拡張 ping および拡張 traceroute コマンドについて

内容

はじめに

このドキュメントでは、拡張 ping さらに拡張された traceroute コマンドを発行します。

前提条件

要件

このドキュメントを読むには、 ping と traceroute コマンドを発行します。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS(R) ソフトウェア
- すべての Cisco シリーズ ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

ドキュメントの表記方法の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

「 ping コマンド

「 ping (Packet InterNet Groper)コマンドは、デバイスのアクセシビリティをトラブルシューティングするための非常に一般的な方法です。これは、2 つの Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル) クエリー メッセージ、ICMP エコー要求、および ICMP エコー応答を使用して、リモート ホストがアクティブであるかどうかを判断します。「 ping また、エコー応答の受信にかかる時間も測定します。

「 ping コマンドは、最初にエコー要求パケットをアドレスに送信し、応答を待ちます。「 ping エコー要求が宛先に到達し、宛先が送信元にエコー応答を返すことができる場合にのみ成功します。 ping 事前に定義された期間内に行う必要があります。

拡張された ping コマンド

通常の ping コマンドはルータから送信されます。pingの送信元アドレスは、パケットがルータを出るために使用するインターフェイスのIPアドレスです。拡張ポートが ping コマンドを使用すると、送信元IPアドレスをルータ上の任意のIPアドレスに変更できます。拡張された ping ホストの到達可能性とネットワーク接続のより高度なチェックを実行するために使用されます。拡張された ping コマンドは、特権EXECコマンドラインでのみ機能します。通常 ping は、ユーザEXECモードと特権EXECモードの両方で動作します。この機能を使用するには、次のように入力します ping コマンドラインでReturnキーを押します。このドキュメントの「ping コマンドのフィールドの説明」セクションで説明されるようなフィールドへの入力を要求されます。

「 ping コマンドフィールドの説明

次の表に、 ping コマンドのフィールドの説明これらのフィールドは、 ping コマンドを使用して、アップグレードを実行します。

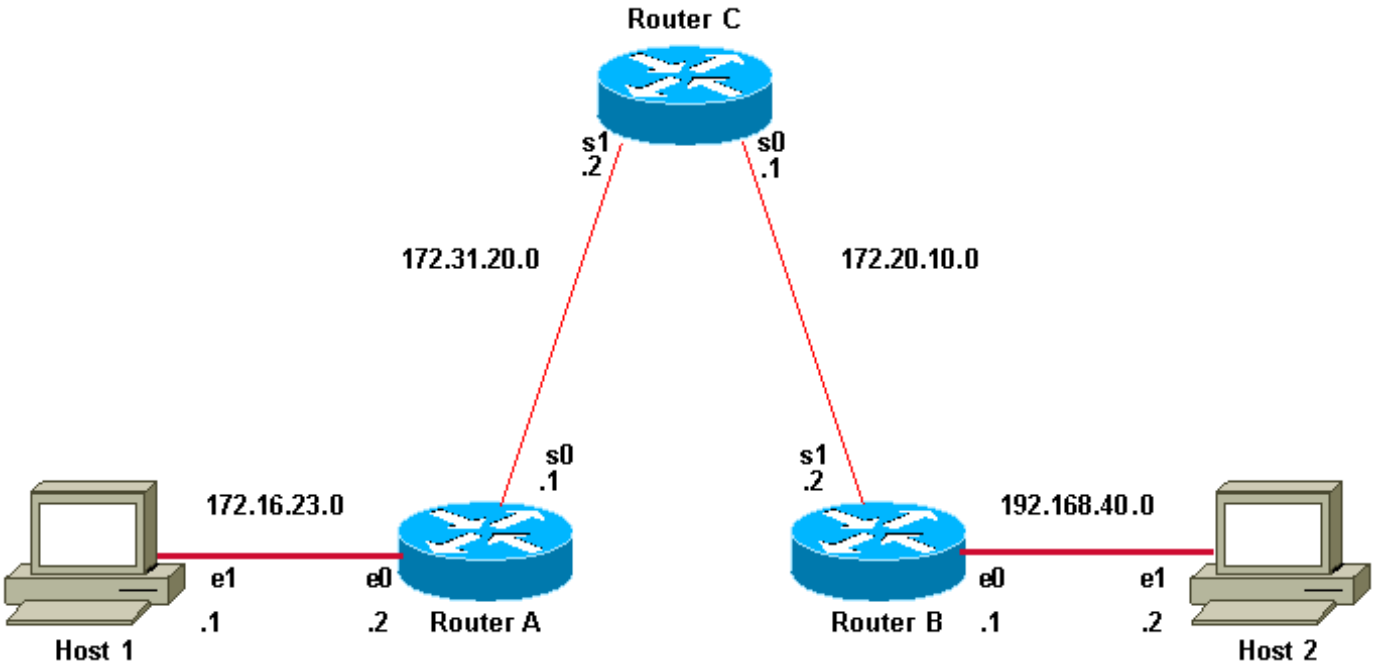
フィールド	説明
Protocol [ip]:	サポートされているプロトコルを入力するように要求されます。appletalk、clns、ip、novell、apollo、vines、decnet、または xns を入力します。デフォルトは ip です。
Target IP address:	ping しようとしている宛先ノードの IP アドレスまたはホスト名を入力するよう要求されます。サポートされているプロトコルに IP 以外を指定した場合は、ここにはそのプロトコルに適したアドレスを入力します。デフォルトは

	none です。
Repeat count [5]:	宛先アドレスに送信される ping パケットの数。デフォルトは 5 です。
Datagram size [100]:	ping パケットのサイズ（バイト単位）。デフォルトは 100 バイトです。
Timeout in seconds [2]:	タイムアウト間隔。デフォルトは 2 秒です。ping は、この時間間隔以内にエコー応答パケットが受信された場合にのみ成功したと見なされます。
Extended commands [n]:	一連の追加コマンドを表示するかどうかを指定します。デフォルトは no です。
入力 ping [n]（Ingress ping [n]）：	入力 ping は、ターゲット接続先への指定された入力インターフェイスで受信されたパケットをシミュレートします。デフォルトは no です。 （このオプションの使用可否は、使用されているソフトウェアリリースによって異なります）
Source address or interface:	プローブの送信元アドレスとして使用するルータのインターフェイスまたは IP アドレス。ルータは、通常、使用する送信インターフェイスの IP アドレスを選択します。インターフェイスも指定できますが、次に示すような正しい構文を使用します。 Source address or interface: ethernet 0 注：これは拡張ACLの出力の一部です。 ping コマンドを使用して、アップグレードを実行します。インターフェイスは、e0 とは記述できません。
DSCP 値 [0]（DSCP Value [0]）：	Diffserv コードポイント（DSCP）を指定します。導入された DSCP 値は、各プローブに配置されます。デフォルトは 0 です。（このオ

	プションの使用可否は、使用されているソフトウェアリリースによって異なります）
Type of service [0]:	Type of Service（ToS）を指定します。要求された ToS が各プローブに配置されますが、すべてのルータが ToS を処理するとは限りません。選択したサービスのインターネット品質次第です。デフォルト値は 0 です。
Set DF bit in IP header?[no]:	次のいずれかを指定します。 Don't Fragment (DF) ビットはpingパケットに設定されます。yes を指定した場合、DF オプションにより、このパケットは最大伝送ユニット（MTU）の小さいセグメントを通過する必要がある場合にフラグメント化されず、パケットをフラグメント化しようとしたデバイスからエラーメッセージを受信します。これは、宛先までのパスでの最小 MTU を判断するのに役立ちます。デフォルトは no です。
Validate reply data?[no]:	応答データを検証するかどうかを指定します。デフォルトは no です。
Data pattern [0xABCD]	データ パターンを指定します。トラブルシューティングには、さまざまなデータパターンが使用されます framing エラーおよび clocking シリアル回線の問題。デフォルトは [0xABCD] です。
Loose, Strict, Record, Timestamp, Verbose[none]:	IP ヘッダーのオプション。このプロンプトでは、選択オプションが複数提供されます。その内容は次のとおりです。 • Verbose はその他のオプションとともに自動的に選択されます。 • Record は、パケットが通過するホップのアドレス（最大 9 つ）を表示するため、非常に便利なオプションです。 • Loose では、パケットが通過するホップのアドレスを指定するときに、パスに影響を与えることができます。 • Strict はパケットを通過させるホップを指定し、その他のホップは通過できないよ

	うにすることを指定します。 • Timestamp は特定のホストまでのラウンドトリップ時間を測定するために使用します。 このコマンドの Record オプションと traceroute コマンドの違いは、Record オプションでは宛先に到達するまでにエコー要求（ping）が通過するホップが表示されるだけでなく、リターンパスで通過するホップも表示される点です。traceroute コマンドを使用すると、エコー応答がとるパスに関する情報は取得されません。traceroute コマンドを入力すると、必要なフィールドを入力するようプロンプトが表示されます。 traceroute コマンドは要求されたオプションを各プローブに配置します。ただし、すべてのルータ（またはエンド ノード）がそれらのオプションを処理するとは限りません。デフォルトは none です。
Sweep range of sizes [n]:	送信されるエコー パケットのサイズを変更できます。これは、宛先アドレスまでのパスに沿ったノード上で設定されている MTU の最小サイズを判断するために使用されます。このようにして、パケットのフラグメント化によって発生するパフォーマンス上の問題が減らされます。デフォルトは no です。
!!!!!	各感嘆符（!）は、応答の受信を示します。ピリオド（.）は、ネットワークサーバーが応答を待機中にタイムアウトしたことを示します。その他の文字の説明は、『ping 文字』を参照してください。
Success rate is 100 percent	ルータに正常にエコー バックされたパケットのパーセンテージ。80% 未満は、通常は問題があると見なされます。
round-trip min/avg/max = 1/2/4 ms	プロトコルのエコーパケット用のラウンドトリップ時間の間隔で、最小/平均/最大（ミリ秒単位）を含みます。

次の図では、ホスト 1 とホスト 2 は互いに ping できません。ルーティングの問題があるかどうか、または 2 つのホストのいずれかでデフォルトゲートウェイが正しく設定されていないかどうかを判断するために、ルータでこの問題をトラブルシューティングできます。



ホスト 1 とホスト 2 で ping を実行できない

次の場合、 ping正常に実行するために、ホスト1からホスト2への各ホストは、それぞれのLANセグメント上のルータに対するデフォルトゲートウェイを指しているか、ホストがルーティングプロトコルを使用するルータとネットワーク情報を交換する必要があります。いずれかのホストでデフォルトゲートウェイが正しく設定されていない場合、またはルーティングテーブルに正しいルートがない場合、Address Resolution Protocol（ARP）キャッシュに存在しない宛先にパケットを送信することはできません。また、ルータの 1 つに、ホストがその ping パケットを送信するサブネットへのルートがないことが原因で、ホストが相互に ping を実行できない可能性もあります。

例

次に、送信元がルータ A のイーサネット 0 インターフェイスになっていて、宛先がルータ B のイーサネット インターフェイスになっている拡張 ping コマンドの例を示します。この PING の成功は、ルーティング問題がないことを示し ます。ルータ A はルータ B のイーサネットへの到達方法を認識し、ルータ B はルータ A のイーサネットへの到達方法を認識しています。また、両方のホストでデフォルトゲートウェイが正しく設定されています。

拡張された pingコマンドをルータAから実行すると失敗します。これはルーティングの問題があることを意味します。3 台のルータのいずれかにルーティング上の問題がある可能性があります。ルータ A では、ルータ B イーサネットのサブネットへのルートや、ルータ C とルータ B 間のサブネットへのルートが失われた可能性があります。ルータ B では、ルータ A のサブネットへのルートや、ルータ C とルータ A 間のサブネットへのルートが失われた可能性があります。ルータ C では、ルータ A またはルータ B のイーサネットセグメントのサブネットへのルートが失われた可能性があります。ルーティングに関する問題を修正してから、ホスト 1 からホスト 2 への ping を実行する必要があります。ホスト 1 からホスト 2 への ping を実行できない場合は、両方のデ

フォルトゲートウェイを確認してください。ルータ A のイーサネットとルータ B のイーサネットの間の接続は、拡張 ping コマンドを使用してチェックします。

ルータ A からルータ B のイーサネット インターフェイスへの通常の ping では、ping パケットの送信元アドレスは発信インターフェイスのアドレス、つまりシリアル 0 インターフェイスのアドレス (172.31.20.1) になります。ルータ B が ping パケットに応答するとき、送信元アドレス (つまり、172.31.20.1) に応答します。このように、ルータ A のシリアル 0 インターフェイス (172.31.20.1) とルータ B のイーサネット インターフェイス (192.168.40.1) の間の接続だけがテストされます。

ルータAのイーサネット0(172.16.23.2)とルータBのイーサネット0(192.168.40.1)の間の接続をテストするには、extended ping コマンドを使用して、アップグレードを実行します。拡張 pingを使用する場合は、 ping次に示すように、パケットを送信します。

<#root>

```
RouterA>

enable


RouterA#

ping


Protocol [ip]:
Target IP address: 192.168.40.1


!--- The address to ping.



Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.23.2


!---Ping packets are sourced from this address.



Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms


!--- Ping is successful.
```

RouterA#

This is an example with extended commands and sweep details:

RouterA>

enable

RouterA#

ping

Protocol [ip]:

!--- The protocol name.

Target IP address: 192.168.40.1

!--- The address to ping.

Repeat count [5]: 10

!--- The number of ping packets that are sent to the destination address.

Datagram size [100]:

!--- The size of the ping packet in size. The default is 100 bytes.

Timeout in seconds [2]:

!--- The timeout interval. The ping is declared successful only if the
!--- ECHO REPLY packet is received before this interval.

Extended commands [n]: y

!--- You choose yes if you want extended command options
!--- (Loose Source Routing, Strict Source Routing, Record route and Timestamp).

```
Source address or interface: 172.16.23.2

!--- Ping packets are sourced from this address and must be the IP address
!--- or full interface name (for example, Serial0/1 or 172.16.23.2).



Type of service [0]:

!--- Specifies Type of Service (ToS).



Set DF bit in IP header? [no]:

!--- Specifies whether or not the Don't Fragment (DF) bit is to be
!--- set on the ping packet.



Validate reply data? [no]:

!--- Specifies whether or not to validate reply data.



Data pattern [0xABCD]:

!--- Specifies the data pattern in the ping payload. Some physical links
!--- might exhibit data pattern dependent problems. For example, serial links
!--- with misconfigured line coding. Some useful data patterns to test
!--- include all 1s (0Xffff), all 0s (0x0000) and alternating
!--- ones and zeros (0Xaaaa).



Loose, Strict, Record, Timestamp, Verbose[none]:

!--- IP header options.



Sweep range of sizes [n]: y

!--- Choose yes if you want to vary the sizes on echo packets that are sent.



Sweep min size [36]:
Sweep max size [18024]:
Sweep interval [1]:
```

```
Sending 179890, [36..18024]-byte ICMP Echos to 192.168.40.1, timeout is 2 seconds:


!--- The count 179890 depends on the values of min sweep,
!--- max sweep, sweep interval and repeat count. Calculations are based on:
!--- 18024(high end of range) - 36(low end of range) = 17988(bytes in range)
!--- 17988(bytes in range) / 1(sweep interval) = 17988 (steps in range)
!--- 17988(bytes in range) + 1 (first value) = 17989(values to be tested)
!--- 17989(values to be tested) * 10(repeat count) = 179890 (pings to be sent)
!--- In order to decrease the value, increase the sweep interval or decrease
!--- the repeat count, or you can even decrease the difference between
!--- Minimum and Maximum sweep size. Based on the previous example, the
!--- number 17890 is an expected value and tries to ping 17890 times.


Packet sent with a source address of 172.16.23.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms


!--- Ping is successful.


RouterA#
```

「 traceroute コマンド

pingを使用してデバイス間の接続を確認できる場合は、 traceroute コマンドを使用して、ルーティングに障害が発生している場所だけでなく、パケットが通過するリモート宛先へのパスを検出できます。

その目的は、 traceroute コマンドは、各ICMP「time exceeded」メッセージの送信元を記録して、パケットが宛先に到達するまでにたどるパスのトレースを提供します。

を実行するデバイス traceroute コマンドは、一連のUser Datagram Protocol（UDP；ユーザデータグラムプロトコル）データグラムを、それぞれTime-To-Live（TTL；存続可能時間）値が増分された状態で、リモートホストの無効なポートアドレス(デフォルトは33434)に送信します。

まず始めに 3 つのデータグラムが送信されます。それぞれの TTL フィールドの値は 1 に設定され

ています。TTL 値が 1 の場合には、データグラムがパス上の最初のルータに到達した時点で、すぐにタイムアウトになります。次に、このルータは、データグラムが期限切れになったことを示すICMP time exceededメッセージで応答します。

次に、さらに 3 つの UDP メッセージが送信されます。それぞれの TTL 値は 2 に設定されています。これにより、宛先へのパスの2番目のルータがICMP「time exceeded」メッセージを返します。

このプロセスは、パケットが宛先に到達し、パケットの送信元のシステムが traceroute 宛先までのパスにあるすべてのルータからICMP「time exceeded」メッセージを受信します。これらのデータグラムは宛先ホストの無効なポート(デフォルトは33434)へのアクセスを試みるため、ホストは到達不能ポートを示すICMPポート到達不能メッセージで応答します。このイベントにより、traceroute プログラムは終了するよう通知されます。

注：どの VLAN でも、ip unreachable コマンドを no ip unreachables で無効にしていないことを確認してください。このコマンドは、ICMP エラーメッセージなしでパケット破棄メッセージを生成します。その場合、traceroute は機能しません。

拡張 traceroute コマンド

拡張された traceroute コマンドは、 traceroute コマンドを使用して、アップグレードを実行します。拡張 traceroute コマンドを使用して、パケットが宛先に到達するまでにたどるパスを確認できます。同時に、このコマンドは、ルーティングをチェックするためにも使用できます。これは、ルーティングループのトラブルシューティングを行う場合や、パケットが失われた場所（ルートが失われた場合、またはパケットがアクセス制御リスト（ACL）またはファイアウォールによってブロックされた場合）を特定する際に役立ちます。拡張 ping コマンドを使用して接続上の問題の種類を判断した後、拡張 traceroute コマンドを使用して問題の発生箇所を絞り込むことができます。

「time exceeded」エラーメッセージは、中継通信サーバがパケットを確認し、破棄したことを示します。destination unreachableエラーメッセージは、宛先ノードがプローブを受信し、パケットを配信できなかったためにプローブを廃棄したことを示します。応答が受信される前にタイマーがオフになった場合、trace ではアスタリスク（*）が表示されます。このコマンドは、次のいずれかが発生した場合に終了します。

- 宛先が応答した場合
- 最大 TTL を超えた場合
- ユーザがエスケープ シーケンスによりトレースを中断した場合

注：Ctrl、Shift、6 を同時に押すと、このエスケープシーケンスを呼び出すことができます。

---

traceroute コマンドのフィールドの説明

次の表に、traceroute コマンドのフィールドの説明を示します。

フィールド	説明
Protocol [ip]:	サポートされているプロトコルを入力するように要求されます。appletalk、clns、ip、novell、apollo、vines、decnet、または xns を入力します。デフォルトは ip です。
Target IP address	ホスト名または IP アドレスを入力する必要があります。デフォルトはありませ ん。
発信元アドレス：	プローブの送信元アドレスとして使用するルータのインターフェイスまたは IP アドレス。ルータは、通常、使用する送信インターフェイスの IP アドレスを選択します。
Numeric display [n]:	デフォルトでは、シンボルと数値の両方が表示されます。ただし、シンボルは非表示にできます。
Timeout in seconds [3]:	プローブ パケットへの応答を待機する秒数。デフォルトは 3 秒です。
Probe count [3]:	各 TTL レベルで送信されるプローブの数。デフォルトは 3 です。
Minimum Time to Live [1]:	最初のプローブの TTL 値。デフォルトは 1 ですが、既知のホッ プを非表示にするため、より大きな値に設定できます。
Maximum Time to Live [30]:	使用可能な最大 TTL 値。デフォルトは 30 です。「 traceroute コマンドは、宛先に到達したとき、またはこの値に到達したときに終了します。
Port Number [33434]:	UDP プローブ メッセージで使用される宛先ポート。デフォルトは 33434 です。
Loose, Strict, Record, Timestamp, Verbose[none]:	IP ヘッダーのオプション。任意の組み合わせを指定できます。「 traceroute コマンドは、必要な

	フィールドのプロンプトを発行します。次の点に注意してください traceroute コマンドは要求されたオプションを各プローブに配置しますが、すべてのルータ（またはエンドノード）がオプションを処理するとは限りません。

例

<#root>

```
RouterA>
enable

RouterA#
traceroute

Protocol [ip]:
Target IP address: 192.168.40.2

!--- The address to which the path is traced.

Source address: 172.16.23.2
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.40.2

1 172.31.20.2 16 msec 16 msec 16 msec
2 172.20.10.2 28 msec 28 msec 32 msec
3 192.168.40.2 32 msec 28 msec *

!--- The traceroute is successful.

RouterA#
```


注：拡張 traceroute コマンドは特権EXECモードでのみ実行できますが、 traceroute コマンドは、ユーザEXECモードと特権EXECモードの両方で機能します。

関連情報

- TCP/IP ルーテッド プロトコル テクノロジーに関するページ
- IP ルーティングに関するサポート ページ
- ping および traceroute コマンドについて
- オペレーティングシステムでの traceroute コマンドの使用
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。