

Comprendre les commandes Ping et Traceroute étendues

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[La commande ping](#)

[La commande étendue ping](#)

[Descriptions des champs de commande Ping](#)

[La commande traceroute](#)

[La commande étendue traceroute](#)

[Descriptions des champs de commande Traceroute](#)

[Informations connexes](#)

Introduction

Ce document décrit comment utiliser les commandes `extended ping` et `extended traceroute`.

Conditions préalables

Exigences

Ce document nécessite une connaissance préalable des commandes `ping` et `traceroute`.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOSMD
- Tous les routeurs de la gamme Cisco

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

La commande `ping` PC

La commande `ping` (Packet InterNet Groper) est une méthode très courante pour dépanner

l'accessibilité des périphériques. Elle utilise les messages de requête de l'Internet Control Message Protocol (ICMP), des demandes d'écho ICMP et les réponses d'écho ICMP pour déterminer si un hôte distant est en activité. La `ping` commande mesure également le temps nécessaire à la réception de la réponse d'écho.

La `ping` commande envoie d'abord un paquet de requête d'écho à une adresse, puis attend une réponse. Le `ping` ne réussit que si la REQUÊTE D'ÉCHO parvient à la destination et que la destination est en mesure de renvoyer une RÉPONSE D'ÉCHO à la source du `ping` dans un intervalle de temps prédéfini.

La commande `ping` PC étendue

Lorsqu'une `ping` commande normale est envoyée à partir d'un routeur, l'adresse source de la requête `ping` est l'adresse IP de l'interface que le paquet utilise pour quitter le routeur. Si une `ping` commande étendue est utilisée, l'adresse IP source peut être remplacée par n'importe quelle adresse IP sur le routeur. Le protocole étendu `ping` est utilisé pour effectuer un contrôle plus avancé de l'accessibilité de l'hôte et de la connectivité réseau. La `ping` commande étendue fonctionne uniquement sur la ligne de commande du mode d'exécution privilégié. Le mode normal `ping` fonctionne à la fois en mode utilisateur et en mode privilégié. Afin d'utiliser cette fonctionnalité, entrez `ping` à la ligne de commande et appuyez sur Retour. Vous êtes invité à remplir les champs tels que donnés dans la section Descriptions du champ de commande `ping` de ce document.

Description des champs de `ping` Command

Ce tableau répertorie les descriptions des champs de `ping` commande. Ces champs peuvent être modifiés à l'aide de la `ping` commande étendue.

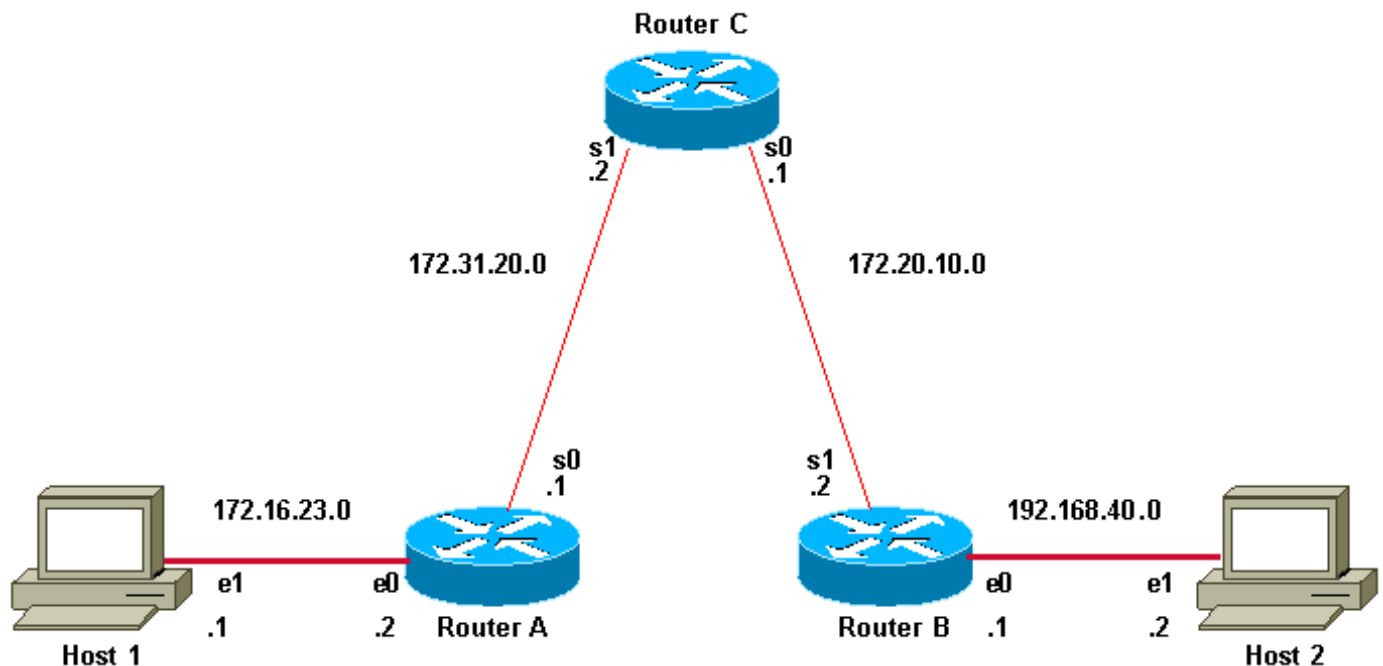
Champ	Description
Protocol [ip] :	Demandes pour protocole pris en charge. Entrez <code>appletalk</code> , <code>clns</code> , <code>ip</code> , <code>novell</code> , <code>apollo</code> , <code>vines</code> , <code>decnet</code> ou <code>xns</code> . Le défaut est <code>ip</code>
Adresse IP cible+ <code>F10534</code> :	Demandes pour l'adresse IP ou le nom hôte du noeud de destination auquel vous prévoyez d'appliquer la commande <code>ping</code> . Si vous avez spécifié un protocole pris en charge autre que l'IP, entrez une adresse appropriée pour ce protocole ici. Le défaut est aucun.
Nombre de répétitions [5] :	Nombre de paquets <code>ping</code> qui sont envoyés à l'adresse de destination. 5 est établi par défaut.

Taille du datagramme [100] :	Taille du paquet ping (en octets). Par défaut : 100 octets.
Délai en secondes [2]:	Délai de temporisation. Par défaut : 2 (secondes). Le ping est déclaré réussi seulement si le paquet de RÉPONSE EN ÉCHO est reçu avant ce délai.
Commandes étendues [n] :	Spécifie si une gamme de commandes supplémentaires apparaît. Non est établi par défaut.
Ping d'entrée [n] :	<p>Le Ping d'entrée simule les paquets reçus sur l'interface d'entrée spécifiée vers la destination cible. Non est établi par défaut.</p> <p>(La disponibilité de cette option diffère de la version logicielle utilisée.)</p>
Adresse source ou interface :	<p>L'interface ou l'adresse IP du routeur à utiliser comme adresse source pour les sondes. Le routeur sélectionne normalement l'adresse IP de l'interface de sortie pour l'utiliser. L'interface peut également être mentionnée, mais avec la syntaxe correcte, comme indiqué ici :</p> <p>Source address or interface: ethernet 0</p> <p>Il s'agit d'un résultat partiel de la ping commande étendue. L'interface ne peut pas être écrite comme e0.</p>
Valeur DSCP.[0] :	Précise le marquage DSCP (Differentiated Services Code Point) La valeur DSCP introduite est placée dans chaque envoi-test. La valeur par défaut est 0. (La disponibilité de cette option diffère de la version du logiciel utilisée.)
Type de service [0] :	Spécifie le Type de service (ToS). Le ToS demandé est placé dans chaque sonde, mais il n'y a aucune garantie que tous les routeurs traitent le ToS. Il s'agit de la sélection de la qualité de service Internet. 0 est établi par

	défaut.
Définir bit DF dans l'en-tête IP ? [non] :	Indique si le bit doit être défini sur Don't Fragment (DF) le paquet ping. Si l'option affirmative (oui) est sélectionnée, l'option DF ne permet pas la fragmentation de ce paquet lorsqu'il doit passer par un segment dont l'unité de transfert maximale (MTU) est inférieure et qu'un message d'erreur est reçu du périphérique qui tentait de fragmenter le paquet. Cela est utile pour déterminer la plus petite MTU dans le chemin vers une destination. Non est établi par défaut.
Validez les données de réponse ? [non] :	Spécifie la validation ou non des données de réponse. Non est établi par défaut.
Structure de données [0xABCD]	Spécifie la structure de données. Différents modèles de données sont utilisés pour dépanner les framing erreurs et les clocking problèmes sur les lignes série. [0xABCD] est établi par défaut.
Lâche, strict, enregistrer, horodatage, prolix [aucun] :	Options d'en-tête IP. Plus d'une option à sélectionner sont proposées. Elles sont : <ul style="list-style-type: none"> • Prolixe est automatiquement sélectionné avec toute autre option. • L'option Record (enregistrement) est très utile, car elle affiche la ou les adresses des sauts (jusqu'à neuf) que traverse le paquet. • L'option Loose (souple) vous permet d'influencer le chemin emprunté lorsque vous précisez la ou les adresses du ou des sauts par lesquels vous souhaitez que le paquet passe. • L'option Strict (stricte) est utilisée pour préciser le ou les sauts par lesquels vous souhaitez faire passer par le paquet, mais aucun autre saut ne pourra être visité. • L'horodatage est utilisé pour mesurer le temps d'aller-retour chez des hôtes

	<p>particuliers.</p> <p>La différence entre l'option Record de cette commande et la commande Traceroute tient à ce que l'option Record vous informe non seulement des sauts que la requête d'écho (message Ping) a parcourus pour arriver à la destination, mais également des sauts visités sur le chemin du retour. Avec la commande traceroute, vous n'obtenez pas d'informations sur le chemin que la réponse d'écho prend. La commande traceroute émet des demandes pour les champs requis.</p> <p>La commande Traceroute place les options demandées dans chaque envoi-test. Cependant, il n'y a aucune garantie que tous les routeurs (ou noeuds d'extrémité) traitent les options. Le défaut est aucun.</p>
Gamme de tailles de balayage [n] :	<p>Vous permet de varier les tailles des paquets d'écho qui sont envoyés. Ceci est utilisé pour déterminer les tailles minimales des MTU configurées sur les noeuds le long du chemin à l'adresse de destination. Des problèmes de performances provoqués par la fragmentation des paquets sont ainsi réduits. Non est établi par défaut.</p>
!!!!	<p>Chaque point d'exclamation (!) indique la réception d'une réponse. Un point (.) indique que le serveur réseau a dépassé le délai d'attente d'une réponse. Reportez-vous aux caractères des messages Ping pour une description des autres caractères.</p>
Le taux de réussite est de 100 %	<p>Pourcentage de paquets avec un écho de retour réussi vers le routeur. Tout pourcentage inférieur à 80 est généralement considéré comme problématique.</p>
aller-retour min/moy/max = 1/2/4 ms	<p>Intervalles du trajet aller-retour pour les paquets d'écho de protocole avec le minimum/la moyenne/le maximum (en millisecondes).</p>

Dans ce diagramme, l'hôte 1 et l'hôte 2 ne peuvent pas s'envoyer des pings. Vous pouvez résoudre ce problème sur les routeurs afin de déterminer s'il y a un problème de routage ou si la passerelle par défaut de l'un des deux hôtes n'est pas correctement définie.



L'hôte 1 et l'hôte 2 ne peuvent pas effectuer de message Ping

Pour réussir la ping transition entre l'hôte 1 et l'hôte 2, chaque hôte doit pointer sa passerelle par défaut vers le routeur sur son segment de réseau local respectif, ou l'hôte doit échanger des informations réseau avec les routeurs qui utilisent un protocole de routage. Si l'un des hôtes n'a pas défini correctement sa passerelle par défaut ou si les voies de routage appropriées ne sont pas définies dans sa table de routage, il ne peut pas envoyer de paquets vers des destinations qui ne sont pas présentes dans le protocole ARP (protocole de résolution d'adresse) mis en mémoire cache. Il est également possible que les hôtes ne puissent pas se envoyer de message Ping, car l'un des routeurs n'a pas de route vers le sous-réseau duquel l'hôte obtient ses paquets Ping.

Exemple

Ceci est un exemple de la commande extended ping créée depuis l'interface de l'Ethernet 0 du routeur A et destinée à l'interface de l'Ethernet du routeur B. Si ce ping réussit, c'est une indication qu'il n'y a aucun problème de routage. Le routeur A sait comment accéder à l'Ethernet du routeur B, et le routeur B sait comment accéder à l'Ethernet du routeur A. De plus, les passerelles par défaut des deux hôtes sont correctement définies.

Si la ping commande étendue du routeur A échoue, cela signifie qu'il y a un problème de routage. Il pourrait il y avoir un problème de routage sur n'importe lequel des trois routeurs. Le routeur A pourrait avoir perdu une route vers le sous-réseau du routeur B Ethernet, ou vers le sous-réseau entre le routeur C et le routeur B. Le routeur B pourrait avoir perdu une route vers le sous-réseau du routeur A, ou vers le sous-réseau entre le routeur C et le routeur A ; et le routeur C pourraient avoir perdu une route vers le sous-réseau des segments Ethernet du routeur A ou du routeur B. Vous devez corriger tout problème de routage, puis l'hôte 1 doit essayer d'envoyer une requête ping à l'hôte 2. Si l'hôte 1 ne peut toujours pas envoyer de requête ping à l'hôte 2, vous devez

vérifier les deux passerelles par défaut. La connectivité entre l'Ethernet du routeur A et l'Ethernet du routeur B est contrôlée avec la commande extended ping.

Dans un message Ping normal de l'interface Ethernet du routeur A à celle du routeur B, l'adresse source du paquet Ping serait l'adresse de l'interface sortante, c'est-à-dire l'adresse de l'interface série 0 (172.31.20.1). Quand le routeur B répond au paquet ping, il répond à l'adresse source (c'est-à-dire 172.31.20.1). De cette façon, seule la connectivité entre l'interface de la série 0 du routeur A (172.31.20.1) et l'interface Ethernet du routeur B (192.168.40.1) est testée.

Afin de tester la connectivité entre le routeur A Ethernet 0 (172.16.23.2) et le routeur B Ethernet 0 (192.168.40.1), utilisez la `ping` commande extended. Avec `extendedping`, vous avez la possibilité de spécifier l'adresse source du `ping`paquet, comme indiqué ici :

```
<#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

[illegible]

Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms

```
!--- Ping is successful.
```

RouterA#

La commande traceroute

Lorsque la commande ping peut être utilisée pour vérifier la connectivité entre les périphériques, la `tracert` commande peut être utilisée pour découvrir les chemins empruntés par les paquets vers une destination distante, ainsi que l'endroit où le routage tombe en panne.

L'objectif de la `tracert` commande est d'enregistrer la source de chaque message ICMP de dépassement de délai afin de fournir une trace du chemin emprunté par le paquet pour atteindre la destination.


Le périphérique qui exécute la `tracroute` commande envoie une séquence de datagrammes UDP (User Datagram Protocol), chacun avec des incréments de durée de vie (TTL), à une adresse de port non valide (par défaut 33434) sur l'hôte distant.

Tout d'abord, trois datagrammes sont envoyés, chacun avec une valeur de champ TTL définie sur 1. La valeur TTL de 1 provoque le dépassement du délai d'attente du datagramme dès qu'il atteint

le premier routeur sur le chemin. Ce routeur répond alors par un message ICMP de dépassement de délai qui indique que le datagramme a expiré.

Ensuite, trois autres messages UDP sont envoyés, chacun avec la valeur TTL définie sur 2. Cela entraîne le renvoi des messages ICMP de dépassement de délai par le deuxième routeur sur le chemin vers la destination.

Ce processus se poursuit jusqu'à ce que les paquets atteignent la destination et jusqu'à ce que le système d'origine `tracert` reçoive des messages ICMP de dépassement de délai de chaque routeur sur le chemin vers la destination. Puisque ces datagrammes tentent d'accéder à un port non valide (par défaut 33434) sur l'hôte de destination, l'hôte répond avec des messages ICMP port unreachable (port inaccessible) qui indiquent un port inaccessible. Cet événement signale le programme `tracert` à finir.

 Remarque : Assurez-vous que vous n'avez pas désactivé la commande `ip unreachable` avec la commande `no ip unreachable` sous n'importe quel VLAN. Cette commande supprime les messages de paquets sans aucun message d'erreur ICMP. Dans ce cas, `tracert` ne fonctionne pas.


La commande étendue `tracert`

La `tracert` commande étendue est une variante de la `tracert` commande. Une commande `tracert` étendue peut être utilisée pour voir quel chemin empruntent les paquets pour atteindre une destination. La commande peut également être utilisée pour contrôler le routage en même temps. Cela est utile lorsque vous dépannez des boucles de routage, ou lorsque vous déterminez où les paquets sont perdus (si une route a disparu, ou si les paquets sont bloqués par une liste de contrôle d'accès ou un pare-feu). Vous pouvez utiliser la commande `extended ping` afin de déterminer le type de problème de connectivité, puis utiliser la commande étendue `tracert` afin de rétrécir le champ où le problème se produit.

Un message d'erreur de dépassement de délai indique qu'un serveur de communication intermédiaire a vu et rejeté le paquet. Un message d'erreur « destination inaccessible » indique que le noeud de destination a reçu la sonde et l'a rejetée parce qu'il n'a pas pu remettre le paquet. Si le temporisateur s'arrête avant qu'une réponse entre, `tracert` imprime un astérisque(*).

La commande se termine quand l'une de ces situations se produit :

- La destination répond.
- le TTL maximum est dépassé.
- L'utilisateur interrompt le tracé avec la séquence d'échappement.

 Remarque : Vous pouvez appeler cette séquence d'échappement quand vous appuyez simultanément sur `Ctrl+Maj et 6`.

Descriptions des champs de commande `Tracert`

Ce tableau présente les descriptions des champs de la commande traceroute :

Champ	Description
Protocol [ip] :	Demandes pour protocole pris en charge. Entrez appletalk, clns, ip, novell, apollo, vines, decnet ou xns. Le défaut est ip
Adresse IP cible+F10534	Vous devez entrer un nom d'hôte ou une adresse IP. Rien n'est établi par défaut.
Adresse source:	L'interface ou l'adresse IP du routeur à utiliser comme adresse source pour les sondes. Le routeur sélectionne normalement l'adresse IP de l'interface de sortie pour l'utiliser.
Affichage numérique [n] :	Le défaut est d'avoir à la fois un affichage symbolique et numérique ; cependant, vous pouvez supprimer l'affichage symbolique.
Délai en secondes [3]:	Le nombre de secondes pour attendre une réponse dans un paquet de sonde. 3 secondes sont établies par défaut.
Nombre de sondes [3] :	Le nombre de sondes à envoyer à chaque niveau TTL. Le nombre par défaut est 3.
Temps de vie minimum [1] :	La valeur de TTL pour les premières sondes. 1 est établi par défaut, mais il peut être fixé à un plus haut niveau pour supprimer l'affichage des sauts connus.
Temps de vie maximal [30] :	La plus grande valeur TTL qui peut être utilisée. La valeur par défaut est 30. La <code>traceroute</code> commande se termine lorsque la destination est atteinte ou lorsque cette valeur est atteinte.
Numéro de port [33434] :	Le port de destination utilisé par les messages de sonde UDP. 33434 est établi par défaut.

<p>Lâche, strict, enregistrer, horodatage, prolix [aucun] :</p>	<p>Options d'en-tête IP. Vous pouvez spécifier n'importe quelle combinaison.</p> <p>La <code>tracert</code> commande génère des invites pour les champs obligatoires. La <code>tracert</code> commande place les options demandées dans chaque sonde ; cependant, il n'y a aucune garantie que tous les routeurs (ou noeuds d'extrémité) traitent les options.</p>
---	--

Exemple

```
<#root>
```

```
RouterA>
```

```
enable
```

```
RouterA#
```

```
tracert
```

```
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 tracert is successful.
```

```
RouterA#
```

 Remarque : La `tracert` commande étendue ne peut être exécutée qu'en mode d'exécution



privilégié, alors que la `traceroute` commande normale fonctionne en mode d'exécution utilisateur et privilégié.

Informations connexes

- [Page de la technologie des protocoles de routage TCP/IP](#)
- [Page de support pour le routage IP](#)
- [Comprendre les commandes Ping et Traceroute](#)
- [Utiliser la commande Traceroute sur les systèmes d'exploitation](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.