CHAPTER 7

ポートのステータスと接続の確認

この章では、Catalyst 4500 シリーズ スイッチ上でスイッチ ポートのステータスと接続を確認する方法について説明します。

この章の主な内容は、次のとおりです。

（注） この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

モジュール ステータスの確認

Catalyst 4500 シリーズ スイッチはマルチモジュール システムです。取り付けられているモジュール、および各モジュールの MAC アドレス範囲とバージョン番号は、**show module** コマンドを使用して確認します。特定のモジュール番号を指定して、そのモジュールの詳細な情報を表示するには、[*mod_num*] 引数を使用します。

次に、スイッチ上のすべてのモジュール ステータスを確認する例を示します。

```
Switch# show module all

Mod  Ports Card Type                                  Model              Serial No.
---+-----+--------------------------------------+------------------+-----------
 1     2   1000BaseX (GBIC) Supervisor Module     WS-X4014          JAB012345AB
 5    24   10/100/1000BaseTX (RJ45)               WS-X4424-GB-RJ45 JAB045304EY
 6    48   10/100BaseTX (RJ45)                    WS-X4148          JAB023402QK

 M MAC addresses                    Hw  Fw                Sw               Stat
--+--------------------------------+---+-----------------+---------------+-----
 1 0004.dd46.9f00 to 0004.dd46.a2ff 0.0 12.1(10r)EW(1.21) 12.1(10)EW(1)    Ok
 5 0050.3e7e.1d70 to 0050.3e7e.1d87 0.0                                    Ok
 6 0050.0f10.2370 to 0050.0f10.239f 1.0                                    Ok
Switch#
```

インターフェイスのステータスの確認

スイッチ ポートのサマリーまたは詳細情報を表示する場合は、**show interfaces status** コマンドを使用します。スイッチ上のすべてのポートの要約情報を表示するには、引数なしの **show interfaces status** コマンドを入力します。特定のモジュール番号を指定すると、そのモジュールのポート情報だけが表示されます。特定のポートの詳細情報を表示するには、モジュール番号とポート番号を入力します。

特定のポートにコンフィギュレーション コマンドを適用するには、適切な論理モジュールを指定する必要があります。詳細については、「モジュール ステータスの確認」（P.7-1）を参照してください。

次に、トランシーバを含む Catalyst 4500 シリーズ スイッチ上のすべてのインターフェイスのステータスを表示する例を示します。このコマンドの出力では、他社製トランシーバの「未承認の GBIC」が表示されます。

```
Switch#show interfaces status

Port     Name               Status       Vlan       Duplex  Speed Type
Gi1/1                       notconnect   1            auto   auto No Gbic
Gi1/2                       notconnect   1            auto   auto No Gbic
Gi5/1                       notconnect   1            auto   auto 10/100/1000-TX
Gi5/2                       notconnect   1            auto   auto 10/100/1000-TX
Gi5/3                       notconnect   1            auto   auto 10/100/1000-TX
Gi5/4                       notconnect   1            auto   auto 10/100/1000-TX
Fa6/1                       connected    1          a-full  a-100 10/100BaseTX
Fa6/2                       connected    2          a-full  a-100 10/100BaseTX
Fa6/3                       notconnect   1            auto   auto 10/100BaseTX
Fa6/4                       notconnect   1            auto   auto 10/100BaseTX

Switch#
```

次に、errdisable ステートのインターフェイスのステータスを表示する例を示します。

```
Switch# show interfaces status err-disabled
Port     Name               Status         Reason
Fa9/4                       err-disabled   link-flap
informational error message when the timer expires on a cause
-----------------------------------------------------------------
5d04h:%PM-SP-4-ERR_RECOVER:Attempting to recover from link-flap err-disable state on Fa9/4
Switch#
```

MAC アドレスの表示

show module コマンドを使用してモジュールの MAC アドレス範囲を表示する以外に、**show mac-address-table address** コマンドと **show mac-address-table interface** コマンドを使用して、特定の MAC アドレスまたはスイッチの特定のインターフェイスの MAC アドレス テーブル情報を表示できます。

次に、特定の MAC アドレスの MAC アドレス テーブル情報を表示する例を示します。

```
Switch# show mac-address-table address 0050.3e8d.6400
vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 200  0050.3e8d.6400  static   assigned  --  Switch
 100  0050.3e8d.6400  static   assigned  --  Switch
   5  0050.3e8d.6400  static   assigned  --  Switch
   4  0050.3e8d.6400  static        ipx  --  Switch
   1  0050.3e8d.6400  static        ipx  --  Switch
   1  0050.3e8d.6400  static   assigned  --  Switch
   4  0050.3e8d.6400  static   assigned  --  Switch
   5  0050.3e8d.6400  static        ipx  --  Switch
 100  0050.3e8d.6400  static        ipx  --  Switch
 200  0050.3e8d.6400  static        ipx  --  Switch
 100  0050.3e8d.6400  static      other  --  Switch
 200  0050.3e8d.6400  static      other  --  Switch
   5  0050.3e8d.6400  static      other  --  Switch
   4  0050.3e8d.6400  static         ip  --  Switch
   1  0050.3e8d.6400  static         ip  --  Route
   1  0050.3e8d.6400  static      other  --  Switch
   4  0050.3e8d.6400  static      other  --  Switch
   5  0050.3e8d.6400  static         ip  --  Switch
 200  0050.3e8d.6400  static         ip  --  Switch
 100  0050.3e8d.6400  static         ip  --  Switch
Switch#
```

次に、特定のインターフェイスの MAC アドレス テーブル情報を表示する例を示します。

```
Switch# show mac-address-table interface gigabit 1/1
Multicast Entries
 vlan    mac address     type    ports
-------+---------------+-------+-----------------------------------------
   1    ffff.ffff.ffff system Switch,Gi6/1,Gi6/2,Gi6/9,Gi1/1
Switch#
```

TDR を使用したケーブル ステータスの確認

リンクを確立できない場合に、Time Domain Reflectometer（TDR; タイム ドメイン リフレクトメータ）機能を使用してケーブル接続に障害があるかどうかを判別できます。

（注） このテストは、既存スイッチの交換、ギガビット イーサネットへのアップグレード、または新しいケーブル プラントを導入する際に特に重要になります。

概要

Catalyst 4500 シリーズ スイッチの 48 ポート 10/100/1000BASE-T モジュール（WS-X4548-GB-RJ45、WS-X4548-GB-RJ45V、WS-X4524-GB-RJ45V、WS-X4013+TS、WS-C4948、および WS-C4948-10GE）では、TDR を使用して銅ケーブルのステータスを確認できます。TDR は、信号をケーブルに送信し、反射して戻ってきた信号を読み取ることによりケーブルの障害を検出します。信号のすべてまたは一部は、ケーブルの障害箇所またはケーブルの終端により反射されて戻されます。

（注） 標準のカテゴリ 5 ケーブルには 4 つのペアがあります。各ペアは、次のステート（オープン（接続されていない）、損傷、ショート、または終端）のいずれかであると想定できます。TDR テストでは 4 つすべてのステートを検出し、最初の 3 つの状態を「Fault」と表示し、4 番めの状態を「Terminated」と表示します。CLI 出力は表示されますが、ケーブル長はステートが「Faulty」の場合にだけ表示されます。

TDR テストの実行

TDR テストを開始するには、特権モードで次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# **test cable-diagnostics tdr** {***interface*** {*interface interface-number*}}	TDR テストを開始します。
ステップ 2	Switch# **show cable-diagnostics tdr** {***interface*** {*interface interface-number*}}	TDR テストのカウンタ情報を表示します。

次に、モジュール 2 のポート 1 上で TDR テストを開始する例を示します。

```
Switch# test cable-diagnostics tdr int gi2/1
Switch#
```

次に、モジュールで TDR テストがサポートされていない場合に表示されるメッセージ例を示します。

```
Switch# test cable-diagnostics tdr int gi2/1
00:03:15:%C4K_IOSDIAGMAN-4-TESTNOTSUPPORTEDONMODULE: Online cable
diag tdr test is not supported on this module
Switch#
```

次に、ポートの TDR テストの結果を表示する例を示します。

```
Switch# show cable-diagnostics tdr interface gi4/13
Interface Speed  Local pair Cable length Remote channel Status
Gi4/13    0Mbps   1-2        102 +-2m     Unknown       Fault
                  3-6        100 +-2m     Unknown       Fault
                  4-5        102 +-2m     Unknown       Fault
                  7-8        102 +-2m     Unknown       Fault
```

（注） このコマンドは、Cisco IOS ソフトウェアの将来のリリースでは廃止される予定です。TDR テストを実行し、テスト結果を表示するには、diagnostic start および **show diagnostic result** コマンドを使用してください。

（注） TDR は、ポートのテストです。ポートは、テストの実行中（通常、1 分間）はトラフィックを処理できません。

ガイドライン

TDR を使用する場合は、次の注意事項が適用されます。

- TDR テストを実行中のポートと Auto-MDIX がイネーブルのポートを接続した場合、この TDR 結果は無効となる可能性があります。この場合、TDR テストを開始する前に WS-X4148-RJ45V 上のポートを管理上のダウンにする必要があります。
- TDR テストを実行中のポートと WS-X4148-RJ45V 上のポートなど 100BASE-T ポートを接続する場合、未使用のペア（4 ～ 5 および 7 ～ 8）はリモート エンドで終端処理されないため、障害としてレポートされます。
- TDR テストの実行中はポート設定を変更しないでください。
- ケーブルの特性から、正確な結果を入手するには TDR テストを複数回行う必要があります。
- （近端または遠端のケーブルを取り外すなど）ポート ステータスを変更しないでください。結果が不正確となる可能性があります。

Telnet の使用

スイッチのコマンドライン インターフェイス（CLI）には、Telnet を使用してアクセスできます。また、スイッチから Telnet を使用して、ネットワークの他のデバイスにアクセスすることも可能です。最大 8 つの Telnet セッションを同時に実行できます。

スイッチとの Telnet セッションを設定する前に、まずスイッチの IP アドレス（場合によりデフォルト ゲートウェイも）を設定する必要があります。IP アドレスとデフォルト ゲートウェイの設定方法については、第 3 章「スイッチの初期設定」を参照してください。

（注） ホスト名を使用してホストとの Telnet 接続を確立するには、ドメイン ネーム システム（DNS）を設定してイネーブルにします。

スイッチからネットワーク上の別のデバイスへの Telnet 接続を確立するには、次の作業を行います。

コマンド	目的
Switch# **telnet** *host* [*port*]	リモート ホストとの Telnet セッションを確立します。

次に、スイッチからリモート ホスト labsparc への Telnet 接続を確立する例を示します。

```
Switch# telnet labsparc
Trying 172.16.10.3...
Connected to labsparc.
Escape character is '^]'.

UNIX(r) System V Release 4.0 (labsparc)

login:
```

ログアウト タイマーの変更

ログアウト タイマーは、ユーザが指定された時間よりも長くアイドル状態にあるとき、自動的にスイッチから切断します。ログアウト タイマーを設定するには、次の作業を行います。

コマンド	目的
Switch# **logoutwarning** ***number***	ログアウト タイマーの値を変更します（タイムアウト値に 0 を指定すると、アイドル状態のセッションが自動的に切断されるのを防ぎます）。 デフォルト値に戻すには、**no** キーワードを使用します。

ユーザ セッションのモニタリング

スイッチ上で現在アクティブなユーザ セッションを表示するには、**show users** コマンドを使用します。このコマンドは、スイッチでアクティブなすべてのコンソール ポートと Telnet セッションのリストを出力します。

スイッチのアクティブなユーザ セッションを表示するには、特権 EXEC モードで次の作業を行います。

コマンド	目的
Switch# **show users [all]**	スイッチで現在アクティブなユーザ セッションを表示します。

次に、コンソールと Telnet セッションでローカル認証がイネーブルの場合の、**show users** コマンドの出力例を示します（アスタリスク [*] が現在のセッションを示します）。

```
Switch# show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00

  Interface      User         Mode                    Idle     Peer Address

Switch# show users all
    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00
   1 vty 0                                      00:00:00
   2 vty 1                                      00:00:00
   3 vty 2                                      00:00:00
   4 vty 3                                      00:00:00
   5 vty 4                                      00:00:00

  Interface      User         Mode                    Idle     Peer Address
Switch#
```

アクティブなユーザ セッションを切断するには、次の作業を行います。

コマンド	目的
Switch# **disconnect** {**console** | *ip_addr*}	スイッチのアクティブなユーザ セッションを切断します。

次に、アクティブなコンソール ポートのセッションとアクティブな Telnet セッションを切断する例を示します。

```
Switch> disconnect console
Console session disconnected.
Console> (enable) disconnect tim-nt.bigcorp.com
Telnet session from tim-nt.bigcorp.com disconnected. (1)
Switch# show users
  Session  User             Location
  -------- ---------------- -------------------------
  telnet   jake             jake-mac.bigcorp.com
* telnet   suzy             suzy-pc.bigcorp.com
Switch#
```

ping の使用

ここでは、IP ping を使用する手順について説明します。

- 「ping の機能」（P.7-7）
- 「ping の実行」（P.7-7）

ping の機能

ping コマンドを使用すると、リモート ホストとの接続を確認できます。異なる IP サブネットワークのホストに ping を実行する場合、ネットワークへのスタティック ルートを定義するか、サブネット間をルーティングするルータを設定する必要があります。

ping コマンドは、ユーザ モードおよび特権 EXEC モードから設定できます。ping は次のいずれかの応答を返します。

- 正常な応答：正常な応答（*hostname* が存在する）は、ネットワーク トラフィックにもよりますが、1 ～ 10 秒以内で発生します。
- 宛先の応答なし：ホストが応答しない場合、No Answer メッセージが返されます。
- ホスト不明：ホストが存在していない場合、Unknown Host メッセージが返されます。
- 宛先到達不能：デフォルト ゲートウェイが指定されたネットワークに到達できない場合、Destination Unreachable メッセージが返されます。
- ネットワークまたはホスト到達不能：ホストまたはネットワークにルート テーブルが存在しない場合、Network または Host Unreachable メッセージが返されます。

実行中の ping を停止するには、Ctrl+C を押します。

ping の実行

スイッチからネットワーク上の別のデバイスに ping を実行するには、ユーザ モードおよび特権 EXEC モードで次の作業を行います。

コマンド	目的
Switch# **ping** *host*	リモート ホストとの接続を確認します。

次に、ユーザ モードからリモート ホストに ping を実行する例を示します。

```
Switch# ping labsparc
labsparc is alive
Switch> ping 72.16.10.3
12.16.10.3 is alive
Switch#
```

次に、パケット数、パケット サイズ、タイムアウト時間を指定して、特権 EXEC モードで **ping** コマンドを入力する例を示します。

```
Switch# ping
Target IP Address []: 12.20.5.19
Number of Packets [5]: 10
Datagram Size [56]: 100
Timeout in seconds [2]: 10
Source IP Address [12.20.2.18]: 12.20.2.18
!!!!!!!!!!

----12.20.2.19 PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 1/1/1
Switch
```

IP traceroute の使用

ここでは、IP traceroute 機能を使用する手順について説明します。

IP traceroute の機能

IP traceroute を使用すると、ネットワーク上でパケットが通過するパスをホップバイホップで識別できます。このコマンドを実行すると、トラフィックが宛先に到達するまでに通過するルータなどのすべてのネットワーク層（レイヤ 3）デバイスが表示されます。

レイヤ 2 スイッチは、**trace** コマンドの送信元または宛先として参加できますが、**trace** コマンド出力ではホップとして表示されません。

trace コマンドは IP ヘッダーの存続可能時間（TTL）フィールドを使用して、ルータとサーバで特定のリターン メッセージが生成されるようにします。traceroute の実行は、ユーザ データグラム プロトコル（UDP）データグラムを、TTL フィールドが 1 に設定されている宛先ホストへ送信することから始まります。ルータが 1 または 0 の TTL 値を検出すると、ルータはデータグラムをドロップして インターネット制御メッセージ プロトコル（ICMP）Time-Exceeded メッセージを送信側に返します。traceroute は、ICMP Time-Exceeded メッセージの送信元アドレス フィールドを調べて、最初のホップのアドレスを判断します。

ネクスト ホップを識別するために、traceroute は TTL 値が 2 の UDP パケットを送信します。1 番めのルータは、TTL フィールドの値から 1 を差し引いて次のルータにデータグラムを送信します。2 番めのルータは TTL の値 1 を確認し、データグラムをドロップして、送信元に Time-Exceeded メッセージを返します。このプロセスは、データグラムが宛先ホストに到達できるだけの値まで TTL が増加するか、最大 TTL に到達するまで続けられます。

データグラムが宛先に到達したことを判断するために、traceroute はデータグラムの UDP 宛先ポートを宛先ホストが使用すると予測される非常に大きな値に設定します。ホストが未確認のポート番号を指定したデータグラムを受け取ると、送信元に ICMP Port Unreachable エラー メッセージを送信します。Port Unreachable エラー メッセージは、宛先に到達していることを traceroute に通知します。

IP traceroute の実行

パケットがネットワークで通過するパスを追跡するには、EXEC モードまたは特権 EXEC モードで次の作業を行います。

コマンド	目的
Switch# **trace** [*protocol*] [*destination*]	IP traceroute を実行して、ネットワークでパケットが通過するパスを追跡します。

次に、**trace** コマンドを使用して、パケットがネットワークで宛先に到達するまでのルートを表示する例を示します。

```
Switch# trace ip ABA.NYC.mil

Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
  1 DEBRIS.CISCO.COM (192.180.1.6) 1000 msec 8 msec 4 msec
  2 BARRNET-GW.CISCO.COM (192.180.16.2) 8 msec 8 msec 8 msec
  3 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
  4 BB2.SU.BARRNET.NET (192.200.254.6) 8 msec 8 msec 8 msec
  5 SU.ARC.BARRNET.NET (192.200.3.8) 12 msec 12 msec 8 msec
  6 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
  7 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
Switch#
```

レイヤ 2 traceroute の使用

レイヤ 2 traceroute 機能により、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスを識別できます。レイヤ 2 Traceroute は、ユニキャストの送信元および宛先 MAC アドレスだけをサポートします。パス内のスイッチが保持する MAC アドレス テーブルを使用してパスを判別します。スイッチがレイヤ 2 traceroute をサポートしないデバイスをパスで検出すると、スイッチはレイヤ 2 トレース キューを送信し続けてタイムアウトにしてしまいます。

スイッチが送信元デバイスのホストから宛先デバイスのホストへのパスを追跡する場合、スイッチは送信元デバイスから宛先デバイスへのパスのみを識別します。パケットが通過する、送信元ホストから送信元デバイスまで、または宛先デバイスから宛先ホストまでのパスは識別できません。

ここでは、レイヤ 2 traceroute 機能を使用する手順について説明します。

- 「レイヤ 2 traceroute の使用上の注意事項」（P.7-9）
- 「レイヤ 2 traceroute の実行」（P.7-10）

レイヤ 2 traceroute の使用上の注意事項

レイヤ 2 traceroute の使用上の注意事項を次に示します。

- Cisco Discovery Protocol（CDP）は、ネットワーク上のすべてのデバイスでイネーブルになっている必要があります。レイヤ 2 traceroute を適切に機能させるためには、CDP をディセーブルにしないでください。

  物理パス内のデバイスが CDP に対して透過的な場合、スイッチはこれらのデバイスを通過するパスを識別できません。

（注）　CDP をイネーブルにする場合の詳細については第 23 章「CDP の設定」を参照してください。

- 物理パス内のすべてのスイッチは IP 接続が可能でなければなりません。スイッチが別のスイッチから到達可能である場合、特権 EXEC モードで **ping** コマンドを使用して接続をテストできます。
- パス内で識別可能な最大ホップ数は 10 です。
- 送信元デバイスから宛先デバイスへの物理パスにないスイッチにおいて、特権 EXEC モードで **traceroute mac** コマンドまたは **traceroute mac ip** コマンドを入力できます。パス内のすべてのスイッチは、このスイッチから到達可能でなければなりません。
- 指定した送信元および宛先 MAC アドレスが同一 VLAN に属する場合、**traceroute mac** コマンド出力はレイヤ 2 パスのみを表示します。指定した送信元および宛先 MAC アドレスが、それぞれ異なる VLAN に属している場合は、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。
- マルチキャスト送信元または宛先 MAC アドレスを指定すると、パスは識別されず、エラー メッセージが表示されます。
- 送信元または宛先 MAC アドレスが複数の VLAN に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。VLAN を指定しないと、パスは識別されず、エラー メッセージが表示されます。
- 指定した送信元および宛先 MAC アドレスが同一サブネットに属する場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。IP アドレスを指定する場合、スイッチは Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用して IP アドレスと対応する MAC アドレスおよび VLAN ID を対応付けます。
  - 指定の IP アドレスの ARP のエントリが存在している場合、スイッチは関連付けられた MAC アドレスを使用し、物理パスを識別します。
  - ARP のエントリが存在しない場合、スイッチは ARP クエリーを送信し、IP アドレスを解決しようと試みます。IP アドレスが解決されない場合は、パスは識別されず、エラー メッセージが表示されます。
- 複数のデバイスがハブを介して 1 つのポートに接続されている場合（たとえば複数の CDP ネイバーがポートで検出された場合）、レイヤ 2 traceroute 機能はサポートされません。複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。
- この機能は、トークンリング VLAN ではサポートされません。

レイヤ 2 traceroute の実行

送信元デバイスから宛先デバイスへ送信されるパケットが通過する物理パスを表示するには、特権 EXEC モードで次の作業のいずれかを行います。

コマンド	目的
Switch# **traceroute mac** {*source-mac-address*} {*destination-mac-address*}	レイヤ 2 traceroute を実行して、ネットワークでパケットが通過するパスを追跡します。

または

コマンド	目的
Switch# **traceroute mac ip** {*source-mac-address*} {*destination-mac-address*}	IP traceroute を実行して、ネットワークでパケットが通過するパスを追跡します。

次の例は、**traceroute mac** および **traceroute mac ip** コマンドを使用して、パケットが宛先に到達するまでに通過したネットワーク上の物理パスを表示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 => Fa0/3
con5                  (2.2.5.5        )  :    Fa0/3 => Gi0/1
con1                  (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                  (2.2.2.2        )  :    Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
Switch#

Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C2950G-24-EI / 2.2.6.6 :
        Fa0/1 [auto, auto] => Fa0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
Switch#
```

ICMP の設定

ICMP は、IP 接続を制御および管理するための多くのサービスを提供します。インターネット ヘッダーに問題が検出された場合に、ICMP メッセージがルータまたはアクセス サーバによってホストまたはその他のルータに送信されます。ICMP の詳細については、RFC 792 を参照してください。

ICMP Protocol Unreachable メッセージのイネーブル化

Cisco IOS ソフトウェアが不明なプロトコルを使用する非ブロードキャスト パケットを受け取ると、送信元に ICMP Protocol Unreachable メッセージを返します。

同様に、宛先アドレスまでのルートを認識していないため最終的な宛先に届かないパケットをソフトウェアが受け取ると、送信元に ICMP Host Unreachable メッセージを返します。この機能は、デフォルトでイネーブルにされています。

ICMP Protocol Unreachable と Host Unreachable メッセージの生成をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを入力します。

コマンド	目的
`Switch (config-if)# [no] ip unreachables`	ICMP 宛先到達不能メッセージをイネーブルにします。 ICMP 宛先到達不能メッセージをディセーブルにするには、**no** キーワードを使用します。

注意　**no ip unreachables** コマンドを実行すると、「パス MTU ディスカバリ」機能が停止します。ネットワークの中のルータは、パケットを強制的に分割します。

ICMP 宛先到達不能メッセージが生成されるレートを制限するには、次の作業を行います。

コマンド	目的
`Switch (config)# [no] ip icmp rate-limit unreachable [df]` *milliseconds*	ICMP 宛先メッセージが生成されるレートを制限します。 レート制限を削除し、CPU 利用を低減させるには、**no** キーワードを使用します。

ICMP Redirect メッセージのイネーブル化

最適なデータ ルートが使用されない場合があります。たとえば、受信したその同じインターフェイスを使用したパケットの再送をルータに強制できます。この場合、Cisco IOS ソフトウェアはパケットの送信元に ICMP Redirect メッセージを送信して、ルータが受信デバイスに直接接続するサブネット上にあること、また、ルータは同じサブネット上の別のシステムにパケットを転送する必要があることを送信元に通知します。ソフトウェアはパケットの送信元に ICMP Redirect メッセージを送信します。これは発信側ホストがすでにネクスト ホップにそのパケットを送信し、それを送信元がまったく認識していない可能性があるためです。Redirect メッセージは、ルートから受信デバイスを削除し、よりダイレクトなパスを示す指定されたデバイスに代えるよう送信側に指示します。この機能は、デフォルトでイネーブルにされています。

ただし、ホットスタンバイ ルータ プロトコル（HSRP）がインターフェイスに設定されている場合、そのインターフェイスでは ICMP Redirect メッセージは（デフォルトで）ディセーブルになります。HSRP の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp_ps6350_TSD_Products_Configuration_Guide_Chapter.html

Cisco IOS ソフトウェアが受信したインターフェイスからパケットを再送するように指定されている場合、ICMP Redirect メッセージの送信をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを入力します。

コマンド	目的
`Switch (config-if)# [no] ip redirects`	ICMP Redirect メッセージをイネーブルにします。 ICMP Redirect メッセージをディセーブルにし、CPU 利用を低減させるには、**no** キーワードを使用します。

ICMP Mask Reply メッセージのイネーブル化

ネットワーク デバイスがインターネットワークの特定のサブネットワークに関して、サブネット マスクを認識していなければならない場合があります。この情報を取得するために、デバイスは ICMP Mask Request メッセージを送信します。これらのメッセージには、要求された情報を保有するデバイスの ICMP Mask Reply メッセージが応答します。Cisco IOS ソフトウェアは、ICMP Mask Reply 機能がイネーブルの場合に、ICMP Mask Request メッセージに応答できます。

Cisco IOS ソフトウェアが ICMP Mask Reply メッセージを送信して、ICMP マスク要求に応答するように指定するには、次の作業を行います。

コマンド	目的
`Switch (config-if)# [no] ip mask-reply`	ICMP 宛先マスク要求への応答をイネーブルにします。 この機能をディセーブルにするには、**no** キーワードを使用します。