Packet Tracer - Utiliser Ping et Traceroute pour tester la connectivité des réseaux - Mode Physique

# Topologie



# Table d'adressage

| Appareil | Interface | Adresse IP / Préfixe | Passerelle par défaut |
| --- | --- | --- | --- |
| R1 | G0/0/0 | 64.100.0.2 /30 | S/O |
| R1 | G0/0/0 | 2001:db8:acad::2 /64 | S/O |
| R1 | G0/0/0 | fe80::2 | S/O |
| R1 | G0/0/1 | 192.168.1.1 /24 | S/O |
| R1 | G0/0/1 | 2001:db8:acad:1 /64 | S/O |
| R1 | G0/0/1 | fe80::1 | S/O |
| ISP | G0/0/0 | 64.100.0.1 /30 | N/A |
| ISP | G0/0/0 | 2001:db8:acad::1 /64 | N/A |
| ISP | G0/0/0 | fe80::1 | S/O |
| ISP | G0/0/1 | 209.165.200.225 /27 | S/O |
| ISP | G0/0/1 | 2001:db8:acad:200::225 /64 | N/A |
| ISP | G0/0/1 | fe80::225 | S/O |
| S1 | VLAN 1 | 192.168.1.2 /24 | 192.168.1.1 |
| S1 | VLAN 1 | 2001:db8:acad:1::2 /64 | fe80::1 |
| S1 | VLAN 1 | fe80::2 | fe80::1 |
| PC-A | Carte réseau (NIC) | 2001:db8:acad:1::10 /64 | fe80::1 |
| PC-A | Carte réseau (NIC) | 192.168.1.10 /24 | 192.168.1.1 |
| Externe | Carte réseau | 209.165.200.226 /27 | 209.165.200.225 |
| Externe | Carte réseau | 2001:db8:acad:200። 226 /64 | fe80::225 |

Ligne vierge - aucune information supplémentaire

# Objectifs

Partie 1: Utiliser la commande **Ping** pour le test de base du réseau

Partie 2: utiliser les commandes **tracert** et **traceroute** pour tester sommairement le réseau

Partie 3: Résoudre les problèmes de topologie

# Contexte/scénario

Ping et traceroute sont deux outils qui sont critique pour tester la connectivité du réseau TCP/IP. La commande ping est un utilitaire de gestion de réseau qui permet de vérifier l'accessibilité d'un périphérique sur un réseau IP. Cet utilitaire mesure également le temps que prennent les messages qui sont envoyés de l'hôte d'origine à un hôte de destination et vice-versa.

L'utilitaire traceroute est un outil de diagnostic de réseau permettant d'afficher le chemin ou la route d'un paquet et de mesurer les délais de transit des paquets circulant sur un réseau IP.

Dans ce PTPM, les commandes ping et traceroute seront examinées, ainsi que les options de commande permettant de modifier le comportement de celles-ci. Des périphériques Cisco et des ordinateurs sont utilisés dans cette activité pour l'exploration des commandes. Les options disponibles pour les commandes ping et tracert sont limitées dans Packet Tracer. Les configurations nécessaires pour les périphériques Cisco sont fournies dans cette activité.

# Instructions

## Utiliser la commande Ping pour le test de base du réseau

Dans la deuxième partie de cette activité, utilisez la commande ping pour vérifier la connectivité de bout en bout. Ping fonctionne comme suit : il envoie des paquets de requête d'écho du protocole ICMP (Internet Control Message Protocol) à l'hôte cible, puis il attend une réponse ICMP. Il peut enregistrer le temps de trajet aller-retour et toute perte de paquets ou de boucles d'acheminement.

Les paquets IP ont une durée de vie limitée sur le réseau. Les paquets IPv4 utilisent un temps de vie (TTL) 8 bits. Les paquets IPv6 utilisent une valeur d'en-tête Limite de tronçon. Le TTL et la limite de tronçon spécifient le nombre maximal de sauts de couche 3 qui peuvent être traversés sur le chemin d'accès à leur destination. Chaque hôte sur un réseau définira la valeur de 8 bits avec une valeur maximale de 255.

Ainsi, chaque fois qu'un paquet IP arrive à un périphérique réseau de couche trois, cette valeur est réduite d'un avant d'être transmis à sa destination. Si cette valeur atteint finalement zéro avant d'atteindre la destination, le paquet IP est rejeté.

Vous examinerez les résultats de la commande **ping** et ses options supplémentaires, qui sont disponibles sur les ordinateurs Packet Tracer et les périphériques Cisco.

### Tester la connectivité réseau vers **R1** à l'aide de **PC-A**.

Toutes les commandes ping émises à partir de PC-A vers d'autres périphériques dans la topologie doivent aboutir. Si elles échouent, vérifiez la topologie et le câblage, ainsi que la configuration des périphériques Cisco et des ordinateurs.

* + - 1. À partir de PC-A, envoyez une requête ping vers la passerelle par défaut en utilisant l'adresse IPv4 (interface GigabitEthernet 0/0/1 de R1).

Ouvrez l'invite de commande.

C:\> **ping 192.168.1.1**

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms

Dans cet exemple, quatre requêtes ICMP de 32 octets chacune ont été envoyées. Les réponses ont été reçues en moins d'une milliseconde sans perte de paquets. Le temps de transmission et de réponse peut s'allonger car les demandes et les réponses de l'ICMP sont traitées par un plus grand nombre d'appareils pendant le trajet vers et depuis la destination.

Cela peut également être fait à l'aide de l'adresse IPv6 de la passerelle par défaut (interface Gigabitethernet 0/0/1 de R1).

C:\> **ping 2001:db8:acad:1::1**

Pinging 2001:db8:acad:1::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255

Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255

Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255

Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:1::1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms

* + - 1. À partir du **PC-A**, effectuez un ping sur les adresses indiquées dans le tableau suivant et enregistrez le temps moyen aller-retour et le TTL (Time to Live) IPv4 ou le Hop Limit IPv6.

| Destination | Durée de transmission moyenne (ms) | TTL / Hop Limit |
| --- | --- | --- |
| 192.168.1.10 |  |  |
| 2001:db8:acad:1። 10 |  |  |
| 192.168.1.1 (R1) |  |  |
| 2001:db8:acad:1። 1 (R1) |  |  |
| 192.168.1.2 (S1) |  |  |
| 2001:db8:acad:1። 2 (S1) |  |  |
| 64.100.0.2 (R1) |  |  |
| 2001:db8:acad። 2 (R1) |  |  |
| 64.100.0.1 (FAI) |  |  |
| 2001:db8:acad። 1 (FAI) |  |  |
| 209.165.200.225 (FAI G0/0/1) |  |  |
| 2001:db8:acad:200። 225 (FAI G0/0/1) |  |  |
| 209.165.200.226 (Externe) |  |  |
| 2001:db8:acad:200። 226 (Externe) |  |  |

Ligne vierge - aucune information supplémentaire

### Exécutez des requêtes ping de **S1** à **Externe**.

À partir de S1, essayez de ping FAI et Externe en utilisant les adresses IPv4 et IPv6.

#### Question :

Quels sont les résultats de ping de S1 à FAI et Externe?

Saisissez vos réponses ici

Fermez l'invite de commandes.

## Utiliser les commandes **Tracert** et **Traceroute** pour les tests de base du réseau

Les commandes permettant de suivre les routes se trouvent sur les ordinateurs et les périphériques réseau. Pour un ordinateur Windows, la commande tracert utilise des messages ICMP pour suivre le chemin vers la destination finale. La commande traceroute utilise les datagrammes du protocole UDP (User Datagram Protocol) pour suivre les routes vers leur destination pour les périphériques Cisco et d'autres ordinateurs de type Unix.

Dans cette partie, vous examinerez les commandes traceroute et déterminerez le chemin qu'emprunte un paquet vers sa destination. Vous utiliserez la commande tracert à partir des ordinateurs Windows et la commande traceroute à partir des périphériques Cisco. Vous étudierez également les options permettant d'affiner les résultats de la commande traceroute.

### Utilisez la commande **tracert** de **PC-A** vers **EXTERNE**.

* + - 1. À l'invite de commandes de PC-A, tapez **tracert 209.165.200.226**.

Ouvrez une invite de commandes.

C:\> **tracert 209.165.200.226**

Tracing route to 209.165.200.225 over a maximum of 30 hops

1 \* \* 1 ms 192.168.1.1

2 \* 0 ms 0 ms 64.100.0.1

3 0 ms \* 0 ms 64.100.0.1

4 \* 11 ms \* Request timed out.

5 0 ms \* 0 ms 64.100.0.1

Control-C

^C

C:\>

**Remarque**: Vous pouvez arrêter la route de trace en appuyant sur Ctrl-C.

Les résultats de commande tracert indiquent que le chemin de PC-A à EXTERNE est de PC-A à R1 à ISP à EXTERNE. Les résultats de commande tracert indiquent un problème au niveau du routeur ISP.

* + - 1. Répétez la commande tracert à l'aide de l'adresse IPv6. À l'invite de commandes, tapez **tracert 2001:db8:acad:200::226**.

Fermez l'invite de commandes.

### À partir de S1, utilisez la commande **traceroute** vers Externe.

À partir S1, tapez traceroute 209.165.200.226 ou traceroute 2001:db8:acad:200::226.

**Remarque**: Pour arrêter le traceroute, appuyez sur Ctrl-Maj-6.

Ouvrez la fenêtre de configuration.

S1# **traceroute 209.165.200.226**

S1# **traceroute 2001:db8:acad:200::226**

Fermez la fenêtre de configuration.

La commande traceroute offre des options supplémentaires. Vous pouvez utiliser le point d'interrogation (?) ou appuyer simplement sur Entrée après avoir tapé traceroute à l'invite pour explorer ces options.

**Remarque**: Les options disponibles sont limitées dans le traceur de paquets.

Le lien suivant fournit des informations supplémentaires sur les commandes ping et traceroute pour un périphérique Cisco :

<http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6057.shtml>

## Corrigez le problème de connectivité réseau chez le **fournisseur de services Internet**.

### Accédez à l'emplacement réseau où le problème de connectivité se produit.

À partir des étapes précédentes, vous aviez déterminé qu'il y avait un problème au niveau du routeur ISP à l'aide des commandes ping et traceroute. Vous disposez d'un accès SSH distant à tous les périphériques réseau à l'aide de nom d'utilisateur administrateur et mot de passe classe.

Ouvrez l'invite de commande.

* + - 1. Depuis le terminal de S1, SSH dans le routeur ISP en utilisant l'interface G0/0/0 pour corriger le problème.

C:\> **ssh -l admin 64.100.0.1**

* + - 1. Utilisez les commandes show pour vérifier les configurations en cours du routeur ISP .

Les sorties des commandes show run et show ip interface brief indiquent que l'interface GigabitEthernet 0/0/1 est up/up, mais a été configurée avec une adresse IP incorrecte.

* + - 1. Corrigez les problèmes détectés. À partir de l'invite de commandes sur PC-A, copiez et collez la configuration suivante dans le routeur ISP pour corriger le problème dans la session SSH sur le routeur ISP .

configure terminal

interface g0/0/1

no ip address 192.168.8.1 255.255.255.0

ip address 209.165.200.225 255.255.255.224

no ipv6 address 2001:db8:acad:201::225/64

adresse ipv6 2001:db8:acad:200::225/64

adresse ipv6 fe80 : :225 lien-local

no shutdown

* + - 1. Quittez la session SSH lorsque vous avez terminé.

Fermez l'invite de commandes.

### Vérifier la connectivité de bout en bout.

À partir de l'invite de commandes PC-A , utilisez les commandes ping et tracert pour vérifier la connectivité de bout en bout au serveur externe aux versions 209.165.200.226 et 2001:db8:acad:200። 226.

## Utilisez les commandes ping étendues.

### Utilisez les commandes ping étendues sur **PC-A**.

La commande **ping** par défaut envoie quatre requêtes à 32 octets chacune. Elle attend 4 000 millisecondes (4 secondes) pour chaque réponse à renvoyer avant d'afficher le message « Request timed out » (délai d'attente de la demande dépassé). La commande ping peut être adaptée pour dépanner un réseau.

Ouvrez l'invite de commande.

* + - 1. À l'invite de commandes, saisissez ping et appuyez sur Enter.

C:\> **ping**

* + - 1. En utilisant l'option –t ping External pour vérifier que External est joignable. L'option -t effectue un ping continu sur la cible jusqu'à ce qu'elle soit arrêtée. Appuyez sur Ctrl+c tpour arrêter la commande ping.

C:\> **ping –t 209.165.200.226**

* + - 1. Pour illustrer les résultats lorsqu'un hôte est injoignable, fermez l'interface GigabitEthernet 0/0/1 sur le routeur du ISP . Du commutateur S1, SSH à l'interface ISP G0/0/0. Utilisez le mot de passe class.

S1# **ssh -l admin 64.100.0.1**

* + - 1. Utilisez la commande shutdown pour désactiver l'interface GigaBitethernet 0/0/1 sur la commande du routeur ISP.

Lorsque le réseau fonctionne correctement, la commande ping peut déterminer si la destination a répondu et combien de temps il a fallu pour recevoir une réponse de la destination. En cas de problème de connectivité réseau, la commande ping affiche un message d'erreur.

* + - 1. Activez de nouveau l'interface GigabitEthernet 0/0/1 sur le routeur d'ISP (en utilisant la commande **n**o shutdown ) avant de passer à l'étape suivante. Après 30 secondes environ, la requête ping devrait à nouveau aboutir.
      2. Appuyez sur Ctrl+c pou arrêter la commande ping .
      3. Les étapes ci-dessus peuvent être répétées pour l'adresse IPv6 pour obtenir un message d'erreur ICMP.

#### Question :

Quels messages d'erreur avez-vous reçus?

Saisissez vos réponses ici

* + - 1. Activez l'interface GigabitEthernet 0/0/1 sur le routeur d'ISP (en utilisant la commande no shutdown ) avant de passer à l'étape suivante. Après 30 secondes environ, la requête ping devrait à nouveau aboutir.

Fermez l'invite de commandes.

### Tester la connectivité du réseau **R1** à l'aide de dispositifs Cisco.

La commande **ping** est également disponible sur les périphériques Cisco. À cette étape, la commande **ping** est examinée avec le routeur R1 et le commutateur S1.

* + - 1. À partir de R1, ping Externe sur le réseau externe en utilisant l'adresse IP de 209.165.200.226.

Ouvrez la fenêtre de configuration.

R1# **ping 209.165.200.226**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Le point d'exclamation (!) indique que le ping a réussi du routeur R1 vers Externe. Le voyage aller-retour prend en moyenne 1 ms sans perte de paquets, comme l'indique un taux de réussite de 100%.

* + - 1. Parce qu'une table d'hôtes locale a été configurée sur le routeur R1, vous pouvez faire un ping à Externev4 sur le réseau externe en utilisant le nom d'hôte configuré depuis le routeur R1.

R1# **ping Externev4**

#### Question :

Quelle est l'adresse IP utilisée ?

Saisissez vos réponses ici

* + - 1. En mode EXEC privilégié, il y a plus d'options disponibles pour la commande ping. À l'invite de line de commandes, saisissez ping et appuyez sur Enter. Utilisez ipv6 comme protocole. Tapez 2001:db8:acad:200::226 ou externe pour l'adresse IPv6 cible. Appuyez sur Entrée pour accepter la valeur par défaut pour d'autres options.

R1# **ping**

Protocol [ip]: **ip**

Adresse IPv6 cible : **2001:db8:acad:200 : :226**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands? [no]:

Sweep range of sizes? [no]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:db8:acad:200::226, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

* + - 1. Vous pouvez utiliser une commande ping étendue pour observer en cas de problème réseau. Lancez la commande ping au 209.165.200.226 en répétant un compte de 50000. Ensuite, arrêtez l'interface GigaBitethernet 0/0/1 sur le routeur ISP .

De la session SSH à l' ISP sur le commutateur S1, désactivez l'interface GigaBitethernet 0/0/1 sur ISP.

* + - 1. Depuis la session SSH, activez l'interface GigabitEthernet 0/0/1 sur ISP après que les points d'exclamation (!) aient été remplacés par la lettre U et des points (.). Après 30 secondes environ, la requête ping devrait à nouveau aboutir. Appuyez sur Ctrl+Shift+6 pour arrêter la commande ping .

R1# **ping**

Protocol [ip]:

Target IP address: **209.165.200.226**

Repeat count [5]: **50000**

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]:

Sweep range of sizes [n]:

Sending 500, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

<output omitted>

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.U.U.U.U.U.

U.U................!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

<output omitted>

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

La lettre U dans les résultats indique qu'une destination est inaccessible. Une erreur de PDU a été reçue par R1. Chaque période (.) de la sortie indique que le ping a expiré en attendant une réponse d'Externe. Dans cet exemple, 1% des paquets ont été perdus lors de la panne de réseau simulée.

Fermez la fenêtre de configuration.

La commande ping est extrêmement utile lors du dépannage de la connectivité réseau.. Cependant, cette commande ping ne permet pas de déterminer l'emplacement du problème lorsqu'une requête ping n'aboutit pas. La commande tracert (ou traceroute) permet d'afficher les informations de latence réseau et de chemin.

* + - 1. Dans la fenêtre Activité PT, cliquez sur Vérifier les résultats pour vérifier que tous les éléments d'évaluation et les tests de connectivité sont corrects.

# Questions de réflexion

* 1. Qu'est-ce qui pourrait empêcher les réponses ping ou traceroute d'atteindre le périphérique source, en dehors de problèmes de connectivité réseau?

Saisissez vos réponses ici

* 1. Si vous envoyez une requête ping à une adresse inexistante sur le réseau distant, telle que 209.165.200.227, quel message est affiché par la commande ping ? Qu’est-ce que cela signifie ? Si vous envoyez une requête ping à une adresse d'hôte valide et recevez cette réponse, que devez-vous vérifier?

Saisissez vos réponses ici

* 1. Si vous envoyez une requête ping à une adresse qui n'existe dans aucun réseau de votre topologie, telle que 192.168.5.3, à partir d'un ordinateur Windows, quel message est affiché par la commande ping ? Qu'indique-t-il ?

Saisissez vos réponses ici

Fin du document