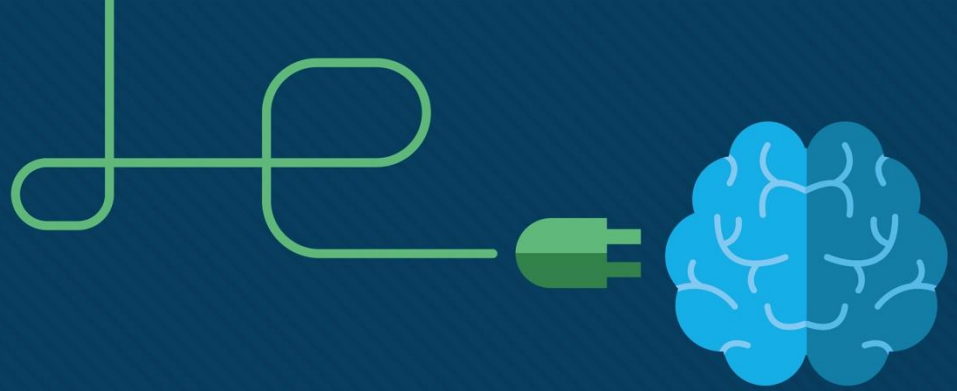
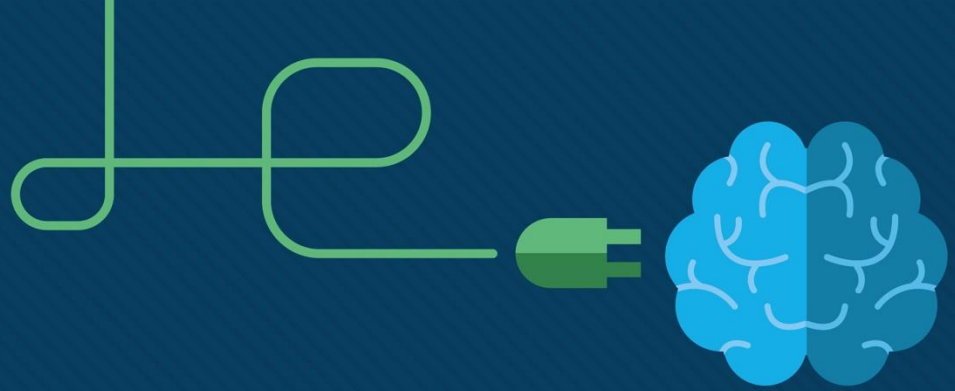


Module 13: ICMP

Contenu Pédagogique de l'instructeur

Introduction aux Réseaux v7.0
(ITN)



Module 13: ICMP

Introduction aux Réseaux v7.0
(ITN)

Objectifs du Module

Titre du module: ICMP

Objectif du Module: Utiliser divers outils pour tester la connectivité des réseaux.

Titre du Rubrique	Objectif du Rubrique
Messages ICMP	Expliquer comment le protocole ICMP sert à tester la connectivité du réseau.
Tests à l'aide des commandes ping et traceroute	Utiliser les utilitaires Ping et Traceroute pour tester la connectivité du réseau.

13.1 Messages ICMP

Messages ICMPv4 et ICMPv6

- ICMP (Internet Control Message Protocol) fournit des commentaires sur les problèmes liés au traitement des paquets IP sous certaines conditions.
- ICMPv4 est le protocole de message des réseaux IPv4. ICMPv6 est le protocole de messagerie pour IPv6 et inclut des fonctionnalités supplémentaires.
- Les messages ICMP communs à ICMPv4 et à ICMPv6 sont notamment les suivants:
  - Accessibilité de l'Hôte
  - Destination ou service inaccessible
  - Délai dépassé

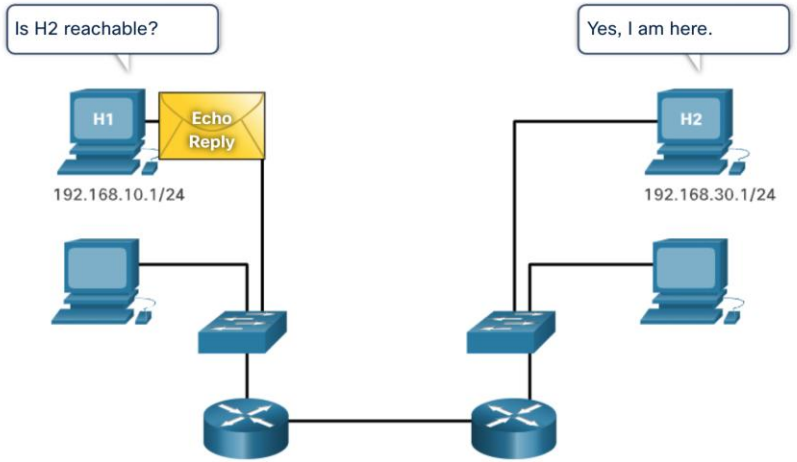
Remarque : les messages ICMPv4 ne sont pas obligatoires et ne sont souvent pas autorisés au sein d'un réseau pour des raisons de sécurité.

Accessibilité de l'hôte

ICMP Echo Message peut être utilisé pour tester l'accessibilité d'un hôte sur un réseau IP.

Dans l'exemple:

- L’hôte local envoie un message ICMP Echo Request (Demande d’écho) à un autre hôte.
- Si l'hôte est disponible, l'hôte de destination répond en envoyant une réponse d'écho.



Destination ou service inaccessible

- Un message ICMP Destination Inaccessible peut être utilisé pour avertir la source qu'une destination ou un service est inaccessible.
- Ce message comprend un code indiquant pourquoi le paquet n'a pas pu être livré.

Certains des codes de Destination Inaccessible pour l'ICMPv4 sont:

- 0 - Réseau inaccessible
- 1 - Hôte inaccessible
- 2 - Protocole inaccessible
- 3 - Port inaccessible

Certains des codes de Destination Inaccessible pour l'ICMPv6 sont:

- 0 - Pas de route vers la destination
- 1 - La communication avec la destination est interdite administrativement (p. ex., pare-feu)
- 2 - Au-delà de la portée de l'adresse source
- 3 - Adresse inaccessible
- 4 - Port inaccessible

Remarque: ICMPv6 a des codes similaires mais légèrement différents pour les messages "Destination Inaccessible".

Délai Dépassé

- Lorsque le champ Durée de vie (TTL) d'un paquet est décrémenté à 0, un message ICMPv4 Délai dépassé est envoyé à l'hôte source.
- ICMPv6 envoie également un message Délai dépassé. Au lieu du champ TTL IPv4, ICMPv6 utilise le champ Hop Limit IPv6 pour déterminer si le paquet a expiré.

```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Remarque: les messages de Délai dépassé sont utilisés par l'outil de **traceroute** .

Messages ICMPv6

ICMPv6 dispose de nouvelles fonctionnalités et fonctionnalités améliorées introuvables dans ICMPv4, y compris quatre nouveaux protocoles dans le cadre du Neighbor Discovery Protocol (ND ou NDP).

La messagerie entre un routeur IPv6 et un périphérique IPv6, y compris l'allocation d'adresses dynamique, est la suivante:

- Message de sollicitation de routeur (RS)
- Message d'annonce de routeur (RA)

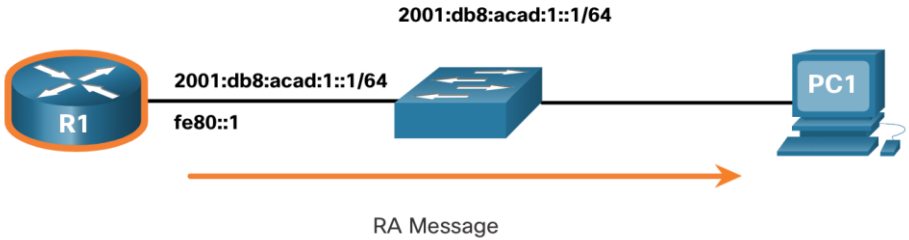
La messagerie entre les périphériques IPv6, y compris la détection d'adresses en double et la résolution d'adresses, est la suivante:

- Message de sollicitation de voisin (NS)
- Messages d'annonce de voisin (NA)

Remarque: ICMPv6 ND inclut également le message de redirection, qui comporte une fonction similaire au message de redirection utilisé dans l'ICMPv4.

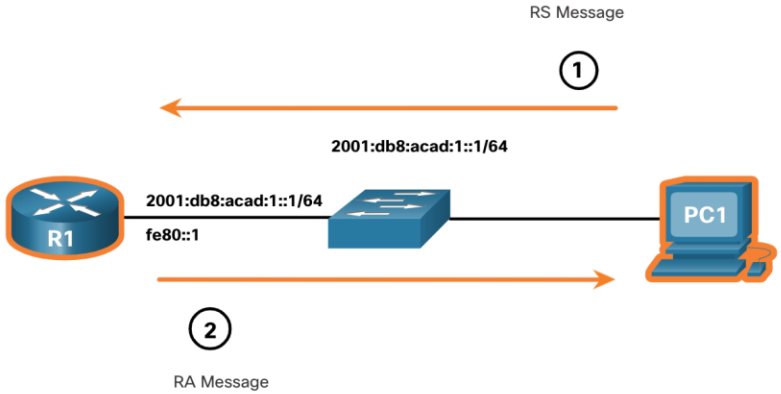
Messages ICMPv6 (suite)

- Les messages RA sont envoyés par des routeurs compatibles IPv6 toutes les 200 secondes pour fournir des informations d'adressage aux hôtes compatibles IPv6.
- Un message d'annonce de routeur peut inclure les informations d'adressage pour l'hôte telles que le préfixe, la longueur de préfixe, l'adresse DNS et le nom de domaine.
- Un hôte utilisant l'auto-configuration d'adresse sans état (SLAAC) définira sa passerelle par défaut sur l'adresse locale du routeur qui a envoyé le RA.



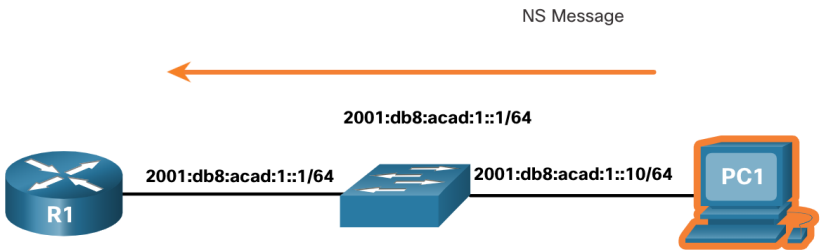
Messages ICMPv6 (suite)

- Un routeur compatible IPv6 enverra également un message RA en réponse à un message RS.
- Dans la figure, PC1 envoie un message RS pour déterminer comment recevoir ses informations d'adresse IPv6 dynamiquement.
  - R1 répond au RS avec un message RA.
  - PC1 envoie un message RS, «Salut, je viens de démarrer. Existe-t-il un routeur IPv6 sur le réseau? J'ai besoin de savoir comment obtenir les informations de mon adresse IPv6 dynamiquement.»
  - R1 répond avec un message RA. «Salut à tous les appareils compatibles IPv6. Je suis R1 et vous pouvez utiliser SLAAC pour créer une adresse de monodiffusion globale IPv6. Le préfixe est 2001:db8:acad:1::/64. Au fait, utilisez mon adresse locale fe80::1 comme passerelle par défaut".



Messages ICMPv6 (suite)

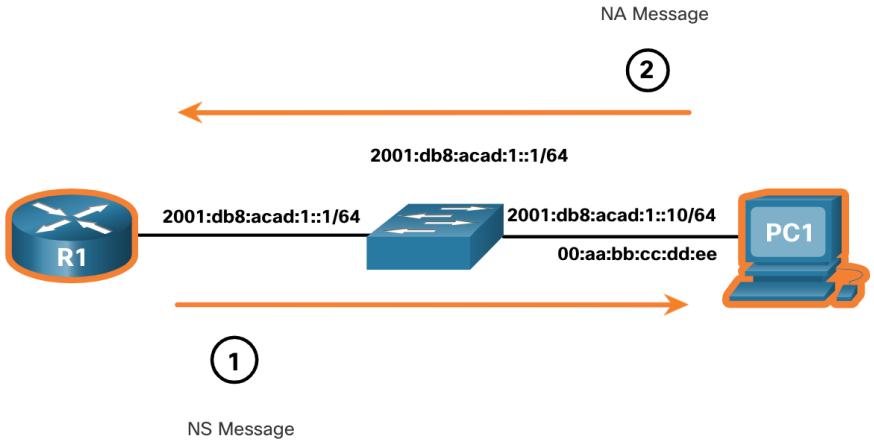
- Un périphérique auquel est attribuée une adresse IPv6 globale ou une adresse monodiffusion locale par lien peut effectuer une détection en double (DAD) pour s'assurer que l'adresse IPv6 est unique.
- Pour vérifier l'unicité d'une adresse, l'appareil enverra un message NS avec sa propre adresse IPv6 comme adresse IPv6 ciblée.
- Si un autre appareil sur le réseau possède cette adresse, il répondra par un message NA notifiant à l'appareil émetteur que l'adresse est utilisée.



Remarque: la DAD n'est pas obligatoire, mais la RFC 4861 recommande que la DAD soit effectuée sur les adresses de monodiffusion.

Messages ICMPv6 (suite)

- Pour déterminer l'adresse MAC de destination, le périphérique envoie un message de sollicitation de voisin à l'adresse du nœud sollicité.
- Le message comprendra l'adresse IPv6 connue (ciblée). Le périphérique portant l'adresse IPv6 ciblée répond par un message d'annonce de voisin qui inclut son adresse MAC Ethernet.
- Dans la figure, R1 envoie un message NS à 2001:db8:acad:1 : :10 demandant son adresse MAC.



13.2 Tests à l'aide des commandes ping et traceroute

Ping - Tester la connectivité

- La commande **ping** est un utilitaire de test IPv4 et IPv6 qui utilise les messages de requête d'écho ICMP et de réponse d'écho pour tester la connectivité entre les hôtes et fournit un résumé qui inclut le taux de réussite et le temps moyen aller-retour vers la destination.
- Si aucune réponse n'est reçue dans ce délai, la commande ping indique dans un message que la réponse n'a pas été reçue.
- Il est courant que le premier ping soit expiré si la résolution d'adresse (ARP ou ND) doit être effectuée avant d'envoyer la demande d'écho ICMP.

```
S1#ping 192.168.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

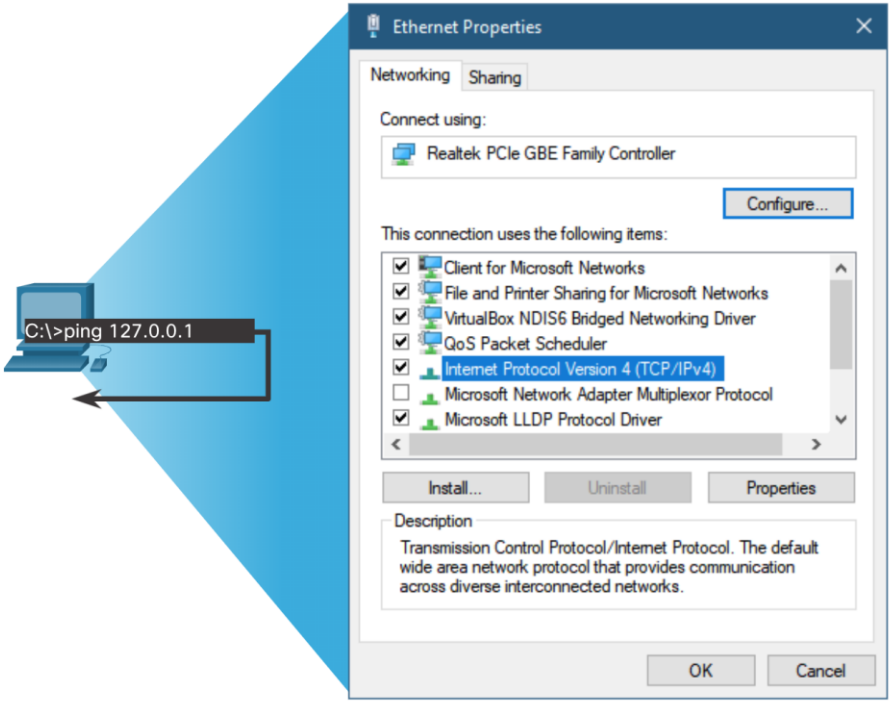
```
R1#ping 2001:db8:acad:1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Ping le Loopback

Ping peut être utilisé pour tester la configuration interne d'IPv4 ou IPv6 sur l'hôte local. Pour réaliser ce test, nous exécutons la commande **ping** sur l'adresse de loopback locale 127.0.0.1 pour l'IPv4 (et ::1 pour l'IPv6).

- Une réponse provenant de l'adresse 127.0.0.1 pour l'IPv4 ou ::1 pour l'IPv6 indique que le protocole IP est correctement installé sur l'hôte.
- Un message d'erreur indique que le TCP/IP n'est pas opérationnel sur l'hôte.

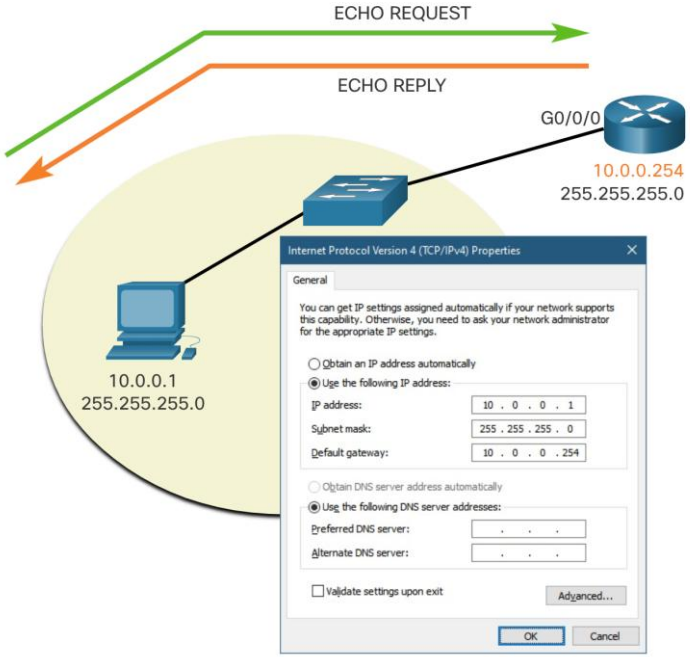


Ping la passerelle par défaut

La commande **ping** peut être utilisée pour tester la capacité d'un hôte à communiquer sur le réseau local.

L'adresse de passerelle par défaut est le plus souvent utilisée car le routeur est normalement toujours opérationnel.

- Un **ping** réussi vers la passerelle par défaut indique que l'hôte et l'interface du routeur servant de passerelle par défaut sont tous deux opérationnels sur le réseau local.
- Si l'adresse de passerelle par défaut ne répond pas, un **ping** peut être envoyé à l'adresse IP d'un autre hôte sur le réseau local dont on sait qu'il est opérationnel.

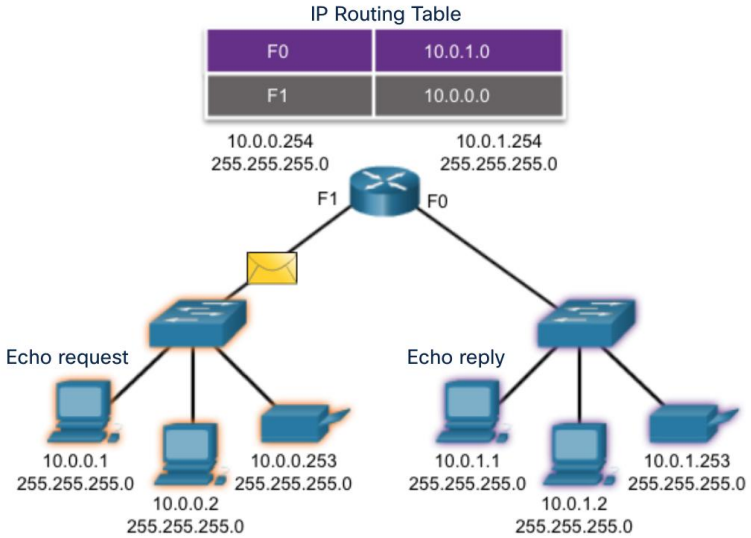


Ping un hôte distant

La commande ping peut aussi être utilisée pour tester la capacité d'un hôte local à communiquer sur un interréseau.

Un hôte local peut effectuer un ping sur un hôte sur un réseau distant. Un succès d'une requête **ping** sur l'interréseau confirme la communication sur le réseau local.

Remarque: de nombreux administrateurs de réseau limitent ou interdisent l'entrée de messages ICMP ; par conséquent, l'absence de réponse **ping** pourrait être due à des restrictions de sécurité.



Traceroute – Tester le chemin

- Traceroute (**tracert**) est un utilitaire qui est utilisé pour tester le chemin entre deux hôtes et fournir une liste des houblons qui ont été atteints avec succès le long de ce chemin.
- Traceroute fournit un temps d'aller-retour pour chaque saut le long du chemin et indique si un saut ne répond pas. Un astérisque (*) indique un paquet perdu ou sans réponse.
- Ces informations peuvent être utilisées pour localiser un routeur problématique dans le trajet ou peuvent indiquer que le routeur est configuré pour ne pas répondre.

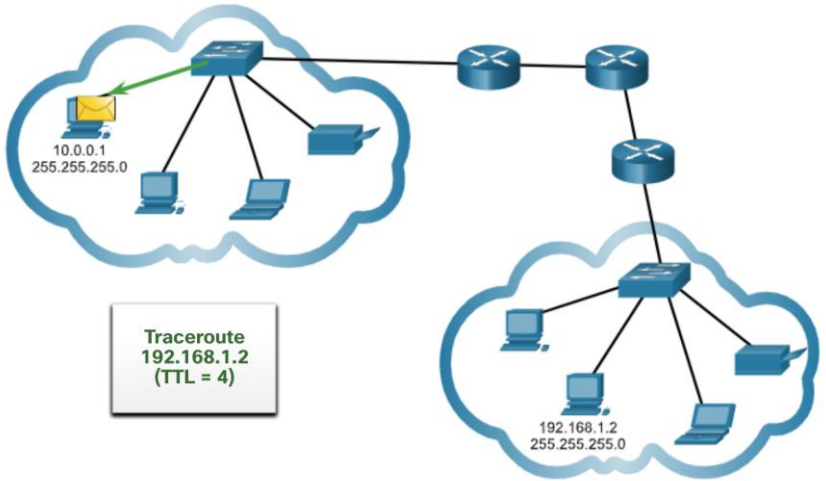
```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

  1   192.168.10.2    1 msec    0 msec    0 msec
  2   192.168.20.2    2 msec    1 msec    0 msec
  3   192.168.30.2    1 msec    0 msec    0 msec
  4   192.168.40.2    0 msec    0 msec    0 msec
```

Remarque: Traceroute utilise une fonction du champ TTL en IPv4 et du champ Hop Limit en IPv6 dans les en-têtes de la couche 3, ainsi que le message ICMP Délai dépassé.

Traceroute – Tester le chemin (suite)

- Le premier message envoyé par traceroute aura une valeur de champ TTL de 1. Le TTL s'arrête alors au premier routeur. Ce routeur répond alors par un message ICMPv4 de Délai dépassé.
- Traceroute incrémente ensuite progressivement le champ TTL (2, 3, 4...) pour chaque séquence de messages. Cela fournit à la trace l'adresse de chaque saut au fur et à mesure que les paquets s'écoulent plus loin sur le chemin.
- Le champ TTL est incrémenté jusqu'à ce que la destination soit atteinte ou jusqu'à une valeur maximale prédéfinie.



Packet Tracer –Vérifier l'adressage IPv4 et IPv6

Dans le cadre de ce Packet Tracer, vous ferez ce qui suit :

- Compléter la documentation du tableau d'adressage
- Tester la connectivité à l'aide de la commande ping
- Découvrez le chemin en traçant l'itinéraire

Packet Tracer – Utiliser Ping et Traceroute pour tester la connectivité réseau

Dans le cadre de ce Packet Tracer, vous ferez ce qui suit :

- Tester et restaurer la connectivité IPv4
- Tester et restaurer la connectivité IPv6

13.3 Module pratique et questionnaire

Packet Tracer — Utiliser ICMP pour tester et corriger la connectivité réseau

Dans le cadre de ce Packet Tracer, vous ferez ce qui suit :

- Utilisez ICMP pour localiser les problèmes de connectivité.
- Configurez les périphériques réseau pour corriger les problèmes de connectivité.

Travail Pratique — Utiliser Ping et Traceroute pour tester la connectivité réseau

Au cours de ce TP, vous aborderez les points suivants:

- Construire et configurer le réseau
- Utiliser la commande ping pour tester sommairement le réseau
- Utiliser les commandes Tracert et Traceroute pour les tests de base du réseau
- Résoudre les problèmes de topologie

Qu'est-ce que j'ai appris dans ce module?

- L'objectif des messages ICMP est de fournir un retour d'information sur les questions liées au traitement des paquets IP sous certaines conditions.
- Les messages ICMP communs à ICMPv4 et ICMPv6 sont les suivants: accessibilité de l'hôte, destination ou service inaccessible et délai dépassée.
- Les messages entre un routeur IPv6 et un périphérique IPv6, y compris l'allocation d'adresses dynamique, incluent RS et RA. Les messages entre les périphériques IPv6 incluent la redirection (similaire à IPv4), NS et NA.
- Ping (utilisé par IPv4 et IPv6) utilise les messages ICMP de demande d'écho et de réponse d'écho pour tester la connectivité entre les hôtes
- Ping peut être utilisé pour tester la configuration interne d'IPv4 ou IPv6 sur l'hôte local.
- Traceroute (tracert) génère une liste des sauts qui ont été atteintes avec succès le long du chemin.


CISCO