

# Begrijp de uitgebreide ping en uitgebreide traceroute-opdrachten

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[De opdracht ping](#)

[Uitgebreide ping-opdracht](#)

[De beschrijvingen van het ping-opdrachtveld](#)

[De traceroute-opdracht](#)

[De uitgebreide traceroute-opdracht](#)

[De beschrijvingen van het opdrachtveld voor traceroute](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft hoe de uitgebreide ping en de uitgebreide traceroute opdrachten.

## Voorwaarden

### Vereisten

Dit document vereist vooraf kennis van de ping en traceroute opdrachten.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS®-software
- Alle Cisco Series routers

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

### Conventies

Raadpleeg voor meer informatie over documentconventies [Cisco Technical Tips Conventions](#).

## Het ping Opdracht

De opdracht ping (Packet InterNet Groper) is een veelgebruikte methode om de toegankelijkheid van apparaten probleemoplossing te bieden. Het gebruikt twee ICMP-query's (Internet Control Message Protocol), ICMP-echoverzoeken en ICMP-echoantwoorden om te bepalen of een externe host actief is. De opdracht ping meet ook de tijd die nodig is om het echoantwoord te ontvangen.

Pingel bevel eerst verzendt een pakket van het echoverzoek naar een adres, en dan wacht het op een antwoord. Pingel is succesvol slechts als het ECHO VERZOEK aan de bestemming krijgt, en de bestemming kan een ECHO ANTWOORD terug naar de bron van pingelen binnen een vooraf bepaald tijdsinterval krijgen.

## Het uitgebreide ping Opdracht

Wanneer normaal pingelen wordt verzonden van een router, is het bronadres van pingel het IP adres van de interface die het pakket gebruikt om de router te verlaten. Als een uitgebreide ping-opdracht wordt gebruikt, kan het IP-bronadres worden gewijzigd in een willekeurig IP-adres op de router. Uitgebreide pingelen wordt gebruikt om een geavanceerdere controle van gastheer bereikbaarheid en netwerkconnectiviteit uit te voeren. Uitgebreid pingel bevel werkt slechts bij de bevoorrechte EXEC bevellijn. Normaal ping werkt zowel in de gebruikersEXEC-modus als in de geprivilegieerde EXEC-modus. Om deze functie te gebruiken, voert u ping in op de opdrachtregel en drukt u op Return. U wordt gevraagd om de velden zoals aangegeven in de sectie [Beschrijvingen](#) van [opdrachtveld](#) van dit document.

## Het ping Beschrijving van opdrachtveld

Deze tabel maakt een lijst van de beschrijvingen van de ping-opdrachtvelden. Deze velden kunnen worden aangepast met het gebruik van de uitgebreide ping-opdracht.

Veld	Beschrijving
Protocol [ip]:	Vragen om een ondersteund protocol. Voer apple, clns, ip, novell, apollo, vines, decnet of xns in. De standaardwaarde is ip.
Doel IP-adres:	Vragen om het IP-adres of de hostnaam van het doelknooppunt dat u wilt pingelen. Als u een ander ondersteund protocol dan IP hebt opgegeven, voer hier een geschikt adres voor dat protocol in. De standaardinstelling is geen.
Herhalingstelling [5]:	Aantal pingpakketten die naar het doeladres worden verzonden. De standaardwaarde is 5.
Datagramgrootte [100]:	Grootte van het ping-pakket (in bytes). Standaard is 100 bytes.
Time-out in seconden [2]:	Time-outinterval. Standaard: 2 (seconden). De ping wordt alleen als succesvol verklaard als het ECHO antwoordpakket voor dit tijdsinterval is ontvangen.
Uitgebreide opdrachten [n]:	Specificeert al dan niet een reeks extra opdrachten die verschijnt. Standaard is dit nr.
Ingress ping [n]:	De toegang pingel simuleert pakketten die op de gespecificeerde toegangsinterface aan de doelbestemming worden ontvangen. Standaard is dit nr. (De beschikbaarheid van deze optie verschilt van de gebruikte softwarerelease)

Bronadres of -interface:

Het interface- of IP-adres van de router dat als bronadres voor de sondes moet worden gebruikt. De router plukt normaal het IP adres van de uitgaande interface aan gebruik. De interface kan ook worden genoemd, maar met de juiste syntaxis zoals hier getoond:

Source address or interface: ethernet 0

**Opmerking:** dit is een gedeeltelijke uitvoer van de uitgebreide ping-opdracht. De interface kan niet a worden geschreven.

DSCP-waarde [0]:

Specificeert het gedifferentieerde servicescodepunt (DSCP). De geïntroduceerde DSCP-waarde wordt op elke sonde geplaatst. De standaardinstelling is 0. De beschikbaarheid van deze optie verschilt van de gebruikte softwarerelease)

Type dienst [0]:

Specificeert het type service (ToS). De gevraagde wordt geplaatst in elke sonde, maar er is geen garantie dat alle routers de ToS verwerken. Het is de internetkwaliteit van de dienstverlening. De standaardwaarde is 0.

DF-bit in IP-header instellen? [nr.]:

Specificeert of de Don't Fragment (DF) het bit moet worden ingesteld op het ping-pakket. Als ja is opgegeven, wordt de DF-optie niet toe dat dit pakket wordt gefragmenteerd wanneer het door een segment moet gaan, en ontvangt u een foutmelding van het apparaat dat het pakket wilde fragmenteren. Dit is handig om de kleinste MTU in het pad naar een bestemming te bepalen. Standaard is dit nr.

Antwoordgegevens valideren? [nr.]:

Specificeert al dan niet om de antwoordgegevens te valideren. Standaard is dit nr.

Gegevenspatroon [0xABCD]

Specificeert het gegevenspatroon. Verschillende gegevenspatronen worden gebruikt voor probleemoplossing framing fouten en clocking problemen met seriële lijnen. De standaardinstelling is [0xABCD]. Deze prompt biedt meer dan één optie om te selecteren. Dit zijn:

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

- Breedsprakig wordt automatisch geselecteerd samen met een andere optie.
- Record is een zeer nuttige optie omdat het het adres(sen) van de hop (tot negen) toont dat het pakket doorgaat.
- Los staat u toe om het pad te beïnvloeden wanneer u het adres (de adressen) van de hop(en) opgeeft waarvan u wilt dat het pakket gaat.
- Strikt wordt gebruikt om de hop(en) op te geven die u wilt dat het pakket doorgaat, maar er mag geen andere hop(en) worden bezocht.
- Tijdstempel wordt gebruikt om de rondreis na

bepaalde hosts te meten.

Het verschil tussen de Record optie van dit commando en de traceroute commando is dat de Record optie alleen informeert u over de hop dat de echo aanvraag (ping) doorgedaan is om de bestemming te bereiken, maar ook informeert u over de hop die het bezocht is op de terugweg. Met de traceroute opdracht krijgt u ook informatie over het pad dat het echoantwoord neemt. Het traceroute-commando geeft vragen voor de volgende vereiste velden.

Het traceroutebevel plaatst de gevraagde opties in de vraag van elke sonde. Er is echter geen garantie dat alle routers (of eindknooppunten) de opties verwerken. De standaardinstelling is geen.

Hier kunt u de grootte van de verzonden echopakketten wijzigen. Dit wordt gebruikt om de maximumgrootte van MTUs te bepalen die op de routers/knooppunten langs de weg aan het bestemmingspunt wordt gevormd. Prestatieproblemen die worden veroorzaakt door pakketfragmentatie worden dus verminderd. Standaard is dit nr.

Elk uitroepteken (!) geeft de ontvangst van een antwoord aan. Een periode (.) geeft aan dat de netwerkserver heeft gewacht op een antwoord. Zie [tekens pinggen](#) voor een beschrijving van de andere tekens.

Het percentage pakketten dat met succes terug naar de router wordt geëchoed. Elk percentage onder 100 wordt doorgaans als problematisch beschouwd.

Ronde reistijdintervallen voor de protocol echopakketten met minimum/gemiddelde/maximum (in milliseconden).

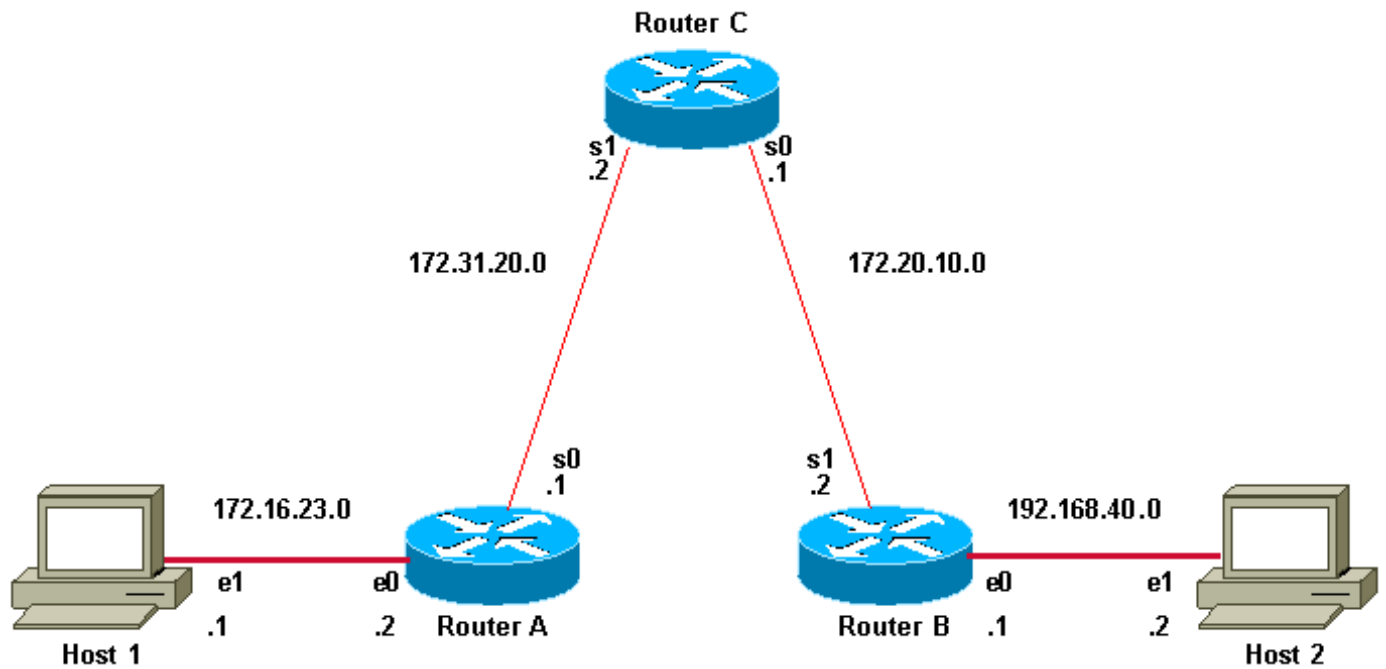
Veegbereik van maten [n]:

!!!!

Succespercentage is 100 procent

min./gem./max. ronde reis = 1/2/4 ms

In dit diagram kunnen host 1 en host 2 niet met elkaar pinggen. U kunt dit probleem op de routers oplossen om te bepalen als er een routeringsprobleem is, of als een van de twee hosts niet de juiste standaardgateway heeft ingesteld.



*Host 1 en Host 2 kunnen niet pingen*

Opdat de ping van host 1 naar host 2 kan slagen, moet elke host zijn standaardgateway naar de router op zijn respectievelijke LAN-segment richten, of moet de host netwerkinformatie uitwisselen met de routers die een routerprotocol gebruiken. Als één van beide gastheer niet zijn standaardgateway heeft die correct wordt geplaatst, of het heeft niet de correcte routes in zijn routingstabel, kan het geen pakketten naar bestemmingen verzenden die niet aanwezig in zijn geheim voorgeheugen van de Resolutie van het Adres van het Protocol (ARP) zijn. Het is ook mogelijk dat de hosts elkaar niet kunnen pingelen omdat een van de routers geen route naar het subnet heeft van waaruit de host haar pingpakketten ontvangt.

## Voorbeeld

Dit is een voorbeeld van de uitgebreide **ping**-opdracht afkomstig van de router A Ethernet 0-interface en bestemd voor de router B Ethernet-interface. Als dit slaagt pingelt, is het een aanwijzing dat er geen routeringsprobleem is. De router A weet hoe te aan Ethernet van router B te krijgen, en de router B weet hoe te aan Ethernet van router A te krijgen. Ook, hebben beide gastheren hun standaardgateways correct geplaatst.

Als het uitgebreide **ping**-commando van router A mislukt, betekent dit dat er een routerprobleem is. Er zou een routeringsprobleem op om het even welke drie routers kunnen zijn. Router A had een route kunnen verliezen naar het subsysteem van Router B Ethernet of naar het subsysteem tussen Router C en Router B. Router B zou een route kunnen zijn kwijtgeraakt aan het subsysteem van Router A of aan het subsysteem tussen Router C en Router A; en de router C zou een route aan het Subnet van de segmenten van de router A of van de router B Ethernet kunnen verloren hebben. U moet eventuele routeringsproblemen corrigeren en vervolgens host 1 moet proberen host 2 te pingelen. Als host 1 nog steeds geen host 2 kan pingelen, moet u beide standaardgateways controleren. De connectiviteit tussen Ethernet van router A en Ethernet van router B wordt gecontroleerd met het uitgebreide **ping** bevel.

Met normaal ping van router A naar router B Ethernet-interface, het bronadres van het ping-pakket zou het adres zijn van de uitgaande interface, dat wil zeggen het adres van de seriële 0-interface (172.31.20.1). Wanneer router B op het ping-pakket antwoordt, antwoordt het op het bronadres (namelijk 172.31.20.1). Op deze manier wordt alleen de connectiviteit tussen seriële 0-interface van router A (172.31.20.1) en de Ethernet-interface van router B (192.168.40.1) getest.

Gebruik de uitgebreide **ping**-opdracht om de connectiviteit tussen router A Ethernet 0 (172.16.23.2) en router B Ethernet 0 (192.168.40.1) te testen. Met uitgebreid **ping**, krijgt u de optie om het bronadres van het **ping** pakket te specificeren, zoals hier getoond:

```
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:  
!---  $18024(\text{high end of range}) - 36(\text{low end of range}) = 17988(\text{bytes in range})$   
!---  $17988(\text{bytes in range}) / 1(\text{sweep interval}) = 17988 (\text{steps in range})$   
!---  $17988(\text{bytes in range}) + 1 (\text{first value}) = 17989(\text{values to be tested})$   
!---  $17989(\text{values to be tested}) * 10(\text{repeat count}) = 179890 (\text{pings to be sent})$   
!--- 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





## De uitgebreide traceroute-opdracht

Het uitgebreide traceroutebevel is een variatie van het traceroutebevel. Een uitgebreide traceroute-opdracht kan worden gebruikt om te zien welke padpakketten er nodig zijn om naar een bestemming te gaan. Het bevel kan ook worden gebruikt om het routing tezelfdertijd te controleren. Dit is handig wanneer u problemen met routing loops oplost, of wanneer u bepaalt waar pakketten verloren gaan (als een route is verlopen of als pakketten worden geblokkeerd door een toegangscontrolelijst (ACL) of firewall). U kunt het uitgebreide pingbevel gebruiken om het type van connectiviteitsprobleem te bepalen, en dan het uitgebreide traceroutebevel gebruiken om naar te versmallen waar het probleem voorkomt.

Een "tijd overschreden" foutmelding geeft aan dat een intermediaire communicatieserver het pakket heeft gezien en verwijderd. Een "bestemmings onbereikbare" foutmelding wijst erop dat de bestemmingsknoop de sonde heeft ontvangen en het verworpen omdat het niet het pakket kon leveren. Als de timer afgaat voordat er een antwoord binnenkomt, wordt een sterretje overgetrokken(\*). De opdracht wordt beëindigd als een van deze situaties zich voordoet:

- De bestemming reageert
- Het maximale TTL wordt overschreden
- De gebruiker onderbreekt het spoor met de vluchtopeenvolging

**Opmerking:** U kunt deze ontsnappingsreeks aanhalen wanneer u tegelijkertijd op Ctrl, Shift en 6 drukt.

## De beschrijvingen van het opdrachtveld voor traceroute

Deze tabel bevat de beschrijvingen van de opsporingsopdracht:

Veld	Beschrijving
Protocol [ip]:	Vragen om een ondersteund protocol. Voer apple, clns, ip, novell, apollo, vines, decnet of xns in. De standaardwaarde is ip.
Doel IP-adres	U moet een hostnaam of een IP-adres invoeren. Het is geen standaard.
Bronadres:	Het interface- of IP-adres van de router dat als bronadres voor de sondes moet worden gebruikt. De router plukt normaal het IP adres van de uitgaande interface aan gebruik.
Numeriek display [n]:	De standaardinstelling is dat de weergave zowel symbolisch als numeriek is; u kunt de symbolische weergave echter onderdrukken.
Time-out in seconden [3]:	Het aantal seconden dat moet worden gewacht op reactie op een sonde-pakket. De standaardinstelling is 3 seconden.
Sonde tellen [3]:	Het aantal sondes dat op elk TTL-niveau moet worden verzonden. De standaardtelling is 3.
Minimumtijd om te leven [1]:	De TTL-waarde voor de eerste sondes. Het gebrek aan 1, maar het kan aan een hogere waarde worden geplaatst om de vertoning van bekende hop te onderdrukken.
Maximale tijd om te leven [30]:	De grootste TTL-waarde die kan worden gebruikt.

Poortnummer [33434]:

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

gebrek is 30. Het **traceroute** bevel eindigt wanneer bestemming wordt bereikt of wanneer deze waarde wordt bereikt.

De bestemmingshaven die door de UDP sonderberichten wordt gebruikt. De standaardwaarde is 33434.

IP-headeropties. U kunt elke combinatie opgeven. De opdracht **traceroute** geeft vragen voor de vereiste opties. Merk op dat het **traceroute** bevel de gevraagde opties in elke sonde plaatst; er is echter geen garantie dat alle routers (of eindknooppunten) de opties verwerken.

## Voorbeeld

```
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#
```

**Opmerking:** De uitgebreide **traceroute**-opdracht kan alleen worden uitgevoerd in de bevoorrechte EXEC-modus, terwijl de normale opdracht **traceroute** werkt in zowel de gebruiker als de bevoorrechte EXEC-modi.

## Gerelateerde informatie

- [Technologische pagina voor TCP/IP-routeringsprotocollen](#)
- [Ondersteuningspagina voor IP-routing](#)
- [De opdrachten ping en traceroute begrijpen](#)
- [Gebruik de opdracht Traceroute op besturingssystemen](#)
- [Technische ondersteuning en downloads - Cisco Systems](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.