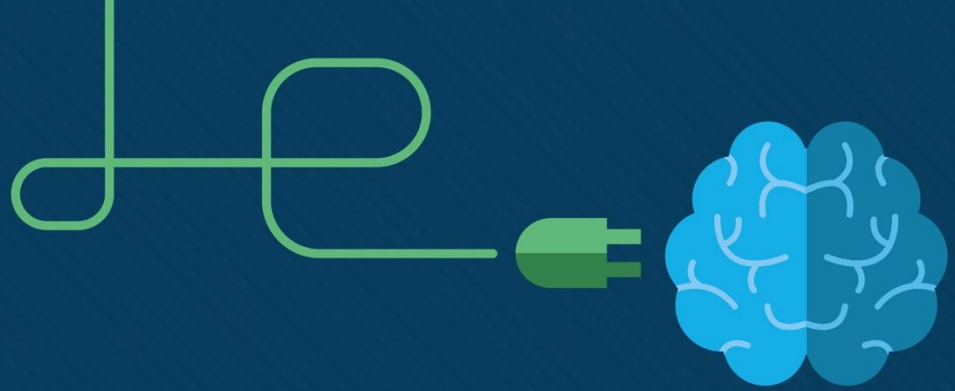
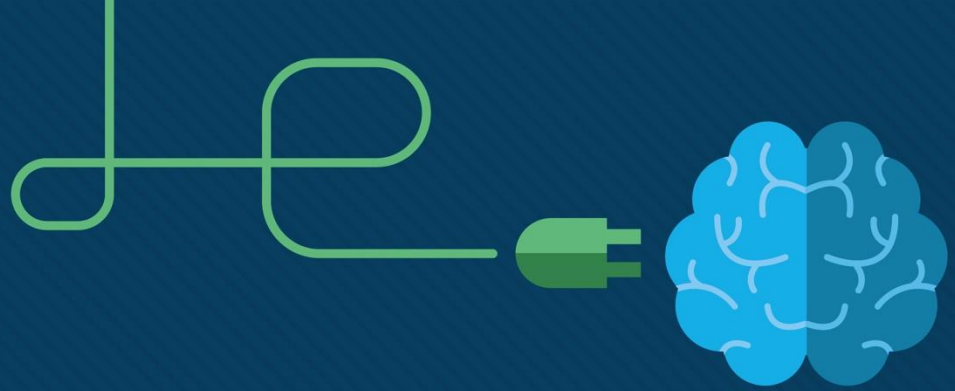


Module 17 : Construire un petit réseau

Contenu Pédagogique de l'instructeur

Présentation des réseaux V7.0
(ITN)



Module 17 : Construire un petit réseau

Présentation des réseaux V7.0 (ITN)

Objectifs de ce module

Titre du module : Construire un petit réseau

Module Objectif: Mettre en œuvre la conception d'un petit réseau avec un routeur, un commutateur et des terminaux.

Titre du rubrique	Objectif du rubrique
Périphériques d'un petit réseau	Identifier les équipements entrant dans la conception d'un petit réseau.
Applications et protocoles des réseaux de petite taille	Identifier les protocoles et applications utilisés dans un petit réseau.
Évolution vers de plus grands réseaux	Expliquer comment un petit réseau sert de base aux réseaux plus importants.
Vérification de la connectivité	Utiliser les résultats des commandes ping et tracert pour vérifier la connectivité et déterminer les performances relatives d'un réseau.
Commandes d'hôte et IOS	Utiliser des commandes d'hôte et IOS pour obtenir des informations sur les périphériques d'un réseau.
Méthodologies de dépannage	Décrire les méthodes courantes de dépannage des réseaux.
Scénarios de dépannage	Dépanner les problèmes liés aux périphériques d'un réseau.

17.1 Périphériques d'un petit réseau

Topologies de petits réseaux

- La majorité des entreprises sont petites, la plupart des réseaux d'entreprises sont également petits.
- Une petite conception de réseau est généralement simple.
- Les petits réseaux ont généralement une seule connexion WAN fournie par DSL, câble ou une connexion Ethernet.
- Les grands réseaux nécessitent un service informatique pour gérer, sécuriser et dépanner les périphériques réseau et protéger les données de l'organisation. Les petits réseaux sont gérés par un technicien informatique local ou par un professionnel contractuel.

Sélection des périphériques dans un petit réseau

Pour répondre aux besoins des utilisateurs, même les réseaux de petite taille doivent faire l'objet d'une planification et d'une conception. La planification garantit que tous les besoins, les facteurs de coûts et les options de déploiement sont pris en compte. Un des premiers critères à prendre en compte lors de la mise en œuvre d'un réseau de petite taille est le type de périphériques intermédiaires à utiliser pour la prise en charge du réseau.

Les facteurs qui doivent être pris en compte lors de la sélection des périphériques réseau sont les suivants :

- Coût
- Vitesse et types de port/d'interface
- Évolutivité
- Caractéristiques et services du système d'exploitation

Adressage IP pour un petit réseau

Lors de la mise en œuvre d'un réseau, créez un système d'adressage IP et utilisez-le. Tous les hôtes d'un interréseau doivent avoir une adresse unique. Les périphériques qui seront pris en compte dans le système d'adressage IP sont les suivants :

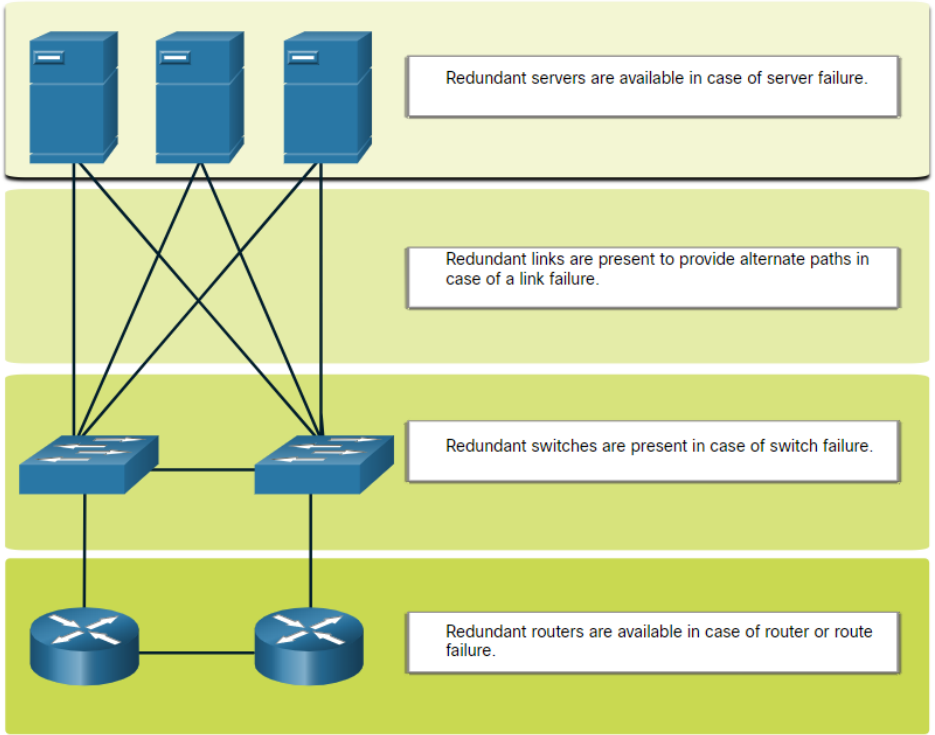
- Appareils de l'utilisateur final - Le nombre et le type de connexions (c.-à-d. filaires, sans fil, accès à distance)
- Serveurs et périphériques (p. ex. imprimantes et caméras de sécurité)
- les périphériques intermédiaires tel que les routeurs, les commutateurs et les points d'accès.

Il est recommandé de planifier, documenter et gérer un système d'adressage IP basé sur le type de périphérique. L'utilisation d'un système d'adressage IP planifié facilite l'identification d'un type de périphérique et la résolution des problèmes.

Redondance dans un petit réseau

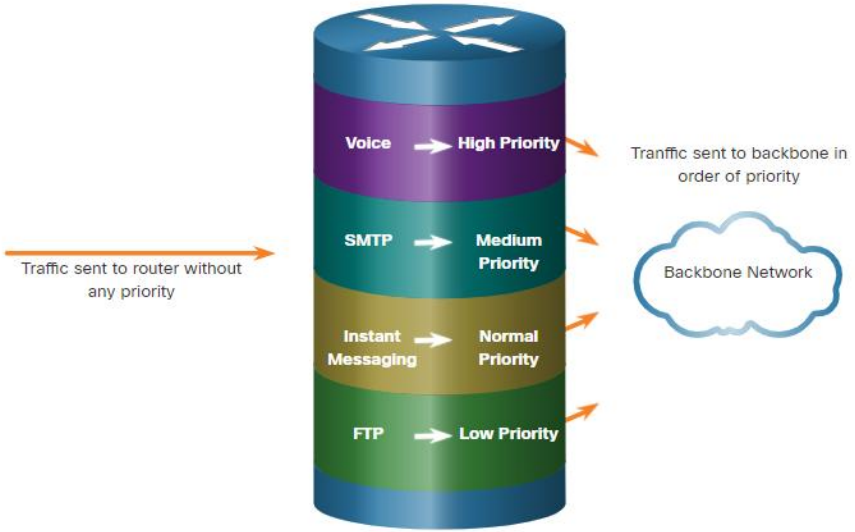
Pour assurer un niveau de fiabilité élevé, la *redondance* doit être pensée dans la conception du réseau. La redondance permet d'éliminer les points de défaillance uniques.

La redondance peut être réalisée en installant des équipements en double. Il peut également être réalisé en fournissant des liaisons réseau en double pour les zones critiques.



Gestion du trafic

- L'objectif de la conception du réseau, quelle que soit sa taille, est d'améliorer la productivité des employés et de réduire le temps d'indisponibilité du réseau.
- Les routeurs et les commutateurs d'un petit réseau doivent être configurés pour prendre en charge le trafic en temps réel, tel que la voix et la vidéo, de manière appropriée par rapport aux autres trafics de données. Une bonne conception de réseau mettra en œuvre la qualité de service (QoS).
- La mise en file d'attente par priorité présente quatre files d'attente. La file d'attente de priorité élevée est toujours vidée en premier.



17.2 – Applications et protocoles des réseaux de petite taille

Applications courantes

Une fois que vous l'avez configuré, votre réseau a toujours besoin de certains types d'applications et de protocoles pour fonctionner. L'utilité du réseau dépend des applications qu'il comporte.

Il existe deux formes de programmes ou processus logiciels permettant d'accéder au réseau :

- **Applications de réseau**: Applications qui mettent en œuvre les protocoles de la couche application et sont capables de communiquer directement avec les couches inférieures de la pile de protocoles.
- **Services de couche d'application** : pour les applications qui ne sont pas compatibles avec le réseau, les programmes qui interfacent avec le réseau et préparent les données pour le transfert.

Applications courantes

Les protocoles réseau prennent en charge les services et applications utilisés par les employés d'un petit réseau.

- Les administrateurs réseau ont généralement besoin d'accéder aux périphériques et serveurs réseau. Les deux solutions d'accès à distance les plus courantes sont Telnet et Secure Shell (SSH).
- Hypertext Transfer Protocol (HTTP) et Hypertext Transfer Protocol Secure (HTTP) sont utilisés entre les clients Web et les serveurs Web.
- Les protocoles SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol) et IMAP (Internet Message Access Protocol) sont utilisés pour l'envoi et la réception des e-mails.
- File Transfer Protocol (FTP) et Security File Transfer Protocol (SFTP) sont utilisés pour télécharger et charger des fichiers entre un client et un serveur FTP.
- Le protocole DHCP (Dynamic Host Configuration Protocol) est utilisé par les clients pour acquérir une configuration IP à partir d'un serveur DHCP.
- Le protocole DNS (Domain Name Service) est utilisé pour convertir les noms de domaine en adresses IP.

Remarque : un serveur peut fournir plusieurs services réseau. Par exemple, un serveur peut être un serveur de messagerie, FTP et SSH.

Applications courantes

Ces protocoles réseau constituent la boîte à outils indispensable d'un professionnel des réseaux.

- Les processus sur l'une des extrémités d'une session de communication.
- Types des messages
- Syntaxe des messages
- Signification des champs d'information
- La manière dont les messages sont envoyés et la réponse attendue
- L'interaction avec la couche du niveau juste en dessous

De nombreuses entreprises ont pris le parti d'utiliser autant que possible les versions (Tel que SSH, SFTP, and HTTPS) sécurisées de ces protocoles.

Applications voix et vidéo

- De nos jours, les entreprises utilisent de plus en plus les solutions de téléphonie IP et de transmission multimédia en continu pour communiquer avec leurs clients et partenaires commerciaux.
- L'administrateur réseau doit s'assurer que l'équipement approprié est installé dans le réseau et que les périphériques réseau sont configurés pour assurer un acheminement prioritaire.
- Les facteurs qu'un petit administrateur réseau doit prendre en compte lorsqu'il prend en charge des applications en temps réel :
  - **Infrastructure -** Dispose-t-elle de la capacité et de les moyens de prendre en charge des applications en temps réel ?
  - **VoIP -** VoIP est généralement moins cher que la téléphonie IP, mais au prix de la qualité et des fonctionnalités.
  - **Téléphonie IP -** Cela emploie des serveurs dédiés sous forme de contrôle d'appel et de signalisation.
  - **Applications en temps réel -**Le réseau doit prendre en charge les mécanismes de qualité de service (QoS) afin de minimiser les problèmes de latence. Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP) and two protocols that support real-time applications.

17.3 - Évolution vers de plus grands réseaux

Croissance des réseaux de petite taille

La plupart des petites entreprises se développent naturellement et leurs réseaux doivent suivre cette évolution. Dans l'idéal, l'administrateur réseau a suffisamment de temps pour prendre des décisions réfléchies concernant l'expansion du réseau en fonction de la croissance de l'entreprise.

Pour faire évoluer un réseau, plusieurs éléments sont nécessaires :

- **Documentation réseau** -Topologie physique et logique
- **Inventaire des équipements** - liste des périphériques qui utilisent ou constituent le réseau
- **Budget** -Budget informatique détaillé, y compris les achats d'équipements pour l'année fiscale
- **- Analyse du trafic** -les protocoles, les applications et les services, ainsi que leurs besoins respectifs en termes de trafic doivent être documentés

Ces éléments servent à éclairer la prise de décision qui accompagne l'évolution d'un petit réseau.

Analyse de protocoles

Il est important de comprendre le type de trafic qui traverse le réseau ainsi que le flux de trafic actuel. Plusieurs outils de gestion réseau peuvent être utilisés à cette fin.

Pour déterminer des modèles de flux de trafic, il est recommandé d'effectuer les points suivants:

- Capturer le trafic pendant les périodes de pointe pour obtenir une représentation juste des différents types de trafic
- Effectuer la capture sur différents segments du réseau et périphériques tel que certaines parties du trafic pouvant être locales sur un segment spécifique.
- Les informations collectées par l'analyseur de protocole sont évaluées en fonction de la source et de la destination du trafic, ainsi que du type de trafic envoyé.
- L'analyse peut ensuite être utilisée pour déterminer comment améliorer la gestion du trafic.

Utilisation du réseau par employés

De nombreux systèmes d'exploitation fournissent des outils intégrés pour afficher ces informations d'utilisation du réseau. Ces outils peuvent être utilisés pour capturer un « instantané » d'informations telles que :

- Système d'exploitation et version du système d'exploitation
- Utilisation de la CPU
- Utilisation de la mémoire vive
- Utilisation des disques durs
- Applications non-réseau
- Applications réseau

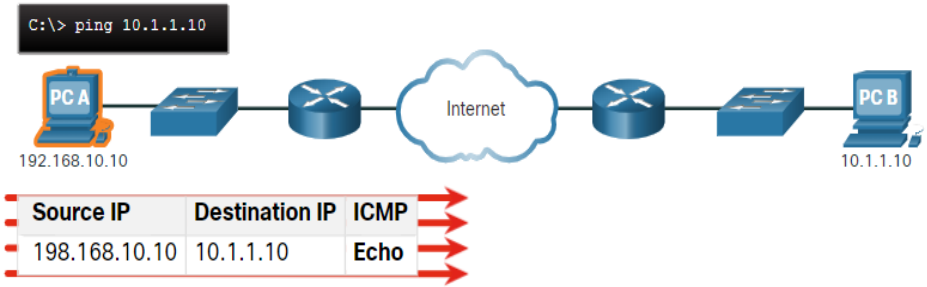
Documenter les instantanés des employés d'un petit réseau sur une certaine période est très utile pour identifier l'évolution des exigences du protocole et les flux de trafic associés.

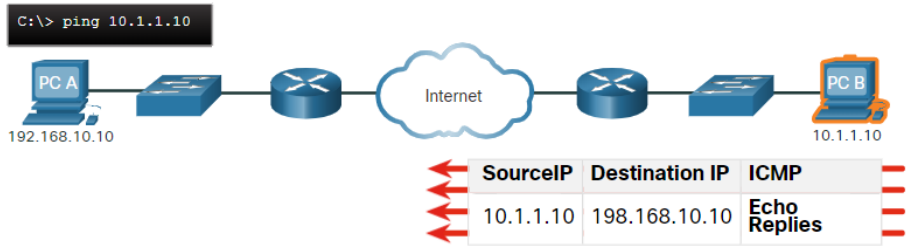
17.4 Vérifiez la connectivité

Vérifier la connectivité avec Ping

Que votre réseau soit petit et neuf, ou que vous mettiez à l'échelle un réseau existant, vous voudrez toujours être en mesure de vérifier que vos composants sont correctement connectés les uns aux autres et à Internet.

- La commande ping, disponible sur la plupart des systèmes d'exploitation, est le moyen le plus efficace de tester rapidement la connectivité de couche 3 entre une adresse IP source et de destination.
- La commande ping utilise les messages d'écho ICMP (Internet Control Message Protocol) (ICMP Type 8) et de réponse d'écho (ICMP Type 0).





Vérifier la connectivité avec Ping (suite)

Sur un hôte Windows 10, la commande ping envoie quatre messages d'écho ICMP consécutifs et attend quatre réponses d'écho ICMP consécutives de la destination. Le ping IOS envoie cinq messages d'écho ICMP et affiche un indicateur pour chaque réponse d'écho ICMP reçue.

Ir

Élément	Description
!	•Le point d'exclamation indique la réception réussie d'un message de réponse d'écho. •Il valide une connexion de couche 3 entre la source et la destination.
.	•Un délai signifie que le temps a expiré en attendant un message de réponse d'écho. •Il peut par exemple indiquer qu'un problème de connectivité a été rencontré sur le chemin parcouru.
U	•La lettre « **U** » indique qu'un routeur situé sur le chemin et ne possédant pas de route vers l'adresse de destination a répondu par un message ICMP d'inaccessibilité. •Les raisons possibles incluent le routeur ne connaît pas la direction vers le réseau de destination ou il n'a pas pu trouver l'hôte sur le réseau de destination.

Note : D'autres réponses ping possibles incluent Q, M, ? , ou &. Cependant, leur signification est hors de portée pour ce module

Ping étendu

Cisco IOS propose un mode « étendu » de la commande **ping** .

Le ping étendu est entré en mode d'exécution privilégié en tapant **ping** sans adresse IP de destination. Vous recevrez ensuite plusieurs invites pour personnaliser le **ping** étendu.

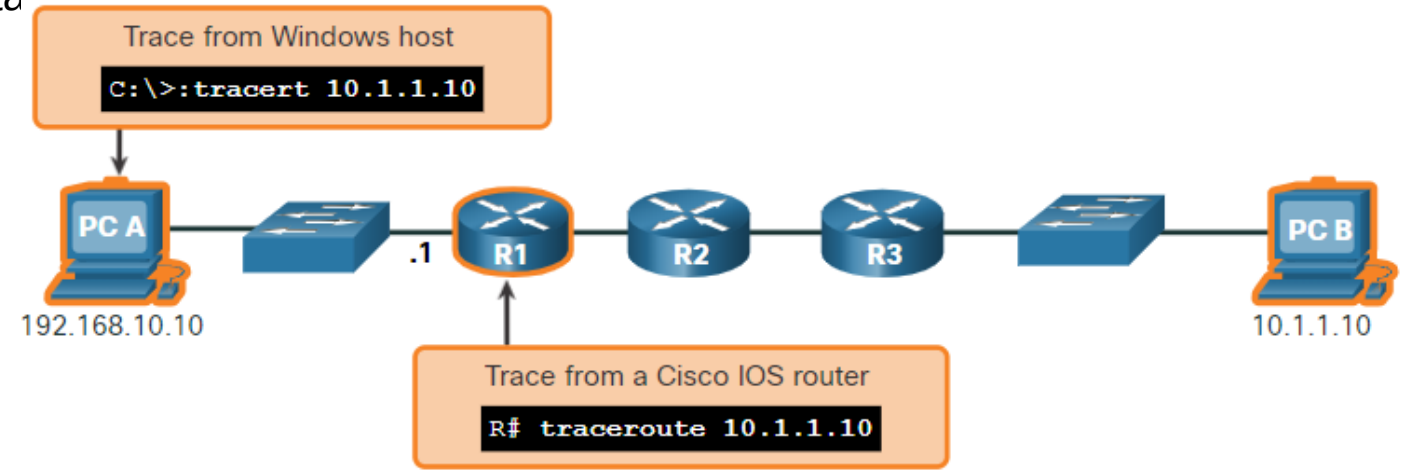
Remarque: Appuyez **Enter** pour accepter les valeurs par défaut indiquées. la commande **ping ipv6** est utilisée pour les ping IPv6 étendus.

```
R1# ping
Protocol [ip]:
Target IP address: 10.1.1.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Ingress ping [n]:
Source address or interface: 192.168.10.1
DSCP Value [0]:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0x0000ABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

Vérifier la connectivité avec Traceroute

La commande ping est utile pour déterminer rapidement s'il existe un problème de connectivité de couche 3. Cependant, il n'identifie pas où le problème se trouve le long du chemin.

- Traceroute peut aider à localiser les zones problématiques de couche 3 dans un réseau. Cette commande renvoie une liste des sauts effectués par un paquet acheminé à travers un réseau.
- La syntaxe de la commande trace varie d'un système d'exploitation à l'autre.



Vérifier la connectivité avec Traceroute (suite)

- Voici un exemple de sortie de la commande **tracert** sur un hôte Windows 10.

  Remarque : Utilisez **Ctrl-C** pour interrompre un **tracert** dans Windows.

- La seule réponse réussie provient de la passerelle sur R1. Les requêtes de suivi vers le saut suivant ont expiré comme indiqué par l'astérisque (*), ce qui signifie que le routeur de saut suivant n'a pas répondu ou qu'il y a une défaillance dans le chemin réseau. Dans cet exemple, il semble y avoir un problème entre R1 et R2.

```
C:\Users\PC-A> tracert 10.1.1.10
Tracing route to 10.1.10 over a maximum of 30 hops:
  1     2 ms     2 ms     2 ms  192.168.10.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
^C
C:\Users\PC-A>
```

Vérifier la connectivité avec Traceroute (suite)

Voici des exemples de sortie de la commande traceroute de R1 :

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3 10.1.1.10 1 msec 0 msec
R1#
```

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3  *  *  *
  4  *  *  *
  5  *
```

- Sur la gauche, la trace a validé qu'elle pouvait atteindre le PC B.
- Sur la droite, l'hôte 10.1.1.10 n'était pas disponible et la sortie affiche des astérisques où les réponses ont expiré. Les délais d'expiration indiquent un problème réseau potentiel.
- Utilisez **Ctrl-Shift-6** pour interrompre un **traceroute** dans Cisco IOS.

Remarque: l'implémentation Windows de traceroute (tracert) envoie des demandes d'écho ICMP. Cisco IOS et Linux utilisent UDP avec un numéro de port non valide. La destination finale renverra un message de port ICMP inaccessible.

Traceroute étendue

Comme la commande **ping** étendue, il y a aussi une commande **traceroute** étendue. Il permet à l'administrateur d'ajuster les paramètres liés à l'opération de commande.

La commande **tracert** Windows permette la saisie de plusieurs paramètres et doit être exécutée par le biais d'options dans la ligne de commande. Cependant, il n'est pas guidé comme la commande traceroute étendue IOS. La sortie suivante affiche les options disponibles pour la commande Windows **tracert** :

```
C:\Users\PC-A> tracert /?
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name
Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
C:\Users\PC-A>
```

Traceroute étendue

- L'option **traceroute** étendue Cisco IOS permet à l'utilisateur de créer un type spécial de trace en ajustant les paramètres liés à l'opération de commande.
- La commande traceroute étendu est entré en mode d'exécution privilégié en tapant **traceroute** sans adresse IP de destination. IOS vous guide à travers les options de commande en proposant un certain nombre d'invites associées au réglage des différents paramètres.

- **Remarque**: Appuyez **Enter** pour accepter les valeurs par défaut indiquées.

```
R1# traceroute
Protocol [ip]:
Target IP address: 10.1.1.10
Ingress traceroute [n]:
Source address: 192.168.10.1
DSCP Value [0]:
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 192.168.10.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 1 msec 1 msec
  2 209.165.200.230 0 msec 1 msec 0 msec
  3  *
    10.1.1.10 2 msec 2 msec
R1#
```

Base du réseau

- L'un des moyens les plus efficaces pour surveiller les performances d'un réseau et le dépanner consiste à établir un profil de référence du réseau.
- Pour commencer à élaborer un profil de référence, vous pouvez copier et coller dans un fichier texte les résultats d'une commande telle que ping, trace ou autre. These text files can be time stamped with the date and saved into an archive for later retrieval and comparison.
- Parmi les éléments dont il faut tenir compte, les messages d'erreur et les temps de réponse d'un hôte à l'autre fournissent des indications précieuses.
- Les réseaux des entreprises doivent disposer de profils de référence si détaillés qu'ils dépassent largement le cadre de ce cours. Il existe toutefois des outils logiciels de qualité professionnelle pour collecter et gérer les informations des profils de référence.

Travaux pratiques - Vérifiez la latence réseau en utilisant les commandes Ping et Traceroute

Au cours de ces travaux pratiques, vous aborderez les points suivants :

- Partie 1 : Utiliser la commande ping pour documenter la latence réseau
- Partie 2 : Utiliser la commande traceroute pour documenter la latence réseau

17.5 Commandes d'hôte et IOS

Configuration IP sur un hôte Windows

Dans Windows 10, vous pouvez accéder aux détails de l'adresse IP à partir du **Centre Réseau et Partage** pour afficher rapidement les quatre paramètres importants : adresse, masque, routeur et DNS. Ou vous pouvez émettre la commande **ipconfig** à la ligne de commande d'un ordinateur Windows.

- Utilisez la commande **ipconfig /all** pour afficher l'adresse MAC, ainsi qu'un certain nombre de détails concernant l'adressage de couche 3 de l'appareil.
- Si un hôte est configuré en tant que client DHCP, la configuration de l'adresse IP peut être renouvelée à l'aide des commandes **ipconfig /release** et **ipconfig /renew** .
- Le service Client DNS sur les ordinateurs Windows optimise également les performances de la résolution des noms DNS en stockant en mémoire les noms déjà résolus. La commande **ipconfig /displaydns** affiche toutes les entrées DNS mises en cache sur un système Windows.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```

Configuration IP sur un hôte Linux

- La vérification des paramètres IP à l'aide de l'interface graphique sur une machine Linux diffère en fonction de la distribution Linux et de l'interface de bureau.
- Sur la ligne de commande, utilisez la commande **ifconfig** pour afficher l'état des interfaces actives et leur configuration IP.
- La commande Linux **ip address** est utilisée pour afficher les adresses et leurs propriétés. Il peut également être utilisé pour ajouter ou supprimer des adresses IP.

```
[analyst@secOps ~]$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:b5:d6:cb
          inet addr: 10.0.2.15  Bcast:10.0.2.255  Mask: 255.255.255.0
          inet6 addr: fe80::57c6:ed95:b3c9:2951/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1332239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105910 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1855455014 (1.8 GB)  TX bytes:13140139 (13.1 MB)
lo: flags=73  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Remarque : La sortie affichée peut varier en fonction de la distribution Linux.

Commandes hôte et IOSConfiguration IP sur un hôte macOS

- Dans l'interface graphique d'un hôte Mac, ouvrez **Préférences réseau > Avancé** pour obtenir les informations d'adressage IP.
- La commande **ifconfig** peut également être utilisée pour vérifier la configuration IP de l'interface sur la ligne de commande.
- Les autres commandes macOS utiles pour vérifier les paramètres IP de l'hôte incluent **networksetup -listallnetworkservices** and the **networksetup -getinfo <***network service***>**.

```
MacBook-Air:~ Admin$ networksetup -listallnetworkservices
An asterisk (*) denotes that a network service is disabled.
iPhone USB
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
MacBook-Air:~ Admin$
MacBook-Air:~ Admin$ networksetup -getinfo Wi-Fi
DHCP Configuration
IP address: 10.10.10.113
Subnet mask: 255.255.255.0
Router: 10.10.10.1
Client ID:
IPv6: Automatic
IPv6 IP address: none
IPv6 Router: none
Wi-Fi ID: c4:b3:01:a0:64:98
MacBook-Air:~ Admin$
```

La commande arp

La commande **arp** est exécutée à partir de l'invite de commande Windows, Linux ou Mac. La commande arp –a répertorie tous les appareils actuellement présents dans le cache ARP de l'hôte.

- La commande **arp -a** affiche l'adresse IP connue et la liaison d'adresse MAC. En effet, le cache ARP n'affiche que les informations provenant d'appareils qui ont été consultés récemment.
- Pour être sûr que le cache ARP contient des informations sur un périphérique donné dans son tableau ARP, envoyez une requête **ping** à ce périphérique.
- Le cache peut être vidé en utilisant la commande **netsh interface ip deletearpcache** dans le cas où l'administrateur réseau souhaite repeupler le cache avec des informations mises à jour.

Remarque : Vous pouvez avoir besoin d'un accès administrateur sur l'hôte pour pouvoir utiliser la commande netsh interface ip delete arpcache.

Révision des commandes de l'émission commune

Commande	Description
show running-config	Vérifie la configuration et les paramètres actuels
show interfaces	Vérifie l'état de l'interface et affiche les messages d'erreur
show ip interface	Vérifie les informations de couche 3 d'une interface
show arp	Vérifie la liste des hôtes connus sur les réseaux locaux Ethernet locaux
show ip route	Vérifie les informations de routage de couche 3
show protocols	Vérifie quels protocoles sont opérationnels
show version	Vérifie la mémoire, les interfaces et les licences du périphérique

La commande show cdp neighbors

Le protocole CDP fournit les informations suivantes concernant chaque périphérique CDP voisin :

- **Identificateurs de périphérique** - nom d'hôte configuré d'un commutateur, d'un routeur ou d'un autre périphérique
- **Liste d'adresses** - jusqu'à une adresse de couche réseau pour chaque protocole pris en charge.
- **Identificateur de port** - le nom du port local et distant sous la forme d'une chaîne de caractères ASCII, comme FastEthernet 0/0.
- **Liste des capacités** : si un périphérique spécifique est un commutateur de couche 2 ou un commutateur de couche 3
- **Plate-forme**

La commande **sh** périphérique voisin.

```
R3# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S3               Gig 0/0/1         122              S I   WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#
```

La commande show ip interface brief

Pour vérifier les interfaces d'un routeur, la commande **show ip interface brief** est l'une des plus utilisées. Cette commande est souvent préférée à la commande **show ip interface**, car ses résultats sont plus abrégés. Elle fournit un résumé des informations clés pour toutes les interfaces réseau d'un routeur.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.254.250 YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  up                    up
```

Vidéo des commandes hôte et IOS — La commande show version

Cette vidéo montrera l'utilisation de la commande show version pour afficher des informations sur le routeur.

Packet Tracer - Analyser le résultat des commandes Show

Cet exercice a pour objectif de vous aider à mieux maîtriser les commandes **show** du routeur. Vous n'avez pas besoin d'effectuer la configuration. Examinez plutôt le résultat de plusieurs commandes show.

17.6 – Méthodologie de dépannage

Méthodes de dépannage de base

Étape	Description
Étape 1. Identifier le problème	•La première étape de la procédure de dépannage. •Si des outils peuvent être utilisés à cette étape, une conversation avec l'utilisateur est souvent très utile.
Étape 2. Élaborer une théorie des causes probables	•Une fois le problème identifié, essayez d'établir une théorie des causes probables. •Cette étape fait généralement naître plusieurs causes probables.
Étape 3. Tester la théorie pour déterminer la cause	•En fonction des causes probables, testez vos théories afin de dégager la véritable cause du problème. •Un technicien peut alors appliquer une rapide procédure et voir si cela permet de résoudre le problème. •Si une procédure rapide ne permet pas de résoudre le problème, il peut être nécessaire d'effectuer des recherches complémentaires en vue de déterminer la cause exacte.
Étape 4. Établir un plan d'action pour résoudre le problème et implémenter la solution	Après avoir déterminé la cause exacte du problème, établissez un plan d'action en vue de le résoudre en implémentant la solution.
Étape 5. Vérifier la solution et mettre en œuvre des mesures préventives	•Après avoir corrigé le problème, vérifiez la fonctionnalité complète. •le cas échéant, mettre en œuvre des mesures préventives.
Étape 6. Documenter les résultats des	•Au cours de la dernière étape du processus de dépannage, vous devez documenter les résultats de vos recherches ainsi que les actions entreprises.

Résoudre ou transférer?

- Dans certains cas, il peut s'avérer impossible de résoudre le problème immédiatement. Lorsqu'un problème nécessite la décision d'un responsable ou une certaine expertise, ou lorsque le technicien ne dispose pas des droits d'accès réseau requis, le problème doit être transféré à qui de droit.
- La politique d'entreprise doit clairement établir les conditions de transfert d'un problème.

La commande debug

- La commande **debug** d'IOS permet à l'administrateur d'afficher ces messages en temps réel pour analyse.
- Toutes les commandes **debug** sont entrées en mode d'exécution privilégié. Le système Cisco IOS permet d'affiner les résultats de la commande **debug** et d'inclure uniquement les fonctionnalités ou sous-fonctionnalité pertinentes. Il est donc conseillé de n'utiliser les commandes **debug** que pour résoudre des problèmes spécifiques.
  - Pour afficher une brève description des options de débogage, utilisez la commande **debug ?** en mode d'exécution privilégié, dans la ligne de commande.
  - Pour désactiver une fonction de débogage spécifique, ajoutez le mot clé **no** devant la commande **debug**
  - Sinon, vous pouvez entrer la forme **undebug** de la commande en mode d'exécution privilégié
  - Pour désactiver toutes les commandes debug actives en une seule fois, utilisez la commande **undebug all**
- Soyez prudents en utilisant certaines commandes **debug** , car elles peuvent générer une quantité substantielle de données et utiliser une grande partie des ressources du système. Le routeur doit afficher un grand nombre de messages **debug** et n'a pas suffisamment de puissance de traitement pour exécuter ses fonctions réseau, voire pour écouter les commandes et désactiver le débogage.

La commande terminal monitor

- **debug** et certains autres messages IOS ne sont pas automatiquement affichés sur les connexions à distance. Ceci est dû au fait que les messages de journal ne peuvent pas être affichés sur les lignes vty.
- Pour afficher les messages de journal sur un terminal (console virtuelle), utilisez la commande d'exécution privilégiée **terminal monitor**. Pour désactiver la journalisation des messages sur un terminal, utilisez la commande d'exécution privilégiée **terminal no monitor**.

```
R2# telnet 209.165.200.225
Trying 209.165.200.225 ... Open
 Authorized access only!
User Access Verification
Password:
R1> enable
Password:
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
```

```
R1#  terminal monitor
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 16:03:49.735: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.737: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.738: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.740: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.741: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
R1# no debug ip icmp
ICMP packet debugging is off
R1#
```

17.7 Scénarios de dépannage

Fonctionnement en duplex et problèmes d'incompatibilité

- Les interfaces Ethernet d'interconnexion doivent fonctionner dans le même mode duplex pour obtenir les meilleures performances de communication et pour éviter l'inefficacité et la latence sur la liaison.
- La fonction de négociation automatique Ethernet facilite la configuration, minimise les problèmes et maximise les performances de liaison entre deux liaisons Ethernet d'interconnexion. Les périphériques connectés annoncent d'abord les fonctionnalités qu'ils prennent en charge, puis choisissent le mode de performances le plus élevé pris en charge par les deux extrémités.
- Si l'un des deux périphériques connectés fonctionne en duplex intégral et l'autre en mode semi-duplex, nous avons un conflit des paramètres duplex. Si la communication de données s'effectue malgré le conflit des paramètres duplex, les performances de liaison sont très faibles.
- Les incompatibilités duplex sont généralement causées par une interface mal configurée ou, dans de rares cas, par une négociation automatique échouée. Résoudre un conflit des paramètres duplex peut s'avérer ardu, car la communication entre les périphériques concernés s'établit sans problème.

Problèmes d'adressage IP sur périphériques IOS

- Parmi les causes les plus courantes d'attribution IPv4 incorrecte, notons les erreurs d'attribution manuelle ou les problèmes DHCP.
- Les administrateurs réseau doivent souvent affecter manuellement des adresses IP à des périphériques tels que des serveurs et des routeurs. Si une erreur est commise au moment de l'affectation, il y a de fortes chances que cela génère des problèmes de communication avec le périphérique.
- Sur un équipement Cisco IOS, utilisez les commandes **show ip interface** ou **show ip interface brief** pour vérifier que les adresses IPv4 ont été attribuées aux interfaces réseau. Par exemple, l'émissi nterface sur R1.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```

Problèmes d'adressage IP sur périphériques finaux

- Sous Windows, lorsque le périphérique ne parvient pas à contacter un serveur DHCP, Windows attribue automatiquement une adresse appartenant à la plage 169.254.0.0/16. Cette fonctionnalité s'appelle l'adressage IP privé automatique (APIPA).
- Un ordinateur avec l'adresse APIPA il n'est généralement pas en mesure de communiquer avec d'autres périphériques du réseau, car il y a de fortes chances que ces périphériques n'appartiennent pas au réseau 169.254.0.0/16.
  - **Remarque** : Les autres systèmes d'exploitation, tels que Linux et OS X, n'utilisent pas APIPA.
- Si le périphérique n'est pas en mesure de communiquer avec le serveur DHCP, le serveur ne pourra pas attribuer d'adresse IPv4 au réseau requis et le périphérique ne pourra pas communiquer.
- Utilisez la commande **ipconfig** pour vérifier l'adresse IP attribuée à un ordinateur Windows.

Problèmes de passerelle par défaut

- La passerelle par défaut pour un appareil terminal est l'appareil de réseau le plus proche, appartenant au même réseau que l'appareil terminal, qui peut acheminer le trafic vers d'autres réseaux. Si un périphérique possède une adresse de passerelle par défaut incorrecte ou inexistante, il ne pourra pas communiquer avec les périphériques de réseaux distants.
- Tout comme les problèmes IPv4, les problèmes de passerelle par défaut peuvent être liés à une mauvaise configuration (en cas d'attribution manuelle) ou à des problèmes DHCP (en cas d'attribution automatique).
- Utilisez la commande **ipconfig** pour connaître la passerelle par défaut sur un ordinateur Windows.
- Sur un routeur, utilisez la commande **show ip route** pour afficher la table de routage et vérifier que la passerelle par défaut, appelée « route par défaut », a été définie. Cette route est utilisée lorsque l'adresse de destination du paquet ne correspond à aucune autre route dans sa table de routage.

Dépannage des problèmes DNS

- Il n'est pas rare qu'un utilisateur confonde le fonctionnement d'un lien Internet avec la disponibilité du service DNS.
- Les adresses du serveur DNS peuvent être attribuées manuellement ou automatiquement.
- Bien qu'il soit courant que les entreprises et les organisations gèrent leurs propres serveurs DNS, il y a toujours la possibilité d'utiliser n'importe quel serveur DNS accessible pour résoudre les noms.
- Cisco offre OpenDNS qui fournit un service DNS sécurisé en filtrant le phishing et certains sites malveillants. Les adresses OpenDNS sont 208.67.222.222 et 208.67.220.220. Des fonctionnalités avancées telles que le filtrage et la sécurité du contenu Web sont disponibles pour les familles et les entreprises.
- Utilisez la commande **ipconfig /all**, comme indiqué pour vérifier quel serveur DNS est utilisé par l'ordinateur Windows.
- La commande **nslookup** est un autre outil de dépannage DNS utile pour les ordinateurs. La commande **nslookup** permet à l'utilisateur de lancer manuellement des requêtes DNS et d'analyser la réponse DNS.

TP – Dépannage des problèmes de connectivité

Au cours de ces travaux pratiques, vous aborderez les points suivants :

- Identification du problème
- Mise en œuvre des modifications réseau
- Vérification du fonctionnement du système complet
- Documentation des résultats des recherches et modifications de configuration

Packet Tracer : Dépannage des problèmes de connectivité

L'objectif de cet exercice Packet Tracer est de résoudre les problèmes de connectivité, si possible. Sinon, les problèmes doivent être soigneusement notés et signalés.

17.8 Module pratique et questionnaire

TP — Concevoir et construire un réseau pour petites entreprises

Dans ce TP, vous allez concevoir et construire un réseau. Vous expliquerez comment un petit réseau de segments directement connectés est créé, configuré et vérifié.

PacketTracer - Exercice d'intégration des compétences

Dans cette activité Packet Tracer, vous utiliserez toutes les compétences que vous avez acquises tout au long de ce cours.

Scénario

Le routeur Central, le cluster ISP et le serveur web sont complètement configurés. vous devrez créer un nouveau système d'adressage IPv4 comprenant quatre sous-réseaux à l'aide du réseau 192.168.0.0/24. Le département IT a besoin de 25 hôtes. Le département des ventes a besoin de 50 hôtes. Le sous-réseau du reste de l'équipe a besoin de 100 hôtes. Un sous-réseau invité de 25 hôtes sera ajouté ultérieurement. Vous devez également configurer les paramètres de sécurité de base ainsi que les configurations des interfaces sur R1. Ensuite, vous devrez configurer l'interface SVI et les paramètres de sécurité élémentaires sur les commutateurs S1, S2 et S3.

Packet Tracer - Exercice de dépannage

Dans cette activité de Packet Tracer, vous allez résoudre un certain nombre de problèmes dans un réseau local existant.

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

- Les facteurs à prendre en compte lors de la sélection de périphériques réseau pour un petit réseau sont le coût, la vitesse et les types de ports/interfaces, l'évolutivité et les fonctionnalités et services du système d'exploitation.
- Lors de la mise en œuvre d'un réseau, créez un schéma d'adressage IP et utilisez-le sur des périphériques, des serveurs et des périphériques et des périphériques intermédiaires.
- La redondance peut être réalisée par l'installation d'équipements en double, mais elle peut aussi être réalisée par la fourniture de liaisons réseau en double pour les zones critiques.
- Les routeurs et les commutateurs d'un petit réseau doivent être configurés pour prendre en charge le trafic en temps réel, tel que la voix et la vidéo, de manière appropriée par rapport aux autres trafics de données.
- Il existe deux types de programmes ou processus logiciels permettant d'accéder au réseau : les applications de réseau et les services de couche application
- Pour mettre à l'échelle un réseau, plusieurs éléments sont requis : documentation réseau, inventaire des périphériques, budget et analyse du trafic.
- La commande ping est le moyen le plus efficace de tester rapidement la connectivité de couche 3 entre une adresse IP source et de destination.
- Le Cisco IOS offre un mode « étendu » de la commande ping qui permet à l'utilisateur de créer des types spéciaux de pings en ajustant les paramètres liés à l'opération de

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

- Cette commande renvoie une liste des sauts effectués par un paquet acheminé à travers un réseau.
- Il existe également une commande traceroute étendue. Il permet à l'administrateur d'ajuster les paramètres liés à l'opération de commande.
- Les administrateurs réseau visualisent les informations d'adressage IP (adresse, masque, routeur et DNS) sur un hôte Windows en émettant la commande ipconfig. Les autres commandes nécessaires sont **ipconfig /all**, **ipconfig /release**et **ipconfig /renew**, et **ipconfig /displaydns**.
- La vérification des paramètres IP à l'aide de l'interface graphique sur une machine Linux diffère en fonction de la distribution Linux (distribution) et de l'interface de bureau. Les commandes nécessaires sont ifconfig et ip address.
- Dans l'interface graphique d'un hôte Mac, ouvrez Préférences réseau > Avancé pour obtenir les informations d'adressage IP. Les autres commandes d'adressage IP pour Mac sont ifconfig, et networksetup -listallnetworkservices et networksetup -getinfo <network service>.
- La commande **arp** est exécutée à partir de l'invite de commande Windows, Linux ou Mac. La commande liste tous les périphériques actuellement dans le cache ARP de l'hôte, ce qui comprend l'adresse IPv4, l'adresse physique et le type d'adressage (statique/dynamique) pour chaque périphérique.

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

- Les commandes show courantes sont **show running-config**, **show interfaces**, **show ip address**, **show arp**, **show ip route**, **show protocols**et **show version**. La commande **show cdp neighbor** fournit les informations suivantes sur chaque voisin CDP: identifiants de périphérique, liste d'adresses, identifiant de port, liste des capacités et plate-forme.
- La commande **show cdp neighbors detail** permet de déterminer si l'un des voisins CDP présente une erreur de configuration IP.
- Le résultat de la commande **show ip interface brief** affiche toutes les interfaces du routeur, l'adresse IP attribuée à chaque interface et, le cas échéant, l'état opérationnel de l'interface.
- Les six étapes de base pour le dépannage Étape 1. Identifier le problème Étape 2. Établir une théorie sur les causes probables Étape 3. Tester la théorie en vue de déterminer la cause Étape 4. Établir un plan d'action pour résoudre le problème et implémenter la solution. Étape 5. Vérifier la solution et mettre en œuvre des mesures préventives. Étape 6. Documenter les constats, les actions et les résultats
- Lorsqu'un problème nécessite la décision d'un responsable ou une certaine expertise, ou lorsque le technicien ne dispose pas des droits d'accès réseau requis, le problème doit être transféré à qui de droit.
- Les processus, protocoles, mécanismes et événements OS génèrent des messages pour communiquer leur état. La commande debug d'IOS permet à l'administrateur d'afficher ces messages en temps réel pour analyse.
- Pour afficher les messages de journal sur un terminal (console virtuelle), utilisez la commande d'exécution privilégiée terminal monitor.


CISCO