

# Chapitre 11 : Conception d'un réseau de petite taille

Présentation des réseaux v5.1

Lawrence BENEDICT

Janvier 2017



# Plan du chapitre

11.0 Introduction

11.1 Conception du réseau

11.2 Sécurité du réseau

11.3 Les performances réseau  
de base

11.4 Résumé

# Section 11.1 : Conception du réseau

À la fin de cette section, vous saurez :

- 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

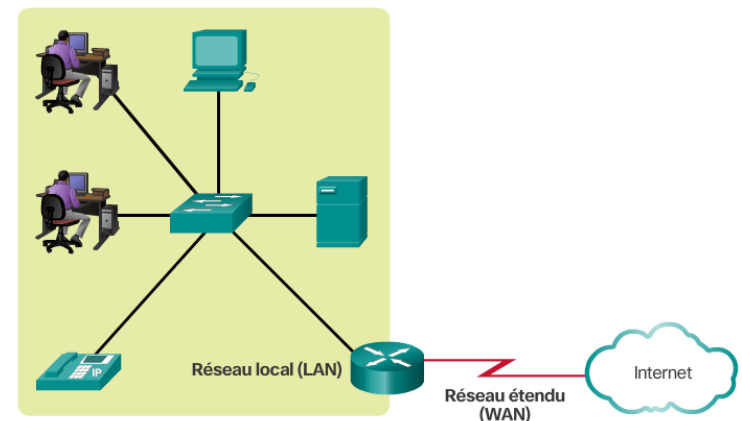
## Rubrique 11.1.1 : Périphériques d'un petit réseau



# Topologies de petits réseaux

## Réseau typique d'une petite entreprise

- La conception d'un petit réseau est simple.
- Seuls quelques périphériques réseau sont nécessaires.
- Un petit réseau est généralement composé d'un routeur, de deux commutateurs et de PC utilisateur.
- Une connexion Internet est établie grâce à une seule liaison WAN (habituellement par câble ou via DSL).
- La plupart des tâches de gestion sont liées à la maintenance et au dépannage des équipements existants.
- La gestion d'un petit réseau peut être réalisée par un employé ou par un prestataire externe.



# Choix des périphériques d'un réseau de petite taille

Pour choisir un équipement, les facteurs à considérer, outre ceux présentés dans les illustrations, sont liés aux fonctionnalités du système d'exploitation :

- Sécurité
- QoS
- VoIP
- Commutation C3
- NAT
- DHCP



Coût



Ports



Vitesse



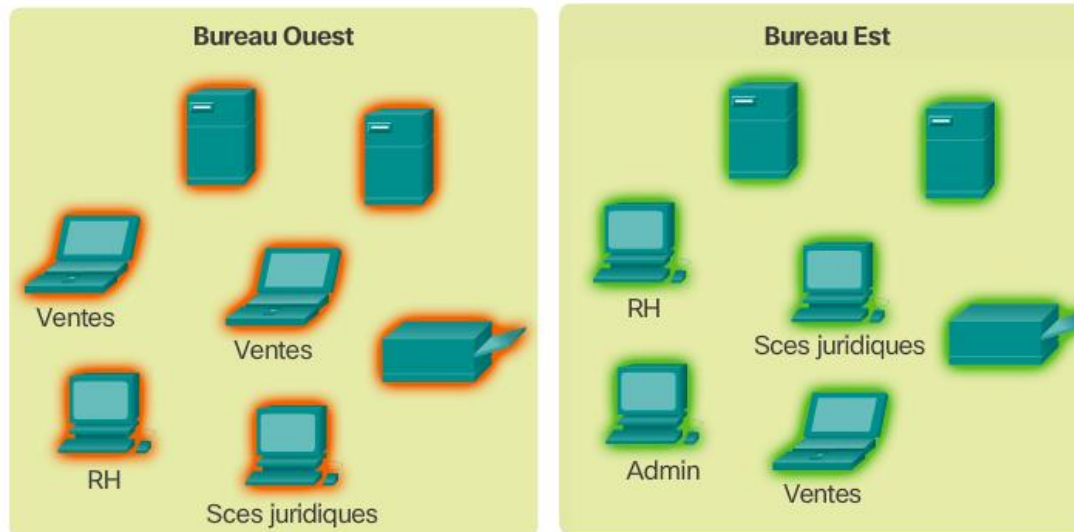
Extensibilité/modularité



Gestion facile

# Adressage IP d'un réseau de petite taille

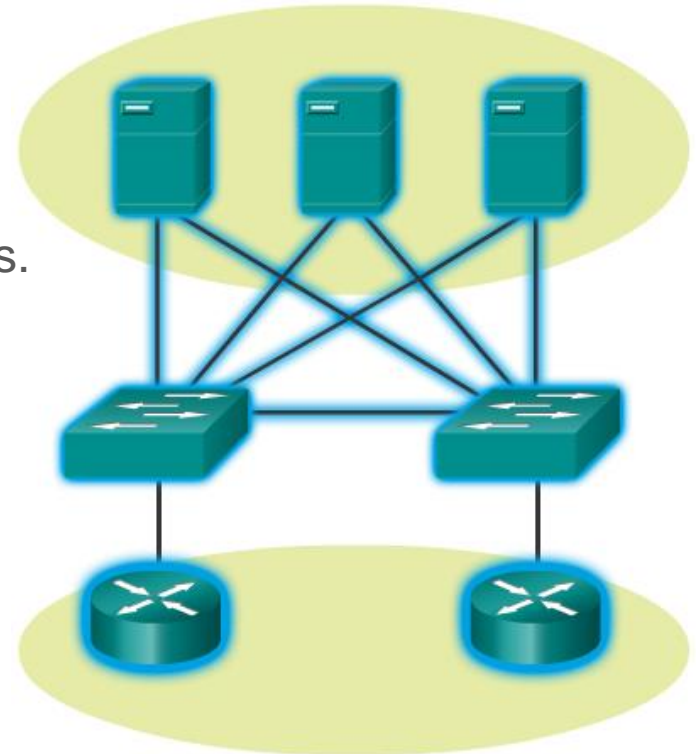
- L'espace d'adressage est un composant crucial de la conception d'un réseau.
- Tous les périphériques connectés au réseau nécessitent une adresse.
- Le schéma d'adressage doit être planifié, documenté et géré.
- La documentation de l'espace d'adressage peut être utile au dépannage.
- Elle est également très importante lors du contrôle de l'accès aux ressources.



# Redondance dans un petit réseau

## Redondance dans une batterie de serveurs

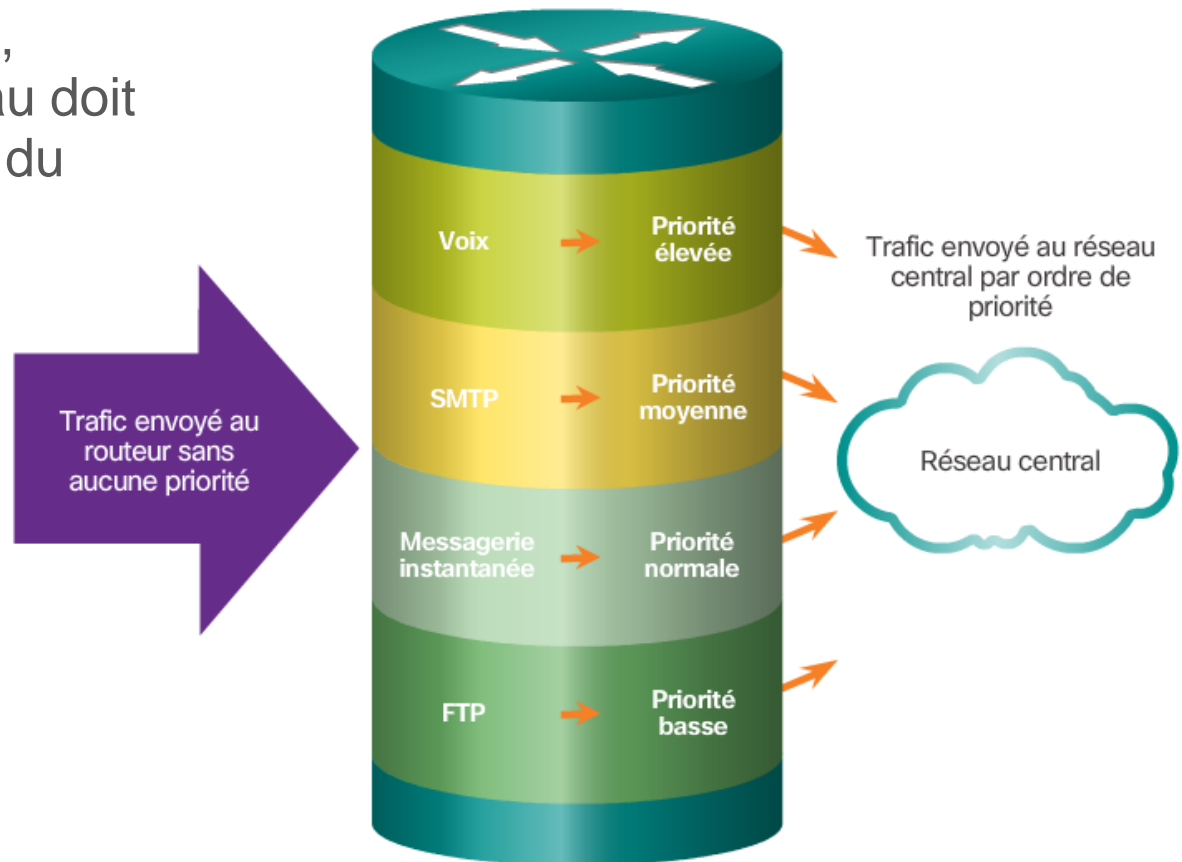
- Un réseau doit être fiable de par sa conception.
- Les pannes réseau sont habituellement très coûteuses.
- La redondance améliore la fiabilité en éliminant les points de défaillance uniques.
- La redondance du réseau peut être atteinte en multipliant l'équipement réseau et les liaisons.
- Une liaison 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.



## Rubrique 11.1.2 :

# Applications et 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.

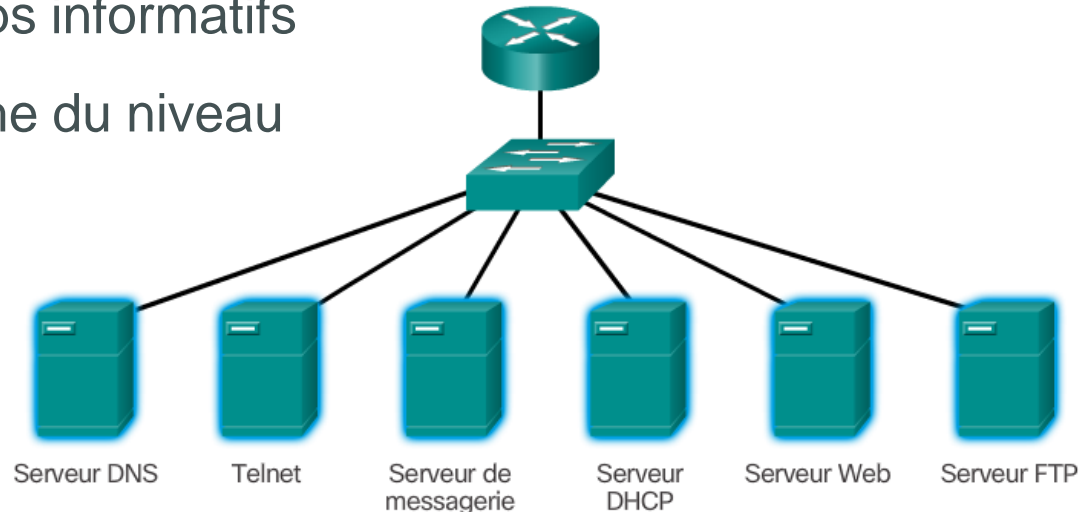
## Services de la couche application

- 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

Chacun des protocoles réseau suivants définit :

- Les processus sur l'une des extrémités d'une session de communication
- La manière dont les messages sont envoyés et la réponse attendue
- Les types de message
- La syntaxe des messages
- La signification des champs informatifs
- L'interaction avec la couche du niveau juste en dessous



# Applications en temps réel

Composants de base :

- Infrastructure
- VoIP
- Téléphonie IP
- Applications en



## Rubrique 11.1.3 : Évolution vers de plus grands réseaux



# Croissance d'un petit réseau

Pour faire évoluer un réseau, plusieurs éléments sont nécessaires :

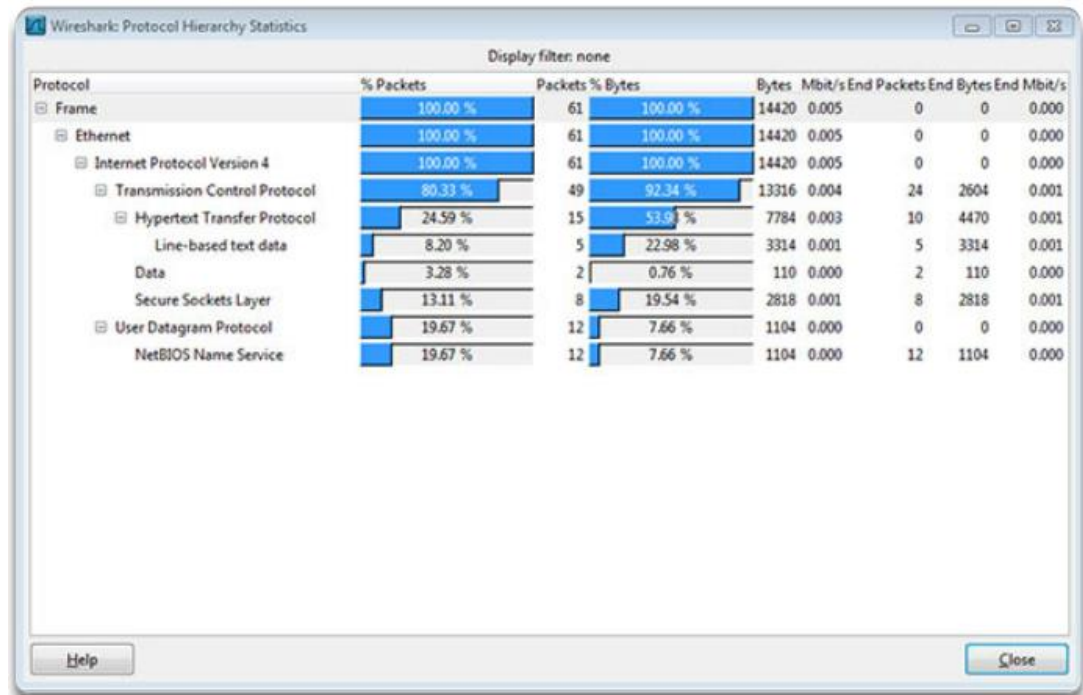
- Documentation du réseau
- Inventaire des périphériques
- Budget
- Analyse du trafic





# Analyse de protocole

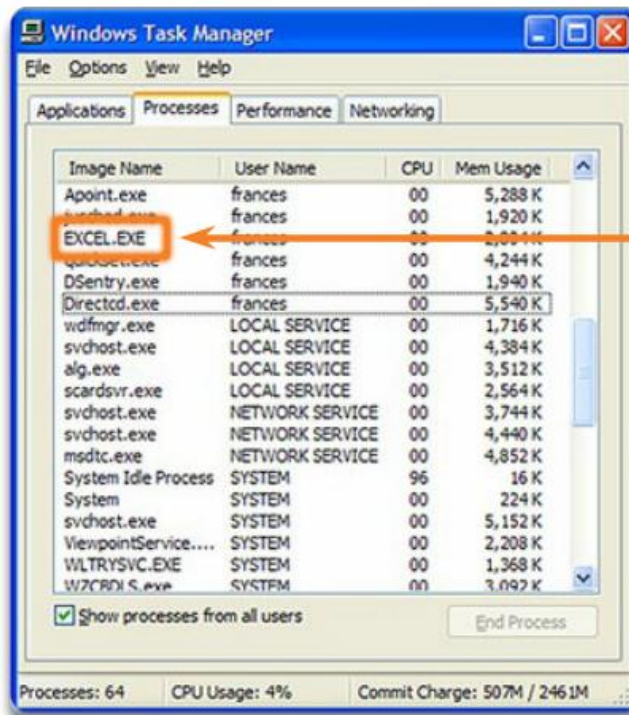
- Un administrateur réseau doit comprendre les protocoles en vigueur sur le réseau. Les programmes d'analyse de protocoles sont des outils conçus pour vous aider dans cette tâche.
- Pour affiner l'analyse des protocoles, il est important de capturer le trafic aux périodes d'utilisation intense et à différents endroits du réseau.
- Le bilan de cette analyse permet de gérer le trafic plus efficacement.





# Utilisation du réseau par les employés

- Il est également important de savoir en quoi l'utilisation du réseau évolue.
- Un administrateur réseau peut créer des « instantanés » sur l'utilisation des applications par les employés.



Les processus sont des programmes logiciels qui s'exécutent simultanément.

**Les processus peuvent être :**

1

Des applications

2

Des services

3

Des opérations système

4

Un programme qui peut s'exécuter plusieurs fois, chaque occurrence dans son propre processus.

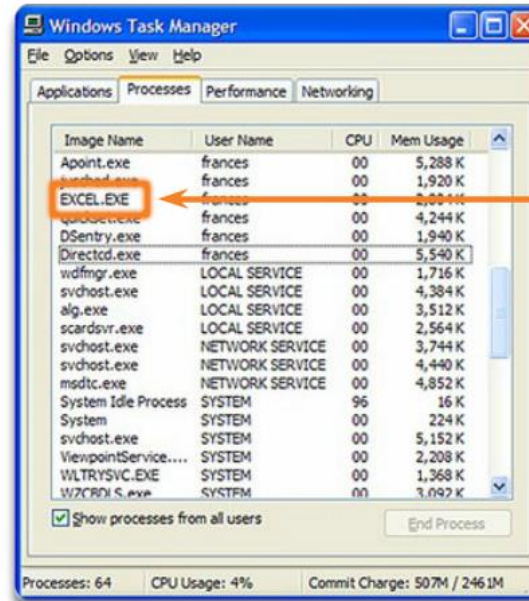
# Utilisation du réseau par les employés (suite)

- Ces instantanées comportent généralement les informations suivantes :

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

- Les instantanés documentés des employés contribuent à informer sur l'évolution des besoins en matière de protocoles.

- Si l'utilisation des ressources change, il peut être nécessaire de modifier l'allocation des ressources réseau en conséquence.



Les processus sont des programmes logiciels qui s'exécutent simultanément.

Les processus peuvent être :

1 Des applications

2 Des services

3 Des opérations système

4 Un programme qui peut s'exécuter plusieurs fois, chaque occurrence dans son propre processus.

# Section 11.2 :

## Sécurité du réseau

À la fin de cette section, vous saurez :

- 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

## Rubrique 11.2.1 : Menaces et failles de sécurité



# Types de menaces

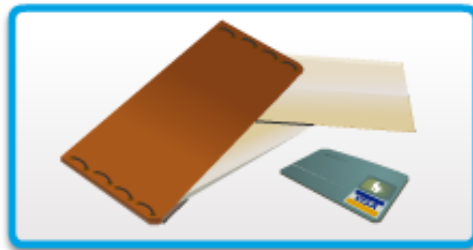
- Les intrusions électroniques peuvent coûter très cher.
- Elles sont souvent le résultat de vulnérabilités logicielles, d'attaques du matériel ou d'usurpation d'informations d'identification.
- Les menaces électroniques les plus courantes sont celles présentées dans l'illustration.



Vol d'informations



Perte et manipulation de données



Usurpation d'identité

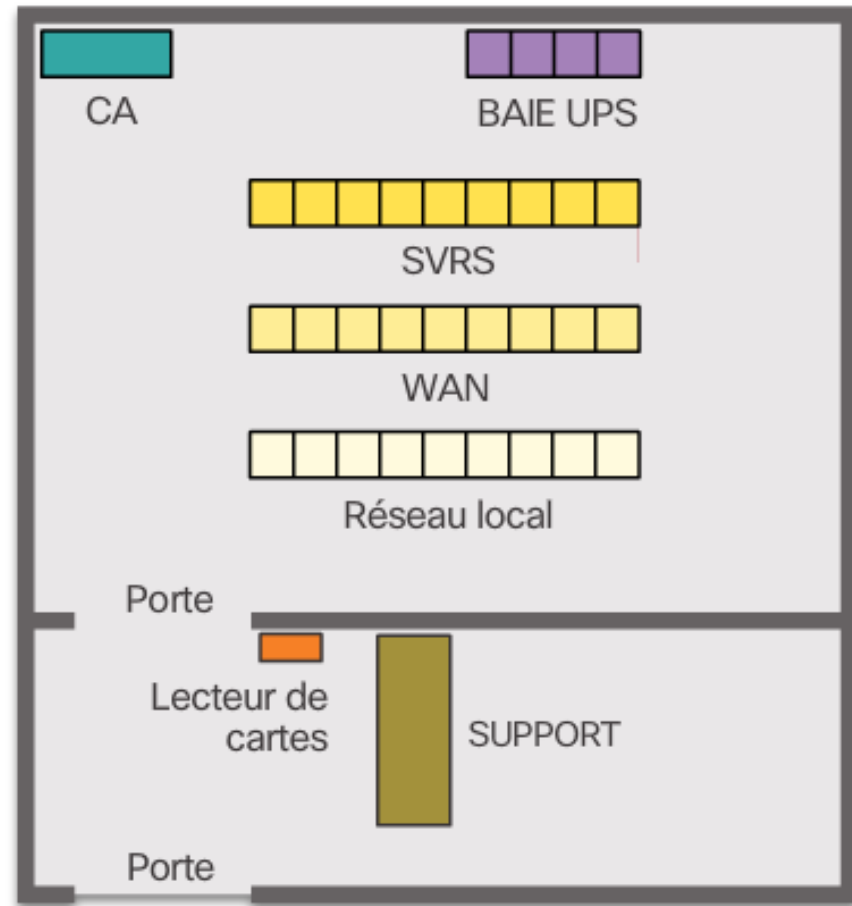


Interruption de service

# Sécurité physique

Catégories de menaces physiques :

- Matériel
- Environnement
- Électricité
- Maintenance



Sécuriser les locaux informatiques

# Types de vulnérabilité

- Les vulnérabilités existent à différents niveaux, dont trois principaux :
  - Technologies. Vulnérabilités qui concernent les protocoles, les systèmes d'exploitation et l'équipement réseau
  - Configuration. Vulnérabilités nées de la mauvaise configuration des périphériques, des valeurs par défaut, et de mots de passe faciles à deviner
  - Stratégie de sécurité. Absence de stratégie de sécurité, inadéquation entre l'installation des logiciels et du matériel et la stratégie de sécurité, et absence de plan de reprise d'urgence
- En général, les périphériques réseau attaqués sont des terminaux, par exemple des serveurs et des ordinateurs de bureau.
- Ces trois types de vulnérabilité sont des failles de sécurité qu'exploitent les hackers.

## Rubrique 11.2.2 : Attaques de réseau





# Types de programme malveillant

- Virus
- Vers
- Chevaux de Troie



# Attaques de reconnaissance

- Détection et mappage de systèmes et de services
- Souvent non considérée comme une attaque à part entière
- L'objectif de ce type d'attaque est d'acquérir suffisamment d'informations sur le système ou le réseau cible pour identifier les failles plus facilement.
- Les outils les plus courants fonctionnent souvent avec des services Internet publics, tels que DNS et Whois.
- Les lecteurs de ports et les renifleurs de paquets sont également utilisés dans la reconnaissance.



Requêtes Internet



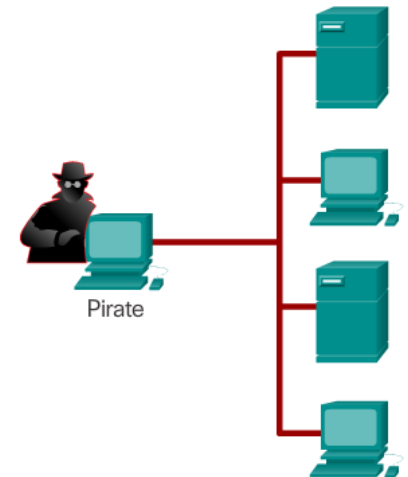
Balayages ping



Balayages de ports



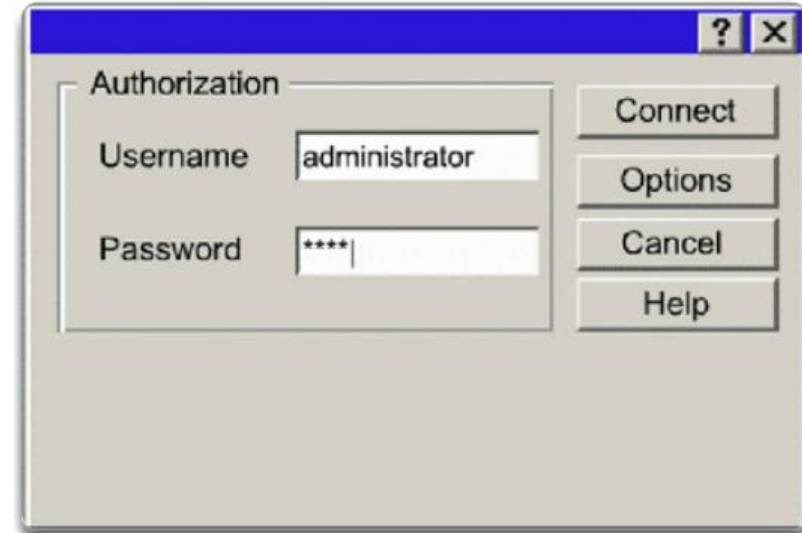
Analyseurs de paquets



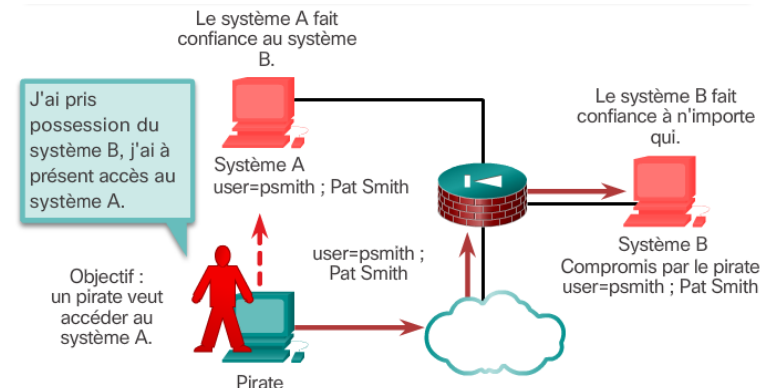
# Attaques par accès

- Attaques contre des vulnérabilités connues et des services.
- L'objectif de ce type d'attaque est d'obtenir l'accès à des informations que l'usurpateur n'a pas le droit de voir.
- Il existe quatre types d'attaques par accès :
  - Attaques de mot de passe
  - Exploitation de la confiance
  - Redirection de port
  - L'homme du milieu (Man in the Middle)

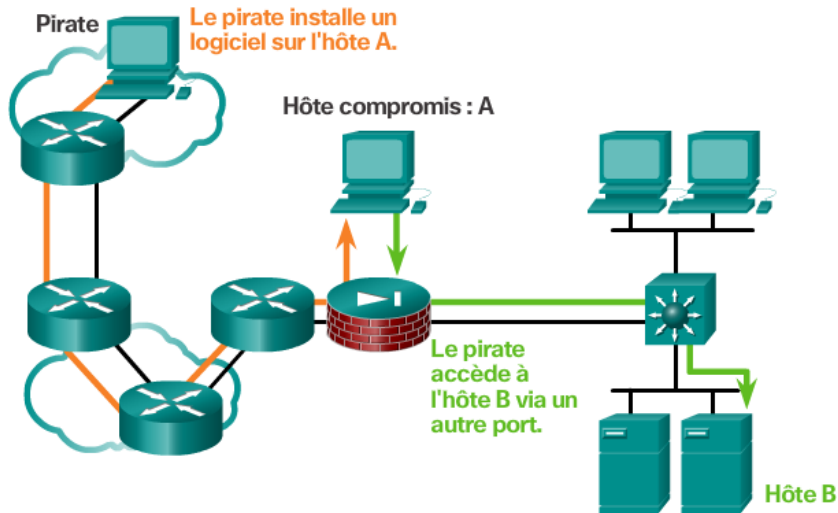
## Attaque de mot de passe



## Exploitation de la confiance

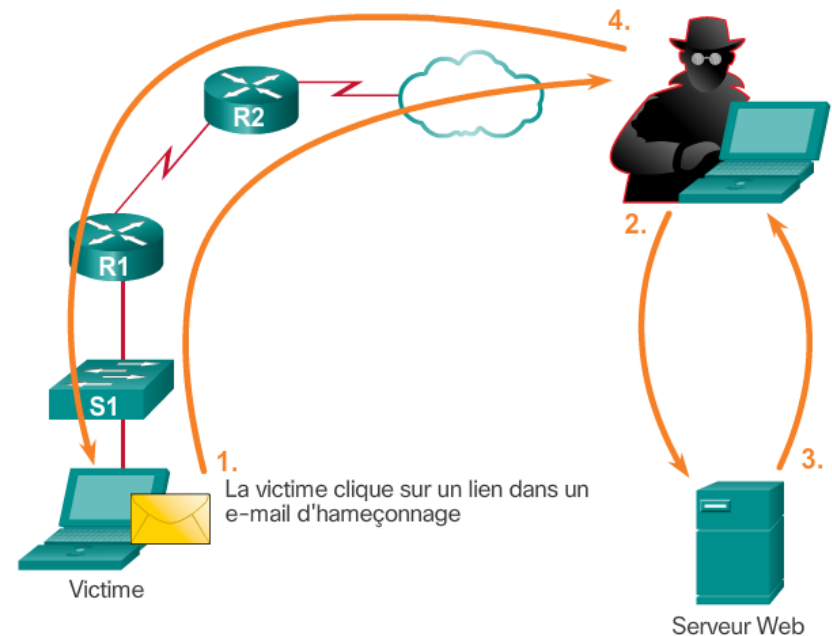


# Attaques par accès (suite)



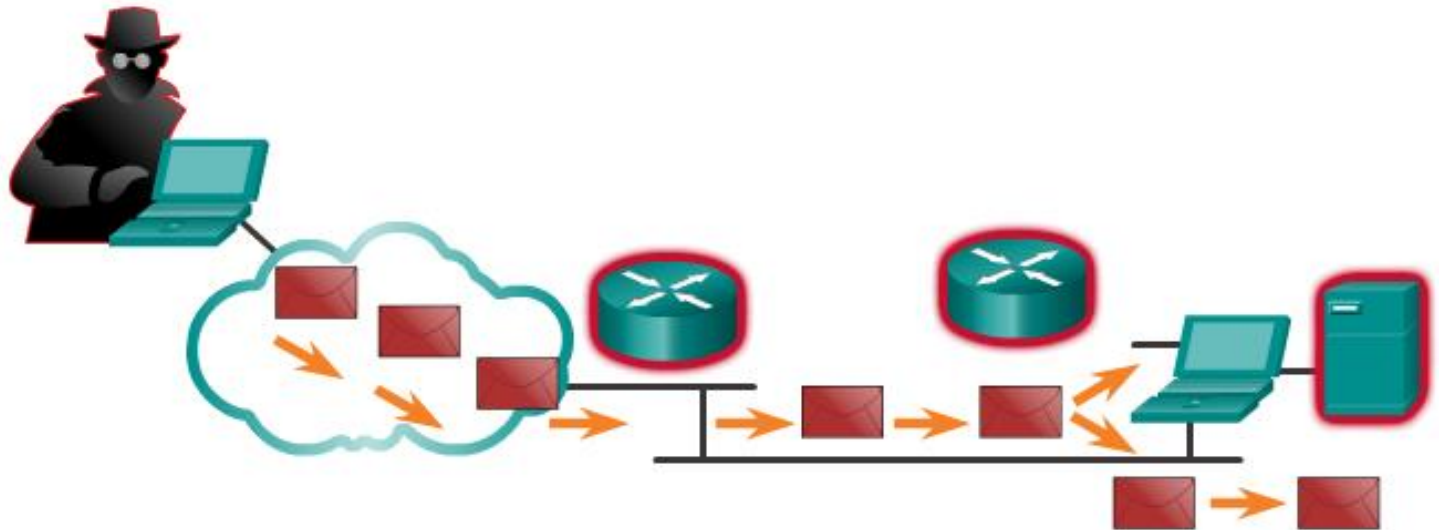
## Redirection de port

## L'homme du milieu (Man in the Middle)



# Attaques par déni de service

- Les attaques par déni de service ou DoS sont difficiles à contrer.
- Banales, elles sont faciles à exécuter.
- Pourtant, bien qu'elles soient simples, les attaques DoS n'en sont pas moins dangereuses.
- Elles empêchent l'utilisation d'un service par les personnes autorisées en épuisant les ressources du système.
- Pour empêcher des attaques DoS, il est impératif d'installer les dernières mises à jour de sécurité.

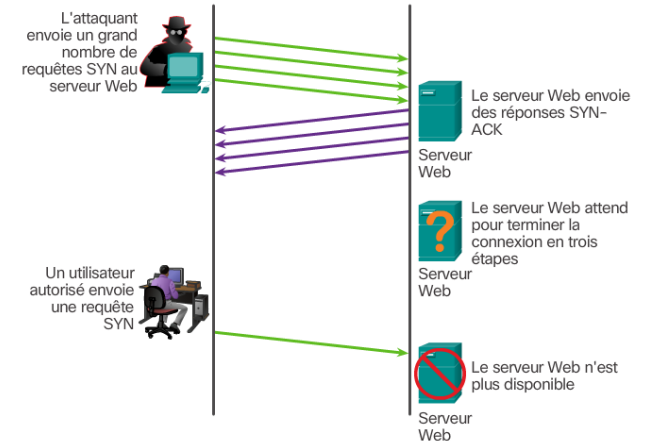


# Attaques par déni de service (suite)

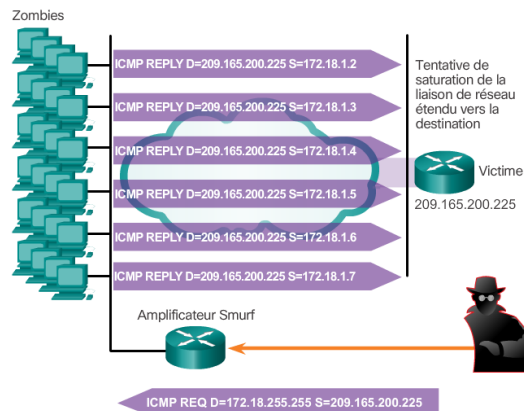
## Attaques DoS courantes :

- Ping fatal
- Attaque par inondation SYN
- DDoS
- Attaque Smurf

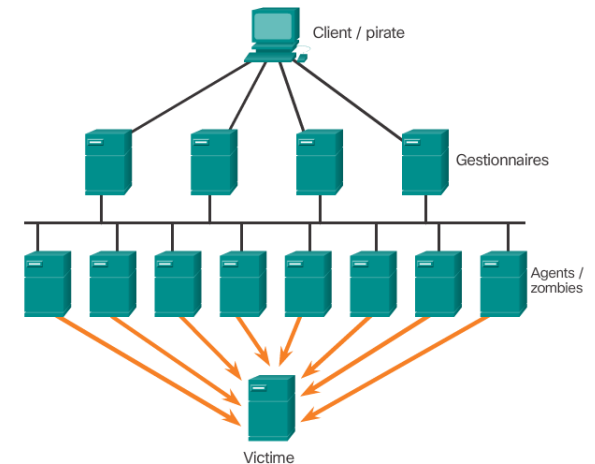
## Attaque



## Attaque Smurf



## DDoS

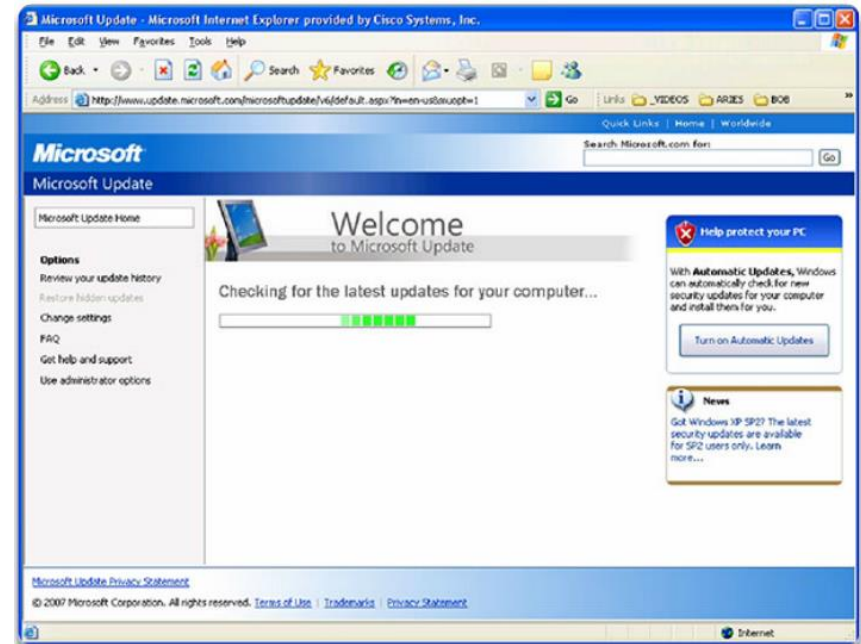


## Rubrique 11.2.3 : Réduction du risque d'attaques du réseau



# Sauvegarde, mise à jour, mise à niveau et correctif

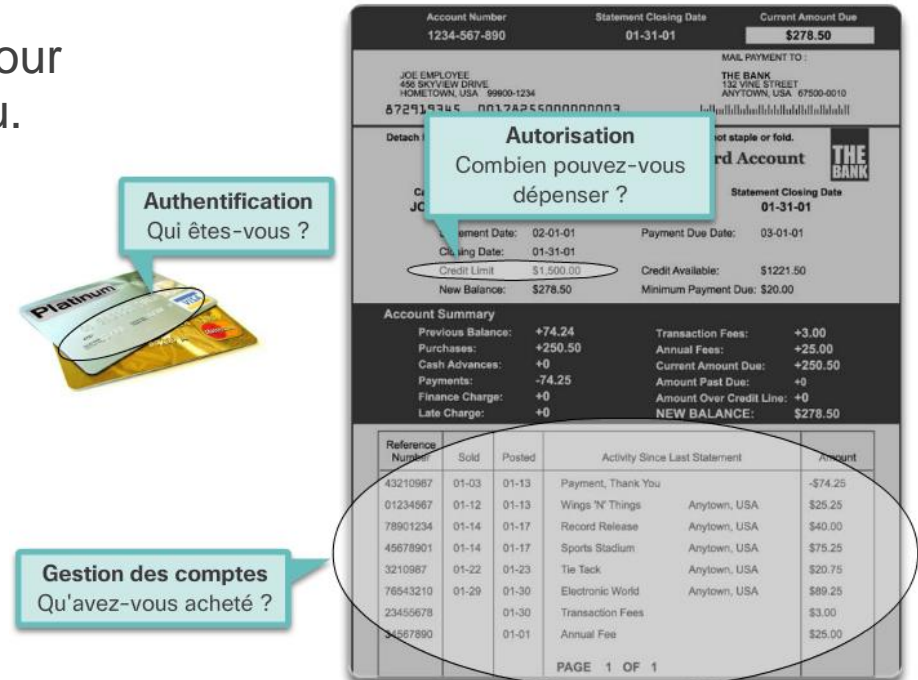
- Pour se protéger efficacement des attaques réseau, il faut s'informer en continu sur les menaces.
- À mesure que de nouveaux programmes malveillants apparaissent, les entreprises doivent mettre à jour leur logiciel antivirus afin de disposer de la version la plus récente.
- Afin de réduire les risques d'attaques par des vers, il faut appliquer des correctifs pour toutes les vulnérabilités connues.
- Un serveur central de correctifs peut être un bon moyen de gérer un grand nombre de serveurs et de systèmes.
- Tout correctif qui n'est pas encore appliqué à un hôte est alors automatiquement téléchargé depuis le serveur et installé sans intervention de l'utilisateur.





# Authentication, Authorization et Accounting

- Les services AAA offrent un contrôle de l'accès sur un périphérique réseau.
- Ces services permettent de contrôler les utilisateurs autorisés à accéder à une ressource (authentification), ce que ces derniers peuvent faire lorsqu'ils sont connectés (autorisation) et les actions qu'ils exécutent lors de l'accès au réseau (gestion des comptes).
- La structure AAA peut être très utile pour atténuer les risques d'attaques réseau.



# 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)



Appareils de sécurité Cisco



Pare-feu basé sur serveur



Routeur sans fil Linksys avec pare-feu intégré



Pare-feu personnel

# 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 sécurisation des terminaux reposent sur le contrôle de l'accès au réseau.

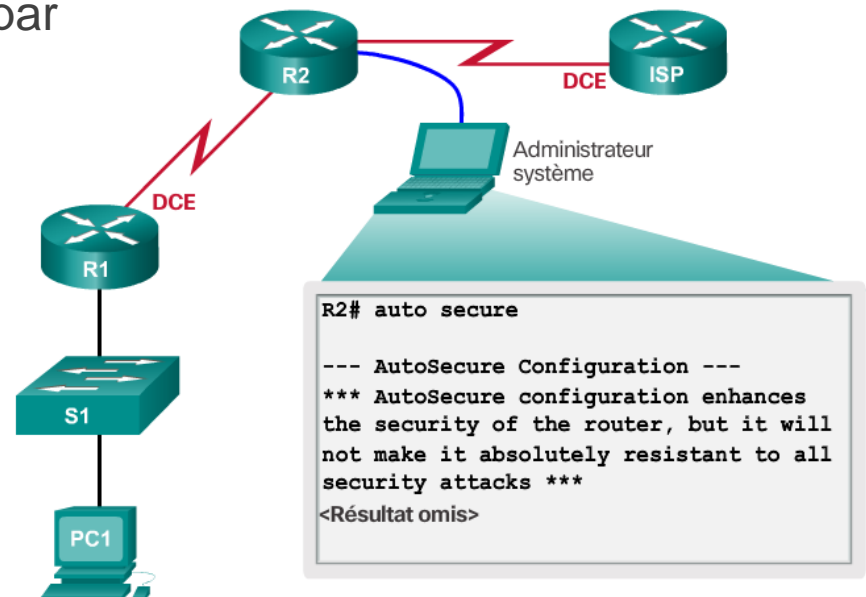


## Rubrique 11.2.4 : Sécurité des périphériques



# 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
  - Autoriser l'accès aux ressources système uniquement pour les particuliers 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 nombreux mots que l'on appelle « phrase de passe ».

Mot de passe faible	Raison de sa faiblesse
secret	Mot de passe simple tiré du dictionnaire
Dupont	Nom de jeune fille de la mère de l'utilisateur
toyota	Marque d'une voiture
bob1967	Nom et année de naissance de l'utilisateur
Blueleaf23	Mots et chiffres simples

Mot de passe fort	Raison de sa force
b67n42d39c	Il combine des caractères alphanumériques.
12^h u4@1p7	Il combine des caractères alphanumériques, des symboles et comprend un espace.

# 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

```
Router(config)#service password-encryption
Router(config)#security password min-length 8
Router(config)#login block-for 120 attempts 3 within 60
Router(config)#line vty 0 4
Router(config-vty)#exec-timeout 10
Router(config-vty)#end
Router#show running-config
-
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 exec-timeout 10
 login
```

# Activer 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 vty inbound SSH.
- Le routeur est alors accessible à distance uniquement via le protocole SSH.



```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Étape 1 : configurez le nom de domaine IP.

Étape 2 : générez des clés secrètes unidirectionnelles.

Étape 3 : vérifiez ou créez l'entrée dans la base de données locale.

Étape 4 : activez les sessions SSH entrantes à l'aide des commandes VTY.



## Rubrique 11.2.5 : Sauvegarde et restauration des fichiers de configuration



# Systèmes de fichiers du routeur

- Le système de fichiers Cisco IOS autorise les opérations de lecture et d'écriture des systèmes de fichiers.
- Utilisez la commande **show file systems** pour répertorier tous les systèmes de fichiers disponibles.
- Ce cours s'intéresse principalement aux systèmes de fichiers **tftp**, **flash** et **nvr**am. L'image IOS amorçable est stockée sur le système de fichiers flash.
- Le système de fichiers Flash
  - Communément, il s'agit du système de fichiers le plus important dans un routeur Cisco.
  - Stocke habituellement l'image IOS.
  - Utilisez la commande **dir** pour répertorier le contenu du système de fichiers flash ou de tout autre système de fichiers.
- Le système de fichiers NVRAM
  - Stocke habituellement les fichiers de configuration.
  - La mémoire vive non volatile d'un IOS est généralement peu importante.

## Systèmes de fichiers

```
Router#show file systems
File Systems:

      Size (b)      Free (b)      Type  Flags  Prefixes
      -          -          -      -      -
      -          -          opaque rw  archive:
      -          -          opaque rw  system:
      -          -          opaque rw  tmpsys:
      -          -          opaque rw  null:
      -          -          network rw  tftp:
* 256487424      183234560      disk  rw  flash0: flash:#
      -          -          disk  rw  flash1:
      262136      254779      nvram  rw  nvram:
      -          -          opaque wo  syslog:
      -          -          opaque rw  xmodem:
      -          -          opaque rw  ymodem:
      -          -          network rw  rcp:
      -          -          network rw  http:
      -          -          network rw  ftp:
      -          -          network rw  scp:
      -          -          opaque ro  tar:
      -          -          network rw  https:
      -          -          opaque ro  cns:
```

## Flash

```
Router#dir
Directory of flash0:/

 1 -rw-      2903 Sep 7 2012 06:58:26 +00:00  cpconfig-
 2 -rw-    3000320 Sep 7 2012 06:58:40 +00:00  cpexpress.tar
 3 -rw-      1038 Sep 7 2012 06:58:52 +00:00  home.shtml
 4 -rw-     122880 Sep 7 2012 06:59:02 +00:00  home.tar
 5 -rw-    1697952 Sep 7 2012 06:59:20 +00:00  securedesktop-
 6 -rw-     415956 Sep 7 2012 06:59:34 +00:00  ios-3.1.1.45-k9.pkg
 7 -rw-    67998028 Sep 26 2012 17:32:14 +00:00  c1900-
  universalk9-
  mz.SPA.152-4.M1.bin

256487424 bytes total (183234560 bytes free)
```

# Systèmes de fichiers du commutateur

## Commutateur Cisco 2960

- Est similaire au système de fichiers du routeur.
- Le système de fichiers flash du commutateur Cisco 2960 prend en charge les fichiers de configuration, la copie et l'archivage (chargement et téléchargement) d'images logicielles.
- La commande utilisée sur le routeur pour afficher les systèmes de fichiers est la même sur le commutateur :  
**show file systems**

```
Switch# show file systems
File Systems:

      Size(b)      Free(b)      Type  Flags  Prefixes
*      32514048      20887552      flash  rw      flash:
      -            -            opaque  rw      vb:
      -            -            opaque  ro      bs:
      -            -            opaque  rw      system:
      -            -            opaque  rw      tmpsys:
      65536         48897         nvram   rw      nvram:
      -            -            opaque  ro      xmodem:
      -            -            opaque  ro      ymodem:
      -            -            opaque  rw      null:
      -            -            opaque  ro      tar:
      -            -            network  rw      tftp:
      -            -            network  rw      rcp:
      -            -            network  rw      http:
      -            -            network  rw      ftp:
      -            -            network  rw      scp:
      -            -            network  rw      https:
      -            -            opaque  ro      cns:
```

# Sauvegarde et restauration à l'aide de fichiers texte

## Sauvegarde de la configuration

- Vous pouvez enregistrer/archiver les fichiers de configuration dans un fichier texte.
- Avec Tera Term, la procédure est la suivante :

**Étape 1.** Dans le menu File (Fichier), cliquez sur **Log** (Journal).

**Étape 2.** Choisissez l'emplacement où vous souhaitez enregistrer le fichier. Tera Term commence à capturer le texte.

**Étape 3.** Le texte affiché dans la fenêtre du terminal est alors dirigé vers le fichier choisi.

**Étape 4.** Une fois la capture terminée, sélectionnez **Close** (Fermer) dans la fenêtre Tera Term:Log (Tera Term : Journal).

**Étape 5.** Affichez le fichier pour vérifier qu'aucun problème n'est survenu.

## Restauration de la configuration

- Il est possible de copier une configuration à partir d'un fichier vers un périphérique.
- IOS exécute, sous forme de commande, le texte collé dans une fenêtre de terminal.
- Le périphérique doit être configuré dans le mode de configuration globale.
- Avec Tera Term, la procédure est la suivante :

**Étape 1.** Dans le menu File (Fichier), cliquez sur **Send** (Envoyer).

**Étape 2.** Recherchez le fichier à copier sur le périphérique et cliquez sur **Open** (Ouvrir).

**Étape 3.** Tera Term colle alors le fichier dans le périphérique. Le texte contenu dans le fichier est appliqué sous forme de commandes dans l'environnement CLI et devient la configuration en cours du périphérique.

# Sauvegarde et restauration via TFTP

## Sauvegarde de la configuration en cours

**Étape 1.** Saisissez la commande **copy running-config tftp**.

Étape 2. Entrez l'adresse IP de l'hôte sur lequel le fichier de configuration sera stocké.

Étape 3. Entrez le nom à attribuer au fichier de configuration.

Étape 4. Appuyez sur Entrée pour confirmer chaque choix.

## Rétablissement de la configuration en cours

**Étape 1.** Saisissez la commande **copy tftp running-config**.

Étape 2. Saisissez l'adresse IP de l'hôte sur lequel le fichier de configuration est stocké.

Étape 3. Entrez le nom à attribuer au fichier de configuration.

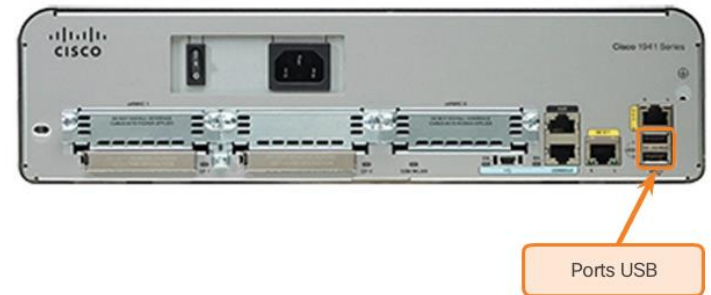
Étape 4. Appuyez sur Entrée pour confirmer chaque choix.

```
Router# copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm]
Writing tokyo.2 !!!!! [OK]
```

# Utilisation des ports USB d'un routeur Cisco

## Ports USB du routeur Cisco 1941

- Certains modèles de routeur Cisco prennent en charge les clés USB.
- La fonction Flash USB fournit une capacité de stockage secondaire en option et un périphérique d'amorçage supplémentaire.
- Elle peut stocker des images, des configurations et d'autres fichiers.
- La mémoire Flash USB présente l'avantage de pouvoir contenir plusieurs copies de Cisco IOS et plusieurs configurations de routeur.
- La commande **dir** permet de voir le contenu de la clé USB, comme indiqué dans l'illustration.



```
Router# dir usbflash0:
Directory of usbflash0:/
1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00
c3825-entservicesk9-mz.123-14.T
63158272 bytes total (33033216 bytes free)
```

# Sauvegarde et restauration sur une clé USB

## Sauvegarde des configurations sur une clé USB

- Confirmez la détection de la clé USB à l'aide de la commande **show file systems**.
- Utilisez la commande **copy run usbflash0:/** pour copier le fichier de configuration vers la clé USB.
- IOS vous invite à indiquer le nom du fichier.
- Utilisez la commande **dir** pour afficher le fichier sur la clé USB.

## Restauration des configurations à l'aide d'une clé USB

- En partant du principe que le nom de fichier est **R1-Config**, utilisez la commande **copy usbflash0:/R1-Config running-config** pour rétablir une configuration en cours.

```
R1# show file systems
File Systems:

      Size(b)      Free(b)      Type  Flags  Prefixes
      -          -          opaque  rw    archive:
      -          -          opaque  rw    system:
      -          -          opaque  rw    tmpsys:
      -          -          opaque  rw    null:
      -          -          network rw    tftp:
* 256487424      184819712      disk   rw    flash0: flash:#
      -          -          disk   rw    flash1:
      262136      249270      nvram  rw    nvram:
      -          -          opaque wo    syslog:
      -          -          opaque rw    xmodem:
      -          -          opaque rw    ymodem:
      -          -          network rw    rcp:
      -          -          network rw    http:
      -          -          network rw    ftp:
      -          -          network rw    scp:
      -          -          opaque ro    tar:
      -          -          network rw    https:
      -          -          opaque ro    cns:
4050042880      3774152704  usbflash  rw    usbflash0:
```

Affiche le port USB et le nom : « usbflash0: ».

# Section 11.3 :

## Performances réseau de base

À la fin de cette section, vous saurez :

- Utiliser les résultats de la commande ping pour déterminer les performances relatives du réseau
- Utiliser les résultats de la commande tracer 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



## Rubrique 11.3.1 : Commande ping



# Interprétation des résultats de requête ping

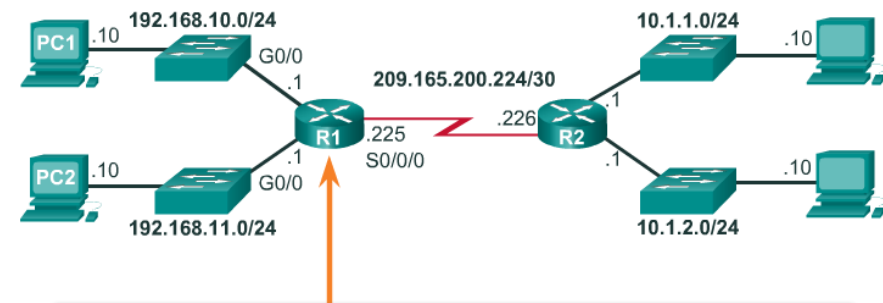
## Indicateurs IOS de la commande ping

- L'utilisation de la commande **ping** constitue un moyen efficace de tester la connectivité.
- Utilisez le protocole ICMP (Internet Control Message Protocol) pour vérifier la connectivité de la couche 3.
- La commande **ping** peut vous aider à identifier la source du problème.
- Une commande ping émise par l'IOS génère une indication pour chaque requête écho ICMP envoyée. Les indicateurs employés le plus souvent par IOS sont les suivants :
  - **!** – indique la réception d'une réponse d'écho ICMP.
  - **.** – indique l'expiration du délai pendant l'attente d'une réponse d'écho ICMP.
  - **U** – indique la réception d'un message ICMP d'inaccessibilité.

# Interprétation des résultats de requête ping (suite)

## Indicateurs IOS de la commande ping

- Le point (.). Il peut par exemple indiquer qu'un problème de connectivité a été rencontré sur le chemin parcouru. Plusieurs raisons expliquent la présence de cet indicateur :
  - Un routeur situé sur le chemin ne possède pas de route vers la destination.
  - La requête ping a été bloquée par la sécurité d'un périphérique.
  - La requête ping a expiré avant la réception de la réponse d'un autre protocole (ARP, par exemple).
- L'indicateur **U** signifie qu'un routeur situé sur le chemin a répondu par un message ICMP de non-accessibilité. Le routeur n'a pas trouvé d'itinéraire jusqu'à l'adresse de destination, ou la requête ping a été bloquée.



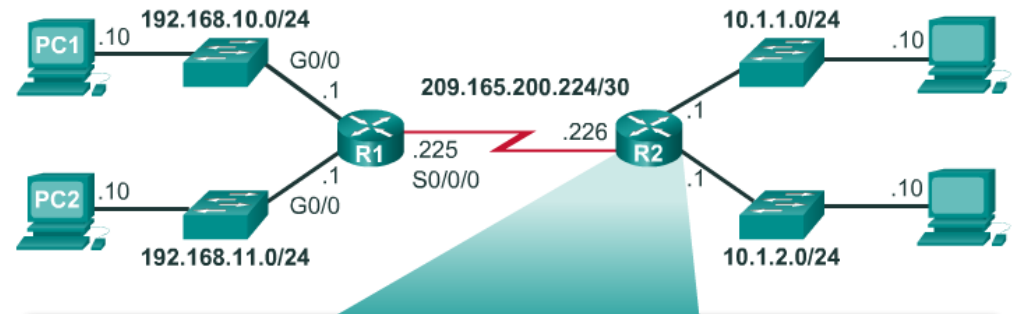
```
R1# ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout
is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
3/3/4 ms

R1#
```

# Extensions de la commande ping

- Cisco IOS propose un mode « étendu » de la commande ping.
- Pour entrer dans ce mode, saisissez **ping** en mode d'exécution privilégié sans spécifier l'adresse IP de destination.
- Une série d'invites vous est présentée.
- Il suffit d'appuyer sur Entrée pour accepter les valeurs par défaut indiquées.



```
R2# ping
Protocol [ip]:
Target IP address: 192.168.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
```

# Performances de référence du réseau

- Le profil de référence des performances d'un réseau est un outil très important.
- Établir un profil de référence efficace pour les performances du réseau prend un certain temps.
- Les résultats fournis par certaines commandes réseau permettent de recueillir des données qui feront partie de la ligne de base du réseau.
- Pour créer le profil de référence du réseau, vous pouvez copier et coller, dans un fichier texte, les résultats d'une commande, telle que ping, trace, etc.
- Ces fichiers texte sont éventuellement horodatés pour pouvoir les comparer par la suite.
- 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.
- Par exemple, un accroissement considérable des temps de réponse peut dénoter un problème de latence.

8 fév 2013 08:14:43

```
C:\>ping 10.66.254.159
```

```
Pinging 10.66.254.159 with 32 bytes of data:
```

```
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 10.66.254.159:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

17 mars 2013 14:41:06

```
C:\>ping 10.66.254.159
```

```
Pinging 10.66.254.159 with 32 bytes of data:
```

```
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
```

```
Ping statistics for 10.66.254.159:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

## Rubrique 11.3.2 : Commandes traceroute et tracert



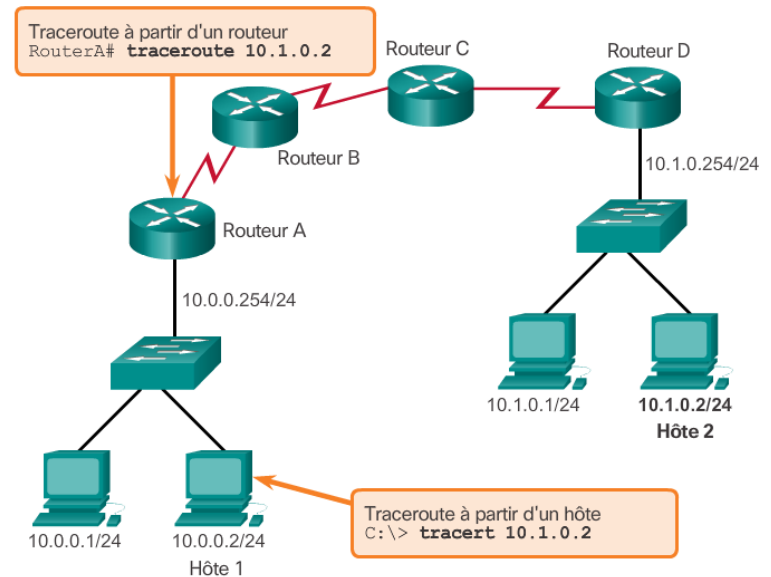
# Interprétation des messages trace

- Cette commande renvoie une liste des sauts effectués par un paquet acheminé à travers un réseau.
- La forme de cette commande dépend de la plate-forme.
- Utilisez la commande **tracert** pour les systèmes Windows et la commande **traceroute** pour les systèmes Cisco IOS et UNIX.

Traçage de l'itinéraire entre l'hôte 1 et l'hôte 2

## Test du chemin vers un hôte distant

```
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:\>
```



## Rubrique 11.3.3 : Commandes show





# Révision des commandes show courantes

- Les commandes **show** de la CLI de 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 périphériques et à consulter l'état de fonctionnement du périphérique.
- 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 notamment :
  - **show running-config**
  - **show interfaces**
  - **show arp**
  - **show ip route**
  - **show protocols**
  - **show version**

```
R1# show running-config
<Résultat omis>
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$dvdpm6zv10E6tSyLdkR5/
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
```

```
!
interface Serial0/0/0
 description WAN link to R2
 ip address 192.168.2.1 255.255.255.0
 encapsulation ppp
 clock rate 64000
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
!
router rip
 version 2
 network 192.168.1.0
 network 192.168.2.0
!
banner motd ^CUnauthorized Access Prohibited^C
!
ip http server
!
```

## Rubrique 11.3.4 : Commandes hôtes et IOS



## ipconfig

# Commande ipconfig

- La commande **ipconfig** peut servir à afficher des informations IP sur un ordinateur Windows.
- La commande **ipconfig** affiche l'hôte et ses adresses IP de passerelle par défaut.
- Utilisez la commande **ipconfig /all** pour afficher les détails de la configuration IP de l'hôte, notamment son adresse MAC.
- La commande **ipconfig /displaydns** affiche toutes les entrées DNS mises en cache sur un système Windows.




```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254
```

### Légende

-  Adresse IP de cet ordinateur hôte
-  Masque de sous-réseau du réseau local
-  Adresse de la passerelle par défaut de cet ordinateur hôte

## ipconfig /all

```
C:\>ipconfig /all

Ethernet adapter Network Connection:

    Connection-specific DNS Suffix: example.com
    Description . . . . . : Intel(R)
    PRO/Wireless 3945ABG Network Connection
    Physical Address. . . . . : 00-18-DE-C7-F3-FB
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 10.2.3.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.2.3.254
    DHCP Server . . . . . : 10.2.3.69
    DNS Servers . . . . . : 192.168.226.120
    Lease Obtained. . . . . : Thursday, May 03,
                             2007 3:47:51 PM
    Lease Expires . . . . . : Friday, May 04,
                             2007 6:57:11 AM

C:\>
```

# Commande ipconfig (suite)

ipconfig /displaydns

```
C:\> ipconfig /displaydns
```

```
Windows IP Configuration
```

```
cisco-tags.cisco.com
```

```
-----
```

```
Record Name . . . . . : cisco-tags.cisco.com
```

```
Record Type . . . . . : 1
```

```
Time To Live . . . . . : 44024
```

```
Data Length . . . . . : 4
```

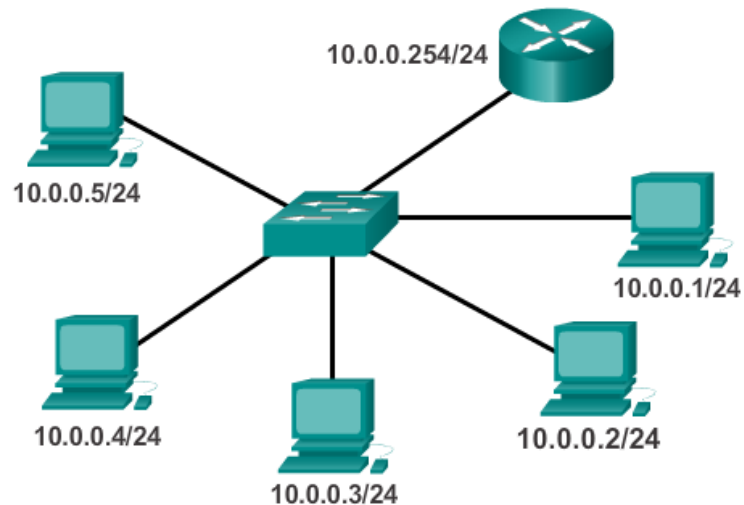
```
Section . . . . . : Answer
```

```
A (Host) Record . . . : 72.163.10.10
```

```
<résultat omis>
```

# Commande arp

- La commande **arp -a** répertorie tous les périphériques actuellement présents dans le cache ARP de l'hôte.
- Elle répertorie aussi l'adresse IPv4, l'adresse physique et le type d'adressage (statique ou dynamique) de chaque périphérique.
- Le cache peut être vidé à l'aide de la commande **arp -d**.



```
c:\>arp -a
Internet Address Physical Address Type
10.0.0.2          00-08-a3-b6-ce-04 dynamic
10.0.0.3          00-0d-56-09-fb-d1 dynamic
10.0.0.4          00-12-3f-d4-6d-1b dynamic
10.0.0.254       00-10-7b-e7-fa-ef dynamic
```

Paire d'adresses  
IP/MAC

# Commande show cdp neighbors

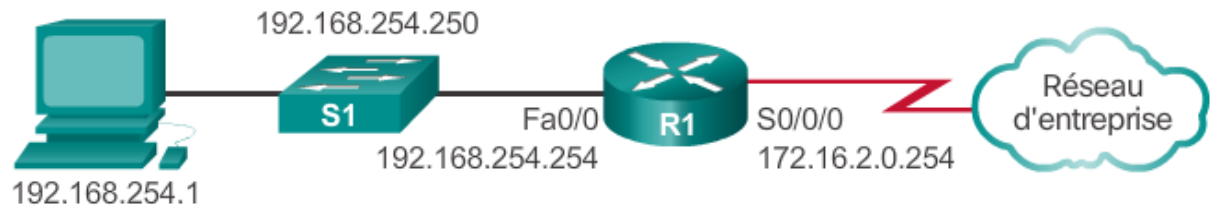
- CDP est un protocole propriétaire de Cisco qui s'exécute au niveau de la couche liaison de données.
- Deux périphériques réseau Cisco ou plus peuvent échanger des informations sur l'un et l'autre même si la connectivité de la couche 3 n'existe pas.
- Lorsqu'un périphérique Cisco démarre, le protocole CDP est par défaut activé.
- Le protocole CDP échange des informations sur les périphériques matériels et logiciels avec ses voisins CDP connectés directement.
- Le protocole CDP fournit les informations suivantes :
  - Identificateurs de périphériques
  - Liste d'adresses
  - Identifiant de port
  - Liste des capacités
  - Plate-forme

## Commande show cdp neighbors (suite)

- La commande **show cdp neighbors detail** indique l'adresse IP d'un périphérique voisin.
- Le protocole CDP révèle l'adresse IP du voisin, que vous puissiez lui envoyer ou non une requête ping.
- La commande **show cdp neighbors detail** permet de déterminer si l'un des voisins CDP présente une erreur de configuration IP.
- 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**.

# Commande show ip interface brief

- La commande **show ip interface brief** affiche un résumé des informations clés pour toutes les interfaces réseau d'un routeur.
- La commande **show ip interface brief** peut également servir à vérifier l'état des interfaces du commutateur.



```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.254.254	YES	NVRAM	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
Serial0/0/0	172.16.0.254	YES	NVRAM	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down

```
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	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	up	up



# Section 11.4 :

## Résumé

Objectifs du chapitre :

- 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
- Expliquer comment créer, configurer et vérifier un petit réseau de segments connectés directement

Merci.



Cisco Networking Academy  
Mind Wide Open