

Comprendere il ping esteso e i comandi estesi di tracciamento routing

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Il comando ping](#)

[Il comando ping esteso](#)

[Descrizioni dei campi del comando ping](#)

[Il comando traceroute](#)

[Il comando traceroute esteso](#)

[Descrizioni dei campi del comando traceroute](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come utilizzare il `ping` e il sistema `traceroute` comandi.

Prerequisiti

Requisiti

Questo documento richiede la conoscenza preliminare `ping` e `traceroute` comandi.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS®
- Router Cisco tutte le serie

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

OSPF (Open Shortest Path First) `ping` Comando

OSPF (Open Shortest Path First) `ping` (Packet InterNet Groper) viene usato spesso per risolvere i problemi di

accessibilità dei dispositivi. Usando due query sul protocollo Internet Control Message Protocol (ICMP), le richieste echo ICMP e le risposte echo ICMP, permette di stabilire se un host remoto è attivo. OSPF (Open Shortest Path First) ping Questo comando misura anche il tempo necessario per ricevere la risposta echo.

OSPF (Open Shortest Path First) ping invia un pacchetto di richiesta echo a un indirizzo, quindi attende una risposta. OSPF (Open Shortest Path First) ping ha esito positivo solo se la RICHIESTA ECHO raggiunge un dispositivo di destinazione e questi è in grado di generare una RISPOSTA ECHO per il dispositivo da cui è stata inviata la richiesta ping entro un intervallo di tempo predefinito.

La scheda ping Comando

Quando un normale ping Quando il comando viene inviato da un router, l'indirizzo di origine del ping corrisponde all'indirizzo IP dell'interfaccia usata dal pacchetto per uscire dal router. Se un ping , l'indirizzo IP di origine può essere modificato in qualsiasi indirizzo IP del router. La scheda ping viene utilizzato per verificare in modo più approfondito se l'host è raggiungibile e la rete connessa. La scheda ping funziona solo sulla riga di comando in modalità di esecuzione privilegiata. Il normale ping funziona sia in modalità di esecuzione utente sia in modalità di esecuzione privilegiata. Per utilizzare questa funzione, immettere: ping sulla riga di comando e premere Invio. Vengono visualizzati i campi indicati nella sezione Descrizioni dei campi del comando ping di questo documento.

OSPF (Open Shortest Path First) ping Descrizioni dei campi del comando

In questa tabella sono elencati ping descrizioni dei campi del comando. I campi possono essere modificati utilizzando il comando ping

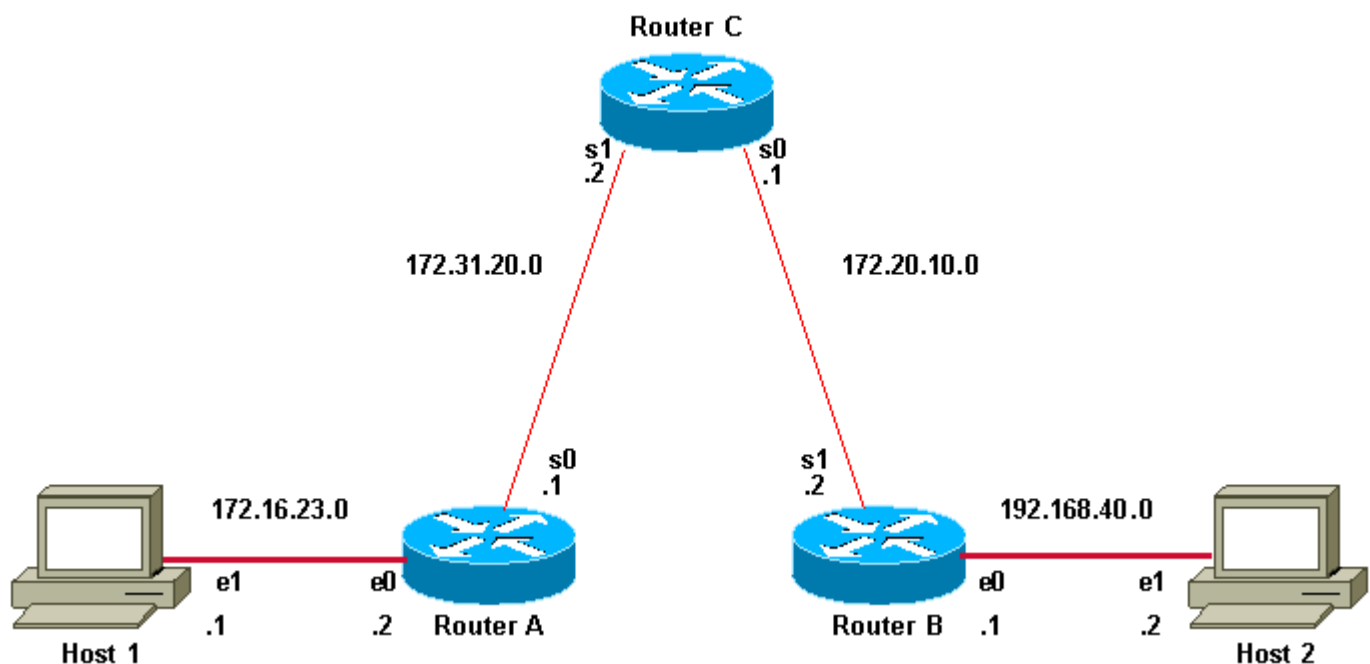
Campo	Descrizione
Protocol [ip]:	Richiede un protocollo supportato. Specificare appletalk, clns, ip, novell, apollo, vines, decnet o xns. Il valore predefinito è ip.
Target IP address:	Richiede l'indirizzo IP o il nome host del nodo di destinazione su cui si intende eseguire il ping. Se il protocollo specificato è diverso da IP, specificare qui un indirizzo appropriato per il protocollo. Il valore predefinito è none (nessuno).
Repeat count [5]:	Numero di pacchetti ping che vengono inviati all'indirizzo di destinazione. Il valore predefinito è 5.
Datagram size [100]:	Dimensioni del pacchetto ping (in byte). Impostazione predefinita: 100 byte.
Timeout in seconds [2]:	Intervallo di timeout. Impostazione predefinita: 2 (secondi). Il ping è ritenuto riuscito solo se il pacchetto di RISPOSTA ECHO viene ricevuto prima di questo intervallo di tempo.

Extended commands [n]:	Permette di specificare se visualizzare una serie di comandi aggiuntivi. Il valore predefinito è no.
ping in ingresso [n]:	<p>Il comando ping in entrata simula alla destinazione i pacchetti ricevuti sull'interfaccia in entrata specificata. Il valore predefinito è no.</p> <p>(la disponibilità di questa opzione è diversa dalla versione software in uso)</p>
Source address or interface:	<p>L'interfaccia o l'indirizzo IP del router che le sonde useranno come indirizzo di origine. Il router in genere sceglie l'indirizzo IP dell'interfaccia in uscita da utilizzare. È possibile specificare anche l'interfaccia, ma con la sintassi corretta, illustrata di seguito:</p> <p>Source address or interface: ethernet 0</p> <p>Nota: questo è l'output parziale del ping L'interfaccia non può essere scritta come e0.</p>
DSCP Value [0]:	Specifica il DSCP (Differentiated Services Code Point). Il valore DSCP introdotto viene inserito in ciascuna sonda. Il valore predefinito è 0. (La disponibilità di questa opzione è diversa da quella della versione software in uso)
Type of service [0]:	Permette di specificare il tipo di servizio (ToS). Il tipo di servizio richiesto viene incluso in ciascuna sonda, ma non è possibile assicurare che tutti i router elaborino il tipo di servizio. È una scelta basata sulla qualità del servizio di Internet. Il valore predefinito è 0.
Set DF bit in IP header? [no]:	Specifica se il Don't Fragment (DF) il bit deve essere impostato sul pacchetto ping. Se si specifica yes (sì) e il pacchetto deve passare attraverso un segmento con MTU (Maximum Transmission Unit) più piccola, l'opzione DF impedisce che il pacchetto venga frammentato. L'utente riceverà un messaggio di errore dal dispositivo che intendeva frammentare il pacchetto. Questa opzione permette di determinare l'MTU più piccola nel percorso verso una destinazione. Il valore predefinito è no.
Validate reply data? [no]:	Permette di specificare se convalidare i dati della

	risposta. Il valore predefinito è no.
Data pattern [0xABCD]	Specifica il modello di dati. I diversi modelli di dati vengono utilizzati per la risoluzione dei problemi framing errori e clocking problemi sulle linee seriali. Il valore predefinito è [0xABCD].
Loose, Strict, Record, Timestamp, Verbose[none]:	<p>Opzioni dell'intestazione IP. Per questa richiesta è possibile selezionare più di un'opzione:</p> <ul style="list-style-type: none"> • L'opzione Verbose (Dettagliata) viene selezionata automaticamente con qualsiasi altra opzione. • L'opzione Record è molto utile perché visualizza gli indirizzi degli hop (fino a nove) attraverso cui deve passare il pacchetto. • L'opzione Loose (Permissiva) consente di influenzare il percorso quando si specificano gli indirizzi degli hop attraverso cui deve passare il pacchetto. • L'opzione Strict (Rigorosa) viene usata per specificare gli hop attraverso cui deve passare il pacchetto, escludendo gli hop che non devono essere attraversati. • L'opzione Timestamp (Data e ora) viene usata per misurare il tempo di ritorno da determinati host. <p>La differenza tra l'opzione Record del comando ping e il comando traceroute è che l'opzione Record informa l'utente sia degli hop attraversati dalla richiesta echo (ping) fino alla destinazione sia degli hop visitati sul percorso di ritorno. Il comando traceroute non restituisce informazioni sul percorso della risposta echo. Il comando traceroute chiede di specificare i campi obbligatori.</p> <p>Il comando traceroute include le opzioni richieste in ciascuna sonda. Tuttavia, non vi è alcuna garanzia che le opzioni siano elaborate da tutti i router (o nodi finali). Il valore predefinito è none (nessuno).</p>
Sweep range of sizes [n]:	Permette di modificare le dimensioni dei pacchetti echo inviati. Questa opzione viene usata per determinare le dimensioni minime delle MTU configurate sui nodi del percorso all'indirizzo di destinazione. Riduce inoltre i problemi di prestazioni causati dalla frammentazione dei pacchetti. Il valore predefinito è no.

!!!!	Ogni punto esclamativo (!) indica la ricezione di una risposta. Un punto (.) indica che il server di rete è scaduto durante l'attesa di una risposta. Fare riferimento ai caratteri ping per una descrizione degli altri caratteri.
Success rate is 100 percent	La percentuale di pacchetti correttamente restituiti dal router. Qualsiasi percentuale inferiore a 80 è in genere considerata problematica.
round-trip min/avg/max = 1/2/4 ms	Intervalli di tempo di andata e ritorno dei pacchetti echo del protocollo con valore minimo/medio/massimo (in millisecondi).

In questo diagramma, l'host 1 e l'host 2 non sono in grado di comunicare tra loro. È possibile risolvere questo problema sui router per stabilire se è presente un problema di routing o se il gateway predefinito di uno dei due host non è impostato correttamente.



L'host 1 e l'host 2 non possono eseguire il ping

Al fine di pingdall'host 1 all'host 2, per funzionare correttamente, ciascun host deve puntare il gateway predefinito al router sul rispettivo segmento LAN, oppure l'host deve scambiare le informazioni di rete con i router che usano un protocollo di routing. Se su uno dei due host il gateway predefinito non è impostato correttamente oppure i percorsi nella tabella di routing non sono corretti, non sarà possibile inviare i pacchetti alle destinazioni che non sono incluse nella cache ARP (Address Resolution Protocol). Inoltre, è possibile che gli host non possano eseguire il ping tra loro perché uno dei router non dispone di un percorso alla subnet da cui l'host origina i pacchetti ping.

Esempio

Questo è un esempio di comando ping esteso inviato dall'interfaccia Ethernet 0 del router A e destinato all'interfaccia Ethernet del router B. Se il ping ha esito positivo, non vi è alcun problema di routing. Il router

A può raggiungere l'interfaccia Ethernet del router B e il router B può raggiungere l'interfaccia Ethernet del router A. Inoltre, su entrambi gli host il gateway predefinito è impostato correttamente.

Se il valore `ping`Il comando dal router A ha esito negativo, indica che è presente un problema di routing. Il problema di routing potrebbe riguardare uno dei tre router. Il router A potrebbe aver perso il percorso alla subnet dell'interfaccia Ethernet del router B o alla subnet tra il router C e il router B. Il router B potrebbe aver perso il percorso alla subnet del router A o alla subnet tra il router C e il router A e il router C potrebbe aver perso il percorso alla subnet del router A o ai segmenti Ethernet del router B. Per risolvere i problemi di routing, provare a eseguire il ping tra l'host 1 e l'host 2. Se l'host 1 non comunica con l'host 2, controllare entrambi i gateway predefiniti. Per controllare la connettività tra l'interfaccia Ethernet del router A e l'interfaccia Ethernet del router B, usare il comando `ping` esteso.

Se le interfacce Ethernet del router A e del router B comunicano normalmente, l'indirizzo di origine del pacchetto ping corrisponde all'indirizzo dell'interfaccia in uscita, ossia l'indirizzo dell'interfaccia 0 seriale (172.31.20.1). Quando il router B risponde al pacchetto ping, risponde all'indirizzo di origine (ossia 172.31.20.1). In questo modo, viene verificata solo la connettività tra l'interfaccia 0 seriale del router A (172.31.20.1) e l'interfaccia Ethernet del router B (192.168.40.1).

Per verificare la connettività tra l'interfaccia Ethernet 0 del router A (172.16.23.2) e l'interfaccia Ethernet 0 del router B (192.168.40.1), usare il comando `ping` Con estensione `ping`, è possibile specificare l'indirizzo di origine del ping come mostrato di seguito:

```
<#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.

Protocol), con incrementi TTL (Time-To-Live), a un indirizzo di porta non valido (predefinito: 33434) sull'host remoto.

All'inizio, vengono inviati tre datagrammi, il cui valore TTL è 1. Quando il valore TTL è 1, il datagramma scade non appena incontra il primo router del percorso. Questo router risponde quindi con un messaggio ICMP "tempo scaduto" per segnalare che il datagramma è scaduto.

Successivamente, vengono inviati altri tre messaggi UDP, il cui valore TTL è 2. In questo modo, sarà il secondo router del percorso a restituire un messaggio ICMP "tempo scaduto".

Questo processo continua finché i pacchetti non raggiungono la destinazione e finché il sistema da cui proviene il `traceroute` riceve messaggi ICMP "time exceeded" (tempo scaduto) da ogni router del percorso verso la destinazione. Poiché questi datagrammi provano ad accedere a una porta non valida (per impostazione predefinita 33434) sull'host di destinazione, l'host risponde con messaggi ICMP "port unreachable" (porta non raggiungibile) per segnalare che non è possibile accedere alla porta. Questo evento determina la fine del programma `traceroute`.

Nota: verificare di aver disattivato il comando **ip unreachable** usando il comando **no ip unreachables** in ciascuna rete VLAN. Con questo comando il pacchetto viene scartato senza alcun messaggio di errore ICMP. In questo caso, il comando `traceroute` non funziona.

Il comando `traceroute` esteso

La scheda `traceroute` è una variante del comando `traceroute` e può essere usato per verificare il percorso scelto dal pacchetto per raggiungere la destinazione. Allo stesso tempo, il comando può verificare anche il routing. Questo comando è utile quando si devono risolvere problemi di loop di routing o quando si deve capire dove il pacchetto si è fermato (per un percorso omissso o per il blocco effettuato da un Access Control List (ACL) o da un firewall). È possibile usare il comando `ping` esteso per capire il tipo di problema di connettività e usare poi il comando `traceroute` esteso per individuare il punto in cui si è verificato.

Un messaggio di errore tempo scaduto indica che un server di comunicazione intermedio ha rilevato il pacchetto e lo ha rifiutato. Un messaggio di errore `destination unreachable` (destinazione non raggiungibile) indica che il nodo di destinazione ha ricevuto la sonda e l'ha scartata perché non poteva consegnare il pacchetto. Se il timer scade prima di ricevere una risposta, il comando `traceroute` restituisce un asterisco (*). Il comando termina quando si verifica una delle seguenti situazioni:

- La destinazione risponde
- viene superato il valore TTL massimo
- L'utente interrompe la traccia con la sequenza di escape

Nota: per richiamare la sequenza di escape, è possibile premere contemporaneamente i tasti Ctrl, Maiusc e 6.

Descrizioni dei campi del comando `traceroute`

In questa tabella vengono descritti i vari campi del comando `traceroute`:

Campo	Descrizione
-------	-------------

Protocol [ip]:	Richiede un protocollo supportato. Specificare appletalk, clns, ip, novell, apollo, vines, decnet o xns. Il valore predefinito è ip.
Target IP address	Specificare un nome host o un indirizzo IP. Non esistono valori predefiniti.
Source address:	L'interfaccia o l'indirizzo IP del router che le sonde useranno come indirizzo di origine. Il router in genere sceglie l'indirizzo IP dell'interfaccia in uscita da utilizzare.
Numeric display [n]:	Per impostazione predefinita, il valore viene visualizzato in formato simbolico e numerico, ma è possibile ignorare la visualizzazione simbolica.
Timeout in seconds [3]:	Numero di secondi di attesa per la risposta a un pacchetto di richiesta. L'impostazione predefinita è 3 secondi.
Probe count [3]:	Il numero di richieste da inviare ad ogni livello TTL. Il numero predefinito è 3.
Minimum Time to Live [1]:	Valore di TTL delle prime richieste. L'impostazione predefinita è 1, ma è possibile impostare un valore superiore per non visualizzare gli hop noti.
Maximum Time to Live [30]:	Valore di TTL massimo utilizzabile. L'impostazione predefinita è 30. OSPF (Open Shortest Path First) traceroute termina quando si raggiunge una destinazione o quando si raggiunge questo valore.
Port Number [33434]:	Porta di destinazione utilizzata per i messaggi di richieste UDP. L'impostazione predefinita è 33434.
Loose, Strict, Record, Timestamp, Verbose[none]:	Opzioni dell'intestazione IP. È possibile specificare qualsiasi combinazione. OSPF (Open Shortest Path First) traceroute il comando chiede di specificare i campi obbligatori. Si noti che la traceroute Il comando include le opzioni richieste in ciascuna sonda; tuttavia, non vi è alcuna garanzia che le opzioni siano elaborate da tutti i router (o nodi finali).

Esempio

```
<#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#
```

Nota: il `traceroute` può essere eseguito solo in modalità di esecuzione privilegiata, mentre il `traceroute` funziona sia in modalità di esecuzione utente sia in modalità di esecuzione privilegiata.

Informazioni correlate

- [Pagina Tecnologia dei protocolli di routing TCP/IP](#)
- [Pagina di supporto per il routing IP](#)
- [Informazioni sui comandi ping e traceroute](#)
- [Uso del comando Traceroute nei vari sistemi operativi](#)
- [Supporto tecnico e download Cisco](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).