Support du formateur Chapitre 11 : Conception d'un réseau de petite taille

CCNA Routing and Switching,

Introduction to Networks v6.0

Cisco | Networking Academy®
Mind Wide Open™

Supports du formateur – Chapitre 11 Guide de planification

Cette présentation PowerPoint est divisée en deux parties :

1. Guide de planification du formateur
   - Informations destinées à vous familiariser avec le chapitre
   - Outils pédagogiques
2. Présentation en classe pour le formateur
   - Diapositives facultatives que vous pouvez utiliser en classe
   - Commence à la diapositive 13

Remarque : retirez le guide de planification de cette présentation avant de la partager avec quiconque.

Introduction to Networks v6.0
Guide de planification
Chapitre 11 : Conception d'un réseau de petite taille

Cisco | Networking Academy®
Mind Wide Open™

Chapitre 11 : exercices

Quels sont les exercices associés à ce chapitre ?

N° de page	Type d'exercice	Nom de l'exercice	Facultatif ?
11.0.1.2	Exercice en classe	Avez-vous remarqué. . . ?	Recommandé
11.2.1.4	Exercice interactif	Menaces et failles de sécurité	Recommandé
11.2.2.5	Exercice interactif	Types d'attaques	Recommandé
11.2.2.6	Travaux pratiques	Menaces pour la sécurité du réseau	En option
11.2.4.5	Packet Tracer	Configuration de mots de passe sécurisés et de SSH	Recommandé
11.2.4.6	Travaux pratiques	Accès aux périphériques réseau avec SSH	En option
11.2.4.7	Travaux pratiques	Analyse de Telnet et de SSH dans Wireshark	En option
11.2.4.8	Travaux pratiques	Sécurisation des périphériques réseau	Recommandé
11.3.2.3	Packet Tracer	Test de la connectivité avec la commande Traceroute	Recommandé
11.3.2.4	Travaux pratiques	Test de la latence réseau avec les commandes ping et traceroute	Recommandé
11.3.3.2	Vidéo	Commande show version	-

Le mot de passe utilisé dans le cadre des exercices Packet Tracer de ce chapitre est : **PT_ccna5**

Chapitre 11 : exercices (suite)

Quels sont les exercices associés à ce chapitre ?

N° de page	Type d'exercice	Nom de l'exercice	Facultatif ?
11.3.3.3	Packet Tracer	Utilisation des commandes show	Recommandé
11.3.4.5	Exercice interactif	Commandes show	Recommandé
11.3.4.6	Travaux pratiques	Utilisation de l'interface de ligne de commande pour la collecte d'informations sur les périphériques réseau	En option
11.4.1.4	Exercice interactif	Classer les étapes de dépannage	Recommandé
11.4.3.5	Travaux pratiques	Résolution des problèmes liés aux câbles et aux interfaces	Recommandé
11.4.3.6	Packet Tracer	Résolution des problèmes de connectivité	Recommandé
11.5.1.1	Exercice en classe	Concevoir et mettre en œuvre le réseau d'une petite entreprise	En option
11.5.1.2	Packet Tracer	Intégration des compétences	Recommandé
11.5.1.3	Packet Tracer	Exercice de dépannage	Recommandé
Annexe	Packet Tracer	Configuration d'un routeur Linksys	Pour approfondir

Le mot de passe utilisé dans le cadre des exercices Packet Tracer de ce chapitre est : **PT_ccna5**

Chapitre 11 : évaluation

- Une fois qu'ils ont terminé le chapitre 11, les élèves doivent se soumettre à l'évaluation correspondante.
- Les questionnaires, les travaux pratiques, les exercices dans Packet Tracer, ainsi que les autres activités peuvent servir à évaluer, de manière informelle, les progrès des élèves.

Chapitre 11 : Les meilleures pratiques

- Avant d'enseigner le contenu du chapitre 11, le formateur doit :
- Réussir la partie « Évaluation » du chapitre 11.
- Assurez-vous que les élèves connaissent bien les modèles TCP/IP et OSI, et l'adressage IP. Ce chapitre explique comment ceux-ci sont implémentés sur un petit réseau.
- Section 11.1
  - Insistez sur la fonction des commutateurs et des routeurs et sur l'importance de la structure hiérarchique du réseau.
  - Expliquez les facteurs à prendre en compte lors de la sélection d'un commutateur et d'un routeur pour une entreprise. Parmi ces facteurs, on compte notamment le nombre d'utilisateurs/de réseaux nécessaires, le coût, la performance, l'évolutivité, la redondance et les fonctions requises. Travaillez avec le département IT de votre établissement ou une PME locale et demandez aux élèves de rechercher des mises à niveau pour le réseau.
  - Consultez le livre blanc Cisco sur les bonnes pratiques en matière de planification initiale :

    http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a008014fb3b.shtml

Chapitre 11 : bonnes pratiques (suite)

- Section 11.2
  - Présentez la sécurité du réseau et les cyberattaques récentes qui ont ciblé les entreprises et le gouvernement.
  - Utilisez le site http://map.norsecorp.com/ pour afficher une carte des attaques réseau.
  - Découvrez la procédure de récupération des mots de passe 1941 :

    http://www.cisco.com/c/en/us/support/docs/routers/3800-series-integrated-services-routers/112058-c1900-pwd-rec-00.html
  - Découvrez le commutateur Catalyst 2960 de récupération des mots de passe :

    http://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/products-password-recoveries-list.html
  - Pour en savoir plus sur la gestion des fichiers de configuration, visitez :

    http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/usb_flash_keys_ps6350_TSD_Products_Configuration_Guide_Chapter.html

Chapitre 11 : bonnes pratiques (suite)

- Section 11.3
  - Les élèves doivent très bien connaître les commandes de base d'hôte et IOS pour être capables de trouver des informations sur les appareils d'un réseau. Donnez-leur autant que possible la possibilité de s'entraîner.
  - Commandes d'hôte : ipconfig, ping, tracert
  - Commandes IOS : show running-config, show version, show interfaces, show ip interface brief, show cdp neighbors, traceroute, show ip route
- Section 11.4
  - Les élèves doivent se familiariser avec la procédure de dépannage.
  - Utilisez les commandes d'hôte et IOS pour résoudre facilement les problèmes.
- Section 11.5
  - Les exercices suivants sont fortement recommandés :
    - Packet Tracer : 11.5.1.2 : challenge d'intégration des compétences
    - Packet Tracer : 11.5.1.3 : challenge de dépannage

Chapitre 11 : bonnes pratiques (suite)

- Section 11.3
  - Les élèves doivent très bien connaître les commandes de base d'hôte et IOS pour être capables de trouver des informations sur les appareils d'un réseau. Donnez-leur autant que possible la possibilité de s'entraîner.
  - Commandes d'hôte : ipconfig, ping, tracert
  - Commandes IOS : show running-config, show version, show interfaces, show ip interface brief, show cdp neighbors, show flash, traceroute, show ip route
- Section 11.5
  - Les exercices suivants sont fortement recommandés :
    - Packet Tracer : 11.5.1.2 : challenge d'intégration des compétences
    - Packet Tracer : 11.5.1.3 : challenge de dépannage

Chapitre 11 : aide supplémentaire

- Pour obtenir davantage d'aide sur les stratégies d'enseignement, notamment les plans de cours, l'utilisation d'analogies pour expliquer des concepts difficiles et les sujets de discussion, consultez la communauté CCNA à l'adresse https://www.netacad.com/group/communities/community-home
- Les bonnes pratiques du monde entier relatives au programme CCNA Routing and Switching sont disponibles à l'adresse https://www.netacad.com/group/communities/ccna-blog
- Si vous souhaitez partager des plans de cours ou des ressources, téléchargez-les sur le site de la communauté CCNA afin d'aider les autres formateurs.

Chapitre 11 : Conception d'un réseau de petite taille

Introduction to Networks v6.0

Cisco | Networking Academy®
Mind Wide Open™

Chapitre 11 – Sections et objectifs

- 11.1 Conception du réseau
  - Identifier les équipements entrant dans la conception d'un petit réseau
  - Identifier les protocoles utilisés dans un petit réseau
  - Expliquer comment un petit réseau sert de base aux réseaux plus importants
- 11.2 Sécurité du réseau
  - Expliquer pourquoi des mesures de sécurité sont nécessaires pour les périphériques réseau
  - Identifier les failles de sécurité
  - Identifier les techniques employées pour atténuer les risques
  - Configurer les périphériques réseau à l'aide des fonctions de sécurisation renforcée pour limiter les menaces de sécurité
  - Appliquer les commandes pour sauvegarder et restaurer un fichier de configuration IOS

Chapitre 11 : Sections et objectifs (suite)

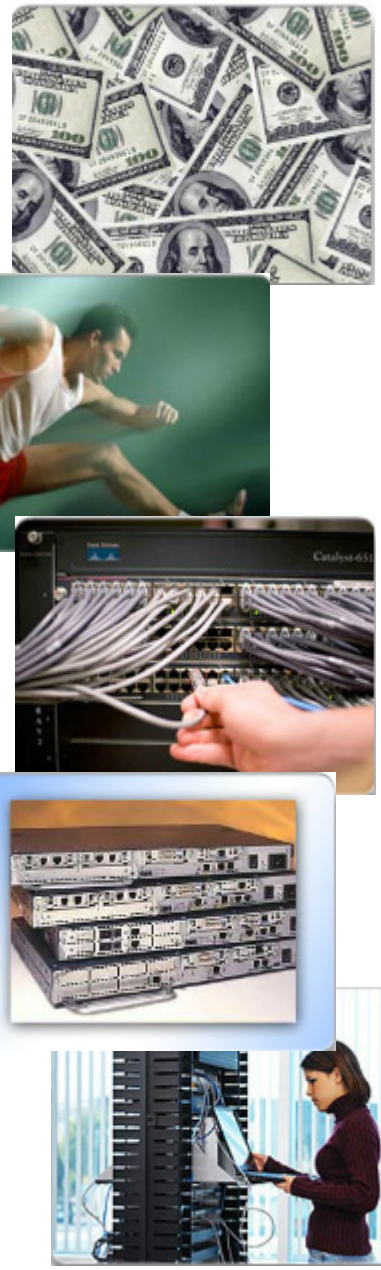
- 11.3 Les performances réseau de base
  - Utiliser les résultats de la commande ping pour déterminer les performances relatives du réseau
  - Utiliser les résultats de la commande tracert pour déterminer les performances relatives du réseau
  - Utiliser les commandes show pour vérifier la configuration et l'état des périphériques réseau
  - Utiliser les commandes d'hôtes et IOS pour obtenir des informations sur les périphériques réseau
- 11.4 Dépannage du réseau
  - Appliquer des méthodologies de dépannage pour résoudre des problèmes
  - Résoudre les problèmes liés aux interfaces et aux câbles
  - Résoudre les problèmes de connectivité du client liés au service DNS

11.1 Conception du réseau

Cisco | Networking Academy®
Mind Wide Open™

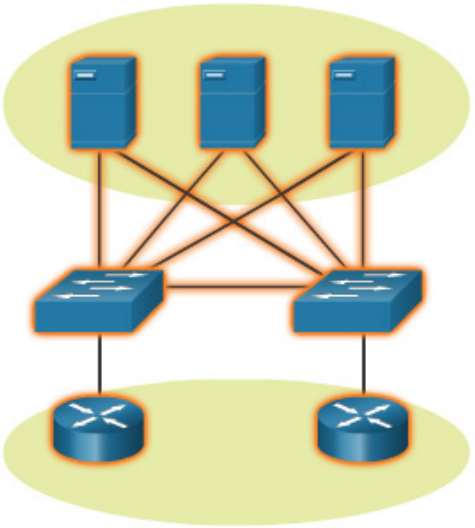
Les appareils d'un petit réseau

- Topologies de petits réseaux
  - Se composent d'un routeur, de quelques commutateurs et des PC des utilisateurs.
  - L'utilisateur accède à Internet par une liaison WAN unique, par câble ou par DSL.
  - La gestion est généralement assurée par une entreprise tierce.
- Choix des périphériques d'un réseau de petite taille
  - Sécurité, QoS, VoIP, commutation de niveau 3, NAT et DHCP.
- Adressage IP d'un réseau de petite taille
  - L'espace d'adressage est un composant crucial de la conception d'un réseau.
  - Tous les périphériques connectés au réseau nécessitent une adresse.
  - Le schéma d'adressage doit être planifié, documenté et géré.
  - La documentation de l'espace d'adressage peut être utile pour :
  - le dépannage et le contrôle ;
  - le contrôle de l'accès aux ressources (elle joue un rôle très important).

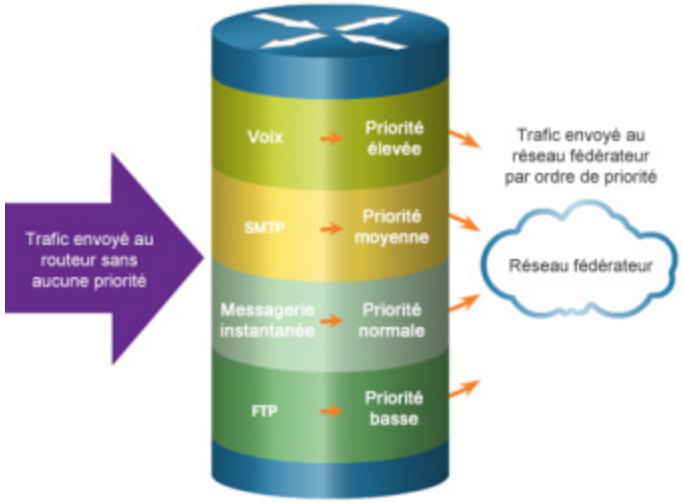


Les appareils d'un petit réseau (suite)

- Redondance dans un petit réseau
  - Un réseau doit être fiable de par sa conception.
  - Les pannes réseau sont habituellement très coûteuses.
  - La redondance améliore la fiabilité en éliminant les points de défaillance uniques.
  - La redondance du réseau peut être atteinte en multipliant l'équipement réseau et les liaisons.
  - Une liaison réseau jusqu'à Internet ou une batterie de serveurs en est un bon exemple.

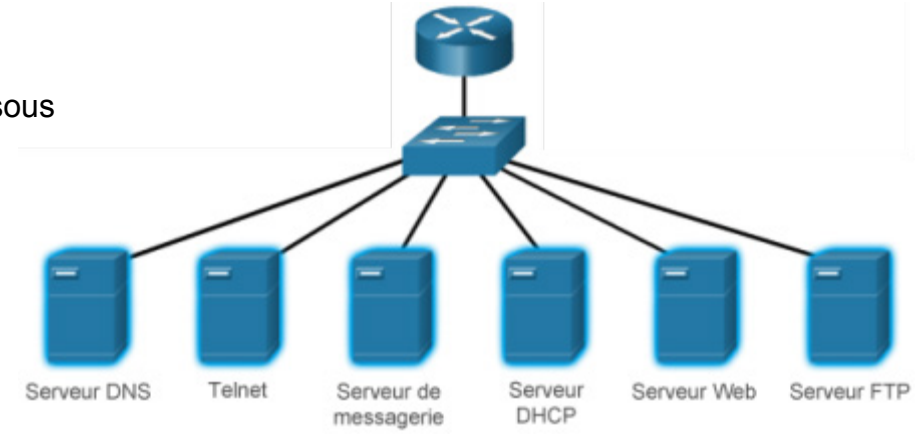


- Gestion du trafic
  - Le type et les modèles de trafic doivent également être pris en compte lors de la conception d'un réseau.
  - Pour être satisfaisante, la conception du réseau doit prévoir un classement du trafic par priorité.



Les applications et les protocoles des réseaux de petite taille

- Applications courantes
  - Applications réseau
    - Elles servent à communiquer sur le réseau.
    - Les clients de messagerie et les navigateurs web sont des exemples de ce type d'application.
  - Services de la couche application
    - Programmes qui communiquent avec le réseau et préparent les données pour qu'elles puissent être transférées.
    - Chaque service utilise des protocoles qui définissent les normes et les formats de données à utiliser.
- Protocoles courants
  - Les processus sur l'une des extrémités d'une session de communication
  - La manière dont les messages sont envoyés et la réponse attendue
  - Types et syntaxe des messages
  - La signification des champs informatifs
  - L'interaction avec la couche du niveau juste en dessous
- Applications vidéo et de communication vocale
  - Infrastructure
  - VoIP
  - Téléphonie IP
  - Applications en temps réel



Évolution vers de plus grands réseaux

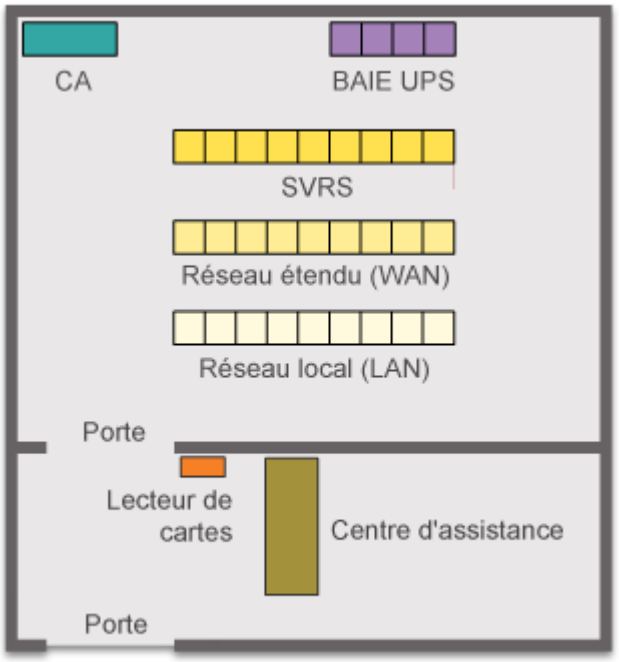
- Croissance d'un petit réseau
  - Pour faire évoluer un réseau, plusieurs éléments sont nécessaires :
    - Documentation du réseau
    - Inventaire des périphériques
    - Budget
    - Analyse du trafic
- Analyse de protocole
  - Identifiez les protocoles exécutés sur le réseau.
  - Les programmes d'analyse de protocoles sont des outils conçus pour vous aider dans cette tâche.
  - Capturez le trafic aux périodes d'utilisation intense et à différents endroits du réseau.
  - Les résultats de cette analyse permettent de gérer le trafic plus efficacement.
- Utilisation du réseau par les employés
  - Soyez conscient de l'évolution de l'utilisation du réseau.
  - Un administrateur réseau peut créer des « instantanés IT » sur l'utilisation des applications par les collaborateurs.

11.2 Sécurité du réseau

Cisco | Networking Academy®
Mind Wide Open™

Menaces pour la sécurité et vulnérabilités

- Types de menaces
  - Les intrusions électroniques peuvent coûter très cher.
  - Elles sont souvent le résultat de vulnérabilités logicielles, d'attaques du matériel ou d'usurpation d'informations d'identification.
  - Les menaces électroniques les plus courantes sont celles présentées dans l'illustration.
- Sécurité physique
  - Matériel
  - Environnement
  - Électricité
  - Maintenance
- Types de vulnérabilité
  - Trois vulnérabilités principales relatives à la technologie, à la configuration et à la politique de sécurité
  - Les terminaux peuvent être attaqués, comme les serveurs et les ordinateurs de bureau.
  - Ces trois types de vulnérabilité sont des failles de sécurité qu'exploitent les hackers.



Sécuriser les locaux informatiques

Attaques réseau

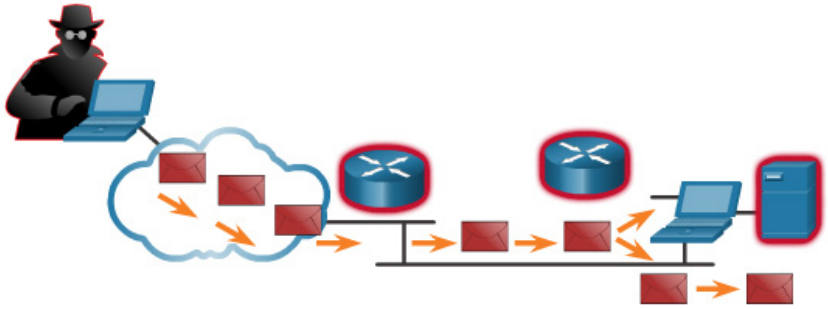
- Types de programme malveillant
  - Virus
  - Vers
  - Chevaux de Troie

- Attaques de reconnaissance
  - Détection et mappage de systèmes et de services.
  - Acquérir suffisamment d'informations sur le système ou le réseau cible pour identifier les vulnérabilités plus facilement.
  - Les outils les plus courants fonctionnent souvent avec des services Internet publics et gratuits, tels que DNS et Whois.
  - Les lecteurs de ports et les renifleurs de paquets sont également souvent utilisés à des fins de reconnaissance.

Attaques réseau (suite)

- Attaques par accès
  - Attaques de mot de passe
  - Exploitation de la confiance
  - Redirection de port
  - L'homme du milieu (Man in the Middle)

- Attaques par déni de service
  - Pourtant, bien qu'elles soient simples, les attaques DoS n'en sont pas moins dangereuses.
  - Elles empêchent les personnes autorisées d'utiliser un service en épuisant les ressources du système.
  - Empêchez les attaques DoS en appliquant les dernières mises à jour de sécurité.
  - Attaques DoS courantes :
    - Ping fatal
    - Attaque par inondation SYN
    - DDoS
    - Attaque Smurf



Réduction des attaques réseau

- Sauvegarde, mise à jour, mise à niveau et correctif
  - Restez informé des derniers développements.
  - Les entreprises doivent faire en sorte de toujours utiliser les versions les plus récentes des antivirus.
  - Les correctifs pour toutes les vulnérabilités connues doivent être appliqués.
  - Un serveur central de correctifs permet de gérer un grand nombre de serveurs et de systèmes.
  - Les correctifs doivent être installés sans intervention de l'utilisateur.
- Authentification, autorisation et gestion des comptes
  - Les services AAA offrent un contrôle de l'accès sur un périphérique réseau.
    - Authentification : l'accès à une ressource
    - Autorisation : ce que vous avez le droit de faire
    - Suivi : les actions exécutées lors de l'accès à la ressource
  - Le cadre AAS peut être très utile pour réduire les attaques réseau.

Réduction des attaques réseau (suite)

- Pare-feux
  - Un pare-feu contrôle le trafic et contribue à empêcher les tentatives d'accès non autorisé.
  - Diverses techniques permettent de déterminer s'il faut autoriser ou non l'accès au réseau :
    - Filtrage des paquets
    - Filtrage des applications
    - Filtrage URL
    - Inspection dynamique de paquets (SPI)
- Sécurité des terminaux
  - Les terminaux les plus courants sont les ordinateurs portables, les ordinateurs de bureau, les serveurs, les smartphones et les tablettes.
  - La sécurisation des terminaux ne se fait pas sans difficulté.
  - Les collaborateurs doivent être formés sur l'utilisation appropriée du réseau.
  - Les stratégies incluent souvent l'utilisation de logiciels antivirus et la prévention des intrusions sur les hôtes.
  - Des solutions plus complètes de sécurité des points de terminaison reposent sur le contrôle d'accès au réseau.

Sécurité des appareils

- Présentation de la sécurité des périphériques
  - Les paramètres par défaut sont dangereux, car ils sont connus.
  - Les routeurs Cisco sont dotés de la fonctionnalité Cisco AutoSecure.
  - De plus, les paramètres suivants sont appliqués pour la plupart des systèmes :
    - Modifier immédiatement les noms d'utilisateur et les mots de passe par défaut.
    - Limiter l'accès aux ressources système uniquement aux utilisateurs autorisés.
    - Désactiver les services inutiles.
    - Mettre à jour tous les logiciels et installer des correctifs de sécurité avant toute activité en production.
- Mots de passe
  - Utilisez des mots de passe forts. Un mot de passe fort comporte/est :
    - Au moins 8 caractères et de préférence plus de 10
    - Une combinaison de lettres majuscules et minuscules, de chiffres, de symboles et d'espaces
    - Exempt de répétition, de nom commun, d'une suite consécutive de lettres ou de chiffre, de nom d'utilisateur, d'ami ou de nom d'animal de compagnie et de toute autre information qui identifierait facilement l'utilisateur
    - Des mots sans orthographe particulière
    - Modifié souvent
  - Les routeurs Cisco prennent en charge l'utilisation d'une expression composée de plusieurs mots que l'on appelle « phrase secrète ».

Sécurité des appareils (suite)

- Principes de sécurité de base
  - Les mots de passe forts sont efficaces uniquement s'ils sont secrets.
  - La commande **service password-encryption** chiffre les mots de passe dans la configuration.
  - La commande **security passwords min-length** permet de garantir que tous les mots de passe configurés ont une taille minimale spécifiée.
  - Le blocage de plusieurs tentatives de connexion consécutives permet de réduire les attaques brute-force de mot de passe.
  - La commande **login block-for 120 attempts 3 within 60** bloque les tentatives de connexion pendant 120 secondes après trois échecs de connexion en l'espace de 60 secondes.
  - La commande **exec timeout** déconnecte automatiquement les utilisateurs inactifs sur une ligne.
- Activation de SSH
  - Ce protocole n'est pas sécurisé.
  - Il est fortement recommandé d'utiliser SSH pour le protocole RSH.
  - Pour configurer la prise en charge de SSH sur un périphérique Cisco, il faut suivre quatre étapes :

    Étape 1. S'assurer que le routeur a un nom d'hôte et un nom de domaine IP uniques.

    Étape 2. Générer les clés SSH.

    Étape 3. Créer un nom d'utilisateur local.

    Étape 4. Activer des sessions SSH entrantes VTY.
  - Le routeur est désormais accessible à distance uniquement au moyen de SSH.

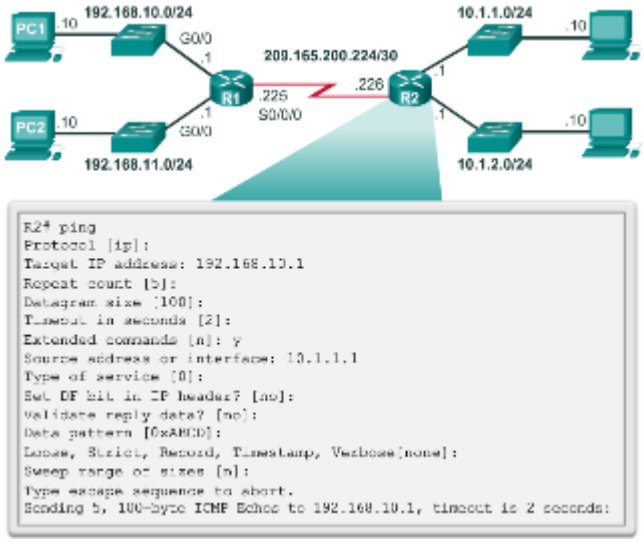
11.3 Les performances réseau de base

Cisco | Networking Academy®
Mind Wide Open™

La commande ping

- Interprétation des résultats de requête ping
  - La commande ping permet de tester efficacement la connectivité.
  - Utilisez le protocole ICMP (Internet Control Message Protocol) pour vérifier la connectivité de la couche 3.
  - Identifiez la source du problème.
  - Que révèlent ces indicateurs courants ping ?

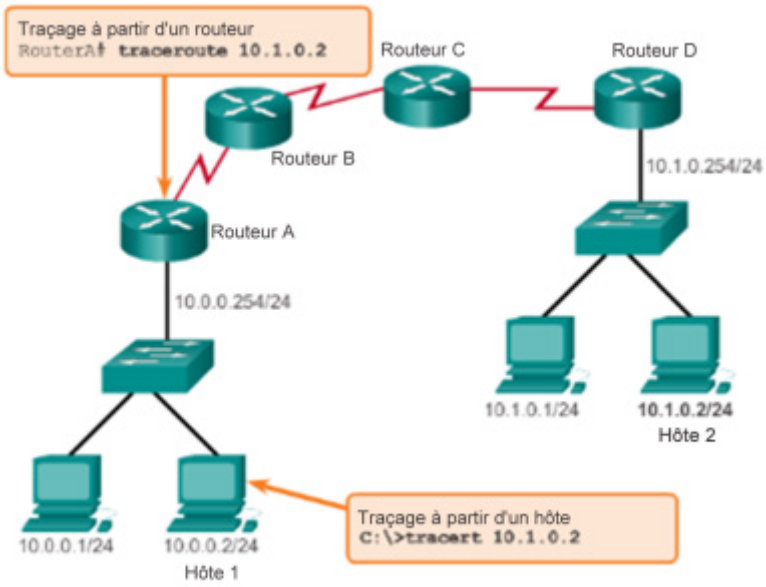
    ! . U
  - Extensions de la commande ping
    - Donne accès à davantage d'options.
- Ligne de base du réseau
  - Basées sur une durée définie.
  - Résultats enregistrés des commandes, telles que ping ou trace, avec des messages d'erreur et les délais de réponse.
  - Horodatées pour des études comparatives ultérieures.
  - Un délai de réponse plus long peut être signe d'un problème de latence.



Les commandes traceroute et tracert

- Interprétation des messages trace
  - Cette commande renvoie une liste des sauts effectués par un paquet acheminé à travers un réseau.
  - Utilisez la commande tracert pour les systèmes Windows.
  - Utilisez la commande Traceroute pour les systèmes Cisco IOS et UNIX.
- Commande extended traceroute
  - Permet d'ajuster les paramètres.
  - La commande se termine lorsque :
    - La destination répond avec une réponse d'écho ICMP.
    - L'utilisateur interrompt le suivi avec la séquence d'échappement.

```
C:\> tracert 10.1.0.2
Tracing route to 10.1.0.2 over a maximum of 30 hops
1  2 ms  2 ms  2 ms  10.0.0.254
2  *  *  *  Request timed out.
3  *  *  *  Request timed out.
4  ^C
C:\>
```



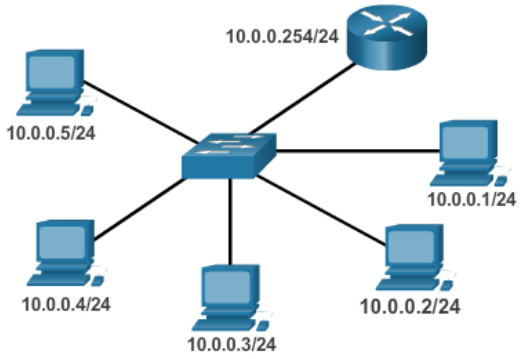
Les commandes show

- Les commandes show de la CLI Cisco IOS sont de puissants outils de dépannage.
- Les commandes show servent à afficher les fichiers de configuration, à vérifier l'état des interfaces et des processus des appareils, et à consulter l'état de fonctionnement de l'appareil.
- Vous pouvez afficher l'état de pratiquement tous les processus ou fonctions du routeur à l'aide d'une commande show.
- Les commandes show les plus couramment utilisées sont :
  - show running-config
  - show interfaces
  - show arp
  - show ip route
  - show protocols
  - show version

```
R1# show running-config
<Output omitted>
Building configuration...
Current configuration : 1063 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
enable secret 5 $1$i6w9$dvdpVM6zV10E6tSyLdkR5/
no ip domain lookup
!
interface FastEthernet0/0
 description LAN 192.168.1.0 default gateway
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
```

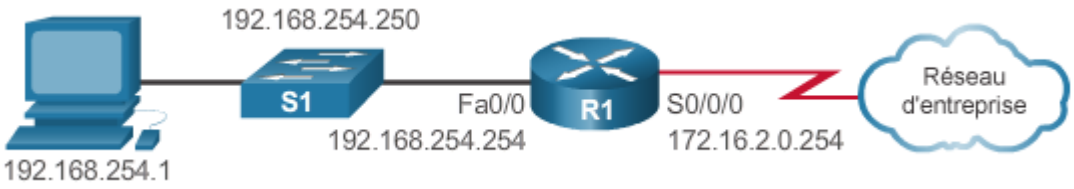
Les commandes d'hôte et IOS

- Commande ipconfig
  - Permet d'afficher des informations sur l'adresse IP et la passerelle par défaut sur un ordinateur Windows.
  - Qu'affichent ces commandes ?
    - ipconfig /all
    - ipconfig /displaydns
- Commande arp
  - La commande arp –a répertorie tous les appareils actuellement présents dans le cache ARP de l'hôte.
  - Le cache peut être vidé à l'aide de la commande arp -d.



Les commandes d'hôte et IOS (suite)

- Commande show cdp neighbors
  - CDP est un protocole propriétaire de Cisco qui s'exécute au niveau de la couche liaison de données.
  - Deux périphériques réseau Cisco ou plus peuvent échanger des informations sur l'un et l'autre même si la connectivité de la couche 3 n'existe pas.
  - Le protocole CDP peut présenter un risque pour la sécurité.
  - Pour désactiver le protocole CDP globalement, utilisez la commande de configuration globale no cdp run.
  - Pour désactiver le protocole CDP sur une interface, utilisez la commande d'interface no cdp enable.
  - Quelles informations la commande cdp neighbors details fournit-elle ?
- Commande show ip interface brief
  - Affiche un résumé des informations clés pour toutes les interfaces réseau d'un routeur.
  - Permet de vérifier l'état des interfaces du commutateur.



Débogage

- Commande debug
  - Permet à l'administrateur d'afficher les messages générés par les processus suivants en temps réel à des fins d'analyse :
    - Processus IOS
    - Protocoles
    - Mécanismes
    - Événements

```
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.0.0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
*Nov 13 12:56:08.147: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
*Nov 13 12:56:08.151: ICMP: echo reply rcvd, src 10.0.0.10, dst 10.0.0.1,
topology BASE, dscp 0 topoid 0
R1# undebug all
All possible debugging has been turned off
R1#
```

  - La commande **undebug all** désactive toutes les commandes de débogage
  - Quelles sont les commandes de débogage disponibles ?
  - Que pouvez-vous faire pour limiter le nombre de messages affichés ?
- Commande terminal monitor
  - Affiche les messages du journal dans le cas d'une connexion à distance, comme SSH
  - Pour arrêter d'afficher le message du journal : **terminal no monitor**

11.4 Dépannage du réseau

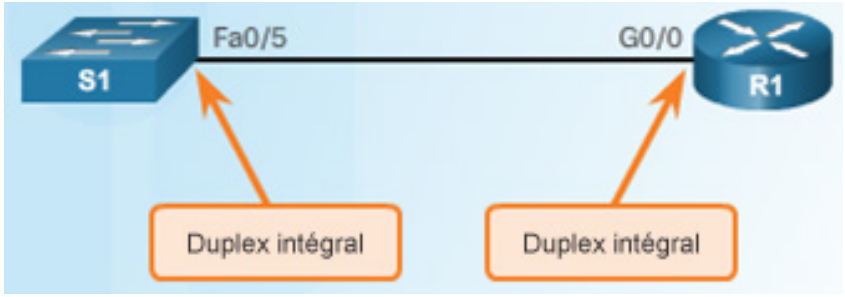
Cisco | Networking Academy®
Mind Wide Open™

Méthodes de dépannage

- Méthodes de dépannage de base
  - Identifier le problème
  - Élaborer une théorie des causes probables
  - Tester la théorie pour déterminer la cause
  - Établir un plan d'action pour résoudre le problème et implémenter la solution
  - Vérifier l'intégralité des fonctionnalités du système et implémenter des mesures préventives
  - Documenter les résultats des recherches et des actions entreprises
- Résoudre ou transférer ?
- Vérification et surveillance de la solution
  - Quelles commandes IOS pouvez-vous utiliser pour vérifier et surveiller la solution ?

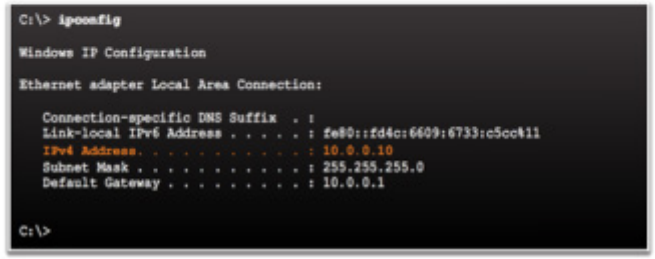
Résolution des problèmes liés aux câbles et aux interfaces

- Fonctionnement en duplex
  - Désigne la direction de la transmission des données entre deux appareils.
  - Pour des performances optimales, deux interfaces réseau Ethernet connectées doivent utiliser le même mode duplex.
- Conflit des paramètres duplex
  - Les messages du journal peuvent signaler un problème de correspondance du mode duplex.
  - Quelles commandes IOS pouvez-vous utiliser pour identifier un problème de correspondance du mode duplex ?



Scénarios de dépannage

- Problèmes d'adressage IP sur périphériques IOS
  - Erreurs d'affectation manuelle
  - Erreurs liées à DHCP
  - Quelle commande show ?



- Problèmes d'adressage IP sur des périphériques finaux
  - 169.254.0.0/16 sur un système Windows
  - ipconfig pour vérifier les adresses IP attribuées à un système Windows
- Problèmes de passerelle par défaut
  - Impossible de communiquer en dehors du réseau
  - **ipconfig** pour vérifier la passerelle par défaut attribuée à un système Windows
- Résolution des problèmes DNS
  - **ipconfig /all** pour déterminer le serveur DNS utilisé
  - **nslookup** pour lancer manuellement des requêtes DNS et analyser la réponse DNS

11.5 Synthèse du chapitre

Cisco | Networking Academy®
Mind Wide Open™

Synthèse du chapitre

Synthèse

- Expliquer comment un petit réseau peut être redimensionné en un réseau de plus grande taille
- Configurer les commutateurs et les routeurs avec des fonctionnalités de sécurisation renforcée pour améliorer la sécurité
- Déterminer un profil de référence des performances du réseau à l'aide de commandes et d'utilitaires show courants
- Appliquer des méthodes de dépannage et des commandes d'hôte et IOS pour résoudre des problèmes
- Expliquer comment créer, configurer et vérifier un petit réseau de segments connectés directement

Section 11.2

Nouveaux termes/commandes

- Filtrage des applications
- Authentification, autorisation et comptabilité (AAA)
- **auto secure** (commande)
- **exec timeout** (commande)
- **crypto key generate rsa general-keys modulus taille du module** (commande)
- Sécurité des terminaux
- **ip domain-name** *domain-name* (commande)
- **login block-for 120 attempts 3 within 60** (commande)
- Filtrage des paquets
- Phrase secrète
- Pare-feu personnels
- **security passwords min-length** (commande)
- Inspection dynamique de paquets
- **service password-encryption** (commande)
- **transport input ssh**
- Filtrage des URL

Section 11.3

Nouveaux termes/commandes

- ! . U
- Protocole ARP (Address Resolution Protocol)
- **exec timeout** (commande)
- **crypto key generate rsa general-keys modulus** *modulus-size* (commande)
- **ip domain-name** *domain-name* (commande)
- **ipconfig** (commande d'hôte)
- **login block-for 120 attempts 3 within 60** (commande)
- Adresse de bouclage 127.0.0.1
- **ping** (commande)
- **security passwords min-length** (commande)
- **service password-encryption** (commande)
- **show cdp neighbors** (commande IOS)
- **show ip interface brief** (commande IOS)
- **tracert** (commande d'hôte)
- **traceroute** (commande IOS)
- **transport input ssh**