

IP

概要・基本設定	7
IP ホストとしての基本設定	7
ルーター（レイヤー 3 スイッチ）としての基本設定	7
IP のデバッグ	8
IP インターフェース	10
VLAN インターフェースの指定方法	10
IP インターフェースの作成・削除	10
DHCP による IP アドレス自動設定	11
マルチホーミング	12
始点 IP アドレスの決定	12
経路制御（スタティック）	14
インターフェース（ダイレクト）経路	14
スタティック経路	16
デフォルト経路	17
経路制御（RIP）	20
プロトコル概要	20
RIP Version1 と 2	20
基本設定	20
経路制御（OSPF）	24
プロトコル概要	24
AS（Autonomous System）	24
エリア	24
仮想リンク（Virtual Link）	25
OSPF ルーター	25
OSPF メッセージ	26
LSA（Link State Advertisement）	27
設定手順	27
基本設定	28
ABR（エリア境界ルーター）	31
ASBR（AS 境界ルーター）	36
仮想リンク	40
経路制御フィルター	48
IP ルートフィルター	48
Trusted Router フィルター	49

名前解決	51
ホストテーブル	51
DNS	51
ARP	53
プロトコル概要	53
ARP エントリーの手動登録	53
プロキシ ARP	54
自動的に設定される例	54
手動で設定する例	55
ソフトウェア IP フィルター	57
基本動作	57
フィルターの構成	57
フィルター処理の流れ	58
設定手順	60
フィルタリング条件の指定	61
処理内容の指定	62
マッチしたパケットの記録	65
インターフェースへの適用	66
フィルターの削除	67
トラフィックフィルターの設定例	67
特定ホストのみ拒否	67
特定のホスト/サービスのみ許可	69
片方向 TCP 通信	72
ポリシーフィルターの設定例	74
IP アドレスによるポリシーベースルーティング	74
その他	76
DNS リレー	78
基本設定	78
DHCP サーバー機能と組み合わせた設定例	78
DHCP/BOOTP リレー	81
基本設定	81
UDP ブロードキャストヘルパー	83
基本設定	83
設定例	83
セキュリティ	86
ソースルートパケットフィルタリング	86
フラグメントオフセットフィルタリング	86
ディレクティッドブロードキャストパケットフィルタリング	87
コマンドリファレンス編	88
機能別コマンド索引	88
ADD BOOTP RELAY	92
ADD IP ARP	93

ADD IP FILTER	94
ADD IP HELPER	100
ADD IP HOST	102
ADD IP INTERFACE	103
ADD IP RIP	106
ADD IP ROUTE	108
ADD IP ROUTE FILTER	110
ADD IP TRUSTED	112
ADD OSPF AREA	113
ADD OSPF HOST	115
ADD OSPF INTERFACE	116
ADD OSPF RANGE	118
ADD OSPF STUB	120
DELETE BOOTP RELAY	121
DELETE IP ARP	122
DELETE IP FILTER	123
DELETE IP HELPER	124
DELETE IP HOST	125
DELETE IP INTERFACE	126
DELETE IP RIP	127
DELETE IP ROUTE	128
DELETE IP ROUTE FILTER	129
DELETE IP TRUSTED	130
DELETE OSPF AREA	131
DELETE OSPF HOST	132
DELETE OSPF INTERFACE	133
DELETE OSPF RANGE	134
DELETE OSPF STUB	135
DELETE TCP	136
DISABLE BOOTP RELAY	137
DISABLE IP	138
DISABLE IP DEBUG	139
DISABLE IP DNSRELAY	140
DISABLE IP ECHOREPLY	141
DISABLE IP FOFILTER	142
DISABLE IP FORWARDING	143
DISABLE IP HELPER	144
DISABLE IP INTERFACE	145
DISABLE IP REMOTEASSIGN	146
DISABLE IP ROUTE	147
DISABLE IP SRCROUTE	148
DISABLE OSPF	149

DISABLE OSPF DEBUG	150
DISABLE OSPF INTERFACE	151
DISABLE OSPF LOG	152
ENABLE BOOTP RELAY	153
ENABLE IP	154
ENABLE IP DEBUG	155
ENABLE IP DNSRELAY	156
ENABLE IP ECHOREPLY	157
ENABLE IP FOFILTER	158
ENABLE IP FORWARDING	159
ENABLE IP HELPER	160
ENABLE IP INTERFACE	161
ENABLE IP REMOTEASSIGN	162
ENABLE IP ROUTE	163
ENABLE IP SRCROUTE	164
ENABLE OSPF	165
ENABLE OSPF DEBUG	166
ENABLE OSPF INTERFACE	167
ENABLE OSPF LOG	168
FINGER	170
PING	171
PURGE BOOTP RELAY	173
PURGE IP	174
PURGE OSPF	175
RESET IP	176
RESET IP COUNTER	177
RESET IP INTERFACE	178
RESET OSPF	179
RESET OSPF COUNTER	180
RESET OSPF INTERFACE	181
SET BOOTP MAXHOPS	182
SET DHCP EXTENDID	183
SET IP ARP	184
SET IP ARP TIMEOUT	185
SET IP DNSRELAY	186
SET IP FILTER	187
SET IP HOST	190
SET IP INTERFACE	191
SET IP LOCAL	193
SET IP NAMESERVER	194
SET IP RIP	195
SET IP RIPTIMER	197

SET IP ROUTE	198
SET IP ROUTE FILTER	199
SET IP SECONDARYNAMESERVER	201
SET OSPF	202
SET OSPF AREA	204
SET OSPF HOST	206
SET OSPF INTERFACE	207
SET OSPF RANGE	209
SET OSPF STUB	210
SET PING	211
SET TRACE	212
SHOW BOOTP RELAY	213
SHOW IP	215
SHOW IP ARP	218
SHOW IP COUNTER	220
SHOW IP DEBUG	227
SHOW IP FILTER	228
SHOW IP FLOW	230
SHOW IP HELPER	232
SHOW IP HOST	234
SHOW IP INTERFACE	235
SHOW IP RIP	238
SHOW IP RIP COUNTER	240
SHOW IP RIPTIMER	242
SHOW IP ROUTE	243
SHOW IP ROUTE FILTER	247
SHOW IP TRUSTED	249
SHOW IP UDP	250
SHOW OSPF	251
SHOW OSPF AREA	253
SHOW OSPF DEBUG	256
SHOW OSPF HOST	258
SHOW OSPF INTERFACE	260
SHOW OSPF LSA	264
SHOW OSPF NEIGHBOUR	268
SHOW OSPF RANGE	270
SHOW OSPF ROUTE	272
SHOW OSPF STUB	274
SHOW PING	276
SHOW TCP	278
SHOW TRACE	282
STOP PING	284

STOP TRACE	285
TRACE	286
付録	288
ARP (Address Resolution Protocol)	288
IP (Internet Protocol)	288
TOS (Type of Service) フィールドのフォーマット	290
Flags フィールドのフォーマット	291
IP オプション	292
おもな IP プロトコル番号	293
ICMP (Internet Control Message Protocol)	294
Echo Reply (タイプ 0)	296
Destination Unreachable (タイプ 3)	296
Source Quench (タイプ 4)	297
Redirect (タイプ 5)	298
Echo (タイプ 8)	300
Router Advertisement (タイプ 9)	300
Router Solicitation (タイプ 10)	301
Time Exceeded (タイプ 11)	302
Parameter Problem (タイプ 12)	303
Timestamp (タイプ 13)	303
Timestamp Reply (タイプ 14)	304
Information Request (タイプ 15)	305
Information Reply (タイプ 16)	306
Address Mask Request (タイプ 17)	306
Address Mask Reply (タイプ 18)	307
TCP (Transmission Control Protocol)	308
UDP (User Datagram Protocol)	309
おもな Well-known ポート	310
IP アドレス	312
IP アドレスクラス一覧	312
プライベート IP アドレス	312
可変長サブネットマスク	313
マルチキャストグループアドレス	314

概要・基本設定

IP (Internet Protocol) 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

本製品はご購入時の状態で、レイヤー 2 スイッチとして機能するよう設定されています。単なるスイッチとして使うだけなら、設置・配線後電源を入れるだけで特に設定は必要ありません。

ただし、その場合でもネットワーク経由で Telnet ログインしたり、SNMP による管理をしたりしたいときは、本製品に IP アドレスを割り当てる必要があります。以下、そのための基本設定について説明します。

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. VLAN default に IP アドレスを設定します。ご購入時の状態ではすべてのポートが VLAN default に所属しています。

```
ADD IP INT=vlan-default IP=192.168.10.5 MASK=255.255.255.0 ↵
```

4. 別サブネットからもアクセスしたい場合は経路の設定も必要になります。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=vlan-default  
NEXTTHOP=192.168.10.1 ↵
```

5. 以上で設定は完了です。次回起動時にも同じ設定が有効になるよう、設定をファイルに保存し、起動スクリプトに指定します。

```
CREATE CONFIG=basic.cfg ↵  
SET CONFIG=basic.cfg ↵
```

IP モジュールの全般的な情報は SHOW IP コマンド (215 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 (235 ページ) で確認します。

経路情報は SHOW IP ROUTE コマンド (243 ページ) で確認します。

ルーター (レイヤー 3 スイッチ) としての基本設定

レイヤー 3 スイッチング (IP 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、複数の VLAN を作成してポートを割り振る必要があります。詳細については「バーチャル LAN」をご覧ください。

1. VLAN を作成します。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
```

2. VLAN にポートを割り当てます。ここではポート 1~4 を VLAN white に、ポート 5~8 を VLAN orange に割り当てています。

```
ADD VLAN=white PORT=1-4 ↵
ADD VLAN=orange PORT=5-8 ↵
```

3. IP モジュールを有効にします。

```
ENABLE IP ↵
```

4. 各 VLAN (VLAN インターフェース) に IP アドレスを割り当てます。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

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

外部への経路は ADD IP ROUTE コマンド (108 ページ) で追加します。たとえば、VLAN orange 側にサブネット 192.168.30.0/24 への経路が存在する場合は次のように設定します。

```
ADD IP ROUTE=192.168.30.0 MASK=255.255.255.0 INT=vlan-orange
NEXTTHOP=192.168.20.254 ↵
```

デフォルトルートを設定するには、ROUTE、MASK パラメーターに 0.0.0.0 を指定します (この場合 MASK は省略可能です)。INTERFACE パラメーターにはデフォルトゲートウェイ (ルーター) のある VLAN を、NEXTTHOP にはデフォルトゲートウェイの IP アドレスを指定します。たとえば、VLAN white 側にデフォルトゲートウェイ 192.168.10.32 がある場合は次のように設定します。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=vlan-white NEXTTHOP=192.168.10.32 ↵
```

IP モジュールの全般的な情報は SHOW IP コマンド (215 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 (235 ページ) で確認します。

経路情報は SHOW IP ROUTE コマンド (243 ページ) で確認します。

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 (171 ページ): 指定した IP ホスト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 (286 ページ)(Traceroute): 指定した IP ホストまでの経路 (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（103 ページ）で VLAN 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。

VLAN インターフェースの指定方法

IP 関連の設定時には下位のインターフェースとして VLAN を指定する場面が数多くあります。VLAN インターフェースの指定方法を次に示します。

- VLAN 名による指定

VLAN 名が「myname」なら、vlan-myname のように「vlan-」+VLAN 名と指定します。次に例を示します。

```
ADD IP INT=vlan-myname IP=192.168.100.10 MASK=255.255.255.0 ↵
```

- VLAN ID（VID）による指定

VID が 10 ならば、vlan10 のように「vlan」+VID のように指定します。VLAN 名のとときは異なり、ハイフンが入らないことに注意してください。

```
ADD IP INT=vlan10 IP=192.168.10.1 MASK=255.255.255.0 ↵
```

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（103 ページ）を使って、VLAN 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=vlan-white 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、vlan-white 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（191 ページ）を使います。

```
SET IP INT=vlan-white 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（126 ページ）を使います。

```
DELETE IP INT=vlan-white ↵
```

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 (235 ページ) で確認できます。

```
SHOW IP INTERFACE ↵
```

- ※ IP アドレスを設定できる VLAN インターフェースは最大 32 個です。

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、VLAN インターフェースの IP アドレスを自動設定することもできます (DHCP クライアント機能)。

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

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

```
ENABLE IP REMOTEASSIGN ↵
```

- ※ ENABLE IP REMOTEASSIGN コマンド (162 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 30 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 (235 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 (215 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 (126 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、IP パラメーターに DHCP を指定します。

```
ADD IP INT=vlan-auto IP=DHCP ↵
```

DHCP で IP アドレスを配布するインターネットサービスプロバイダー (ISP) をご利用の場合、接続認証用の「コンピューター名」を指定されることがあります。その場合は、DHCP クライアント機能の設定に先立ち、SET SYSTEM NAME コマンド (「運用・管理」の 234 ページ) で指定されたコンピューター名を設定してください。これにより、同コマンドで設定したコンピューター名が、DHCP パケットの Hostname フィールドにセットされて送信されるようになります。

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

本製品の DHCP クライアント機能では、IP アドレス、サブネットマスクに加え、DNS サーバーアドレス (2 個まで) とデフォルトルート、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 30 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（235 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（243 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（215 ページ）で確認します。「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 VLAN 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、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 1VLAN あたり 16 個まで作成できます。

論理インターフェースは「VLAN-name-n」、または、「VLANvid-n」の形式で指定します（name は VLAN 名、vid は VLAN ID）。「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（VLAN-name-0 または VLANvid-0）。

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

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

上と同じ設定を VLAN ID で指定するときは次のようにします。「vlan10-0」は「vlan10」と書くこともできます。

```
ADD IP INT=vlan10-0 IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan10-1 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、vlan-white-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 vlan-white-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。
- ✧ マルチホーミングによって VLAN 上に複数の IP インターフェースを作成した場合、その VLAN では DHCP サーバー機能を使用できません。DHCP サーバー機能を使用する VLAN ではマルチホーミングを使わないでください。

始点 IP アドレスの決定

ルーター（レイヤー 3 スイッチ）は複数のインターフェースを持つため、IP アドレスも複数あるのが普通です。ルーター本来の役割を果たすとき、すなわち他のホストが送信したパケットを中継するときには、IP パケットにルーター自身の IP アドレスが入ることはありません。

しかし、ルーター自身がパケットを送信するときには、複数ある IP アドレスのどれが始点アドレスとして使われるのかが重要なケースがあります。ここでは、本製品自身が送信するパケットの始点アドレスとして、どのアドレスが使われるのかを例を挙げながら解説します。

本製品自身が IP パケットを送信するとき、始点アドレスは以下の基準にしたがって決定されます。

1. コマンド等で始点アドレスまたは始点インターフェースを明示的に指定した場合は、そのアドレスが使われる。PING コマンド（171 ページ）の SIPADDRESS パラメーターがこれに当たる。
2. 1 に該当せず、なおかつ、SET IP LOCAL コマンド（193 ページ）で IP アドレスが指定されている場合は、そのアドレスが使われる。
3. 1、2 のいずれにも該当しない場合は、パケットを送出するインターフェースのアドレスが使われる。

経路制御（スタティック）

本製品は以下の IP ユニキャスト経路制御方式に対応しています。

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

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、「経路制御（RIP）」、「経路制御（OSPF）」をご覧ください。

スタティックルーティング（静的経路制御）は、管理者が経路情報を手動で登録するもっとも基本的な経路制御方式です。静的経路には次の種類があります。

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

インターフェース（ダイレクト）経路

本製品に直接接続されているネットワークへの経路情報です。ADD IP INTERFACE コマンド（103 ページ）で VLAN に IP アドレスを割り当てると、VLAN へのダイレクト経路が経路表に自動登録されます。たとえば、次のコマンドを実行すると、

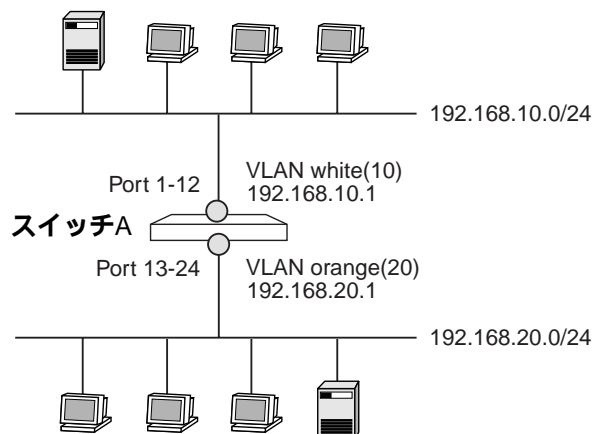
```
ADD IP INTERFACE=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
```

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	vlan10	7124
-	direct	0	interface	1	0

本製品は、複数の VLAN に IP アドレスを割り当てた時点で VLAN 間の IP ルーティングが有効になります。逆にいうと、VLAN 間ルーティングの必要がない場合は VLAN に IP アドレスを割り当てる必要はありません。

ここでは例として、VLAN を 2 つ作成し、VLAN 間で IP がルーティングされるよう設定します。



1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=vlan-white PORT=1-12 ↵
ADD VLAN=vlan-orange PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを割り当てます。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

以上で設定は完了です。IP 割り当てと同時に各 VLAN への経路情報が登録され、VLAN 間で IP のルーティングが行われるようになります。経路表を確認するには、SHOW IP ROUTE コマンド (243 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	vlan10	7475
-	direct	0	interface	1	0
192.168.20.0	255.255.255.0		0.0.0.0	vlan20	7472
-	direct	0	interface	1	0

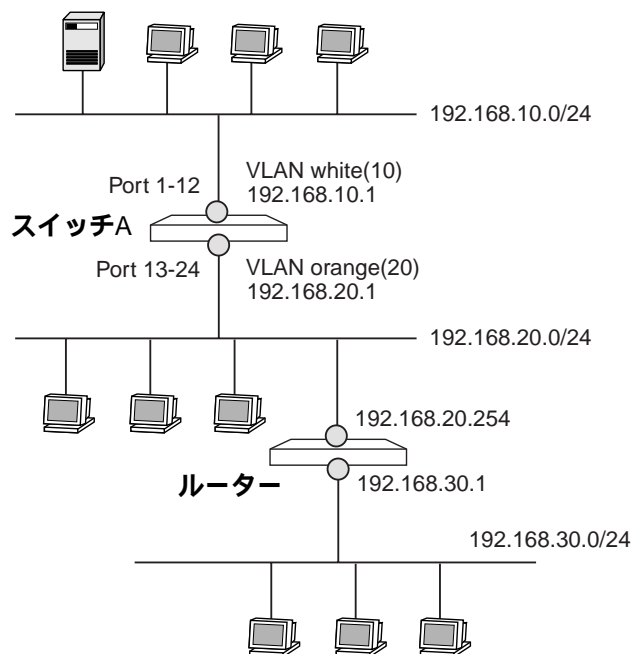
スタティック経路

ネットワーク上に他のルーターが存在するような場合には、ADD IP ROUTE コマンド (108 ページ) を使って、離れたネットワークへの経路を手動で登録することができます。

経路の登録には、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。

ここでは例として、次のようなネットワークにおけるスイッチ A の設定を示します。



1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=vlan-white PORT=1-12 ↵
ADD VLAN=vlan-orange PORT=13-24 ↵
```

2. IP モジュールを有効にします。


```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを割り当てます。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
```

```
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

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

```
ADD IP ROUTE=192.168.30.0 MASK=255.255.255.0 INT=vlan-orange
NEXTHOP=192.168.20.254 METRIC=2 ↵
```

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

経路表を確認するには、SHOW IP ROUTE コマンド (243 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	vlan10	7475
-	direct	0	interface	1	0
192.168.20.0	255.255.255.0		0.0.0.0	vlan20	7472
-	direct	0	interface	1	0
192.168.30.0	255.255.255.0		192.168.20.254	vlan20	1
-	remote	0	static	2	60

経路を削除するには DELETE IP ROUTE コマンド (128 ページ) を使います。経路削除時は、ROUTE、MASK、INTERFACE、NEXTHOP の全パラメーターを指定する必要があります。

```
DELETE IP ROUTE=192.168.30.0 MASK=255.255.255.0 INT=vlan-orange
NEXTHOP=192.168.20.254 ↵
```

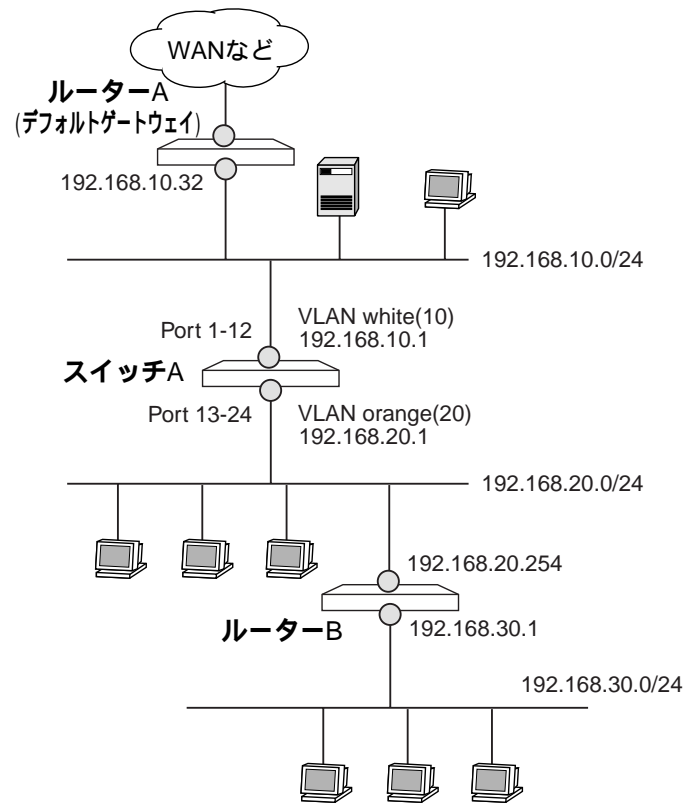
デフォルト経路

末端のネットワークでは、経路表にないネットワーク宛てのパケットをすべて特定のルーターに転送するように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 (108 ページ) の ROUTE、MASK オプションに 0.0.0.0 を指定することによって作成します (この場合 MASK は省略可能です)。たとえば、VLAN-white

上にデフォルトルート 192.168.10.32 があるならば、次のようにして登録します。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=vlan-white NEXTHOP=192.168.10.32 ↵
```

ここでは例として、次のようなネットワークにおけるスイッチ A の設定を示します。



1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=vlan-white PORT=1-12 ↵
ADD VLAN=vlan-orange PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを割り当てます。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

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

```
ADD IP ROUTE=192.168.30.0 MASK=255.255.255.0 INT=vlan-orange
NEXTTHOP=192.168.20.254 METRIC=2 ↵
```

5. それ以外のネットワーク宛てのパケットはデフォルトゲートウェイに転送します。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=vlan-white
NEXTTHOP=192.168.10.32 ↵
```

以上で設定は完了です。IP 割り当てと同時に各 VLAN への経路情報が登録され、VLAN 間で IP のルーティングが行われるようになります。また、静的経路設定により、192.168.30.0/24 宛てのパケットはルーター B のインターフェース「192.168.20.254」に転送されるようになります。また、それ以外のネットワーク（スイッチ直下の 192.168.10.0/24、192.168.20.0/24 と、スタティック登録された 192.168.30.0/24 以外）宛てのパケットは、デフォルトゲートウェイ（ルーター A）192.168.10.32 に転送されるようになります。

経路表を確認するには、SHOW IP ROUTE コマンド（243 ページ）を使います。

```
Manager > show ip route
```

IP Routes					
Destination DLCI/Circ.	Mask Type	Policy	NextHop Protocol	Interface Metrics	Age Preference
0.0.0.0	0.0.0.0		192.168.10.32	vlan10	6800
-	direct	0	static	1	360
192.168.10.0	255.255.255.0		0.0.0.0	vlan10	7475
-	direct	0	interface	1	0
192.168.20.0	255.255.255.0		0.0.0.0	vlan20	7472
-	direct	0	interface	1	0
192.168.30.0	255.255.255.0		192.168.20.254	vlan20	1
-	remote	0	static	2	60

経路を削除するには DELETE IP ROUTE コマンド（128 ページ）を使います。経路削除時は、ROUTE、MASK、INTERFACE、NEXTTHOP 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=vlan-white
NEXTTHOP=192.168.10.32 ↵
```

経路制御 (RIP)

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

- RIP (Version 1/2)
- OSPF

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

プロトコル概要

RIP (Routing Information Protocol) は比較的小規模なネットワーク用に設計されたシンプルなダイナミックルーティングプロトコルです。RIP ルーターは、自分の持つ経路表を定期的にブロードキャスト (RIP2 ではマルチキャスト) し、隣接するルーターに経路情報を伝えます。RIP パケットを受け取った各ルーターは、自分の経路表と受け取った情報を比べ、必要に応じて経路エントリーを追加・削除・修正して経路情報を最新に保ちます。

RIP にはさまざまな制限がありますが、そのシンプルさゆえに設定が簡単であり、小規模なネットワークでは有効に機能します。より大規模なネットワークでは後述する OSPF のほうが適しています。

RIP はトランスポート層として UDP を利用します。始点・終点ポートは 520 番です。

RIP Version1 と 2

現在使用されている RIP には 2 つのバージョンがあります。オリジナルの RIP (RIP Version 1) は RFC1058 で、改良版の RIP Version 2 は RFC2453 でそれぞれ規定されています。

RIP Version1 (以下 RIP1) で交換される経路情報は次のとおりです。

- 宛先ネットワークアドレス
- メトリック (ホップ数)

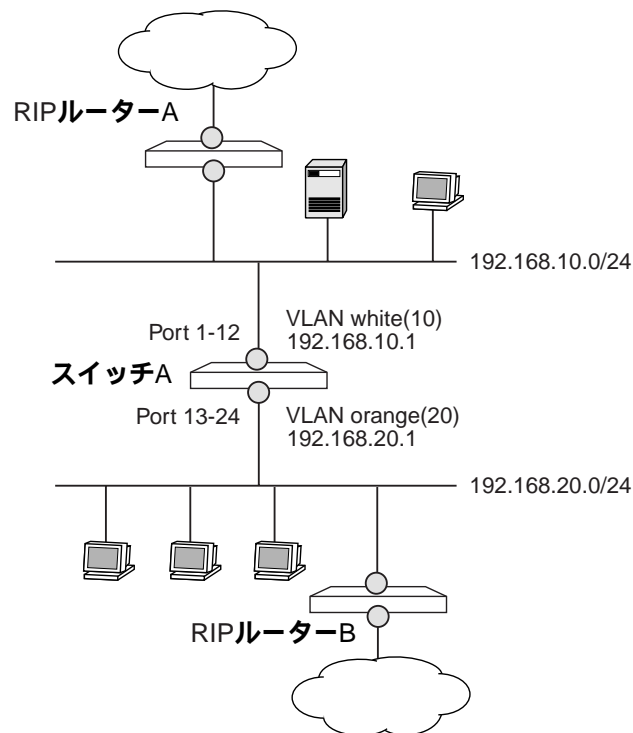
RIP1 にはサブネットマスクの概念がないため、RIP1 の経路エントリーにはクラス A、B、C に基づく標準マスクが適用されます。

一方、RIP Version2 (以下 RIP2) は、RIP1 の未使用フィールドを用いて以下の点を改良しています。

- サブネットマスクの情報を扱う
- ネクストホップルーターアドレスを扱う
- 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、スイッチ A で RIP を使用するための設定方法を説明します。



1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=vlan-white PORT=1-12 ↵
ADD VLAN=vlan-orange PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを割り当てます。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. 各 VLAN 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=vlan-white ↵
ADD IP RIP INT=vlan-orange ↵
```

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=vlan-white SEND=RIP2 ↵
ADD IP RIP INT=vlan-orange SEND=RIP2 ↵
```

設定は以上です。これにより、VLAN white、VLAN orange 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 (243 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		192.168.10.32	vlan10	4576
-	remote	0	rip	2	100
192.168.10.0	255.255.255.0		0.0.0.0	vlan10	7475
-	direct	0	interface	1	0
192.168.20.0	255.255.255.0		0.0.0.0	vlan20	7472
-	direct	0	interface	1	0
192.168.30.0	255.255.255.0		192.168.20.254	vlan20	4576
-	remote	0	rip	2	100

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 (238 ページ) を使います。

RIP インターフェースを追加するには、ADD IP RIP コマンド (106 ページ) で IP インターフェース (VLAN) を指定します。

```
ADD IP RIP INT=vlan-beige SEND=RIP2 RECEIVE=RIP2 ↵
```

RIP パケットの送受信をオフにするには、DELETE IP RIP コマンド (127 ページ) で IP インターフェース (VLAN) を指定します。

```
DELETE IP RIP INT=vlan-white ↵
```

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=vlan-white SEND=NONE RECEIVE=RIP2 ↵
```

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=vlan-white 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 (195 ページ) を使います。

```
SET IP RIP INT=vlan-white 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=vlan-white SEND=RIP2 RECEIVE=RIP2 AUTHENTICATION=PASSWORD  
PASSWORD=himitsu ↵
```

RIP パケットの送受信統計は SHOW IP RIP COUNTER コマンド (240 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 (197 ページ) で行います。

経路制御 (OSPF)

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

- RIP (Version 1/2)
- OSPF

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

プロトコル概要

OSPF (Open Shortest Path First) は中規模以上のネットワークでの使用を想定して開発された経路制御プロトコルです。現在のバージョンである OSPF Version 2 は RFC2328 で規定されています。

RIP がネットワーク全体をフラットなものとして扱うのに対し、OSPF ではネットワークをエリアと呼ばれる小さな単位に分割して、経路情報をエリアごとに管理する点が特徴的です。また、使用するアルゴリズムも異なり、OSPF ではリンクステートアルゴリズム、RIP はディスタンスベクターアルゴリズムを使用しています。

OSPF が採用するリンクステートアルゴリズムでは、同一エリア内のすべてのルーターが同じトポロジーデータベースを保持しています。各ルーターはこのデータベースをもとに経路表を作成し、これに基づいてエリア内の経路選択を行います。エリア内部の詳細なトポロジーは他のエリアからは見えないようになっており、経路情報の削減に貢献しています。

AS (Autonomous System)

経路制御プロトコルには、組織内で使用する IGP (Interior Gateway Protocol) と組織間で使用する EGP (Exterior Gateway Protocol) がありますが、OSPF は RIP と同様 IGP に分類されます。

ここでいう「組織」は、より正確には「AS (Autonomous System = 自律システム)」と呼ぶべきものです。AS とは、同じルーティングプロトコルを使用して経路情報を交換しあっているルーターの集まり、すなわち、OSPF なら OSPF、RIP なら RIP を使用しているネットワークの範囲を示します。AS はルーティングドメインなどと呼ばれることもあります。

エリア

OSPF では、ネットワークを複数のエリアに分割して、それぞれを経路情報の管理範囲とします。各エリアは、エリア ID と呼ばれる 32 ビットの数値で識別されます。通常エリア ID は「1.1.1.1」のように IP アドレスと同じ形式で書き表します。エリア ID は ADD OSPF AREA コマンド (113 ページ) でエリアを作成するときに指定します。エリア ID 0.0.0.0 は、後述するバックボーンエリアのために予約されています。

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

各エリアで分散管理されている経路情報を束ねるのは、バックボーンと呼ばれる特殊なエリアです。OSPF ネットワークを構成する各エリアは必ずバックボーンエリア（エリア ID 0.0.0.0）に接続されており、エリアごとに管理されている経路情報は、バックボーンエリア経由で他のエリアに伝えられます。

このとき重要な役割を果たすのが、各エリアとバックボーンの境界に位置するエリア境界ルーター（ABR）です。ABR はエリア内の情報を要約した上で、これを他エリアの ABR にバックボーン経由で伝える役割を持ちます。また、バックボーン経由で入手した他エリアの経路情報をエリア内部に通知する役割も果たします。始点・終点ともに同一エリア内のトラフィックは、エリア内の情報だけに基づいて配送されます（エリア内ルーティング）。一方、エリアをまたがるトラフィックは、エリア内 エリア間 エリア内の 2 レベル 3 段階で配送されます（エリア間ルーティング）。

OSPF エリアには次のような種類があります。

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

表 1: OSPF エリアの種類

仮想リンク (Virtual Link)

OSPF ネットワークでは、バックボーン以外のすべてのエリアが、バックボーンエリアと接続されている必要があります。物理的にバックボーンエリアと隣接することが不可能なエリアでは、仮想リンクを使って論理的にバックボーンとの接続を確立します。これは、バックボーンエリアの ABR と孤立したエリアの ABR が、ノーマルエリアをはさんで仮想的な接続を張ることによって実現されます。これにより、孤立エリアは、ノーマルエリアと直接接続され、バックボーンエリアとは間接的に接続されていることになります。詳細は、「仮想リンクの設定例」をご覧ください。

OSPF ルーター

OSPF ルーターは、それぞれルーター ID という識別子を持ちます。ルーター ID はエリア ID と同様の 32 ビット値で、通常はエリア ID と同じように IP アドレスと同じ形式で書き表します (例: 2.2.2.2)。

ルーター ID は、SET OSPF コマンド (202 ページ) の ROUTERID パラメーターで設定することができます。特に設定しなかった場合はルーターのインターフェースに割り当てられた IP アドレスのうち、もっとも大きなものがルーター ID として使用されます。

- ルーター ID は IP アドレスと同じ形式で表しますが、IP アドレスと直接の関係はありません。明示的に設定しなかった場合はインターフェースのアドレスのうちもっとも大きなものが使われますが、これも一意の識別子を得るための方法として使っているだけであり、実際には任意の数値を使うことができます。管理上わかりやすい番号を付けるとよいでしょう。

OSPF ルーターは、役割によって以下のとおり分類できます。

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

表 2: OSPF ルーターの種類

OSPF メッセージ

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

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

OSPF メッセージには以下の種類があります。

タイプ	メッセージ名	説明
1	Hello (Hello)	隣接ルーターの探索、代表ルーター (DR) の決定などに使用する

2	Database Description(データベース記述)	隣接関係の形成時にトポロジデータベースの内容を要約して通知する
3	Link State Request(リンク状態要求)	隣接関係形成の最終段階において追加の LSA (トポロジ情報) を要求する
4	Link State Update(リンク状態更新)	LSA (トポロジ情報) を通知する
5	Link State Ack (リンク状態確認)	リンク状態更新パケットに対する確認応答

表 3:

LSA (Link State Advertisement)

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

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

表 4: LSA の種類

設定手順

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

1. エリアを作成します。

OSPF ルーターは必ずエリアに属さなければなりません。また、OSPF ネットワークには、必ずバックボーンエリア (0.0.0.0) というエリアが存在しなければなりません。最初に ADD OSPF AREA コ

マンド (113 ページ) を実行して、バックボーンエリアを作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

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

2. エリアに所属するネットワークの範囲を設定します。

手順 1 で作成したエリアの範囲を IP アドレスとネットマスクによって定義します。たとえば、バックボーンエリアの範囲として 172.16.0.0 ~ 172.16.255.255 を指定するには、ADD OSPF RANGE コマンド (118 ページ) を使って以下のように定義します。

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

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

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

3. OSPF インターフェースの設定をします。

OSPF メッセージの送受信を行う IP インターフェース (VLAN) をエリアに割り当てます。これには ADD OSPF INTERFACE コマンド (116 ページ) を使います。ここで指定するインターフェースのアドレスは、手順 2 で設定したネットワーク範囲内のアドレスでなくてはなりません。この例では、vlan-red の IP アドレスは、172.16.0.1 ~ 172.16.255.254 の範囲内である必要があります。

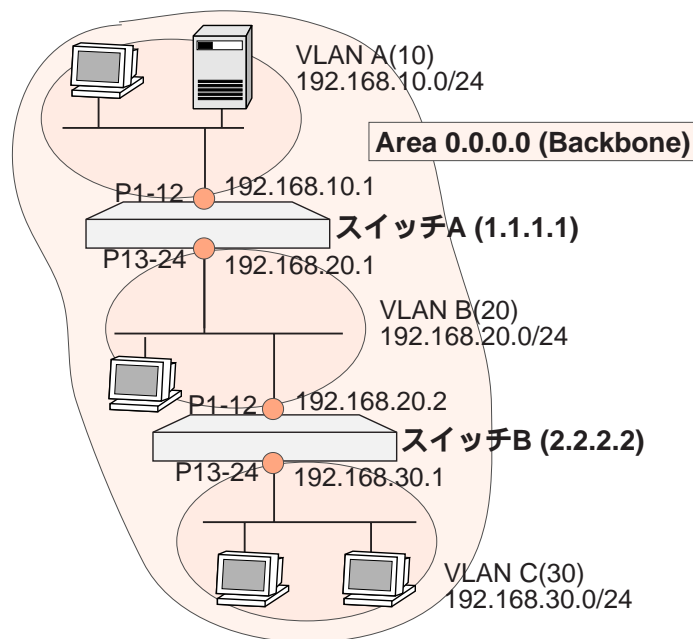
```
ADD OSPF INTERFACE=vlan-red AREA=0.0.0.0 ↵
```

4. OSPF を有効にします。

```
ENABLE OSPF ↵
```

基本設定

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



スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
ADD VLAN=A PORT=1-12 ↵
ADD VLAN=B PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-A IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-B IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=1.1.1.1 ↵
```

5. バックボーンエリア (0.0.0.0) を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

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

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

7. バックボーンエリアに所属する IP インターフェースを指定します。

```
ADD OSPF INT=vlan-A AREA=0.0.0.0 ↵
ADD OSPF INT=vlan-B AREA=0.0.0.0 ↵
```

8. OSPF を有効にします。

```
ENABLE OSPF ↵
```

スイッチ B の設定

1. VLAN の設定を行います。

```
CREATE VLAN=B VID=20 ↵
CREATE VLAN=C VID=30 ↵
ADD VLAN=B PORT=1-12 ↵
ADD VLAN=C PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-B IP=192.168.20.2 MASK=255.255.255.0 ↵
ADD IP INT=vlan-C IP=192.168.30.1 MASK=255.255.255.0 ↵
```

4. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=2.2.2.2 ↵
```

5. バックボーンエリア (0.0.0.0) を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

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

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

7. バックボーンエリアに所属する IP インターフェースを指定します。

```
ADD OSPF INT=vlan-B AREA=0.0.0.0 ↵  
ADD OSPF INT=vlan-C AREA=0.0.0.0 ↵
```

8. OSPF を有効にします。

```
ENABLE OSPF ↵
```

設定は以上です。

経路表を確認するには、SHOW IP ROUTE コマンド (243 ページ) を使います。

OSPF インターフェースの状態は SHOW OSPF INTERFACE コマンド (260 ページ) で確認します。

```
SHOW OSPF INT ↵  
SHOW OSPF INT=vlan-A ↵
```

隣接ルーターの情報を確認するには、SHOW OSPF NEIGHBOUR コマンド (268 ページ) を使います。

```
SHOW OSPF NEIGHBOUR ↵
```

OSPF エリアの情報を確認するには、SHOW OSPF AREA コマンド (253 ページ) を使います。

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

OSPF エリアの範囲を確認するには、SHOW OSPF RANGE コマンド (270 ページ) を使います。

```
SHOW OSPF RANGE ↵
```

トポロジデータベースの情報を確認するには SHOW OSPF LSA コマンド (264 ページ) を使います。

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

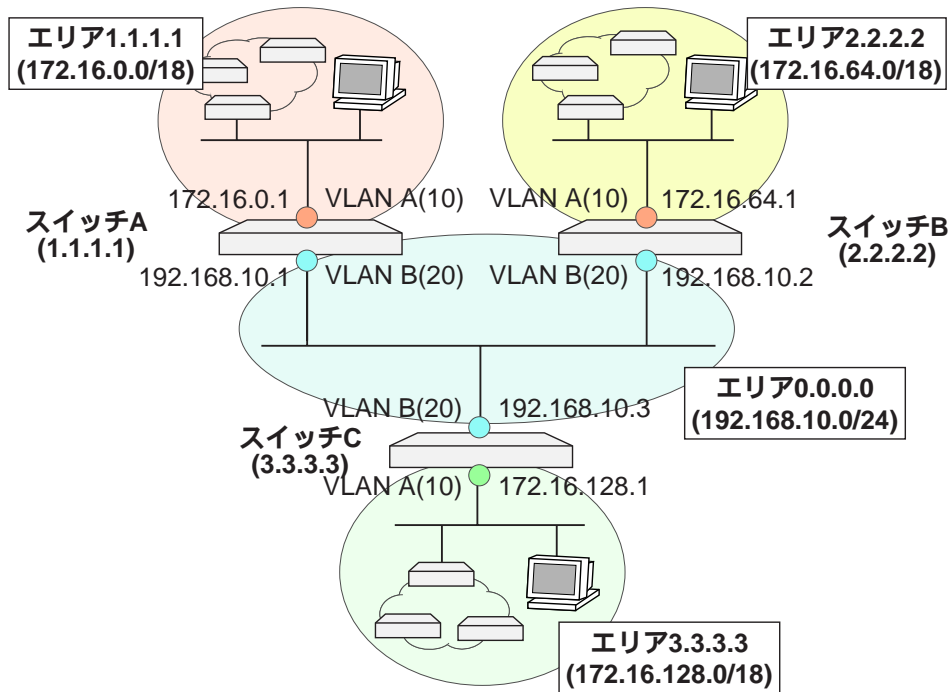
OSPF の設定情報を確認するには SHOW OSPF コマンド (251 ページ) を使います。

```
SHOW OSPF ↵
```

ABR (エリア境界ルーター)

バックボーン (0.0.0.0) とエリア 1.1.1.1、2.2.2.2、3.3.3.3 の 4 エリアで構成される OSPF ネットワークの設定例を示します。エリア間に位置する ABR は、各エリア内の経路情報を要約して他のエリアに伝える役割を

果たします。ここでは、スイッチ A、B、C を ABR とする次のようなネットワーク構成を例に解説します。
ここでは、ABR でのエリア範囲設定 (ADD OSPF RANGE コマンド (118 ページ)) によって、各エリア内の経路情報を集約してバックボーンに広報するよう設定します。



各エリアの範囲は次の通りです。

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

表 5:

スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
ADD VLAN=A PORT=1-12 ↵
ADD VLAN=B PORT=13-24 ↵
```

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


```
ENABLE IP ↵
ADD IP INT=vlan-A IP=172.16.0.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-B IP=192.168.10.1 MASK=255.255.255.0 ↵
```

3. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=1.1.1.1 ↵
```

4. バックボーンエリア (0.0.0.0) を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

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

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

6. バックボーンエリアに所属する IP インターフェースを指定します。

```
ADD OSPF INT=vlan-B AREA=0.0.0.0 ↵
```

7. エリア 1.1.1.1 を作成します。

```
ADD OSPF AREA=1.1.1.1 ↵
```

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

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

9. エリア 1.1.1.1 に所属する IP インターフェースを指定します。

```
ADD OSPF INT=vlan-A AREA=1.1.1.1 ↵
```

10. OSPF を有効にします。

```
ENABLE OSPF ↵
```

スイッチ B の設定

1. VLAN の設定を行います。

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
ADD VLAN=A PORT=1-12 ↵
ADD VLAN=B PORT=13-24 ↵
```

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

```
ENABLE IP ↵
ADD IP INT=vlan-A IP=172.16.64.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-B IP=192.168.10.2 MASK=255.255.255.0 ↵
```

3. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=2.2.2.2 ↵
```

4. バックボーンエリア (0.0.0.0) を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

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

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

6. バックボーンエリアに所属する IP インターフェースを指定します。

```
ADD OSPF INT=vlan-B AREA=0.0.0.0 ↵
```

7. エリア 2.2.2.2 を作成します。

```
ADD OSPF AREA=2.2.2.2 ↵
```

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

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

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

```
ADD OSPF INT=vlan-A AREA=2.2.2.2 ↵
```

10. OSPF を有効にします。

```
ENABLE OSPF ↵
```

スイッチ C の設定

1. VLAN の設定を行います。

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
ADD VLAN=A PORT=1-12 ↵
ADD VLAN=B PORT=13-24 ↵
```

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

```
ENABLE IP ↵
ADD IP INT=vlan-A IP=172.16.128.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-B IP=192.168.10.3 MASK=255.255.255.0 ↵
```

3. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=3.3.3.3 ↵
```

4. バックボーンエリア (0.0.0.0) を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

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

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

6. バックボーンエリアに所属する IP インターフェースを指定します。

```
ADD OSPF INT=vlan-B AREA=0.0.0.0 ↵
```

7. エリア 3.3.3.3 を作成します。

```
ADD OSPF AREA=3.3.3.3 ↵
```

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

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

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

```
ADD OSPF INT=vlan-A AREA=3.3.3.3 ↵
```

10. OSPF を有効にします。

```
ENABLE OSPF ↵
```

設定は以上です。

経路表を確認するには、SHOW IP ROUTE コマンド (243 ページ) を使います。

OSPF インターフェースの状態は SHOW OSPF INTERFACE コマンド (260 ページ) で確認します。

```
SHOW OSPF INT ↵
```

```
SHOW OSPF INT=vlan-A ↵
```

隣接ルーターの情報を確認するには、SHOW OSPF NEIGHBOUR コマンド (268 ページ) を使います。

```
SHOW OSPF NEIGHBOUR ↵
```

OSPF エリアの情報を確認するには、SHOW OSPF AREA コマンド (253 ページ) を使います。

```
SHOW OSPF AREA ↵
```

```
SHOW OSPF AREA=0.0.0.0 ↵
```

OSPF エリアの範囲を確認するには、SHOW OSPF RANGE コマンド (270 ページ) を使います。

```
SHOW OSPF RANGE ↵
```

トポロジーデータベースの情報を確認するには SHOW OSPF LSA コマンド (264 ページ) を使います。

```
SHOW OSPF LSA ↵
```

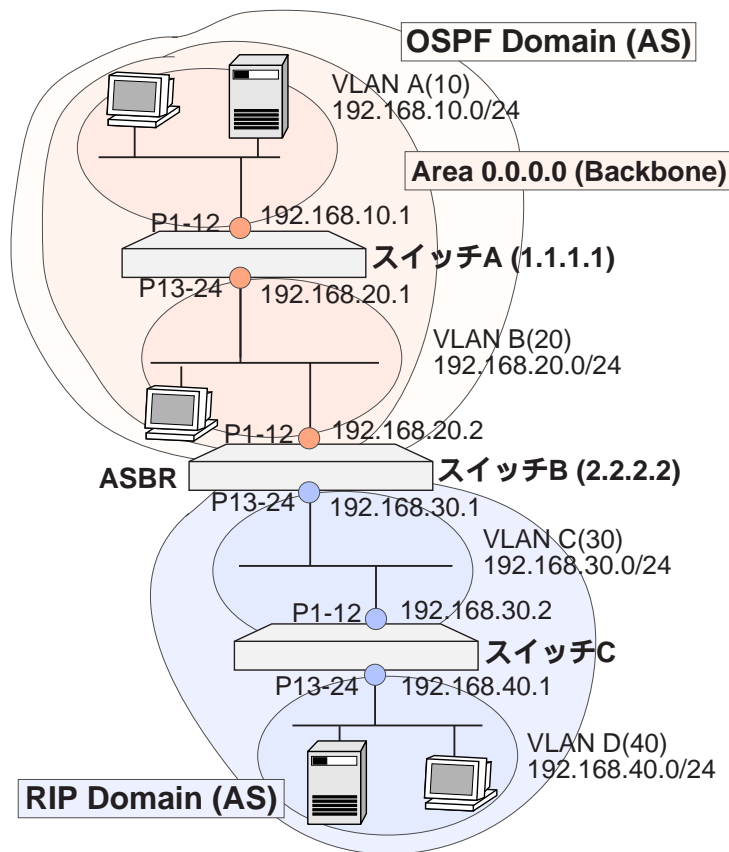
```
SHOW OSPF LSA FULL ↵
```

OSPF の設定情報を確認するには SHOW OSPF コマンド (251 ページ) を使います。

```
SHOW OSPF ↵
```

ASBR (AS 境界ルーター)

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



スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
ADD VLAN=A PORT=1-12 ↵
ADD VLAN=B PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-A IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-B IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=1.1.1.1 ↵
```

5. OSPF のバックボーンエリア (0.0.0.0) を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

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

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

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

7. バックボーンエリアに所属する IP インターフェースを設定します。

```
ADD OSPF INT=vlan-A AREA=0.0.0.0 ↵
```

```
ADD OSPF INT=vlan-B AREA=0.0.0.0 ↵
```

8. OSPF を有効にします。

```
ENABLE OSPF ↵
```

スイッチ B の設定

1. VLAN の設定を行います。

```
CREATE VLAN=B VID=20 ↵
```

```
CREATE VLAN=C VID=30 ↵
```

```
ADD VLAN=B PORT=1-12 ↵
```

```
ADD VLAN=C PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-B IP=192.168.20.2 MASK=255.255.255.0 ↵
```

```
ADD IP INT=vlan-C IP=192.168.30.1 MASK=255.255.255.0 ↵
```

4. VLAN C 側で RIP パケットの送受信を有効にします。

```
ADD IP RIP INT=vlan-C ↵
```

※ RIP ではなくスタティックルーティングを行う場合は、ADD IP ROUTE コマンド (108 ページ) で経路情報を登録してください。たとえば、この例では「ADD IP ROUTE=192.168.40.0 MASK=255.255.255.0 INT=vlan-C NEXT=192.168.30.2」などとしています。

5. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=2.2.2.2 ↵
```

6. バックボーンエリア (0.0.0.0) を作成します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

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

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

8. バックボーンエリアに所属する IP インターフェースを設定します。

```
ADD OSPF INT=vlan-B AREA=0.0.0.0 ↵
```

9. ASBR ルーターの設定をします。「RIP=BOTH」は、RIP と OSPF の間で経路情報を相互に交換するための設定です。

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

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

10. OSPF を有効にします。

```
ENABLE OSPF ↵
```

スイッチ C の設定

1. VLAN の設定を行います。

```
CREATE VLAN=C VID=30 ↵
```

```
CREATE VLAN=D VID=40 ↵
```

```
ADD VLAN=C PORT=1-12 ↵
```

```
ADD VLAN=D PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-C IP=192.168.30.2 MASK=255.255.255.0 ↵
```

```
ADD IP INT=vlan-D IP=192.168.40.1 MASK=255.255.255.0 ↵
```

4. VLAN C 側で RIP パケットの送受信を有効にします。また、VLAN D 側では RIP パケットの送信のみを有効にします。

```
ADD IP RIP INT=vlan-C ↵
ADD IP RIP INT=vlan-D SEND=RIP1 RECEIVE=NONE ↵
```

✎ RIPではなくスタティックルーティングを行う場合は、ADD IP ROUTE コマンド (108 ページ) で経路情報を登録してください。たとえば、この例では「ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=vlan-C NEXT=192.168.30.1」とすれば、直接接続されていないネットワーク宛てのパケットがすべてデフォルトルート (スイッチ B) に送られるようになります。

経路表を確認するには、SHOW IP ROUTE コマンド (243 ページ) を使います。

OSPF インターフェースの状態は SHOW OSPF INTERFACE コマンド (260 ページ) で確認します。

```
SHOW OSPF INT ↵
SHOW OSPF INT=vlan-B ↵
```

OSPF エリアの情報を確認するには、SHOW OSPF AREA コマンド (253 ページ) を使います。

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

OSPF エリアの範囲を確認するには、SHOW OSPF RANGE コマンド (270 ページ) を使います。

```
SHOW OSPF RANGE ↵
```

トポロジデータベースの情報を確認するには SHOW OSPF LSA コマンド (264 ページ) を使います。

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

OSPF の設定情報を確認するには SHOW OSPF コマンド (251 ページ) を使います。

```
SHOW OSPF ↵
```

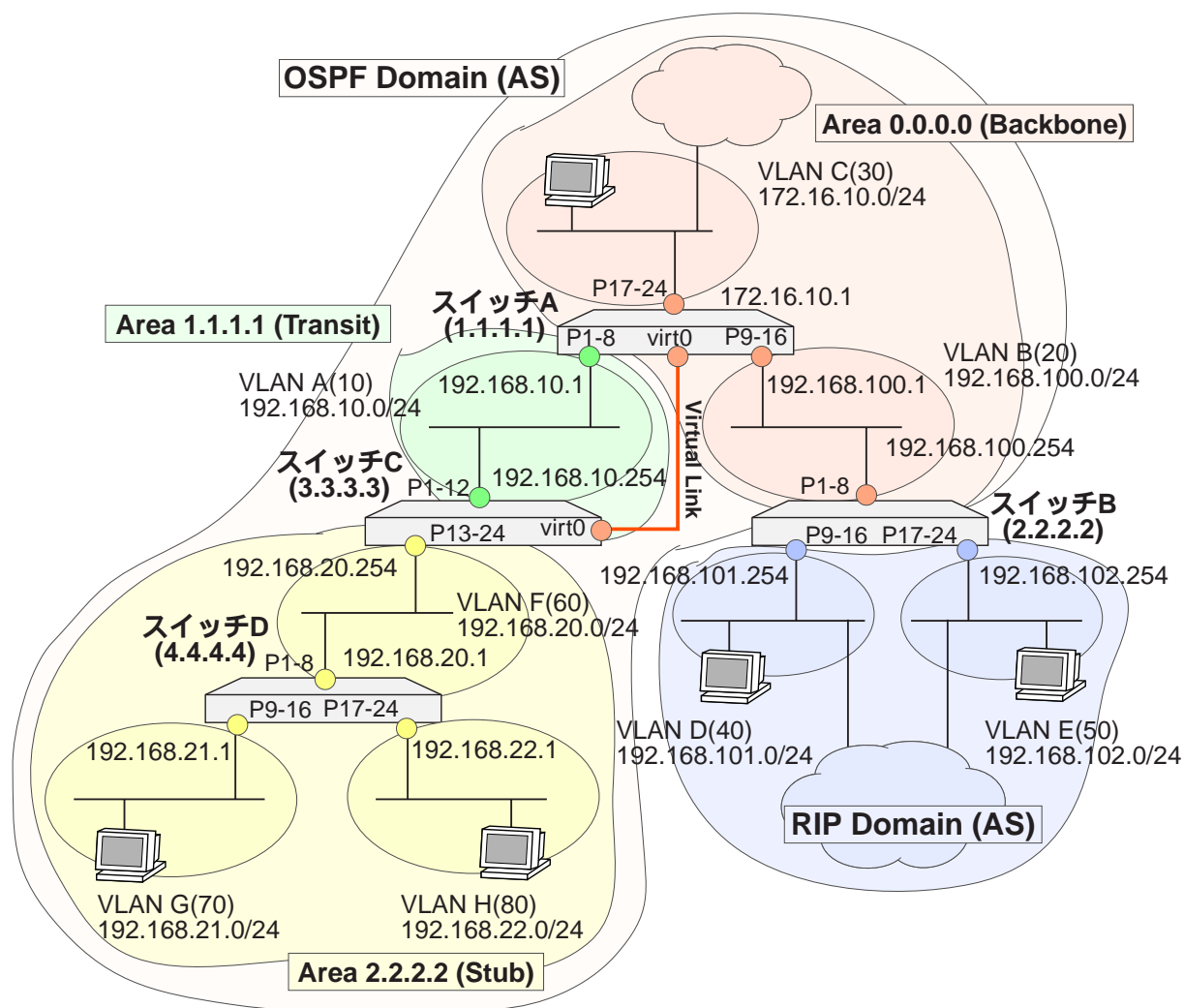
RIP の設定を確認するには SHOW IP RIP コマンド (238 ページ) を使います。

仮想リンク

ここでは仮想リンクの設定方法について説明します。

OSPF ではエリア間の経路情報をバックボーンエリア (0.0.0.0) 経由で交換するため、すべてのエリアがバックボーンエリアと接していないわけではありません。しかし、仮想リンクを設定することにより、バックボーンと直接接続されていないエリアとバックボーンを仮想的に接続することができます。

ここでは次のような構成のネットワークを例に説明します。



各エリアの範囲は次の通りです。

エリア	範囲
0.0.0.0 (バックボーン)	172.16.0.0/16, 192.168.100.0/24
1.1.1.1 (通過エリア)	192.168.10.0/24
2.2.2.2 (スタブエリア)	192.168.20.0/24, 192.168.21.0/24, 192.168.22.0/24
AS 外部 (RIP ドメイン)	192.168.101.0/24, 192.168.102.0/24

表 6:

OSPF ルーター (スイッチ) は 4 台あります。各スイッチの設定を次にまとめます。

スイッチ A

- ルーター ID は 1.1.1.1
- 2 つのエリア、0.0.0.0 (バックボーン) と 1.1.1.1 に所属するエリア境界ルーター (ABR)

- 通常のインターフェースは3つ。VLAN A は 1.1.1.1 に、VLAN B と C は 0.0.0.0 に所属
- スイッチ C (ID 3.3.3.3) との間に仮想リンクを張り、エリア 2.2.2.2 とバックボーンエリアを接続。

スイッチ B

- ルーター ID は 2.2.2.2
- 1つのエリア、0.0.0.0 (バックボーン) にだけ所属。OSPF ドメインの境界に位置する AS 境界ルーター (ASBR)
- 通常のインターフェースは3つ。VLAN B だけが 0.0.0.0 に所属。D と E は AS 外 (RIP を使用)

スイッチ C

- ルーター ID は 3.3.3.3
- 3つのエリア、0.0.0.0 (バックボーン)、1.1.1.1、2.2.2.2 に所属するエリア境界ルーター (ABR)
- バックボーンエリアとは、スイッチ A (ID 1.1.1.1) との間に張られた仮想リンクで結ばれている。
- インターフェースは2つ。VLAN A は 1.1.1.1 に、VLAN F は 2.2.2.2 に所属している。

スイッチ D

- ルーター ID は 4.4.4.4
- 1つのエリア、2.2.2.2 にだけ所属する内部ルーター (IR)
- インターフェースは3つ。VLAN F、G、H ともエリア 2.2.2.2 に所属。

スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
CREATE VLAN=C VID=30 ↵
ADD VLAN=A PORT=1-8 ↵
ADD VLAN=B PORT=9-16 ↵
ADD VLAN=C PORT=17-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-A IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-B IP=192.168.100.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-C IP=172.16.10.1 MASK=255.255.255.0 ↵
```

4. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=1.1.1.1 ↵
```

5. バックボーンエリア (0.0.0.0) を作成し、範囲を指定します。

```
ADD OSPF AREA=0.0.0.0 ↵
ADD OSPF RANGE=172.16.0.0 MASK=255.255.0.0 AREA=0.0.0.0 ↵
ADD OSPF RANGE=192.168.100.0 MASK=255.255.255.0 AREA=0.0.0.0 ↵
```

6. エリア 1.1.1.1 を作成し、範囲を指定します。仮想リンクの通過エリアとなるため、STUBAREA=OFF を指定します。

```
ADD OSPF AREA=1.1.1.1 STUBAREA=OFF ↵
ADD OSPF RANGE=192.168.10.0 MASK=255.255.255.0 AREA=1.1.1.1 ↵
```

※ STUBAREA=OFF を忘れるとスタブエリアとなり、仮想リンクが通過できなくなりますのでご注意ください。

7. バックボーンエリアに所属するインターフェースを指定します。

```
ADD OSPF INT=vlan-B AREA=0.0.0.0 ↵
ADD OSPF INT=vlan-C AREA=0.0.0.0 ↵
```

8. エリア 1.1.1.1 に所属するインターフェースを指定します。

```
ADD OSPF INT=vlan-A AREA=1.1.1.1 ↵
```

9. エリア 2.2.2.2 の ABR (ID 3.3.3.3) との間に仮想リンクを張ります。AREA には通過エリアを、VIRTUALLINK には対向 ABR のルーター ID を指定します。

```
ADD OSPF INT=virt0 AREA=1.1.1.1 VIRTUALLINK=3.3.3.3 ↵
```

10. OSPF を有効にします。

```
ENABLE OSPF ↵
```

スイッチ B の設定

1. VLAN の設定を行います。

```
CREATE VLAN=B VID=20 ↵
CREATE VLAN=D VID=40 ↵
CREATE VLAN=E VID=50 ↵
ADD VLAN=B PORT=1-8 ↵
ADD VLAN=D PORT=9-16 ↵
ADD VLAN=E PORT=17-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-B IP=192.168.100.254 MASK=255.255.255.0 ↵
```

```
ADD IP INT=vlan-D IP=192.168.101.254 MASK=255.255.255.0 ↵
```

```
ADD IP INT=vlan-E IP=192.168.102.254 MASK=255.255.255.0 ↵
```

4. VLAN-D と E で RIP を有効にします。

```
ADD IP RIP INT=vlan-D ↵
```

```
ADD IP RIP INT=vlan-E ↵
```

5. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=2.2.2.2 ↵
```

6. バックボーンエリア (0.0.0.0) を作成し、範囲を指定します。他のルーターと同じ設定になるよう注意してください。

```
ADD OSPF AREA=0.0.0.0 ↵
```

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

```
ADD OSPF RANGE=192.168.100.0 MASK=255.255.255.0 AREA=0.0.0.0 ↵
```

7. バックボーンエリアに所属するインターフェースを指定します。

```
ADD OSPF INT=vlan-B AREA=0.0.0.0 ↵
```

8. AS 境界ルーター (ASBR) として動作するよう設定します。

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

9. OSPF を有効にします。

```
ENABLE OSPF ↵
```

スイッチ C の設定

1. VLAN の設定を行います。

```
CREATE VLAN=A VID=10 ↵
```

```
CREATE VLAN=F VID=60 ↵
```

```
ADD VLAN=A PORT=1-12 ↵
```

```
ADD VLAN=F PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェイスに IP アドレスを設定します。

```
ADD IP INT=vlan-A IP=192.168.10.254 MASK=255.255.255.0 ↵
```

```
ADD IP INT=vlan-F IP=192.168.20.254 MASK=255.255.255.0 ↵
```

4. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=3.3.3.3 ↵
```

5. バックボーンエリア (0.0.0.0) を作成し、範囲を指定します。他のルーターと同じ設定になるよう注意してください。バックボーンエリアとは仮想リンクで接続します。

```
ADD OSPF AREA=0.0.0.0 ↵
```

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

```
ADD OSPF RANGE=192.168.100.0 MASK=255.255.255.0 AREA=0.0.0.0 ↵
```

6. エリア 1.1.1.1 を作成し、範囲を指定します。仮想リンクの通過エリアとなるため、STUBAREA=OFF を指定します。他のルーターと同じ設定になるよう注意してください。

```
ADD OSPF AREA=1.1.1.1 STUBAREA=OFF ↵
```

```
ADD OSPF RANGE=192.168.10.0 MASK=255.255.255.0 AREA=1.1.1.1 ↵
```

※ STUBAREA=OFF を忘れるとスタブエリアとなり、仮想リンクが通過できなくなりますのでご注意ください。

7. エリア 2.2.2.2 を作成し、範囲を指定します。

```
ADD OSPF AREA=2.2.2.2 ↵
```

```
ADD OSPF RANGE=192.168.20.0 MASK=255.255.255.0 AREA=2.2.2.2 ↵
```

```
ADD OSPF RANGE=192.168.21.0 MASK=255.255.255.0 AREA=2.2.2.2 ↵
```

```
ADD OSPF RANGE=192.168.22.0 MASK=255.255.255.0 AREA=2.2.2.2 ↵
```

8. エリア 1.1.1.1 に所属するインターフェイスを指定します。

```
ADD OSPF INT=vlan-A AREA=1.1.1.1 ↵
```

9. エリア 2.2.2.2 に所属するインターフェイスを指定します。

```
ADD OSPF INT=vlan-F AREA=2.2.2.2 ↵
```

10. バックボーンエリア (0.0.0.0) の ABR (ID 1.1.1.1) との間に仮想リンクを張ります。AREA には通過エリアを、VIRTUALLINK には対向 ABR のルーター ID を指定します。

```
ADD OSPF INT=virt0 AREA=1.1.1.1 VIRTUALLINK=1.1.1.1 ↵
```

11. OSPF を有効にします。

```
ENABLE OSPF ↵
```

スイッチ D の設定

1. VLAN の設定を行います。

```
CREATE VLAN=F VID=60 ↵
CREATE VLAN=G VID=70 ↵
CREATE VLAN=H VID=80 ↵
ADD VLAN=F PORT=1-8 ↵
ADD VLAN=G PORT=9-16 ↵
ADD VLAN=H PORT=17-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-F IP=192.168.20.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-G IP=192.168.21.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-H IP=192.168.22.1 MASK=255.255.255.0 ↵
```

4. OSPF のルーター ID を設定します。

```
SET OSPF ROUTERID=4.4.4.4 ↵
```

5. エリア 2.2.2.2 を作成し、範囲を指定します。他のルーターと同じ設定になるよう注意してください。

```
ADD OSPF AREA=2.2.2.2 ↵
ADD OSPF RANGE=192.168.20.0 MASK=255.255.255.0 AREA=2.2.2.2 ↵
ADD OSPF RANGE=192.168.21.0 MASK=255.255.255.0 AREA=2.2.2.2 ↵
ADD OSPF RANGE=192.168.22.0 MASK=255.255.255.0 AREA=2.2.2.2 ↵
```

6. エリア 2.2.2.2 に所属するインターフェースを指定します。

```
ADD OSPF INT=vlan-F AREA=2.2.2.2 ↵
ADD OSPF INT=vlan-G AREA=2.2.2.2 ↵
ADD OSPF INT=vlan-H AREA=2.2.2.2 ↵
```

7. OSPF を有効にします。

```
ENABLE OSPF ↵
```

経路表を確認するには、SHOW IP ROUTE コマンド (243 ページ) を使います。

OSPF インターフェースの状態は SHOW OSPF INTERFACE コマンド (260 ページ) で確認します。

```
SHOW OSPF INT ↵
```

```
SHOW OSPF INT=vlan-B ↵
```

OSPF エリアの情報を確認するには、SHOW OSPF AREA コマンド (253 ページ) を使います。

```
SHOW OSPF AREA ↵
```

```
SHOW OSPF AREA=0.0.0.0 ↵
```

OSPF エリアの範囲を確認するには、SHOW OSPF RANGE コマンド (270 ページ) を使います。

```
SHOW OSPF RANGE ↵
```

トポロジデータベースの情報を確認するには SHOW OSPF LSA コマンド (264 ページ) を使います。

```
SHOW OSPF LSA ↵
```

```
SHOW OSPF LSA FULL ↵
```

OSPF の設定情報を確認するには SHOW OSPF コマンド (251 ページ) を使います。

```
SHOW OSPF ↵
```

RIP の設定を確認するには SHOW IP RIP コマンド (238 ページ) を使います。

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、外部から受信した特定の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 7:

IP ルートフィルター

IP ルートフィルターは、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 (110 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 (110 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 (247 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 ↵
```

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。VLAN orange 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=vlan-orange
DIRECTION=SEND ACTION=INCLUDE ↵
ADD IP ROUTE FILTER=2 IP=.*.*.*.* MASK=.*.*.*.* INTERFACE=vlan-orange
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 (199 ページ) を使います。エントリー番号は可変なので、必ず SHOW IP ROUTE FILTER コマンド (247 ページ) で希望するエントリーの番号を確認してから指定してください。

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

IP ルートフィルターからエントリーを削除するには DELETE IP ROUTE FILTER コマンド (129 ページ) を使います。エントリー番号は可変なので、必ず SHOW IP ROUTE FILTER コマンド (247 ページ) で希望するエントリーの番号を確認してから指定してください。削除したエントリーより後ろのエントリー (番号が大きいエントリー) は 1 つずつ番号が繰り上がります。

```
DELETE IP ROUTE FILTER=2 ↵
```

IP ルートフィルターの内容を確認するには、SHOW IP ROUTE FILTER コマンド (247 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（112 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（249 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（130 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 340 ページ)、TRACE コマンド (286 ページ)、PING コマンド (171 ページ)、FINGER コマンド (170 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 (102 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 (125 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 (190 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 (234 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 340 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/DNS リレー」をご覧ください。

ㄱ PING コマンド (171 ページ) や TRACE コマンド (286 ページ) は DNS を使用しません。

本製品が使用するプライマリー DNS サーバーは、SET IP NAMESERVER コマンド (194 ページ) で設定します。

```
SET IP NAMESERVER=192.168.10.1 ↵
```

セカンダリー DNS サーバーは、SET IP SECONDARYNAMESERVER コマンド (201 ページ) で設定します。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

せます。

```
SET IP SECONDARYNAME SERVER=192.168.20.100 ↵
```

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/インターフェース」をご覧ください。

DNS サーバーの設定は SHOW IP コマンド (215 ページ) で確認できます (Name Server、Secondary Name Server 欄をご覧ください)。

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「c8624.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 234 ページ) で設定します) 次のように TELNET コマンド (「運用・管理」の 340 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=c8624.mydomain.com ↵  
TELNET bulbul ↵
```

ARP

IP アドレスから物理アドレス (MAC 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。

プロトコル概要

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 はこれを支援するために開発された IP の重要なサポートプロトコルです。

同じ VLAN 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 (93 ページ) を使います。

```
ADD IP ARP=192.168.10.5 INT=vlan-white PORT=3
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 (122 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 (218 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。デフォルトでは、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（103 ページ）、SET IP INTERFACE コマンド（191 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=vlan-white IP=192.168.10.1 MASK=255.255.255.0 PROXYARP=OFF ↓
```

```
SET IP INT=vlan-orange PROXYARP=OFF ↓
```

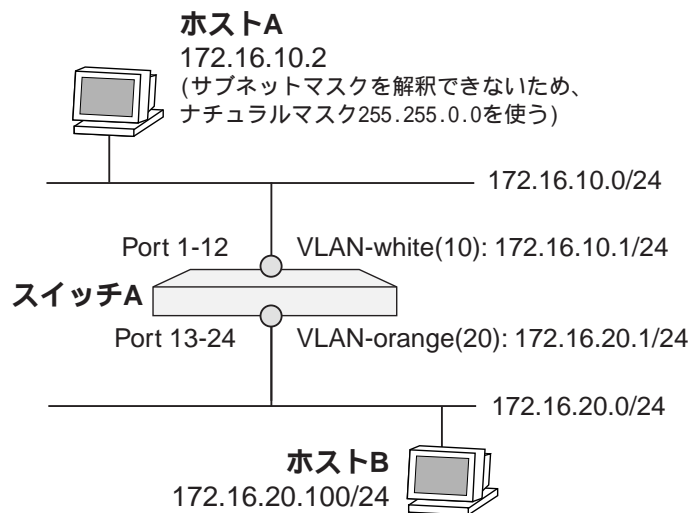
マルチホーミングを使って同一 VLAN 上に複数の論理インターフェースを作成している場合、プロキシー ARP の有効・無効はすべての論理インターフェースに共通して適用されます。

プロキシー ARP の状態は、SHOW IP INTERFACE コマンド（235 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

ここでは、例として異なる VLAN 上にあるホスト A とホスト B を考えます。ホスト A はサブネットマスクをサポートしていない旧式の IP ホスト、ホスト B はサブネットマスクをサポートしている普通の IP ホストです。

VLAN white と VLAN orange のインターフェースには、それぞれクラス B のプライベートアドレスが設定され、サブネットマスクとして 24 ビットの 255.255.255.0 が設定されています。また、ホスト A には 172.16.10.2（サブネットマスクなし）、ホスト B には 172.16.20.100（サブネットマスク 255.255.255.0）が設定されています。



ここで、Host A が Host B との IP 通信を試みるものとします。Host A はサブネットマスクをサポートしていないため、自分の所属する IP ネットワークを 172.16.0.0 であると認識しています。また、通信相手である Host B の IP アドレス 172.16.20.100 も、Host A にとっては同じ 172.16.0.0 所属と認識されるため、Host A は Host B が同一ネットワーク上にあると見なし、172.16.20.100 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 Host B は別 VLAN にあるため、通常であれば ARP Request が届くことはなく、Host A に ARP Reply が返ることもありません。そのため、このままでは Host A と Host B は IP による通信ができません。

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

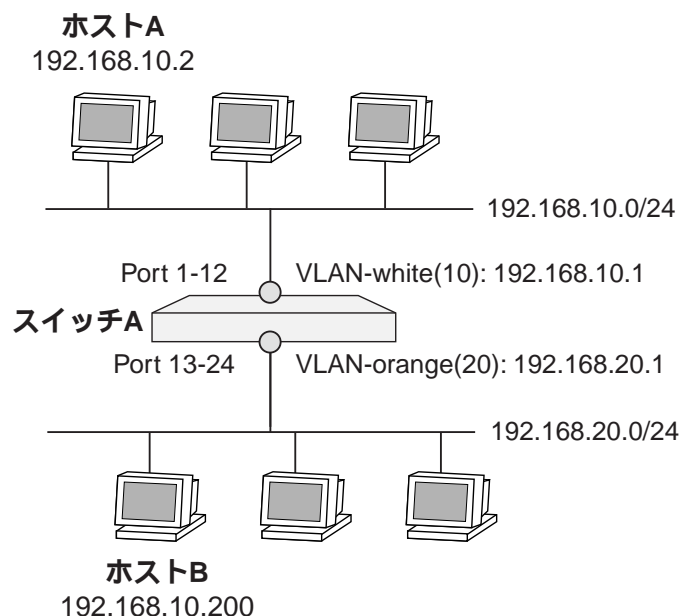
今度は戻ります。Host B はサブネットマスクをサポートしているため、Host A が別サブネットにいることを認識できます。そのため、Host A と直接 MAC アドレスで通信しようとはせずに、ルーターにパケットの転送を依頼します。

このようにして、Host A と Host B は個々の Host で特別な設定を行うことなく透過的に通信ができます。

手動で設定する例

今度はプロキシ ARP を効かせるために手動で設定を行う方法を説明します。ここでは、設定方法を示すために非常に極端な例を挙げます。現実のネットワークでこのような設定を行う直接的なメリットはありませんので、あくまでも設定を説明するためだけの例とお考えください。

ここでは、例として異なる VLAN 上にある Host A と Host B を考えます。VLAN white 上の Host A には 192.168.10.2、VLAN orange 上の Host B には 192.168.10.200 が設定されているものとします。Host B のアドレスは、192.168.20.200 の間違いではありません。たとえば、本来 VLAN white (192.168.10.0/24) 上にあった Host B が、何らかの理由で VLAN orange (192.168.20.0/24) に移動されたと考えましょう。



ここで、ホスト A がホスト B との IP 通信を試みるものとします。ホスト A は、通信相手であるホスト B の IP アドレス 192.168.10.200 が同一 IP ネットワーク上にあると見なし、192.168.10.200 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 は別 VLAN にあるため、ARP Request が届くことはなく、ホスト A に ARP Reply が返ることもありません。そのため、このままではホスト A とホスト B は IP による通信ができません。また、先ほどの例とは異なり、ルーターはホスト B が VLAN orange 側にいることを知らないため、代理応答も行われません。

このような状況では、ADD IP ROUTE コマンド (108 ページ) を使って、ホスト B への経路を明示的に登録し、ルーターにホスト B の存在場所を知らせる必要があります。ここでは次のようにします。MASK にはホスト経路であることを示すため 32 ビットマスクを指定し、INTERFACE にはホスト B が存在するインターフェース (VLAN) を指定します。PREFERENCE は経路の優先度を指定するもので、0 はもっとも優先度の高い経路であることを示します。

```
ADD IP ROUTE=192.168.10.200 MASK=255.255.255.255 INT=vlan-orange
NEXTTHOP=0.0.0.0 PREFERENCE=0 ↵
```

これにより、ホスト B に対するプロキシ ARP が有効になり、ホスト A とホスト B は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ができるようになります。

ソフトウェア IP フィルター

ソフトウェア IP フィルターは、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。

※ ソフトウェア IP フィルターとハードウェア IP フィルターを同時に使用することはできません。

ここでのフィルタリングとは、IP 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。

ソフトウェア 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 2 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

表 8:

- ※ ソフトウェア IP フィルターは CPU を用いてソフトウェア的に処理されます。そのため、通常のハードウェアルーティング使用時に比べてパフォーマンスが低下します。スループット等を重視する場合は、ハードウェア IP フィルターのご使用をお勧めします。一方、ソフトウェア IP フィルターの利点としては、ハードウェア IP フィルターよりも柔軟な設定が可能なことや、パケットのログをとれること、ポリシーフィルターによる経路選択フィルターとして使用できる点が挙げられます。
- ※ ソフトウェア IP フィルターによってフィルタリングできるのは、IP ルーティングの対象となるパケット（VLAN を越えるパケット）だけです。一方、ハードウェア IP フィルターは、同一 VLAN 内でスイッチングされるパケットに対しても有効です。

基本動作

ソフトウェア IP フィルターの基本動作について説明します。

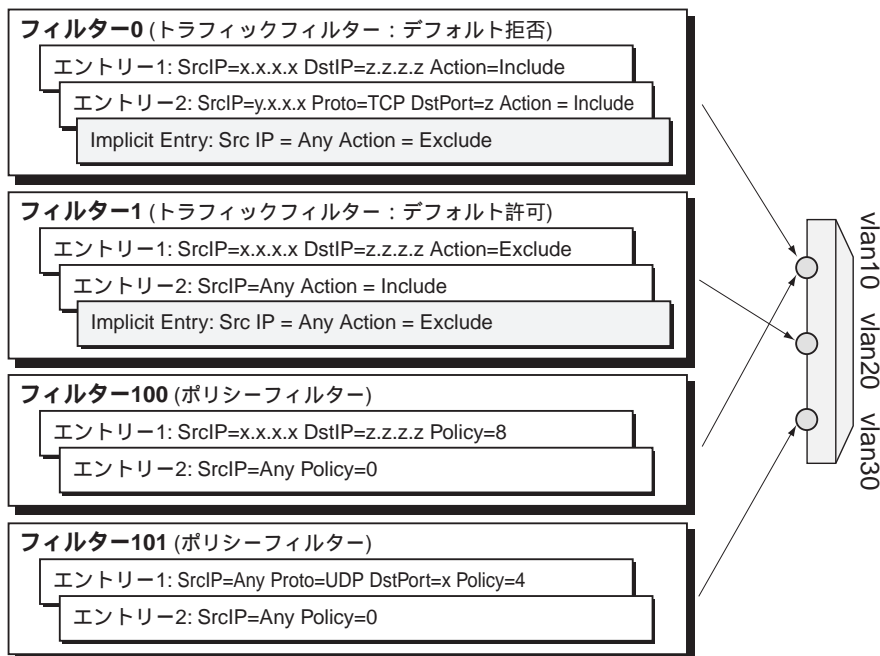
フィルターの構成

ソフトウェア 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）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では、パケットをふるいわけのための条件と、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)

各フィルターに追加できるエントリ数 (エントリ番号 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、受信 IP インターフェース (VLAN) に適用して初めて効果を発揮します。パケットのフィルタリング (ふるいわけ) はつねに受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。

IP インターフェースには、トラフィックフィルターとポリシ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

ソフトウェア 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。

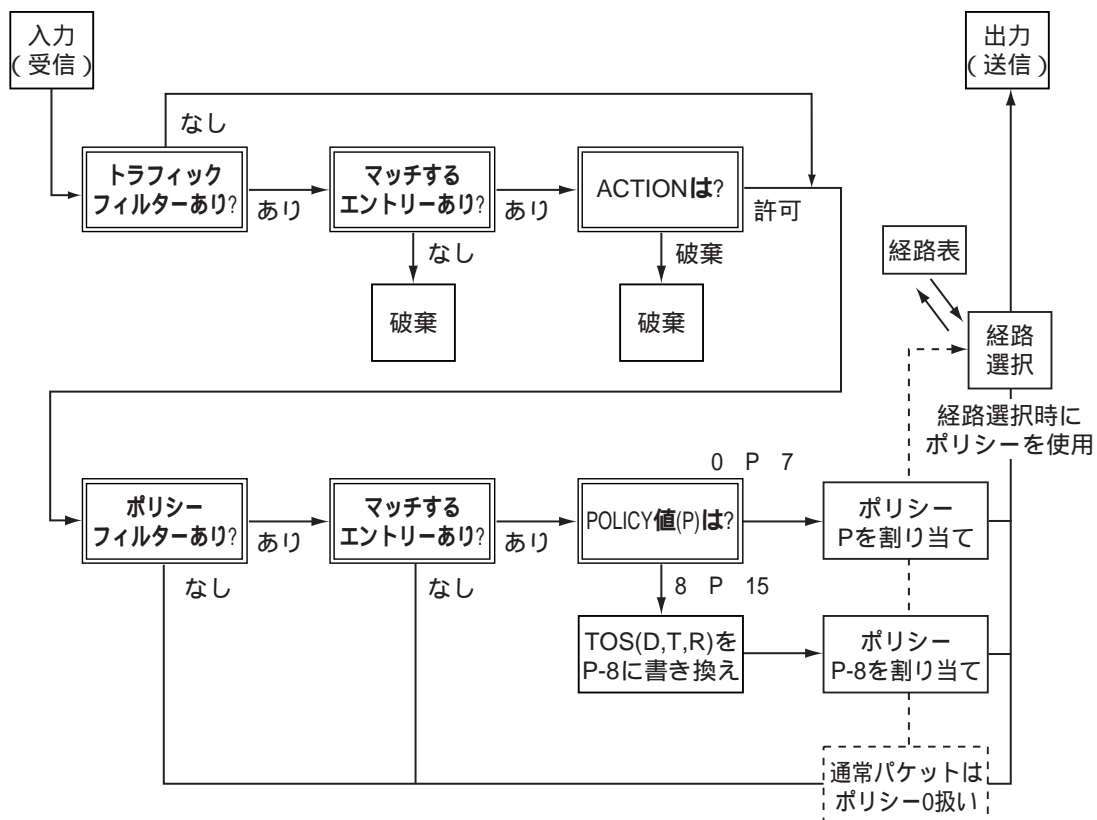
1. 受信 IP インターフェースにおいて、ヘッダー情報 (IP アドレス、ポート番号など) に基づきパケットをふるいわけ (フィルタリング)
2. 選別されたパケットに対してなんらかの処理 (破棄、経路選択ポリシー設定など) を実行する

トラフィックフィルターとポリシーフィルターは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

ソフトウェア IP フィルターの詳細な処理順序について説明します。

- ㄨ 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。



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、フィルター番号の小さい順、すなわち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。

1. 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小さい順にチェックし、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。
2. 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小さい順にチェックし、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、ソフトウェア IP フィルターの処理を完了し、通常のパケット処理に移ります。
- (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。
- ㄨ 経路エントリーの作成は ADD IP ROUTE コマンド (108 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 IP フィルターの処理を完了し、通常のパケット処理に移ります。

これでパケットに対するフィルター処理は完了です。トラフィックフィルターで破棄された場合を除き、その後通常のパケット処理に移ります。

設定手順

ソフトウェア 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) または経路選択ポリシー (ポリシーフィルター) を指定します。フィルターは ADD IP FILTER コマンド (94 ページ) / SET IP FILTER コマンド (187 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受信 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。パケットのフィルタリング（ふるいわけ）はつねに受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（103 ページ）/SET IP INTERFACE コマンド（191 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とポリシ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す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
ICMP TYPE	ICMP メッセージタイプ
ICMP CODE	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 9: ソフトウェア 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트리リストの末尾に「すべてを破棄」する暗黙のエンتری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)	<p>POLICY</p> <p>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の TOS ビットは 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。</p>
-----------------------	---

表 10: 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=vlan-orange NEXT=192.168.20.10 ↵
```

```
ADD IP ROUTE=0.0.0.0 INT=vlan-orange NEXT=192.168.20.11 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、ネクストホップ「192.168.20.11」に転送されます。

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、ネクストホップ「192.168.20.10」に転送されます。

※ ADD IP ROUTE コマンド (108 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。

ADD IP FILTER コマンド (94 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 11: 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 (94 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 (108 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。

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 (94 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 12: LOG パラメーター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受信 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。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 (191 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とポリシ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 VLAN white に割り当て。

```
SET IP INT=vlan-white FILTER=0 ↓
```

ポリシーフィルター「100」を VLAN orange に割り当て。

```
SET IP INT=vlan-orange POLICYFILTER=100 ↓
```

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=vlan-white 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 (123 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 (228 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 ↓
```

ㄨ 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 (191 ページ) の FILTER、POLICYFILTER パラメーターに NONE を指定します。

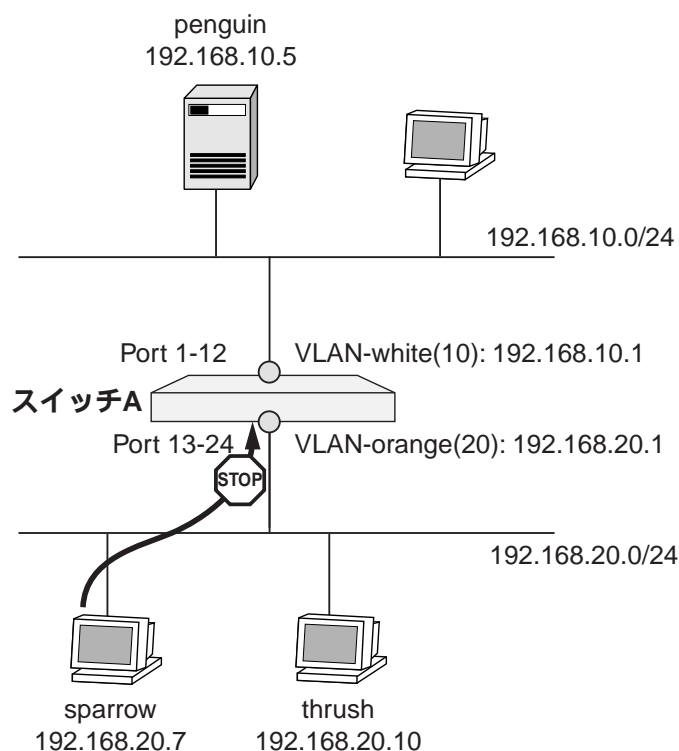
```
SET IP INT=vlan-white POLICYFILTER=NONE ↓
```

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、ヘッダー情報の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。

特定ホストのみ拒否

ここでは、トラフィックフィルターを利用して、特定ホストからのトラフィックのみを VLAN 外に出さないようにする設定例を示します（デフォルト許可）。ここでは、次のようなネットワーク構成を例に説明します。



ここでは、次のようなフィルタリング条件を考えます。

- ホスト sparrow (192.168.20.7) からの IP パケットを VLAN orange の外に出さない。すなわち、ホスト sparrow と VLAN white 内のホストが通信できないようにする（VLAN orange 内での通信（sparrow - thrush 間）は可能）。
- その他の IP トラフィックはすべて許可。

＼ 「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。ただし、トラフィックフィルターのエントリリストの末尾には、「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」のエントリを明示的に作成する必要があります。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。

スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=white PORT=1-12 ↵
ADD VLAN=orange PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. VLAN orange の IP インターフェースに適用するソフトウェア IP フィルター「0」を作成します。

- sparrow (192.168.20.7) からの IP パケットはすべて破棄します。

```
ADD IP FILTER=0 SOURCE=192.168.20.7 SMASK=255.255.255.255
ACTION=EXCLUDE ↵
```

- その他のパケットはすべて通過させます。

```
ADD IP FILTER=0 SOURCE=192.168.20.0 SMASK=255.255.255.0
ACTION=INCLUDE ↵
```

5. VLAN orange の IP インターフェースにソフトウェア IP フィルター「0」を適用します。

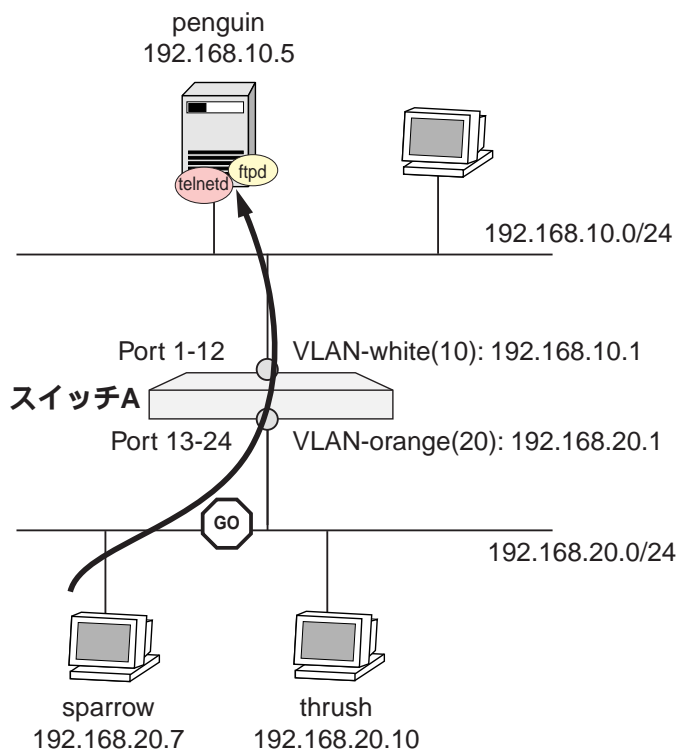
```
SET IP INT=vlan-orange FILTER=0 ↵
```

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 ↵
```

特定のホスト/サービスのみ許可

ここでは、トラフィックフィルターを利用して、特定ホストから特定サービスに対してのみ通信を許可する設定例を示します（デフォルト拒否）。ここでは、次のようなネットワーク構成を例に説明します。



ここでは、次のようなフィルタリング条件を設定します。

- 原則として VLAN white - orange 間の通信は不許可
- ただし、ホスト sparrow (192.168.20.7) から penguin (192.168.10.5) の Telnet サービスと FTP サービスにだけは通信を許可する。

＼ 「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。

スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=white PORT=1-12 ↵
ADD VLAN=orange PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. VLAN white の IP インターフェースに適用するソフトウェア IP フィルター「1」を作成します。

- penguin の Telnet サービスポートから sparrow へ送られる IP パケットを通過させます。「SESSION=ESTABLISHED」により、sparrow 側からコネクションが張られた場合にのみ通過を許可します。

```
ADD IP FILT=1 SO=192.168.10.5 SMA=255.255.255.255 DES=192.168.20.7
DMA=255.255.255.255 AC=INCLUDE ↵
SET IP FILT=1 ENTRY=1 PROTO=TCP SPORT=TELNET SESS=ESTAB ↵
```

- penguin から sparrow への FTP コントロールパケットを通過させます。「SESSION=ESTABLISHED」により、sparrow 側からコネクションが張られた場合にのみ通過を許可します。

```
ADD IP FILT=1 SO=192.168.10.5 SMA=255.255.255.255 DES=192.168.20.7
DMA=255.255.255.255 AC=INCLUDE ↵
SET IP FILT=1 ENTRY=2 PROTO=TCP SPORT=FTP SESS=ESTAB ↵
```

- penguin から sparrow への FTP データパケットを通過させます。FTP のデータコネクションは通常サーバー側から張られるので、SESSION パラメーターは「ANY」とします

```
ADD IP FILT=1 SO=192.168.10.5 SMA=255.255.255.255 DES=192.168.20.7
DMA=255.255.255.255 AC=INCLUDE ↵
SET IP FILT=1 ENTRY=3 PROTO=TCP SPORT=FTPDATA SESS=ANY ↵
```

5. VLAN white の IP インターフェースにソフトウェア IP フィルター「1」を適用します。

```
SET IP INT=vlan-white FILTER=1 ↵
```

6. VLAN orange の IP インターフェースに適用するソフトウェア IP フィルター「2」を作成します。

- sparrow から penguin の Telnet サービスポートへ送られる IP パケットを通過させます。

```
ADD IP FILT=2 SO=192.168.20.7 SMA=255.255.255.255 DES=192.168.10.5
DMA=255.255.255.255 AC=INCLUDE ↵
SET IP FILT=2 ENTRY=1 PROTO=TCP DPORT=TELNET SESS=ANY ↵
```

- sparrow から penguin への FTP コントロールパケットを通過させます。

```
ADD IP FILT=2 SO=192.168.20.7 SMA=255.255.255.255 DES=192.168.10.5
    DMA=255.255.255.255 AC=INCLUDE ↵
SET IP FILT=2 ENTRY=2 PROTO=TCP DPORT=FTP SESS=ANY ↵
```

- sparrow から penguin への FTP データパケットを通過させます。

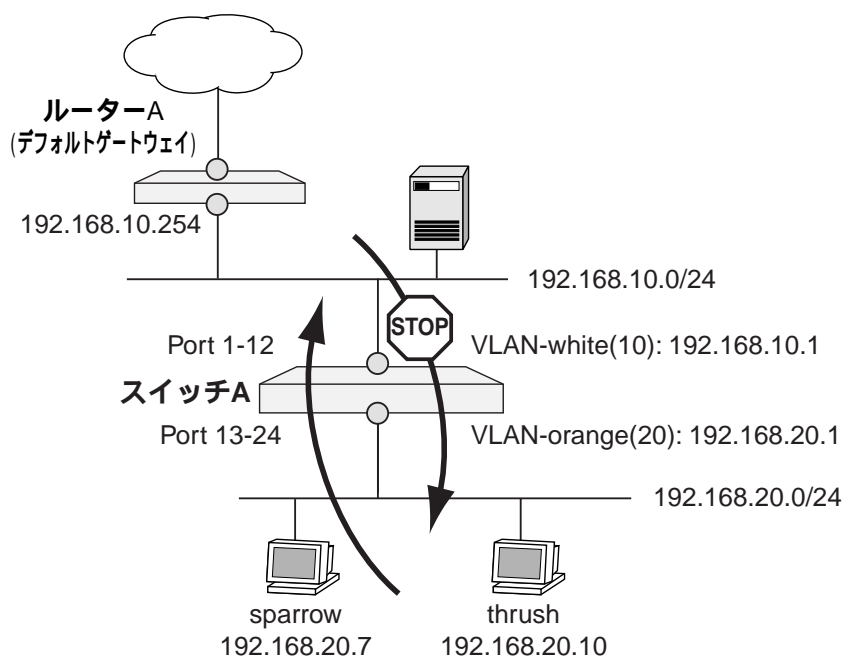
```
ADD IP FILT=2 SO=192.168.20.7 SMA=255.255.255.255 DES=192.168.10.5
    DMA=255.255.255.255 AC=INCLUDE ↵
SET IP FILT=2 ENTRY=3 PROTO=TCP DPORT=FTPDATA SESS=ANY ↵
```

7. VLAN orange の IP インターフェースにソフトウェア IP フィルター「2」を適用します。

```
SET IP INT=vlan-orange FILTER=2 ↵
```

片方向 TCP 通信

トラフィックフィルターを利用して、2 つの VLAN の片側からのみ TCP の通信を開始できるように設定します。ここでは、次のような構成のネットワークを例に説明します。



ここでは、次のようなフィルタリング条件を設定します。

- TCP は orange から white の方向へのみ通信を開始できる。white から orange への通信開始は拒否。
- UDP はすべて拒否。

- ICMP はすべて許可。

スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=white PORT=1-12 ↵
ADD VLAN=orange PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. デフォルトルートを設定します。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=vlan-white NEXT=192.168.10.254
↵
```

5. VLAN orange の IP インターフェースに適用するソフトウェア IP フィルター「1」を作成します。

- orange から外部へ向けての TCP パケットはすべて許可します。

```
ADD IP FILT=1 SO=192.168.20.0 SMA=255.255.255.0 PROTO=TCP SESS=ANY
AC=INCLUDE ↵
```

- UDP パケットはすべて破棄します。

```
ADD IP FILT=1 SO=192.168.20.0 SMA=255.255.255.0 PROTO=UDP
AC=EXCLUDE ↵
```

- ICMP はすべて許可します。

```
ADD IP FILT=1 SO=192.168.20.0 SMA=255.255.255.0 PROTO=ICMP
AC=INCLUDE ↵
```

6. VLAN orange の IP インターフェースにソフトウェア IP フィルター「1」を適用します。

```
SET IP INT=vlan-orange FILTER=1 ↵
```

7. VLAN white の IP インターフェースに適用するソフトウェア IP フィルター「2」を作成します。

- orange 宛ての TCP パケットは、orange からコネクションが張られた場合にのみ (SESSION=ESTABLISHED) 通過を許可します。

```
ADD IP FILT=2 SO=0.0.0.0 SMA=0.0.0.0 DES=192.168.20.0
DMA=255.255.255.0 PROTO=TCP SESS=ESTAB AC=INCLUDE ↵
```

- UDP パケットはすべて破棄します。

```
ADD IP FILT=2 SO=0.0.0.0 SMA=0.0.0.0 PROTO=UDP AC=EXCLUDE ↵
```

- ICMP はすべて許可します。

```
ADD IP FILT=2 SO=0.0.0.0 SMA=0.0.0.0 PROTO=ICMP AC=INCLUDE ↵
```

8. VLAN white の IP インターフェースにソフトウェア IP フィルター「2」を適用します。

```
SET IP INT=vlan-white FILTER=2 ↵
```

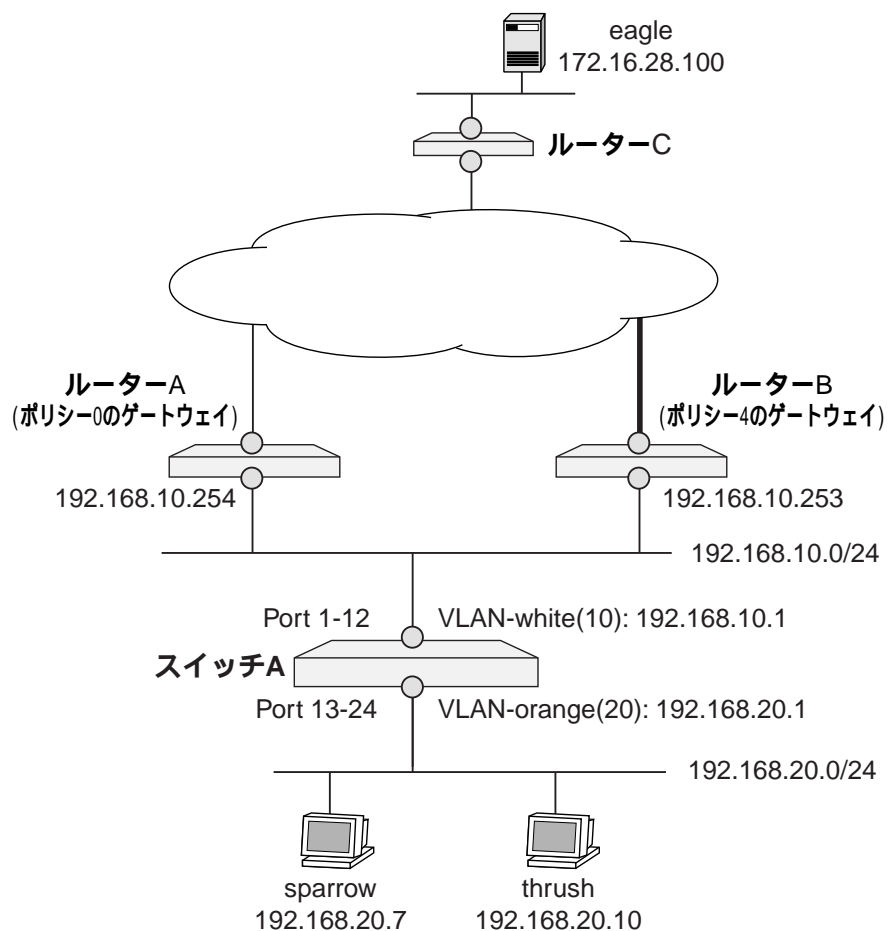
ポリシーフィルターの設定例

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。

IP アドレスによるポリシーベースルーティング

特定 IP アドレス間のトラフィックのみ、通常とは異なる経路を通すポリシーベースルーティングの設定例を紹介します。

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。



ここでは、次のような経路選択ポリシーを設定します。

- VLAN orange (192.168.20.0/24) とサーバー (172.16.28.100) 間のトラフィックは、太い回線につながっているルーター B 経由で送信します。
- その他のトラフィックはルーター A 経由で送信します。

スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=white PORT=1-12 ↵
ADD VLAN=orange PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. VLAN orange の IP インターフェースに適用するポリシーフィルター「100」を作成します。ポリシーフィルターには、フィルター番号 100～199 番を使います。

- VLAN orange とサーバー間のトラフィックにはポリシー 4 を割り当てます。

```
ADD IP FILT=100 SO=192.168.20.0 SMA=255.255.255.0
    DEST=172.16.28.100 DMA=255.255.255.255 POLICY=4 ↵
```

- その他のトラフィックにはポリシー 0 を割り当てます。

```
ADD IP FILT=100 SO=192.168.20.0 SMA=255.255.255.0 POLICY=0 ↵
```

5. VLAN orange の IP インターフェースにポリシーフィルター「100」を適用します。

```
SET IP INT=vlan-orange POLICYFILTER=100 ↵
```

6. 経路情報を設定します。

- 通常トラフィック(ポリシー 0)のためのデフォルトルートを設定します。こちらは 192.168.10.254 のルーター A を使います。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=vlan-white
    NEXT=192.168.10.254 POLICY=0 ↵
```

- VLAN orange とサーバーとの間のトラフィック(ポリシー 4)のためのデフォルトルートを設定します。こちらは 192.168.10.253 のルーター B を使います。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=vlan-white
    NEXT=192.168.10.253 POLICY=4 ↵
```

経路表を確認するには SHOW IP ROUTE コマンド (243 ページ) を使います。

```
SHOW IP ROUTE ↵
```

その他

ソフトウェア 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/コマンドプロセッサ」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 (228 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 (235 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。

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。

```
SET IP NAMESERVER=192.168.10.5 ↵
```

2. DNS リレー機能を有効にします。

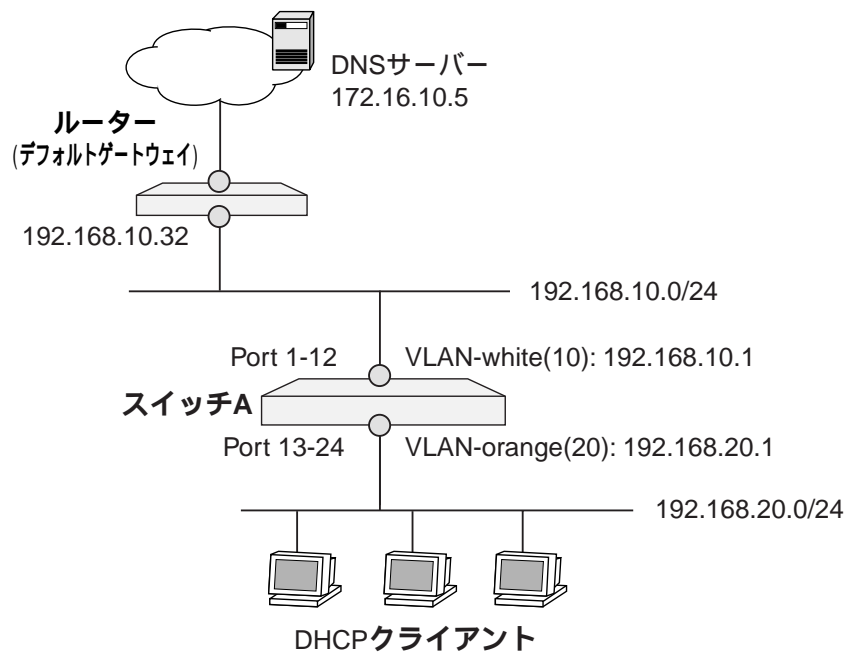
```
ENABLE IP DNSRELAY ↵
```

設定は以上です。

これで本製品宛での 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。

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、192.168.20.240 ~ 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 リクエストを実際の DNS サーバー (172.16.10.5) に中継します。



1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=white PORT=1-12 ↵
ADD VLAN=orange PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを割り当てます。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. デフォルトルートを設定します。

```
ADD IP ROUTE=0.0.0.0 INT=vlan-white NEXTHOP=192.168.10.32 ↵
```

5. 本製品が使用する DNS サーバーアドレスを設定します。

```
SET IP NAMESERVER=172.16.10.5 ↵
```

6. DNS リレー機能を有効にします。

```
ENABLE IP DNSRELAY ↵
```

7. DHCP サーバー機能を有効にします。

```
ENABLE DHCP ↵
```

8. 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、本製品のアドレスを教えるようにします。

```
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 ↵
```

9. 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。

DHCP/BOOTP リレー

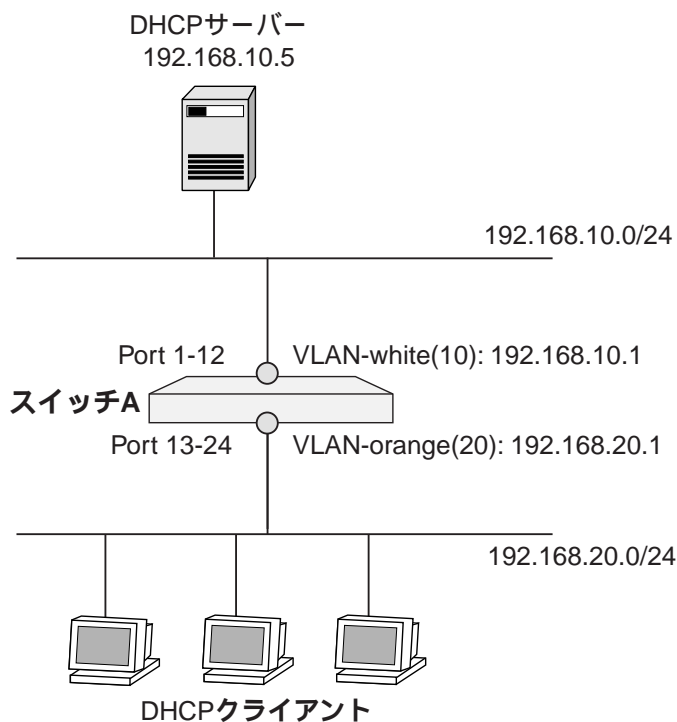
DHCP/BOOTP リレーエージェント機能は、受信した DHCP/BOOTP パケットを別セグメントの DHCP/BOOTP サーバーに転送する機能です。

一般的に、DHCP/BOOTP パケットはブロードキャストで送信されるため、クライアントとサーバーは同一のセグメント（VLAN）上にある必要があります。

このような場合でも、DHCP/BOOTP リレーエージェント機能を使用すれば、クライアントとサーバーが別の VLAN にある場合でも、DHCP/BOOTP を利用することができます。

基本設定

ここでは、次のようなネットワーク構成を例に解説します。



スイッチ A の設定

1. VLAN の設定を行います。

```

CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=white PORT=1-12 ↵
ADD VLAN=orange PORT=13-24 ↵
  
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
```

```
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. DHCP/BOOTP リレーエージェント機能を有効にします。

```
ENABLE BOOTP RELAY ↵
```

5. DHCP/BOOTP パケットの転送先を指定します。

```
ADD BOOTP RELAY=192.168.10.5 ↵
```

以上で設定は完了です。

DHCP/BOOTP リレーエージェント機能の設定内容を確認するには、SHOW BOOTP RELAY コマンド (213 ページ) を使います。

DHCP/BOOTP パケットの最大転送回数を設定するには、SET BOOTP MAXHOPS コマンド (182 ページ) を使います。デフォルトは 4 ホップです。

```
SET BOOTP MAXHOPS=3 ↵
```

UDP ブロードキャストヘルパー

UDP ブロードキャストヘルパー（UDP ヘルパー、IP ヘルパー）は、特定サービスポート宛ての UDP ブロードキャストを、あらかじめ指定した IP アドレス（ユニキャスト、ブロードキャスト）に転送する機能です。この機能は、VLAN で分割された Windows ネットワークにおいて、クライアントに特別な設定を施さずに別 VLAN のドメインコントローラにログインさせたいような場合に便利です。

基本設定

UDP ヘルパー機能の基本的な設定方法について説明します。

1. UDP ブロードキャストヘルパー機能を有効にします。

```
ENABLE IP HELPER ↵
```

2. 転送元の VLAN インターフェース、転送対象の UDP パケット（終点 UDP ポートまたは定義済みのサービス名）転送先の IP アドレスを指定する。定義済みのサービス名については、ADD IP HELPER コマンド（100 ページ）の説明をご覧ください。

```
ADD IP HELPER DESTINATION=192.168.20.100 INT=vlan-white  
PORT=NETBIOS ↵
```

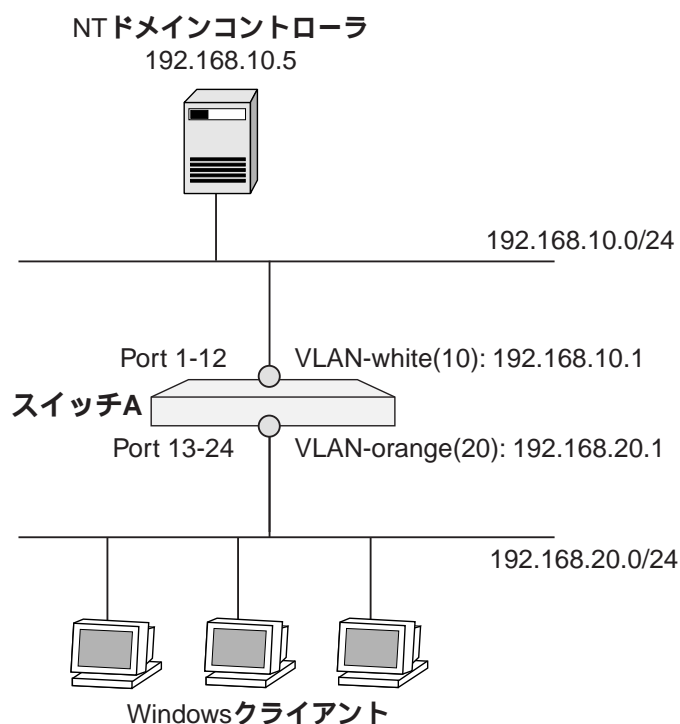
基本設定は以上です。

これで、VLAN white 側で受信した NetBIOS ブロードキャストパケットが、192.168.20.100 に転送されるようになります。

＼ 始点アドレスが 0.0.0.0 となるような UDP パケット（DHCP request など）は転送の対象となりません。

設定例

次のようなネットワーク構成を例に解説します。ここでは、VLAN orange 側の Windows クライアントが VLAN white 側のドメインコントローラにログインできるようにします。



1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=white PORT=1-12 ↵
ADD VLAN=orange PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを割り当てます。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. UDP ブロードキャストヘルパー機能を有効にします。

```
ENABLE IP HELPER ↵
```

5. VLAN orange 側で受信した NetBIOS ブroadcast (終点ポート 137-138) をドメインコントローラ 192.168.10.5 に転送するよう設定します。

```
ADD IP HELPER DESTINATION=192.168.10.5 INT=vlan-orange PORT=NetBIOS ↵
```

設定は以上です。

UDP ブroadcastキャストヘルパーの設定内容を確認するには、SHOW IP HELPER コマンド (232 ページ) を使います。

```
SHOW IP HELPER ↵
```

UDP ブroadcastキャストヘルパーの設定を解除するには、DELETE IP HELPER コマンド (124 ページ) を使います。

```
DELETE IP HELPER DESTINATION=192.168.10.5 INT=vlan-orange PORT=NetBIOS ↵
```

UDP ブroadcastキャストヘルパー機能を無効にするには、DISABLE IP HELPER コマンド (144 ページ) を使います。

```
DISABLE IP HELPER ↵
```

始点アドレスが 0.0.0.0 となるような UDP パケット (DHCP request など) は転送の対象となりません。なお、DHCP/BOOTP パケットを転送したい場合は、本製品の DHCP/BOOTP リレー機能が使えます。

セキュリティ

IP 層でのセキュリティ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（164 ページ）\ DISABLE IP SRCROUTE コマンド（148 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（215 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（158 ページ）と DISABLE IP FOFILTER コマンド（142 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（215 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。

ディレクティッ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（ディレクティッドブロードキャストフィルタリング）。ディレクティッ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。

ディレクティッ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（103 ページ）、SET IP INTERFACE コマンド（191 ページ）のDIRECTEDBROADCAST パラメータに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=vlan-white DIRECTEDBROADCAST=ON ↓
SET IP INTERFACE=vlan-white 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。

ディレクティッ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、ディレクティッ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。

ディレクティッ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（235 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。

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

DELETE TCP	136
DISABLE IP	138
DISABLE IP DEBUG	139
DISABLE IP ECHOREPLY	141
DISABLE IP FORWARDING	143
DISABLE IP REMOTEASSIGN	146
ENABLE IP	154
ENABLE IP DEBUG	155
ENABLE IP ECHOREPLY	157
ENABLE IP FORWARDING	159
ENABLE IP REMOTEASSIGN	162
FINGER	170
PING	171
PURGE IP	174
RESET IP	176
RESET IP COUNTER	177
SET PING	211
SET TRACE	212
SHOW IP	215
SHOW IP COUNTER	220
SHOW IP DEBUG	227
SHOW IP FLOW	230
SHOW IP UDP	250
SHOW PING	276
SHOW TCP	278
SHOW TRACE	282
STOP PING	284
STOP TRACE	285
TRACE	286

IP インターフェース

ADD IP INTERFACE	103
DELETE IP INTERFACE	126
DISABLE IP INTERFACE	145
ENABLE IP INTERFACE	161
RESET IP INTERFACE	178

SET DHCP EXTENDID	183
SET IP INTERFACE	191
SET IP LOCAL	193
SHOW IP INTERFACE	235
経路制御 (スタティック)	
ADD IP ROUTE	108
DELETE IP ROUTE	128
DISABLE IP ROUTE	147
ENABLE IP ROUTE	163
SET IP ROUTE	198
SHOW IP ROUTE	243
経路制御 (RIP)	
ADD IP RIP	106
DELETE IP RIP	127
SET IP RIP	195
SET IP RIPTIMER	197
SHOW IP RIP	238
SHOW IP RIP COUNTER	240
SHOW IP RIPTIMER	242
経路制御 (OSPF)	
ADD OSPF AREA	113
ADD OSPF HOST	115
ADD OSPF INTERFACE	116
ADD OSPF RANGE	118
ADD OSPF STUB	120
DELETE OSPF AREA	131
DELETE OSPF HOST	132
DELETE OSPF INTERFACE	133
DELETE OSPF RANGE	134
DELETE OSPF STUB	135
DISABLE OSPF	149
DISABLE OSPF DEBUG	150
DISABLE OSPF INTERFACE	151
DISABLE OSPF LOG	152
ENABLE OSPF	165
ENABLE OSPF DEBUG	166
ENABLE OSPF INTERFACE	167
ENABLE OSPF LOG	168
PURGE OSPF	175
RESET OSPF	179
RESET OSPF COUNTER	180

RESET OSPF INTERFACE	181
SET OSPF	202
SET OSPF AREA	204
SET OSPF HOST	206
SET OSPF INTERFACE	207
SET OSPF RANGE	209
SET OSPF STUB	210
SHOW OSPF	251
SHOW OSPF AREA	253
SHOW OSPF DEBUG	256
SHOW OSPF HOST	258
SHOW OSPF INTERFACE	260
SHOW OSPF LSA	264
SHOW OSPF NEIGHBOUR	268
SHOW OSPF RANGE	270
SHOW OSPF ROUTE	272
SHOW OSPF STUB	274
経路制御フィルター	
ADD IP ROUTE FILTER	110
ADD IP TRUSTED	112
DELETE IP ROUTE FILTER	129
DELETE IP TRUSTED	130
SET IP ROUTE FILTER	199
SHOW IP ROUTE FILTER	247
SHOW IP TRUSTED	249
名前解決	
ADD IP HOST	102
DELETE IP HOST	125
SET IP HOST	190
SET IP NAMESERVER	194
SET IP SECONDARYNAMESERVER	201
SHOW IP HOST	234
ARP	
ADD IP ARP	93
DELETE IP ARP	122
SET IP ARP	184
SET IP ARP TIMEOUT	185
SHOW IP ARP	218
ソフトウェア IP フィルター	
ADD IP FILTER	94

DELETE IP FILTER	123
SET IP FILTER	187
SHOW IP FILTER	228
DNS リレー	
DISABLE IP DNSRELAY	140
ENABLE IP DNSRELAY	156
SET IP DNSRELAY	186
DHCP/BOOTP リレー	
ADD BOOTP RELAY	92
DELETE BOOTP RELAY	121
DISABLE BOOTP RELAY	137
ENABLE BOOTP RELAY	153
PURGE BOOTP RELAY	173
SET BOOTP MAXHOPS	182
SHOW BOOTP RELAY	213
UDP ブロードキャストヘルパー	
ADD IP HELPER	100
DELETE IP HELPER	124
DISABLE IP HELPER	144
ENABLE IP HELPER	160
SHOW IP HELPER	232
セキュリティ	
DISABLE IP FOFILTER	142
DISABLE IP SRCROUTE	148
ENABLE IP FOFILTER	158
ENABLE IP SRCROUTE	164

ADD BOOTP RELAY

カテゴリー：IP / DHCP/BOOTP リレー

対象機種：8624、9606

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 (121 ページ)

DISABLE BOOTP RELAY (137 ページ)

ENABLE BOOTP RELAY (153 ページ)

PURGE BOOTP RELAY (173 ページ)

SET BOOTP MAXHOPS (182 ページ)

SHOW BOOTP RELAY (213 ページ)

ADD IP ARP

カテゴリー：IP / ARP

対象機種：8624、9606

ADD IP ARP=*ipadd* **INTERFACE=***vlan-if* **PORT=***port-number* **ETHERNET=***macadd*

ipadd: IP アドレス

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

port-number: スイッチポート番号 (1 ~)

macadd: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

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 (VLAN) インターフェース

PORT スイッチポート番号

ETHERNET 物理 (MAC) アドレス

例

VLAN「red」のポート10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 INTERFACE=vlan-red PORT=10
ETHERNET=00-00-F4-12-34-56
```

関連コマンド

DELETE IP ARP (122 ページ)

SET IP ARP (184 ページ)

SHOW IP ARP (218 ページ)

ADD IP FILTER

カテゴリー：IP / ソフトウェア IP フィルター

対象機種：8624、9606

```
ADD IP FILTER=filter-id SOURCE=ipadd {ACTION={INCLUDE|EXCLUDE}|
    POLICY=0..15} [SMASK=ipadd] [SPORT={port-name|port:[port]}]
    [DESTINATION=ipadd [DMASK=ipadd]] [DPORT={port-name|port:[port]}]
    [ICMPCODE={icmp-code-name|icmp-code-id}] [ICMPTYPE={icmp-type-name|
    icmp-type-id}] [LOG={4..1600|DUMP|HEADER|NONE}] [OPTIONS={YES|NO}]
    [PROTOCOL={protocol|ANY|ICMP|OSPF|TCP|UDP}] [SESSION={ANY|ESTABLISHED|
    START}] [SIZE=size] [ENTRY=entry-id]
```

filter-id: フィルター番号 (0~299)

ipadd: IP アドレスまたはネットマスク

port-name: サービス名

port: TCP/UDP ポート番号 (0~65535)

icmp-code-name: ICMP コード名

icmp-code-id: ICMP コード番号 (0~65535)

icmp-type-name: ICMP メッセージ名

icmp-type-id: ICMP メッセージ番号 (0~65535)

protocol: IP プロトコル番号 (0~65535)

size: データグラム長

entry-id: エントリー番号 (1~)

解説

ソフトウェア IP フィルターにエントリー（ルール）を追加する。

ソフトウェア 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）と、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）の 2 種類がある。トラフィックフィルターとポリシーフィルターは、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。

各 IP インターフェースには、トラフィックフィルターとポリシ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。作成したフィルターは、パケットの受信インターフェースに適用して初めて効果を発揮する。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。

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 は使用不可。

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。POLICY とは同時に指定できない。

POLICY ポリシーフィルター（フィルター番号 100～199）において、マッチしたパケットに割り当てる経路選択ポリシー（サービスタイプ）を指定する。経路選択ポリシーの範囲は 0～7 だが、POLICY パラメーターには 0～15 の範囲を指定することができる。0～7 を指定した場合は、指定値がそのまま経路選択ポリシー値となる。8～15 を指定した場合は、経路選択ポリシーとして「POLICY - 8」を割り当て、さらに、パケットの TOS ビット（D、T、R）を「POLICY - 8」に書き換える。詳細は別表を参照。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せられ、一致する経路が最優先で使用される。ACTION 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またはネットワークアドレスを指定する。SOURCE で指定した IP アドレスがネットワークアドレスなら適切な長さのネットマスクを、ホストアドレスなら 255.255.255.255 を指定する。また、SOURCE に 0.0.0.0（ANY）を指定した場合は 0.0.0.0 を指定する（省略可）。

SPORT 始点 TCP/UDP ポートあるいは定義済みのサービス名。本パラメーター指定時は PROTOCOL パラメーターに TCP か UDP を指定する必要がある。low:high の形式で low～high の範囲指定も可能。「low:」は low～65535 の意味、「:high」は 0～high の意味になる。デフォルトは ANY（すべてのポート）。

DESTINATION 終点 IP アドレス。デフォルトは 0.0.0.0（すべて）

DMASK 終点 IP アドレスに対応するマスク値。DESTINATION と組み合わせてホストアドレスまたはネットワークアドレスを指定する。省略時は 255.255.255.255（ホストマスク）とみなされる。

DPORT 終点 TCP/UDP ポートあるいは定義済みのサービス名。本パラメーター指定時は PROTOCOL パラメーターに TCP か UDP を指定する必要がある。low:high の形式で low～high の範囲指定も可能。「low:」は low～65535 の意味、「:high」は 0～high の意味になる。デフォルトは ANY（すべてのポート）。

ICMPCODE ICMP コード番号または定義済みのコード名。PROTOCOL=ICMP の場合のみ有効

ICMPTYPE ICMP メッセージ番号または定義済みのメッセージ名。PROTOCOL=ICMP の場合のみ有効

LOG このエントリーにマッチしたパケットの情報をログに記録するかどうか、記録する場合はどの情報を記録するかを指定する。NONE はログに記録しないことを意味する。4～1600 の数値を指定した場合は、フィルター番号、エントリー番号、IP ヘッダー情報（IP アドレス、プロトコル、ポート番号、サイズ）が「IPFIL/PASS」（INCLUDE アクションの場合）または「IPFIL/FAIL」（EXCLUDE アクションの場合）タイプのメッセージとして記録される。これに加え、TCP、UDP、ICMP の場合はデータ部分の先頭 4～1600 バイトが、その他プロトコルの場合は IP データの先頭 4～1600 バイトが、「IPFIL/DUMP」タイプのメッセージとして記録される。DUMP は LOG=32 と同じ動作となる。HEADER を指定した場合は、フィルター番号、エントリー番号、IP ヘッダー情報のみが記録される。デフォルトは NONE（記録しない）。

OPTIONS パケットが IP オプション付きかどうか。

PROTOCOL IP プロトコル番号または定義済みのプロトコル名。DPORT、SPORT を指定するときは、PROTOCOL に TCP か UDP を指定する必要がある。また、ICMPCODE、ICMPTYPE 指定時は ICMP を指定する。

SESSION TCP のセッション制御情報。ANY はすべての TCP パケット、START は接続開始パケット（SYN=1、ACK=0）、ESTABLISHED は接続済みパケット（ACK=1）を意味する。

SIZE 再構成後のデータグラムサイズ。パケット（フラグメント）ごとに $\text{length} + \text{offset} * 8 \leq \text{SIZE}$ がチェックされ、真ならマッチし、偽ならマッチしない。length と offset は、それぞれ IP ヘッダーの Length フィールドと Fragment Offset フィールドを示す。

ENTRY エントリー番号。省略時はエントリーリストの末尾に追加される。すでに n 個のエントリーが存在している場合（1～n が存在）、本パラメーターを省略すると「n+1」を指定したのと同じ動作になる。また、「n+1」より大きなエントリー番号を指定した場合も「n+1」を指定したものと見なされる。既存エントリーと同じ番号を指定した場合は、既存エントリーの前に新規エントリーが追加され、既存エントリー以降は番号が 1 つずつ後ろにずれる。

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 13: 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 14: 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	サブコードあり？	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)
TSTAMPRLPY	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 15: 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 16: 定義済みの ICMP コード名一覧 (最後の数字は「タイプ:コード」の形式)

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 VLAN red に適用する。

```
ADD IP FILTER=0 SOURCE=200.100.10.100 SMASK=255.255.255.255
```

```
ACTION=INCLUDE
```

```
SET IP INT=vlan-red 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 VLAN orange 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=vlan-orange POLICYFILTER=100
```

関連コマンド

DELETE IP FILTER (123 ページ)

SET IP FILTER (187 ページ)

SHOW IP FILTER (228 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：8624、9606

```
ADD IP HELPER DESTINATION=ipadd INTERFACE=vlan-if PORT={port|port-name}
```

ipadd: IP アドレス
vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)
port: UDP ポート番号 (1 ~ 65535)
port-name: サービス名

解説

UDP ブロードキャストパケットの転送先を設定する。32 個まで設定可能。

パラメーター

DESTINATION UDP パケットの転送先 IP アドレス。ユニキャスト、ブロードキャストともに指定可能
INTERFACE UDP ブロードキャストを監視する IP (VLAN) 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 17: 定義済みの UDP サービス名

例

VLAN orange 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 192.168.30.8 に転送する。

```
ENABLE IP HELPER  
ADD IP HELPER DESTINATION=192.168.30.8 INT=vlan-orange PORT=NETBIOS
```

VLAN orange 側で受信した NetBIOS ブroadcastキャストを VLAN white 側 (192.168.10.0/24) に再ブロードキャストする。

```
ENABLE IP HELPER
```

```
ADD IP HELPER DESTINATION=192.168.10.255 INT=vlan-orange PORT=NETBIOS
```

備考・注意事項

始点アドレスが 0.0.0.0 のパケット (例 : DHCP request) は転送されない。DHCP/BOOTP パケットを転送したい場合は、DHCP/BOOTP リレー機能 (ENABLE BOOTP RELAY コマンド、ADD BOOTP RELAY コマンドなど) を使う。

DESTINATION パラメーターでリモートのブroadcast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roadcast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roadcast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 (124 ページ)

DISABLE IP HELPER (144 ページ)

ENABLE IP HELPER (160 ページ)

SHOW IP HELPER (232 ページ)

ADD IP HOST

カテゴリー：IP / 名前解決

対象機種：8624、9606

ADD IP HOST=hostname IPADDRESS=ipadd

hostname: ホスト名

ipadd: IP アドレス

解説

IP ホストテーブルに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、FINGER 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

DELETE IP HOST (125 ページ)

FINGER (170 ページ)

PING (171 ページ)

SET IP HOST (190 ページ)

SET IP NAMESERVER (194 ページ)

SET IP SECONDARYNAMESERVER (201 ページ)

SHOW IP HOST (234 ページ)

TELNET (「運用・管理」の 340 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：8624、9606

```
ADD IP INTERFACE=vlan-if IPADDRESS={ipadd|DHCP} [MASK=ipadd]
[BROADCAST={0|1}] [DIRECTEDBROADCAST={YES|NO|ON|OFF}] [FILTER={0..99|
NONE}] [FRAGMENT={YES|NO}] [OSPFMETRIC=1..65534] [POLICYFILTER={100..199|
NONE}] [PROXYARP={ON|OFF}] [RIPMETRIC=1..16]
```

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

ipadd: IP アドレスまたはネットマスク

解説

IP インターフェースを作成する。

パラメーター

INTERFACE 下位のインターフェース (VLAN) 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、「VLAN-name-1」または「VLAN10-1」のように、インターフェース名の後にハイフンと論理インターフェース番号 (0~15) を付ける。論理インターフェース番号を省略したとき (例: vlan1) は「0」を指定したものと見なされる (例: vlan1-0 として扱われる)。

IPADDRESS インターフェースに割り当てる IP アドレス。DHCP を指定した場合は、DHCP サーバーから IP 設定情報を取得し自動設定する。DHCP で取得できる情報は、IP アドレス、ネットマスク、DNS サーバーアドレス (プライマリー、セカンダリー)、デフォルトルート、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。また、複数の VLAN インターフェースを DHCP で自動設定するときは、SET DHCP EXTENDID コマンドで「EXTENDID=ON」に設定すること。

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ッ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。

OSPFMETRIC OSPF が用いる本インターフェースのメトリック（通過コスト）。デフォルトは 1

POLICYFILTER このインターフェースで受信した IP パケットに適用するポリシーフィルターの番号を指定する。ポリシーフィルターによって設定された経路選択ポリシー（サービスタイプ）は経路表の検索に使用される。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。

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

例

VLAN orange のインターフェースに IP アドレス 192.168.100.1 を設定する。

```
ADD IP INT=vlan-orange IP=192.168.100.1 MASK=255.255.255.0
```

VLAN white のインターフェースに 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=vlan-white IP=DHCP
```

VLAN beige 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=vlan-beige-0 IP=172.16.10.1 MASK=255.255.255.0
```

```
ADD IP INT=vlan-beige-1 IP=172.16.20.1 MASK=255.255.255.0
```

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、vlan-white 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、この範囲を他のインターフェース（たとえば vlan-white-1 や vlan-red）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 (126 ページ)

DISABLE IP INTERFACE (145 ページ)

ENABLE IP INTERFACE (161 ページ)

RESET IP INTERFACE (178 ページ)

SET DHCP EXTENDID (183 ページ)
SET IP INTERFACE (191 ページ)
SHOW IP INTERFACE (235 ページ)

ADD IP RIP

カテゴリー：IP / 経路制御 (RIP)

対象機種：8624、9606

```
ADD IP RIP INTERFACE=vlan-if [IP=ipadd] [SEND={NONE|RIP1|RIP2|
COMPATIBLE}] [RECEIVE={NONE|RIP1|RIP2|BOTH}] [DEMAND={YES|NO}]
[AUTHENTICATION={NONE|PASSWORD|MD5}] [PASSWORD=password]
```

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

ipadd: IP アドレス

password: パスワード (1~16 文字)

解説

指定した IP (VLAN) 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 (VLAN) 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 VLAN 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 (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

例

VLAN orange の IP インターフェースで RIP2 の送受信 (マルチキャスト) を有効にする。

```
ADD IP RIP INT=vlan-orange SEND=RIP2 RECEIVE=RIP2
```

VLAN beige の IP インターフェースで RIP2 の受信だけを有効にする。

```
ADD IP RIP INT=vlan-beige SEND=NONE RECEIVE=RIP2
```

VLAN white 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 VLAN に対して RIP1 のブロードキャストで経路情報を送信する。

```
ADD IP RIP INT=vlan-white IP=192.168.10.5 SEND=NONE RECEIVE=RIP2
```

```
    AUTH=PASSWORD PASSWORD=secrets
```

```
ADD IP RIP INT=vlan-white SEND=RIP1 RECEIVE=NONE
```

関連コマンド

DELETE IP RIP (127 ページ)

SET IP RIP (195 ページ)

SHOW IP (215 ページ)

SHOW IP RIP (238 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：8624、9606

```
ADD IP ROUTE=ipadd INTERFACE=vlan-if NEXTHOP=ipadd [MASK=ipadd]
[METRIC=1..16] [METRIC1=1..16] [METRIC2=1..65535] [POLICY=0..7]
[PREFERENCE=0..65535]
```

ipadd: IP アドレスまたはネットマスク

vlan-if: VLAN インターフェース（VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID）

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（VLAN）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

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）

METRIC1 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。METRIC パラメーターも同じ意味。省略時は 1

METRIC2 OSPF が使用するメトリック。省略時は 1

POLICY 本経路のサービスタイプ（TOS）。省略時は 0

PREFERENCE 経路選択時の優先度。小さいほど優先度が高い。複数の経路が存在するときはもっとも優先度の高い経路が使用される。省略時の値はデフォルト経路（0.0.0.0）が 360、その他のスタティック経路が 60。なお、インターフェース経路は優先度 0、RIP 経路は優先度 100 となる

例

デフォルトルートを設定する。

```
ADD IP ROUTE=0.0.0.0 INT=vlan-white NEXTHOP=192.168.10.1
```

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=vlan-black  
NEXTTHOP=172.16.1.1
```

関連コマンド

DELETE IP ROUTE (128 ページ)

SET IP ROUTE (198 ページ)

SHOW IP ROUTE (243 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：8624、9606

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

entry-id: エントリー番号 (1~100)

ipadd: IP アドレスまたはネットマスク

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

解説

IP ルートフィルターリストにフィルターエントリーを追加する。

経路情報の送受信時には、ルートフィルターリストが番号の小さい順に検索され、最初にマッチしたフィルターエントリーが適用される。

ルートフィルターは、おもにダイナミックルーティングプロトコルによる経路情報の交換を制御するもので、内部の経路情報 (の一部) を外部に知らせないようにしたり、他のルーターから得た経路情報の一部を破棄したりする設定が可能。

パラメーター

FILTER フィルターエントリー番号。省略時はフィルターリストの末尾に追加される。すでに n 個のエントリーが存在している場合 (1~ n が存在) 本パラメーターを省略すると「 $n+1$ 」を指定したのと同じ動作になる。また、「 $n+1$ 」より大きなエントリー番号を指定した場合も「 $n+1$ 」を指定したものと見なされる。既存エントリーと同じ番号を指定した場合は、既存エントリーの前に新規エントリーが追加され、既存エントリー以降は番号が 1 つずつ後ろにずれる。

IP ネットワークアドレスを指定する。バイト単位でワイルドカード (*) の指定が可能。たとえば、「192.168.*.*」は「192.168」で始まるすべてのアドレスにマッチする。「192.168.12*.*」のような指定は無効。

MASK ネットマスクを指定。IP パラメーター同様、ワイルドカードを使用可能。

ACTION 条件にマッチした経路情報に対するアクションを指定する。INCLUDE は経路情報をメッセージに含める (送信時) あるいはルーティングテーブルに追加する (受信時)。EXCLUDE は経路情報をメッセージに含めない (送信時) あるいはルーティングテーブルに追加しない (受信時)。

DIRECTION 経路情報の送信時 (SEND) にフィルターをかけるか、受信時 (RECEIVE) にかけるか、あるいは、送信時受信時とも (BOTH) かを指定する。

INTERFACE フィルターを適用する IP (VLAN) 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 (129 ページ)

SET IP ROUTE FILTER (199 ページ)

SHOW IP ROUTE FILTER (247 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：8624、9606

ADD IP TRUSTED=ipadd

ipadd: IP アドレス

解説

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 (94 ページ)

DELETE IP FILTER (123 ページ)

DELETE IP TRUSTED (130 ページ)

SET IP FILTER (187 ページ)

SHOW IP FILTER (228 ページ)

SHOW IP TRUSTED (249 ページ)

ADD OSPF AREA

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

```
ADD OSPF AREA={BACKBONE|area-number} [AUTHENTICATION={NONE|PASSWORD}]
[STUBAREA={ON|OFF|YES|NO|TRUE|FALSE}] [STUBMETRIC=0..16777215]
[SUMMARY={SEND|NONE|OFF|NO|FALSE}]
```

area-number: OSPF エリア ID (a.b.c.d の形式)

解説

OSPF エリアを作成する。

パラメーター

AREA エリア ID。0.0.0.0 (バックボーンエリア) はキーワード「BACKBONE」で指定することもできる。

AUTHENTICATION エリア内での認証方式。NONE (無認証) と PASSWORD (簡易パスワード) がある。実際のパスワードはインターフェースごとに設定する (ADD OSPF INTERFACE コマンド)。デフォルトは NONE。

STUBAREA 対象エリアをスタブエリアにするかどうか。ON、YES、TRUE (スタブエリアにする) および OFF、NO、FALSE (スタブエリアにしない) はそれぞれ同じ意味。スタブエリアは AS 外部の経路情報を持たないエリアで、AS 外部へのトラフィックはすべてデフォルトルートに送られる。バックボーン (0.0.0.0) エリアと仮想リンクの通過エリアでは必ず OFF に設定すること。また、スタブエリア内に複数の OSPF ルーターが存在する場合は、STUBAREA パラメーターの設定を同じにすること。バックボーンエリアのデフォルトは OFF、その他のエリアのデフォルトは ON。

STUBMETRIC スタブエリア内に通知するデフォルトルート (デフォルトサマリー LSA) のメトリック。デフォルトは 50000。本パラメーターはスタブエリアのエリア境界ルーター (ABR) でのみ有効。

SUMMARY スタブエリア内にデフォルトルート以外の経路情報を通知するかどうか。SEND を指定した場合は、デフォルト以外のエリア情報もサマリー LSA でスタブエリア内に通知される。NONE を指定した場合は、デフォルトのサマリー LSA だけが ABR によってスタブエリア内に通知される。NONE、OFF、NO、FALSE は同義。デフォルトは NONE。

例

バックボーンエリアを作成する。

```
ADD OSPF AREA=0.0.0.0
```

エリア 1.1.1.1 をノーマルエリア (STUBAREA=OFF) として作成する。

```
ADD OSPF AREA=1.1.1.1 STUBAREA=OFF
```

備考・注意事項

- ・各ルーター上では、自分の所属するエリアだけを作成すればよい。
- ・仮想リンクの通過エリアを作成するときは、必ず STUBAREA=OFF を指定すること。

関連コマンド

ADD OSPF RANGE (118 ページ)

DELETE OSPF AREA (131 ページ)

DELETE OSPF RANGE (134 ページ)

SET OSPF AREA (204 ページ)

SET OSPF RANGE (209 ページ)

SHOW OSPF AREA (253 ページ)

SHOW OSPF RANGE (270 ページ)

ADD OSPF HOST

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

ADD OSPF HOST=*ipadd* [METRIC=0..65535]

ipadd: IP アドレス

解説

OSPF ルーティングテーブルにホスト経路を追加する。

ホスト経路は、ルートマスク 255.255.255.255 でエリア内に通知される経路。PPP や SLIP でルーターと一対一接続されているホストへの経路を示すために使用される。

パラメーター

HOST ホストの IP アドレス。ルーター上で設定したエリア範囲内のアドレスでなくてはならない。

METRIC メトリック。デフォルトは 1。

関連コマンド

ADD OSPF INTERFACE (116 ページ)

DELETE OSPF HOST (132 ページ)

SET OSPF HOST (206 ページ)

SHOW OSPF HOST (258 ページ)

SHOW OSPF INTERFACE (260 ページ)

ADD OSPF INTERFACE

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

```
ADD OSPF INTERFACE=vlan-if AREA={BACKBONE|area-number}
[DEADINTERVAL=2..2147483647] [HELLOINTERVAL=1..65535]
[PASSWORD=password] [PRIORITY=0..255] [RXMTINTERVAL=1..3600]
[TRANSITDELAY=1..3600] [VIRTUALLINK=area-number]
```

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または仮想インターフェース (VIRTx)

area-number: OSPF エリア ID (a.b.c.d の形式)

password: パスワード (1~8 文字。任意の印刷可能文字を使用可能。空白を含む場合はダブルクォートで囲む)

解説

OSPF インターフェースを追加する。仮想リンクの作成も本コマンドで行う。

インターフェースを追加するには、あらかじめエリアの作成とアドレスレンジの指定が必要。

パラメーター

INTERFACE IP インターフェース (VLAN) 名または仮想インターフェース名 (VIRTx) を指定する。該当インターフェースは、AREA で指定したエリアの範囲内になくはない。

AREA エリア ID。仮想インターフェースの場合は通過エリアのエリア ID を指定する。

DEADINTERVAL Hello パケットの Router Dead Interval タイマー (秒)。隣接ルーターから Hello パケットを受信できなくなったときに、隣接ルーターがダウンしたと判断するまでの時間を示す。同一ネットワーク上のすべてのルーターに同じ値を設定する必要がある。最小値は HELLOINTERVAL × 2、推奨値は HELLOINTERVAL × 4。デフォルト値は HELLOINTERVAL × 4 (秒)。

HELLOINTERVAL Hello パケットの送信間隔 (Hello Interval) (秒)。同一ネットワーク上のすべてのルーターに同じ値を設定する必要がある。デフォルトは 10 秒。

PASSWORD 認証用パスワード。エリア内での認証方法がパスワード認証の場合 (ADD OSPF AREA コマンド/SET OSPF AREA コマンドの AUTHENTICATION パラメーターに PASSWORD を指定した場合) にのみ必要。デフォルトはパスワードなし (null)。

PRIORITY ルーター優先度 (0~255)。大きいほど優先度が高く、指名ルーター (DR) に選出される可能性が高くなる。優先度が同じときはルーター ID の大きいほうが DR となる。0 は DR になる資格がないことを示す。デフォルトは 1。

RXMTINTERVAL データベース記述パケット (タイプ 2)、リンク状態要求パケット (タイプ 3)、リンク状態更新パケット (タイプ 4) の送信間隔 (秒)。隣接ルーター間のパケット往復時間よりも十分に大きな値でなくてはならない。LAN では 5 秒が標準的。デフォルトは 5 秒。

TRANSITDELAY リンク状態更新パケットの送信遅延時間 (秒)。同パケットに含まれる LSA のエイジフィールドはこの値だけ増分される。LAN では通常 1 に設定される。デフォルトは 1。

VIRTUALLINK 仮想リンクの対向に位置するバックボーンルーター（ABR）のルーター ID。仮想インターフェース追加時（INTERFACE=VIRTx）の必須パラメーター。このとき、AREA には通過エリアの ID を指定する。

例

バックボーンエリアに VLAN orange のインターフェースを追加する。

```
ADD OSPF INT=vlan-orange AREA=BACKBONE
```

ルーター 192.168.10.1 と 192.168.10.254 の間に仮想リンクを作成する。通過エリアは 1.1.1.1。通過エリア 1.1.1.1 を作成するときは STUBAREA=OFF を指定して、スタブエリアでないように設定しなくてはならない。

[ルーター 192.168.10.254 側]

```
ADD OSPF INT=virt0 AREA=1.1.1.1 VIRTUALLINK=192.168.10.1
```

[ルーター 192.168.10.1 側]

```
ADD OSPF INT=virt0 AREA=1.1.1.1 VIRTUALLINK=192.168.10.254
```

備考・注意事項

- ・仮想リンクは両エンドで設定する必要がある。
- ・仮想リンクを作成するときは、SET OSPF コマンドの ROUTERID パラメーターでルーター ID を明示的に指定しておく設定がやりやすい。

関連コマンド

ADD OSPF AREA (113 ページ)

ADD OSPF RANGE (118 ページ)

DELETE OSPF INTERFACE (133 ページ)

DISABLE OSPF INTERFACE (151 ページ)

ENABLE OSPF INTERFACE (167 ページ)

RESET OSPF INTERFACE (181 ページ)

SET OSPF AREA (204 ページ)

SET OSPF INTERFACE (207 ページ)

SET OSPF RANGE (209 ページ)

SHOW OSPF AREA (253 ページ)

SHOW OSPF INTERFACE (260 ページ)

SHOW OSPF RANGE (270 ページ)

ADD OSPF RANGE

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

```
ADD OSPF RANGE=ipadd AREA={BACKBONE|area-number} [MASK=ipadd]
[EFFECT={ADVERTISE|DONOTADVERTISE}]
```

ipadd: IP アドレスまたはネットマスク

area-number: OSPF エリア ID (a.b.c.d の形式)

解説

OSPF エリアを構成するネットワークの範囲を定義する。

基本的には直接接続されているネットワークの範囲だけを指定すればよいが、ABR ではエリア範囲を広く (短いマスクで) 指定することにより、他エリアに通知する経路情報をまとめることができる。

パラメーター

RANGE IP ネットワークアドレス

AREA エリア ID

MASK ネットマスク。RANGE パラメーターと組み合わせてエリアに所属するネットワークの範囲を指定する。省略時は RANGE で指定した IP アドレスのクラス (クラス A、B、C) に応じた標準ネットマスクが使用される

EFFECT 指定したネットワーク範囲をエリア外部に通知するかどうか。エリア境界ルーター (ABR) でのみ有効。ADVERTISE を指定した場合、該当範囲の情報を 1 つのサマリー LSA としてエリア外に通知する。DONOTADVERTISE を指定した場合は情報を通知しない。デフォルトは ADVERTISE

例

バックボーンエリアに所属するネットワークの範囲を定義する。ここでは、172.16.0.0 ~ 172.16.255.255 と 172.17.0.0 ~ 172.17.255.255 の範囲を指定している。基本的には直接接続されているネットワークの範囲だけを指定すればよいが、ABR ではエリア範囲を広く (短いマスクで) 指定することにより、他エリアに通知する経路情報をまとめることができる。

```
ADD OSPF RANGE=172.16.0.0 MASK=255.255.0.0 AREA=BACKBONE
```

```
ADD OSPF RANGE=172.17.0.0 MASK=255.255.0.0 AREA=BACKBONE
```

関連コマンド

DELETE OSPF RANGE (134 ページ)

SET OSPF RANGE (209 ページ)

SHOW OSPF RANGE (270 ページ)

ADD OSPF STUB

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

ADD OSPF STUB=*ipadd* **MASK=***ipadd* [METRIC=0..65535]

ipadd: IP アドレスまたはネットマスク

解説

OSPF ルーティングテーブルに、OSPF を使用していないネットワーク (スタブネットワーク) への経路情報を追加する。

パラメーター

STUB スタブネットワークのネットワークアドレス。ルーター上で定義されているエリアの範囲内でなくてはならない

MASK STUB に対するネットワークマスク

METRIC メトリック。デフォルトは 1

関連コマンド

ADD OSPF HOST (115 ページ)

ADD OSPF INTERFACE (116 ページ)

DELETE OSPF STUB (135 ページ)

SET OSPF STUB (210 ページ)

SHOW OSPF STUB (274 ページ)

DELETE BOOTP RELAY

カテゴリー：IP / DHCP/BOOTP リレー

対象機種：8624、9606

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 (92 ページ)

DISABLE BOOTP RELAY (137 ページ)

ENABLE BOOTP RELAY (153 ページ)

PURGE BOOTP RELAY (173 ページ)

SET BOOTP MAXHOPS (182 ページ)

SHOW BOOTP RELAY (213 ページ)

DELETE IP ARP

カテゴリー：IP / ARP

対象機種：8624、9606

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 (93 ページ)

SHOW IP ARP (218 ページ)

DELETE IP FILTER

カテゴリー：IP / ソフトウェア IP フィルター

対象機種：8624、9606

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

filter-id: フィルター番号 (0 ~ 299)

entry-id: エントリー番号 (1 ~)

解説

IP フィルターからエントリー (ルール) を削除する。

エントリー番号は可変なので、必ず SHOW IP FILTER コマンドで確認してから指定すること。エントリーを削除すると、後続のエントリー番号が 1 つずつ前にずれるので注意。

パラメーター

FILTER フィルター番号

ENTRY エントリー番号。この番号は可変なので、必ず SHOW IP FILTER コマンドで確認してから指定すること (Ent.フィールド)。ALL を指定した場合は、該当するフィルターのすべてのエントリーが削除される。

例

トラフィックフィルター「0」から 2 番のエントリーを削除する。

```
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 (94 ページ)

SET IP FILTER (187 ページ)

SHOW IP FILTER (228 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：8624、9606

```
DELETE IP HELPER DESTINATION=ipadd INTERFACE=vlan-if PORT={port|  
    port-name}
```

ipadd: IP アドレス

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

port: UDP ポート番号 (1～65535)

port-name: サービス名

解説

UDP ブロードキャストパケットの転送先登録を削除する。

パラメーター

DESTINATION UDP ブロードキャストの転送先 IP アドレス

INTERFACE UDP ブロードキャストを監視する IP (VLAN) インターフェース

PORT UDP ポート番号

関連コマンド

ADD IP HELPER (100 ページ)

DISABLE IP HELPER (144 ページ)

ENABLE IP HELPER (160 ページ)

SHOW IP HELPER (232 ページ)

DELETE IP HOST

カテゴリー：IP / 名前解決

対象機種：8624、9606

DELETE IP HOST=hostname

hostname: 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 HOST (102 ページ)

SET IP HOST (190 ページ)

SET IP NAMESERVER (194 ページ)

SET IP SECONDARYNAMESERVER (201 ページ)

SHOW IP HOST (234 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：8624、9606

DELETE IP INTERFACE=*vlan-if*

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

解説

IP インターフェースを削除する。

パラメーター

INTERFACE IP (VLAN) インターフェース名

関連コマンド

ADD IP INTERFACE (103 ページ)

DISABLE IP INTERFACE (145 ページ)

ENABLE IP INTERFACE (161 ページ)

RESET IP INTERFACE (178 ページ)

SET IP INTERFACE (191 ページ)

SHOW IP INTERFACE (235 ページ)

DELETE IP RIP

カテゴリー：IP / 経路制御 (RIP)

対象機種：8624、9606

DELETE IP RIP INTERFACE=vlan-if [IP=ipadd]

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

ipadd: IP アドレス

解説

指定した IP (VLAN) インターフェースで RIP を無効にする。

パラメーター

INTERFACE IP (VLAN) 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

VLAN white 上での RIP 送受信を停止する。

```
DELETE IP RIP INT=vlan-white
```

VLAN orange 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=vlan-orange IP=192.168.20.254
```

関連コマンド

ADD IP RIP (106 ページ)

SET IP RIP (195 ページ)

SHOW IP (215 ページ)

SHOW IP RIP (238 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：8624、9606

```
DELETE IP ROUTE=ipadd MASK=ipadd INTERFACE=vlan-if NEXTHOP=ipadd
```

ipadd: IP アドレスまたはネットマスク

vlan-if: VLAN インターフェース（VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID）

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（VLAN）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=vlan-white NEXTHOP=192.168.1.32
```

関連コマンド

ADD IP ROUTE（108 ページ）

SET IP ROUTE（198 ページ）

SHOW IP ROUTE（243 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：8624、9606

DELETE IP ROUTE FILTER=entry-id

entry-id: エントリー番号 (1~100)

解説

IP ルートフィルターリストから指定したフィルターエントリーを削除する。

フィルターエントリーの番号は可変なので、必ず SHOW IP ROUTE FILTER コマンドで確認してから指定すること。エントリーを削除すると、後続のエントリー番号が1つずつ前にずれるので注意。

パラメーター

FILTER フィルターエントリー番号。この番号は可変なので、必ず SHOW IP ROUTE FILTER コマンドで確認してから指定すること (Ent.フィールド)。

関連コマンド

ADD IP ROUTE FILTER (110 ページ)

SET IP ROUTE FILTER (199 ページ)

SHOW IP ROUTE FILTER (247 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：8624、9606

DELETE IP TRUSTED=*ipadd*

ipadd: IP アドレス

解説

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 (94 ページ)

ADD IP TRUSTED (112 ページ)

DELETE IP FILTER (123 ページ)

SET IP FILTER (187 ページ)

SHOW IP FILTER (228 ページ)

SHOW IP TRUSTED (249 ページ)

DELETE OSPF AREA

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

DELETE OSPF AREA={BACKBONE|*area-number*}

area-number: OSPF エリア ID (a.b.c.d の形式)

解説

OSPF エリアを削除する。

パラメーター

AREA エリア ID。バックボーンエリア (0.0.0.0) はキーワード「BACKBONE」で指定することもできる

関連コマンド

ADD OSPF AREA (113 ページ)

ADD OSPF RANGE (118 ページ)

DELETE OSPF RANGE (134 ページ)

SET OSPF AREA (204 ページ)

SET OSPF RANGE (209 ページ)

SHOW OSPF AREA (253 ページ)

SHOW OSPF RANGE (270 ページ)

DELETE OSPF HOST

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

DELETE OSPF HOST=*ipadd*

ipadd: IP アドレス

解説

OSPF ルーティングテーブルからホストルートを削除する。

パラメーター

HOST ホストの IP アドレス

関連コマンド

ADD OSPF HOST (115 ページ)

SET OSPF HOST (206 ページ)

SHOW OSPF HOST (258 ページ)

DELETE OSPF INTERFACE

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

DELETE OSPF INTERFACE=vlan-if

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または仮想インターフェース (VIRTx)

解説

OSPF インターフェースを削除する。

パラメーター

INTERFACE IP (VLAN) インターフェース名 (例: vlan10) または、仮想インターフェース名 (VIRTx)。

関連コマンド

ADD OSPF INTERFACE (116 ページ)

DISABLE OSPF INTERFACE (151 ページ)

ENABLE OSPF INTERFACE (167 ページ)

RESET OSPF INTERFACE (181 ページ)

SET OSPF INTERFACE (207 ページ)

SHOW OSPF INTERFACE (260 ページ)

DELETE OSPF RANGE

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

DELETE OSPF RANGE=*ipadd*

ipadd: IP アドレス

解説

OSPF エリアを構成するネットワークの範囲を削除する。

パラメーター

RANGE ネットワークアドレス

例

エリア 1.1.1.1 からネットワーク 192.168.10.0 を削除する。

DELETE OSPF RANGE=192.168.10.0

関連コマンド

ADD OSPF AREA (113 ページ)

ADD OSPF RANGE (118 ページ)

SET OSPF RANGE (209 ページ)

SHOW OSPF RANGE (270 ページ)

DELETE OSPF STUB

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

DELETE OSPF STUB=*ipadd* MASK=*ipadd*

ipadd: IP アドレスまたはネットマスク

解説

OSPF ルーティングテーブルから、OSPF を使用していないネットワーク (スタブネットワーク) への経路を削除する。

パラメーター

STUB スタブネットワークのネットワークアドレス

MASK STUB に対するネットマスク

関連コマンド

ADD OSPF STUB (120 ページ)

DELETE OSPF HOST (132 ページ)

DELETE OSPF INTERFACE (133 ページ)

SET OSPF STUB (210 ページ)

SHOW OSPF STUB (274 ページ)

DELETE TCP

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

DELETE TCP=*tcb*

tcb: TCP コネクション番号

解説

スイッチ自身と任意の 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 (278 ページ)

DISABLE BOOTP RELAY

カテゴリー：IP / DHCP/BOOTP リレー

対象機種：8624、9606

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 (92 ページ)

DELETE BOOTP RELAY (121 ページ)

ENABLE BOOTP RELAY (153 ページ)

PURGE BOOTP RELAY (173 ページ)

SET BOOTP MAXHOPS (182 ページ)

SHOW BOOTP RELAY (213 ページ)

DISABLE IP

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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 (143 ページ)

DISABLE IP SRCROUTE (148 ページ)

ENABLE IP (154 ページ)

ENABLE IP FORWARDING (159 ページ)

ENABLE IP SRCROUTE (164 ページ)

SHOW IP (215 ページ)

DISABLE IP DEBUG

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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 of 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 (155 ページ)

SHOW IP (215 ページ)

SHOW IP DEBUG (227 ページ)

DISABLE IP DNSRELAY

カテゴリー：IP / DNS リレー

対象機種：8624、9606

DISABLE IP DNSRELAY

解説

DNS リレー機能を無効にする。デフォルトは無効。

関連コマンド

ENABLE IP DNSRELAY (156 ページ)

SET IP DNSRELAY (186 ページ)

SHOW IP (215 ページ)

DISABLE IP ECHOREPLY

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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 (157 ページ)

DISABLE IP FOFILTER

カテゴリー：IP / セキュリティー

対象機種：8624、9606

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（94 ページ）

DELETE IP FILTER（123 ページ）

ENABLE IP FOFILTER（158 ページ）

SET IP FILTER（187 ページ）

SHOW IP FILTER（228 ページ）

DISABLE IP FORWARDING

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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（138 ページ）

DISABLE IP SRCROUTE（148 ページ）

ENABLE IP（154 ページ）

ENABLE IP FORWARDING（159 ページ）

ENABLE IP SRCROUTE（164 ページ）

SHOW IP（215 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：8624、9606

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 (100 ページ)

DELETE IP HELPER (124 ページ)

ENABLE IP HELPER (160 ページ)

SHOW IP HELPER (232 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：8624、9606

DISABLE IP INTERFACE=*vlan-if*

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

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 (VLAN) インターフェース

関連コマンド

ADD IP INTERFACE (103 ページ)

DELETE IP INTERFACE (126 ページ)

ENABLE IP INTERFACE (161 ページ)

RESET IP INTERFACE (178 ページ)

SET IP INTERFACE (191 ページ)

SHOW IP INTERFACE (235 ページ)

DISABLE IP REMOTEASSIGN

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

DISABLE IP REMOTEASSIGN

解説

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 (162 ページ)

SHOW IP (215 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：8624、9606

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（163 ページ）

SHOW IP ROUTE（243 ページ）

DISABLE IP SRCROUTE

カテゴリー：IP / セキュリティー

対象機種：8624、9606

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（138 ページ）

ENABLE IP（154 ページ）

ENABLE IP FORWARDING（159 ページ）

ENABLE IP SRCROUTE（164 ページ）

SHOW IP（215 ページ）

DISABLE OSPF

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

DISABLE OSPF

解説

OSPF モジュールを無効にする。デフォルトは無効。

関連コマンド

ENABLE OSPF (165 ページ)

SHOW OSPF (251 ページ)

DISABLE OSPF DEBUG

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

DISABLE OSPF DEBUG

解説

OSPF モジュールのデバッグ機能を無効にする。

関連コマンド

DISABLE OSPF LOG (152 ページ)

ENABLE OSPF DEBUG (166 ページ)

ENABLE OSPF LOG (168 ページ)

SHOW OSPF (251 ページ)

DISABLE OSPF INTERFACE

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

DISABLE OSPF INTERFACE=*vlan-if*

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または仮想インターフェース (VIRTx)

解説

OSPF インターフェースを一時的に無効にする。

パラメーター

INTERFACE IP インターフェース (VLAN) 名、または仮想インターフェース名 (VIRTx)。

関連コマンド

ADD OSPF INTERFACE (116 ページ)

DELETE OSPF INTERFACE (133 ページ)

ENABLE OSPF INTERFACE (167 ページ)

RESET OSPF INTERFACE (181 ページ)

SET OSPF INTERFACE (207 ページ)

SHOW OSPF INTERFACE (260 ページ)

DISABLE OSPF LOG

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

DISABLE OSPF LOG

解説

OSPF イベントのログ記録を無効にする。デフォルトは無効。

関連コマンド

ENABLE OSPF LOG (168 ページ)

SHOW OSPF (251 ページ)

ENABLE BOOTP RELAY

カテゴリー：IP / DHCP/BOOTP リレー

対象機種：8624、9606

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 (92 ページ)

DELETE BOOTP RELAY (121 ページ)

DISABLE BOOTP RELAY (137 ページ)

PURGE BOOTP RELAY (173 ページ)

SET BOOTP MAXHOPS (182 ページ)

SHOW BOOTP RELAY (213 ページ)

ENABLE IP

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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 (138 ページ)

DISABLE IP FORWARDING (143 ページ)

DISABLE IP SRCROUTE (148 ページ)

ENABLE IP FORWARDING (159 ページ)

ENABLE IP SRCROUTE (164 ページ)

SHOW IP (215 ページ)

ENABLE IP DEBUG

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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

<I/C/B=vlan10/0/0, l=41, ttl=63, p=6, addr=192.168.10.1>192.168.40.1
>I/C/T/R/Id=vlan10/0/fw/??/55378, l=41, ttl=63, p=6, addr=192.168.10.1>192.168.40.1
<I/C/B=vlan20/14/0, l=40, ttl=64, p=6, addr=192.168.40.1>192.168.10.1
>I/C/T/R/Id=vlan20/14/fw/??/60319, l=40, ttl=64, p=6, addr=192.168.40.1>192.168.10.1
```

備考・注意事項

DEBUG=PACKET を指定すると、端末画面に大量の情報が表示されるようになるので注意すること。

関連コマンド

DISABLE IP DEBUG (139 ページ)

SHOW IP (215 ページ)

SHOW IP DEBUG (227 ページ)

ENABLE IP DNSRELAY

カテゴリー：IP / DNS リレー

対象機種：8624、9606

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 (SET IP NAMESERVER コマンド、SET IP SECONDARYNAMESERVER コマンドで設定)。

関連コマンド

DISABLE IP DNSRELAY (140 ページ)

SET IP DNSRELAY (186 ページ)

SHOW IP (215 ページ)

ENABLE IP ECHOREPLY

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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（141 ページ）

ENABLE IP FOFILTER

カテゴリー：IP / セキュリティー

対象機種：8624、9606

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（94 ページ）

DELETE IP FILTER（123 ページ）

DISABLE IP FOFILTER（142 ページ）

SET IP FILTER（187 ページ）

SHOW IP FILTER（228 ページ）

ENABLE IP FORWARDING

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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（138 ページ）

DISABLE IP FORWARDING（143 ページ）

DISABLE IP SRCROUTE（148 ページ）

ENABLE IP（154 ページ）

ENABLE IP SRCROUTE（164 ページ）

SHOW IP（215 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：8624、9606

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。

備考・注意事項

本機能では、始点アドレスが 0.0.0.0 のパケット（例：DHCP request）は転送されない。DHCP/BOOTP パケットを転送したい場合は、DHCP/BOOTP リレー機能（ENABLE BOOTP RELAY コマンド、ADD BOOTP RELAY コマンドなど）を使う。

関連コマンド

ADD IP HELPER（100 ページ）

DELETE IP HELPER（124 ページ）

DISABLE IP HELPER（144 ページ）

SHOW IP HELPER（232 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：8624、9606

ENABLE IP INTERFACE=*vlan-if*

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

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 (VLAN) インターフェース名

関連コマンド

ADD IP INTERFACE (103 ページ)

DELETE IP INTERFACE (126 ページ)

DISABLE IP INTERFACE (145 ページ)

RESET IP INTERFACE (178 ページ)

SET IP INTERFACE (191 ページ)

SHOW IP INTERFACE (235 ページ)

ENABLE IP REMOTEASSIGN

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

ENABLE IP REMOTEASSIGN

解説

DHCP による IP アドレスの動的設定機能を有効にする。

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（146 ページ）

SHOW IP（215 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：8624、9606

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 (147 ページ)

SHOW IP ROUTE (243 ページ)

ENABLE IP SRCROUTE

カテゴリー：IP / セキュリティー

対象機種：8624、9606

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（138 ページ）

DISABLE IP SRCROUTE（148 ページ）

ENABLE IP（154 ページ）

ENABLE IP FORWARDING（159 ページ）

SHOW IP（215 ページ）

ENABLE OSPF

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

ENABLE OSPF

解説

OSPF モジュールを有効にする。デフォルトは無効。

関連コマンド

DISABLE OSPF (149 ページ)

SHOW OSPF (251 ページ)

ENABLE OSPF DEBUG

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

ENABLE OSPF DEBUG

解説

OSPF モジュールのデバッグ機能を有効にする。

関連コマンド

DISABLE OSPF DEBUG (150 ページ)

DISABLE OSPF LOG (152 ページ)

ENABLE OSPF LOG (168 ページ)

SHOW OSPF (251 ページ)

ENABLE OSPF INTERFACE

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

ENABLE OSPF INTERFACE=vlan-if

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または仮想インターフェース (VIRTx)

解説

無効状態の OSPF インターフェースを有効にする。

パラメーター

INTERFACE IP インターフェース (VLAN) 名、または仮想インターフェース名 (VIRTx)。

関連コマンド

ADD OSPF INTERFACE (116 ページ)

DELETE OSPF INTERFACE (133 ページ)

DISABLE OSPF INTERFACE (151 ページ)

RESET OSPF INTERFACE (181 ページ)

SET OSPF INTERFACE (207 ページ)

SHOW OSPF INTERFACE (260 ページ)

ENABLE OSPF LOG

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

ENABLE OSPF LOG

解説

OSPF イベントのログ記録を有効にする。デフォルトは無効。

OSPF イベントはログレベル 2 で (DETAIL) で記録される。各メッセージの先頭には、「OSPF-」に続けてイベント種別を示す下記コードが付加される。

T1	インターフェースの状態が変化
T2	隣接ルーターの状態が変化
T3	指名ルーター (DR) の変更
T4	新規 LSA の生成
T5	新規 LSA の受信
T6	ルーティングテーブル変更
C1	ヘッダーエラーにより OSPF パケットを破棄
C2	Hello パケットを破棄
C3	隣接ルーターの状態が不正なためその他のパケットを破棄
C4	データベース記述 (DD) パケット再送
E1	受信 LSA のチェックサムエラー
E2	データベース LSA のチェックサムエラー
R1	同一 LSA が複数存在
R2	LSA のエイジ (Link State Age) 不一致
R3	より新しい LSA を受信
R4	未知の LSA に対する Ack を受信
R5	古い LSA を受信
N1	LSA 更新タイマーが満了
N2	LSA が MaxAge に達した
N3	MaxAge に達した LSA をフラッシュ

表 18: イベント種別コード

備考・注意事項

本コマンドを実行しても、デフォルトのログフィルター設定では、SHOW LOG コマンドで OSPF のログが表示されない。これは、OSPF イベントのログレベルが 2 であるため。オンメモリーのログ (TEMPORARY) には、デフォルトでレベル 3 以上のイベントしか記録されない。

関連コマンド

DISABLE OSPF LOG (152 ページ)

SHOW OSPF (251 ページ)

FINGER

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

```
FINGER [username]@{hostname|ipadd}[@{hostname|ipadd}]... [DETAIL={HIGH|LOW}]
```

username: ユーザー名 (1~20 文字)

hostname: ホスト名

ipadd: IP アドレス

解説

finger サーバー (RFC1288) にログインユーザーの情報を問い合わせる。

パラメーター

DETAIL サーバーに要求する情報の詳細さを指定する。ただし、応答はサーバーの実装による。

入力・出力・画面例

```
Manager > finger zeit@afrika
Login: zeit                               Name: Zeit JOGERING
Directory: /home/zeit                     Shell: /usr/local/bin/tcsh
On since Wed May 30 17:30 (JST) on tty0 (messages off) from yes
No Mail.
Mail forwarded to:
<zeijoger@foobar.com>
Plan:
1: Finish 8624 reference
2: Finish AR reference
3: Play
```

例

finger サーバー 192.168.10.1 にユーザー pon の情報を問い合わせる。

```
FINGER pon@192.168.10.1
```

PING

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

```
PING [[IPADDRESS=ipadd] [DELAY=seconds] [LENGTH=0..1500] [NUMBER={count|
CONTINUOUS}]] [PATTERN=hexnum] [SIPADDRESS=ipadd] [SCREENOUTPUT={YES|NO}]
[TIMEOUT=0..65535] [TOS=0..255]
```

ipadd: IP アドレス

seconds: 時間 (0 ~ 4294967295 秒)

count: 個数 (1 ~ 4294967295)

hexnum: バイナリースtring (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 TOS オクテットの値を指定する。

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
```

PING

```
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 ホスト 192.168.10.23 に対する PING

```
PING 192.168.10.23
```

関連コマンド

ADD IP HOST (102 ページ)

SET PING (211 ページ)

SHOW PING (276 ページ)

STOP PING (284 ページ)

PURGE BOOTP RELAY

カテゴリー：IP / DHCP/BOOTP リレー

対象機種：8624、9606

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 (92 ページ)

DELETE BOOTP RELAY (121 ページ)

DISABLE BOOTP RELAY (137 ページ)

ENABLE BOOTP RELAY (153 ページ)

SET BOOTP MAXHOPS (182 ページ)

SHOW BOOTP RELAY (213 ページ)

PURGE IP

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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 (176 ページ)

PURGE OSPF

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

PURGE OSPF

解説

OSPF の設定情報をすべて削除し、グローバルな設定パラメーターをデフォルトに戻す。OSPF モジュールは無効状態になる。

関連コマンド

DISABLE OSPF (149 ページ)

ENABLE OSPF (165 ページ)

RESET OSPF (179 ページ)

SHOW OSPF (251 ページ)

RESET IP

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

RESET IP

解説

IP モジュールをリセットする。

備考・注意事項

通常使う必要はない。

関連コマンド

PURGE IP (174 ページ)

RESET IP COUNTER (177 ページ)

RESET IP INTERFACE (178 ページ)

RESET IP COUNTER

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

RESET IP COUNTER={ALL|GENERAL|ICMP|INTERFACE|ROUTE|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 (176 ページ)

RESET IP INTERFACE (178 ページ)

SHOW IP COUNTER (220 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：8624、9606

RESET IP INTERFACE=vlan-if

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

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 (VLAN) インターフェース

関連コマンド

ADD IP INTERFACE (103 ページ)

DELETE IP INTERFACE (126 ページ)

DISABLE IP INTERFACE (145 ページ)

ENABLE IP INTERFACE (161 ページ)

RESET IP (176 ページ)

RESET IP COUNTER (177 ページ)

SET IP INTERFACE (191 ページ)

SHOW IP INTERFACE (235 ページ)

RESET OSPF

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

RESET OSPF

解説

OSPF モジュールをリセットし、各種データを再初期化する。

本コマンドでは OSPF の統計カウンタはリセットされない (RESET OSPF COUNTER コマンドでリセットする)。

関連コマンド

DISABLE OSPF (149 ページ)

ENABLE OSPF (165 ページ)

PURGE OSPF (175 ページ)

RESET OSPF COUNTER (180 ページ)

RESET OSPF INTERFACE (181 ページ)

SHOW OSPF (251 ページ)

RESET OSPF COUNTER

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

RESET OSPF COUNTER

解説

OSPF の統計カウンターをリセットする。

関連コマンド

PURGE OSPF (175 ページ)

RESET OSPF (179 ページ)

RESET OSPF INTERFACE (181 ページ)

SHOW OSPF (251 ページ)

RESET OSPF INTERFACE

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

RESET OSPF INTERFACE=*vlan-if*

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または仮想インターフェース (VIRTx)

解説

OSPF インターフェースをリセットする。

インターフェースをいったんクローズして配下ネットワークの経路情報をすべて破棄した後、インターフェースを再オープンし経路情報を再学習する。

パラメーター

INTERFACE IP インターフェース (VLAN) 名、または仮想インターフェース名 (VIRTx)

関連コマンド

ADD OSPF INTERFACE (116 ページ)

DELETE OSPF INTERFACE (133 ページ)

DISABLE OSPF INTERFACE (151 ページ)

ENABLE OSPF INTERFACE (167 ページ)

SET OSPF INTERFACE (207 ページ)

SHOW OSPF INTERFACE (260 ページ)

SET BOOTP MAXHOPS

カテゴリー：IP / DHCP/BOOTP リレー

対象機種：8624、9606

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 (92 ページ)

DELETE BOOTP RELAY (121 ページ)

DISABLE BOOTP RELAY (137 ページ)

ENABLE BOOTP RELAY (153 ページ)

PURGE BOOTP RELAY (173 ページ)

SHOW BOOTP RELAY (213 ページ)

SET DHCP EXTENDID

カテゴリー：IP / IP インターフェース

対象機種：8624、9606

SET DHCP EXTENDID={ON|OFF}

解説

DHCP クライアントとしての動作時に用いる Client ID の形式を設定する。

本製品のデフォルト状態 (EXTENDID=OFF) では、DHCP Discover や Request メッセージの Client ID として、スイッチ本体の MAC アドレス (SHOW SWITCH コマンドで確認可能) を使用する。

複数の VLAN インターフェースを DHCP クライアントとして動作させる場合であっても Client ID は同じものが使われるため、複数インターフェースが同じ DHCP サーバーを利用する場合は、サーバーが各インターフェースを同一クライアントと見なしてしまい、同じ IP アドレスが割り当てられてしまう。

複数の VLAN インターフェースが同一の DHCP サーバーを利用する場合は、本コマンドで EXTENDID=ON に設定し、各インターフェースが異なる Client ID を送信するようにすること。

パラメーター

EXTENDID DHCP メッセージの Client ID として、標準形式 (スイッチ本体の MAC アドレス。すべての VLAN インターフェースで同じ ID) を使うか、拡張形式 (VLAN インターフェースごとに異なる ID) を使うかを指定する。OFF なら標準形式、ON なら拡張形式を使う。デフォルトは OFF。

備考・注意事項

本コマンド入力後は、設定をファイルに保存してスイッチを再起動する必要がある。

関連コマンド

ADD IP INTERFACE (103 ページ)

SET IP INTERFACE (191 ページ)

SHOW DHCP (「DHCP サーバー」の 30 ページ)

SHOW IP INTERFACE (235 ページ)

SET IP ARP

カテゴリー：IP / ARP

対象機種：8624、9606

```
SET IP ARP=ipadd INTERFACE=vlan-if PORT=port-number ETHERNET=macadd
```

ipadd: IP アドレス

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

port-number: スイッチポート番号 (1 ~)

macadd: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

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 (VLAN) インターフェース

PORT スイッチポート番号

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=vlan-orange PORT=8  
ETHERNET=00-00-F4-FE-DC-BA
```

関連コマンド

ADD IP ARP (93 ページ)

DELETE IP ARP (122 ページ)

SHOW IP ARP (218 ページ)

SET IP ARP TIMEOUT

カテゴリー：IP / ARP

対象機種：8624、9606

SET IP ARP TIMEOUT=1..1023

解説

ARP タイムアウトの決定に用いる乗数を変更する。

パラメーター

TIMEOUT ARP タイムアウト（可変）の範囲を決定する乗数（正の整数）。ARP キャッシュのタイムアウトは、 $(256 * \text{TIMEOUT}) \sim (512 * \text{TIMEOUT})$ 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（93 ページ）

DELETE IP ARP（122 ページ）

SET IP ARP（184 ページ）

SHOW IP（215 ページ）

SHOW IP ARP（218 ページ）

SET IP DNSRELAY

カテゴリー：IP / DNS リレー

対象機種：8624、9606

SET IP DNSRELAY INTERFACE={*vlan-if*|NONE}

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

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。

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 (VLAN) インターフェース名

関連コマンド

DISABLE IP DNSRELAY (140 ページ)

ENABLE IP DNSRELAY (156 ページ)

SET IP NAMESERVER (194 ページ)

SET IP FILTER

カテゴリー：IP / ソフトウェア IP フィルター

対象機種：8624、9606

```
SET IP FILTER=filter-id ENTRY=entry-id {ACTION={INCLUDE|EXCLUDE}|
POLICY=0..15} [SOURCE=ipadd] [SMASK=ipadd] [SPORT={port-name|
[port]:[port]}] [DESTINATION=ipadd [DMASK=ipadd]] [DPORT={port-name|
[port]:[port]}] [ICMPCODE={icmp-code-name|icmp-code-id}]
[ICMPTYPE={icmp-type-name|icmp-type-id}] [LOG={4..1600|DUMP|HEADER|
NONE}] [OPTIONS={YES|NO}] [PROTOCOL={protocol|ANY|ICMP|OSPF|TCP|UDP}]
[SESSION={ANY|ESTABLISHED|START}] [SIZE=size]
```

filter-id: フィルター番号 (0~299)

entry-id: エントリー番号 (1~)

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 アドレスまたはネットマスク

port-name: サービス名

port: TCP/UDP ポート番号 (0~65535)

protocol: IP プロトコル番号 (0~65535)

size: データグラム長

解説

IP フィルターエントリー (ルール) の設定を変更する。

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 は使用不可。

ENTRY エントリー番号。この番号は可変なので、必ず SHOW IP FILTER コマンドで確認してから指定すること (Ent.フィールド)。

ACTION トラフィックフィルター (フィルター番号 0~99) 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。POLICY とは同時に指定できない。

POLICY ポリシーフィルター (フィルター番号 100~199) において、マッチしたパケットに割り当てる経路選択ポリシー (サービスタイプ) を指定する。経路選択ポリシーの範囲は 0~7 だが、POLICY パラメーターには 0~15 の範囲を指定することができる。0~7 を指定した場合は、指定値がそのまま経路選択ポリシー値となる。8~15 を指定した場合は、経路選択ポリシーとして「POLICY - 8」を割り当て、さらに、パケットの TOS ビット (D、T、R) を「POLICY - 8」に書き換える。詳細は ADD IP FILTER コマンドの表を参照。経路表を検索するときは、本フィルターによって割り当てられた経

路選択ポリシー値と経路エントリーのサービスタイプがつきあわされ、一致する経路が最優先で使用される。ACTION 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。必須パラメーター

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またはネットワークアドレスを指定する。SOURCE で指定した IP アドレスがネットワークアドレスなら適切な長さのネットマスクを、ホストアドレスなら 255.255.255.255 を指定する。また、SOURCE に 0.0.0.0 (ANY) を指定した場合は 0.0.0.0 を指定する (省略可)。

SPORT 始点 TCP/UDP ポートあるいは定義済みのサービス名。本パラメーター指定時は PROTOCOL パラメーターに TCP か UDP を指定する必要がある。low:high の形式で low ~ high の範囲指定も可能。「low:」は low ~ 65535 の意味、「:high」は 0 ~ high の意味になる。デフォルトは ANY (すべてのポート)。

DESTINATION 終点 IP アドレス。デフォルトは 0.0.0.0 (すべて)

DMASK 終点 IP アドレスに対応するマスク値。DESTINATION と組み合わせてホストアドレスまたはネットワークアドレスを指定する。省略時は 255.255.255.255 (ホストマスク) とみなされる。

DPORT 終点 TCP/UDP ポートあるいは定義済みのサービス名。本パラメーター指定時は PROTOCOL パラメーターに TCP か UDP を指定する必要がある。low:high の形式で low ~ high の範囲指定も可能。「low:」は low ~ 65535 の意味、「:high」は 0 ~ high の意味になる。デフォルトは ANY (すべてのポート)。

ICMPCODE ICMP コード番号または定義済みのコード名。PROTOCOL=ICMP の場合のみ有効

ICMPTYPE ICMP メッセージ番号または定義済みのメッセージ名。PROTOCOL=ICMP の場合のみ有効

LOG このエントリーにマッチしたパケットの情報をログに記録するかどうか、記録する場合はどの情報を記録するかを指定する。NONE はログに記録しないことを意味する。4 ~ 1600 の数値を指定した場合は、フィルター番号、エントリー番号、IP ヘッダー情報 (IP アドレス、プロトコル、ポート番号、サイズ) が「IPFIL/PASS」(INCLUDE アクションの場合) または「IPFIL/FAIL」(EXCLUDE アクションの場合) タイプのメッセージとして記録される。これに加え、TCP、UDP、ICMP の場合はデータ部分の先頭 4 ~ 1600 バイトが、その他プロトコルの場合は IP データの先頭 4 ~ 1600 バイトが、「IPFIL/DUMP」タイプのメッセージとして記録される。DUMP は LOG=32 と同じ動作となる。HEADER を指定した場合は、フィルター番号、エントリー番号、IP ヘッダー情報のみが記録される。デフォルトは NONE (記録しない)。

OPTIONS パケットが IP オプション付きかどうか。

PROTOCOL IP プロトコル番号または定義済みのプロトコル名。DPORT、SPORT を指定するときは、PROTOCOL に TCP か UDP を指定する必要がある。また、ICMPCODE、ICMPTYPE 指定時は ICMP を指定する。

SESSION TCP のセッション制御情報。ANY はすべての TCP パケット、START は接続開始パケット (SYN=1、ACK=0)、ESTABLISHED は接続済みパケット (ACK=1) を意味する。

SIZE 再構成後のデータグラムサイズ。パケット (フラグメント) ごとに $\text{length} + \text{offset} * 8 \leq \text{SIZE}$ 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 (94 ページ)

DELETE IP FILTER (123 ページ)

SET IP FILTER (187 ページ)

SET IP HOST

カテゴリー：IP / 名前解決

対象機種：8624、9606

```
SET IP HOST=hostname IPADDRESS=ipadd
```

hostname: ホスト名

ipadd: IP アドレス

解説

IP ホストテーブルエントリーの 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 HOST (102 ページ)

DELETE IP HOST (125 ページ)

SET IP NAMESERVER (194 ページ)

SET IP SECONDARYNAMESERVER (201 ページ)

SHOW IP HOST (234 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：8624、9606

```
SET IP INTERFACE=vlan-if [ IPADDRESS=ipadd|DHCP ] [ MASK=ipadd ]
    [ BROADCAST={0|1} ] [ DIRECTEDBROADCAST={YES|NO|ON|OFF} ] [ FILTER={0..99|
    NONE} ] [ FRAGMENT={YES|NO} ] [ OSPFMETRIC=1..65534 ] [ POLICYFILTER={100..199|
    NONE} ] [ PROXYARP={ON|OFF} ] [ RIPMETRIC=1..16 ]
```

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

ipadd: IP アドレスまたはネットマスク

解説

IP インターフェースの設定を変更する。

ソフトウェア 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 (VLAN) 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、「VLAN-name-1」または「VLAN10-1」のように、インターフェース名の後にハイフンと論理インターフェース番号 (0~15) を付ける。論理インターフェース番号を省略したとき (例: vlan1) は「0」を指定したものと見なされる (例: vlan1-0 として扱われる)。

IPADDRESS インターフェースに割り当てる IP アドレス。DHCP を指定した場合は、DHCP サーバーから IP 設定情報を取得し自動設定する。DHCP で取得できる情報は、IP アドレス、ネットマスク、DNS サーバーアドレス (プライマリー、セカンダリー)、デフォルトルート、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。また、複数の VLAN インターフェースを DHCP で自動設定するときは、SET DHCP EXTENDID コマンドで「EXTENDID=ON」に設定すること。

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ッ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。

OSPFMETRIC OSPF が用いる本インターフェースのメトリック（通過コスト）。デフォルトは 1

POLICYFILTER このインターフェースで受信した IP パケットに適用するポリシーフィルターの番号を指定する。ポリシーフィルターによって設定された経路選択ポリシー（サービスタイプ）は経路表の検索に使用される。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。

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

例

VLAN white の IP アドレスを変更する。

```
SET IP INT=vlan-white IP=10.1.1.1 MASK=255.255.255.0
```

VLAN orange に IP トラフィックフィルター「0」を適用する。

```
SET IP INT=vlan-orange FILTER=0
```

関連コマンド

ADD IP INTERFACE (103 ページ)

DELETE IP INTERFACE (126 ページ)

DISABLE IP INTERFACE (145 ページ)

ENABLE IP INTERFACE (161 ページ)

RESET IP INTERFACE (178 ページ)

SET DHCP EXTENDID (183 ページ)

SHOW IP INTERFACE (235 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：8624、9606

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

filter-id: フィルター番号 (0 ~ 299)

ipadd: IP アドレス

解説

ローカル IP インターフェースの設定を変更する。

ローカル IP インターフェースは、IP モジュール自体をあらわす仮想的なインターフェースで、スイッチ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、スイッチ自身が送信する RIP、OSPF、PING、NTP パケット等の始点アドレスとして使用される可能性がある。スイッチが送信する 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。

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

関連コマンド

ADD IP INTERFACE (103 ページ)

DELETE IP INTERFACE (126 ページ)

SET IP INTERFACE (191 ページ)

SHOW IP INTERFACE (235 ページ)

SET IP NAMESERVER

カテゴリー：IP / 名前解決

対象機種：8624、9606

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。

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

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 HOST (102 ページ)

DELETE IP HOST (125 ページ)

SET IP DNSRELAY (186 ページ)

SET IP HOST (190 ページ)

SET IP SECONDARYNAMESERVER (201 ページ)

SHOW IP (215 ページ)

SHOW IP HOST (234 ページ)

SET IP RIP

カテゴリー：IP / 経路制御 (RIP)

対象機種：8624、9606

```
SET IP RIP INTERFACE=vlan-if [IP=ipadd] [SEND={NONE|RIP1|RIP2|
COMPATIBLE}] [RECEIVE={NONE|RIP1|RIP2|BOTH}] [DEMAND={YES|NO}]
[AUTHENTICATION={NONE|PASSWORD|MD5}] [PASSWORD=password]
```

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

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 (VLAN) 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 VLAN 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 (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

例

VLAN orange 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=vlan-orange SEND=RIP1 RECEIVE=RIP1
```

関連コマンド

ADD IP RIP (106 ページ)

DELETE IP RIP (127 ページ)

SET IP RIPTIMER (197 ページ)

SHOW IP RIP (238 ページ)

SET IP RIPTIMER

カテゴリー：IP / 経路制御 (RIP)

対象機種：8624、9606

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

seconds: 時間 (秒)

解説

RIP のタイマー設定を変更する。

パラメーター

FLUSH 最後の更新パケット受信から経路情報が削除されるまでの期間 (秒)。FLUSH >= INVALID + HOLDDOWN になるようにする。デフォルトは 300 秒。

HOLDDOWN ホールドダウンタイム。ルートタイムアウトにより無効 (メトリック 16) となった経路エントリーを無効状態のまま保持する期間 (秒)。この期間中は、該当経路の更新情報を受け取ってもエントリーを更新せず、無効状態のまま止めおく。デフォルトは 120 秒。

INVALID ルートタイムアウト。経路が更新されなくなってから、該当する経路情報を無効とみなす (メトリックを 16 にする) までの期間 (秒)。デフォルトは 180 秒。

UPDATE アップデートタイマー。RIP 更新パケットの送信間隔 (秒)。デフォルトは 30 秒。

関連コマンド

SET IP RIP (195 ページ)

SHOW IP RIP (238 ページ)

SHOW IP RIPTIMER (242 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：8624、9606

```
SET IP ROUTE=ipadd INTERFACE=vlan-if MASK=ipadd NEXTHOP=ipadd
[METRIC=1..16] [METRIC1=1..16] [METRIC2=1..65535] [POLICY=0..7]
[PREFERENCE=0..65535]
```

vlan-if: VLAN インターフェース（VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID）

ipadd: IP アドレスまたはネットマスク

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（VLAN）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。ダイレクト経路の場合は 0.0.0.0 を指定する

METRIC1 RIP が使用するメトリック。通常は 2～16 の範囲で指定する。1 はダイレクトルートにしか使
うべきでない。METRIC パラメーターも同じ意味。省略時は 1

METRIC2 OSPF が使用するメトリック。省略時は 1

POLICY 本経路のサービスタイプ（TOS）。省略時は 0

PREFERENCE 経路選択時の優先度。小さいほど優先度が高い。複数の経路が存在するときはもっとも優先度の高い経路が使用される。省略時の値はデフォルト経路（0.0.0.0）が 360、その他のスタティック経路が 60。なお、インターフェース経路は優先度 0、RIP 経路は優先度 100 となる

関連コマンド

ADD IP ROUTE（108 ページ）

DELETE IP ROUTE（128 ページ）

SHOW IP ROUTE（243 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：8624、9606

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

entry-id: エントリー番号 (1~100)

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

ipadd: IP アドレスまたはネットマスク

解説

IP ルートフィルターエントリーの設定内容を変更する。

パラメーター

FILTER フィルターエントリー番号。この番号は可変なので、必ず SHOW IP ROUTE FILTER コマンドで確認してから指定すること (Ent.フィールド)。

IP ネットワークアドレスを指定する。バイト単位でワイルドカード (*) の指定が可能。たとえば、「192.168.*.*」は「192.168」で始まるすべてのアドレスにマッチする。「192.168.12.*.*」のような指定は無効。

MASK ネットマスクを指定。IP パラメーター同様、ワイルドカードを使用可能。

ACTION 条件にマッチした経路情報に対するアクションを指定する。INCLUDE は経路情報をメッセージに含める (送信時) あるいはルーティングテーブルに追加する (受信時)。EXCLUDE は経路情報をメッセージに含めない (送信時) あるいはルーティングテーブルに追加しない (受信時)。

DIRECTION 経路情報の送信時 (SEND) にフィルターをかけるか、受信時 (RECEIVE) にかけるか、あるいは、送信時受信時とも (BOTH) かを指定する。

INTERFACE フィルターを適用する IP (VLAN) 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 \(110 ページ \)](#)

[DELETE IP ROUTE FILTER \(129 ページ \)](#)

[SHOW IP ROUTE FILTER \(247 ページ \)](#)

SET IP SECONDARYNAMESEVER

カテゴリー：IP / 名前解決

対象機種：8624、9606

SET IP SECONDARYNAMESEVER=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。

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

SECONDARYNAMESEVER 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。

関連コマンド

ADD IP HOST (102 ページ)

DELETE IP HOST (125 ページ)

SET IP HOST (190 ページ)

SET IP NAMESERVER (194 ページ)

SHOW IP (215 ページ)

SHOW IP HOST (234 ページ)

SET OSPF

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

```
SET OSPF [ASEXTERNAL={ON|OFF}] [DEFROUTE={ON|OFF|TRUE|FALSE|YES|NO}
[TYPE={1|2}] [METRIC=0..16777215]] [RIP={OFF|EXPORT|IMPORT|BOTH}]
[ROUTERID=ipadd]
```

ipadd: IP アドレス

解説

OSPF のグローバル設定パラメーターを変更する。

パラメーター

ASEXTERNAL AS 境界ルーター (ASBR) として動作させるかどうか。ON を指定した場合は、AS 外部の経路情報 (他の経路制御プロトコルの情報とスタティック経路) を AS 内に通知する。デフォルトは OFF

DEFROUTE デフォルトルート (0.0.0.0) の AS 外部 LSA を AS 内に通知するかどうか。ON のときはデフォルトルートが通知される。OFF のときはすべての AS 外部経路が AS 内に通知される。本パラメーターは ASBR として設定したルーターでのみ使用する。スタティックルートを設定している場合は、自動的に AS 内に通知されるため本オプションをオンにする必要はない。デフォルトは OFF

TYPE デフォルト AS 外部 LSA のタイプ (1 または 2)。DEFROUTE=ON の場合のみ有効。デフォルトは 1

METRIC デフォルト AS 外部 LSA のメトリック。DEFROUTE=ON の場合のみ有効。デフォルトは 1

RIP RIP と OSPF の間でどのように情報をやりとりするかを指定する。EXPORT を指定した場合、OSPF の経路情報が RIP のルーティングテーブルに取り込まれる。IMPORT を指定した場合、RIP の経路情報が OSPF のルーティングテーブルに取り込まれる。BOTH を指定した場合は、OSPF と RIP で互いに情報を交換しあう。OFF を指定した場合は、RIP と OSPF のやりとりは行われない。デフォルトは OFF

ROUTERID ルーター ID。IP アドレスと同じ形式で指定する。指定しなかった場合は、インターフェースに設定された IP アドレスの中でもっとも大きなものがルーター ID として使われる。

例

ルーター ID として「1.1.1.1」を設定する

```
SET OSPF ROUTERID=1.1.1.1
```

備考・注意事項

- ・ 仮想リンクを使用するときは、リンクの両エンドのルーターにルーター ID を設定しておく設定がやりやすい。
- ・ RIP および ASEXTERNAL パラメーターを変更すると、一時的にネットワークが不安定になるので注意。

関連コマンド

DISABLE OSPF DEBUG (150 ページ)

DISABLE OSPF LOG (152 ページ)

ENABLE OSPF DEBUG (166 ページ)

SHOW OSPF (251 ページ)

SET OSPF AREA

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

```
SET OSPF AREA={BACKBONE|area-number} [AUTHENTICATION={NONE|PASSWORD}]
[STUBAREA={ON|OFF|YES|NO|TRUE|FALSE}] [STUBMETRIC=0..16777215]
[SUMMARY={SEND|NONE|OFF|NO|FALSE}]
```

area-number: OSPF エリア ID (a.b.c.d の形式)

解説

OSPF エリアの設定パラメーターを変更する。

パラメーター

AREA エリア ID。0.0.0.0 (バックボーンエリア) はキーワード「BACKBONE」で指定することもできる。

AUTHENTICATION エリア内での認証方式。NONE (無認証) と PASSWORD (簡易パスワード) がある。実際のパスワードはインターフェースごとに設定する (ADD OSPF INTERFACE コマンド)。デフォルトは NONE。

STUBAREA 対象エリアをスタブエリアにするかどうか。ON、YES、TRUE (スタブエリアにする) および OFF、NO、FALSE (スタブエリアにしない) はそれぞれ同じ意味。スタブエリアは AS 外部の経路情報を持たないエリアで、AS 外部へのトラフィックはすべてデフォルトルートに送られる。バックボーン (0.0.0.0) エリアと仮想リンクの通過エリアでは必ず OFF に設定すること。また、スタブエリア内に複数の OSPF ルーターが存在する場合は、STUBAREA パラメーターの設定を同じにすること。バックボーンエリアのデフォルトは OFF、その他のエリアのデフォルトは ON。

STUBMETRIC スタブエリア内に通知するデフォルトルート (デフォルトサマリー LSA) のメトリック。デフォルトは 50000。本パラメーターはスタブエリアのエリア境界ルーター (ABR) でのみ有効。

SUMMARY スタブエリア内にデフォルトルート以外の経路情報を通知するかどうか。SEND を指定した場合は、デフォルト以外のエリア情報もサマリー LSA でスタブエリア内に通知される。NONE を指定した場合は、デフォルトのサマリー LSA だけが ABR によってスタブエリア内に通知される。NONE、OFF、NO、FALSE は同義。デフォルトは NONE。

関連コマンド

ADD OSPF AREA (113 ページ)

ADD OSPF RANGE (118 ページ)

DELETE OSPF AREA (131 ページ)

DELETE OSPF RANGE (134 ページ)

SET OSPF RANGE (209 ページ)

SHOW OSPF AREA (253 ページ)

SHOW OSPF RANGE (270 ページ)

SET OSPF HOST

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

```
SET OSPF HOST=ipadd METRIC=0..65535
```

ipadd: IP アドレス

解説

OSPF ルーティングテーブル内のホスト経路のメトリックを変更する。

パラメーター

HOST ホストの IP アドレス。ルーター上で設定したエリア範囲内のアドレスでなくてはならない

METRIC メトリック。デフォルトは 1

関連コマンド

ADD OSPF HOST (115 ページ)

DELETE OSPF HOST (132 ページ)

SHOW OSPF HOST (258 ページ)

SET OSPF INTERFACE

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

```
SET OSPF INTERFACE=vlan-if [AREA={BACKBONE|area-number}]
[DEADINTERVAL=2..2147483647] [HELLOINTERVAL=1..65535]
[PASSWORD=password] [PRIORITY=0..255] [RXMTINTERVAL=1..3600]
[TRANSITDELAY=1..3600] [VIRTUALLINK=area-number]
```

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または仮想インターフェース (VIRTx)

area-number: OSPF エリア ID (a.b.c.d の形式)

password: パスワード (1~8 文字。任意の印刷可能文字を使用可能。空白を含む場合はダブルクォートで囲む)

解説

OSPF インターフェースのパラメーターを変更する。

パラメーター

INTERFACE IP インターフェース (VLAN) 名または仮想インターフェース名 (VIRTx)

AREA エリア ID。仮想インターフェースの場合は通過エリアのエリア ID を指定する。

DEADINTERVAL Hello パケットの Router Dead Interval タイマー (秒)。隣接ルーターから Hello パケットを受信できなくなったときに、隣接ルーターがダウンしたと判断するまでの時間を示す。同一ネットワーク上のすべてのルーターに同じ値を設定する必要がある。最小値は HELLOINTERVAL × 2、推奨値は HELLOINTERVAL × 4。デフォルト値は HELLOINTERVAL × 4 (秒)。

HELLOINTERVAL Hello パケットの送信間隔 (Hello Interval) (秒)。同一ネットワーク上のすべてのルーターに同じ値を設定する必要がある。デフォルトは 10 秒。

PASSWORD 認証用パスワード。エリア内での認証方法がパスワード認証の場合 (ADD OSPF AREA コマンド/SET OSPF AREA コマンドの AUTHENTICATION パラメーターに PASSWORD を指定した場合) にのみ必要。デフォルトはパスワードなし (null)。

PRIORITY ルーター優先度 (0~255)。大きいほど優先度が高く、指名ルーター (DR) に選出される可能性が高くなる。優先度が同じときはルーター ID の大きいほうが DR となる。0 は DR になる資格がないことを示す。デフォルトは 1。

RXMTINTERVAL データベース記述パケット (タイプ 2)、リンク状態要求パケット (タイプ 3)、リンク状態更新パケット (タイプ 4) の送信間隔 (秒)。隣接ルーター間のパケット往復時間よりも十分に大きな値でなくてはならない。LAN では 5 秒が標準的。デフォルトは 5 秒。

TRANSITDELAY リンク状態更新パケットの送信遅延時間 (秒)。同パケットに含まれる LSA のエイジフィールドはこの値だけ増分される。LAN では通常 1 に設定される。デフォルトは 1

VIRTUALLINK 仮想リンクの対向に位置するバックボーンルーター (ABR) の ID。仮想インターフェース追加時 (INTERFACE=VIRTx) の必須パラメーター。このとき、AREA には通過エリアの ID を

指定する。

関連コマンド

ADD OSPF INTERFACE (116 ページ)

ADD OSPF RANGE (118 ページ)

DELETE OSPF INTERFACE (133 ページ)

DISABLE OSPF INTERFACE (151 ページ)

ENABLE OSPF INTERFACE (167 ページ)

RESET OSPF INTERFACE (181 ページ)

SET OSPF AREA (204 ページ)

SET OSPF AREA (204 ページ)

SET OSPF RANGE (209 ページ)

SHOW OSPF AREA (253 ページ)

SHOW OSPF INTERFACE (260 ページ)

SHOW OSPF RANGE (270 ページ)

SET OSPF RANGE

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

```
SET OSPF RANGE=ipadd [AREA={BACKBONE|area-number}] [MASK=ipadd]
[EFFECT={ADVERTISE|DONOTADVERTISE}]
```

ipadd: IP アドレスまたはネットマスク

area-number: OSPF エリア ID (a.b.c.d の形式)

解説

OSPF エリアを構成するネットワーク範囲の設定を変更する。

パラメーター

RANGE ネットワークアドレス

AREA エリア ID

MASK ネットマスク。RANGE パラメーターと組み合わせてネットワークの範囲を指定する。省略時は RANGE で指定した IP アドレスのクラス (クラス A、B、C) に応じた標準ネットマスクが使用される

EFFECT 指定したアドレス範囲をエリア外部に通知するかどうか。エリア境界ルーター (ABR) でのみ有効。ADVERTISE を指定した場合、該当範囲の情報を 1 つのサマリー LSA としてエリア外に通知する。DONOTADVERTISE を指定した場合は情報を通知しない。デフォルトは ADVERTISE

関連コマンド

ADD OSPF RANGE (118 ページ)

DELETE OSPF RANGE (134 ページ)

SHOW OSPF RANGE (270 ページ)

SET OSPF STUB

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

```
SET OSPF STUB=ipadd MASK=ipadd METRIC=0..65535
```

ipadd: IP アドレスまたはネットマスク

解説

OSPF を使用していないネットワーク (スタブネットワーク) の設定を変更する。

パラメーター

STUB スタブネットワークのネットワークアドレス。ルーター上で定義されているエリアの範囲内でなくてはならない

MASK STUB に対するネットマスク

METRIC メトリック。デフォルトは 1

関連コマンド

ADD OSPF STUB (120 ページ)

DELETE OSPF STUB (135 ページ)

SET OSPF HOST (206 ページ)

SET OSPF INTERFACE (207 ページ)

SHOW OSPF STUB (274 ページ)

SET PING

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

```
SET PING [[ IPADDRESS=ipadd] [DELAY=seconds] [LENGTH=0..1500]
          [NUMBER={count|CONTINUOUS}] [PATTERN=hexnum] [SIPADDRESS=ipadd]
          [SCREENOUTPUT={YES|NO}] [TIMEOUT=0..65535] [TOS=0..255]
```

ipadd: IP アドレス

seconds: 時間 (0 ~ 4294967295 秒)

count: 個数 (1 ~ 4294967295)

hexnum: バイナリースtring (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 TOS オクテットの値を指定する。

関連コマンド

ADD IP HOST (102 ページ)

PING (171 ページ)

SHOW PING (276 ページ)

STOP PING (284 ページ)

SET TRACE

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

```
SET TRACE [[ IPADDRESS=ipadd] [MAXTTL=1..255] [MINTTL=1..255]
  [NUMBER=1..100] [PORT=port] [SCREENOUTPUT={YES|NO}] [SOURCE=ipadd]
  [TIMEOUT=0..65535] [TOS=0..255]
```

ipadd: IP アドレス

port: UDP ポート番号 (0~65535)

解説

TRACE コマンドのデフォルトパラメーターを設定する。

TRACE コマンド実行時に指定されなかったパラメーターについては、本コマンドで設定したデフォルト値が使用される。

パラメーター

IPADDRESS 宛先 IP アドレス

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。

関連コマンド

ADD IP HOST (102 ページ)

SHOW TRACE (282 ページ)

STOP TRACE (285 ページ)

TRACE (286 ページ)

SHOW BOOTP RELAY

カテゴリー：IP / DHCP/BOOTP リレー
対象機種：8624、9606

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される。

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 19:

関連コマンド

ADD BOOTP RELAY (92 ページ)

DELETE BOOTP RELAY (121 ページ)

DISABLE BOOTP RELAY (137 ページ)

ENABLE BOOTP RELAY (153 ページ)

PURGE BOOTP RELAY (173 ページ)

SET BOOTP MAXHOPS (182 ページ)

SHOW IP

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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
Name Server ..... 192.168.10.100
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
EGP Autonomous System Number ... Not Set
Transfer RIP to EGP ..... Disabled
ARP aging timer multiplier..... 4 (1024-2048 secs)
OSPF Status ..... DISABLED
IGMP Status ..... DISABLED
DVMRP Status ..... DISABLED
PIM Status ..... DISABLED
IP Multicast HW switching ..... DISABLED

Active Routes

Static ..... 2
Interface ..... 2
RIP ..... 0
EGP ..... 0
```

```

OSPF ..... 0
Other ..... 0
Multicast ..... 0

IP Filter Configuration

Total filters ..... 0

Dynamic Interfaces ..... 0

```

Module Status	IP モジュールの有効・無効
IP Packet Forwarding	IP 転送（ルーティング）機能の有効・無効
IP Echo Reply	ICMP エコー要求（PING）に応答するかどうか
Debugging	IP モジュールのデバッグ機能の有効・無効
IP Fragment Offset Filter	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）
Name Server	プライマリー DNS サーバーの IP アドレス
Secondary Name Server	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	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
OSPF Status	OSPF モジュールの有効・無効
IGMP Status	IGMP モジュールの有効・無効
DVMRP Status	DVMRP モジュールの有効・無効
PIM Status	PIM モジュールの有効・無効
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
OSPF	OSPF 経路エントリー数
Other	その他の経路エントリー数
Multicast	マルチキャスト転送表エントリー数
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 20:

関連コマンド

DISABLE IP (138 ページ)
DISABLE IP DEBUG (139 ページ)
DISABLE IP DNSRELAY (140 ページ)
DISABLE IP FORWARDING (143 ページ)
DISABLE IP SRCROUTE (148 ページ)
DISABLE SNMP (「 運用 ・ 管理 」 の 151 ページ)
ENABLE IP (154 ページ)
ENABLE IP DEBUG (155 ページ)
ENABLE IP DNSRELAY (156 ページ)
ENABLE IP FORWARDING (159 ページ)
ENABLE IP SRCROUTE (164 ページ)
ENABLE SNMP (「 運用 ・ 管理 」 の 173 ページ)
SET IP NAMESERVER (194 ページ)
SET IP SECONDARYNAMESERVER (201 ページ)

SHOW IP ARP

カテゴリー：IP / ARP
対象機種：8624、9606

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
vlan10(9)	172.16.28.1	00-a0-c9-5a-b3-33	Dynamic	Active
vlan10(9)	172.16.28.3	00-90-27-92-63-22	Dynamic	Active
vlan10(9)	172.16.28.4	00-01-e1-20-2e-35	Dynamic	Active
vlan10(9)	172.16.28.32	02-41-f4-02-c2-4b	Dynamic	Active
vlan10(9)	172.16.28.33	00-90-99-1b-65-c7	Dynamic	Active
vlan10(9)	172.16.28.37	00-a0-d2-3c-1c-e0	Dynamic	Active
vlan10(9)	172.16.28.38	00-a0-d2-3c-00-c6	Dynamic	Active
vlan10(9)	172.16.28.65	00-90-99-38-00-2f	Dynamic	Active
vlan10(9)	172.16.28.84	00-05-02-d1-af-6b	Dynamic	Active
vlan10(9)	172.16.28.103	00-00-f4-97-00-19	Dynamic	Active
vlan10(9)	172.16.28.126	00-00-f4-95-9f-31	Dynamic	Active
vlan10(9)	172.16.28.141	00-05-02-99-4c-0d	Dynamic	Active
vlan10(9)	172.16.28.144	00-50-e4-fa-02-4a	Dynamic	Active
vlan10(9)	172.16.28.148	00-05-02-77-24-c7	Dynamic	Active
vlan10(9)	172.16.28.149	00-05-02-31-9d-18	Dynamic	Active
vlan10(9)	172.16.28.162	00-0a-27-ae-59-70	Dynamic	Active
vlan10(9)	172.16.28.166	00-30-65-bd-00-7a	Dynamic	Active
vlan10(9)	172.16.28.169	00-00-cd-00-8b-00	Dynamic	Active
vlan10(9)	172.16.28.180	08-00-2b-e7-05-8b	Dynamic	Active
vlan10(9)	172.16.28.233	00-05-02-ec-c1-1a	Dynamic	Active
vlan10	172.16.28.255	ff-ff-ff-ff-ff-ff	Other	Active
vlan20	192.168.10.255	ff-ff-ff-ff-ff-ff	Other	Active
vlan20	255.255.255.255	ff-ff-ff-ff-ff-ff	Other	Active

Interface	インターフェース（VLAN）名。カッコ内はポート番号
IP Address	IP アドレス
Physical Address	物理アドレス（MAC アドレス）

ARP Type	エントリー種別。Static (スタティックエントリー。ADD IP ARP コマンドで登録) Dynamic (ダイナミックエントリー。ARP パケットから学習) Invalid (無効エントリー) Other (システムによって自動生成されるエントリー。IP ブロードキャストアドレスなど)
Status	エントリーの状態。Active が Inactive

表 21:

関連コマンド

ADD IP ARP (93 ページ)

DELETE IP ARP (122 ページ)

SET IP ARP (184 ページ)

SHOW IP COUNTER

カテゴリー：IP / 一般コマンド
対象機種：8624、9606

SHOW IP COUNTER[={ALL|ARP|ICMP|INTERFACE|IP|MULTICAST|RIP|ROUTES|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
-----

Interface Counters

Interface: port1
  ifInOctets ..... 0          ifOutOctets ..... 0
  ifInUcastPkts ..... 0        ifOutUcastPkts ..... 0
  ifInNUcastPkts ..... 0        ifOutNUcastPkts ..... 0
  ifInDiscards ..... 0          ifOutDiscards ..... 0
  ifInErrors ..... 0            ifOutErrors ..... 0

Interface: port2
  ifInOctets ..... 0          ifOutOctets ..... 0
  ifInUcastPkts ..... 0        ifOutUcastPkts ..... 0
  ifInNUcastPkts ..... 0        ifOutNUcastPkts ..... 0
  ifInDiscards ..... 0          ifOutDiscards ..... 0
  ifInErrors ..... 0            ifOutErrors ..... 0

Interface: port17
  ifInOctets ..... 2376069      ifOutOctets ..... 163132
  ifInUcastPkts ..... 1741       ifOutUcastPkts ..... 1452
  ifInNUcastPkts ..... 11552     ifOutNUcastPkts ..... 6
  ifInDiscards ..... 0           ifOutDiscards ..... 0
  ifInErrors ..... 0             ifOutErrors ..... 0
```

```

Interface: port18
  ifInOctets ..... 0          ifOutOctets ..... 0
  ifInUcastPkts ..... 0        ifOutUcastPkts ..... 0
  ifInNUcastPkts ..... 0       ifOutNUcastPkts ..... 0
  ifInDiscards ..... 0         ifOutDiscards ..... 0
  ifInErrors ..... 0           ifOutErrors ..... 0

Interface: port19
  ifInOctets ..... 60440       ifOutOctets ..... 132329
  ifInUcastPkts ..... 933      ifOutUcastPkts ..... 682
  ifInNUcastPkts ..... 4       ifOutNUcastPkts ..... 440
  ifInDiscards ..... 0         ifOutDiscards ..... 0
  ifInErrors ..... 0           ifOutErrors ..... 0

Interface: port20
  ifInOctets ..... 0          ifOutOctets ..... 0
  ifInUcastPkts ..... 0        ifOutUcastPkts ..... 0
  ifInNUcastPkts ..... 0       ifOutNUcastPkts ..... 0
  ifInDiscards ..... 0         ifOutDiscards ..... 0
  ifInErrors ..... 0           ifOutErrors ..... 0

Interface: port21
  ifInOctets ..... 0          ifOutOctets ..... 0
  ifInUcastPkts ..... 0        ifOutUcastPkts ..... 0
  ifInNUcastPkts ..... 0       ifOutNUcastPkts ..... 0
  ifInDiscards ..... 0         ifOutDiscards ..... 0
  ifInErrors ..... 0           ifOutErrors ..... 0

Interface: vlan1
  ifInOctets ..... 2489321     ifOutOctets ..... 0
  ifInUcastPkts ..... 2624     ifOutUcastPkts ..... 2123
  ifInNUcastPkts ..... 11556   ifOutNUcastPkts ..... 2
  ifInDiscards ..... 4823      ifOutDiscards ..... 0
  ifInErrors ..... 0           ifOutErrors ..... 0

Interface: vlan10
  ifInOctets ..... 0          ifOutOctets ..... 0
  ifInUcastPkts ..... 0        ifOutUcastPkts ..... 0
  ifInNUcastPkts ..... 0       ifOutNUcastPkts ..... 164
  ifInDiscards ..... 0         ifOutDiscards ..... 0
  ifInErrors ..... 0           ifOutErrors ..... 0

IP counters
  inReceives ..... 8695       outRequests ..... 166
  inHdrErrors ..... 0          outDiscards ..... 4
  inAddrErrors ..... 0         outNoRoutes ..... 2
  inUnknownProtos ..... 0      forwDatagrams ..... 2282
  inDiscards ..... 0           routingDiscards ..... 0

```

SHOW IP COUNTER

inDelivers	8594		
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	97	outMsgs	0
inErrors	0	outErrors	0
inDestUnreachs	0	outDestUnreachs	0
inTimeExcds	0	outTimeExcds	0
inParamProbs	0	outParamProbs	0
inSrcQuenchs	0	outSrcQuenchs	0
inRedirects	0	outRedirects	0
inEchos	0	outEchos	0
inEchoReps	0	outEchoReps	0
inTimestamps	0	outTimestamps	0
inTimestampReps	0	outTimestampReps	0
inAddrMasks	0	outAddrMasks	0
inAddrMaskReps	0	outAddrMaskReps	0
UDP counters			
inDatagrams	5076	outDatagrams	166
inErrors	0	noPorts	210
EGP counters			
inMsgs	0	outMsgs	0
inErrors	0	outErrors	0
SNMP counters:			
inPkts	0	outPkts	2
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	2		
inTotalReqVars	0				
inTotalSetVars	0				
inGetRequests	0				
inGetNexts	0				
inSetRequests	0				
inGetResponses	0				
inTraps	0				

Info (105336): IP Route counting is disabled.					
Route Counters					
IP address	NextHop	Interface	Metric	Octets rcvd	Octets sent

172.16.28.0	0.0.0.0	vlan1	1	0	0

IP Multicast Counters					

Interface	ifInMultPkts	ifInMultDiscard	ifOutMultPkts	ifOutMultDiscards	

vlan1	4	0	0	0	
vlan10	0	0	4	4	

IP ARP counters					
arpRxPkts	662	arpTxPkts	0		
arpRxReqPkts	660	arpTxReqPkts	2		
arpRxRespPkts	2	arpTxRespPkts	7		
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 22: 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 23: ICMP カウンター

ifInOctets	受信オクテット数
ifInUcastPkts	ユニキャストパケット受信数
ifInNUcastPkts	マルチキャストパケット受信数
ifInDiscards	受信後破棄パケット数
ifInErrors	エラーパケット受信数
ifUnknownProtos	未サポートプロトコルパケット受信数
ifOutOctets	送信オクテット数
ifOutUcastPkts	ユニキャストパケット送信数
ifOutNUcastPkts	マルチキャストパケット送信数
ifOutDiscards	送信前破棄パケット数
ifOutErrors	送信前破棄パケット数 (エラーによる)

表 24: 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	ディレクティッ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 25: 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 26: MULTICAST カウンター

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 27: RIP 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 28: ROUTES 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 29: UDP カウンター

関連コマンド

SHOW IP INTERFACE (235 ページ)

SHOW IP ROUTE (243 ページ)

SHOW SNMP (「運用・管理」の 315 ページ)

SHOW TCP (278 ページ)

SHOW IP DEBUG

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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 = vlan10
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 (139 ページ)

ENABLE IP DEBUG (155 ページ)

SHOW IP (215 ページ)

SHOW IP FILTER

カテゴリー：IP / ソフトウェア IP フィルター

対象機種：8624、9606

SHOW IP FILTER[=*filter-id*]

filter-id: 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 Dest. Port Type	Source Address Dest. Address Act/Pol/Pri	Source Mask Dest. Mask Logging	Session Prot.(T/C)	Size Options 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	再構成後の最大 IP データグラムサイズ。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。
Logging	本エントリーにマッチしたパケットをログに記録するかどうか。Off (記録せず)、Head (ヘッダー情報のみ)、Dump (ヘッダーおよびデータ先頭 32 オクテット)、4 ~ 1600 の数値 (ヘッダー情報とデータの先頭指定バイト数)
Matches	このエントリーにマッチした IP パケットの数
Requests	このフィルターと照合された IP パケットの数
Passes	このフィルターによって通過が許可されたパケットの数
Fails	このフィルターによって通過を拒否されたパケットの数

表 30:

関連コマンド

ADD IP FILTER (94 ページ)

DELETE IP FILTER (123 ページ)

SET IP FILTER (187 ページ)

SHOW IP FLOW

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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
-----
192.168.40.1 - 192.168.20.1    ICMP      0 - 0                1  000000  2
0 vlan20 -vlan10              0  n   n    0  0191eb9c  00000000  01c3ea9c  n/n/n
192.168.30.1 - 192.168.30.254  ICMP      8 - 0                2  000000  2
0 vlan10 -                    0  n   n    1  00000000  00000000  00000000  n/n/n
192.168.10.100 - 192.168.30.254 ICMP      0 - 0                5  000000  2
0 vlan10 -                    0  n   n    1  00000000  00000000  00000000  n/n/n
192.168.40.1 - 192.168.40.254  ICMP      8 - 0                5  000000  2
0 vlan20 -                    0  n   n    1  00000000  00000000  00000000  n/n/n
192.168.30.1 - 224.0.0.9       UDP       520 - 520            12  000000  2
0 vlan10 -                    0  n   n    2  00000000  00000000  00000000  n/n/n

```

IP Addresses	フローを構成する両エンドの IP アドレス (a.b.c.d - e.f.g.h)
Prot	IP プロトコル名またはプロトコル番号
Port Numbers	プロトコルが TCP/UDP の場合、フローを構成する両エンドのポート番号 (x - y)。ICMP の場合はメッセージタイプとコード (type - code)。その他のプロトコルでは意味を持たない (0 - 0 と表示)。
Hits	このフローエントリの使用回数
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 31:

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：8624、9606

SHOW IP HELPER [COUNTER]

解説

UDP ブロードキャストパケットの転送先設定を表示する。

パラメーター

COUNTER 本パラメーター指定時は、UDP ブロードキャスト転送機能の統計情報が表示される。

入力・出力・画面例

```
Manager > show ip helper

IP HELPER Configuration

Status : Disabled
-----
Interface : vlan10
  UDP port : 137
    Destination(s) ..... 172.16.28.5
  UDP port : 138
    Destination(s) ..... 172.16.28.5
-----
```

Status	UDP ブロードキャスト転送機能の有効・無効。
Interface	UDP ブロードキャストを監視するインターフェース。
UDP port	転送する UDP パケットの終点ポート番号
Destination	UDP パケットの転送先 IP アドレス

表 32:

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 33: COUNTER オプション

関連コマンド

- ADD IP HELPER (100 ページ)
- DELETE IP HELPER (124 ページ)
- DISABLE IP HELPER (144 ページ)
- ENABLE IP HELPER (160 ページ)

SHOW IP HOST

カテゴリー：IP / 名前解決
対象機種：8624、9606

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 34:

関連コマンド

- ADD IP HOST (102 ページ)
- DELETE IP HOST (125 ページ)
- SET IP HOST (190 ページ)
- SET IP NAMESERVER (194 ページ)
- SET IP SECONDARYNAMESERVER (201 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：8624、9606

SHOW IP INTERFACE[=*vlan-if*] [COUNTER]

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

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 (VLAN) インターフェース名。省略時はすべてのインターフェースの情報が表示される。

COUNTER このオプションを指定したときは、インターフェースのパケット送受信統計が表示される。

入力・出力・画面例

Manager > show ip interface										
Interface	Type	IP Address	Bc	Fr	PArp	Filt	RIP	Met.	SAMode	IPSc
Pri. Filt	Pol.Filt	Network Mask	MTU	VJC	GRE	OSPF	Met.	DBcast	Mul.	
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
Local	---	Not set	-	-	-	---	--		Pass	--
---	---	Not set	1500	-		---	--		---	---
vlan5	Static	192.168.5.1	1	n	On	---	01		Pass	No
---	---	255.255.255.0	1500	-		---	0000000001	No		Rec
vlan10	Static	192.168.10.250	1	n	On	---	01		Pass	No
---	---	255.255.255.0	1500	-		---	0000000001	No		Rec
vlan20#	Static	192.168.20.250	1	n	On	---	01		Pass	No
---	---	255.255.255.0	1500	-		---	0000000001	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。名前の後の「#」は、該当インターフェースがリンクダウンしていることを示す
Type	インターフェース種別。Static(静的に設定されたインターフェース) Dynamic(外部からの SLIP/PPP 接続によって動的に作成され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。
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)
OSPF Met.	OSPF メトリック。
DBcast	このインターフェース下のネットワークに対するディレクティッドブロードキャストを転送するかどうか。Yes または No。

表 35:

Interface	インターフェース名。「LOCAL」はローカル IP インターフェースを示す。名前の後の「#」は、該当インターフェースがリンクダウンしていることを示す
Type	インターフェース種別。Static(静的に設定されたインターフェース) Dynamic(外部からの SLIP/PPP 接続によって動的に作成され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 36: COUNTER オプション

関連コマンド

ADD IP INTERFACE (103 ページ)

DELETE IP INTERFACE (126 ページ)

DISABLE IP INTERFACE (145 ページ)

ENABLE IP INTERFACE (161 ページ)

RESET IP INTERFACE (178 ページ)
SET IP INTERFACE (191 ページ)
SHOW IP COUNTER (220 ページ)

SHOW IP RIP

カテゴリー：IP / 経路制御 (RIP)

対象機種：8624、9606

```
SHOW IP RIP [ INTERFACE=vlan-if ] [ IP=ipadd ]
```

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

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 (VLAN) 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

vlan10	-	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 37:

関連コマンド

ADD IP RIP (106 ページ)

DELETE IP RIP (127 ページ)
SET IP RIP (195 ページ)
SHOW IP (215 ページ)
SHOW IP COUNTER (220 ページ)

SHOW IP RIP COUNTER

カテゴリー：IP / 経路制御 (RIP)

対象機種：8624、9606

SHOW IP RIP COUNTER[={DETAIL|SUMMARY}] [INTERFACE=*vlan-if*] [IP=*ipadd*]

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

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 (VLAN) 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:

```
inResponses ..... 0
inTrigRequests ..... 0
inTrigResponses ..... 0
inTrigAcks ..... 0
inDiscards ..... 0
```

Output:

```
outResponses ..... 2
outTrigRequests ..... 0
outTrigResponses ..... 0
outTrigAcks ..... 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 38:

関連コマンド

SHOW IP COUNTER (220 ページ)

SHOW IP RIP (238 ページ)

SHOW IP RIPTIMER

カテゴリー：IP / 経路制御 (RIP)

対象機種：8624、9606

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 39:

関連コマンド

SET IP RIPTIMER (197 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：8624、9606

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

ipadd: IP アドレス

解説

IP ルーティングテーブルを表示する。

パラメーター

ROUTE 表示させたい経路の宛先ネットワークアドレス。ワイルドカード(*)の指定も可能で、「192.*.*」と指定すると「192」で始まる経路だけが表示される。省略時はすべての経路が表示される。

GENERAL ルーティングに関するサマリーを表示する。

CACHE ルートキャッシュの内容を表示する。ROUTE パラメーター指定時は該当する経路だけが表示される。

COUNT 経路ごとの送受信オクテット数を表示する。送受信オクテット数は、ENABLE IP ROUTE コマンドでルートカウンター（COUNT オプション）を有効にしているときだけカウントされる。

入力・出力・画面例

Manager > show ip route					
IP Routes					
Destination DLCI/Circ.	Mask Type	Policy	NextHop Protocol	Interface Metrics	Age Preference
172.16.10.0	255.255.255.0		0.0.0.0	vlan172	8007
-	direct	0	interface	1	0
172.16.10.0	255.255.255.0		0.0.0.0	vlan172	3646
-	remote	0	ospf-Intra	1	10
192.168.10.0	255.255.255.0		0.0.0.0	vlan10	8007
-	direct	0	interface	1	0
192.168.10.0	255.255.255.0		0.0.0.0	vlan10	3646
-	remote	0	ospf-Intra	1	10
192.168.20.0	255.255.255.0		0.0.0.0	vlan10	3066
-	remote	0	ospf-Intra	2	10
192.168.21.0	255.255.255.0		0.0.0.0	vlan10	2908
-	remote	0	ospf-Intra	3	10
192.168.22.0	255.255.255.0		0.0.0.0	vlan10	2908

SHOW IP ROUTE

```

-                remote    0          ospf-Intra          3              10
192.168.100.0    255.255.255.0          0.0.0.0          vlan100        8007
-                direct    0          interface          1              0
192.168.100.0    255.255.255.0          0.0.0.0          vlan100        3653
-                remote    0          ospf-Intra          1              10
192.168.101.0    255.255.255.0          192.168.100.254  vlan100        137
-                remote    0          ospf-EXT1          2              150
192.168.102.0    255.255.255.0          192.168.100.254  vlan100        3481
-                remote    0          ospf-Intra          2              10
-----

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
-----
192.168.10.1      192.168.10.0    255.255.255.0    0.0.0.0          vlan10
192.168.50.16     0.0.0.0         0.0.0.0         192.168.30.254   vlan30
192.168.10.1      192.168.10.0    255.255.255.0    0.0.0.0          vlan10
192.168.50.16     0.0.0.0         0.0.0.0         192.168.30.254   vlan30
                hits:          13          misses:          4
-----

Manager > show ip route count

Route Counters

IP address        NextHop          Interface  Metric  Octets rcvd  Octets sent
-----
0.0.0.0           192.168.100.254  vlan100    1        260          520
192.168.30.0      0.0.0.0          vlan30     1       24312         0
192.168.10.0      0.0.0.0          vlan10#    1         0           0
-----

```

Destination	経路の宛先ネットワークアドレス
Mask	サブネットマスク
NextHop	ネクストホップルーターの IP アドレス

Interface	本経路宛てのパケットを送出するインターフェース。名前の後の「#」は、該当インターフェースがリンクダウンしていることを示す
Age	経路情報取得後の経過時間
Type	経路エントリーの種類。remote、direct、other のいずれか。
Policy	本経路のサービスタイプ（経路選択ポリシー）
Protocol	経路情報のソースプロトコル。静的経路（static）、RIP（rip）、OSPF（ospf）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 40:

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 41: GENERAL オプション

Destination	宛先 IP アドレス
Route	宛先ネットワークアドレス
Route mask	サブネットマスク
NextHop	ネクストホップルーターの IP アドレス
Interface	送出インターフェース。名前の後の「#」は、該当インターフェースがリンクダウンしていることを示す

表 42: CACHE オプション

IP address	経路の宛先ネットワークアドレス
NextHop	ネクストホップルーターの IP アドレス
Interface	送出インターフェース。名前の後の「#」は、該当インターフェースがリンクダウンしていることを示す
Metric	メトリック（コスト）
Octets rcvd	本経路経由で受信したオクテット数
Octets sent	本経路経由で送信したオクテット数

表 43: COUNT オプション

関連コマンド

ADD IP ROUTE (108 ページ)

DELETE IP ROUTE (128 ページ)

DISABLE IP ROUTE (147 ページ)

ENABLE IP ROUTE (163 ページ)

SET IP ROUTE (198 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：8624、9606

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 Protocol	Mask Direction	Nexthop Interface	Policy Action	Matched
1	200.200.20.* Any	*.*.*.* Both	Any -	- Exclude	0
2	*.*.*.* Any	*.*.*.* Both	Any -	- Include	0
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 44:

関連コマンド

ADD IP ROUTE FILTER (110 ページ)

DELETE IP ROUTE FILTER (129 ページ)

SET IP ROUTE FILTER (199 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：8624、9606

SHOW IP TRUSTED

解説

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 (94 ページ)

ADD IP TRUSTED (112 ページ)

DELETE IP FILTER (123 ページ)

DELETE IP TRUSTED (130 ページ)

SET IP FILTER (187 ページ)

SHOW IP FILTER (228 ページ)

SHOW IP UDP

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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 45:

関連コマンド

SHOW IP COUNTER (220 ページ)

SHOW TCP (278 ページ)

SHOW OSPF

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

SHOW OSPF

解説

OSPF モジュールのグローバル設定情報を表示する。

入力・出力・画面例

```
Manager > show ospf

Router ID ..... 1.1.1.1
OSPF module status ..... Enabled
Area border router status ..... Yes
AS border router status ..... Disabled
PTP stub network generation ..... Enabled
External LSA count ..... 2
External LSA sum of checksums ... 5086
New LSAs originated ..... 119
New LSAs received ..... 55
RIP ..... None
Dynamic interface support ..... None
Number of active areas ..... 3
Logging ..... Disabled
Debugging ..... Disabled
AS external default route:
  Status ..... Disabled
  Type ..... 1
  Metric ..... 1
```

Router ID	ルーター ID
OSPF module status	OSPF モジュールの有効・無効
Area border router status	エリア境界ルーター (ABR) として動作中かどうか
AS border router status	AS 境界ルーター (ASBR) として動作中かどうか
PTP stub network generation	PPP インターフェイスがリンクアップしたときに、対応する LSA を動的作成するかどうか。
External LSA count	トポロジデータベース内の AS 外部 LSA の数
External LSA sum of checksums	AS 外部 LSA のチェックサム合計値。ルーター間でトポロジデータベースを比較するためのもの

New LSAs originated	本システムが送信した新規 LSA の数
New LSAs received	本システムが受信した新規 LSA の数
RIP	RIP と情報の交換を行うかどうか。None (交換しない)、Import (RIP の情報を取り込む)、Export (RIP に情報を提供する)、Import/export (RIP と OSPF の間で情報を相互に交換する)
Dynamic interface support	ダイナミックインターフェースの経路情報をインポートするかどうか。Stub (ホストルートとしてインポート)、AS external (AS 外部 LSA としてインポート)、None (インポートしない)、Undefined (未指定) のいずれか
Number of active areas	本システム上で定義されているエリアの数
Logging	OSPF イベントをログに記録するかどうか (ENABLE OSPF LOG コマンド)
Debugging	OSPF モジュールのデバッグ機能の有効・無効 (ENABLE OSPF DEBUG コマンド)
AS external default route	AS 外部 LSA に関する情報が表示される
Status	デフォルトルート (0.0.0.0) の AS 外部 LSA を生成するかどうか。
Type	デフォルトルートの AS 外部 LSA タイプ。タイプ 1、タイプ 2 または Undefined
Metric	デフォルト AS 外部 LSA のメトリック

表 46:

関連コマンド

SET OSPF (202 ページ)

SHOW OSPF AREA

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

SHOW OSPF AREA [= {BACKBONE|*area-number*}] [{FULL|SUMMARY}]

area-number: OSPF エリア ID (a.b.c.d の形式)

解説

OSPF エリアに関する情報を表示する。

パラメーター

AREA エリア ID。省略時はすべてのエリアに関する情報が表示される。指定時は該当エリアの詳細な情報が表示される。

FULL 詳細な情報を表示する。

SUMMARY サマリー情報を表示する。

入力・出力・画面例

```
Manager > show ospf area
```

Area	State	Authentication	StubArea	StubMetric	Summary LSAs
Backbone	Active	None	No	1	Send
1.1.1.1	Active	None	No	1	None
2.2.2.2	Active	None	Yes	1	None

```
Manager > show ospf area=backbone
```

```
Area Backbone:
```

```

State ..... Active
Authentication ..... None
Stub area ..... No
Stub Cost ..... 1
Summary LSAs ..... Send
SPF runs ..... 16
Area border router count ..... 2
AS border router count ..... 1
LSA count ..... 7
LSA sum of checksums ..... 244417
```

```

Ranges:
  Range 172.16.0.0:
    Mask ..... 255.255.0.0
  Range 192.168.100.0:
    Mask ..... 255.255.255.0

Interfaces:
  vlan100:
    Type ..... Broadcast
    State ..... DR
  vlan172:
    Type ..... Broadcast
    State ..... DR

```

Area	エリア ID
State	エリアの状態。エリアの範囲と所属するインターフェースが設定されていれば Active、そうでなければ Inactive と表示される。
Authentication	受信 OSPF パケットの認証方式。None（無認証）または Password（簡易パスワード認証）。
StubArea	スタブエリアかどうか
StubMetric	スタブエリアのデフォルトメトリック
Summary LSAs	デフォルトルート以外のサマリー LSA をスタブエリア内に通知するかどうか。Send（通知する） None（通知しない） Undefined（未定義）

表 47:

Area	エリア ID
State	エリアの状態。エリアの範囲と所属するインターフェースが設定されていれば Active、そうでなければ Inactive と表示される。
Authentication	受信 OSPF パケットの認証方式。None（無認証）または Password（簡易パスワード認証）。
Stub area	スタブエリアかどうか
Stub Cost	スタブエリアのデフォルトメトリック
Summary LSAs	デフォルトルート以外のサマリー LSA をスタブエリア内に通知するかどうか。Send（通知する） None（通知しない） Undefined（未定義）
SPF runs	エリア内部の経路表を再計算した回数
Area border router count	エリア内にあるエリア境界ルーター（ABR）の数
AS border router count	エリア内にある AS 境界ルーター（ASBR）の数
LSA count	該当エリアのトポロジデータベースに格納されている LSA の合計数。AS 外部 LSA は除く。
LSA sum of checksums	該当エリアの LSA チェックサム合計値。ルーター間でトポロジデータベースの同一性をチェックするために使用される。

Range	エリアを構成するネットワークのベースアドレス
Mask	Range に対するネットマスク
Interfaces	エリアに所属する OSPF インターフェース
Type	インターフェースタイプ。Unknown (不明)、Broadcast (ブロードキャスト型)、NMBA (非ブロードキャスト型)、Point to Point (ポイントツーポイント型)、Virtual (仮想インターフェース) のいずれか。
State	OSPF インターフェースとしての状態。unknown (不明)、down (送受信を行わない初期状態)、loopback (ループバック状態)、waiting (Hello パケットをモニターしてバックアップ DR の存在を確認している状態)、ptp (仮想リンクに接続されている状態)、DR (DR に選出されている状態)、backupDR (バックアップ DR に選出されている状態)、otherDR (DR、バックアップ DR のいずれにも選出されていない状態) のいずれか。

表 48: エリア指定時

関連コマンド

ADD OSPF AREA (113 ページ)

ADD OSPF RANGE (118 ページ)

DELETE OSPF AREA (131 ページ)

DELETE OSPF RANGE (134 ページ)

RESET OSPF COUNTER (180 ページ)

SET OSPF AREA (204 ページ)

SET OSPF RANGE (209 ページ)

SHOW OSPF RANGE (270 ページ)

SHOW OSPF DEBUG

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

SHOW OSPF DEBUG

解説

OSPF モジュールの内部デバッグ情報を表示する。

入力・出力・画面例

```
Manager > show ospf debug
```

OSPF event timers

Delay	Event	Argument
-------	-------	----------

0.34	LSDBTIMER	-
3.82	HELLO	Int: vlan10
6.18	HELLO	Int: virt0
6.40	HELLO	Int: vlan100
8.30	HELLO	Int: vlan172
36.94	NBR_INACT	Nbr: vlan100, 192.168.100.254
37.60	NBR_INACT	Nbr: vlan10, 192.168.10.254
39.00	NBR_INACT	Nbr: virt0, 192.168.10.254
756.40	REFRESHLSA	LSA: Network, 192.168.100.1, area=0.0.0.0
1073.84	REFRESHLSA	LSA: Network, 192.168.10.1, area=1.1.1.1
1084.18	REFRESHLSA	LSA: Router, 1.1.1.1, area=1.1.1.1
1192.56	REFRESHLSA	LSA: Router, 1.1.1.1, area=0.0.0.0
1366.54	REFRESHLSA	LSA: Summary, 172.16.0.0, area=1.1.1.1
1366.54	REFRESHLSA	LSA: Summary, 192.168.10.0, area=0.0.0.0
1366.54	REFRESHLSA	LSA: Summary, 192.168.20.0, area=1.1.1.1
1366.54	REFRESHLSA	LSA: Summary, 192.168.100.0, area=1.1.1.1
1366.54	REFRESHLSA	LSA: Summary, 192.168.101.0, area=1.1.1.1
1366.54	REFRESHLSA	LSA: Summary, 192.168.102.0, area=1.1.1.1
1368.56	REFRESHLSA	LSA: Summary, 192.168.21.0, area=1.1.1.1
1368.56	REFRESHLSA	LSA: Summary, 192.168.22.0, area=1.1.1.1

OSPF SPF list

Area	Vertex ID	Type	Dist	#NH	Next hop	Int
0.0.0.0	1.1.1.1	Net	0	0		
	192.168.100.1	Rou	1	1	0.0.0.0	vlan100
	3.3.3.3	Net	1	1	0.0.0.0	vlan10
	2.2.2.2	Rou	1	1	192.168.100.254	vlan100
	192.168.20.254	Rou	2	1	0.0.0.0	vlan10

	4.4.4.4	Rou	2	1	0.0.0.0	vlan10
1.1.1.1	1.1.1.1	Rou	0	0		
	192.168.10.1	Rou	1	1	0.0.0.0	vlan10
	3.3.3.3	Net	1	1	192.168.10.254	vlan10

SHOW OSPF HOST

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

SHOW OSPF HOST [=ipadd] [AREA={BACKBONE|area-number}]

ipadd: IP アドレス

area-number: OSPF エリア ID (a.b.c.d の形式)

解説

OSPF ルーティングテーブルにスタティック登録されたホスト経路 (ネットマスクが 255.255.255.255 の経路) の情報を表示する。

パラメーター

HOST ホストの IP アドレス

AREA ホストの所属エリア

入力・出力・画面例

Manager > show ospf host						
IP address	Mask	State	Area	Metric	TOS	Type
192.168.10.100	255.255.255.255	Active	Backbone	1	0	Stat

IP address	ホストまたは Point-to-Point ネットワークの IP アドレス
Mask	ネットマスク
State	経路エントリの状態。Active か Inactive。
Area	所属エリア ID
Metric	メトリック
TOS	サービスタイプ (TOS)
Type	エントリタイプ。Stat (スタティックルート)、Dyn (ダイナミックルート) のいずれか。

表 49:

関連コマンド

ADD OSPF HOST (115 ページ)

DELETE OSPF HOST (132 ページ)

SET OSPF HOST (206 ページ)

SHOW OSPF INTERFACE

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

SHOW OSPF INTERFACE [=vlan-if] [AREA={BACKBONE|area-number}]
[IPADDRESS=ipadd] [{FULL|SUMMARY}]

vlan-if: VLAN インターフェイス (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または仮想インターフェイス (VIRTx)

area-number: OSPF エリア ID (a.b.c.d の形式)

ipadd: IP アドレス

解説

OSPF インターフェイスの情報を表示する。

パラメーター

INTERFACE IP (VLAN) インターフェイス名、または仮想インターフェイス名 (VIRTx)。省略時は全インターフェイスのサマリー情報が表示される。インターフェイス指定時は該当インターフェイスの詳細情報が表示される。

AREA エリア ID

IPADDRESS インターフェイスの IP アドレス

FULL 詳細な情報を表示する。

SUMMARY サマリー情報を表示する。

入力・出力・画面例

```
Manager > show ospf interface
```

Iface	Status	Area	State	Designated rtr / Virtual nbr	Backup DR / Transit area
virt0	Enabled	Backbone	ptp	3.3.3.3	1.1.1.1
vlan10	Enabled	1.1.1.1	DR	192.168.10.1	192.168.10.254
vlan100	Enabled	Backbone	DR	192.168.100.1	192.168.100.254
vlan172	Enabled	Backbone	DR	172.16.10.1	None

```
Manager > show ospf interface=vlan10
```

```
vlan10:
  Status ..... Enabled
  Area ..... 1.1.1.1
```

```

IP address ..... 192.168.10.1
IP net mask ..... 255.255.255.0
IP network number ..... 192.168.10.0
Type ..... Broadcast
State ..... DR
Router priority ..... 1
Transit delay ..... 1 second
Retransmit interval ..... 5 seconds
Hello interval ..... 10 seconds
Router dead interval ..... 40 seconds
Interface events ..... 2
Password .....
Designated router ..... 192.168.10.1
Backup designated router ..... 192.168.10.254
Metric boost 1 ..... 0

```

Manager > show ospf interface=virt0

```

virt0:
Status ..... Enabled
Area ..... Backbone
Type ..... Virtual
State ..... ptp
Transit delay ..... 1 second
Retransmit interval ..... 5 seconds
Hello interval ..... 10 seconds
Router dead interval ..... 40 seconds
Interface events ..... 1
Password .....
Virtual neighbour ..... 3.3.3.3
Transit Area ..... 1.1.1.1
Metric boost 1 ..... 0

```

Status	インターフェースの管理ステータス
Area	所属エリア
State	OSPF インターフェースとしての状態。unknown（不明）、down（送受信を行わない初期状態）、loopback（ループバック状態）、waiting（Hello パケットをモニターしてバックアップ DR の存在を確認している状態）、ptp（仮想リンクに接続されている状態）、DR（DR に選出されている状態）、backupDR（バックアップ DR に選出されている状態）、otherDR（DR、バックアップ DR のいずれにも選出されていない状態）のいずれか。

Designated rtr / Virtual nbr	VLAN インターフェースの場合は、配下ネットワークの指名ルーター (DR)。仮想インターフェース (VIRTx) の場合は、仮想リンクの対向に位置するバックボーンルーター (ABR)。
Backup DR / Transit area	VLAN インターフェースの場合は、配下ネットワークのバックアップ指名ルーター。仮想インターフェース (VIRTx) の場合は、仮想リンクの通過エリア ID

表 50: インターフェース省略時または SUMMARY オプション指定時

Status	インターフェースの管理ステータス
Area	所属エリア
IP address	IP アドレス
IP net mask	ネットマスク
IP network number	IP ネットワークアドレス
Type	配下ネットワークの種別。Broadcast (ブロードキャスト)、NBMA (非ブロードキャスト)、Point to Point (ポイントツーポイント)、Unknown (不明)、Virtual (仮想) のいずれか。
State	OSPF インターフェースとしての状態。unknown (不明)、down (送受信を行わない初期状態)、loopback (ループバック状態)、waiting (Hello パケットをモニターしてバックアップ DR の存在を確認している状態)、ptp (仮想リンクに接続されている状態)、DR (DR に選出されている状態)、backupDR (バックアップ DR に選出されている状態)、otherDR (DR、バックアップ DR のいずれにも選出されていない状態) のいずれか。
Router priority	ルーター優先度。大きいほど DR になる可能性が高い。0 は DR の資格がないことを示す。
Transit delay	本インターフェースにおけるリンク状態更新パケットの送信遅延時間。通常は 1 (秒)
Retransmit interval	データベース記述パケット (タイプ 2)、リンク状態要求パケット (タイプ 3)、リンク状態更新パケット (タイプ 4) の再送信間隔
Hello interval	Hello パケット (タイプ 1) の送信間隔
Router dead interval	隣接ルーターからの Hello パケットが途絶えてから、隣接ルーターがダウンしたと見なすまでの時間
Poll interval	非ブロードキャスト型のネットワークにおいて、アクティブでないと思われる隣接ルーターに対する Hello パケットによるポーリング間隔
Interface events	OSPF インターフェースの状態が変化した回数とエラーが発生した回数の合計
Password	認証用パスワード。エリアの認証方式が PASSWORD (簡易パスワード認証) のときに有効
Designated router	配下ネットワークの指名ルーター (DR)
Backup designated router	配下ネットワークのバックアップ指名ルーター

Virtual neighbour	仮想リンクの対向に位置するバックボーンルーター (ABR)
Transit area	仮想リンクの通過エリア ID

表 51: インターフェース指定時または FULL オプション指定時

関連コマンド

ADD OSPF INTERFACE (116 ページ)

DELETE OSPF INTERFACE (133 ページ)

RESET OSPF COUNTER (180 ページ)

SET OSPF INTERFACE (207 ページ)

SHOW OSPF LSA

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

```
SHOW OSPF LSA=link-id [ AREA={BACKBONE|area-number} ] [ {FULL|SUMMARY} ]
    [ TYPE={ASEXTERNAL|ASBRSUMMARY|ASSUMMARY|IPSUMMARY|SUMMARY|NETWORK|
ROUTER} ]
```

link-id: リンク状態 ID (IP アドレスと同じ形式)

area-number: OSPF エリア ID (a.b.c.d の形式)

解説

トポロジータベースに格納されているリンク情報 (LSA) を表示する。

パラメーター

LSA リンク状態 ID。省略時はすべてのリンク情報が簡潔に表示される。指定時は該当リンクの詳細な情報が表示される。「0」によるワイルドカード指定も可能で、「172.16.0.0」のように指定すると「172.16」ではじまるすべてのリンク状態 ID にマッチする。

AREA エリア ID。指定時は該当エリアに所属するリンク情報だけが表示される。「0」によるワイルドカード指定が可能。

FULL 詳細な情報を表示させたいときに指定する。

SUMMARY サマリー情報を表示させたいときに指定する。

TYPE 表示する LSA のタイプを指定する。ASEXTERNAL (AS 外部 (タイプ 5))、ASBRSUMMARY、ASSUMMARY (ASBR サマリー (タイプ 4))、IPSUMMARY、SUMMARY (ネットワークサマリー (タイプ 3))、NETWORK (ネットワーク (タイプ 2))、ROUTER (ルーター (タイプ 1)) から選択する。省略時はすべての LSA が表示される。

入力・出力・画面例

Manager > show ospf lsa						
Type	LS ID	Router ID	Sequence	Age	Len	Csum

Area backbone:						
Router	1.1.1.1	1.1.1.1	80000008	805	60	0532
Router	2.2.2.2	2.2.2.2	80000003	1141	36	8e15
Router	3.3.3.3	3.3.3.3	80000002	804	36	dae1
Network	192.168.100.1	1.1.1.1	80000001	1144	32	dd9d
Summary	192.168.10.0	3.3.3.3	80000012	337	28	d8f2
Summary	192.168.10.0	1.1.1.1	80000017	335	28	0bc3
Summary	192.168.20.0	3.3.3.3	80000002	337	28	8a47

Area 1.1.1.1:

Type	LS ID	Router ID	Sequence	Age	Len	Csum
Router	1.1.1.1	1.1.1.1	80000005	814	36	2c31
Router	3.3.3.3	3.3.3.3	80000002	823	36	7dd4
Network	192.168.10.1	1.1.1.1	80000001	824	32	f1df
Summary	172.16.0.0	3.3.3.3	8000000a	337	28	8dfb
Summary	172.16.0.0	1.1.1.1	80000016	335	28	a7de
Summary	192.168.20.0	3.3.3.3	80000002	337	28	8a47
Summary	192.168.20.0	1.1.1.1	80000002	331	28	d008
Summary	192.168.100.0	3.3.3.3	8000000a	337	28	1167
Summary	192.168.100.0	1.1.1.1	80000017	335	28	294b
AsSummary	2.2.2.2	3.3.3.3	8000000a	337	28	a894
AsSummary	2.2.2.2	1.1.1.1	8000000e	335	28	d26f

Area 2.2.2.2:

Summary	0.0.0.0	1.1.1.1	80000002	1269	28	73e5
---------	---------	---------	----------	------	----	------

External:

AsExternal	192.168.101.0	2.2.2.2	80000002	1174	36	0f6a
AsExternal	192.168.102.0	2.2.2.2	80000002	1174	36	0474

Manager > show ospf lsa area=1.1.1.1 full

Type	LS ID	Router ID	Sequence	Age	Len	Csum
------	-------	-----------	----------	-----	-----	------

Area 1.1.1.1:

Router	1.1.1.1	1.1.1.1	80000005	856	36	2c31
Options: --B Number of links: 1						
Link	1: Type: Transit	ID: 192.168.10.1	Data: 192.168.10.1			
TOS 0 metric: 1 Number of other metrics: 0						
Router	3.3.3.3	3.3.3.3	80000002	865	36	7dd4
Options: --B Number of links: 1						
Link	1: Type: Transit	ID: 192.168.10.1	Data: 192.168.10.254			
TOS 0 metric: 1 Number of other metrics: 0						
Network	192.168.10.1	1.1.1.1	80000001	866	32	f1df
Network Mask: 255.255.255.0						
Attached router: 1.1.1.1						
Attached router: 3.3.3.3						
Summary	172.16.0.0	3.3.3.3	8000000a	379	28	8dfb
Network Mask: 255.255.0.0						
TOS: 0 Metric: 2						
Summary	172.16.0.0	1.1.1.1	80000016	377	28	a7de
Network Mask: 255.255.0.0						
TOS: 0 Metric: 1						
Summary	192.168.20.0	3.3.3.3	80000002	379	28	8a47
Network Mask: 255.255.255.0						
TOS: 0 Metric: 1						
Summary	192.168.20.0	1.1.1.1	80000002	373	28	d008
Network Mask: 255.255.255.0						
TOS: 0 Metric: 2						

Summary	192.168.100.0	3.3.3.3	8000000a	379	28	1167
Network Mask:	255.255.255.0					
TOS:	0	Metric:	2			
Summary	192.168.100.0	1.1.1.1	80000017	377	28	294b
Network Mask:	255.255.255.0					
TOS:	0	Metric:	1			
AsSummary	2.2.2.2	3.3.3.3	8000000a	379	28	a894
Network Mask:	0.0.0.0					
TOS:	0	Metric:	2			
AsSummary	2.2.2.2	1.1.1.1	8000000e	377	28	d26f
Network Mask:	0.0.0.0					
TOS:	0	Metric:	1			

Type	LSA タイプ。Router(ルーター LSA) Network(ネットワーク LSA) Summary (ネットワークサマリー LSA) AsSummary(ASBR サマリー LSA) A s External (AS 外部 LSA) がある。
LS ID	リンク状態 ID。LSA タイプによって意味が異なる (別表参照)
RouterID	LSA 通知ルーター ID
Sequence	LSA シーケンス番号 (32 ビットの符号付き整数)
Age	LSA エイジ (Link State Age) LSA 生成後の推定経過時間 (秒)。最大値は 3600 秒
Len	LSA の長さ (バイト)。LSA ヘッダー 20 バイトを含む
Csum	LSA チェックサム。LSA エイジフィールドを除く。LSA を比較するときに用いられる。

表 52:

Type	LSA タイプ。Router (ルーター LSA) Network (ネットワーク LSA) Summary (ネットワークサマリー LSA) AsSummary (ASBR サマリー LSA) A s External (AS 外部 LSA) がある。
LS ID	リンク状態 ID。LSA タイプによって意味が異なる (別表参照)
Router ID	LSA 通知ルーター ID
Sequence	LSA シーケンス番号 (32 ビットの符号付き整数)
Age	LSA エイジ (Link State Age) LSA 生成後の推定経過時間 (秒)。最大値は 3600 秒
Len	LSA の長さ (バイト)。LSA ヘッダー 20 バイトを含む
Csum	LSA チェックサム。LSA エイジフィールドを除く。LSA を比較するときに用いられる。
Router	ルーター LSA に関する情報
Options	ルーター LSA のオプションフラグ。生成元ルーターの種類を示す。B (ABR) E (ASBR) V (仮想リンクの終端ルーター) - (フラグがセットされていない)

Number of links	LSA 内のリンク数
Link	LSA 内でのリンク番号
Type	リンクタイプ
ID	リンク ID。リンクの対向に位置するルーターの ID またはインターフェースアドレス
Data	リンクデータ。リンクタイプによって意味が異なる。Stub の場合はサブネットマスク、それ以外は LSA を生成したルーターの IP アドレス
TOS 0 metric	デフォルトサービスタイプ (TOS=0) のメトリック
Number of other metrics	サービスタイプ (TOS) 数。デフォルト TOS 以外のメトリックエントリー数
TOS	サービスタイプ (TOS) 別メトリックエントリー
Metric	サービスタイプ (TOS) 別のメトリック値
Network	ネットワーク LSA に関する情報
Network mask	ネットワークマスク
Attached router	該当ネットワークに接続されているルーターの ID
Summary	ネットワークサマリー LSA に関する情報
AsSummary	ASBR サマリー LSA に関する情報
AsExternal	AS 外部 LSA に関する情報
Forward	サービスタイプ別の転送先 IP アドレス。同一ネットワーク上によりよい経路がある場合に使用される。
Tag	外部経路タグ。ASBR 間 (他のルーティングプロトコル間) の通信に使われるもので OSPF では使用しない。

表 53: FULL オプション指定時

LSA タイプ	リンク状態 ID
ルーター LSA (タイプ 1)	LSA を生成したルーターの ID
ネットワーク LSA (タイプ 2)	指名ルーター (DR) の IP アドレス
ネットワークサマリー LSA (タイプ 3)	宛先ネットワークアドレス
ASBR サマリー LSA (タイプ 4)	AS 境界ルーター (ASBR) の ID
AS 外部 LSA (タイプ 5)	宛先ネットワークアドレス

表 54: LSA タイプとリンク状態 ID

SHOW OSPF NEIGHBOUR

カテゴリー：IP / 経路制御 (OSPF)
対象機種：8624、9606

```
SHOW OSPF NEIGHBOUR [=ipadd] [INTERFACE=vlan-if]
```

ipadd: IP アドレス
vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID) または仮想インターフェース (VIRTx)

解説

隣接する OSPF ルーターの情報を表示する。

パラメーター

NEIGHBOUR 隣接ルーターの IP アドレス。指定時は該当隣接ルーターのみ、省略時はすべての隣接ルーターに関する情報が表示される。
INTERFACE IP (VLAN) インターフェース名。指定時は該当インターフェース下に存在する隣接ルーターだけが表示される。

入力・出力・画面例

Manager > show ospf neighbour

IP address	State	Interface	Router ID	Priority	LSRxmtQ	Type
172.16.192.2	full	vlan2	4.4.4.5	1	0	Dyn
192.168.10.1	full	vlan1	1.1.1.1	1	0	Dyn
192.168.10.2	full	vlan1	2.2.2.2	1	0	Dyn
192.168.10.3	full	vlan1	3.3.3.3	1	0	Dyn

IP address	隣接ルーターの IP アドレス
State	隣接ルーター (との通信) の状態。Down (初期状態) Attempt (静的設定された隣接ルーターに Hello を送り、通信を試行中) Init (該当ルーターから Hello を受信したが、まだ通信は片方向) Two-Way (双方向の通信が確立した) ExStart (隣接関係の確立開始) Exchange (DD パケットの交換中) Loading (データベースの同期をとるため LSR パケットで最新情報を要求) Full (隣接関係の完成) のいずれか。

Interface	隣接ルーターが存在するインターフェース
Router ID	隣接ルーターの ID
Priority	隣接ルーターの DR 優先度（隣接ルーターからの Hello パケットで示された値）
LSRetransQ	LSA 再送信キューの長さ
Type	エントリタイプ。Dyn（動的学習したダイナミックエントリー）、Stat（ステティックエントリー）

表 55:

関連コマンド

RESET OSPF COUNTER（180 ページ）

SHOW OSPF RANGE

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

SHOW OSPF RANGE [=ipadd] [AREA={BACKBONE|area-number}]

ipadd: IP アドレス

area-number: OSPF エリア ID (a.b.c.d の形式)

解説

本システム上で定義されているエリアの構成ネットワーク範囲の情報を表示する。

パラメーター

RANGE レンジアドレス。省略時はすべてのレンジが表示される。

AREA OSPF エリア ID。省略時はすべてのエリアが表示される。

入力・出力・画面例

```
Manager > show ospf range
```

Base IP address	State	Mask	Area	Effect
172.16.0.0	Active	255.255.0.0	Backbone	Advertise
192.168.10.0	Active	255.255.255.0	1.1.1.1	Advertise
192.168.20.0	Active	255.255.255.0	2.2.2.2	Advertise
192.168.21.0	Active	255.255.255.0	2.2.2.2	Advertise
192.168.22.0	Active	255.255.255.0	2.2.2.2	Advertise
192.168.100.0	Active	255.255.255.0	Backbone	Advertise

Base IP address	ネットワーク範囲のベースアドレス
State	該当ネットワーク範囲の状態。Active または Inactive。アクティブなエリアに関連付けられているときに Active と表示される
Mask	ネットマスク
Area	所属エリア ID
Effect	該当アドレス範囲の経路情報をネットワークサマリー LSA でエリア外部に通知するかどうか。「Advertise」(通知する)か「Do not advertise」(通知しない)のいずれか。

表 56:

関連コマンド

ADD OSPF RANGE (118 ページ)

DELETE OSPF RANGE (134 ページ)

SET OSPF AREA (204 ページ)

SHOW OSPF ROUTE

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

SHOW OSPF ROUTE[=*ipadd*] [AREA={BACKBONE|*area-number*}] [TYPE={AB|ASBR}]

ipadd: IP アドレス

area-number: OSPF エリア ID (a.b.c.d の形式)

解説

エリア境界ルーター (ABR) および AS 境界ルーター (ASBR) への経路情報を表示する。

パラメーター

ROUTE 経路の宛先となるルーターの ID。「0」によるワイルドカード指定も可能で、「172.16.0.0」のように指定すると「172.16」ではじまるすべてのルーター ID にマッチする。省略時はすべての経路が表示される。

AREA エリア ID。省略時はすべてのエリアが対象となる。

TYPE 経路の種類。AB は ABR への経路、ASBR は ASBR への経路だけを表示する。省略時はすべての経路が表示される。

入力・出力・画面例

Manager > show ospf route					
OSPF Routes					
Destination DLCI/Circ.	Mask Type	Policy	NextHop Protocol	Interface Metrics	Age Preference

Area backbone AB routes:					
3.3.3.3	255.255.255.255		0.0.0.0	vlan10	0
-	ospfAB	0	ospf	1	10
Area 1.1.1.1 AB routes:					
3.3.3.3	255.255.255.255		192.168.10.254	vlan10	0
-	ospfAB	0	ospf	1	10
ASBR routes:					
2.2.2.2	255.255.255.255		192.168.100.254	vlan100	0
-	ospfAS	0	ospf	1	10

Destination	ABR/ASBR のルーター ID
DLCI/Circ.	フレームリレー/X.25T の論理チャンネル
Mask	ルートマスク。常に 255.255.255.255
Type	経路エントリタイプ。ospfAB (ABR への経路)、ospfAS (ASBR への経路) のいずれか。
Policy	ルーティングポリシー。常に 0
NextHop	ネクストホップルーター。宛先に直接到達できる場合は 0.0.0.0
Protocol	経路情報のソースプロトコル。常に ospf
Interface	同経路宛てのパケットを送出するインターフェース
Metrics	メトリック
Age	経路情報の年齢 (秒)
Preference	送出時の優先度。エリア内の経路は 10、エリアをまたぐ経路は 11。

表 57:

関連コマンド

SHOW OSPF AREA (253 ページ)

SHOW OSPF INTERFACE (260 ページ)

SHOW OSPF RANGE (270 ページ)

SHOW OSPF STUB

カテゴリー：IP / 経路制御 (OSPF)

対象機種：8624、9606

SHOW OSPF STUB[=*ipadd*] [AREA={BACKBONE|*area-number*}]

ipadd: IP アドレス

area-number: OSPF エリア ID (a.b.c.d の形式)

解説

OSPF を使用していないネットワーク (スタブネットワーク) へのスタティックな経路情報を表示する。

パラメーター

STUB スタブネットワークのネットワークアドレス

AREA OSPF エリア ID

入力・出力・画面例

```
Manager > show ospf stub
```

IP address	Mask	State	Area	Metric	TOS	Type
192.168.10.100	255.255.255.255	Active	Backbone	1	0	Stat

IP address	スタブネットワークのネットワークアドレス
Mask	ネットマスク
State	経路エントリーの状態。Active または Inactive。Active なエントリーはルーター LSA で通知される。
Area	所属エリア ID
Metric	メトリック
TOS	サービスタイプ (TOS)
Type	エントリータイプ。Stat (スタティックエントリー) Dyn (ダイナミックエントリー) のどちらか。

表 58:

関連コマンド

ADD OSPF STUB (120 ページ)

DELETE OSPF STUB (135 ページ)

SET OSPF STUB (210 ページ)

SHOW PING

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

SHOW PING

解説

PING コマンドのデフォルト設定、および、実行中あるいは前回の PING に関する情報を表示する。

入力・出力・画面例

```
Manager > show ping

Ping Information
-----
Defaults:
Type ..... -
Source ..... Undefined
Destination ..... Undefined
Number of packets ..... 5
Size of packets (bytes) ..... 24
Timeout (seconds) ..... 1
Delay (seconds) ..... 1
Data pattern ..... Not set
Type of service ..... 0
Direct output to screen ..... Yes

Current:
Type ..... IP
Source ..... 172.16.28.160
Destination ..... 172.16.28.1
Number of packets ..... 5
Size of packets (bytes) ..... 24
Timeout (seconds) ..... 1
Delay (seconds) ..... 1
Data pattern ..... Not set
Type of service ..... 0
Direct output to screen ..... Yes

Results:
Ping in progress ..... No
Packets sent ..... 5
Packets received ..... 5
Round trip time minimum (ms) .. 0
Round trip time average (ms) .. 0
```

```
Round trip time maximum (ms) .. 0
Last message ..... Finished succesfully
-----
```

Type	ネットワーク層プロトコル (IP)
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
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 59:

関連コマンド

PING (171 ページ)

SET PING (211 ページ)

STOP PING (284 ページ)

SHOW TCP

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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 60: 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 ($2 \times \text{MSL}$) 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 61: 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 62: コネクション番号指定時

関連コマンド

DELETE TCP (136 ページ)

SHOW IP COUNTER (220 ページ)

SHOW IP UDP (250 ページ)

SHOW TRACE

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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 63:

関連コマンド

SET TRACE (212 ページ)

STOP TRACE (285 ページ)

TRACE (286 ページ)

STOP PING

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

STOP PING

解説

実行中の PING を停止する

関連コマンド

PING (171 ページ)

SET PING (211 ページ)

SHOW PING (276 ページ)

STOP TRACE

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

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 (212 ページ)

SHOW TRACE (282 ページ)

TRACE (286 ページ)

TRACE

カテゴリー：IP / 一般コマンド

対象機種：8624、9606

```
TRACE [[ IPADDRESS=] ipadd] [MAXTTL=1..255] [MINTTL=1..255]
      [NUMBER=1..100] [PORT=port] [SCREENOUTPUT={YES|NO}] [SOURCE=ipadd]
      [TIMEOUT=0..65535] [TOS=0..255]
```

ipadd: IP アドレス

port: UDP ポート番号 (0~65535)

解説

指定したアドレスまでの経路をトレースする。

指定しなかったパラメーターについては、SET TRACE コマンドで設定したデフォルト値が用いられる。

パラメーター

IPADDRESS 宛先 IP アドレス

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

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 (212 ページ)

SHOW TRACE (282 ページ)

STOP TRACE (285 ページ)

付録

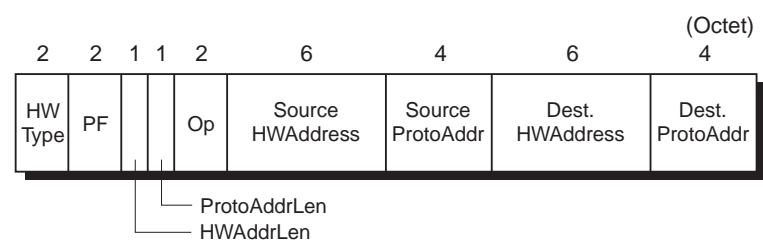
ARP (Address Resolution Protocol)

IP アドレスから物理アドレス (MAC アドレス) を調べるためのプロトコル。データリンクフレームを直接利用して送信されます。Ethernet プロトコルタイプは 0806 (ARP) \ 8035 (RARP) です。

RFC826, An Ethernet Address Resolution Protocol

RFC903, A Reverse Address Resolution Protocol

ARP パケットのフォーマット



フィールド	オクテット長	内容
HW Type	2	ハードウェアタイプ。データリンクの種類を示す。Ethernet は 1
PF	2	プロトコルファミリー。IP は 0x0800
HWAddrLen	1	ハードウェアアドレス長。データリンクアドレス (MAC アドレス) の長さ (オクテット) を示す。Ethernet は 6 オクテット。
ProtoAddrLen	1	プロトコルアドレス長。IP は 4 オクテット。
Op	2	オペレーションコード。1=Request(ARP 要求) 2=Reply(ARP 応答)。3 と 4 は別プロトコル RARP (Ethernet プロトコルタイプ 0x8035) のメッセージで 3=Request Reverse (RARP 要求) 4=Reply Reverse (RARP 応答)
Source HWAddress	6	送信元 MAC アドレス。
Source ProtoAddr	4	送信元 IP アドレス。
Dest. HWAddress	6	宛先 MAC アドレス。Request ではそもそも不明なので 0 または前回使ったバッファの内容が入る。Request の受信側はこのフィールドを無視する。
Dest. ProtoAddr	4	宛先 IP アドレス。Request では解決対象の IP アドレスが入る。

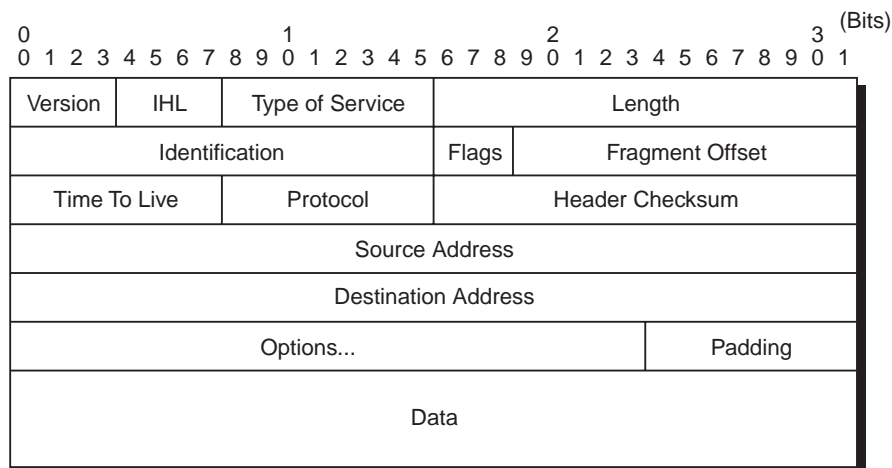
表 64:

IP (Internet Protocol)

インターネットワーク上のノード間でのパケット配送をつかさどるコネクションレス型のネットワーク層プロトコル。

RFC791, INTERNET PROTOCOL

IP データグラムのフォーマット



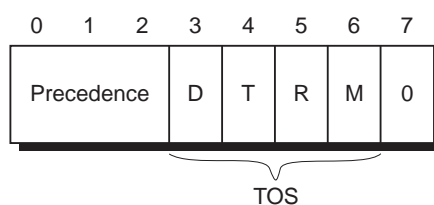
フィールド	ビット長	内容
Ver (Version)	4	IP プロトコルのバージョン番号。IPv4 では 4
IHL (Internet Header Length)	4	IP ヘッダー部分の長さ。32 ビットワード単位で表す。最小値は 5 ワード (20 オクテット)。オプションフィールドが含まれる場合はこれよりも長くなる。最大値は 15 ワード (60 オクテット)
TOS (Type of Service)	8	サービスタイプ。3 ビットの優先度 (precedence) フィールドと、4 ビットの (狭い意味での) TOS フィールド、1 ビットの未使用フィールドからなる。TOS フィールドは、遅延 (Delay)、スルーブット (T)、信頼性 (R)、金銭コスト (M) に対する要求を示すビットフラグ 4 つからなる。
Len (Total Length)	16	データグラムの全長 (ヘッダー+データ)。オクテット単位で表す。16 ビットなので最大値は 65535。すべての IP ホストは、少なくとも 576 オクテットまでのデータグラムを受け取れなくてはならない。
Id (Identification)	16	データグラムを識別するための番号 (ID)
Flags	3	フラグメント制御フラグ。Flags フィールドのフォーマットを参照。

Fragment Offset	13	フラグメントオフセット。データ部分がフラグメント内のどの位置に属するかを示す。64 ビット (8 オクテット) を 1 単位として表す。
TTL (Time to Live)	8	データグラムの生存期間。単位は秒だが、現実には単なるホップカウントとして扱われている。ルーターを経由するごとに (少なくとも) 1 ずつ減算される。0 になった場合は破棄される。
Protocol	8	上位プロトコル番号。おもな IP プロトコル番号を参照
Header Checksum	16	ヘッダー部分のチェックサム。各ルーターで再計算される (TTL が減算されるため)
Source Address	32	始点 IP アドレス。ユニキャストアドレスでなくてはならない。
Destination Address	32	終点 IP アドレス。ユニキャスト、マルチキャスト、ブロードキャストアドレスが入る。
Options	可変	オプションフィールド
Padding	可変	パディング。ヘッダー長が 32 ビットの整数倍になるように調整するためのもの。0~3 オクテットの可変長。
Data	可変	データ

表 65:

TOS (Type of Service) フィールドのフォーマット

RFC1349, Type of Service in the Internet Protocol Suite



フィールド/フラグ名	ビット長	内容
Precedence	3	データグラムの優先度。0 (低) ~ 7 (高) で示す。
D (Delay)	1	遅延フラグ。1 のときは少ない遅延で送信することを示す。
T (Throughput)	1	スループットフラグ。1 のときは高スループットを確保することを示す。
R (Reliability)	1	信頼性フラグ。1 のときは高い信頼性を与えることを示す。
M (Monetary Cost)	1	金銭的成本フラグ。1 のときは金銭的成本を最小限に抑えることを示す。

0 (not used)	1	未使用。常に 0 (MBZ=Must Be Zero)
----------------	---	-------------------------------

表 66:

値	定義
8 (1000)	遅延最小
4 (0100)	スループット最大
2 (0010)	信頼性最大
1 (0001)	金銭的成本最小
0 (0000)	通常サービス

表 67: RFC1349 による TOS フィールドの定義

値	定義
7 (111)	Network Control
6 (110)	Internetwork Control
5 (101)	CRITIC/ECP
4 (100)	Flash Override
3 (011)	Flash
2 (010)	Immediate
1 (001)	Priority
0 (000)	Routine

表 68: RFC791 による優先度フィールドの定義

Flags フィールドのフォーマット



フラグ名	ビット長	内容
0 (not used)	1	未使用。常に 0 (MBZ=Must Be Zero)
DF (Don't Fragment)	1	1 のとき、このデータグラムをフラグメント化 (分割) してはならないことを示す。
MF (More Fragments)	1	1 のとき、後続するフラグメントがあることを示す。フラグメント化されていないデータグラムおよび最終フラグメントでは 0 になる。

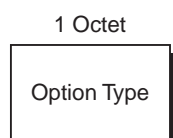
表 69:

IP オプション

番号	オクテット長	クラス	オプションタイプ	内容
0	-	0	0	オプションリスト終了 (End of Option list)。オプションリストの最後に置かれる。1 オクテットのみで長さフィールド以降はない
1	-	0	1	NOOP (No Operation)。次のオプションフィールドを 32 ビット境界に揃えるため、オプションフィールドの間に置かれる。1 オクテットのみで長さフィールド以降はない。
2	11	0	130	セキュリティー (Security)
3	可変	0	131	ルーズソースルーティング (Loose Source Routing)。緩い始点経路制御。オプションデータに経由するアドレスを列挙する。経路の途中で指定外のルーターが使われてもよい。
4	可変	2	68	インターネットタイムスタンプ (Internet Timestamp)。データグラムが通った経路上のルーターで時刻を記録する。
7	可変	0	7	レコードルート (Record Router)。データグラムが通った経路をルーターに記録させるためのオプション。
8	4	0	136	Stream ID。現在は使用されていない。
9	可変	0	138	ストリクトソースルーティング (Strict Source Routing)。厳密な始点経路制御。オプションデータ部に列挙されたルーターだけを使って配送するよう指示する。

表 70: IP オプション一覧

オプションタイプオクテットのための固定長フォーマット



オプションタイプ、オプション長、オプションデータからなる可変長フォーマット

1 Octet	1 Octet	Variable
Option Type	Option Length	Option Data...

フィールド	オクテット長	内容
Option Type	1	オプションタイプ。オプションの種類を示す。別表を参照
Option Length	1	オプション長。オプションフィールド全体（オプションタイプ、オプション長、オプションデータ）の長さ（オクテット）
Option Data	可変	オプションデータ。オプション本体

表 71:

オプションタイプ（Option Type）オクテットのフォーマット

0	1	2	3	4	5	6	7
Copied	Option Class		Option Number				

フィールド	オクテット長	内容
Copied	1	コピーフラグ。フラグメント化時にすべてのフラグメントにこのオプションをコピーすべきかどうか。1 ならコピーする、0 ならコピーしない。
Option Class	2	オプションクラス。0（コントロールオプション）、2（デバッグオプション）がある。オプション番号によってどちらを使うが決まっている。
Option Number	5	オプション番号。別表を参照

表 72:

おもな IP プロトコル番号

RFC1700, ASSIGNED NUMBERS

RFC2893, Transition Mechanisms for IPv6 Hosts and Routers

<http://www.iana.org/assignments/protocol-numbers>

1	ICMP (Internet Control Message Protocol) RFC792
2	IGMP (Internet Group Management Protocol) RFC2236
4	IP in IP
6	TCP (Transmission Control Protocol) RFC793
8	EGP (Exterior Gateway Protocol) RFC888
9	各種の内部ゲートウェイプロトコル (IGP)
17	UDP (User Datagram Protocol) RFC768
41	IPv6 (IPv6-over-IPv4 トンネリング)
46	RSVP (Reservation Protocol)
47	GRE (General Routing Encapsulation)
89	OSPF (Open Shortest Path First)
103	PIM (Protocol Independent Multicast)
112	VRRP (Virtual Router Redundancy Protocol)

表 73:

ICMP (Internet Control Message Protocol)

IP ネットワークにおいて、エラーの通知や制御情報のやりとり（要求/応答）に使用されるプロトコル。IP を利用して配送されます。IP プロトコル番号は 1。ICMP のエラーに対する ICMP メッセージは生成されません。

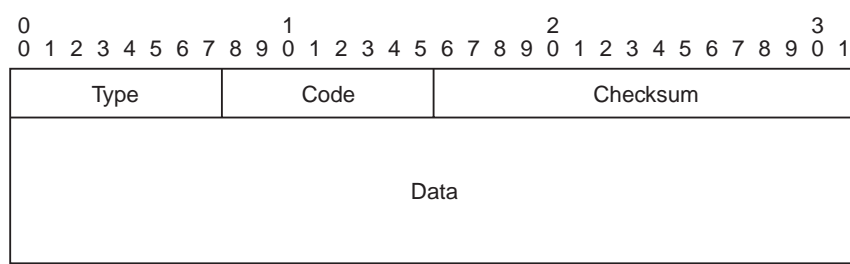
RFC792, INTERNET CONTROL MESSAGE PROTOCOL

RFC950, Internet Standard Subnetting Procedure

RFC1256, ICMP Router Discovery Messages

RFC1700, Assigned Numbers

ICMP メッセージの基本フォーマット



フィールド	ビット長	内容
Type	8	メッセージタイプ
Code	8	サブコード。特定タイプのメッセージの内容をさらに細かく分類したもの
Checksum	16	チェックサム
Data	可変	データ。フォーマットはメッセージタイプによって異なる

表 74:

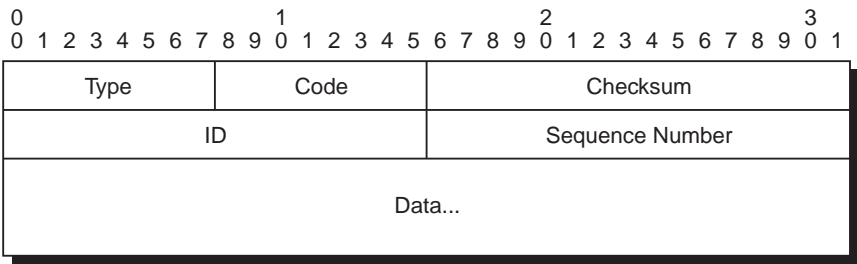
タイプ	名称	内容
0	Echo Reply (エコー応答)	Echo (エコー要求) メッセージ (タイプ 8) に対する応答。
3	Destination Unreachable (宛先到達不可能)	指定された宛先に到達できないことを示す。
4	Source Quench (送信抑制要求)	送信元に対してデータグラムの送信レートを落とすよう要求する。受信側の処理能力を上回る速度でデータグラムが送られてきたときに送信される。
5	Redirect (経路変更要求)	指定された宛先へのよりよい経路が存在することを送信元に伝える。
8	Echo (エコー要求)	相手側に Echo Reply (エコー応答) を要求する。PING コマンドなどの診断用に使われることが多い。
9	Router Advertisement (ルーター広告)	ルーターが自らの IP アドレスをホストに通知するためのメッセージ。本メッセージタイプを実装したルーターは各インターフェースから定期的にこのメッセージをリンクローカルな全システムマルチキャストアドレス (224.0.0.1) 宛てに送信する。また、ホストから Router Solicitation (ルーター要請) メッセージを受け取ったときにもこのメッセージで応答する。
10	Router Solicitation (ルーター要請)	ホストが自ネットワーク上のルーターを探すためのメッセージ。リンクローカル全ルーターマルチキャストアドレス (224.0.0.2) に送信される。
11	Time Exceeded (時間超過)	ルーターにおいてパケットの TTL がゼロになった、あるいは、ホストが一定時間内にフラグメントを再構成できなかったことを示す。
12	Parameter Problem (パラメーター異常)	IP ヘッダーにエラーがあったためデータグラムを破棄したことを示す。
13	Timestamp (タイムスタンプ要求)	相手側に時刻情報 (本メッセージの受信時刻と返信時刻) を要求する。往復時間と相手のシステム負荷を測定するためなどに使われる。
14	Timestamp Reply (タイムスタンプ応答)	Timestamp (タイムスタンプ要求) メッセージ (タイプ 13) に対する応答。
15	Information Request (情報要求)	ホストが自分の IP アドレスを知るために使用するメッセージ。
16	Information Reply (情報応答)	Information Request (情報要求) メッセージ (タイプ 15) に対する応答。要求元ホストに IP アドレスを教える。
17	Address Mask Request (アドレスマスク要求)	ホストがサブネットマスクを知るために使用するメッセージ。

18	Address Mask Reply	Address Mask Request (アドレスマスク要求) メッセージ (タイプ (アドレスマスク応答) 17) に対する応答。要求元ホストにサブネットマスクを教える。
----	--------------------	---

表 75: ICMP メッセージ一覧

Echo Reply (タイプ 0)

Echo (エコー要求) メッセージ (Type 8) に対する応答。Echo メッセージの ID、シーケンス番号、データをそのまま送り返す。ホストとルーターの両方が使用する。

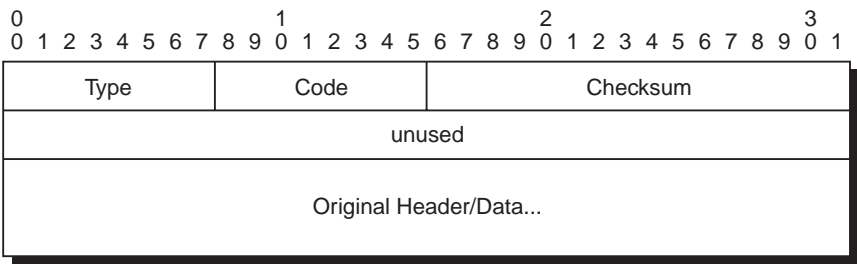


フィールド	ビット長	内容
Type	8	0
Code	8	0
Checksum	16	チェックサム
ID	16	識別子 (ID)。要求と応答をつきあわせるための番号
Sequence Number	16	シーケンス番号。要求と応答をつきあわせるための番号。
Data	可変	任意のデータ。Echo (エコー要求) で送られてきたデータをそのまま送り返す。

表 76:

Destination Unreachable (タイプ 3)

指定された宛先に到達できないことを示す。サブコードにより、より詳細な理由が示される。



フィールド	ビット長	内容
Type	8	3
Code	8	別表参照
Checksum	16	チェックサム
unused	32	未使用。すべて 0
Original Header/Data	可変	オリジナルの IP ヘッダー + データの先頭 64 ビット

表 77:

コード	名称	内容	送信者
0	net unreachable	ネットワーク到達不可能。宛先ネットワークへの経路が無効、あるいは経路がないことを示す	ルーター
1	host unreachable	ホスト到達不可能。宛先ホストの所属ネットワークのルーターが、ホストがダウンしていることを知っている場合などに返す	ルーター
2	protocol unreachable	プロトコル到達不可能。指定された上位プロトコルを扱うルーチンが存在しないことを示す	ホスト
3	port unreachable	ポート到達不可能。指定された TCP/UDP ポートがオープンされていないことを示す	ホスト
4	fragmentation needed and DF set	フラグメント化不可能。フラグメント化が必要だが、DF (フラグメント化不可) ビットが立っているためデータグラムを破棄したことを示す	ルーター
5	source route failed	始点経路制御失敗。始点経路制御が無効、あるいは失敗したことを示す	ルーター

表 78:

Source Quench (タイプ 4)

送信元に対してデータグラムの送信レートを落とすよう要求するフロー制御メッセージ。受信側の処理能力を上回る速度でデータグラムが送られてきたためにバッファがあふれ、データグラムを破棄したことを示す。ホスト、ルーターの両方が返す。

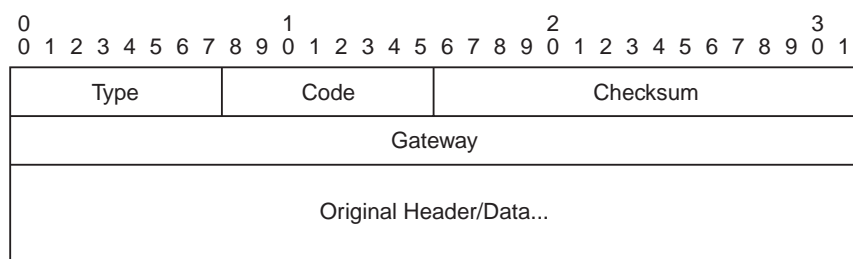
										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
Type										Code										Checksum																			
unused																																							
Original Header/Data...																																							

フィールド	ビット長	内容
Type	8	4
Code	8	0
Checksum	16	チェックサム
unused	32	未使用。すべて 0
Original Header/Data	可変	オリジナルの IP ヘッダー + データの先頭 64 ビット

表 79:

Redirect (タイプ 5)

指定された宛先へのよりよい経路が存在することを送信元に伝えるメッセージ。送信元に対し、同じ宛先へのデータグラムを Gateway フィールドで指定した IP アドレスに送るよう要求する。オリジナルのデータグラム自体は Gateway に転送される。



フィールド	ビット長	内容
Type	8	5
Code	8	別表参照
Checksum	16	チェックサム
Gateway	32	同じ宛先へのデータグラム送信時に使用すべきゲートウェイの IP アドレス
Original Header/Data	可変	オリジナルの IP ヘッダー + データの先頭 64 ビット

表 80:

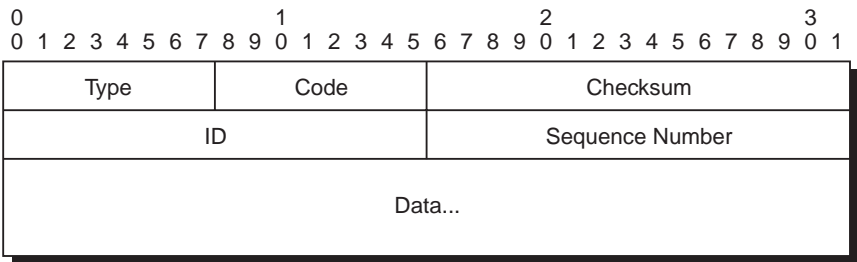
コード	名称	内容	送信者
0	Redirect datagrams for the Network	ネットワークへの経路変更要求	ルーター
1	Redirect datagrams for the Host	ホストへの経路変更要求	ルーター
2	Redirect datagrams for the Type of Service and Network	ネットワークへの経路変更要求(指定サービスタイプを持つデータグラムに関してのみ)	ルーター

3	Redirect datagrams for the Type of Service and Host	ホストへの経路変更要求（指定サービスタイプを持つデータグラムに関してのみ）	ルーター
---	---	---------------------------------------	------

表 81:

Echo（タイプ 8）

相手側に Echo Reply（エコー応答）を要求する。PING コマンド（171 ページ）などで診断用に使われることが多い。ホストとルーターの両方が使用する。



フィールド	ビット長	内容
Type	8	8
Code	8	0
Checksum	16	チェックサム
ID	16	識別子（ID）。要求と応答をつきあわせるための番号
Sequence Number	16	シーケンス番号。要求と応答をつきあわせるための番号。
Data	可変	任意のデータ。受信側は Echo Reply でデータ部分をそのまま送り返す。

表 82:

Router Advertisement（タイプ 9）

ルーターが自らの IP アドレスをホストに通知するためのメッセージ。本メッセージタイプを実装したルーターは各インターフェースから定期的にこのメッセージをリンクローカル全システムマルチキャストアドレス（224.0.0.1）に送信する。また、ホストから Router Solicitation（ルーター要請）メッセージを受け取ったときにもこのメッセージで応答する。

0										1										2										3																					
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Type										Code										Checksum																															
Num Addr										Addr Entry Size										Lifetime																															
Router Address[1]																																																			
Preference Level[1]																																																			
Router Address[2]																																																			
Preference Level[2]																																																			
.....																																																			

フィールド	ビット長	内容
Type	8	9
Code	8	0
Checksum	16	チェックサム
Num Addr	8	このメッセージに含まれるルーターアドレスの数
Addr Entry Size	8	各アドレスエントリー (Router Address[n] と Preference Level[n]) の大きさ (32 ビット=1 ワードとした場合のワード数)。IPv4 では 2 ワード (64 ビット)。
Lifetime	16	本メッセージで通知されるアドレスの有効期限 (秒)。
Router Address[n]	32	ルーターアドレス。ルーターインターフェースの IP アドレス。
Preference Level[n]	32	該当するルーターアドレス (Router Address[n]) の優先度。符号付きの 2 の補数表現。大きいほど優先度が高い。

表 83:

Router Solicitation (タイプ 10)

ホストが自ネットワーク上のルーターを探すためのメッセージ。リンクローカル全ルーターマルチキャストアドレス (224.0.0.2) に送信され、Router Advertisement (ルーター広告) メッセージ (タイプ 9) による応答を依頼する。

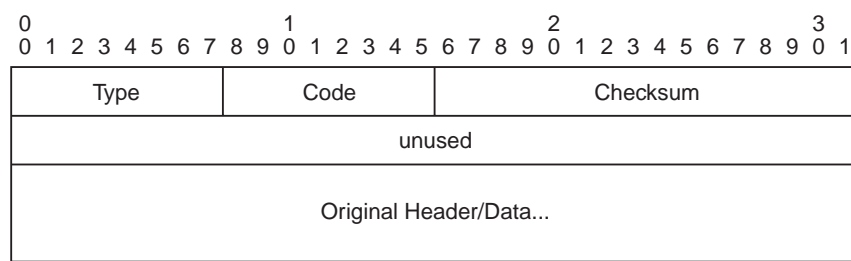
0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
Type										Code										Checksum																			
Reserved																																							

フィールド	ビット長	内容
Type	8	10
Code	8	0
Checksum	16	チェックサム
Reserved	32	予約済み。すべて 0 に設定される。

表 84:

Time Exceeded (タイプ 11)

ルーターにおいてパケットの TTL がゼロになった、あるいは、ホストが一定時間内にフラグメントを再構成できなかったことを示す。



フィールド	ビット長	内容
Type	8	11
Code	8	別表参照
Checksum	16	チェックサム
unused	32	未使用。すべて 0
Original Header/Data	可変	オリジナルの IP ヘッダー + データの先頭 64 ビット

表 85:

コード	名称	内容	送信者
0	time to live exceeded in transit	生存時間 (TTL) 超過。生存時間フィールドの値がゼロになったため、データグラムを転送せずに破棄したことを示す	ルーター
1	fragment reassembly time exceeded	フラグメント再構成時間超過。先頭フラグメントを受信してから一定時間の間にすべてのフラグメントを受信できなかったため、これまでに受信したフラグメントをすべて破棄したことを示す。このメッセージは先頭フラグメントに対してのみ送られる	ホスト

表 86:

Parameter Problem (タイプ 12)

IP ヘッダーにエラーがあったためデータグラムを破棄したことを示す。

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
Type	Code	Checksum	
Pointer	unused		
Original Header/Data...			

フィールド	ビット長	内容
Type	8	12
Code	8	別表参照
Checksum	16	チェックサム
Pointer	8	オリジナル IP ヘッダーの何オクテット目にエラーがあったかを示す。先頭オクテットを 0 とする。
unused	24	未使用。すべて 0
Original Header/Data	可変	オリジナルの IP ヘッダー + データの先頭 64 ビット

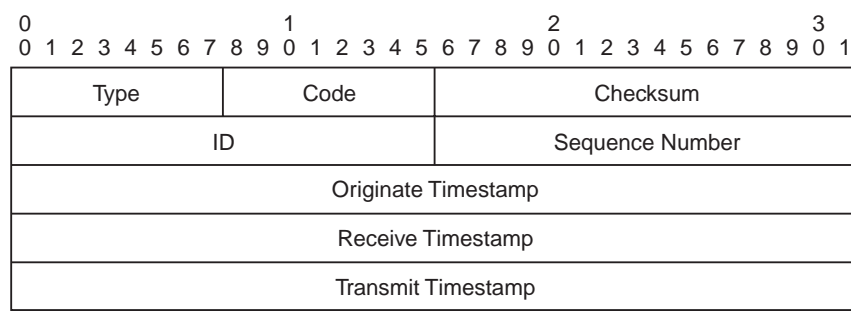
表 87:

コード	名称	内容	送信者
0	pointer indicates the error	オリジナルの IP ヘッダーにエラーがあったことを示す。Pointer フィールドがエラーのあったオクテットを示している	ホスト、ルーター

表 88:

Timestamp (タイプ 13)

相手側に時刻情報（本メッセージの受信時刻と返信時刻）を要求する。往復時間と相手のシステム負荷を測定するためなどに使われる。ホストとルーターの両方が使用する。



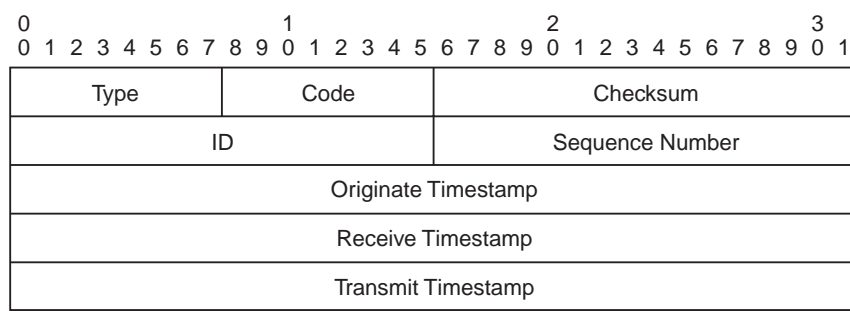
フィールド	ビット長	内容
Type	8	13
Code	8	0
Checksum	16	チェックサム
ID	16	識別子 (ID)。要求と応答をつきあわせるための番号
Sequence Number	16	シーケンス番号。要求と応答をつきあわせるための番号。
Originate Timestamp	32	タイムスタンプ要求メッセージの送信時刻。UTC 深夜からの経過時間をミリ秒単位で示したもの。要求メッセージの送信側が送信直前に書き込む。
Receive Timestamp	32	タイムスタンプ要求メッセージの受信時刻。応答メッセージの送信者が書き込む。
Transmit Timestamp	32	タイムスタンプ応答メッセージの送信時刻。応答メッセージの送信者が送信直前に書き込む。

表 89:

- ＼ UTC からの経過ミリ秒を得られない場合、各タイムスタンプフィールドには任意の時刻情報を入れることができる。その際、標準外のフォーマットであることを示すために、各フィールドの最上位ビットを 1 にする。

Timestamp Reply (タイプ 14)

Timestamp (タイムスタンプ要求) メッセージ (Type 13) に対する応答。要求メッセージの受信時刻と応答メッセージの返信時刻を UTC (協定世界時) 深夜からの経過時間をミリ秒単位で示す。ホストとルーターの両方が使用する。



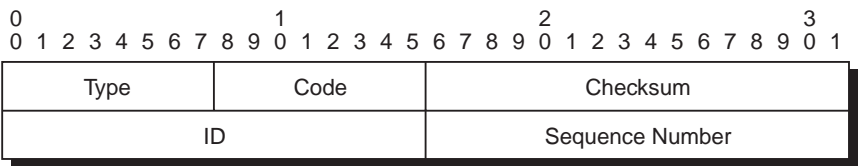
フィールド	ビット長	内容
Type	8	14
Code	8	0
Checksum	16	チェックサム
ID	16	識別子 (ID)。要求と応答をつきあわせるための番号
Sequence Number	16	シーケンス番号。要求と応答をつきあわせるための番号。
Originate Timestamp	32	タイムスタンプ要求メッセージの送信時刻。UTC 深夜からの経過時間をミリ秒単位で示したもの。要求メッセージの送信側が送信直前に書き込む。
Receive Timestamp	32	タイムスタンプ要求メッセージの受信時刻。応答メッセージの送信者が書き込む。
Transmit Timestamp	32	タイムスタンプ応答メッセージの送信時刻。応答メッセージの送信者が送信直前に書き込む。

表 90:

- 、 UTC からの経過ミリ秒を得られない場合、各タイムスタンプフィールドには任意の時刻情報を入れることができる。その際、標準外のフォーマットであることを示すために、各フィールドの最上位ビットを 1 にする。

Information Request (タイプ 15)

ホストが自分の IP アドレスを知るために使用するメッセージ。送信側は、IP データグラムの始点・終点 IP アドレスにゼロ（このネットワーク）をセットして本メッセージを送信する。応答側は始点に自分のアドレス、終点に要求側の正式な IP アドレスをセットして Information Reply メッセージ（タイプ 16）を返送する。ホストとルーターの両方が使用する。

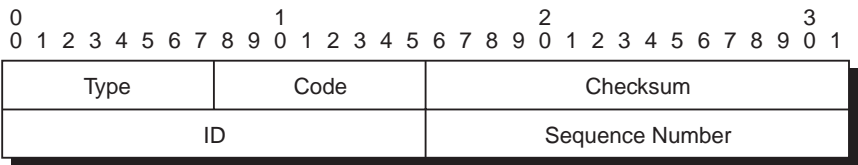


フィールド	ビット長	内容
Type	8	15
Code	8	0
Checksum	16	チェックサム
ID	16	識別子 (ID)。要求と応答をつきあわせるための番号
Sequence Number	16	シーケンス番号。要求と応答をつきあわせるための番号。

表 91:

Information Reply (タイプ 16)

ホストが自分の IP アドレスを知るために使用するメッセージ。送信側は、IP データグラムの始点・終点 IP アドレスにゼロ (このネットワーク) をセットして本メッセージを送信する。応答側は始点に自分のアドレス、終点に要求側の正式な IP アドレスをセットして Information Reply メッセージ (タイプ 16) を返送する。ホストとルーターの両方が使用する。

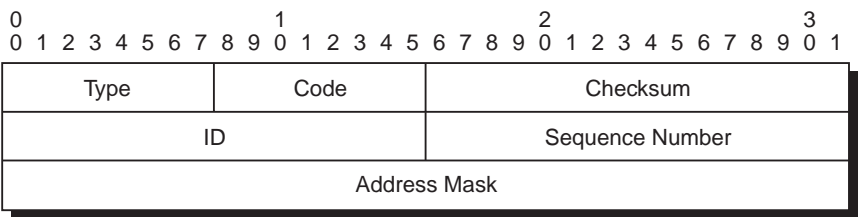


フィールド	ビット長	内容
Type	8	16
Code	8	0
Checksum	16	チェックサム
ID	16	識別子 (ID)。要求と応答をつきあわせるための番号
Sequence Number	16	シーケンス番号。要求と応答をつきあわせるための番号。

表 92:

Address Mask Request (タイプ 17)

ホストがサブネットマスクを知るために使用するメッセージ。

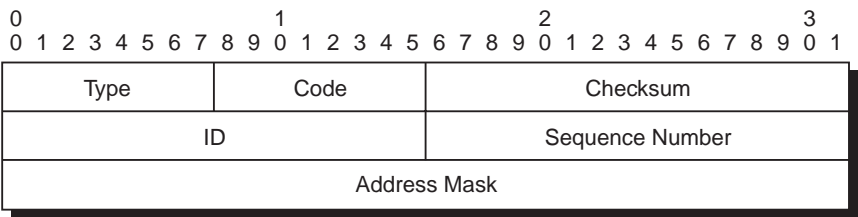


フィールド	ビット長	内容
Type	8	17
Code	8	0
Checksum	16	チェックサム
ID	16	識別子 (ID)。要求と応答をつきあわせるための番号
Sequence Number	16	シーケンス番号。要求と応答をつきあわせるための番号。
Address Mask	32	サブネットマスク。要求時は 0。

表 93:

Address Mask Reply (タイプ 18)

Address Mask Request (アドレスマスク要求) メッセージ (タイプ 17) に対する応答。要求元ホストにサブネットマスクを教える。



フィールド	ビット長	内容
Type	8	18
Code	8	0
Checksum	16	チェックサム
ID	16	識別子 (ID)。要求と応答をつきあわせるための番号
Sequence Number	16	シーケンス番号。要求と応答をつきあわせるための番号。
Address Mask	32	サブネットマスク

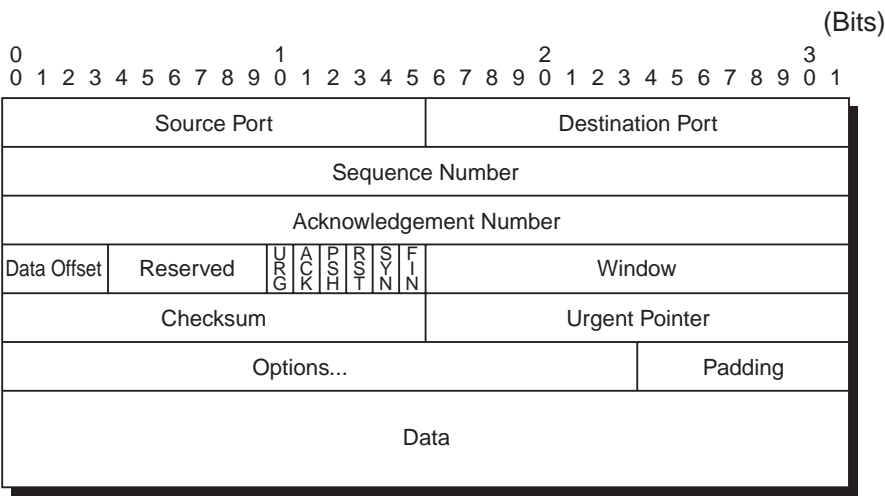
表 94:

TCP (Transmission Control Protocol)

IP ネットワーク上のプロセス間で信頼性のあるコネクション型全二重通信を提供するプロトコル。IP プロトコル番号は 6。

RFC793, TRANSMISSION CONTROL PROTOCOL

TCP セグメントのフォーマット



フィールド	ビット長	内容
Source Port	16	始点ポート。送信元ホスト上のプロセスを示す。
Destination Port	16	終点ポート。宛先ホスト上のプロセスを示す
Sequence Number	32	シーケンス番号。データ (Data) の先頭オクテットのシーケンス番号。Syn フラグがセットされているとき (コネクション開始時) は、ISN (初期シーケンス番号) という値が選択され、このフィールドにセットされる。コネクション確立後の最初のデータオクテットのシーケンス番号は ISN+1 となる。
Acknowledgement Number	32	応答確認番号。このセグメントの送信者が次に受け取ると期待しているセグメントのシーケンス番号。応答確認番号より前のオクテットをすべて受信したことを示す。
Data Offset	4	データオフセット。TCP セグメントヘッダーの長さ。32 ビットワード単位で表す。
Reserved	6	未使用 (常に 0)

URG	1	Urgent (緊急) フラグ。Urgent Pointer フィールドが指し示す位置に緊急データ (制御コードなど) が置かれていることを示す。
ACK	1	Acknowledgement (応答確認) フラグ。Acknowledgement Number が有効であり、受信セグメントに対する応答確認を含むことを示す。
PSH	1	Push (プッシュ) フラグ。可能な限り早く終点ポート番号で示した上位プロセスにデータを渡すよう指示する。対話型アプリケーションのように小さなデータを断続的に送信するような場合に使用される。
RST	1	Reset (リセット) フラグ。コネクションをリセット (強制切断) するよう要求する。RST フラグのセットされたセグメントを受信した側はただちにコネクションを切断しなくてはならない。
SYN	1	Synchronize (同期) フラグ。コネクション確立時にのみ使用されるもので、Sequence Number フィールドに ISN (初期シーケンス番号) が入っていることを相手側に伝える。コネクション確立要求を受け入れる側は、ただちに ISN に対する応答確認を送る。
FIN	1	Finish (終了) フラグ。セグメントの送信者にもはや送るべきデータがないことを示す。FIN フラグを送った側も受信は継続するため、片側が FIN を送った段階でコネクションは単方向になる。
Window	16	セグメントの送信者が受信可能なデータ量 (受信ウィンドウサイズ) を示す。このデータ量は、Acknowledgement フィールドが示すオクテットを起点として数える。
Checksum	16	チェックサム。
Urgent Pointer	16	緊急ポインター。URG フラグがセットされている場合にのみ有効。受信側が一番最初に処理すべきデータ (制御コードなど) の格納位置を、Sequence Number フィールドが示すオクテットからのオフセット (オクテット単位) であらわす。
Options	可変	オプションフィールド
Padding	可変	パディング。ヘッダー長が 32 ビットの整数倍になるように調整するためのもの。1~3 オクテットの可変長。
Data	可変	データ

表 95:

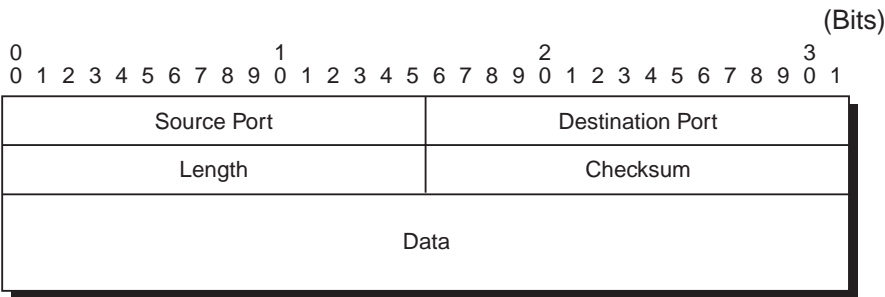
UDP (User Datagram Protocol)

IP ネットワーク上のプロセス間でベストエフォート型のコネクションレストランザクション機能を提供す

るプロトコル。わずか 8 オクテットのシンプルなヘッダーにより、オーバーヘッドの少ない通信を可能にする。IP プロトコル番号は 17。

RFC768, User Datagram Protocol

UDP データグラムのフォーマット



フィールド	ビット長	内容
Source Port	16	始点ポート（オプション）。送信元ホスト上のプロセスを示す。使用しないときは 0 が入る。
Destination Port	16	終点ポート。宛先ホスト上のプロセスを示す
Length	16	データグラム長（オクテット）。UDP ヘッダー + データ（Data フィールド）の長さ。最小は 8
Checksum	16	チェックサム（オプション）。使用しないときは 0 が入る。
Data	可変	データ

表 96:

おもな Well-known ポート

RFC1700, ASSIGNED NUMBERS

<http://www.iana.org/assignments/port-numbers>

7/tcp	echo
7/udp	echo
9/tcp	discard
9/udp	discard
13/tcp	daytime
13/udp	daytime
19/tcp	chargen (Character Generator)
19/udp	chargen (Character Generator)
20/tcp	FTP (データ用)
20/udp	FTP (データ用)

21/tcp	FTP (制御用)
21/udp	FTP (制御用)
23/tcp	Telnet
23/udp	Telnet
25/tcp	SMTP
25/udp	SMTP
37/tcp	Time
37/udp	Time
53/tcp	Domain Name Server
53/udp	Domain Name Server
65/tcp	TACACS-Database Service
65/udp	TACACS-Database Service
67/tcp	BOOTP サーバー
67/udp	BOOTP サーバー
68/tcp	BOOTP クライアント
68/udp	BOOTP クライアント
69/tcp	TFTP
69/udp	TFTP
70/tcp	gopher
70/udp	gopher
79/tcp	finger
79/udp	finger
80/tcp	HTTP (WWW)
80/udp	HTTP (WWW)
88/tcp	Kerberos
88/udp	Kerberos
110/tcp	POP3
110/udp	POP3
111/tcp	SUN Remote Procedure Call (sunrpc)
111/udp	SUN Remote Procedure Call (sunrpc)
113/tcp	ident (auth)
113/udp	ident (auth)
119/tcp	NNTP (ネットニュース)
119/udp	NNTP (ネットニュース)
123/tcp	NTP (Network Time Protocol)
123/udp	NTP (Network Time Protocol)
137/tcp	NETBIOS Name Service (netbios-ns)
137/udp	NETBIOS Name Service (netbios-ns)

138/tcp	NETBIOS Datagram Service (netbios-dgm)
138/udp	NETBIOS Datagram Service (netbios-dgm)
139/tcp	NETBIOS Session Service (netbios-ssn)
139/udp	NETBIOS Session Service (netbios-ssn)
161/tcp	SNMP
161/udp	SNMP
162/tcp	SNMP Trap
162/udp	SNMP Trap
194/tcp	IRC (Internet Relay Chat)
194/udp	IRC (Internet Relay Chat)
389/tcp	LDAP (Lightweight Directory Access Protocol)
389/udp	LDAP (Lightweight Directory Access Protocol)
443/tcp	https
443/udp	https
445/tcp	Microsoft-DS
445/udp	Microsoft-DS
512/tcp	rexec
512/udp	biff
513/tcp	rlogin
513/udp	rwho
514/tcp	rcmd
514/udp	syslog
515/tcp	LPD (Line Printer Spooler)
515/udp	LPD (Line Printer Spooler)

表 97:

IP アドレス

IP アドレスクラス一覧

クラス	アドレス範囲	先頭ビットパターン	ネットワーク部の長さ	ホスト部の長さ
A	0.0.0.0-127.255.255.255	0	7	24
B	128.0.0.0-191.255.255.255	10	14	16
C	192.0.0.0-223.255.255.255	110	21	8
D	224.0.0.0-239.255.255.255	1110	28 (グループ ID)	-
E	240.0.0.0-247.255.255.255	11110	-	-

表 98:

127.0.0.0/8 (特に 127.0.0.1) はループバックアドレスとして使われることが多い。

プライベート IP アドレス

RFC1918, Address Allocation for Private Internets

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

可変長サブネットマスク

RFC1878, Variable Length Subnet Table For IPv4

マスク長	10 進	16 進	ホスト数	備考
1	128.0.0.0	80000000	$2^{31} = 2,147,483,648$ (2048M)	クラス A 128 個
2	192.0.0.0	c0000000	$2^{30} = 1,073,741,824$ (1024M)	クラス A 64 個
3	224.0.0.0	e0000000	$2^{29} = 536,870,912$ (512M)	クラス A 32 個
4	240.0.0.0	f0000000	$2^{28} = 268,435,456$ (256M)	クラス A 16 個
5	248.0.0.0	f8000000	$2^{27} = 134,217,728$ (128M)	クラス A 8 個
6	252.0.0.0	fc000000	$2^{26} = 67,108,864$ (64M)	クラス A 4 個
7	254.0.0.0	fe000000	$2^{25} = 33,554,432$ (32M)	クラス A 2 個
8	255.0.0.0	ff000000	$2^{24} = 16,777,216$ (16M)	クラス A 1 個
9	255.128.0.0	ff800000	$2^{23} = 8,388,608$ (8M)	クラス B 128 個
10	255.192.0.0	ffc00000	$2^{22} = 4,194,304$ (4M)	クラス B 64 個
11	255.224.0.0	ffe00000	$2^{21} = 2,097,152$ (2M)	クラス B 32 個
12	255.240.0.0	fff00000	$2^{20} = 1,048,576$ (1024K)	クラス B 16 個
13	255.248.0.0	fff80000	$2^{19} = 524,288$ (512K)	クラス B 8 個
14	255.252.0.0	fffc0000	$2^{18} = 262,144$ (256K)	クラス B 4 個
15	255.254.0.0	fffe0000	$2^{17} = 131,072$ (128K)	クラス B 2 個
16	255.255.0.0	ffff0000	$2^{16} = 65,536$ (64K)	クラス B 1 個
17	255.255.128.0	ffff8000	$2^{15} = 32,768$ (32K)	クラス C 128 個
18	255.255.192.0	ffffc000	$2^{14} = 16,384$ (16K)	クラス C 64 個
19	255.255.224.0	ffffe000	$2^{13} = 8,192$ (8K)	クラス C 32 個
20	255.255.240.0	fffff000	$2^{12} = 4,096$ (4K)	クラス C 16 個
21	255.255.248.0	fffff800	$2^{11} = 2,048$ (2K)	クラス C 8 個
22	255.255.252.0	fffffc00	$2^{10} = 1,024$ (1K)	クラス C 4 個
23	255.255.254.0	fffffe00	$2^9 = 512$	クラス C 2 個
24	255.255.255.0	fffff00	$2^8 = 256$	クラス C 1 個
25	255.255.255.128	fffff80	$2^7 = 128$	クラス C 1/2 個
26	255.255.255.192	fffffc0	$2^6 = 64$	クラス C 1/4 個
27	255.255.255.224	fffffe0	$2^5 = 32$	クラス C 1/8 個
28	255.255.255.240	fffff0	$2^4 = 16$	クラス C 1/16 個

29	255.255.255.248	ffffff8	$2^3 = 8$	クラス C 1/32 個
30	255.255.255.252	ffffffc	$2^2 = 4$	クラス C 1/64 個
31	255.255.255.254	ffffffe	$2^1 = 2$	クラス C 1/128 個
32	255.255.255.255	fffffff	$2^0 = 1$	単一ホスト

表 99:

マルチキャストグループアドレス

RFC1700, ASSIGNED NUMBERS

<http://www.iana.org/assignments/multicast-addresses>

アドレス	対象グループ
224.0.0.0/24	経路制御プロトコルなどのために予約。転送されない
224.0.0.0	使用されない
224.0.0.1	同一サブネット上の全ノード
224.0.0.2	同一サブネット上の全ルーター
224.0.0.4	DVMRP ルーター
224.0.0.5	OSPF ルーター
224.0.0.6	OSPF 代表ルーター
224.0.0.9	RIP Version 2 ルーター
224.0.0.13	PIM ルーター
224.0.0.18	VRRP
224.0.1.1	NTP (Network Time Protocol)
224.0.1.24	microsoft-ds

表 100: