット数
ifOutBcastPkts	マルチキャストパケット送信数
ifOutUcastPkts	ユニキャストパケット送信数
ifOutDiscards	送信前破棄パケット数

表 51: INTERFACE カウンター

inReceives	受信 IP パケット数
inHdrErrors	受信 IP パケットのうち、ヘッダーエラーがあったものの数
inAddrErrors	受信 IP パケットのうち、アドレスエラーがあったものの数
inUnKnownProtos	受信 IP パケットのうち、上位プロトコルが未サポートだったものの数
inDiscards	受信 IP パケットのうち、IP レベルでのリソース不足により破棄されたものの数
inDelivers	受信 IP パケットのうち、上位層に配送されたものの数
reasmReqds	受信 IP パケットのうち、再構成が必要だったものの数
reasmOKs	受信 IP パケットのうち、再構成に成功したものの数
reasmFails	受信 IP パケットのうち、再構成に失敗したものの数
outRequests	上位層から送信要求を受けた IP パケットの数
outDiscards	送信対象 IP パケットのうち、IP レベルでのリソース不足により破棄されたものの数
outNoRoutes	送信対象 IP パケットのうち、経路がないため破棄されたものの数
forwDatagrams	IP パケット転送数
routingDiscards	転送対象 IP パケットのうち、エラーがないにもかかわらず、バッファー容量不足などの要因で破棄されたものの数
fragCreates	生成されたフラグメントの数
fragOKs	フラグメント化に成功した IP パケットの数
fragFails	フラグメント化が必要だが、フラグメント不可（DF）ビットが立っているためフラグメント化できなかった IP パケットの数
tinyFragments	Tiny Fragment 攻撃と見なされ破棄された IP パケットの数
invalHdrOption	無効な IP オプションを含んでいたため破棄された IP パケットの数
saSpoofedPkts	SA（Security Association）からのパケットのように見えるが、正しくエンコードされていなかったために破棄された IP パケットの数
saEncodeFails	SA のエンコーディングに失敗して破棄された IP パケットの数
spoofedPkts	アドレス詐称により破棄された IP パケットの数
dirBroadcasts	ディレクティドブロードキャストが禁止されているため破棄された IP パケットの数
saBlockedPkts	SA に所属していないアドレスから送られたため、SA によって破棄されたパケットの数

表 52: IP カウンター

Interface	IP インターフェース名。「LOCAL」はローカル IP インターフェースを示す
ifInMultPkts	受信 IP マルチキャストパケット数
ifInMultDiscard	受信 IP マルチキャストパケットのうち、破棄されたものの数
ifOutMultPkts	送信 IP マルチキャストパケット数
ifOutMultDiscards	送信されずに破棄された IP マルチキャストパケットの数

表 53: MULTICAST カウンター

IP address	経路の最終目的地
NextHop	ネクストホップルーターの IP アドレス
Interface	本経路宛てパケットを送出するインターフェース
Metric	メトリック
Octets rcvd	本経路経由の受信オクテット数
Octets sent	本経路経由の送信オクテット数

表 54: ROUTE カウンター

inPkts	受信 SNMP パケット数
inBadVersions	未サポートのバージョン番号を持つ SNMP メッセージの受信総数
inBadCommunityNames	不明なコミュニティー名を持つ SNMP メッセージの受信総数
inBadCommunityUses	コミュニティー名とオペレーションの権限が一致しない SNMP メッセージの受信総数
inASNParseErrs	ASN.1 構文エラーによりデコードできなかった SNMP メッセージの受信総数
inTooBigs	エラー状態フィールドに「tooBig」がセットされていた SNMP メッセージの受信総数
inNoSuchNames	エラー状態フィールドに「noSuchName」がセットされていた SNMP メッセージの受信総数
inBadValues	エラー状態フィールドに「badValue」がセットされていた SNMP メッセージの受信総数
inReadOnlys	エラー状態フィールドに「readOnly」がセットされていた SNMP メッセージの受信総数
inGenErrs	エラー状態フィールドに「genErr」がセットされていた SNMP メッセージの受信総数
inTotalReqVars	受信した GetRequest および GetNextRequest メッセージに応じて読み出された MIB オブジェクトの合計数
inTotalSetVars	受信した SetRequest メッセージに応じて変更された MIB オブジェクトの合計数
inGetRequests	受信した GetRequest メッセージの総数
inGetNexts	受信した GetNextRequest メッセージの総数
inSetRequests	受信した SetRequest メッセージの数
inGetResponses	受信した GetResponse メッセージの総数
inTraps	受信した SNMP トラップの総数
outPkts	送信 SNMP パケット数
outTooBigs	エラー状態フィールドに「tooBig」をセットして送信された SNMP メッセージの数
outNoSuchNames	エラー状態フィールドに「noSuchName」をセットして送信された SNMP メッセージの数

outBadValues	エラー状態フィールドに「badValue」をセットして送信された SNMP メッセージの数
outGenErrs	エラー状態フィールドに「genErr」をセットして送信された SNMP メッセージの数
outGetRequests	送信した GetRequest メッセージの総数
outGetNexts	送信した GetNextRequest メッセージの総数
outSetRequests	送信した SetRequest メッセージの総数
outGetResponses	送信した GetResponse メッセージの総数
outTraps	送信した SNMP トラップの総数

表 55: SNMP カウンター

inDatagrams	受信 UDP パケット数
inErrors	受信 UDP パケットのうち、UDP レベルでのエラーにより破棄されたものの数
outDatagrams	送信 UDP パケット数
noPorts	受信 UDP パケットのうち、終点ポートのリスナー不在のため破棄されたものの数

表 56: UDP カウンター

関連コマンド

SHOW IP INTERFACE（458 ページ）
SHOW IP ROUTE（473 ページ）
SHOW SNMP（「運用・管理」の 342 ページ）
SHOW TCP（519 ページ）

SHOW IP DEBUG

カテゴリー：IP / 一般コマンド

SHOW IP DEBUG[*=1..40*]

解説

IP デバッグキューに保存されているエラーパケットのヘッダー情報を表示する。
IP デバッグキューをアクティブにするには、ENABLE IP DEBUG を実行する。このキューには、ヘッダーエラーのあった IP データグラムの先頭 64 オクテットが保存される。キューのサイズは 40 エントリー。

パラメーター

DEBUG キュー内エントリーの番号（1〜40）を指定する。番号を省略した場合は、キュー内のエントリー数が表示される。

入力・出力・画面例

```
Manager > show ip debug

1 packets are in the IP debug queue.

Manager > show ip debug=1

1 packets are in the IP debug queue.

Error     = Bad source or destination address
Interface = eth0
45 00 00 28 20 04 00 00 - 80 11 9b c0 7f 00 00 01
ff ff ff ff 08 fd 08 fd - 00 14 58 9f 01 00 00 30
c4 c1 14 3a 3c 00 00 00 - 00 00 00 00 00 00 ab 87
5b 29 00 00 00 00 00 ff - ff ff ff ff ff ff ff 09
```

関連コマンド

DISABLE IP DEBUG（265 ページ）
ENABLE IP DEBUG（296 ページ）
SHOW IP（429 ページ）

SHOW IP DNS

カテゴリー：IP / 名前解決

SHOW IP DNS

解説

DNS サーバーリストと DNS キャッシュ機能の設定を表示する。

入力・出力・画面例

```
Manager > show ip dns

DNS Server Configuration
-------------------------------------------------------------------------------
Domain                      Int/Status   Primary         Secondary       Requests
-------------------------------------------------------------------------------
ANY                         No           192.168.10.100  0.0.0.0               16
mikan.fruit.xxx             No           172.20.10.1     172.20.10.2           0
ringo.fruit.xxx             No           172.20.20.1     172.20.20.2           0
-------------------------------------------------------------------------------

Cache:
  Maximum entries ................... 100
  Current entries ................... 5 (1480 bytes)
  Timeout (minutes) ................. 30
  Cache hits ........................ 3
```

Domain	該当サーバーの担当ドメイン。ANY はマッチするドメインがなかった場合に使用するデフォルトサーバーを示す
Int/Status	DNS サーバーアドレスを IPCP か DHCP で動的に取得する場合、情報を取得する IP インターフェースの名前とインターフェースの状態（Up/Down）が表示される。サーバーアドレスを固定的に設定している場合は、No と表示される
Primary	プライマリー DNS サーバーアドレス。未設定の場合は 0.0.0.0 と表示される。サーバーアドレスを動的に取得しているときは、該当インターフェースがダウンだとアドレスは未設定状態となる
Secondary	セカンダリー DNS サーバーアドレス。未設定の場合は 0.0.0.0 と表示される
Requests	該当サーバーへの問い合わせ回数
Cache セクション	DNS キャッシュ機能に関する情報が表示される
Maximum entries	DNS キャッシュに保持できるエントリーの最大数
Current entries	現時点でのキャッシュエントリー数（カッコ内はメモリー消費量）

Timeout (minutes)	キャッシュエントリーの有効期限（分）
Cache hits	キャッシュヒット回数。DNS の問い合わせに対し、キャッシュエントリーの情報で応答できた回数

表 57:

関連コマンド

ADD IP DNS（167 ページ）
DELETE IP DNS（228 ページ）
DISABLE IP DNSRELAY（266 ページ）
ENABLE IP DNSRELAY（297 ページ）
SET IP DNS（356 ページ）
SET IP DNS CACHE（358 ページ）
SHOW IP DNS CACHE（447 ページ）
TELNET（「運用・管理」の 380 ページ）

SHOW IP DNS CACHE

カテゴリー：IP / 名前解決

SHOW IP DNS CACHE

解説

DNS キャッシュの内容を表示する。

入力・出力・画面例

```
Manager > show ip dns cache

DNS Cache                Entries ... 5 (1480 bytes)
-------------------------------------------------------------------------------
Domain Name                                      IP Address        TTL   Matches
  (IPv6 Address)                                                  (Min)
-------------------------------------------------------------------------------
ar720-2-eth1.birds.or.jp                         192.168.20.1       29         0
ar410-vlan1.birds.or.jp                          ---                29         0
  ::
ar410-eth0.birds.or.jp                           172.16.10.254      29         0
ar720-1-eth0.birds.or.jp                         192.168.10.1       29         1
kijitora.birds.or.jp                             192.168.10.100     17         2
-------------------------------------------------------------------------------
```

Entries	キャッシュエントリー数（カッコ内はメモリー消費量）
Domain Name	ドメイン名
IP Address	IP アドレス
TTL	エントリーの残り有効期限（分）
Matches	キャッシュヒット数（問い合わせに対してキャッシュエントリーの内容で応答した回数）

表 58:

関連コマンド

ADD IP DNS（167 ページ）
DELETE IP DNS（228 ページ）
DISABLE IP DNSRELAY（266 ページ）
ENABLE IP DNSRELAY（297 ページ）
SET IP DNS（356 ページ）
SET IP DNS CACHE（358 ページ）

SHOW IP DNS（445 ページ）
TELNET（「運用・管理」の 380 ページ）

SHOW IP FILTER

カテゴリー：IP / IP フィルター

SHOW IP FILTER[=*filter-id*]

filter-id: フィルター番号（0〜399）

解説

IP フィルターの内容を表示する。
どのインターフェースにフィルターが適用されているかは、SHOW IP INTERFACE コマンドで確認する。

パラメーター

FILTER　フィルター番号。指定した番号のフィルターだけを表示する。無指定時はすべてのフィルターを表示する。

入力・出力・画面例

```
Manager > show ip filter

IP Filters
------------------------------------------------------------------------------
No. Ent. Source Port    Source Address     Source Mask       Session           Size
         Dest. Port     Dest. Address      Dest. Mask        Prot.(T/C)     Options
         Type           Act/Pol/Pri        Logging                          Matches
------------------------------------------------------------------------------
1     1  ---            192.168.30.7       255.255.255.255   ---               Any
         ---            Any                Any               Any               Any
         General        Exclude            Off                                   4
      2  ---            192.168.30.0       255.255.255.0     ---               Any
         ---            Any                Any               Any               Any
         General        Include            Off                                   0

     Requests: 13            Passes: 9            Fails: 4
------------------------------------------------------------------------------
2     1  ---            Any                Any               ---               Any
         ---            Any                Any               Any               Any
         General        Include            Off                                   0

     Requests: 0             Passes: 0            Fails: 0
------------------------------------------------------------------------------
```

No.	フィルター番号
Ent.	フィルターエントリー番号
Source Port	始点 TCP/UDP ポート
Source Address	始点 IP アドレス
Source Mask	始点 IP アドレスに対するネットマスク
Session	TCP セッションタイプ。START、ESTABLISHED、ANY のいずれか
Size	再構成後の IP データグラムサイズ（length + offset * 8）。制限なしのときは Any
Dest. Port	終点 TCP/UDP ポート
Dest. Address	終点 IP アドレス
Dest. Mask	終点 IP アドレスに対するネットマスク値
Prot. (T/C)	プロトコル。ANY、ICMP、OSPF、TCP、UDP のいずれか。ICMP の場合は、ICMP メッセージタイプとサブコードも表示される
Options	IP オプション。Any、Yes、No のいずれか
Type	パターンの種類。General か Specific
Act/Pol/Pri	（トラフィックフィルターの）アクション。Exclude か Include。（ポリシーフィルターの）経路選択ポリシー値。（プライオリティーフィルターの）プライオリティー
Logging	このエントリーにマッチしたパケットをログに記録するかどうか。Off（記録せず）、Head（ヘッダー情報のみ）、Dump（ヘッダーおよびデータ先頭 32 オクテット）、4〜1600 の数値（ヘッダー情報とデータの先頭指定バイト数）
Matches	このエントリーにマッチした IP パケットの数
Requests	このフィルターと照合された IP パケットの数
Passes	このフィルターによって通過が許可されたパケットの数
Fails	このフィルターによって通過を拒否されたパケットの数

表 59:

関連コマンド

ADD IP FILTER（169 ページ）
ADD IP INTERFACE（179 ページ）
DELETE IP FILTER（230 ページ）
SET IP FILTER（360 ページ）
SET IP INTERFACE（364 ページ）

SHOW IP FLOW

カテゴリー：IP / 一般コマンド

SHOW IP FLOW

解説

IP トラフィックフローテーブルを表示する。

入力・出力・画面例

```
SecOff > show ip flow

IP Flow Table (Max. Flows = 4000)
IP Addresses                          Prot    Port Numbers          Hits  Flag   St
Int (in->out)            Dump  Mc   Bc Local  route     mroute    Arp        Filt
-------------------------------------------------------------------------------
192.168.1.200   - 192.168.10.103     ICMP        8 - 0             338  005000  2
0 vlan1     -               0  n   n      0  00000000  00000000  00000000  n/n/n
192.168.10.103  - 192.168.1.200      ICMP        0 - 0             339  002000  2
0 eth0      -vlan           0  n   n      0  008f3d0c  00000000  00000000  n/n/n
192.168.1.200   - 192.168.1.1        ESP         0 - 0            2715  001000  2
0 vlan1     -               0  n   n      1  00000000  00000000  00000000  n/n/n
192.168.10.103  - 192.168.10.255     UDP       138 - 138             1  000000  2
0 eth0      -               0  n   n      2  00000000  00000000  00000000  n/n/n
192.168.10.103  - 192.168.10.255     UDP       137 - 137             4  000000  2
0 eth0      -               0  n   n      2  00000000  00000000  00000000  n/n/n
```

IP Addresses	フローを構成する両エンドの IP アドレス（a.b.c.d - e.f.g.h）
Prot	IP プロトコル名またはプロトコル番号
Port Numbers	プロトコルが TCP/UDP の場合、フローを構成する両エンドのポート番号（x - y）。ICMP の場合はメッセージタイプとコード（type - code）。その他のプロトコルでは意味を持たない（0 - 0 と表示）
Hits	このフローエントリーの使用回数
Flag	フローに対する処理を示すビットフラグ
St	フローの状態
Int (in->out)	インターフェース
Dump	該当フローのパケットを破棄するかどうか。理由（フィルタリング、インターフェースが無効状態、など）により番号が異なる
Mc	マルチキャストフローかどうか
Bc	ブロードキャストフローかどうか

Local	IP ルーティングにおけるパケットタイプ
route	ユニキャスト経路情報の保存先メモリーアドレス
mroute	マルチキャスト経路情報の保存先メモリーアドレス
Arp	ARP 情報の保存先メモリーアドレス
Filt	該当フローが IP フィルターを通過するかどうか。スラッシュで区切られた 3 つの項目は、左からトラフィックフィルター、ポリシーフィルター、プライオリティーフィルターを示す

表 60:

SHOW IP HELPER

カテゴリー：IP / UDP ブロードキャストヘルパー

SHOW IP HELPER [COUNTER]

解説

UDP ブロードキャストパケットの転送先設定を表示する。

パラメーター

COUNTER　本パラメーター指定時は、UDP ブロードキャスト転送機能の統計情報が表示される。

入力・出力・画面例

```
Manager > show ip helper

IP HELPER Configuration

Status : Disabled
------------------------------------------------------------------------------
Interface : vlan10
  UDP port : 137
     Destination(s) ..... 172.16.28.5
  UDP port : 138
     Destination(s) ..... 172.16.28.5
------------------------------------------------------------------------------
```

Status	UDP ブロードキャスト転送機能の有効・無効
Interface	UDP ブロードキャストを監視するインターフェース
UDP port	転送する UDP パケットの終点ポート番号
Destination	UDP パケットの転送先 IP アドレス

表 61:

Interface	UDP ブロードキャストを監視するインターフェース
InPackets	受信した UDP ブロードキャストパケット数
InNoDestination	受信した UDP ブロードキャストパケットのうち、終点ポートが転送対象でないため転送しなかったものの数
Port	転送対象ポート番号

OutPackets	転送した UDP パケット数

表 62: COUNTER オプション

関連コマンド

ADD IP HELPER（176 ページ）
DELETE IP HELPER（231 ページ）
DISABLE IP HELPER（270 ページ）
ENABLE IP HELPER（301 ページ）

SHOW IP HOST

カテゴリー：IP / 名前解決

SHOW IP HOST

解説

IP ホストテーブルの内容を表示する。

入力・出力・画面例

```
Manager > show ip host

  IP Address          Host Name
--------------------------------------------------------------------------------
  192.168.10.1        bulbul
  192.168.10.2        hiyo
  192.168.10.4        suzuta
  192.168.10.5        orange
  192.168.10.6        shiro
  192.168.10.7        konyanko
  192.168.10.8        mikeo
  192.168.10.10       usako
  192.168.10.11       wagtail
  192.168.10.12       shirokuro
--------------------------------------------------------------------------------
```

IP Address	IP アドレス
Host name	ホスト名

表 63:

関連コマンド

ADD IP DNS（167 ページ）
ADD IP HOST（178 ページ）
DELETE IP DNS（228 ページ）
DELETE IP HOST（232 ページ）
DISABLE IP DNSRELAY（266 ページ）
ENABLE IP DNSRELAY（297 ページ）
FINGER
PING（319 ページ）
SET IP DNS（356 ページ）

SET IP DNS CACHE（358 ページ）
SET IP HOST（363 ページ）
SHOW IP DNS（445 ページ）
SHOW IP DNS CACHE（447 ページ）
TELNET（「運用・管理」の 380 ページ）

SHOW IP ICMPREPLY

カテゴリー：IP / 一般コマンド

SHOW IP ICMPREPLY

解説

ICMP メッセージの送信/非送信設定を表示する。

入力・出力・画面例

```
Manager > show ip icmpreply

SHOW IP ICMP REPLY MESSAGES
------------------------------------------------------------------------------
ICMP REPLY MESSAGES:
  Network Unreachable ................ disabled
  Host Unreachable ................... disabled
  Redirect ........................... enabled
------------------------------------------------------------------------------
```

ICMP REPLY MESSAGES	設定変更可能な ICMP メッセージと送信（enabled）/非送信（disable）

表 64:

関連コマンド

DISABLE IP ICMPREPLY（271 ページ）
ENABLE IP ICMPREPLY（302 ページ）

SHOW IP INTERFACE

カテゴリー：IP / IP インターフェース

SHOW IP INTERFACE[=*interface*] [COUNTER]

interface: IP インターフェース名（eth0、ppp0 など）

解説

IP インターフェースの情報を表示する。

パラメーター

INTERFACE　IP インターフェース名。省略時はすべてのインターフェースの情報が表示される。
COUNTER　このオプションを指定したときは、インターフェースのパケット送受信統計が表示される。

入力・出力・画面例

```
Manager > show ip interface

Interface     Type     IP Address       Bc Fr PArp  Filt RIP Met.   SAMode  IPSc
Pri. Filt     Pol.Filt Network Mask     MTU   VJC   GRE  OSPF Met.  DBcast  Mul.
VLAN Tag
-------------------------------------------------------------------------------
LOCAL         ---      Not set          -  -  -     ---  --         Pass    --
---           ---      Not set          1500  -     ---  --         ---     ---
none
vlan1         Static   172.28.28.186    1  n  On    ---  01         Pass    No
---           ---      255.255.255.0    1500  -     ---  0000000001 No      Rec
none          -
ppp0          Remote   10.0.0.200       1  n  -     ---  01         Pass    No
---           ---      255.255.255.255  1492  Off   ---  0000000001 No      Rec
none
ppp1#         Static   0.0.0.0          1  n  -     ---  01         Pass    No
---           ---      0.0.0.0          1492  Off   ---  0000000001 No      Rec
none
-------------------------------------------------------------------------------
```

Interface	インターフェース名。「Local」はローカル IP インターフェースを示す。名前の後の「#」は、該当インターフェースがリンクダウンしていることを示す
Type	インターフェース種別。Static（静的に設定されたインターフェース）、Dynamic（外部からの SLIP/PPP 接続によって動的に作成されたインターフェース）、Inactive（何らかの理由によりレイヤー 2 インターフェースとのバインドが切れたインターフェース）
IP Address	IP アドレス。0.0.0.0 は IP アドレスが決まっていないことを示す
Bc	ブロードキャストアドレスの表現方法。0 はオール 0、1 はオール 1 を示す。通常は 1
Fr	MTU 値を超えるパケットをフラグメント化するかどうか。y は DF ビットを無視して常にフラグメント化することを示す。n は DF ビットの指示に従うことを示す
PArp	プロキシー ARP が有効かどうかを示す
Filt	トラフィックフィルター番号
RIP Met.	RIP メトリック
IPSc	IPsec ポリシーが割り当てられているかどうか。Yes か No
Pri. Filt	プライオリティーフィルター番号
Pol.Filt	ポリシーフィルター番号
Network Mask	サブネットマスク。0.0.0.0 は DHCP 使用時などにサブネットマスクが未決定であることを示す
MTU	インターフェースの最大送信パケットサイズ（MTU）
VJC	VJ 圧縮（Van Jacobson の TCP/IP ヘッダー圧縮）を使用しているかどうか。PPP インターフェースでのみ有効
GRE	未サポート
OSPF Met.	OSPF メトリック
DBcast	このインターフェース下のネットワークに対するディレクティドブロードキャストを転送するかどうか。Yes または No
Mul.	マルチキャストパケットの扱い。On（送受信）、Rec（受信のみ）、Snd（送信のみ）、Off（送受信ともしない）

表 65:

Interface	インターフェース名。「Local」はローカル IP インターフェースを示す。名前の後の「#」は、該当インターフェースがリンクダウンしていることを示す
Type	インターフェース種別。Static（静的に設定されたインターフェース）、Dynamic（外部からの SLIP/PPP 接続によって動的に作成されたインターフェース）、Inactive（何らかの理由によりレイヤー 2 インターフェースとのバインドが切れたインターフェース）
ifInPkts	受信パケット数
ifOutPkts	送信パケット数
ifInBcastPkts	受信マルチキャストパケット数
ifOutBcastPkts	送信マルチキャストパケット数

ifInUcastPkts	受信ユニキャストパケット数
ifOutUcastPkts	送信ユニキャストパケット数
ifInDiscards	受信後に破棄したパケット数
ifOutDiscards	送信前に破棄したパケット数

表 66: COUNTER オプション

関連コマンド

ADD IP INTERFACE（179 ページ）
DELETE IP INTERFACE（233 ページ）
DISABLE IP INTERFACE（272 ページ）
ENABLE IP INTERFACE（303 ページ）
RESET IP INTERFACE（329 ページ）
SET IP INTERFACE（364 ページ）
SHOW IP COUNTER（437 ページ）

SHOW IP NAT

カテゴリー：IP / レンジ NAT

SHOW IP NAT [COUNTER] [SUMMARY]

解説

IP NAT（レンジ NAT）モジュールの設定、統計情報を表示する。

パラメーター

COUNTER　統計情報を表示する。
SUMMARY　概要だけを表示する。

入力・出力・画面例

```
Manager > show ip nat

IP NAT Configuration

Status  : Enabled
Logging : Disabled
Enhanced Fragment Handling : none
Maximum Packet Fragments : 20
------------------------------------------------------------------------------
Private IP : 192.168.10.0 - 192.168.10.255
Global Interface : eth1
  Method ................. Dynamic Interface ENAT
  Number of entries ....... 0
  Current port ............ 5024
------------------------------------------------------------------------------

Manager > show ip nat counter

IP NAT Counters

------------------------------------------------------------------------------
Private IP : 192.168.10.0 - 192.168.10.255
Global Interface : eth1
  Total packets received from private address(es) ....... 7
  Total packets received by global address(es) .......... 0
  Number of cache hits from private address(es) ......... 85
  Number of cache hits from global address(es) .......... 75
  Number of entries created for configuration ........... 7
  Number of dropped packets due to no match ............. 0
```

```
  Number of unknown IP protocols packets dropped ........ 0
  Number of unknown ICMP type packets dropped ........... 0
  Number of dropped ICMP packets ........................ 0
  Number of spoofing packets for private address(es) .... 0
  Number of dropped packets as global address zero ...... 0
  Number of dropped packets due to no spare entries ..... 0
  Number of FTP port commands processed ................. 0
  Number of FTP port commands dropped ................... 0
  Current entries:
    Protocol  PrivateIP:Port        GlobalIP:Port         DestinationIP:Port
    TCP       192.168.10.100:65210  172.17.28.185:26652   172.17.28.103:23
      Packets from private IP .............. 41
      Octets from private IP ............... 2348
      Packets to private IP ................ 33
      Octets to private IP ................. 3850
    UDP       192.168.10.100:63533  172.17.28.185:26107   172.17.28.1:53
      Packets from private IP .............. 1
      Octets from private IP ............... 70
      Packets to private IP ................ 1
      Octets to private IP ................. 180
    UDP       192.168.10.100:63534  172.17.28.185:17394   172.17.28.1:53
      Packets from private IP .............. 1
      Octets from private IP ............... 70
      Packets to private IP ................ 1
      Octets to private IP ................. 180
------------------------------------------------------------------------------
```

Status	NAT 機能の状態。Enabled または Disabled
Logging	ログに記録する NAT イベント。Disabled または Fails、InTCP、InUDP、OutTCP、OutUDP の組み合わせ
Enhanced Fragment Handling	フラグメント化を許可するプロトコル
Private IP	変換前のプライベート IP アドレス
Global IP	変換後のグローバル IP アドレス
Global interface	インターフェース NAT（GBLINT 指定によるダイナミック ENAT）における、グローバル IP アドレスの割り当てられたインターフェース
Method	NAT の種類。Static NAT、Dynamic NAT、Static ENAT、Dynamic ENAT、Interface ENAT のいずれか
Number of entries	アドレス変換テーブル内のエントリー数（TCP セッション、UDP フロー、ICMP リクエストなど）
Current port	ENAT で使用する変換後のポート番号の現在値
Protocol	IP 上のプロトコル。GRE、ICMP、OSPF、SA、TCP、UDP のいずれか、あるいは IP プロトコル番号
PrivateIP:Port	プライベート IP アドレス・ポート（変換前）
GlobalIP:Port	グローバル IP アドレス・ポート（変換後）

DestinationIP:Port	通信相手の IP アドレス・ポート
Start time	セッションあるいはフローの開始日時。SUMMARY オプション指定時には表示されない
TCP state	（TCP セッションのみ）TCP セッションの状態。SUMMARY オプション指定時には表示されない
ICMP type	（ICMP フローのみ）フローを開始したパケットの ICMP メッセージタイプ。SUMMARY オプション指定時には表示されない
Minutes to deletion	無通信状態になってから NAT エントリーを削除するまでの時間。SUMMARY オプション指定時には表示されない

表 67:

Private IP	変換前のプライベート IP アドレス
Global IP	変換後のグローバル IP アドレス
Global interface	インターフェース NAT（GBLINT 指定によるダイナミック ENAT）における、グローバル IP アドレスの割り当てられたインターフェース
Total packets received from private address(es)	NAT 対象のプライベート IP アドレスを始点とするパケット受信数
Total packets received by global address(es)	NAT 対象のグローバル IP アドレス宛てパケット受信数
Number of cache hits from private address(es)	NAT 対象のプライベート IP アドレスを始点とするパケットのうち、NAT テーブル登録済みのセッションと一致したものの数
Number of cache hits from global address(es)	NAT 対象のグローバル IP アドレス宛てのパケットのうち、NAT テーブル登録済みのセッションと一致したものの数
Number of entries created for configuration	これまでに作成されたセッションエントリーの数
Number of dropped packets due to no match	NAT テーブル内に該当するセッションがなかったため破棄されたパケットの数
Number of unknown IP protocols packets dropped	未サポートの IP プロトコル番号を持つため破棄されたパケットの数
Number of unknown ICMP type packets dropped	未サポートの ICMP タイプを持つため破棄されたパケットの数
Number of dropped ICMP packets	破棄された ICMP パケットの数
Number of spoofing packets for private address(es)	終点としてプライベート IP アドレスを指定していたため破棄されたパケットの数
Number of dropped packets as global address zero	インターフェース ENAT のエントリーにおいて、グローバル側インターフェースのアドレスが未決定などの理由で破棄されたパケットの数
Number of dropped packets due to no spare entries	NAT テーブルがいっぱいのため新規にセッションを登録できず破棄されたパケットの数
Number of FTP port commands processed	FTP の PORT コマンドを解釈・処理した回数
Number of FTP port commands dropped	FTP の PORT コマンドの解釈・処理に失敗した回数
Current entries セクション	NAT テーブルの内容が表示される
Protocol	IP プロトコル名またはプロトコル番号
PrivateIP:Port	該当セッションのローカル側プライベート IP アドレスおよびポート（変換前）

GlobalIP:Port	該当セッションのローカル側グローバル IP アドレスおよびポート（変換後）
DestinationIP:Port	該当セッションのリモート側 IP アドレスおよびポート
Packets from private IP	該当セッションのプライベート側ホストから受信したパケット数
Octets from private IP	該当セッションのプライベート側ホストから受信したオクテット数
Packets to private IP	該当セッションのプライベート側ホスト宛てに送信したパケット数
Octets to private IP	該当セッションのプライベート側ホスト宛てに送信したオクテット数

表 68: COUNTER オプション指定時

関連コマンド

ADD IP NAT（184 ページ）
DELETE IP NAT（235 ページ）
DISABLE IP NAT（273 ページ）
DISABLE IP NAT FRAGMENT（274 ページ）
DISABLE IP NAT LOG（275 ページ）
ENABLE IP NAT（305 ページ）
ENABLE IP NAT FRAGMENT（306 ページ）
ENABLE IP NAT LOG（307 ページ）

SHOW IP POOL

カテゴリー：IP / IP アドレスプール

SHOW IP POOL[=*pool-name*] [IP=*ipadd*[-*ipadd*]] [SUMMARY]

pool-name: IP プール名（1〜15 文字）
ipadd: IP アドレス

解説

IP アドレスプールの情報を表示する。

パラメーター

POOL　表示するプールの名前を指定する。無指定時はすべてのプールが表示される。
IP　　表示するプールアドレスの範囲を限定する。ハイフン区切りで範囲指定が可能
SUMMARY　本オプション指定時は IP プールのサマリー情報だけを表示する。

入力・出力・画面例

```
IP Pool
-------------------------------------------------------------------------------
Pool Name: dialin ( 192.168.1.1 - 192.168.1.8 )
Number of requests ..................... 102
Request successes ...................... 101
Request failures ....................... 1
Number in use .......................... 5
IP Address Interface Status Start Time End time
192.168.1.1 PPP0 inuse 24-Jun-1999 15:21:58
192.168.1.2 PPP1 free  24-Jun-1999 10:02:04 24-Jun-1999 16:23:50
192.168.1.3 PPP2 inuse 24-Jun-1999 15:32:17
192.168.1.4 PPP3 inuse 24-Jun-1999 15:36:01
192.168.1.5 PPP4 inuse 24-Jun-1999 15:37:46
192.168.1.6 PPP5 inuse 24-Jun-1999 15:51:06
192.168.1.7 PPP6 free 24-Jun-1999 15:59:51 24-Jun-1999 16:03:11
192.168.1.8       free never used
-------------------------------------------------------------------------------
```

Pool Name	IP プール名およびプールされている IP アドレスの範囲
Number of requests	IP プールに対するアドレス割り当て要求の回数
Request successes	IP アドレス割り当てに成功した回数
Request failures	IP アドレス割り当てに失敗した回数

Number in use	使用中のプールアドレス数
IP Address	プールされている IP アドレス
Interface	前回アドレス割り当てを要求したインターフェース
Status	割り当て状況。inuse または free
Start Time	割り当て開始日時
End Time	割り当て解除日時

表 69:

関連コマンド

CREATE IP POOL（217 ページ）
DESTROY IP POOL（254 ページ）

SHOW IP RIP

カテゴリー：IP / 経路制御（RIP）

SHOW IP RIP [INTERFACE=*interface*] [IP=*ipadd*]

interface: IP インターフェース名（eth0、ppp0 など）
ipadd: IP アドレス

解説

RIP の設定情報を表示する。

パラメーター

INTERFACE　IP インターフェース名。
IP　　指定した IP アドレスに関連する情報だけを表示する。

入力・出力・画面例

```
Manager > show ip rip

Interface  IP Address      Send  Receive  Demand  Static  Auth  Password
-------------------------------------------------------------------------
vlan1      -               RIP2  RIP2     OFF     YES     NONE
eth0       -               RIP2  RIP2     OFF     YES     NONE
-------------------------------------------------------------------------
```

Interface	RIP パケットを送受信するインターフェース
IP Address	隣接 RIP ルーター（ピア）の IP アドレス
Send	送信する RIP パケットの種類。NONE、RIP1、RIP2、COMP のいずれか
Receive	受信する RIP パケットの種類。NONE、RIP1、RIP2、BOTH のいずれか
Demand	トリガーアップデート（RFC1582）を使用するかどうか
Static	スタティック経路を通知するかどうか
Auth	RIP パケットの認証方式。NONE、PASS、MD5 のいずれか
Password	認証パスワード。設定時は「********」と表示される

表 70:

関連コマンド

ADD IP RIP（187 ページ）

DELETE IP RIP（236 ページ）
SET IP RIP（369 ページ）
SHOW IP（429 ページ）
SHOW IP COUNTER（437 ページ）

SHOW IP RIP COUNTER

カテゴリー：IP / 経路制御（RIP）

SHOW IP RIP COUNTER[={DETAIL|SUMMARY}] [INTERFACE=*interface*] [IP=*ipadd*]

interface: IP インターフェース名（eth0、ppp0 など）
ipadd: IP アドレス

解説

RIP に関する各種統計値を表示する。

パラメーター

COUNTER　情報の詳細さを指定する。DETAIL を指定した場合は、隣接 RIP ルーター（ピア）ごとの統計と全体の統計の両方が表示される。SUMMARY を指定した場合は、全体の統計だけが表示される。無指定の場合は SUMMARY と同様。

INTERFACE　IP インターフェース名

IP　指定した IP アドレスに関連する情報だけを表示する。

入力・出力・画面例

```
Manager > show ip rip counter

IP RIP Counter Summary:
  Input:                                    Output:
    inResponses ................... 95       outResponses ................. 190
    inTrigRequests ................ 0        outTrigRequests ............... 0
    inTrigResponses ............... 0        outTrigResponses .............. 0
    inTrigAcks .................... 0        outTrigAcks ................... 0
    inDiscards .................... 0
```

inResponses	RIP Response パケット受信数
inTrigRequests	Triggered Request パケット受信数
inTrigResponses	Triggered Response パケット受信数
inTrigAcks	Triggered Acknowledgement パケット受信数
inDiscards	認証失敗、受信ディセーブル時の受信パケット、Triggered Acknowledgement のシーケンス番号不一致などが原因で破棄したパケット数
outResponses	RIP Response パケット送信数
outTrigRequests	Triggered Request パケット送信数

outTrigResponses	Triggered Response パケット送信数
outTrigAcks	Triggered Acknowledgement パケット送信数

表 71:

関連コマンド

SHOW IP COUNTER（437 ページ）
SHOW IP RIP（468 ページ）

SHOW IP RIPTIMER

カテゴリー：IP / 経路制御（RIP）

SHOW IP RIPTIMER

解説

RIP タイマーの設定情報を表示する。

入力・出力・画面例

```
Manager > show ip riptimer

IP RIP timers
Timer name    Default     Current
-----------------------------------
Update        30          30
Invalid       180         180
Holddown      120         120
Flush         300         300
-----------------------------------
```

Timer name	タイマー名称
Default	デフォルト値（秒）
Current	現在値（秒）
Update	アップデートタイマー。RIP 更新パケットの送信間隔（秒）。RIP オンデマンドを使用していないすべてのインターフェースで共通
Invalid	ルートタイムアウト。経路が更新されない場合に、該当する経路情報を無効と見なすまでの期間（秒）
Holddown	ホールドダウンタイム。ルートタイムアウトにより無効（メトリック 16）となった経路エントリーを無効状態のまま保持する期間（秒）。この期間中は、該当経路の更新情報を受け取ってもエントリーを更新せず、無効状態のまま止めおく
Flush	最後の更新パケット受信から経路情報が削除されるまでの期間（秒）

表 72:

関連コマンド

SET IP RIPTIMER（371 ページ）

SHOW IP ROUTE

カテゴリー：IP / 経路制御（スタティック）

SHOW IP ROUTE[=*ipadd*] [{GENERAL|CACHE|COUNT}]

ipadd: IP アドレス

解説

IP ルーティングテーブルを表示する。

パラメーター

ROUTE　表示させたい経路の宛先ネットワークアドレス。ワイルドカード（*）の指定も可能で、「192.*.*.*」と指定すると「192」で始まる経路だけが表示される。省略時はすべての経路が表示される。

GENERAL　ルーティングに関するサマリーを表示する。

CACHE　ルートキャッシュの内容を表示する。ROUTE パラメーター指定時は該当する経路だけが表示される。

COUNT　経路ごとの送受信オクテット数を表示する。送受信オクテット数は、ENABLE IP ROUTE コマンドでルートカウンター（COUNT オプション）を有効にしているときだけカウントされる。

入力・出力・画面例

```
Manager bulbul> show ip route

IP Routes
-------------------------------------------------------------------------------
Destination       Mask              NextHop             Interface           Age
                  Type     Policy   Protocol            Metrics      Preference
-------------------------------------------------------------------------------
0.0.0.0           0.0.0.0           0.0.0.0             ppp0                570
                  direct   0        static              1                   360
10.100.200.30     255.255.255.255   0.0.0.0             ppp0                570
                  direct   0        interface           1                     0
172.26.0.0        255.255.0.0       0.0.0.0             ppp1                570
                  direct   0        static              1                    60
172.26.190.136    255.255.255.255   0.0.0.0             ppp1                543
                  direct   0        interface           1                     0
192.168.1.0       255.255.255.0     0.0.0.0             vlan1               570
                  direct   0        interface           1                     0
-------------------------------------------------------------------------------

Manager > show ip route general
```

```
IP Route General Information
----------------------------
Number of routes ............... 3
Cache size ..................... 1024
Source route byte counting ..... no
Route debugging ................ no
Multipath routing .............. yes

Manager > show ip route cache

IP Route Cache
------------------------------------------------------------------------------
Destination      Route            Route mask       Nexthop          Interface
------------------------------------------------------------------------------
192.168.100.2    192.168.100.0    255.255.255.0    0.0.0.0          eth1
192.168.10.100   192.168.10.0     255.255.255.0    0.0.0.0          eth0
            hits:          2          misses:          7
------------------------------------------------------------------------------

Manager > show ip route count

Route Counters

 IP address       NextHop         Interface  Metric  Octets rcvd   Octets sent
------------------------------------------------------------------------------
 192.168.10.0     0.0.0.0         eth0          1          27864         27864
 192.168.20.0     192.168.100.2   eth1          2          12384         12384
 192.168.100.0    0.0.0.0         eth1          1          15480         15480
------------------------------------------------------------------------------
```

Destination	経路の宛先ネットワークアドレス
Mask	サブネットマスク
NextHop	ネクストホップルーターの IP アドレス
Interface	本経路宛てのパケットを送出するインターフェース。名前の後の「#」は、該当インターフェースがリンクダウンしていることを示す
Age	経路情報取得後の経過時間
Type	経路エントリーの種類。remote、direct、other のいずれか
Policy	本経路のサービスタイプ（経路選択ポリシー）
Protocol	経路情報のソースプロトコル。インターフェース経路（interface）、静的経路（static）、RIP（rip）、OSPF（ospf）、BGP-4（bgp）、ルートテンプレート（template）がある
Metrics	メトリック（コスト）
Preference	経路選択時の優先度。小さいほど優先度が高い

表 73:

Number of routes	経路エントリー数
Cache size	ルートキャッシュサイズ（バイト）
Source route byte counting	ソースルートバイトカウンティングの有効・無効（ENABLE IP ROUTE COUNT）
Route debugging	経路デバッグの有効・無効
Multipath routing	等価コストマルチパスルーティングの有効・無効（ENABLE IP ROUTE MULTIPATH）

表 74: GENERAL オプション

Destination	宛先 IP アドレス
Route	宛先ネットワークアドレス
Route mask	サブネットマスク
NextHop	ネクストホップルーターの IP アドレス
Interface	送出インターフェース。名前の後の「#」は、該当インターフェースがリンクダウンしていることを示す

表 75: CACHE オプション

IP address	経路の宛先ネットワークアドレス
NextHop	ネクストホップルーターの IP アドレス
Interface	送出インターフェース。名前の後の「#」は、該当インターフェースがリンクダウンしていることを示す
Metric	メトリック（コスト）
Octets rcvd	本経路経由で受信したオクテット数
Octets sent	本経路経由で送信したオクテット数

表 76: COUNT オプション

関連コマンド

ADD IP ROUTE（189 ページ）
DELETE IP ROUTE（237 ページ）
DISABLE IP ROUTE（277 ページ）
ENABLE IP ROUTE（309 ページ）
SET IP ROUTE（372 ページ）

SHOW IP ROUTE FILTER

カテゴリー：IP / 経路制御フィルター

SHOW IP ROUTE FILTER

解説

IP ルートフィルターの情報を表示する。

入力・出力・画面例

```
Manager > show ip route filter

IP Route Filters
-------------------------------------------------------------------------------
Ent.    IP Address        Mask              Nexthop           Policy      Matched
        Protocol          Direction         Interface         Action
-------------------------------------------------------------------------------
  1     200.200.20.*      *.*.*.*           Any               -                 0
        Any               Both              -                 Exclude
  2     *.*.*.*           *.*.*.*           Any               -                 0
        Any               Both              -                 Include

        Request: 4                Passes: 4               Fails: 0
-------------------------------------------------------------------------------
```

Ent.	フィルターエントリー番号
IP Address	宛先ネットワークアドレス
Mask	ネットワークマスク
Nexthop	ネクストホップアドレス
Policy	TOS 値
Matched	該当エントリーのマッチ回数
Protocol	ルーティングプロトコル
Direction	フィルターの適用方向。Receive（受信時）、Send（送信時）、Both（送受信時）のいずれか
Interface	フィルターが適用されているインターフェース
Action	フィルターアクション。Include（許可）または Exclude（拒否）

表 77:

関連コマンド

ADD IP ROUTE FILTER（191 ページ）
DELETE IP ROUTE FILTER（238 ページ）
SET IP ROUTE FILTER（374 ページ）

SHOW IP ROUTE PREFERENCE

カテゴリー：IP / 経路制御（スタティック）

SHOW IP ROUTE PREFERENCE

解説

経路制御プロトコルによって学習した経路の優先度（preference）を表示する。

入力・出力・画面例

```
Manager > show ip route preference

IP Route Preference
-------------------------------------------------------------------------------
 Protocol                          Preference
-------------------------------------------------------------------------------
 RIP ............................. 100 (default)
 OSPF-INTRA ...................... 10 (default)
 OSPF-INTER ...................... 11 (default)
 OSPF-EXT1 ....................... 150 (default)
 OSPF-EXT2 ....................... 151 (default)
 OSPF-OTHER ...................... 152 (default)
 BGP-INT ......................... 170 (default)
 BGP-EXT ......................... 170 (default)
-------------------------------------------------------------------------------
```

Protocol	経路種別。詳細は SET IP ROUTE PREFERENCE コマンドの表を参照
Preference	経路選択時の優先度。デフォルト値のときは「(default)」と表示される、

表 78:

関連コマンド

SET IP ROUTE PREFERENCE（376 ページ）

SHOW IP ROUTE TEMPLATE

カテゴリー：IP / 経路制御

SHOW IP ROUTE TEMPLATE[=*template*]

template: ルートテンプレート名（1〜31 文字。大文字小文字を区別しない）

解説

IP ルートテンプレートの情報を表示する。

パラメーター

TEMPLATE　テンプレート名。指定時は該当テンプレートの詳細情報が表示される。省略時は全テンプレートのサマリー情報が表示される。

入力・出力・画面例

```
Manager > show ip route template

  Template                          Interface
  ------------------------------------------------------------------
  net10                             ppp0
  net20                             ppp0
  ------------------------------------------------------------------

Manager > show ip route template=net10

  IP route template ................... net10
  Interface ........................... ppp0
  Next hop ............................ 0.0.0.0
  Rip metric .......................... 2
  Ospf metric ......................... DEFAULT (FFFFFFFF)
  Policy .............................. DEFAULT (0)
  Preference .......................... DEFAULT (FFFFFFFF)
```

Template	テンプレート名
Interface	IP インターフェース名

表 79:

IP route template	テンプレート名

Interface	IP インターフェース名
Next hop	ネクストホップアドレス
Rip metric	RIP メトリック
Ospf metric	OSPF メトリック
Policy	サービスタイプ（TOS）
Preference	経路選択時の優先度
Dlci	未サポート

表 80: テンプレート名指定時

関連コマンド

ADD IP ROUTE TEMPLATE（193 ページ）
CREATE IPSEC POLICY（「IPsec」の 39 ページ）
DELETE IP ROUTE TEMPLATE（239 ページ）
SET IP ROUTE TEMPLATE（378 ページ）

SHOW IP ROUTEMAP

カテゴリー：IP / 経路制御（BGP-4）

SHOW IP ROUTEMAP[=*routemap*]

routemap: ルートマップ名（0〜15 文字。英数字とアンダースコアを使用可能。大文字小文字を区別する）

解説

ルートマップの情報を表示する。

パラメーター

ROUTEMAP　ルートマップ名。省略時はすべてのルートマップが表示される。

入力・出力・画面例

```
Manager > show ip routemap
IP route Maps

Map Name
  Entry       Action
      Clauses
-------------------------------------------------------------
color_slow_path
  1           Include
         set   Community   1000 Add=no
-------------------------------------------------------------
add_myasn_twice
  1           Include
       match   Community   1 Exact=no
         set   AS-path     65010 65010
-------------------------------------------------------------
```

Map name	ルートマップ名
Entry	エントリー番号
Action	エントリーのアクション
Clauses	SET 節、MATCH 節の設定内容。MATCH 節はマッチング条件。SET 節はマッチした経路エントリーに対する属性設定の内容

表 81:

関連コマンド

ADD IP ROUTEMAP（195 ページ）
DELETE IP ROUTEMAP（240 ページ）
SET IP ROUTEMAP（379 ページ）

SHOW IP TRUSTED

カテゴリー：IP / 経路制御フィルター

SHOW IP TRUSTED

解説

RIP の Trusted Router リストを表示する。

入力・出力・画面例

```
Manager > show ip trusted


   Host address
------------------
   192.168.1.100
   172.16.28.32
   172.16.28.169
------------------
```

関連コマンド

ADD IP FILTER（169 ページ）
ADD IP TRUSTED（198 ページ）
DELETE IP FILTER（230 ページ）
DELETE IP TRUSTED（241 ページ）
SET IP FILTER（360 ページ）
SHOW IP FILTER（449 ページ）

SHOW IP UDP

カテゴリー：IP / 一般コマンド

SHOW IP UDP

解説

UDP リスニングポートの状態を表示する。

入力・出力・画面例

```
Manager > show ip udp

   Local port     Local address     Remote port
-------------------------------------------------
    1698          0.0.0.0            4660
     520          0.0.0.0               0
     500          0.0.0.0             500
    5023          0.0.0.0            5023
    5024          0.0.0.0            5024
     514          0.0.0.0             514
-------------------------------------------------
```

Local port	ローカル側 UDP ポート
Local address	ローカル側 IP アドレス
Remote port	リモート側 UDP ポート

表 82:

関連コマンド

SHOW IP COUNTER（437 ページ）
SHOW TCP（519 ページ）

SHOW OSPF

カテゴリー：IP / 経路制御（OSPF）

SHOW OSPF

解説

OSPF モジュールのグローバル設定情報を表示する。

入力・出力・画面例

```
Manager > show ospf

Router ID ..................... 1.1.1.1
OSPF module status ............. Enabled
Area border router status ..... Yes
AS border router status ........ Disabled
PTP stub network generation ..... Enabled
External LSA count ............. 2
External LSA sum of checksums ... 77843
New LSAs originated ............ 17
New LSAs received .............. 31
RIP ............................ None
Dynamic interface support ..... None
Number of active areas ......... 2
Logging ........................ Disabled
Debugging ...................... Disabled
AS external default route:
  Status ....................... Disabled
  Type ......................... 1
  Metric ....................... 1

OSPF thread debugging

  Total thread entries ... 15479
  Packet entries ......... 581
  Timer entries .......... 14898
  Command busy entries ... 0
  Highest timer tick ..... 1

Timer LSA timestamping
  N ......... 1489
  Sum ....... 32722
  Num LSAs .. 14
  Lo ........ 6
  Hi ........ 24
```

```
SPF timestamping
  N ......... 6
  Sum ....... 8524
  Lo ........ 936
  Hi ........ 2354
```

Router ID	ルーター ID
OSPF module status	OSPF モジュールの有効・無効
Area border router status	エリア境界ルーター（ABR）として動作中かどうか
AS border router status	AS 境界ルーター（ASBR）として動作中かどうか
PTP stub network generation	PPP インターフェースがリンクアップしたときに、対応する LSA を動的作成するかどうか
External LSA count	トポロジーデータベース内の AS 外部 LSA の数
External LSA sum of checksums	AS 外部 LSA のチェックサム合計値。ルーター間でトポロジーデータベースを比較するためのもの
New LSAs originated	本システムが送信した新規 LSA の数
New LSAs received	本システムが受信した新規 LSA の数
RIP	RIP と情報の交換を行うかどうか。None（交換しない）、Import（RIP の情報を取り込む）、Export（RIP に情報を提供する）、Import/export（RIP と OSPF の間で情報を相互に交換する）
Dynamic interface support	ダイナミックインターフェースの経路情報をインポートするかどうか。Stub（ホスト経路としてインポート）、AS external（AS 外部 LSA としてインポート）、None（インポートしない）、Undefined（未指定）のいずれか
Number of active areas	本システム上で定義されているエリアの数
Logging	OSPF イベントをログに記録するかどうか（ENABLE OSPF LOG コマンド）
Debugging	OSPF モジュールのデバッグ機能の有効・無効（ENABLE OSPF DEBUG コマンド）
AS external default route	AS 外部 LSA に関する情報が表示される
Status	デフォルト経路（0.0.0.0）の AS 外部 LSA を生成するかどうか
Type	デフォルト経路の AS 外部 LSA タイプ。タイプ 1、タイプ 2 または Undefined
Metric	デフォルト AS 外部 LSA のメトリック

表 83:

関連コマンド

SET OSPF（381 ページ）

SHOW OSPF AREA

カテゴリー：IP / 経路制御（OSPF）

SHOW OSPF AREA[={BACKBONE|*area-number*}] [{FULL|SUMMARY}]

area-number: OSPF エリア ID（a.b.c.d の形式）

解説

OSPF エリアに関する情報を表示する。

パラメーター

AREA　エリア ID。省略時はすべてのエリアに関する情報が表示される。指定時は該当エリアの詳細な情報が表示される。

FULL　詳細な情報を表示する。

SUMMARY　サマリー情報を表示する。

入力・出力・画面例

```
Manager > show ospf area


Area             State     Authentication  StubArea  StubMetric  Summary LSAs
--------------------------------------------------------------------------------
Backbone         Active       None            No             1       Send
1.1.1.1          Active       None            Yes            1       None
--------------------------------------------------------------------------------

Manager > show ospf area=1.1.1.1

Area 1.1.1.1:
  State ......................... Active
  Authentication ................ None
  Stub area ..................... Yes
  Stub Cost ..................... 1
  Summary LSAs .................. None
  SPF runs ...................... 6
  Area border router count ...... 1
  AS border router count ........ 0
  LSA count ..................... 2
  LSA sum of checksums .......... 39181

  Ranges:
    Range 172.16.0.0:
```

```
    Mask ..................... 255.255.192.0

Interfaces:
  eth0:
    Type ..................... Broadcast
    State .................... DR
```

Area	エリア ID
State	エリアの状態。エリアの範囲と所属するインターフェースが設定されていれば Active、そうでなければ Inactive と表示される
Authentication	受信 OSPF パケットの認証方式。None（無認証）または Password（簡易パスワード認証）
StubArea	スタブエリアかどうか
StubMetric	スタブエリア内に通知するデフォルトルート（デフォルトサマリー LSA）のメトリック
Summary LSAs	デフォルト経路以外のサマリー LSA をスタブエリア内に通知するかどうか。Send（通知する）、None（通知しない）、Undefined（未定義）

表 84:

Area	エリア ID
State	エリアの状態。エリアの範囲と所属するインターフェースが設定されていれば Active、そうでなければ Inactive と表示される
Authentication	受信 OSPF パケットの認証方式。None（無認証）または Password（簡易パスワード認証）
Stub area	スタブエリアかどうか
Stub Cost	スタブエリア内に通知するデフォルトルート（デフォルトサマリー LSA）のメトリック
Summary LSAs	デフォルト経路以外のサマリー LSA をスタブエリア内に通知するかどうか。Send（通知する）、None（通知しない）、Undefined（未定義）
SPF runs	エリア内部の経路表を再計算した回数
Area border router count	エリア内にあるエリア境界ルーター（ABR）の数
AS border router count	エリア内にある AS 境界ルーター（ASBR）の数
LSA count	該当エリアのトポロジーデータベースに格納されている LSA の合計数。AS 外部 LSA は除く
LSA sum of checksums	該当エリアの LSA チェックサムの合計値。ルーター間でトポロジーデータベースの同一性をチェックするために使用される
Range	エリアを構成するネットワークのベースアドレス
Mask	Range に対するネットマスク
Interfaces	エリアに所属する OSPF インターフェース
Type	インターフェースタイプ。Unknown（不明）、Broadcast（ブロードキャスト型）、NMBA（非ブロードキャスト型）、Point to Point（ポイントツーポイント型）、Virtual（仮想インターフェース）のいずれか
State	OSPF インターフェースとしての状態。unknown（不明）、down（送受信を行わない初期状態）、loopback（ループバック状態）、waiting（Hello パケットをモニターしてバックアップ DR の存在を確認している状態）、ptp（仮想リンクに接続されている状態）、DR（DR に選出されている状態）、backupDR（バックアップ DR に選出されている状態）、otherDR（DR、バックアップ DR のいずれにも選出されていない状態）のいずれか

表 85: エリア指定時

関連コマンド

ADD OSPF AREA（199 ページ）
ADD OSPF RANGE（208 ページ）
DELETE OSPF AREA（242 ページ）
DELETE OSPF RANGE（247 ページ）
RESET OSPF COUNTER（331 ページ）
SET OSPF AREA（384 ページ）
SET OSPF RANGE（390 ページ）
SHOW OSPF RANGE（505 ページ）

SHOW OSPF DEBUG

カテゴリー：IP / 経路制御（OSPF）

SHOW OSPF DEBUG

解説

OSPF モジュールの内部デバッグ情報を表示する。

入力・出力・画面例

```
Manager > show ospf debug

OSPF event timers
Delay      Event          Argument
-------------------------------------------------------------------------------
    0.2   LSDBTIMER      -
    4.5   HELLO          Int: eth0
    4.5   HELLO          Int: eth1
   31.1   NBR_INACT      Nbr: eth1, 192.168.10.2
   36.8   NBR_INACT      Nbr: eth1, 192.168.10.3
   39.1   NBR_INACT      Nbr: eth1, 192.168.10.4
  274.5   REFRESHLSA     LSA: Summary, 0.0.0.0, area=1.1.1.1
  309.3   REFRESHLSA     LSA: Router, 1.1.1.1, area=1.1.1.1
  329.0   REFRESHLSA     LSA: Router, 1.1.1.1, area=0.0.0.0
  341.2   REFRESHLSA     LSA: Summary, 172.16.0.0, area=0.0.0.0
-------------------------------------------------------------------------------

OSPF SPF list
Area            Vertex ID       Type Dist  #NH Next hop        Int
-------------------------------------------------------------------------------
0.0.0.0         1.1.1.1         Rou     0   0
                192.168.10.4    Net     1   1  0.0.0.0         eth1
                4.4.4.4         Rou     1   1  192.168.10.4    eth1
                2.2.2.2         Rou     1   1  192.168.10.2    eth1
                3.3.3.3         Rou     1   1  192.168.10.3    eth1
1.1.1.1         1.1.1.1         Rou     0   0
-------------------------------------------------------------------------------
```

SHOW OSPF HOST

カテゴリー：IP / 経路制御（OSPF）

SHOW OSPF HOST[=*ipadd*] [AREA={BACKBONE|*area-number*}]

ipadd: IP アドレス
area-number: OSPF エリア ID（a.b.c.d の形式）

解説

OSPF ルーティングテーブルにスタティック登録されたホスト経路（ネットマスクが 255.255.255.255 の経路）の情報を表示する。

パラメーター

HOST　ホストの IP アドレス
AREA　ホストの所属エリア

入力・出力・画面例

```
Manager > show ospf host


IP address       Mask             State     Area            Metric  TOS  Type
-------------------------------------------------------------------------------
192.168.10.100   255.255.255.255  Active    Backbone             1    0  Stat
-------------------------------------------------------------------------------
```

IP address	ホストまたは Point-to-Point ネットワークの IP アドレス
Mask	ネットマスク
State	経路エントリーの状態。Active か Inactive
Area	所属エリア ID
Metric	メトリック
TOS	サービスタイプ（TOS）
Type	エントリータイプ。Stat（スタティック経路）、Dyn（ダイナミック経路）のいずれか

表 86:

関連コマンド

ADD OSPF HOST（201 ページ）

DELETE OSPF HOST（243 ページ）
SET OSPF HOST（385 ページ）

SHOW OSPF INTERFACE

カテゴリー：IP / 経路制御（OSPF）

SHOW OSPF INTERFACE[=*interface*] [AREA={BACKBONE|*area-number*}]
[IPADDRESS=*ipadd*] [{FULL|SUMMARY}]

interface: IP インターフェース名（eth0、ppp0 など）または仮想インターフェース名（VIRTn）
area-number: OSPF エリア ID（a.b.c.d の形式）
ipadd: IP アドレス

解説

OSPF インターフェースの情報を表示する。

パラメーター

INTERFACE IP インターフェース名、または仮想インターフェース名（VIRTn）。省略時は全インターフェースのサマリー情報が表示される。インターフェース指定時は該当インターフェースの詳細情報が表示される。
AREA エリア ID
IPADDRESS インターフェースの IP アドレス
FULL 詳細な情報を表示する。
SUMMARY サマリー情報を表示する。

入力・出力・画面例

```
Manager > show ospf interface


                                                Designated rtr   Backup DR
Iface    Status    Area             State      / Virtual nbr    / Transit area
-------------------------------------------------------------------------------
eth0     Enabled   1.1.1.1          DR         172.16.0.1       None
eth1     Enabled   Backbone         otherDR    192.168.10.4     192.168.10.3
-------------------------------------------------------------------------------

Manager > show ospf interface=eth1

eth1:
  Status ..................... Enabled
  Area ....................... Backbone
  IP address ................. 192.168.10.1
  IP net mask ................ 255.255.255.0
  IP network number ..... 192.168.10.0
```

```
Type ........................... Broadcast
OSPF on demand ................. OFF (OFF)
State .......................... otherDR
Router priority ................ 1
Transit delay .................. 1 second
Retransmit interval ............ 5 seconds
Hello interval ................. 10 seconds
Router dead interval ........... 40 seconds
Interface events ............... 2
Password .......................
Designated router .............. 192.168.10.4
Backup designated router ...... 192.168.10.3
Metric boost 1 ................. 0
```

Status	インターフェースの管理ステータス
Area	所属エリア
State	OSPF インターフェースとしての状態。unknown（不明）、down（送受信を行わない初期状態）、loopback（ループバック状態）、waiting（Hello パケットをモニターしてバックアップ DR の存在を確認している状態）、ptp（仮想リンクに接続されている状態）、DR（DR に選出されている状態）、backupDR（バックアップ DR に選出されている状態）、otherDR（DR、バックアップ DR のいずれにも選出されていない状態）のいずれか
Designated rtr / Virtual nbr	通常の IP インターフェースの場合は、配下ネットワークの指名ルーター（DR）。仮想インターフェース（VIRTn）の場合は、仮想リンクの対向に位置するバックボーンルーター（ABR）
Backup DR / Transit area	通常の IP インターフェースの場合は、配下ネットワークのバックアップ指名ルーター。仮想インターフェース（VIRTn）の場合は、仮想リンクの通過エリア ID

表 87: インターフェース省略時または SUMMARY オプション指定時

Status	インターフェースの管理ステータス
Area	所属エリア
IP address	IP アドレス
IP net mask	ネットマスク
IP network number	IP ネットワークアドレス
Type	配下ネットワークの種別。Broadcast（ブロードキャスト）、NBMA（非ブロードキャスト）、Point to Point（ポイントツーポイント）、Unknown（不明）、Virtual（仮想）のいずれか
OSPF on demand	インターフェースがオンデマンドリンクとして設定されているかどうか。仮想インターフェースの場合は常に ON。ポイントツーポイントインターフェースの場合は、リモートエンドとのネゴシエーション結果がカッコ内に表示される
State	OSPF インターフェースとしての状態。unknown（不明）、down（送受信を行わない初期状態）、loopback（ループバック状態）、waiting（Hello パケットをモニターしてバックアップ DR の存在を確認している状態）、ptp（仮想リンクに接続されている状態）、DR（DR に選出されている状態）、backupDR（バックアップ DR に選出されている状態）、otherDR（DR、バックアップ DR のいずれにも選出されていない状態）のいずれか
Router priority	ルーター優先度。大きいほど DR になる可能性が高い。0 は DR の資格がないことを示す
Transit delay	本インターフェースにおけるリンク状態更新パケットの送信遅延時間。通常は 1（秒）
Retransmit interval	データベース記述パケット（タイプ 2）、リンク状態要求パケット（タイプ 3）、リンク状態更新パケット（タイプ 4）の再送信間隔
Hello interval	Hello パケット（タイプ 1）の送信間隔
Router dead interval	隣接ルーターからの Hello パケットが途絶えてから、隣接ルーターがダウンしたと見なすまでの時間
Poll interval	非ブロードキャスト型のネットワークにおいて、アクティブでないと思われる隣接ルーターに対する Hello パケットによるポーリング間隔
Interface events	OSPF インターフェースの状態が変化した回数とエラーが発生した回数の合計
Password	認証用パスワード。エリアの認証方式が PASSWORD（簡易パスワード認証）のときに有効
Designated router	配下ネットワークの指名ルーター（DR）
Backup designated router	配下ネットワークのバックアップ指名ルーター
Virtual neighbour	仮想リンクの対向に位置するバックボーンルーター（ABR）
Transit area	仮想リンクの通過エリア ID

表 88: インターフェース指定時または FULL オプション指定時

関連コマンド

ADD OSPF INTERFACE（202 ページ）
DELETE OSPF INTERFACE（244 ページ）
RESET OSPF COUNTER（331 ページ）
SET OSPF INTERFACE（386 ページ）

SHOW OSPF LSA

カテゴリー：IP / 経路制御（OSPF）

SHOW OSPF LSA=*link-id* [AREA={BACKBONE|*area-number*}] [{FULL|SUMMARY}]
[TYPE={ASEXTERNAL|ASBRSUMMARY|ASSUMMARY|IPSUMMARY|SUMMARY|NETWORK|
ROUTER}]

link-id: リンク状態 ID（IP アドレスと同じ形式）
area-number: OSPF エリア ID（a.b.c.d の形式）

解説

トポロジーデータベースに格納されているリンク情報（LSA）を表示する。

パラメーター

LSA リンク状態 ID。省略時はすべてのリンク情報が簡潔に表示される。指定時は該当リンクの詳細な情報が表示される。「0」によるワイルドカード指定も可能で、「172.16.0.0」のように指定すると「172.16」ではじまるすべてのリンク状態 ID にマッチする。

AREA エリア ID。指定時は該当エリアに所属するリンク情報だけが表示される。「0」によるワイルドカード指定が可能。

FULL 詳細な情報を表示させたいときに指定する。

SUMMARY サマリー情報を表示させたいときに指定する。

TYPE 表示する LSA のタイプを指定する。ASEXTERNAL（AS 外部（タイプ 5））、ASBRSUMMARY、ASSUMMARY（ASBR サマリー（タイプ 4））、IPSUMMARY、SUMMARY（ネットワークサマリー（タイプ 3））、NETWORK（ネットワーク（タイプ 2））、ROUTER（ルーター（タイプ 1））から選択する。省略時はすべての LSA が表示される。

入力・出力・画面例

```
Manager > show ospf lsa

 Type        LS ID            Router ID        Sequence    Age    Len  Csum
-------------------------------------------------------------------------------
Area backbone:
 Router      1.1.1.1          1.1.1.1          80000005   1520     36  68d1
 Router      2.2.2.2          2.2.2.2          80000004   1525     36  2c06
 Router      3.3.3.3          3.3.3.3          80000004   1516     36  ed3b
 Router      4.4.4.4          4.4.4.4          80000008   1521     36  a774
 Network     192.168.10.4     4.4.4.4          80000003   1526     40  215f
 Summary     172.16.0.0       1.1.1.1          80000008   1508     28  a50e
 Summary     172.16.64.0      2.2.2.2          80000009   1497     28  c2ab
 Summary     172.16.128.0     3.3.3.3          80000006   1509     28  e745
```

```
 Summary     172.16.192.0     4.4.4.4          8000000b   1436     28  fce6
 AsSummary   4.4.4.5          4.4.4.4          80000002   1436     28  48d0

Area 1.1.1.1:
 Router      1.1.1.1          1.1.1.1          80000002   1540     36  0766
 Summary     0.0.0.0          1.1.1.1          80000002   1574     28  91a7

External:
 AsExternal  10.1.0.0         4.4.4.5          80000001   1455     36  9e04
 AsExternal  10.2.0.0         4.4.4.5          80000001   1455     36  920f
--------------------------------------------------------------------------------

Manager > show ospf lsa area=backbone full

 Type        LS ID            Router ID        Sequence    Age    Len  Csum
--------------------------------------------------------------------------------
Area backbone:
 Router      1.1.1.1          1.1.1.1          80000005   1529     36  68d1
   Options: --B   Number of links:   1
     Link   1:  Type: Transit   ID: 192.168.10.4      Data: 192.168.10.1
       TOS 0 metric:     1    Number of other metrics: 0
 Router      2.2.2.2          2.2.2.2          80000004   1534     36  2c06
   Options: --B   Number of links:   1
     Link   1:  Type: Transit   ID: 192.168.10.4      Data: 192.168.10.2
       TOS 0 metric:     1    Number of other metrics: 0
 Router      3.3.3.3          3.3.3.3          80000004   1525     36  ed3b
   Options: --B   Number of links:   1
     Link   1:  Type: Transit   ID: 192.168.10.4      Data: 192.168.10.3
       TOS 0 metric:     1    Number of other metrics: 0
 Router      4.4.4.4          4.4.4.4          80000008   1530     36  a774
   Options: --B   Number of links:   1
     Link   1:  Type: Transit   ID: 192.168.10.4      Data: 192.168.10.4
       TOS 0 metric:     1    Number of other metrics: 0
 Network     192.168.10.4     4.4.4.4          80000003   1535     40  215f
   Network Mask: 255.255.255.0
     Attached router: 4.4.4.4
     Attached router: 1.1.1.1
     Attached router: 2.2.2.2
     Attached router: 3.3.3.3
 Summary     172.16.0.0       1.1.1.1          80000008   1517     28  a50e
   Network Mask: 255.255.192.0
     TOS:  0  Metric:        1
 Summary     172.16.64.0      2.2.2.2          80000009   1506     28  c2ab
   Network Mask: 255.255.192.0
     TOS:  0  Metric:        1
 Summary     172.16.128.0     3.3.3.3          80000006   1518     28  e745
   Network Mask: 255.255.192.0
     TOS:  0  Metric:        1
 Summary     172.16.192.0     4.4.4.4          8000000b   1445     28  fce6
   Network Mask: 255.255.192.0
     TOS:  0  Metric:        1
```

```
AsSummary   4.4.4.5          4.4.4.4          80000002   1445     28  48d0
  Network Mask: 0.0.0.0
    TOS:  0  Metric:        1
```

Type	LSA タイプ。Router（ルーター LSA）、Network（ネットワーク LSA）、Summary（ネットワークサマリー LSA）、AsSummary（ASBR サマリー LSA）、A s External（AS 外部 LSA）がある
LS ID	リンク状態 ID。LSA タイプによって意味が異なる（別表参照）
RouterID	LSA 通知ルーター ID
Sequence	LSA シーケンス番号（32 ビットの符号付き整数）
Age	LSA エイジ（Link State Age）。LSA 生成後の推定経過時間（秒）。最大値は 3600 秒
Len	LSA の長さ（バイト）。LSA ヘッダー 20 バイトを含む
Csum	LSA チェックサム。LSA エイジフィールドを除く。LSA を比較するときに用いられる

表 89:

Type	LSA タイプ。Router（ルーター LSA）、Network（ネットワーク LSA）、Summary（ネットワークサマリー LSA）、AsSummary（ASBR サマリー LSA）、A s External（AS 外部 LSA）がある
LS ID	リンク状態 ID。LSA タイプによって意味が異なる（別表参照）
Router ID	LSA 通知ルーター ID
Sequence	LSA シーケンス番号（32 ビットの符号付き整数）
Age	LSA エイジ（Link State Age）。LSA 生成後の推定経過時間（秒）。最大値は 3600 秒
Len	LSA の長さ（バイト）。LSA ヘッダー 20 バイトを含む
Csum	LSA チェックサム。LSA エイジフィールドを除く。LSA を比較するときに用いられる
Router	ルーター LSA に関する情報
Options	ルーター LSA のオプションフラグ。生成元ルーターの種類を示す。B（ABR）、E（ASBR）、V（仮想リンクの終端ルーター）、-（フラグがセットされていない）
Number of links	LSA 内のリンク数
Link	LSA 内でのリンク番号
Type	リンクタイプ
ID	リンク ID。リンクの対向に位置するルーターの ID またはインターフェースアドレス
Data	リンクデータ。リンクタイプによって意味が異なる。Stub の場合はサブネットマスク、それ以外は LSA を生成したルーターの IP アドレス

TOS 0 metric	デフォルトサービスタイプ（TOS=0）のメトリック
Number of other metrics	サービスタイプ（TOS）数。デフォルト TOS 以外のメトリックエントリー数
TOS	サービスタイプ（TOS）別メトリックエントリー
Metric	サービスタイプ（TOS）別のメトリック値
Network	ネットワーク LSA に関する情報
Network mask	ネットワークマスク
Attached router	該当ネットワークに接続されているルーターの ID
Summary	ネットワークサマリー LSA に関する情報
AsSummary	ASBR サマリー LSA に関する情報
AsExternal	AS 外部 LSA に関する情報
Forward	サービスタイプ別の転送先 IP アドレス。同一ネットワーク上によりよい経路がある場合に使用される
Tag	外部経路タグ。ASBR 間（他のルーティングプロトコル間）の通信に使われるもので OSPF では使用しない

表 90: FULL オプション指定時

LSA タイプ	**リンク状態 ID**
ルーター LSA（タイプ 1）	LSA を生成したルーターの ID
ネットワーク LSA（タイプ 2）	指名ルーター（DR）の IP アドレス
ネットワークサマリー LSA（タイプ 3）	宛先ネットワークアドレス
ASBR サマリー LSA（タイプ 4）	AS 境界ルーター（ASBR）の ID
AS 外部 LSA（タイプ 5）	宛先ネットワークアドレス

表 91: LSA タイプとリンク状態 ID

SHOW OSPF MD5KEY

カテゴリー：IP / 経路制御（OSPF）

SHOW OSPF MD5KEY [INTERFACE=*interface*]

interface: IP インターフェース名（eth0、ppp0 など）または仮想インターフェース名（VIRTn）

解説

OSPF インターフェースで使用する MD5 ダイジェスト認証用の鍵を表示する。

パラメーター

INTERFACE　OSPF インターフェース名。省略時はすべての OSPF インターフェースが対象となる。

入力・出力・画面例

```
Manager > show ospf md5key

OSPF MD5 keys
-----------------------------------------
Interface   ID    Key               Active
-----------------------------------------
vlan10      1     kadjfkadhfhad     No
            2     Bhpoia8f723ad9    Yes

vlan20      1     132p98yfHU        Yes
-----------------------------------------
```

Interface	OSPF インターフェース
ID	鍵番号（Key ID）
Key	鍵の値
Active	該当鍵が現在使用中かどうか

表 92:

関連コマンド

ADD OSPF AREA（199 ページ）
ADD OSPF INTERFACE（202 ページ）
ADD OSPF MD5KEY（205 ページ）
DELETE OSPF MD5KEY（245 ページ）

SET OSPF AREA（384 ページ）
SET OSPF INTERFACE（386 ページ）
SHOW OSPF AREA（487 ページ）
SHOW OSPF INTERFACE（493 ページ）

SHOW OSPF NEIGHBOUR

カテゴリー：IP / 経路制御（OSPF）

SHOW OSPF NEIGHBOUR[=*ipadd*] [INTERFACE=*interface*]

ipadd: IP アドレス
interface: IP インターフェース名（eth0、ppp0 など）または仮想インターフェース名（VIRTn）

解説

隣接する OSPF ルーターの情報を表示する。

パラメーター

NEIGHBOUR　隣接ルーターの IP アドレス。指定時は該当隣接ルーターのみ、省略時はすべての隣接ルーターに関する情報が表示される。

INTERFACE　IP インターフェース名。指定時は該当インターフェース下に存在する隣接ルーターだけが表示される。

入力・出力・画面例

```
Manager > show ospf neighbour


IP address       State     Interface  Router ID        Priority  LSRxmtQ  Type
-------------------------------------------------------------------------------
192.168.10.2     twoWay     eth1      2.2.2.2             1         0    Dyn
192.168.10.3     full       eth1      3.3.3.3             1         0    Dyn
192.168.10.4     full       eth1      4.4.4.4             1         0    Dyn
-------------------------------------------------------------------------------
```

IP address	隣接ルーターの IP アドレス
State	隣接ルーター（との通信）の状態。Down（初期状態）、Attempt（静的設定された隣接ルーターに Hello を送り、通信を試行中）、Init（該当ルーターから Hello を受信したが、まだ通信は片方向）、Two-Way（双方向の通信が確立した）、ExStart（隣接関係の確立開始）、Exchange（DD パケットの交換中）、Loading（データベースの同期をとるため LSR パケットで最新情報を要求）、Full（隣接関係の完成）のいずれか

Interface	隣接ルーターが存在するインターフェース
Router ID	隣接ルーターの ID
Priority	隣接ルーターの DR 優先度（隣接ルーターからの Hello パケットで示された値）
LSRxmtQ	LSA 再送信キューの長さ
Type	隣接ルーターの種別。Dyn（動的に発見した隣接ルーター）、Stat（静的に設定した隣接ルーター）

表 93:

関連コマンド

ADD OSPF NEIGHBOUR（207 ページ）
DELETE OSPF NEIGHBOUR（246 ページ）
RESET OSPF COUNTER（331 ページ）
SET OSPF NEIGHBOUR（389 ページ）

SHOW OSPF RANGE

カテゴリー：IP / 経路制御（OSPF）

SHOW OSPF RANGE[=*ipadd*] [AREA={BACKBONE|*area-number*}]

ipadd: IP アドレス
area-number: OSPF エリア ID（a.b.c.d の形式）

解説

本システム上で定義されているエリアの構成ネットワーク範囲の情報を表示する。

パラメーター

RANGE　レンジアドレス。省略時はすべてのレンジが表示される。
AREA　OSPF エリア ID。省略時はすべてのエリアが表示される。

入力・出力・画面例

```
Manager > show ospf range


Base IP address    State     Mask             Area             Effect
-------------------------------------------------------------------------------
172.16.0.0         Active    255.255.192.0    1.1.1.1          Advertise
192.168.10.0       Active    255.255.255.0    Backbone         Advertise
-------------------------------------------------------------------------------
```

Base IP address	ネットワーク範囲のベースアドレス
State	該当ネットワーク範囲の状態。Active または Inactive。アクティブなエリアに関連付けられているときに Active と表示される
Mask	ネットマスク
Area	所属エリア ID
Effect	該当アドレス範囲の経路情報をネットワークサマリー LSA でエリア外部に通知するかどうか。「Advertise」（通知する）か「Do not advertise」（通知しない）のいずれか

表 94:

関連コマンド

ADD OSPF RANGE（208 ページ）

DELETE OSPF RANGE（247 ページ）
SET OSPF AREA（384 ページ）

SHOW OSPF REDISTRIBUTE

カテゴリー：IP / 経路制御（OSPF）

SHOW OSPF REDISTRIBUTE

解説

スタティック経路を AS 外部 LSA で AS 内に通知するときのメトリックとメトリックタイプの設定（ADD OSPF REDISTRIBUTE コマンドで設定したもの）を表示する。
本コマンドは AS 境界ルーター（ASBR）でのみ意味を持つ。

入力・出力・画面例

```
Manager > show ospf redistribute
OSPF Redistribute

Protocol     Metric       RouteMap           Subnet   Tag          Type
-------------------------------------------------------------------------
Static       100          -                  YES      0            Ext1
```

Protocol	AS 外部経路の起源。現在有効な値は Static（スタティック経路）のみ
Metric	Protocol 欄に示された起源を持つ AS 外部経路のメトリック
RouteMap	未サポート
Subnet	未サポート
Tag	未サポート
Type	Protocol 欄に示された起源を持つ起源を持つ AS 外部経路のメトリックタイプ。Ext1（タイプ 1）か Ext2（タイプ 2）

表 95:

関連コマンド

ADD OSPF REDISTRIBUTE（210 ページ）
DELETE OSPF REDISTRIBUTE（248 ページ）
SET OSPF REDISTRIBUTE（391 ページ）

SHOW OSPF ROUTE

カテゴリー：IP / 経路制御（OSPF）

SHOW OSPF ROUTE[=*ipadd*] [AREA={BACKBONE|*area-number*}] [TYPE={AB|ASBR}]

ipadd: IP アドレス
area-number: OSPF エリア ID（a.b.c.d の形式）

解説

エリア境界ルーター（ABR）および AS 境界ルーター（ASBR）への経路情報を表示する。

パラメーター

ROUTE　経路の宛先となるルーターの ID。「0」によるワイルドカード指定も可能で、「172.16.0.0」のように指定すると「172.16」ではじまるすべてのルーター ID にマッチする。省略時はすべての経路が表示される。

AREA　エリア ID。省略時はすべてのエリアが対象となる。

TYPE　経路の種類。AB は ABR への経路、ASBR は ASBR への経路だけを表示する。省略時はすべての経路が表示される。

入力・出力・画面例

```
Manager > show ospf route

OSPF Routes

Destination       Mask              NextHop             Interface           Age
DLCI/Circ.        Type     Policy   Protocol            Metrics      Preference
-------------------------------------------------------------------------------
Area backbone AB routes:
4.4.4.4           255.255.255.255   192.168.10.4        eth1                 0
-                 ospfAB   0        ospf                1                   10
3.3.3.3           255.255.255.255   192.168.10.3        eth1                 0
-                 ospfAB   0        ospf                1                   10
2.2.2.2           255.255.255.255   192.168.10.2        eth1                 0
-                 ospfAB   0        ospf                1                   10

ASBR routes:
4.4.4.5           255.255.255.255   192.168.10.4        eth1                 0
-                 ospfAS   0        ospf                2                   11
-------------------------------------------------------------------------------
```

Destination	ABR/ASBR のルーター ID
DLCI/Circ.	未サポート
Mask	経路マスク。常に 255.255.255.255
Type	経路エントリータイプ。ospfAB（ABR への経路）、ospfAS（ASBR への経路）のいずれか
Policy	ルーティングポリシー。常に 0
NextHop	ネクストホップルーター。宛先に直接到達できる場合は 0.0.0.0
Protocol	経路情報のソースプロトコル。常に ospf
Interface	同経路宛てのパケットを送出するインターフェース
Metrics	メトリック
Age	経路情報の年齢（秒）
Preference	送出時の優先度。エリア内の経路は 10、エリアをまたぐ経路は 11

表 96:

関連コマンド

SHOW OSPF AREA（487 ページ）
SHOW OSPF INTERFACE（493 ページ）
SHOW OSPF RANGE（505 ページ）

SHOW OSPF STUB

カテゴリー：IP / 経路制御（OSPF）

SHOW OSPF STUB[=*ipadd*] [AREA={BACKBONE|*area-number*}]

ipadd: IP アドレス
area-number: OSPF エリア ID（a.b.c.d の形式）

解説

OSPF を使用していないネットワーク（スタブネットワーク）へのスタティックな経路情報を表示する。

パラメーター

STUB　スタブネットワークのネットワークアドレス
AREA　OSPF エリア ID

入力・出力・画面例

```
Manager > show ospf stub


IP address       Mask             State     Area            Metric  TOS  Type
-------------------------------------------------------------------------------
192.168.10.100   255.255.255.255  Active    Backbone             1    0  Stat
-------------------------------------------------------------------------------
```

IP address	スタブネットワークのネットワークアドレス
Mask	ネットマスク
State	経路エントリーの状態。Active または Inactive。Active なエントリーはルーター LSA で通知される
Area	所属エリア ID
Metric	メトリック
TOS	サービスタイプ（TOS）
Type	エントリータイプ。Stat（スタティックエントリー）、Dyn（ダイナミックエントリー）のどちらか

表 97:

関連コマンド

ADD OSPF STUB（211 ページ）
DELETE OSPF STUB（249 ページ）
SET OSPF STUB（392 ページ）

SHOW OSPF SUMMARYADDRESS

カテゴリー：IP / 経路制御（OSPF）

SHOW OSPF SUMMARYADDRESS

解説

AS 外部経路の集約設定（集約経路エントリー）の一覧を表示する。

入力・出力・画面例

```
Manager > show ospf summaryaddress


Base IP address     Mask             Advertise        Tag
--------------------------------------------------------------------------------
192.168.0.0         255.255.0.0      Yes              0
--------------------------------------------------------------------------------
```

Base IP address	集約後のネットワークアドレス
Mask	Base IP address に対するネットワークマスク
Advertise	集約経路（Base IP address/Mask）を AS 外部 LSA で AS 内に通知するかどうか。Yes（通知する）、No（通知しない）のいずれか
Tag	集約経路の AS 外部 LSA にセットする外部経路タグ値

表 98:

関連コマンド

ADD OSPF SUMMARYADDRESS（212 ページ）
DELETE OSPF SUMMARYADDRESS（250 ページ）
SET OSPF SUMMARYADDRESS（393 ページ）

SHOW PING

カテゴリー：IP / 一般コマンド

SHOW PING

解説

PING コマンドのデフォルト設定、および、実行中あるいは前回の PING に関する情報を表示する。

入力・出力・画面例

```
Manager > show ping

Ping Information
--------------------------------------------------------------------------------
Defaults:
  Type ........................... -
  Source ......................... Undefined
  Destination .................... Undefined
  Number of packets .............. 5
  Size of packets (bytes) ....... 24
  Timeout (seconds) .............. 1
  Delay (seconds) ................ 1
  Data pattern ................... Not set
  Type of service ................ 0
  Direct output to screen ....... Yes

Current:
  Type ........................... IP
  Source ......................... 172.16.28.160
  Destination .................... 172.16.28.1
  Number of packets .............. 5
  Size of packets (bytes) ....... 24
  Timeout (seconds) .............. 1
  Delay (seconds) ................ 1
  Data pattern ................... Not set
  Type of service ................ 0
  Direct output to screen ....... Yes


Results:
  Ping in progress ............... No
  Packets sent ................... 5
  Packets received ............... 5
  Round trip time minimum (ms) .. 0
  Round trip time average (ms) .. 0
  Round trip time maximum (ms) .. 0
```

```
  Last message ................. Finished succesfully
-------------------------------------------------------------------------------
```

Type	ネットワーク層プロトコル。IP（IPv4）、IPV6 のいずれか
Source	PING パケットの始点 IP（IPv4、IPv6）アドレス
Destination	PING パケットの終点 IP アドレスまたはホスト名
Number of packets	送信パケット数
Size of packets (bytes)	PING パケットのデータサイズ（バイト）
Timeout (seconds)	タイムアウト（秒）
Delay (seconds)	パケット送信間隔（秒）
Data pattern	データ部分のバイナリーパターン（4 バイト）
Type of service	PING パケットの TOS 値（IPv4 のみ）
Direct output to screen	結果を端末画面に出力するかどうか
Ping in progress	現在 PING を実行中かどうか
Packets sent	送信パケット数
Packets received	受信パケット数
Round trip time minimum (ms)	最小往復時間（ミリ秒）
Round trip time average (ms)	平均往復時間（ミリ秒）
Round trip time maximum (ms)	最大往復時間（ミリ秒）
Last message	前回 PING コマンドを実行したときのメッセージ

表 99:

関連コマンド

PING（319 ページ）
SET PING（394 ページ）
STOP PING（525 ページ）

SHOW PING POLL

カテゴリー：IP / Ping ポーリング

SHOW PING POLL[=*poll-id*] [COUNTER] [FULL] [STATE={UP|DOWN|CRITICAL}]

poll-id: Ping ポーリング ID（1〜100）

解説

Ping ポーリングの設定または統計カウンターを表示する。

パラメーター

POLL　Ping ポーリング ID。指定時は、指定した ID の設定が詳細に表示される。省略時は全 ID の設定が簡潔に一覧表示される。

COUNTER　ポーリングカウンターを表示する。POLL パラメーターに ID を指定したとき、または、FULL オプションを指定した場合だけ有効。

FULL　POLL パラメーターに ID を指定しなかった場合に、全 ID の詳細情報を表示する。POLL パラメーターに ID を指定した場合は、本パラメーターの有無は意味を持たない。

STATE　指定した状態にあるものだけを表示させたいときに指定する。UP（Up）、DOWN（Down）、CRITICAL（Critical Up と Critical Down）のどれかを指定する。省略時は状態にかかわらずすべての ID が対象になる。

入力・出力・画面例

```
Manager > show ping poll

Ping Status
--------------------------------------------------------------------------
ID   State                    Destination
      upCountCurrent   Upcount   failCountCurrent   Failcount/Sample Size
--------------------------------------------------------------------------
1    Up                       172.17.28.100
      14               30        0                  5/5
--------------------------------------------------------------------------

Manager > show ping poll=1

Ping Polling Information
------------------------------------------------------------------------------
Poll 1:
  Destination IP address ..............172.17.28.100
  Description .........................
  State ..............................Critical Up
```

```
  Poll enabled ....................... Yes
  Normal interval (seconds) ........... 30
  Critical interval (seconds) ......... 1
  Samplesize .......................... 5
  Failcount ........................... 5
  Upcount ............................. 30
  Timeout (seconds) ................... 1
  Source IP address ................... -
  Length (bytes) ...................... 32

------------------------------------------------------------------------------
Manager > show ping poll=1 counter

Ping Polling Information
------------------------------------------------------------------------------
Poll 1:
  Destination IP address .............. 172.17.28.100
  Description .........................
  State ............................... Down
  Poll enabled ........................ Yes
  Normal interval (seconds) ........... 30
  Critical interval (seconds) ......... 1
  Samplesize .......................... 5
  Failcount ........................... 5
  Upcount ............................. 30
  Timeout (seconds) ................... 1
  Source IP address ................... -
  Length (bytes) ...................... 32

 Counters:
  upStateEntered .................. 1     downStateEntered .................. 2
  pingsSent ....................... 98     pingsFailedUpstate ................ 10
  pingsFailedDownstate ........... 35
  upCountCurrent .................. 0     failCountCurrent .................. 5
------------------------------------------------------------------------------
```

ID	Ping ポーリング ID
State	対象機器の状態（Up、Critical Up、Critical Down、Down）
Destination	対象機器の IP アドレス
upCountCurrent	「応答あり」の連続回数。「Down」状態、「Critical Down」状態から「Up」状態に遷移するには、本カウンターの値が Upcount に達する必要がある。1 度でも無応答があると、本カウンターはゼロになる
Upcount	「Down」状態、「Critical Down」状態から「Up」状態に遷移するために必要な連続した「応答あり」の回数
failCountCurrent	直前の Samplesize 回における「無応答」の回数。本カウンターの値が Failcount に達すると、「Down」状態に遷移する

Failcount/Sample Size	「Up」状態、「Critical Up」状態から「Down」状態に遷移するために必要な「無応答」の回数（Failcount）と、到達性判断のために結果（応答、無応答）を保持しておく Ping パケットの数（Sample Size）

表 100: POLL 無指定時および FULL 省略時

Poll	Ping ポーリング ID
Destination IP address	対象機器の IP アドレス
Description	メモ
State	対象機器の状態（Up、Critical Up、Critical Down、Down）。ポーリングが停止状態のときは「-」と表示される
Poll enabled	ポーリングを実行中かどうか。Yes（実行中）、No（停止中）のどちらか
Normal interval (seconds)	「Up」状態におけるポーリング間隔（秒）
Critical interval (seconds)	「Up」状態以外（Critical Up、Critical Down、Down）におけるポーリング間隔（秒）
Samplesize	到達性判断のために結果（応答、無応答）を保持しておく Ping パケットの数
Failcount	「Up」状態、「Critical Up」状態から「Down」状態に遷移するために必要な「無応答」の回数
Upcount	「Down」状態、「Critical Down」状態から「Up」状態に遷移するために必要な連続した「応答あり」の回数
Timeout (seconds)	Ping パケットの応答待ち時間（秒）
Source IP address	Ping パケットの始点 IP アドレス。未指定（システムが自動的に判断）のときは「-」と表示される
Length (bytes)	Ping パケットのデータ長（バイト）

表 101: POLL または FULL 指定時

upStateEntered	「Down」状態、「Critical Down」状態から「Up」状態に遷移した回数（DEVICEUP = 到達性回復イベントの発生回数）。
downStateEntered	「Up」状態、「Critical Up」状態から「Down」状態に遷移した回数（DEVICEDOWN = 到達性喪失イベントの発生回数）
pingsSent	送信した Ping パケットの総数
pingsFailedUpstate	「Up」状態、「Critical Up」状態のときに発生した無応答の回数
pingsFailedDownstate	「Down」状態、「Critical Down」状態のときに発生した無応答の回数
upCountCurrent	「応答あり」の連続回数。「Down」状態、「Critical Down」状態から「Up」状態に遷移するには、本カウンターの値が Upcount に達する必要がある。1 度でも無応答があると、本カウンターはゼロになる
failCountCurrent	直前の Sample Size 回における「無応答」の回数。「Up」状態、「Critical Up」状態において、本カウンターの値が Failcount に達すると、「Down」状態に遷移する

表 102: COUNTER 指定時（カウンター項目のみ。他は表 2 と同じ）

関連コマンド

ADD PING POLL（213 ページ）
DISABLE PING POLL（283 ページ）
ENABLE PING POLL（316 ページ）
RESET PING POLL（334 ページ）
SET PING POLL（396 ページ）

SHOW TCP

カテゴリー：IP / 一般コマンド

SHOW TCP[=*tcb*]

tcb: TCP コネクション番号

解説

TCP に関する情報を表示する。

パラメーター

TCP　TCP コネクション番号を指定。SHOW TCP コマンドで表示される Connection Table の Index。

入力・出力・画面例

```
Manager > show tcp

  TCP MIB parameters, counters and connections
------------------------------------------------------------------------
  RTO Algorithm:           vanj
  RTO Min (ms):      0000000080   RTO Max (ms):    0000010000

  Maximum connections:    01000

  Active Opens:           00000   Passive Opens:        00005
  Attempt Fails:          00000   Established Resets:   00000
  Current Established:    00002

  In Segs:           0000000052   In Segs Error:   0000000000
  Out Segs:          0000000048   Out Segs Retran: 0000000000
  Out Segs With RST: 0000000000

  Connection Table:
  Index   Proto   State
          Local port and address
          Remote port and address
  ------------------------------------------------------------------------
      0   IPv4   listen
          00023  0.0.0.0
          00000  0.0.0.0
  ------------------------------------------------------------------------
      1   IPv6   listen
          00023  ::
          00000  ::
```

```
  ------------------------------------------------------------------------
      2   IPv4   listen
          00080  0.0.0.0
          00000  0.0.0.0
  ------------------------------------------------------------------------
      3   IPv6   established
          00023  3ffe:0b80:003c:0001::0001
          01030  3ffe:0b80:003c:0001:0290:99ff:fe1e:e00a
  ------------------------------------------------------------------------
      4   IPv4   established
          00023  192.168.1.1
          65156  192.168.10.103
  ------------------------------------------------------------------------

Manager > show tcp=4

  TCB: 4  Local: 192.168.1.1,00023  Remote: 192.168.10.103,65156
  State: ESTAB  O/P State: IDLE
  SND.UNA: 2109324330  SND.NXT: 2109324330  SND.WND: 17520
  Last Seq: 3298709664  Last Ack: 2109324330
  SendCon: 17068  DataCount: 0000000000
  RCV.NXT: 3298709664  RCV.WND: 01024
  Round Trip Time
  SendSrt: 00037  Deviation: 00018  SendReXmit: 00025
  Timers:
  Event       Time (cs)
  No events in timer queue
  Fragment list:
  Sequence     Length    End sequence
  No fragments in fragment list
```

RTO Algorithm	TCPセグメントの再送時間決定アルゴリズム。vanjはVan Jacobsonのアルゴリズムを示す
RTO Min (ms), RTO Max (ms)	再送タイマーの最小値と最大値（ミリ秒）
Maximum connections	サポートするTCPコネクションの最大数
Active Opens	アクティブオープン回数
Passive Opens	パッシブオープン回数
Attempt Fails	TCPコネクションの確立に失敗した回数
Established Resets	コネクションをリセットした回数
Current Established	現在確立中のコネクション数
In Segs	受信したTCPセグメント数
In Segs Error	受信したTCPセグメントのうちエラーがあったものの数
Out Segs	送信したTCPセグメント数
Out Segs Retran	再送したTCPセグメント数
Out Segs With RST	送信したTCPセグメントのうち、RSTフラグがオンに設定されていたものの数

Connection Table セクション	TCP コネクションの一覧が表示される
Index	個々のコネクションを識別するインデックス番号。SHOW TCP コマンド、DELETE TCP コマンドで使用する
Proto	プロトコルファミリー。IPv4 か IPv6
State	TCP コネクションの状態。別表を参照
Local port and address	コネクションのローカル側 TCP ポート番号と IP アドレス
Remote Port and address	コネクションのリモート側 TCP ポート番号と IP アドレス

表 103: コネクション番号無指定時

CLOSED	TCP 状態遷移図の起点および終点
LISTEN	リモートからの接続要求を待ち受けている状態（パッシブオープン）
SYNSENT	リモート側に接続要求（SYN）を送信した状態（アクティブオープン）
SYNRECEIVED	リモート側から接続要求（SYN）を受信した状態
ESTABLISHED	コネクションが確立している状態。ローカル・リモートの両エンド間に信頼性のある全二重通信路が構築されている状態
FINWAIT1	リモート側に切断要求（FIN）を送信した状態（アクティブクローズ）。これに対し、CLOSEWAIT はリモート側から切断要求（FIN）を受信した状態
FINWAIT2	アクティブクローズのため送信した切断要求（FIN）に対して、送達確認（ACK）を受信した状態。リモートエンドからの FIN 待ち状態
CLOSEWAIT	リモート側から切断要求（FIN）を受信した状態
LASTACK	リモート側からの切断要求（FIN）に対して送達確認（ACK）を返し、さらにリモート側に切断要求（FIN）を送信した状態。最後の送達確認（ACK）待ちの状態
CLOSING	同時クローズを実行した状態。両エンドがほぼ同時に切断要求（FIN) を送信し（FINWAIT1 状態に遷移）、その後ほぼ同時に FIN を受信した状態
TIMEWAIT	アクティブクローズの最終段階として、リモート側からの切断要求（FIN）に対し最後の ACK を送信した状態。最後の ACK が失われる可能性を考慮して、TIMEWAIT 状態の間（2*MSL)、コネクションの情報を保持しておく。この期間がすぎると CLOSED 状態に戻る

表 104: TCP コネクションの状態

TCB	TCP コネクションを識別するインデックス番号
Local	ローカル側 IP アドレスと TCP ポート番号
Remote	リモート側 IP アドレスと TCP ポート番号
State	TCP コネクションの状態。FREE、CLOSD、LISTN、SYNSN、SYNRC、ESTAB、FINW1、FINW2、CLOSW、LSTAK、CLOSG、TIMEW、DELET のいずれか
O/P State	送信キューの状態。IDLE（アイドル状態）、PERST（受信側のウィンドウがクローズされているため、1 バイト単位でデータを送信して受信側のウィンドウオープンを促している状態）、TRANS（送信データがある状態）、RETRN（データを再送している状態）がある
SND.UNA	まだ ACK を受け取っていない最後の送信データのシーケンス番号
SND.NXT	次に送信するデータのシーケンス番号
SND.WND	送信ウィンドウサイズ
Last Seq	最後に受信したセグメントのシーケンス番号
Last Ack	最後に受信した送達確認（ACK）
SendCon	内部的な輻輳パラメーター
DataCount	送信したデータのオクテット数
RCV.NXT	次に受信すると期待されるセグメントのシーケンス番号
RCV.WND	受信ウィンドウサイズ
SendSrt, Deviation, SendReXmit	Van Jacobson の再送時間決定アルゴリズムが使用する往復時間（RTT）関連パラメーター
Event	タイマーキューイベント。NONE、SEND（データ送信）、PERSIST（1 バイトずつデータを送信。O/P State が PERST 状態のとき）、TRANSMIT（データ再送）、DELETE（TCP コネクションをクリア）
Time (cs)	イベントの時間（1/100 秒）
Sequence	再構成待ちフラグメントの最初のシーケンス番号
Length	フラグメント長
End sequence	フラグメントの最終シーケンス番号

表 105: コネクション番号指定時

関連コマンド

DELETE TCP（252 ページ）
SHOW IP COUNTER（437 ページ）
SHOW IP UDP（484 ページ）

SHOW TRACE

カテゴリー：IP / 一般コマンド

SHOW TRACE

解説

TRACE コマンドのデフォルト設定、および、実行中あるいは前回のトレースルートに関する情報を表示する。

入力・出力・画面例

```
Manager > show trace

Trace information
--------------------------------------------------------------------------------
Defaults:
  Destination ..................... 0.0.0.0
  Source .......................... 0.0.0.0
  Number of packets per hop ..... 3
  Timeout (seconds) ............. 3
  Type of service ............... 0
  Port ........................... 33434
  Minimum time to live .......... 1
  Maximum time to live .......... 30
  Addresses only output ......... Yes
  Direct output to screen ....... Yes

Current:
  Destination ..................... 172.16.212.32
  Source .......................... 0.0.0.0
  Number of packets per hop ..... 3
  Timeout (seconds) ............. 3
  Type of service ............... 0
  Port ........................... 33434
  Minimum time to live .......... 1
  Maximum time to live .......... 30
  Addresses only output ......... Yes
  Direct output to screen ....... Yes


Results:
  Trace route in progress ....... No

 1. 172.16.28.32         9      9     10 (ms)
 2. 172.16.31.33         5      5      6 (ms)
 3. ***
```

```
 4. 172.16.16.32          9     10     11 (ms)
 5. 172.16.244.33        88     91     96 (ms)

  Last message ..................
Target reached
-------------------------------------------------------------------------------
```

Destination	トレースルートの目的地
Source	トレースルートパケットの始点 IP アドレス
Number of packets per	各ホップで送信するパケットの数
Timeout	各パケットのタイムアウト値
Type of service	トレースルートパケットの TOS 値
Port	終点 UDP ポート番号
Minimum time to live	1 個目のパケットの TTL。最初の数ホップをスキップするためのもの
Maximum time to live	最大ホップ数
Addresses only output	名前解決をするかどうか
Direct output to screen	結果を端末画面に表示するかどうか
Trace route in progress	現在トレースルートを実行中かどうか
1- n	ホップ数、ゲートウェイの IP アドレス、最大、最小、平均往復時間（ミリ秒）
Last message	前回 TRACE コマンド実行時のメッセージ

表 106:

関連コマンド

SET TRACE（398 ページ）
STOP TRACE（526 ページ）
TRACE（527 ページ）

STOP PING

カテゴリー：IP / 一般コマンド

STOP PING

解説

実行中の PING を停止する

関連コマンド

PING（319 ページ）
SET PING（394 ページ）
SHOW PING（513 ページ）

STOP TRACE

カテゴリー：IP / 一般コマンド

STOP TRACE

解説

実行中のトレースルートを停止する。

関連コマンド

SET TRACE（398 ページ）
SHOW TRACE（523 ページ）
TRACE（527 ページ）

TRACE

カテゴリー：IP / 一般コマンド

TRACE [[IPADDRESS=]{*ipadd*|*hostname*}] [MAXTTL=*1..255*] [MINTTL=*1..255*]
[NUMBER=*1..100*] [PORT=*port*] [SCREENOUTPUT={YES|NO}] [SOURCE=*ipadd*]
[TIMEOUT=*0..65535*] [TOS=*0..255*]

ipadd: IP アドレス（IPv4 または IPv6）
hostname: ホスト名
port: UDP ポート番号（0～65535）

解説

指定したアドレスまでの経路をトレースする。
指定しなかったパラメーターについては、SET TRACE コマンドで設定したデフォルト値が用いられる。

パラメーター

IPADDRESS 宛先 IP アドレス（IPv4、IPv6）。ホストテーブルに登録されているホスト名も使用可能。また、ADD IP DNS コマンドで DNS サーバーのアドレスを設定している場合は DNS に登録されているホスト名（ドメイン名）も使用可能。

MAXTTL 最大ホップ数。トレースルートの範囲をここで指定したホップ数までに制限する。

MINTTL 最小ホップ数。1 個目のパケットの TTL フィールドには MINTTL の値が設定される。最初の数ホップをスキップするために使用する。

NUMBER 各ホップで送信するパケットの数。最大 100 個。デフォルトは 3 個。

PORT トレースパケットの終点 UDP ポート。未使用と思われるポートを指定する。デフォルトは 33434。

SCREENOUTPUT 端末画面に結果を出力するかどうか。デフォルトは YES。NO を指定した場合、SHOW TRACE コマンドで結果を見ることができる。

SOURCE 始点 IP アドレス。省略時は送信インターフェースの IP アドレスが使われる。

TIMEOUT ホップごとの応答待ち時間。デフォルトは 3 秒。

TOS IPv4 の場合は TOS オクテットフィールドの値。IPv6 の場合は Traffic Class フィールドの値を指定する。0～255 の 10 進数値で指定する。

入力・出力・画面例

```
Manager > trace 172.16.212.32

Trace from 0.0.0.0 to 172.16.212.32, 1-30 hops
 0. 172.16.28.32          9      9     10 (ms)
 1. 172.16.31.1           5      5      6 (ms)
 2. ***                   ?      ?      ? (ms)
 3. 172.16.16.3           9     10     11 (ms)
```

```
 4. 172.16.244.33       88     91     96 (ms)
***
Target reached

Manager > trace 3ffe:b80:3c:10:200:f4ff:fec4:463

Trace from 3ffe:0b80:003c:0030:0290:99ff:fe1b:600a to 3ffe:0b80:003c:0010:0200:f
4ff:fec4:0463, 1-30 hops
 0. 3ffe:0b80:003c:0030::0001                    2      3      4 (ms)
 1. 3ffe:0b80:003c:0020::0001                    3      3      4 (ms)
 2. 3ffe:0b80:003c:0100::0001                    4      5      6 (ms)
 3. 3ffe:0b80:003c:0010:0200:f4ff:fec4:0463      4      5      6 (ms)
***
Target reached
```

関連コマンド

ADD IP DNS（167 ページ）
ADD IP HOST（178 ページ）
ADD IPV6 HOST（「IPv6」の 44 ページ）
SET TRACE（398 ページ）
SHOW TRACE（523 ページ）
STOP TRACE（526 ページ）