# 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、AR ルーター（ルーターとしては機能していませんが）から他のコンピューターに Telnet したり、PING コマンド（120 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、eth0 が LAN に接続されていると仮定します。

   ```
   ADD IP INT=eth0 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=eth0
  NEXTHOP=192.168.10.254 ↵
```

あるいは、デフォルトルート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=eth0 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（157 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（181 ページ）で確認します。

■ 経路情報は SHOW IP ROUTE コマンド（191 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（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。

## リモートルーター

同一構内の LAN 同士を接続するローカルルーターに対し、WAN 回線を使用して物理的に離れたネットワーク同士を接続するルーターをリモートルーターと呼びます。
本製品は、ローカル LAN を接続する LAN 側インターフェース（ETH）と、WAN 回線経由でリモート LAN に接続する WAN 側インターフェース（BRI）を 1 つずつ持っており、リモートルーターとして使用できます。
LAN 側インターフェースは Ethernet なので、特別な設定を行うことなくデータリンク層インターフェースとして使用できます。
一方、WAN 側インターフェースに接続する回線には ISDN と専用線の 2 種類があります。
ここでは代表的な例として、以下の構成における IP リモートルーターの基本設定について解説します。なお、ここでは簡単な説明にとどめますので、各回線上での詳細な設定方法については、それぞれ該当する章をご覧ください。また、具体例については「設定例集」もご参照ください。

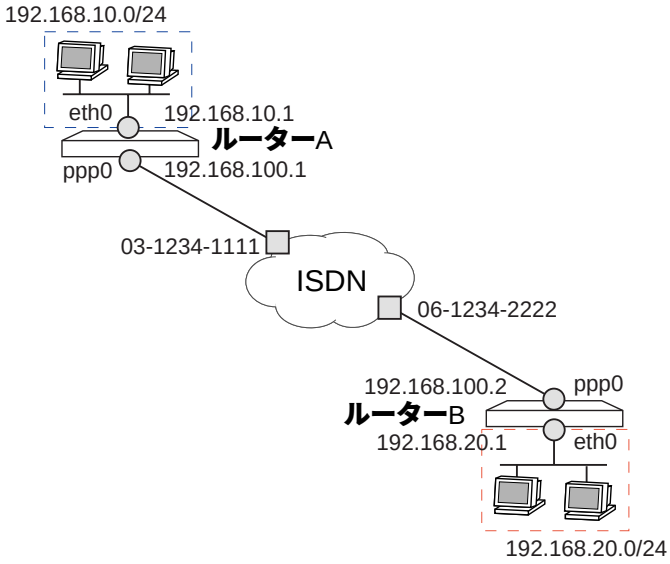
- ISDN 回線上で PPP を使用する場合（BRI → ISDN → PPP）
- 専用線上で PPP を使用する場合（BRI → TDM → PPP）

### 交換回線による PPP ダイヤルオンデマンド接続

ISDN 網のような交換回線を使う場合は、必要なときに発呼して対向拠点と接続し、無通信状態が一定期間続いたら回線を切断するダイヤルオンデマンド接続が適しています。
ダイヤルオンデマンドを使用する場合は、次の設定がポイントになります。

- CREATE PPP コマンド（「PPP」の 26 ページ）で PPP インターフェースを作成するとき、IDLE パラメーターに ON（または自動切断までの秒数）を指定してダイヤルオンデマンドを有効にする
- 経路情報をスタティックに登録する

ここでは、次のような構成のネットワークを例に解説します。




ルーター A の設定

1. ISDN の接続先を設定します。

   ```
   ADD ISDN CALL=remote NUMBER=0612342222 PRECEDENCE=OUT INTREQ=BRI0
     OUTSUB=LOCAL SEARCHSUB=LOCAL ↵
   ```

2. PPP インターフェースを作成します。

   ```
   CREATE PPP=0 OVER=ISDN-remote IDLE=ON USER=RouterA PASSWORD=PasswordA
     AUTHENTICATION=CHAP ↵
   ```

3. ルーター B の PPP ユーザー名を登録します。

   ```
   ADD USER=RouterB PASSWORD=PasswordB LOGIN=NO ↵
   ```

4. IP モジュールを有効にします。

   ```
   ENABLE IP ↵
   ```

5. LAN 側（eth0）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 ↵
   ```

6. WAN 側（ppp0）インターフェースに IP アドレスを割り当てます。

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

7. ルーター B の LAN 側ネットワークへの経路を設定します。

   ```
   ADD IP ROUTE=192.168.20.0 MASK=255.255.255.0 INT=ppp0
     NEXTHOP=192.168.100.2 ↵
   ```

ルーター B の設定

1. ISDN の接続先を登録します。

   ```
   ADD ISDN CALL=remote NUMBER=0312341111 PRECEDENCE=IN INTREQ=BRI0
     OUTSUB=LOCAL SEARCHSUB=LOCAL ↵
   ```

2. PPP インターフェースを作成します。

   ```
   CREATE PPP=0 OVER=ISDN-remote IDLE=ON USER=RouterB PASSWORD=PasswordB
     AUTHENTICATION=CHAP ↵
   ```

3. ルーター A の PPP ユーザー名を登録します。

   ```
   ADD USER=RouterA PASSWORD=PasswordA LOGIN=NO ↵
   ```

4. IP モジュールを有効にします。

   ```
   ENABLE IP ↵
   ```

5. LAN 側（eth0）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=192.168.20.1 MASK=255.255.255.0 ↵
   ```

6. WAN 側（ppp0）インターフェースに IP アドレスを割り当てます。

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

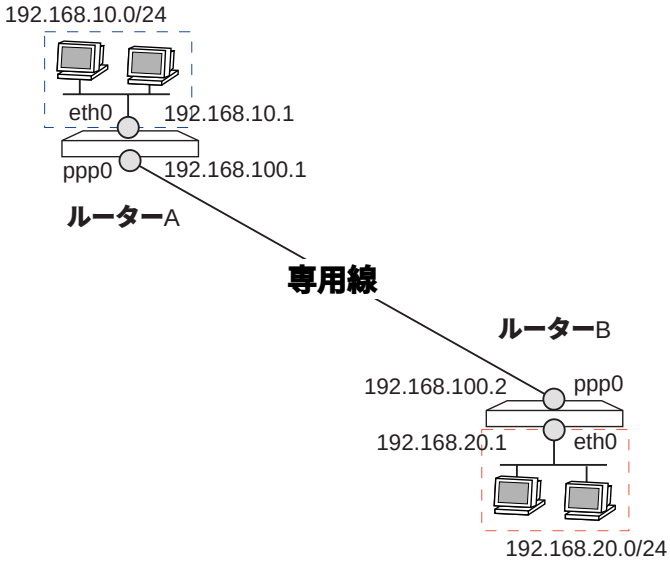
7. ルーター A の LAN 側ネットワークへの経路を設定します。

   ```
   ADD IP ROUTE=192.168.10.0 MASK=255.255.255.0 INT=ppp0
     NEXTHOP=192.168.100.1 ↵
   ```

設定は以上です。

### 専用回線による PPP 常時接続

専用線のような常時接続回線における IP リモートルーターの設定例を示します。ここでは、次のような構成のネットワークを例に解説します。




ルーター A の設定

1. BRI インターフェース「0」の全スロット（1〜2）を常時起動の専用線モードに変更します（デフォルトは ISDN モード）

   ```
   SET BRI=0 MODE=TDM ACTIVATION=ALWAYS TDMSLOTS=1-2 ↵
   ```

2. BRI0 のスロット 1 だけ（64Kbps）を使う TDM グループ「remote」を作成します。

   ```
   CREATE TDM GROUP=remote INT=BRI0 SLOTS=1 ↵
   ```

3. TDM グループ「remote」上に PPP インターフェース「0」を作成します。

   ```
   CREATE PPP=0 OVER=TDM-remote ↵
   ```

4. IP モジュールを有効にします。

   ```
   ENABLE IP ↵
   ```

5. LAN 側（eth0）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 ↵
   ```

6. WAN 側（ppp0）インターフェースに IP アドレスを割り当てます。

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

7. ルーター B の LAN 側ネットワークへの経路を設定します。

   ```
   ADD IP ROUTE=192.168.20.0 MASK=255.255.255.0 INT=ppp0
     NEXTHOP=192.168.100.2 ↵
   ```

ルーター B の設定

1. BRI インターフェース「0」の全スロット（1〜2）を常時起動の専用線モードに変更します（デフォルトは ISDN モード）

   ```
   SET BRI=0 MODE=TDM ACTIVATION=ALWAYS TDMSLOTS=1-2 ↵
   ```

2. BRI0 のスロット 1 だけ（64Kbps）を使う TDM グループ「remote」を作成します。

   ```
   CREATE TDM GROUP=remote INT=BRI0 SLOTS=1 ↵
   ```

3. TDM グループ「remote」上に PPP インターフェース「0」を作成します。

   ```
   CREATE PPP=0 OVER=TDM-remote ↵
   ```

4. IP モジュールを有効にします。

   ```
   ENABLE IP ↵
   ```

5. LAN 側（eth0）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=192.168.20.1 MASK=255.255.255.0 ↵
   ```

6. WAN 側（ppp0）インターフェースに IP アドレスを割り当てます。

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

7. ルーター A の LAN 側ネットワークへの経路を設定します。

   ```
   ADD IP ROUTE=192.168.10.0 MASK=255.255.255.0 INT=ppp0
     NEXTHOP=192.168.100.1 ↵
   ```

設定は以上です。

## IP のデバッグ

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（120 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（208 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（71 ページ）でデータリンク層インターフェース（eth、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 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）
- 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（71 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=eth0 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、eth0 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（140 ページ）を使います。

```
SET IP INT=eth0 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（89 ページ）を使います。

```
DELETE IP INT=eth0 ↵
```

■ 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（181 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になります（eth0、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（71 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=ISDN-isp IDLE=ON LQR=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（117 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（157 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（89 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 26 ページ）、SET PPP コマンド（「PPP」の 48 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（117 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 60 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（181 ページ）で確認します。

■ デフォルトルートは SHOW IP ROUTE コマンド（191 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ルートです。

■ DNS サーバーアドレスの設定状況は、SHOW IP コマンド（157 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 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（117 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 27 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（181 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（157 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（89 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 ↵
   ```

■ 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）、デフォルトルート、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 27 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（181 ページ）で確認します。

■ デフォルトルートは SHOW IP ROUTE コマンド（191 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ルートです。

■ DNS サーバーアドレスの設定状況は、SHOW IP コマンド（157 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「eth0-n」の形式で指定します（eth0 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 eth0-0）。

■ eth0 上に IP インターフェースを 2 つ作成します。「eth0-0」は単に「eth0」と書いてもかまいません。

```
ADD IP INT=eth0-0 IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=eth0-1 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、eth0-0 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 eth0-1）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。

# 経路制御（スタティック）

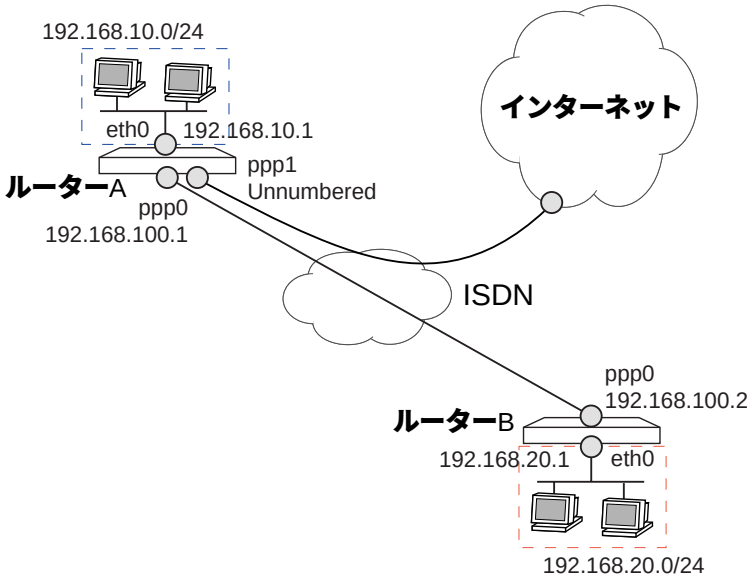
本製品は以下の IP ユニキャスト経路制御方式に対応しています。

- 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

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）」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

以下、次のネットワーク構成を例に各種経路の設定方法を解説します。




## 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（71 ページ）でインターフェース（eth、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
DLCI/Circ.        Type     Policy   Protocol            Metrics      Preference
-------------------------------------------------------------------------------
192.168.10.0      255.255.255.0     0.0.0.0             eth0               7124
-                 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（76 ページ）を使って、離れたネットワーク（ルーターに直接接続されていないネットワーク）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、最低限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。

■ ルーター A に対し、ネットワーク 192.168.20.0 / 24 へのスタティック経路を設定するには次のようにします。自分以外のルーター（ルーター B）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=192.168.20.0 MASK=255.255.255.0 INT=ppp0
  NEXTHOP=192.168.100.2 METRIC=2 ↵
```

これにより、192.168.20.0 / 24 宛てのパケットはルーター B（192.168.100.2）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（191 ページ）を使います。

```
Manager > show ip route

IP Routes
-------------------------------------------------------------------------------
Destination       Mask              NextHop             Interface           Age
DLCI/Circ.        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     192.168.100.2       ppp0                  1
-                 remote   0        static              2                    60
-------------------------------------------------------------------------------
```

■ 経路を削除するには DELETE IP ROUTE コマンド（91 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=192.168.20.0 MASK=255.255.255.0 INT=ppp0
  NEXTHOP=192.168.100.2 ↵
```

## 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ルート（経路）と呼びます。デフォルトルートは、ADD IP ROUTE コマンド（76 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）。

■ ルーター A に対し、デフォルトルートを ppp1 側に向けて設定するには次のようにします。この例では ppp1 が Unnumbered なので NEXTHOP には 0.0.0.0 を指定します。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=ppp1 NEXTHOP=0.0.0.0 ↵
```

これにより、ルーター A 直下の 192.168.10.0 / 24、スタティック登録した 192.168.20.0 / 24 以外宛てのパケットは、すべてデフォルトゲートウェイ（ISP のルーター）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（191 ページ）を使います。

```
Manager > show ip route

IP Routes
-------------------------------------------------------------------------------
Destination       Mask              NextHop             Interface           Age
DLCI/Circ.        Type     Policy   Protocol            Metrics      Preference
-------------------------------------------------------------------------------
0.0.0.0           0.0.0.0           0.0.0.0             ppp1                 6
-                 remote   0        static              1                  360
192.168.10.0      255.255.255.0     0.0.0.0             eth0              9425
-                 direct   0        interface           1                    0
192.168.20.0      255.255.255.0     192.168.100.2       ppp0               343
-                 remote   0        static              2                   60
-------------------------------------------------------------------------------
```

■ 経路を削除するには DELETE IP ROUTE コマンド（91 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=ppp1 NEXTHOP=0.0.0.0 ↵
```

# 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。本製品ではルーティングプロトコルとして RIP（v1、v2）を使用できます。ここでは、RIP の設定手順について解説します。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。
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。

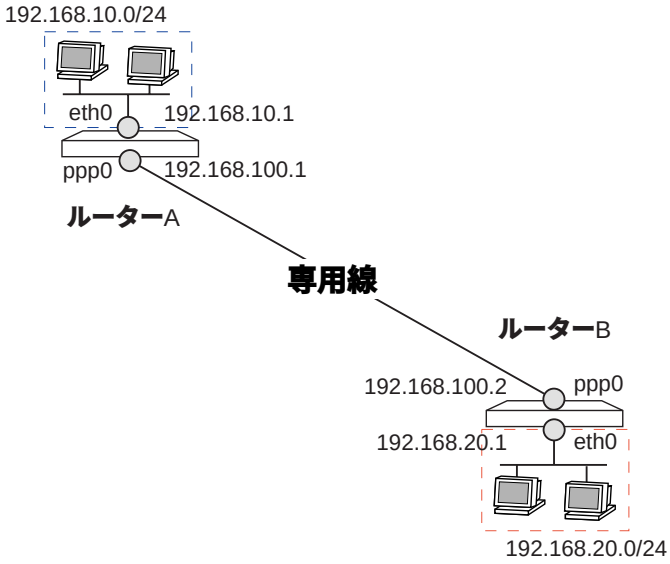
- 宛先ネットワークアドレス
- メトリック（ホップ数）

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

次のような構成のネットワークを例に、ルーター A で RIP を使用するための設定方法を説明します。




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=eth0 IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=ppp0 IP=192.168.100.1 MASK=255.255.255.0 ↵
```

4. 各インターフェース上で RIP パケットの送受信が行われるようにします。

```
ADD IP RIP INT=eth0 ↵
ADD IP RIP INT=ppp0 ↵
```

   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=eth0 SEND=RIP2 RECEIVE=RIP2 ↵
ADD IP RIP INT=ppp0 SEND=RIP2 RECEIVE=RIP2 ↵
```

設定は以上です。また、ルーター B も同様に設定してください。これにより、eth0、ppp0 の両インター

フェースで RIP パケットの送受信が行われ、他のルーターからの情報を元に経路表が動的に構築されていきます。

■ 経路表を確認するには、SHOW IP ROUTE コマンド（191 ページ）を使います。

```
Manager > show ip route

IP Routes
-------------------------------------------------------------------------------
Destination       Mask              NextHop             Interface           Age
DLCI/Circ.        Type     Policy   Protocol            Metrics      Preference
-------------------------------------------------------------------------------
192.168.10.0      255.255.255.0     0.0.0.0             eth0                155
-                 direct   0        interface           1                     0
192.168.20.0      255.255.255.0     192.168.100.2       ppp0                143
-                 remote   0        rip                 2                   100
192.168.100.0     255.255.255.0     0.0.0.0             ppp0                155
-                 direct   0        interface           1                     0
-------------------------------------------------------------------------------
```

■ 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（186 ページ）を使います。

■ RIP パケットの送受信をオフにするには、DELETE IP RIP コマンド（90 ページ）で IP インターフェースを指定します。

```
DELETE IP RIP INT=eth0 ↵
```

■ 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=eth0 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=eth0 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（146 ページ）を使います。

```
SET IP RIP INT=eth0 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=eth0 SEND=RIP2 RECEIVE=RIP2 AUTHENTICATION=PASSWORD
  PASSWORD=himitsu ↵
```

■ スタティック経路を通知したくない場合は次のようにします。デフォルトではスタティック経路を通知します。

```
SET IP RIP INT=eth0 STATICEXPORT=NO ↵
```

■ RIP パケットの送受信統計は SHOW IP RIP COUNTER コマンド（188 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（148 ページ）で行います。

# 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 1:

## 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。

■ IP ルートフィルターは、ADD IP ROUTE FILTER コマンド（78 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（78 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（194 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 ↵
```

■ 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 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（150 ページ）を使います。

```
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（92 ページ）を使います。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（194 ページ）を使います。

## 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（80 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（196 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（93 ページ）を使います。

# 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 264 ページ）、TRACE コマンド（208 ページ）、PING コマンド（120 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（69 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（88 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（138 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（179 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 264 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。

✎ PING コマンド（120 ページ）や TRACE コマンド（208 ページ）は DNS を使用しません。

■ 本製品が使用する DNS サーバーは、ADD IP DNS コマンド（59 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 ↵
```

✎ ファームウェアバージョン 2.1 までは、DNS サーバーの指定に SET IP NAMESERVER コマンド（144 ページ）、SET IP SECONDARYNAMESERVER コマンド（152 ページ）を使用していました。これらのコマンドは後方互換性のために残されていますが、設定保存時には ADD IP DNS コマンド（59 ページ）に変換されて保存されます。

■ 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（59 ページ）の DOMAIN パラメーターを指定します。
次の例では、mikan.fruit.com ドメインの問い合わせは 172.20.10.1、172.20.10.2 に、ringo.fruit.com 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.com PRIMARY=172.20.10.1
  SECONDARY=172.16.10.2 ↵
ADD IP DNS DOMAIN=ringo.fruit.com 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 サーバーの設定は SHOW IP DNS コマンド（169 ページ）、SHOW IP コマンド（157 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「ar1.mydomain.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 181 ページ）で設定します）、次のように TELNET コマンド（「運用・管理」の 264 ページ）を実行すると、bulbul のあとにドメイン名「mydomain.com」が補われ、「bulbul.mydomain.com」に対して DNS の検索が行われます。

```
SET SYSTEM NAME=ar1.mydomain.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（132 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（132 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（169 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（171 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（58 ページ）を使います。

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

■ ARP エントリーを削除するには、DELETE IP ARP コマンド（83 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（160 ページ）を実行します。

```
SHOW IP ARP ↵
```

## 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（71 ページ）、SET IP INTERFACE コマンド（140 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 ↵
```

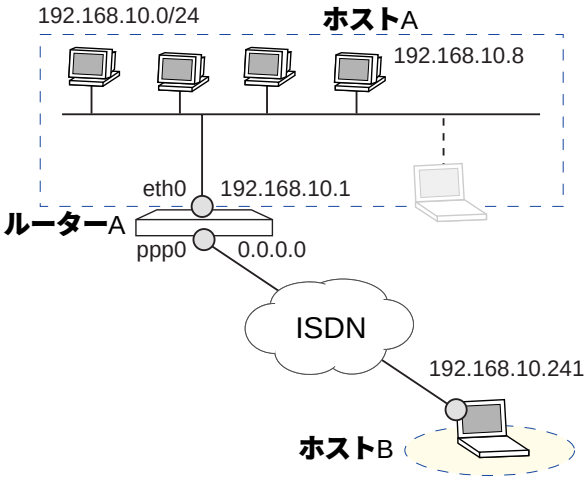
```
SET IP INT=eth0 PROXYARP=OFF ↵
```

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（181 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。

### 自動的に設定される例

プロキシー ARP の使用例として、ダイヤルアップ PPP 接続のケースを考えます。




この例では、ホスト B が ISDN などの交換回線網経由でルーター A に接続します。ルーター A では、着信時に PPP インターフェースを動的作成し、LAN 側アドレスの 1 つをホスト B に割り当てます（ここでは 192.168.10.241）。これにより、ホスト B は遠隔地にありながらも、LAN（192.168.10.0/24）に直接接続されているかのように他のホストと通信できるようになります。

ホスト B から見た場合、送信するすべてのパケットがルーター A を経由しなくてはならないことは明らかです。ホスト B では、ネットワークとの唯一の接点であるダイヤルアップ PPP インターフェースの方向をデフォルトルートに設定します。

一方、LAN 上のホストにとっては状況が異なります。ここでは、ホスト A（192.168.10.8）を LAN 上ホストの代表として取り上げます。

ホスト A がホスト B との IP 通信を開始するとします。ホスト A は、管理者が設定した IP アドレスとサブネットマスクの情報から、自分の所属する IP ネットワークが 192.168.10.0/24（アドレス範囲は 192.168.10.0 ～192.168.10.255）であることを認識しています。通信相手であるホスト B の IP アドレス 192.168.10.241 もこの範囲に収まるため、ホスト A はホスト B が同一ネットワーク上にあると見なして、192.168.10.241 に対する ARP Request をブロードキャストします。

しかし、実際にはホスト B はルーター A と ISDN 網経由で接続されているため、LAN 上にブロードキャストされた ARP Request を受け取ることができません。そのため、このままではホスト A とホスト B 間の IP 通信が成立しません。

しかし、本製品はデフォルトでプロキシー ARP が有効であるため、ホスト A が送信した ARP Request を受け取ると、ホスト B が別インターフェース（ppp0）上にあることを認識して、代理の ARP Reply をホスト A に返します。ホスト A は本製品をホスト B だと思ってパケットを送信してきますが、本製品はこれを ppp0 側のホスト B に転送します。これでホスト A からホスト B にパケットが届きました。

今度は戻りです。ホスト B は自分宛てでないパケットをすべてルーター A に転送します。ルーター A はホスト B から受け取ったパケットの宛先が自分でない場合、経路表を参照して適切に配送します。このように、プロキシー ARP の働きによって、LAN 上のホスト A と WAN 経由で LAN に接続しているホスト B が、個々のホストで特別な設定を行うことなく透過的に通信できるようになります。

# IP フィルター

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） |

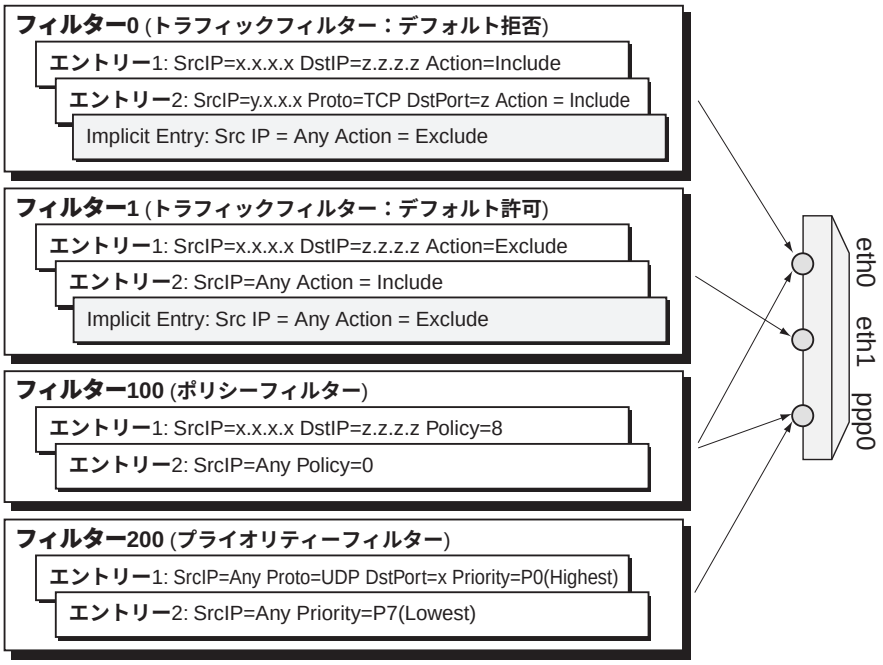
表 2:

## 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）

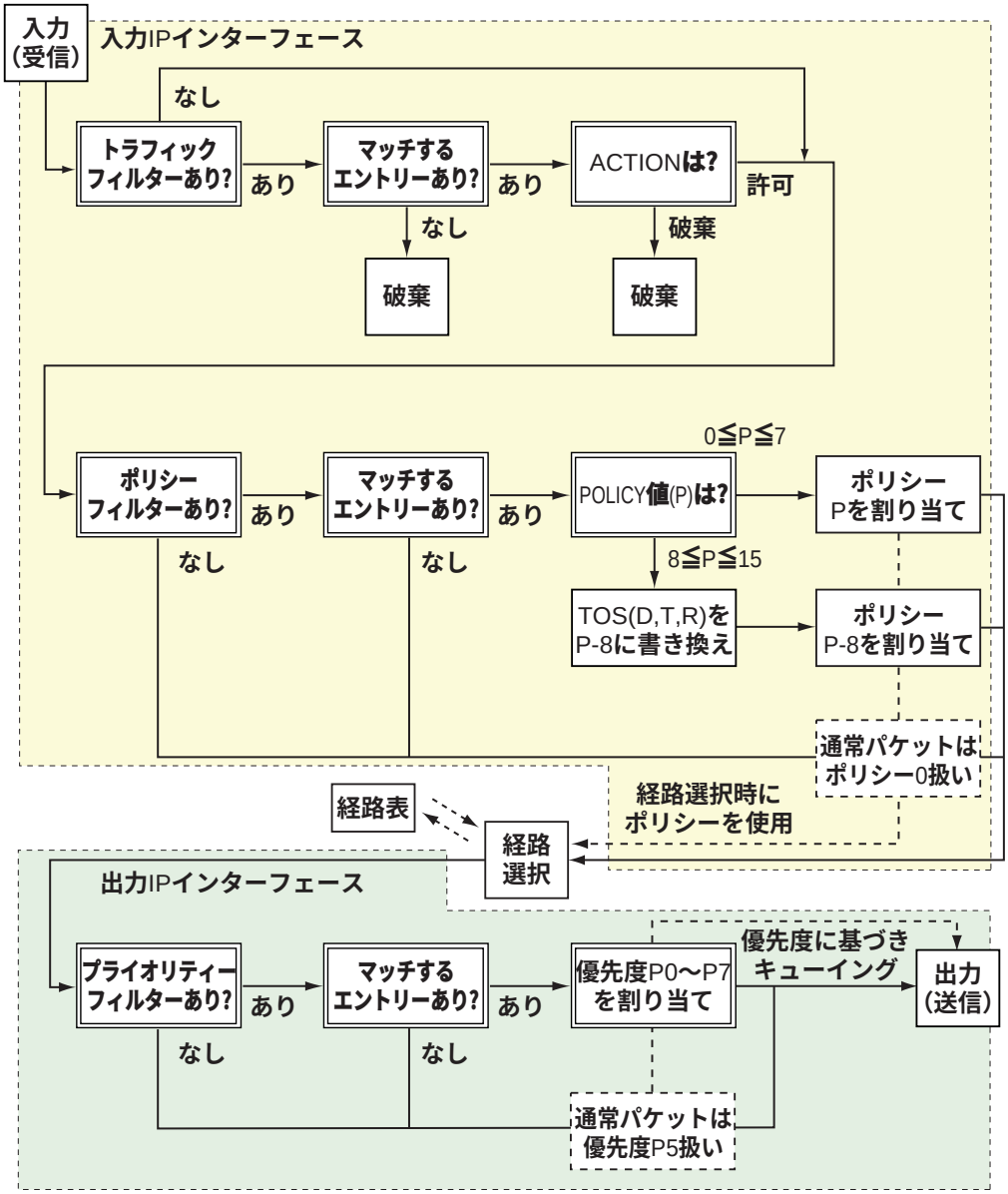
2. 選別されたパケットに対してなんらかの処理（破棄、経路選択ポリシー設定、優先度設定など）を実行する

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（76 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（61 ページ）/ SET IP FILTER コマンド（135 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（71 ページ）/ SET IP INTERFACE コマンド（140 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 3: 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 4: 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、デフォルトルートの選択では 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、デフォルトルートの選択では 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（76 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（61 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 5: 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（61 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（76 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（61 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 6: 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（140 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 eth0 に割り当て。

```
SET IP INT=eth0 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=ppp0 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（86 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（173 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 ↵
```

✎ エントリーを削除すると、後続のエントリー番号が 1 つずつ前にずれます。

■ 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（140 ページ）の FILTER、POLICYFILTER、PRIORITYFILTER パラメーターに NONE を指定します。

```
SET IP INT=eth0 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 eth0 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=eth0 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、eth0 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 eth0 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。

```
SET IP FILTER=0 ENTRY=1 LOG=HEADER ↵
```

■ eth0 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=eth0 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各必要はありません。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、eth0 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。ppp0 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=ppp0 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=eth0 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、ppp1 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 ppp0 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=eth0 POLICYFILTER=100 ↵
ADD IP ROUTE=192.168.20.0 MASK=255.255.255.0 INTERFACE=ppp1 NEXT=0.0.0.0
  POLICY=1 ↵
ADD IP ROUTE=192.168.20.0 MASK=255.255.255.0 INTERFACE=ppp0 NEXT=0.0.0.0
  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 eth0 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、それぞれ経由する PPP インターフェースを異ならせています（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=eth0 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（173 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（181 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（132 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（132 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（169 ページ）で確認できます。

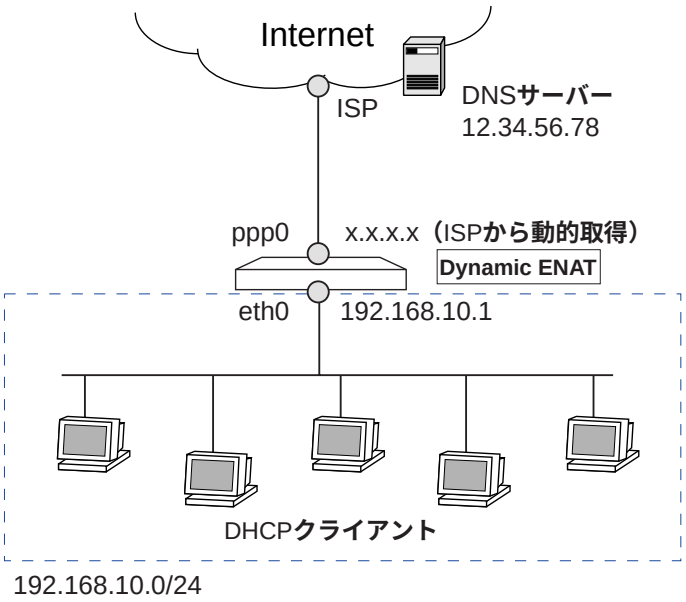
```
SHOW IP DNS ↵
```

■ キャッシュテーブルの内容は、SHOW IP DNS CACHE コマンド（171 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 ↵
```

# 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（119 ページ）、DISABLE IP SRCROUTE コマンド（107 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（157 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（113 ページ）と DISABLE IP FOFILTER コマンド（101 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（157 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（71 ページ）、SET IP INTERFACE コマンド（140 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=eth0 DIRECTEDBROADCAST=ON ↵
SET IP INTERFACE=eth0 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（181 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（81 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「dialin」とします。

```
CREATE IP POOL=dialin IP=192.168.10.240-192.168.10.250 ↵
```

■ ISDN 網経由で 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 31 ページ）、SET PPP TEMPLATE コマンド（「PPP」の 54 ページ））で指定します。

```
CREATE PPP TEMPLATE=0 IDLE=ON BAP=OFF IPPOOL=dialin AUTHENTICATION=CHAP ↵
```

■ IP アドレスプールの設定内容は SHOW IP POOL コマンド（184 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（95 ページ）を使います。

```
DESTROY IP POOL=dialin ↵
```

## 設定例

IP アドレスプールを使用した設定例を示します。

### PPP ダイヤルアップサーバー（ISDN）

ここでは、ISDN 網経由での PPP 接続を受け入れるダイヤルアップサーバー的な設定例を示します。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。

1. IP モジュールを有効にします。

   ```
   ENABLE IP ↵
   ```

2. LAN 側（eth0）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 ↵
   ```

3. IP アドレスプール「dialin」を作成して、ダイヤルアップ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=dialin IP=192.168.10.240-192.168.10.250 ↵
   ```

4. PPP テンプレート「0」を作成します。これは、外部からの着呼時に動的作成される PPP インターフェースの仕様を定めるものです。IP アドレスプール「dialin」を使用するよう指定します。

```
CREATE PPP TEMPLATE=0 IDLE=ON BAP=OFF IPPOOL=dialin
  AUTHENTICATION=CHAP ↵
```

5. 外部からの着呼を受け入れる ISDN コール「pppserv」を作成します。着呼のみで発呼は行わないため、接続先番号として「0」を指定しています。また「INANY=ON」を指定して、ISDN レベルでの認証・識別は行わずにすべての着信呼を受け入れるよう設定します。また、「USER=PPP」を指定して着呼時に PPP インターフェースを動的作成するよう指定します。そのときに使うテンプレートは「PPPTEMPLATE=0」で指定しています。

```
ADD ISDN CALL=pppserv NUMBER=0 PRECEDENCE=IN INTREQ=pri0 INANY=ON
  USER=PPP PPPTEMPLATE=0 ↵
```

6. ダイヤルアップユーザーの PPP ユーザー名とパスワードを登録します。これらは PPP 接続のためだけのアカウントなので、LOGIN=NO を指定してルーターにはログインできないようにします。

```
ADD USER=UserA PASSWORD=PasswordA ↵
ADD USER=UserB PASSWORD=PasswordB ↵
ADD USER=UserC PASSWORD=PasswordC ↵
```

設定は以上です。

# 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**

**IP フィルター**



**DNS リレー**



**DHCP/BOOTP リレー**



**UDP ブロードキャストヘルパー**



**セキュリティー**



**IP アドレスプール**

# ADD BOOTP RELAY

**カテゴリー：**IP / DHCP/BOOTP リレー
**対象機種：**AR130、AR160

**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（82 ページ）
DISABLE BOOTP RELAY（96 ページ）
ENABLE BOOTP RELAY（108 ページ）
PURGE BOOTP RELAY（122 ページ）
SET BOOTP MAXHOPS（127 ページ）
SHOW BOOTP RELAY（155 ページ）

# ADD IP ARP

**カテゴリー：**IP / ARP
**対象機種：**AR130、AR160

**ADD IP ARP=*ipadd* INTERFACE=*interface* ETHERNET=*macadd***

***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（例：00-00-f4-12-34-56）

## 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

## 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
```

## 関連コマンド

DELETE IP ARP（83 ページ）
SET IP ARP（128 ページ）
SHOW IP ARP（160 ページ）

# ADD IP DNS

**カテゴリー：**IP / 名前解決
**対象機種：**AR130、AR160

**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 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.com 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.com 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.com PRIMARY=172.20.20.1
  SECONDARY=172.20.20.2
```

## 備考・注意事項

ファームウェアバージョン 2.1.x までは、DNS サーバーの指定を SET IP NAMESERVER コマンド、SET IP SECONDARYNAMESERVER コマンドで行っていたが、バージョン 2.3.x からは ADD IP DNS コマンド、SET IP DNS コマンドで設定するように変更された。なお、従来のコマンドも後方互換性のために残されているが、設定保存時には ADD IP DNS / SET IP DNS に自動変換される。
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.com」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.com」に対する検索が実施される。

## 関連コマンド

DELETE IP DNS（84 ページ）
DISABLE IP DNSRELAY（99 ページ）
ENABLE IP DNSRELAY（111 ページ）
SET IP DNS（130 ページ）
SET IP DNS CACHE（132 ページ）
SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP DNS（169 ページ）
SHOW IP DNS CACHE（171 ページ）
TELNET（「運用・管理」の 264 ページ）

# ADD IP FILTER

**カテゴリー：**IP / IP フィルター
**対象機種：**AR130、AR160

```
ADD IP FILTER=filter-number SOURCE=ipadd {ACTION={INCLUDE|EXCLUDE}|
   POLICY=0..15|PRIORITY=P0..P7} [SMASK=ipadd] [SPORT={port-name|port-id}]
   [DESTINATION=ipadd [DMASK=ipadd]] [DPORT={port-name|port-id}]
   [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-number]
```

***filter-number***: フィルター番号（0〜299）
***ipadd***: IP アドレス
***port-name***: TCP / UDP ポート名（サービス名）
***port-id***: TCP / UDP ポート番号（0〜65535。low:high の形式で範囲指定も可）
***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-number***: フィルタールール番号

## 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）の 3 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。
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。

## パラメーター

**FILTER**　フィルター番号。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用。

**SOURCE** 始点 IP アドレス。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（フィルター番号 0〜99）の動作を指定する。INCLUDE はマッチしたパケットを通過させる。EXCLUDE はマッチしたパケットを破棄する。ACTION、POLICY、PRIORITY はどれかひとつしか指定できない。

**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（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

**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（トラフィックフィルター）を指定する。トラフィックフィルターの場合、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。PROCOTOL=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。PROCOTOL=ICMP の場合のみ有効

**LOG** フィルタールール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、ルール番号、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、ルール番号、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** フィルター内におけるルールの位置。省略時はフィルターの末尾に追加される。既存ルールと同じ番号を指定した場合は、既存ルールの前に新規ルールが追加され、既存ルール以降はひとつずつ後ろに下がる。

| 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 7: 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 8: 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 | ルーター広告（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 9: 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 10: 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 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 eth0 に適用。

```
ADD IP FILTER=100 SOURCE=10.1.1.10 SMASK=255.255.255.255 DEST=10.2.2.12
  POLICY=4
SET IP INT=eth0 POLICYFILTER=100
```

■TCP を最優先で転送するプライオリティーフィルター「200」を eth0 に適用

```
ADD IP FILTER=200 SOURCE=0.0.0.0 PROTOCOL=TCP PRIORITY=P0
SET IP INT=eth0 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ルールが存在する。そのため、特定のパケットだけを破棄したい場合は、フィルターリストの最後に「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 IP INTERFACE（71 ページ）
DELETE IP FILTER（86 ページ）
SET IP FILTER（135 ページ）
SET IP INTERFACE（140 ページ）
SHOW IP FILTER（173 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
**対象機種：**AR130、AR160

**ADD IP HELPER DESTINATION=*ipadd* INTERFACE=*interface* PORT=*port-number***

***ipadd***: IP アドレス
***interface***: IP インターフェース名（eth0、ppp0 など）
***port-number***: UDP ポート番号（1〜65535）または定義済みの UDP 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 11: 定義済みの UDP サービス名

## 例

■eth0 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=eth0 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（87 ページ）
DISABLE IP HELPER（103 ページ）
ENABLE IP HELPER（115 ページ）
SHOW IP HELPER（177 ページ）

# ADD IP HOST

**カテゴリー：**IP / 名前解決
**対象機種：**AR130、AR160

**ADD IP HOST=*name* IPADDRESS=*ipadd***

***name***: ホスト名
***ipadd***: IP アドレス

## 解説

IP ホストテーブルにエントリーを追加する。
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（59 ページ）
DELETE IP DNS（84 ページ）
DELETE IP HOST（88 ページ）
DISABLE IP DNSRELAY（99 ページ）
ENABLE IP DNSRELAY（111 ページ）
PING（120 ページ）
SET IP DNS（130 ページ）
SET IP DNS CACHE（132 ページ）
SET IP HOST（138 ページ）
SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP DNS（169 ページ）
SHOW IP DNS CACHE（171 ページ）

SHOW IP HOST（179 ページ）
TELNET（「運用・管理」の 264 ページ）

# ADD IP INTERFACE

**カテゴリー：**IP / IP インターフェース
**対象機種：**AR130、AR160

**ADD IP INTERFACE=*interface* IPADDRESS=**{***ipadd*|**DHCP**} [MASK=*ipadd*]
[BROADCAST={*0*|*1*}] [DIRECTEDBROADCAST={YES|NO|ON|OFF}] [FILTER={*0..99*|
NONE}] [FRAGMENT={YES|NO}] [METRIC=*1..16*] [MULTICAST={OFF|SEND|RECEIVE|
BOTH|ON}] [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

## 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、eth0-0、eth0-1、eth0-2 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：eth0）は「0」を指定したものと見なされる（例：eth0-0 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）、デフォルトルート、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を指定する。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。

**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。

**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を指定する。ポリシーフィルターによって設定されたルーティングポリシー（サービスタイプ）は経路選択時に使用される。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。

**PRIORITYFILTER** 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プライオリティーフィルターの番号を指定する。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は、パケット送出時のキューイングに使用される。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。

**PROXYARP** ProxyARP（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

■eth0 に IP アドレス 192.168.100.1 を設定する。

```
ADD IP INT=eth0 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
```

■eth0 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=eth0-0 IP=172.16.10.1 MASK=255.255.255.0
ADD IP INT=eth0-1 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、eth0 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 eth0-1 や eth1）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（89 ページ）
DISABLE IP INTERFACE（104 ページ）
ENABLE IP INTERFACE（116 ページ）
RESET IP INTERFACE（126 ページ）
SET IP INTERFACE（140 ページ）
SHOW IP INTERFACE（181 ページ）

# ADD IP RIP

**カテゴリー：**IP / 経路制御（RIP）
**対象機種：**AR130、AR160

```
ADD IP RIP INTERFACE=interface [IP=ipadd] [SEND={NONE|RIP1|RIP2|
   COMPATIBLE}] [RECEIVE={NONE|RIP1|RIP2|BOTH}] [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**　同一サブネット上にある 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 RIP ルーターとのユニキャスト通信に関する設定となる。本パラメーターを省略した場合は、該当インターフェースで受信したすべての RIP パケットを受け入れ、送信時はブロードキャストアドレスか RIP2 ルーターマルチキャストグループアドレスに送信する。

**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（クラスフルな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。

**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 PASSWORD 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
```

■eth1 で RIP2 の受信だけを有効にする。

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

■eth0 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=eth0 IP=192.168.10.5 SEND=NONE RECEIVE=RIP2 AUTH=PASSWORD
  PASSWORD=secrets
ADD IP RIP INT=eth0 SEND=RIP1 RECEIVE=NONE
```

## 関連コマンド

DELETE IP RIP（90 ページ）
SET IP RIP（146 ページ）
SHOW IP（157 ページ）
SHOW IP RIP（186 ページ）

# ADD IP ROUTE

**カテゴリー：**IP / 経路制御（スタティック）
**対象機種：**AR130、AR160

**ADD IP ROUTE=*ipadd* INTERFACE=*interface* NEXTHOP=*ipadd*** [MASK=*ipadd*]
[METRIC=*1..16*] [POLICY=*0..7*] [PREFERENCE=*0..65535*]

***ipadd***: IP アドレス
***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ルートを追加する。

## 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。デフォルトルートの場合は 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。デフォルトルートのマスクは 0.0.0.0 とする（省略可能）

**METRIC** RIP が使用するメトリック。通常は「経由するルーターの数+1」を指定する。有効範囲は 1〜16。デフォルトは 1

**POLICY** 本経路のサービスタイプ（TOS）

**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。デフォルト値は次のとおり。インターフェース 0、RIP 100、デフォルト経路 360、デフォルト以外のスタティック経路 60。

## 例

■ppp0 上にデフォルトルートを設定する。

```
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=eth0 NEXTHOP=172.16.1.1
```

## 関連コマンド

DELETE IP ROUTE（91 ページ）
SET IP ROUTE（149 ページ）
SHOW IP ROUTE（191 ページ）

# ADD IP ROUTE FILTER

**カテゴリー：**IP / 経路制御フィルター
**対象機種：**AR130、AR160

```
ADD IP ROUTE FILTER[=filter-id] IP=ipadd MASK=ipadd ACTION={INCLUDE|
   EXCLUDE} [DIRECTION={RECEIVE|SEND|BOTH}] [INTERFACE=interface]
   [NEXTHOP=ipadd] [POLICY=0..7] [PROTOCOL={ANY|RIP|STATIC|INTERFACE}]
```

***filter-id***: フィルター番号（1〜100）
***ipadd***: IP アドレス
***interface***: IP インターフェース名（eth0、ppp0 など）

## 解説

IP ルートフィルターのリストにフィルターを追加する。100 件まで登録可能。
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**　フィルター番号を指定する。省略時はリストの末尾に追加される。

**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。

**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。STATIC は ADD IP ROUTE コマンドによるスタティック経路の登録を抑止・許可するためのもの。また、INTERFACE

は、ADD IP INTERFACE コマンドによる IP インターフェース作成時のインターフェース経路登録を抑止・許可するためのオプション。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
```

## 関連コマンド

DELETE IP ROUTE FILTER（92 ページ）
SET IP ROUTE FILTER（150 ページ）
SHOW IP ROUTE FILTER（194 ページ）

# ADD IP TRUSTED

**カテゴリー：**IP / 経路制御フィルター
**対象機種：**AR130、AR160

**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（61 ページ）
DELETE IP FILTER（86 ページ）
DELETE IP TRUSTED（93 ページ）
SET IP FILTER（135 ページ）
SHOW IP FILTER（173 ページ）
SHOW IP TRUSTED（196 ページ）

# CREATE IP POOL

**カテゴリー：**IP / IP アドレスプール
**対象機種：**AR130、AR160

**CREATE IP POOL=*pool-name* IP=*ipadd*[-*ipadd*]**

***pool-name***: IP プール名（1〜15 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）
***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 31 ページ）
DESTROY IP POOL（95 ページ）
SHOW IP POOL（184 ページ）

# DELETE BOOTP RELAY

**カテゴリー：**IP / DHCP/BOOTP リレー
**対象機種：**AR130、AR160

**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（57 ページ）
DISABLE BOOTP RELAY（96 ページ）
ENABLE BOOTP RELAY（108 ページ）
PURGE BOOTP RELAY（122 ページ）
SET BOOTP MAXHOPS（127 ページ）
SHOW BOOTP RELAY（155 ページ）

# DELETE IP ARP

**カテゴリー：**IP / ARP
**対象機種：**AR130、AR160

**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（58 ページ）
SHOW IP ARP（160 ページ）

# DELETE IP DNS

**カテゴリー：**IP / 名前解決
**対象機種：**AR130、AR160

**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.com ドメイン用の DNS サーバー情報を削除する。

```
DELETE IP DNS DOMAIN=ringo.fruit.com
```

■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

ファームウェアバージョン 2.1.x までは、DNS サーバーの指定を SET IP NAMESERVER コマンド、SET IP SECONDARYNAMESERVER コマンドで行っていたが、バージョン 2.3.x からは ADD IP DNS コマンド、SET IP DNS コマンドで設定するように変更された。なお、従来のコマンドも後方互換性のために残されているが、設定保存時には ADD IP DNS / SET IP DNS に自動変換される。
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（59 ページ）
DELETE IP DNS（84 ページ）

DISABLE IP DNSRELAY（99 ページ）
ENABLE IP DNSRELAY（111 ページ）
SET IP DNS（130 ページ）
SET IP DNS CACHE（132 ページ）
SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP DNS（169 ページ）
SHOW IP DNS CACHE（171 ページ）
TELNET（「運用・管理」の 264 ページ）

# DELETE IP FILTER

**カテゴリー：**IP / IP フィルター
**対象機種：**AR130、AR160

**DELETE IP FILTER=*filter-number* ENTRY=**{***entry-number***|ALL}

***filter-number***: フィルター番号（0〜299）
***entry-number***: フィルタールール番号

## 解説

IP フィルターからフィルタールールを削除する。

## パラメーター

**FILTER**　フィルター番号

**ENTRY**　フィルタールール番号。ルール番号は SHOW IP FILTER コマンドで確認できる（Ent.フィールド）。ルール番号は固定でなく、あるルールを削除すると以降のルールは番号が 1 つずつ前にずれる。ALL を指定した場合は、該当するフィルターの全ルールが削除される。

## 例

■トラフィックフィルター「0」から 2 番のルールを削除する。

```
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
```

## 関連コマンド

ADD IP FILTER（61 ページ）
SET IP FILTER（135 ページ）
SHOW IP FILTER（173 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
**対象機種：**AR130、AR160

**DELETE IP HELPER DESTINATION=*ipadd* INTERFACE=*interface* PORT=*port-number***

***ipadd***: IP アドレス
***interface***: IP インターフェース名（eth0、ppp0 など）
***port-number***: UDP ポート番号

## 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（67 ページ）
DISABLE IP HELPER（103 ページ）
ENABLE IP HELPER（115 ページ）
SHOW IP HELPER（177 ページ）

# DELETE IP HOST

**カテゴリー：**IP / 名前解決
**対象機種：**AR130、AR160

**DELETE IP HOST=*name***

***name***: ホスト名

## 解説

IP ホストテーブルからエントリーを削除する。

## 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（59 ページ）
ADD IP HOST（69 ページ）
DELETE IP DNS（84 ページ）
DISABLE IP DNSRELAY（99 ページ）
ENABLE IP DNSRELAY（111 ページ）
PING（120 ページ）
SET IP DNS（130 ページ）
SET IP DNS CACHE（132 ページ）
SET IP HOST（138 ページ）
SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP DNS（169 ページ）
SHOW IP DNS CACHE（171 ページ）
SHOW IP HOST（179 ページ）
TELNET（「運用・管理」の 264 ページ）

# DELETE IP INTERFACE

**カテゴリー：**IP / IP インターフェース
**対象機種：**AR130、AR160

**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（71 ページ）
DISABLE IP INTERFACE（104 ページ）
ENABLE IP INTERFACE（116 ページ）
RESET IP INTERFACE（126 ページ）
SET IP INTERFACE（140 ページ）
SHOW IP INTERFACE（181 ページ）

# DELETE IP RIP

**カテゴリー：**IP / 経路制御（RIP）
**対象機種：**AR130、AR160

**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
```

■eth0 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=eth0 IP=192.168.20.254
```

## 関連コマンド

ADD IP RIP（74 ページ）
SET IP RIP（146 ページ）
SHOW IP（157 ページ）
SHOW IP RIP（186 ページ）

# DELETE IP ROUTE

**カテゴリー：**IP / 経路制御（スタティック）
**対象機種：**AR130、AR160

**DELETE IP ROUTE=*ipadd* MASK=*ipadd* INTERFACE=*interface* NEXTHOP=*ipadd***

***ipadd***: IP アドレス
***interface***: IP インターフェース名（eth0、ppp0 など）

## 解説

スタティックルートを削除する。ダイナミックルートは削除できない。

## 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

■デフォルトルートを削除する。

```
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（76 ページ）
SET IP ROUTE（149 ページ）
SHOW IP ROUTE（191 ページ）

# DELETE IP ROUTE FILTER

**カテゴリー：**IP / 経路制御フィルター
**対象機種：**AR130、AR160

**DELETE IP ROUTE FILTER=*filter-id***

***filter-id***: フィルター番号（1〜100）

## 解説

IP ルートフィルターのリストから指定したフィルターを削除する。

## パラメーター

**FILTER**　IP ルートフィルターの番号を指定する。フィルター番号は SHOW IP ROUTE FILTER コマンドで確認できる。フィルターを削除すると、それより番号の大きなものが 1 つずつ前にずれる。

## 関連コマンド

ADD IP ROUTE FILTER（78 ページ）
SET IP ROUTE FILTER（150 ページ）
SHOW IP ROUTE FILTER（194 ページ）

# DELETE IP TRUSTED

**カテゴリー：**IP / 経路制御フィルター
**対象機種：**AR130、AR160

**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（61 ページ）
ADD IP TRUSTED（80 ページ）
DELETE IP FILTER（86 ページ）
SET IP FILTER（135 ページ）
SHOW IP FILTER（173 ページ）
SHOW IP TRUSTED（196 ページ）

# DELETE TCP

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（200 ページ）

# DESTROY IP POOL

**カテゴリー：**IP / IP アドレスプール
**対象機種：**AR130、AR160

**DESTROY IP POOL=*pool-name***

***pool-name***: IP プール名（1〜15 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

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（81 ページ）
SHOW IP POOL（184 ページ）

# DISABLE BOOTP RELAY

**カテゴリー：**IP / DHCP/BOOTP リレー
**対象機種：**AR130、AR160

**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（57 ページ）
DELETE BOOTP RELAY（82 ページ）
ENABLE BOOTP RELAY（108 ページ）
PURGE BOOTP RELAY（122 ページ）
SET BOOTP MAXHOPS（127 ページ）
SHOW BOOTP RELAY（155 ページ）

# DISABLE IP

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（102 ページ）
DISABLE IP SRCROUTE（107 ページ）
ENABLE IP（109 ページ）
ENABLE IP FORWARDING（114 ページ）
ENABLE IP SRCROUTE（119 ページ）
SHOW IP（157 ページ）

# DISABLE IP DEBUG

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（110 ページ）
SHOW IP（157 ページ）
SHOW IP DEBUG（168 ページ）

# DISABLE IP DNSRELAY

**カテゴリー：**IP / DNS リレー
**対象機種：**AR130、AR160

**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。

## 備考・注意事項

ファームウェアバージョン 2.1.x までは、DNS サーバーの指定を SET IP NAMESERVER コマンド、SET IP SECONDARYNAMESERVER コマンドで行っていたが、バージョン 2.3.x からは ADD IP DNS コマンドで設定するように変更された。なお、従来のコマンドも後方互換性のために残されているが、設定保存時には ADD IP DNS / SET IP DNS に自動変換される。

## 関連コマンド

ADD IP DNS（59 ページ）
DELETE IP DNS（84 ページ）
ENABLE IP DNSRELAY（111 ページ）
SET IP DNS（130 ページ）
SET IP DNS CACHE（132 ページ）
SET IP DNSRELAY（134 ページ）
SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP（157 ページ）
SHOW IP DNS（169 ページ）
SHOW IP DNS CACHE（171 ページ）

# DISABLE IP ECHOREPLY

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（112 ページ）

# DISABLE IP FOFILTER

**カテゴリー：**IP / セキュリティー
**対象機種：**AR130、AR160

**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（61 ページ）
DELETE IP FILTER（86 ページ）
ENABLE IP FOFILTER（113 ページ）
SET IP FILTER（135 ページ）
SHOW IP FILTER（173 ページ）

# DISABLE IP FORWARDING

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（97 ページ）
DISABLE IP SRCROUTE（107 ページ）
ENABLE IP（109 ページ）
ENABLE IP FORWARDING（114 ページ）
ENABLE IP SRCROUTE（119 ページ）
SHOW IP（157 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
**対象機種：**AR130、AR160

**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（67 ページ）
DELETE IP HELPER（87 ページ）
ENABLE IP HELPER（115 ページ）
SHOW IP HELPER（177 ページ）

# DISABLE IP INTERFACE

**カテゴリー：**IP / IP インターフェース
**対象機種：**AR130、AR160

**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（71 ページ）
DELETE IP INTERFACE（89 ページ）
ENABLE IP INTERFACE（116 ページ）
RESET IP INTERFACE（126 ページ）
SET IP INTERFACE（140 ページ）
SHOW IP INTERFACE（181 ページ）

# DISABLE IP REMOTEASSIGN

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（117 ページ）
SHOW IP（157 ページ）

# DISABLE IP ROUTE

**カテゴリー：**IP / 経路制御（スタティック）
**対象機種：**AR130、AR160

**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（118 ページ）
SHOW IP ROUTE（191 ページ）

# DISABLE IP SRCROUTE

**カテゴリー：**IP / セキュリティー
**対象機種：**AR130、AR160

**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（97 ページ）
ENABLE IP（109 ページ）
ENABLE IP FORWARDING（114 ページ）
ENABLE IP SRCROUTE（119 ページ）
SHOW IP（157 ページ）

# ENABLE BOOTP RELAY

**カテゴリー：**IP / DHCP/BOOTP リレー
**対象機種：**AR130、AR160

**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。

## 関連コマンド

ADD BOOTP RELAY（57 ページ）
DELETE BOOTP RELAY（82 ページ）
DISABLE BOOTP RELAY（96 ページ）
PURGE BOOTP RELAY（122 ページ）
SET BOOTP MAXHOPS（127 ページ）
SHOW BOOTP RELAY（155 ページ）

# ENABLE IP

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（97 ページ）
DISABLE IP FORWARDING（102 ページ）
DISABLE IP SRCROUTE（107 ページ）
ENABLE IP FORWARDING（114 ページ）
ENABLE IP SRCROUTE（119 ページ）
SHOW IP（157 ページ）

# ENABLE IP DEBUG

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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
```

## 関連コマンド

DISABLE IP DEBUG（98 ページ）
SHOW IP（157 ページ）
SHOW IP DEBUG（168 ページ）

# ENABLE IP DNSRELAY

**カテゴリー：**IP / DNS リレー
**対象機種：**AR130、AR160

**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。

## 備考・注意事項

ファームウェアバージョン 2.1.x までは、DNS サーバーの指定を SET IP NAMESERVER コマンド、SET IP SECONDARYNAMESERVER コマンドで行っていたが、バージョン 2.3.x からは ADD IP DNS コマンドで設定するように変更された。なお、従来のコマンドも後方互換性のために残されているが、設定保存時には ADD IP DNS / SET IP DNS に自動変換される。

## 関連コマンド

ADD IP DNS（59 ページ）
DELETE IP DNS（84 ページ）
DISABLE IP DNSRELAY（99 ページ）
SET IP DNS（130 ページ）
SET IP DNS CACHE（132 ページ）
SET IP DNSRELAY（134 ページ）
SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP（157 ページ）
SHOW IP DNS（169 ページ）
SHOW IP DNS CACHE（171 ページ）

# ENABLE IP ECHOREPLY

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（100 ページ）

# ENABLE IP FOFILTER

**カテゴリー：**IP / セキュリティー
**対象機種：**AR130、AR160

**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（61 ページ）
DELETE IP FILTER（86 ページ）
DISABLE IP FOFILTER（101 ページ）
SET IP FILTER（135 ページ）
SHOW IP FILTER（173 ページ）

# ENABLE IP FORWARDING

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（97 ページ）
DISABLE IP FORWARDING（102 ページ）
DISABLE IP SRCROUTE（107 ページ）
ENABLE IP（109 ページ）
ENABLE IP SRCROUTE（119 ページ）
SHOW IP（157 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
**対象機種：**AR130、AR160

**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（67 ページ）
DELETE IP HELPER（87 ページ）
DISABLE IP HELPER（103 ページ）
SHOW IP HELPER（177 ページ）

# ENABLE IP INTERFACE

**カテゴリー：**IP / IP インターフェース
**対象機種：**AR130、AR160

**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（71 ページ）
DELETE IP INTERFACE（89 ページ）
DISABLE IP INTERFACE（104 ページ）
RESET IP INTERFACE（126 ページ）
SET IP INTERFACE（140 ページ）
SHOW IP INTERFACE（181 ページ）

# ENABLE IP REMOTEASSIGN

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（105 ページ）
SHOW IP（157 ページ）

# ENABLE IP ROUTE

**カテゴリー：**IP / 経路制御（スタティック）
**対象機種：**AR130、AR160

**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（106 ページ）
SHOW IP ROUTE（191 ページ）

# ENABLE IP SRCROUTE

**カテゴリー：**IP / セキュリティー
**対象機種：**AR130、AR160

**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（97 ページ）
DISABLE IP SRCROUTE（107 ページ）
ENABLE IP（109 ページ）
ENABLE IP FORWARDING（114 ページ）
SHOW IP（157 ページ）

# PING

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**PING** [[IPADDRESS=]*ipadd*] [DELAY=*seconds*] [LENGTH=*number*] [NUMBER={*number*|CONTINUOUS}] [PATTERN=*hexnum*] [SIPADDRESS=*ipadd*] [SCREENOUTPUT={YES|NO}] [TIMEOUT=*number*] [TOS=*number*]

***ipadd***: IP アドレス
***seconds***: 秒数（0〜4294967295）
***number***: 10 進数値
***hexnum***: バイナリーストリング（16 進数 8 文字まで）

## 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。ホストテーブルに登録されているホスト名も使用可能。PING コマンドは DNS を使わないので、DNS にしか登録されていないホスト名は指定できない。
**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。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。
**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**　IP パケットの TOS オクテットの値を指定する。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
```

## 関連コマンド

ADD IP HOST（69 ページ）
SET PING（153 ページ）
SHOW PING（198 ページ）
STOP PING（206 ページ）

# PURGE BOOTP RELAY

**カテゴリー：**IP / DHCP/BOOTP リレー
**対象機種：**AR130、AR160

**PURGE BOOTP RELAY**

## 解説

DHCP/BOOTP リレー機能の設定情報をすべて破棄する。

## 関連コマンド

ADD BOOTP RELAY（57 ページ）
DELETE BOOTP RELAY（82 ページ）
DISABLE BOOTP RELAY（96 ページ）
ENABLE BOOTP RELAY（108 ページ）
SET BOOTP MAXHOPS（127 ページ）
SHOW BOOTP RELAY（155 ページ）

# PURGE IP

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**PURGE IP**

## 解説

IP 関連の設定をすべて消去し、IP モジュールを無効にする。

## 関連コマンド

RESET IP（124 ページ）

# RESET IP

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（123 ページ）
RESET IP COUNTER（125 ページ）
RESET IP INTERFACE（126 ページ）

# RESET IP COUNTER

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（124 ページ）
RESET IP INTERFACE（126 ページ）
SHOW IP COUNTER（161 ページ）

# RESET IP INTERFACE

**カテゴリー：**IP / IP インターフェース
**対象機種：**AR130、AR160

**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ルート、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（71 ページ）
DELETE IP INTERFACE（89 ページ）
DISABLE IP INTERFACE（104 ページ）
ENABLE IP INTERFACE（116 ページ）
RESET IP（124 ページ）
RESET IP COUNTER（125 ページ）
SET IP INTERFACE（140 ページ）
SHOW IP INTERFACE（181 ページ）

# SET BOOTP MAXHOPS

**カテゴリー：**IP / DHCP/BOOTP リレー
**対象機種：**AR130、AR160

**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（57 ページ）
DELETE BOOTP RELAY（82 ページ）
DISABLE BOOTP RELAY（96 ページ）
ENABLE BOOTP RELAY（108 ページ）
PURGE BOOTP RELAY（122 ページ）
SHOW BOOTP RELAY（155 ページ）

# SET IP ARP

**カテゴリー：**IP / ARP
**対象機種：**AR130、AR160

**SET IP ARP=*ipadd* INTERFACE=*interface* ETHERNET=*macadd***

***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（例：00-00-f4-12-34-56）

## 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

## 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（58 ページ）
DELETE IP ARP（83 ページ）
SHOW IP ARP（160 ページ）

# SET IP ARP TIMEOUT

**カテゴリー：**IP / ARP
**対象機種：**AR130、AR160

**SET IP ARP TIMEOUT=*multiplier***

***multiplier***: 整数値

## 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（58 ページ）
DELETE IP ARP（83 ページ）
SET IP ARP（128 ページ）
SHOW IP（157 ページ）
SHOW IP ARP（160 ページ）

# SET IP DNS

**カテゴリー：**IP / 名前解決
**対象機種：**AR130、AR160

**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 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

ファームウェアバージョン 2.1.x までは、DNS サーバーの指定を SET IP NAMESERVER コマンド、SET IP SECONDARYNAMESERVER コマンドで行っていたが、バージョン 2.3.x からは ADD IP DNS コマンド、SET IP DNS コマンドで設定するように変更された。なお、従来のコマンドも後方互換性のために残されているが、設定保存時には ADD IP DNS / SET IP DNS に自動変換される。

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.com」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.com」に対する検索が実施される。

## 関連コマンド

ADD IP DNS（59 ページ）

DELETE IP DNS（84 ページ）
DISABLE IP DNSRELAY（99 ページ）
ENABLE IP DNSRELAY（111 ページ）
SET IP DNS CACHE（132 ページ）
SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP DNS（169 ページ）
SHOW IP DNS CACHE（171 ページ）
TELNET（「運用・管理」の 264 ページ）

# SET IP DNS CACHE

**カテゴリー：**IP / 名前解決
**対象機種：**AR130、AR160

**SET IP DNS CACHE** [SIZE=*cache-entries*] [TIMEOUT=*cache-max-age*]

***cache-entries***: キャッシュエントリー数（0〜1000）
***cache-max-age***: キャッシュエントリーの有効期限（1〜60 分）

## 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（59 ページ）
DELETE IP DNS（84 ページ）
DISABLE IP DNSRELAY（99 ページ）
ENABLE IP DNSRELAY（111 ページ）
SET IP DNS（130 ページ）

SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP DNS（169 ページ）
SHOW IP DNS CACHE（171 ページ）
TELNET（「運用・管理」の 264 ページ）

# SET IP DNSRELAY

**カテゴリー：**IP / DNS リレー
**対象機種：**AR130、AR160

**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

## 備考・注意事項

ファームウェアバージョン 2.3.x より、本コマンドは ADD IP DNS コマンド、SET IP DNS コマンドに置き換えられた。本コマンドは後方互換性のためだけに残されているが、設定保存時には ADD IP DNS / SET IP DNS に自動変換される。

## 関連コマンド

ADD IP DNS（59 ページ）
DELETE IP DNS（84 ページ）
DISABLE IP DNSRELAY（99 ページ）
ENABLE IP DNSRELAY（111 ページ）
SET IP DNS（130 ページ）
SET IP DNS CACHE（132 ページ）
SET IP DNSRELAY（134 ページ）
SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP（157 ページ）
SHOW IP DNS（169 ページ）
SHOW IP DNS CACHE（171 ページ）

# SET IP FILTER

**カテゴリー：**IP / IP フィルター
**対象機種：**AR130、AR160

**SET IP FILTER=***filter-number* **ENTRY=***entry-number* {**ACTION=**{**INCLUDE**|**EXCLUDE**}|
**POLICY=***0..15*|**PRIORITY=P0..P7**} [SOURCE=*ipadd*] [SMASK=*ipadd*]
[SPORT={*port-name*|*port-id*}] [DESTINATION=*ipadd* [DMASK=*ipadd*]]
[DPORT={*port-name*|*port-id*}] [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-number***: フィルター番号（0〜299）
***entry-number***: フィルタールール番号
***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）
***ipadd***: IP アドレス
***port-name***: TCP / UDP ポート名（サービス名）
***port-id***: TCP / UDP ポート番号（0〜65535。low:high の形式で範囲指定も可）
***protocol***: IP プロトコル番号（0〜255）
***size***: データグラム長

## 解説

IP フィルタールールの設定を変更する。

## パラメーター

**FILTER**　フィルター番号。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用。

**ENTRY**　フィルタールール番号。SHOW IP FILTER コマンドで確認できる（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）の動作を指定する。INCLUDE はマッチしたパケットを通過させる。EXCLUDE はマッチしたパケットを破棄する。ACTION、POLICY、PRIORITY はどれかひとつしか指定できない。

**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（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

**SOURCE** 始点 IP アドレス。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（トラフィックフィルター）を指定する。トラフィックフィルターの場合、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。PROCOTOL=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。PROCOTOL=ICMP の場合のみ有効

**LOG** フィルタールール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、ルール番号、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、ルール番号、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 IP FILTER（61 ページ）
ADD IP INTERFACE（71 ページ）
DELETE IP FILTER（86 ページ）
SET IP INTERFACE（140 ページ）
SHOW IP FILTER（173 ページ）

# SET IP HOST

**カテゴリー：**IP / 名前解決
**対象機種：**AR130、AR160

**SET IP HOST=*name* IPADDRESS=*ipadd***

***ipadd***: IP アドレス
***name***: 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（59 ページ）
ADD IP HOST（69 ページ）
DELETE IP DNS（84 ページ）
DELETE IP HOST（88 ページ）
DISABLE IP DNSRELAY（99 ページ）
ENABLE IP DNSRELAY（111 ページ）
PING（120 ページ）
SET IP DNS（130 ページ）
SET IP DNS CACHE（132 ページ）
SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP DNS（169 ページ）
SHOW IP DNS CACHE（171 ページ）
SHOW IP HOST（179 ページ）

TELNET（「運用・管理」の 264 ページ）

# SET IP INTERFACE

**カテゴリー：**IP / IP インターフェース
**対象機種：**AR130、AR160

**SET IP INTERFACE=*interface*** [IPADDRESS=*ipadd*|DHCP] [MASK=*ipadd*]
[BROADCAST={*0*|*1*}] [DIRECTEDBROADCAST={YES|NO|ON|OFF}] [FILTER={*0..99*|NONE}] [FRAGMENT={YES|NO}] [METRIC=*1..16*] [MULTICAST={OFF|SEND|RECEIVE|BOTH|ON}] [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

## 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、eth0-0、eth0-1、eth0-2 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：eth0）は「0」を指定したものと見なされる（例：eth0-0 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）、デフォルトルート、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を指定する。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。

**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。

**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を指定する。ポリシーフィルターによって設定されたルーティングポリシー（サービスタイプ）は経路選択時に使用される。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。

**PRIORITYFILTER** 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プライオリティーフィルターの番号を指定する。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は、パケット送出時のキューイングに使用される。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。

**PROXYARP** ProxyARP（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

■eth0 の IP アドレスを変更する。

```
SET IP INT=eth0 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（71 ページ）
DELETE IP INTERFACE（89 ページ）
DISABLE IP INTERFACE（104 ページ）
ENABLE IP INTERFACE（116 ページ）
RESET IP INTERFACE（126 ページ）
SHOW IP INTERFACE（181 ページ）

# SET IP LOCAL

**カテゴリー：**IP / IP インターフェース
**対象機種：**AR130、AR160

```
SET IP LOCAL [IPADDRESS=ipadd] [FILTER={filter-number|NONE}]
   [POLICYFILTER={filter-number|NONE}] [PRIORITYFILTER={filter-number|
   NONE}]
```

***filter-number***: 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、AR ルーター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、AR ルーター自身が送信する RIP、PING 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。AR ルーターが送信する 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（71 ページ）
DELETE IP INTERFACE（89 ページ）
SET IP INTERFACE（140 ページ）

SHOW IP INTERFACE（181 ページ）

# SET IP NAMESERVER

**カテゴリー：**IP / 名前解決
**対象機種：**AR130、AR160

**SET IP NAMESERVER=*ipadd***

***ipadd***: IP アドレス

## 解説

プライマリー DNS サーバーの IP アドレスを設定する（ADD IP DNS コマンドに置き換え）。
DNS サーバーは TELNET コマンドなどで使用されるほか、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 コマンドで確認できる。

## パラメーター

**NAMESERVER**　DNS サーバーの IP アドレス。設定を解除するには 0.0.0.0 を指定する。

## 備考・注意事項

ファームウェアバージョン 2.3 より、本コマンドは ADD IP DNS コマンド、SET IP DNS コマンドに置き換えられた。後方互換性のために残されているが、設定保存時には ADD IP DNS / SET IP DNS に自動変換される。
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.com」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.com」に対する検索が実施される。

## 関連コマンド

ADD IP DNS（59 ページ）
ADD IP HOST（69 ページ）
DELETE IP DNS（84 ページ）
DELETE IP HOST（88 ページ）
SET IP DNS（130 ページ）
SET IP DNS CACHE（132 ページ）
SET IP DNSRELAY（134 ページ）
SET IP HOST（138 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP（157 ページ）
SHOW IP DNS（169 ページ）

SHOW IP DNS CACHE（171 ページ）
SHOW IP HOST（179 ページ）
TELNET（「運用・管理」の 264 ページ）

# SET IP RIP

**カテゴリー：**IP / 経路制御（RIP）
**対象機種：**AR130、AR160

```
SET IP RIP INTERFACE=interface [IP=ipadd] [SEND={NONE|RIP1|RIP2|
   COMPATIBLE}] [RECEIVE={NONE|RIP1|RIP2|BOTH}] [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**　同一サブネット上にある 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 RIP ルーターとのユニキャスト通信に関する設定となる。本パラメーターを省略した場合は、該当インターフェースで受信したすべての RIP パケットを受け入れ、送信時はブロードキャストアドレスか RIP2 ルーターマルチキャストグループアドレスに送信する。

**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（クラスフルな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。

**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 PASSWORD 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=eth0 SEND=RIP1 RECEIVE=RIP1
```

## 関連コマンド

ADD IP RIP（74 ページ）
DELETE IP RIP（90 ページ）
SET IP RIPTIMER（148 ページ）
SHOW IP RIP（186 ページ）

# SET IP RIPTIMER

**カテゴリー：**IP / 経路制御（RIP）
**対象機種：**AR130、AR160

**SET IP RIPTIMER** [FLUSH=*seconds*] [HOLDDOWN=*seconds*] [INVALID=*seconds*] [UPDATE=*seconds*]

***seconds***: 期間（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（146 ページ）
SHOW IP RIP（186 ページ）
SHOW IP RIPTIMER（190 ページ）

# SET IP ROUTE

**カテゴリー：**IP / 経路制御（スタティック）
**対象機種：**AR130、AR160

**SET IP ROUTE=*ipadd* INTERFACE=*interface* MASK=*ipadd* NEXTHOP=*ipadd***
[METRIC=*1..16*] [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

## 解説

スタティックルート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。デフォルトルートの場合は 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。デフォルトルートのマスクは 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
**METRIC** RIP が使用するメトリック。通常は 2〜16 の範囲で指定する。デフォルトは 1
**POLICY** 本経路のサービスタイプ（TOS）
**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。デフォルト値は次のとおり。インターフェース 0、RIP 100、デフォルト経路 360、デフォルト以外のスタティック経路 60。

## 関連コマンド

ADD IP ROUTE（76 ページ）
DELETE IP ROUTE（91 ページ）
SHOW IP ROUTE（191 ページ）

# SET IP ROUTE FILTER

**カテゴリー：**IP / 経路制御フィルター
**対象機種：**AR130、AR160

```
SET IP ROUTE FILTER=filter-id IP=ipadd MASK=ipadd ACTION={INCLUDE|
   EXCLUDE} [DIRECTION={RECEIVE|SEND|BOTH}] [INTERFACE=interface]
   [NEXTHOP=ipadd] [POLICY=0..7] [PROTOCOL={ANY|RIP|STATIC|INTERFACE}]
```

***filter-id***: フィルター番号（1〜100）
***interface***: IP インターフェース名（eth0、ppp0 など）
***ipadd***: IP アドレス

## 解説

IP ルートフィルターの設定内容を変更する。

## パラメーター

**FILTER**　設定を変更するフィルターの番号を指定する。ルートフィルターの番号は、SHOW IP ROUTE FILTER コマンドで確認できる。

**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。

**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。STATIC は ADD IP ROUTE コマンドによるスタティック経路の登録を抑止・許可するためのもの。また、INTERFACE は、ADD IP INTERFACE コマンドによる IP インターフェース作成時のインターフェース経路登録を抑止・許可するためのオプション。デフォルトは ANY（すべて）。

## 関連コマンド

ADD IP ROUTE FILTER（78 ページ）
DELETE IP ROUTE FILTER（92 ページ）
SHOW IP ROUTE FILTER（194 ページ）

# SET IP SECONDARYNAMESERVER

**カテゴリー：**IP / 名前解決
**対象機種：**AR130、AR160

**SET IP SECONDARYNAMESERVER=*ipadd***

***ipadd***: IP アドレス

## 解説

セカンダリー DNS サーバーの IP アドレスを設定する（ADD IP DNS コマンドに置き換え）。
セカンダリー DNS サーバーは、プライマリー DNS サーバーから 20 秒間応答がなかった場合に使用される。
DNS サーバーアドレスの設定は SHOW IP コマンドで確認できる。

## パラメーター

**SECONDARYNAMESERVER**　セカンダリー DNS サーバーの IP アドレス。設定を解除するには 0.0.0.0 を指定する。

## 備考・注意事項

ファームウェアバージョン 2.3 より、本コマンドは ADD IP DNS コマンド、SET IP DNS コマンドに置き換えられた。後方互換性のために残されているが、設定保存時には ADD IP DNS / SET IP DNS に自動変換される。

## 関連コマンド

ADD IP DNS（59 ページ）
ADD IP HOST（69 ページ）
DELETE IP DNS（84 ページ）
DELETE IP HOST（88 ページ）
SET IP DNS（130 ページ）
SET IP DNS CACHE（132 ページ）
SET IP DNSRELAY（134 ページ）
SET IP HOST（138 ページ）
SET IP NAMESERVER（144 ページ）
SHOW IP（157 ページ）
SHOW IP DNS（169 ページ）
SHOW IP DNS CACHE（171 ページ）
SHOW IP HOST（179 ページ）
TELNET（「運用・管理」の 264 ページ）

# SET PING

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

```
SET PING [[IPADDRESS=]ipadd] [DELAY=seconds] [LENGTH=number]
   [NUMBER={number|CONTINUOUS}] [PATTERN=hexnum] [SIPADDRESS=ipadd]
   [SCREENOUTPUT={YES|NO}] [TIMEOUT=number] [TOS=number]
```

***ipadd***: IP アドレス
***seconds***: 秒数（0〜4294967295）
***number***: 10 進数値
***hexnum***: バイナリーストリング（16 進数 8 文字まで）

## 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。ホストテーブルに登録されているホスト名も使用可能。PING コマンドは DNS を使わないので、DNS にしか登録されていないホスト名は指定できない。
**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。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。
**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**　IP パケットの TOS オクテットの値を指定する。有効範囲は 0〜255。

## 関連コマンド

ADD IP HOST（69 ページ）
PING（120 ページ）
SHOW PING（198 ページ）
STOP PING（206 ページ）

# SET TRACE

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**SET TRACE** [[IPADDRESS=]*ipadd*] [MAXTTL=*number*] [MINTTL=*number*]
[NUMBER=*number*] [PORT=*port-number*] [SCREENOUTPUT={YES|NO}]
[SOURCE=*ipadd*] [TIMEOUT=*number*] [TOS=*number*]

***ipadd***: IP アドレス
***number***: 10 進数値
***port-number***: 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
**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**　TOS オクテットフィールドの値。0〜255 の 10 進数値で指定する。

## 関連コマンド

ADD IP HOST（69 ページ）
SHOW TRACE（204 ページ）
STOP TRACE（207 ページ）
TRACE（208 ページ）

# SHOW BOOTP RELAY

**カテゴリー：**IP / DHCP/BOOTP リレー
**対象機種：**AR130、AR160

**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 12:

## 関連コマンド

ADD BOOTP RELAY（57 ページ）
DELETE BOOTP RELAY（82 ページ）
DISABLE BOOTP RELAY（96 ページ）
ENABLE BOOTP RELAY（108 ページ）
PURGE BOOTP RELAY（122 ページ）
SET BOOTP MAXHOPS（127 ページ）

# SHOW IP

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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 .......... Not Set
  Secondary Name Server ........ Not Set
Source-Routed Packets .......... Discarded
Remote IP address assignment ... DISABLED
DNS Relay ...................... DISABLED

Routing Protocols

RIP Neighbours ................. 0
EGP Status ..................... DISABLED
Autonomous System Number ....... Not Set
Transfer RIP to EGP ............ Disabled
ARP aging timer multiplier...... 4 (1024-2048 secs)

Active Routes

Static ......................... 1
Interface ...................... 2
RIP ............................ 0
EGP ............................ 0
Other .......................... 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 |
| RIP Neighbours | 隣接 RIP ルーター（RIP ピア）の数 |
| 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 |
| Static | スタティック経路エントリー数 |
| Interface | インターフェース経路エントリー数 |
| RIP | RIP 経路エントリー数 |
| Other | その他の経路エントリー数 |
| Filter n | IP フィルター「n」に設定されているフィルタールール数 |
| 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 13:

## 関連コマンド

DISABLE IP（97 ページ）
DISABLE IP DEBUG（98 ページ）
DISABLE IP DNSRELAY（99 ページ）
DISABLE IP FORWARDING（102 ページ）
DISABLE IP SRCROUTE（107 ページ）
DISABLE SNMP（「運用・管理」の 120 ページ）
ENABLE IP（109 ページ）
ENABLE IP DEBUG（110 ページ）

ENABLE IP DNSRELAY（111 ページ）
ENABLE IP FORWARDING（114 ページ）
ENABLE IP SRCROUTE（119 ページ）
ENABLE SNMP（「運用・管理」の 139 ページ）
SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）

# SHOW IP ARP

**カテゴリー：**IP / ARP
**対象機種：**AR130、AR160

**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
--------------------------------------------------------------------------------
  eth0             192.168.1.2      00-00-f4-e5-00-41     Dynamic     Active
  eth0             192.168.1.5      00-00-f4-42-01-6b     Dynamic     Active
  eth0             192.168.1.11     00-90-99-0e-6a-7f     Dynamic     Active
  eth0             192.168.1.255    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 アドレスか DLCI） |
| 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 14:

## 関連コマンド

ADD IP ARP（58 ページ）
DELETE IP ARP（83 ページ）
SET IP ARP（128 ページ）

# SHOW IP COUNTER

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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 15: 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 16: 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 17: 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 18: 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 19: 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 20: 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 Trap 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 Trap の総数 |

表 21: 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 22: UDP カウンター

## 関連コマンド

SHOW IP INTERFACE（181 ページ）
SHOW IP ROUTE（191 ページ）
SHOW SNMP（「運用・管理」の 242 ページ）
SHOW TCP（200 ページ）

# SHOW IP DEBUG

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（98 ページ）
ENABLE IP DEBUG（110 ページ）
SHOW IP（157 ページ）

# SHOW IP DNS

**カテゴリー：**IP / 名前解決
**対象機種：**AR130、AR160

**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.com             No           172.20.10.1     172.20.10.2           0
ringo.fruit.com             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 23:

## 関連コマンド

ADD IP DNS（59 ページ）
DELETE IP DNS（84 ページ）
DISABLE IP DNSRELAY（99 ページ）
ENABLE IP DNSRELAY（111 ページ）
SET IP DNS（130 ページ）
SET IP DNS CACHE（132 ページ）
SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP DNS CACHE（171 ページ）
TELNET（「運用・管理」の 264 ページ）

# SHOW IP DNS CACHE

**カテゴリー：**IP / 名前解決
**対象機種：**AR130、AR160

**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)
-------------------------------------------------------------------------------
ar720-2-eth1.birds.or.jp                           192.168.20.1     1794         0
ar410-vlan1.birds.or.jp                            ---              1778         0
  ::
ar410-eth0.birds.or.jp                             172.16.10.254    1775         0
ar720-1-eth0.birds.or.jp                           192.168.10.1     1770         1
kijitora.birds.or.jp                               192.168.10.100   1026         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（秒） |
| 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 24:

## 関連コマンド

ADD IP DNS（59 ページ）
DELETE IP DNS（84 ページ）
DISABLE IP DNSRELAY（99 ページ）
ENABLE IP DNSRELAY（111 ページ）
SET IP DNS（130 ページ）

SET IP DNS CACHE（132 ページ）
SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP DNS（169 ページ）
TELNET（「運用・管理」の 264 ページ）

# SHOW IP FILTER

**カテゴリー：**IP / IP フィルター
**対象機種：**AR130、AR160

**SHOW IP FILTER**[=*filter-number*]

***filter-number***: フィルター番号（0～299）

## 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. | フィルター内のルールエントリー番号 |
| 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 | 本ルール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 | このルールにマッチした 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 25:

## 関連コマンド

ADD IP FILTER（61 ページ）
ADD IP INTERFACE（71 ページ）
DELETE IP FILTER（86 ページ）
SET IP FILTER（135 ページ）
SET IP INTERFACE（140 ページ）

# SHOW IP FLOW

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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

```
Manager > 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
-------------------------------------------------------------------------------
192.168.10.100  - 172.16.20.254     UDP        53 - 2060           1  000000  2
0 eth0      -               0  n   n      1  00000000  00000000  00000000  y/n/n
192.168.20.200  - 192.168.20.1      ICMP        3 - 3              1  000000  2
0 eth1      -               0  n   n      1  00000000  00000000  00000000  n/n/n
192.168.20.200  - 192.168.20.1      UDP     65525 - 53             1  000000  2
0 eth1      -               0  n   n      1  00000000  00000000  00000000  n/n/n
192.168.10.100  - 172.16.20.254     UDP        53 - 2059           1  000000  2
0 eth0      -               0  n   n      1  00000000  00000000  00000000  y/n/n
192.168.20.200  - 192.168.20.1      UDP     65526 - 53             1  000000  2
0 eth1      -               0  n   n      1  00000000  00000000  00000000  n/n/n
192.168.10.100  - 172.16.20.254     UDP        53 - 2058           1  000000  2
0 eth0      -               0  n   n      1  00000000  00000000  00000000  y/n/n
192.168.20.200  - 192.168.20.1      UDP     65527 - 53             1  000000  2
0 eth1      -               0  n   n      1  00000000  00000000  00000000  n/n/n
192.168.10.100  - 172.16.20.254     UDP        53 - 2057           1  000000  2
0 eth0      -               0  n   n      1  00000000  00000000  00000000  y/n/n
192.168.20.200  - 192.168.20.1      UDP     65528 - 53             1  000000  2
0 eth1      -               0  n   n      1  00000000  00000000  00000000  n/n/n
192.168.10.100  - 172.16.20.254     UDP        53 - 2056           1  000000  2
0 eth0      -               0  n   n      1  00000000  00000000  00000000  y/n/n
192.168.20.200  - 192.168.20.1      UDP     65529 - 53             1  000000  2
0 eth1      -               0  n   n      1  00000000  00000000  00000000  n/n/n
172.16.20.1     - 224.0.0.9         UDP       520 - 520           21  000000  2
0 eth0      -               0  n   n      5  00000000  00000000  00000000  y/n/n
192.168.10.100  - 192.168.30.200    ICMP        8 - 0              2  000008  2
0 eth0      -              11  n   n      0  00000000  00000000  00000000  y/n/n
172.16.10.1     - 172.16.20.254     41          0 - 0              62  000000  2
0 eth0      -               0  n   n      1  00000000  00000000  00000000  y/n/n
192.168.20.200  - 224.0.0.9         UDP       520 - 520           46  000000  2
```

```
0 eth1      -               0  n   n      5  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 26:

# SHOW IP HELPER

**カテゴリー：**IP / UDP ブロードキャストヘルパー
**対象機種：**AR130、AR160

**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 : eth0
  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 27:

| | |
|---|---|
| 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 28: COUNTER オプション

## 関連コマンド

ADD IP HELPER（67 ページ）
DELETE IP HELPER（87 ページ）
DISABLE IP HELPER（103 ページ）
ENABLE IP HELPER（115 ページ）

# SHOW IP HOST

**カテゴリー：**IP / 名前解決
**対象機種：**AR130、AR160

**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 29:

## 関連コマンド

ADD IP DNS（59 ページ）
ADD IP HOST（69 ページ）
DELETE IP DNS（84 ページ）
DELETE IP HOST（88 ページ）
DISABLE IP DNSRELAY（99 ページ）
ENABLE IP DNSRELAY（111 ページ）
PING（120 ページ）
SET IP DNS（130 ページ）

SET IP DNS CACHE（132 ページ）
SET IP HOST（138 ページ）
SET IP NAMESERVER（144 ページ）
SET IP SECONDARYNAMESERVER（152 ページ）
SHOW IP DNS（169 ページ）
SHOW IP DNS CACHE（171 ページ）
TELNET（「運用・管理」の 264 ページ）

# SHOW IP INTERFACE

**カテゴリー：**IP / IP インターフェース
**対象機種：**AR130、AR160

**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 int

Interface     Type     IP Address       Bc Fr PArp  Filt RIP Met.
Pri. Filt     Pol.Filt Network Mask     MTU   VJC   GRE  DBcast  Mul.
------------------------------------------------------------------------
Local         ---      Not set          -  -  -     ---  --
---           ---      Not set          1500  -     ---  ---
eth0          Static   192.168.10.1     1  n  On    ---  01
---           ---      255.255.255.0    1500  -     ---  No      Rec
ppp0          Dynamic  12.34.56.78      1  n  Off   ---  01
---           ---      255.255.255.255  1500  -     ---  No      Rec
------------------------------------------------------------------------
```

| | |
|---|---|
| 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。 |
| 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 PPP 接続によって動的に作成されるインターフェース）、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 | Proxy 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。 |
| 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 |
| 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 30:

| | |
|---|---|
| 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。 |
| 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るインターフェース）、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 31: COUNTER オプション

## 関連コマンド

ADD IP INTERFACE（71 ページ）
DELETE IP INTERFACE（89 ページ）
DISABLE IP INTERFACE（104 ページ）
ENABLE IP INTERFACE（116 ページ）

RESET IP INTERFACE（126 ページ）
SET IP INTERFACE（140 ページ）
SHOW IP COUNTER（161 ページ）

# SHOW IP POOL

**カテゴリー：**IP / IP アドレスプール
**対象機種：**AR130、AR160

**SHOW IP POOL**[=*pool-name*] [IP=*ipadd*[-*ipadd*]] [SUMMARY]

***pool-name***: IP プール名（1〜15 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）
***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 32:

## 関連コマンド

CREATE IP POOL（81 ページ）
DESTROY IP POOL（95 ページ）

# SHOW IP RIP

**カテゴリー：**IP / 経路制御（RIP）
**対象機種：**AR130、AR160

**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  Circuit/DLCI    IP Address      Send  Receive  Demand  Auth  Password
-------------------------------------------------------------------------------
eth0       -               172.16.28.129   RIP1  BOTH     OFF     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。 |
| 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。未設定時は「NOT SET」と表示 |

表 33:

## 関連コマンド

ADD IP RIP（74 ページ）

DELETE IP RIP（90 ページ）
SET IP RIP（146 ページ）
SHOW IP（157 ページ）
SHOW IP COUNTER（161 ページ）

# SHOW IP RIP COUNTER

**カテゴリー：**IP / 経路制御（RIP）
**対象機種：**AR130、AR160

**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 ................... 0          outResponses .................. 2
    inTrigRequests ................ 0          outTrigRequests ............... 0
    inTrigResponses ............... 0          outTrigResponses .............. 0
    inTrigAcks .................... 0          outTrigAcks ................... 0
    inDiscards .................... 0
```

| | |
|---|---|
| Interface | 隣接 RIP ルーター（ピア）が存在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 |
| 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 34:

## 関連コマンド

SHOW IP COUNTER（161 ページ）
SHOW IP RIP（186 ページ）

# SHOW IP RIPTIMER

**カテゴリー：**IP / 経路制御（RIP）
**対象機種：**AR130、AR160

**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 35:

## 関連コマンド

SET IP RIPTIMER（148 ページ）

# SHOW IP ROUTE

**カテゴリー：**IP / 経路制御（スタティック）
**対象機種：**AR130、AR160

**SHOW IP ROUTE**[=*ipadd*] [{GENERAL|CACHE|COUNT}]

***ipadd***: IP アドレス。バイト単位でワイルドカード（*）の指定が可能。

## 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 > show ip route

IP Routes
-------------------------------------------------------------------------------
Destination       Mask             NextHop            Interface          Age
DLCI/Circ.        Type     Policy  Protocol           Metrics      Preference
-------------------------------------------------------------------------------
192.168.10.0      255.255.255.0     0.0.0.0            eth0               155
-                 direct   0        interface          1                    0
192.168.20.0      255.255.255.0     192.168.100.2      ppp0               143
-                 remote   0        rip                2                  100
192.168.100.0     255.255.255.0     0.0.0.0            ppp0               155
-                 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 |
| 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（ルーティングポリシー） |
| Protocol | 経路情報のソースプロトコル。静的経路（static）、RIP（rip）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 36:

| | |
|---|---|
| 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 37: 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 |

表 38: 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 |
| 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 39: COUNT オプション

## 関連コマンド

ADD IP ROUTE（76 ページ）
DELETE IP ROUTE（91 ページ）
DISABLE IP ROUTE（106 ページ）
ENABLE IP ROUTE（118 ページ）
SET IP ROUTE（149 ページ）

# SHOW IP ROUTE FILTER

**カテゴリー：**IP / 経路制御フィルター
**対象機種：**AR130、AR160

**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 40:

## 関連コマンド

ADD IP ROUTE FILTER（78 ページ）
DELETE IP ROUTE FILTER（92 ページ）
SET IP ROUTE FILTER（150 ページ）

# SHOW IP TRUSTED

**カテゴリー：**IP / 経路制御フィルター
**対象機種：**AR130、AR160

**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（61 ページ）
ADD IP TRUSTED（80 ページ）
DELETE IP FILTER（86 ページ）
DELETE IP TRUSTED（93 ページ）
SET IP FILTER（135 ページ）
SHOW IP FILTER（173 ページ）

# SHOW IP UDP

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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
      68          0.0.0.0               0
     161          0.0.0.0               0
      67          0.0.0.0               0
    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 41:

## 関連コマンド

SHOW IP COUNTER（161 ページ）
SHOW TCP（200 ページ）

# SHOW PING

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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 |
| Source | PING パケットの始点 IP 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 42:

## 関連コマンド

PING（120 ページ）
SET PING（153 ページ）
STOP PING（206 ページ）

# SHOW TCP

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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 bulbul> 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:        00017
  Attempt Fails:          00000   Established Resets:   00000
  Current Established:    00001

  In Segs:           0000002193   In Segs Error:   0000000000
  Out Segs:          0000001694   Out Segs Retran: 0000000015
  Out Segs With RST: 0000000000

  Connection Table:
  Index   State         Local port and address   Remote port and address
  ------------------------------------------------------------------------
    00    listen        00023  0.0.0.0           00000  0.0.0.0
    01    listen        05025  0.0.0.0           00000  0.0.0.0
    02    listen        00515  0.0.0.0           00000  0.0.0.0
    03    established   00023  192.168.1.1       01043  192.168.1.5
    04    listen        00113  0.0.0.0           00000  0.0.0.0
  ------------------------------------------------------------------------

Manager > show tcp=3
```

```
TCB: 03  Local: 192.168.1.1,00023  Remote: 192.168.1.5,01043
State: ESTAB  O/P State: IDLE
SND.UNA: 0309555091  SND.NXT: 0309555091  SND.WND: 16312
Last Seq: 4236410158  Last Ack: 0309555091
SendCon: 66729  DataCount: 0000000000
RCV.NXT: 4236410160  RCV.WND: 01024
Round Trip Time
SendSrt: 00046  Deviation: 00008  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。 |
| 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 43: 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 44: 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 45: コネクション番号指定時

## 関連コマンド

DELETE TCP（94 ページ）
SHOW IP COUNTER（161 ページ）
SHOW IP UDP（197 ページ）

# SHOW TRACE

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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 46:

## 関連コマンド

SET TRACE（154 ページ）
STOP TRACE（207 ページ）
TRACE（208 ページ）

# STOP PING

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**STOP PING**

## 解説

実行中の PING を停止する

## 関連コマンド

PING（120 ページ）
SET PING（153 ページ）
SHOW PING（198 ページ）

# STOP TRACE

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**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（154 ページ）
SHOW TRACE（204 ページ）
TRACE（208 ページ）

# TRACE

**カテゴリー：**IP / 一般コマンド
**対象機種：**AR130、AR160

**TRACE** [[IPADDRESS=]*ipadd*] [MAXTTL=*number*] [MINTTL=*number*]
[NUMBER=*number*] [PORT=*port-number*] [SCREENOUTPUT={YES|NO}]
[SOURCE=*ipadd*] [TIMEOUT=*number*] [TOS=*number*]

***ipadd***: IP アドレス
***number***: 10 進数値
***port-number***: UDP ポート番号

## 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
**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** TOS オクテットフィールドの値。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
```

## 関連コマンド

SET TRACE（154 ページ）
SHOW TRACE（204 ページ）
STOP TRACE（207 ページ）