

확장 ping 및 확장 traceroute 명령 이해

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[ping 명령](#)

[확장 ping 명령](#)

[ping 명령 필드 설명](#)

[traceroute 명령](#)

[확장 traceroute 명령](#)

[traceroute 명령 필드 설명](#)

[관련 정보](#)

소개

이 문서에서는 확장 기능을 사용하는 방법을 설명합니다 ping 그리고 확장된 traceroute 명령을 사용합니다.

사전 요구 사항

요구 사항

이 문서에는 ping 및 traceroute 명령을 사용합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어
- 모든 Cisco 시리즈 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco Technical Tips Conventions](#)를 참조하십시오.

이 ping 명령을 사용합니다

이 ping (Packet InterNet Groper) 명령은 디바이스의 액세스 가능성 문제를 해결하기 위한 매우 일반적인 방법입니다. 2가지 ICMP(Internet Control Message Protocol) 쿼리 메시지, ICMP 에코 요청과 ICMP 에코 회신을 사용하여 원격 호스트의 활성 상태 여부를 확인합니다. 이 ping 또한 명령은 에코 응답을 수신하는 데 걸리는 시간을 측정합니다.

이 ping 명령은 먼저 에코 요청 패킷을 주소로 전송한 다음 응답을 기다립니다. 이 ping 는 ECHO REQUEST가 목적지에 도달하고 목적지가 ECHO REPLY를 의 소스로 다시 가져올 수 있는 경우에만 성공합니다. ping 미리 정의된 시간 간격 내에 포함됩니다.

확장된 ping 명령을 사용합니다

정상적인 경우 ping 이 명령은 라우터에서 전송되며 ping의 소스 주소는 패킷이 라우터를 종료하는 데 사용하는 인터페이스의 IP 주소입니다. 확장되면 ping 명령을 사용하면 소스 IP 주소를 라우터의 모든 IP 주소로 변경할 수 있습니다. 확장된 ping 은(는) 호스트 연결성 및 네트워크 연결을 보다 상세하게 확인하는 데 사용됩니다. 확장된 ping 명령은 특별 권한 EXEC 명령줄에서만 작동합니다. 더 노멀 ping 사용자 EXEC 모드와 특권 EXEC 모드에서 모두 작동합니다. 이 기능을 사용하려면 다음을 입력합니다 ping 명령줄에서 Return 키를 누릅니다. 이 문서의 ping 명령 필드 설명 섹션에 따라 필드 입력 메시지가 나타납니다.

이 ping 명령 필드 설명

이 표에는 ping 명령 필드 설명 이러한 필드는 extended를 사용하여 수정할 수 있습니다 ping 명령을 실행합니다.

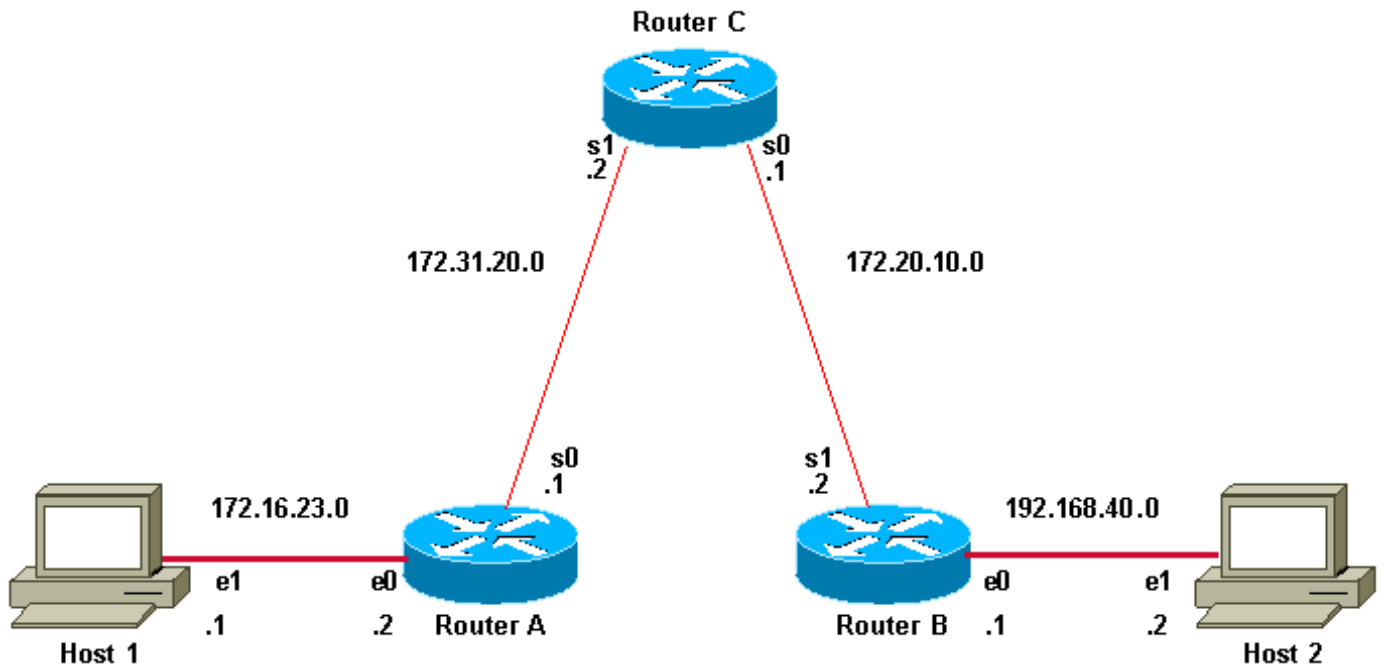
필드	설명
Protocol [ip]:	지원되는 프로토콜에 대한 프롬프트입니다. appletalk, clns, ip, novell, apollo, vines, decnet 또는 xns를 입력합니다. 기본값은 ip입니다.
Target IP address:	ping하려는 대상 노드의 IP 주소 또는 호스트 이름에 대한 프롬프트입니다. 지원되는 프로토콜로 IP가 아닌 값을 지정한 경우, 해당 프로토콜에 적합한 주소를 여기에 입력합니다. 기본값은 none(없음)입니다.
Repeat count [5]:	목적지 주소로 보내진 ping 패킷 수. 기본값은 5입니다.
Datagram size [100]:	ping 패킷 크기(바이트)입니다. 기본값: 100바이트

	트.
Timeout in seconds [2]:	시간 초과 간격입니다. 기본값: 2(초) 이 시간 초과 간격 이전에 ECHO REPLY 패킷을 수신한 경우에만 ping이 성공한 것으로 간주합니다.
Extended commands [n]:	일련의 추가 명령이 나타나는지 여부를 지정합니다. 기본값은 no입니다.
인그레스 ping [n]:	인그레스 ping은 지정된 인그레스 인터페이스에서 수신된 패킷을 대상 대상으로 시뮬레이션합니다. 기본값은 no입니다. (이 옵션의 사용 가능 여부는 사용된 소프트웨어 릴리스와 다름)
Source address or interface:	프로브의 소스 주소로 사용할 라우터의 인터페이스 또는 IP 주소입니다. 일반적으로 라우터는 사용할 아웃바운드 인터페이스의 IP 주소를 선택합니다. 인터페이스도 언급할 수 있으나, 다음과 같은 정확한 구문을 사용해야 합니다. Source address or interface: ethernet 0 참고: 확장 의 일부 출력입니다. ping 명령을 실행합니다. 인터페이스를 e0로 표시할 수 없습니다.
DSCP 값 [0]:	DSCP(Differentiated Services Code Point)를 지정합니다. 도입된 DSCP 값은 각 프로브에 배치됩니다. 기본값은 0입니다. 이 옵션의 사용 가능 여부는 사용된 소프트웨어 릴리스와 다릅니다.
Type of service [0]:	ToS(Type of Service)를 지정합니다. 요청된 ToS는 각 프로브에 위치합니다. 그러나 모든 라우터가 ToS를 처리한다는 보장은 없습니다. Internet Quality of Service 선택입니다. 기본값은 0입니다.
Set DF bit in IP header? [no]:	WebEx가 Don't Fragment (DF) ping 패킷에서 비트를 설정합니다. yes를 지정하면 DF 옵션은 패킷이 더 작은 MTU(최대 전송 단위)의 세그먼트를 통

	<p>과해야 할 때 이 패킷을 프래그먼트화할 수 없으며, 패킷을 프래그먼트화하려는 디바이스에서 오류 메시지를 수신합니다. 이는 대상에 대한 경로에서 가장 작은 MTU를 확인하는 데 유용합니다. 기본값은 no입니다.</p>
<p>Validate reply data? [no]:</p>	<p>회신 데이터를 검증할지 여부를 지정합니다. 기본값은 no입니다.</p>
<p>Data pattern [0xABCD]</p>	<p>데이터 패턴을 지정합니다. 트러블슈팅에 다양한 데이터 패턴이 사용됨 framing 오류 및 clocking 직렬 회선에 문제가 있습니다. 기본값은 [0xABCD]입니다.</p>
<p>Loose, Strict, Record, Timestamp, Verbose[none]:</p>	<p>IP 헤더 옵션입니다. 이 프롬프트에서는 2가지 이상의 옵션 중에서 선택할 수 있습니다. 제품:</p> <ul style="list-style-type: none"> • Verbose는 다른 옵션과 함께 자동으로 선택됩니다. • Record는 패킷이 통과하는 홑(최대 9개)의 주소를 표시하기 때문에 매우 유용한 옵션입니다. • Loose(느슨함)를 사용하면 패킷이 통과할 홑의 주소를 지정할 때 경로에 영향을 줄 수 있습니다. • Strict는 패킷이 지날 홑을 지정할 때 사용합니다. 다른 어떤 홑도 방문할 수 없습니다. • Timestamp는 특정 호스트와의 왕복 시간을 측정할 때 사용합니다. <p>이 명령의 Record 옵션과 traceroute 명령의 차이점은 Record 옵션은 에코 요청(ping)이 목적지에 도달하기 위해 통과한 홑을 알려줄 뿐만 아니라 반환 경로에서 방문한 홑을 알려준다는 것입니다. traceroute 명령을 사용하면, 에코 회신의 경로에 관한 정보는 얻지 못합니다. traceroute 명령은 필수 필드에 관한 정보를 묻습니다.</p> <p>traceroute 명령은 각 프로브에 요청된 옵션을 배치합니다. 그러나 모든 라우터(또는 엔드 노드)가 이 옵션을 처리한다는 보장은 없습니다. 기본값은 none(없음)입니다.</p>

Sweep range of sizes [n]:	전송되는 에코 패킷의 크기를 다르게 할 수 있습니다. 노드에 구성된 MTU의 최소 크기를 대상 주소에 대한 경로와 함께 확인하는 데 사용됩니다. 그러면 패킷 프래그먼트화로 인한 성능 문제가 줄어듭니다. 기본값은 no입니다.
!!!!	각 느낌표(!)는 회신을 받았음을 나타냅니다. 마침표(.)는 네트워크 서버가 응답을 대기하는 시간을 초과했음을 나타냅니다. 다른 문자에 대한 설명 은 ping 문자를 참조하십시오.
Success rate is 100 percent	성공적으로 라우터에 에코 응답한 패킷의 비율입니다. 80퍼센트 미만은 보통 문제가 있는 것으로 간주된다.
round-trip min/avg/max = 1/2/4 ms	최소/평균/최대(밀리초)의 프로토콜 에코 패킷에 대한 왕복 이동 시간 간격입니다.

이 다이어그램에서 호스트 1과 호스트 2는 서로 ping할 수 없습니다. 라우터에서 이 문제를 해결하여 라우팅 문제가 있는지 또는 두 호스트 중 하나에 기본 게이트웨이가 올바르게 설정되지 않았는지 확인할 수 있습니다.



호스트 1 및 호스트 2는 Ping할 수 없습니다.

를 위해 ping 성공하려면 호스트 1에서 호스트 2까지 각 호스트가 해당 LAN 세그먼트의 라우터에 기본 게이트웨이를 지정하거나, 호스트가 라우팅 프로토콜을 사용하는 라우터와 네트워크 정보를 교환해야 합니다. 두 호스트 중 하나에 기본 게이트웨이가 올바르게 설정되어 있지 않거나 라우팅 테

이불에 올바른 경로가 없으면 ARP(Address Resolution Protocol) 캐시에 없는 대상으로 패킷을 전송할 수 없습니다. 라우터 중 하나에 호스트가 핑 패킷을 소싱할 서브넷에 대한 경로가 없기 때문에 호스트가 서로 ping할 수 없는 경우도 있습니다.

예

이는 라우터 A 이더넷 0 인터페이스가 소스이고 라우터 B 이더넷 인터페이스가 대상인 확장 ping 명령의 예입니다. 이 ping이 성공한다면 라우팅 문제가 없음을 의미합니다. 라우터 A는 라우터 B의 이더넷에 도달하는 방법을 알고 있고, 라우터 B는 라우터 A의 이더넷에 도달하는 방법을 알고 있습니다. 또한 두 호스트 모두 기본 게이트웨이가 올바르게 설정되어 있습니다.

확장되면 ping 라우터 A의 명령이 실패하고 라우팅 문제가 있음을 의미합니다. 3개의 라우터 중 하나에 라우팅 문제가 생겼을 수도 있습니다. 라우터 A는 라우터 B 이더넷의 서브넷 또는 라우터 C와 라우터 B 사이의 서브넷에 대한 경로를 잃을 수 있습니다. 라우터 B는 라우터 A의 서브넷 또는 라우터 C와 라우터 A 사이의 서브넷에 대한 경로를 잃을 수 있으며 라우터 C는 라우터 A 또는 라우터 B 이더넷 세그먼트의 서브넷에 대한 경로를 잃을 수 있습니다. 라우팅 문제를 모두 해결한 다음 호스트 1에서 호스트 2에 ping을 시도해야 합니다. 호스트 1에서 여전히 호스트 2를 ping할 수 없는 경우 두 기본 게이트웨이를 모두 확인해야 합니다. 라우터 A 이더넷과 라우터 B 이더넷 간의 연결을 확장 ping 명령으로 확인합니다.

라우터 A에서 라우터 B 이더넷 인터페이스로 일반 ping을 수행할 경우 ping 패킷의 소스 주소는 발신 인터페이스의 주소, 즉 직렬 0 인터페이스(172.31.20.1)의 주소입니다. 라우터 B가 ping 패킷에 회신할 때 소스 주소(즉, 172.31.20.1)에 회신합니다. 그러면 라우터 A의 시리얼 0 인터페이스(172.31.20.1)와 라우터 B의 이더넷 인터페이스(192.168.40.1) 간 연결만 테스트합니다.

라우터 A 이더넷 0(172.16.23.2)과 라우터 B 이더넷 0(192.168.40.1) 간의 연결을 테스트하려면 확장 ping 명령을 실행합니다. 확장 ping의 소스 주소를 지정하는 옵션이 제공됩니다. ping패킷(여기에 표시된 것처럼):

```
<#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).

이 `traceroute` 명령을 사용합니다

디바이스 간 연결을 확인하는 데 ping을 사용할 수 있는 경우 `traceroute` 명령을 사용하여 패킷이 원격 대상으로 이동하는 경로 및 라우팅이 중단된 위치를 검색할 수 있습니다.


Cisco의 목표는 `traceroute` 명령은 패킷이 목적지에 도달하는 데 걸린 경로의 추적을 제공하기 위해 각 ICMP 시간 초과 메시지의 소스를 기록합니다.

를 실행하는 디바이스 `traceroute` 이 명령은 TTL(Time-To-Live) 값 증가분을 갖는 UDP(User Datagram Protocol) 데이터그램의 시퀀스를 원격 호스트의 잘못된 포트 주소(Default 33434)로 전송합니다.

먼저 3개의 데이터그램을 보내는데, 각각 TTL 필드 값이 1로 설정되어 있습니다. TTL 값 1을 지정하면 데이터그램이 경로의 첫 번째 라우터에 도달하는 즉시 시간 초과됩니다. 그런 다음 이 라우터는 데이터그램이 만료되었음을 나타내는 ICMP time exceeded 메시지로 응답합니다.

그 다음에 3개의 UDP 메시지를 추가로 보내는데, 각각 TTL 값이 2로 설정되어 있습니다. 그러면 대상에 대한 경로의 두 번째 라우터가 ICMP 시간 초과 메시지를 반환합니다.

이 프로세스는 패킷이 대상에 도달할 때까지 그리고 를 시작하는 시스템이 시작할 때까지 계속됩니다. `traceroute` 대상에 대한 경로의 모든 라우터에서 ICMP 시간 초과 메시지를 수신합니다. 이러한 데이터그램은 목적지 호스트에서 유효하지 않은 포트(기본 33434)에 액세스하려고 시도하므로, 호스트는 도달할 수 없는 포트를 나타내는 ICMP 포트 도달할 수 없는 메시지로 응답합니다. 이 이벤트는 트레이스라우트(traceroute) 프로그램의 종료를 나타냅니다.


 참고: VLAN에서 `no ip unreachable(no ip unreachable)` 명령과 함께 `ip unreachable` 명령을 비활성화하지 않았는지 확인합니다. 이 명령을 사용하면 패킷이 ICMP 오류 메시지 없이 메시지를 폐기합니다. 이 경우에는 트레이스라우트(traceroute)가 작동하지 않습니다.

확장 `traceroute` 명령

확장된 `traceroute` 명령은 `traceroute` 명령을 실행합니다. 확장 `traceroute` 명령을 사용하여 패킷이 목적지로 도달하는 데 어떤 경로를 사용하는지 확인할 수 있습니다. 이 명령은 동시에 라우팅을 확인할 때에도 사용할 수 있습니다. 이는 라우팅 루프 문제를 해결할 때 또는 패킷이 손실되는 위치를 결정할 때(경로가 사라진 경우 또는 패킷이 ACL(Access Control List) 또는 방화벽에 의해 차단된 경우)에 유용합니다. 연결 문제의 유형을 확인하기 위해 확장 ping 명령을 사용한 다음, 문제 발생 범위를 좁히기 위해 확장 `traceroute` 명령을 사용할 수 있습니다.

시간 초과 오류 메시지는 중간 통신 서버에서 패킷을 확인하고 삭제했음을 나타냅니다. 목적지 도달 불가 오류 메시지는 목적지 노드가 프로브를 수신한 후 패킷을 전달할 수 없어 이를 삭제했음을 나타냅니다. 응답을 수신하기 전에 타이머가 종료한 경우 trace는 별표(*)를 출력합니다. 다음과 같은 조건이 되면 이 명령은 종료합니다.

- 대상이 응답합니다.
- 최대 TTL을 초과했습니다.
- 사용자가 이스케이프 시퀀스로 추적을 인터럽트합니다.

 참고: Ctrl, Shift 및 6을 동시에 누를 때 이 이스케이프 시퀀스를 호출할 수 있습니다.

traceroute 명령 필드 설명

다음 표는 traceroute 명령 필드 설명을 정리한 것입니다.

필드	설명
Protocol [ip]:	지원되는 프로토콜에 대한 프롬프트입니다. appletalk, clns, ip, novell, apollo, vines, decnet 또는 xns를 입력합니다. 기본값은 ip입니다.
Target IP address	호스트 이름 또는 IP 주소를 입력해야 합니다. 기본값이 없습니다.
Source address:	프로브의 소스 주소로 사용할 라우터의 인터페이스 또는 IP 주소입니다. 일반적으로 라우터는 사용할 아웃바운드 인터페이스의 IP 주소를 선택합니다.
Numeric display [n]:	기본값은 기호 표시와 숫자 표시를 모두 사용하는 것이지만 기호 표시를 억제할 수 있습니다.
Timeout in seconds [3]:	프로브 패킷에 대한 응답을 기다리는 시간(초)입니다. 기본값은 3초입니다.
Probe count [3]:	각 TTL 수준에서 전송할 프로브 수입니다. 기본 count는 3입니다.
Minimum Time to Live [1]:	첫 번째 프로브의 TTL 값입니다. 기본값은 1이지만 더 높은 값으로 설정하여 알려진 홉 표시를 무시할 수 있습니다.
Maximum Time to Live [30]:	사용할 수 있는 최대 TTL 값입니다. 기본값은 30입니다. 이 traceroute 목적지에 도달하거나 이 값에 도달하면 명령이 종료됩니다.

Port Number [33434]:	UDP 프로브 메시지에서 사용하는 대상 포트입니다. 기본값은 33434입니다.
Loose, Strict, Record, Timestamp, Verbose[none]:	IP 헤더 옵션입니다. 어떤 조합도 지정할 수 있습니다. 이 <code>traceroute</code> 명령에서 필수 필드에 대한 프롬프트를 표시합니다. 참고: <code>traceroute</code> 명령은 각 프로브에 요청된 옵션을 배치합니다. 그러나 모든 라우터(또는 엔드 노드)가 옵션을 처리한다는 보장은 없습니다.

예

```
<#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#
```

 참고: 확장 `traceroute` 명령은 특별 권한 EXEC 모드에서만 실행할 수 있는 반면 일반 명령은 `traceroute` 명령은 사용자 및 특권 EXEC 모드에서 모두 작동합니다.

관련 정보

- [TCP/IP 라우팅 프로토콜 기술 페이지](#)
- [IP 라우팅 지원 페이지](#)
- [Ping 및 Traceroute 명령 이해](#)
- [운영 체제에서 Traceroute 명령 사용](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.